

Top 25 Active Directory Security Practices

 Summarize   

Last Updated: August 1, 2023 by [Robert Allen](#)



This is the most comprehensive list of Active Directory Security Best Practices online.

In this guide, I'll share my recommendations for Active Directory Security and how you can improve the security of your Windows domain environment.

You don't have to spend a fortune to improve security there are many no cost and low cost solutions that I'll show you in this guide.

AD Security topics covered in this guide:

1. [Limit the use of Domain Admins and other Privileged Groups](#)

2. Use at least two accounts
3. Secure the domain administrator account
4. Disable the local administrator account (on all computers)
5. Use Laps
6. Use a secure admin workstation (SAW)
7. Enable audit policy settings with group policy
8. Monitor for signs of compromise
9. Password complexity sucks (use passphrases)
10. Use descriptive security group names
11. Find and remove unused user and computer accounts
12. Remove Users from the Local Administrator Group
13. Do not install additional software or server roles on DCs
14. Patch management and vulnerability scanning
15. Use secure DNS services to block malicious domains
16. Run supported operating systems
17. Use two factor for office 365 and remote access
18. Monitor DHCP logs for connected devices
19. Monitor DNS logs for malicious network activity
20. Use latest ADFS and azure security features
21. Use office 365 secure score
22. Have a recovery plan
23. Document delegation to Active Directory
24. Lock down service accounts
25. Use security baselines and benchmarks
26. Active Directory Security Checklist

Why Securing Active Directory is Essential

In many organizations, Active Directory is the centralized system that authenticates and authorizes access to the network. Even in the cloud or hybrid environments, it can still be the centralized system that grants access to resources. When accessing a

document on the network, OneDrive, printing to the network printer, accessing the internet, checking your email, and so on, all of these resources often go through Active Directory to grant you access.

Active Directory has been around for a long time and over the years we have discovered vulnerabilities in the system and ways to exploit them. In addition to vulnerabilities, it becomes very easy for hackers to just steal or obtain user credentials which then gives them access to your data. If they can get access to your computer or your login then they could potentially gain Full access to Active Directory and own your network.

Now let's dive into the list of Active Directory Security Best Practices.

1. Limit the use of Domain Admins and other Privileged Groups

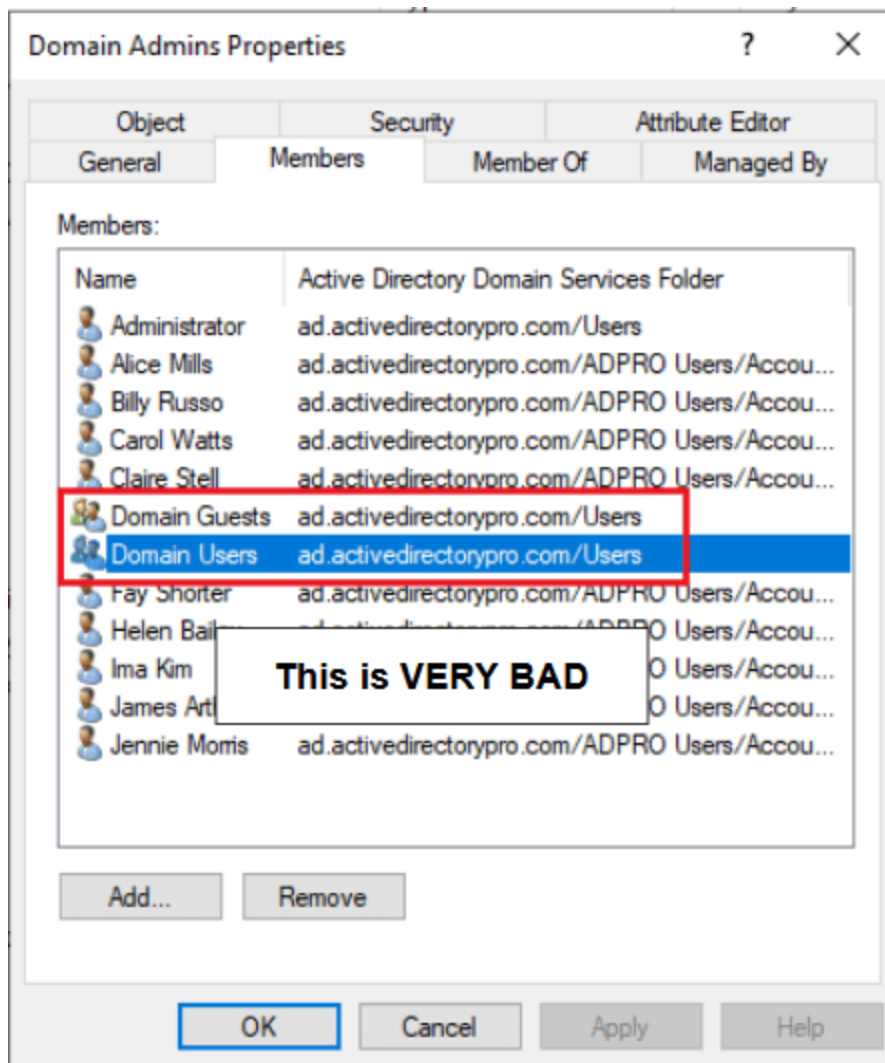
Members of Domain Admins and other privileged groups are very powerful. They can have access to the entire domain, all systems, all data, computers, laptops, and so on.

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.

Domain Admins are what the bad guys try to seek out.

Microsoft recommends that when DA access is needed, you temporarily place the account in the DA group. When the work is done you should remove the account from the DA group.

This process is also recommended for the Enterprise Admins, Backup Admins, and Schema Admin groups.



What's the big deal?

It's become way too easy for attackers to obtain or crack user credentials.

Once attackers gain access to one system they can move laterally within a network to seek out higher permissions (domain admins).

One method of doing this is called pass the hash.

Pass the hash allows an attacker to use the password hash to authenticate to remote systems instead of the regular password. These hashes can be obtained from end user computers.

Scary right?

All it takes is for one compromised computer or a user account for an attacker to compromise a network.

Cleaning up the Domain Admins group is a great first step to increasing your network security. This can defiantly slow down an attacker.

The process to remove accounts from the DA group is not easy. I know first hand as I've recently gone through this process. It's very common to have way too many accounts in the DA group.

Things will break so be prepared.

2. Use Two Accounts or more (Regular and Administrator Account)

You should not be logging in every day with an account that is a local admin or has privileged access (Domain Admin).

Instead create two accounts, a regular account with no admin rights and a privileged account that is used only for administrative tasks.

BUT

Do not put your secondary account in the Domain Admins group, at least permanently.

Instead, follow the **least privileged administrative model**. Basically, this means all users should log on with an account that has the minimum permissions to complete their work.

You may read other articles and forums to put your secondary account in the Domain Admins group.

This is not a Microsoft best practice and I would advise against it. Again temporary is OK but it needs to be removed as soon as the work is done.

With that said Microsoft does not make it easy to get away from Domain admin rights. There is no easy process to delegate rights to all systems like DNS, DHCP, group policy, and so on. This is often the reason so many people have Domain Admin rights.

You should use a regular non admin account for day to day tasks such as checking email, browsing the internet, ticket system, and so on. You would only use the privileged account when you need to perform admin tasks such as creating a user in Active Directory, logging into a server, adding a DNS record, etc.

Look at these two scenarios.

Scenario 1 – IT Staff with Domain Rights

Steve logs into his computer with a privileged account, checks his email, and inadvertently downloads a virus. Since Steve is a member of the DA group the virus has full rights to his computer, all servers, all files, and the entire domain. This could cause serious damage and result in critical systems going down.

Now, take the same scenario but this time Steve is logged in with his regular non admin account.

Scenario 2 – IT Staff with Regular Rights

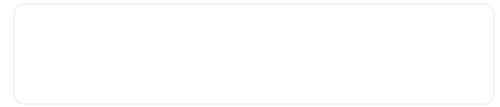
Steve checks his email and inadvertently downloads a virus. The virus has limited access to the computer and no access to the domain or other servers. This would cause minimal damage and prevent the virus from spreading through the network.

By simply using a regular account you can increase security and avoid causing serious damage.

Here are some common tasks that can be delegated to a secondary admin account.

- Rights to Active Directory Users and Computers
- DNS

- DHCP
- Local admin rights on servers
- Group Policy
- Exchange
- Local admin rights on workstations
- Vsphere or Hyper-v Administration



Some organizations use more than two accounts and use a tiered approach. This is defiantly more secure but may be an inconvenience to some.

- Regular account
- Account for Server Administration
- Account for Network Administration
- Account for Workstation Administration

3. Secure the Domain Administrator Account

Every domain includes an Administrator account, this account by default is a member of the Domain Admins group.

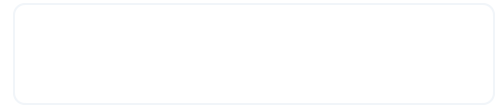
The built-in Administrator account should only be used for the domain setup and disaster recovery (restoring Active Directory).

Anyone requiring administrative-level access to servers or Active Directory should use their own individual account.

No one should know the Domain Administrator account password. Set a really long 20+ characters password and lock it in a vault. Again the only time this is needed is for recovery purposes.

In addition, Microsoft has several recommendations for securing the built-in Administrator Account. These settings can be applied to group policy and applied to all computers.

- Enable the Account is sensitive and cannot be delegated.
- Enable the smart card is required for interactive logon
- Deny access to this computer from the network
- Deny logon as batch job
- Deny log on as a service
- Deny log on through RDP



For more details on securing the Domain Administrator account see this Microsoft article, [Securing Built in Administrator Accounts in Active Directory](#).

4. Disable the Local Administrator Account (on all computers)

The local administrator account is a well-known account in Domain environments and is not needed.

Not needed, is that true?

Yes

You should be using an individual account that has the necessary rights to complete tasks.

What is the problem with the local admin account?

Two Problems.

1. It is a well-known account, even if you rename it the SID is the same and is well-known by attackers.
2. It's often configured with the same password on every computer in the domain.

Attackers just need to compromise one system and now they have local admin rights on every domain-joined computer. They could then use this account to pivot to another system with the goal of finding domain admin access.

If you need to perform admin tasks on the computer (install software, delete files, etc) you should be doing so with your individual account, not the local admin account.

Even if the account is disabled you can boot into safe mode and log in as the local administrator account.

As an administrator, I know these best practices are not always practical or introduce a huge inconvenience.

What if the network is down or the NIC card died, what if you need to drop it from the domain and re-add it? There are ways around this but it can really slow you down.

If you cannot disable the account here are recommendations for securing the account. **A better alternative is to use the Microsoft LAPS tool (Covered below in tip #5)**

- Deny access to this computer from the network
- Deny log on as a batch job
- Deny log on as a service
- Deny log on through RDP

For more details see the following article, [Securing local administrator accounts and groups](#)

5. Use Local Administrator Password Solution (LDAPS)

Local Administrator Password Solution (LAPS) is becoming a popular tool to handle the local admin password on all computers.

LAPS is a Microsoft tool that provides management of local account passwords of domain-joined computers. It will set a unique password for every local administrator account and store it in Active Directory for easy access.

This is one of the best free options for mitigation against pass the hash attacks and lateral movement from computer to computer.

It's very common that organizations deploy Windows using an image based system. This makes it quick to deploy a standard configuration to

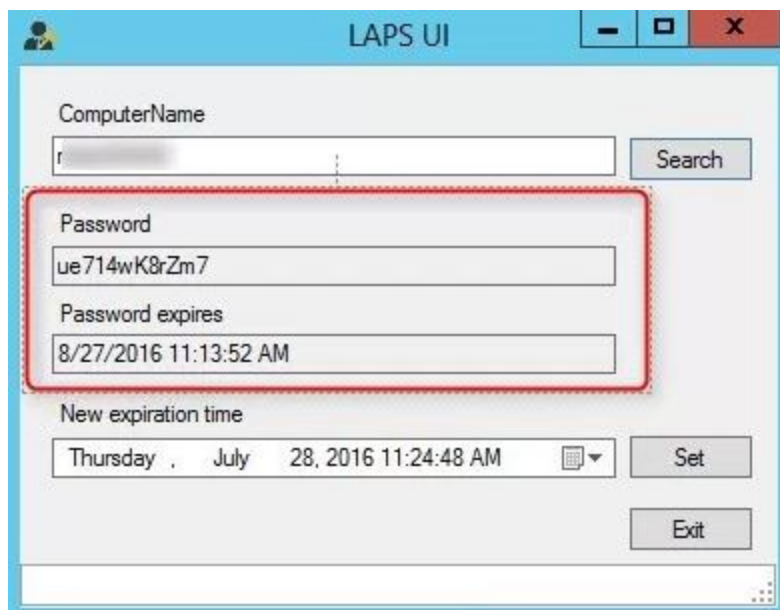
But..

This often means the local administrator account will be the same on every computer. Since the local Administrator account has full rights to everything on the computer, all it takes is for one of them to get compromised, then the hacker can access all the systems.

LAPS is built upon the Active Directory infrastructure so there is no need to install additional servers.

The solution uses the group policy client side extension to perform all the management tasks on the workstations. It is supported on Active Directory 2003 SP1 and above and client Vista Service Pack 2 and above.

If you need to use the local admin account on a computer you would retrieve the password from Active Directory and it would be unique to that single computer.



For step-by-step instructions on installing LAPS see this article, [How to Install Local Administrator Password Solution \(LAPS\)](#).

6. Use a Secure Admin Workstation (SAW)

A secure admin workstation is a dedicated system that should only be used to perform administrative tasks with your privileged account.

It should not be used for checking email or browsing the internet. In fact... it should not even have internet access.

What tasks would you do on a SAW?

- Active Directory administration
- Group Policy
- Managing DNS & DHCP Servers
- Any task that requires admin rights on servers
- Admin rights to Management Systems such as VMware, Hyper-v, Citrix
- Office 365 Administration

You get the idea.

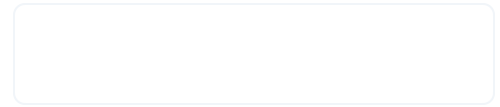
Basically, when you need to use your privileged account to perform admin tasks you should be doing it from a SAW. Daily use workstations are more vulnerable to compromise from pass the hash, phishing attacks, fake websites, keyloggers, and more.

Using a secure workstation for your elevated account provides much greater protection from those attack vectors. Since attacks can come from internal and external it's best to adopt an assumed breach of security posture.

Due to the continuous threats and changes to technology the methodology on how to deploy a SAW keeps changing. There are also PAW and jump servers to make it even more confusing.

Here are some tips to help get you started:

- Use a clean OS install (use the latest Windows OS)
- Apply hardening security baseline (See tip#25)
- Enable full disk encryption
- Restrict USB ports
- Enable the [Windows Firewall](#)
- Block internet
- Use a VM – Terminal Server works well
- Minimal software installed
- Use two factor or smart card for access
- Restrict systems to only accept connections from the SAW



Here is my typical workflow using a SAW:

1. Log into my computer with my regular account to check email and view new support requests.
2. If I have some administrative task I will log into my SAW with my privileged account that has rights to modify AD group membership and add the user to the necessary AD security group.

Pretty straightforward right?

It may seem like a hassle but I actually find it more convenient this way. I can remote in when off network and have a server that has all the tools I need. I also don't have to worry about re-install all of my support software if I need to re-image my computer.

For more information on this topic check out Microsoft's [Privileged access devices](#) documentation.

7. Enable Audit Policy Settings with Group Policy

Ensure the following Audit Policy settings are configured in group policy and applied to all computers and servers.

Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration

Account Logon

Ensure 'Audit Credential Validation' is set to 'Success and Failure'

Account Management

Audit 'Application Group Management' is set to 'Success and Failure'

Audit 'Computer Account Management' is set to 'Success and Failure'

Audit 'Other Account Management Events' is set to 'Success and Failure'

Audit 'Security Group Management' is set to 'Success and Failure'

Audit 'User Account Management' is set to 'Success and Failure'

Detailed Tracking

Audit 'PNP Activity' is set to 'Success'

Audit 'Process Creation' is set to 'Success'

Logon/Logoff

Audit 'Account Lockout' is set to 'Success and Failure'

Audit 'Group Membership' is set to 'Success'

Audit 'Logoff' is set to 'Success'

Audit 'Logon' is set to 'Success and Failure'

Audit 'Other Logon/Logoff Events' is set to 'Success and Failure'

Audit 'Special Logon' is set to 'Success'

Object Access

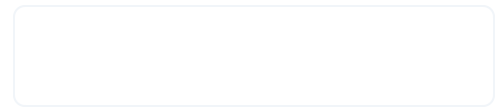
Audit 'Removable Storage' is set to 'Success and Failure'

Policy Change

Audit 'Audit Policy Change' is set to 'Success and Failure'

Audit 'Authentication Policy Change' is set to 'Success'

Audit 'Authorization Policy Change' is set to 'Success'



Privilege Use

Audit 'Sensitive Privilege Use' is set to 'Success and Failure'

System

Audit 'IPsec Driver' is set to 'Success and Failure'

Audit 'Other System Events' is set to 'Success and Failure'

Audit 'Security State Change' is set to 'Success'

Audit 'Security System Extension' is set to 'Success and Failure'

Audit 'System Integrity' is set to 'Success and Failure'

Malicious activity often starts on workstations, if you're not monitoring all systems you could be missing early signs of an attack.

In the next section, I'll cover what events you should be monitoring.

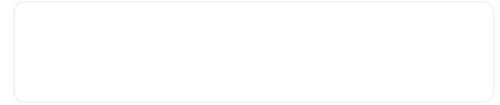
8. Monitor Active Directory for Signs of Compromise

You should be monitoring the following Active Directory events to help detect compromise and abnormal behavior on the network.

Here are some events you should be monitoring and reviewing on a weekly basis.

- Changes to privileged groups such as Domain Admins, Enterprise Admins, and Schema Admins
- A spike in bad password attempts
- A spike in locked out accounts
- Account lockouts

- Disabled or removal of antivirus software
- All actives performed by privileged accounts
- Logon/Logoff events
- Use of local administrator accounts



How do you monitor events in Active Directory?

The best way is to collect all the logs on a centralized server and then use log analyzing software to generate reports.

Some log analyzers come pre-built with Active Directory security reports and others you will need to build yourself.

Here are some of the most popular log analyzers.

- [Elk Stack](#)
- [Lepid](#)
- [Splunk](#)
- [ManageEngine ADAudit Plus](#)
- [Windows Event Forwarding](#)

With a good log analyzer, you will be able to quickly spot suspicious activity in your Active Directory environment.

Here are some screenshots from an analyzer that I use. The first screenshot shows a spike in account lockouts.

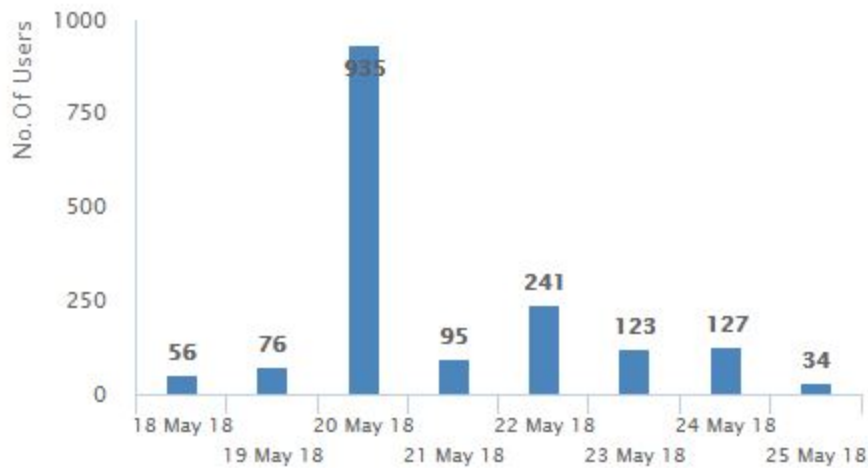
That is definitely not normal.

Account Locked Out Users



LAST 7 DAY

LAST 30 DAY



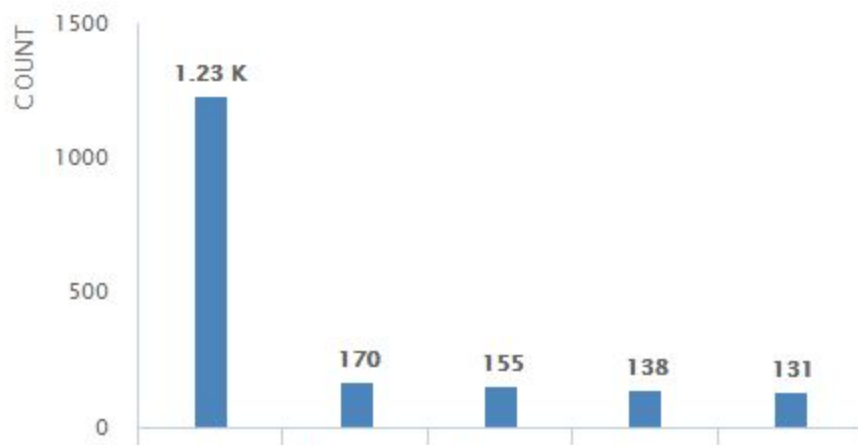
In this screenshot, you can see a huge spike in logon failures. Without a log analyzer, these events would be hard to spot.

Top User Logon Failures



LAST 1 DAY

LAST 2 DAY

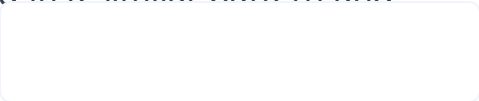


9. Password Complexity Sucks (use passphrases)

8 characters with complexity is no longer a secure password. Instead, use a minimum of 12 characters and train users on passphrases.

The longer the password the better.

Passphrases are simply two or more random words put together. You can add numbers and characters if you want but I wouldn't make it a requirement.

Studies have shown when you require complexity it is used in a similar pattern and then repeated. Hackers have caught onto this and there are  (freely available) that contain millions of easy to guess passwords.

Know anyone that uses passwords like this?

S@mmer2018, or Winter2018! June2018\$

These are awful passwords and are easily guessed.

Long passwords and using the passphrase technique make it more difficult for password cracking software and for hackers to guess.

Better Password Policy

- Set 12 character passwords
- Remember 10 password history
- use passphrases
- Lockout policy 5 attempts

The key to using passphrases is to be totally random with each word, you don't want to type out a sentence where the next word can be guessed.

Good passwords using passphrases

Bucketguitartire22

Screenjugglered

RoadbluesaltCloud

The above examples are totally random. These would take a very long time to crack and most likely no one would guess them.

Bad passphrase examples

Ireallylikepizza22

Theskyisblue44

[NIST](#) recently updated its password policy guidelines in [Special Publication 800-63](#) to address new requirements for password policies.

If your organization must meet certain standards then make sure those standards support these password recommendations.

Also, be sure to update your company's written policy.

10. Use Descriptive Security Group Names

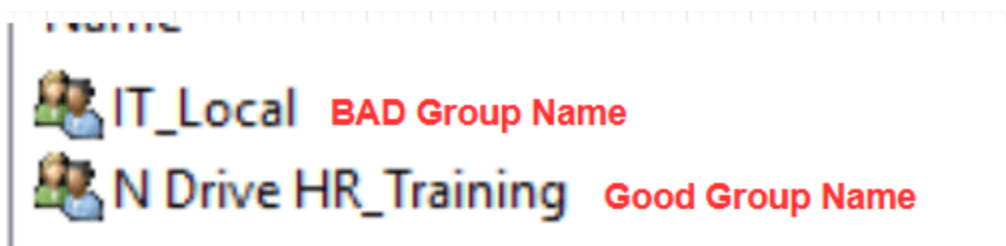
First of all, make sure you apply permissions to resources with security groups, not individual accounts, this makes managing resources much easier.

Next, don't name your security groups with a generic name like helpdesk or HR Training.


When you have generic names like this they will get used on all kinds of resources and you will have lost all control of security.

And there is no easy way to see where security groups are being used. Yes, there are tools that you can run but if you have a medium or large size environment this will be a huge task.

Here is an example



IT_Local is very generic. Just by looking at the name, I don't know what this is used for. Yes, it's probably used by the IT department but where?

This is how permissions can get out of control and you could end up giving people access to things they shouldn't have access to. Some sysadmin might get a request for access to the IT department network share and add users to this group. But what he doesn't know is that the group might be used on other systems. 

When you use a descriptive name like the "N Drive HR_Training" group you can look at the name and have a good idea of what it is for. In this example, it's for the N drive, it's for HR, and has something to do with Training. Your IT staff should have a good idea of what this is just by the name.

Here is a real-world example of how bad group names can lead to issues.

I was working with a client on cleaning up permissions to Active Directory. There were multiple security groups that had delegated permissions to Active Directory.

There was a group called helpdesk, another group IS Support, and one more called AD Modify.

I was under the impression only Helpdesk staff had rights to Active Directory to reset passwords and unlock accounts.

Come to find out these groups were used for other resources such as the helpdesk software, network share, and printers. So it included various IT staff.

Once I removed these groups I got phone calls from programmers and business analysts asking why they couldn't reset user's passwords anymore. Why on earth are programmers resetting user passwords?

A clear precise Security group name would have prevented this from happening.

If you don't name the security group specific then it can be a catch all for permissions to many other things.

Here are some good examples of how to name groups.

Example 1: Allow helpdesk to reset passwords

Security group name: IT-Helpdesk-PW-Reset

Since the group name is precise, this would help prevent i
resources like a printer or network share.

Example 2: Allow HR rights to a shared folder

Security group name: N Drive HR-Training-Folder-RW

Again, this has a very specific name and helps identify what it should be used for.

You can come up with your own naming convention just get specific with the name and avoid generic one word group names.

11. Find and Remove Inactive User and Computer Accounts

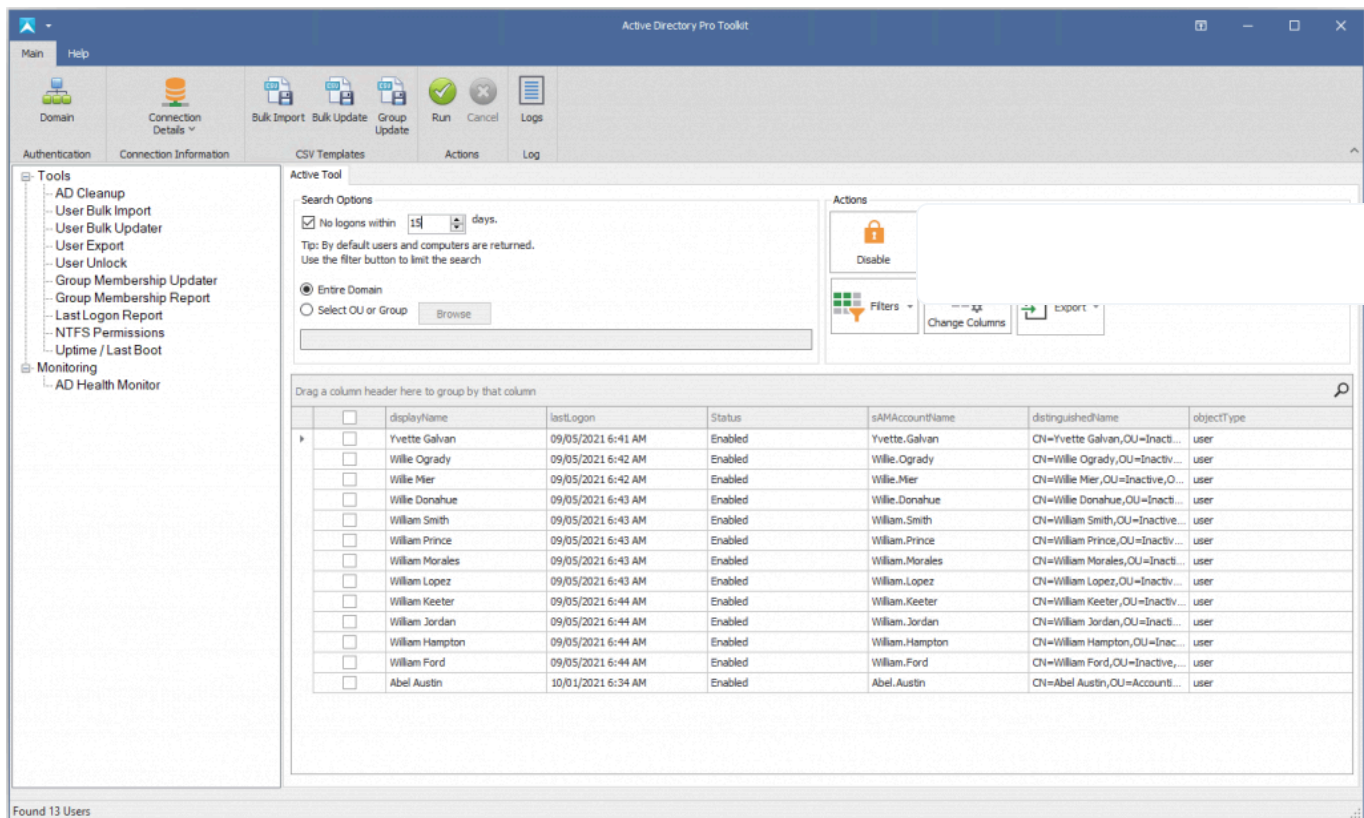
You need to have a procedure in place to detect inactive users and computer accounts in Active Directory.

You don't want a bunch of unused accounts sitting in Active Directory just waiting for an attacker to discover and use. This can also cause issues with reporting, patching, and slowing down group policy.

[CIS Critical Security Controls](#) says "There are many ways to covertly obtain access to user accounts, including weak passwords, accounts still valid after a user leaves the enterprise, dormant or lingering test accounts"

CIS recommends deleting or disabling dormant accounts after 45 days of inactivity

I created a tool called [AD Cleanup Tool](#) that lets you quickly find inactive users and computer accounts.



If you want more details on finding inactive users or how to do this with PowerShell check out this article titled [Finding inactive Users in Active Directory](#)

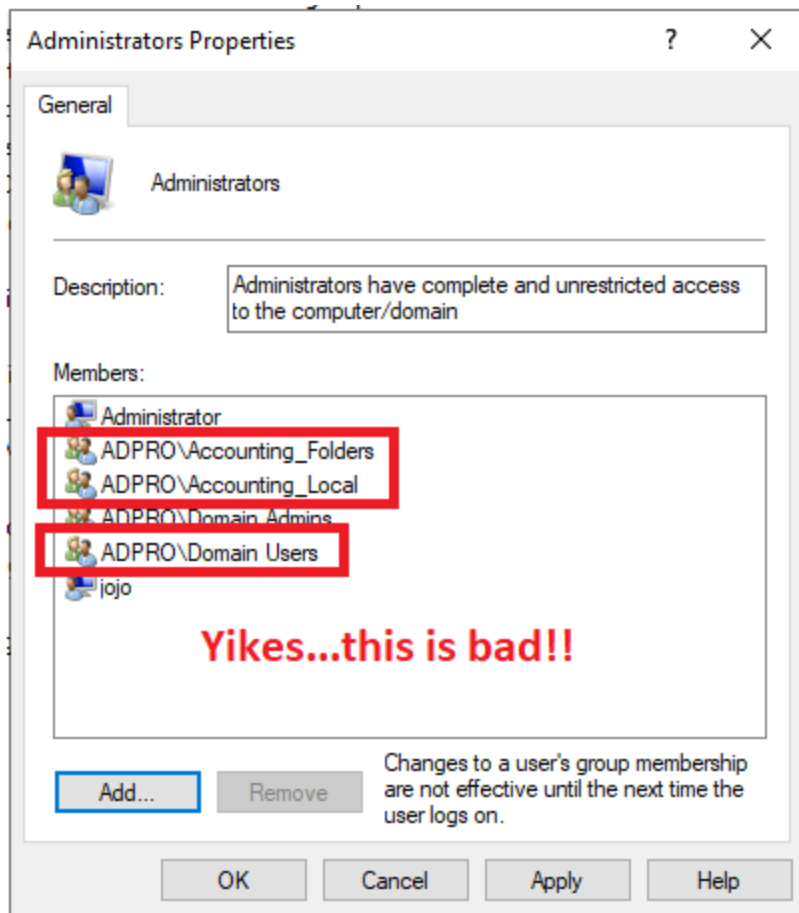
12. Remove Users from the Local Administrator Group

A regular user should not be in the local administrator group on computers.

A user with local admin rights has full access to the entire Windows Operating system. This can lead to all kinds of security issues, such as installing software, disabling antivirus, downloading and installing malware, stealing data, hacking credentials, pivoting to other computers, and so on.

A Microsoft vulnerabilities report says:

“Of all the Windows vulnerabilities discovered in 2018, 169 of these were considered ‘critical’. Removing admin rights could have mitigated 85% of these critical vulnerabilities”



By removing users from the local administrator group you greatly reduce the opportunities for attackers to gain access to your computer and network.

I recommend you control the local administrator group by using group policy. If you remove them from the computer with no centralized control then someone will just add the rights back. I have fought this battle many times with helpdesk. I remove the rights then they just add it back when troubleshooting an issue.

Using group policy and restricted groups will prevent your staff from leaving accounts in the group.

I wrote a complete guide on this check it out here -> [Remove Users from Local Administrator Group using Group Policy](#).

13. Do Not Install Additional Software or Server Roles on DCs

Domain controllers should have limited software and roles installed on them.

DC's are critical to the enterprise, you don't want to increase security risks by having additional software running on them.

Windows Server Core is a great option for running the DC role and other roles such as DHCP, DNS, print servers, and file servers. Server Core requires fewer security patches due to its smaller footprint.

Server core can have its challenges though with some 3rd party software not being compatible.

14. Patch Management and Vulnerability Scanning

Attackers are quick to exploit known vulnerabilities.

If you do not regularly scan and remediate discovered vulnerabilities you are at a much greater risk for compromise.

There are a large number of vulnerability and scanning tools available, see my list of the [best patch management software](#).

Tips for Continues Vulnerability Management

- Scan all systems at least once a month to identify all potential vulnerabilities. If you can scan more frequently that's even better.
- Prioritize the finding of the vulnerability scans and first fix the ones that have known vulnerabilities in the wild.
- Deploy automated software updates to operating systems
- Deploy automated updates to 3rd party software
- Identify out-of-date software that is no longer supported and get it updated.

15. Use Secure DNS Services to Block Malicious Domains

You can prevent a lot of malicious traffic from entering your network by blocking malicious DNS lookups.

Anytime a system needs to access the internet it will in most cases use a domain name. Computers talk to each other by IP address so the computer needs a way to convert a domain name to an IP address.

There are several services available that check DNS queries for malicious domains and blocks them.

How does this work?

These DNS services gather intelligence about malicious domains from various public and private sources. When it gets a query for a domain that it has flagged as malicious it will block access when your system attempts to contact them.

Here is an example:



Step1: The client clicks a link that goes to example.net

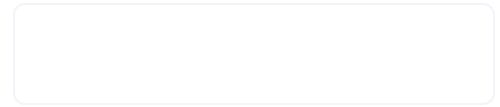
Step2: Local cache is checked

Step 3: DNS Service checks if the domain is on its threat list, it is so it returns a block reply.

In the above example since the DNS query returned a block, no malicious traffic ever entered the network.

Here are some of the most popular secure DNS services.

- [Quad9](#)
- [OpenDNS](#)
- [Comodo Secure DNS](#)



I'm currently using Quad9, it's free and easy to setup.

Also, most IPS (Intrusion Prevention Systems) systems support the ability to check DNS lookups against a list of malicious domains.

16. Run Supported Operating Systems

With each new version of Windows OS, Microsoft includes built in security features and enhancements. More importantly, you get security updates.

Just staying on the latest OS will increase overall security.

New Security Features in Server 2022:

- Secured-core Server
- Hardware root of trust
- Firmware protection
- UEFI secure boot
- Virtualization based security

Here is a video from Robert McMillen on Security features in server 2002.



17. Use two-factor authentication for office 365 and remote access

Compromised accounts are very common and this can provide attackers remote access to your systems through VPN, Citrix, or other remote access systems.

Check your Office 365 or ADFS logs, you will be surprised at how many login attempts are coming from China and Russia.

One of the best ways to protect against compromised accounts is two factor authentication. This will also help against password spraying attacks.

Let's say a user fell for a phishing attempt that asked the user to verify their username and password.

Now the attacker has that user's Active Directory credentials. The attacker could now gain access to a number of systems from anywhere.

If the user had two-factor enabled this could prevent access even though the account has been compromised. The attacker would need the second set of credentials to get logged in.

There really is no stopping accounts from getting compromised there are too many ways for attackers to gain the credentials.

If you are using Office 365 and depending on what package you have MFA may be included. Take advantage of this feature.



Popular two-factor authentication solutions

- [DUO](#)
- [RSA](#)
- [Office 365 MFA Setup](#)

18. Monitor DHCP logs for connected devices

You should know what is connected to your network if you have multiple locations with lots of users and computers this can be challenging.

There are ways to prevent only authorized devices from connecting but this can be costly and a lot of work to set up. If you have the resources then that is the way to go.

Another method that is already available to you is to monitor the DHCP logs for connected devices.

You should have all end user devices setup to use DHCP. You can then look at the logs to see what is connecting. You should have a naming convention for your equipment, this will make it easy to spot possible unauthorized devices.

In the screenshot below I can easily spot a device that does not follow my computer naming convention.

minint-1bdvd67 is not something I recognize. I will need to look into this and see if it is an authorized device.

10.2.10.186	L-FI-02-80042.sp...	5/1/2018 7:40:11
10.2.10.187	W-HE-18-86060....	5/31/2018 7:30:11
10.2.10.188	minint-1bdvd67....	5/31/2018 5:29:11
10.2.10.190	W-EN-02-82223....	5/31/2018 11:56:11
10.2.10.191	W-FI-02-82870.s...	5/31/2018 8:26:11
10.2.10.192	W-IC-02-86776...	5/31/2018 11:16:11

19. Monitor DNS Logs for Malicious

Most connections start with a DNS query. All domain joined systems should be set up to use your local Windows DNS server.

With this setup, you can log every internal and external DNS lookup. When a client device makes a connection to a malicious site it will log that site name in the DNS logs.

These malicious domains are usually odd, random character domains that don't look normal.

Here are some screenshots of suspicious DNS lookups from my logs. These repeatedly show up in my logs for a handful of devices.

I seriously doubt a user is trying to go to this site intentionally. These kinds of lookup need to be looked into to determine if it's malicious or not.

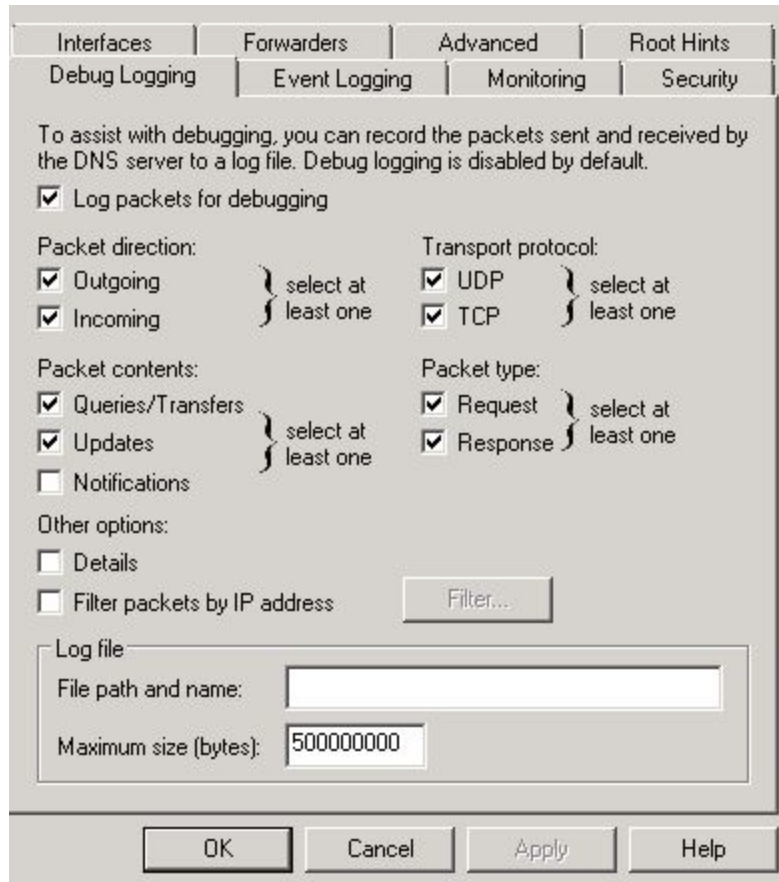
```
(3)b-0(11)19-a7000008(1)0(4)170c(4)22c7(4)2f4a(3)410(1)0(26)5b574pzbk36prdvz9m3i196i4t(4)avts(6)mcafee(3)com(0)
(3)b-0(11)19-a7000008(1)0(4)170c(4)22c7(4)2f4a(3)410(1)0(26)5b574pzbk36prdvz9m3i196i4t(4)avts(6)mcafee(3)com(0)
(3)b-0(11)19-a3000008(1)1(4)170c(4)22c7(4)2f4a(3)410(1)0(26)srd2mzbvmsqv7dm1sar1nvuazq(4)avts(6)mcafee(3)com(0)
(3)b-0(11)19-a3000008(1)1(4)170c(4)22c7(4)2f4a(3)410(1)0(26)srd2mzbvmsqv7dm1sar1nvuazq(4)avts(6)mcafee(3)com(0)
```

```
NOERROR] A (55)c-6rtwjumjzx7877x241ttlqjfix789x2elx2eitzgqjhqnhpx2esjy(3)g00(3)msn(3)com(0)
NOERROR] A (55)c-6rtwjumjzx7877x241ttlqjfix789x2elx2eitzgqjhqnhpx2esjy(3)g00(3)msn(3)com(0)
NOERROR] A (38)c-6rtwjumjzx7877x24fix2efrnstufdx2esjy(3)g00(3)msn(3)com(0)
NOERROR] A (33)c-6rtwjumjzx7877x24ix2ef1psx2ehtr(3)g00(3)msn(3)com(0)
```

To view the DNS lookups you first need to enable the DNS debug logs on the Windows Servers.

Steps to enable DNS debug logs on Windows Server

Step 1: Open the DNS Management Console

Step 2: Right click and select properties**Step 3:** Click Debug Logging Tab**Step 4:** Check the box "Log packets for debugging"

Once you have the debug logs setup you can import those logs into an analyzer to quickly spot malicious activity.

You can also convert the log file to a CSV to make it easier to read and filter.

20. Use Latest ADFS and Azure Security Features

ADFS and Azure have some great security features. These features will help with password spraying, account compromise, phishing, and so on.

No matter what level of office 365 you are on there are some features you should look into.

Of course, premium subscriptions have the best security features.

But

Microsoft does improve and add new features at every level (I've noticed since being on Office 365).

Here are some features that are worth looking into:

- Smart Lockout – Uses algorithms to spot unusual sign on activity.
- IP Lockout – Uses Microsoft's database of known malicious IP addresses to block sign on ins.
- Attack Simulations – You should be doing regular phishing tests to help train end users. Microsoft will be releasing phish simulator software very soon.
- MFA Authentication – Microsoft's 2 factor solution
- Banned passwords – Checks passwords against a known list
- Azure AD Connect Health – Provides several good reports
- Custom bad passwords – Ability to add custom banned passwords to check against.

I'm currently running a hybrid office 365 setup. In azure, I can see several risky sign on reports.

RISK LEVEL	DETECTION TYPE	RISK EVENT TYPE
High	Offline	Users with leaked credentials ⓘ
Medium	Real-time	Sign-ins from anonymous IP addresses ⓘ
Medium	Offline	Impossible travels to atypical locations ⓘ
Medium	Real-time	Sign-ins from unfamiliar locations ⓘ

Azure alerted me to a sign on that came from China from one of our accounts.

DESCRIPTION

Sign-ins from a new location based on user's past login history.

SECURITY IMPACT

This risk event may indicate that an attacker has access to the user's credentials and has signed in to this account from a new location.

IP

222.33.117.102

LOCATION

Wanghua District, Liaoning, China

SIGN-IN TIME (UTC)

5/22/2018 11:28 PM

STATUS

Active

Some of these features are available with the latest ADFS version and some are included with an office 365 subscription.

Definitely check out all the available security features in ADFS, Office 365, and Azure.

Resources:

[Defending against password spray attacks](#)

21. Use Office 365 Secure Score

Secure score analyzes your office 365 organization security based on activity and security settings.

Secure Score checks your Office 365 services then checks your settings and activities and provides you a security score.

Once it analyzes your score it will provide a detailed list of what was scored and recommended actions to fix the issues.

You will need a Premium or Enterprise subscription to access this feature, in addition, you will need to be assigned the global admin or custom role.

Microsoft continues to expand and add additional features to Secure Score

If you have access to this feature then take advantage of it.



Refer to my article [Office 365 Security best practices](#) for more details.

22. Have a Recovery Plan

If your network was compromised today or hit with RansomWare, what would you do?

- Do you have a response policy?
- Have you tested and trained staff on how to handle such an event?
- Do you have a [system state backup of active directory](#)? This is a must have incase you need to restore your domain from a backup.

Cyber attacks can shut down systems and bring business operations to a halt.

The City of Atlanta was shut down by a cyber attack, which prevented residents from paying online utility bills. In addition, Police officers had to write reports by hand.

Last I checked it cost more than \$5 million for them to recover from the attack.

A good incident response plan could have limited the impact and enabled services back online much faster.

Here are a few things to include in an incident response plan

- Create an incident response policy and plan
- Create procedures for performing incident handling and reporting
- Establish procedures for communicating with outside parties
- Establish response teams and leaders
- Prioritize servers
- Walkthrough and training

NIST has a great [computer security incident handling guide](#) that I recommend looking at.

23. Document Delegation to AD

The best way to control access to Active Directory and related resources is to use Security Groups.

If you are delegating rights to individuals then you are losing control of who has access.

Create custom groups with very specific names, document who has rights, and a process for adding new users. Don't just allow users to be added to these custom groups without an approval process. This is just another way permissions can get out of control.

Know what groups are delegated to what resources, document it, and make sure your team is on the same page.

24. Lock Down Service Accounts

Service accounts are those accounts that run an executable, task, or service, AD authentication, etc.

These are wildly used and often have a password set to never expire.

These accounts will often end up with too many permissions and more often than not are a member of the domain admins group.

Bad..very bad

Sometimes this is suggested by the vendor.

Don't allow that to happen, there are ways to make it work without DA access.

Here are some tips for locking down service accounts.

- Use [Managed Service Accounts instead](#)
- Use long Strong passwords
- Give access to only what is needed
- Try to avoid granting local administrator rights
- Do not put in Domain Admins
- Deny logon locally
- Deny logon as a batch
- Require vendors to make their software work without domain admin rights

25. Use Security Baselines and Benchmarks

A default install of the Windows Operating system has many features, services, default settings, and enabled ports that are not secure.

These default settings should be reviewed against known security benchmarks.

Establishing a secure configuration on all systems can reduce the attack surface while maintaining functionality. There are several resources that provide security benchmarks.

Microsoft has a [Security Compliance Toolkit](#) that allows you to analyze and test against Microsoft's recommended security configuration baselines.

Another great resource is [CIS SecureSuite](#)

It also provides security configuration baselines. In addition, it provides tools that can scan a system and provide a report on failures.

Most of the recommended settings can be set up using Group Policy and deployed to all computers.

Here is a screenshot of the CIS Securesuite tool. It ran a scan on my computer and generated a report on all the settings that passed and failed.

Summary

Description	Tests				Scoring		
	Pass	Fail	Error	Unkn.	Score	Max	Percent
1 Account Policies	5	4	0	0	5.0	9.0	56%
1.1 Password Policy	2	4	0	0	2.0	6.0	33%
1.2 Account Lockout Policy	3	0	0	0	3.0	3.0	100%
2 Local Policies	63	41	0	0	63.0	104.0	61%
2.1 Audit Policy	0	0	0	0	0.0	0.0	0%
2.2 User Rights Assignment	27	12	0	0	27.0	39.0	69%
2.3 Security Options	36	29	0	0	36.0	65.0	55%
2.3.1 Accounts	2	4	0	0	2.0	6.0	33%
2.3.2 Audit	1	1	0	0	1.0	2.0	50%
2.3.3 DCOM	0	0	0	0	0.0	0.0	0%
2.3.4 Devices	0	2	0	0	0.0	2.0	0%
2.3.5 Domain controller	0	0	0	0	0.0	0.0	0%
2.3.6 Domain member	6	0	0	0	6.0	6.0	100%
2.3.7 Interactive logon	5	3	0	0	5.0	8.0	62%
2.3.8 Microsoft network client	2	1	0	0	2.0	3.0	67%
2.3.9 Microsoft network server	1	4	0	0	1.0	5.0	20%
2.3.10 Network access	8	4	0	0	8.0	12.0	67%
2.3.11 Network security	2	7	0	0	2.0	9.0	22%
2.3.12 Recovery console	0	0	0	0	0.0	0.0	0%
2.3.13 Shutdown	0	0	0	0	0.0	0.0	0%
2.3.14 System cryptography	0	1	0	0	0.0	1.0	0%
2.3.15 System objects	2	0	0	0	2.0	2.0	100%
2.3.16 System settings	0	0	0	0	0.0	0.0	0%
2.3.17 User Account Control	7	2	0	0	7.0	9.0	78%
3 Event Log	0	0	0	0	0.0	0.0	0%

CIS Securesuite can also scan against other systems like Cisco, VMware, Linux, and more.

Active Directory Security Checklist

Download this guide in a simple checklist format. It includes 3 bonus security tips.

[Download PDF Checklist](#)

I hope you found my list of Active Directory security best practices useful.

If you have a question or comment, please post it below.

 [Best Practices](#)

[< Run ADUC as Another User \(RUNAS\)](#)

[> 5 Best SSH Clients for Windows](#)

66 thoughts on “Top 25 Active Directory Security Best Practices”



Samir

[October 10, 2022 at 4:01 am](#)

hi, if you remove local admin account for workstation how do you install the apps again or troubleshoot?

Regards,

[Reply](#)

Robert Allen

[October 10, 2022 at 12:05 pm](#)

With an individual account that has those permissions.

I prefer using LAPS over disabling the local admin account.

[Reply](#)**Samir**[October 10, 2022 at 1:45 pm](#)

If we can't install LAPS is there any other option? Creating a new account individually in every single PC or might be create a domain account that has role for installation?

[Reply](#)**Robert Allen**[October 11, 2022 at 11:29 am](#)

Create a domain account that has install permissions. You can use group policy and restricted groups to add accounts or groups to computers.

[Reply](#)**Duff Browne**[August 12, 2022 at 3:11 pm](#)

Thanks for the excellent ideas in this. Glad I ran across it!
Do you have any warnings about domain member laptops that travel outside

the corporate network, which are connecting in via VPN? Is this a serious security concern, or manageable?

[Reply](#)

Robert Allen

[August 17, 2022 at 10:58 pm](#)

Hi Duff,

Use always-on VPN or a cloud based management solution such as intune.

[Reply](#)

Geert

[April 4, 2022 at 8:46 am](#)

First of all, great post with a lot of useful tips, thanks!

A question regarding the SAW .. it typically shouldn't have internet access, but you need internet access for O365 management, right...? 😊 Or should only O365 Portal traffic be whitelisted?

Thanks for your feedback!

[Reply](#)

Robert Allen

[April 4, 2022 at 11:35 am](#)

You could allow it through the firewall for the SAW. There are a lot of URLs and IPs that need allow. Here is the Microsoft list

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/address-ranges?view=o365-worldwide>

[Reply](#)

Michael

September 14, 2021 at 8:42 am

Thanks for this great summery of a admin best practice!

Topic 2 mentions under Scenario 2 what rights a second admin-account might have.

Is there a tutorial anywhere, how to set this up?

[Reply](#)

Robert Allen

September 16, 2021 at 3:49 pm

Seems like I remember seeing a guide from Microsoft but now I can't find it. Here is a process I use:

1. For anyone that needs admin rights to a system they get a secondary admin account

2. This secondary account gets added to an AD group that gives them access to only what they need. For example, a database administrator needs rights to the SQL server. This user's admin account will go into the AD-SQL-ADMIN group. VMware admins go into the AD-VMW group. You would need to configure each system to set these groups as administrators. Like in vmware you would need to configure it to set the AD-VMWare-Admin group as admins to that system, or whatever rights you want to give it.
3. I then monitor each privileged group for changes. Anytime a user is added/removed from an admin group I get an email alert.
4. No admin account has remote access and ideally no internet access.

[Reply](#)

Pablo

[April 10, 2021 at 12:48 am](#)

Amazing guide!

Can you please share your feedback about Account Operators and Administrators groups?

Best practices on these two groups. Thanks in advance.

[Reply](#)

Leif

March 29, 2021 at 1:49 pm

Hi,

What about securing communication between domain controllers. Any recommendations here?

Ipsec or don't do it??

[Reply](#)

Sandeep

January 19, 2021 at 3:20 pm

Excellent Guide !! Hats off

[Reply](#)

Kristof Reinkens

December 9, 2020 at 10:54 pm

really nice guide!

[Reply](#)**Robert Allen**

December 12, 2020 at 2:59 pm

Thank Kristof

[Reply](#)**Travis Widener**

November 4, 2020 at 4:44 pm

Great Info! Thank you for sharing this and I will be reading your Office 365 best practice guide when you complete it.

[Reply](#)**Fabio Moretto**

October 15, 2020 at 6:38 pm

Guide level God!

[Reply](#)

Robert Allen

November 7, 2020 at 3:52 pm

Thanks Fabio

[Reply](#)

Clement

September 22, 2020 at 9:43 am

This is a wonderful guide. Thank you very much for it. I am still new in system administration, so I need article on how to secure office 365

[Reply](#)

Robert Allen

September 24, 2020 at 11:09 am

Thanks Clement.

I'm actually working on an office 365 best practice guide. It may be awhile before I get it completed.

[Reply](#)

Dhananjay Vadukul

August 24, 2021 at 12:03 pm

Can you please share that link over here for O365 best practices...Thanks in Advance!

[Reply](#)

Robert Allen

August 24, 2021 at 1:46 pm

Hi, I don't have that guide created yet.

[Reply](#)

jon

August 27, 2020 at 9:27 pm

If using a SAW and no internet allowed on it, how do I use powershell to manage the cloud like azure or o365?

[Reply](#)

Robert Allen

January 2, 2021 at 4:20 pm

Make a firewall rule and only allow the saw access to the azure cloud and only allow the needed ports.

Example firewall rule. The FQDN is made up, you wo
correct FQDN.

Source IP: 192.168.15.10

Destination FQDN: azure.cloud.com

Destination port: https

In addition, you could require this firewall rule to include ldap authentication.

[Reply](#)

David

[August 6, 2020 at 11:37 pm](#)

Hi,

Excellent Article by the way.

What would be your recommended approach as to how to create system accounts vs user accounts. Many times have seen systems accounts created in AD like a user account. Using the same OU and DC as user account. Other than looking at the general information?

[Reply](#)**Robert Allen**

August 10, 2020 at 11:17 pm

Are you talking about service accounts? Accounts to run a service?

1. Check out Manages Service Accounts, this is probably the most secure method. – > <https://techcommunity.microsoft.com/t5/ask-the-directory-services-team/managed-service-accounts-understanding-implementing-best/ba-p/397009>
2. If its a service on a server that doesn't need access to other systems, create a local account on that server.
3. If you create a regular user account then read these tips -> <https://www.lepide.com/blog/nine-tips-for-preventing-misuse-of-service-accounts-in-active-directory/>

[Reply](#)**fabio**

July 29, 2020 at 3:05 pm

u miss a MUST in the IT server Admin procedure !!!!

APPLOCKER !!!!!

APPLOCKER for admin and user is a MUST in every server !!!!

so whitelist just installed app , and no NEW app can RUN from user.

so usually virus .exe .visual cannot run and install !!

so No more Cryptofile or virus!!

And that must do on all SERVER , Domain , active , terminal server, Gateway.

[Reply](#)

Robert Allen

[August 9, 2020 at 2:22 pm](#)

I agree. Application whitelisting is a must. I'll have to add that to the list.

Thanks for the tip.

[Reply](#)

Radim

[June 12, 2020 at 8:32 am](#)

Hello,

Great article ! 😊

I have a question, I want to know your opinion what is better for logging into domain servers (DC even member servers):

IT staff user Steve has two account. First account with "Regular Rights" (e.g. SteveD) and second account with "privileged Domain Rights" (e.g. Admin01).

Scenario 1 : Steve logs into domain server as Admin01 and he does his all job with "privileged Domain Rights".

Scenario 2 : Steve logs into domain server as SteveD and he does his job with "Regular Rights". If he needs escalate he use "run as administrator ...

Admin01".

Thanks for reply.

Reply

Robert Allen

June 20, 2020 at 8:23 pm

Hi Radim.

I would not recommend logging into a domain controller and doing daily work from there.

Logging into a computer with a regular account then escalate as needed is ok. A better option is to set up a dedicated workstation for performing tasks that require escalated rights. This dedicated workstation would be locked down with things like two factor authentication, no internet access and so on. Microsoft calls these secure admin workstations and has some good documentation on it.

<https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations>

I typically setup a server with remote desktop services for admin work. Most admin tools get installed on this server and then consoles and access to critical infrastructure can be locked down to this admin server.

Reply

Naren

June 5, 2020 at 6:03 am

Well done Bro, The best guide

[Reply](#)**Robert Allen**

June 6, 2020 at 3:03 pm

Thanks dude! 😊

[Reply](#)**Homayoon**

March 31, 2020 at 5:47 am

How about the firewall in active direcotry?

[Reply](#)**Robert Allen**

January 1, 2021 at 5:43 pm

Homayoon,

Very important, it should be enabled on every computer to add this to the article.

Thanks for the comment.

[Reply](#)

Byron

[March 8, 2020 at 4:51 pm](#)

Under the "Monitor Active Directory Events for Signs of Compromise" section, you listed some popular log analyzers:

Elk Stack

Lepid

Splunk

ManageEngine ADAudit Plus

Windows Event Forwarding

Just curious which analyzer you currently use? If you don't mind sharing.

Thanks!

[Reply](#)

Robert Allen

March 15, 2020 at 2:38 pm

I'm currently using ManageEngine ADAudit Plus. It has some really good pre-configured audit reports and it's easy to setup.

[Reply](#)

Ren

February 10, 2020 at 8:22 am

This is a fantastic guide on AD security.
Do you see a risk with OUs? Do we need to put in additional checks on OUs?

[Reply](#)

Robert Allen

February 15, 2020 at 8:14 pm

OUs are a great way to organize your users and computers. I don't see any security risk with them. I provide some OU organizing tips in another article <https://activedirectorypro.com/active-directory-management-tips/>

[Reply](#)**Geekgal**

November 20, 2019 at 5:20 pm

The best guide I have ever seen!! Thank you for publishing this, as a sysadmin this really helps to make my points to the boss.

[Reply](#)**Robert Allen**

November 23, 2019 at 9:24 pm

Geekgal, thanks for the feedback.

[Reply](#)**Vasil Lilov**

November 2, 2019 at 5:46 pm

Great article!!! I really enjoyed. Thank you for supporting the community.

[Reply](#)

Robert Allen

November 3, 2019 at 3:15 pm

Thanks for the feedback.

[Reply](#)

Brian Kelly

September 3, 2019 at 2:31 pm

Great to see this information clearly listed in a single location. If I rename the different AD 'privileged groups' can it be considered a valid security measure too?

[Reply](#)

fenrizx

August 30, 2019 at 8:48 am

well done broo!!

some new info and knowledge to me.

[Reply](#)**Robert Allen**[September 1, 2019 at 2:37 pm](#)

Thanks

[Reply](#)**William**[July 30, 2019 at 1:19 pm](#)

Hi, Robert. Excellent info here. Quick question if there are no Domain Admins what account is used to grant temporary access to Domain Admins especially since it states no one should know the Built-in Administrator password?

[Reply](#)**Robert Allen**[August 1, 2019 at 12:49 am](#)

The default domain administrator account should still be in the domain admins group. This account can be used to add accounts into the domain admins groups. The domain admin account should have a very strong password.

[Reply](#)**Inky**[July 26, 2019 at 9:11 am](#)

Outstanding guide! Thank you very much

[Reply](#)**Mike Ivanoff**[May 21, 2019 at 9:52 am](#)

Nice summary, but you haven't mentioned:
Account lockout analysis tools (which is quite important)
Sysinternals tools – there's plenty of them
Netwrix – to review audit logs (free version)

[Reply](#)**Robert Allen**[May 21, 2019 at 12:33 pm](#)

Hi Mike. There are many log and analysis tools out there, I did list a few of them under tip #8. ManageEngine ADAudit Plus is a great tool for auditing

and analyzing account lockouts. I'm also creating a simple PowerShell tool that will help troubleshoot account lockouts and test for weak passwords.

[Reply](#)

David

[May 24, 2019 at 1:17 am](#)

When will you have PowerShell tool available? Do you have a more detail list then what you posted that you can share?

[Reply](#)

Robert Allen

[May 29, 2019 at 10:35 pm](#)

Hi David. I have a lockout tool created, I'll be posting it soon. It's nothing fancy, it finds all locked account and allows you to quickly unlock it. It also has a function that finds the source of account lockouts.

[Reply](#)

Minh

[May 10, 2019 at 10:32 pm](#)

Setting account lockout threadhold to 3 is too low. Three is too low because users maybe logon to multiple computers or getting email with mobile devices which will easily cause the account lockout wh password. 10 is the lowest number recommended by Microsoft.

[Reply](#)

Robert Allen

January 1, 2021 at 5:13 pm

I agree 3 is too low and would recommend 5 bad password attempts. I would only recommend 10 if you can set your password length to a minimum of 15 characters.

[Reply](#)

Edward

April 9, 2019 at 2:09 am

Excellent, Thanks for posting this Guide.

[Reply](#)

Robert Allen

April 12, 2019 at 11:14 pm

No problem, Edward.

[Reply](#)

Rick

[March 13, 2019 at 1:50 pm](#)

Great information!! A great consolidated list of high hitting items that give you best bang for your time as system admins.

[Reply](#)

ce1

[February 12, 2019 at 10:32 am](#)

Thank you for share that information with the community

[Reply](#)

Ed Kuskowski

[January 28, 2019 at 2:31 pm](#)

Robert,

I've enabled policies according to step 7. Enable Audit policy Settings with Group Policy

If a user fails logon with bad password, will I see this on a domain controller log ? what log, where ?

I definitely see it on the workstation log, but I would like to see it on the DC. Maybe I need a rebpoot of DC's . let me know. Thanks . The guide is great

[Reply](#)

Robert Allen

January 29, 2019 at 11:06 pm

I left out some important details.

You will need to enable this in the default domain controller policy or create a new GPO and link it to the domain controllers OU. This will log security related events on the domain controllers security event logs.

[Reply](#)

Ale

September 17, 2018 at 9:18 am

Hi,

great guide, really!

What about application that may require admin rights (e.g. Backup)?
Is there any best practice in term of using one admin credentials OR create dedicated ones and assign a human responsible... ?

BR

[Reply](#)

Robert Allen

September 22, 2018 at 7:14 pm

Limit the permissions as much as you can. There are programs such as [Powerbrowker for windows](#) that can escalate permissions to a program only when its executed, you can also specify the credentials. So instead of escalating permissions to a domain account you could use the local system account.

To answer your question though I find it best to create credentials specific to the application or function. Backups for example, create an account for that program, limit permissions as much as you can so that it can only perform that function.

[Reply](#)

Leandro

August 22, 2018 at 3:16 pm

Hi There,

That`s a good guide!!!

Thank you for share that information with the commu

[Reply](#)

Robert Allen

August 23, 2018 at 11:58 am

Leandro, you are welcome.

[Reply](#)

Damon Hina

June 2, 2019 at 8:32 am

Excellent guide. Very readable.

[Reply](#)

Robert Allen

June 2, 2019 at 6:39 pm

Thanks Damon

[Reply](#)

Leave a Comment

Contact

✉ support@activedirectorypro.com

Products

AD Pro Toolkit

Active Directory Reports

Company

About

Contact

Customer Portal

Learn

Blog

Best Practices

Documentation

© 2024 Active Directory Pro LLC | [Terms and Conditions](#) | [Privacy Policy](#)