Privileged access: who could take over everything today?

This quarter, find every account, app and server that can control Active Directory or Entra ID, and cut it to a few dedicated admin accounts that hold their roles only while activated. Guard the sync servers, certificate authorities and apps that can change those accounts as strictly as the accounts.

Reviewed	Next review	Version	Written for
4 Nov 2026	**4 Dec 2026**	**1.0**	**IT and security teams running Active Directory, Microsoft Entra ID or both, with Azure and Microsoft 365 admin roles**

Latest version
sheets.einblick.dev/privileged-access/

If you only do five things

1. **Find out who holds Tier 0 today.**
   List AD admin group members, holders of Entra roles marked **PRIVILEGED**, and the apps and servers that can change them. Microsoft calls excessive privilege one of its most common findings[1].
2. **Cut standing admin rights.**
   Keep fewer than five Global Administrators, including two emergency accounts, and fewer than ten privileged role assignments[2]. Keep day-to-day accounts out of Domain and Enterprise Admins[3].
3. **Make the rest time-limited.**
   In Entra Privileged Identity Management (PIM), make roles eligible, not active, so admins activate them for 1 to 24 hours[4]. Require approval for Global Administrator[5].
4. **Guard what controls the admins.**
   Microsoft counts PAM tools, jump hosts, automation and apps with privileged roles as Tier 0[6], and the Entra Connect server too[7]. Treat certificate authorities and device management the same way.
5. **Alert on every change to Tier 0.**
   Send alerts where admins can't close them: Storm-2885 used a privileged cloud identity to close alerts[8].

Find everyone who can take over

1. **Who is in the AD admin groups?**
   Export the nested members of every group AdminSDHolder protects, including Account, Backup, Server and Print Operators[9]. Most should be empty.
2. **Who holds privileged Entra roles?**
   In **Roles & admins**, filter on **Privileged** and count active and eligible assignments, including through groups[6,5]. Add Azure subscription admins and Microsoft 365 roles managed outside Entra ID[10].
3. **Which apps act as admins?**
   List service principals with Entra roles or with Graph permissions such as `RoleManagement.ReadWrite.Directory` or `AppRoleAssignment.ReadWrite.All`, which let an app grant more privileges to itself or anyone else[11]. Add each app's owners, who can act as the app[24].
4. **Which servers and tools control them?**
   Add domain controllers, sync servers, certificate authorities, AD FS, and the hypervisors, backups and device management that reach them.

Tier 0 in Active Directory

- **Keep top admins off other machines.** Deny Domain Admins all sign-in to member servers and workstations by Group Policy, except DC jump servers[3].
- **Put admins in Protected Users.** Members can't use NTLM, RC4, delegation or offline sign-in, and their Kerberos TGTs last four hours. Test first, add admins in stages and never add service or computer accounts[12].
- **Watch AdminSDHolder.** SDProp copies its permissions to every protected account and group hourly[9], so one added permission reaches all admins.
- **Fix certificate templates.** A template any user can enroll in, with **Supply in the request** and client authentication, lets them take over any user, even a domain admin. It's a common misconfiguration[13], and Mandiant saw attackers abuse AD CS templates to create admin accounts[14].
- **Replace service account passwords.** gMSA passwords rotate automatically; Windows Server 2025 dMSAs also bind to named machines and help prevent Kerberoasting[15].

Tier 0 in Entra ID and the cloud

- **Treat three more roles like Global Administrator.** Privileged Authentication Administrators can reset its password[6], Privileged Role Administrators assign roles[19], and Conditional Access Administrators can remove the checks on PIM activation[4].
- **Use cloud-only admin accounts.** A compromised synced account can compromise Entra ID too[2]. Keep Tier 0 AD accounts out of sync[10].
- **Ask for more at activation.** Point PIM at a Conditional Access authentication context with a phishing-resistant authentication strength and sign-in frequency **Every time**[4].
- **Give apps certificates or managed identities.** Microsoft prefers them to client secrets[16], which CISA's baseline says to block[5].
- **Count device management as Tier 0.** After the March 2026 attack on Stryker, CISA urged least-privilege Intune roles and Multi Admin Approval for wipes and changes to apps, scripts and roles[17].

Paths between on-premises and cloud

- **Harden the sync server as Tier 0.** Whoever controls an Entra Connect or Cloud Sync server can change Entra users, for example reset their passwords, so require MFA for every admin[7,18].
- **Turn off matching you don't need.** Disable soft matching and hard match takeover, so an AD object can't take over a cloud account[7].
- **Watch cloud tools that reach back.** Intune and similar tools run code on managed devices. Storm-2885 used Intune to deploy scripts and open tunnels into on-premises environments[8].

Alert on these changes

- **AD admin groups.** Events 4728, 4732 and 4756 log a member added to a global, local or universal security group[19].
- **AdminSDHolder, GPOs and SID history.** Audit directory service changes: 5136 logs a changed object, 4765 SID history added to an account[19].
- **Entra roles and Azure. Add member to role** and **Add eligible member to role**[16], each Global Administrator activation[5] and elevated access to Azure[20].

- **Apps. Add app role assignment to service principal** for Microsoft Graph, **Add owner to application** and new app credentials[16].

What changed in 2026

- **Entra ID blocks hard-match takeover of admins.** Since July 2026, sync can't hard-match onto a cloud user who holds or is eligible for a privileged role[21].
- **Entra Connect Sync needs a certificate.** Run 2.6.84.0 or later with application-based authentication by 7 April 2027, or sync stops[7].
- **Domain controllers stopped assuming RC4.** Since April 2026 they assume AES for accounts without explicit encryption types, and July 2026 updates remove the rollback. Check KDCSVC events 201 to 209 for accounts still on RC4, whose tickets can be cracked offline[22].

What you can skip

- **A separate admin forest.** Microsoft now treats the red forest (ESAE) as a custom configuration for exception cases, such as disconnected environments[1]. Its PAWs, MFA and least privilege still apply.
- **A password vault before cutting rights.** Vaulting the passwords of 30 Domain Admins still leaves 30 Domain Admins. Shrink the list first.
- **PAWs for everyone in IT.** Give full PAWs, with no email or web browsing, to Tier 0 admins. Others can use hardened devices without local admin rights.

Mistakes that cost the most

- **Letting PIM licenses lapse.** Eligible assignments disappear and time-bound active ones become permanent[23].
- **Requiring approval with no active admins.** Name approvers and keep emergency accounts active, or no one can approve and you're locked out[4].
- **Running services as Domain Admins.** Kerberoasting is a common issue with service accounts[15], so one weak password can hand over the domain.
- **Leaving Azure elevated access on.** Deactivating Global Administrator in PIM leaves it on[20].

What this looks like at your size

Small team, no security staff

- Keep two emergency accounts and at most two named, cloud-only Global Administrators.
- Business Premium includes Entra ID P1, not P2: buy P2 only for admins and PIM approvers[23].
- Ask your IT provider which accounts it uses, and drop the deprecated Partner Tier1 and Tier2 roles[6].

Growing, with IT or security staff

- Put every Entra role in PIM, with approval for Global Administrator and alerts on each activation.
- Give Tier 0 admins PAWs on a management subnet, as the network segmentation sheet describes.
- Review apps with Graph write permissions, and their owners, every quarter.

Enterprise or regulated

- Run quarterly access reviews of Tier 0, licensed for reviewers and reviewed users[23].
- Put Defender for Identity sensors on AD CS servers: several certificate checks need them[13].
- Twice a year, add a test account to Domain Admins and an Entra role, and time the alert.

Version history

4 Nov 2026, version 1.0	Published after a copy edit and a source-by-source fact check, which fixed a jump server lockout and narrowed 7 statements to what the sources say.

Sources

1. Enhanced Security Admin Environment (ESAE) architecture mainstream retirement. Microsoft Learn, 14 Feb 2023. learn.microsoft.com
2. Best practices for Microsoft Entra roles. Microsoft Learn, 1 Jun 2026. learn.microsoft.com
3. Appendix F: Securing Domain Admins Groups in Active Directory. Microsoft Learn, 12 May 2025. learn.microsoft.com
4. Configure Microsoft Entra role settings in PIM. Microsoft Learn, 23 Apr 2026. learn.microsoft.com
5. CISA M365 Secure Configuration Baseline for Microsoft Entra ID. CISA (ScubaGear), ScubaGear v2.0.0, Oct 2026. github.com
6. Privileged roles and permissions in Microsoft Entra ID. Microsoft Learn, 5 Jun 2026. learn.microsoft.com
7. Microsoft Entra Connect: Prerequisites and hardware. Microsoft Learn, 16 Jan 2026. learn.microsoft.com
8. Microsoft Digital Defense Report 2026. Microsoft Threat Intelligence, Oct 2026. cdn-dynmedia-1.microsoft.com
9. Appendix C: Protected Accounts and Groups in Active Directory. Microsoft Learn, 12 May 2025. learn.microsoft.com
10. Secure access practices for administrators in Microsoft Entra ID. Microsoft Learn, 21 Nov 2024. learn.microsoft.com
11. Microsoft Graph permissions reference. Microsoft Learn, 14 Sep 2026. learn.microsoft.com
12. Protected Users Security Group. Microsoft Learn, 27 Jun 2025. learn.microsoft.com
13. Certificates security posture assessment in Microsoft Defender for Identity. Microsoft Learn, 2 Jul 2026. learn.microsoft.com
14. M-Trends 2026: Data, Insights, and Strategies From the Frontlines. Google Cloud (Mandiant), 23 Mar 2026. cloud.google.com
15. Delegated Managed Service Accounts overview. Microsoft Learn, 30 May 2025. learn.microsoft.com
16. Microsoft Entra security operations for applications. Microsoft Learn, 6 Sep 2022. learn.microsoft.com
17. CISA Urges Endpoint Management System Hardening After Cyberattack Against US Organization. CISA, 18 Mar 2026. cisa.gov
18. Prerequisites for Microsoft Entra Cloud Sync. Microsoft Learn, 22 Oct 2026. learn.microsoft.com
19. Appendix L: Events to Monitor. Microsoft Learn, 30 May 2025. learn.microsoft.com
20. Elevate access to manage all Azure subscriptions and management groups. Microsoft Learn, 10 Mar 2025. learn.microsoft.com
21. Microsoft Entra Connect: Troubleshoot errors during synchronization. Microsoft Learn, 1 Jul 2026. learn.microsoft.com
22. KB5073381: Managing Kerberos KDC usage of RC4 (CVE-2026-20833). Microsoft Support, updated 14 Apr 2026. support.microsoft.com
23. Microsoft Entra ID Governance licensing fundamentals. Microsoft Learn, 29 Jul 2026. learn.microsoft.com
24. Overview of enterprise application ownership. Microsoft Learn, 6 Dec 2024. learn.microsoft.com