Non-human identities: who owns each service account and key, and when is it rotated?

Within 90 days, list every service account, app registration, API key and token with an owner and a rotation date, and block or cap new secrets in policy. Then replace each static secret with a managed identity or federation wherever the platform supports it, and rotate the rest on a schedule your policies enforce.

Reviewed	Next review	Version
5 Nov 2026	**5 Dec 2026**	**1.1**

Written for
IT, cloud and security teams on Microsoft 365, Azure, AWS or Google Cloud, with or without on-premises Active Directory

Latest version
sheets.einblick.dev/non-human-identities/

If you only do five things

1. **List every non-human identity with an owner and a rotation date.**
   Add purpose, permissions and a review date[1]. Improper offboarding tops OWASP's list of NHI risks[2].
2. **Replace static secrets with federation.**
   Use managed identities in Azure, which are free[3], and federation elsewhere, as Microsoft, AWS and Google advise[4,5,6].
3. **Block or cap secrets in policy.**
   Block new Entra client secrets or cap them at 180 days[7], exempting apps that still need them[2,8]. Rotate Google keys: expiry can cause outages[6].
4. **Log what they do.**
   Send service principal and managed identity sign-ins to your SIEM[7]. Intruders who compromise a person's account go looking for service principals and API keys[8].
5. **Move on-premises services to gMSAs.**
   Their passwords change every 30 days[9]. Ordinary service accounts invite Kerberoasting[10].

Find every non-human identity

1. **Export Entra apps and their credentials.**
   List app registrations, service principals and managed identities with credential type and end date. Treat those with privileged roles as Tier 0, as the privileged-access sheet describes.
2. **Pull the cloud credential reports.**
   The AWS report lists access keys and their last use but skips service-specific credentials such as Bedrock long-term API keys[11]. In Google Cloud, list user-managed service account keys. The cloud configuration sheet covers removing cloud keys.
3. **Search AD for service accounts.**
   Look for user accounts with SPNs, delegation or passwords that never expire[12].
4. **Ask about the rest.**
   SaaS API keys, GitHub tokens and deploy keys, SSH keys, what your IT provider set up, CI secrets (see the supply-chain sheet) and agents (see the agentic AI sheet). Check sign-ins, disable what nobody claims, delete it after a set period[1].

Replace static secrets, platform by platform

- **Azure: managed identities.** Where an app registration is unavoidable, use a managed identity as its federated credential[3].
- **Into Entra: federated credentials.** They accept tokens from GitHub Actions, Kubernetes, Google Cloud, AWS and SPIFFE[4].
- **Into AWS: roles.** From outside AWS, use IAM Roles Anywhere with an X.509 certificate, or `AssumeRoleWithWebIdentity`[5].
- **Into Google Cloud: Workload Identity Federation.** Then block key creation; organizations created before 3 May 2024 may not block it by default[13].
- **Secrets that must stay: your platform's store.** Key Vault, AWS Secrets Manager or Google Secret Manager, each with a rotation schedule. Key Vault can trigger rotation 30 days before expiry[14]. Encryption keys are in the encryption sheet.
- **Self-hosted stores: check the license.** HashiCorp Vault's Business Source License allows internal production use, but not a competing hosted or embedded paid offering[15]. OpenBao, a fork managed by the Linux Foundation's OpenSSF[16], uses the open-source MPL 2.0[17].

Service accounts in Active Directory

- **Prefer gMSAs and dMSAs.** A Windows Server 2025 dMSA replaces a service account and disables its password, so every machine using it must support dMSA[19]. Keep user accounts out of privileged groups[12].
- **Patch BadSuccessor.** With a Windows Server 2025 DC, the right to create a dMSA in an OU let users take over any account. Users outside Domain Admins held it in 91% of environments Akamai examined[18]. Install the August 2025 fix (CVE-2025-53779)[19], limit dMSA creation to trusted admins and audit events 5137 and 5136[18].
- **Guard the KDS root key as Tier 0.** Whoever reads it can compute gMSA and dMSA passwords offline, unlogged by default. Audit reads of `msKds-RootKeyData`[20].

When a secret leaks

1. **Revoke it where it was issued.**
   Add a new credential, switch over, then delete the leaked one, or all of them if unsure[21]. Deleting it from the repository isn't enough[6]; for scanning, see the attack-surface sheet.
2. **Check whether it was used.**
   Search sign-in and audit logs since the leak for unusual sign-ins, new credentials, configuration changes and app roles[21].
3. **Rotate what it could reach.**
   Include vault secrets the identity could read[21] and, if a developer machine leaked it, that machine's SSH, API and cloud keys[8].

Monitoring, and the licenses it needs

- **Keep the logs.** Entra keeps sign-ins 7 days on Free and 30 on P1 or P2. Graph activity logs need P1 or P2 and an export[22].
- **Read the detections.** ID Protection flags leaked app credentials and anomalous activity, but not for managed identities[21].
- **Pay for details and blocking.** Workload ID Premium, $3 per workload identity a month[23], adds full risk details[21] and Conditional Access by location or risk for your own single-tenant apps[24].

What you can skip

- **An NHI security platform before a list.** Credential reports and sign-in logs hold most of the data. Buy tooling once owners are named.
- **Workload ID Premium everywhere.** Its Conditional Access covers only your own single-tenant apps[24]. Buy it for privileged ones.
- **Vaulting secrets you could delete.** A vaulted secret is still a secret, and a self-hosted vault is one more Tier 0 system.

What changed in 2026

- **Agents got their own identities.** Entra Agent ID became generally available in April 2026, and Lifecycle Workflows can hand sponsorship to a leaver's manager[25]. Entra security features for agents need Agent 365[26].
- **CISA set credential limits.** ScubaGear 2.0 recommends app secrets of up to 180 days and certificates up to 365 (enter 181 and 366)[7].
- **AWS federates outward.** Since November 2025, workloads can use short-lived tokens instead of stored API keys for external services[27].

Mistakes that cost the most

- **One person as the only owner.** Name a team too, or a leaver orphans it.
- **Expecting a policy to fix old credentials.** Entra app management policies leave existing apps and their secrets working[28].
- **Trusting private repositories.** GitGuardian's vendor report found secrets in 32.2% of internal repositories and 5.6% of public ones[29].

What this looks like at your size

Small team, no security staff

- Keep the inventory in a shared spreadsheet; review it quarterly.
- Block new Entra client secrets (free, per Microsoft's FAQ[23]), exempting apps that need them[28].

Growing, with IT or security staff

- Alert on new app credentials and on interactive service account sign-ins.
- Move AD services to gMSAs, starting with accounts that have SPNs.

Enterprise or regulated

- Buy Workload ID Premium for privileged apps; reviewing them needs P2 for reviewers[23].
- Give each AI agent a sponsor who confirms twice a year that it's still needed.

Version history

5 Nov 2026, version 1.1 Noted that Microsoft's pages disagree on licensing for app management policies; the sheet now attributes 'free' to Microsoft's FAQ.

Sources

1. Governing Microsoft Entra service accounts. Microsoft Learn, 9 Feb 2023. learn.microsoft.com
2. OWASP Top 10 Non-Human Identities Risks, 2025. OWASP, 2025. owasp.org
3. Managed identities for Azure resources. Microsoft Learn, 19 Aug 2025. learn.microsoft.com
4. Workload identity federation. Microsoft Learn, 9 Apr 2025. learn.microsoft.com
5. Security best practices in IAM. AWS, checked 5 Nov 2026. docs.aws.amazon.com
6. Best practices for managing service account keys. Google Cloud, updated 4 Nov 2026. docs.cloud.google.com
7. CISA M365 Secure Configuration Baseline for Microsoft Entra ID. CISA (ScubaGear), ScubaGear v2.0.0, Oct 2026. github.com
8. Microsoft Digital Defense Report 2026. Microsoft Threat Intelligence, Oct 2026. cdn-dynmedia-1.microsoft.com
9. Secure group managed service accounts. Microsoft Learn, 9 Feb 2023. learn.microsoft.com
10. Delegated Managed Service Accounts overview. Microsoft Learn, 30 May 2025. learn.microsoft.com
11. Generate credential reports for your AWS account. AWS, checked 5 Nov 2026. docs.aws.amazon.com
12. Secure user-based service accounts in Active Directory. Microsoft Learn, 9 Feb 2023. learn.microsoft.com
13. Manage Google Cloud security baseline constraints. Google Cloud, updated 26 Oct 2026. docs.cloud.google.com
14. Rotation tutorial for resources with one set of authentication credentials. Microsoft Learn, 7 Jul 2026. learn.microsoft.com
15. Vault LICENSE (Business Source License 1.1). HashiCorp (IBM), checked 5 Nov 2026. github.com
16. OpenBao. OpenBao (OpenSSF), checked 5 Nov 2026. openbao.org
17. OpenBao LICENSE (Mozilla Public License 2.0). OpenBao, checked 5 Nov 2026. github.com
18. BadSuccessor: Abusing dMSA to Escalate Privileges in Active Directory (vendor research). Akamai, 21 May 2025. akamai.com
19. CVE-2025-53779: Windows Kerberos Elevation of Privilege Vulnerability. Microsoft (MSRC), 12 Aug 2025. msrc.microsoft.com
20. Golden dMSA: What Is dMSA Authentication Bypass? (vendor research). Semperis, 16 Jul 2025. semperis.com
21. Securing workload identities with Microsoft Entra ID Protection. Microsoft Learn, 6 Aug 2025. learn.microsoft.com
22. Microsoft Entra data retention. Microsoft Learn, 6 Jan 2026. learn.microsoft.com
23. Frequently asked questions about Microsoft Entra Workload ID. Microsoft Learn, 18 Mar 2025. learn.microsoft.com
24. Conditional Access for workload identities. Microsoft Learn, 24 Mar 2026. learn.microsoft.com
25. Microsoft Entra releases and announcements. Microsoft Learn, 26 Jun 2026. learn.microsoft.com
26. What is Microsoft Entra Agent ID?. Microsoft Learn, 14 Apr 2026. learn.microsoft.com
27. Federating AWS identities to external services (IAM User Guide). AWS, checked 5 Nov 2026. docs.aws.amazon.com
28. Microsoft Entra application management policy API overview. Microsoft Learn, 13 Sep 2024. learn.microsoft.com
29. The State of Secrets Sprawl 2026 (vendor research report). GitGuardian, 2026. gitguardian.com