ManageEngine
PAM360

Best practices guide

Table of Contents

1.0 Overview

1.1 About PAM360

PAM360 is a web-based privileged access management (PAM) solution that defends enterprises against privilege misuse by regulating access to sensitive company information. Through powerful privileged access governance, smoother workflow automation, advanced analytics, and contextual integrations with various IT services, PAM360 enables enterprises to bring different avenues of their IT management system together, facilitating meaningful inferences and quicker remedies. It also helps prove compliance with regulations like PCI DSS, GDPR, NERC CIP, and SOX that mandate stringent privileged access control.

1.2 About the guide

This guide describes the best practices for setting up and using PAM360 in an enterprise network environment. Coming from our experience of helping organizations around the world deploy PAM360 successfully and streamline their privileged access management practices, this guide offers direction to IT administrators for quick and efficient software setup. The best practices can be adopted during all stages—product installation, configuration, deployment, and maintenance—and they are explained below with a special focus on data security, scalability, and performance.

2.0 Recommended system configuration

2.1 Minimum system requirements

Before installing PAM360, you need to decide on the system configuration. The minimum system requirements to run PAM360 can be found here. In general, the performance and scalability depends on the following factors:

- Number of users and groups.
- Number of resources and groups.
- Frequency of resource or password sharing.
- Number of scheduled tasks.

Based on the above factors, the following system settings are recommended for medium and large enterprises:

Medium enterprises

No. of users: 100-500
No. of resources/passwords: Up to 10,000

- Dual core processor or above
- 8 GB RAM
- 40 GB hard drive space

Large enterprises

No. of users: More than 500
No. of resources/passwords: More than 10,000

- Quad core processor or above
- 16 GB RAM
- 100 GB hard drive space

Note: We also recommend you install PAM360 on a dedicated, hardened, high-end server for superior performance and security.

3.0 Installation

3.1 Windows and Linux

PAM360 can be installed on either Windows or Linux. Though the software runs equally on both the platforms, installing on Windows provides the following inherent advantages:

Active Directory (AD) integration: A Windows installation of PAM360 can be directly integrated with Active Directory to import users and groups. Moreover, users who have logged into their Windows system with domain account credentials can use single sign-on (NTLM-SSO) to automatically log in to PAM360. With a Linux installation, you have to rely on LDAP-based authentication for Active Directory services.

Password resets for Windows resources: A Windows installation of PAM360 can perform password resets in agentless mode for all supported target systems, as long as there is direct connectivity. On the other hand, Linux installation requires an agent to be deployed on all Windows resources and domain controllers to reset passwords of Windows domain accounts, service accounts, and local accounts.

Apart from the above, password resets for Windows service accounts, scheduled tasks, IIS Web.Config files and IIS app pool accounts are supported only from a Windows installation of PAM360.

3.2 Backend database

PAM360 supports PostgreSQL and MS SQL Server out of the box. By default, the product comes bundled with PostgreSQL database, which is ideal for small and medium businesses. Meanwhile, for large businesses, we highly recommend you use MS SQL Server as your back end for better scalability, performance, clustering, and disaster recovery.

If you're using MS SQL Server as your back end, we suggest the following practices:

- PAM360 can communicate with MS SQL Server only over SSL, with a valid certificate configuration. Therefore, we recommend you have a dedicated SQL instance for PAM360 to avoid any conflicts or disruptions with existing databases.

- While using MS SQL Server as your back end, a unique key is auto-generated for database-level encryption and by default, this key file will be stored in the <PAM360 HOME/conf> directory. We recommend you move the key file to a different location to protect it from unauthorized access. Since this key file is required for high availability configurations and during disaster recovery, its safety is paramount. Losing the key will lead to an MS SQL Server reconfiguration and may even result in data loss.

- Use Windows authentication while configuring MS SQL Server as your back end rather than using an SQL local account.

- We recommend you use Windows authentication mode with the same domain account to set up MS SQL Server as your back end, so you can run SQL service and SQL agent services.

- The force encryption option should be enabled to allow all clients to connect to this SQL instance. When this is done, all client-to-server communication will be encrypted and clients that cannot support encryption will be denied access.

- Disable all protocols other than TCP/IP in the machine where MS SQL server is running.

- Hide this SQL instance to prevent it from being enumerated by other tools and disable access to this database for all other users except PAM360's service account.

- Set up firewall rules to allow access only for the required ports in the machine where MS SQL server is running.

3.3 Secure the installation master key

PAM360 uses AES-256 encryption to secure passwords and other sensitive information. The key used for encryption (PAM360_key.key) is auto-generated and unique for every installation. By default, this key will be stored in the **<PAM360 HOME/conf>** directory, in a file named **<PAM360_key.key>**. The path of this key needs to be configured in the manage_key.conf file present in the PAM360 HOME/conf directory. PAM360 requires this folder to be accessible with necessary permissions to read the PAM360_key.key file when it starts up every time. After a successful start-up, it does not need access to the file anymore and so the device with the file can be taken offline. We highly recommend you move this key to a different secure location and lock it down by providing read access only to PAM360's service account. Also, update this remote path in the **"manage_key.conf"** file so that the product can read the encryption key during start up. You can also secure this key by storing it in a USB drive or disk drive. For extreme security, create script files to copy this key into a readable location and then destroy the copy upon service start up.

3.4 Take control of the database credential

Apart from AES encryption, the PAM360 database is secured through a separate key, which is auto-generated and unique for every installation. This database key can be securely stored in PAM360 itself. But we recommend you store the key in some other secure location accessible to the product server.

By default, the database information, such as the JDBC URL, log in credentials, and other parameters, will be stored in a file named database_params.conf, which is present in the **<PAM360 HOME/conf>** directory. Although the database is configured to not accept any remote connections, we recommend you move this file to a secure location, restrict access, and make it available only for PAM360's service account. If you place the database_params.conf file outside the PAM360 installation folder, you need to specify the location along with the filename in <PAM360-Home>\conf\wrapper.conf file (for Windows) or <PAM360-Home>\conf\"wrapper_lin.conf file (for Linux). Note that the service cannot be started if the entire location is not specified here.

- The path of this file is configured in the “wrapper.conf” file present in the <PAM360 HOME/conf> directory. Edit this file and look for the line wrapper.java.additional.9=-Ddatabaseparams.file.

- If you are using a Linux installation, then you will have to edit the file “wrapper_lin.conf” present in the <PAM360 HOME/conf> directory.

- The default patch will be configured as ./../conf/database_params.conf. Move the “database_params.conf” file to a secure location and specify its path in the above file. For example, wrapper.java.additional.9=-Ddatabaseparams.file=\\remoteserver1\tapedrive\sharedfiles\database_params.conf

- Save the file and restart PAM360 for the change to take effect.

4.0 Server and environmental settings

4.1 Server hardening

By default, all components required for PAM360 to function are stored in the installation directory (ManageEngine/PAM360). Therefore, we highly recommend you harden the server in which PAM360 is installed. Some of the basic steps you should carry out are as follows:

- Disable remote access to this server for all regular domain users in your organization using domain group policies. Restrict read permissions for all regular administrators, and provide write permissions to PAM360 drive or directories for only one or two domain administrators.

- Set up inbound and outbound firewalls to protect against incoming and outgoing traffic, respectively. Using this setting, you can also specify which server ports must be opened and, ideally, used to carry out various password management operations such as remote password resets.

4.2 Use a dedicated service account

Create a separate service account for PAM360 in your domain controller and use it in all areas of PAM360. The same account will be used to run PAM360. To begin using the service account created for PAM360, go to the service console (“services.msc”) in the server where PAM360 is

installed and navigate to the properties of PAM360. Change the configured local system account with the service account created. This same service account can also be used for importing users and resources from Active Directory.

4.3 Configure a bound IP address for the web server

By default, PAM360's web-server will bind to all available IP addresses of the server in which the application is installed. Due to this, PAM360 will be reachable on any or all IP address(es) with the configured port (7272). To restrict this, we recommend you configure the web server to bind to a single IP address and receive incoming communications from that IP address alone. The following steps can be used to configure the bound IP:

- Stop PAM360 if it is running.

- Open the "server.xml" file present in the <PAM360_HOME>\conf folder

- Search for this line:
  <Connector SSLEnabled="true" URIEncoding="UTF-8" acceptCount="100" ciphers="TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256" clientAuth="false" debug="0" disableUploadTimeout="true" enableLookups="false" keystoreFile="conf/server.keystore" keystorePass="passtrix" maxHttpHeaderSize="32768" maxSpareThreads="75" maxThreads="150" minSpareThreads="25" port="7272" scheme="https" secure="true" server="PAM360" sslProtocol="TLS" truststoreFile="jre/lib/security/cacerts" truststore-Pass="changeit" truststoreType="JKS" useBodyEncodingForURI="true"/> In the above line, next to the value port="7272", add the attribute address="127.0.0.1". Replace 127.0.0.1 with the actual IP address of the server that you want to use for binding.

4.4 Restrict access by black or white listing IP addresses

PAM360 can be accessed from any client system, as long as there is connectivity. So, we recommend you restrict and provision only a limited number of client systems with access to PAM360. To configure IP based restrictions, navigate to **Admin > Configuration > IP Restrictions**. The IP restrictions can be set at various levels and combinations, such as defined IP ranges or individual IP addresses. You can choose to allow web access to specific IP ranges and addresses or alternatively, restrict access by adding them to the blocked IP addresses field.

5.0 User onboarding and management

5.1 Leverage AD/LDAP integration for authentication and provisioning

Integrating PAM360 with Active Directory or any LDAP-compliant directory can be very useful, as it provides the following benefits:

User provisioning or deprovisioning: With AD/LDAP/Azure AD integration, user addition in PAM360 is quick and easy. Once integrated, you can directly import the user profiles and groups or OUs from your directory to PAM360. Moreover, user account provisioning in the product also becomes a simple process, since you can effortlessly assign required privilege levels to users based on their AD/LDAP profiles. For instance, if you import an existing OU of "Database Administrators" from your directory to PAM360, you can easily allocate the database passwords to that imported group.

On top of this, you can enable synchronization while integrating PAM360 with your directory so that any change, such as a user newly added or moved around between OUs in your directory, will automatically reflect in PAM360. Synchronizing PAM360 with your directory will also keep you notified when a user is permanently deleted from the corresponding user directory. PAM360 disables and locks such user accounts, notifies you of the same through an email and alert notification, upon which you can chose to either delete those accounts or reactivate them.

Active Directory authentication: Another benefit is that you can leverage your directory's respective authentication mechanism and provide your users with single sign-on (SSO) options. Once you activate this option, users will be automatically authenticated into PAM360 (using NTLM-based authentication) as long as they have already logged in to the system with their directory credentials. Using AD/LDAP credentials for PAM360 authentication ensures that login passwords are not stored locally in PAM360, since users will be directly authenticated from your directory.

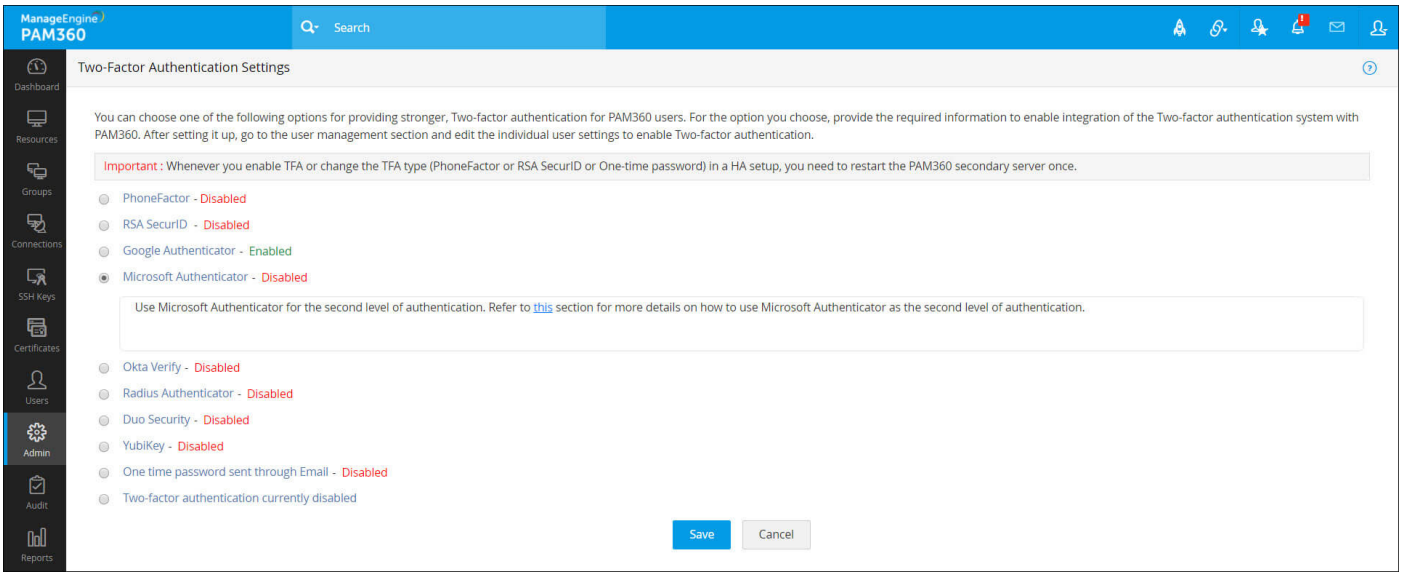
5.2 Disable local authentication

After integrating PAM360 with your AD/LDAP-compliant directory, we advise you disable local authentication and let users log on to PAM360 using their AD/LDAP credentials. To disable local authentication, navigate to **Admin > Settings > General Settings > User Management**. However, if you have configured a local PAM360 account for break glass purposes, you cannot

disable local authentication. In such cases, if you still want to have only AD/LDAP authentication, we recommend you disable the **"Forgot Password"** option in the same section (option used to reset the local authentication password for all users in PAM360). Disabling this option will ensure users can log in to PAM360 using only their AD/LDAP credentials, even if local authentication is enabled.

5.3 Use two-factor authentication

An additional protective layer of user authentication ensures that only the right people have access to your sensitive resources. PAM360 provides multiple options for configuring a second level of authentication before providing access to the product's web interface. The second factor options include Azure MFA, RSA SecurID tokens, Duo Security, Google Authenticator, unique passwords through email, and any RADIUS-compliant two-factor authentication. It's highly recommended to configure two-factor authentication for your users.



5.3 Two-factor authentications options in PAM360

5.4 Assign user roles based on job responsibilities

After adding users, assign them proper roles. PAM360 has four predefined user roles: administrator, password administrator, password auditor, and password user. To learn more about the privileges of each role, please refer to our help documentation. Administrator roles should be restricted only to the handful of people who need to perform user management operations and product-level configurations besides password management.

Using the super administrator role: A super administrator in PAM360 has access to all stored passwords. Ideally, this role is not required. However, if you would like to have a dedicated account for emergency purposes, you can create a super administrator for your organization. For security reasons, this role should always be limited to the top people in the organizational hierarchy. Also, the best practice approach in such cases is to create only one super administrator. Once an administrator has been promoted to a super administrator, they can prevent the creation of more super admins in the future as needed. This can be done by the super administrator navigating to **Admin > Authentication > Super Administrators**, and then enabling **Deny Creation of Super Admins by Admins**.

5.5 Create user groups

Organize your users into groups—for example, Windows administrators, Linux administrators, and so on. User grouping helps immensely while sharing resources and delegating passwords. If you've integrated PAM360 with AD/LDAP, you can import user groups directly from the directory and use the same hierarchical structure.

5.6 Remove the default admin account

For security reasons, we highly recommend you delete the default admin and guest accounts in PAM360, after you've added one or more users with the administrator role.

5.7 Restrict access to mobile apps and browser extensions

By default, all users will be able to access PAM360's native mobile applications and browser extensions. If you would like your users to not be able to access any of the passwords from any device other than their workstation, disable access to mobile apps globally across your organization. If needed, you can enable access for required users or administrators alone. Similarly, you can also enable or disable access to browser extensions. These restrictions can be enforced by navigating to **Users > More Actions** and selecting **Restrict Mobile Access/ Restrict Browser Extension** from the drop-down menu.

6.0 Data population and organization

6.1 Adding resources: Choose a convenient method

The first step to getting started with password management in PAM360 is adding resources. The quickest and most convenient way to do this is automated discovery of privileged accounts. The other ways are manual addition and CSV import. Use the import via CSV/TSV feature if you used another tool before switching to PAM360 or have your credentials stored in spreadsheets.

6.2 Remember to specify resource types

While adding resources manually or via CSV import, check whether all resources have been properly sorted under a resource type. This is mandatory for using features such as password resets since PAM360 uses different modes of communication for different resources, based on the applied resource type. Unless specified, resources will be sorted under **"Unknown"** and in that case, password resets will fail. PAM360 supports many default resource types, listed under **Admin > Resource Config > Resource Types**.

6.3 Remove unauthorized or unwanted privileged accounts

When you use the auto-discovery feature to inventory the IT resources on your network and their respective privileged accounts, PAM360 will, by default, fetch every single account associated with the resources detected on the network. Some accounts may be unauthorized, unwanted, or orphaned. For instance, when you add a Windows resource, all guest accounts will also be fetched.

From a security perspective, unauthorized accounts should be identified and deleted to avoid any unforeseen vulnerabilities in the future. Password management best practices demand that the number of privileged accounts should be kept at a minimum. Moreover, dumping unwanted resources can clutter the database and make data organization a daunting task. Therefore, we recommend you remove these unwanted accounts in the target machine itself before running auto-discovery in PAM360.

6.4 Randomize passwords after resource discovery

Once you have completed resource discovery and account enumeration, we highly recommend you randomize the passwords for all accounts. This practice is important because before deploying PAM360, your employees may have stored their passwords in different media such as spreadsheets and text files or may have even copied them down on paper. If the passwords are not changed, those employees can still access the resources directly, outside of PAM360. Therefore, passwords must be duly randomized after resource discovery to block all direct, unauthorized access to resources. In addition, randomization also gets rid of weak passwords and assigns strong, unique passwords for resources. Password randomization for the discovered accounts can be carried out from **Resources > Select the specific resource(s) > Resource Actions** (at the top) **> Configure Remote Password Reset.**

Note: In future, if you would like to preset password randomization for new accounts when they are discovered, you can configure the same from **Resources > Select the specific resource(s) > Resource Actions** (at the top) **> Discover Accounts**, and then enable **Randomize Passwords After Discovery** in the new window that opens.

6.5 Leverage the power of resource groups

Resource groups are quite powerful in PAM360. Most of the advanced password management operations, such as automated password delegation and scheduled password rotation, can be performed only at the resource group level. Among the two types of resource group creation, **"Criteria-based"** groups are highly recommended.

Criteria-based groups are basically dynamic groups. They provide you the flexibility to consolidate resources that satisfy certain criteria into a single group. Once you define the criteria, PAM360 will automatically identify all matching resources and create the group, no manual intervention needed.

6.6 Use nested resource groups and order resources based on department

For ease of use and navigational convenience while retrieving a single resource from a huge database, you can leverage the explorer tree view setting in PAM360 (i.e. create nested resource groups). By default, the tree displayed will be different for each user. Enable this tree view setting to globally display a uniform explorer tree across the organization. After enabling, change the name of the main node from **"Resource Groups"** to your organization's name.

Under this, create multiple sub-nodes based on the different teams or departments you have. Subsequently, you can designate the resource groups under the sub-nodes of the team or department they belong to.

By manipulating the explorer tree as mentioned above, you can create a clear hierarchy of resource groups that provides easy accessibility. To allow manipulation of the explorer tree, navigate to **Admin > General Settings > Password Retrieva**l, and enable **"Allow all admin users to manipulate the entire explorer tree."**

6.7 Additional fields for easy reference and search

While adding resources, additional fields can be used to create custom columns and values. The fields will come in handy for creating criteria-based groups, searching specific resources or passwords, sharing resources, and more.

7.0 Password sharing and granular access control workflows

7.1 Share passwords with varying access privileges

While sharing resources, password owners can grant different permission levels to users and groups by choosing one of the following privileges:

- **RemoteApp only:** Users and User groups can access and use the Remote Apps associated with the resources.
- **View Passwords:** Users can only access the password.
- **Modify Passwords:** Users can access and modify the shared password.
- **Full Access:** Users have complete management of a resource or group, and can re-share the resource, group, or individual account passwords.

We recommend you provide users only with **"View Passwords"** permissions as that will be mostly sufficient for various password-related operations. Exercise caution while providing **"Full Access"** permissions, because a user with **"Full Access"** permissions over a password is almost a co-owner and will be able to modify, delete, and even reshare the password with more users.

Note: Apart from these sharing privileges, you can also share resources without revealing the passwords in plain-text. This is possible when auto-logon is configured for the resource. To learn more about this feature, refer to section 10.1.

7.2 Use resource group to user group sharing

Though PAM360 has provisions to share a single password or resource with a single user or a group, the best practice approach is sharing a resource group with a user group. This will work best for performing bulk operations efficiently and saving time. For instance, if you need to provide Windows administrators in your organization with access to all Windows resources, you can complete the operation in two simple steps:

- Create a criteria-based resource group (with "Windows" resource type as the matching criterion). That way, all existing Windows resources are added to the group and new resources created in the future will also automatically added to the group.

Create a user group for Windows administrators. If you have integrated AD/LDAP, you can import the group directly and enable auto-synchronization of the user database. That way, whenever a new Windows administrator joins the organization, their AD account will automatically be added to PAM360's user group, and the new user will subsequently inherit the group's permissions to view Windows server passwords.

7.3 Leverage access control workflows

Access control in PAM360 is a request-release mechanism that doesn't allow users to access passwords directly. Instead, users have to raise a request to the admin for access approval. The feature also helps you introduce various access restrictions for your resources such as time limited access, concurrency controls, and automated resets after the usage period. So we highly recommend you enable this release control for the credentials of your critical resources. For better security, you can also configure dual approvals for critical resources, which mandates that two or more admins approve a request before the passwords are released for a temporary period. This setting comes in handy when an administrative credential is primarily owned by two different departments in your organization. Access controls can be configured by going to **Resources > Resource Actions > Configure Access Control.**

7.4 Just-in-time privilege elevation for local user accounts

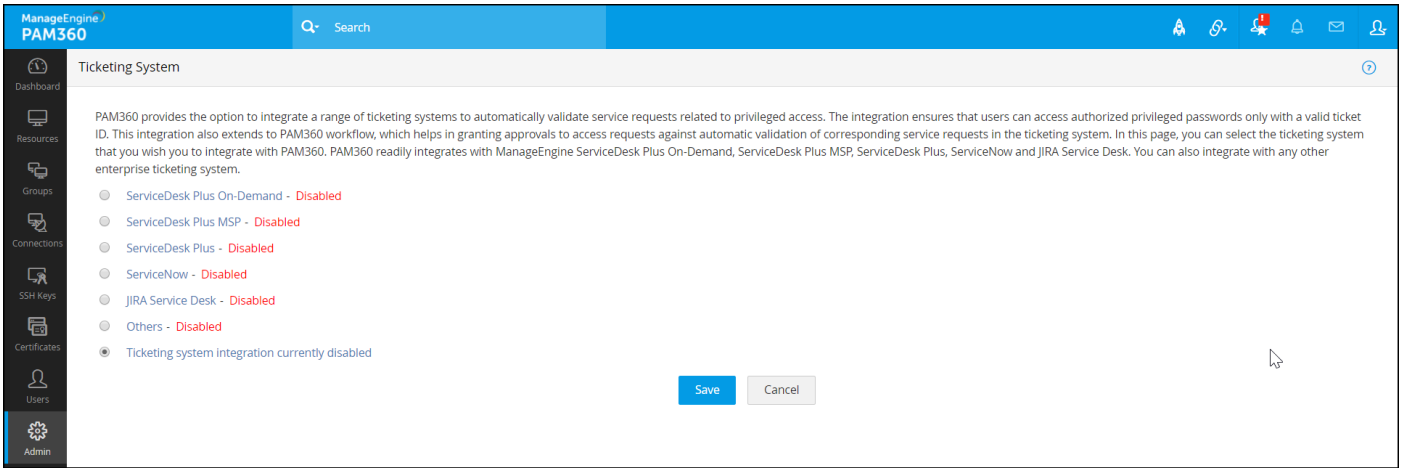
PAM360 also allows administrators to grant password access to users for a specific period, by providing just-in-time (JIT) privilege elevation to local user accounts in a Windows resource. For example, if "dbuser" is a local Windows account without any admin privileges, an admin can elevate its privileges equal to that of an admin or any other privileged user for a specific period.

7.5 Require users to provide their reason for retrieving passwords

By default, all password-related operations are captured in PAM360's audit trails, complete with timestamp and IP address details. Optionally, you can require that users provide a reason for access to a password. These reasons will also be recorded in the audit trails, which can be used for cross-verification and validation in forensic investigations. Therefore, whenever a user tries to retrieve the password of a resource, we recommend you mandate that they provide a credible reason for requiring access, irrespective of whether access controls are configured. This option can be activated under **Admin > Settings > General Settings > Password Retrieval.**

7.6 Integrate PAM360 with enterprise ticketing systems

PAM360 provides the option to integrate a range of ticketing systems to automatically validate service requests related to privileged access.The integration ensures that users can access authorized privileged passwords only with a valid ticket ID. In order to enable a stronger retrieval workflow for your critical resource passwords, we suggest you integrate PAM360 with your enterprise ticketing system. Currently, PAM360 readily integrates with ManageEngine ServiceDesk Plus On-Demand, ServiceDesk Plus MSP, ServiceDesk Plus, ServiceNow, and JIRA. You can integrate PAM360 with the aforementioned ticketing systems by navigating to **Admin > Integration > Ticketing System Integration.**



7.6 Integration with leading enterprise ticketing systems

8.0 Password policies

8.1 Set separate password policies for critical resource groups

Primarily, password policies help you define password strength by specifying character complexities. PAM360 allows you to customize and configure different password policies for different groups of resources. If you have a handful of resources that are ultra-sensitive in nature, organize them all into a resource group and configure a separate policy with very strict requirements. Policies for resource groups can be configured from **Groups > Select the specific groups > Bulk Configuration > Associate Password Policy.**

8.2 Account-level password policies

Normally, each resource is provisioned with one or a few administrative accounts and other normal accounts. To protect these privileged accounts, we recommend you configure a strong password policy separately for sensitive accounts of important resources. Account-level password policies can be configured from **Resources > Select the specific resource(s) > Resource Actions** (at the top) **> Associate Password Policy.**

8.3 Define the age for your passwords while creating policies

While configuring a new password policy, always remember to set the maximum password age. Specifying an age lets PAM360 automatically reset the password when the age expires. If you do not fill out the field, the passwords will not expire, which is NOT the recommended practice.

9.0 Password resets and SSH key rotation

9.1 Periodic password randomization and key rotation

Secure management of privileged accounts requires the use of strong, unique passwords that are periodically reset. Ideally, passwords should be reset at least once every 90 days—the most common timeframe stated by IT regulations such as PCI-DSS. We recommend you configure regular password resets for resource groups in PAM360 using the scheduled password reset feature. More importantly, configure passwords to be automatically reset during the following situations, as well:

- After a user is done using the password and checks it in.
- When share permissions are revoked for users with whom the password was initially shared.
- When passwords expire, as set through password policies.

For SSH, it's highly recommended to rotate keys every 30-45 days and effectuate bulk rotation immediately after onboarding users.

9.2 Choose the most suitable password reset mode

Password resets can be carried out in one of the two following modes in PAM360: agentless or agent-based.

For agentless mode, PAM360 directly connects with the target system and changes the password. Administrative credentials have to be supplied to perform password changes. If it is a Linux installation of PAM360, two accounts are required: one with root privileges and one with normal user privileges that can be used to log in remotely.

On the other hand, agent-based mode comes in handy when you have to reset passwords for resources without direct connectivity, such as those in DMZ locations or with firewall restrictions. To accomplish those password resets, PAM360 deploys an agent to the remote host, which executes the task. All communication between the agent and the application server is one way and over HTTPS, so you don't have to open any firewall ports for in-bound traffic.Basically, among both modes, the agentless mode is the most convenient and reliable way of changing passwords and we recommend you choose the same whenever resources can be directly reached. However, you have to choose the agent-based mode for the following use cases:

- When administrative credentials are unavailable in PAM360 for a particular resource.
- When required services are not running on the target resource (Telnet/SSH for Linux, RPC for Windows)
- When PAM360 is running on Linux and you need to make password changes to a Windows resource.
- When you have two different environments "A" and "B" with firewalls in between. During such cases, you can install PAM360 in one environment, say A, and use agentless mode for the machines in environment A. On the other hand, you can install agents in environment B's machines for password reset. That way, all passwords can be managed in both A and B without adding firewall port exceptions.

9.3 Restart services to achieve a complete management routine

With PAM360, Windows domain accounts that are used to run various services and IIS application pools can also be subject to periodic password resets, along with subsequent password propagation across all dependent services and application pools. To ensure that services, tasks, and app pools are properly updated with the password change, PAM360 offers an option to automatically restart services after the password is reset, which we recommend.

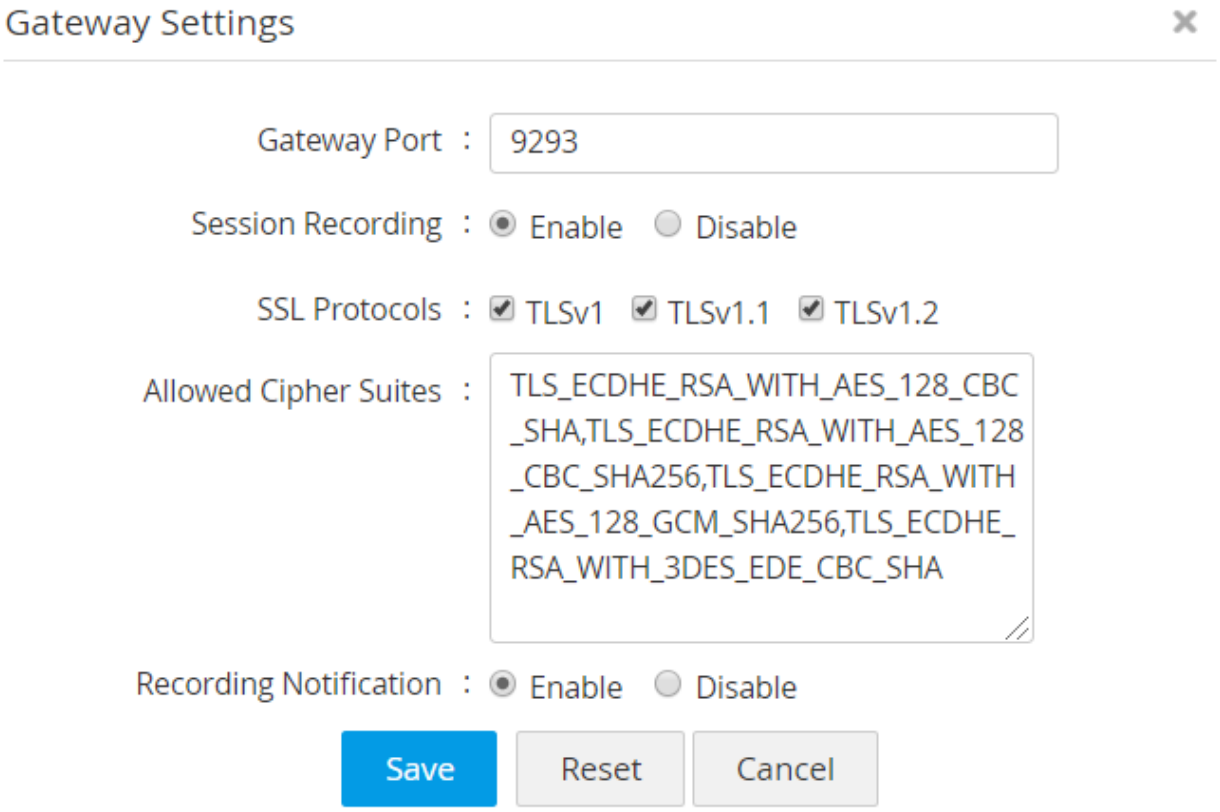
10.0 Secure remote access

10.1 Enable users to automatically log on to remote systems without revealing passwords in plain text

After you configure auto-logon options to remotely connect to the machines, PAM360 allows users to establish a direct connection to the remote system with just a single click, eliminating the need to copy and paste passwords. In such cases, we recommend that you prevent users from retrieving the passwords in plain text, since it is not required. Plain text retrieval of passwords can be disabled from **Admin > Settings > General Settings > Password Retrieval.**

10.2 Configure gateway settings

PAM360 allows you to customize gateway settings. You can edit and control the cipher suites that are used for SSL communication, set up a different port, choose SSL protocols to be used for securing remote connections initiated from the product, customize HTTP header log settings, etc. To edit the gateway settings, navigate to **Admin > Connections > Gateway Settings.** Apart from this, you can also refer to the gateway.conf file in the path <PAM360_installation_directory>\conf for a more extensive customization and for other technical details.



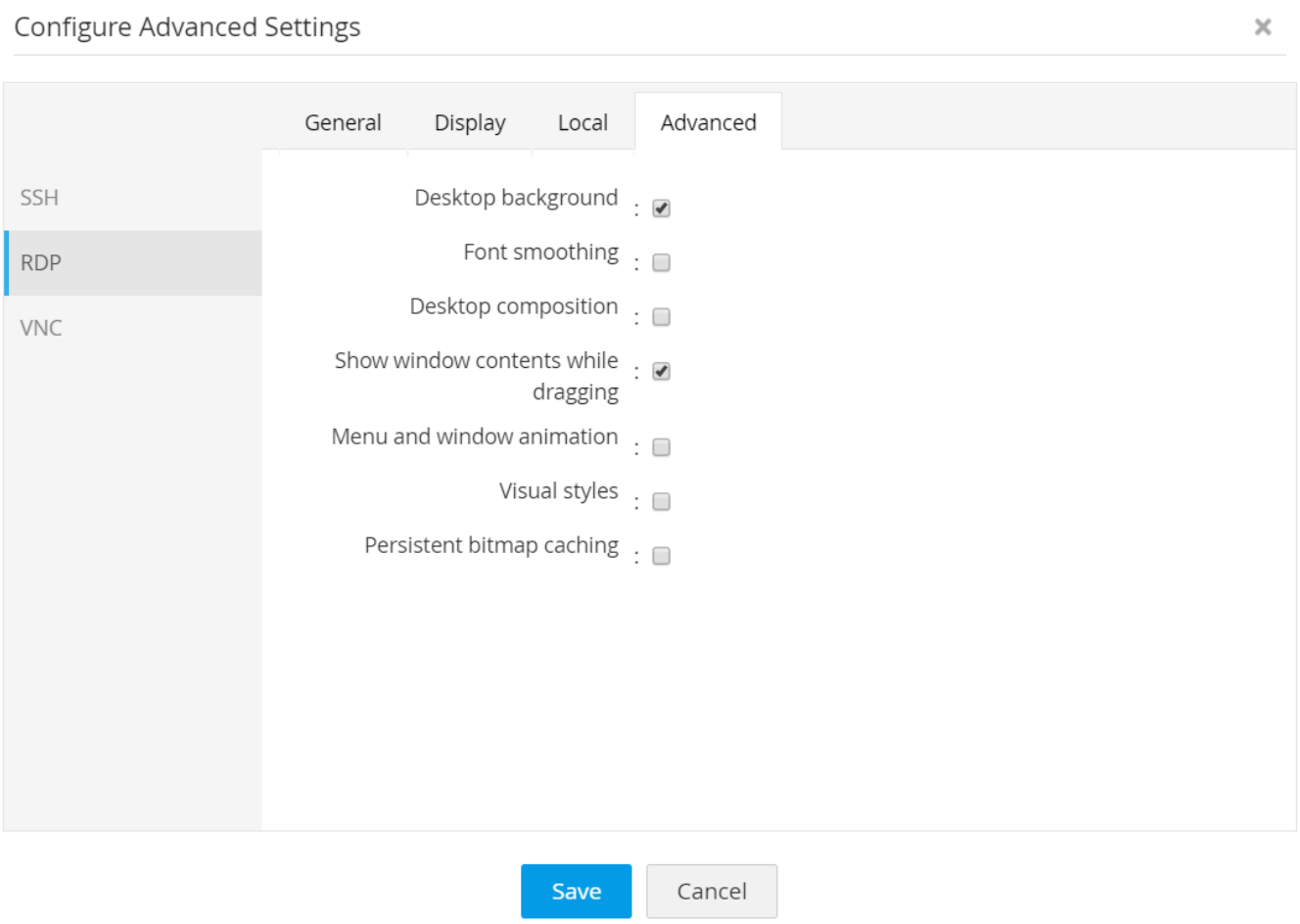
10.2 Configuring gateway settings

10.3 Leverage advanced settings for connections

PAM360 offers advanced configuration settings for connections that can be customized to improve the speed and performance of the remote connections initiated from within the product. These enhancements are available for SSH, RDP, and VNC connections for centralized configuration and ease of use. All the settings changes made here will be applied locally on the remote system too. Some of the advanced settings include keyboard layout, desktop backgrounds, map drives, remote audio support, etc.

To configure these settings, navigate to the **Resources module** and switch to the **Passwords** tab. Here, click the **Account Actions** drop-down beside the required account and click **Connection Settings** in the drop-down. Connection settings for the selected account type (SSH/RDP/VNC) alone will open up.

Click here to learn more about the advanced settings.

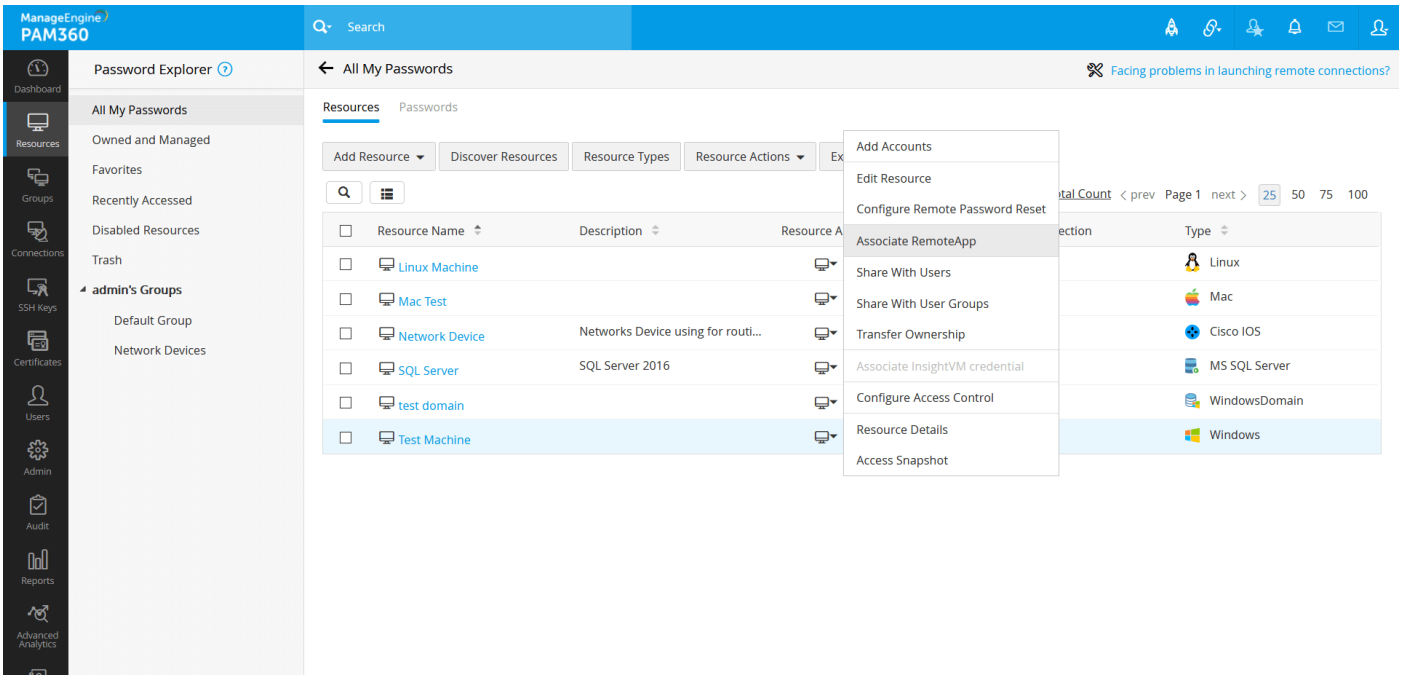


10.3 Advanced settings for RDP

10.4 Discover and configure RemoteApp for Windows servers

Note: You need to install the required RemoteApps on the remote target servers to use this feature.

Apart from launching direct connections to remote systems, you can allow users to connect to particular apps that are configured as RemoteApps in the target systems. You can either automatically discover RemoteApps configured in the target Windows systems, or manually add them in PAM360. Configuring RemoteApps for Windows connections makes managing privileged RDP sessions more secure, as it limits a user's access to the particular application that is launched, instead of the entire remote desktop. For example, consider that if you've whitelisted an app, say SQL Studio, for a particular user. Now, when the user launches a session, it will automatically open SQL Studio and the user can only use that application. They cannot see the taskbar or navigate to any other area or perform any other operation other than using SQL Studio.



10.4 Configuring RemoteApp

11.0 Privileged access to third parties

11.1 Manage third party access to corporate systems

Most often, third parties such as contractors, consultants, and vendors require access to corporate IT resources for various contractual duties and other business needs. When you provide privileged access to a third party, we always recommend you provision them only with temporary access, restricted with time stipulations and minimum necessary privileges. On top of that, here are a few more suggested practices to follow while sharing critical information with third parties:

- Since contractors connect remotely to your resources, add all your third parties as users in PAM360 and require them to establish direct sessions to target systems only through PAM360.
- After configuring auto-logon for the resource, the best practice approach is to share the login credentials without displaying the passwords in plain text.
- Also, configure access control workflows for such resources. This helps implement time limits for access to the passwords, including an automatic password reset at the end of the usage period.
- Shadow sessions regularly to detect any trace of malicious behavior and instantly adopt remediation measures.
- When you end a contract with a vendor, immediately execute password resets for all resources that the vendor had access to.

12.0 Data center remote access

12.1 Avoid circulating jump server credentials

Normally, connecting to remote data center resources is a lengthy process, since direct access is restricted from a security perspective. Instead, admins and users must hop through a series of jump servers before ultimately connecting to the target device, authenticating themselves manually at each stage. This process of multiple hops introduces separate credentials for each jump server, which requires users to launch a data center connection. For these cases, circulating all the credentials among users is not a secure practice. Instead, use the landing server configuration feature in PAM360 to require your users to connect to data centers only through PAM360. The application provides secure, one-click automated access to the data center resources, eliminating the need for manual authentication at every hop. It also centralizes the management of jump server credentials.

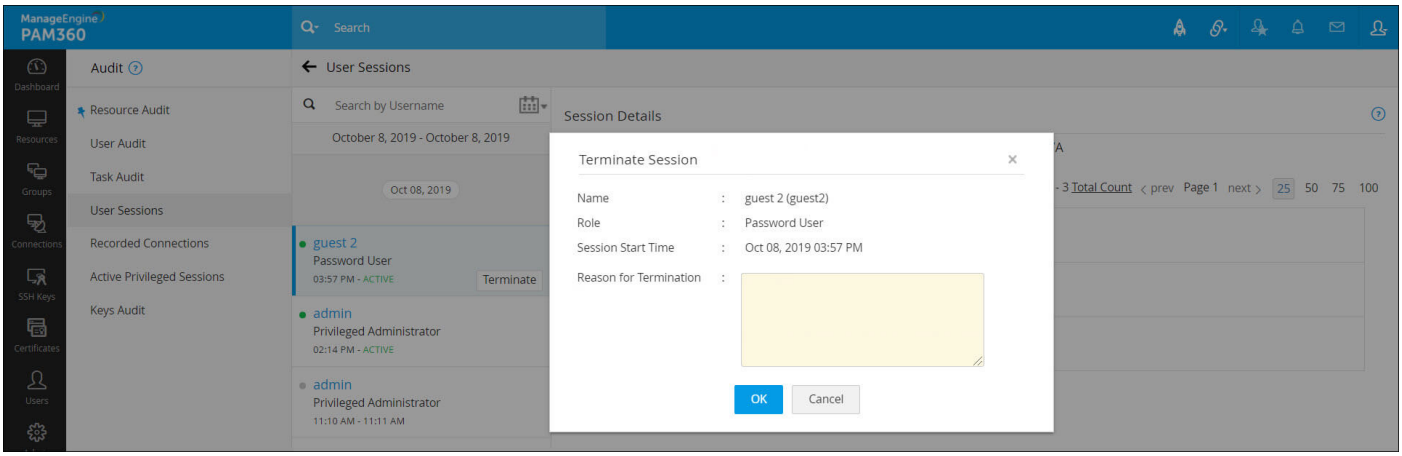
12.2 Export passwords beforehand to keep them ready for offline access

If a data center environment does not allow internet connectivity, you will not be able to access PAM360 from that network. In that case, export all required passwords as an encrypted HTML file beforehand and access passwords offline. If the export option is enabled, you can download the file from **Resources > Resource Actions** (at the top) **> Export Passwords**.

13.0 Session management and monitoring

13.1 Monitor critical sessions in real time

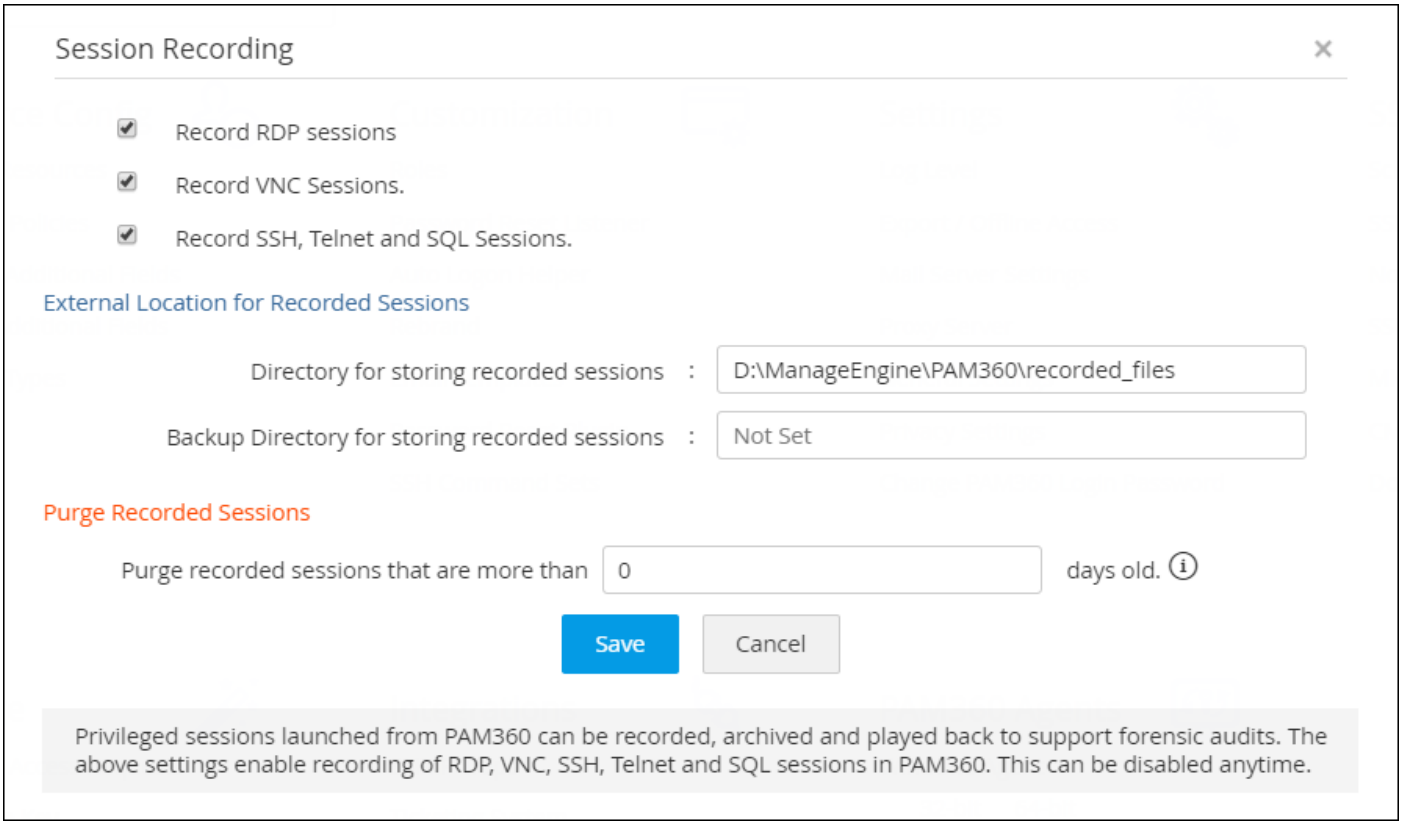
PAM360 offers session shadowing, which can be used to establish dual controls on privileged sessions. Use this feature to monitor remote sessions in real time and supervise user activity. Dual controls are helpful to provide remote assistance and thwart malicious activities. If you are an admin, you can track critical sessions launched from the application by joining active sessions and observing concurrently, without affecting the end user. You can join an active session by navigating to **Audit > Active Privileged Sessions > Join**. Session collaboration will be especially useful for troubleshooting as all the users will be able to control the mouse cursor and work collaboratively in the same RDP or SSH session. In case any suspicious activity is detected, you can terminate the session immediately to avoid any misuse of privileged access. This can be done by navigating to **Audit > Active Privileged Sessions**, and clicking on **Terminate** beside the required session.



13.1 Terminating a suspicious user session

13.2 Record every privileged session

By default, PAM360 records all RDP, VNC, SSH, and SQL sessions launched from the application. We recommend that you configure session recording for all the privileged sessions, and customize the external storage location by navigating to the Resources tab and clicking on **Resource Actions > Configure > Session Recording**. All the recorded sessions will be displayed under **Audit > Recorded Connections**. You can trace sessions using any detail such as the name of the connection, the user who launched the session, or the time at which the session was launched.



13.2 Configuring session recording for RDP, VNC, SSH and SQL connections

13.3 Regularly purge recorded sessions

By default, PAM360 records all RDP, VNC, SSH, Telnet, and SQL sessions launched from the application. If your organization is large, with a comprehensive range of resources for which session recording is enabled, the recorded sessions will naturally grow at a faster rate. If you do not need recordings that are older than a specified number of days, we recommend you purge them to keep disk space free. You can also store these recordings in the local drive, so they can be moved elsewhere. On the other hand, if you want to delete a selective session or the chat history of a particular session, you can do so by navigating to **Audit > Recorded Sessions**, and then clicking the **"Delete"** icon beside the selected session. Note that PAM360 mandates the approval of at least two administrators to delete a particular session recording or a chat session.

14.0 SSL/TLS certificate management

14.1 Discovery and import

PAM360 enables you to automatically discover and import the certificates mapped to user accounts in the AD, certificates in Microsoft Certificate Store, and certificates issued by local certificate authorities. Optionally, you can also create scheduled tasks for SSL certificate discovery to achieve periodic discovery and import of certificates from the required resources into PAM360.

14.2 Certificate request and acquisition

PAM360 facilitates the creation of self-signed certificates but it's highly recommended that you strictly deploy these certificates only within your internal network, where you are sure about the trust established by all resources. Since the recommended signature algorithm is SHA-2, we encourage you to isolate and replace all SHA-1 certificates with SHA-2 using PAM360.

You should always obtain SSL certificates from trusted third party certificate authorities for public facing websites. As and when a certificate is obtained from a trusted CA, attach the obtained certificate while closing the certificate request to facilitate its management from PAM360. It's also recommended to organize the acquired certificates into various logical groups that enable you execute actions in bulk.

14.3 Certificate deployment

Always ensure the latest version of a certificate is active on its deployed servers. At instances where two or more versions of the same certificate is managed using PAM360, it's important to keep a check on whether the right version of the certificate is deployed to its end-servers). The best practice approach is to have the latest version of certificate on end-point servers. You can also leverage bulk deployment at instances where the same SSL certificate is to be installed on various end-servers.

14.4 Integration with certificate authorities

PAM360 facilitates end-to-end life cycle management of certificates issued by public certificate authorities. This functionality is powered through seamless API integration with third-party certificate authorities, and allows administrators to request, acquire, consolidate, deploy, renew, and track the lifecycle of certificates in a centralized fashion directly from the PAM360's web interface. You can raise requests for certificates from public certificate authorities using the built-in CSR generation tool. Here are some of the recommended best practices while requesting certificates from CAs.

- Immediately revoke a certificate if the private key is compromised and raise a fresh request with a new private key.
- Generate a new private key every time a certificate is renewed.
- Configure agent mapping to achieve timely renewal of certificates through automated domain validation.

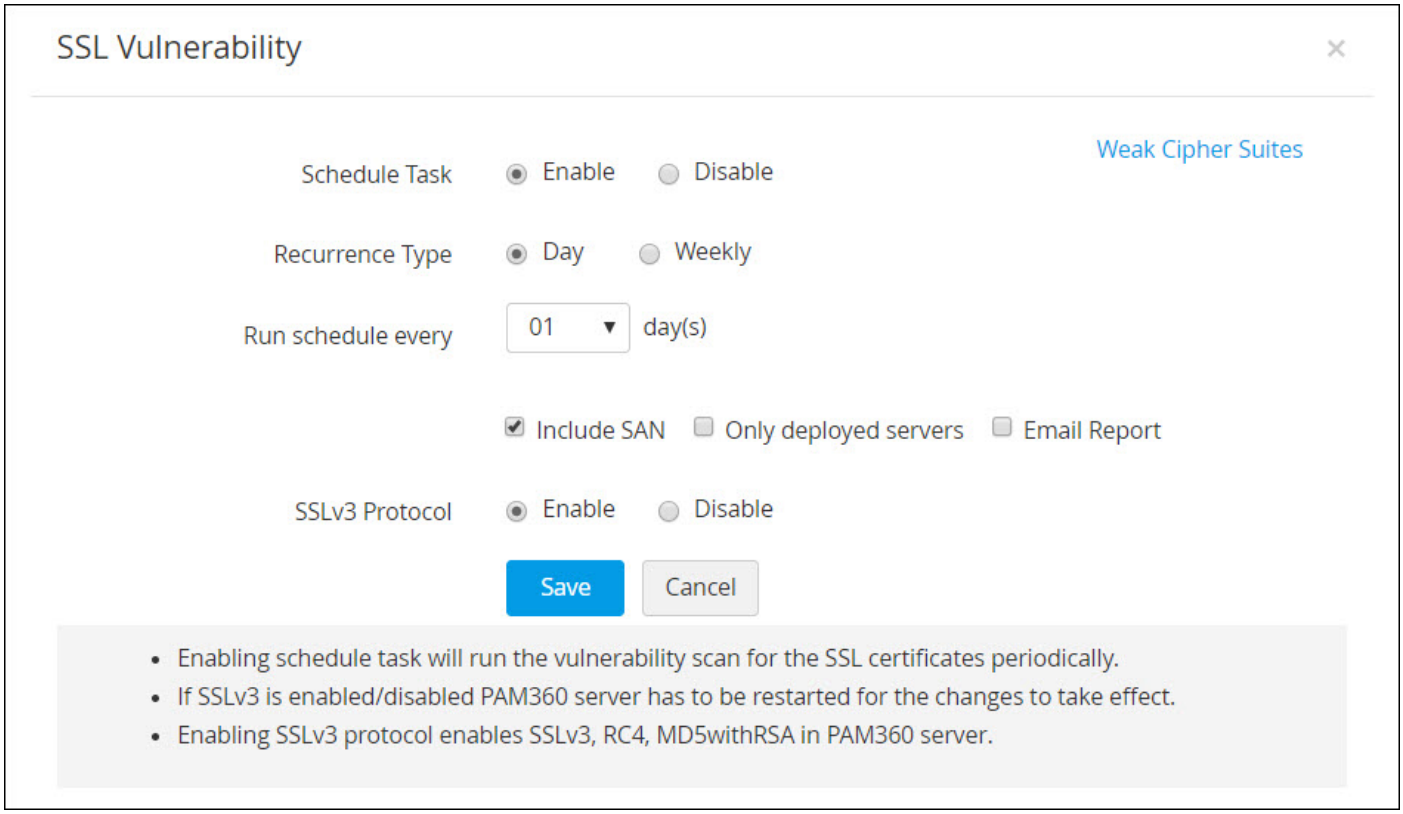
14.5 Leverage integration with Service Desk Plus' CMDB

PAM360 provides the option to integrate with ManageEngine Service Desk Plus' configuration management database (CMDB). You can leverage this integration to export SSL certificate details from PAM360's repository to Service Desk Plus's CMDB, thereby allowing administrators to monitor the usage, expiry, and other aspects of SSL certificates across the organization directly from Service Desk Plus interface.

14.6 SSL vulnerability scanning

PAM360 scans SSL certificates in its repository for any vulnerability, like HEARTBLEED or POODLE, followed by CRL and OCSP revocation statuses. When one or more of the above vulnerability checks renders a positive result, PAM360 flags the particular certificate as vulnerable. This way, users are kept informed of certificates/server configurations that are insecure. Users can then take necessary remedial measures to replace or change the SSL certificates or server configurations. Furthermore, it's recommended to disable SSL 3.0 protocol for all endpoints across the corporate network to prevent any forceful fallback to SSL 3.0, which can open up your communication to security vulnerabilities such as the POODLE.

You can also schedule automatic periodic vulnerability checks for your SSL certificates using PAM360 and notify administrators via email as and when the tests are completed.



14.6 Scheduling SSL vulnerability scanning

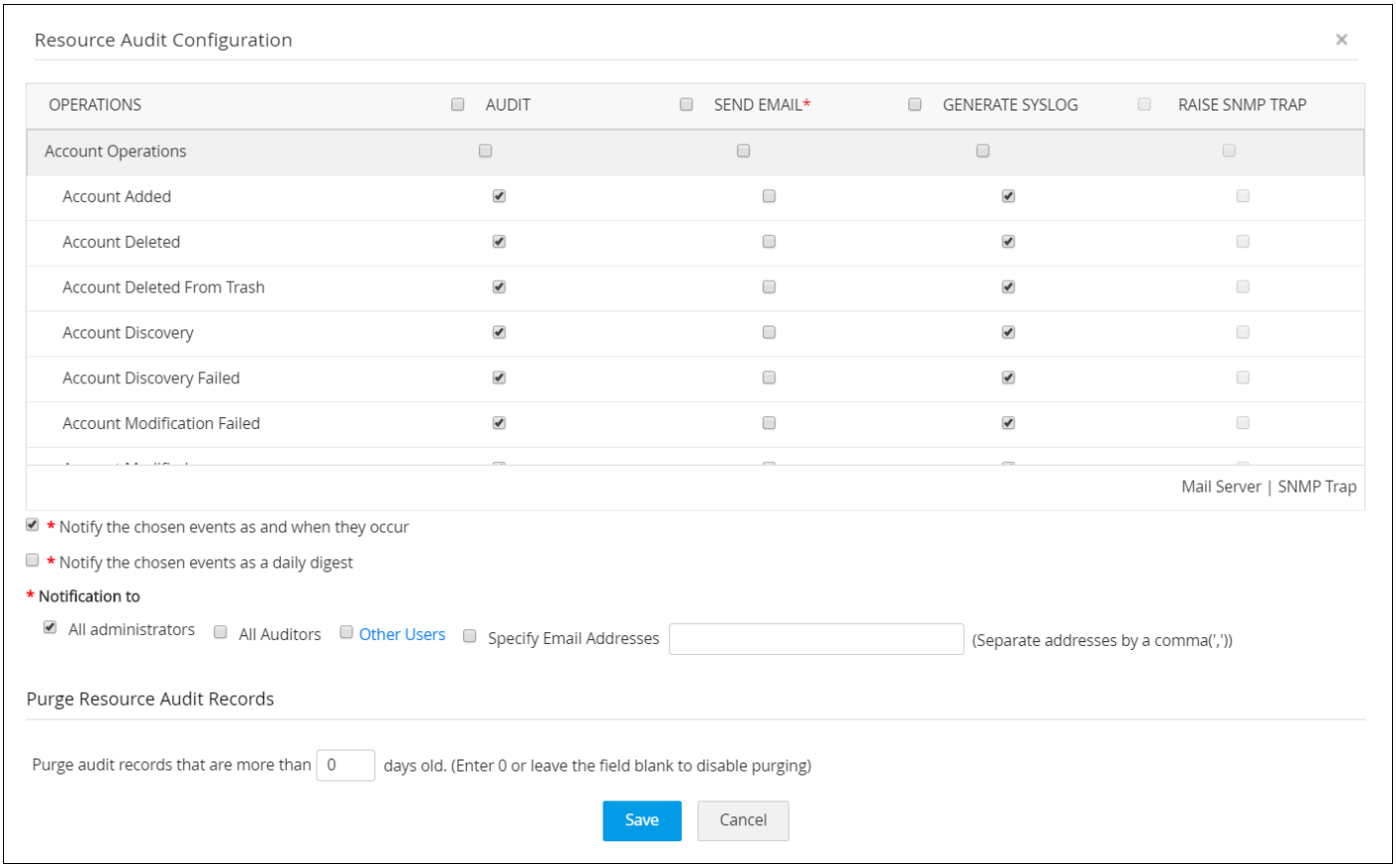
15.0 Auditing and reporting

15.1 Facilitate regular internal audits

Use PAM360's audit trails to instantly record all events around privileged account operations, user logon attempts, scheduled tasks, and completed tasks. By converting this information into well-presented reports, you can facilitate regular internal audits and forensic investigations, easily discovering who did what with a password, where, and when.

15.2 Keep a tab on select activities with instant alerts

PAM360 also lets you send instant email notifications to chosen recipients when certain events take place. This option is very handy to stay constantly updated on what your users are doing. So we recommend you configure alerts for important operations such as new user addition, password deletion, password shares, and so on. Email alerts at the operational level can be enabled by going to **Audit > Resource Audit** (for example) **> Audit Actions > Configure Resource Audit**. Password level alerts can be enabled from **Groups> Actions > Configure Notifications**.



15.2 Configuring resource audits

15.3 Opt for daily digest emails to avoid inbox clutter

If you have enabled alerts and updates for a number of resources, your inbox may overflow with notification emails. In case this occurs, you can choose to receive a daily digest email at the end of each day with a consolidated list of notifications, if hourly updates are not a priority.

15.4 Configure email templates

By default, PAM360 has specific content for email notifications. We recommend you configure the template to suit your needs and customize your own content. This can be done by going to **Admin > Customization > Email Templates**.

15.5 Generate syslog messages and generate SNMP traps to your management systems

If you use a third-party SIEM tool in your organization, you can integrate PAM360 with the tool. This integration allows you to feed syslog messages to the tool whenever an activity takes place within PAM360. This will help you acquire a holistic view of privileged access, along with overall network activity, from a central location.

15.6 Schedule periodic report generation

PAM360 offers a variety of default reports that provide information on password inventory, expiration status, user access frequencies, user activity, and more. Instead of generating these reports manually, we recommend you use the schedule report feature for the required reports to save time. Once scheduled, reports will automatically be generated during the specified interval and sent to your registered email.

15.7 Purge audit records

Naturally, when each and every operation is audited, the audit records grow at a faster rate. If you do not need audit records older than a specified number of days, you can purge them. This can be configured by navigating to **Audit > User Audit** (for example) **> Audit Actions > Configure User Audit**. By default, the purge option will be disabled with the days set to zero (0).

16.0 Integrations with other products and advanced technologies

16.1 Advanced analytics

PAM360 integrates with data analytics tools to help you manage and automatically analyze privileged activities. Through advanced analytics, you can

- Spot unusual user behavior and gain insights to identify security threats.
- Intelligently monitor historical audit logs for malicious account activities.
- Identify sources of anomalies through Zia, the analytics assistant powered by machine learning.
- Blend data from several sources and PAM360 modules to get unified insights for better visibility.
- Get notified of suspicious activity when pre-configured thresholds are breached.
- Email, export, publish, and share key findings through secure sharing options.

PAM360 integrates with ManageEngine Analytics Plus and ManageEngine Log360 UEBA, letting you gain a comprehensive analysis of all your privileged account activities through a unified console.

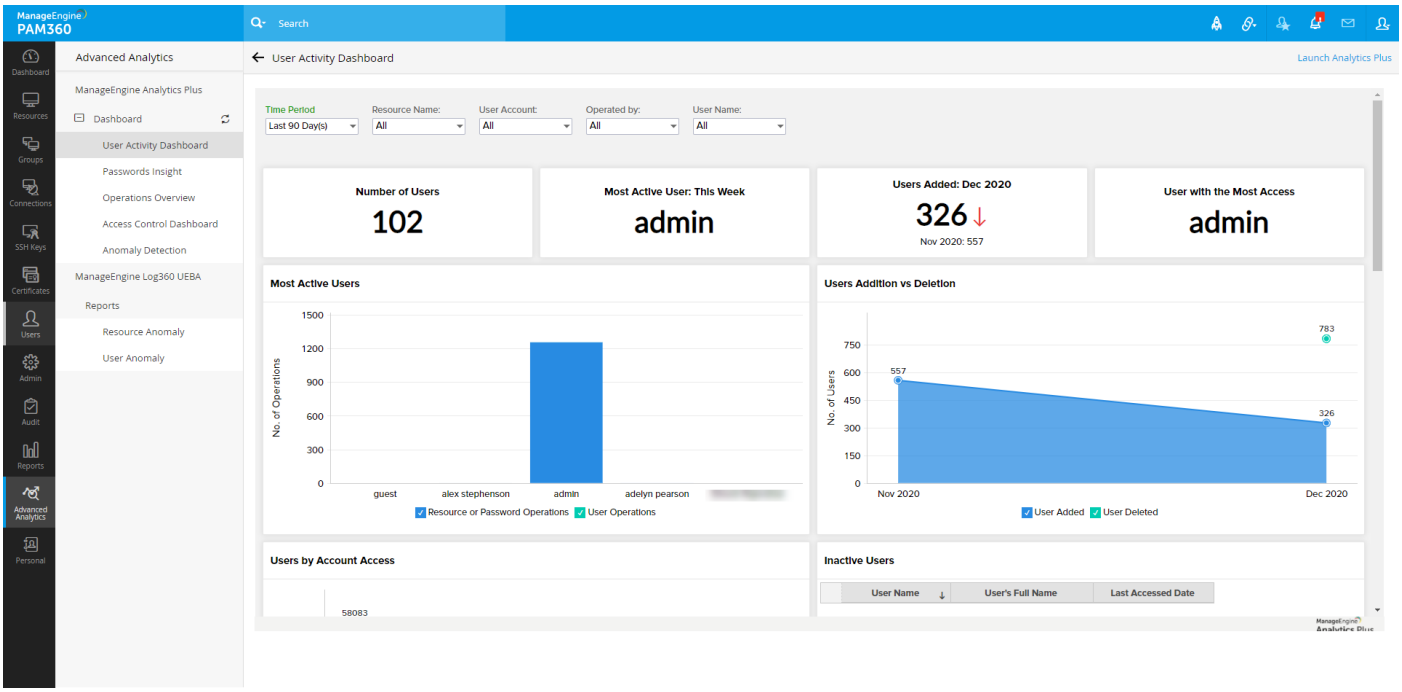
Analytics Plus integration: The Advanced Analytics tab displays different types of dashboards based on the data already imported to Analytics Plus from PAM360.

- **User Activity Dashboard:** Gives you all possible data related to user activity in your PAM360 environment, like the number of users who have accessed a particular resource/account in a particular time period, most active user, number of users added within the selected time period, and the user who has the highest level access.
- **Operations Overview:** Provides a detailed overview of the resource and password related operations, like the number of resources and accounts present, the most active user, the most active resource, and the password access percentage.

- **Access Control Dashboard:** Provides access-related information, like the user who has access to the most number of accounts, the name of the account which is widely shared, and the total number of password requests, and the number of requests revoked for the selected time period.

- **Anomaly Detection:** Provides you details about any anomalous activities that may have taken place within the selected time period, like the number of operations performed in non-business hours, the most frequent non-business hour operation, the number of user sessions carried out during non-business hours, the name of the account that was widely accessed during non-business hours, the user who had the most number of authentication failures, and the user who performed the most number of unauthorized access.

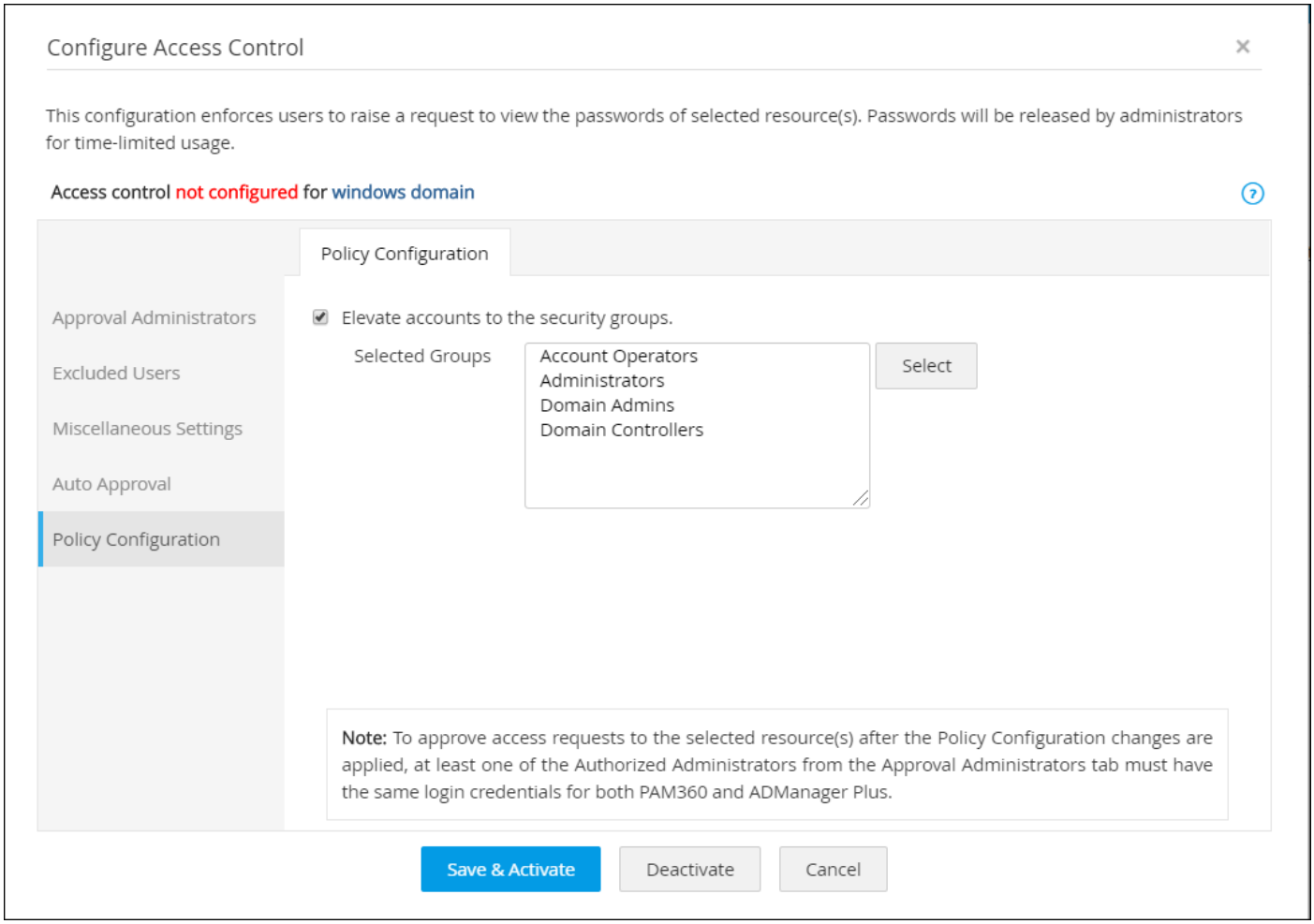
Log360 UEBA integration: Log360 UEBA segregates resource and user audit trails from PAM360 and generates patterns for user behavior, according to the time at which user activity is detected and the number of times a user activity is detected. Through a score-based risk assessment, Log360 UEBA marks any activity that strays from the normal pattern as an anomaly. You can also visualize the anomaly reports in the form of bar graphs and pie charts, schedule their generation, and export them in CSV, PDF, XLS, and HTML formats.



16.1 Advanced Analytics dashboard

16.2 Just-in-time privilege elevation for domain accounts

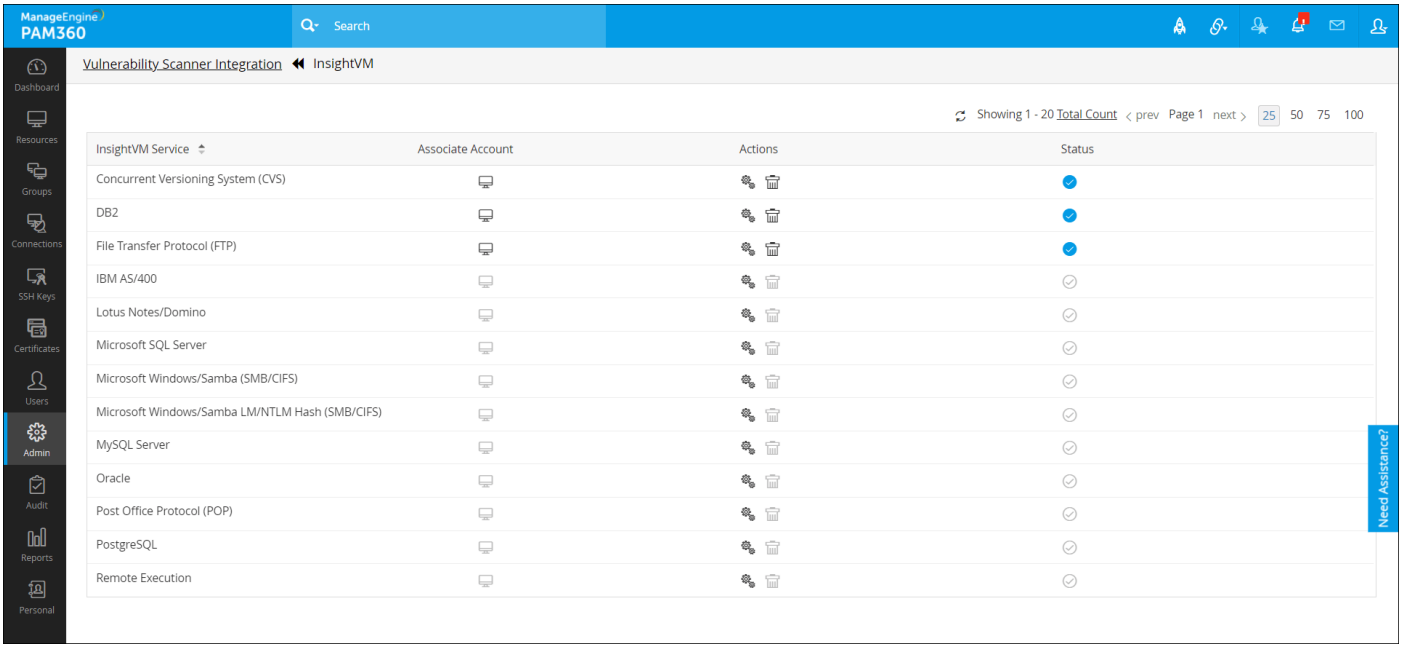
Apart from enabling just-in-time privilege elevation for local Windows accounts, you can also elevate or delegate the privileges of domain users in the AD security groups by integrating with ManageEngine ADManager Plus. By leveraging this integration, we recommend you to enforce access control for PAM360 users on domain accounts and provide them with just-in-time privilege elevation. You can also add and remove accounts from the AD security groups right from the PAM360 interface through this integration.



16.2 Configuring just-in-time privileged access control

16.3 Vulnerability scanners

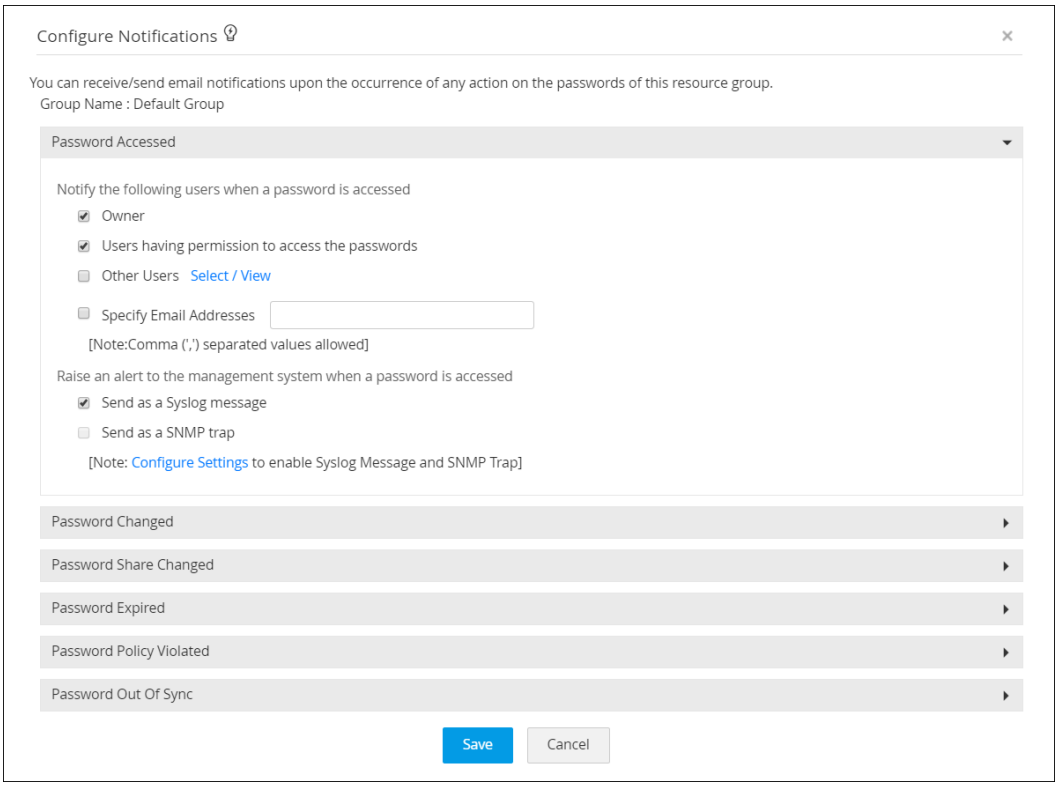
PAM360 integrates with Rapid7 InsightVM, a vulnerability management tool that automatically scans and collects data from all endpoints available in a network and identifies the ones that may pose a security risk. You can leverage the PAM360-InsightVM integration to secure and centrally manage the shared credentials that are necessary to run vulnerability scans, right from the PAM360 interface.



16.3 Integrating InsightVM with PAM360

16.4 Integration with SIEM tools

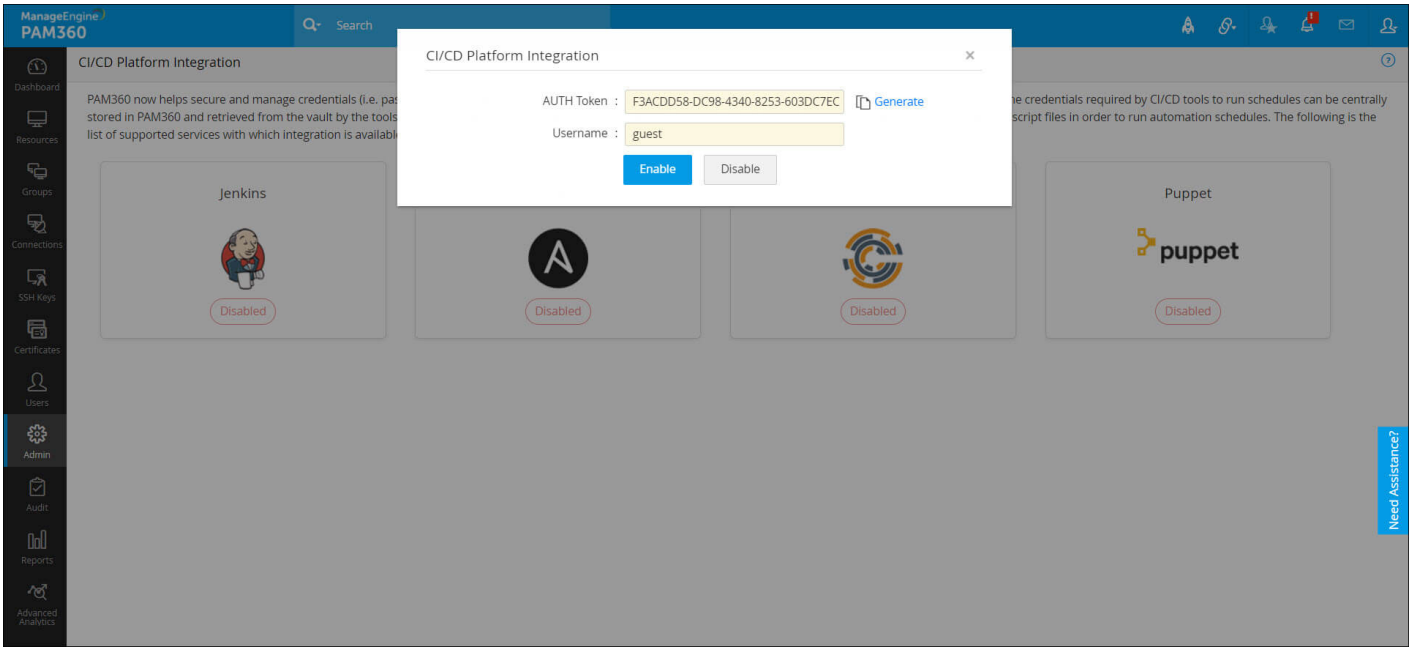
PAM360 integrates with various SIEM tools that help in gathering and processing audit logs for resources, passwords, and users from PAM360 in real time and send them as syslog messages to external log management systems. PAM360 integrates with Splunk, ManageEngine EventLog Analyzer, Sumo Logic, and other syslog collectors. The SIEM integrations will be help you gain deeper visibility into privileged access and the overall network activity, from a single console.



16.4 Customizing syslog event notifications in PAM360

16.5 Plugins for CI/CD platforms

Execution of automation pipelines to run routine tasks often requires sensitive information like privileged passwords, API keys, and access tokens to communicate with other systems, applications, and services in the environment. In most DevOps environments, such credentials are stored in plaintext within script files to enable smooth task execution but that can lead to many security issues. To mitigate such risks, PAM360 helps eliminate embedded credentials in the DevOps pipeline by providing integration capabilities with various CI/CD tools, like Jenkins, Ansible, Chef, and Puppet. The integration ensures that the required credentials are retrieved securely from PAM360's vault every time a task is executed, instead of being stored in plaintext within the script files.



16.5 Enabling Jenkins integration in PAM360

16.6 Robotic process automation (RPA)

PAM360's bot can automate the process of fetching passwords from the repository to connect to a machine, application, or a database, thereby eliminating the need to retrieve passwords manually to perform different tasks. You can combine the PAM360 bot with other RPA bots in your enterprise, like Automation Anywhere, to create a complete endpoint management workflow. For example, if your enterprise needs a secure remote login setup automated through bots, you can configure PAM360's bot to fetch the passwords from the vault and combine it with another bot that initiates the remote connection.

16.7 Self-service password management and SSO capabilities

PAM360 integrates with ManageEngine ADSelfService Plus (ADSSP) to assist domain users in performing activities such as self-service password reset, self-service account unlock, etc. With PAM360-ADSSP integration, the privileged domain account details of ADSSP will be mapped with that of the domain account in PAM360. This ensures that the password of a privileged domain account in PAM360 automatically remains in sync with that in ADSSP, eliminating the need for manual password updates and reducing help desk calls.

17.0 Data redundancy and recovery

17.1 Set up disaster recovery

Data stored in PAM360's database is of critical importance. In the unlikely event of a production setup glitch, all data could be lost. So, disaster recovery is essential. The application provides provisions for both live data backup and automated periodic backups through scheduled tasks. Choose the method that suits your organization best. Also, ensure that the configured destination directory for the backup is in a secure remote location.

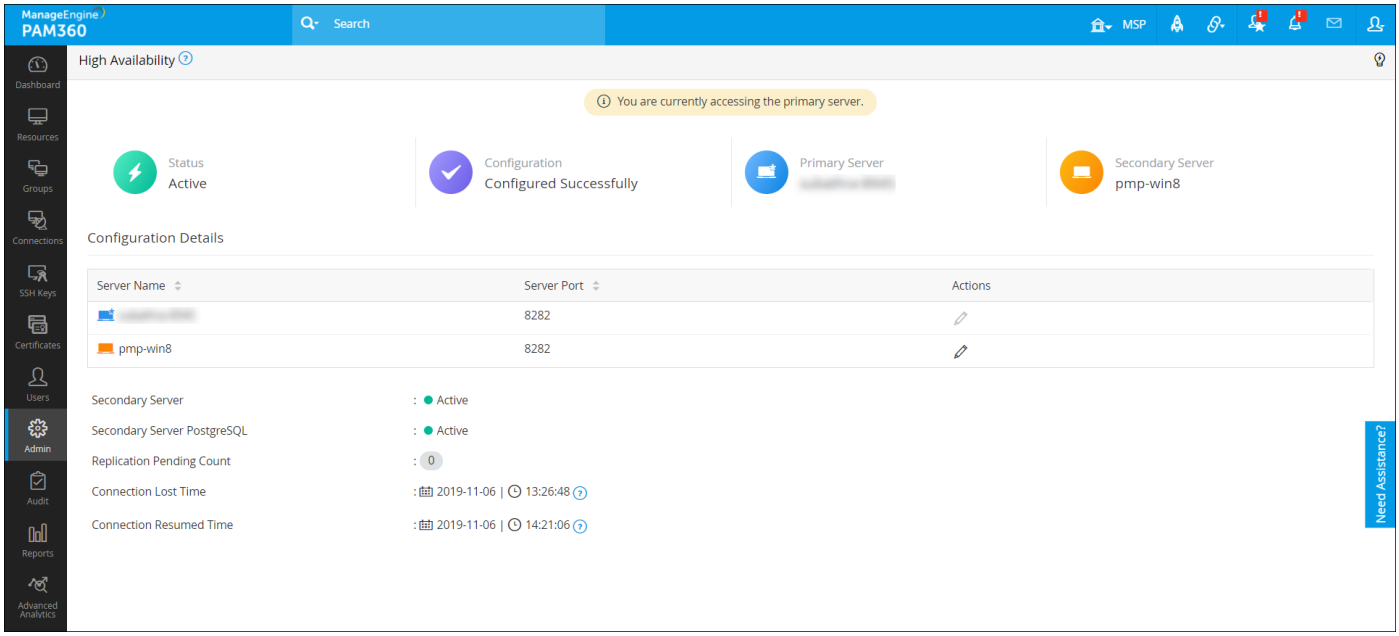
17.2 Deploy a secondary server with a high availability architecture

High availability architecture in PAM360 is a recommended setup that helps you tackle downtime and assure continued access to passwords. This is achieved by installing another instance of PAM360 on a secondary server, in addition to the primary application server. If you have different networks within your workplace (separate networks for each floor, for instance), we recommend you install primary and secondary application servers in different networks.

On the other hand, if you have offices in two different geographical locations, the best practice for a high availability setup is to configure PAM360's primary server in your headquarters and deploy a secondary server in the other office. This way, employees in both locations enjoy uninterrupted access to passwords in the event of server downtime. To set up high availability, go to **Admin > Configuration > High Availability**, and configure a standby server for PAM360.

Monitoring high availability: Continuous monitoring of your endpoints and associated database operations ensures early detection of issues. In the case of the database server, it's essential to have a reliable monitoring system in place, as it measures availability, detects

events that can put down the database server, and provides immediate notifications about critical failures to the concerned parties. PAM360 has built-in high availability management and monitoring capabilities with various notification options. Once you have set up the high availability, you can start monitoring the PostgreSQL HA setup from the PAM360 console by navigating to **Admin > Configuration > High Availability**. The high availability console monitors the availability of your primary and secondary servers and the associated databases.



17.2 Monitoring high availablity

17.3 Application scaling with MS SQL server

For a privileged access security solution like PAM360, it is essential to make it highly available and scalable so that even with increased complexity, the application can render the maximum overall performance without having any significant effect on the average service level per node. It's highly recommended to leverage the application scaling model in PAM360 to ensure uninterrupted access to the privileged resources and passwords. The model works with one main PAM360 node and several sub-nodes, all of them connected to a single MS SQL database cluster. Click here to learn how to configure the main node and the sub nodes in PAM360.

17.4 Failover service

The failover service in PAM360 is also aimed at ensuring uninterrupted access to passwords and other privileged resources. While the high availability feature requires two separate database instances to be mapped to the primary and secondary servers of PAM360 respectively, the failover service functions with redundant PAM360 server instances which have access to a

common MS SQL cluster, which in turn has multiple PAM360 database instances bound to it. Click here to learn more about the failover service.

18.0 Maintenance

18.1 Keep your installation updated

The team at PAM360 constantly releases upgrade packs containing enhancements and fixes. Ideally, major upgrades are released once a quarter, while minor upgrades may be announced once every month or two. These upgrade packs will also contain updates for the Tomcat webserver, PostgreSQL database, and JRE that come bundled with the product. To keep your PAM360 installation properly maintained for optimum performance, we recommend you download and apply upgrade packs for PAM360 as and when they are released. Upgrade packs can be downloaded here.

18.2 Choose your maintenance window wisely

In order to apply upgrade packs, PAM360 has to be temporarily stopped. If high availability is configured, both primary and secondary servers will be down. Moreover, the current design of PAM360 requires high availability to be re-configured after every upgrade. Therefore, we highly recommend you schedule the maintenance window during weekends or non-business hours.

If you cannot avoid carrying out an upgrade during work hours, you can alert your users prior to the upcoming maintenance operation with PAM360's **Message Board**. The **Message Board** option can be found under **Admin > Manage**. You can send the message that you type as an email or an online alert to all users.

18.3 Update your mobile apps and browser extensions periodically

Updates for PAM360's native mobile apps and browser plug-ins are released on a regular basis. We recommend you check for updates in the app and browser stores periodically .

18.4 Look for security advisories

If any security vulnerabilities are discovered in the product, fixes are immediately provided through upgrade packs. A security advisory is also sent to the customer email that you have registered with us. Keep an eye on that email to ensure you don't miss any advisories from us. Whenever you receive one, act as advised in the email.

18.5 Moving the PAM360 installation from one machine to another

To move the PAM360 installation from one machine to another, follow the procedure detailed below:

- Quit PAM360, if it's running.
- Simply copy the entire PAM360 installation folder from one machine to another.
- Then, install it to run as service. In this option, you will not be able to uninstall the program through Windows or add or remove the programs console. If you want to re-install anytime, just delete the entire installation folder.

Caution: Do not remove the existing installation of PAM360 until you've ensured the new installation works fine. This ensures you'll have a valid backup set up in case you need to overcome disasters or data corruption during the move.

19.0 Emergency access provisions

19.1 Use a local PAM360 account for emergency purposes

In the rare event that your Active Directory servers go down, users may be locked out. To deal with this, we recommend you have a local account in PAM360.

19.2 Export passwords as an encrypted HTML file for offline access

Usually, in controlled environments such as data centers, internet connectivity is not allowed on other devices. To ensure access to passwords in such places, PAM360 provides offline access. This feature allows you to export all your passwords as an encrypted HTML file periodically, as desired, and store the file in a secure location. The file will be encrypted with

a 16-digit passphrase provided by you. Only users who know the passphrase can unlock the offline file. You can also configure automatic logout for the file by specifying a time interval (for example, 15 minutes). These settings can be configured by navigating to **Admin > Settings > Export / Offline Access**. Apart from on-demand exports, you can also schedule export operations for the passwords of your resource groups by navigating to Groups, and selecting **Periodic Password Export** from the drop down menu under **Actions**. You can schedule the exports on a daily, weekly or monthly basis.

20.0 When an administrator leaves

There may come a time when one of your administrators leaves the organization. If this happens, make sure to do the following:

20.1 Prepare exit report

When an administrator leaves the organization, you need to first determine their privilege levels in the company and assess the associated vulnerabilities. This practice is critical, since they possess unrestricted access to your IT assets. In these cases, we recommend you generate a custom report in PAM360 containing the complete list of passwords that the specific user had access to. To generate user-specific custom reports, navigate to **Users**, select specific user and then click on **'User Report'** icon under **Reports** column.

20.2 Transfer ownership of resources

After acquiring the list of resources created by the leaving administrator, transfer the ownership of all those resources to yourself or another administrator in PAM360. You cannot delete the administrator's account in the application until you do this. Transferring ownership of resources can be done by navigating to **Users**, selecting the leaving administrator, and then choosing **Transfer Ownership** from the drop down menu under **User Actions**.

20.3 Transfer approver privileges

If you have access controls configured, the leaving administrator may have been an approver for certain resource (i.e., they might have handled password access requests from other users in PAM360). We recommend you transfer their approver privileges to another administrator when they leave. Approver privileges can be transferred by clicking **Users**, selecting the leaving administrator, and clicking on **Transfer Approver Privileges** from the drop down menu under **User Actions**.

20.4 Reset passwords instantly

To rule out security breaches or unauthorized access attempts in the future, we highly recommend you reset the passwords of all the resources owned by the leaving administrator immediately after the ownership for those resources has been transferred to another user with admin-level permissions.

21.0 Security

21.1 Always choose SSL in all communications

PAM360 offers both SSL and non-SSL modes for sensitive operations including password reset and resource addition or import. For obvious security advantages, we recommend you always opt for SSL communication.

21.2 Prudently execute scripts and prevent malicious inputs

By default, PAM360 will be configured to identify harmful scripts or codes and prevent their execution. In addition, it also prohibits running scripts that contain HTML tags and attributes. This option is a highly recommended best practice since it enhances security. If you need to run a genuine script, temporarily disable this option and enable it immediately after completing the task.

21.3 Configure inactivity timeout

Allowing web-interface sessions to remain alive when users leave their workstations unattended is hazardous from a security point of view. By default, PAM360's web session auto-logout will be set to 30 minutes. We recommend you set it to 15 minutes or even fewer, just to be safe. To configure an inactivity timeout, navigate to **Admin > Settings > General Settings >User Management.**

21.4 Configure auto-logout for browser extensions

You can choose how long your browser extension session should remain active. For maximum security, we recommend you set up automatic logout after a period of 15-30 minutes. Logout periods can be configured under Settings in the browser extension.

21.5 Offline access: Disable passwords' export

PAM360 provides multiple export options for secure offline access, such as plain text spreadsheet files and encrypted HTML files. We always recommend you allow users to export passwords only as encrypted HTML files. In case you've allowed users to export password information in CSV files, disable passwords from being exported as plain text. This can be done by navigating to **Admin > Settings > Export / Offline Access**.

21.6 Restrict API calls, web access, and agent access by black or white listing IP addresses

PAM360 allows you to enable IP based restrictions for web access, API calls, communication from native mobile apps and browser extensions, as well as agent communication from target machines to PAM360 server. We recommend you restrict and provision only a limited number of client systems with access to PAM360. To configure IP based restrictions, navigate to **Admin > Configuration > IP Restrictions > Web Access (or) API Access (or) Agent Access**. The IP restrictions can be set at various levels and combinations, such as defined IP ranges or individual IP addresses.

22.0 Privacy

22.1 Privacy controls

To enhance privacy within the product, PAM360 helps you customize and control the inclusion of personal data in canned reports' generation processes. You can decide whether each personal data input in PAM360 should go as masked entries in the reports or be completely removed from them by navigating to **Admin > Settings > Privacy Settings > Privacy Controls.** We recommend you mask or remove highly confidential data while generating reports.

22.2 Encrypted exports

In order to have an additional layer of security for all the export operations across PAM360, we suggest you enable encryption of exported files by navigating to A**dmin > Settings > Privacy Settings > Encrypted Exports**. You can either set a global passphrase which will be uniformly used for all the export operations or allow users to define their own passphrase for their exported files. Users will then need to provide the passphrase for viewing the exported file.

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