ManageEngine
PAM360

The dawn of passwordless administration and how to prepare for it

With the rapid adoption of hybrid work models, organizations face the daunting challenge of staying safe from emerging cyberthreats. They are increasingly considering novel security frameworks, such as Zero Trust, to reinforce their security perimeters, but even with such advanced frameworks in place, passwords happen to be the last line of defense.

Despite their versatility in securing access to critical assets, passwords are the primary target of cyberattacks. In addition, privilege abuse and insider threats are becoming rampant among organizations preparing to foolproof their security strategy. Over 500 million passwords are known to have been compromised in the last few years, and this list grows by the day.

A recent report from HYPR and Cybersecurity Insiders states that 96% of respondents want to stop using shared secrets for authentication. The shift to remote work has given urgency to the search for passwordless authentication options to protect privileged resources and systems from credential abuse.

Passwordless administration: A silver lining on the horizon

Passwordless administration is the ability to perform administrative operations without requiring privileged credentials. The primary goal of passwordless administration is not to eliminate passwords but to avoid the exposure of credentials in plaintext and hard-coded formats. Passwordless administration works by the simple logic that if passwords are not exposed to users, they can never be compromised or misused.

When passwordless administration is implemented, users are automatically authenticated and assigned the appropriate privileges to access confidential assets. In other words, they are provided with all the necessary entitlements, including network authentication, to access privileged applications, databases, OSs, virtual machines, and other assets that require multiple levels of authorization.

With passwordless administration controls, IT teams can ensure that access to privileged information systems is secure and that credentials are not shared or reused, which means users will not fall prey to phishing, brute-force, or social engineering attacks. As an additional security advantage, with this approach, user authentication data is never stored within the end users' systems and browsers.

Why going passwordless is still impractical for some enterprises

Although passwordless controls present a more reliable and secure method of IT administration, enterprises face two big challenges when switching to a passwordless environment: budget and migration complexities. The migration process involves installing biometric hardware, which demands significant initial capital. It also requires moving away from legacy security mechanisms that deal with passwords, which may interfere with organizations' daily operations.

Unlike biometrics, which require a margin of error, the binary nature of passwords keeps the authentication process free from biases. Passwords are still the primary form of authentication and the most effective, so it is difficult for passwordless alternatives to replace passwords. Although there is room for constant improvement, the

effective management, secure storage, and periodic rotation of passwords ensures that privileged accounts are protected without requiring a complex infrastructure.

While FIDO-based authentication controls have gained prominence over the years, they can only act as a secondary gatekeeper for privileged data. For instance, Apple gives users the ability to unlock their iPhones using facial recognition, but the technology still requires user passwords to encode the face mapping data into the devices' internal storage. Even if the mapping data is lost, users can still unlock their devices using passwords.

Another common misconception tied to these controls is that they cannot be duplicated; however, biometric data is also vulnerable to breaches. Back in 2017, Japanese researchers warned that hackers could gain access to fingerprints from high-resolution photographs.

The best MFA protocols only act as a reinforcement for conventional authentication procedures based on passwords, an inherently vulnerable entity. The use of credentials for authentication purposes forces IT teams to not just maintain an ever-inflating database of passwords but also keep track of them for manual resets and rotation. While password management solutions aid in enforcing strict governance of passwords, they still leverage stringent policies and MFA to safeguard access to privileged systems. After all, passwords can only authenticate users, not their intentions, so credentials must be administered effectively.

Passwordless administration: A case for privileged access management (PAM)

Passwordless administration is an inherent use case of the PAM process, which connects the dots between privileged session management, secure remote access, and user account management. It validates privileged users without requiring them to manually enter credentials so they can perform administrative actions via secure remote sessions (SSH, VNC, SQL, or RDP). Passwordless administration is different from passwordless authentication, which involves the approval of authentication requests based on biometrics or other attributes, such as a PIN or one-time password.

Administrative accounts are generally provided with elevated privileges and direct access to an enterprise's classified assets, databases, and networks. However, these accounts are sometimes delegated to normal users so they can perform certain administrative functions on their local endpoints.

For instance, any standard Linux endpoint user may require administrative privileges to perform activities such as:

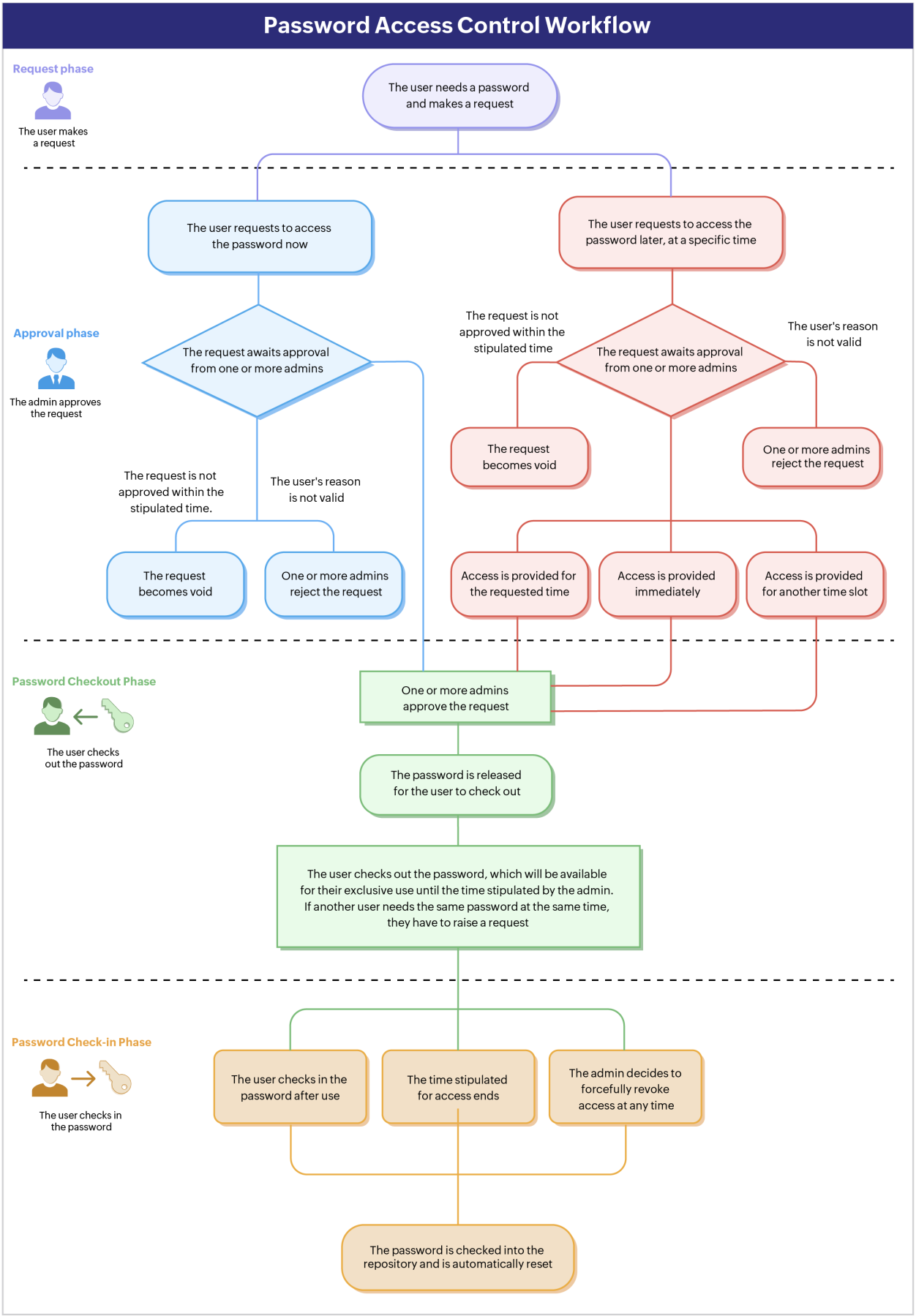
- Installing third-party software.
- Configuring dotfiles.
- Transfering proprietary files via PowerShell.
- Upgrading to the latest OS or security patch.

In the use cases above, admin credentials are granted by either assigning the user a secondary admin account or making them a temporary local administrator. Account duplication may create more attack vectors, increasing the chances of malicious activities via phishing, malware,

and more. Therefore, the administrative credentials of these accounts will have to be revoked to prevent threat actors from abusing the privileges associated with them.

Passwordless environments make it easier to secure these accounts by enforcing the principle of least privilege for general user accounts and elevating privileges only when necessary. This is called just-in-time privileged access, where select users are provided with the necessary privileges to perform their requested administrative tasks for a stipulated period.

Instead of requiring users to enter credentials for any temporary administrative task, they are trusted, authenticated, and given all the necessary entitlements based on the validity of their requests and their current privilege levels. Once the specified actions are completed, the exclusive privileges are revoked, leaving the users with their default privileges.


Password Access Control Workflow
Request phase
The user makes a request
The user needs a password and makes a request
The user requests to access the password now
The user requests to access the password later, at a specific time
Approval phase
The admin approves the request
The request awaits approval from one or more admins
The request awaits approval from one or more admins
The request is not approved within the stipulated time
The user's reason is not valid
The request becomes void
One or more admins reject the request
The request is not approved within the stipulated time.
The user's reason is not valid
The request becomes void
One or more admins reject the request
Access is provided for the requested time
Access is provided immediately
Access is provided for another time slot
Password Checkout Phase
The user checks out the password
One or more admins approve the request
The password is released for the user to check out
The user checks out the password, which will be available for their exclusive use until the time stipulated by the admin. If another user needs the same password at the same time, they have to raise a request
Password Check-in Phase
The user checks in the password
The user checks in the password after use
The time stipulated for access ends
The admin decides to forcefully revoke access at any time
The password is checked into the repository and is automatically reset

User authentication might be based on standard confidence mechanisms, such as their personal passwords, SSO, biometrics, or MFA, which play a major part in building context for a user's administrative request.

All the above use cases show that passwordless administration is an interesting blend of least privilege, remote access, and privileged account management.

Implementing passwordless administration: Where enterprises can get started

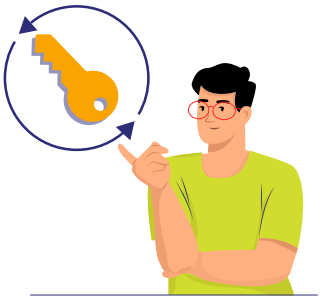
Passwords, although vulnerable, are here to stay until passwordless authentication options become more robust and bias-free. While personal account passwords can be protected using standard FIDO-compliant security controls, such as MFA or biometrics, organizations need to think beyond just passwords to protect privileged entities, such as service and domain accounts, endpoints, and databases. As organizations slowly transition to passwordless alternatives, they should consider employing a strong PAM strategy until biometric tools are proven to be foolproof.

5 steps to fortifying IT administration with passwordless alternatives

1. **Maintain** a complete list of all active privileged accounts, resources, and credentials in your network and update that list whenever a new account is created. Store privileged identities like passwords, SSH

keys, and SSL certificates in a secure vault using standardized encryption algorithms, such as AES-256.

2. **Mandate** stringent password policies that cover password complexity, frequency of password resets, strong SSH key pair generation, automatic reset upon one-time use, and other robust controls.



3. **Enable** privileged users to launch secure, one-click connections to remote endpoints without agents, browser plug-ins, or add-ons. Tunnel remote sessions with encrypted, passwordless gateways for ultimate protection. Monitor and record all privileged user sessions and activities in real time.

4. **Enforce** least privilege controls to eliminate unnecessary local administrator privileges and ensure that all human users and non-human users only have just enough privileges to perform their work. Establish a request-release workflow to grant just-in-time, elevated access to privileged resources based on the validity of the users' requirements. Upon expiration of the requested time, revoke temporary privileges and automatically rotate passwords to invalidate old credentials and prevent any unauthorized access attempts in the future.

5. **Audit** all identity-related operations, such as privileged user logins, password shares, password access attempts, and resets. These audits will help IT teams identify and eliminate blind spots and make informed security decisions.

How can enterprises get ready to ride the passwordless wave?

The success of any business depends on the privacy and accuracy of the data it processes. Therefore, controlling access to data and enterprise assets should be paramount for any organization. To avoid any penalties or lawsuits due to data breaches, organizations must ensure a streamlined workflow when it comes to securing access to their privileged data.

Traditional security measures no longer suffice as workforces become increasingly mobile and distributed. The current socioeconomic climate, the rapid transition to hybrid workplaces, and the advent of remote work tools present perfect opportunities for cybercriminals to become more creative with every passing day.

The road to passwordless IT administration is an incremental process with multiple milestones, the first of which is protecting privileged pathways. With a strong PAM plan in place, organizations can secure and manage access to critical resources, improve their security posture, effectively thwart attacks, and ensure digital prosperity.

To learn how ManageEngine's PAM solutions can give you a head start on passwordless administration, identity and eliminate security blind spots, and lower the risks of insider threats and privilege abuse, contact us today.

ManageEngine PAM360

ManageEngine PAM360 is a complete privileged access management solution for enterprises. It enables IT administrators and privileged users to gain complete, granular control over critical IT resources, such as passwords, digital signatures and certificates, license keys, documents, images, service accounts, and more.

Recognized by Gartner and Forrester as one of the top PAM vendors of 2020, ManageEngine PAM360 includes contextual integrations with SIEM, ticketing, and analytics solutions to help IT teams build user behaviour models to identify and terminate anomalous activities, generate comprehensive audit and compliance reports, and make data-driven security decisions.

Try ManageEngine PAM360 now

Start a free, 30-day trial