Active Directory Security Checklist

☐	**#1 Limit the use of Domain Admins and other Privileged Groups** Members of Domain Admins and other privileged groups are very powerful. They can have access to the entire domain, all systems, all data, computers, laptops, and so on. It is recommended to have no day to day user accounts in the Domain Admins group, the only exception is the default Domain Administrator account.
☐	**#2 Use at least two Accounts** You should use a regular account with no administrator rights for day-to-day tasks like checking email, browsing the internet and so on. Use a secondary account when you need to perform admin tasks. Use the least privilege model, give permissions to only what is needed.
☐	**#3 Secure the Domain Administrator Account** The built-in administrator account should only be used for domain setup and recovery. Set a 20+ character password on it and lock the password in a vault. No one should know the password or be using this account
☐	**#4 Disable Local Administrator Account** Disable the local administrator account on all computers and use your individual domain account instead. The local admin is a well-known account that attackers will try to compromise and often has the same password on every computer. See #5 if this is not possible.
☐	**#5 Use LAPS (Local Administrator Password Solution)** If you are unable to disable the local administrator account, then use Microsoft LAPS. This will set a random unique password on all computers. The password is stored in Active Directory.

Active Directory Security Checklist

☐	**#6 Use a Secure Workstation for administrator tasks** Use a dedicated secure workstation for performing administrative tasks. The secure admin workstation should not have internet access or be used for checking email. Login into this workstation with your admin account not your regular account.
☐	**#7 Enable Audit Policy Settings** Use group policy to set an audit policy on all computers. Malicious activity often starts on end user devices, so it is important that auditing is enabled on all computers.
☐	**#8 Monitor AD Events for Compromise** Monitor changes to privileged groups, spike in bad password attempts, account lockouts, use of administrator accounts and other abnormal behavior. Recommended Tool: Security Event Log Manager
☐	**#9 Use Long Passwords** If your company policy allows it, set the minimum password length to 15 characters. This is often driven by various compliance requirements.
☐	**#10 Use Descriptive Security Groups** Avoid naming security groups with random or meaningless names. It is not easy tracking down where or how groups are used and better naming conventions can help. Example, N-Drive-HR-RW
☐	**#11 Cleanup inactive user and computer accounts** Have a process in place to find and disable stale/unused active directory computer and user accounts.

Active Directory Security Checklist

	Automate this task with the AD Cleanup Tool
☐	**#12 Remove Users from the Local Administrator Group** Regular users should not have local administrator rights on computers. This makes it easy for attackers to install malicious files and compromise a network. Use PowerShell or a 3rd party tool to inventory who has local administrator rights. How to Guide -> How to Remove Local Administrator rights with Group Policy
☐	**#13 Do not install additional software on domain controllers** Domain controllers should have very limited software and roles installed on them. More software you install the bigger the security risk. These are the most important servers in your domain so keep them secure by limiting what is running on them.
☐	**#14 Patch & Vulnerability Scanning** Attackers are quick to exploit known vulnerability's, you need to continuously scan and patch systems. Make sure you are patching 3rd party programs and upgrading or removing software that is no longer supported.
☐	**#15 Use Secure DNS Services to block malicious traffic** You can easily block malicious traffic by using a secure DNS service such as QUAD9 or OpenDNS.
☐	**#16 Run Supported Operating System** Keep systems on the latest operating system will help to increase overall security. Each new version of Windows includes new built-in security features and enhancements.

Active Directory Security Checklist

☐	**#17 Use Two Factor Authentication** It is easy for attackers to compromise accounts, which can allow remote unauthorized access. Two factor authentication should be used for all remote access.
☐	**#18 Monitor DHCP Logs** You need to know what is connecting to your network. A simple way to check this is by looking at the DHCP logs, look for hostnames that you do not recognize. If you have a naming convention it should be easy to identify unauthorized devices**.**
☐	**# 19 Monitor DNS Logs** DNS logs can be used to identify malicious DNS lookups. You will need to enable the windows DNS debug logs; steps are provided in full post. DNS logging is also provided on next gen firewalls. DNS lookups for random domain names are a good sign of malicious traffic on your network. Example, efdvessdtgsdg.3dfxo.com
☐	**#20 Use ADFS & Azure Security** Take advantage of the latest ADFS & Azure security features. Microsoft continues to develop and provide security enhancements to both services.
☐	**#21 Use Office 365 Secure Score** Secure score analyzes your office 365 tenant and provides a score based on your settings. It provides a list of issues and recommended actions to fix. May require a subscription.
☐	**#22 Have a recovery plan**

Active Directory Security Checklist

	Have a response plan on how to handle a cyber-attack. See the NIST Computer Security Incident Handling Guide for guidelines on incident handling.
☐	**#23 Document Delegation to Active Directory** Delegation and AD permissions can easily get out of control. Document these permissions or use PowerShell to create a report and review regularly.
☐	**#24 Lock Down Service Accounts** Service accounts are used to run executables, tasks, services, authentication and so on. These accounts are often set with passwords that never expire and are granted more permissions than needed. See full post for a list of tips for locking down service accounts. A better option is to use Managed service accounts.
☐	**#25 Use Secure Baselines** Default installs are not secure, use secure benchmarks and baselines to secure default settings. These settings can be deployed with group policy. Microsoft Security Compliance Toolkit and CIS SecureSuite provide baseline templates and tools.
☐	**#26 Enable Windows Firewall** Use group policy to deploy and control the windows firewall on all computers in your organization. The firewall can control incoming/outgoing traffic to your systems. Recommended reading -> 11 Windows Firewall Best Practices
☐	**#27 Use application whitelisting**

Active Directory Security Checklist

	With application whitelisting you can block unwanted programs from running. There are third party programs that offer these features, Windows Enterprise also has this feature.
☐	**#28 Block PowerShell for regular users** Viruses will often use PowerShell to execute commands on computers. Most of the time regular users do not need to execute PowerShell. You can control who has permissions to run PowerShell with Group Policy. How to guide on blocking PowerShell
☐	

Link to full post
https://activedirectorypro.com/active-directory-security-best-practices/

Recommended Tools:

1. NTFS Permissions Reporter – Easily audit folder permissions and see who has permissions to what.
2. AD Cleanup Tool – Find inactive user and computer accounts, bulk move and disable accounts.
3. Export Group Membership – Get all users group membership and export to a CSV file.
4. User Unlock & lockout troubleshooter – Quickly find all locked users and the source of account lockouts.
5. Bulk User Updater – Bulk update user account properties. Huge time saver