ManageEngine
Password Manager Pro

Guía de mejores prácticas

www.passwordmanagerpro.com

Tabla de contenido

1.0 Resumen general

1.1 Sobre Password Manager Pro

Password Manager Pro es una solución web para la gestión de identidades privilegiadas que permite a los equipos de TI gestionar identidades privilegiadas—contraseñas, claves SSH y certificados SSL—así como controlar y monitorear el acceso privilegiado a sistemas de información crítica desde una sola consola centralizada. También ayuda a cumplir con regulaciones como PCI DSS, NERC CIP y SOX que obligan al control del acceso privilegiado.

1.2 Sobre esta guía

Esta guía describe las mejores prácticas para configurar y usar Password Manager Pro en un entorno de red empresarial. A partir de nuestra experiencia en ayudar a organizaciones alrededor del mundo a implementar Password Manager Pro exitosamente y optimizar sus prácticas de gestión de acceso privilegiado, esta guía ofrece dirección para los administradores de TI para una configuración rápida y eficiente del software, así como para proteger la implementación de la gestión de cuentas privilegiadas. Las mejores prácticas se pueden adoptar durante todas las etapas—instalación, configuración, implementación y mantenimiento del producto—y se explican abajo con un enfoque especial en la seguridad, escalabilidad y desempeño de los datos.

2.0 Configuración recomendada del sistema

2.1 Requisitos mínimos del sistema

Antes de instalar Password Manager Pro, debe decidir sobre la configuración del sistema. Puede encontrar aquí los requisitos mínimos del sistema para ejecutar Password Manager Pro.

En general, el desempeño y la escalabilidad dependen de los siguientes factores:

- Cantidad de usuarios y grupos.
- Cantidad de recursos y grupos.
- Frecuencia del intercambio de recursos o contraseñas.
- Cantidad de tareas programadas.

Según los factores anteriores, se recomiendan los siguientes parámetros del sistema para empresas medianas y grandes:

Empresas medianas

Cant. de usuarios: 100-500

Cant. de recursos/contraseñas: Hasta 10.000

- Procesador Dual core o superior
- 8 GB RAM
- 40 GB espacio de disco duro

Empresas grandes

Cant. de usuarios: Más de 500

Cant. de recursos/contraseñas: Más de 10.000

- Procesador Quad core o superior
- 16 GB RAM
- 100 GB espacio de disco duro

Nota: Le recomendamos también instalar Password Manager Pro en un servidor dedicado, protegido y de gama alta para un desempeño y seguridad superiores.

3.0 Instalación

3.1 Windows vs Linux

Password Manager Pro se puede instalar en Windows o Linux. Aunque el software se puede instalar igualmente en ambas plataformas, instalarlo en Windows tiene las siguientes ventajas inherentes:

Integración de Active Directory (AD): Una instalación en Windows de Password Manager Pro puede integrarse directamente con Active Directory para importar usuarios y grupos. Además, los usuarios que hayan iniciado sesión en su sistema Windows con credenciales de cuenta de dominio pueden usar el inicio de sesión único (NTLM-SSO) para iniciar sesión automáticamente en Password Manager Pro. Con una instalación en Linux, usted debe depender de la autenticación basada en LDAP para servicios de Active Directory.

Reinicios de contraseñas para recursos de Windows: Una instalación en Windows de Password Manager Pro puede realizar reinicios de contraseñas en modo sin agente para todos los sistemas objetivo compatibles, en tanto haya una conectividad directa. Por otro lado, la instalación en Linux requiere que se implemente un agente en todos los recursos y controladores de dominios en Windows para reiniciar contraseñas en cuentas de dominio, de servicio y locales de Windows.

Aparte de lo anterior, el reinicio de contraseñas para cuentas de servicios, tareas programadas, archivos IIS Web.Config y cuentas de pool de aplicaciones IIS en Windows es compatible solo para la instalación en Windows de Password Manager Pro.

3.2 Base de datos del servidor

Password Manager Pro ofrece compatibilidad de servidor para bases de datos PostgreSQL y servidores MS SQL. Por defecto, el producto tiene incorporada una base de datos PostgreSQL, que es ideal para compañías pequeñas y medianas. Entretanto, para compañías grandes, recomendamos encarecidamente que use un Servidor MS SQL como su servidor para una mejor escalabilidad, desempeño, agrupamiento y recuperación ante desastres.

Si usted está utilizando un Servidor MS SQL como su servidor, le sugerimos las siguientes prácticas:

- Password Manager Pro también se comunica con el servidor MS SQL con SSL, con una configuración válida de certificados. Por tanto, le recomendamos tener una instancia de SQL dedicada para Password Manager Pro con el fin de evitar cualquier conflicto o interrupción con las bases de datos existentes.

- Mientras usa el Servidor MS SQL como su servidor, se genera automáticamente una clave única para la codificación a nivel base de datos y, por defecto, esta clave se almacenará en el directorio <PMP HOME/conf>, en un archivo llamado <masterkey.key>. Le recomendamos mover el archivo de la clave a una ubicación distinta para protegerlo de accesos no autorizados. Ya que se requiere de esta clave para configuraciones de alta disponibilidad y durante la recuperación ante desastres, su seguridad es vital. Perder la clave conllevará una reconfiguración del Servidor MS SQL y puede incluso derivar en pérdidas de datos.

- Use la autenticación de Windows mientras configura el Servidor MS SQL como su servidor en lugar de usar una cuenta local de SQL.

- Le recomendamos usar la misma cuenta de dominio para ejecutar el servidor de Password Manager Pro y el servidor MS SQL, de forma que pueda ejecutar el servicio de SQL y los servicios de agente de SQL.

- Se debe habilitar la opción codificación de fuerza para permitir a todos los clientes conectarse a esta instancia de SQL. Cuando se hace esto, todas las comunicaciones cliente a servidor se codificarán y se les negará el acceso a los clientes no compatibles con la codificación.

- Deshabilite todos los protocolos distintos a TCP/IP en el equipo donde se ejecuta el servidor MS SQL.

- Esconda esta instancia de SQL para evitar que otras herramientas la enumeren y deshabilite el acceso a esta base de datos para todos los otros usuarios, excepto la cuenta de servicio de Password Manager Pro.

- Establezca reglas de firewall para permitir el acceso solo a los puertos requeridos en el equipo donde se ejecuta el servidor MS SQL.

3.3 Proteja la clave maestra de instalación

Password Manager Pro usa una codificación AES-256 para proteger contraseñas y otra información sensible. La clave usada para la codificación (pmp_key.key) se genera automáticamente y es única para cada instalación. Por defecto, esta clave se almacena en el directorio <PMP HOME/conf>, en un archivo llamado <pmp_key.key>. La ruta de esta clave debe configurarse en el archivo manage_key. conf file presente en el directorio PMP HOME/conf. Password Manager Pro requiere que esta carpeta se accesible con permisos necesarios para leer el archivo pmp_key.key cuando inicie cada vez. Luego de un inicio exitoso, no necesita acceder más al archivo y, por tanto, el dispositivo con el archivo se puede sacar de línea. Le recomendamos encarecidamente que mueva esta clave a una ubicación segura distinta y la bloquee al darle acceso de lectura solo a la cuenta de servicio de Password Manager Pro. Asimismo, actualice esta ruta remota en el archivo "manage_key.conf" de forma que el producto pueda leer la clave de codificación durante el inicio. Puede también proteger esta clave al almacenarla en una memoria USB o disco duro portátil. Para una seguridad extrema, cree archivos de script para copiar esta clave en una ubicación legible y luego destruya la copia tras el inicio del servicio.

3.4 Tome el control de las credenciales de la base de datos

Aparte de la codificación de AES, la base de datos de Password Manager Pro se protege mediante una contraseña separada, que se genera automáticamente y es única para cada instalación. Esta contraseña de la base de datos se puede almacenar de manera segura en Password Manager Pro. Pero le recomendamos que almacene la contraseña en otra ubicación segura accesible al servidor del producto.

Por defecto, la información de la base de datos, como la JDBC URL, credenciales de inicio de sesión y otros parámetros, se almacenarán en un archivo llamado database_params.conf, que está presente en el directorio <PMP HOME/conf>. Aunque la base de datos se configura para no aceptar conexiones remotas, le recomendamos mover este archivo a una ubicación segura, restringir el acceso y dejarlo disponible solo para la cuenta de servicio de Password Manager Pro. Si coloca el archivo database_params.conf fuera de la carpeta de instalación de PMP, necesita especificar la ubicación junto con el nombre del archivo en el archivo <PMP-Home>\conf\wrapper.conf (para Windows) o el archivo <PMPHome>\conf\"wrapper_lin.conf (para Linux). Nótese que el servicio no puede iniciarse si no se especifica toda la ubicación aquí.

- La ruta de esta fila se configura en el archivo “wrapper.conf” presente en el directorio <PMP HOME/conf>. Edite este archivo y busque la línea `wrapper.java.additional.9=-Ddatabaseparams.file.`

- Si usa una instalación de Linux, entonces tendrá que editar el archivo “wrapper_lin.conf” presente en el directorio <PMP HOME/conf>.

- La ruta por defecto se configurará como `./../conf/database_params.conf.` Mueva el archivo “database_params.conf” para proteger la ubicación y especifique su ruta en el archivo de arriba. Por ejemplo, `wrapper.java.additional.9=-Ddatabaseparams.file=\\remoteserv-er1\tapedrive\sharedfiles\database_params.conf.`

- Guarde el archivo y reinicie Password Manager Pro para que el cambio surta efecto.

Nota: Los pasos anteriores solo aplican para PostgreSQL y MySQL. Si usa un servidor MS SQL como su servidor, vaya a la sección 3.2.

4.0 Parámetros del servidor y del entorno

4.1 Fortalecimiento del servidor

Por defecto, todos los componentes requeridos para que Password Manager Pro funcione se almacenan en el directorio de instalación (ManageEngine/PMP). Por tanto, le recomendamos encarecidamente que proteja el servidor en el que se instale Password Manager Pro. Algunos de los pasos básicos que debe llevar a cabo son:

- Deshabilitar el acceso remoto a este servidor para todos los usuarios regulares de dominio en su organización usando políticas de grupos de dominio. Restringir permisos de lectura para todos los administradores regulares y dar permisos escritos al disco o directorios de Password Manager Pro a solo uno o dos administradores de dominio.

- Establezca los firewall de entrada y salida para protegerse contra el tráfico entrante y saliente, respectivamente. Al usar este ajuste, usted también puede especificar qué puertos de servidores deben abrirse e, idealmente, usarse para realizar varias operaciones de gestión de contraseñas como reinicios remotos de contraseñas.

4.2 Use una cuenta de servicios dedicada

Cree una cuenta de servicio separada para Password Manager Pro en su controlador del dominio y úsela en todas las áreas de Password Manager Pro. Se usará la misma cuenta para ejecutar Password Manager Pro. Para empezar a usar la cuenta de servicio creada para Password Manager Pro, vaya a la consola de servicio ("services.msc") en el servidor donde se instala Password Manager Pro y navegue a las propiedades de Password Manager Pro. Cambie la cuenta de sistema local configurada por la cuenta de servicio creada. Esta misma cuenta de servicio puede usarse para importar usuarios y recursos de Active Directory.

4.3 Configure una dirección IP única para el servidor web

Por defecto, el servidor web de Password Manager Pro se vinculará a todas las direcciones IP disponibles del servidor en que se instala la aplicación. Debido a esto, Password Manager Pro será alcanzable en cualquiera o todas las direcciones IP con el puerto configurado (7272). Para restringir esto, le recomendamos que configure el servidor web para que se una a una sola dirección IP y así recibir comunicaciones entrantes solo de dicha dirección. Se pueden hacer los siguientes pasos para configurar la IP única:

- Detenga Password Manager Pro si se está ejecutando.
- Abra el archivo "server.xml" presente en la carpeta <PMP_HOME>\conf.
- Busque esta línea:

```
<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"/>
```

- En la línea anterior, luego del valor `port="7272"`, añada el atributo `address="127.0.0.1"`. Reemplace `127.0.0.1` con la dirección IP real del servidor que desea usar para el vínculo. Parámetros del servidor y del entorno.

4.4 Restrinja el acceso al servidor web al colocar en la lista blanca o negra direcciones IP

Se puede acceder a Password Manager Pro desde cualquier sistema de cliente, en tanto haya una conectividad. Por tanto, le recomendamos restringir y dar solo a un número limitado de sistemas de clientes acceso a Password Manager Pro. Para configurar las restricciones basadas en IP, navegue a **Administrador >> Configuración >> Restricciones de IP >> Acceso web**. Las restricciones de IP se pueden establecer en varios niveles y combinaciones, como rangos de IP definidos o direcciones IP individuales. Puede escoger que se permita el acceso web a rangos y direcciones IP específicos o, alternativamente, restringir el acceso al añadirlos al campo de direcciones IP bloqueadas.

5.0 Incorporación y gestión de usuarios

5.1 Aproveche la integración AD/LDAP para la autenticación y el aprovisionamiento

La integración de Password Manager Pro con Active Directory o cualquier directorio que cumpla con LDAP puede ser muy útil, ya que da las siguientes ventajas:

Aprovisionamiento y desaprovisionamiento de usuarios: Con la integración de AD/LDAP, la adición de usuarios a Password Manager Pro es rápida y fácil. Una vez integrados, usted puede importar directamente los perfiles y grupos u OU de los usuarios desde su directorio a Password Manager Pro. Además, el aprovisionamiento de cuentas de usuarios en el producto se vuelve un proceso simple. Por ejemplo, si importa una OU existente de "Administradores de bases de datos" desde su directorio a Password Manager Pro, usted puede asignar fácilmente las contraseñas de las bases de datos a ese grupo importado.

Además de esto, usted puede habilitar la sincronización mientras se integra Password Manager Pro con su directorio, de forma que cualquier cambio, como un usuario recién añadido o movido entre OU en su directorio, se reflejará automáticamente en Password Manager Pro. Sincronizar Password Manager Pro con su directorio también le permitirá mantenerse informado cuando un usuario se elimina permanentemente del correspondiente directorio de usuarios. Password Manager Pro deshabilita y bloquea dichas cuentas de usuarios, le notifica de esto mediante una notificación de correo electrónico y de alerta, tras lo cual usted puede escoger eliminar estas cuentas o reactivarlas.

Autenticación de Active Directory: Otra ventaja es que puede aprovechar el respectivo mecanismo de autenticación de su directorio y darles a sus usuarios opciones de inicio de sesión único (SSO). Una vez que active esta opción, los usuarios se autenticarán automáticamente en Password Manager Pro (con autenticación basada en NTLM) en tanto que ya hayan iniciado sesión en el sistema con sus credenciales de directorio. Usar las credenciales de AD para la autenticación de Password Manager Pro garantiza que las contraseñas de inicio de sesión no se almacenan localmente en Password Manager Pro, ya que los usuarios se autenticarán directamente desde su directorio.

5.2 Deshabilite la autenticación local

Después de integrar Password Manager Pro con su directorio que cumple con AD/LDAP, le recomendamos que deshabilite la autenticación local y permita que los usuarios inicien sesión en Password Manager Pro con sus credenciales de AD/LDAP. Para deshabilitar la autenticación local, navegue a **Administrador >> Ajustes >> Ajustes generales >> Gestión de usuarios**.

No obstante, si ha configurado una cuenta local de Password Manager Pro para fines de emergencia, usted no puede deshabilitar la autenticación local. En dichos casos, si aún desea tener solo autenticación de AD/LDAP, le recomendamos que deshabilite la opción **"Olvidó la contraseña"** en la misma sección (la opción se usa para reiniciar la contraseña de autenticación local para todos los usuarios de Password Manager Pro). Deshabilitar esta opción garantizará que los usuarios puedan iniciar sesión en Password Manager Pro usando solo sus credenciales de AD/LDAP, incluso si se habilita la autenticación local.

5.3 Use autenticación de dos factores

Una capa protectora adicional de la autenticación de usuarios garantiza que solo las personas correctas tengan acceso a sus recursos sensibles. Password Manager Pro da varias opciones para configurar un segundo nivel de autenticación antes de dar acceso a la interfaz web del producto. Las opciones de segundo factor son: PhoneFactor, tokens de RSA SecurID, Duo Security, Google Authenticator, contraseñas únicas mediante correo electrónico, cualquier autenticación de dos factores que cumpla con RADIUS, Microsoft Authenticator, Okta Verify y YubiKey. Se recomienda encarecidamente configurar la autenticación de dos factores para sus usuarios.

5.4 Asigne roles de usuarios con base en responsabilidades de trabajo

Luego de añadir usuarios, asígneles roles adecuados. Password Manager Pro has tiene cuatro roles predefinidos para los usuarios: administrador, administrador de contraseñas, auditor de contraseñas y usuario de contraseñas. Para obtener más información sobre los privilegios de cada rol, consulte nuestra documentación de ayuda. Los roles de administrador se deben restringir solo a un pequeño grupo de personas que necesitan realizar operaciones de gestión de usuarios y

configuraciones a nivel producto, además de la gestión de contraseñas.

Con el rol de súper administrador: Un súper administrador en Password Manager Pro tiene acceso a todas las contraseñas almacenadas. Es ideal que no se solicite este rol. No obstante, si le gustaría tener una cuenta dedicada para fines de emergencia, usted puede crear un súper administrador para su organización. Por razones de seguridad, este rol se debe limitar siempre a las personas principales en la jerarquía organizacional. Asimismo, el método de mejores prácticas en dichos casos es crear solo un súper administrador. Una vez que se ha promovido un administrador a súper administrador, pueden evitar la creación de más súper administradores en el futuro, según se requiera. Esto lo puede hacer el súper administrador al ir a **Administrador >> Autenticación >> Súper administradores**, y luego debe habilitar **Denegar la creación de súper administradores por parte de administradores**.
Para obtener más información, consulte esta documentación.

5.5 Cree grupos de usuarios

Organice a sus usuarios en grupos—por ejemplo, administradores de Windows, administradores de Linux y así sucesivamente. Agrupar a los usuarios ayuda muchísimo a la hora de intercambiar recursos y eliminar contraseñas. Si ha integrado Password Manager Pro con AD/LDAP, usted puede importar grupos de usuarios directamente desde el directorio y usar la misma estructura jerárquica.

5.6 Elimine la cuenta de administrador por defecto

Por razones de seguridad, le recomendamos encarecidamente que elimine las cuentas por defecto de administrador e invitado en Password Manager Pro, después de añadir uno o más usuarios con el rol de administrador.

5.7 Restrinja el acceso a aplicaciones móviles y extensiones de navegadores

Por defecto, todos los usuarios serán capaces de acceder a las aplicaciones móviles nativas y extensiones de navegadores de Password Manager Pro. Si quiere que sus usuarios no sean capaces de acceder a ninguna contraseña desde ningún dispositivo distinto a su estación de trabajo, deshabilite el acceso a aplicaciones móviles globalmente en su organización. Si es necesario, usted puede habilitar el acceso solo a los usuarios o administradores que lo requieren. De forma similar, usted también puede habilitar o deshabilitar el acceso a extensiones de los navegadores. Estas restricciones se pueden aplicar al ir a **Usuarios >> Más acciones** y seleccionando **Restringir el acceso móvil/ Restringir las extensiones de navegadores** del menú desplegable.

6.0 Colocación y organización de datos

6.1 Añada recursos: escoja un método conveniente

El primer paso para empezar con la gestión de contraseñas en Password Manager Pro es añadir recursos. La forma más rápida y conveniente de hacer esto es el descubrimiento automatizado de cuentas privilegiadas. Las otras formas son la adición manual y la importación de CSV. Use la importación mediante la función CSV/TSV si usó otra herramienta antes de cambiar a Password Manager Pro o si tiene sus credenciales almacenadas en hojas de cálculo.

6.2 Recuerde especificar los tipos de recursos

Mientras se añaden recursos manualmente o por importación de CSV, verifique si todos los recursos se están almacenando bajo un tipo de recursos. Esto es obligatorio para usar funciones como reinicios de contraseñas, ya que Password Manager Pro usa distintos modos de comunicación para diferentes recursos, con base en el tipo de recurso aplicado. A menos que se especifique, los recursos se almacenarán bajo "Desconocido" y, en ese caso, los reinicios de contraseñas fallarán. Password Manager Pro da 32 tipos de recursos por defecto, enumerados en **Administrador >> Tipos de recursos.**

6.3 Elimine cuentas privilegiadas no autorizadas

Cuando use la función de auto descubrimiento para inventariar los recursos de TI en su red y sus respectivas cuentas privilegiadas, Password Manager Pro, por defecto, buscará toda cuenta asociada con los recursos detectados en la red. Algunas cuentas pueden ser no autorizadas, no deseadas o huérfanas. Por ejemplo, cuando añade un recurso de Windows, todas las cuentas de invitados también se buscarán.

Desde la perspectiva de la seguridad, se deben identificar y eliminar cuentas no autorizadas para evitar cualquier vulnerabilidad no prevista en el futuro. Las mejores prácticas de gestión de contraseñas demandan que el número de cuentas privilegiadas debe mantenerse en el mínimo. Además, volcar cuentas no deseadas también puede desordenar la base de datos y hacer que la organización de los datos sea una tarea abrumadora. Por tanto, le recomendamos eliminar estas cuentas no deseadas en el equipo objetivo en sí antes de ejecutar el auto descubrimiento en Password Manager Pro.

6.4 Aleatorice contraseñas después del descubrimiento de recursos

Una vez que haya completado el descubrimiento de recursos y la enumeración de cuentas, le recomendamos encarecidamente que aleatorice las contraseñas para todas las cuentas. Esta práctica es importante debido a que antes de implementar Password Manager Pro, sus empleados pueden haber almacenado sus contraseñas en distintos medios como hojas de cálculo y archivos de texto, o pueden incluso haberlas copiado en un papel. Si no se cambian las contraseñas, estos empleados aún pueden acceder a los recursos directamente, fuera de Password Manager Pro. En consecuencia, las contraseñas deben aleatorizarse debidamente después del descubrimiento de los recursos para bloquear todo acceso directo no autorizado a estos. Además, la aleatorización también se deshace de contraseñas débiles y asigna contraseñas fuertes y únicas para los recursos. La aleatorización de contraseñas para las cuentas descubiertas puede realizarse desde **Recursos >> seleccione los recursos específicos >> Acciones de recursos** (en la parte superior) **>> Configurar reinicio remoto de contraseñas.**

Nota: En el futuro, si desea predeterminar la aleatorización de contraseñas para nuevas cuentas cuando se descubran, usted puede configurar de la misma manera desde **Recursos >> seleccione los recursos específicos >> Acciones de recursos** (en la parte superior) **>> Descubrir cuentas,** y habilitar **Aleatorizar contraseñas después del descubrimiento** en la nueva ventana que se abre.

6.5 Aproveche la potencia de los grupos de recursos

Los grupos de recursos son bastante potentes en Password Manager Pro. La mayoría de las operaciones avanzadas de gestión de contraseñas, como la delegación automatizada de contraseñas y la rotación programada de contraseñas, pude realizarse solo en el nivel de grupo de recursos. Entre los dos tipos de creación de grupos de recursos, se recomiendan encarecidamente los grupos “basados en criterios”.

Los grupos basados en criterios son básicamente grupos dinámicos. Ellos le dan la flexibilidad para consolidar recursos que satisfagan ciertos criterios en un solo grupo. Una vez define los criterios, Password Manager Pro identificará automáticamente los recursos que concuerden y creará el grupo, sin necesidad de intervenciones manuales.

6.6 Use grupos de recursos anidados y ordene los recursos según los departamentos

Para facilidad de uso y conveniencia en la navegación mientras recupera un único recurso de una base de datos enorme, usted puede aprovechar el parámetro vista de árbol explorador en Password Manager Pro (es decir, crear grupos de recursos anidados). Por defecto, el árbol mostrado será diferente para cada usuario. Habilite este parámetro vista de árbol para mostrar globalmente un árbol explorador uniforme de la organización. Luego de habilitarlo, cambie el nombre del nodo principal de 'Grupos de recursos' al nombre de su organización. Bajo esto, cree varios subnodos con base en los distintos equipos o departamentos que tenga. Luego, usted puede designar los grupos de recursos bajo los subnodos del equipo o departamento al que pertenecen.

Al manipular el árbol explorador como se mencionó arriba, usted puede crear una jerarquía clara de grupos de recursos que dan una fácil accesibilidad. Para permitir la manipulación del árbol explorador, vaya a **Administrador >> Ajustes generales >> Recuperación de contraseñas, y habilite "Permitir a todos los usuarios administradores manipular todo el árbol explorador"**.

6.7 Campos adicionales para referencia y búsqueda fáciles

Mientras se añaden recursos, se pueden usar campos adicionales para crear columnas y valores personalizados. Los campos serán útiles para crear grupos basados en criterios, buscar recursos o contraseñas específicos, compartir recursos y más. Por ejemplo, asuma que tiene tres niveles de administradores de TI en su organización. Por tanto, si crea un campo de recurso adicional titulado **"Nivel de acceso"**, usted puede organizar fácilmente recursos bajo "Nivel I/II/III". Con el campo **"Nivel de acceso"** como criterio, puede crear tres grupos de recursos distintos. De forma similar, usted puede crear tres grupos de usuarios, cada uno con usuarios que pertenezcan a distintos niveles, y luego asignarles recursos de "Nivel I" a usuarios de "Nivel I" y así sucesivamente.

7.0 Compartir contraseñas y restricciones detalladas

7.1 Comparta contraseñas con privilegios de acceso variables

Mientras comparten recursos, los propietarios de contraseñas pueden otorgar distintos niveles de permisos a los usuarios y grupos al escoger uno de los siguientes privilegios:

- **Ver contraseñas:** Los usuarios solo pueden acceder a la contraseña.
- **Modificar contraseñas:** Los usuarios pueden acceder y modificar la contraseña compartida.
- **Acceso completo:** Los usuarios gestionan por completo un recurso o grupo, y pueden intercambiar el recurso, grupo o contraseñas de cuentas individuales.

Le recomendamos solo darles a los usuarios permisos de "Ver contraseñas", ya que en su mayoría es suficiente para varias operaciones relacionadas con contraseñas. Tenga cuidado de dar permisos de "Acceso completo", debido a que un usuario estos permisos sobre una contraseña es casi u copropietario y será capaz de modificar, eliminar e incluso intercambiar la contraseña con más usuarios.

Nota: Aparte de estos privilegios de intercambio, usted también puede compartir recursos sin revelar las contraseñas en texto sin formato. Esto es posible cuando el auto inicio de sesión se configura para el recurso. Para obtener más información sobre esta función, consulte la sección 10.1.

7.2 Use los grupos de recursos para compartir grupos de usuarios

Aunque Password Manager Pro tiene disposiciones para compartir una sola contraseña o recurso con un solo usuario o grupo, el método de mejores prácticas es compartir un recurso con un grupo. Esto funcionará mejor para realizar operaciones a granel eficientemente y ahorrará tiempo. Por ejemplo, si necesita dar a los administradores de Windows en su organización acceso a todos los recursos de Windows, usted puede completar la operación en dos pasos sencillos:

- Cree un grupo de recursos basado en criterios (el tipo de recurso "Windows" es el criterio correspondiente). De esta forma, todos los recursos de Windows existentes se añaden al grupo y los nuevos recursos creados en el futuro también se añadirán automáticamente al grupo.

- Cree un grupo de usuarios para administradores de Windows. Si ha integrado AD/LDAP, usted puede importar el grupo directamente y permitir la sincronización automática de la base de datos de los usuarios. De esta forma, cuando sea que se una un nuevo administrador de Windows a la organización, su cuenta de AD se añadirá automáticamente al grupo de usuarios de contraseñas y el nuevo usuario heredará subsecuentemente los permisos del grupo para ver las contraseñas del servidor de Windows.

7.3 Haga uso de los flujos de trabajo para el control del acceso

El control de acceso en Password Manager Pro es un mecanismo de liberación por solicitud que no permite a los usuarios acceder directamente a las contraseñas. En su lugar, los usuarios tienen que generar una solicitud al administrador para la aprobación del acceso. La función también le ayuda a introducir varias restricciones de acceso para sus recursos, como acceso por tiempo limitado, controles de simultaneidad y reinicios automatizados después del periodo de uso. Así, le recomendamos encarecidamente que habilite este control de liberación para las credenciales de sus recursos críticos.

Para una mejor seguridad, usted puede configurar también aprobaciones duales para recursos críticos, que obligan que dos administradores aprueben una solicitud antes de que las contraseñas se liberen por un periodo temporal. Este ajuste es útil cuando dos departamentos distintos principalmente poseen una credencial administrativa en su organización. Los controles de acceso se pueden configurar al ir a **Recursos >> Acciones de recursos >> Configurar el control del acceso.**

7.4 Solicite que los usuarios den la razón para recuperar contraseñas

Por defecto, todas las operaciones relacionadas con contraseñas se captan en los rastros de auditoría de Password Manager Pro, completar con la fecha y los detalles de la dirección IP. De forma opcional, usted puede solicitar que los usuarios ingresen una razón de por qué necesitan acceder a una contraseña. Estas razones también se registrarán en los rastros de auditoría, que pueden usarse para verificaciones cruzadas y validaciones en investigaciones forenses. Por tanto, cuando sea que un usuario trate de recuperar la contraseña de un recurso, nosotros le

recomendamos obligar a que ellos den una razón creíble para solicitar el acceso, sin importar si se han configurado o no los controles de acceso. Esta opción se puede activar en **Administrador >> Ajustes >> Ajustes generales>> Recuperación de contraseñas**.

7.5 Integre Password Manager Pro con sistemas de tickets empresariales

Password Manager Pro da la opción de integrar un rango de sistemas de ticketing para validar automáticamente solicitudes de servicios relacionadas con accesos privilegiados. La integración garantiza que los usuarios pueden acceder a contraseñas privilegiadas autorizadas solo con una ID de ticket válida. Con el fin de habilitar un flujo de trabajo de recuperación más fuerte para sus contraseñas de recursos críticos, le sugerimos integrar Password Manager Pro a su sistema de ticketing empresarial. En la actualidad, Password Manager Pro se integra inmediatamente con ManageEngine ServiceDesk Plus On-Demand, ServiceDesk Plus MSP, ServiceDesk Plus, ServiceNow y JIRA. Usted puede integrar Password Manager Pro con los sistemas de ticketing arriba mencionados al ir a **Administrador >> Integración >> Integración del sistema de ticketing**.

8.0 Políticas de contraseñas

8.1 Establezca políticas de contraseñas separadas para grupos de recursos críticos

Sobre todo, las políticas de contraseñas le ayudan a definir la fortaleza de las contraseñas al especificar las complejidades de los caracteres. Password Manager Pro le permite personalizar y configurar distintas políticas de contraseñas para distintos grupos de recursos. Si tiene un pequeño grupo de recursos que son de naturaleza ultrasensible, organícelos todos en un grupo de recursos y configurar una política separada con requisitos muy estrictos. Las políticas para los grupos de recursos se pueden configurar en **Grupos >> Seleccionar los grupos específicos >> Configuración a granel >> Políticas de contraseñas asociada**.

8.2 Política de contraseñas a nivel cuenta

Por lo general, cada recurso se da con una o pocas cuentas administrativas y otras cuentas normales. Para proteger estas cuentas privilegiadas, le recomendamos configurar una política de contraseñas segura por separado para las cuentas sensibles de recursos importantes. Las política de contraseñas a nivel cuenta se pueden configurar en **Recursos >> Seleccionar los recursos específicos >> Acciones de recursos** (en la parte superior) **>> Política de contraseñas asociada.**

8.3 Defina la edad de sus contraseñas mientras crea políticas

Mientras configura una nueva política de contraseñas, recuerde siempre ajustar la edad máxima de la contraseña. Especificar una edad permite a Password Manager Pro reiniciar automáticamente la contraseña cuando la edad expira. Sino completa el campo, las contraseñas no expirarán, lo que **NO** es una práctica recomendada.

9.0 Reinicios de contraseñas

9.1 Aleatorización periódica de contraseñas

Proteger la gestión de cuentas privilegiadas requiere el uso de contraseñas fuertes y únicas que se reinician periódicamente. Es ideal que las contraseñas se deban reiniciar al menos una vez cada 90 días—el marco temporal más frecuente establecido por regulaciones de TI como PCI-DSS. Le recomendamos configurar reinicios regulares de contraseñas para grupos de recursos en Password Manager Pro con la función de reinicio programado de contraseñas. Aún más importante, configure contraseñas que se reinicien automáticamente durante las siguientes situaciones, así como:

- después de que un usuario termine de usar una contraseña y la registre.
- cuando se revoquen permisos de intercambio para usuarios con quienes se compartió inicialmente la contraseña.
- cuando la contraseña expire, como se estableció mediante las políticas de contraseñas.

9.2 Escoja el modo de reinicio de contraseñas más adecuado

Los reinicios de contraseñas se pueden realizar de una de las dos formas en Password Manager Pro: con o sin agente.

Para el modo sin agente, Password Manager Pro se conecta directamente con el sistema objetivo y cambia la contraseña. Se deben dar las credenciales administrativas para realizar cambios en las contraseñas. Más específicamente, para realizar reinicios de contraseñas para recursos de Linux desde una instalación en Windows de Password Manager Pro, se requieren dos cuentas, una con privilegios raíz y una con privilegios normales de usuarios que se pueden usar para iniciar sesión de manera remota.

Por otro lado, el modo basado en agentes es útil cuando tiene que reiniciar contraseñas para recursos sin conectividad directa, como aquellos en ubicaciones DMZ o con restricciones de firewall. Para lograr estos reinicios de contraseñas, Password Manager Pro implementa un agente al host remoto, que ejecuta la tarea. Toda la comunicación entre el agente y el servicio de aplicaciones es una forma y sobre HTTPS, de forma que no tenga que abrir ningún puerto de firewall para el tráfico entrante.

Básicamente, entre ambos modos, el modo sin agente es el método más conveniente y fiable de cambiar contraseñas y le recomendamos escoger este cuando se puedan alcanzar los recursos directamente. No obstante, tiene que escoger el modo basado en agentes para los siguientes casos de uso:

- Cuando las credenciales administrativas no están disponibles en Password Manager Pro para un recurso particular.
- Cuando los servicios requeridos por Password Manager Pro para reiniciar no se ejecutan en el recurso objetivo (Telnet/SSH para Linux, RPC para Windows)
- Cuando Password Manager Pro se ejecuta en Linux y necesita hacer cambios en contraseñas a un recurso de Windows.
- Cuando tiene dos entornos distintos, "A" y "B", con firewalls entre ellos. Durante dichos casos, usted puede instalar Password Manager Pro en un entorno, digamos A, y usar el modo sin agente para los equipos en dicho entorno. Por otro lado, usted puede instalar agentes en los equipos del entorno B para reinicios de contraseñas. De esta forma, todas las contraseñas se pueden gestionar en A y B sin añadir excepciones a puertos de firewall.

9.3 Reinicie servicios para lograr una rutina completa de gestión

Con Password Manager Pro, las cuentas de dominio de que se usan para ejecutar varios servicios y pools de aplicaciones IIS pueden también someterse a reinicios periódicos de contraseñas, junto con una propagación subsecuente de contraseñas en todos los servicios dependientes y pools de aplicaciones. Para garantizar que se actualizan adecuadamente esos servicios, tareas y pools de aplicaciones con cambios de contraseñas, Password Manager Pro ofrece una opción para reiniciar automáticamente servicios después de que se reinicie la contraseña, lo que recomendamos.

10.0 Gestión de sesiones

10.1 Permita que los usuarios inicien sesión automáticamente en sistemas remotos sin revelar contraseñas en texto sin formato

Luego de configurar las opciones de inicio de sesión automático para conectarse de forma remota a recursos, Password Manager Pro permite a los usuarios establecer una conexión directa con el recurso con solo un clic, eliminando la necesidad de copiar y pegar contraseñas. En dichos casos, recomendamos evitar que los usuarios recuperen las contraseñas en texto sin formato, ya que no se requiere. La recuperación en texto sin formato se puede deshabilitar **Administrador >> Ajustes >> Ajustes generales >> Recuperación de contraseñas.**

10.2 Monitoree sesiones críticas en tiempo real

Password Manager Pro ofrece ocultamiento de sesiones, que se puede usar para establecer controles duales sobre sesiones privilegiadas. Use esta función para monitorear sesiones remotas en tiempo real y supervise la actividad de los usuarios. Básicamente, los controles duales son útiles para dar asistencia remota e impedir actividades maliciosas. Si es un administrador, usted puede controlar sesiones críticas lanzadas desde la aplicación al unir sesiones activas y observar la simultaneidad, sin afectar al usuario final. En caso de detectar cualquier actividad sospechosa, usted puede terminar inmediatamente la sesión para evitar cualquier mal uso del acceso privilegiado.

10.3 Depure regularmente las sesiones registradas

Por defecto, Password Manager Pro registra todas las sesiones de RDP, VNC, SSH, Telnet y SQL lanzadas desde la aplicación. Si su organización es grande, con un rango integral de recursos para los cuales el registro de sesiones está habilitado, las sesiones registradas crecerán naturalmente a una tasa más rápida. Si no necesita registros anteriores a un número especificado de días, le recomendamos depurarlos para mantener libre el espacio del disco. También puede almacenar estos registros en el disco local, de forma que los pueda llevar a todas partes. Por otro lado, si desea eliminar una sesión seleccionada o el historial de chat de una sesión particular, puede hacerlo al ir a **Auditorías >> Sesiones registradas**, y luego al hacer clic en el ícono **"Eliminar"** al lado de la sesión seleccionada. Nótese que Password Manager Pro obliga la aprobación de al menos dos administradores para eliminar el registro de una sesión particular o el chat de una.

11.0 Acceso privilegiado a terceros

11.1 Gestione el acceso a terceros a sistemas corporativos

Lo más frecuente es que terceros como contratistas, consultores y proveedores soliciten acceso a los recursos corporativos de TI para llevar a cabo deberes contractuales y otras necesidades corporativas. Cuando usted da acceso privilegiado a un tercero, siempre recomendamos que les dé **solo acceso temporal, restringido con estipulaciones temporales y los privilegios mínimos necesarios**. Además de esto, se sugiere que siga unas pocas prácticas mientras comparte información crítica con terceros:

- Ya que los contratistas se conectan de manera remota a sus recursos, añada todos sus terceros como usuarios en Password Manager Pro y solicíteles establecer sesiones directas a sistemas objetivos solo mediante Password Manager Pro.

- Después de configurar el auto inicio de sesión para el recurso, el método de mejores prácticas es compartir las credenciales de inicio de sesión sin mostrar las contraseñas en texto sin formato.

- Asimismo, configure los flujos de trabajo para el control del acceso para dichos recursos. Esto ayuda a implementar límites temporales para el acceso a las contraseñas, incluido un reinicio automático de las contraseñas al final del periodo de uso.

- Esconda las sesiones regularmente para detectar cualquier rastro de comportamiento malicioso y adoptar instantáneamente medidas de remediación.

- Cuando finalice el contrato con un proveedor, ejecute inmediatamente los reinicios de contraseñas para todos los recursos a los que el proveedor tuvo acceso.

12.0 Acceso remoto a centros de datos

12.1 Evite la circulación de las credenciales de servidores de salto

Por lo general, conectarse a recursos de centros de datos remotos es un proceso tedioso, ya que el acceso directo está restringido desde una perspectiva de la seguridad. En su lugar, los administradores deben pasar una serie de servidores de salto antes de conectarse finalmente al dispositivo objetivo, autenticándose manualmente en cada etapa. Este proceso de varios pasos introduce varias credenciales para cada servidor de salto, que los usuarios necesitan para lanzar una conexión al centro de datos. Para estos casos, hacer circular todas las credenciales entre los usuarios no es una práctica segura. En su lugar, use la función configuración de servidor de arribo en Password Manager Pro para hacer que sus usuarios se conecten a centros de datos solo mediante Password Manager Pro. La aplicación da un acceso protegido y automatizado con un solo clic a los recursos de los centros de datos, eliminando la necesidad de la autenticación manual en cada paso. También centraliza la gestión de las credenciales del servidor de salto.

12.2 Exporte contraseñas de antemano para tenerlas listas para el acceso fuera de línea

Si un entorno de centros de datos no permite la conectividad a internet, usted no podrá acceder a Password Manager Pro desde dicha red. En este caso, exporte todas las contraseñas requeridas como un archivo HTML codificado de antemano y acceda a las contraseñas fuera de línea. Si la opción de exportación está habilitada, usted puede descargar el archivo desde **Recursos >> Acciones de recursos** (en la parte superior) **>> Exportar contraseñas**.

13.0 Auditorías e informes

13.1 Facilite auditorías internas regulares

Use los rastros de auditoría de Password Manager Pro para registrar instantáneamente todos los eventos alrededor de las operaciones de cuentas privilegiadas, intentos de inicios de sesión de usuarios, tareas programadas y tareas completadas. Al convertir esta información en informes bien presentados, usted puede facilitar auditorías internas regulares e investigaciones forenses, y así descubrir fácilmente quién hizo qué con una contraseña, dónde y cuándo.

13.2 Controle actividades seleccionadas con alertas instantáneas

Password Manager Pro también le permite enviar notificaciones instantáneas por correo electrónico a destinatarios escogidos cuando se den ciertos eventos. Esta opción es muy útil para estar constantemente actualizados sobre qué hacen los usuarios. Por tanto, le recomendamos configurar alertas para operaciones importantes como adición de nuevos usuarios, eliminación de contraseñas, intercambios de contraseñas y más. Se pueden habilitar las alertas por correo electrónico a nivel operativo al ir a **Auditorías >> Auditorías de recursos** (por ejemplo) **>> Acciones de auditorías >> Configurar auditorías de recursos**. Las alertas a nivel contraseñas se pueden habilitar desde **Grupos >> Acciones >> Configurar notificaciones**.

13.3 Opte por digerir diariamente correos para evitar desórdenes en las bandejas de entrada

Si tiene habilitada las alertas y las actualizaciones para un número de recursos, puede que su bandeja de entrada se vea saturada de correos electrónicos de notificaciones. En caso de que esto se presente, usted puede escoger recibir un correo de digestión diario al final de cada día con una lista consolidada de notificaciones, si las actualizaciones por hora no son una prioridad.

13.4 Configure plantillas de correos electrónicos

Por defecto, Password Manager Pro tiene un contenido específico para las notificaciones por correo electrónico. Le recomendamos configurar la plantilla para ajustarse a sus necesidades y personalizar su propio contenido. Esto se puede hacer al ir a **Administrador >> Personalización >> Plantillas de correos electrónicos**.

13.5 Genere mensajes de syslog y traps de SNMP para sus sistemas de gestión

Manager Pro con la herramienta. Esta integración le permite enviar mensajes de syslog a la herramienta cuando sea que suceda la actividad dentro de Password Manager Pro. De forma opcional, usted también puede integrar su gestor de SNMP con la aplicación y generar traps de SNMP. Esto le ayudará a tener una vista holística del acceso privilegiado, junto con la actividad general de la red, desde una ubicación central.

13.6 Programe la generación periódica de informes

Password Manager Pro ofrece una variedad de informes prefabricados que dan información sobre el inventario de las contraseñas, el estado de vencimiento, las frecuencias de acceso de los usuarios, su actividad y más. En lugar de generar estos informes manualmente, le recomendamos que use la función **Programar informe** para los informes requeridos y así ahorrará tiempo. Una vez programados, los informes se generarán automáticamente durante el intervalo especificado y se enviarán a su correo electrónico registrado.

13.7 Depure los registros de auditorías

Resulta normal que cuando se audita cada operación, los registros de auditoría crezcan a una tasa más rápida. Si no necesita auditar registros anteriores a un número especificado de días, usted puede depurarlos. Esto se puede configurar al ir a **Auditorías >> Auditorías de usuarios** (por ejemplo) **>> Acciones de auditorías >> Configurar auditorías de usuarios**. Por defecto, la opción de depuración se deshabilitará cuando los días se ajusten a cero (0).

14.0 Redundancia y descubrimiento de datos

14.1 Establezca la recuperación ante desastres

Los datos almacenados en la base de datos de Password Manager Pro son de importancia crítica. En el evento improbable de que falle un parámetro de producción, se pueden perder todos los datos. Por tanto, la recuperación ante desastres es esencial. La aplicación da disposiciones para el respaldo de datos en tiempo real y para respaldos periódicos automatizados mediante tareas programadas. Escoja el método que se ajuste mejor a su organización. Asimismo, garantice que el directorio de destino configurado para el respaldo se encuentra en una ubicación remota segura.

14.2 Implemente un servidor secundario con una arquitectura de alta disponibilidad

La arquitectura de alta disponibilidad en Password Manager Pro es un ajuste recomendado que le ayuda a superar inactividades y garantizar el acceso continuo a las contraseñas. Esto se logra al instalar otra instancia de Password Manager Pro en un servidor secundario, además del servidor primario de aplicaciones. Si tiene distintas redes dentro de su lugar de trabajo (redes separadas para cada piso, por ejemplo), le recomendamos instalar servidores de aplicaciones primarios y secundarios en distintas redes.

Por otro lado, si tiene oficinas en dos ubicaciones diferentes, la mejor práctica para un ajuste de alta disponibilidad es configurar el servidor primario de Password Manager Pro en su sede e implementar un servidor secundario en la otra oficina. De esta forma, los empleados en ambas ubicaciones disfrutarán de acceso ininterrumpido a contraseñas en el caso de una interrupción en el servidor. Para ajustar la alta disponibilidad, vaya a **Administrador >> Configuración >> Alta disponibilidad**, y configure un servidor en espera para Password Manager Pro.

15.0 Mantenimiento

15.1 Mantenga su instalación actualizada

El equipo en Paquetes de actualización publica constantemente paquetes de actualización que contienen mejoras y arreglos. Es ideal que las actualizaciones importantes se publiquen una vez cada trimestre, mientras que las menores se pueden anunciar una vez cada mes o dos. Estos paquetes de actualización también contendrán actualizaciones para el servidor web Tomcat, la base de datos PostGresSQL database y JRE que vienen con el producto. Con el fin de dar el adecuado mantenimiento a su instalación de Paquetes de actualización para un óptimo desempeño, le recomendamos descargar y aplicar los paquetes de actualización para Paquetes de actualización tan pronto como se publiquen. Los paquetes de actualización se pueden descargar aquí.

Actualizar el SO de Windows donde se instale Password Manager Pro: Cuando tenga que instalar parches de Windows en el servidor de Password Manager Pro, realice los siguientes pasos:

1. Abra la consola Servicios (services.msc) y detenga el servicio Password Manager Pro.
2. Haga una copia de todo el directorio de Password Manager Pro y almacénela en cualquier otro equipo como respaldo. O si el servidor es un VM, solo tome un snapshot.
3. Ahora, actualice el SO de Windows.

15.2 Escoja sabiamente su ventana de mantenimiento

Con el fin de aplicar los paquetes de actualización, Paquetes de actualización se debe detener temporalmente. Si se configura la alta disponibilidad, se apagarán los servidores primario y secundario. Además, el diseño actual de Password Manager Pro requiere reconfigurar la alta disponibilidad después de cada actualización. Por tanto, le recomendamos encarecidamente programar la ventana de mantenimiento durante los fines de semana u horas no laborales.

Si no puede evitar la realización de una actualización durante las horas laborales, usted puede alertar a sus usuarios antes de la siguiente operación de mantenimiento con la **Mesa de mensajes** de Password Manager Pro. La opción **Mesa de mensajes** se puede encontrar en **Administrador >> Gestionar**. Usted puede enviar el mensaje que escriba como correo electrónico o alerta en línea a todos los usuarios.

15.3 Actualice sus aplicaciones móviles y extensiones de navegador periódicamente

Las actualizaciones para las aplicaciones móviles y plug-ins de navegadores nativos de Password Manager Pro se publican regularmente. Le recomendamos verificar las actualizaciones en las tiendas de aplicaciones y navegadores periódicamente.

15.4 Busque asesorías de seguridad

Si se descubre alguna vulnerabilidad de seguridad en el producto, se dan arreglos inmediatamente mediante paquetes de actualización. Se enviará también un consejo de seguridad al correo electrónico del cliente que tenga registrado con nosotros. Controle ese correo electrónico para garantizar que no se pierda nuestros consejos. Cuando reciba uno, haga lo que el correo le recomienda.

15.5 Pase la instalación de Password Manager Pro de un equipo a otro equipo

Para pasar una instalación de Password Manager Pro de un equipo a otro, siga el procedimiento que se detalla a continuación:

- Salga de Password Manager Pro, si se está ejecutando.
- Solo copie toda la carpeta de instalación de Password Manager Pro de un equipo a otro equipo.
- Luego, instálelo para ejecutar como servicio. En esta opción, no será capaz de desinstalar el programa en Windows o añadir o eliminar la consola de programas. Si desea reinstalar en cualquier momento, solo elimine toda la carpeta de instalación.

Precaución: No elimine la instalación existente de Password Manager Pro hasta que garantice que la nueva instalación funciona bien. Esto garantiza que tiene listo un respaldo válido, en el caso de que necesite superar desastres o corrupción de datos durante el movimiento.

16.0 Aprovisionamientos de acceso de emergencia

16.1 Use una cuenta local de Password Manager Pro para fines de emergencia

En el raro evento de que los servidores de Active Directory se apaguen, los usuarios pueden quedar bloqueados. Para tratar esto, le recomendamos tener una cuenta local en Password Manager Pro.

16.2 Exporte contraseñas como un archivo HTML codificado para el acceso fuera de línea

Por lo general, en entornos controlados como centros de datos, no se permite la conectividad a internet en otros dispositivos. Para garantizar el acceso a las contraseñas en dichos lugares, Password Manager Pro da acceso fuera de línea. Esta función le permite exportar todas sus contraseñas como un archivo de HTML codificado periódicamente, según se desee, y almacena el archivo en una ubicación protegida. El archivo se codificará con una frase de contraseña de 16 dígitos que usted dé. Solo los usuarios que saben la frase de contraseña pueden desbloquear el archivo fuera de línea. Usted puede también configurar el cierre de sesión automático para el archivo al especificar un intervalo de tiempo (por ejemplo, 15 minutos). Estos parámetros se pueden configurar al ir a **Administrador >> Ajustes >> Exportar / Acceso fuera de línea**. Aparte de exportaciones por demanda, usted puede también programar operaciones de exportación para las contraseñas de sus grupos de recursos al ir a **Grupos**, y seleccionar **Exportación periódica de contraseñas** del menú desplegable bajo **Acciones**. Usted puede programar las exportaciones de forma diaria, semanal o mensualmente.

17.0 Cuando un administrador se va

Hay momentos cuando uno de los administradores deja la organización. Si esto sucede, asegúrese de hacer lo siguiente:

17.1 Prepare el informe de salida

Cuando un administrador se va de la organización, necesita determinar primero sus niveles de privilegios en la compañía y evaluar las vulnerabilidades asociadas. Esta práctica es crítica ya que ellos poseen acceso sin restricción a sus activos de TI. En estos casos, le recomendamos generar un informe personalizado en Password Manager Pro que contiene la lista completa de contraseñas a las que el usuario tuvo acceso. Para generar informes personalizados específicos de usuarios, vaya a **Usuarios**, seleccione el usuario específico y haga clic en **'Informe de usuario'** en la columna **Informes**.

17.2 Transfiera la propiedad de los recursos

Luego de adquirir la lista de recursos creada por el administrador saliente, transfiera la propiedad de todos esos recursos a sí mismo o a otro administrador en Password Manager Pro. Usted no puede eliminar la cuenta del administrador en la aplicación hasta que haga esto. Se puede realizar la transfiera la propiedad de los recursos al ir a **Usuarios**, seleccionando al administrador saliente, y escoja **Transferir propiedad** del menú desplegable en **Acciones de usuario**.

17.3 Transfiera los privilegios del responsable de las aprobaciones

Si tiene controles de acceso configurados, el administrador saliente puede haber sido un responsable de aprobación para ciertos recursos (es decir, podrían haber manejado solicitudes de acceso a contraseñas de otros usuarios en Password Manager Pro). Le recomendamos transferir sus privilegios de responsable de aprobación a otro administrador cuando se vaya. Los privilegios del responsable de las aprobaciones se pueden transferir al hacer clic en Usuarios, seleccionando al administrador saliente, y haga clic en **Transferir privilegios del responsable de las aprobaciones** del menú desplegable en **Acciones de usuario**.

17.4 Reinicie contraseñas instantáneamente

Para descartar fallas de seguridad o intentos de acceso no autorizado en el futuro, le recomendamos encarecidamente que reinicie las contraseñas de todos los recursos propiedad del administrador que se va inmediatamente después de que se haya transferido la propiedad para esos recursos a otro usuario con permisos a nivel administrador.

18.0 Seguridad

18.1 Escoja siempre SSL en todas las comunicaciones

Password Manager Pro ofrece modos con y sin SSL para operaciones sensibles, incluido el reinicio de contraseñas y adición o importación de recursos. Debido a obvias ventajas de seguridad, le recomendamos siempre optar por la comunicación con SSL.

18.2 Ejecute prudentemente scripts y evite entradas maliciosas

Por defecto, Password Manager Pro se configurará para identificar scripts o códigos dañinos y evitar su ejecución. Además, también prohíbe ejecutar scripts que contienen etiquetas y atributos de HTML. No deshabilite esta opción, ya que es una mejor práctica altamente recomendada para aumentar la seguridad. Si necesita ejecutar un script genuino, deshabilite temporalmente esta opción y habilítela inmediatamente después de completar la tarea.

18.3 Configure la caducidad por inactividad

Permitir que sigan activas las sesiones de interfaz web cuando los usuarios dejan las estaciones de trabajo desatendidas es peligroso desde el punto de vista de la seguridad. Por defecto, la sesión web de Password Manager Pro se cerrará automáticamente en 30 minutos. Le recomendamos ajustarlo a 15 minutos o incluso menos, solo por seguridad. Para configura la caducidad por inactividad, vaya a **Administrador >> Ajustes >> Ajustes generales >> Gestión de usuarios**.

18.4 Configure el cierre de sesión automático para extensiones de navegadores

Usted puede escoger cuánto debe permanecer activa la sesión de extensión de un navegador. Para máxima seguridad, le recomendamos establecer el cierre de sesión automático después de un periodo de 15–30 minutos. Los periodos de cierre de sesión se pueden configurar en **Ajustes** en la extensión del navegador.

18.5 Acceso fuera de línea: deshabilite la exportación de contraseñas

Password Manager Pro da varias opciones de exportación para proteger el acceso fuera de línea, como archivos de hojas de cálculo con texto sin formato y archivos de HTML codificados. Siempre recomendamos que permita a los usuarios exportar contraseñas solo como archivos de HTML codificados. En el caso de que haya permitido que los usuarios exporten información de contraseñas en archivos CSV, deshabilite que las contraseñas se exporten como texto sin formato. Esto se puede hacer al ir a **Administrador >> Ajustes >> Exportar / Acceso fuera de línea**.

18.6 Restrinja las llamadas API y el acceso de agentes al colocar en la lista blanca o negra direcciones IP

Password Manager Pro le permite habilitar las restricciones basadas en IP para llamadas de API, comunicaciones desde aplicaciones móviles y extensiones de navegadores nativas, así como la comunicación de agentes desde equipos objetivos al servidor de Password Manager Pro. Le recomendamos restringir y dar solo a un número limitado de sistemas de clientes acceso a Password Manager Pro. Para configurar las restricciones basadas en IP, navegue a **Administrador >> Configuración >> Restricciones de IP >> Acceso de API** (o) **Acceso de agentes**. Las restricciones de IP se pueden establecer en varios niveles y combinaciones, como rangos de IP definidos o direcciones IP individuales.

19.0 Privacidad

19.1 Controles de privacidad

Para aumentar la privacidad dentro del producto, Password Manager Pro le ayuda a personalizar y controlar la inclusión de datos personales en los procesos de generación de informes preconfigurados. Usted puede decidir si cada entrada de datos personales en Password Manager Pro debe ir como entradas ocultas en los informes o se deben eliminar por completo de ellos al ir a **Administrador >> Ajustes >> Ajustes de privacidad >> Controles de privacidad**. Le recomendamos ocultar o eliminar datos altamente confidenciales mientras genera informes.

19.2 Exportaciones codificadas

Con el fin de tener una capa adicional de seguridad para todas las operaciones de exportación en Password Manager Pro, le sugerimos habilitar la codificación de archivos exportados al ir a **Administrador >> Ajustes >> Ajustes de privacidad>> Exportaciones codificadas**. Usted puede establecer una frase de contraseña global que se usará uniformemente para todas las operaciones de exportación o permita que los usuarios definan su propia frase de contraseña global para sus archivos exportados. Los usuarios necesitarán dar su frase de contraseña para ver el archivo exportado.