Password Manager Pro

最佳实践指南

密码安全存储库，用于存储和管理共享的敏感信息，

如企业密码、文档和数字标识。

ManageEngine
Password Manager Pro

1. 概述

1.1. 关于 Password Manager Pro

Password Manager Pro 是一个基于 Web 的特权实体管理解决方案，允许 IT 团队管理特权身份 - 密码，SSH 密钥和 SSL 证书 - 以及从单个集中控制台监控对关键信息系统的特权访问。它还有助于证明符合授权特权访问控制的 PCI DSS，NERC CIP 和 SOX 等法规。

1.2. 关于本指南

本指南介绍了在企业网络环境中设置和使用 Password Manager Pro 的最佳实践。 凭借我们帮助世界各地组织成功部署 Password Manager Pro 并简化其特权访问管理实践的经验，本指南为 IT 管理员提供了快速有效的软件设置以及安全的特权账号管理实施方向。 在所有阶段 - 产品安装，配置，部署和维护 - 中都可以采用该最佳实践。下面将主要从三个方面（包括数据安全性，可伸缩性和性能）对其进行说明。

ManageEngine
Password Manager Pro

2. 推荐系统配置

2.1. 最低系统要求

在安装 Password Manager Pro 之前，您需要确定系统配置。 此处是运行 Password Manager Pro 的最低系统要求。

通常，性能和可伸缩性取决于以下因素：

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

基于以上因素，建议大中型企业采用以下系统设置：

中型企业

- 用户数量：100-500 个
- 资源/密码数量：最多 10,000 个
- 双核处理器或以上
- 8 GB RAM
- 40 GB 硬盘空间

大型企业

- 用户数量：超过 500 个

- 资源/密码数量：超过 10,000 个
- 四核处理器或更高
- 16 GB RAM
- 100 GB 硬盘空间

注意：我们建议您在性能强大的高端服务器上安装 Password Manager Pro，以便实现其卓越的性能和安全性。

ManageEngine
Password Manager Pro

3. 安装

3.1. Windows vs Linux

Password Manager Pro 可以安装在 Windows 或 Linux 上，但在 Windows 上安装有以下几点优势：

- ✓ Active Directory（AD）集成：Password Manager Pro 的 Windows 安装可以直接与 Active Directory 集成以导入用户和组。此外，使用域账号凭据登录 Windows 系统的用户可以使用单点登录（NTLM-SSO）自动登录到 Password Manager Pro。使用 Linux 安装时，您必须依赖基于 LDAP 的身份验证进行 Active Directory 服务。
- ✓ Windows 资源的密码重置：只要有直接连接，Windows 安装的 Password Manager Pro 就可以在所有支持的目标系统的无代理模式下执行密码重置。Linux 安装需要在所有 Windows 资源和域控制器上部署代理，以重置 Windows 域账号，服务账号和本地账号的密码。

除此之外，仅 Windows 安装的 Password Manager Pro 支持 Windows 服务账号，计划任务，IIS Web. 配置文件和 IIS 应用程序池账号的密码重置。

3.2. 后端数据库

Password Manager Pro 为 Postgre SQL 数据库和 MS SQL 服务器提供后端支持。默认情况下，该产品与 Postgre SQL 数据库捆绑在一起，非常适合中小型企业。对于大型企业，我们强烈建议您使用 MS SQL 服务器作为后端，以实现更好的可扩展性，性能，群集和灾难恢复。

如果您使用 MS SQL 服务器作为后端，我们建议采用以下做法：

- ✓ Password Manager Pro 只能通过 SSL 与 MS SQL 服务器通信，并具有有效的证书配置。因此，我们建议您为 Password Manager Pro 提供专用的 SQL 实例，以避免与现有数据库发生任何冲突或中断。
- ✓ 使用 MS SQL 服务器作为后端时，会自动为数据库级加密生成唯一键，默认情况下，此键将存储在名为<masterkey 的文件的<PMP HOME / conf>目录中。我们建议您将密钥文件移动到其他位置，以防止未经授权的访问。由于此密钥文件是高可用性配置和灾难恢复期间所必需的，因此其安全性至关重要。丢失密钥将导致 MS SQL 服务器重新配置，甚至数据丢失。
- ✓ 将 MS SQL 服务器配置为后端而不是使用 SQL 本地账号时，请使用 Windows 身份验证。
- ✓ 我们建议您使用相同的域账号运行 Password Manager Pro 服务器和 MS SQL 服务器，以便您可以运行 SQL 服务和 SQL 代理服务。
- ✓ 应启用强制加密选项以允许所有客户端连接到此 SQL 实例。完成此操作后，将加密所有客户端到服务器的通信，并且将拒绝不支持加密的客户端访问。
- ✓ 在运行 MS SQL 服务器的计算机上禁用 TCP / IP 以外的所有协议。
- ✓ 隐藏此 SQL 实例以防止其他工具枚举该实例，并禁止除 Password Manager Pro 的服务账号以外的所有其他用户访问此数据库。
- ✓ 设置防火墙规则以仅允许访问运行 MS SQL 服务器的计算机中的所需端口。

3.3. 保护安装密钥

Password Manager Pro 使用 AES-256 加密来保护密码和其他敏感信息。用于加密的密钥（pmp_key.key）是自动生成的，并且对于每个安装都是唯一的。默认情况下，此密钥将存储在<PMP HOME / conf>目录中，名为<pmp_key.key>的文件中。需要在 manage_key 中配置此密钥的路径。 conf 文件存在于 PMP HOME / conf 目录中。 Password Manager Pro 要求可以访问此文件夹，并具有必要的权限，以便在每次启动时读取 pmp_key.key 文件。成功启动后，它不再需要访问该文件，因此带有该文件的设备可以离线。我们强烈建议您将此密钥移至不同的安全位置，并通过仅向 Password Manager Pro 的服务账号提供读取权限将其锁定。此外，在"manage_key.conf"文件中更新此远程路径，以便产品可以在启动期间读取加密密钥。您还可以通过将此密钥存储在 USB 驱动器或磁盘驱动器中来保护此密钥。最大安全起见，请创建脚本文件以将此密钥复制到可读位置，然后在服务启动时销毁该副本。

3.4. 控制数据库凭证

除 AES 加密外，Password Manager Pro 数据库还通过单独的密码进行保护，该密码是自动生成的，并且对于每个安装都是唯一的。此数据库密码可以安全地存储在 Password Manager Pro 中。但我们建议您将密码存储在产品服务器可访问的其他安全位置。

默认情况下，数据库信息（例如 JDBC URL，登录凭据和其他参数）将存储在名为 database_params.conf 的文件中，该文件存在于<PMP HOME / conf>目录。虽然数据库配置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限制访问，并使其仅可用于 Password Manager Pro 的服务账号。如果将 data-base_params.conf 文件放在 PMP 安装文

件夹之外，则需要在<PMP-Home> \ conf \ wrapper.conf 文件（对于 Windows）或<PMP- Home>中指定位置以及文件名。 conf \"wrapper_lin.conf 文件（适用于 Linux）。请注意，如果未在此处指定整个位置，则无法启动该服务。

- ✓ 此文件的路径在<PMP HOME / conf>目录中的"wrapper.conf"文件中配置。编辑此文件并查找 line wrapper.java.addition- al.9 = -Ddatabaseparams.file。
- ✓ 如果您使用的是 Linux 安装，则必须编辑<PMP HOME / conf>目录中的文件"wrapper_lin.conf"
- ✓ 默认路径将配置为./../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 = \\ remoteserv- er1 \ tapedrive \ sharedfiles \ database_params.conf。
- ✓ 保存文件并重新启动 Password Manager Pro 以使更改生效。

注意：以上步骤仅适用于 PostgreSQL 和 MySQL。如果您使用 MS SQL 服务器作为后端，请参阅 3.2 节。

ManageEngine
Password Manager Pro

4.0 服务器&环境配置

12

4.1. 服务器强化

默认情况下，Password Manager Pro 运行所需的所有组件都存储在安装目录（ManageEngine / PMP）中。 因此，我们强烈建议您强化安装了 Password Manager Pro 的服务器。 为此您应执行以下基本步骤：

- ✓ 使用域组策略禁用组织中所有常规域用户对此服务器的远程访问。 限制所有常规管理员的读取权限，并仅为一个或两个域管理员提供对 Password Manager Pro 驱动器或目录的写入权限。
- ✓ 设置入站和出站防火墙，分别防止传入和传出流量。 使用此设置，您还可以指定必须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）。

4.2. 使用专用服务器账号

在域控制器中为 Password Manager Pro 创建单独的服务账号，并在 Password Manager Pro 的所有区域中使用它。 将使用相同的账号运行 Password Manager Pro。 要开始使用为 Password Manager Pro 创建的服务账号，可以到安装了 Password Manager Pro 的服务器中的服务控制台（“services.msc”），然后到 Password Manager Pro 的属性。 使用创建的服务账号更改已配置的本地系统账号。 此相同的服务账号还可用于从 Active Directory 导入用户和资源。

4.3. 配置 Web 服务器的绑定 IP 地址

默认情况下，Password Manager Pro 的 Web 服务器将绑定到安装该应用程序的服务器的所有可用 IP 地址。 因此，可以使用配置的端口（7272）在任何或所有 IP 地址上访问 Password Manager Pro。 要对此进行限制，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：

1. 如果 Password Manager Manager 正在运行，请将其停止。
2. 打开<PMP_HOME> \ conf 文件夹中的"server.xml"文件。
3. 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" keystore-
File="conf/server.keystore" keystorePass="passtrix" maxHttp-
HeaderSize="32768" maxSpareThreads="75" maxThreads="150"
minSpareThreads="25" port="7272" scheme="https" se-
cure="true" server="PMP" sslProtocol="TLS" truststoreFile="-
jre/lib/security/cacerts" truststorePass="changeit" trust-
storeType="JKS" useBodyEncodingForURI="true"/>
```

4. 在上面的行中，在值 port ="7272"旁边，添加属性 address ="127.0.0.1"。 将 127.0.0.1 替换为要用于绑定的服务器的实际 IP 地址。

4. 4. 通过黑名单或白名单 IP 地址限制 Web 服务器访问

只要有连接，就可以从任何客户端系统访问 Password Manager Pro。 因此，我们建议您限制

和配置部分可访问 Password Manager Pro 的客户端系统。 要配置基于 IP 的限制，可以到**更新>>配置>> IP 限制>> Web 访问**。 可以在各种级别和组合中设置 IP 限制，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，或者通过将其添加到阻止的 IP 地址字段来限制访问。

ManageEngine
Password Manager Pro

5.0 添加用户账号

5.1. 利用 AD / LDAP 集成进行身份验证和配置

将 Password Manager Pro 与 Active Directory 或任何符合 LDAP 的目录集成非常有用，因为它提供了以下好处：

用户配置或取消配置：通过 AD / LDAP 集成，可以快速轻松地在 Password Manager Pro 中添加用户。集成后，您可以直接将目录中的用户配置文件和组或 OU 导入 Password Manager Pro。此外，产品中的用户账号供应变为简单的过程。例如，如果从目录中将现有的"数据库管理员"OU 导入到 Password Manager Pro，则可以轻松地将数据库密码分配给该导入的组。

除此之外，您还可以在将 Password Manager Pro 与目录集成时启用同步，以便任何更改（例如，在目录中的 OU 之间新添加或移动的用户）将自动反映在 Password Manager Pro 中。当您从相应的用户目录中永久删除用户时，将 Password Manager Pro 与您的目录同步也会通知您。 Password Manager Pro 禁用并锁定此类用户账号，通过电子邮件和警报通知通知您，您可以选择删除这些账号或重新激活它们。

Active Directory 身份验证：另一个好处是您可以利用目录的相应身份验证机制，并为您的用户提供单点登录（SSO）选项。激活此选项后，只要用户已使用其目录凭据登录系统，用户将自动通过 Password Manager Pro（使用基于 NTLM 的身份验证）进行身份验证。使用 AD 凭据进行 Password Manager Pro 身份验证可确保登录密码不会本地存储在 Password Manager Pro 中，因为用户将直接从您的目录进行身份验证。

5.2. 禁用本地认证

在将 Password Manager Pro 与 AD / LDAP 兼容目录集成后，我们建议您禁用本地身份验证，并允许用户使用其 AD / LDAP 凭据登录 Password Manager Pro。 要禁用本地身份验证，可以到**管理>>设置>>常规设置>>用户管理。**

但是，如果您已配置本地 Password Manager Pro 账号以进行损坏，则无法禁用本地身份验证。在这种情况下，如果您仍希望仅使用 AD / LDAP 身份验证，我们建议您在同一部分中禁用"忘记密码"选项（用于重置 Password Manager Pro 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只能使用其 AD / LDAP 凭据登录 Password Manager Pro，即使启用了本地身份验证也是如此。

5.3. 使用双因素认证

用户身份验证的附加保护层可确保只有合适的人才能访问您的敏感资源。 Password Manager Pro 提供了多个选项，用于在提供对产品 Web 界面的访问之前配置第二级身份验证。 第二个因素选项包括：PhoneFactor，RSA SecurID 令牌，Duo Security，Google 身份验证器，通过电子邮件发送的唯一密码，任何符合 RADIUS 标准的双因素身份验证，Microsoft 身份验证器，Okta 验证和 YubiKey。 强烈建议为用户配置双因素身份验证。

5.4. 基于工作职责分配用户角色

添加用户后，为用户分配适当的角色。 Password Manager Pro 有四个预定义的用户角色：管理员，密码管理员，密码审计员和密码用户。 要了解有关每个角色特权的更多信息，请参阅我们的帮助文档。

除密码管理外，管理员角色应仅限于少数需要执行用户管理操作和产品级配置的人员。

使用超级管理员角色：Password Manager Pro 中的超级管理员可以访问所有存储的密码。 理想情况下，此角色不是必需的。 但是，如果您希望有一个专用账号用于紧急情况，您可以为您的组织创建一个超级管理员。 出于安全原因，此角色应始终仅限于组织中的高层管理人员。 此外，在这种情况下，最佳实践方法是只创建一个超级管理员。 管理员升级为超级管理员后，可以根据需要阻止将来创建更多超级管理员。 超级管理员可以到**管理>>身份验证>>超级管理员**启用**管理员拒绝创建超级管理员**来完成。

更多信息，请参阅此文档。

5.5. 创建用户组

将用户组织到组中 —— 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非常有用。 如果已将 Password Manager Pro 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。

5.6. 移除默认管理员账号

安全起见，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 Password Manager Pro 中的默认管理员和用户账号。

5.7. 限制移动访问和浏览器扩展访问

默认情况下，所有用户都可以访问 Password Manager Pro 的本机移动应用程序和浏览器扩展。如果您希望用户无法访问工作站以外的任何设备上的任何密码，请在整个组织内禁用全局移动应用程序访问权限。 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。 可以到**用户>>更多操作**并从下拉菜单中选择**限制移动访问/限制浏览器扩展**来强制执行这些限制。

ManageEngine
Password Manager Pro

6.0 数据统计和管理

6.1. 添加资源：选择一个便捷的方式

在 Password Manager Pro 中开始使用密码管理的第一步是添加资源。 最快捷，最方便的方法是自动发现特权账号。另一种方式是手动添加和 CSV 导入。 如果在切换到 Password Manager Pro 之前使用其他工具或将凭据存储在电子表格中，请使用 CSV / TSV 导入功能。

6.2. 明确资源类型

手动或通过 CSV 导入添加资源时，请检查是否已在资源类型下正确排序所有资源，这对于使用密码重置等功能是必要的操作，因为 Password Manager Pro 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，否则资源将在"未知"下排序，在这种情况下，密码重置将失败。 Password Manager Pro 提供了 32 种默认资源类型，列在**管理>>资源类型**下。

6.3. 移除未授权特权账号

当您使用自动发现功能清点网络上的 IT 资源及其各自的特权账号时，默认情况下，Password Manager Pro 将获取与网络上检测到的资源关联的每个账号。 某些账号可能是未经授权的，不需要的或孤立的。 就比如当您添加 Windows 资源时会获取所有用户账号。从安全角度来说，应识别和删除未经授权的账号，以避免将来出现无法预料的漏洞。 密码管理最佳实践要求特权账号的数量应保持在最低限度。 此外，转储不需要的账号也会使数据库混乱，使数据组织成为一项艰巨的任务。 因此，我们建议您在 Password Manager Pro 中运行自动发现之前删除目标计算机本身中的这些不需要的账号。

6.4. 资源发现后随机化密码

完成资源发现和帐户枚举后，我们强烈建议您随机化所有帐户的密码。这种做法很重要，因为在部署 Password Manager Pro 之前，您的员工可能已将其密码存储在不同的媒体（如电子表格和文本文件）中，或者甚至可能将其复制到纸上。如果密码未更改，则这些员工仍可以在 Password Manager Pro 之外直接访问资源。因此，密码必须在资源发现后适当随机化，以阻止对资源的所有直接，未经授权的访问。此外，随机化还可以消除弱密码并为资源分配强大，唯一的密码。已发现帐户的密码随机化可以到**资源>>选择特定资源>>资源操作**（在顶部）>>**配置远程密码重置**。

注意：将来，如果您想在发现新帐户时预设密码随机化，可以到**资源>>选择特定资源>>资源操作**（在顶部）>>**发现帐户**中配置相同的密码随机化，然后在打开的新窗口中启用在发现后随机化密码。

6.5. 利用资源组

资源组在 Password Manager Pro 中非常强大。 大多数高级密码管理操作（例如自动密码委派和预定密码轮换）只能在资源组级别执行。 在两种类型的资源组创建中，强烈建议使用"基于标准"的组。

基于标准的组基本上是动态组。 它们使您可以灵活地将满足特定条件的资源整合到一个组中。定义条件后，Password Manager Pro 将自动识别所有匹配的资源并创建组，无需人工干预。

6.6. 使用嵌套资源组，根据部门组织资源

为了便于从大型数据库中检索单个资源，您可以利用 Password Manager Pro 中的资源管理器树视图设置（即创建嵌套资源组）。默认情况下，每个用户显示的树是不同的。启用此树视图设置以在整个组织中全局显示统一资源管理器树。启用后，将主节点的名称从“资源组”更改为组织的名称。之后，根据您的不同团队或部门创建多个子节点。随后，您可以在其所属的团队或部门的子节点下指定资源组。

通过上述的资源管理器树操作后，您可以创建一个清晰的资源组层次结构，以提供方便的可访问性。要允许操作资源管理器树，可以到**管理>>常规设置>>密码检索**启用**允许所有管理员用户操作整个资源管理器树**。

6.7. 其他参考和搜索的字段

添加资源时，可以使用其他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，搜索特定资源或密码，共享资源等。 例如，假设您的组织中有三个级别的 IT 管理员。那么，如果您创建标题为“访问级别”的其他资源字段，便可轻松地在“级别 I / II / III”下对资源进行排序。 使用“访问级别”字段作为标准，您可以创建三个不同的资源组。 同样，您可以创建三个用户组，每个用户组包含属于不同级别的用户，然后将“一级”资源分配给“一级”用户，依此类推。

ManageEngine
Password Manager Pro

7.0 密码共享和细粒度限制

7.1. 使用不同的访问权限共享密码

共享资源时，密码所有者可以通过选择以下特权之一为用户和组授予不同的权限级别：

- ✓ **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。
- ✓ **完全访问权限**：用户可以完全管理资源或组，并可以重新共享资源，组或个人帐户密码。

我们建议您仅向用户提供"查看密码"权限，因为这对于各种与密码相关的操作来说已足够。提供"完全访问"权限时请务必小心，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，删除甚至转发更多用户的密码。

注意：除了这些共享权限之外，您还可以共享资源而不以纯文本形式显示密码。为资源配置自动登录时，可以执行此操作。要了解有关此功能的更多信息，请参阅第 10.1 节。

7.2. 使用资源组进行用户组共享

虽然 Password Manager Pro 具有与单个用户或组共享单个密码或资源的规定，但最佳的实践方法是与用户组共享资源组。这将能最有效地执行批量操作，同时节省时间。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，则可以通过两个简单步骤完成此操作：

1. 创建基于条件的资源组（使用"Windows"资源类型作为匹配条件）。这样，所有现有的 Windows 资源都会添加到组中，将来创建的新资源也会自动添加到组中。
2. 为 Windows 管理员创建用户组。如果已集成 AD / LDAP，则可以直接导入组并启用用户数据库的自动同步。这样，每当新的 Windows 管理员加入组织时，他们的 AD 帐户将自动添加到密码用户组，新用户随后将继承该组的权限以查看 Windows 服务器密码。

7.3. 利用访问控制工作流

Password Manager Pro 中的访问控制是一种请求释放机制，该机制不允许用户直接访问密码，用户必须向管理员提出访问批准请求。 该功能还可以帮助您为资源引入各种访问限制，例如时间限制访问，并发控制以及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据启用此版本控制。

为了更好的安全性，您还可以为关键资源配置双重批准，这要求两个管理员在密码临时释放之前批准请求。 当组织中的两个不同部门同时拥有管理凭据时，此设置非常有用。 可以到**资源>>资源操作>>配置访问控制**来配置访问控制。

7.4. 要求用户提供检索密码的原因

默认情况下，所有与密码相关的操作都可以从 Password Manager Pro 的审计跟踪中获得，并附有时间戳和 IP 地址详细信息。同时， 您也可以要求用户输入他们需要访问密码的原因。 这些原因也将记录在审计跟踪中，可用于法庭调查中的交叉验证和验证。 因此，每当用户尝试

检索资源的密码时，无论是否配置了访问控制，我们都建议您强制要求他们提供访问的可靠理由。 可以到**管理>>设置>>常规设置>>密码检索**下激活此选项。

7.5. 将 Password Manager Pro 与企业工单系统集成

Password Manager Pro 提供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。 为了为您的关键资源密码启用更强大的检索工作流程，我们建议您将 Password Manager Pro 与企业工单系统集成。 目前，Password Manager Pro 可与 ManageEngine ServiceDesk Plus On-Demand，ServiceDesk Plus MSP，ServiceDesk Plus，ServiceNow 和 JIRA 轻松集成。 您可以到**管理>>集成>>工单系统集成**将 Password Manager Pro 与上述工单系统集成。

ManageEngine
Password Manager Pro

8.0 密码策略

8.1. 为关键资源组设置单独的密码策略

密码策略主要可帮助您通过指定字符复杂性来定义密码强度。 Password Manager Pro 允许您为不同的资源组自定义和配置不同的密码策略。 如果您有一些本质上非常敏感的资源，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。 可以到**组>>配置特定组>>批量配置>>关联密码策略**配置资源组的密码策略。

8.2. 账号级密码策略

通常，每个资源都配置有一个或几个管理账号和其他普通账号。 为保护这些特权账号，我们建议您为重要资源的敏感账号单独配置强密码策略。可以到**资源>>配置特定资源>>资源操作**（在顶部）**>>关联密码策略**配置账号级密码策略。

8.3. 创建策略时，定义您的密码期限

配置新密码策略时，请始终记住设置密码最长使用期限。 指定期限可让 Password Manager Pro 在到期时自动重置密码。 如果您没有填写该字段，密码将不会过期，因此我们建议您最好设置一个。

ManageEngine
Password Manager Pro

9.0 密码重置

9.1. 定期密码随机化

特权帐户的安全管理需要使用定期重置的高级别、唯一的密码。 理想情况下，密码应至少每 90 天重置一次——这是 IT 规则（如 PCI-DSS）规定的最常见时间范围。 我们建议您使用计划密码重置功能为 Password Manager Pro 中的资源组配置常规密码重置。 更重要的是，将密码配置为在以下情况下自动重置：

- ✓ 用户成功使用该密码后。
- ✓ 为与最初共享密码的用户撤消共享权限时。
- ✓ 密码过期时，通过密码策略设置。

9.2. 选择最合适的密码重置模式

密码重置可以在 Password Manager Pro 中的以下两种模式之一中执行：无代理或基于代理。

对于无代理模式，Password Manager Pro 直接与目标系统连接并更改密码。必须提供管理凭据才能执行密码更改。更具体地说，就是要从 Windows 安装的 Password Manager Pro 执行 Linux 资源的密码重置，需要两个帐户：一个具有 root 权限，另一个具有可用于远程登录的普通用户权限。

另一方面，当您必须重置没有直接连接的资源的密码（例如 DMZ 位置或具有防火墙限制的密码）时，基于代理的模式会派上用场。要完成这些密码重置，Password Manager Pro 会将代

理部署到执行任务的远程主机。代理与应用程序服务器之间的所有通信都是通过 HTTPS 进行的一种方式，因此您无需为入站流量打开任何防火墙端口。

基本上，在这两种模式中，无代理模式是更方便可靠的密码更改方式，我们建议您在可以直接访问资源时选择相同的方式。但是，以下情况您必须选择基于代理的模式：

- ✓ 当 Password Manager Pro 中的特定资源的管理凭据不可用时。
- ✓ 当目标资源上没有运行 Password Manager Pro 重置所需的服务（适用于 Linux 的 Telnet / SSH，适用于 Windows 的 RPC）时。
- ✓ 当 Password Manager Pro 在 Linux 上运行时，您需要对 Windows 资源进行密码更改。
- ✓ 当您有两个不同的环境"A"和"B"，其间有防火墙。在这种情况下，您可以在一个环境中安装 Password Manager Pro，例如 A，并为环境 A 中的计算机使用无代理模式。另一方面，您可以在环境 B 的计算机中安装代理以进行密码重置。这样，可以在 A 和 B 中管理所有密码，而无需添加防火墙端口另当别论。

9.3. 重启服务，实现完整的管理流程

通过 Password Manager Pro，用于运行各种服务和 IIS 应用程序池的 Windows 域帐户也可以定期进行密码重置，以及后续所有相关服务和应用程序池的密码传播。 为确保通过密码更改正确更新服务，任务和应用程序池，Password Manager Pro 提供了在重置密码后自动重新启动服务的选项，这也是我们提倡的做法。

ManageEngine
Password Manager Pro

10.0 会话管理

34

10.1. 允许用户自动登录远程系统，无需明文显示密码

配置自动登录选项以远程连接资源后，Password Manager Pro 允许用户只需单击即可建立与资源的直接连接，无需复制和粘贴密码。我们建议您阻止用户以明文格式检索密码，因为这种做法没有任何必要。 可以到**管理>>设置>>常规设置>>密码检索**中禁用密码的纯文本检索。

10.2. 实时监控关键会话

Password Manager Pro 提供会话映射功能，可用于在特权会话上建立双重控制。 使用此功能可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并阻止恶意活动。 如果您是管理员，则可以通过加入并同时观察活动会话来跟踪从应用程序启动的关键会话，该过程不会影响用户使用。 如果检测到任何可疑活动，您可以立即终止会话以避免特权访问滥用。

10.3. 定期清除被记录的会话

默认情况下，Password Manager Pro 会记录从应用程序启动的所有 RDP，VNC，SSH，Telnet 和 SQL 会话。 如果组织规模很大，同时启用了大量资源的会话记录功能，则记录的会话会越来越多。 如果您不需要超过指定天数的会话记录，建议您清除会话以保持磁盘空间正常。 您也可以将这些记录存储在本地驱动器中，便于移动到其他位置。 另一方面，如果要删除选择性会话或特定会话的聊天记录，可以到**审计>>已记录的会话**，然后单击所选会话旁边的**删除**图标来执行此操作。

注意：Password Manager Pro 要求至少两位管理员批准删除特定会话记录或聊天会话。

ManageEngine
Password Manager Pro

11.0 第三方特权访问

11.1. 管理第三方对公司系统的访问

很多情况下，承包商，顾问和供应商等第三方需要访问公司 IT 资源，以履行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时，我们始终建议您仅为其提供临时访问权限，并限制时间规定和最低必要权限。最重要的是，在与第三方共享关键信息时，我们建议您遵循如下几点：

- ✓ 由于承包商远程连接到您的资源，因此将所有第三方作为用户添加到 Password Manager Pro 中，并要求他们仅通过 Password Manager Pro 建立与目标系统的直接会话。
- ✓ 配置资源的自动登录后，最佳实践方法是共享登录凭据，而不以纯文本格式显示密码。
- ✓ 另外，为这些资源配置访问控制工作流。这有助于实现访问密码的时间限制，包括在使用期结束时自动重置密码。
- ✓ 定期映射会话来检测任何恶意行为痕迹并立即采取补救措施。
- ✓ 当您与供应商签订合同时，立即对供应商有权访问的所有资源执行密码重置。

ManageEngine
Password Manager Pro

12.0 数据中心移除访问

12.1. 避免循环跳转服务器凭据

通常，连接到远程数据中心资源是一个耗时的过程，因为直接访问受到安全性的限制。 相反，管理员和用户必须在最终连接到目标设备之前跳过一系列跳转服务器，在每个阶段手动验证。这种多跳的过程为每个跳转服务器引入了单独的凭证，用户需要这些凭证来启动数据中心连接。 对于这些情况，在用户之间传递所有凭据并不安全。

但是，当您使用 Password Manager Pro 中的登陆服务器配置功能时，用户仅仅通过 Password Manager Pro 连接到数据中心。 该应用程序提供对数据中心资源的安全，一键式自动访问，无需在每一跳进行手动身份验证。 它还集中管理跳转服务器凭据。

12.2. 提前导出密码，为离线访问做准备

如果数据中心环境不允许 Internet 连接，您将无法从该网络访问 Password Manager Pro。 在这种情况下，请事先将所有必需的密码导出为加密的 HTML 文件，并离线访问密码。 如果启用了导出选项，则可以到**资源>> 资源动作**（在顶部）>> **导出密码**下载该文件。

ManageEngine
Password Manager Pro

13.0 审计和报表

40

13.1. 促进定期内部审计

使用 Password Manager Pro 的审计跟踪可以立即记录特权帐户操作，用户登录尝试，计划任务和已完成任务的所有事件。 通过将此信息转换为一目了然的报表，可以促进定期内部审计和取证调查，轻松了解谁在何时何地使用了密码。

13.2. 通过即时警报为活动贴个小标签

Password Manager Pro 还允许您在发生特定事件时向所选收件人发送即时电子邮件通知。此选项非常便于同步更新用户执行的操作。 因此，我们建议您为重要操作配置警报，例如新用户添加，密码删除，密码共享等。 可以到**审计>>资源审计（例如）>>审计动作>>配置资源审计**启用操作级别的电子邮件警报。 可以到**组>>动作>>配置通知**中启用密码级别警报。

13.3. 选择每日电子邮件摘要

如果为许多资源启用警报和更新，那么收件箱可能会塞满了通知电子邮件。为了 避免发生这种情况，您可以选择在每天结束时使用统一的通知列表接收每日电子邮件摘要（在每小时更新也无济于事的情况下）。

13.4. 配置邮件模板

默认情况下，Password Manager Pro 有自己的邮件通知模板。我们建议您自行配置模板，以

满足您的需求，同时也能自定义专属的内容。可以到**管理>>自定义>>邮件模板**中执行。

13.5. 将 syslog 消息和 SNMP 陷阱集成到管理系统

如果您在组织中使用第三方 SIEM 工具，则可以将 Password Manager Pro 与该工具集成。 此集成允许您在 Password Manager Pro 中进行活动时将 syslog 消息提供给工具。 或者，您也可以将 SNMP 管理器与应用程序集成并生成 SNMP 陷阱。这有助于您从中心位置获取特权访问的整体视图以及整体网络活动。

13.6. 计划定期生成报表

Password Manager Pro 提供各种预制报表，提供有关密码清单，过期状态，用户访问频率，用户活动等信息。 我们建议您使用"计划报表"功能获取所需的报表以节省时间，而不是选择手动生成。 计划报表后，报表将在指定的时间间隔内自动生成并发送到您注册的电子邮件。

13.7. 清楚审计记录

通常情况下，当每个操作都被审计时，审计记录增多的速度会越来越快。 如果您不需要超过指定天数的审计记录，可以清除它们。 请到**审计>>用户审计（例如）>>审计操作>>配置用户审计**来配置。 默认情况下，清除选项是被禁用的，且清除日期为零。

ManageEngine
Password Manager Pro

14.0 数据冗余和恢复

14.1. 设置灾难恢复

存储在 Password Manager Pro 数据库中的数据至关重要。 如果发生生产设置故障，所有数据都可能丢失， 因此灾难恢复至关重要。 该应用程序通过计划任务提供实时数据备份和自动定期备份， 请选择最适合您的方法。

此外，请确保为备份配置的目标目录位于安全的远程位置。

14.2. 部署一个高可用性的备用服务器

我们推荐您设置 Password Manager Pro 中的高可用性体系结构，其可确保停机时密码访问的不间断性。除了主应用程序服务器之外，还可以通过在辅助服务器上安装另一个 Password Manager Pro 实例来实现此目的。如果您的工作场所中有不同的网络（例如，每个楼层都有不同的网络），我们建议您在不同的网络中安装主要和辅助应用服务器。

另一方面，如果在两个不同的地理位置设有办事处，则设置高可用性的最佳做法是在总部配置 Password Manager Pro 主服务器，在另一个办公室部署辅助服务器。这样，两个位置的员工都可以在服务器停机时访问密码。要设置高可用性，请到**管理>>配置>>高可用性**，并为 Password Manager Pro 配置备用服务器。

ManageEngine
Password Manager Pro

15.0 维护

45

15.1. 保持安装更新

Password Manager Pro 团队经常会更新发布一些新增功能和修复的升级包。 理想情况下，主要升级每季度发布一次，而微型升级可能每月或每两个月发布一次。 这些升级包还包含与产品捆绑在一起的 Tomcat Web 服务器，PostGresSQL 数据库和 JRE 的更新。 为了正确维护 Password Manager Pro 的安装，获得最佳性能，我们建议您在 Password Manager Pro 发布时下载并应用升级包。 升级包可以点击此处下载。

在安装 Password Manager Pro 的地方升级 Windows 操作系统：如果要在 Password Manager Pro 服务器中安装 Windows 修补程序，请执行以下步骤：

1. 打开服务控制台（services.msc），同时停止 Password Manager Pro 服务。
2. 获取整个 Password Manager Pro 目录的副本，并将其存储在其他计算机上作为备份。 如果服务器是 VM，只要一个快照即可。
3. 然后，更新 Windows 操作系统。

15.2. 慎重选择维护窗口

要应用升级包，必须暂时停止 Password Manager Pro。 如果配置了高可用性，则主服务器和辅助服务器都将关闭。 此外，Password Manager Pro 的当前设计要求在每次升级后重新配置高可用性。 因此，我们强烈建议您在周末或非工作时间安排维护时段。

如果您无法避免在工作时间内进行升级，则可以在维护之前使用 Password Manager Pro 的留言板提醒用户。 请在**管理>>管理**下找到留言板选项。 您可以将您键入的消息作为电子邮件或在线提醒发送给所有用户。

15.3. 定期更新手机 app 和浏览器扩展

Password Manager Pro 的本地手机 app 和浏览器插件的更新定期发布。 建议您定期检查应用和浏览器商店中的更新。

15.4. 安全建议

如果在产品中发现任何安全漏洞，我们会立即通过升级包提供修复程序。 安全建议也会发送到您注册时填写的客户电子邮件。 请留意该电子邮件，以确保不会错过任何建议。 收到邮件后请按照电子邮件中的建议操作。

15.5. 将 PMP 移动到另一台计算机

要将 Password Manager Pro 安装在两台计算机之间移动，请按照以下步骤操作：

1. 退出 Password Manager Pro。
2. 将整个 Password Manager Pro 安装文件夹复制到另一台机器即可。
3. 然后安装，作为服务运行。 在此选项中，您无法通过 Windows 卸载程序或添加、删除程序控制台。 如果要重新安装，只要删除整个安装文件夹即可。

警告：在确保新安装正常工作之前，请不要删除现有的 Password Manager Pro 安装。 这可确保您准备好有效备份，以应对移动过程中需要克服灾难或数据损坏。

ManageEngine
Password Manager Pro

16.0 紧急访问条款

16.1. 使用本地 Password Manager Pro 账号，以备不时之需

在极少数情况下，您的 Active Directory 服务器出现故障，用户可能会被锁定。 为解决此问题，建议您在 Password Manager Pro 中使用本地账号。

16.2. 导出密码为加密 HTML 文件，以备离线访问

通常，在数据中心等受控环境中，其他设备不允许联网。 为确保在这些位置访问密码的顺利进行，Password Manager Pro 提供离线访问。 此功能允许您根据需要定期将所有密码导出为加密的 HTML 文件，并将文件存储在安全的位置。 该文件将使用您提供的 16 位密码加密。 只有知道密码的用户才能解锁离线文件。 您还可以通过指定时间间隔（例如，15 分钟）自动注销文件配置。 通过**管理>>设置>>导出/离线访问**配置这些设置。 除在线导出外，您还可以通过**组**，从**操作**下的下拉菜单中选择**定期密码导出来**计划资源组密码的导出操作。 您可以按日，按周或按月安排导出。

ManageEngine
Password Manager Pro

17.0 管理员离职

当组织中的管理员离职时，请确保执行以下操作：

17.1. 准备资源报表

当管理员离开组织时，首先要确定他们在公司中的权限级别并评估相关的漏洞。 这个至关重要，因为管理员可以不受限制地访问您的 IT 资产。 在这些情况下，建议您在 Password Manager Pro 中生成包含特定用户有权访问的完整密码列表的自定义报表。 要生成特定于用户的自定义报表，请到**用户**，选择特定用户，然后单击**报表**列下的**用户报表**图标。

17.2. 转移资源所有权

获取离职管理员创建的资源列表后，将所有资源的所有权转移给您自己或 Password Manager Pro 中的其他管理员。 在执行此操作之前，您无法从应用程序中删除该管理员账号。转移资源所有权可以通过**用户**>>选择离职管理员，然后从**用户动作**下的下拉菜单中选择**转移所有权**来完成。

17.3. 转移批准者权限

如果您配置了访问控制，则该离职管理员可能是某个资源的批准者（即，他们可能已经处理过 Password Manager Pro 中其他用户的密码访问请求）。 我们建议您将其批准权限转让给其他管理员。 可以通过单击**用户**，选择该离职管理员，然后从**用户动作**下的下拉菜单中单击**转移批准者权限**来传输审批者权限。

17.4. 立即重置密码

为了排除将来的安全漏洞或未经授权的访问尝试，我们强烈建议您在将这些资源的所有权转移给具有管理级权限的其他用户后立即重置密码。

ManageEngine
Password Manager Pro

18.0 安全

54

18.1. 始终使用 SSL

Password Manager Pro 为敏感操作（包括密码重置和资源添加或导入）提供 SSL 和非 SSL 模式。鉴于 SSL 明显的安全优势，建议您始终选择 SSL。

18.2. 谨慎执行脚本,防止恶意输入

默认情况下，Password Manager Pro 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。 强烈建议您不要禁用此选项，因为其可以增强安全性。 如果需要运行正版脚本，请暂时禁用此选项并在完成任务后立即启用。

18.3. 配置闲置超时

从安全角度来看，当用户离开，工作站无人看管时，允许 Web 界面会话保持活动是有及其危险的。 默认情况下，Password Manager Pro 的 Web 会话自动注销被设置为 30 分钟。 我们建议您将其设置为 15 分钟甚至更短，以确保安全。 要配置闲时超时，请到**管理>>设置>>常规设置>>用户管理**。

18.4. 配置浏览器扩展的自动注销

您可以选择浏览器扩展会话应保持活动的时长。 为了最大限度地提高安全性，我们建议您在 15-30 分钟后设置自动注销。 可以在浏览器扩展中的设置下配置注销时间。

18.5. 离线访问：禁用密码导出

为实现安全离线访问，Password Manager Pro 提供了多个导出选项，例如纯文本电子表格文件和加密的 HTML 文件。 我们始终建议仅允许用户将密码导出为加密的 HTML 文件。 如果您允许用户在 CSV 文件中导出密码信息，请禁止将密码导出为纯文本。 请到**管理>>设置>>导出/离线访问**来完成。

18.6. 通过黑名单或白名单 IP 地址限制 API 调用和代理访问

对于本地手机 app 和浏览器扩展的 API 电话，通信，以及从目标计算机到 Password Manager Pro 服务器的代理访问，您可以通过 Password Manager Pro 启用基于 IP 的限制。 我们建议您限制有限数量的可访问 Password Manager Pro 的客户端系统。 要配置基于 IP 的限制，请到**管理>>配置>> IP 限制>> API 访问（或）代理访问。** 可以在各种级别和组合中设置 IP 限制，例如定义的 IP 范围或单个 IP 地址。

ManageEngine
Password Manager Pro

19.0 隐私

19.1. 隐私控制

为了提高隐私性，Password Manager Pro 可帮助您自定义和控制在报表生成过程中包含的个人数据。 您可以决定 Password Manager Pro 中的个人数据是否被屏蔽或者被删除。请到**管理>>设置>>隐私设置>>隐私控制。** 我们建议您在生成报告时屏蔽或删除高度机密的数据。

19.2. 加密导出

为了通过 Password Manager Pro 为所有导出操作提供高级别安全性，建议您到**管理>>设置>>隐私设置>>加密导出**来启用导出文件的加密。 您可以设置全局密码，该密码将统一用于所有导出操作，或允许用户为其导出的文件定义自己的密码。 然后，用户需要提供密码以查看导出的文件。