semperis

Active Directory Security Best Practices

SEAN DEUBY
PRINCIPAL TECHNOLOGIST, SEMPERIS

Within your IT infrastructure, Active Directory (AD) is the central hub for controlling access to resources and keeping your business operational. However, Active Directory's importance to your organization puts it in the crosshairs of threat actors. If Active Directory is successfully breached, attackers can get their hands on privileged credentials and potentially compromise company data security or affect applications. Implementing Active Directory security best practices is therefore an important part of planning a digital security policy.

What are Active Directory security best practices?

Protecting Active Directory means making life as difficult as possible for cyberattackers. These 12 Active Directory security best practices can help reduce the risk of security breach and increase your cyber resilience. The goal: **Reduce the attack surface to protect and harden your Active Directory environment.**

1. Maintain a minimal number of privileged users.
2. Use groups to assign privileges.
3. Secure accounts with administrator privileges.
4. Enforce modern password policies.
5. Enforce strong passwords on service accounts.
6. Conduct regular assessments to detect password policy violations.
7. Turn off the Print Spooler service.
8. Disable Server Message Block v1 (SMBv1) and restrict New Technology LAN Manager (NTLM).
9. Restrict access to domain controllers (DCs).
10. Plan for Active Directory recovery.
11. Use SID filtering across all forest trusts.
12. Monitor Active Directory for suspicious activity and unsecure configurations.

Ready to get started?

1. Maintain a minimal number of privileged users

Users with excessive privileges directly challenge security and regulatory compliance requirements. If compromised, these accounts enable attackers to gain a larger foothold in your environment. Managing privileged users is a crucial part of overall Active Directory management, but it can also be time-consuming. Large enterprises might have hundreds of accounts in privileged groups.

Some accounts might be granted excessive permissions to get new applications working quickly. Others might have inherited permissions that they no longer need. If you're responsible for granting access, solving this challenge requires you to understand the principle of least privilege and use it to determine which permissions each user or group needs to do their jobs effectively.

Begin by reviewing the following groups to verify that every member has a legitimate reason to be included:

- Enterprise Admins
- Schema Admins
- Domain Admins
- Account Operators (if applicable)
- Server Operators (if applicable)
- Print Operators (if applicable)
- DHCP Administrators
- DNSAdmins

2. Use groups to assign privileges

Leveraging groups simplifies the process of doling out permissions to users. Rather than managing permissions individually (which can lead to errors), organize users into groups and then assign appropriate permissions to those groups.

A collection of users can represent a business unit or an internal team in which users have identical needs regarding access rights. Determining who should belong to each group (e.g., who serves as a Domain Admin or Schema Admin) and which rights those groups should have requires communication between the Active Directory management team and business stakeholders.

3. Secure accounts with administrator privileges

When a domain is created in Active Directory, the local Administrator account becomes the Administrator domain account and a default member of the domain's Domain Admins and Administrators groups. If the domain is the forest root domain, the account also becomes a member of the Enterprise Admins group.

To protect this account, Microsoft recommends setting the "Account is sensitive and cannot be delegated" flag. Also verify that Group Policy Objects (GPOs) are configured to restrict the use of the Domain Administrator and built-in Administrator accounts on domain-joined systems. Specifically, block these accounts from:

- Accessing members' servers and workstations
- Logging on as a batch job
- Logging on as a service
- Accessing member servers and workstations using Remote Desktop Services

4. Enforce modern password policies

At the center of every enterprise attack or security breach, there's often a stolen password credential. In addition to using such credentials for initial access, threat actors can use the credentials to move laterally throughout the compromised environment.

For this reason, password security is paramount. However, experience in large cloud service providers has shown that traditional password policies are inadequate against modern attacks. NIST and other large organizations have updated their password policies to recognize this reality.

Brute force attacks against internet-facing services have waned. They've been replaced by password spray attacks, in which well-known common passwords are attempted against many users in an organization. Such attacks are now common—and often successful. Password spray attacks exploit users' tendency to create passwords that are easy to remember—and easy to guess.

A better strategy is to first focus on eliminating common passwords from Active Directory. This can be accomplished with third-party password filters or with Microsoft Azure AD Password Protection.

The second step to a strong password policy is to recognize that enforcing complexity can lead to passwords that users can't remember and easily recognizable patterns that attackers can quickly crack. Instead, encourage password or passphrase length, with the addition of numbers and special characters, that allow for passwords that are easy for users to remember but difficult for attackers to guess.

For example, the password **Implicate-Research1-Uncooked** can be remembered easily but (according to the Bitwarden password strength tool) would take centuries to crack. Both online sources and major password managers contain utilities to generate passphrases. A user can simply keep generating until they find a password that they can remember.

Finally, requiring password expiration is discouraged. Experience has shown that rotation forces users into easily crackable password patterns. If an organization has been breached or a user's credentials compromised, passwords should be updated. Otherwise, leave them alone.

Simultaneously implement all these controls: banning common passwords, reducing complexity, increasing length, and disabling password expiration. Otherwise, you risk the creation of easily crackable passwords.

One other good practice: Leverage the fine-grained password policy feature. Although administrators can use the default domain policy to set a single password policy for all domain members, fine-grained password policies enable admins to set stricter passwords for individual users and global groups.

5. Enforce strong passwords on service accounts

Kerberoasting is the most common way to compromise a privileged account and gain control of an Active Directory server. Kerberoasting attacks have been on the rise, by some estimates increasing 500+% since early 2022.

In this technique, a threat actor begins by gaining regular user access through phishing or another method. With that access, the attacker can easily gain a list of service accounts by enumerating service principal names (SPNs) in Active Directory.

Next, the attacker correlates these accounts with memberships in privileged groups to obtain a list of privileged service accounts. The threat actor then requests a Kerberos service ticket from one of these privileged accounts. This ticket is

encrypted with the service account's password hash, which the attacker can typically crack offline.

With the cracked service account password hash, the threat actor can quickly gain control of Active Directory. A successful Kerberoasting attack can compromise an Active Directory forest in minutes.

The only way to combat a Kerberoasting attack is to make service account passwords extremely hard to crack:

- Use a minimum of 25 characters.
- Use a password generator to create a long, complex, highly entropic password and store it in a password vault.

Consider using a group managed service account (gMSA) that automatically rotates complex passwords. (First, though, make sure you're familiar with potential vulnerabilities related to gMSAs.)

6. Conduct regular assessments to detect password policy violations

Regular reviews of password policies and settings can help to detect issues that can expose Active Directory to attack. For example, scrutinize any account with the PASSWD_NOTREQD flag set. In addition, examine accounts that are set to enable anonymous access to Active Directory, which allows unauthenticated users to query Active Directory.

7. Turn off the Print Spooler service

The Print Spooler service manages printing processes and is run by default on Windows clients and servers. Although that seems fine on the surface, any authenticated user can remotely connect to the service, request an update on new jobs, and tell the DC to send the notification to the system with unconstrained delegation. And that exposes the DC's computer account credential. Due to the risk, the best practice is to disable the service on all DCs.

8. Disable SMBv1 and restrict NTLM

DCs that enable the SMBv1 protocol are also at risk. Microsoft deprecated SMBv1, which is vulnerable to multiple attacks, in 2014 and recommends disabling it.

Similarly, restrict the use of NTLM. Many organizations are slow to disable NTLM due to the impact this action can have. However, IT leaders should consider limiting its use as much as possible.

9. Restrict access to domain controllers

Organizations should restrict access to domain controllers to limit the threat of the DC being compromised by malware:

- No web browsing should be allowed on the DC.
- GPOs linked to all DC organizational units in a forest should be set only to permit Remote Desktop Protocol (RDP) connections from authorized users and systems.

10. Plan for Active Directory recovery

Establishing a comprehensive, detailed Active Directory recovery plan is a crucial part of building cyber resilience. Organizations should back up at least two DCs per domain, including the root domain. These backups should be kept offline to prevent them from being infected by malware.

11. Use SID filtering across all forest trusts

To understand the security importance of SID filtering, consider how Active Directory access control is managed between forests.

A forest trust connects two Active Directory forests to enable users in one forest to access resources in the other. Forest trusts are essential for maintaining access in an organization with multiple forests. In one common scenario, users in a centralized account forest access applications (such as file servers or SharePoint servers) in one or more resource forests.

Every user, group, or computer (known as security principals) in an Active Directory domain and forest has a unique security identifier (SID). This identifier is used in the user's access token to grant access to resources throughout the forest using access control lists (ACLs).

I encountered a SID-related challenge back at Intel while testing the beta versions of Active Directory: When we migrated a user to a new Active Directory forest, the user lost access to their source forest resources. This happened because the SID that a user was granted in the new forest differed from the user's original SID. Thus, they lost authorization to access the resource.

Steve Grobman (now McAfee CTO) proposed to Microsoft the idea of an attribute that would contain the original SID from the source forest, thus retaining access to the original resources. Microsoft accepted this design change request and the **sIDHistory** attribute was born. During any Active Directory migration or consolidation project, **sIDHistory** is essential to maintain users' access to resources in the source forest when the user has migrated to the destination forest but the resources have not.

However, once the migration or consolidation project is complete, **sIDHistory** should be removed. A threat actor with elevated rights could take advantage of **sIDHistory** to copy a SID from a trusting domain (for example the SID of a Domain Admins group member) and add it to the sIDHistory attribute of a security principal in the trusted domain—thus granting the attacker admin rights in the trusting domain.

This is where SID filtering comes in. It removes all foreign (i.e., not the local domain) SIDs from the user's access token, thus preventing this escalation attack. **SID filtering should be enabled on all forest trusts unless a migration or consolidation process is underway**.

Unfortunately, in my experience most migration and consolidation projects never really end. They just peter out during the more difficult application migration phase, and SID History is left enabled so that users can continue to access their original resources.

Be aware that certain configuration mistakes can reduce the effectiveness of SID filtering. For example:

- Outbound forest trusts that have the **TRUST_ATTRIBUTE_TREAT_AS_EXTERNAL** flag set to true treat a cross-forest trust to a domain as an external trust, relaxing the more stringent filtering performed on cross-forest trusts.
- Trusts with either the **TRUST_ATTRIBUTE_ CROSS_ORGANIZATION_ENABLE_TGT_ DELEGATION** or **TRUST_ATTRIBUTE_ PIM_ TRUST** attribute set allow a Kerberos ticket to be delegated, decreasing the protection that SID filtering offers.

12. Monitor Active Directory for suspicious activity and unsecure configurations

Attackers often exploit configurations that enable them to quickly escalate privileges and persist undetected in your environment. Therefore, regularly audit and monitor access rights for any indications that an attack is underway or that your organization is vulnerable to attack.

Some objects, such as the **AdminSDHolder** object, are rarely changed legitimately. The **AdminSDHolder** object serves as a template of permissions for protected groups and accounts in a domain. If inheritance is enabled, an attacker might be trying to alter permissions on privileged objects controlled by **AdminSDHolder**.

Administrators should know that a change was made and be able to articulate the reason for the change. If the modification was unintentional, the likelihood of compromise is high. Monitoring for this type of activity is critical to catching attacks quickly and preventing settings from being exploited.

How Semperis can help you secure Active Directory

Semperis provides Active Directory security assessment and recovery solutions to help focus your efforts.

- The free Purple Knight security assessment tool scans Active Directory, Entra ID (formerly Azure AD), and Okta environments to quickly identify vulnerabilities in hybrid identity environments and provide prioritized, expert remediation guidance.
- Directory Services Protector (DSP) features Active Directory security assessment, automatic rollback of suspicious changes to Active Directory, and more.
- Active Directory Forest Recovery (ADFR) speeds Active Directory recovery by 90% compared with manual recovery.
- Our Migrator for AD tool and expert migration services support the three critical phases of any Active Directory consolidation, migration, or modernization project: preparation, execution, and post-migration monitoring.
- Semperis' Breach Preparedness & Response Services experts can help you review and analyze your security architecture and configurations, operational procedures, and potential attack paths. We can provide a roadmap for recommended security improvements as well as remediation and recovery plans.

Protecting Active Directory can seem like a monumental task. By adopting best practices for Active Directory security, you can raise the level of difficulty for attackers and improve the overall security posture of your environment.

Learn more about Active Directory security best practices

- Active Directory Security: Top Risks & Best Practices
- Top Tips for Protecting Active Directory
- Essential Guide to Securing Active Directory
- AD Security 101: Domain Controller Security

Semperis Headquarters
221 River Street
9th Floor
Hoboken, NJ 07030
+1-703-918-4884
info@semperis.com

Microsoft Partner
Enterprise Cloud Alliance
Microsoft Accelerator Alumni
Microsoft Co-sell
Microsoft Intelligent Security Association (MISA)

About Semperis

Semperis protects critical enterprise identity services for security teams charged with defending hybrid and multi-cloud environments from cyberattacks, data breaches, and operational errors. Purpose-built for securing hybrid identity environments—including Active Directory, Entra ID, and Okta, Semperis' patented technology protects 100+ million identities across government agencies and the world's leading enterprises.

As part of its mission is to be a force for good, Semperis offers a variety of cyber community resources, including the award-winning Hybrid Identity Protection (HIP) Conference, HIP Podcast and free identity security tools Purple Knight and Forest Druid. Semperis is a privately-owned, international company headquartered in Hoboken, New Jersey, with customers in more than 40 countries. The company has received the highest level of industry accolades, recently named to Inc. Magazine's list of best workplaces for 2023 and ranked the fastest-growing cybersecurity company in America by the Financial Times. Semperis is a Microsoft Enterprise Cloud Alliance and Co-Sell partner.