

# 最佳实践指南



# 目录

关于 PAM360 .....	1
关于本指南 .....	1
推荐的系统配置 .....	1
最低系统要求 .....	1
中型企业 .....	1
大型企业 .....	2
安装 .....	2
Windows 和 Linux .....	2
后端数据库 .....	3
确保安装主密钥安全 .....	4
控制数据库凭证 .....	4
服务器和环境设置 .....	5
服务器加固 .....	5
使用专用服务帐户 .....	5
为 Web 服务器配置绑定的 IP 地址 .....	6
通过黑名单或白名单 IP 地址限制访问 .....	6
用户入职和管理 .....	6
利用 AD/LDAP 集成进行身份验证和配置 .....	6
禁用本地身份验证 .....	7
使用双因素认证 .....	7
根据工作职责分配用户角色 .....	8
创建用户组 .....	8
删除默认管理员帐户 .....	8
限制对移动应用程序和浏览器扩展的访问 .....	9
数据的收集和组织 .....	9
添加资源：选择适当的方法 .....	9
记得指定资源类型 .....	9
删除未经授权或不需要的特权帐户 .....	9
在发现资源后随机化密码 .....	10
充分利用资源组的力量 .....	10

使用嵌套资源组并根据部门对资源进行排序.....	10
利用自定义字段提供更加便捷的检索.....	11
密码共享和精细访问控制工作流程.....	11
以不同的访问权限共享密码.....	11
充分利用资源组到用户组的共享.....	11
利用访问控制工作流程.....	12
即时提升本地用户帐户的权限.....	12
要求用户提供查看密码的原因.....	12
将 PAM360 与企业工单系统集成.....	12
密码策略.....	13
为关键资源组设置单独的密码策略.....	13
帐户级密码策略.....	13
在创建策略时定义密码的使用期限.....	14
密码重置和 SSH 密钥轮换.....	14
定期密码随机化和密钥轮换.....	14
选择最适合的密码重置模式.....	14
自动重启服务，实现完整的管理例程.....	15
安全的远程访问.....	15
使用户能够自动登录到远程系统，而无需以纯文本形式泄露密码.....	15
配置网关设置.....	15
充分利用连接的高级设置.....	16
发现和配置Windows 服务器的RemoteApp.....	17
对第三方的特权访问.....	18
管理第三方对公司系统的访问.....	18
数据中心远程访问.....	19
避免循环跳转的服务器凭证.....	19
预先导出密码以备离线访问.....	19
会话管理和监控.....	19
实时监控关键会话.....	19
记录每个特权会话.....	20
定期清除记录的会话.....	21
SSL/TLS 证书管理.....	21
发现和导入.....	21
证书申请和获取.....	22

证书部署 .....	22
与证书颁发机构集成 .....	22
充分利用与Service Desk Plus的CMDB的集成 .....	22
SSL 漏洞扫描 .....	23
审计和报告 .....	23
有助于定期内部审计 .....	23
通过即时警报密切关注特定活动的情况 .....	24
选择每日摘要邮件，以避免收件箱混乱 .....	24
配置电子邮件模板 .....	24
在管理系统内生成Syslog和SNMP 陷阱 .....	24
计划定期报告生成 .....	25
清除审计记录 .....	25
与其他产品和先进技术的集成 .....	25
高级分析 .....	25
域帐户的即时权限提升 .....	27
漏洞扫描器 .....	28
与 SIEM 工具集成 .....	28
CI/CD 平台的插件 .....	29
机器人过程自动化 (RPA) .....	30
自助密码管理和 SSO 功能 .....	30
数据冗余和恢复 .....	30
设置灾难恢复 .....	30
部署具有高可用性架构的备服务器 .....	31
使用 MS SQL 服务器扩展应用程序 .....	31
故障转移服务 .....	32
维护 .....	32
保持版本更新 .....	32
明智地选择您的维护窗口 .....	32
定期更新您的移动应用程序和浏览器扩展程序 .....	32
寻找安全建议 .....	33
将 PAM360 迁移到另一台机器 .....	33
紧急访问功能 .....	33
使用本地 PAM360 帐户进行紧急访问 .....	33
将密码导出为加密的 HTML 文件以供离线访问 .....	33

当管理员离职时 .....	34
编写离职报告 .....	34
转移资源所有权 .....	34
转移审批者权限 .....	34
立即重置密码 .....	34
安全 .....	34
在所有通信中始终选择 SSL .....	35
谨慎执行脚本并防止恶意输入 .....	35
配置不活动超时 .....	35
配置浏览器扩展的自动注销功能 .....	35
离线访问：禁用密码导出 .....	35
通过黑名单或白名单 IP 地址限制 API 调用、Web 访问和代理访问 .....	35
隐私 .....	36
隐私控制 .....	36
加密导出 .....	36

## 关于 PAM360

PAM360 是一个基于 Web 的特权访问管理 (PAM) 解决方案, 可通过对公司敏感信息的规范访问, 避免企业受到特权滥用的风险。通过强大的特权访问治理、更顺畅的工作流程自动化、高级分析以及与各种 IT 服务的上下文集成, PAM360 使企业能够将其 IT 管理系统的不同途径整合在一起, 促进有意义的推断和更快的补救措施。它还有助于证明符合 PCI DSS、GDPR、NERC CIP 和 SOX 等要求严格的特权访问控制的法规。

## 关于本指南

本指南介绍在企业网络环境中设置和使用 PAM360 的最佳实践。根据帮助世界各地的企业机构成功部署 PAM360, 对其特权访问管理实践经验的简化, 为 IT 管理员提供了快速有效的软件设置指导。最佳实践可以在产品安装、配置、部署和维护的所有阶段采用, 下文将重点介绍产品的数据安全性、可扩展性和性能。

## 推荐的系统配置

### 最低系统要求

在安装 PAM360 之前, 您需要考虑系统配置。运行 PAM360 的最低系统要求如下, 一般来说, 性能和可扩展性取决于以下因素:

- 用户和组的数量
- 资源和组的数量
- 资源或密码共享的频率
- 计划任务数

基于以上因素, 建议大中型企业进行以下系统设置:

### 中型企业

用户数: 100-500

资源/密码数：低于 10,000

- 双核处理器或以上
- 8 GB 内存
- 40 GB 硬盘空间

## 大型企业

用户数：超过 500

资源/密码数：超过 10,000

- 四核处理器或以上
- 16 GB 内存
- 100 GB 硬盘空间

**注意：**我们还建议您将PAM360安装在一个专用的、经过加固的高端服务器上，以获得卓越的性能和安全性。

## 安装

### Windows 和 Linux

PAM360 可以安装在 Windows 或 Linux 上。尽管该软件在两个平台上都能运行，但在Windows上安装具有以下固有优势：

**活动目录 (AD) 集成：** PAM360的Windows安装可以直接与活动目录集成，导入用户和组。此外，使用域帐户凭证登录 Windows 系统的用户可以使用单点登录 (NTLM-SSO) 自动登录 PAM360。在 Linux 安装中，您必须依赖基于 LDAP 的 Active Directory 服务身份验证。

**Windows 资源的密码重置：** 只要存在直接连接，PAM360 的 Windows 安装就可以在无代理模式下，对所有支持的目标系统执行密码重置。另一方面，Linux 安装需要在Windows 资源和域控制器上部署代理，以

重置 Windows 域帐户、服务帐户和本地帐户的密码。

除此以外，Windows服务账户、计划任务、IIS Web.Config文件和IIS应用池账户的密码重置，只支持从PAM360的Windows安装中进行。

## 后端数据库

PAM360安装支持其在无需配置情况下，可即时使用PostgreSQL 和 MSSQL。默认情况下，该产品内置了 PostgreSQL 数据库，非常适合中小型企业。同时，对于大型企业，我们强烈建议您使用 MSSQL 作为后端数据库，以获得更好的可扩展性、性能，以及集群和灾难恢复功能。

如果您使用 MSSQL 作为后端数据库，我们建议您采用以下做法：

- PAM360仅能通过 SSL 与 MSSQL 进行配置，并具有有效的证书配置。因此，我们建议您为 PAM360 使用专用的 SQL 实例，以避免与现有数据库发生任何冲突或中断。
- 使用 MSSQL 作为后端数据库时，会自动生成一个唯一密钥，用于数据库级加密，默认情况下，此密钥文件将存储在 <PAM360 HOME/conf> 目录中。我们建议您将密钥文件移动到其他位置，以防未经授权的访问。由于高可用性配置和灾难恢复期间需要这个密钥文件，因此其安全性至关重要。密钥丢失将需要您重新配置MSSQL，甚至可能导致数据丢失。
- 在配置MS SQL Server为后端数据库时，请使用 Windows 身份验证，而非使用 SQL 本地帐户。
- 我们建议您使用Windows认证模式，使用相同的域账户来设置MS SQL Server作为您的后端数据库，这样您就可以运行SQL服务和SQL代理服务。
- 建议启用强制加密选项，以允许所有客户端连接到此 SQL 实例。完成后，所有客户端到服务器的通信都将被加密，不支持加密的客户端将被拒绝访问。
- 在运行 MS SQL 服务器的机器上，禁用除 TCP/IP 之外的所有协议。



- 隐藏此 SQL 实例以防止它被其他工具枚举，并禁止除 PAM360 的服务帐户之外的所有其他用户访问此数据库。
- 设置防火墙规则，只允许访问运行 MSSQL 服务器的机器中所需的端口。

## 确保安装主密钥安全

PAM360 使用 AES-256 加密来保护密码和其他敏感信息。由于加密的密钥 (PAM360\_key.key) 是自动生成的，且对于每次安装都是唯一的。默认情况下，此密钥将存储在 **<PAM360 HOME/conf>** 目录下名为 **<PAM360\_key.key>** 的文件中。这个密钥的路径需要在 PAM360 HOME/conf 目录下的 manage\_key.conf 文件中进行配置。PAM360 要求此文件夹具有必要的访问权限，以便在每次启动时读取 PAM360\_key.key 文件。成功启动后，不再需要访问该文件，因此可以使带有该文件的设备脱机。我们强烈建议您将此密钥移动到不同的安全位置，并通过只向 PAM360 服务的运行帐户提供读取访问权限将其锁定。此外，在“manage\_key.conf”文件中更新此远程路径，以便产品在启动时可以读取加密密钥，读取后可以将副本进行删除。您还可以通过将其存储在 USB 驱动器或磁盘驱动器中来保护此密钥，获得极高的安全性。请您创建脚本文件，以将此密钥复制到可读位置，然后在启动后删除该副本。

## 控制数据库凭证

除了 AES 加密之外，PAM360 数据库还通过一个单独的密钥进行保护，该密钥是自动生成的，并且对于每次安装都是唯一的。该数据库密钥可以安全地存储在 PAM360 本身中。但我们建议您将密钥存储在产品服务器中可访问的其他安全位置。

默认情况下，数据库信息（例如 JDBC URL、登录凭证和其他参数）将存储于 **<PAM360 HOME/conf>** 目录下名为 database\_params.conf 的文件中。尽管数据库配置设定为不接受任何远程连接，但我们建议您将此文件移动到安全位置，同时限制访问，并使其仅可用于 PAM360 的服务帐户。如果您将 database\_params.conf 文件放在 PAM360 安装文件夹之外，您需要在 **<PAM360-Home>/conf/wrapper.conf** 文件（Windows）或 **<PAM360-Home>/conf/wrapper\_lin.conf** 文件（Linux）中指定该位置以及文件名。请注意，如果此处未指定位置，则无法启动服务。

- 此文件的路径在 **<PAM360 HOME/conf>** 目录中的“wrapper.conf”文件中配置。编辑此文件并查

找行 `wrapper.java.additional.9=-Ddatabaseparams.file。`

- 如果您使用的是 Linux 系统进行安装，则需要编辑 <PAM360 HOME/conf> 目录中的“wrapper\_lin.conf”文件。
- 默认路径将配置在 `../conf/database_params.conf`。将“database\_params.conf”文件移动到安全位置，并在上述文件中指定其路径。例如，  
`wrapper.java.additional.9=-Ddatabaseparams.file=\\remoteserver1\tapedrive\shared-files\data  
base_params.conf`
- 保存文件并重新启动 PAM360 以使变更生效。

## 服务器和环境设置

### 服务器加固

默认情况下，PAM360 运行所需的所有组件都存储在安装目录（ManageEngine/PAM360）中。因此，我们强烈建议您对安装了 PAM360 的服务器进行加固。您应该执行的一些基本步骤如下：

- 使用域组策略，为组织中的所有常规域用户禁用对此服务器的远程访问。限制所有普通管理员的读取权限，仅为一两个域管理员提供PAM360驱动器或目录的写入权限。
- 设置出入站防火墙，分别保护出入站流量。使用此设置，您还可以选择需要打开哪些服务器端口，用于执行各种密码管理操作，例如远程密码重置等。

### 使用专用服务帐户

在您的域控制器中为 PAM360 创建一个单独的服务帐户，并在其所有区域中使用。此服务帐户将用于运行 PAM360，请到 PAM360 所在服务器中的服务控制台（“services.msc”），安装并导航到 PAM360 的属性，使用创建的服务帐户更改配置的本地系统帐户。同样的服务帐户也可用来从活动目录导入用户和资源。

## 为 Web 服务器配置绑定的 IP 地址

默认情况下, PAM360 的 Web 服务器将绑定到安装应用程序的服务器的所有可用 IP 地址。因此, PAM360 可以通过配置的端口 (7272) 在任何 IP 地址上进行访问。为了限制这种情况, 我们建议您将 Web 服务器配置为绑定到单个 IP 地址, 并仅接收来自该 IP 地址的传入通信。以下步骤可用于配置绑定 IP:

- 如果 PAM360 正在运行, 请立即停止。
- 打开 <PAM360\_HOME>\conf 文件夹中的“server.xml”文件
- 搜索此行:

```
<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"/>
```

在上面行中, 在port="7272" 旁边的位置, 添加属性address="127.0.0.1". 将 127.0.0.1 替换为您要用于绑定的服务器的实际 IP 地址。

## 通过黑名单或白名单 IP 地址限制访问

只要有连接, 就能够从任何客户端系统访问 PAM360。因此, 我们建议您仅限制或配置有限数量的客户端系统对PAM360 的访问。要配置基于IP的限制, 导航到 **管理 > 配置 > IP限制**。IP 限制可以设置为各种级别和组合, 例如定义的 IP 范围或单个 IP 地址。您可以选择允许 Web 访问特定 IP范围和地址, 或者通过将它们添加到阻止的 IP 地址字段来限制访问。

## 用户入职和管理

### 利用 AD/LDAP 集成进行身份验证和配置

将 PAM360 与活动目录或任何符合 LDAP 的目录集成可能非常有用, 因为它提供了以下好处:

**用户预配或取消预配：**通过 AD/LDAP/Azure AD 集成，PAM360 中的用户添加既快捷又简单。集成后，您可以直接将用户配置文件或从组或 OU 的目录导入至 PAM360。此外，您可以根据用户的 AD/LDAP 配置文件轻松地将所需的权限级别分配给用户，简化了产品中的用户帐户配置。例如，如果您将现有的“数据库管理员”OU 从目录导入到 PAM360，可以轻松地将数据库密码分配给该导入组。

最重要的是，您可以在 PAM360 与您的目录集成后启用同步，以便任何更改（例如新添加的用户或在目录中的 OU 之间移动的用户）都会自动反映在 PAM360 中。将 PAM360 与您的目录同步，还会在从相应的用户目录中永久删除用户时通知您。PAM360 会禁用和锁定这些用户账户，并通过电子邮件和警报来通知您，您可以选择删除这些帐户或重新激活。

**活动目录身份验证：**另一个好处是您可以利用目录各自的身份验证机制，为您的用户提供单点登录 (SSO) 选项。激活此选项后，只要用户已经使用其目录凭证登录到系统，就会自动在 PAM360 中进行身份验证（使用基于 NTLM 的身份验证）。使用 AD/LDAP 凭证进行 PAM360 身份验证，可确保登录密码不会存储在本地 PAM360 中，因为用户将直接从您的目录中进行身份验证。

## 禁用本地身份验证

将 PAM360 与您的 AD/LDAP 兼容目录集成后，我们建议您禁用本地身份验证并让用户使用其 AD/LDAP 凭证登录 PAM360。要禁用本地认证，请导航到 **管理 > 设置 > 常规设置 > 用户管理**。

但是，如果您已配置本地 PAM360 帐户用于“break glass”（检查系统账户密码的行为，以绕过正常的访问控制程序，应对重大紧急情况），则不能禁用本地身份验证。在这种情况下，如果您仍然希望只进行 AD/LDAP 身份验证，我们建议您禁用同一部分中的“**忘记密码**”选项（用于重置 PAM360 中所有用户的本地身份验证密码的选项）。禁用此选项将确保用户可以仅使用其 AD/LDAP 凭证登录 PAM360，即使启用了本地身份验证也是如此。

## 使用双因素认证

用户身份验证添加额外的保护层，可确保只有正确的人才能访问您的敏感资源。PAM360 提供了多个选项，用于提供在对产品 Web 界面访问之前配置二次身份验证。第二因素选项包括 Azure MFA、RSA SecurID 令牌、Duo Security、Google Authenticator、通过电子邮件的唯一密码以及任何符合 RADIUS 的双因素身份验证等。我们强烈建议为您的用户配置双因素认证。



PAM360中的双因素认证选项

## 根据工作职责分配用户角色

添加用户后，为其分配适当的角色。PAM360 有四个预定义的用户角色：管理员、密码管理员、密码审核员和密码用户。要了解更多关于每个角色的权限，请参考我们的 [帮助文档](#)。管理员角色应仅限于除了密码管理之外，需要执行用户管理操作和产品级配置的少数员工。

**使用超级管理员角色：**PAM360 中的超级管理员可以访问所有存储的密码。理想情况下，是不需要此角色的。但是，如果您想拥有一个用于紧急情况的专用帐户，您可以为您的组织创建一个超级管理员。出于安全考虑，此角色应始终限于组织层次结构中的最高层人员。此外，在这种情况下，最好的做法是只创建一个超级管理员。一旦一个管理员被提升为超级管理员，他们就可以根据需要阻止在未来创建更多的超级管理员。这可以通过超级管理员导航到 **管理员 > 认证 > 超级管理员**，然后启用 **拒绝由管理员创建超级管理员** 来完成。

## 创建用户组

将您的用户组织成组，例如 Windows 管理员、Linux 管理员等。用户分组在共享资源和委派密码时有很大帮助。如果您已将 PAM360 与 AD/LDAP 集成，则可以直接从目录导入用户组并使用相同的层次结构。

## 删除默认管理员帐户

出于安全原因，我们强烈建议您在添加一个或多个具有管理员角色的用户后，删除 PAM360 中的默认管理员和访客帐户。

## 限制对移动应用程序和浏览器扩展的访问

默认情况下，所有用户都可以访问 PAM360 的原生移动应用程序和浏览器扩展。如果您希望用户从其工作站以外的任何设备都无法访问任何密码，请在您的企业结构中全局禁用对移动应用程序的访问。如果需要，您可以单独为所需用户或管理员启用访问权限。同样，您也可以启用或禁用对浏览器扩展的访问。这些限制可以通过导航到 **用户 > 更多操作** 并从下拉菜单中选择 **启用浏览器扩展访问** 来实施。

## 数据的收集和组织

### 添加资源：选择适当的方法

在 PAM360 中开始使用密码管理的第一步是添加资源。自动发现特权帐户是一个最快速方便的方法。其他方法是手动添加和 CSV 导入。如果您在使用 PAM360 之前使用的另一个工具，或者您有自己的帐户，那么可以通过使用 CSV/TSV 功能将您的资源存储在 spreadsheets 中。

### 记得指定资源类型

在手动或通过 CSV 导入添加资源时，请务必确保资源是否已导入至正确的资源类型下。这对于使用密码重置等功能是强制性的，因为 PAM360 根据应用的资源类型对不同的资源使用不同的通信模式。除非指定，否则资源将被放置在“未知”下，在这种情况下，密码重设将失败。PAM360 支持许多默认的资源类型，在 **管理 > 资源配置 > 资源类型** 下可以看到。

### 删除未经授权或不需要的特权帐户

当您使用自动发现功能来清点网络上的 IT 资源及其各自的特权帐户时，默认情况下，PAM360 将获取与网络上检测到的资源相关联的所有帐户。某些帐户可能是未经授权的、不需要的或孤立的。例如，当您添加 Windows 资源时，所有访客帐户也将被获取。

从安全角度来看，应识别和删除未经授权的帐户，以避免将来出现任何不可预见的漏洞。密码管理最佳实践要求特权帐户的数量应保持在最低限度。此外，管理过多不需要的密码资源会使数据库杂乱无章，使数据组织成为一项艰巨的任务。因此，我们建议您在 PAM360 中执行**自动发现**功能之前，删除目标计算机中的这

些不需要的帐户。

## 在发现资源后随机化密码

完成资源发现和帐户枚举后，我们强烈建议您将所有帐户的密码随机化。这种做法很重要，因为在部署 PAM360 之前，您的员工可能已将其密码存储在不同的媒介中，例如电子表格和文本文件，甚至可能采用明文纸张的方式记录密码。如果不更改密码，这些员工仍然可以绕过 PAM360 直接访问之外的资源。因此，密码必须在资源发现后适当地随机化，以阻止所有对资源的直接、未经授权的访问。此外，随机化还能够帮助消除弱密码，并为资源分配了强且唯一的密码。可以从 **资源 > 选择特定资源 > 资源操作 (顶部) > 配置 > 远程密码重置** 对发现的帐户执行密码随机化

**提示:** 在发现新帐户时预设密码随机化，您可以从 **资源 > 选择特定资源 > 资源操作 (在顶部) > 发现账户** 进行配置，然后在打开的新窗口中启用 **发现后随机密码**。

## 充分利用资源组的力量

PAM360 中的资源组的特权等级是很高的。大多数高级密码管理操作（例如自动密码委派和计划的密码轮换）只能在资源组级别执行。在两种类型的资源组创建中，强烈推荐“**基于标准**”的组。

**基于标准的组即动态组**。它们具有基于您所设置的条件，将满足特定标准的资源整合到一个组中的灵活性。定义条件后，PAM360 将自动识别所有匹配资源并创建组，无需人工干预。

## 使用嵌套资源组并根据部门对资源进行排序

为了方便使用和导航，从庞大的数据库中检索单一的资源时，您可以利用 PAM360 中的资源管理器树形视图设置（即创建嵌套的资源组）。默认情况下，每个用户显示的树形图都是不同的。启用这个树状视图设置，可以在整个组织内全局显示统一的资源管理器树形视图。启用后，将主节点的名称从“**资源组**”变更为您组织的名称。

基于此，您可根据拥有的不同团队或部门创建树形目录中的子节点。随后，您可以将子节点下的资源组与所属团队或部门相关联。

通过以上方法操作资源管理器树，您可以得到一个清晰的资源组层次结构，从而提供轻松、便捷的

访问体验。要允许操作资源管理器树，请导航到 **管理 > 全局设置 > 密码检索**，然后启用“**允许所有管理员用户操作整个资源树**”。

## 利用自定义字段提供更加便捷的检索

添加资源时，您可以使用附加字段来创建自定义列和值。这些字段可用于创建基于标准的组、检索特定资源或密码、共享资源等。

## 密码共享和精细访问控制工作流程

### 以不同的访问权限共享密码

在共享资源时，密码所有者可以选择以下选项向用户和组授予不同的权限级别：

- **仅限Remote App**：用户和用户组只能访问和使用与资源关联的远程应用程序。
- **查看密码**：用户只能访问密码。
- **修改密码**：用户可以访问和修改共享密码。
- **完全访问**：用户对资源或组具有完整的管理权，并且可以重新共享资源、组或个人帐户密码。

我们建议您向用户仅提供“**查看密码**”权限，因为这对于各种与密码相关的操作来说已经足够了。在提供“**完全访问**”权限时要小心，因为对密码具有“**完全访问**”权限的用户几乎是共同所有者，并且能够修改、删除甚至将密码共享给更多用户。

**注意**：除了这些共享权限，您还可以共享资源而不透露明文的密码（本功能仅限资源配置了自动登录时）。要了解有关此功能的更多信息，请参阅第 10.1 节。

### 充分利用资源组到用户组的共享

尽管 PAM360 支持将单个密码或资源与单个用户或组共享，但最佳实践方法是将资源组共享到用户组。这样执行批量操作，能有效的节省时间。例如，如果您需要为组织中的 Windows 管理员提供对所有 Windows



资源的访问权限，您可以通过两个简单的步骤完成该操作：

- 创建一个基于标准的资源组（将“Windows”资源类型作为匹配标准）。这样，所有的 Windows 资源都会添加到组中，并且将来创建的新资源也将自动添加到组中。
- 为 Windows 管理员创建用户组。如果您已经集成了 AD/LDAP，您可以直接导入 AD 域中的组并启用用户数据库的自动同步。这样，每当有新的 Windows 管理员加入该组后，他们的 AD 帐户将自动添加到 PAM360 的用户组中，新用户随后将继承该组的权限即查看 Windows 关联的服务器的密码。

## 利用访问控制工作流程

PAM360 中的访问控制是一种请求-释放机制，不允许用户直接访问密码，而是要求用户必须向管理员提出请求获得访问批准。

该功能还可以帮助您为资源引入各种访问限制，例如限时访问、并发控制和使用期后的自动重置。因此，我们强烈建议您为关键资源的凭证启用此释放机制。为了提高安全性，您还可以为关键资源配置双重批准，这要求两个或多个管理员在释放密码之前必须批准请求。当管理凭证主要由组织中的两个不同部门拥有时，此设置会派上用场。可以通过转到 **资源 > 资源操作 > 配置 > 访问控制** 来配置访问控制。

## 即时提升本地用户帐户的权限

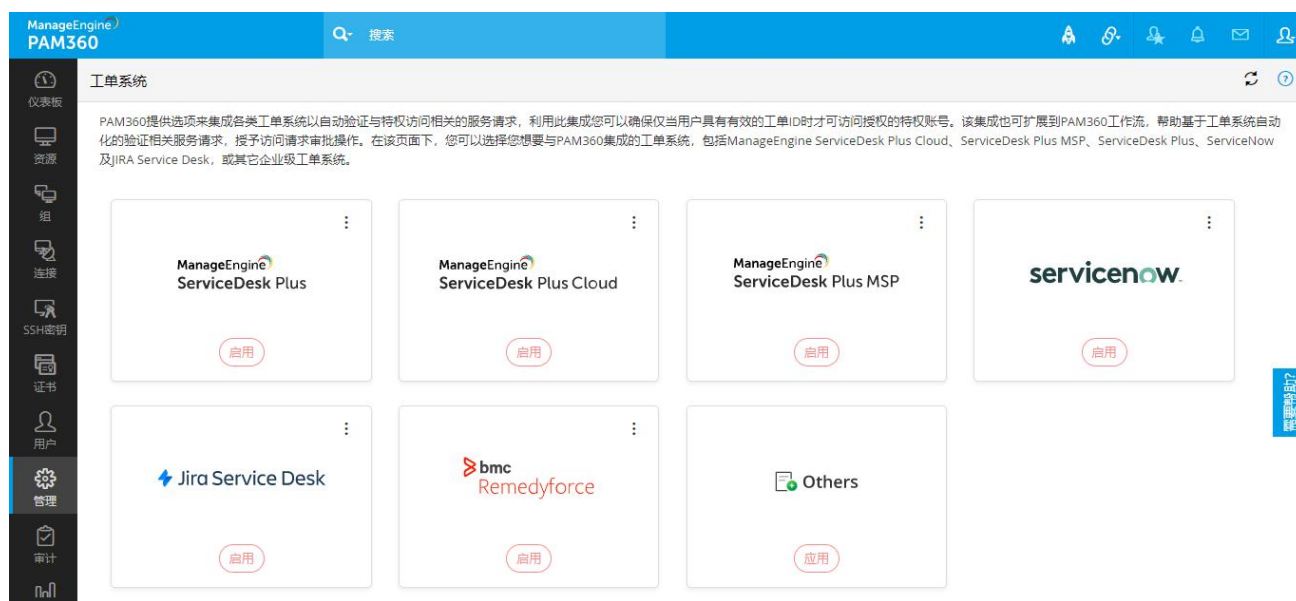
PAM360 还允许管理员通过向 Windows 资源中的本地用户帐户提供即时 (JIT) 权限提升，在特定时期内向用户授予密码访问权限。例如，如果“dbuser”是没有任何管理员权限的本地 Windows 帐户，则管理员可以在特定时间段内将其权限提升为与管理员或任何其他特权用户相同的权限。

## 要求用户提供查看密码的原因

默认情况下，所有与密码相关的操作都记录在 PAM360 的审计跟踪中，并附有时间戳和 IP 地址详细信息。或者，您可以要求用户提供访问密码的原因。这些原因也将记录在审计跟踪中，可用于法务取证。因此，每当用户尝试检索资源的密码时，我们建议您强制要求他们提供要求访问的可信理由，无论是否配置了访问控制。此选项可以在 **管理 > 设置 > 全局设置 > 密码检索** 下激活。

## 将 PAM360 与企业工单系统集成

PAM360 提供了集成一系列工单系统的选项，以自动验证与特权访问相关的服务请求。集成确保用户只能使用有效的工单 ID 访问授权的特权密码。为了您的关键资源密码能够启用更强大的检索工作流程，我们建议您将 PAM360 与您的企业工单系统集成。目前，PAM360 可轻松与 ManageEngine ServiceDesk Plus On-Demand、ServiceDesk Plus MSP、ServiceDesk Plus、ServiceNow 和 JIRA 集成。您可以通过导航到**管理 > 集成 > 工单系统集成**，将 PAM360 与上述工单系统集成。



与领先的企业工单系统集成

## 密码策略

### 为关键资源组设置单独的密码策略

首先，密码策略通过指定字符的复杂性来帮助您定义密码强度。PAM360 允许您为不同的资源组自定义和配置不同的密码策略。如果您有少数资源本质上是超敏感的，请将它们全部组织到一个资源组中，并配置一个具有非常严格要求的单独策略。资源组的策略可以从 **组 > 选择特定组 > 批量配置 > 关联密码策略** 来配置。

### 帐户级密码策略

通常，每个资源都会配备一个或几个管理帐户，或其他普通账户。为了保护这些特权账户，我们建议您为重要资源的敏感账户单独配置强密码策略。帐户级密码策略可以从 **资源 > 选择特定的资源 > 资源操作**（在顶部）> **关联密码策略** 中配置。

## 在创建策略时定义密码的使用期限

配置新密码策略时，请务必记住设置最长密码使用期限。指定期限让 PAM360 在期限到期时自动重置密码。如果您不填写该字段，密码将不会过期，我们并不推荐您这样做。

## 密码重置和 SSH 密钥轮换

### 定期密码随机化和密钥轮换

特权账户的安全管理需要使用强大、独特的密码，并定期重置。理想情况下，密码应该至少每90天重置一次--这是IT法规（如PCI-DSS）规定的最常见的时间框架。我们建议您在PAM360中使用预定的密码重置功能为资源组配置定期密码重置。更重要的是，在以下情况下，也要配置密码自动重置：

- 用户使用完密码后
- 撤销用户的密码共享时
- 当密码过期时

对于 SSH 密钥，强烈建议每 30至45 天轮换一次密钥，以及在出现人员变动后立即进行批量轮换。

### 选择最适合的密码重置模式

密码重置可以在 PAM360 中以以下两种模式之一进行：非代理或代理。

对于非代理模式，PAM360 直接与目标系统连接并更改密码。此时，您必须提供管理凭证。针对Linux操作系统，需要两个账户：一个是具有root权限的账户，一个是普通用户权限的账户，普通权限账户即可以用来远程登录。

另一方面，当您必须为没有直接连接的资源重置密码时，代理模式就派上用场了，例如那些在 DMZ 位置或有防火墙限制的资源。为了完成这些密码重置，您可将PAM360代理部署到执行任务的远程主机。代理到应用服务器之间的所有通信都是单向的，且是通过 HTTPS 进行的，所以您不必在目的设备防火墙上开启任何额外的防火墙端口。基本上，在这两种模式中，非代理模式是最方便、最可靠的修改密码的方式，只要资

源可以直接到达，我们就推荐您选择该模式。但是，针对以下用例，您需要选择基于代理的模式：

- 当 PAM360 中特定资源的管理凭证不可用时。
- 当所需服务未在目标资源上运行时（Linux 为 Telnet/SSH，Windows 为 RPC）。
- 当 PAM360 在 Linux 上运行时，而您需要更改 Windows 资源的密码时。
- 当您有两个不同的环境“A”和“B”，且在二者之间有防火墙时。在这种情况下，您可以在 A 环境中安装 PAM360，并在环境 A 的机器上使用非代理模式。另一方面，您可以在环境 B 的机器中安装代理进行密码重置。这样，所有密码都可以在 A 和 B 中进行管理，而无需添加另外的防火墙端口。

## 自动重启服务，实现完整的管理例程

使用 PAM360，也可以用于定期重置运行各种服务和 IIS 应用程序池的 Windows 域帐户的密码。为确保服务、任务和应用程序池在密码更改后仍能正常工作，我们建议您在 PAM360 中启用提供的**在密码重置后自动重启**的服务选项。

## 安全的远程访问

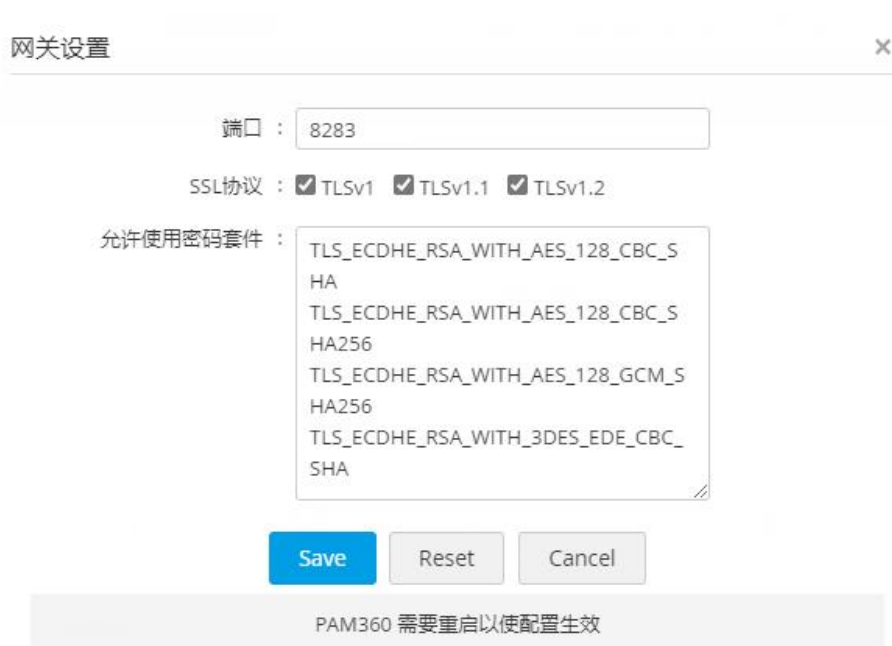
### 使用户能够自动登录到远程系统，而无需以纯文本形式泄露密码

在您配置自动登录选项以远程连接到机器后，PAM360 允许用户只需单击一下即可建立与远程系统的直接连接，无需复制粘贴密码。在这种情况下，我们建议您禁用用户以纯文本形式检索密码，您可以从 **管理 > 设置 > 全局设置 > 密码检索**中选择**如果已经配置自动登录，允许用户查看密码**选项。

## 配置网关设置

PAM360 允许您自定义网关设置。您可以编辑和控制用于 SSL 通信的密码套件，设置不同的端口，选择 SSL 协议用于保护从产品发起的远程连接，自定义 HTTP 头的日志设置等。要编辑网关设置，请导航到 **管理 > 连接 > 网关设置**。除此之外，您还可以参考 `<PAM360_installation_directory>\conf` 路径中的 `gateway.conf`

文件，以获得更广泛的自定义和其他技术细节。



网关设置

端口 : 8283

SSL协议 :  TLSv1  TLSv1.1  TLSv1.2

允许使用密码套件 :

- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

Save Reset Cancel

PAM360 需要重启以使配置生效

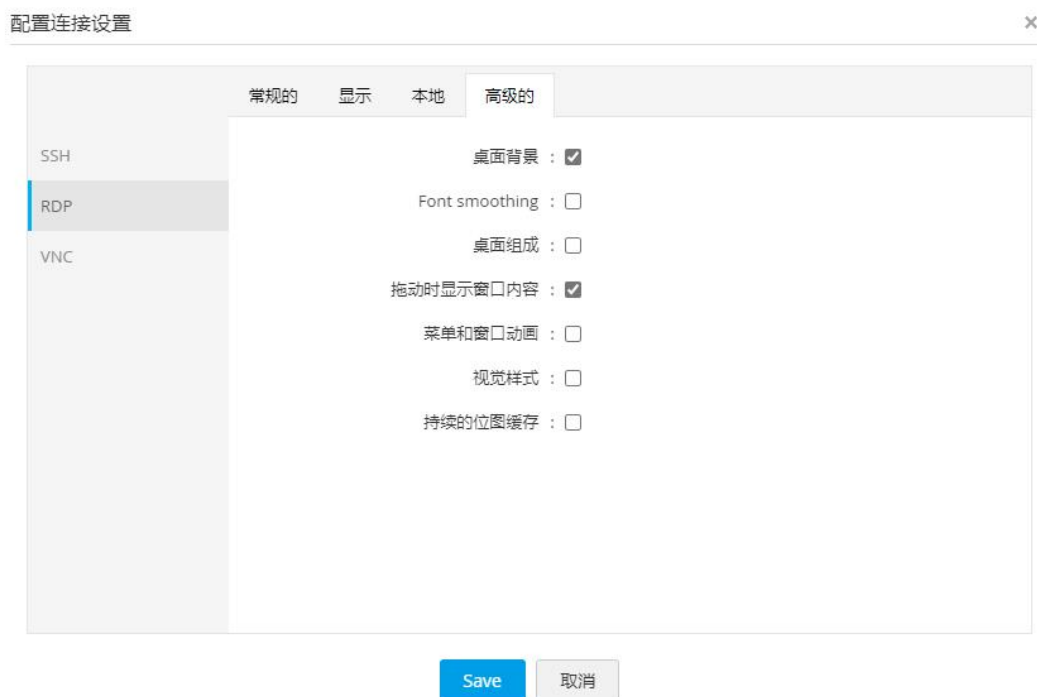
#### 配置网关设置

## 充分利用连接的高级设置

PAM360 为可以定制的连接提供高级配置设置，以提高从产品内部发起的远程连接的速度和性能。这些增强功能可用于 SSH、RDP 和 VNC 连接，以实现集中配置和易用性。此处所做的所有设置更改也将应用在远程系统上。一些高级设置包括键盘布局、桌面背景、映射驱动卷、远程音频支持等。

要配置这些设置，请导航到“资源模块”并切换到“密码”选项卡。在这里，点击所需账户旁边的“账户操作”下拉，并点击下拉中的“连接设置”。将单独打开所选帐户类型 (SSH/RDP/VNC) 的连接设置。

[点击这里](#) 了解更多高级设置。



RDP 的高级设置

## 发现和配置Windows 服务器的RemoteApp

**注意：**您需要在远程目标服务器上安装所需的RemoteApps才能使用此功能。

除了启动与远程系统的直接连接外，您还可以允许用户连接到在目标系统中配置为 RemoteApps 的特定应用程序。您可以自动发现配置在目标Windows系统中的RemoteApps，或可在PAM360中进行手动添加。为Windows 连接配置 RemoteApps 可以更安全地管理特权 RDP 会话。例如：假设您为特定用户将应用程序（例如 SQL Studio）列入白名单。那么，当用户启动会话时，它将自动打开 SQL Studio，并且用户只能使用该应用程序。除了使用 SQL Studio 之外，他们无法看到任务栏、或导航到任何其他区域、或执行任何其他操作。



配置远程应用程序

## 对第三方的特权访问

### 管理第三方对公司系统的访问

大多数情况下，承包商、顾问和供应商等第三方需要访问公司 IT 资源，以满足各种合同职责和其他业务需求。当您向第三方提供特权访问权限时，我们建议您：仅向他们提供临时访问权限，并设定时间限制和最低权限的限制。此外，在与第三方共享关键信息时，我们建议您：

- 由于承包商远程连接到您的资源，请把所有的第三方在PAM360中添加为用户，并限制他们只通过PAM360建立与目标系统的直接会话。
- 在为资源配置自动登录后，最佳做法是共享登录凭证，而不以纯文本形式显示密码。
- 此外，为此登陆信息配置访问控制工作流。这有助于实施访问密码的时间限制，包括在使用期结束时自动重置密码。
- 定期进行影子会话以检测任何恶意行为痕迹并立即采取补救措施。

- 当您终止与供应商的合同时，应立即对供应商有权访问的所有资源执行密码重置。

## 数据中心远程访问

### 避免循环跳转的服务器凭证

通常情况下，连接到远程数据中心资源是一个漫长的过程，因为从安全角度来看，直接访问是受到限制的。从安全角度讲，管理员和用户在最终连接到目标设备之前，必须跳过一系列的跳转服务器，在每个阶段都必须进行身份验证。在每次跳转中，用户都需要采用单独的凭证，才可以连接到数据中心。这种情况对于用户来说，分享过多的凭证并不是一种安全的做法。而使用 PAM360 中的登陆服务器配置功能，您的用户仅需要通过 PAM360 连接到数据中心即可进行自动验证。该应用程序提供了安全的、一键式自动访问数据中心资源的功能，消除了在一跳中进行手工验证的动作需求，此外，它还集中管理了跳转服务器的凭证。

### 预先导出密码以备离线访问

如果数据中心环境不允许互联网连接，您将无法从该网络访问 PAM360。在这种情况下，请事先将所有需要密码导出到加密的 HTML 文件，以离线访问密码。如果导出选项被启用，您可以从 **资源 > 资源操作**（在顶部） > **导出所有密码** 下载文件。

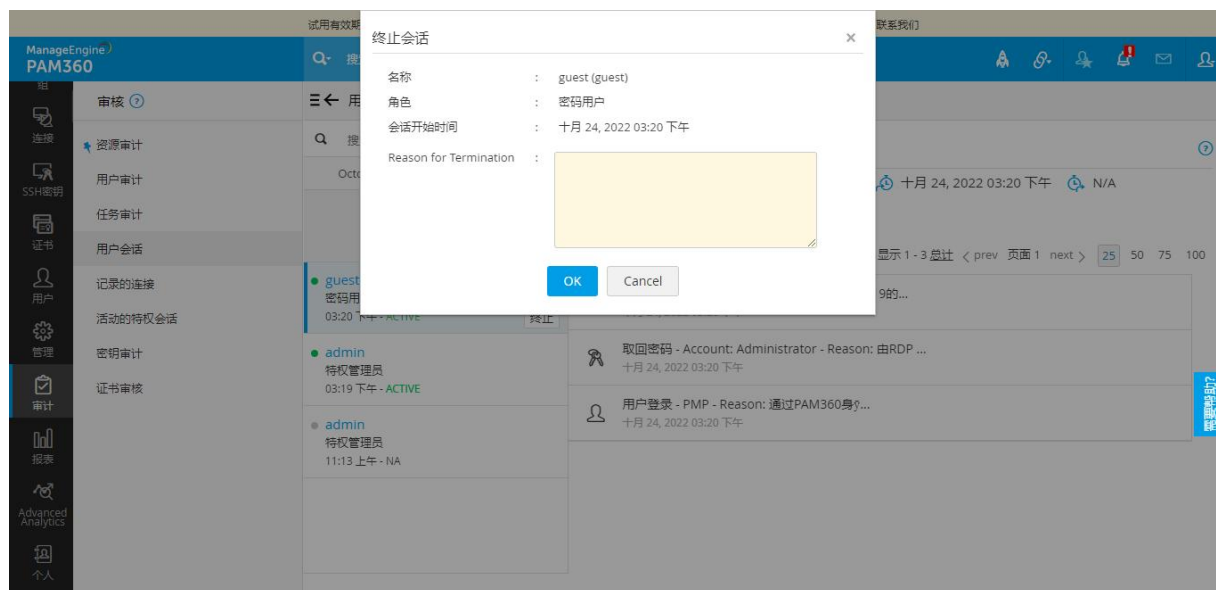
## 会话管理和监控

### 实时监控关键会话

PAM360 提供影子会话，可用于对特权会话建立双重控制。使用此功能实时监控远程会话并监督用户活动。

双重控制有助于提供远程协助和阻止恶意活动。如果您是管理员，您可以通过加入活动会话，以实时观察从 PAM360 启动的关键会话，而不影响最终用户。您可以通过导航到 **审计 > 活动的特权会话 > 加入** 来加入活动会话。这种会话协作对于故障排查特别有用，因为所有的会话中都能够看到相同的操作，如果检测到任何可疑活动，您可以立即终止会话以避免滥用特权访问。这可以通过导航到 **审计 > 活动的特权会话**，并点击所需会话旁边的 **结束** 来完成。





### 终止可疑用户会话

## 记录每个特权会话

默认情况下，PAM360 记录从应用程序启动的所有 RDP、VNC、SSH 和 SQL 会话。我们建议您为所有特权会话配置会话记录，并通过导航到资源选项卡并单击**资源 > 资源操作 > 配置 > 会话记录**自定义外部存储位置。所有记录的会话将显示在**审计 > 记录的连接**下。您可以使用各种详细信息来跟踪会话，例如连接名称、启动会话的用户或启动会话的时间。

### 会话记录 ✕

记录RDP会话       记录SSH/Telnet及SQL命令会话

记录VNC会话       在会话标签显示会话录制状态

**存储记录会话的外部位置**

存储记录会话的目录 : C:\Program Files\ManageEngine\PAM360\recorded\_files

存储记录会话的备份目录 : 没有设置

选择日期格式 : 十月 20, 2022 03:40 下午 ▼

**清除记录的会话**

清除  天以前 ⓘ

**欢迎消息**

在会话开始时显示欢迎消息

剩余字符 : 4000

为 RDP、VNC、SSH 和 SQL 连接配置会话记录

## 定期清除记录的会话

默认情况下，PAM360 记录从应用程序启动的所有 RDP、VNC、SSH、Telnet 和 SQL 会话。如果您的企业机构很大，并且启用会话记录的资源也非常多，那么记录的会话自然会以更快的速度增长。如果您仅需保留特定天数的记录，我们建议您删除多余的记录，以保留足够可用的磁盘空间，此外，您还可以将其移动到其位置。另一方面，如果您想删除选择性会话或特定会话的聊天历史记录，您可以导航到 **审计 > 记录的会议**，然后单击所选会话旁边的“删除”图标。请注意，PAM360 要求至少要有两名管理员批准才能删除特定会话记录或聊天会话。

## SSL/TLS 证书管理

### 发现和导入

PAM360 使您能够自动发现并导入映射到 AD 中用户帐户的证书、Microsoft 证书存储库中的证书以及本地

证书颁发机构颁发的证书。此外，您还可以创建 SSL 证书发现计划，以实现定期发现证书并在 PAM360 中进行添加。

## 证书申请和获取

PAM360 为创建自签名证书提供了便利，但我们强烈建议您只在您的内部网络中严格部署这些证书，因为您对所有资源建立的信任有把握。由于推荐的签名算法是 SHA-2，我们建议您使用 PAM360 隔离所有 SHA-1 证书并将其替换为 SHA-2。

对于面向公众的网站，您应该始终从受信任的第三方证书颁发机构获取 SSL 证书。当您从受信任的 CA 获得证书后，我们强烈建议您将其添加到 PAM360 对其进行管理。我们建议您将各种证书组织到不同的组下，以便进行批量操作。

## 证书部署

始终确保部署的证书是有效的。在使用 PAM360 管理同一证书的两个或多个版本的情况下，必须随时检查是否将正确版本的证书部署到其终端服务器上。最佳做法是在终端服务器上始终部署最新版本的证书。在同一证书需要部署到多台终端服务器的情况下，您还可以利用批量部署。

## 与证书颁发机构集成

PAM360 促进了公共证书颁发机构颁发的证书的端到端生命周期管理。此功能通过与第三方证书颁发机构的无缝 API 集成提供支持，并允许管理员直接从 PAM360 的 Web 界面以集中方式管理证书的生命周期，包括请求、获取、合并、部署、更新等。您可以使用内置的 CSR 生成工具向公共证书颁发机构提出证书请求。以下是向 CA 请求证书时推荐的一些最佳实践：

- 如果私钥被泄露，请立即撤销证书，并使用新的私钥提出新的请求。
- 每次更新证书时生成一个新的私钥。
- 配置代理映射，通过自动域验证实现证书的及时更新。

## 充分利用与 Service Desk Plus 的 CMDB 的集成

PAM360 提供与 ManageEngine Service Desk Plus 的配置管理数据库 (CMDB) 集成的选项。您可以利用此集成, 将 SSL 证书详细信息从 PAM360 的存储库导出到 Service Desk Plus 的 CMDB, 从而允许管理员直接从 Service Desk Plus 界面监控整个组织的 SSL 证书的使用、到期和其他方面。

## SSL 漏洞扫描

PAM360 可扫描其存储库中的 SSL 证书以确定是否存在任何漏洞, 如 HEARTBLEED 或 POODLE, 然后是 CRL 和 OCSP 吊销状态。当上述一项或多项漏洞检查得到了确定了结果时, PAM360 会将特定证书标记为易受攻击。通过这种方式, 用户可以随时了解不安全的证书/服务器配置。然后, 用户可以采取必要的补救措施来替换或更改 SSL 证书或服务器配置。此外, 建议对整个企业网络的所有终端禁用SSL 3.0协议, 以防止任何强制回退到SSL 3.0的动作, 避免使您的通信受到安全漏洞 (如POODLE) 的影响。

您还可以在 PAM360 中为您的 SSL 证书配置自动定期漏洞检查计划, 并在计划完成时通过电子邮件通知管理员。

SSL漏洞

计划任务  启用  禁用

重复类型  天  每周

运行计划每过 01 天

包括SAN  只有部署的服务器  电子邮件报表

SSLv3 协议  启用  禁用

保存 取消

- 启用计划任务将定期运行SSL证书的漏洞扫描。
- 如果启用/禁用SSLv3, 则必须重新启动PAM360服务器才能使更改生效。
- 启用SSLv3协议可在PAM360服务器中启用SSLv3, RC4, MD5withRSA。

### 安排SSL 漏洞扫描

## 审计和报告

### 有助于定期内部审计

使用 PAM360 的审计跟踪能够即时记录与特权帐户操作、用户登录尝试、计划任务和已完成任务的所有事件的操作信息。通过将此信息转换为呈现良好的报告, 您可以用此以促进企业内部定期的审计和取证调查,

轻松发现谁使用密码、何时何地做了什么。

## 通过即时警报密切关注特定活动的情况

PAM360 还允许您在某些事件发生时向选定的收件人发送即时电子邮件通知。此选项非常有用，您可以随时了解您的用户正在做什么。所以我们建议您为重要的操作配置警报，如新用户添加、密码删除、密码共享等。操作层面的电子邮件警报可以通过进入 **审计 > 资源审计 > 审核动作 > 配置资源审核** 来启用。密码级别的警报可以通过 **组 > 动作 > 配置通知** 启用。

操作	<input type="checkbox"/> 审计	<input type="checkbox"/> 发送邮件*	<input type="checkbox"/> 生成SYSLOG	<input type="checkbox"/> 生成SNMP陷阱	<input type="checkbox"/> 清除审计
账户操作	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
InsightVM帐户关联已创建	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
InsightVM帐户关联已删除	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
从回收站中删除帐户	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

邮件服务器设置 | SNMP陷阱

\* 当发生选择的事件时发送通知  
 \* 以每天摘要的方式报告选择的事件

\* 通知  
 所有管理员  所有审计员  用户  用户组  (说明: 使用英文逗号(,)分隔邮件地址)

选择日期格式: 十月 24, 2022 03:33 下午

清理资源审计记录

清理超过  天的审计记录。(输入0或保留为空表示禁止清理记录)

### 配置资源审计

## 选择每日摘要邮件，以避免收件箱混乱

如果您为多个资源启用了警报和更新，您的收件箱可能会充斥着各种各样的电子邮件。在这种情况下，如果您想避免收到如此大量的邮件，您可以选择在每天结束时，仅收取一个具有综合性通知的每日摘要电子邮件。

## 配置电子邮件模板

默认情况下，PAM360 具有电子邮件通知的特定内容。我们建议您根据自己的需要配置模板并定制内容。这可以通过转到 **管理 > 自定义 > 邮件模板** 来完成。

## 在管理系统内生成Syslog和SNMP 陷阱

如果您在组织中使用第三方 SIEM 工具，则可以将 PAM360 与该工具集成。此集成允许您在 PAM360 中发生活动时向该工具提供syslog消息。这将帮助您从一个中心位置全面了解特权访问以及整体网络活动。

## 计划定期报告生成

PAM360 提供各种默认报告，提供有关密码清单、到期状态、用户访问频率、用户活动等的信息。我们建议您对所需报告使用计划报表功能，而不是手动生成这些报告，以节省时间。一旦计划设定，报告将在指定的时间间隔内自动生成，并发送至指定邮箱。

## 清除审计记录

自然情况下，当每个操作都被审计时，审计记录会以高速增长。如果您不需要超过指定天数的审计记录，您可以进行清除。这可以通过导航到**审计 > 用户审计 > 审核动作 > 配置用户审核**来配置。默认情况下，清除选项将被禁用，天数设置为零 (0)。

## 与其他产品和先进技术的集成

### 高级分析

PAM360 与数据分析工具集成，帮助您管理和自动分析特权活动。通过高级分析，您可以

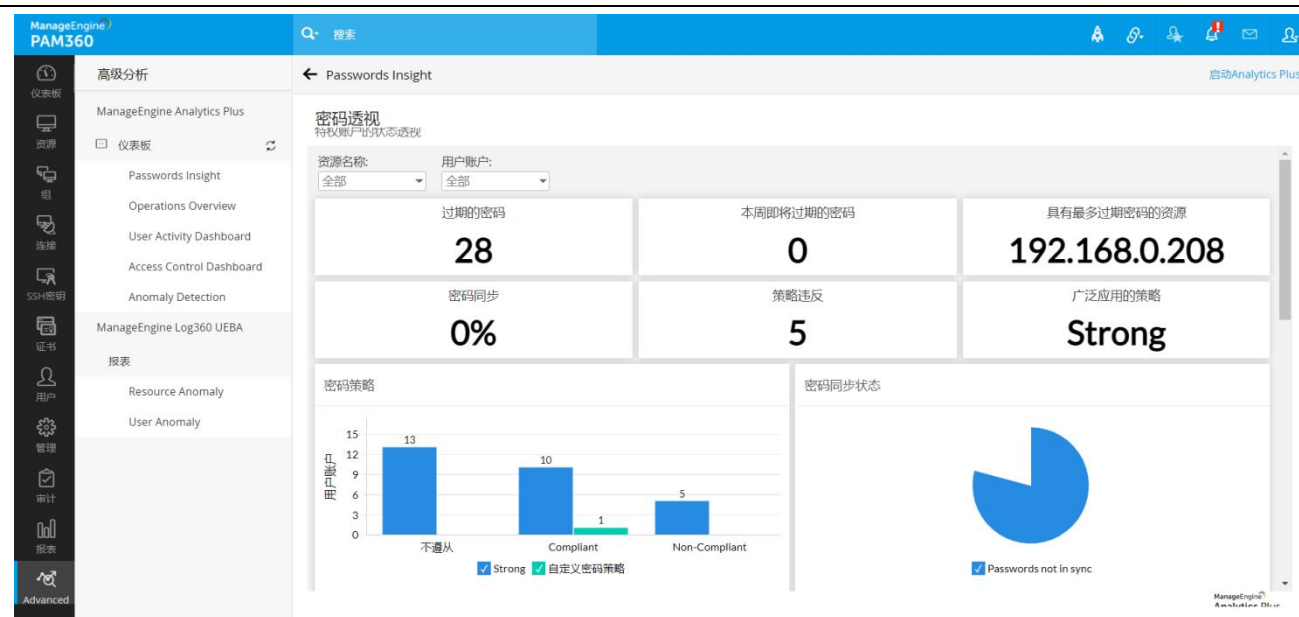
- 发现异常的用户行为，并获得洞察力以识别安全威胁。
- 智能监控恶意账户活动的历史审计日志。
- 通过Zia（由机器学习驱动的分析助手）来识别异常的来源。
- 混合来自多个来源和 PAM360 模块的数据，以获得统一的洞察力以提高可见性。
- 当预先配置的阈值被突破时，您可以通过统一控制台全面分析所有特权账户的活动。
- 通过安全的共享选项，用电子邮件发送、导出、发布和分享关键的发现。

PAM360 与 ManageEngine Analytics Plus 和 ManageEngine Log360 UEBA 集成，让您可以通过统一控制台全面分析所有特权帐户的活动。

**Analytics Plus 集成：**高级分析选项卡根据从 PAM360 导入到 Analytics Plus 的数据，显示不同类型的仪表板。

- **用户活动仪表板：**为您提供与PAM360环境中的用户活动中所有相关的数据，如在特定时间段内访问过特定资源/账户的用户数量、最活跃的用户、在选定时间段内增加的用户数量，以及拥有最高级别访问权限的用户。
- **操作一览：**提供资源和密码相关操作的详细概述，例如存在的资源和帐户数量、最活跃的用户、最活跃的资源 and 密码访问百分比。
- **访问控制仪表板：**提供与访问相关的信息，如访问最多帐户的用户、广泛共享的帐户名称、密码请求总数以及在选定时间段内撤销的请求数。
- **异常检测：**为您提供有关在选定时间段内可能发生的任何异常活动的详细信息，例如在非工作时间执行的操作数量、最频繁的非工作时间操作、在非工作时间执行的用户会话数，在非工作时间被广泛访问的帐户名称，身份验证失败次数最多的用户，以及执行未经授权访问次数最多的用户。

**Log360 UEBA 集成：**Log360 UEBA 从 PAM360 中分离出资源和用户审计跟踪，并根据检测到用户活动的时间和检测到用户活动的次数来生成用户行为模式。通过基于分数的风险评估，Log360 UEBA 将任何偏离正常模式的活动标记为异常。您还可以以柱状图和饼状图的形式可视化异常报告，安排其生成时间，并以 CSV、PDF、XLS 和 HTML 格式导出报告。



高级分析仪表盘

## 域帐户的即时权限提升

除了为本地 Windows 帐户启用即时权限提升之外，您还可以通过与 ManageEngine ADManager Plus 集成来提升或委派 AD 安全组中域用户的权限。通过此集成，我们建议您对 PAM360 用户实施严格的访问控制，以控制对域帐户的访问，以及在其需要时提供即时的权限提升。您还可以通过此集成直接从 PAM360 界面添加和删除 AD 安全组中的帐户。

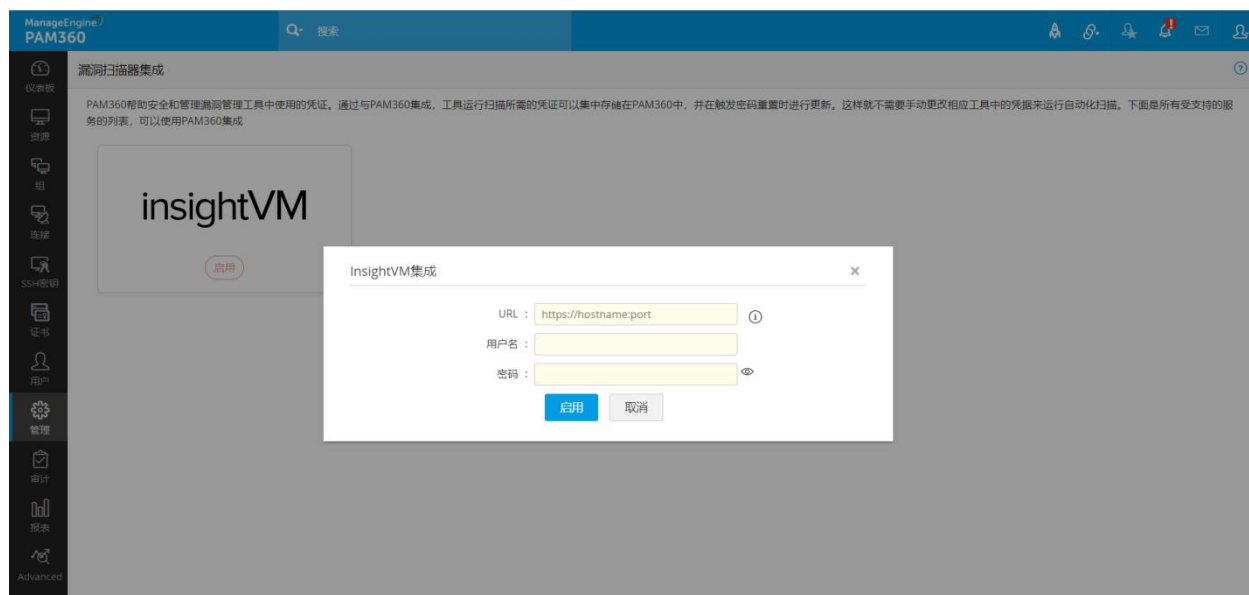


配置即时特权访问控制



## 漏洞扫描器

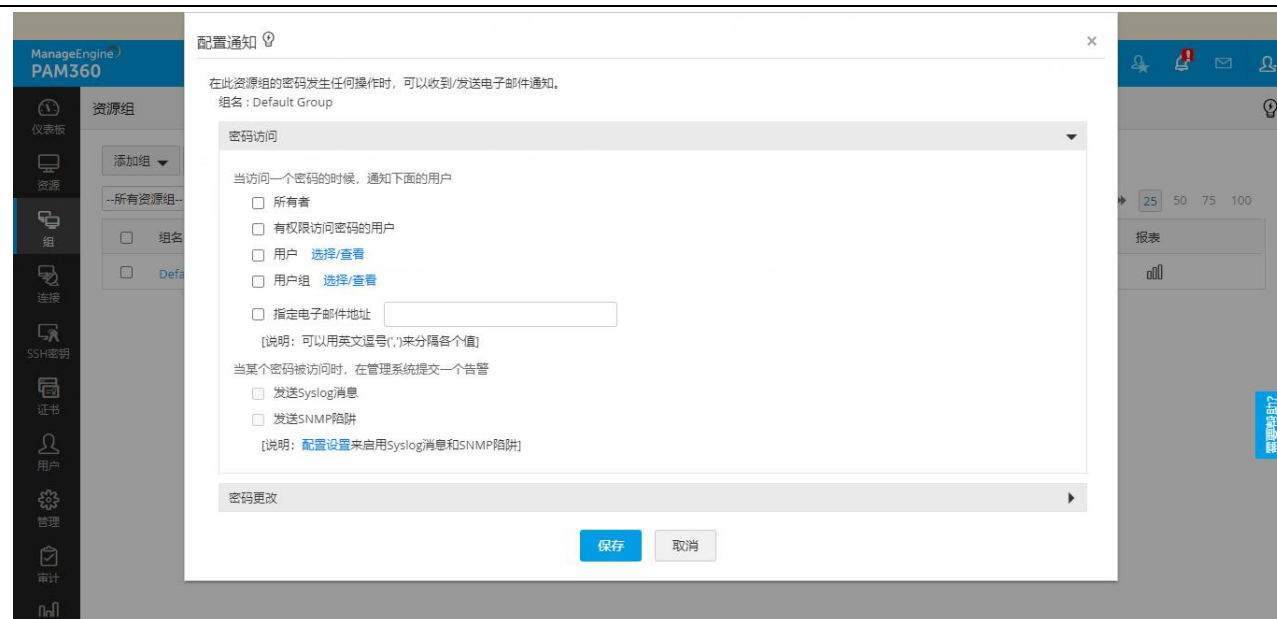
PAM360 与 Rapid7 InsightVM 集成，后者是一种漏洞管理工具，可自动扫描和收集来自网络中所有可用终端的数据，并识别可能构成安全风险的终端。您可以直接从 PAM360 界面利用 PAM360-InsightVM 集成来保护和集中管理运行漏洞扫描所需的共享凭证。



将 InsightVM 与 PAM360 集成

## 与 SIEM 工具集成

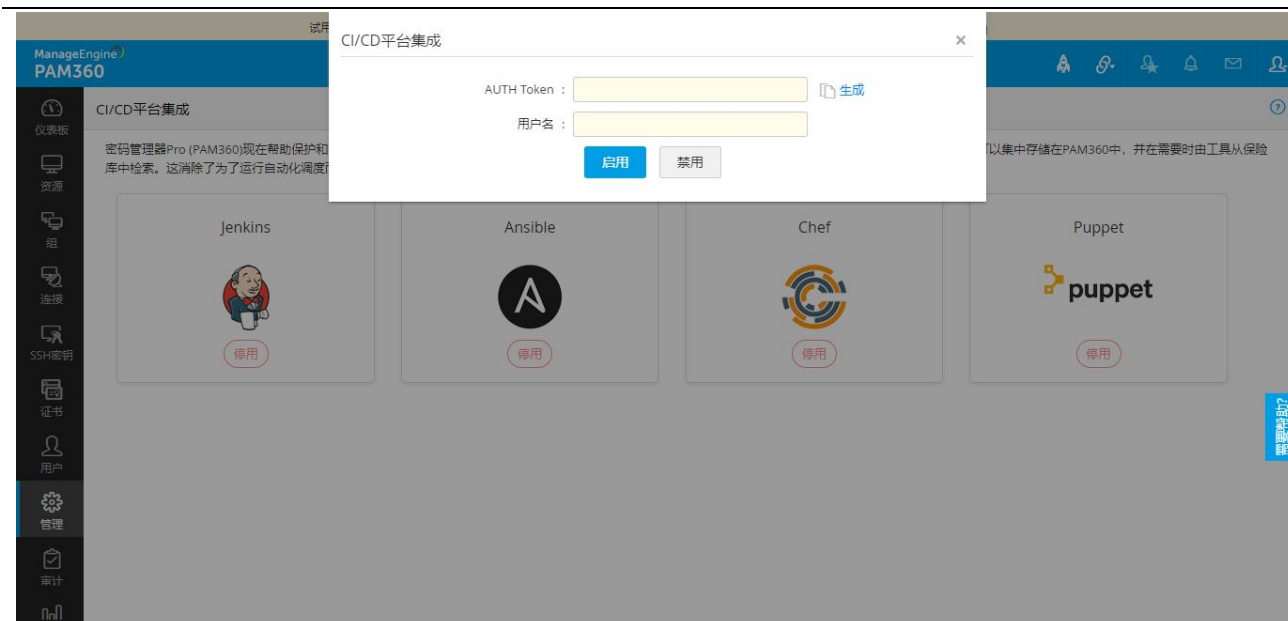
PAM360 与各种 SIEM 工具集成，这些工具有助于从 PAM360 实时收集和處理资源、密码和用户的审计日志，并将它们作为 syslog 消息发送到外部日志管理系统。PAM360 与 Splunk、ManageEngine、EventLog Analyzer、Sumo Logic 和其他系统日志收集器集成。SIEM 的集成将帮助您从一个控制台获得对特权访问和整个网络活动的更深的可见性。



在 PAM360 中自定义 syslog 事件通知

## CI/CD 平台的插件

执行自动化管道以运行例行任务通常需要敏感信息，例如特权密码、API 密钥和访问令牌，以便与环境中的其他系统、应用程序和服务进行通信。在大多数 DevOps 环境中，此类凭证以明文形式存储在脚本文件中，以便顺利执行任务，但这可能导致许多安全问题。为了降低此类风险，PAM360 通过提供与各种 CI/CD 工具（如 Jenkins、Ansible、Chef 和 Puppet）的集成功能，帮助消除 DevOps 管道中的嵌入式凭证，该集成确保每次执行任务时，都能从 PAM360 的保险库中安全地检索所需的凭证，而不是以明文形式存储在脚本文件中。



在 PAM360 中启用 Jenkins 集成

## 机器人过程自动化 (RPA)

PAM360的机器人可以自动完成从存储库中获取密码以连接到机器、应用程序或数据库的过程，从而消除了手动检索密码以执行不同任务的需要。您可以将 PAM360 机器人与企业中的其他 RPA 机器人（如 Automation Anywhere）结合起来，以创建完整的终端管理工作流程。例如，如果您的企业需要通过机器人自动进行安全的远程登录设置，您可以配置PAM360的机器人从保险库中获取密码，并将其与另一个启动远程连接的机器人相结合。

## 自助密码管理和 SSO 功能

PAM360与ManageEngine ADSelfService Plus (ADSSP)集成，可协助域用户执行诸如自助密码重置、自助账户解锁等活动。通过PAM360-ADSSP集成，ADSSP的特权域账户详细信息将与PAM360中的域账户信息进行映射。这可确保 PAM360 中特权域帐户的密码自动与 ADSSP 中的密码保持同步，从而无需手动更新密码并减少服务台呼叫。

## 数据冗余和恢复

### 设置灾难恢复

存储在 PAM360 数据库中的数据至关重要。万一生产环境出现故障，所有数据都可能丢失。所以，灾难恢

复是必不可少的。该应用程序提供了实时数据备份和通过计划任务自动定期备份的功能。选择最适合您企业的方法。此外，请您确保备份文件处于安全的位置。

## 部署具有高可用性架构的备服务器

PAM360 中的高可用性架构是一种推荐设置，可帮助您解决主服务器停机时能确保继续访问密码。这可以通过在主服务器之外的备服务器上安装另一个PAM360实例来实现。如果您的 workplaces 内有不同的网络（例如，每个楼层有不同的网络），我们建议您将主服务器和备服务器安装在不同的网络中。

另一方面，如果您在两个不同的地理位置设有办事处，则高可用性设置的最佳实践是在您的总部配置 PAM360 的主服务器，并在另一个办公室部署备服务器。这样，两个地点的员工都可以在服务器停机时不间断地访问密码。要设置高可用性，请转到 **管理 > 全局设置 > 高可用性**，并为 PAM360 配置备服务器。

**监控高可用性：**对端点和相关数据库操作的持续监控可确保及早发现问题。对于数据库服务器，必须有一个可靠的监控系统，以对服务器可用性进行测量，检测可能导致数据库服务器瘫痪的事件，并向有关方面提供关于关键故障的即时通知。PAM360 具有内置的高可用性管理和监控功能以及各种通知选项。设置高可用性后，您可以从 PAM360 控制台开始监控 PostgreSQL HA 设置，方法是导航到 **管理 > 配置 > 高可用性**。高可用性控制台监控您的主服务器和备服务器以及相关数据库的可用性。



监控高可用性

## 使用 MS SQL 服务器扩展应用程序

对于像 PAM360 这样的特权访问安全解决方案，必须使其具有高可用性和可扩展性，以便即使复杂性增加，应用程序也可以呈现最大的整体性能，而不会对每个节点的平均服务水平产生任何重大影响。强烈建议利用 PAM360 中的应用扩展模型，以确保对特权资源和密码的不间断访问。该模型包含一个 PAM360 主节点和几个子节点，所有节点都连接到一个 MS SQL 数据库集群上。[点击这里](#) 了解如何在 PAM360 中配置主节点和子节点。

## 故障转移服务

PAM360 中的故障转移服务还旨在确保不间断地访问密码和其他特权访问。虽然高可用性功能需要将两个独立的数据库实例分别映射到 PAM360 的主服务器和备服务器上，但故障转移服务是通过冗余的 PAM360 服务器实例来实现的，这些实例可以访问一个共同的 MS SQL 集群，而该集群又有多个 PAM360 数据库实例与之绑定。[单击此处](#) 了解有关故障转移服务的更多信息。

## 维护

### 保持版本更新

PAM360 的团队不断发布包含功能增强和补丁修复的升级包。理想情况下，主要升级每季度发布一次，而次要升级版本可能每两个月发布一次。这些升级包还将包含内置在产品中的 Tomcat Web 服务器、PostgreSQL 数据库以及 JRE 的更新。为了使您的 PAM360 产品得到适当的维护以获得最佳性能，我们建议您在 PAM360 的升级包发布时下载并安装它们。升级包可以在 [这里](#) 下载。

### 明智地选择您的维护窗口

升级 PAM360 时需停止其服务。如果配置了高可用性，主服务器和备服务器都将关闭。此外，目前 PAM360 的设计需要在每次升级后重新配置高可用性。因此，我们强烈建议您在计划维护时间段、或周末、或非工作时间执行维护计划。

如果您无法避免在工作时间进行升级，您可以在即将进行的维护操作之前通过 PAM360 的 **留言板** 提醒您的用户。**留言板** 选项可以在 **管理 > 管理 > 留言板** 下找到。您可以将键入的消息作为电子邮件或在线提醒发送给所有用户。

### 定期更新您的移动应用程序和浏览器扩展程序

PAM360 的本地移动应用程序和浏览器插件的更新会定期发布。我们建议您定期检查应用商店和浏览器商店中的更新。

## 寻找安全建议

如果在产品中发现任何安全漏洞，产品将以升级包的形式提供漏洞修复程序。安全咨询也会发送到您在我们这里注册的客户电子邮件中。请密切关注该电子邮件，以确保您不会错过我们的任何建议。每当您收到一封邮件时，请按照电子邮件中的建议行事。

## 将 PAM360 迁移到另一台机器

要将 PAM360 迁移到另一台机器，请按照以下详细步骤操作：

- 如果 PAM360 正在运行，请将其停止。
- 只需将整个 PAM360 安装文件夹从一台机器复制到另一台机器。
- 然后，将其安装为以服务方式运行。在这个选项中，您将无法通过Windows卸载程序，也无法在程序控制台中添加或删除程序。如果您想随时重新安装，只需删除整个安装文件夹即可。

**警告：**在确保新安装工作正常之前，不要删除现有的 PAM360 安装。这可确保您设置有效的备份，以防您在移动过程中需要克服灾难或数据损坏。

## 紧急访问功能

### 使用本地 PAM360 帐户进行紧急访问

在特殊情况下，如果您的活动目录服务器发生故障，用户可能会被锁定。为了应对这种情况，我们建议您在 PAM360 中保留一个本地帐户。

### 将密码导出为加密的 HTML 文件以供离线访问

通常，在数据中心等受控环境中，不允许连接其他设备。为了能够在这些地方访问所需密码，PAM360 提供了离线访问功能。此功能允许您根据需要定期将所有密码导出至加密的 HTML 文件，并将文件存储在安

全位置。该文件将用您所设置的密码短语进行加密。只有知道此密码短语的用户才能解锁此文件。您还可以设定一个时间间隔（例如15分钟）来配置文件的自动注销。可以通过导航到 **管理 > 设置 > 导出密码-离线访问** 来配置这些设置。除了按需导出之外，您还可以通过导航到**组**并从 **动作**下的下拉菜单中选择 **定期密码导出**来安排资源组密码的导出操作。您可以在每天、每周或每月的基础上安排导出。

## 当管理员离职时

您的管理员可能会离开企业机构。如果发生这种情况，请确保执行以下操作：

### 编写离职报告

当管理员离职时，您需要首先确定他们在公司中的权限级别并评估相关的漏洞。这种做法很关键，因为他们拥有对您IT资产不受限制的访问。在这种情况下，我们建议您在 PAM360 中生成自定义报告，其中包含特定用户有权访问的密码的完整列表。要生成特定用户的自定义报告，请导航到 **用户**，选择特定用户，然后点击在 **报表** 列下的**用户报表**图标。

### 转移资源所有权

在获得离职管理员创建的资源列表后，将所有这些资源的所有权转移给您自己或PAM360中的另一个管理员。在执行此操作之前，您无法删除应用程序中的管理员帐户。转移资源的所有权可以通过导航到 **用户**，选择离职的管理员，然后从 **用户动作**下的下拉菜单中选择 **转让所有权** 来完成。

### 转移审批者权限

如果您配置了访问控制，则离职管理员可能是某些资源的批准者（即，他们可能已处理 PAM360 中其他用户的密码访问请求）。我们建议您在他们离开时将其批准者权限转移给其他管理员。可以通过单击 **用户** 来转移批准者权限，选择**管理员**，然后从 **用户动作** 下的下拉菜单中单击 **访问控制转移**。

### 立即重置密码

为了排除未来的安全漏洞或未经授权的访问尝试，我们强烈建议您在离职管理员拥有的所有资源的所有权被转移给另一个具有管理级别权限的用户后，立即重置这些资源的密码。

## 安全

## 在所有通信中始终选择 SSL

PAM360 为敏感操作提供 SSL 和非 SSL 模式，包括密码重置和资源添加或导入。为获得明显的安全优势，我们建议您始终选择 SSL 通信。

## 谨慎执行脚本并防止恶意输入

默认情况下，PAM360 的默认配置将会识别有害脚本或代码并阻止其执行。此外，它还禁止运行包含 HTML 标记和属性的脚本。此选项是强烈推荐的最佳实践，因为它增强了安全性。如果您确定运行这些脚本，请暂时禁用此选项，并在完成任务后立即启用它。

## 配置不活动超时

从安全的角度来看，当用户离开他们的工作站无人看管时，允许 Web 界面会话保持活跃是危险的。默认情况下，PAM360 的 Web 会话自动注销将被设置为 30 分钟。为了安全起见，我们建议您将其设置为 15 分钟，甚至更短。要配置不活动超时，请导航到 **管理 > 设置 > 全局设置 > 用户管理**。

## 配置浏览器扩展的自动注销功能

您可以选择浏览器扩展会话应保持活动状态的时间。为了获得最大的安全性，我们建议您在 15-30 分钟后设置自动注销。注销期限可以在浏览器扩展的设置下进行配置。

## 离线访问：禁用密码导出

PAM360 为安全的离线访问提供了多种导出选项，例如纯文本电子表格文件和加密的 HTML 文件。我们始终建议您只允许用户将密码导出为加密的 HTML 文件。如果您允许用户以 CSV 文件形式导出密码信息，请禁止将密码导出为纯文本。这可以通过导航到 **管理 > 设置 > 导出密码-离线访问** 来完成。

## 通过黑名单或白名单 IP 地址限制 API 调用、Web 访问和代理访问

PAM360 允许您为 Web 访问、API 调用、来自本机移动应用程序和浏览器扩展的通信以及从目标机器到 PAM360 服务器的代理通信启用基于 IP 的限制。我们建议您仅限制和配置有限数量的、可访问 PAM360 的客户端系统。要配置基于 IP 的限制，请导航至 **管理 > 配置 > IP 限制 > Web 访问（或）API 访问（或）代理访问**。IP 限制可以设置为各种级别和组合，例如定义的 IP 范围或单个 IP 地址。



## 隐私

### 隐私控制

PAM360提供了隐私增强管理功能，您可以在这里自定义和控制报表中个人数据的展现。您可以通过导航到**管理 > 设置 > 隐私设置 > 隐私控制**来决定是否删除数据。我们建议您在生成报告时屏蔽或删除高度机密的数据。

### 加密导出

为了给整个PAM360的所有导出操作增加一层安全性，我们建议您通过导航到**管理 > 设置 > 隐私设置 > 加密导出**启用导出文件的加密功能。您可以设置一个全局口令，统一用于所有的导出操作，或者允许用户为他们的导出文件定义自己的口令。然后，用户将需要提供密码以查看导出的文件。

ManageEngine  卓豪

PAM360

<https://www.manageengine.cn/privileged-access-management/>

产品购买/市场合作

电话：010-82738868

[china-sales@zohocorp.com](mailto:china-sales@zohocorp.com)

技术支持

电话：400-660-8680

010-82738868

邮箱：[support@manageengine.cn](mailto:support@manageengine.cn)

公司地址：

北京市海淀区后屯路28号KPHZ国际技术转移中心3层