LEPIDE

LEPIDE
DEEP DIVE

AD AUDIT REPORTS

TOP 10 AD AUDITING REPORTS FOR SYSADMINS

The relentless threat of data breaches demands proactive defense for every organization. Lepide's core mission is to provide comprehensive visibility into your data, empowering you to understand exactly what's happening and take necessary steps to minimize risk and maintain compliance.

www.lepide.com

Top 10 AD Auditing Reports for Sysadmins

Threats

Data breaches are a serious threat to any organization, and so action needs to be taken to minimize the risk of these threats to a minimum. The focus at Lepide is to provide visibility over what's happening with your data, and through visibility, you can take the necessary steps to mitigate risk and stay compliant.

Identify

Lepide Auditor for Active Directory provides a straightforward and comprehensive approach to auditing your Active Directory changes. It overcomes the limitations of native auditing and helps ensure security and compliance. It tracks object modification changes, permission changes, user login history, account lockouts, and more.

Overview

Active Directory (AD) is a database and set of services that connects users with the resources they need to do their work. It is a fundamental element of any Microsoft Windows environment and plays an essential part in authentication, access management, account management, and authorization. It is because of this that it's crucial to engage in Active Directory auditing and reporting best practices.

Reports

Our AD auditing software addresses critical information about user account changes in Active Directory, including when a user account was created, deleted, locked out, disabled, deleted, changed, or when the name of an account was changed. All this information is presented in easy-to-read, filterable, searchable, and sortable reports.

Limitations of Native Active Directory Auditing Methods

Microsoft does have some auditing capabilities for Active Directory, but these capabilities have several limitations, which are described as follows:

- To get an accurate picture of AD activity, administrators must analyze the security event log for each domain controller where auditing is enabled
- Critical aspects of Active Directory, such as Group Policy, are either partially audited or not audited at all.
- The log data can be noisy and hard to interpret. Events often contain irrelevant or difficult-to-understand information, plus a single audited event can generate multiple events in the log

A more straightforward approach is to use Lepide Auditor for Active Directory. The focus at Lepide is to provide visibility over what's happening with your network and through visibility you can take the necessary steps to mitigate risk and stay compliant.

1. Group Membership Changes

Group membership specifies groups of users with access privileges to sensitive resources within an organization. If a potential attacker gains access to a group that has privileged credentials, it gives them the permissions they need to get inside critical systems. It is, therefore, crucial to monitor Active Directory group membership changes to maintain a secure IT environment and to meet compliance regulations.

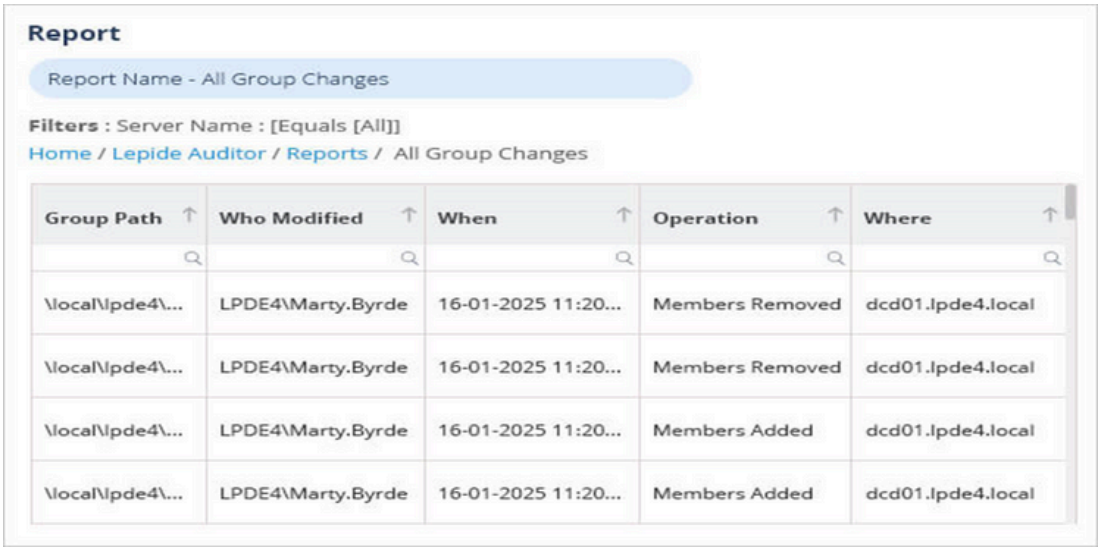
Native Method

Using native methods, you can use Active Directory Users and Computers (ADUC) to review user object properties manually. An alternative is to use PowerShell scripts to generate reports that list specific domain local group names (such as Enterprise Admins and Domain Administrators) and then manually check which groups a particular user account belongs to. However, both options are time-consuming and can be complex, and if you want to filter your report or add more details, you will need more expertise in PowerShell scripting and cmdlet parameters.

The Lepide Group Membership Changes Report

A more straightforward method is to use the Group Membership Changes Report from the Lepide Auditor for Active Directory. The Group Membership Changes Report shows activity where members have been added or removed from groups. The report includes information such as who made the change, when the change was made, and what the change was.

The following is an example of the Lepide Group Membership Changes Report:



2. Users With Admin Rights

Auditing is essential to ensure data security in any enterprise that uses file servers to store and share data. Proper monitoring of all file servers in a domain can help identify unwanted or potentially damaging events, including file accesses and read events on files containing sensitive data.

Using Native Methods

Using PowerShell, you can use the Get-LocalGroupMember cmdlet to get members of the local administrator group. For example:

Get-LocalGroupMember -Group "Administrators"

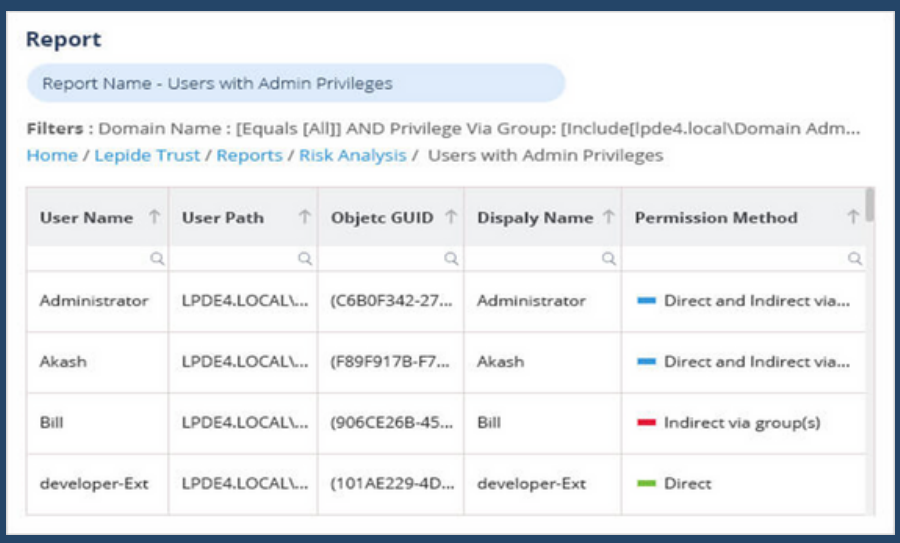
In Windows, you can use the Computer Management snap-in (compmgmt.msc) to view, add, or remove users in the local Administrators group.

By default, when a Windows computer is joined to an Active Directory domain, administrator rights are granted to local administrator users and the Domain Admins security group.

The Lepide Users With Admin Rights Report

A more straightforward method which requires no knowledge of PowerShell is to use the Lepide Users with Admin Privileges Report. This report allows you to gain complete visibility into who holds privileged access within your organization. You can see which users have administrative privileges and how those privileges are derived.

The Lepide Solution also allows you to easily identify users that have excessive permissions based on their data usage patterns, leveling up your privileged access management efforts.



3. The Inactive Users Report

The misuse of user privileges is one of the main sources of data breaches within an organization, and so action must be taken to keep the risk of these threats to a minimum. One such threat is inactive or stale users. Accounts can become obsolete for many reasons, including long absences or employees leaving an organization, and these obsolete accounts could be used by an attacker or former employee to gain access to the network and cause a data breach.

Once you have visibility over any inactive user accounts, it is a straightforward process to take action to disable or remove them. However, while constant monitoring of user accounts is achievable, it can be complex and time-consuming without the right solution in place.

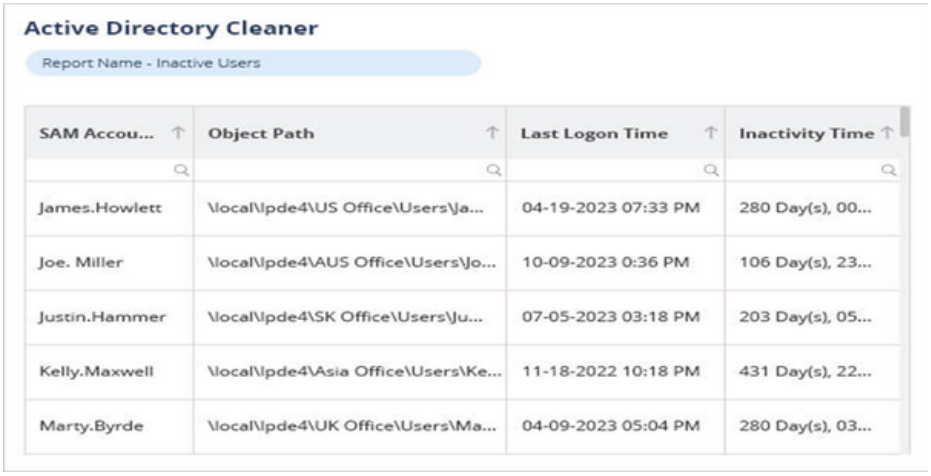
Using Native Methods

You can use the Microsoft Entra ID admin center or the Microsoft Graph API to find inactive user accounts. However, there isn't a built-in report for these accounts, so you would need to use the Last interactive sign-in time to identify inactive user accounts. Another native method is to use PowerShell to find Inactive Users in AD by filtering on the user's LastLogonDate; however, this method requires knowledge of PowerShell scripting.

The Lepide Inactive Users Report

A more straightforward approach is to use Lepide's Active Directory Cleanup solution which provides a complete solution to simplify the detection and clean-up of obsolete accounts in Active Directory.

The Inactive Users Report lists all inactive users including account information such as SAM Account Name, email address and Inactivity Time in days. The report includes the option to change the number of days where an account is deemed to be inactive; in the example below, it is the default value of 30 days.



4. Users Whose Password Never Expires

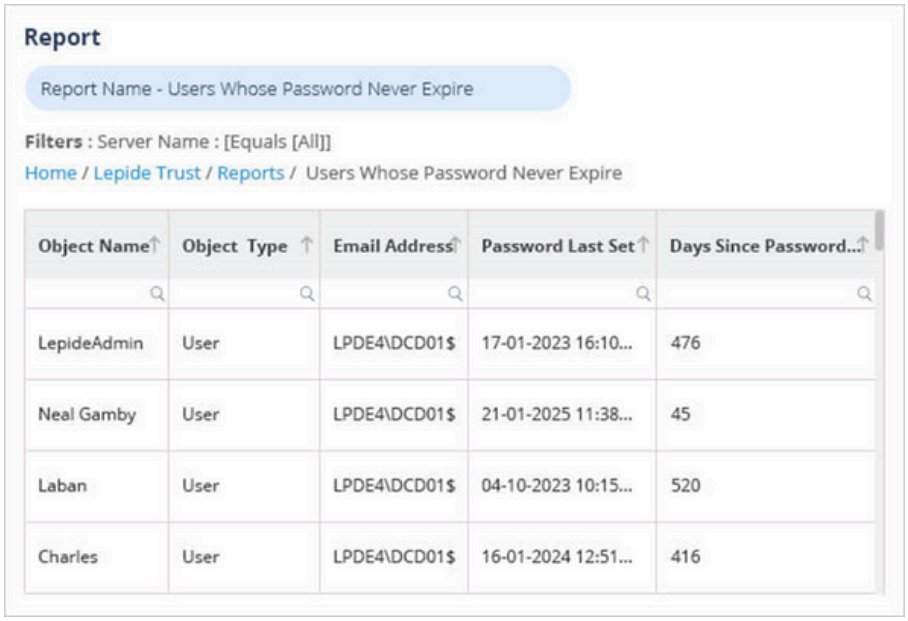
Passwords set to never expire in Active Directory pose multiple security risks including password compromise, compliance risk, and increase chances of phishing or social engineering attacks. If an attacker gains access to this account, they will have access forever. It is good security practice, therefore, to regularly audit your domain user accounts for any that have the "**Password never expires**" option enabled.

Using Native Methods

Users whose password never expires can be listed using the get-aduser cmdlet in PowerShell. However, this method requires a good knowledge of PowerShell.

The Lepide User Whose Password Never Expires Report

With Lepide, you can generate a detailed report on users with passwords that never expire so that you can reduce your potential threat surface area and implement stricter password policies. An example of this report is shown below:



Report

Report Name - Users Whose Password Never Expire

Filters : Server Name : [Equals [All]]

Home / Lepide Trust / Reports / Users Whose Password Never Expire

Object Name	Object Type	Email Address	Password Last Set	Days Since Password...
LepideAdmin	User	LPDE4\DCD01$	17-01-2023 16:10...	476
Neal Gamby	User	LPDE4\DCD01$	21-01-2025 11:38...	45
Laban	User	LPDE4\DCD01$	04-10-2023 10:15...	520
Charles	User	LPDE4\DCD01$	16-01-2024 12:51...	416

5. Failed Logons

Visibility over user activity in your critical systems is a crucial part of identifying potential suspicious behavior which may lead to security breaches. Tracking user actions provides the necessary information to spot malicious activity and stop an organization falling victim to a potential cyberattack.

The auditing of logon events in Active Directory (AD) is a mandatory task to help with the detection of malicious activity. Any anomaly in the audit report will help to detect security risks in multiple ways; for example, an employee's account becoming locked out after multiple logon failures is a potential threat to a company's data security.

A login failure could just be an employee who has forgotten their credentials. However, in a different scenario, it could be a hacker trying to enter the network through an employee's legitimate account. So, any failed login attempt needs to be monitored to mitigate any security risk.

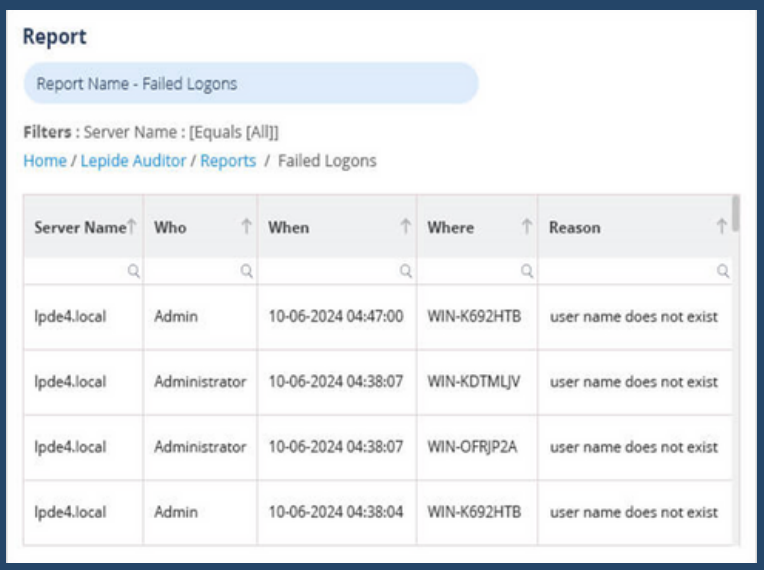
Using Native Methods

Logon activity can be monitored using the native Active Directory auditing tools. This is done by enabling auditing using the Group Policy Management console and then using Event Viewer to see the logs and review events.

The Lepide Failed Logon Reports

Although logon activity can be monitored using the native methods, it is a time consuming and often complex task. Lepide Active Directory Auditor overcomes the limitations of native auditing by giving you pre-defined reports which provide the visibility you need to detect and react to insider threats quickly and efficiently.

Using the Lepide Solution, you can run the Failed Logons Report to see Who, When, Where and Why logons have failed. An example of this report is shown below:



Report

Report Name - Failed Logons

Filters : Server Name : [Equals [All]]

Home / Lepide Auditor / Reports / Failed Logons

Server Name	Who	When	Where	Reason
lpde4.local	Admin	10-06-2024 04:47:00	WIN-K692HTB	user name does not exist
lpde4.local	Administrator	10-06-2024 04:38:07	WIN-KDTMLJV	user name does not exist
lpde4.local	Administrator	10-06-2024 04:38:07	WIN-OFRJP2A	user name does not exist
lpde4.local	Admin	10-06-2024 04:38:04	WIN-K692HTB	user name does not exist

6. Account Lockouts

A common problem for Active Directory administrators is how to identify the source of frequent account lockouts. If user accounts are getting locked out frequently for any reason, it may result in downtime, and it can often be a time-consuming and frustrating process to get the AD account re-enabled.

There are several reasons why accounts can become locked out and here are some of the most common causes: Hackers and password guessing attacks, Outdated windows cached credentials, Mobile devices and disconnected sessions, Scheduled tasks, Services using expired passwords, Users forgetting their passwords.

Using Native Methods

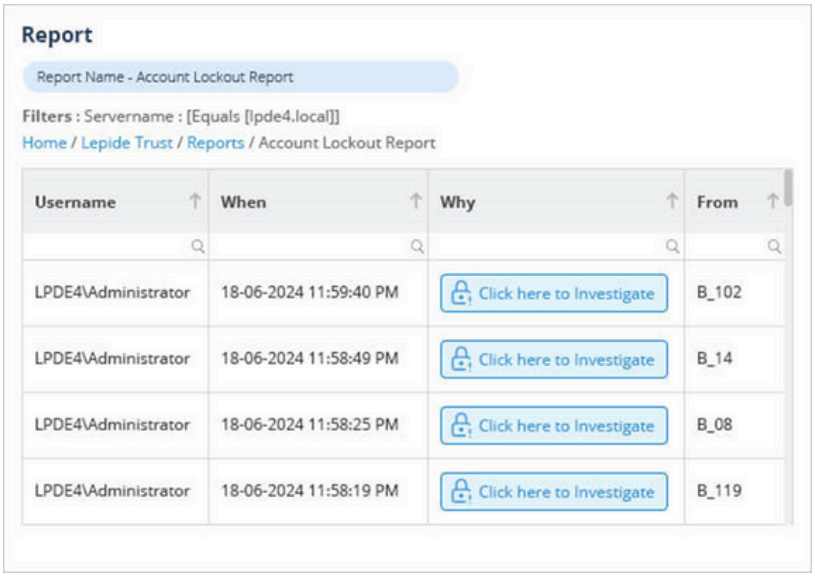
An account lockout threshold can be set to specify the number of times a user can attempt to log on with an invalid password before their account is locked. The amount of time an account stays locked out can also be defined using the account lockout duration setting. These account lockout policies help guard your network against password guessing attempts and potential brute-force attacks.

The native way of finding account lockouts is to search the event logs for Event ID 4740 using the Event Log Viewer.

The Lepide Account Lockout Report

An alternative, more straightforward, solution is to use the Account Lockout Report, which is one of the pre-defined reports included in the Lepide's Active Directory Auditing tool. An example of this report is shown below. It provides information including the Username, When the lockout happened, Why it happened and Where.

An example of the Account Lockout Report is shown below:



7. Admin Group/Security Group Changes

Users who have administrative privileges are the most important users within your organization, but they also represent the biggest risk to your data security. For this reason, particularly in today's world of ever-increasing cyber risk, it is imperative to limit the number of user accounts with administrative privileges to the bare minimum and to have visibility over any changes to administrative groups.

The Principle of Least Privilege (PoLP) is an information security concept in which a user is given the minimum levels of access needed to perform their job functions. Applying this principle is a highly effective way to greatly reduce the chance of an attack within an organization.

Once this has been followed within an organization, it is essential to have visibility over any subsequent changes made to these administrative user groups. The adding or removal of admin users needs to be monitored so that the number of users with admin privileges stays at the bare minimum. In this way, companies can remain compliant and reduce the chance of a security breach.

It is essential, therefore, for organizations to have visibility over these changes. But as organizations grow, and Active Directory structures evolve, being able to keep track of what modifications are happening within the admin user group can become a complex and time-consuming task.

Using Native Methods

Changes made to AD groups will result in an event being logged in the security log of the domain controller. This will happen once the Audit Security Group Management policy has been enabled with Success events logging.

Event ID 4732 is logged when a member was added to a security-enabled local group and 4728 is logged when a member was added to a security-enabled global group. Events can then be viewed using the Windows Event Viewer.

An alternative native method is to use a PowerShell script. You can use the Get-WinEvent PowerShell cmdlet to get information about all the recent 4732 and 4728 events on a domain controller in the last 24 hours.

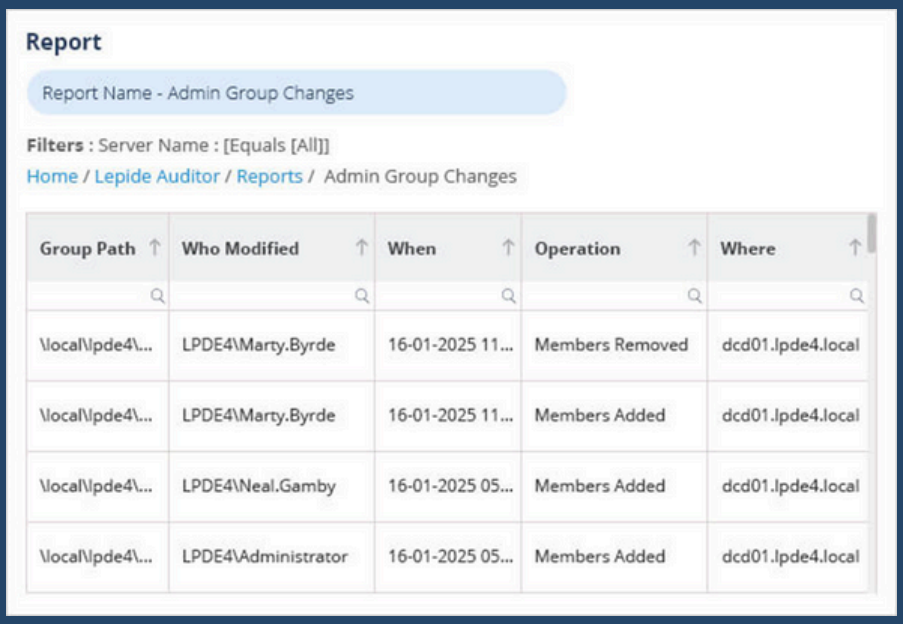
While these native methods provide the information required, it is a time consuming and complex way to achieve this.

The Lepide Admin Group Changes Reports

Lepide overcomes this complexity and provides visibility in a clear and easy-to-understand way. By running the Admin Group Changes Report, you can quickly identify all changes within the admin group.

The report can be run immediately and/or scheduled to run on a daily, weekly, or monthly basis therefore providing up-to-date visibility to mitigate the risk of privilege abuse.

Here is an example of the Admin Group Changes Report:



Report

Report Name - Admin Group Changes

Filters : Server Name : [Equals [All]]

Home / Lepide Auditor / Reports / Admin Group Changes

Group Path	Who Modified	When	Operation	Where
\local\lpde4\...	LPDE4\Marty.Byrde	16-01-2025 11...	Members Removed	dcd01.lpde4.local
\local\lpde4\...	LPDE4\Marty.Byrde	16-01-2025 11...	Members Added	dcd01.lpde4.local
\local\lpde4\...	LPDE4\Neal.Gamby	16-01-2025 05...	Members Added	dcd01.lpde4.local
\local\lpde4\...	LPDE4\Administrator	16-01-2025 05...	Members Added	dcd01.lpde4.local

8. Password Policy Changes

Implementing strong password policies in Active Directory is a fundamental requirement to maintain security and meet compliance regulations.

By regularly monitoring password policies, any potential vulnerabilities or weaknesses in your system can be identified and immediate action can be taken to address them. This includes monitoring password strength requirements, expiration dates, and enforcing multi-factor authentication.

Using Native Methods

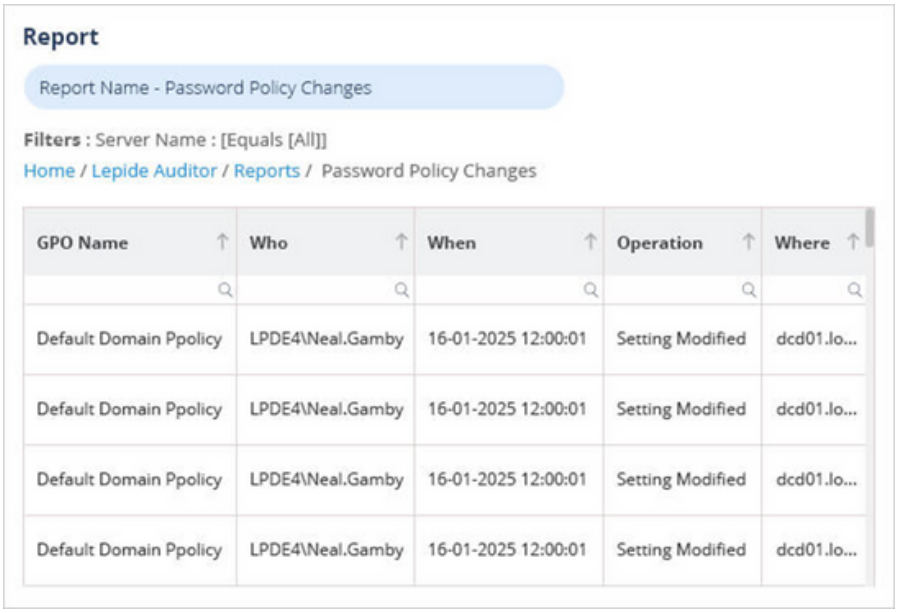
There are native tools you can use to validate and manage your Active Directory password policies:

- **Group Policy Management Console:** Navigate to Computer Configuration, Policies, Windows Settings, Security Settings, Account Policies, Password Policy to view and edit each password policy in your domain.
- **PowerShell:** Use '**Get-ADDefaultDomainPasswordPolicy**' to view the current password policy in your default domain policy. You can also use 'Get-ADFineGrainedPasswordPolicy' to examine your current FGPPs.

The Lepide Password Policy Changes Report

The Lepide Solution is a more straightforward way to have visibility over Password Policy Changes using the Password Policy Changes Report. An example of this is shown below and includes information such as Who made the change, When it was made and What was changed.

The following is an example of the Password Policy Changes Report:



9. Activity Outside of Business Hours

A user account is compromised when an attacker gains access to credentials to perform actions on behalf of the targeted user. There are several ways in which potentially compromised user accounts can be detected, however, without a solution in place, this can be a complex and time-consuming process. It is essential to not only be able to track potentially compromised users but also to react quickly enough to mitigate any damage.

One indication of a compromised user account is if the user logs on outside of business hours, or outside of their normal working pattern. This could happen because either their account has been compromised, or they plan to act maliciously. There are, of course, situations when users have legitimate reasons to log onto the system out of hours but by having visibility over all out of hours activity, anomalies can be detected which trigger alerts and the threat mitigation process initiated.

Using Native Methods

1. Event Viewer: The Windows Event Viewer allows you to examine event logs, including security-related events like login attempts and user actions.

2. Group Policy: You can utilize Group Policy settings to enable auditing and tracking of activities on Windows servers and workstations.

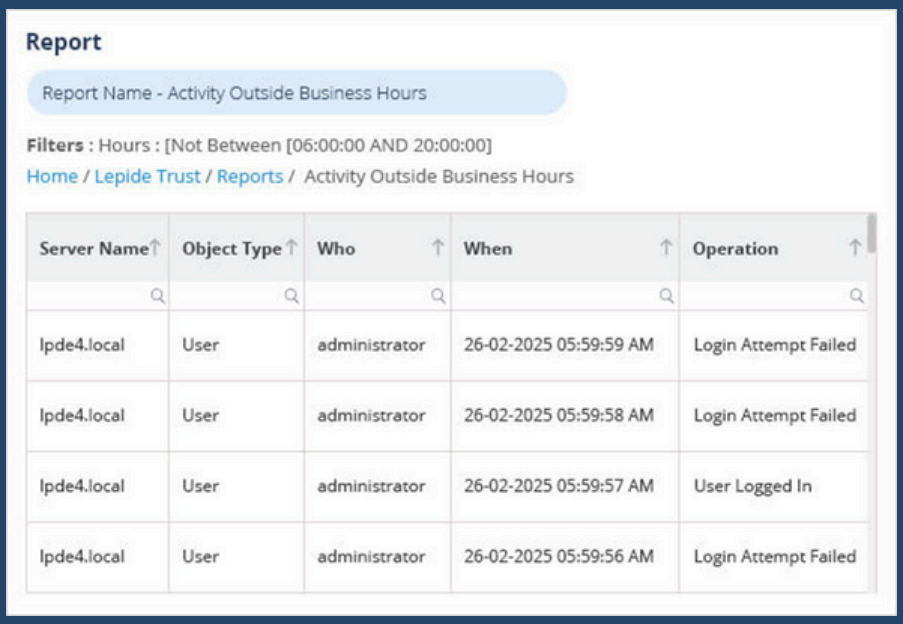
3. PowerShell: There are several different tools to get information about the time of a user logon to an Active Directory domain. The time of the last successful user authentication in an AD domain may be obtained from the user lastLogon attribute (it is only updated on the domain controller on which the user is authenticated) or the lastLogonTimpestamp attribute (it is replicated between the DCs in a domain, but only in 14 days by default).

You can check the value of the user attribute using the AD attribute editor or with the Get-ADUser PowerShell cmdlet.

The Lepide Activity Outside of Business Hours Report

Within the Lepide solution, a summary of activity outside of business hours is provided by the Activity Outside of Business Hours Report.

This report will show all out of business hours activity within a selected time scale and can be further filtered to focus on whatever data is required. Alerts can be configured to run with this report so that if suspicious activity is detected, an alert is sent, and a manual or automated response activated to reduce any damage and stop any further malicious activity.



Report

Report Name - Activity Outside Business Hours

Filters : Hours : [Not Between [06:00:00 AND 20:00:00]

Home / Lepide Trust / Reports / Activity Outside Business Hours

Server Name	Object Type	Who	When	Operation
lpde4.local	User	administrator	26-02-2025 05:59:59 AM	Login Attempt Failed
lpde4.local	User	administrator	26-02-2025 05:59:58 AM	Login Attempt Failed
lpde4.local	User	administrator	26-02-2025 05:59:57 AM	User Logged In
lpde4.local	User	administrator	26-02-2025 05:59:56 AM	Login Attempt Failed

10. User/Computer Status Changes

Auditing user account changes in Active Directory is crucial for ensuring the security, integrity, and accountability of an organization's IT environment. Here are the key reasons why auditing AD user account changes is important:

User account changes, such as password resets, account lockouts, or privilege modifications, can be indicators of unauthorized access attempts or insider threats. Auditing these changes allows for the early detection of suspicious activities and potential security breaches, enabling organizations to take immediate action to mitigate risks and protect sensitive information.

In addition, many regulatory frameworks, including the Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act (SOX), require organizations to maintain comprehensive audit trails of user account changes. Auditing user account changes helps demonstrate compliance with these regulations, ensuring that the organization's IT environment is monitored and controlled effectively.

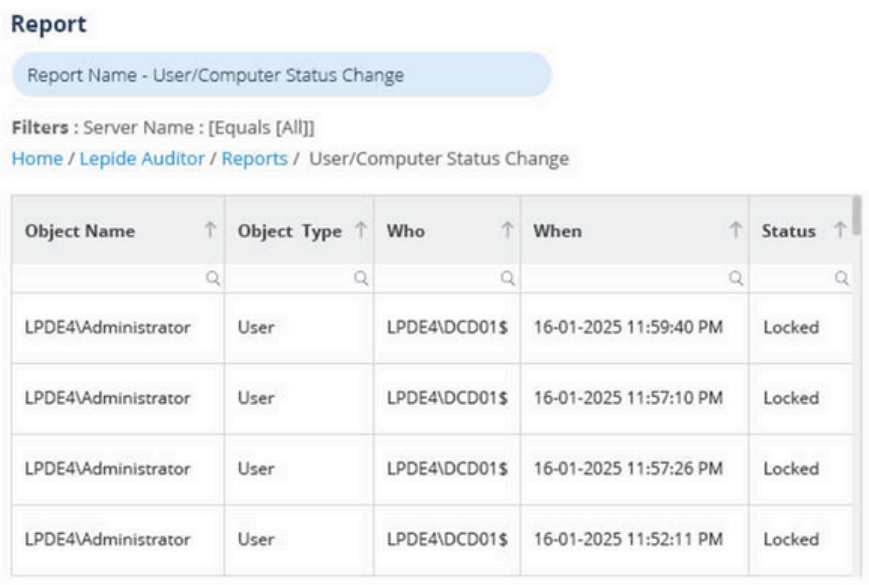
Using Native Methods

To track user account changes in Active Directory, open Windows Event Viewer, and go to Windows Logs, Security. Use the Filter Current Log option in the right-hand pane to find the relevant events.

The Lepide User/Computer Status Change Report

Lepide presents critical information about user account changes in Active Directory, including when a user account was created, deleted, locked out, disabled, deleted, changed, or when the name of an account was changed. All this information is presented in easy-to-read, filterable, searchable and sortable reports.

The following example shows the User/ Status Change Report. All audit information about when the status of a user account has changed is shown in a single line record:



Report

Report Name - User/Computer Status Change

Filters : Server Name : [Equals [All]]

Home / Lepide Auditor / Reports / User/Computer Status Change

Object Name	Object Type	Who	When	Status
LPDE4\Administrator	User	LPDE4\DCD01$	16-01-2025 11:59:40 PM	Locked
LPDE4\Administrator	User	LPDE4\DCD01$	16-01-2025 11:57:10 PM	Locked
LPDE4\Administrator	User	LPDE4\DCD01$	16-01-2025 11:57:26 PM	Locked
LPDE4\Administrator	User	LPDE4\DCD01$	16-01-2025 11:52:11 PM	Locked

About Lepide

Mission

Our mission is to break the mold by delivering simple auditing and security solutions that enable organizations to protect their data and user directories, minimize their risks, and thrive.

Who we are

At Lepide, we believe that managing and securing your data shouldn't be complicated. Since 2005, we've empowered thousands of companies to protect and manage their unstructured data effectively. Lepide audits and protects files and folders, and the systems that govern access to them, without requiring a massive IT security team to manage it.

Why we exist

52% of organizations do not have the tools to confidently handle insider threats. 63% of companies admit that sensitive files are accessible to all employees. Companies simply don't have the visibility to detect threats and lack the speed to respond. Most enterprise-grade solutions that try to address these problems come with high costs and steep learning curves. Not Lepide.

What we do

- Lepide audits and protects files, folders, and access control systems.
- We offer this protection without requiring a large IT security team.
- Lepide unifies data security and Active Directory (AD) auditing across on-premises and cloud platforms.
- We provide enterprise-grade security at a non-enterprise cost.
- Lepide emphasizes faster reporting.
- The platform is designed for ease of use.
- Lepide is competitively priced.

Lepide in Numbers

Customers

1,000+

AND CLIMBING

Employees

100+

AND CLIMBING

Global Offices

3

AND CLIMBLING!

Solutions up close

Lepide Auditor

Find out more

Change Auditing and Reporting Solution

Audit and report on changes taking place to your key systems and data to help reduce your threat surface area, detect threats and meet compliance demands.

Lepide Trust

Find out more

Permissions Analysis Solution

Get instant visibility over the changes being made to permissions and determine users with excessive permissions to implement a policy of least privilege.

Lepide Detect

Find out more

Real Time Threat Detection and Response Solution

Pre-defined threat models, and automated threat response, mean you can detect the signs of a compromise or security incident, and react in real time before it causes significant damage.

Lepide Identify

Find out more

Data Discovery and Classification Solution

Persistent data classification adds context to your security efforts. E-Discovery helps to speed up privacy and data subject access requests.

Lepide Protect

Find out more

Permissions Management Software

Easily define, monitor, and adjust permissions across your environments to prevent unauthorized access to sensitive information by ensuring that only authorized personnel have access to critical data.

Lepide IQ

Find out more

Our AI helper

Lepide IQ, ensures that organizations stay agile by interrogating data faster to provide essential information on demand and in turn saving valuable time in decision-making processes.