storm
a littlefish company

Securing Microsoft Administrative & Service Accounts

Microsoft
Solutions partner

AMTIVO
ISO 9001
Certified
Quality Management

AMTIVO
ISO 27001
Certified
Information Security Management

Program Code:	Guide
Author(s)	Roughan Bass; Stuart Gleasure
Reviewed by	Peter Grogan
Date:	26/05/2025
Document Version:	0.2

Change History

Version	Date	Revision Description
0.1	26/05/2025	Initial Document
0.2	10/06/2025	Following Internal Review

1. Introduction

In today's cloud-first enterprise environments, service accounts play a critical role in enabling automation, integrations, and background operations across Microsoft applications. However, when left unmanaged or misconfigured, these accounts can become significant security liabilities—often targeted by attackers due to their elevated privileges and lack of user oversight.

This guide provides a practical framework for **securing service accounts within Microsoft ecosystems** such as Azure Active Directory, Microsoft 365, and Dynamics 365. It draws on best practices from internal security assessments and customer engagements.

We outline actionable steps to **reduce risk, improve auditability, and align with principles such as least privilege and zero trust.**

Whether you're transitioning from traditional service accounts to Azure AD Service Principals, or simply looking to harden your existing configurations, this guide will help you implement robust controls that protect your organisation's data and infrastructure.

⚠ Important Disclaimer

The Client shall be solely responsible for ensuring that adequate security measures are in place to protect their internal IT applications and data. This includes, but is not limited to, implementing and maintaining appropriate access controls, user authentication, encryption, and regular security audits. The Client shall provide Storm with the necessary accounts and access rights to perform the support services and shall ensure that these accounts are configured with the least privilege necessary to perform the required tasks. The Client agrees to promptly notify the Service Provider of any security incidents or breaches that may affect Storm's access or the integrity of the supported applications or platforms.

2. Understanding the Risks

Poor management of service accounts can expose your environment to serious risks such as.

Unauthorised Access

Accounts without Multi-Factor Authentication (MFA) are vulnerable to attack.

Audit Challenges

Lack of individual accountability for shared or generic accounts make it difficult to track malicious activity.

Resource Exploitation

Compromised accounts can be used to spin up unauthorized services (e.g. Crypto-mining servers), incurring costs and damaging security posture.

Privilege Misuse

Accounts with elevated roles like Global Administrator can be misused to create or modify critical resources.

3. Recommendations and Best Practices

To help protect your environment, we recommend the following best practices:

A. Account Creation & Management

- Use dedicated service accounts for specific applications or integrations
- Avoid using personal or shared user accounts for service-related tasks.
- Follow a clear naming convention (e.g., svc_<application>_prod) for traceability

B. Apply the Principle of Least Privilege

- Assign only the necessary permissions required for the task.
- The use of Global Admin for service accounts is **NOT** recommended, especially considering service accounts often need to have MFA disabled.
- Microsoft recommends less than five global administrator accounts per tenant. Two of which are recommended to be Break Glass accounts. Global Admin accounts have access to all resources (subscriptions, mailboxes etc) within a tenant & unauthorised access can cause immense reputational damage. Extra precautions should be taken to protect and isolate Global Admin accounts, such as disabling SMS for MFA., use FIDO2 authentication methods where possible.
- Implement Role-Based Access Control (RBAC) to scope permissions appropriately in Azure.

C. Enforce Strong Authentication

- Not all service accounts are suitable for MFA. Understand what is appropriate for your accounts and implement authentication as appropriate:
    - MFA enabled on svc accounts where possible
    - Where MFA is not possible, these svc accounts need to be targeted by Conditional access policies that limit access down to trusted networks (IP ranges) & location or compliant managed devices
- Apply Conditional Access policies to limit access to trusted locations and devices.
- Block legacy authentication protocols that don't support MFA.

D. Secure Credentials and Secrets

- Use of Managed Identities /Service Principals/App registrations should all be explored as options before opting to use service accounts as these approaches are both more secure and more auditable. They also remove issues where accounts are tied to individual actors.
- Store credentials securely in Azure Key Vault.
- Rotate passwords and certificates regularly (e.g., every 90 days).

E. Monitor Activity and Set Alerts

- Enable sign-in logs and audit trails for all service accounts.
- Use Azure Monitor or Microsoft Sentinel to detect abnormal behaviour. Consider creating custom alerts to email/text action groups when a service account is logged into.
- Monitor resource usage to identify unexpected patterns (e.g., VM spikes).

F. Maintain Oversight and Governance

- Regularly review the purpose and activity of all service accounts.
- Keep an up-to-date inventory of service accounts and their access levels.
- Implement Just-In-Time (JIT) access controls where appropriate.
- Identify Lifecycle Management
    - Joiner-Mover-Leaver (JML) processes for service accounts
    - Automated deprovisioning of unused or orphaned accounts
    - Ownership assignment and review cadence

4. Customer-Controlled Account Recommendations

For customers who manage their own service accounts, including those with Global Admin roles:

- **MFA is Mandatory:** Enforce Multi-Factor Authentication on **all** service and privileged accounts where possible and use custom conditional access where it's not. Use more secure variants of MFA when possible. Consider using FIDO, MFA with Geo location, temporary access a key (for local admin) and passkeys.
- **Limit Global Admin Use:** Restrict Global Administrator role assignments to only those who require it, and leverage Azure AD Privileged Identity Management (PIM) for time-limited elevation.
- **Auditing and Accountability:** Maintain a clear record of who owns and manages each service account. Review logs monthly for signs of unusual behaviour.
- **Use Conditional Access:** Apply policies that restrict access by IP range, device compliance, or restrict access to trusted network's (IP range) plus (+) location) / or compliant managed device.
- **Avoid Shared Credentials:** Ensure every administrator and service has a uniquely identifiable account.
- **Educate Staff:** Train your IT teams and administrators on secure account practices and the consequences of non-compliance.
- **Review Admin Roles Periodically:** Conduct quarterly audits to review all privileged roles and reduce where possible.
- **Disable Legacy Auth:** Block protocols like POP, IMAP, or SMTP AUTH which do not support modern security controls.

Include a clear security policy for internal staff outlining these expectations. In environments where customers retain full control of their service accounts, it is crucial to establish these standards to reduce the risk of compromise

5. Responding to a Compromised Account

In the event of a security breach:

- Disable the affected service account immediately.
- Revoke active sessions and reset all associated credentials.
- Review audit logs to identify the scope of impact.
- Notify your internal security team and, if needed, escalate to Microsoft support.

6. Tools and Resources to Assist You

- Microsoft Secure Score (https://security.microsoft.com/securescore)
- Azure AD Identity Protection
- Azure Monitor and Microsoft Sentinel
- Microsoft Defender for Identity and Defender for Cloud
- Microsoft Purview for centralized audit logging
- Microsoft Sentinel – integrated SIEM for automated detection and response

7. Maintenance & Governance Plan

Task	Frequency	Responsibility
Review service account inventory	Quarterly	IT Security / Admin
Rotate credentials and secrets	Every 90 days	IT / DevOps
Audit account permissions	Biannually	Azure Admin
Confirm MFA compliance	Monthly	IT Security

8. Closing Note

By adopting these best practices, your organisation will be better equipped to prevent security incidents, maintain compliance and build a more resilient cloud environment.

If you have any questions or require support implementing the above recommendations, please reach out to your Storm account manager directly or via sales@storm.ie.

Appendix: 1

Storm Security Services

Storm Technology offers a comprehensive suite of security services designed to help organisations safeguard their Microsoft environments—particularly where service accounts, administrative access, and cloud-based integrations are concerned. These services are grounded in industry best practices and tailored to the specific needs of each client, ensuring both compliance and operational resilience.

Our security services include:

1. **Service Account Hardening**: Storm provides hands-on support in securing customer-managed administrative and service accounts across Microsoft Dynamics 365 and Azure. This includes implementing Multi-Factor Authentication (MFA), enforcing least privilege access, and configuring Role-Based Access Control (RBAC) to reduce exposure to privilege misuse and unauthorised access
2. **Security Assessments and Advisory:** We conduct structured reviews of your Microsoft cloud environment to identify vulnerabilities, misconfigurations, and compliance gaps. These assessments are delivered with actionable recommendations and can be aligned with ISO 27001 and other regulatory frameworks
3. **Support and Incident Response:** Our ITIL-aligned support model includes proactive monitoring, escalation management, and post-incident reviews. We offer Level 1–3 support tiers, real-time reporting, and monthly service reviews to ensure transparency and accountability
4. **Governance and Oversight:** Storm helps clients establish governance frameworks for identity and access management, including credential rotation policies, audit logging, and secure storage of secrets using Azure Key Vault

Whether you're looking to secure a single integration or overhaul your entire identity and access strategy, Storm's security services are designed to scale with your needs and provide peace of mind in an increasingly complex threat landscape.

If you wish to engage Storm specialized security services to help you evaluate, design, and implement robust controls that align with your organisation's needs and compliance obligations please request a quote on sales@storm.ie.