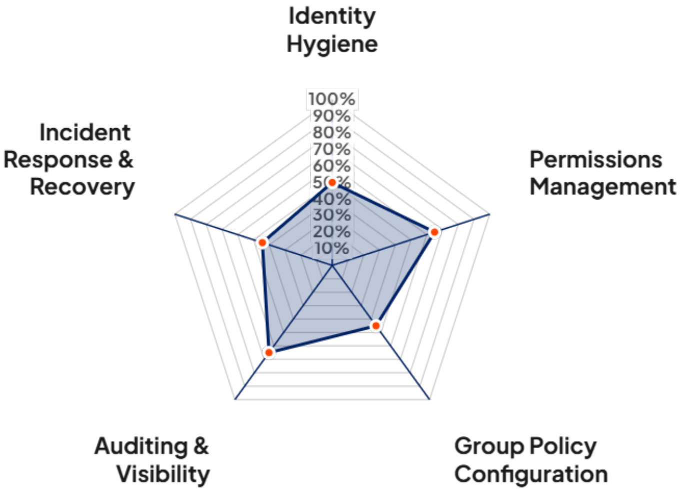
Lepide

Results of your Active Directory Security Self Assessment

Results Summary

High – you have significant AD risks to address, particularly in the Permissions Management, Auditing & Visibility categories. Use this guide to begin strengthening your AD security posture.

Category Assessment



Percent your security activities address each category of the AD assessment

Identity Hygiene	**50%**
Permissions Management	**65%**
Group Policy Configuration	**45%**
Auditing & Visibility	**65%**
Incident Response & Recovery	**44%**

Maturity Dimensions, Categories, and Security Objective Alignment

Each category in this assessment aligns to one of three core dimensions of Active Directory security maturity:

Governance, Risk, and Compliance

Ensures your AD environment meets internal policies and external regulations through continuous oversight, risk reduction, and audit readiness.

Categories aligned:

- Identity Hygiene
- Group Policy Configuration
- Auditing & Visibility

Access Control & Permissions Management

Focuses on minimizing excessive access, enforcing least privilege, and managing entitlements across users, groups, and systems.

Categories aligned:

- Permissions Management
- Group Policy Configuration

Detection & Response Readiness

Evaluates your ability to detect threats early, respond to incidents, and recover from compromise across the AD ecosystem.

Categories aligned:

- Auditing & Visibility
- Incident Response & Recovery

You can strengthen your Active Directory security posture by maturing in each of these dimensions—addressing the most common gaps that attackers exploit, and ensuring you're prepared for both audits and active threats.

Maturity Dimension	Assessment Category	Security Objective
Governance, Risk, and Compliance	**Identity Hygiene**	• Regularly identify and remove inactive, orphaned, and duplicate accounts to reduce attack surface. • Implement strict offboarding processes to ensure accounts are disabled immediately upon termination. • Automate detection of stale computer and service accounts to minimize lateral movement opportunities.
	Group Policy Configuration	• Maintain a baseline of approved GPO settings and monitor for unauthorized changes. • Regularly clean up and consolidate legacy or unused GPOs. • Track GPO linking across OUs to ensure policy inheritance is functioning as expected. • Establish ownership and change control processes for GPO management.
	Auditing & Visibility	• Enable auditing of key changes (user creation, group membership, GPO edits, etc.) across AD. • Centralize logs and integrate with a SIEM for analysis and alerting. • Protect audit logs from tampering and ensure appropriate retention policies. • Generate regular reports to support compliance with standards like ISO 27001, NIST, and GDPR.
Access Control & Permissions Management	**Permissions Management**	• Apply least privilege access models across all users and groups. • Regularly review group membership, nested groups, and inherited access rights. • Continuously identify and remediate excessive permissions. • Tie access requests and provisioning to roles and business justifications.
	Group Policy Configuration	• Enforce security baselines for access controls via GPO (e.g., password policies, lockout thresholds). • Use tiered access models to separate privileged accounts from standard users. • Prevent privilege escalation via GPO hardening (e.g., deny logon locally, restrict delegation).

Maturity Dimension	Assessment Category	Security Objective
Detection & Response Readiness	**Auditing & Visibility**	• Alert in real time on critical events (e.g., failed logins, changes to admin groups). • Correlate user activity with AD events to detect suspicious behavior. • Use behavior analytics to identify anomalies (e.g., login location, time-based deviations). • Ensure visibility across hybrid environments (on-prem and Azure AD).
	Incident Response & Recovery	• Maintain and test AD-specific incident response playbooks. • Implement rapid isolation and deactivation processes for compromised accounts. • Ensure AD backups are frequent, tested, and recoverable. • Use Lepide to track and roll back critical changes when necessary. • Practice tabletop exercises to validate response readiness for AD-related attacks.

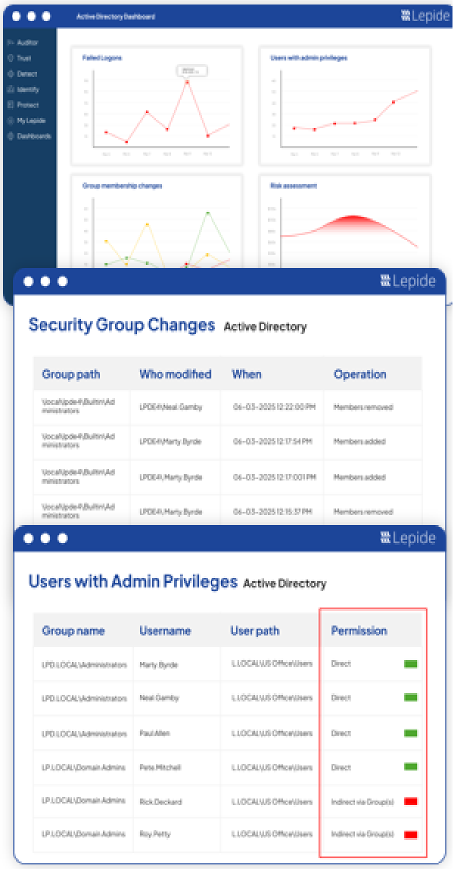
Lepide is your Partner Towards Active Directory Security.

Active Directory is at the heart of your identity infrastructure—but it's also a prime target for attackers. Misconfigurations, over-permissioned users, and lack of visibility are common challenges that create serious risk. At Lepide, we help organizations take back control of their AD environments by providing real-time auditing, risk analysis, and automated response capabilities that align with best practices for identity hygiene, access control, and incident readiness.

Our platform is purpose-built to simplify Active Directory security. From identifying stale or orphaned accounts, to detecting changes in group membership permissions, Lepide ensures you know exactly who has access to what—and when that access changes. With continuous monitoring, instant alerts, and prebuilt reports for compliance audits, we empower both IT teams and CISOs to move from reactive firefighting to proactive security.

Whether you're just starting your AD security journey or looking to optimize an existing program, Lepide gives you the visibility, control, and confidence to protect what matters most.

Talk with an Active Directory expert today to see how we can help you.



Security Group Changes Active Directory

Group path	Who modified	When	Operation
\local\lpde4\Builtin\Administrators	LPDE4\Neal Gamby	06-03-2025 12:22:00 PM	Members removed
\local\lpde4\Builtin\Administrators	LPDE4\Marty Byrde	06-03-2025 12:17:54 PM	Members added
\local\lpde4\Builtin\Administrators	LPDE4\Marty Byrde	06-03-2025 12:17:00 PM	Members added
\local\lpde4\Builtin\Administrators	LPDE4\Marty Byrde	06-03-2025 12:15:37 PM	Members removed

Users with Admin Privileges Active Directory

Group name	Username	User path	Permission
LPD.LOCAL\Administrators	Marty Byrde	L.LOCAL\US Office\Users	Direct 🟩
LPD.LOCAL\Administrators	Neal Gamby	L.LOCAL\US Office\Users	Direct 🟩
LPD.LOCAL\Administrators	Paul Allen	L.LOCAL\US Office\Users	Direct 🟩
LP.LOCAL\Domain Admins	Pete Mitchell	L.LOCAL\US Office\Users	Direct 🟩
LP.LOCAL\Domain Admins	Rick Deckard	L.LOCAL\US Office\Users	Indirect via Group(s) 🟥
LP.LOCAL\Domain Admins	Roy Petty	L.LOCAL\US Office\Users	Indirect via Group(s) 🟥

Your Answers

Identity Hygiene

To what degree of coverage do you have in the following areas:	Your Answer
1. Inactive user accounts are identified and reviewed regularly to ensure they are removed or disabled in a timely manner.	**High**
2. Stale or unused computer accounts are monitored and cleaned up to reduce attack surface.	**Medium**
3. Service accounts are documented, reviewed regularly, and validated for legitimate use.	**Low**
4. Accounts belonging to former employees or third parties are promptly disabled or deleted following offboarding.	**Low**
5. Duplicate, orphaned, or misconfigured accounts are identified and resolved as part of routine hygiene.	**High**
6. All active user accounts can be confidently tied back to valid, known identities.	**Medium**
7. Temporary accounts are provisioned with expiration dates and reviewed periodically.	**Low**
8. Account creation is controlled via an approval workflow and clear ownership.	**Medium**
9. Key account lifecycle events (creation, modification, deletion) are tracked and visible.	**High**
10. Privileged service accounts are reviewed regularly to ensure they remain necessary and are appropriately secured.	**Medium**

Permissions Management

To what degree of coverage do you have in the following areas:	Your Answer
1. Group memberships are reviewed regularly to identify excessive or unnecessary access.	**High**
2. Nested group structures are monitored to detect and reduce hidden permissions.	**Medium**
3. The principle of least privilege is applied consistently across user and group assignments.	**High**
4. Membership in privileged groups (e.g., Domain Admins) is actively audited and tightly controlled.	**Medium**
5. Elevated permissions that are no longer required are identified and revoked promptly.	**Low**
6. Access to sensitive systems or data is clearly documented and regularly reviewed.	**High**
7. Permissions are adjusted when users change roles, departments, or responsibilities.	**Medium**
8. Privilege escalation paths are analyzed and remediated to reduce risk.	**Medium**
9. Access provisioning is role-based and aligned to business function.	**High**
10. Visibility into share-level and NTFS-level permissions is maintained across critical file systems.	**Medium**

Group Policy Configuration

To what degree of coverage do you have in the following areas:	Your Answer
1. Group Policy changes are monitored and reviewed on a regular basis.	**High**
2. Unauthorized or unexpected changes to GPOs can be quickly detected and investigated.	**Low**
3. Approved GPO configurations are documented and used as a baseline for comparison.	**Medium**
4. GPO sprawl is kept under control through regular consolidation and cleanup.	**Medium**
5. Key security settings (e.g., password and lockout policies) are enforced through GPOs and monitored.	**High**
6. GPOs are tested in a controlled environment before deployment to production systems.	**Low**
7. Legacy or unused GPOs are reviewed and removed as part of routine maintenance.	**Low**
8. GPO linking across domains and OUs is documented and reviewed for accuracy.	**Low**
9. Policy changes can be correlated with user or system activity to support investigations.	**Medium**
10. GPO ownership is clearly defined, and version control or change tracking is in place.	**High**

Auditing & Visibility

To what degree of coverage do you have in the following areas:	Your Answer
1. Changes to privileged groups (e.g., Domain Admins) are audited in real time.	**High**
2. Group Policy Object (GPO) changes are logged and reviewed regularly.	**Medium**
3. Failed login attempts and account lockouts are tracked and investigated in a timely manner.	**High**
4. User account changes — including creation, deletion, and password resets — are audited.	**High**
5. User and service activity can be correlated with specific AD changes.	**Medium**
6. Reports for AD activity can be quickly generated for security or compliance purposes.	**High**
7. Access to critical AD-integrated systems (e.g., file servers, Exchange) is audited centrally.	**Medium**
8. Alerts are triggered for high-risk or suspicious AD behavior.	**Medium**
9. Audit logs are actively monitored for signs of insider threats or misuse.	**Medium**
10. Logs are protected from tampering and retained securely in accordance with policy or regulation.	**Low**

Incident Response & Recovery

To what degree of coverage do you have in the following areas:	Your Answer
1. Documented procedures are in place for responding to AD-related security incidents.	**Medium**
2. Compromised accounts can be isolated or disabled quickly during an incident.	**High**
3. Changes made to AD can be rolled back to a known good state, when needed.	**Low**
4. Active Directory backups are performed and regularly tested for recoverability.	**Medium**
5. Alerts are configured to detect high-risk or anomalous AD activity in real time.	**Low**
6. Incident response procedures are tested through exercises or simulations.	**Medium**
7. Lateral movement or privilege escalation attempts can be detected within AD.	**Low**
8. AD logs are integrated with a centralized SIEM or SOC platform.	**N/A**
9. Indicators of compromise specific to AD (e.g., Pass-the-Ticket, Golden Ticket) are actively monitored.	**Medium**
10. Post-incident analysis can reconstruct a timeline of AD activity and attacker behavior.	**High**