ManageEngine
Log360 Cloud

PROACTIVE AD MONITORING

with Log360 Cloud

5 CRITICAL USE CASES

Enterprises rely on Active Directory (AD) because of its ability to manage and organize resources such as users, computers, and services in a centralized, secure manner. As a result, there is always the possibility that threat actors will target AD and make modifications and configuration changes to gain unauthorized access, leading to data breaches, service disruptions, and other security incidents. In this document, we will look at five critical use cases that IT administrators and security teams should consider when it comes to securing their AD environment.

1. Auditing GPO modifications

A group policy object (GPO) defines various settings for users and computer accounts inside an AD environment. Any unauthorized GPO change related to privileges, access to information or services, or security settings can lead to outages as well as security challenges.
Auditing GPO modifications in AD is crucial because of the following reasons:

1. Auditing critical policy changes like changes to account lockout policy and password change policy helps in detecting and responding to malicious activities instantly.

2. Monitoring any unauthorized change or modification to GPO security changes is crucial. Some modifications—like reducing the password complexity or length requirements, disabling Windows firewalls, or allowing remote desktop services on insecure networks—make the organization vulnerable to potential security breaches.

3. Auditing GPOs is also crucial, as it is used to manage the policy settings for Windows Updates across organizational units. Monitoring these changes would ensure that these policies are configured properly, preventing any unapproved changes that may pose a threat to their security.

PROBLEM:

Imagine a scenario where a malicious actor gains unauthorized access to the AD environment and modifies GPO settings. The attacker might weaken password policies, disable critical security configurations, or grant unauthorized access to sensitive files.

Let's take the example of an attacker who wants to weaken the password policies so that they can have unauthorized access to the user accounts.

In a native AD environment, the password policy settings are configured through GPO settings, usually found in the Default Domain Policy.

One of the settings associated with password policies is Minimum Password Length.

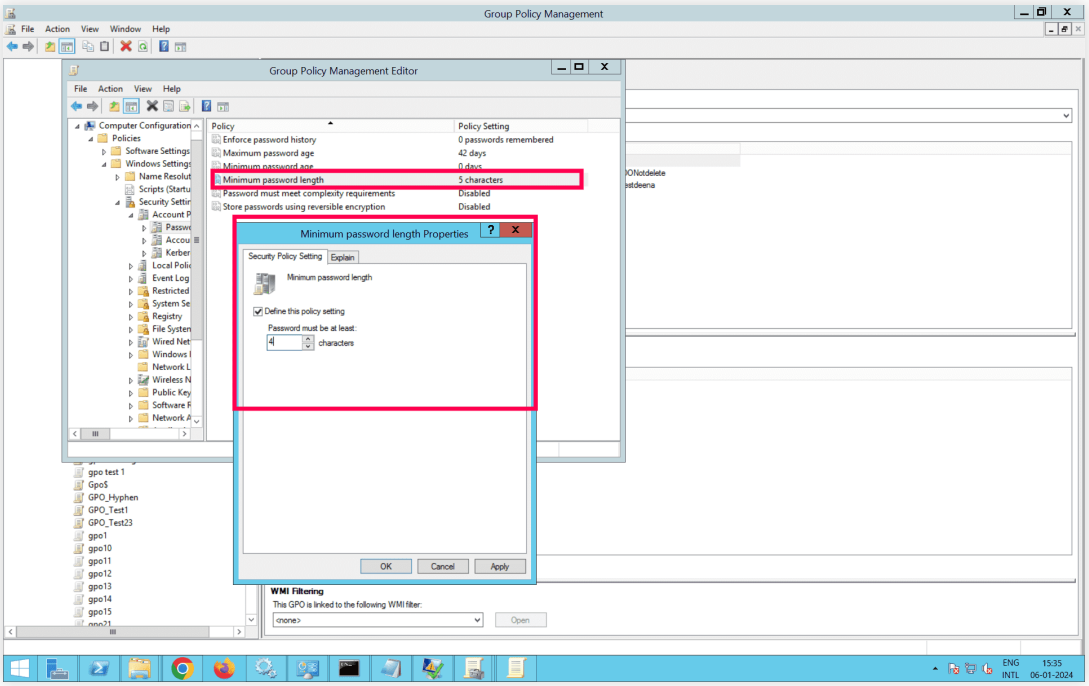

Fig. 1: Modifying the minimum password length property

The attacker might modify this configuration to weaken the password policy by reducing the minimum password length, thus increasing the vulnerability of user accounts.

SOLUTION:

GPO Setting Changes > Password Policy Changes

In Log360 Cloud (See Figure 2):

1. Go to the **Reports** tab.
2. Navigate to **Devices** in the dropdown, then the **Active Directory** menu.
3. Go to **GPO Setting Changes > Password Policy Changes.**

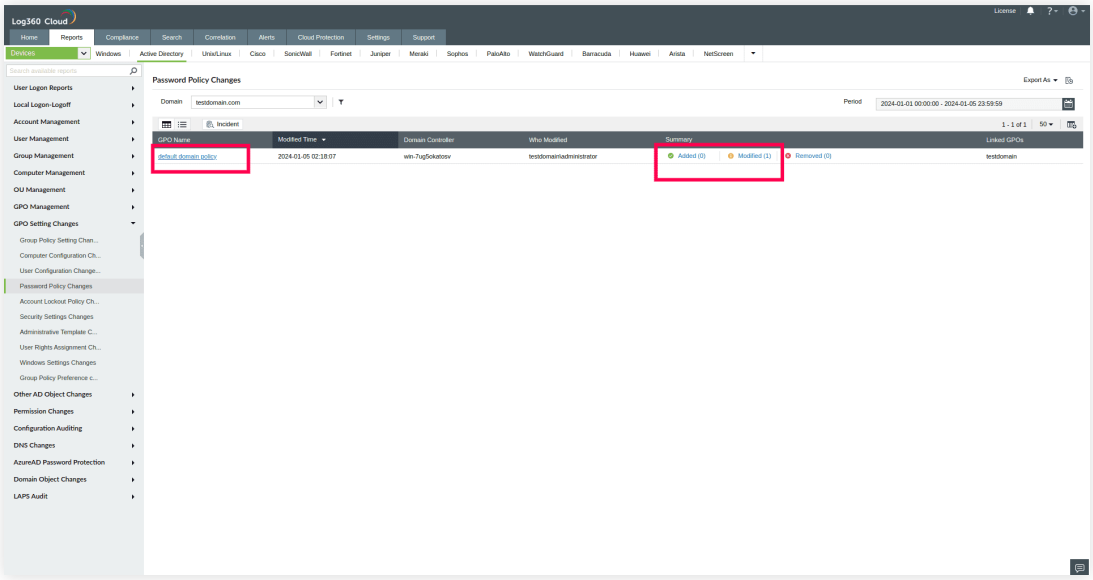

Fig. 2: Password Policy Change

4. Click on the change reported.
5. View the changed GPO setting (as shown in Figure 3)

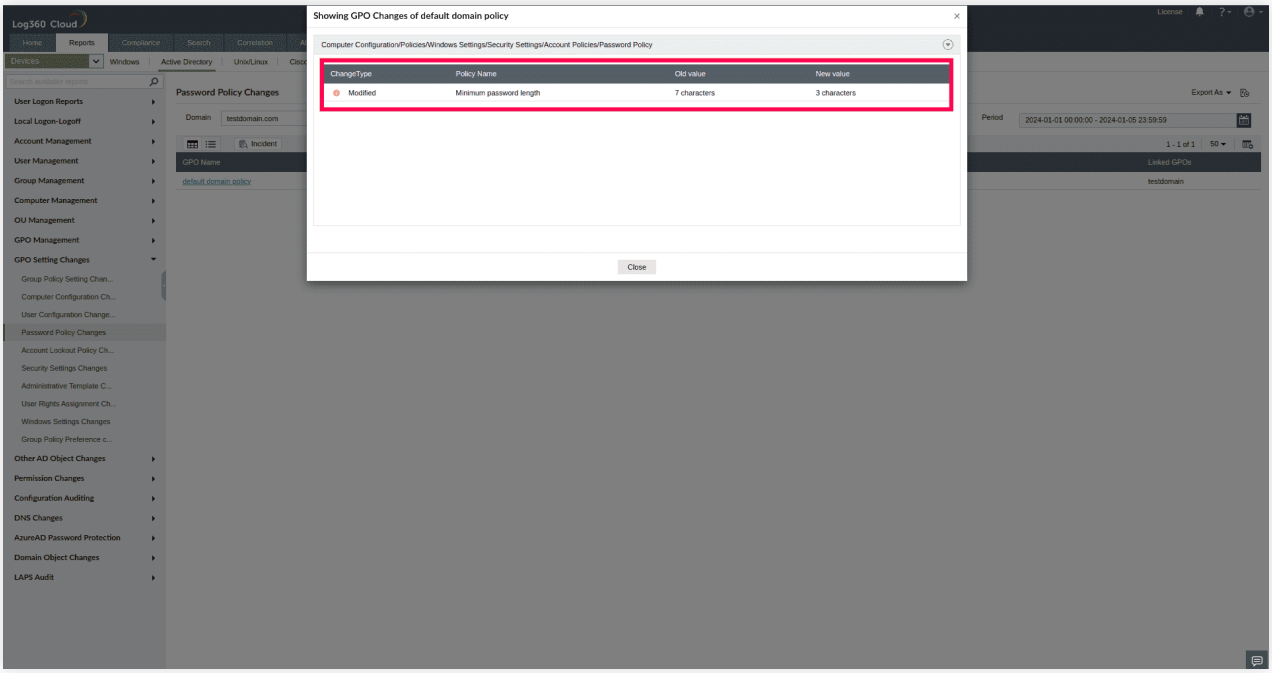

Fig. 3: GPO Changes to default domain policy

2. Auditing recently created users

A user, with the right account permissions, can make almost any change to the AD environment.

PROBLEM:

Consider a scenario where an intruder creates a new user account and adds this user to a privileged group. User creation can be a part of the kill chain the attacker uses to navigate within the network. This user might gain unrestricted access to sensitive data, depending on the group they were added to.

SOLUTION:

User Management > Recently Created Users

In Log360 Cloud (See Figure 4):

1. Go to the **Reports** tab.
2. Navigate to **Devices** in the dropdown, then the **Active Directory** menu.
3. Go to User **Management > Recently Created Users.**
4. View the recently created users.

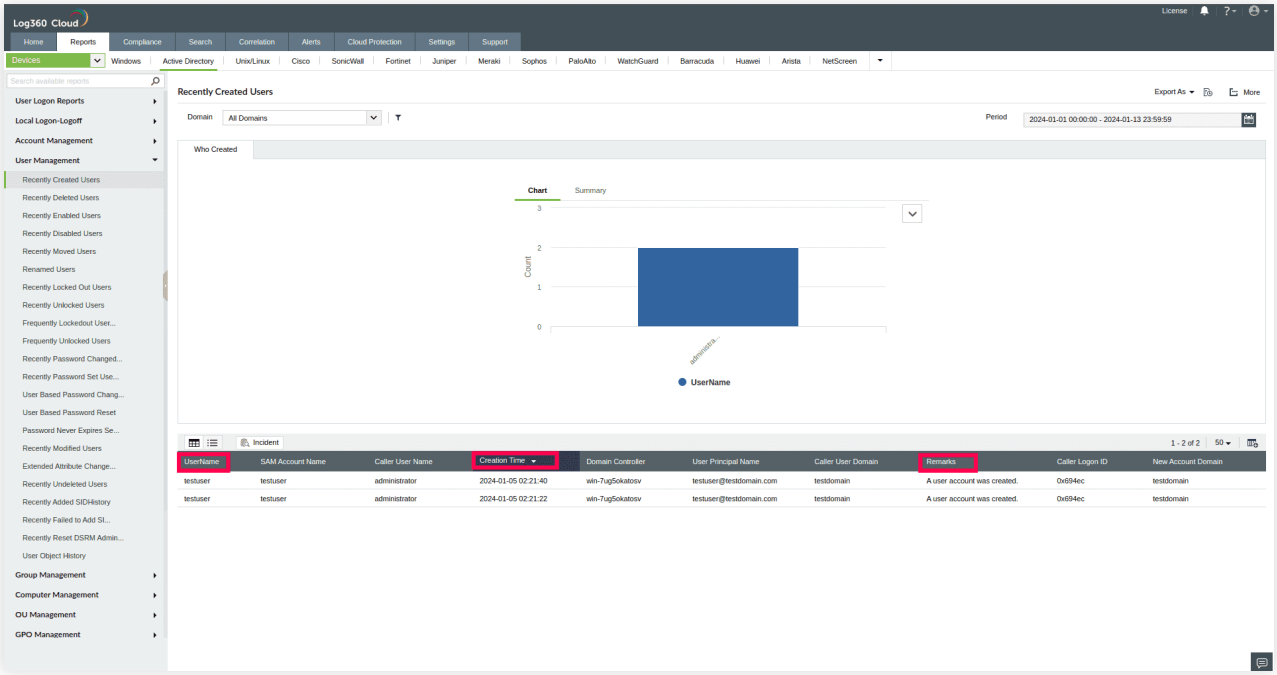

Fig. 4: Recently Created Users

3. Auditing recently enabled users

Malicious actors may attempt to enable user accounts that have remained in the stale or disabled state for extended time periods to avoid detection. Instances where the disabled account has administrative privileges can lead to privilege escalation, granting the attackers elevated permissions.

PROBLEM:

Consider a case where a disabled user account has been enabled and misused by malicious agents. This can facilitate lateral movement within the network. Since disabled accounts attract less attention, re-enabling one may help an attacker maintain a stealthier presence in the network. Auditing recently enabled users is especially important when it comes to changes in user privileges. Sudden modifications to user accounts, such as enabling administrative access, could indicate a security incident or an attempt to escalate privileges.

SOLUTION:

User Management > Recently Enabled Users

In Log360 Cloud (See Figure 5):

1. Go to the **Reports** tab.
2. Navigate to **Devices** in the dropdown, then the **Active Directory** menu.
3. Go to **User Management > Recently Enabled Users.**
4. View the recently enabled users.

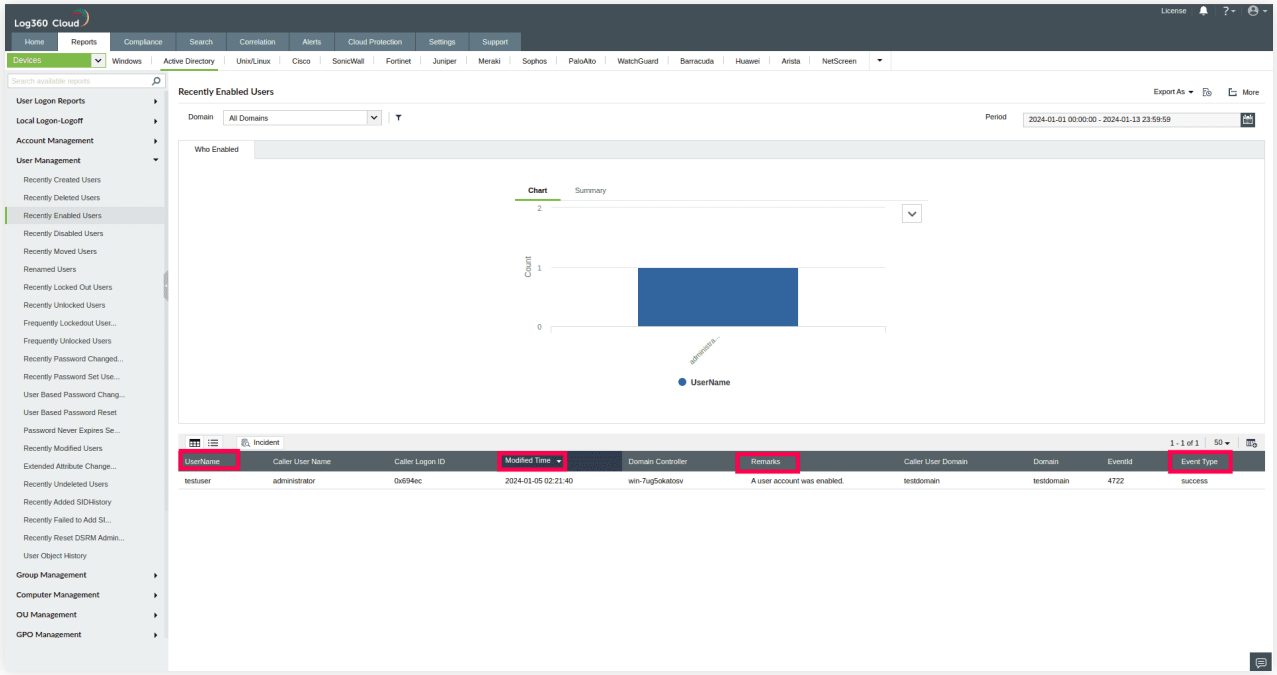

Fig. 5: Recently Enabled Users

4. Auditing recently modified OUs

It is critical to audit changes to organizational units (OUs) because they are an administrative boundary. They can contain users, computers, groups, and other OUs within them. Policy settings may be applied at an OU level by linking a GPO to an OU. Any unauthorized modification such as adding a user to an OU can pose a threat to the organization's security posture, as all the settings applied to the OU will also be applicable to the newly added OU.

PROBLEM:

Imagine that an attacker blocks a specific OU from inheriting the security policies the admin has deployed by manipulating the Group Policy Inheritance settings of the OU. This would mean that the users and computers within that OU are vulnerable to malicious activity.

SOLUTION:

OU Management > Recently Modified OUs

In Log360 Cloud (See Figure 6):

1. Go to the **Reports** tab.
2. Navigate to **Devices** in the dropdown, then the **Active Directory** menu.
3. Go to **OU Management > Recently Modified OUs.**
4. View the recently modified OUs.

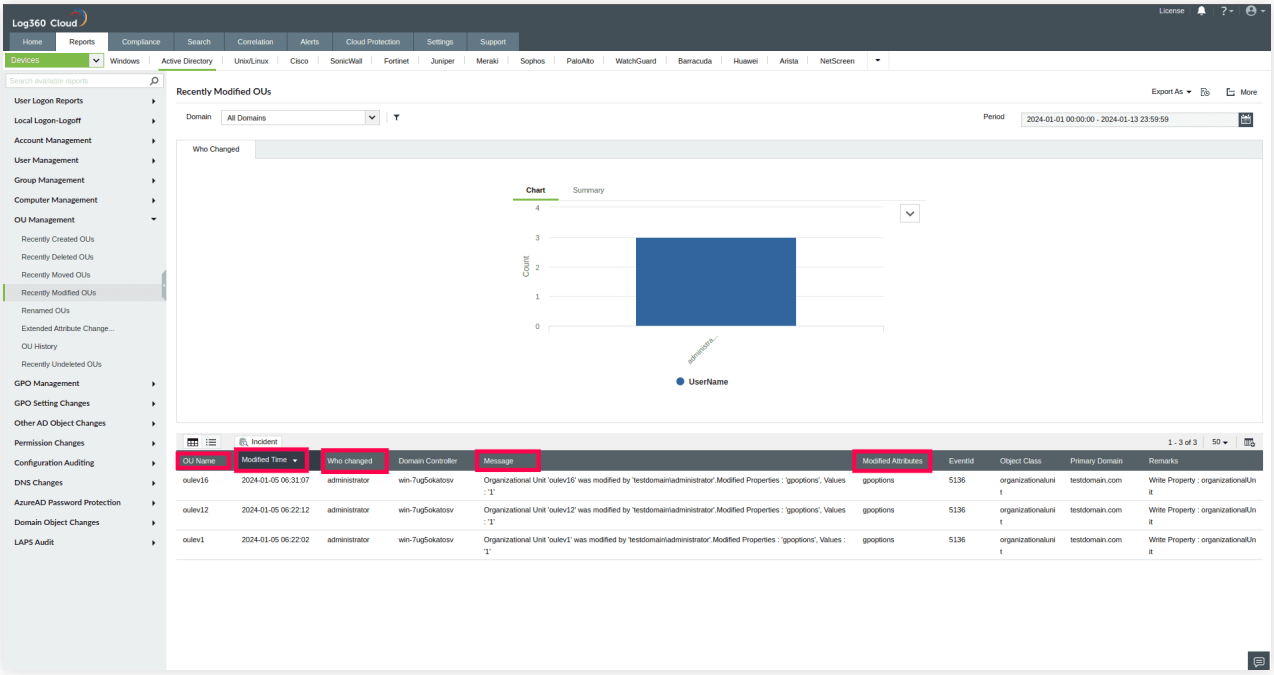

Fig. 6: Recently Modified OUs

5. Auditing new members added to the Domain Admins security group

The Domain Admins group in AD is used to assign administrative roles to users in the domain. By default, this group is a member of the Administrators group and therefore carries a set of privileges associated with it.

Members of the Domain Admins group have unrestricted access to shared resources and AD objects.

PROBLEM:

Consider a scenario where a malicious actor adds a new user to the Domain Admins group. This would provide the new member with unrestricted access to shared resources and AD objects.

SOLUTION:

Group management > Recently Added Members to Security Groups

In Log360 Cloud (See Figure 7):

1. Go to the **Reports** tab.
2. Navigate to **Devices** in the dropdown, then the **Active Directory** menu.
3. Go to **Group Management > Recently added Members to Security Groups.**
4. View the recently modified OUs.

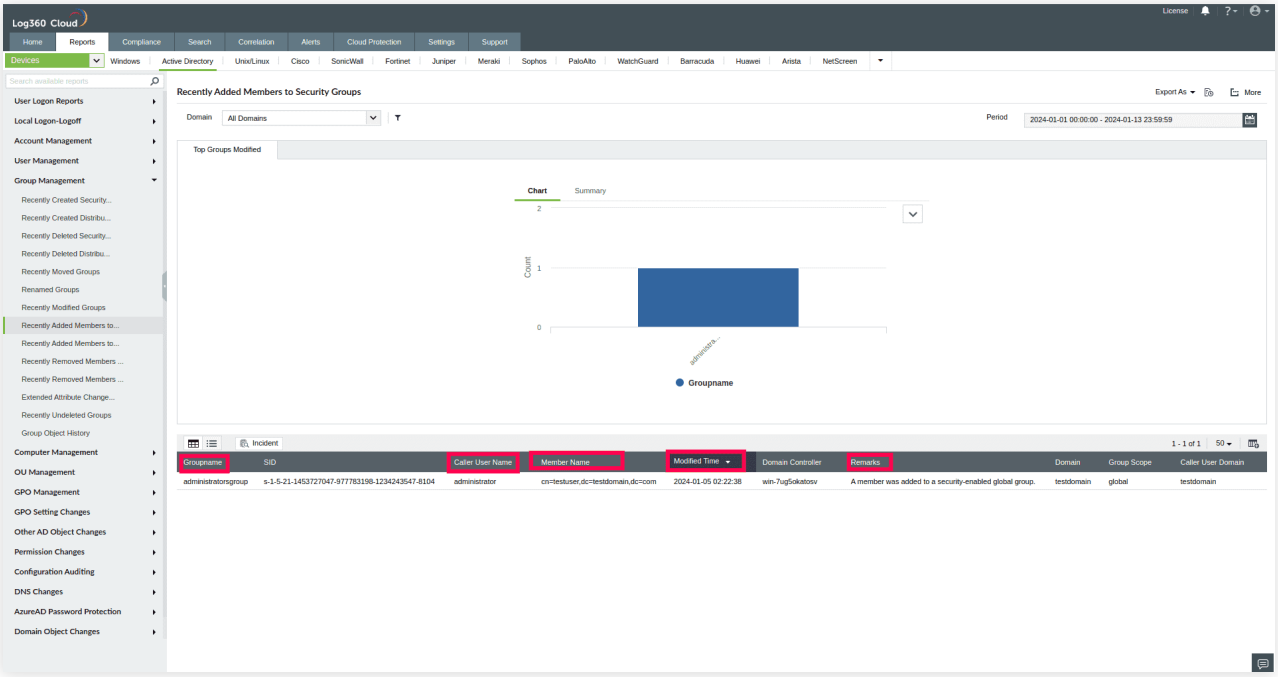

Fig. 7: Recently Added Members to Security Groups

About Log360 Cloud

ManageEngine Log360 Cloud, a unified cloud SIEM solution with integrated CASB capabilities, helps enterprises secure their network from cyberattacks. With its security analytics, threat intelligence, and incident management capabilities, Log360 Cloud helps security analysts spot, prioritize, and resolve threats in both on-premises and cloud environments. The solution is highly scalable and helps drive down infrastructure and storage costs.

For more information about Log360 Cloud, visit www.manageengine.com/cloud-siem/.

Sign up for free

Personalized Demo