ManageEngine
PAM360

Privilege elevation and delegation management (PEDM)

Eliminate standing privileges and mitigate the security risk posed by over-privileged users by employing just-in-time privilege elevation and least privilege controls

Privilege elevation and delegation management (PEDM) is a part of privileged access management (PAM), which is designed to provide non-admin users with temporary, granular privileges based on their requirements.

Granting users higher privileges and permanent access to critical accounts introduces significant security risks. Even through accidental exposure, such standing privileges give attackers access to an organization's most valuable resources. Furthermore, if these users share their credentials with other users or have their passwords compromised, they are likely offering complete control of their privileges to attackers who can remain undetected by traditional security measures.

By leveraging PEDM, IT teams can ensure that access to privileged accounts and resources is granted only when the need arises. Simply put, instead of granting permanent or standing privileges, PEDM grants limited access to certain privileged assets for a specific time frame. This granular capability, when integrated with PAM systems, mitigates the risk of accidental exposure of accounts and passwords, thereby preventing the lateral movement of attackers and malicious insiders through an enterprise's privileged pathways.

PEDM is an essential cog in an enterprise's PAM strategy

At times, users may need only temporary access to critical resources to which they normally would not have access. On such occasions, IT teams require a mechanism to temporarily
elevate the privileges of non-admin users and have these privileges revoked later because even ephemeral admin accounts are at risk of being compromised, just like their superadmin counterparts.

While privileged account and session management (PASM) solutions can provide temporary access to privileged credentials via their digital password vaults, they can grant access only on an all-or-nothing basis. In such cases, users will be provisioned with temporary admin accounts, also known as ephemeral accounts, which give them full access to the target systems, including applications and services they do not need or should not be able to access. If these ephemeral accounts are shared with more users or, much worse, compromised, any threat actor could gain complete control over the target system.

PEDM aims to solve this problem by allowing users and applications to access privileged information using a time- and request-based approach. In other words, access to sensitive information is given for a stipulated time based on the validation of their requirements, and these privileges are revoked after that time. This model puts an end to providing users with permanent standing privileges, which is a vector for abuse.

How does PEDM work?

PEDM enables IT teams to enforce granular privileges based on the validity of a user's request. Organizations can improve their privileged access security posture by imposing built-in limitations and time-based requirements when granting higher privileges associated with certain applications, systems, scripts, and processes. These granular controls allow IT teams to employ the principle of least privilege in order to provide non-admin users with only the privileges necessary to carry out their jobs.

If these users require higher privileges to access critical systems and applications, they must send privilege elevation requests to the admins. These requests will be reviewed and validated by the admins, who will then grant privilege elevation to the users for a limited period. This is called just-in-time privilege elevation, a model of temporarily granting privileges based on the merits of the requests.

For instance, admins can grant database access to a user for a stipulated period and can disable any critical actions, such as change password, delete, and edit, in order to avoid unauthorized modifications to the database. Furthermore, this user will be given only basic view access, which will be revoked after the requested period. The credentials for such critical assets will subsequently be rotated using the PAM module to ensure that there are no unauthorized access attempts in the future.

Business benefits of PEDM

Achieve a better security posture

A cooperative relationship between PEDM, least privilege, and PAM can significantly reduce the risks of standing privileges and credential abuse by external attackers and rogue insiders. Because privileges are granted at a granular level, temporary admins do not get complete access to their target systems, preventing threat actors from gaining control over the critical data.

Enforce granular privilege restrictions

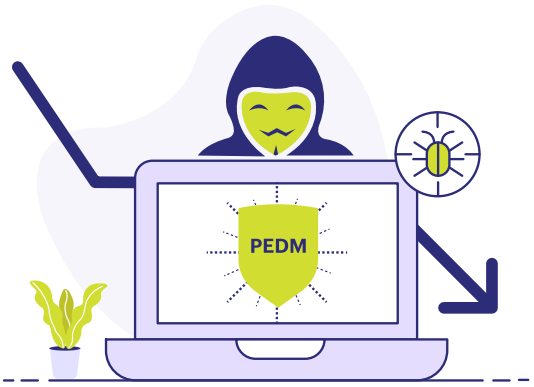
With PEDM capabilities in place, IT teams can create access control policies at the device, application, service, and process level rather than at the user level. The biggest advantage of these policies is being able to grant higher privileges with limitations. Users will be allowed to access and view applications but may not be able to configure or make any modifications to the data in those applications.

Adapt to dynamic privilege requirements

PEDM also enables users to request customized roles best suited to their privileged access requirements. Self-service elevation requests are validated based on predetermined criteria, thereby automatically approving just-in-time controls. Additionally, PEDM helps organizations meet compliance requirements, as they usually include session monitoring, auditing, and reporting capabilities.

Reduce the attack surface significantly

The key benefit of employing PEDM is that it reduces an organization's attack surface by limiting the number of privileged user accounts and sessions. This leaves cybercriminals with significantly fewer vulnerable vectors to exploit.



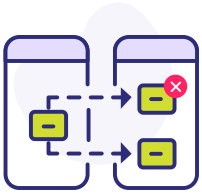
How to implement a sound PEDM strategy

Including privilege elevation and delegation controls in your PAM strategy involves a six-fold approach.

Conduct a detailed privilege audit

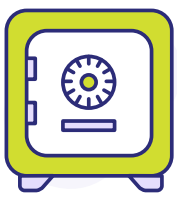
Identify and eliminate standing privileges and overprivileged user accounts. Design access control policies at the application, service, and device level rather than the user level. This also includes separating admin accounts from regular user accounts.

Include least privilege measures



Assign default privileges to user accounts, which should ideally be set as low as possible. This step ensures that unnecessary local admin privileges are eliminated and that human users and machine identities only have the bare minimum of privileges to perform their designated tasks.

Enforce privileged account governance



Protect access to admin credentials using a secure vault (an inherent module in PASM solutions). Rotate these passwords periodically and after each use to invalidate any compromised credentials. In addition, continuously monitor all privileged sessions and activities to proactively detect and terminate any suspicious behavior.

Enable just-in-time access controls

Allow users to access critical systems on a temporary basis. Grant higher privileges for a specific amount of time based on the validity of their requirements, monitor their sessions in real time, and revoke their access and rotate the credentials upon session expiration to prevent any unauthorized access in the future.

Review privileged activity logs frequently

Monitor and log privileged activities and sessions and look for suspicious activities, such as newly added network configurations or failed login attempts, that were carried out without prior authorization. Leverage context-aware log correlation to study user behavior patterns and make data-driven security decisions.

Check user accounts and privileges regularly

Review privileges on a regular basis to ensure that active user accounts only have the designated minimum of privileges. Revoke any excess privileges and remove inactive accounts to eliminate the weakest links.

PEDM: Some business use cases for PAM solutions

Remote employees need time- and requirement-based access to privileged assets

PAM solutions allow admins to grant privileged access with a set start and end time to remote employees. Temporary access rights will be automatically revoked at the set end time. Some advanced PAM solutions include options to automatically validate and approve user requests based on predefined access policies, granting temporary admins just enough privileges to carry out their activities while staying well within their access

limits. Credentials are rotated as soon as the specified time period expires to prevent any unauthorized access attempts in the future.

Engineering teams need just-in-time access to build, test, and deploy their products

Engineers require frequent access to their development and cloud platforms to carry out routine tasks. This is typically addressed by storing sensitive credentials in plaintext within script files and keeping these credentials unchanged to avoid causing any disruptions in the CI/CD pipeline. Such hard-coded credentials in the hands of malicious insiders pose a dire security threat. They need to be duly secured and shared only when the need arises.

PAM solutions help engineers by storing and managing credentials in a secure vault where they are rotated periodically to avoid any reuse or misuse. Additionally, PAM solutions include built-in options to provide engineers with time-limited, direct access to CI/CD platforms without exposing their credentials.

Third-party contractors need temporary access privileges

IT admins often face difficulties in assigning privileged access to third-party vendors and contractors whose privileges are different and sometimes also lesser than those of an average internal employee. PEDM controls enable admins to provision third parties with single-use, time-restricted access on a case-by-case basis so they can perform activities such as remote troubleshooting, installations, deployments, and tests.

Get started with PEDM

PEDM is a true game changer in the PAM sphere, and industry regulators and leaders are now pushing for it as a benchmark access control strategy. One of the biggest advantages of including PEDM in your PAM strategy is proactive prevention of internal and external threat actors through the effective management of privileges. With additional controls such as least privilege in place, PEDM works at the application and process level rather than at the user level, which makes it easier for admins to take complete and granular control of privileged accounts and resources.

If you want to get a hands-on understanding of PEDM, sign up for a free demo of ManageEngine PAM360, our enterprise PAM solution that leverages just-in-time access controls to secure your local and domain accounts in Windows.

Secure and manage user accounts and privileges effectively with PAM360

Download the free, 30-day trial

www.manageengine.com/pam360

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.manageengine.com/pam360

ManageEngine
PAM360