Jacen R Kohler

Universit of North Texas

Windows Server 2012 Playbook

Table of Contents

[Quick Checklist First Things ToDo 5](#_Toc474757774)

[Security 5](#_Toc474757775)

[Accounts 5](#_Toc474757776)

[Updates 5](#_Toc474757777)

[Use Security Configuration Wizard 5](#_Toc474757778)

[Network security 5](#_Toc474757779)

[Network access 5](#_Toc474757780)

[Interactive logon 5](#_Toc474757781)

[Audit 5](#_Toc474757782)

[User Rights Assignment 5](#_Toc474757783)

[Local GOPs 5](#_Toc474757784)

[Other 5](#_Toc474757785)

[Complete Checklist 7](#_Toc474757786)

[Updates 7](#_Toc474757787)

[User Account Policies 7](#_Toc474757788)

[Set Minimum Password Length 7](#_Toc474757789)

[Enable Password Complexity Requirements 7](#_Toc474757790)

[Do not store passwords using reversible encryption. (Default) 7](#_Toc474757791)

[Configure account lockout policy 7](#_Toc474757792)

[User Rights Assignment Restrict the ability to access this computer from the network to Administrators 7](#_Toc474757793)

[Do not grant any users the 'act as part of the operating system' right (Default) 7](#_Toc474757794)

[Restrict local logon access to Administrators 7](#_Toc474757795)

[Deny guest accounts the ability to logon as a service, a batch job, locally, or via RDP 7](#_Toc474757796)

[Security Settings 7](#_Toc474757797)

[Place the warning banner in the Message Text for users attempting to log on 7](#_Toc474757798)

[Disallow users from creating and logging in with Microsoft accounts 7](#_Toc474757799)

[Disable the guest account (Default) 8](#_Toc474757800)

[Require Ctrl+Alt+Del for interactive logins (Default) 8](#_Toc474757801)

[Configure machine inactivity limit to protect idle interactive sessions 8](#_Toc474757802)

[Configure Microsoft Network Client to always digitally sign communications 8](#_Toc474757803)

[Configure Microsoft Network Client to digitally sign communications if server agrees (Default) 8](#_Toc474757804)

[Disable the sending of unencrypted passwords to third party SMB servers 8](#_Toc474757805)

[Configure Microsoft Network Server to always digitally sign communications 8](#_Toc474757806)

[Configure Microsoft Network Server to digitally sign communications if client agrees 8](#_Toc474757807)

[Network Access Controls 8](#_Toc474757808)

[Disable anonymous SID/Name translation (Default) 8](#_Toc474757809)

[Do not allow anonymous enumeration of SAM accounts (Default) 8](#_Toc474757810)

[Do not allow anonymous enumeration of SAM accounts and shares 8](#_Toc474757811)

[Do not allow Everyone permissions to apply to anonymous users (Default) 8](#_Toc474757812)

[Do not allow any named pipes to be accessed anonymously 8](#_Toc474757813)

[Restrict anonymous access to named pipes and shares (Default) 8](#_Toc474757814)

[Do not allow any shares to be accessed anonymously 8](#_Toc474757815)

[Require the "Classic" sharing and security model for local accounts (Default) 8](#_Toc474757816)

[Network Security Settings 8](#_Toc474757817)

[Allow Local System to use computer identity for NTLM 8](#_Toc474757818)

[Disable Local System NULL session fallback 8](#_Toc474757819)

[Configure allowable encryption types for Kerberos 8](#_Toc474757820)

[Do not store LAN Manager hash values 8](#_Toc474757821)

[Set LAN Manager authentication level to only allow NTLMv2 and refuse LM and NTLM. 8](#_Toc474757822)

[Enable the Windows Firewall in all profiles (domain, private, public) (Default) 8](#_Toc474757823)

[Configure the Windows Firewall in all profiles to block inbound traffic by default (Default) 8](#_Toc474757824)

[Active Directory Domain Member Security Settings 8](#_Toc474757825)

[Digitally encrypt or sign secure channel data (always) (Default) 8](#_Toc474757826)

[Digitally encrypt secure channel data (when possible) (Default) 8](#_Toc474757827)

[Digitally sign secure channel data (when possible) (Default) 8](#_Toc474757828)

[Require strong (Windows 2000 or later) session keys 8](#_Toc474757829)

[Configure the number of previous logons to cache 8](#_Toc474757830)

[Run Microsoft’s Domain Controller Diagnostics 9](#_Toc474757831)

[Check your backups 9](#_Toc474757832)

[Check to make sure that AD replication is working correctly. 9](#_Toc474757833)

[Allow only secure dynamic updates for all DNS zones. 9](#_Toc474757834)

[Audit Policy Settings 9](#_Toc474757835)

[Configure Account Logon audit policy 9](#_Toc474757836)

[Configure Account Management audit policy 9](#_Toc474757837)

[Configure Logon/Logoff audit policy 9](#_Toc474757838)

[Configure Policy Change audit policy 10](#_Toc474757839)

[Configure Privilege Use audit policy 10](#_Toc474757840)

[Event Log Settings 10](#_Toc474757841)

[Configure Event Log retention method and size 10](#_Toc474757842)

[Configure log shipping (e.g. to Splunk) 10](#_Toc474757843)

[Additional Security Protection 11](#_Toc474757844)

[Disable or uninstall unused services 11](#_Toc474757845)

[Disable or delete unused users 11](#_Toc474757846)

[Configure User Rights to be as secure as possible 11](#_Toc474757847)

[Ensure all volumes are using the NTFS file system 11](#_Toc474757848)

[Configure file system permissions 11](#_Toc474757849)

[Configure registry permissions 11](#_Toc474757850)

[Disallow remote registry access if not required 11](#_Toc474757851)

[Additional Steps 11](#_Toc474757852)

[Set the system date/time and configure it to synchronize against campus time servers 11](#_Toc474757853)

[Install and enable anti-virus software 12](#_Toc474757854)

[Install and enable anti-spyware software 12](#_Toc474757855)

[Configure anti-virus software to update daily 12](#_Toc474757856)

[Configure anti-spyware software to update daily 12](#_Toc474757857)

[Provide secure storage for data 12](#_Toc474757858)

[Install software to check the integrity of critical operating system files 12](#_Toc474757859)

[If RDP is utilized, set RDP connection encryption level to high 12](#_Toc474757860)

[Physical Security 13](#_Toc474757861)

[Set a BIOS/firmware password to prevent alterations in system start up settings 13](#_Toc474757862)

[Disable automatic administrative logon to recovery console 13](#_Toc474757863)

[Do not allow the system to be shut down without having to log on (Default) 13](#_Toc474757864)

[Configure the device boot order to prevent unauthorized booting from alternate media 13](#_Toc474757865)

[Resources 13](#_Toc474757866)

# Quick Checklist First Things ToDo

## Security

### Accounts

#### Change Local admin password

(start -> right click on ‘computer’ -> ‘manage’ -> ‘Local Users and Groups’ -> ‘users’ -> right click on ‘administrator’ -> ‘change password’) OR ( in cmd.exe “net user administrator ‘type new password here”’)

#### Check for additional admin accounts

(start > admin tools > computer management > local users and groups > users)

#### Disable Guest

### Updates

MS10-025

MS09-050

MS08-069

MS08-067

MS03-026

### Use Security Configuration Wizard

The Security Configuration Wizard can greatly simplify the hardening of the server. Once the role for the host is defined, the Security Configuration Wizard can help create a system configuration based specifically on that role. It does not completely get rid of the need to make other configuration changes, though.

<https://technet.microsoft.com/en-us/library/cc754997.aspx>

GUI: Start->Administrative Tools->Security Configuration Wizard  
CMD: scwcmd

### Network security

LAN Manager authentication level - Send NTLMv2 response only\refuse NTLM & LM

Do not store LAN Manager hash value on next password change – Enabled

### Network access

Do not allow anonymous enumeration of SAM accounts and shares - Enabled

Do not allow anonymous enumeration of SAM accounts - Enabled

Allow anonymous SID/name translation – Disabled

### Interactive logon

Message text for users attempting to log on - sometimes an inject

## Audit

Audit process tracking - Successes

Audit account management - Successes, Failures

Audit logon events - Successes, Failures

Audit account logon events - Successes, Failures

### User Rights Assignment

Debug programs - Remove all groups/users

Allow log on through Terminal Services - Leave blank to disallow login via TS even if it has been started.

### Local GOPs

Export a config from a VM or other default install for reference:

secedit /export /cfg checkme.inf

Edit to to have more secure settings then import onto your target system:

secedit /configure /db secedit.sdb /cfg securecheckme.inf

### Other

#### Disable RDP

Start->right click ‘my computer’->properties->remote settings->disable

‘select users’->remove all

#### Configure Microsoft Security Essentials

#### Remove Unnecessary Roles/Services

#### Disable IPv6

control panel->network and internet->change adapter settings->right click ‘properties’ on active NIC->uncheck ipv6

#### Microsoft Security Baseline Analyzer

#### Windows Firewall Configuration

control panel->windows firewall

#### Configure BitLocker

cmd.exe ‘-install BitLocker –restart’

#### Disable Shares

cmd.exe ‘net share’

# Complete Checklist

### Updates

MS10-025

MS09-050

MS08-069

MS08-067

MS03-026

## User Account Policies

Start->Run, gpedit.msc, click OK

Computer Configuration->Policies->Windows Settings->Security Settings->Account Policies->Password Policy

### Set Minimum Password Length

Configuring the minimum password length settings is important only if another method of ensuring compliance with [the company policy handbook](http://security.utexas.edu/policies/irusp.html#sec16)is not in place.

### Enable Password Complexity Requirements

Configuring the password complexity setting is important only if another method of ensuring compliance with company policy handbook is not in place.

### Do not store passwords using reversible encryption. (Default)

If this option is enabled, the system will store passwords using a weak form of encryption that is susceptible to compromise. This configuration is disabled by default.

### Configure account lockout policy

Account lockout duration — 5 minutes

Account lockout threshold — 5 failed attempts

Reset account lockout counter — 5 minutes

## User Rights Assignment Restrict the ability to access this computer from the network to Administrators

Any account with this role is permitted to log in to the console. By default, this includes users in the Administrators, Users, and Backup Operators groups. Remove all but Administrators

### Do not grant any users the 'act as part of the operating system' right (Default)

### Restrict local logon access to Administrators

Any account with this role is permitted to log in to the console. By default, this includes users in the Administrators, Users, and Backup Operators groups. It's unlikely that non-administrative users require this level of access and, in cases where the server is not physically secured, granting this right may facilitate a compromise of the device.

### Deny guest accounts the ability to logon as a service, a batch job, locally, or via RDP

## Security Settings

### Place the warning banner in the Message Text for users attempting to log on

### Disallow users from creating and logging in with Microsoft accounts

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\NoConnectedUser

### Disable the guest account (Default)

### Require Ctrl+Alt+Del for interactive logins (Default)

### Configure machine inactivity limit to protect idle interactive sessions

### Configure Microsoft Network Client to always digitally sign communications

### Configure Microsoft Network Client to digitally sign communications if server agrees (Default)

### Disable the sending of unencrypted passwords to third party SMB servers

### Configure Microsoft Network Server to always digitally sign communications

### Configure Microsoft Network Server to digitally sign communications if client agrees

## Network Access Controls

### Disable anonymous SID/Name translation (Default)

### Do not allow anonymous enumeration of SAM accounts (Default)

### Do not allow anonymous enumeration of SAM accounts and shares

### Do not allow Everyone permissions to apply to anonymous users (Default)

### Do not allow any named pipes to be accessed anonymously

### Restrict anonymous access to named pipes and shares (Default)

### Do not allow any shares to be accessed anonymously

### Require the "Classic" sharing and security model for local accounts (Default)

## Network Security Settings

### Allow Local System to use computer identity for NTLM

### Disable Local System NULL session fallback

### Configure allowable encryption types for Kerberos

### Do not store LAN Manager hash values

### Set LAN Manager authentication level to only allow NTLMv2 and refuse LM and NTLM.

### Enable the Windows Firewall in all profiles (domain, private, public) (Default)

### Configure the Windows Firewall in all profiles to block inbound traffic by default (Default)

## Active Directory Domain Member Security Settings

### Digitally encrypt or sign secure channel data (always) (Default)

### Digitally encrypt secure channel data (when possible) (Default)

### Digitally sign secure channel data (when possible) (Default)

### Require strong (Windows 2000 or later) session keys

### Configure the number of previous logons to cache

Logon information for domain accounts can be cached locally to allow users who have previously authenticated to do so again even if a domain controller cannot be contacted. By default 10 accounts will be cached locally, but there is a risk that in the event of a compromise an attacker could locate the cached credentials and use a brute force attack to discover the passwords. Therefore, it is recommended that this value be reduced so that fewer credentials will be placed at risk, and credentials will be cached for shorter periods of time in the case of devices that are logged into frequently by multiple users.

The group policy object below should be set to 0 or fewer logons:

Computer Configuration\Windows Settings\Security Settings\Local Policies\ Security Options\Interactive logon: Number of previous logons to cache (in case domain controller is not available)

### Run Microsoft’s Domain Controller Diagnostics

If the commands are unrecognized, install Windows Support Tools.

### Check your backups

AD backup includes capturing system state, information related to AD database, logs, registry, boot files, SYSVOL and other system files.

### Check to make sure that AD replication is working correctly.

To check, you can run the following command: repadmin /showrepl

### Allow only secure dynamic updates for all DNS zones.

This ensures that only authenticated users can submit DNS updates using a secure method, which helps prevent the IP addresses of trusted hosts from being hijacked by an attacker.

If the server running the DNS Server service is a domain controller, use AD ACLs to secure access control of the DNS Server service.

## Audit Policy Settings

### Configure Account Logon audit policy

The Account Logon audit policy logs the results of validation tests of credentials submitted for user account logon requests. The server that is authoritative for the credentials must have this audit policy enabled. For domain member machines, this policy will only log events for local user 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

### Configure Account Management audit policy

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

### Configure Logon/Logoff audit policy

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

### Configure Policy Change audit policy

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

### Configure Privilege Use audit policy

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

## Event Log Settings

### Configure Event Log retention method and size

The university requires the following event log settings instead of those recommended by the CIS Benchmark:

Application: Maximum log size — **32,768 KB**

Security: Maximum log size—**196,608 KB**

Setup: Maximum log size —**32,768 KB**

System: Maximum log size — **32,768 KB**

The recommended retention method for all logs is: **Overwrite events older than 14 days**

These are minimum requirements. The most important log here is the security log. 100 MB is a suggested minimum, but if you have a high-volume service, make the file as large as necessary to make sure at least 14 days of security logs are available. You may increase the number of days that you keep, or you may set the log files to not overwrite events.

Note that if the event log reaches its maximum size and no events older than the number of days you specified exist to be deleted, or if you have disabled overwriting of events, no new events will be logged. This may happen deliberately as an attempt by an attacker to cover his tracks. For critical services working with Cat 1 or other sensitive data, you should use syslog, Splunk, Intrust, or a similar service to ship logs to another device.

Another option is to configure Windows to rotate event log files automatically when an event log reaches its maximum size as described in the article <http://support.microsoft.com/kb/312571>using the the AutoBackupLogFiles registry entry.

### Configure log shipping (e.g. to Splunk)

It is highly recommended that logs are shipped from any devices to a service like Splunk, which provides log aggregation, processing, and real-time monitoring of events among many other things. This helps to ensure that logs are preserved and unaltered in the event of a compromise, in addition to allowing proactive log analysis of multiple devices.

Splunk licenses are available through ITS at no charge. ITS also maintains a centrally-managed Splunk service that may be leveraged.

## Additional Security Protection

### Disable or uninstall unused services

### Disable or delete unused users

### Configure User Rights to be as secure as possible

Configure user rights to be as secure as possible. Every attempt should be made to remove Guest, Everyone, and ANONYMOUS LOGON from the user rights lists.

### Ensure all volumes are using the NTFS file system

Volumes formatted as FAT or FAT32 can be converted to NTFS, by using the convert.exe utility provided by Microsoft. Microsoft has provided [instructions on how to perform the conversion.](http://support.microsoft.com/kb/314097)Windows servers used with Category I data must use the NTFS file system for all partitions where Category I data is to be stored.

### Configure file system permissions

**Be extremely careful, as setting incorrect permissions on system files and folders can render a system unusable.**

### Configure registry permissions

Be extremely careful, as setting incorrect permissions on registry entries can render a system unusable.

### Disallow remote registry access if not required

Some remote administration tools, such as Microsoft Systems Management Server, require remote registry access to managed devices. Disabling remote registry access may cause such services to fail. If remote registry access is not required, it is recommended that the remote registry service be stopped and disabled.

If remote registry access is required, the remotely accessible registry paths should still be configured to be as restrictive as possible. The group policy object below controls which registry paths are available remotely:

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 with the group policy object:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths and sub-paths

## Additional Steps

### Set the system date/time and configure it to synchronize against campus time servers

By default, domain members synchronize their time with domain controllers using Microsoft's [Windows Time Service](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03mngd/26_s3wts.mspx). The domain controller should be configured to synchronize its time with an external time source, such as the university's network time servers.

### Install and enable anti-virus software

### Install and enable anti-spyware software

Anti-spyware software is only required to be installed if the server is used to browse Web sites not specifically related to the administration of the server, which is not recommended. At a minimum, SpyBot Search and Destroy should be installed. We also recommend the installation of a secondary anti-spyware application, such as SpyWare Blaster, EMS Free Surfer, or AdAware. Both SpyWare Blaster and EMS Free Surfer are available from [BevoWare](http://www.utexas.edu/its/bevoware/download).

An additional measure that can be taken is to install [Firefox](http://www.mozilla.com/en-US/firefox/personal.html) with the [NoScript](https://addons.mozilla.org/en-US/firefox/addon/722/) and [uBlock](https://addons.mozilla.org/en-us/firefox/addon/ublock/) add-ons.

### Configure anti-virus software to update daily

Microsoft Forefront may be used, and can be [configured directly](http://www.utexas.edu/its/help/anti-virus-software/456)or through the use of [GPOs](http://www.utexas.edu/its/help/anti-virus-software/448), which can simplify the management of multiple servers.

### Configure anti-spyware software to update daily

### Provide secure storage for data

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

Windows provides the Encrypting File System as a built-in mechanism to allow the encryption of individual users' files and folders. Be aware of the caveats involved in the use of EFS before implementing it for general use, though. Other options such as [PGP](http://www.pgp.com/) and [GNUPG](http://www.gnupg.org/) also exist.

Another encryption option to consider is whole-disk encryption, which encrypts the entire contents of the drive instead of just specific files and folders. Windows comes with BitLocker for this.

If encryption is being used in conjunction with Category I data, one of the solutions listed in the [Approved Encryption Methods](https://wikis.utexas.edu/display/ewde/ApprovedEncryptionMethods) (EID required) must be implemented.

### Install software to check the integrity of critical operating system files

Windows has a feature called Windows Resource Protection which automatically checks certain key files and replaces them if they become corrupted. It is enabled by default.

You can audit in much more in depth using Tripwire. Modern versions of Tripwire require the purchase of licenses in order to use it. The Tripwire management console can be very helpful for managing more complex installations.

### If RDP is utilized, set RDP connection encryption level to high

This setting is configured by group policy object at:

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

Remote Desktop Session Host\Security

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 — Enabled

## Physical Security

### Set a BIOS/firmware password to prevent alterations in system start up settings

### Disable automatic administrative logon to recovery console

### Do not allow the system to be shut down without having to log on (Default)

### Configure the device boot order to prevent unauthorized booting from alternate media

Configure a screen-saver to lock the console's screen automatically if the host is left unattended

Open the Display Properties control panel.

Select the Screen Saver tab.

Select a screen saver from the list. Although there are several available, consider using a simple one such as "Blank."

The value for Wait should be no more than 15 minutes.

Select the On resume, password protect option.

## Sources

<https://wikis.utexas.edu/display/ISO/Windows+Server+2012+R2+Hardening+Checklist>

http://mubix.github.io/blog/2012/03/19/how-to-win-ccdc-slides/