≡

WINDOWS SERVER 2016 HARDENING CHECKLIST

The hardening checklists are based on the comprehensive checklists produced by the Center for Internet Security (CIS). The Information Security Office (http://security.utexas.edu/) (http://security.utexas.edu/)(ISO) has distilled the CIS lists down to the most critical steps for your systems, with a focus on issues unique to the computing environment at The University of Texas at Austin.

How to Use the Checklist

Print the checklist and check off each item you complete to ensure that you cover the critical steps for securing your server. The ISO uses this checklist during risk assessments as part of the process to verify server security.

Server Information

MAC Address	
IP Address	
Machine Name	

Asset Tag	
Administrator Name	
Date	

Checklist

Step - The step number in the procedure. If there is a **UT Note** for this step, the note number corresponds to th
Check (√) - This is for administrators to check off when she/he completes this portion.
To Do - Basic instructions on what to do to harden the respective system
CIS - Reference number in the Center for Internet Security Windows Server 2016 Benchmark v1.0.0 (https://utex
much greater detail how to complete each step.
UT Note - The **UT Note** at the bottom of the page provides additional detail about the step for the university co
Confidential - For systems that include Confidential data (http://security.utexas.edu/policies/data_classification
Other - For systems that include Controlled or Published data (http://security.utexas.edu/policies/data_classifica
Min Std - This column links to the specific requirement for the university in the Minimum Security Standards for

Step	√	To Do	CIS	UT Note	Confidential
		Preparation and Installation			
1		If machine is a new install, protect it from hostile network traffic, until the operating system is installed and hardened.		§	!
		Service Packs and Hotfixes			
2		Install the latest service packs and hotfixes from Microsoft.		§	!
3		Enable automatic notification of patch availability.		§	!
		User Account Policies			
4		Set minimum password length.	1.1.4	§	!
5		Enable password complexity requirements.	1.1.5	§	!
6		Do not store passwords using reversible encryption. (Default)	1.1.6	§	!
7		Configure account lockout policy.	1.2	§	!
		User Rights Assignment			

Step	√	To Do	CIS	UT Note	Confidential
8		Restrict the ability to access this computer from the network to Administrators and Authenticated Users.	2.2.2		
9		Do not grant any users the 'act as part of the operating system' right. (Default)	2.2.3		!
10		Restrict local logon access to Administrators.	2.2.6	§	
11		Deny guest accounts the ability to logon as a service, a batch job, locally, or via RDP.	2.2.18-21		!
		Security Settings			
12		Place the University warning banner in the Message Text for users attempting to log on.	2.3.7.4	§	!
13		Disallow users from creating and logging in with Microsoft accounts.	2.3.1.2	§	!
14		Disable the guest account. (Default)	2.3.1.3		!
15		Require Ctrl+Alt+Del for interactive logins. (Default)	2.3.7.2		!
16		Configure machine inactivity limit to protect idle interactive sessions.	2.3.7.3		!
17		Configure Microsoft Network Client to always digitally sign communications.	2.3.8.1		!
18		Configure Microsoft Network Client to digitally sign communications if server agrees. (Default)	2.3.8.2		!
19		Disable the sending of unencrypted passwords to third party SMB servers.	2.3.8.3		!
20		Configure Microsoft Network Server to always digitally sign communications.	2.3.9.2		!
21		Configure Microsoft Network Server to digitally sign communications if client agrees.	2.3.9.3		!
		Network Access Controls			
22		Disable anonymous SID/Name translation. (Default)	2.3.10.1		!
23		Do not allow anonymous enumeration of SAM accounts. (Default)	2.3.10.2		!

Step	√	To Do	CIS	UT Note	Confidential
24		Do not allow anonymous enumeration of SAM accounts and shares.	2.3.10.3		!
25		Do not allow everyone permissions to apply to anonymous users. (Default)	2.3.10.5		!
26		Do not allow any named pipes to be accessed anonymously.	2.3.10.6		!
27		Restrict anonymous access to named pipes and shares. (Default)	2.3.10.9		!
28		Do not allow any shares to be accessed anonymously.	2.3.10.11		!
29		Require the "Classic" sharing and security model for local accounts. (Default)	2.3.10.12		!
		Network Security Settings			
30		Allow Local System to use computer identity for NTLM.	2.3.11.1		
31		Disable Local System NULL session fallback.	2.3.11.2		
32		Configure allowable encryption types for Kerberos.	2.3.11.4		
33		Do not store LAN Manager hash values.	2.3.11.5		!
34		Set LAN Manager authentication level to only allow NTLMv2 and refuse LM and NTLM.	2.3.11.7		!
35		Enable the Windows Firewall in all profiles (domain, private, public). (Default)	9.{{1-3}}.1		!
36		Configure the Windows Firewall in all profiles to block inbound traffic by default. (Default)	9.{{1-3}}.2		!
37		Configure Windows Firewall to restrict remote access services (VNC, RDP, etc.) to authorized campus-only networks .			
38		Configure Windows Firewall to restrict remote access services (VNC, RDP, etc.) to the campus VPN.			!
		Active Directory Domain Member Security Settings			
39		Digitally encrypt or sign secure channel data (always). (Default)	2.3.6.1		!

Step	✓	To Do	CIS	UT Note	Confidential
40		Digitally encrypt secure channel data (when possible). (Default)	2.3.6.2		!
41		Digitally sign secure channel data (when possible). (Default)	2.3.6.3		!
42		Require strong (Windows 2000 or later) session keys.	2.3.6.6		!
43		Configure the number of previous logons to cache.	2.3.7.6	§	
		Audit Policy Settings			
44		Configure Account Logon audit policy.	17.1	§	!
45		Configure Account Management audit policy.	17.2	§	!
46		Configure Logon/Logoff audit policy.	17.5	§	!
47		Configure Policy Change audit policy.	17.7	§	!
48		Configure Privilege Use audit policy.	17.8	§	!
		Event Log Settings			
49		Configure Event Log retention method and size.	18.3.12; 18.9.26	§	!
50		Configure log shipping (e.g. to Splunk (https://ut.service-now.com/utss/catalogoverview.do?sysparam_citems_id=2bc53c004f8f924031eb7bcd0210c772)).		§	
		Linux Subsystem			
51		Configure all Linux elements according to the Linux Hardening Guide (https://security.utexas.edu/os-hardening-checklist/linux-7), keeping in mind that some elements will require Windows tools (like Windows Firewall vs. iptables)			
		Additional Security Protection			
52		Disable or uninstall unused services.			!
53		Disable or delete unused users.			!
54		Configure user rights to be as secure as possible: Follow the Principle of Least Privilege (https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models)		§	!

Step	✓	To Do	CIS	UT Note	Confidential
55		Ensure all volumes are using the NTFS file system.		§	!
56		Configure file system permissions.		§	!
57		Configure registry permissions.		§	!
58		Disallow remote registry access if not required.	2.3.10.7-8	§	
		Additional Steps			
59		Set the system date/time and configure it to synchronize against campus time servers.		§	!
60		Install and enable anti-virus software.		§	!
61		Install and enable anti-spyware software.		§	!
62		Configure anti-virus software to update daily.		§	!
63		Configure anti-spyware software to update daily.		§	!
64		Provide secure storage for Confidential (category-I) Data as required. Security can be provided by means such as, but not limited to, encryption, access controls, filesystem audits, physically securing the storage media, or any combination thereof as deemed appropriate.		§	!
65		Install software to check the integrity of critical operating system files.		§	!
66		If RDP is utilized, set RDP connection encryption level to high.		§	!
		Physical Security			
67		Unless the server is in the UDC or a managed VM cluster, set a BIOS/firmware password to prevent alterations in system start up settings.			
68		Do not allow the system to be shut down without having to log on. (Default)	2.3.13.1		!
69		Configure the device boot order to prevent unauthorized booting from alternate media.			!
70		Configure a screen-saver to lock the console's screen automatically if the host is left unattended.		§	!

UT Addendum

This list provides specific tasks related to the computing environment at The University of Texas at Austin.

1 If other alternatives are unavailable, this can be accomplished by installing a SOHO router/firewall in betw

2 There are several methods available to assist you in applying patches in a timely fashion:

Microsoft Update Service

- Microsoft Update (http://www.update.microsoft.com/)checks your machine to identify missing patc
- This is different than the "Windows Update" that is the default on Windows. Microsoft Update inclu
- This service is compatible with Internet Explorer only.

Windows AutoUpdate via WSUS
ITS offers a Windows Server Update Services Server for campus use (https://ut.service-now.com/utss/cat sysparam_citems_id=e546bc004f8f924031eb7bcd0210c7b5&sysparam_cat_id=e0d08b13c3330100c8b837 Microsoft's own update servers. It includes updates for additional Microsoft products, just like Microsoft U

Microsoft Baseline Security Analyzer
This is a free host-based application that is available to download from Microsoft (http://technet.microsof issues found.

Upguard
This is a compliance management tool that ensures basic patching and compliance is being consistently r sysparam_citems_id=2bc53c004f8f924031eb7bcd0210c772)).

3 Configure Automatic Updates from the Automatic Updates control panel

- On most servers, you should choose either "Download updates for me, but let me choose when to
- The campus Windows Server Update Services server (https://ut.service-now.com/utss/catalogoverv sysparam_citems_id=e546bc004f8f924031eb7bcd0210c7b5&sysparam_cat_id=e0d08b13c3330100c be used as the source of automatic updates.

4 Configuring the minimum password length settings is important only if another method of ensuring comp characters in length. It is **strongly** recommended that passwords be at least 14 characters in length (whic

5	Configuring the password complexity setting is important only if another method of ensuring compliance special characters. Ensure Domain Administrators (and even Departmental/GPO Admin accounts used by TSCs) have a highe Austin AD context.
6	If this option is enabled, the system will store passwords using a weak form of encryption that is susceptil For further password protections: 1. Update Active Directory functional level to 2012 R2 or higher. 2. In Registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\WDigest, s 3. Implement MS KBs 2928120 (https://support.microsoft.com/en-us/help/2928120/ms14-025-descriptior
7	Instead of the CIS recommended values, the account lockout policy should be configured as follows: • Account lockout duration — 5 minutes • Account lockout threshold — 5 failed attempts • Reset account lockout counter — 5 minutes
10	Any account with this role is permitted to log in to the console. By default, this includes users in the Admi this right may facilitate a compromise of the device.
12	The text of the university's official warning banner (http://security.utexas.edu/policies/login_banner.html
13	The use of Microsoft accounts can be blocked by configuring the group policy object at: **Computer Configuration\Windows Settings\Security Settings\Local Policies\ Security Options\Accounts: Block Microsoft accounts** This setting can be verified by auditing the registry key: **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\NoConnect**

43	Logon information for domain accounts can be cached locally to allow users who have previously authent .ocate the cached credentials and use a brute force attack to discover the passwords. Therefore, it is reco frequently by multiple users. The group policy object below should be set to 4 or fewer logins: **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Inter**
44	The Account Logon audit policy logs the results of validation tests of credentials submitted for user accou accounts. Configure the group policy object below to match the listed audit settings: **Computer Configuration\Windows Settings\Security Settings\ Advanced Audit Policy Configuration\Audit Policies\Account Logon\** • Credential Validation — Success and Failure
45	Configure the group policy object below to match the listed audit settings: **Computer Configuration\Windows Settings\Security Settings\ Advanced Audit Policy Configuration\Audit Policies\Account Management\** • Computer Account Management — Success and Failure • Other Account Management Events — Success and Failures • Security Group Management — Success and Failure • User Account Management — Success and Failure
46	Configure the group policy object below to match the listed audit settings: **Computer Configuration\Windows Settings\Security Settings\ Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\** • Account Lockout — Success • Logoff — Success • Logon — Success and Failure • Other Logon/Logoff Events — Success and Failure • Special Logon — Success

47 Configure the group policy object below to match the listed audit settings:

**Computer Configuration\Windows Settings\Security Settings\
Advanced Audit Policy Configuration\Audit Policies\Policy Change**

- Audit Policy Change — Success and Failure
- Authentication Policy Change — Success

48 Configure the group policy object below to match the listed audit settings:

Computer Configuration\Windows Settings\Security Settings\
Advanced Audit Policy Configuration\Audit Policies\Privilege Use\

- Sensitive Privilege Use — Success and Failure

49 The university requires the following event log settings instead of those recommended by the CIS Benchn

- Application: Maximum log size — **163,840 KB**
- Security: Maximum log size — **983,040 KB**
- Setup: Maximum log size — **163,840 KB**
- System: Maximum log size — **163,840 KB**

The recommended retention method for all logs is: **Retain events for at least 14 days**

These are minimum requirements. The most important log here is the security log. 1 GB is a suggested m
will be to respond in the event of a breach. In rare cases, a breach may go on for months before detectior

Note that if the event log reaches its maximum size and no events older than the number of days you spe
critical services working with Confidential or other sensitive data, use Syslog, Splunk (https://ut.service-no
Windows to rotate event log files automatically when an event log reaches its maximum size as described
AutoBackupLogFiles registry entry.

50 It is highly recommended that logs are shipped from any Confidential cdevices to a service like Splunk (ht
events among many other things. This helps to ensure that logs are preserved and unaltered in the event
Splunk licenses are available through ITS at no charge. ITS also maintains a centrally-managed Splunk ser
If using Splunk:
Ensure all key systems and services are logging to Splunk and that verbosity is appropriately set. Ensure S

54 Configure user rights to be as secure as possible, following the recommendations in section 2.2 of the CIS
the System User. Ensure scheduled tasks are run with a dedicated Service account and not a Domain Adm
access/privileged-access-workstations) and ensure system logs are routed to Splunk (https://ut.service-nc

55	Volumes formatted as FAT or FAT32 can be converted to NTFS, by using the convert.exe utility provided b NTFS file system for all partitions where Category I data is to be stored.
56	**Be extremely careful, as setting incorrect permissions on system files and folders can render a sys**
57	**Be extremely careful, as setting incorrect permissions on registry entries can render a system unu**
58	Some remote administration tools, such as Microsoft Systems Management Server, require remote regist service be stopped and disabled. If remote registry access is required, the remotely accessible registry paths should still be configured to b **Computer Configuration\Windows Settings\Security Settings\Local Policies\ Security Options\Network access: Remotely accessible registry paths** This object should be set to allow access only to: • System\CurrentControlSet\Control\ProductOptions • System\CurrentControlSet\Control\Server Applications • Software\Microsoft\Windows NT\CurrentVersion Further restrictions on the registry paths and subpaths that are remotely accessible can be configured wi **Computer Configuration\Windows Settings\Security Settings\Local Policies\ Security Options\Network access: Remotely accessible registry paths and sub-paths**
59	By default, domain members synchronize their time with domain controllers using Microsoft's Windows T synchronize its time with an external time source, such as the university's network time servers.
60	ITS provides FireAMP, a managed, cloud-based antivirus service, free of charge for all university owned de
61	Anti-spyware software is only required to be installed if the server is used to browse Web sites not specifi be installed. We also recommend the installation of a secondary anti-spyware application, such as SpyWa An additional measure that can be taken is to install Firefox (http://www.mozilla.com/en-US/firefox/perso
62	FireAMP is the recommended AV solution.

63 **Spyware Blaster** - Enabling auto-update functionality requires the purchase of an additional subscriptior
SpyBot Search and Destroy - Automatic update tasks can be created inside the program itself and are sc

1. In the Spybot Application, click on Mode --> Advanced View.
2. Click Settings on the left hand side of the window.
3. You should now see an option labeled "Scheduler." Select that option.
4. Adding the task to update automatically is relatively straightforward.
    - Click **Add** to create a task.
    - Click **Edit** to edit the task schedule.
    - In the Scheduled Task window that pops up, enter the following In the **Run** field:

        - **C:\Program Files\Spybot - Search & Destroy\SpybotSD.exe" /AUTOUPDATE /TASKB**

    - Click the **Schedule** tab and choose a time for it to update. The duration of the update is very

64 Windows provides the Encrypting File System as a built-in mechanism to allow the encryption of individua
(http://www.gnupg.org/) also exist.

Another encryption option to consider is whole-disk encryption, which encrypts the entire contents of the

If encryption is being used in conjunction with Confidential data, one of the solutions listed in the Approv

65 Windows has a feature called Windows Resource Protection which automatically checks certain key files a

You can audit in much more in depth using Tripwire; consider this for your highest-risk systems. Modern

66 This setting is configured by group policy object at:

\Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Servi

This policy object should be configured as below:

- Set client connection encryption level — High
- Require use of specific security layer for remote (RDP) connections — SSL (TLS 1.0)
- Require user authentication for remote connections by using Network Level Authentication — Enab

70	1. Open the Display Properties control panel. 2. Select the Screen Saver tab. 3. Select a screen saver from the list. Although there are several available, consider using a simple one 4. The value for **Wait** should be no more than 15 minutes. 5. Select the **On resume, password protect** option.

(https://www.facebook.com/UTAustinISO)(https://twitter.com/ut_iso)(https://www.instagram.com/ut_iso/)

INFORMATION SECURITY OFFICE

Privacy Policy (https://www.utexas.edu/web-privacy-policy) | **Accessibility Policy** (https://www.utexas.edu/web-accessibility-policy)

(https://www.utexas.edu/)