Active Directory: could any user become Domain Admin today?

This month, run PingCastle or Defender for Identity on every domain and close what lets any user reach Domain Admin: weak certificate templates, unconstrained delegation, loose permissions and a machine account quota above 0. Then retire NTLM, RC4 and stale accounts behind audit logs, and reassess quarterly.

Reviewed	Next review	Version	Written for
5 Nov 2026	**5 Dec 2026**	**1.0**	**IT and security teams running Active Directory, with or without Entra Connect or Cloud Sync**

Latest version
sheets.einblick.dev/active-directory/

If you only do five things

1. **Find the paths before attackers do.**
   Run PingCastle or Purple Knight, and BloodHound CE, on every domain. Any AD user can find and exploit its weaknesses[1].
2. **Fix certificate templates.**
   A template any user can enroll in, with a supplied subject name, client authentication and no approval, lets them impersonate anyone, even a domain admin[5].
3. **Remove unconstrained delegation.**
   Use resource-based constrained delegation instead, set **Account is sensitive and cannot be delegated** on admins and stop the Print Spooler on DCs[1].
4. **Set the machine account quota to 0.**
   By default any user can add ten computers to the domain[1]; BSI requires limiting this to admins[2]. Delegate join rights to the accounts that join PCs first.
5. **Rotate krbtgt twice a year.**
   Reset it twice, at least 10 hours apart[9], every six months and after a suspected compromise[1].

Run your first assessment

1. **What do you already own?**
   Defender for Identity (Microsoft 365 E5, E5 Security, EMS E5 or standalone[12]) shows findings in Secure Score. Its CA checks need a sensor on the CA servers[5].
2. **What does a free scan find?**
   PingCastle's open source edition is free for internal use, also by your IT provider, but not to sell as a service[22]. Purple Knight is free, needs no admin rights[23] and is barred in or for China, Russia and other listed countries[24]. Ask Semperis for its EULA first.
3. **Who can reach Tier 0?**
   Load SharpHound data into BloodHound CE (Apache 2.0[25]) and list the paths from Domain Users and Domain Computers to Tier 0. Tell your SOC first.
4. **What do you fix first?**
   What any user can exploit: templates, stray DCSync rights[10] and write access to AdminSDHolder, GPOs or admin groups. Then delegation and NTLM.
5. **When do you look again?**
   Every quarter and after major changes. For high protection needs, BSI recommends regular attack path analysis[2].

Certificate Services (ESC1 to ESC17)

- **Templates (ESC1 to ESC4, named by SpecterOps[3]).** Turn off **Supply in the request** or require approval, remove write rights for broad groups and unpublish unused templates[5].
- **CA settings (ESC6, ESC11, ESC15, ESC16).** Clear `EDITF_ATTRIBUTESUBJECTALTNAME2`, set `IF_ENFORCEENCRYPTICERTREQUEST`, patch CVE-2024-49019[5] and keep the SID extension out of `DisableExtensionList`[4].
- **Web enrollment (ESC8).** Require EPA and HTTPS[6], or remove it if unused[4].
- **Log it.** Turn on CA auditing, off by default, and alert on events 4886, 4887, 4899 and 4900[1].

NTLM and LDAP

- **Log NTLM for the whole domain.** Check that **Log Enhanced Domain-wide NTLM Logs** is on for DCs. Events 4030 to 4033 show NTLM and NTLMv1 use; Server 2019 and 2022 got them in October 2026[14].
- **Restrict it in stages.** After the audit, deny NTLM on CA, Entra Connect and Cloud Sync servers first, as Microsoft advises[6,16,17]. Then deny it domain-wide with **Restrict NTLM** and server exceptions.
- **Get ready for NTLM off by default** in the next major Windows Server release[15].
- **Require LDAP signing and channel binding** once their audit events stop, as BSI expects[2]. Defender for Identity lists clear-text binds[10].

Kerberos, delegation and krbtgt

- **Find what still uses RC4.** KDCSVC errors 203, 204, 208 and 209 show requests DCs now block; keytab devices can fail with no event[7]. Run `Get-KerbEncryptionUsage.ps1 -Encryption RC4` and reset accounts without AES keys[8].
- **Check all delegation.** Defender for Identity flags any delegation that exposes sensitive accounts[10]. Protected Users can't be delegated[1], and BSI requires privileged accounts there[2].
- **Rotate krbtgt in two steps.** Let the first reset reach every DC before the second[1]. RODCs have their own `krbtgt_` accounts[9]. Move SPN accounts to gMSAs, as the non-human identities sheet describes.

Permissions and stale objects

- **Take DCSync rights from non-admins.** Defender for Identity lists them[10]; review the remaining holders every six months[1].
- **Check who can change the admins.** Remove non-admin rights on AdminSDHolder and sensitive groups[10]. Give Domain Computers no write rights anywhere[1].
- **Clear risky attributes.** Remove passwords from descriptions, **Password not required** and **Do not require Kerberos preauthentication**[10].
- **Disable accounts idle for 90 days** and delete them weeks later[10], within your retention rules[2].
- **Guard DC and CA backups like the servers.** They hold every password hash and the CA key[1]. The ransomware sheet covers forest recovery.

Entra Connect, Cloud Sync and Seamless SSO

- **Move Connect Sync to application-based authentication** on 2.6.84.0 or later by 7 April 2027, or sync stops[16]. Keep its key in a TPM, delete the `Sync_` account and treat Application Administrators as sync admins: they can act as the app[18].
- **Rotate the `MSOL_` password** in AD and Connect every 90 days, keep it out of admin groups and drop replication rights without password hash sync[11].
- **Roll the Seamless SSO key at least every 30 days** with `Update-AzureADSSOForest`, once per forest[20]. Its holder can impersonate any synced user[11].
- **Harden Cloud Sync the same way:** gMSA agent, Tier 0 server, no NTLM[17]. For both, block soft matching and hard match takeover[16].

What you can skip

- **Paid AD audit suites first.** Fix what the free tools find, then buy continuous monitoring.
- **Studying all 17 ESC classes.** Let a scanner find them. Some need parts you may not run, like web enrollment (ESC8) or a YubiHSM (ESC12)[4].
- **Monthly krbtgt rotation.** ASD asks for every six months and after a suspected compromise[1].

What changed in 2026

- **DCs assume AES for accounts without set encryption types** since April 2026, with no rollback since July. A DC with its own `DefaultDomainSupportedEncTypes` keeps it and logs event 205 if it allows RC4[7].
- **Connect Sync tenants are moving to Cloud Sync.** Microsoft notifies each tenant of its window from July 2026, simple setups first[21].
- **Synced users can become cloud users.** Since January 2026 you can move a user's source of authority to Entra ID[21].
- **Defender for Identity's v3 sensor reached CA and Entra Connect servers** in September 2026, as a preview. October brought ESC1, ESC8 and ESC11 alerts[13].

Mistakes that cost the most

- **Re-enabling RC4 domain-wide.** A `DefaultDomainSupportedEncTypes` of 0x24 leaves every account vulnerable; allow RC4 per service[7].
- **Fixing a template, keeping its certificates.** They stay valid until they expire or are revoked[1]; revoke those issued to someone else.
- **Running the Seamless SSO rollover twice in a row.** A second run on one forest breaks Seamless SSO until users' Kerberos tickets expire[20].

What this looks like at your size

Small team, no security staff

- Have your IT provider run PingCastle or Purple Knight quarterly and fix what any user can exploit.
- Set the machine account quota to 0 and remove unconstrained delegation outside DCs.
- If all PCs are Entra or hybrid joined, you may not need Seamless SSO[19].

Growing, with IT or security staff

- Run BloodHound CE every quarter and track the paths from Domain Users to Tier 0.
- Log NTLM domain-wide and give each dependency an owner and an end date.
- Rotate krbtgt every six months from a written runbook.

Enterprise or regulated

- Put Defender for Identity sensors on every DC, online CA and Entra Connect server[12].
- Map BSI APP.2.2 into your baseline, such as Protected Users, gMSAs and AES-only Kerberos[2].
- Rehearse a forest recovery in isolation every year, as the ransomware sheet describes.

Version history

5 Nov 2026, version 1.0	Published after a copy edit and a source-by-source fact check, which made the machine account quota, LDAP, NTLM and krbtgt steps safe to roll out, updated the RC4 changes to July 2026 enforcement, added the April 2027 Entra Connect deadline and stated PingCastle's and Purple Knight's license terms for companies.

Sources

1. Detecting and mitigating Active Directory compromises. ASD, CISA, NSA, CCCS, NCSC-NZ, NCSC UK, Sep 2026. ncsc.govt.nz
2. IT-Grundschutz-Kompendium, APP.2.2 Active Directory Domain Services. BSI, Edition 2023. bsi.bund.de
3. Certified Pre-Owned (vendor research). SpecterOps, 17 Jun 2021. specterops.io
4. Certipy wiki: Privilege Escalation, ESC1 to ESC17 (tool docs). Certipy on GitHub, updated 22 Jun 2026. github.com
5. Certificates security posture assessment in Defender for Identity. Microsoft Learn, 2 Jul 2026. learn.microsoft.com
6. KB5005413: Mitigating NTLM relay attacks on AD CS. Microsoft Support, checked 5 Nov 2026. support.microsoft.com
7. KB5073381: Managing Kerberos KDC usage of RC4 (CVE-2026-20833). Microsoft Support, updated 14 Apr 2026. support.microsoft.com
8. Detect and remediate RC4 usage in Kerberos. Microsoft Learn, 6 Feb 2026. learn.microsoft.com
9. Reset the krbtgt password. Microsoft Learn, 21 May 2025. learn.microsoft.com
10. Accounts security posture assessment. Microsoft Learn, 18 Aug 2026. learn.microsoft.com
11. Hybrid security posture assessments in Defender for Identity. Microsoft Learn, 18 Aug 2026. learn.microsoft.com
12. Defender for Identity sensor v2.x prerequisites: licensing. Microsoft Learn, 8 Jun 2026. learn.microsoft.com
13. What's new in Microsoft Defender for Identity. Microsoft Learn, 28 Oct 2026. learn.microsoft.com
14. KB5064479: Overview of NTLM auditing enhancements. Microsoft Support, updated 13 Oct 2026. support.microsoft.com
15. Advancing Windows security: Disabling NTLM by default. Windows IT Pro Blog, 29 Jan 2026, updated 22 Oct 2026. techcommunity.microsoft.com
16. Microsoft Entra Connect: Prerequisites and hardware. Microsoft Learn, 16 Jan 2026. learn.microsoft.com
17. Cloud Sync prerequisites. Microsoft Learn, 22 Oct 2026. learn.microsoft.com
18. Authenticate to Microsoft Entra ID by using application identity. Microsoft Learn, 24 Jul 2025. learn.microsoft.com
19. Microsoft Entra Connect: Seamless single sign-on. Microsoft Learn, 9 Apr 2025. learn.microsoft.com
20. Microsoft Entra Seamless SSO: Frequently asked questions. Microsoft Learn, 15 Sep 2026. learn.microsoft.com
21. Microsoft Entra releases and announcements. Microsoft Learn, updated 8 Oct 2026. learn.microsoft.com
22. PingCastle README: License. Netwrix, checked 5 Nov 2026. github.com
23. Purple Knight FAQ. Semperis, checked 5 Nov 2026. semperis.com
24. Deployment restrictions. Semperis, Nov 2025. semperis.com
25. BloodHound CE license. SpecterOps, checked 5 Nov 2026. github.com