ManageEngine
Password Manager Pro

Guía del usuario final

Diseñada para usuarios y auditores de contraseñas.

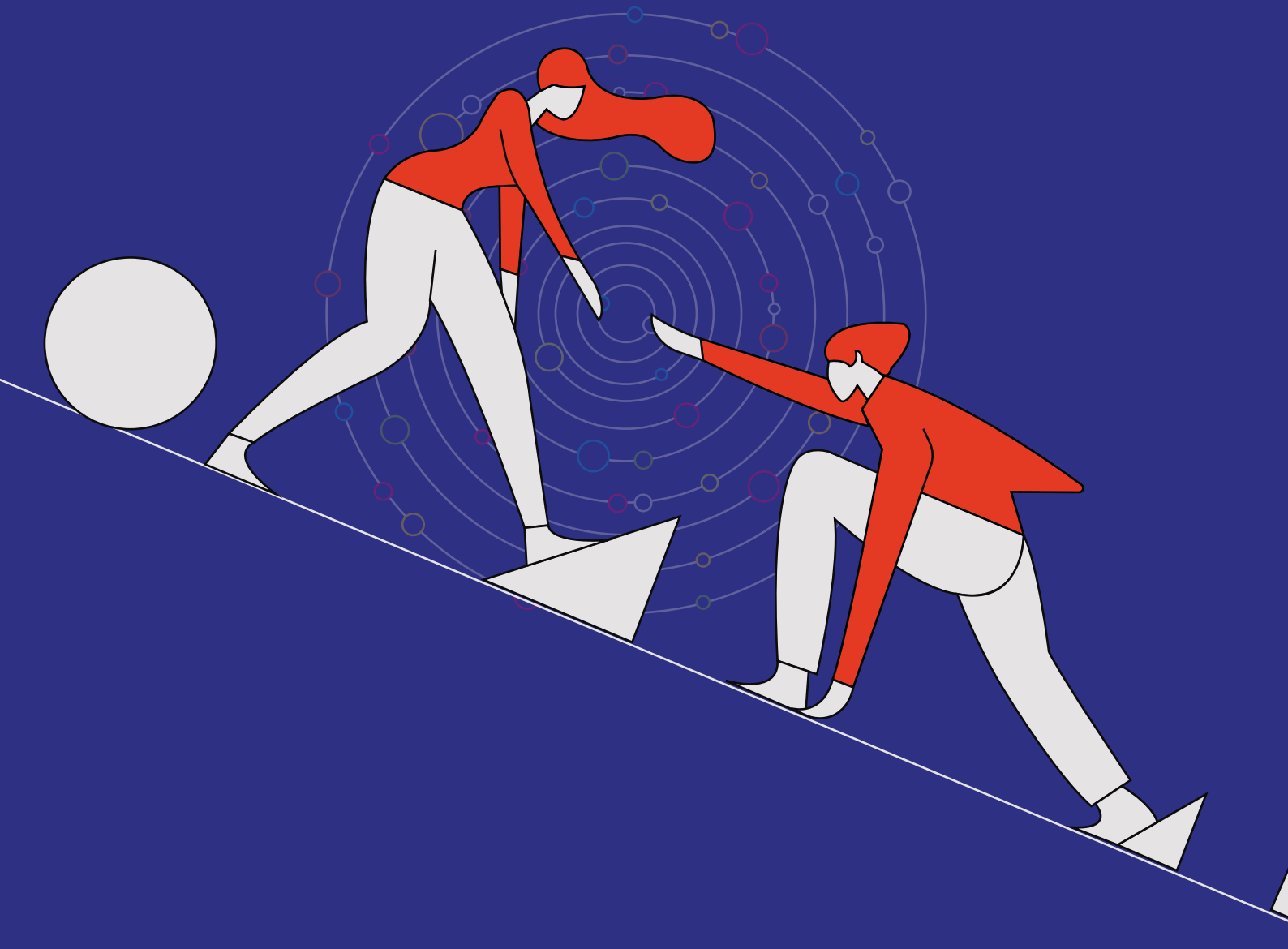


TABLA DE CONTENIDO

Acerca de Password Manager Pro

ManageEngine Password Manager Pro es una solución integral de gestión de cuentas privilegiadas que ayuda a las organizaciones a consolidar las identidades privilegiadas en un repositorio seguro y centralizado. Las credenciales de cualquier activo de TI sensible, como servidores, equipos de red, aplicaciones web, dispositivos virtuales y cuentas de SaaS (incluyendo certificados y otros archivos digitales) se pueden almacenar y gestionar a través de Password Manager Pro.

Esta solución también permite establecer conexiones directas RDP, SSH y SQL a los sistemas remotos a través de un gateway de sesión cifrado para garantizar la máxima seguridad. Sus funciones de auditoría exhaustivas también supervisan quién ha accedido a qué y cuándo, garantizando así la transparencia en un entorno multiusuario.

Acerca de esta guía

Esta guía ha sido diseñada como un material informativo para los usuarios finales de Password Manager Pro, es decir, los usuarios con los siguientes roles:

1. Usuarios de contraseñas
2. Auditores de contraseñas
3. Roles personalizados con los mismos privilegios que los usuarios de contraseñas y los auditores de contraseñas.

Esta guía destaca qué operaciones pueden realizar los usuarios finales en Password Manager Pro, a qué módulos y funciones tendrán acceso y cómo pueden utilizar la solución para gestionar cuentas privilegiadas de forma segura, así como para gestionar contraseñas personales.

Si usted es un **Usuario de Contraseñas**, tendrá acceso a las siguientes pestañas en la interfaz web de Password Manager Pro:

1. Recursos: Aquí encontrará todos los recursos y las cuentas correspondientes que su administrador ha compartido con usted.
2. Conexiones: A través de esta pestaña, puede establecer conexiones remotas (RDP, VNC, SSH, SQL) a los sistemas de destino utilizando las credenciales compartidas.
3. Personal: La pestaña Personal le permite almacenar sus datos personales como números de tarjetas de crédito, información de cuentas bancarias, direcciones de contacto, números de teléfono, direcciones de correo electrónico, etc. También puede protegerlos con una frase de contraseña exclusiva a la que sólo usted tendrá acceso.

Si usted es un **Auditor de Contraseñas**, además de las pestañas mencionadas, también tendrá acceso a las siguientes pestañas:

4. Dashboard: Esta pestaña ofrece un resumen general de todas las actividades relacionadas con las contraseñas y los usuarios en forma de tablas y gráficos.
5. Auditoría: Obtenga un registro completo de quién accedió a qué recurso y en qué momento, junto con pistas de auditoría de cada acción que los usuarios realizan dentro de la aplicación. Con base en su rol, esta pestaña le permite auditar todas las actividades privilegiadas realizadas en recursos, grupos de recursos, cuentas, contraseñas, certificados, tareas programadas y políticas en Password Manager Pro.

6. Informes: Esta pestaña le ayuda a generar informes intuitivos sobre las operaciones relacionadas con las contraseñas y los usuarios que puede utilizar para mejorar la gestión de los datos privilegiados en su organización. Además de los informes integrados, puede filtrar la información de la base de datos de Password Manager Pro como informes personalizados.

Qué tan protegidas están sus credenciales en Password Manager Pro.

El mecanismo de bóveda de Password Manager Pro ofrece una completa defensa contra las intrusiones con las siguientes medidas:

- Los datos sensibles, como las contraseñas y las claves, se someten a una doble encriptación; es decir, se encriptan una vez en la aplicación utilizando AES-256 y otra vez en la base de datos.
- Todas sus contraseñas personales que se almacenan en Password Manager Pro también se encriptan. Para mejorar aún más la seguridad, su administrador también puede exigirle que cree una frase de contraseña segura para acceder a sus contraseñas personales.
- La autenticación de usuario basada en roles y granular garantiza que los usuarios puedan ver las contraseñas únicamente con base en la autorización que se les haya proporcionado.
- Todas las transacciones a través del navegador de Password Manager Pro se realizan a través de HTTPS.

Consulte nuestro documento de Especificaciones de Seguridad para obtener más detalles sobre las medidas de seguridad que utiliza Password Manager Pro.

Terminología relevante

Consulte la siguiente tabla para consultar las explicaciones sobre los distintos términos utilizados en esta guía.

Término	Definición
Recurso	Cualquier servidor/aplicación/dispositivo cuyos nombres de usuario y contraseñas serán gestionados por Password Manager Pro.
Grupo de recursos	Grupo conformado por recursos similares. Por ej, si tiene varios recursos Windows XP entre varios servidores Windows, puede agrupar todos los servidores Windows XP en un único grupo de recursos.
Cuenta	La cuenta de usuario y la contraseña correspondiente que será gestionada por Password Manager Pro.
Sistema remoto	Un sistema remoto es un dispositivo, aplicación o servidor al que no tiene acceso físico, pero al que puede acceder o manipular a través de una red.

1. Conectarse a la interfaz web de Password Manager Pro

Abra un navegador y vaya a **https://<nombre de host>:puerto** (pero con su nombre de host en lugar de *nombre de host* y su número de puerto en lugar de *puerto*). Como la conexión es a través de HTTPS, los datos que se comunican por este canal son seguros. Si dispone de un certificado adecuado, la consola web le llevará a la página de autenticación al instante. Por otro lado, si utiliza un certificado autofirmado, aparecerá un mensaje de advertencia sobre la seguridad del certificado, que tendrá que aceptar para seguir a la página de autenticación.

2. Iniciar sesión en Password Manager Pro

En la página de autenticación, inicie sesión en Password Manager Pro ingresando sus credenciales. Puede hacerlo a través de la autenticación local de Password Manager Pro, o utilizando credenciales de AD, LDAP, RADIUS o Smartcard, cualquiera que sea la opción configurada por su administrador.

Si su cuenta tiene configurada la autenticación local, póngase en contacto con su administrador para obtener las credenciales. Si su administrador le exige la autenticación de dos factores, tendrá que autenticarse con un segundo método para acceder a la interfaz web de Password Manager Pro. El segundo nivel de autenticación puede ser a través de cualquiera de los siguientes métodos según lo establecido por su administrador:

- Autenticación con PhoneFactor
- Autenticación con RSA SecurID
- Google Authenticator
- Microsoft Authenticator
- Okta Verify Authenticator
- Servidor RADIUS o cualquier autenticación compatible con RADIUS
- Autenticación con Duo Security
- Autenticación con YubiKey
- Contraseña única enviada por correo electrónico

> **Nota:** *Los usuarios que no tengan activada la autenticación de dos factores podrán iniciar sesión en Password Manager Pro si completan el primer nivel de autenticación.*

3. Recursos

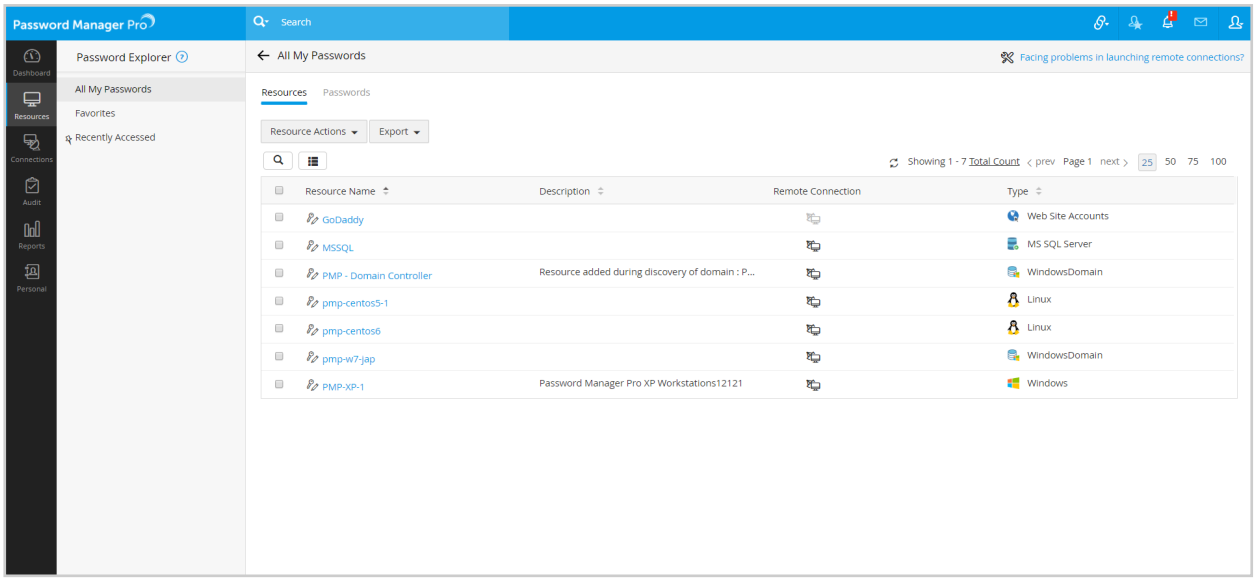
Puede ver todos los recursos que los administradores han compartido con usted, así como los detalles de la cuenta correspondiente, en la pestaña *Recursos*. El menú *Explorador de contraseñas* muestra lo siguiente:

A. Todas mis contraseñas
B. Favoritos
C. Accedidos recientemente
D. Árbol del explorador de contraseñas

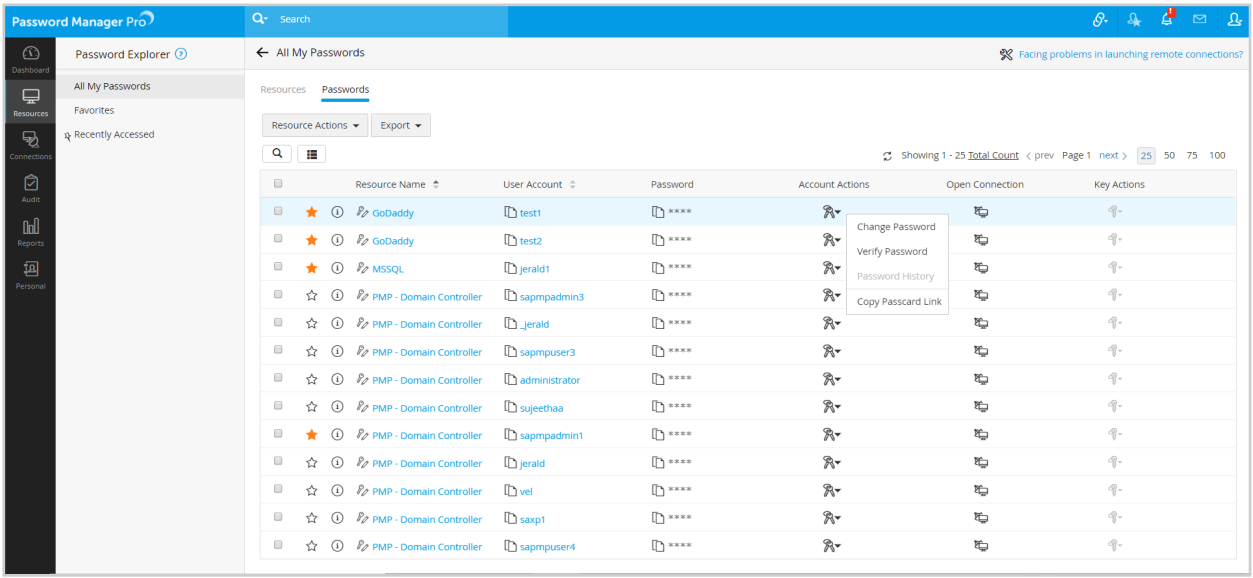
A. Todas mis contraseñas

En esta pestaña, puede encontrar todos los recursos que se comparten con usted, las cuentas correspondientes bajo esos recursos y sus respectivas contraseñas/claves SSH (enmascaradas con asteriscos).

- La pestaña *Recursos*, situada en la parte superior, muestra los detalles de los recursos. Desde aquí, puede realizar operaciones basadas en los recursos. Puede hacer clic en cualquier recurso de la lista para encontrar sus cuentas y las contraseñas correspondientes.



- En la pestaña *Contraseñas*, puede encontrar los recursos y las cuentas compartidas con usted junto con sus respectivas contraseñas. En el menú desplegable *Acciones de la cuenta*, también puede realizar operaciones para la cuenta, como cambiar y verificar las contraseñas y ver el historial de contraseñas.



Nota: *Podrá ver y/o cambiar las contraseñas según el nivel de acceso que le haya proporcionado el propietario del recurso.*

Operaciones que puede realizar en la pestaña Recursos

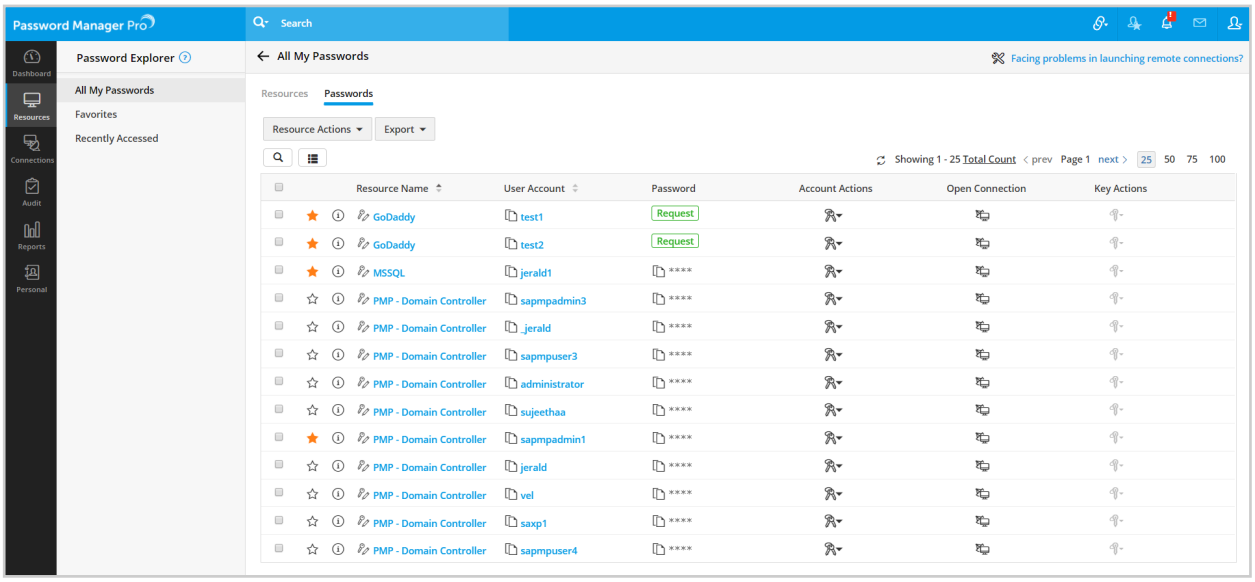
En la pestaña *Recursos*, puede realizar varias acciones como recuperar y copiar contraseñas, exportar contraseñas, buscar una contraseña específica o establecer una conexión remota al sistema de destino.

Recuperar contraseñas

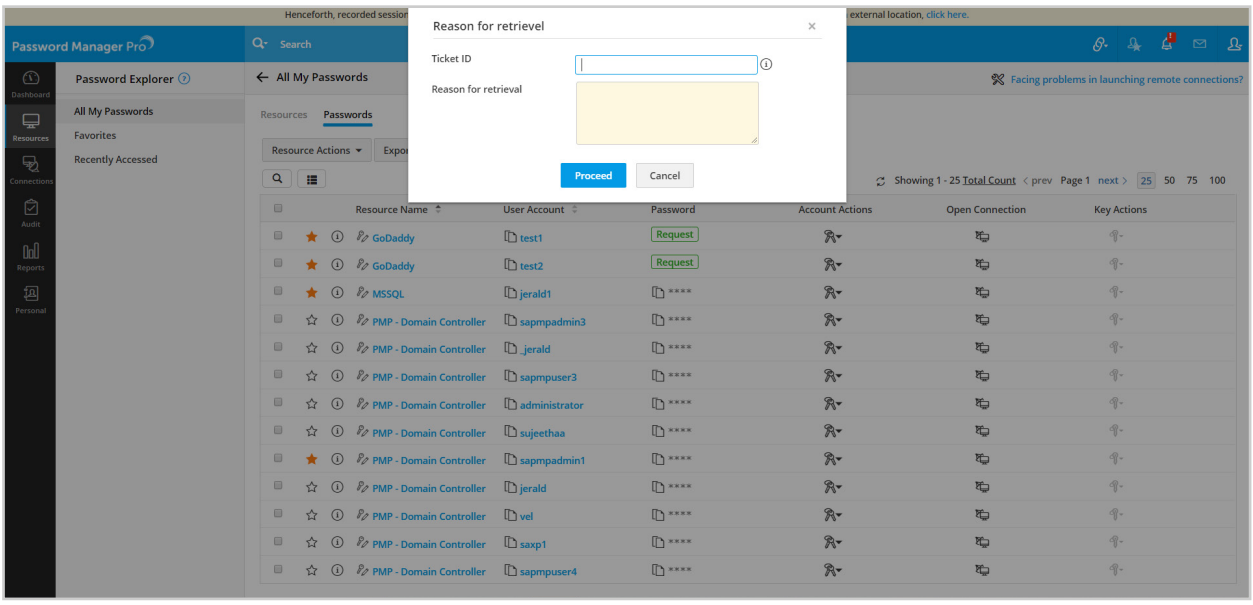
Caso 1: Ver las contraseñas haciendo clic en los asteriscos. Por defecto, las contraseñas están ocultas y se muestran como asteriscos. Si su administrador no ha configurado ninguna restricción para recuperar las contraseñas, puede simplemente hacer clic en los asteriscos para ver las contraseñas en texto plano.

Caso 2: Recuperar contraseñas proporcionando una razón válida. En este caso, cuando intente ver, copiar o modificar las contraseñas, se le pedirá que proporcione una razón para hacerlo. Una vez que proporcione una razón válida, las contraseñas estarán disponibles hasta el momento que determine su administrador.

Caso 3: Flujo de trabajo para el control de acceso. Hay casos en los que su administrador puede aplicar el control de acceso a determinados recursos. En tales circunstancias, Password Manager Pro le pedirá que presente una solicitud a su administrador cuando necesite acceder a las cuentas de esos recursos. Los recursos que tienen el control de acceso habilitado mostrarán un botón de Solicitar como se muestra en la siguiente imagen. Una vez que el administrador autorizado revise y apruebe su solicitud, podrá acceder a las credenciales durante un período de tiempo específico según lo dispuesto por el administrador.



Caso 4: Recuperar contraseñas proporcionando un ID de ticket válido. Si su organización gestiona todas sus operaciones privilegiadas (como el restablecimiento de contraseñas del sistema, la asistencia técnica remota y la resolución de problemas) a través de un sistema de tickets, su administrador podría habilitar este sistema dentro de Password Manager Pro. Esto requerirá que proporcione un ID de ticket válido o los detalles del ticket correspondiente cada vez que necesite acceder a las credenciales privilegiadas almacenadas en Password Manager Pro.



Copiar contraseñas

Puede copiar directamente las contraseñas haciendo clic en el icono de *Copiar* junto a los asteriscos para evitar exponer las credenciales en texto plano. Las contraseñas copiadas se guardarán en el portapapeles durante 30 segundos de forma predeterminada, pero esto varía según lo dispuesto por su administrador. También puede borrar manualmente el portapapeles haciendo clic en el icono de *Mi Perfil* en la esquina superior derecha y seleccionando *Borrar portapapeles* en el menú desplegable.

Exportar contraseñas para un acceso sin conexión seguro

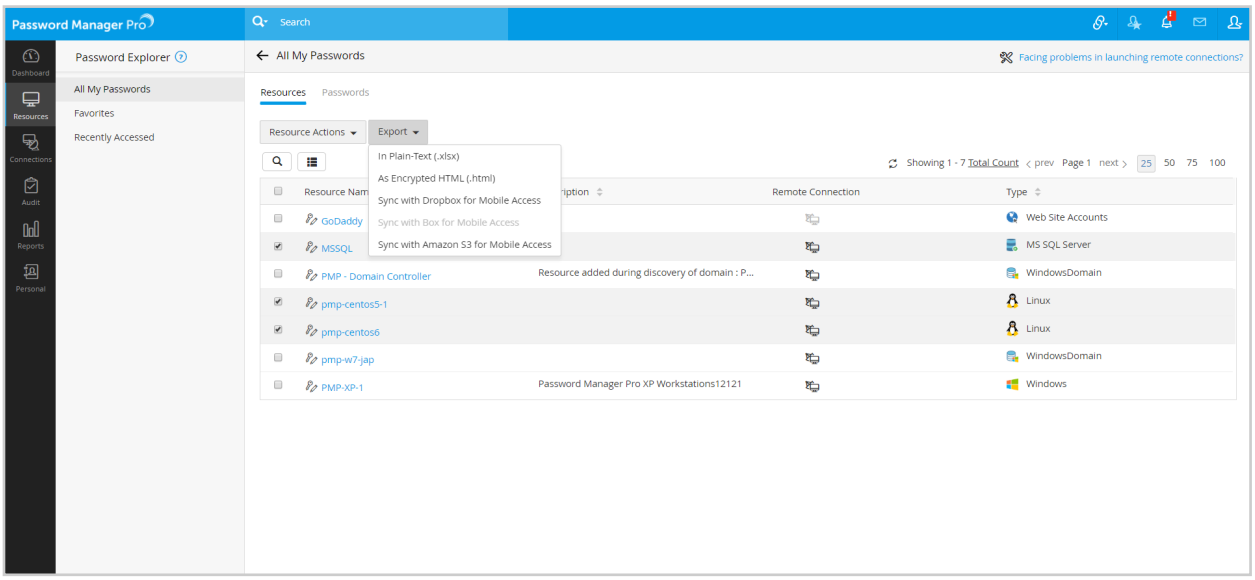
Password Manager Pro le permite exportar información como nombres de recursos, nombres de cuentas y contraseñas a través de diversas opciones para un acceso rápido y seguro sin conexión:

1. En texto plano (XLSX): Esta opción le permitirá exportar los detalles de los recursos en texto plano a una hoja de cálculo. Sin embargo, si su administrador deshabilita la opción para evitar que las contraseñas se impriman en texto plano, las contraseñas se enmascaran con asteriscos en la hoja de cálculo.

Descargo de responsabilidad: *Si su administrador habilita el cifrado para todas las operaciones de exportación en Password Manager Pro, el archivo Excel exportado estará protegido por contraseña. Tendrá que proporcionar la frase de contraseña de cifrado cada vez que necesite acceder a él.*
Si el administrador configura una frase de contraseña global para las operaciones de exportación, puede recuperar la frase de contraseña haciendo clic en el icono Mi perfil en la esquina superior derecha y seleccionando Ajustes de exportación en el menú desplegable. En algunos casos el administrador le permite utilizar la frase de contraseña global o establecer una exclusiva para sus operaciones de exportación. Si prefiere utilizar su propia frase de acceso, puede establecerla en la ventana de Ajustes de exportación.

2. As an encrypted HTML file (HTML): Puede exportar sus contraseñas como un archivo HTML para acceder sin conexión. Este archivo se encriptará utilizando el algoritmo AES-256 bits con una frase de contraseña que se proporciona al exportar. Puede abrir este archivo en cualquier navegador web y acceder a las contraseñas después de proporcionar la frase de contraseña.

Password Manager Pro no almacena esta frase de contraseña en ningún sitio y le recomendamos que tampoco la almacene en ningún sitio. El archivo HTML no se puede abrir sin la frase de contraseña. En caso de que olvide la frase de contraseña, elimine inmediatamente el archivo HTML correspondiente y luego exporte un nuevo archivo.



3. Sincronizar con Dropbox para el acceso móvil: Password Manager Pro le permite exportar las contraseñas de un recurso compartido a un archivo cifrado y sincronizarlo automáticamente con su cuenta de Dropbox. Si el administrador habilita esta opción, la encontrará en el menú desplegable *Exportar*. Al hacer clic, será redirigido al servicio de Dropbox. Inicie sesión en su cuenta de Dropbox, autorice a Password Manager Pro y podrá cargar el archivo exportado que contiene las contraseñas en su cuenta de Dropbox.

4. Sincronizar con Box para el acceso móvil: Al igual que en Dropbox, puede exportar las contraseñas requeridas a un archivo HTML cifrado y sincronizarlo con su cuenta de Box para un rápido acceso sin conexión. Una vez que elija la opción en el menú desplegable *Exportar*, se le pedirá que inicie sesión en su cuenta de Box y autorice a Password Manager Pro para cargar el archivo exportado que contiene las contraseñas en su cuenta de Box.

5. Sincronizar con Amazon S3 para el acceso móvil: También hay una opción para exportar las contraseñas a un archivo HTML cifrado y sincronizarlo automáticamente con su cuenta de Amazon S3. Después de seleccionar esta opción, Password Manager Pro le pedirá que introduzca su ID de clave de acceso, la clave de acceso secreta y el nombre del bucket para sincronizar Password Manager Pro con su cuenta de Amazon S3.

Buscar

Esta función le permite encontrar un recurso o una cuenta en particular proporcionando los detalles en las columnas respectivas.

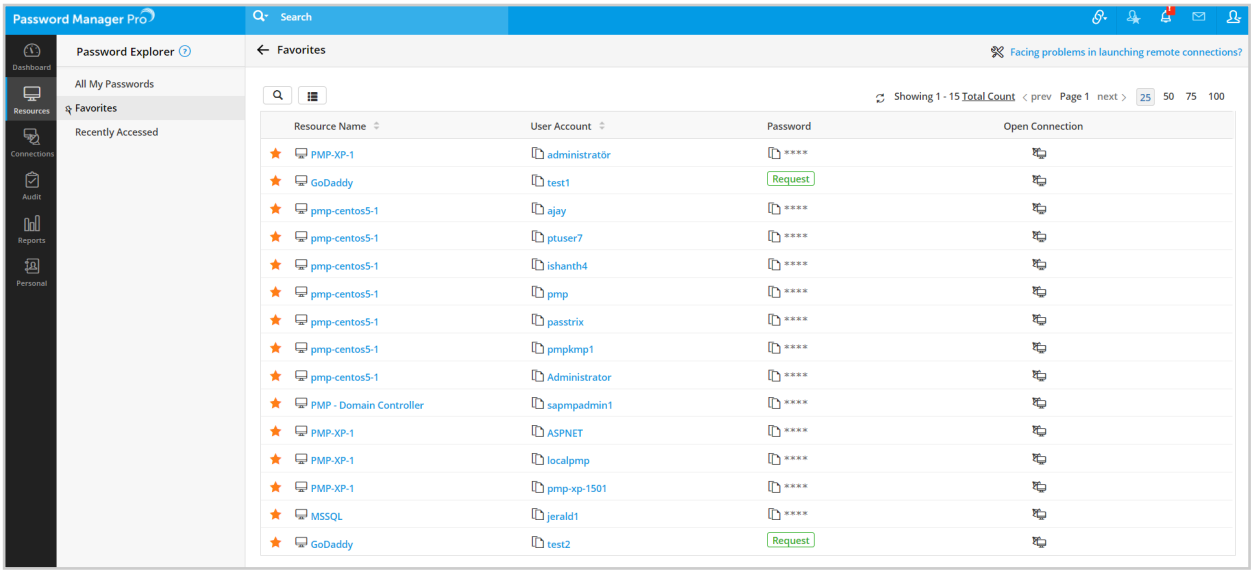
Selector de columnas

El icono de *Lista* le permite definir las columnas que desea tener en las secciones *Recursos* y *Contraseñas*.

B. Favoritos

Esta opción le permite acceder rápidamente a la lista de todas las contraseñas que ha marcado como favoritas. Marcar una contraseña como favorita le ayudará a localizar un recurso específico y la contraseña asociada fácilmente, de modo que no necesite desplazarse por toda la lista cada vez que lo requiera. Para marcar una contraseña como favorita, simplemente haga clic en el icono de la estrella a la izquierda del recurso respectivo que aparece en *Todas mis contraseñas*.

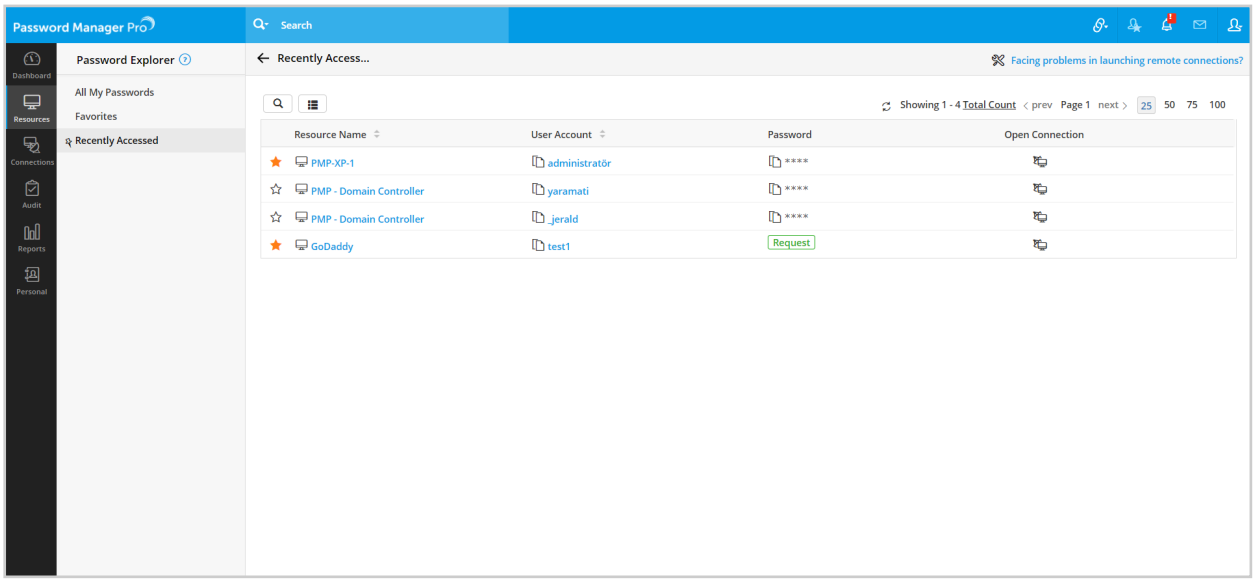
También puede utilizar el icono de *Búsqueda* en la parte superior para encontrar una contraseña específica de su lista de *Favoritos* y el icono *Selector de columnas* para definir las columnas que le gustaría ver en esta sección.



Nota: *Cuando un administrador le revoque el acceso a un recurso que haya marcado como favorito, el recurso se eliminará automáticamente de su lista de "Favoritos".*

C. Accesos recientes

- Esta sección le ayuda a ver la lista de recursos a los que se ha accedido recientemente y sus contraseñas.



- También puede utilizar el icono de Búsqueda de la parte superior para buscar un recurso o una cuenta específica en la lista de *Accesos recientes*. A continuación, puede definir las columnas que le gustaría ver en esta sección utilizando el *Selector de columnas*.

D. Árbol del explorador de contraseñas

Password Manager Pro proporciona una opción para ver todos los grupos de recursos creados por los administradores en una estructura jerárquica, es decir, la vista de árbol. En el *Árbol del explorador de contraseñas*, encontrará los grupos de recursos y subgrupos que su administrador ha compartido con usted. Esta estructura de árbol representa los grupos de recursos de su organización para facilitar el acceso, la identificación y la navegación. Puede ver los grupos de recursos en la misma estructura que la de la agrupación interna de su organización. Sin embargo, sólo podrá ver los recursos que se comparten con usted; los grupos de recursos que no se comparten con usted se mostrarán como subnodos vacíos (sin ningún recurso dentro) en el árbol del explorador.

4. Conexiones

La pestaña *Conexiones* le permite conectarse de forma segura a servidores y sistemas remotos directamente desde la interfaz de Password Manager Pro a través de un gateway de sesión cifrada. Actualmente, puede iniciar sesiones RDP, VNC, SSH y SQL. A continuación se muestra un resumen general de cómo el administrador le proporciona funciones RDP para un recurso de Windows:

- El administrador añade un recurso Windows y sus respectivas cuentas en Password Manager Pro.
- A continuación, configura el inicio de sesión automático para el recurso de Windows.
- Por último, comparte el recurso con usted.
- Ahora, el recurso se muestra automáticamente en las pestañas Recursos y Conexiones, permitiéndole establecer conexiones RDP al recurso.

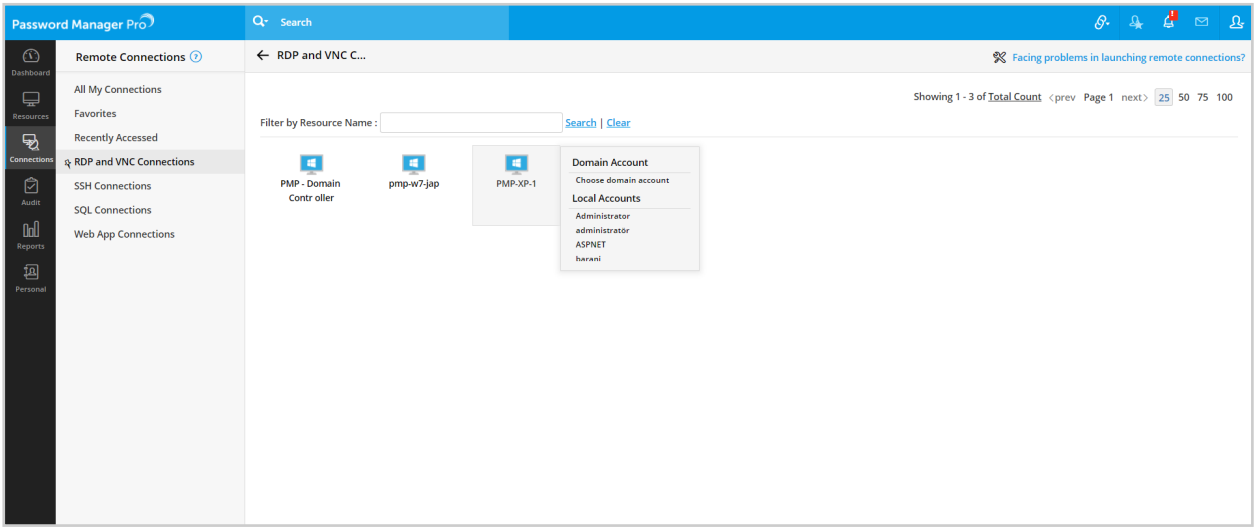
Nota: *Para garantizar la máxima seguridad, Password Manager Pro también permite a los administradores deshabilitar la recuperación de contraseñas por parte de los usuarios para los recursos que admiten el inicio de sesión automático. En estos casos, podrá conectarse directamente al recurso remoto con un solo clic, pero no podrá acceder al nombre de usuario y la contraseña de la cuenta del recurso correspondiente.*

Pasos para iniciar conexiones remotas utilizando el inicio de sesión automático:

1. Conexiones RDP y VNC

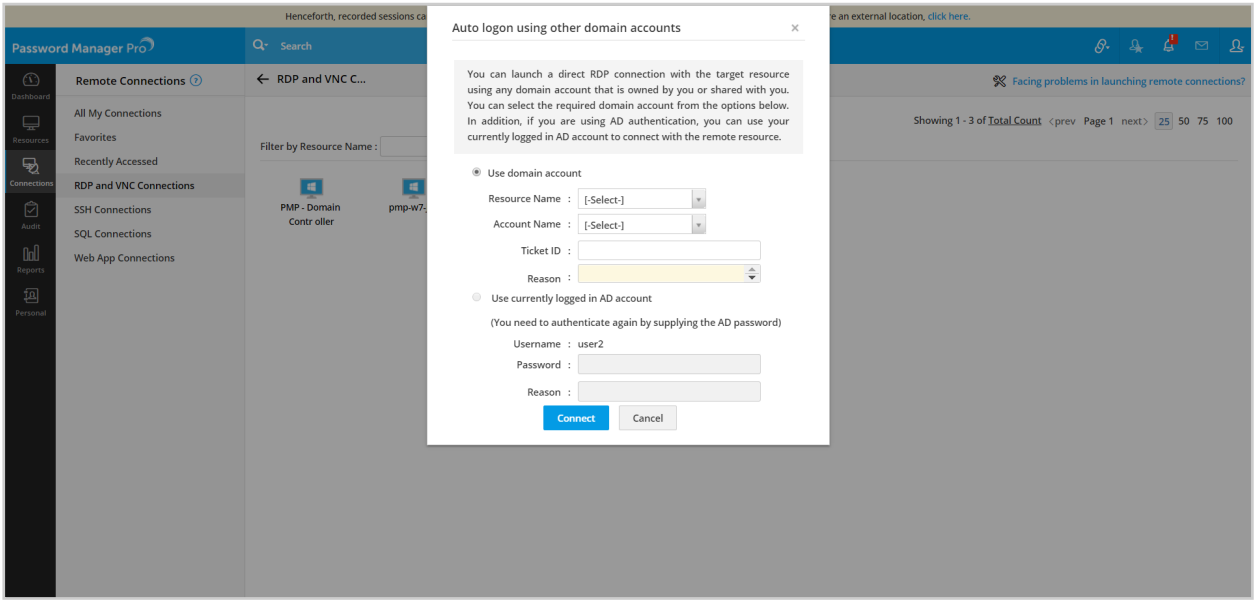
Vaya a **Conexiones** > **Conexiones RDP y VNC** y mueva el cursor sobre el recurso Windows deseado. Para una conexión RDP, normalmente tiene tres opciones:

1. Conectarse usando una cuenta local: Esta es la opción predeterminada. Al delegarle los respectivos recursos de Windows, el administrador le compartirá al menos una de las cuentas locales del recurso. Puede encontrar la cuenta compartida en *Cuentas locales* en el menú que aparece al mover el cursor. Al hacer clic en la cuenta se iniciará inmediatamente la conexión RDP.



2. Conectarse usando una cuenta de dominio: Si su administrador le comparte una cuenta de dominio, seleccione *Elegir cuenta de dominio* en el menú que aparece al mover el cursor. En la ventana que se abre, seleccione la opción *Usar cuenta de dominio* y luego proporcione el nombre del recurso de dominio y el nombre de la cuenta. Luego de añadir el motivo por el que se utiliza una cuenta de dominio para la conexión RDP, haga clic en *Conectar*.

3. Conectarse usando su cuenta de AD: Si inicia sesión en Password Manager Pro a través de la autenticación con AD/LDAP, puede utilizar esas credenciales para conectarse con un recurso remoto a través de RDP. Mueva el cursor por encima del recurso, haga clic en *Elegir cuenta de dominio* y seleccione la opción *Utilizar la cuenta de AD activa* en la nueva ventana. Proporcione su contraseña de AD y la razón para iniciar la conexión, y haga clic en *Conectar*.



En el caso de las conexiones VNC, la opción *Conectar a través de VNC* se mostrará en la parte superior del menú que aparece al mover el cursor sobre el recurso si su administrador ha habilitado esta función.

2. Conexiones SSH

Esta opción le permite conectarse automáticamente a cualquier dispositivo basado en SSH que se comparta con usted, como un servidor Linux o un dispositivo de red a través de una sesión SSH remota. Vaya a **Conexiones > Conexiones SSH** y mueva el cursor sobre el recurso deseado. Para una conexión SSH, normalmente tiene tres opciones:

1. Conectarse usando una cuenta local: Esta es la opción predeterminada. Al delegarle los respectivos recursos, el administrador le compartirá al menos una de las cuentas locales del recurso. Puede encontrar la cuenta compartida en *Cuentas locales* en el menú que aparece al mover el cursor. Al hacer clic en la cuenta se iniciará inmediatamente la conexión SSH.

2. Conectarse usando una cuenta de dominio de Windows: Password Manager Pro le permite iniciar una sesión de terminal remota SSH utilizando cualquiera de las cuentas de dominio de Windows almacenadas en su base de datos. Si su administrador le comparte una cuenta de dominio de Windows, seleccione *Elegir cuenta de dominio* en el menú que aparece al mover el cursor. En la ventana que se abre, seleccione el nombre del recurso de dominio y el nombre de la cuenta. Luego de añadir el motivo por el que se utiliza una cuenta de dominio para la conexión SSH, haga clic en *Conectar*.

3. Conectarse usando su cuenta de AD: Si inicia sesión en Password Manager Pro a través de la autenticación con AD/LDAP, puede utilizar esas credenciales para conectarse con un recurso remoto a través de una sesión SSH. Mueva el cursor por encima del recurso, haga clic en *Elegir cuenta de dominio* y seleccione la opción *Utilizar la cuenta de AD activa* en la nueva ventana. Proporcione su contraseña de AD y la razón para iniciar la conexión, y haga clic en *Conectar*.

3. Conexiones SQL

Puede conectarse automáticamente a una instancia de base de datos desde Password Manager Pro a través de una conexión SQL remota. Esta función es compatible con las bases de datos MySQL, PostgreSQL, MS SQL, Sybase ASE y Oracle DB Server. Para iniciar una sesión SQL, haga clic en **Conexiones SQL** en la pestaña *Conexiones*, mueva el cursor por encima del recurso necesario y haga clic en la cuenta local compartida. Tenga en cuenta que las conexiones SQL están basadas en la CLI; permiten ejecutar consultas para realizar operaciones.

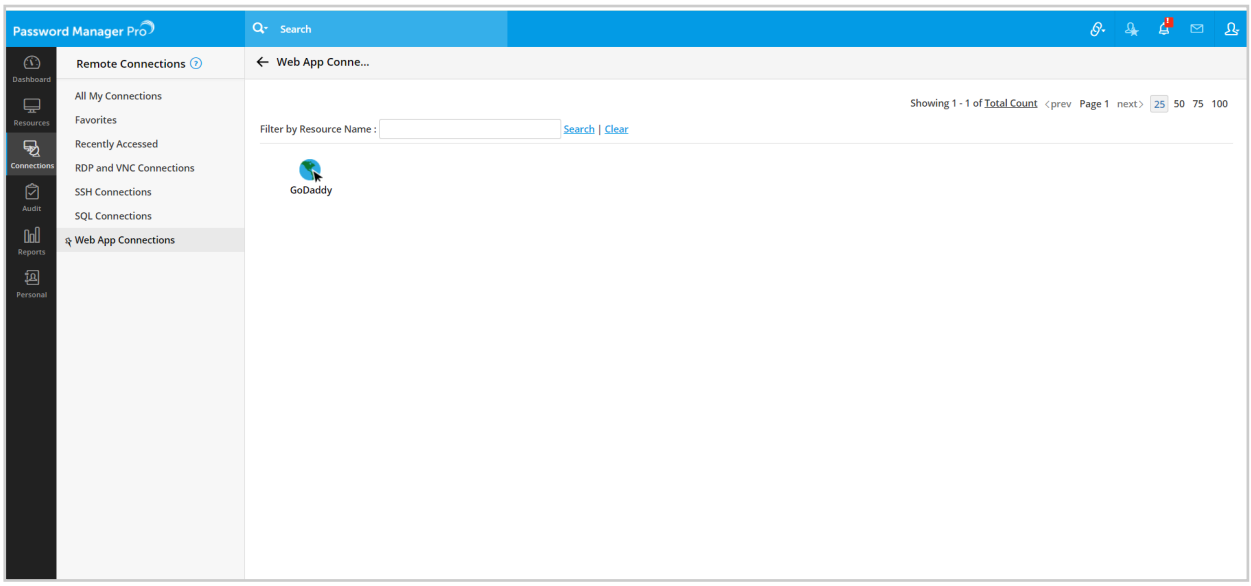
1. Conectarse a servidores de bases de datos utilizando su cuenta local: Para iniciar una conexión remota a un servidor de base de datos, puede elegir cualquiera de sus cuentas locales compartidas. Puede encontrar la cuenta compartida en *Cuentas locales* en el menú que aparece al mover el cursor. Al hacer clic en la cuenta se iniciará inmediatamente la sesión SQL.

2. Conectarse a un servidor MS SQL utilizando una cuenta de dominio de Windows: Password Manager Pro le permite conectarse a servidores MS SQL utilizando cualquiera de las cuentas de dominio de Windows almacenadas en su base de datos. Si su administrador le comparte una cuenta de dominio de Windows, seleccione *Elegir cuenta de dominio* en el menú que aparece al mover el cursor sobre el recurso. En la ventana que se abre, seleccione el nombre del recurso de dominio y el nombre de la cuenta en la opción *Usar cuenta de dominio*. Luego de añadir el motivo por el que se utiliza una cuenta de dominio para la conexión SQL, haga clic en *Conectar*. Tenga en cuenta que esta función no estará disponible para otros servidores de bases de datos, ya que no están integrados con AD.

3. Conectarse a un servidor MS SQL utilizando su cuenta de AD: También puede conectarse a un servidor MS SQL utilizando sus credenciales de AD/LDAP, siempre que haya iniciado sesión en Password Manager Pro mediante la autenticación con AD/LDAP. Para ello, haga clic en *Elegir cuenta de dominio* en el menú que aparece a mover el cursor sobre el recurso y proporcione sus credenciales de AD en la opción *Usar la cuenta de AD activa*. Después de proporcionar una razón válida, haga clic en *Conectar*. Tenga en cuenta que esta función no estará disponible para otros servidores de bases de datos, ya que no son compatibles con la autenticación de AD.

4. Conexiones a aplicaciones web

Puede iniciar conexiones directas a sitios web o aplicaciones web (ejemplos: GoDaddy, Slack, YellowPages, Evernote, etc.) que su administrador añade como recursos y comparte con usted. Para conectarse a un recurso basado en la web directamente desde Password Manager Pro, vaya a **Conexiones > Conexiones a aplicaciones web** y haga clic en la aplicación web requerida. Esto abrirá la aplicación en una nueva pestaña y se conectará automáticamente a ella.

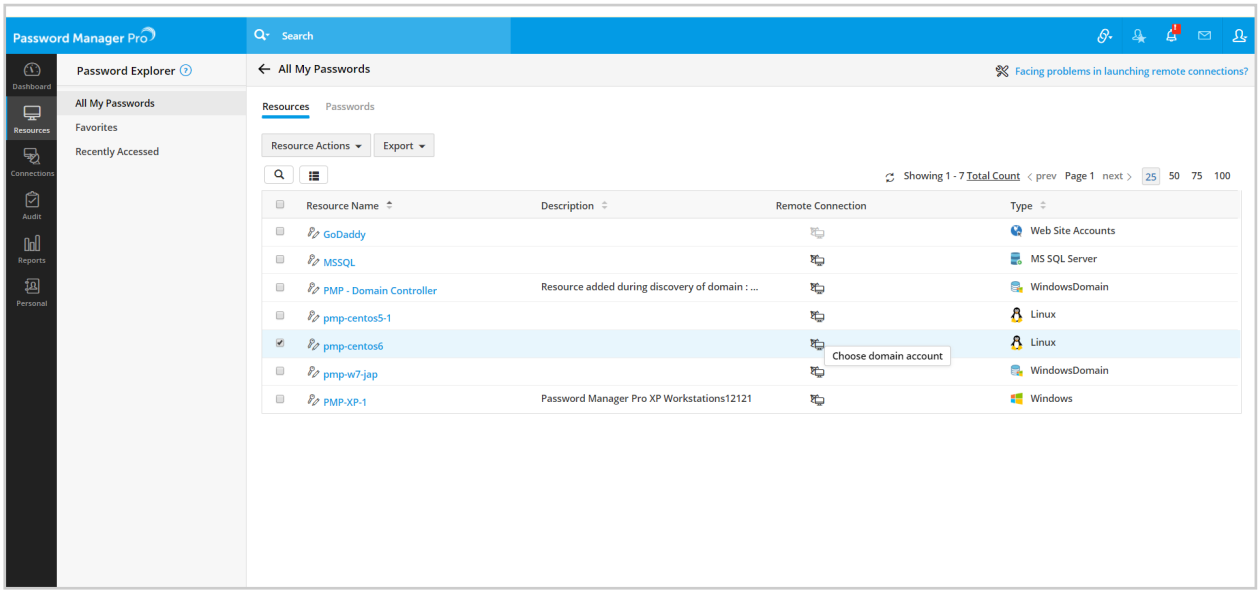


Nota: *Esta función sólo funcionará si ha instalado alguna de las extensiones de navegador disponibles de Password Manager Pro, ya que Password Manager Pro utiliza la función de completar automáticamente de los navegadores para iniciar sesión automáticamente en los respectivos sitios web y aplicaciones.*

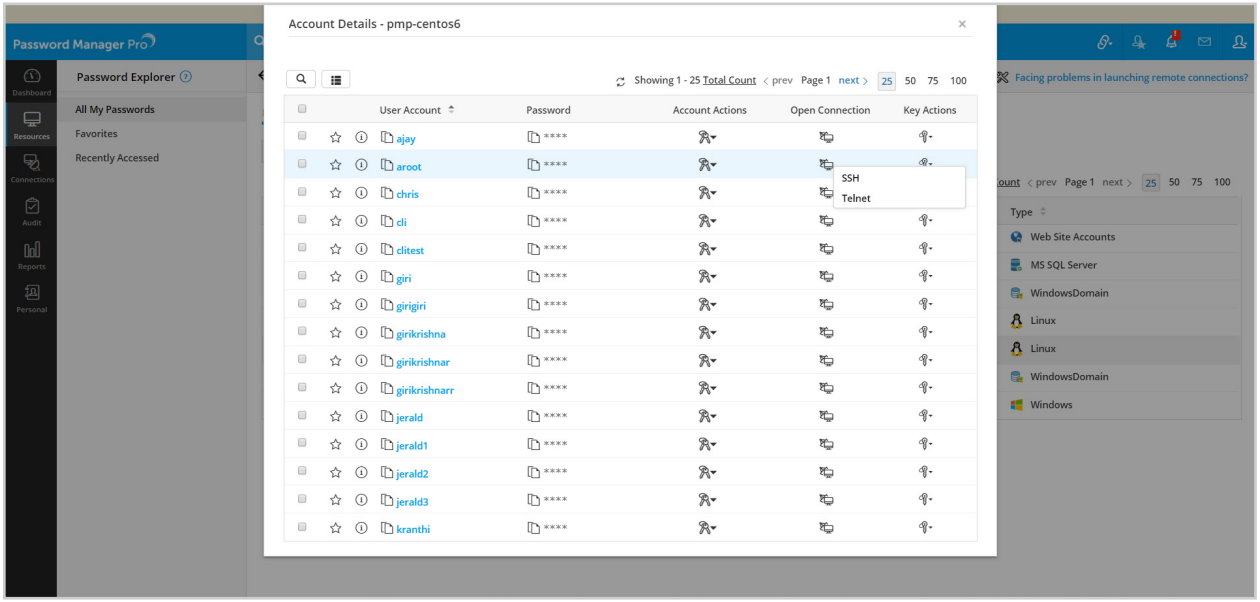
Iniciar conexiones remotas desde la pestaña Recursos

Además de la pestaña *Conexiones*, también puede establecer conexiones directas RDP, SSH y SQL desde la pestaña *Recursos*.

- Vaya a la pestaña *Recursos*, haga clic en el icono de *Conexión remota* adyacente al recurso deseado y elija la opción de iniciar una conexión utilizando una cuenta de dominio que su administrador comparta con usted.

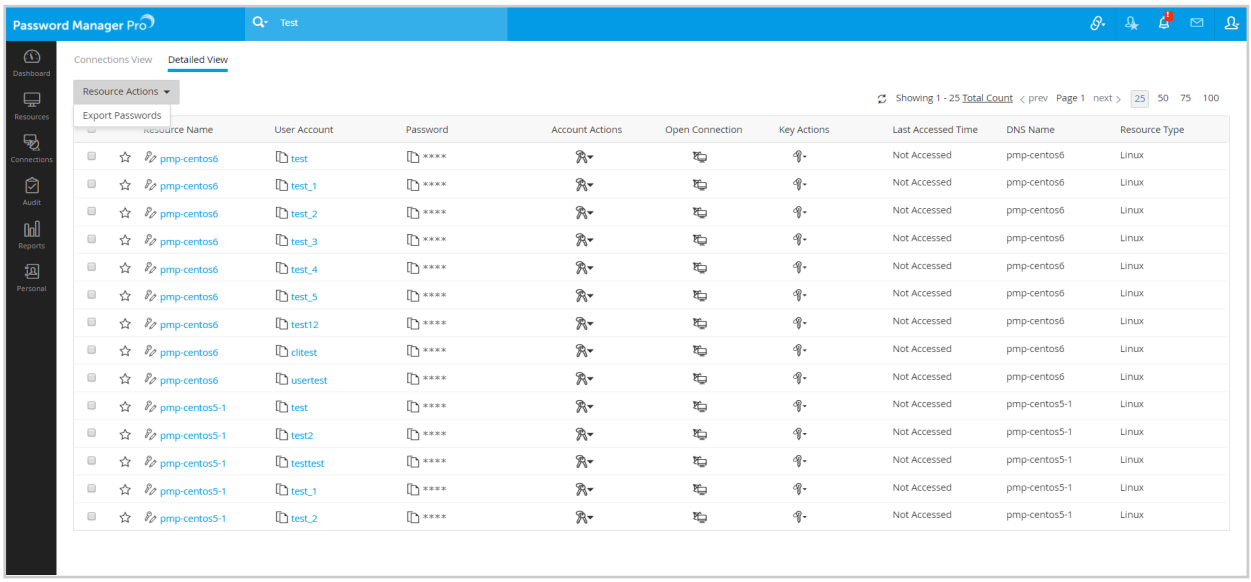


- En la ventana que se abre, proporcione el nombre del recurso de dominio y el nombre de la cuenta en la opción *Usar cuenta de dominio*, o proporcione sus credenciales de AD en la opción *Usar cuenta de AD activa*, si ha iniciado sesión en Password Manager Pro mediante la autenticación con AD/LDAP. Proporcione una razón válida para iniciar esta conexión y haga clic en *Conectar*.
- Si desea iniciar una conexión a través de cualquiera de las cuentas locales del recurso, haga clic en el recurso deseado para ver todas las cuentas locales respectivas que se comparten con usted. Haga clic en el icono de *Abrir conexión* junto a la cuenta local que desee utilizar y elija el modo de conexión deseado. A continuación, proporcione una razón y/o un ID de ticket para iniciar esta conexión, y haga clic en *Proceder*.



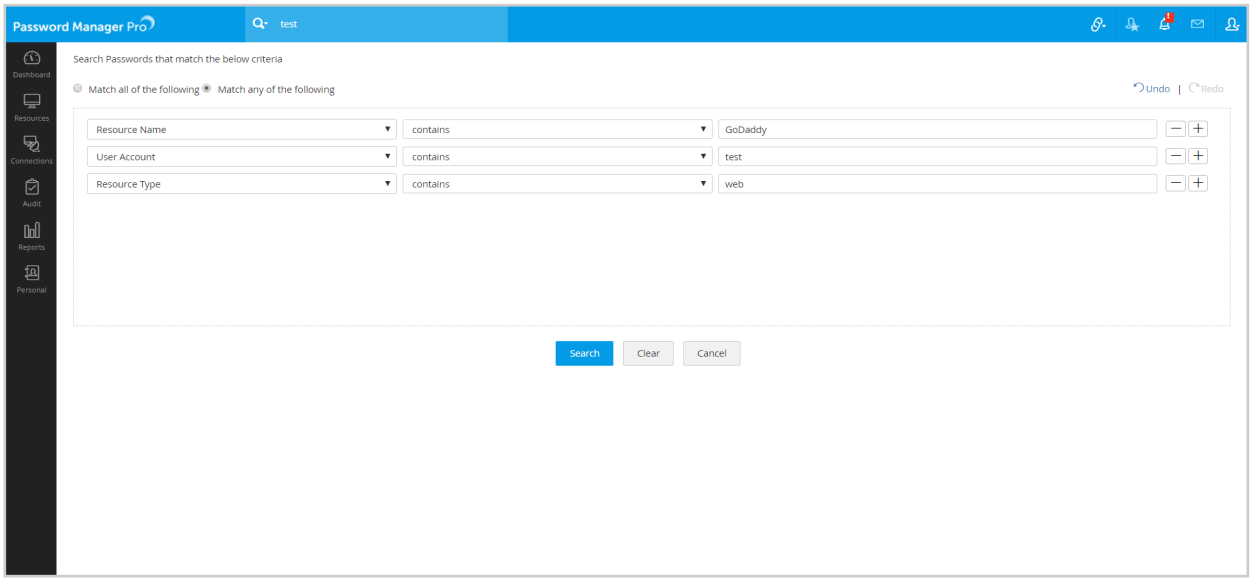
5. Búsqueda global

- El botón de búsqueda en la parte superior de la pantalla le permite buscar recursos, cuentas, etc. en Password Manager Pro.
- Ingrese una palabra clave válida y pulse *Intro*, o seleccione la opción deseada en el menú desplegable. Ambas opciones mostrarán las entradas resultantes en la sección *Vista detallada*.
- Seleccione *Exportar contraseñas* en el menú desplegable de *Acciones de los recursos* para exportar los datos a un archivo CSV según las políticas de exportación establecidas por su administrador. Tenga en cuenta que esta opción sólo estará disponible si su administrador habilita el acceso sin conexión para usted.
- Para cambiar una contraseña específica de la lista, haga clic en *Cambiar contraseña* en el menú desplegable *Acciones de la cuenta* proporcione una razón válida y/o el ID de ticket correspondiente, y haga clic en *Guardar*. Este menú también incluye opciones para verificar las contraseñas y ver el historial de contraseñas.



- La sección *Vista de conexiones* es similar a la pestaña *Conexiones*, excepto que sólo muestra los recursos de los resultados de la búsqueda.

Búsqueda avanzada: Esta opción disponible en el menú desplegable *Búsqueda* le permite definir sus propios criterios para obtener las contraseñas necesarias que coincidan con todos o alguno de los criterios especificados



Nota: *Sus contraseñas personales no se incluirán en los resultados de la búsqueda.*

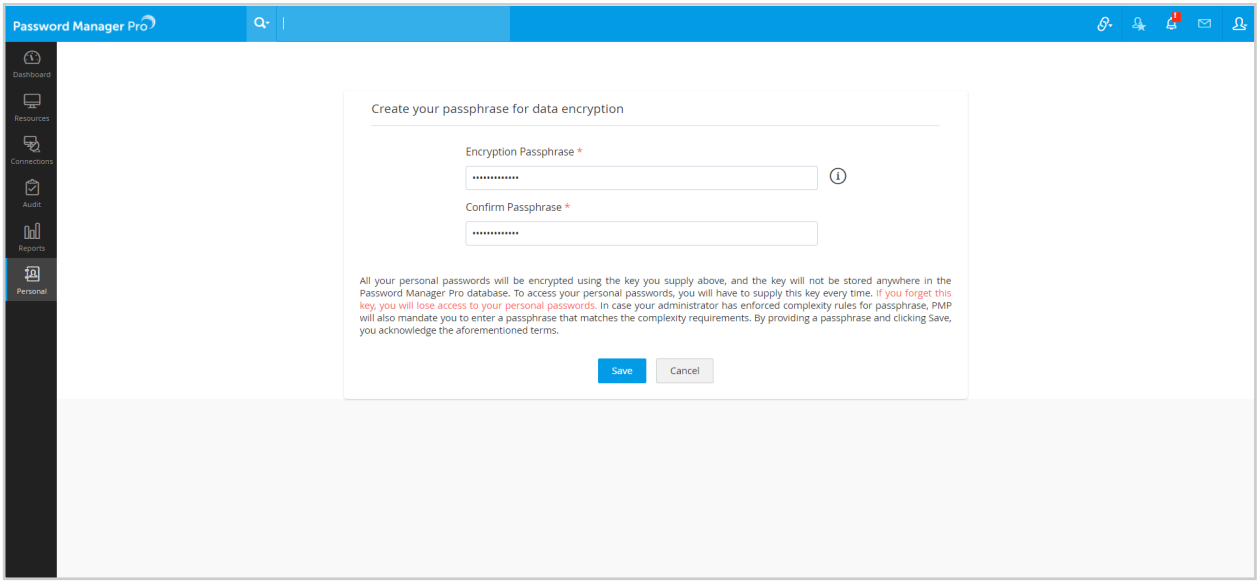
6. Personal

Tendrá acceso a la pestaña *Personal* sólo si su administrador habilita la opción para permitirle almacenar sus contraseñas personales en Password Manager Pro. Si tiene acceso a esta pestaña, puede almacenar sus cuentas de correo electrónico personales, números de tarjetas de crédito, información de cuentas bancarias, direcciones de contacto, números de teléfono, direcciones de correo electrónico, etc., en la interfaz web de Password Manager Pro.

La información personal que almacene en Password Manager Pro estará encriptada y nadie podrá acceder a ella, lo que garantiza la total privacidad de los datos. Para mejorar la seguridad, se le pedirá que cree una frase de contraseña la primera vez que acceda a la pestaña Personal, que luego se utilizará como la clave de cifrado para sus contraseñas personales.

Crear una frase de contraseña para acceder a sus cuentas personales

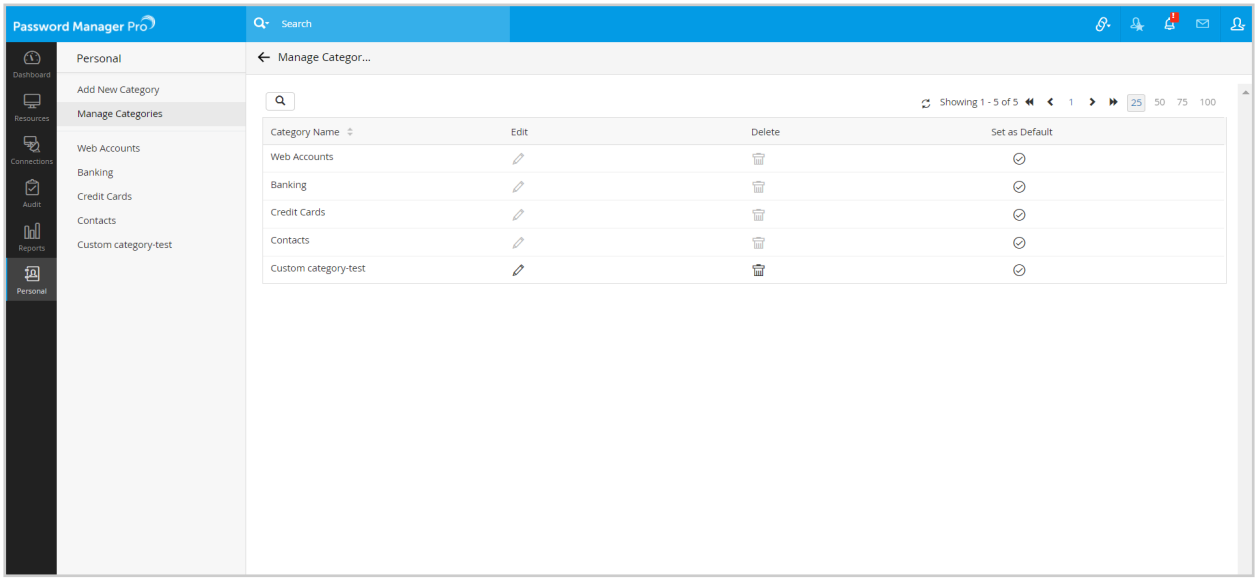
Recomendamos encarecidamente que cree una frase de contraseña larga y fácil de recordar. Deberá ingresar esta frase de contraseña cada vez que necesite acceder a sus contraseñas personales. Tenga en cuenta que si olvida esta frase de contraseña, no hay forma de recuperar los datos personales que haya almacenado en Password Manager Pro.



Almacenar cuentas personales

Una vez que haya configurado una frase de acceso, podrá añadir sus cuentas personales, como cuentas web, cuentas bancarias, cuentas de tarjetas de crédito y listas de contactos personales. También puede añadir sus propias categorías si no están disponibles las que usted necesita. Puede añadir campos personalizados para todas las cuentas según sus necesidades.

Nota: *Hay cuatro categorías predeterminadas (Cuentas web, Banca, Tarjetas de crédito y Contactos) que sólo podrá ver si su administrador las habilita. Estas categorías no se pueden eliminar. Sin embargo, puede eliminar las categorías personalizadas que cree.*



Para crear cuentas personales en cualquiera de las categorías predeterminadas:

- Vaya a la pestaña *Personal*.
- Haga clic en cualquiera de las categorías predeterminadas de la parte izquierda.
- Haga clic en *Agregar cuentas*.
- Ingrese los detalles requeridos y haga clic en *Guardar*.
- Las cuentas añadidas aparecerán bajo las categorías respectivas.

Para eliminar cuentas personales:

- Vaya a la pestaña *Personal*.
- Haga clic en la categoría requerida.
- Seleccione las cuentas que se deben eliminar.
- Haga clic en *Eliminar cuentas*.
- Confirme la acción haciendo clic en *OK*.

Nota: *Se recomienda discreción al eliminar las cuentas, ya que la acción elimina permanentemente la(s) cuenta(s) seleccionada(s) de la base de datos de Password Manager Pro.*

Campos personalizados

Puede añadir cualquier cantidad de campos personalizados adicionales en una categoría particular. Para añadir un campo personalizado, haga clic en el botón *Personalizar campos* de la parte superior. Sus campos adicionales pueden estar en cualquiera de los cuatro formatos: Carácter/lista, Numérico, Contraseña, Fecha.

Puede añadir un máximo de nueve campos de Carácter/lista, cuatro campos Numéricos, tres campos de Contraseña y cuatro campos de Fecha. Después de ingresar el nombre de la columna, la descripción (opcional) y el valor predeterminado (opcional), haga clic en *Guardar*.

> **Nota:** *Una vez creado, no podrá eliminar un campo personalizado.*

Categorías personalizadas

Además de las cuatro categorías predeterminadas, puede crear cualquier cantidad de categorías adicionales para almacenar otra información y también añadir nombres de columna personalizados.

Para crear una categoría personalizada,

- Vaya a la pestaña *Personal*.
- Haga clic en *Agregar nueva categoría*.
- Ingrese un nombre para la nueva categoría.
- Añada nombres de columna que contengan caracteres, números, contraseñas y fechas.
- Guarde la categoría.

Gestionar las categorías

Esta opción le permite editar o eliminar las categorías personalizadas. Tenga en cuenta que una vez elimine una categoría, no podrá recuperarla.

Importar contraseñas

Los detalles de su cuenta personal se pueden importar a Password Manager Pro de forma masiva desde un archivo CSV/TSV. Haga clic en el botón *Importar cuentas* y envíe los detalles requeridos. Se admiten archivos CSV/TSV con extensiones .txt, .tsv y .csv.

Exportar contraseñas

De forma similar a la operación de importación, Password Manager Pro también le permite exportar sus contraseñas personales como un archivo PDF o Excel. Para ello, haga clic en el icono de *Exportar* disponible en la parte superior derecha de la pantalla y seleccione la opción deseada.

7. Cambiar la contraseña de Password Manager Pro

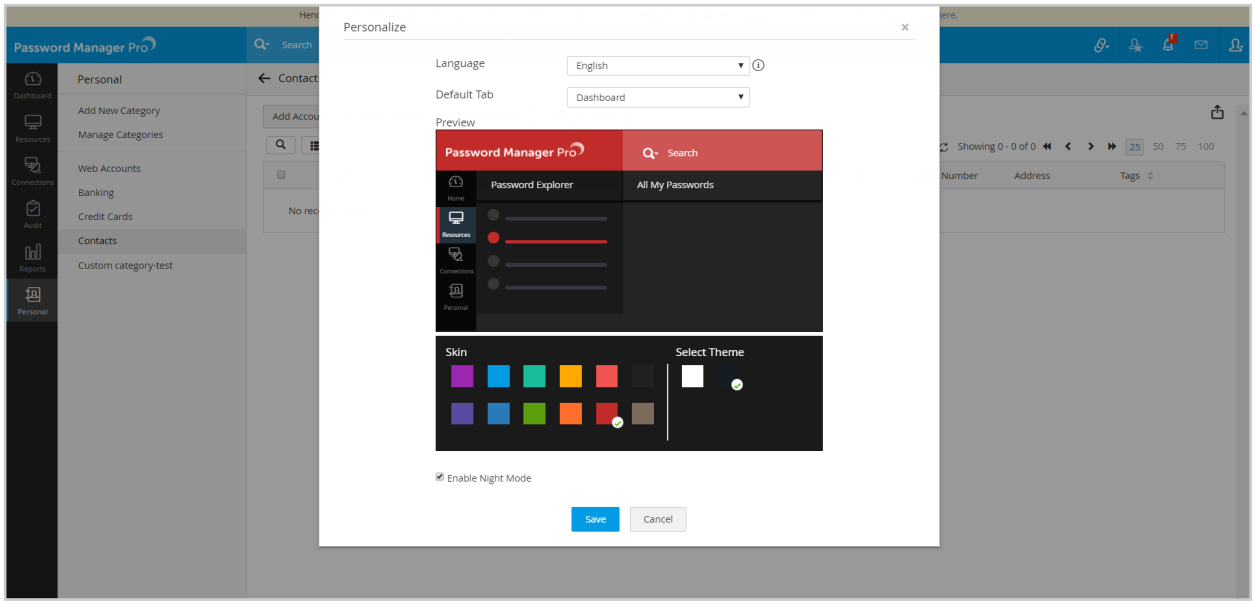
Puede restablecer su contraseña de autenticación local haciendo clic en *Cambiar contraseña* en la lista desplegable bajo el icono de *Mi perfil* en la esquina superior derecha. Tenga en cuenta que si su administrador implementa una política de contraseñas para su organización, la nueva contraseña que establezca aquí tiene que cumplir con la política.

También puede utilizar el generador de contraseñas para generar contraseñas que cumplan con las políticas de su organización. Asegúrese de recordar su nueva contraseña, ya que no se le enviará por correo electrónico. Si olvida su contraseña, utilice el enlace *¿Olvidó su contraseña?* disponible en la página de inicio de sesión de Password Manager Pro para restablecer su contraseña.

8. Ajustes de visualización personalizados

Password Manager Pro le permite personalizar los ajustes de visualización de su cuenta de Password Manager Pro. Para ello, haga clic en el icono de *Mi Perfil* en la esquina superior derecha, y seleccione *Personalizar* en el menú desplegable.

- En el menú desplegable *Idioma*, seleccione un idioma para la interfaz web. Password Manager Pro estará disponible en el idioma elegido después de guardar los cambios. Actualmente, Password Manager Pro está disponible en inglés, francés, alemán, japonés, polaco, español, chino simplificado, chino tradicional y turco.
- En el menú desplegable *Pestaña predeterminada*, seleccione la pestaña predeterminada que desea que se muestre al iniciar la sesión, es decir, la pestaña *Recursos*, *Conexiones*, o *Personal*.
- También puede elegir un color de fondo y un tema entre las opciones disponibles.
- Si desea activar el modo nocturno, seleccione la opción *Activar modo nocturno*.
- Puede ver una vista previa rápida de su cuenta con todas las funciones elegidas en la opción *Vista previa*.
- Haga clic en *Guardar* para aplicar los cambios.



9. Extensiones del navegador

Hay disponibles extensiones nativas del navegador para Chrome, Firefox e Internet Explorer, que simplifican la gestión de contraseñas y las actividades de inicio de sesión automático.

Instalar extensiones del navegador

1. Chrome

- Inicie sesión en Password Manager Pro a través de Chrome, y seleccione *Extensiones del navegador* en el menú desplegable *Mi perfil* en la esquina superior derecha. Esto le llevará a la página de Password Manager Pro en la página de la tienda web de Chrome. También puede añadir la extensión de Chrome de Password Manager Pro aquí.
- En la ventana que se abre, haga clic en el botón *Añadir a Chrome* junto a Password Manager Pro.
- Confirme la acción haciendo clic en *Añadir* en la ventana emergente.
- Una vez instalada, el icono de Password Manager Pro aparecerá en la barra de direcciones; para iniciar sesión en Password Manager Pro, haga clic en el ícono.

2. Firefox

- Inicie sesión en Password Manager Pro a través de Firefox, y seleccione *Extensiones del navegador* en el menú desplegable *Mi perfil* en la esquina superior derecha. Esto le llevará al add-on de Password Manager Pro en la página de Firefox. También puede añadir la extensión de Firefox de Password Manager Pro aquí.
- En la ventana que se abre, haga clic en *Añadir a Firefox* bajo Password Manager Pro.
- Confirme la acción haciendo clic en *Instalar* en la ventana emergente.
- Una vez instalada, el icono de Password Manager Pro estará disponible al final de la barra de direcciones; haga clic en el ícono para iniciar sesión.

3. Internet Explorer

- Inicie sesión en Password Manager Pro a través de Internet Explorer, y seleccione *Extensiones del navegador* en el menú desplegable *Mi perfil* en la esquina superior derecha. El archivo de configuración se descargará automáticamente. También puede descargar el asistente de configuración aquí.
- Una vez realizado, ejecute el archivo Setup.exe y siga las instrucciones del asistente.
- Después de la instalación, abra el navegador Internet Explorer, haga clic derecho en la barra de *pestañas*, y haga clic en la *Barra de comandos* para ver el add-on de Password Manager Pro.
- A continuación, haga clic en el icono de *Herramientas* (Alt+X) en la esquina superior derecha, y seleccione *Opciones de Internet* en el menú desplegable. Vaya a **Seguridad > Sitios de confianza > Sitios**, añada la **URL de Password Manager Pro** (https://<Password Manager Pro-Acceso-URL>:puerto), y haga clic en *Añadir*.
- Ahora, vaya a la pestaña *Avanzado* y habilite la opción *Permitir que el contenido activo se ejecute en los archivos en Mi PC*, bajo la sección Seguridad. A continuación, haga clic en *Aplicar*.
- Reinicie el equipo para que los ajustes surtan efecto.
- Una vez realizado, abra el add-on y proporcione las credenciales.

Iniciar sesión en las extensiones del navegador

En la pantalla de inicio de sesión, ingrese el nombre del host donde se ejecuta Password Manager Pro y el puerto de conexión. La extensión del navegador también es compatible con todos los tipos de inicio de sesión (local/AD/LDAP/RADIUS) y los mecanismos de autenticación disponibles en la consola web.

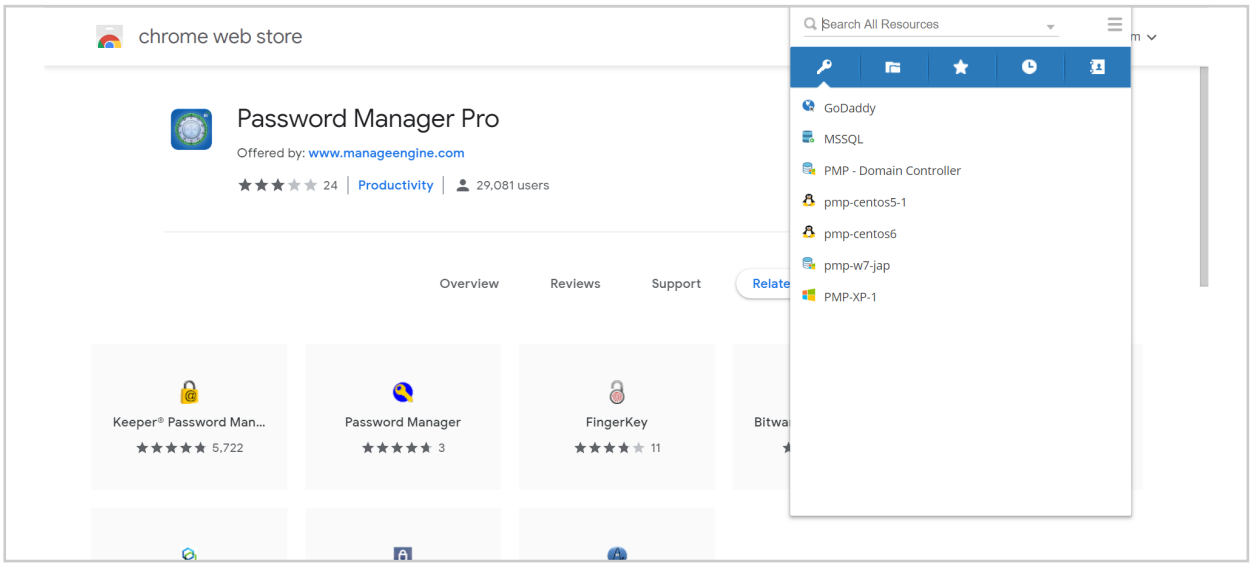
Operaciones que puede realizar con las extensiones del navegador

Puede iniciar sesión automáticamente en sitios web y aplicaciones desde el propio navegador sin necesidad de abrir la interfaz web de Password Manager Pro. Haga clic

en cualquier recurso que aparece en la pestaña *Todas las contraseñas* para ver los nombres de cuenta asociados a ese recurso. Haga clic en cualquier cuenta para ver su contraseña.

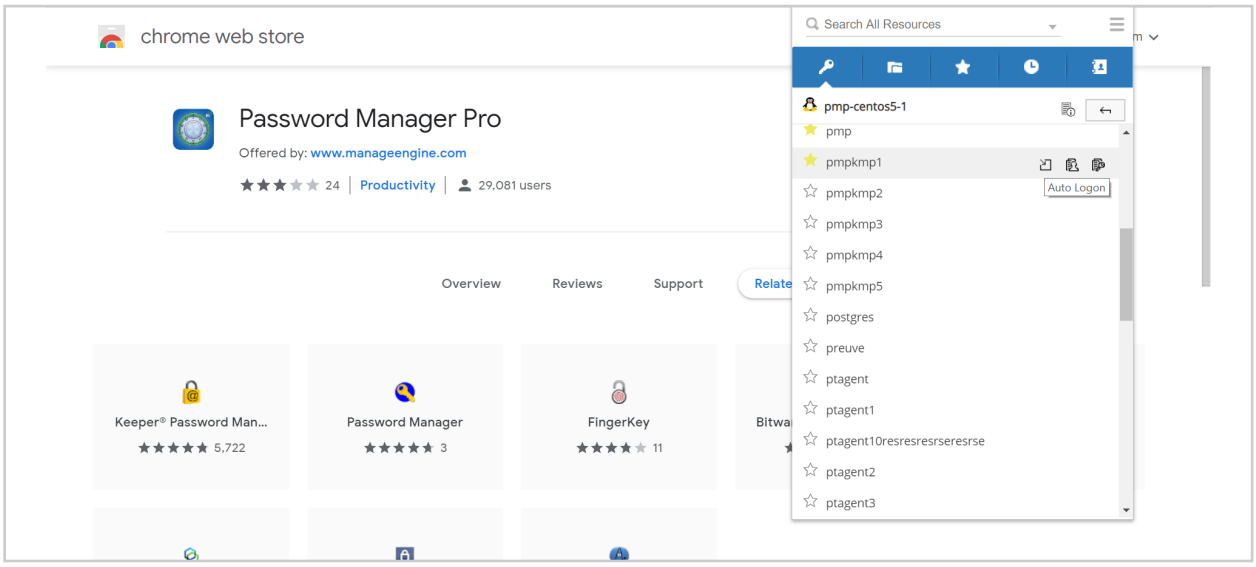
1. Todas las contraseñas

Esta pestaña del menú principal muestra todas las contraseñas disponibles. Haga clic en un recurso en particular para ver todas las cuentas asociadas, y haga clic en el icono de *Descripción del recurso* junto al recurso para ver los detalles del mismo.



a) Iniciar sesiones RDP o SSH automáticamente: Esta opción le permite iniciar una conexión directa a sitios web y recursos de Windows/Linux haciendo clic en el icono de *Inicio de sesión automático* junto a una cuenta.

b) Copiar las contraseñas de la cuenta: También puede copiar el nombre de usuario y la contraseña pertenecientes a una cuenta haciendo clic en los respectivos iconos junto a la cuenta.



Nota: *Podrá acceder a las contraseñas según los ajustes de recuperación de contraseñas configurados por su administrador. Consulte la sección recuperar contraseñas para obtener más detalles.*

2. Grupos de recursos

La opción de *Grupos de recursos* le permite ver las contraseñas específicas de un grupo de recursos que su administrador ha compartido con usted. Aquí, la extensión del navegador mantendrá la misma estructura de árbol de los grupos de recursos y las cuentas asociadas que la interfaz web.

3. Recursos favoritos

Esta opción proporciona un acceso rápido a la lista de todas las contraseñas que ha marcado como favoritas, y le ayuda a localizar sus recursos favoritos y las contraseñas asociadas fácilmente. Puede marcar una contraseña como favorita haciendo clic en el icono de la estrella que aparece junto a ella.

4. Recursos utilizados recientemente

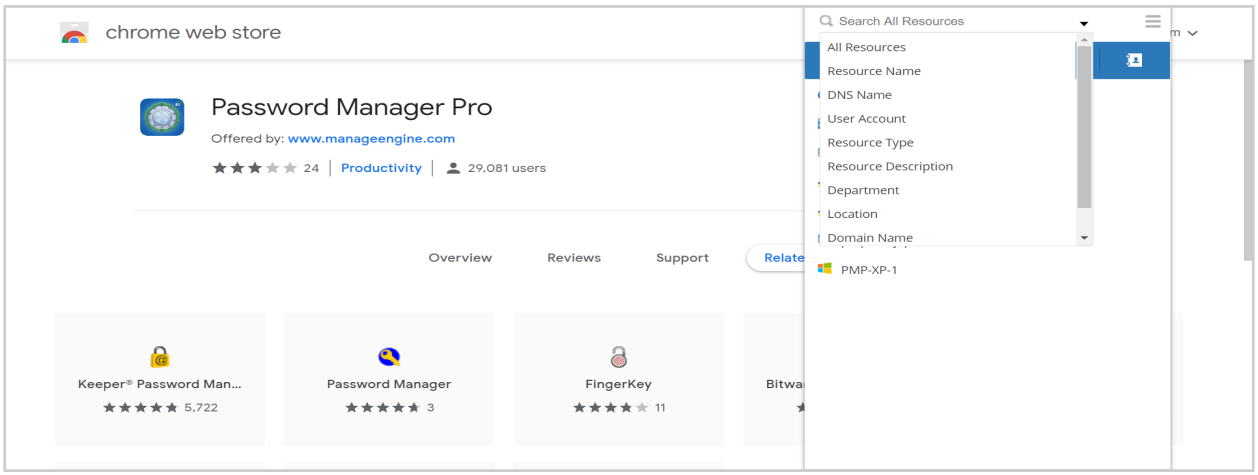
Esta opción le ayuda a ver la lista de recursos a los que se ha accedido recientemente y sus contraseñas. Puede hacer clic en cualquier recurso de la lista para ver sus cuentas.

5. Contraseñas personales

Al igual que la interfaz web, esta opción le permite acceder a todas sus contraseñas personales guardadas en su cuenta de Password Manager Pro.

6. Buscar todos los recursos

Puede buscar contraseñas directamente desde la extensión del navegador basándose en varios criterios, como el nombre del recurso, el nombre de usuario, el nombre DNS, la cuenta de usuario, el tipo de recurso, la descripción del recurso, el departamento, la ubicación, el nombre de dominio o campos personalizados adicionales.

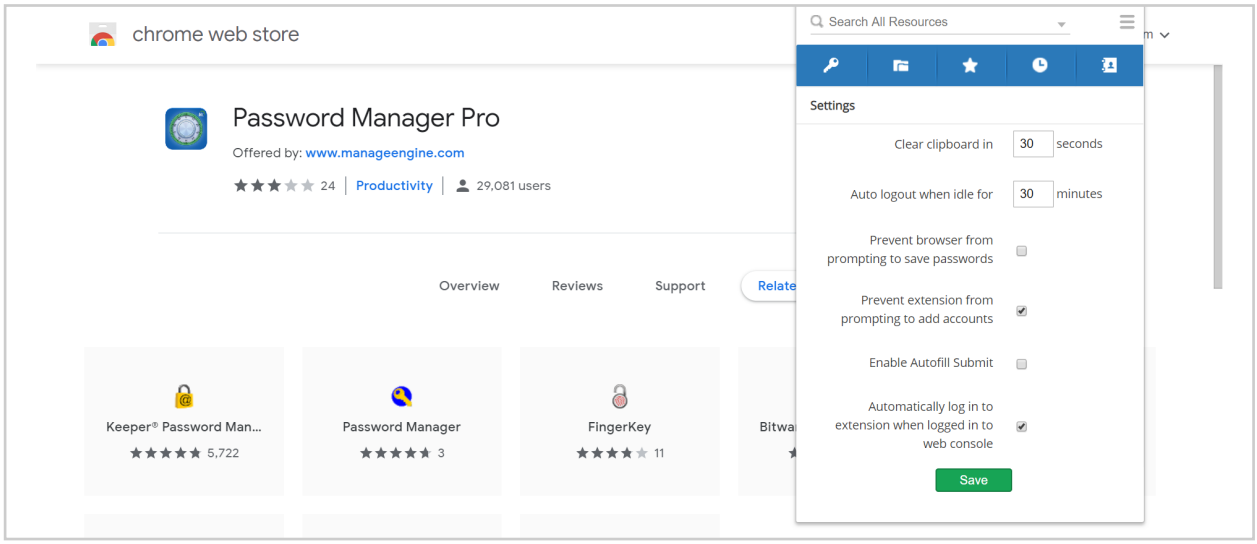


7. Ajustes

a) Borrar el portapapeles en: Define el tiempo que los datos copiados deben permanecer en el portapapeles después de cerrar la aplicación.

b) Cerrar la sesión automáticamente cuando esté inactiva durante: Muestra el tiempo que permanecerá activa su sesión una vez que se conecte. La sesión se cerrará automáticamente si permanece inactiva durante el tiempo especificado aquí. Sin embargo, puede configurar la opción como "0" para que nunca se cierre la sesión.

c) Evitar que el navegador solicite guardar las contraseñas: Evita que el navegador guarde sus contraseñas para futuros inicios de sesión.



d) Evitar que la extensión solicite añadir cuentas: Le permite impedir que se añadan cuentas a Password Manager Pro a través de la extensión del navegador.

e) Habilitar la función de autocompletar y enviar: Además de autocompletar los nombres de usuario y las contraseñas en los formularios en línea, Password Manager Pro también ofrece una opción para enviar automáticamente el formulario. Puede habilitar esta opción para enviar automáticamente los formularios en línea en las páginas web.

f) Iniciar sesión automáticamente en la extensión cuando haya iniciado sesión en la consola web: Le permite iniciar sesión automáticamente en la extensión del navegador cuando ya ha iniciado sesión en la interfaz web de Password Manager Pro.

8. Completar automáticamente un nombre de usuario y una contraseña en un sitio/aplicación

Si se encuentra en la página de inicio de sesión de un sitio web o aplicación y si las credenciales de ese sitio o aplicación ya se han almacenado en Password Manager Pro,

haga clic en el icono de la extensión del navegador que aparece en el campo de credenciales de usuario y seleccione la cuenta. El nombre de usuario y la contraseña correspondientes se completarán automáticamente, y luego podrá aplicarlos manualmente para el inicio de sesión automático.

10. Acceso móvil

Password Manager Pro ofrece aplicaciones nativas para iOS, Android y Windows que le ayudan a acceder y recuperar de forma segura todas las contraseñas de la empresa que se comparten con usted, así como sus contraseñas personales, **siempre que su administrador le haya permitido el acceso móvil.**

- La aplicación móvil es tan segura como la instalación de desktop; utiliza el mismo cifrado AES-256 para almacenar información sensible.
- Toda la comunicación entre Password Manager Pro y la aplicación móvil se protege con el protocolo HTTPS sobre SSL, siempre que tenga un certificado válido para su servidor.
- La aplicación móvil también admite la autenticación de dos factores. Si su administrador habilita la autenticación de dos factores, deberá autenticarse en dos etapas consecutivas antes de tener acceso a la interfaz móvil.
- Tras la autenticación, deberá ingresar una frase de contraseña que tendrá que proporcionar cada vez que intente acceder a su cuenta. Esta frase de contraseña se utilizará para cifrar los datos sin conexión.

Instalación e inicio

Dispositivos compatibles	iPhone, iPad, iPod touch	Todos los dispositivos Android
Compatibilidad	Requiere una versión iOS 6.0 o superior	Requiere una versión Android 4.3 o superior
Tamaño	13.5MB	5.98MB
Idiomas compatibles	Inglés, francés, alemán, japonés, polaco, español, chino simplificado, chino tradicional y turco.	Inglés, francés, alemán, japonés, polaco, español, chino simplificado, chino tradicional y turco.

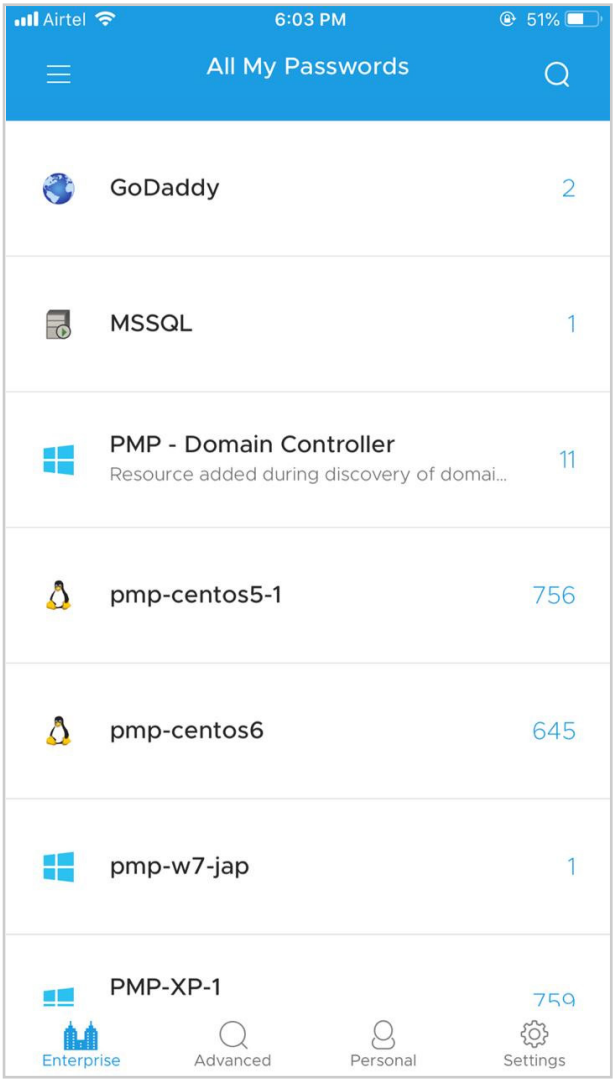
Android **iOS** **BlackBerry**

Después de instalar correctamente la aplicación móvil,

- Ingrese el nombre del servidor o la dirección IP en la que se está ejecutando Password Manager Pro. Asegúrese de que el servidor de Password Manager Pro y la aplicación móvil están conectados a la misma red.
- Ingrese el número de puerto.
- En caso de que sea un usuario MSP, ingrese el nombre de su organización y haga clic en Guardar.
- En la pantalla de inicio de sesión que aparece a continuación, ingrese las credenciales de autenticación local o AD, Azure AD, LDAP o Radius para iniciar sesión en su cuenta de Password Manager Pro. Si la autenticación de dos factores está habilitada, el segundo nivel de autenticación será a través del método de autenticación de dos factores configurado por su administrador en la interfaz web.
- Establezca una frase de contraseña para su cuenta. Esta opción sólo estará disponible si el administrador habilita el almacenamiento en caché de la contraseña para el acceso sin conexión. Una vez establecida, tendrá que introducir esta frase de contraseña cada vez que necesite acceder a la aplicación.

ManageEngine Password Manager Pro iOS

- Una vez que haya accedido a su cuenta, encontrará una lista de todos los recursos compartidos con usted en la sección Empresa.



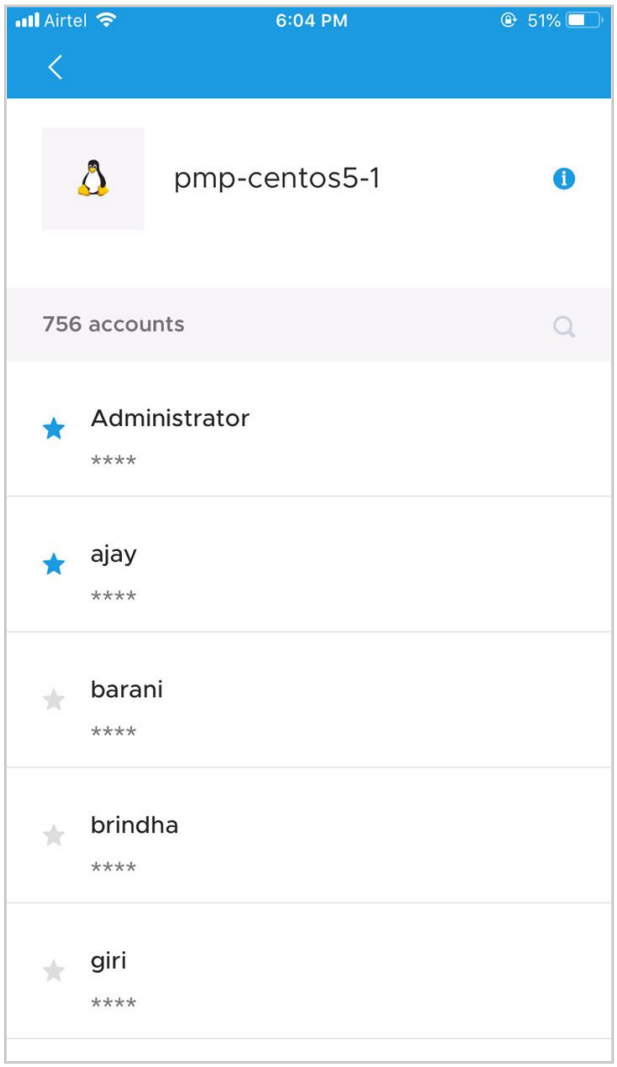
Menú de navegación

Puede abrir el menú de navegación deslizando la pantalla de izquierda a derecha o haciendo clic en el botón de la esquina superior izquierda de la pantalla principal. Este menú mostrará las siguientes pestañas:

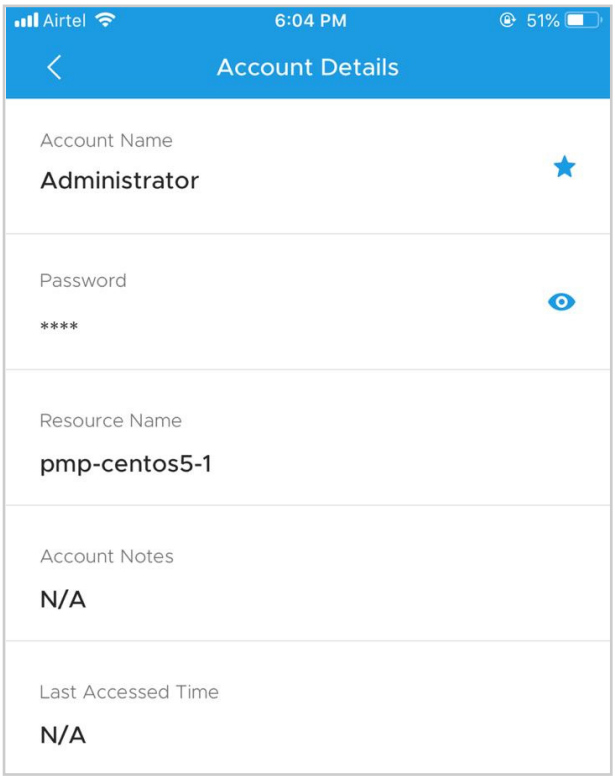
- Todas mis contraseñas
- Favoritos
- Recientes
- Contraseñas RDP de Windows
- Contraseñas SSH

A) Todas mis contraseñas

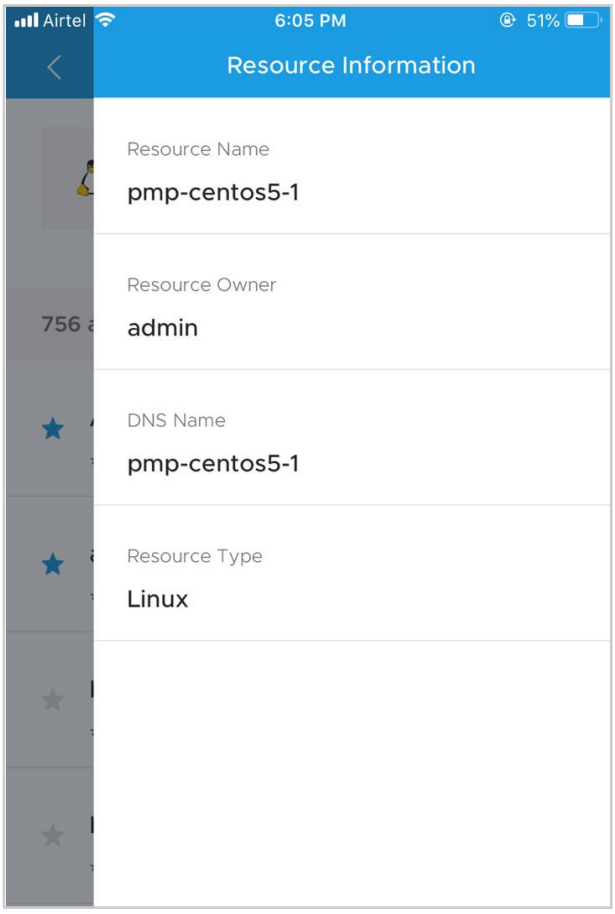
- Al iniciar sesión, la aplicación mostrará una lista de todos los recursos en su pantalla principal de forma predeterminada. Haga clic en cualquier recurso para ver sus cuentas.



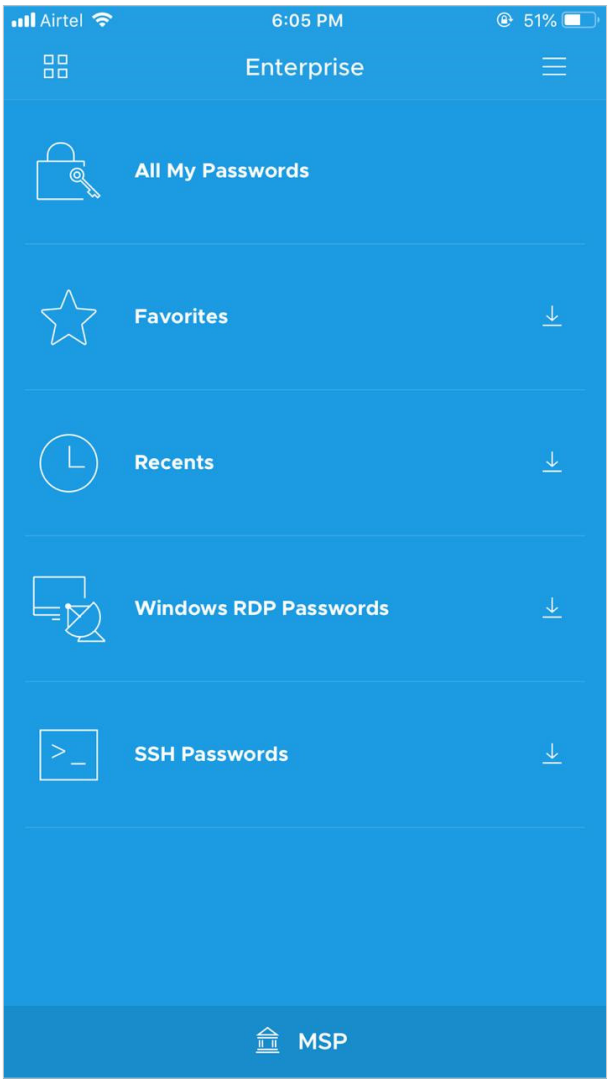
- Al hacer clic en cualquier cuenta, podrá ver la contraseña (enmascarada con asteriscos), el nombre del recurso, el nombre de la cuenta y la última vez que se accedió a él.
- Haga clic nuevamente en los asteriscos para ver la contraseña.
- Puede marcar cualquier contraseña como favorita haciendo clic en el icono de la estrella. También puede eliminar contraseñas de la lista de *Favoritos* haciendo clic nuevamente en el icono.



- Haga clic en el icono de la derecha en la parte superior de la pantalla para ver los detalles del recurso, incluyendo el nombre del recurso, el propietario del recurso, el nombre DNS, etc.



- Para recuperar contraseñas específicas como sus favoritos, contraseñas a las que ha accedido recientemente, contraseñas RDP de Windows, contraseñas SSH, etc., haga clic en el botón superior izquierdo. Aparecerá un menú en el que podrá ver la lista que desee.



B) Favoritos

Esta opción le permite acceder rápidamente a la lista de todas las contraseñas que ha marcado como favoritas. Puede marcar cualquier contraseña como favorita desde la pantalla *Todas mis contraseñas* haciendo clic en el icono de la estrella junto a la contraseña deseada.

C) Recientes

Esta opción le ayuda a ver la lista de recursos a los que se ha accedido recientemente y sus contraseñas. Puede hacer clic en cualquier recurso de la lista para ver sus cuentas de usuario.

D) Contraseñas RDP de Windows

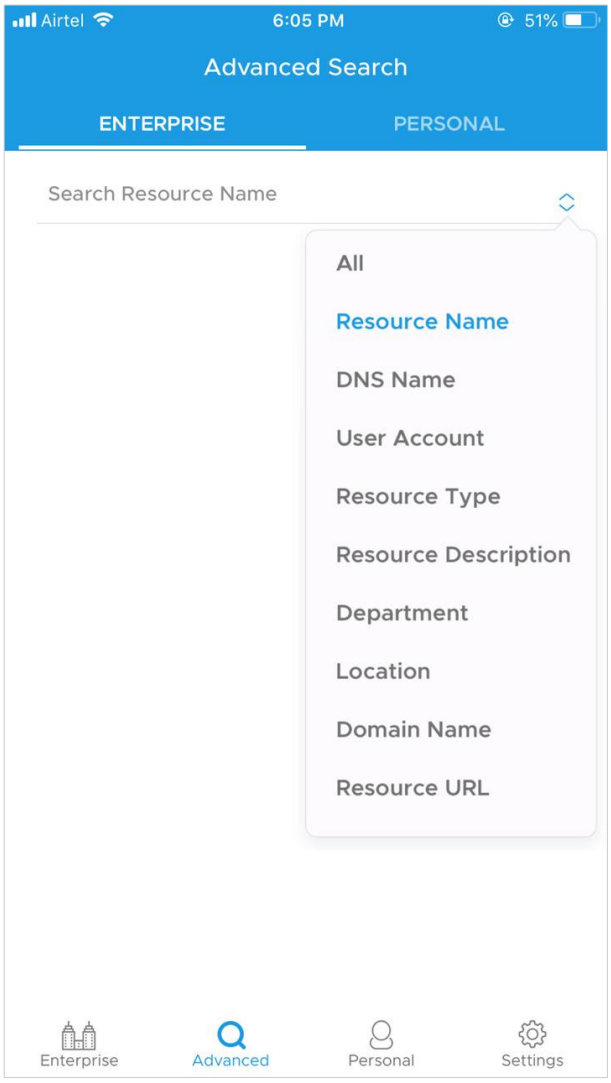
Si su red tiene una lista de recursos heterogéneos, esta opción le ayudará a ver sólo la lista de recursos de Windows. Haga clic en cualquier recurso de la lista para ver sus cuentas de usuario.

E) Contraseñas SSH

Esta opción le ayuda a ver los recursos que se pueden conectar a través de SSH. Haga clic en cualquier recurso de la lista para ver sus cuentas de usuario.

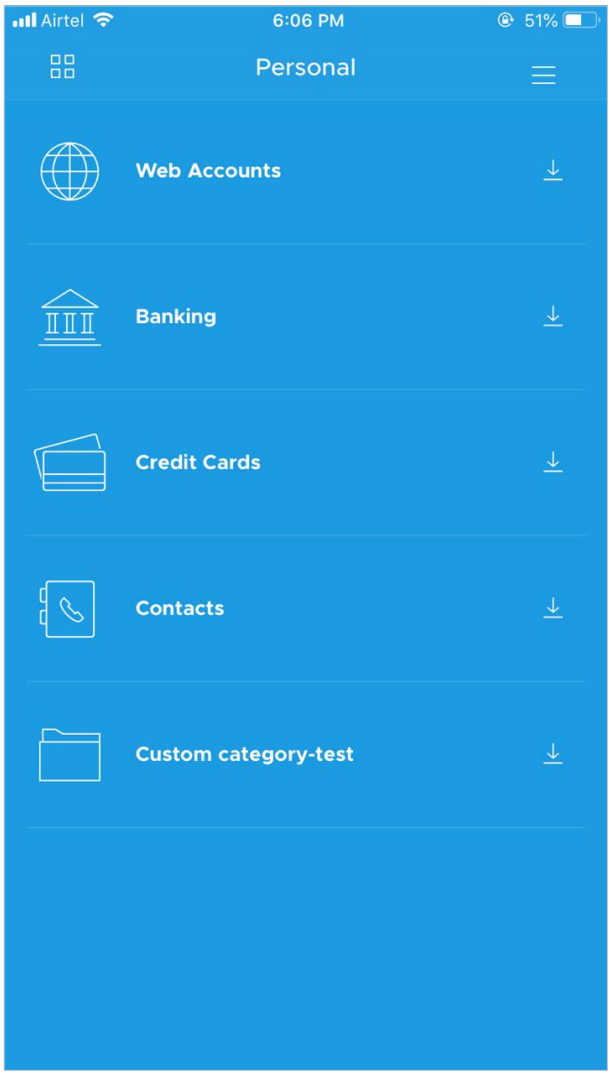
F) Búsqueda avanzada

Puede buscar un usuario o recurso específico fácilmente utilizando palabras clave como nombre, departamento, ubicación, etc.



G) Personal

Además de los datos de la empresa, la aplicación móvil también le permite almacenar y acceder a las cuentas personales que ha creado a través de la interfaz web de Password Manager Pro. Algunos ejemplos de datos personales son sus cuentas de correo electrónico personales, números de tarjetas de crédito, información de cuentas bancarias, detalles de contacto, números de teléfono y direcciones de correo electrónico.
Sin embargo, puede almacenar sus contraseñas personales en Password Manager Pro sólo si su administrador habilita esta opción para usted.



Para obtener más información sobre cómo añadir cuentas personales a través de la interfaz web de Password Manager Pro, consulte esta sección de nuestra documentación de ayuda.

Después de añadir una cuenta personal a su cuenta de Password Manager Pro, puede acceder a ella a través de la aplicación móvil proporcionando la frase de contraseña que estableció al configurar la cuenta.

a) Favoritos: Puede marcar cualquiera de sus cuentas personales como favorita haciendo clic en el icono de la estrella. Sin embargo, estas cuentas no se mostrarán en la lista de *Favoritos* bajo el menú de navegación.

b) Buscar: Encuentre una cuenta en particular haciendo clic en el icono de *Búsqueda* en la parte superior de la pantalla y proporcionando palabras clave relacionadas con la cuenta.

H) Ajustes

Con la opción de *Ajustes*, puede personalizar varias opciones de seguridad, ver los detalles de inicio de sesión y conocer la política de privacidad de Password Manager Pro para su aplicación de iOS.

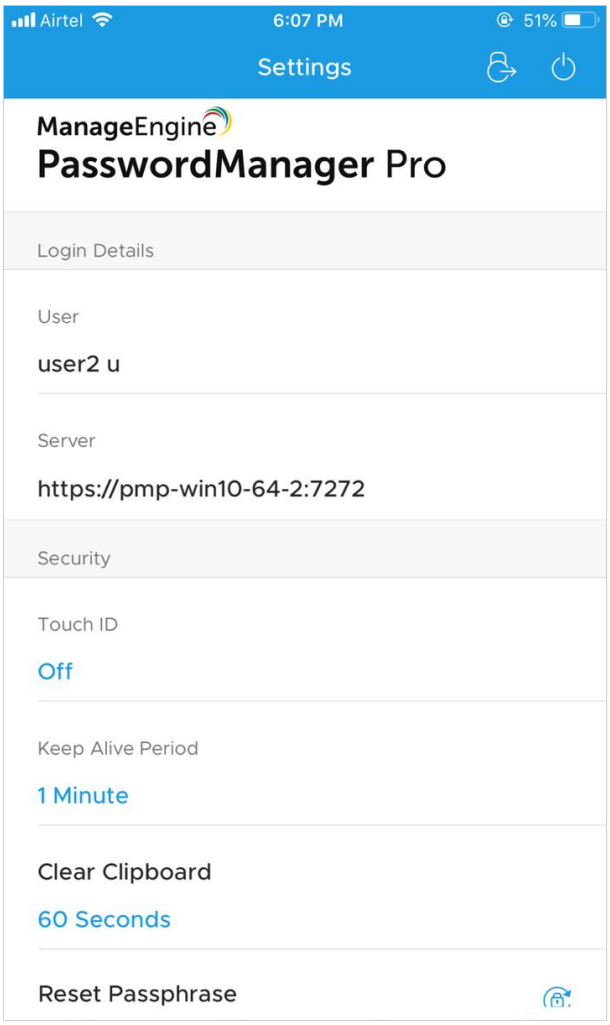
a) Detalles del inicio de sesión: Muestra el nombre de usuario y la dirección del servidor al que está conectado actualmente Password Manager Pro. Si la función de replicación (alta disponibilidad) está activada, la aplicación también proporcionará los detalles del servidor secundario en esta página. Si el servidor primario no funciona, puede conectarse al servidor secundario para mantener un servicio ininterrumpido.

b) Seguridad: Para mejorar la seguridad del dispositivo y de los datos, Password Manager Pro ofrece varias opciones como ID táctil, Periodo de actividad, Borrar el portapapeles y Restablecer la frase de contraseña.

i) ID táctil: Si su dispositivo es compatible con el escaneo de huellas dactilares, este ajuste le permite omitir la frase de contraseña cada vez que necesite acceder a su cuenta de Password Manager Pro. Podrá acceder a su cuenta directamente proporcionando su ID táctil.

ii) Período de actividad: Por defecto, Password Manager Pro no le permitirá mantener la sesión en la aplicación después de salir de ella, y le obligará a introducir sus credenciales cada vez que necesite acceder. Sin embargo, puede establecer el período de actividad como 1 minuto, 2 minutos, 5 minutos, 10 minutos, o hacer que se bloquee al salir de la aplicación. Esto es útil cuando se quiere cambiar entre Password Manager Pro y otras aplicaciones dentro de un determinado período de tiempo. Por razones de seguridad, no hay ninguna opción para mantener su aplicación activa por más de 10 minutos, y la opción más segura es utilizar el período de actividad mínimo, es decir, 1 minuto.

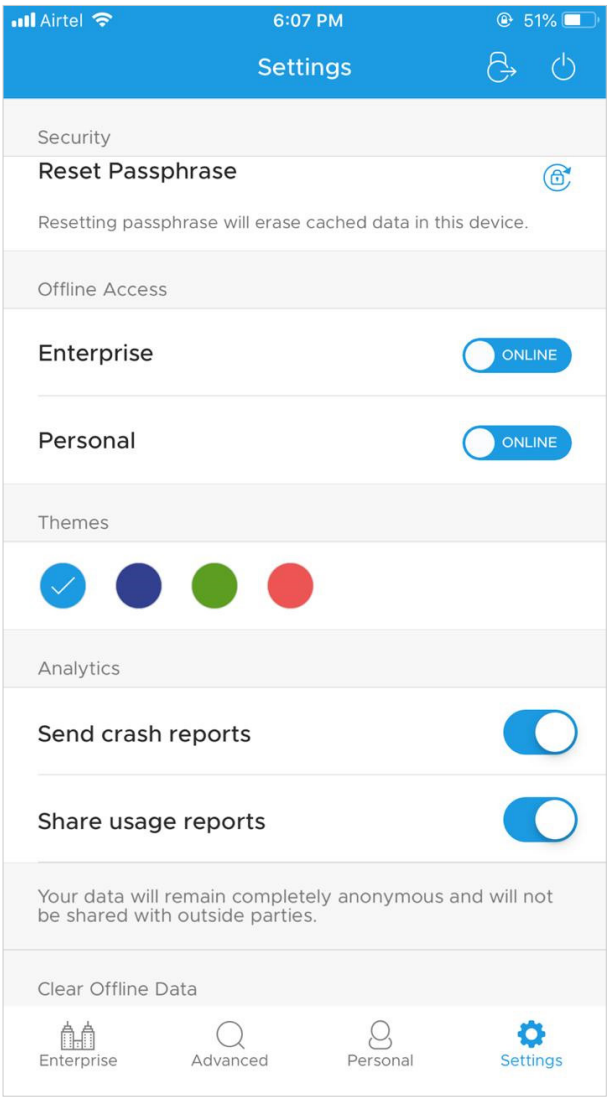
iii) Borrar el portapapeles: Defina cuánto tiempo debe permanecer una contraseña copiada en el portapapeles: 30 segundos, 60 segundos, 90 segundos o 120 segundos. También hay una opción para no borrar nunca el portapapeles.



c) Restablecer la frase de contraseña: Puede modificar la frase de contraseña siempre que sea necesario, siempre que esté utilizando el modo con conexión. Se recomienda cambiar la frase de contraseña a intervalos regulares. Tenga en cuenta que al restablecer la frase de contraseña se borrarán los datos almacenados en la caché de la aplicación de su dispositivo. Esto incluye tanto los datos sin conexión de la empresa como los personales si ha establecido la misma frase de contraseña para ambos. De lo contrario, sólo se borrarán los datos sin conexión de la empresa.

d) Acceso sin conexión: Elija si desea utilizar el modo con conexión o sin conexión para sus cuentas empresariales y/o personales.

e) Temas: Elija un color de fondo para su aplicación entre las opciones disponibles.

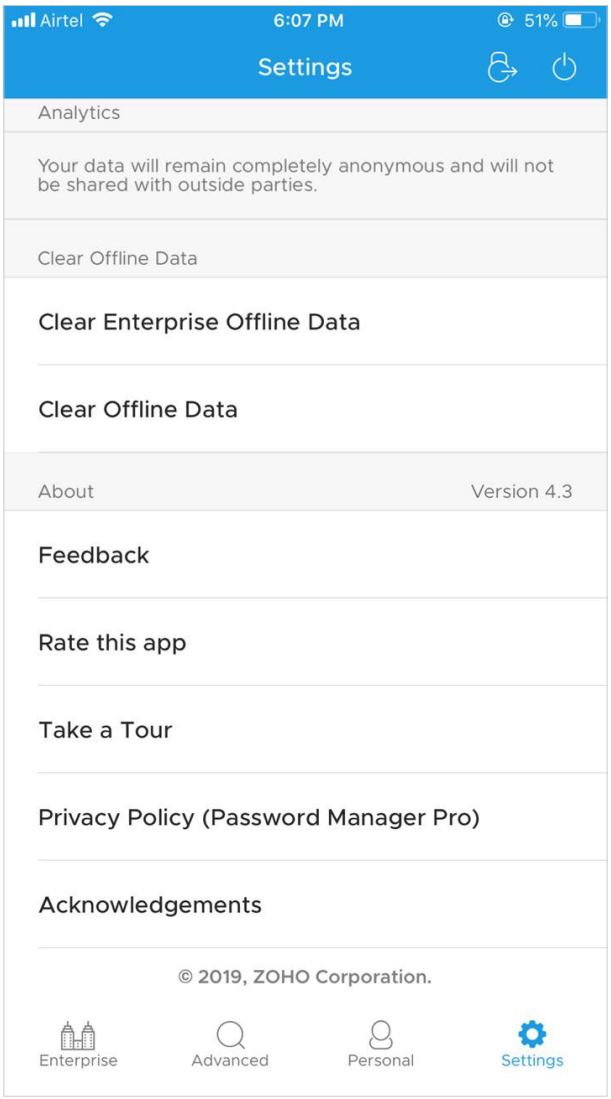


f) Borrar los datos sin conexión: Borre sus datos empresariales y/o personales sin conexión.

g) Acerca de: Envíe comentarios sobre el producto por correo, califique el producto en Play Store, obtenga información sobre el producto y lea la política de datos y privacidad.

h) Bloquear: Para bloquear la aplicación vaya a *Ajustes* y haga clic en *Bloquear* en la esquina superior derecha. Esta acción cerrará su sesión en Password Manager Pro. Sin embargo, se conservarán todos los datos almacenados en la caché local. Simplemente tendrá que proporcionar la contraseña de inicio de sesión y la frase de contraseña para iniciar sesión en su cuenta nuevamente.

i) Cerrar sesión: Para cerrar la sesión de la aplicación vaya a *Ajustes* y haga clic en el icono de *Cerrar sesión* en la esquina superior derecha. Esta acción borrará todos los datos sin conexión así como los datos del usuario según los requisitos del GDPR.



I) Copiar fácilmente los secretos a su portapapeles

Para no tener que introducir manualmente las contraseñas, Password Manager Pro le permite copiarlas en el portapapeles. Puede copiar cualquier contraseña pulsando prolongadamente sobre ella. La opción de copiar aparecerá en la pantalla.

J) Opción para acceder sin conexión de forma segura

La aplicación móvil también ofrece un modo seguro sin conexión para acceder a las contraseñas, cuando no tiene acceso a Internet.

Para acceder a las contraseñas sin conexión, debe descargar todas las contraseñas necesarias cuando esté conectado antes de pasar al modo sin conexión. Sólo las contraseñas que se descarguen en línea estarán disponibles para el acceso sin conexión. Las contraseñas que se ven en el modo con conexión también estarán disponibles junto con las contraseñas descargadas una vez que se desconecte.

Descargar todas las contraseñas es prácticamente imposible, por lo que se aconseja descargar la lista de contraseñas que necesita mientras está en línea para poder acceder a ella cuando esté en modo sin conexión. Para descargar una lista, haga clic en el icono *Descargar* que aparece junto a la contraseña deseada.

> **Nota:** *Si desinstala la aplicación, todos los datos de Password Manager Pro también se eliminarán del dispositivo.*

ManageEngine Password Manager Pro Android

La aplicación Android de Password Manager Pro admite las mismas funciones que la aplicación iOS. Consulte esta documentación para obtener más detalles.

11. Rol de los auditores de contraseñas en Password Manager Pro

Además de todos los módulos y funciones mencionadas a los que tienen acceso los usuarios de contraseñas, los auditores de contraseñas también tienen acceso a las pestañas *Dashboard*, *Auditoría* e *Informes* de Password Manager Pro.

A. Dashboard

El *Dashboard* ofrece un resumen general de todas las actividades relacionadas con las contraseñas y los usuarios mediante tablas y gráficos.

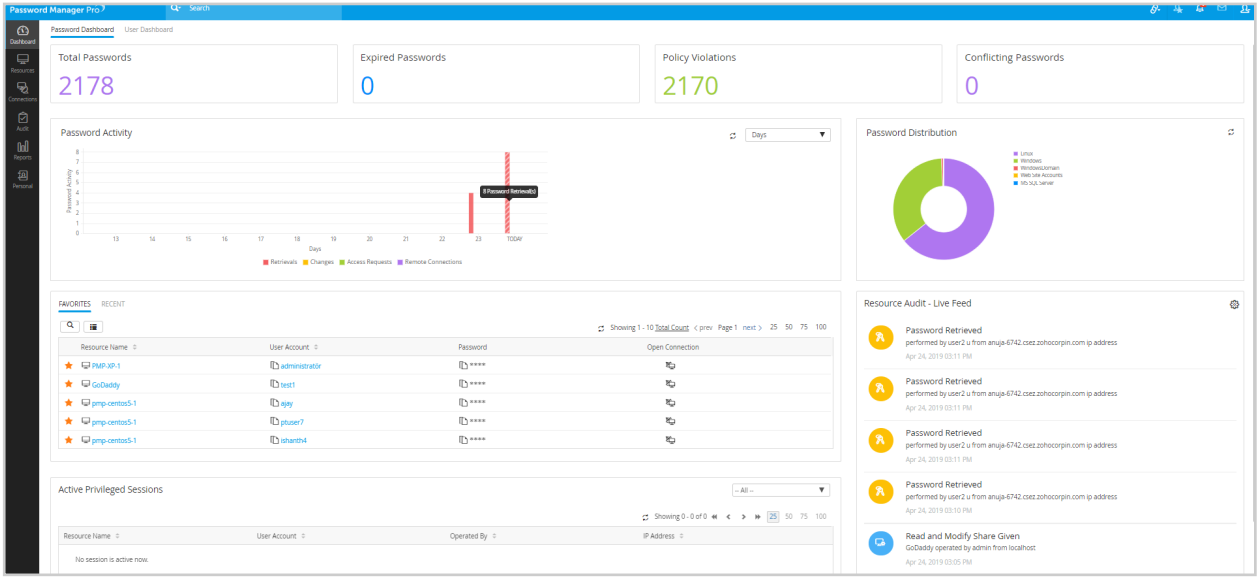
Dashboard de contraseñas

Los datos estadísticos en la sección del *Dashboard de contraseñas* proporcionan la siguiente información:

a) Contraseñas caducadas e infracciones de la política: Proporciona el número de contraseñas caducadas y que infringen las políticas de contraseñas estándar. Puede hacer clic en las cifras para ver más detalles.

b) Actividad de las contraseñas: El gráfico de barras muestra todas las actividades relacionadas con las contraseñas, como las recuperaciones de contraseñas, los cambios de contraseñas, las solicitudes de acceso a contraseñas y las conexiones remotas durante un período de tiempo determinado (los últimos 12 minutos, horas, días o meses).

c) Distribución de contraseñas: El gráfico circular muestra el número de contraseñas distribuidas en cada tipo de recurso (predeterminado y personalizado).



d) Favoritos y recientes: Estas listas muestran un resumen general de todas las contraseñas a las que se ha accedido recientemente y las que ha marcado como favoritas. Puede obtener los detalles de los recursos y las cuentas de acceso, ver y/o copiar las contraseñas asociadas y abrir una conexión remota directamente desde el dashboard.

e) Auditoría de recursos - Información en tiempo real: Proporciona actualizaciones en tiempo real de todas las actividades relacionadas con los recursos, las cuentas y las contraseñas. Haga clic en el icono de *Ajustes* para configurar las actividades para las que desea recibir actualizaciones en tiempo real. También puede establecer la frecuencia (en minutos) con la que se actualiza la información.

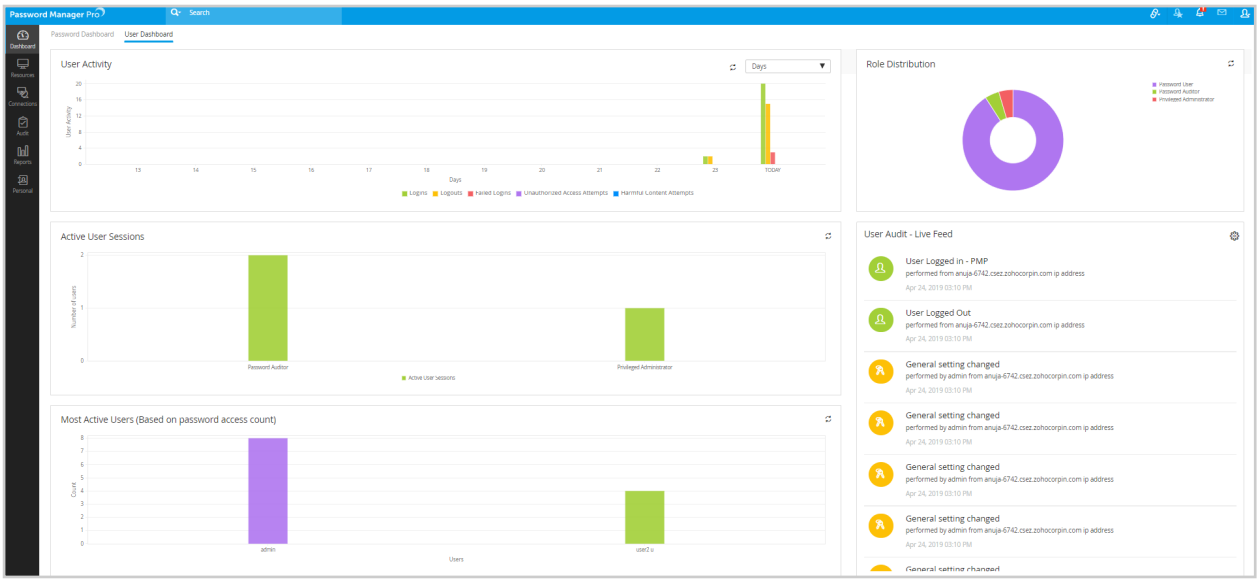
f) Sesiones privilegiadas activas: Aquí obtendrá una lista de todas las sesiones privilegiadas activas. También puede ocultar o finalizar una sesión desde el dashboard.

Dashboard de usuarios

La sección del *Dashboard de usuarios* proporciona los siguientes datos estadísticos:

a) Actividad de los usuarios: El gráfico representa todas las actividades de los usuarios, incluidas las actividades de inicio y cierre de sesión exitosas, los intentos de inicio de sesión fallidos y no autorizados, etc., durante un período de tiempo determinado (últimos 12 minutos, horas, días o meses).

b) Distribución de roles: El gráfico circular representa el número de usuarios bajo cada uno de los roles predeterminados y personalizados.



c) Sesiones de usuario activas: Aquí obtendrá una lista de todas las sesiones de usuario activas. Puede hacer clic en las cifras para obtener los detalles de la sesión.

d) Auditoría de usuarios - Información en tiempo real: TEsto proporciona actualizaciones en tiempo real de todas las actividades de los usuarios. Haga clic en el icono de *Ajustes* para configurar las actividades para las que desea recibir actualizaciones en tiempo real. También puede establecer la frecuencia (en minutos) con la que se actualiza la información.

e) Usuarios más activos: Este gráfico representa a los usuarios más activos en función del número de contraseñas a las que han accedido.

B. Auditoría

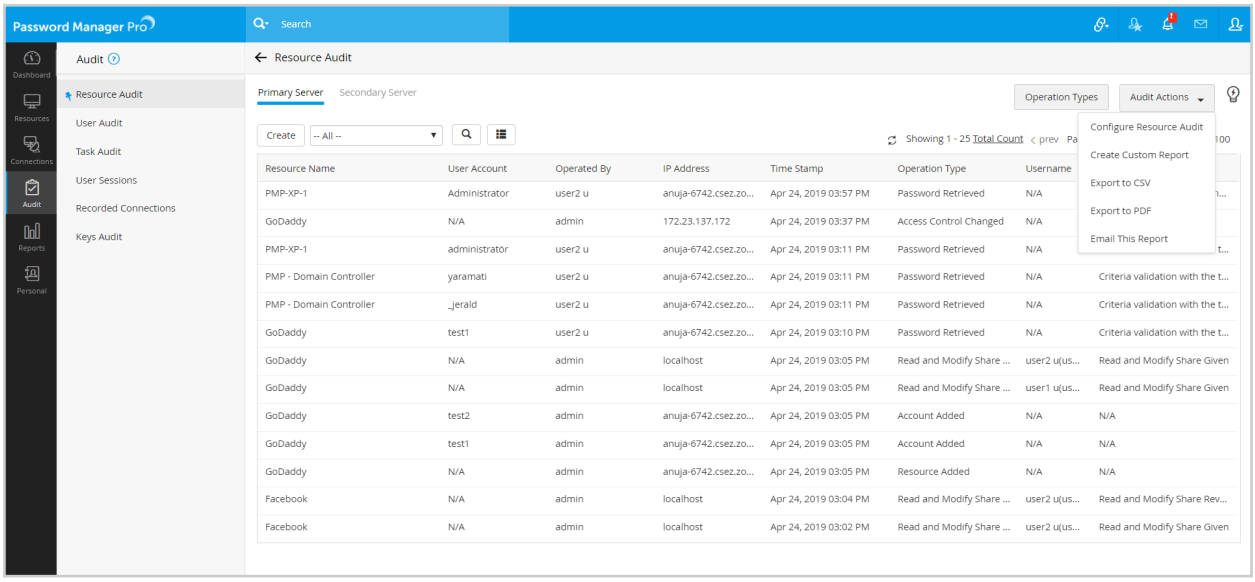
Password Manager Pro viene con un mecanismo de auditoría eficaz que registra las pistas de auditoría de cada acción realizada por cada usuario. Puede auditar todas las operaciones realizadas por los usuarios en la interfaz web junto con las marcas de tiempo de cada operación y la dirección IP desde la que accedieron a la aplicación.

Tipos de auditoría

a) Auditoría de recursos: Registra todas las operaciones relacionadas con recursos, grupos de recursos, cuentas, contraseñas y políticas.

b) Auditoría de usuarios: Registra todas las operaciones realizadas por un usuario en Password Manager Pro.

c) Auditoría de tareas: Vea las diferentes tareas programadas que se han creado.



d) Sesiones de usuario: Cuenta todas las operaciones realizadas por un usuario durante sus sesiones activas.

e) Conexiones grabadas: Enumera los vídeos grabados de las sesiones de usuario que se inician en sistemas remotos a través de Password Manager Pro. Esto le dará información completa sobre quién hizo qué, cuándo y desde dónde.

Acciones de auditoría

Las auditorías de Password Manager Pro son bastante completas: se auditan casi todas las acciones. Sin embargo, si sólo desea auditar operaciones específicas, puede especificarlas en función del tipo de operación. También hay una opción para enviar notificaciones a los usuarios deseados cada vez que se produce un evento específico en Password Manager Pro. A continuación se detallan las operaciones que puede realizar desde la pestaña de *Auditoría*.

a) Configurar auditorías

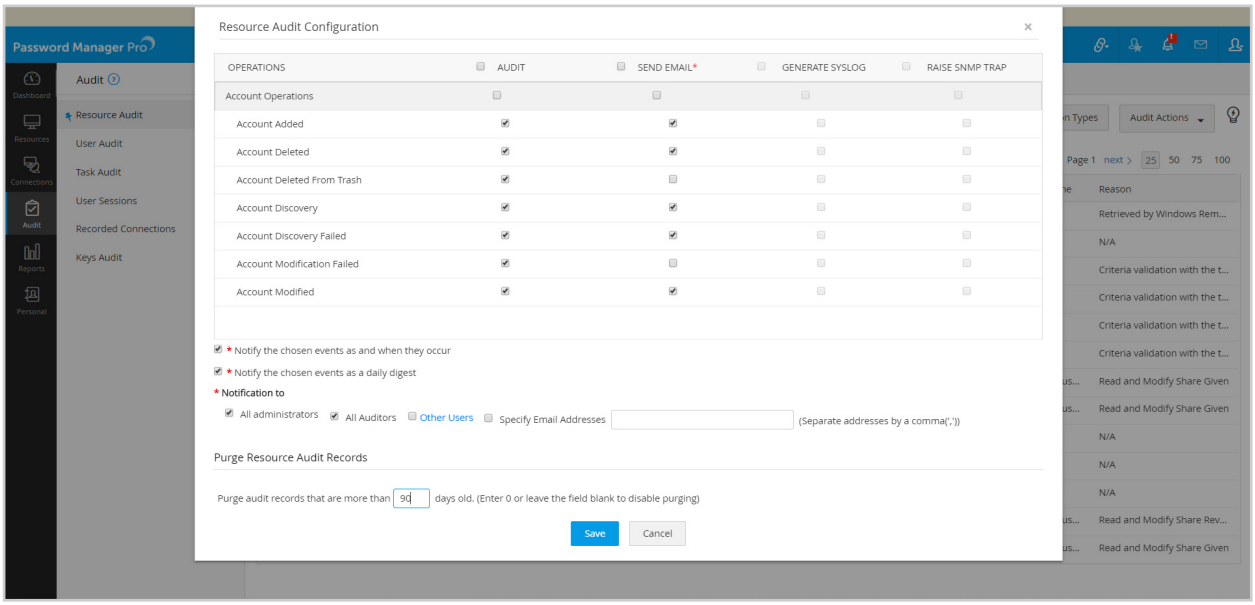
- Vaya a **Auditoría > Auditoría de recursos/usuarios/tareas**, y haga clic en *Acciones de auditoría* en la esquina superior derecha. En el menú desplegable, seleccione *Configurar auditoría de recursos/usuarios/tareas* (según la sección de auditoría en la que se encuentre).
- En la columna *Auditoría*, seleccione las operaciones para las que desea generar pistas de auditoría; en la columna Enviar correo electrónico, seleccione todas las operaciones para las que desea recibir notificaciones por correo electrónico.

i) Notificar los eventos elegidos a medida que se produzcan: Habilite esta casilla para generar notificaciones instantáneas, traps de SNMP o mensajes de syslog siempre que se produzcan los eventos seleccionados dentro de Password Manager Pro. Los traps de SNMP y los mensajes de syslog sólo se pueden generar si su administrador ha configurado una integración con soluciones de monitoreo.

ii) Notificar los eventos elegidos como un resumen diario: Habilite esta opción para recibir una única notificación cada día (que contenga información sobre los eventos seleccionados ocurridos durante el día) como un resumen diario.

iii) Notificación a: Seleccione los usuarios deseados, o proporcione los detalles de los usuarios a los que le gustaría enviar las notificaciones configuradas anteriormente.

iv) Depurar los registros de auditoría de recursos/usuarios/tareas: Para mantener suficiente espacio en disco, puede depurar los registros de auditoría más antiguos especificando el número de días que deben conservarse en Password Manager Pro. Por ejemplo, si selecciona 90, los registros de auditoría que tengan más de 90 días de antigüedad serán depurados automáticamente por Password Manager Pro.



b) Exportar a CSV / PDF

Haga clic en *Exportar a CSV* o *Exportar a PDF* en el menú desplegable de *Acciones de auditoría* para exportar las pistas de auditoría en el formato deseado y guardarlas para futuras consultas. Tenga en cuenta que si su administrador habilita el cifrado para todas las operaciones de exportación en Password Manager Pro, el archivo exportado estará protegido por contraseña y tendrá que proporcionar la frase de contraseña de cifrado para ver este archivo.

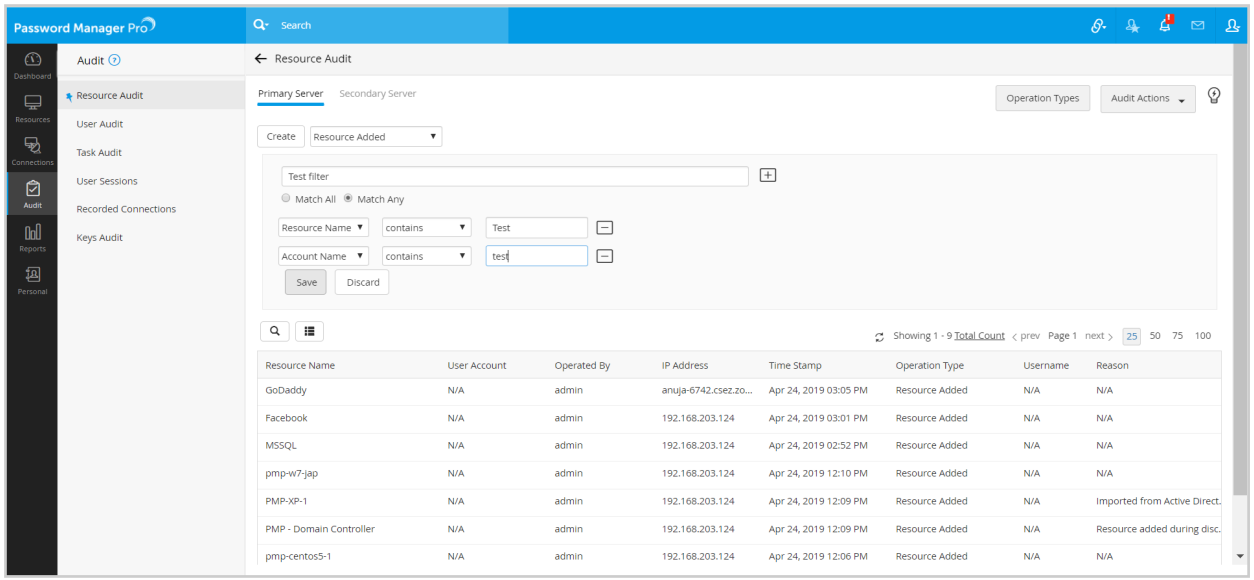
Puede ver o copiar la frase de contraseña iniciando sesión en Password Manager Pro y seleccionando *Ajustes de exportación* en el menú desplegable de *Mi perfil* en la esquina superior derecha.from the *My Profile* drop-down menu at the top right corner. Consulte la sección Exportar contraseñas para un acceso sin conexión seguro para obtener más detalles.

c) Enviar este informe por correo electrónico

Haga clic en este enlace bajo *Acciones de auditoría* para enviar los informes de auditoría de una sección específica a los usuarios deseados por correo electrónico.

d) Crear un filtro de auditoría

- Haga clic en el botón *Crear* para crear vistas personalizadas de las pistas de auditoría, añadiendo filtros para mostrando sólo aquellos registros de auditoría que sean de su interés.
- Proporcione un nombre para su filtro, ingrese sus criterios (si desea elegir un tipo de operación como uno de los criterios, haga clic en el botón *Tipos de operación* e ingrese el tipo preferido). Haga clic en *Guardar*.



e) Filtros de auditoría

Haga clic en el menú desplegable junto a Crear para mostrar las auditorías que pertenecen a una operación específica dentro de Password Manager Pro. Los filtros que cree se mostrarán bajo el título *Filtros personalizados* en el mismo menú desplegable.

f) Eliminar o editar un filtro personalizado

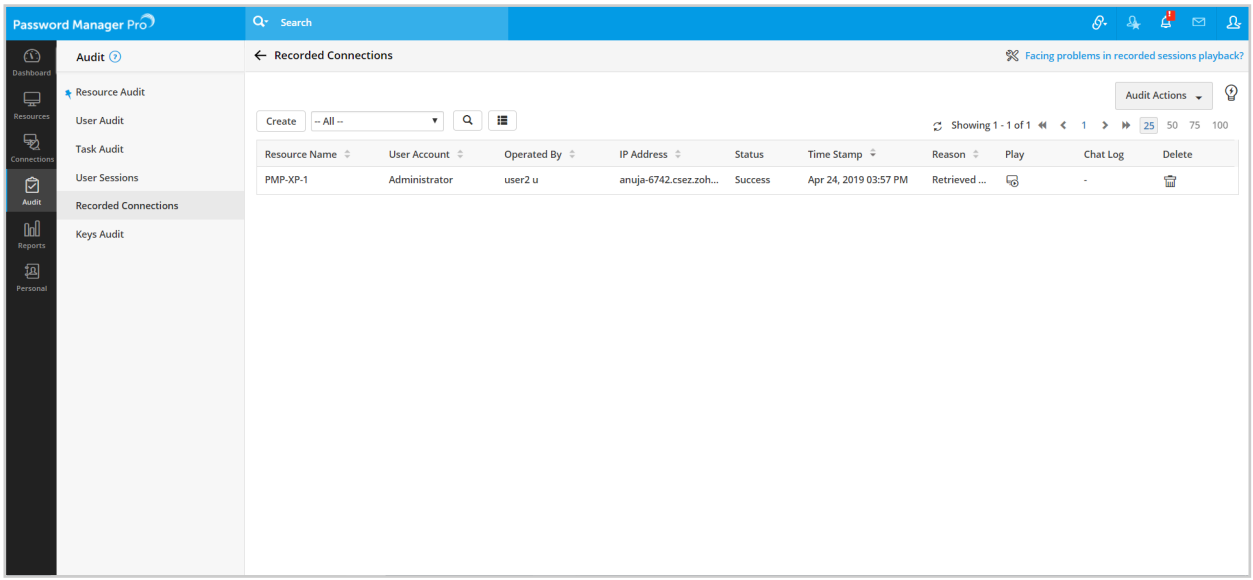
Puede eliminar o editar un filtro personalizado seleccionándolo en el menú desplegable y haciendo clic en los botones *Eliminar* o *Editar*.

g) Configurar la grabación de las sesiones

Para configurar las sesiones RDP, VNC, SSH y SQL, vaya a la pestaña *Conexiones grabadas*, haga clic en *Configurar la grabación de las sesiones*, y seleccione las opciones necesarias en la ventana que se abre. En esa misma ventana, también puede especificar en qué directorio almacenar los archivos grabados, definir el directorio para la copia de seguridad, y depurar las sesiones grabadas antes de un periodo de tiempo especificado.

h) Ver o reproducir las sesiones grabadas

- En la pestaña *Conexiones grabadas*, puede rastrear las sesiones utilizando el nombre del recurso, el usuario que inició la sesión, la hora a la que se inició la sesión, etc.



- Haga clic en el icono de *Reproducir* junto a cada entrada para ver la sesión grabada. Mientras visualiza una sesión grabada, puede ir a una parte específica de la grabación haciendo clic en la barra de búsqueda.

C. Informes

Password Manager Pro proporciona información sobre todo el proceso de gestión de cuentas privilegiadas en su empresa mediante informes completos. Puede obtener una visión más amplia y profunda de la gestión de contraseñas y de la actividad de los usuarios privilegiados en su organización con informes puntuales sobre los resúmenes del inventario de contraseñas, el cumplimiento de TI, el uso compartido de contraseñas, las estadísticas de acceso de los usuarios, el historial de restablecimiento de contraseñas y mucho más, lo que le ayudará a tomar decisiones bien informadas sobre la gestión de contraseñas.

Tipos de informes

Password Manager Pro proporciona informes en varias categorías y también le permite crear sus propios informes.

a) Informes de contraseña: Proporciona detalles sobre el número total de recursos, contraseñas y tipos de recursos en Password Manager Pro junto con los detalles de propiedad, el cumplimiento de la política de contraseñas, la caducidad de las contraseñas, el uso de las contraseñas, el flujo de trabajo del control de acceso a las contraseñas, las contraseñas no compartidas, etc.

b) Informes de usuario: Registra los detalles de todos los usuarios del sistema en relación con el acceso a las contraseñas y a los recursos, las acciones de los usuarios que implican contraseñas, los recursos y los grupos de recursos que posee/comparte cada usuario, los privilegios de los usuarios, los usuarios que pertenecen a todos los grupos de usuarios, el uso de contraseñas por parte de todos los usuarios del sistema, etc.

c) Informes generales: Proporciona información sobre todos los accesos con contraseña y las actividades de los usuarios en el sistema. Este informe es una combinación de los informes de contraseña y de usuario, y registra las estadísticas de las contraseñas, las actividades de las contraseñas, las políticas de contraseñas, la caducidad de las contraseñas, las contraseñas no sincronizadas, las estadísticas de los usuarios, las actividades de los usuarios, etc.

d) Informes de cumplimiento: Muestra el nivel de cumplimiento de su organización respecto a varias regulaciones gubernamentales y de la industria como GDPR, PCI-DSS, ISO/IEC-27001 y NERC-CIP.

e) Informes personalizados: Además de los diversos informes predeterminados, Password Manager Pro le permite aprovechar los datos disponibles para cumplir con los requisitos de auditoría, los mandatos de seguridad y diversos criterios de cumplimiento a través de informes personalizados. Por ejemplo, puede generar informes específicos del departamento para sus auditorías de seguridad, extraer la lista de recursos a los que un antiguo empleado tenía acceso, agregar cierta información sobre el acceso privilegiado y generar un informe integrado para demostrar el cumplimiento de las normas de TI.

Acciones de informes

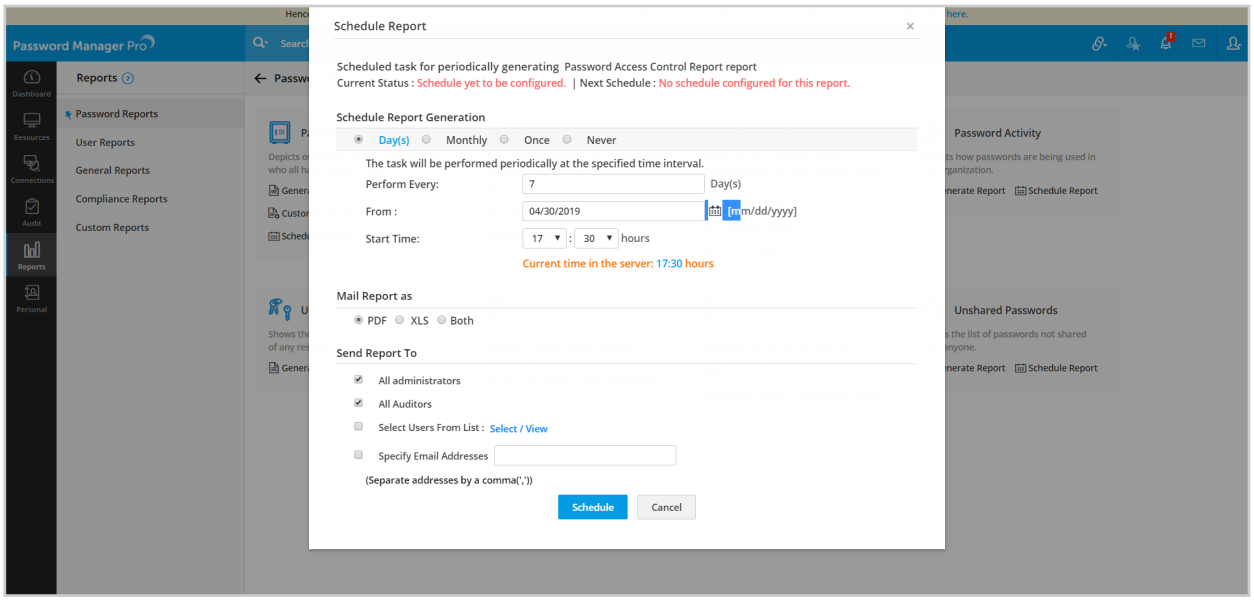
a) Generar informes: Esto le ayuda a generar instantáneamente el informe correspondiente en una nueva ventana.

b) Personalizar informes: Este enlace, que se encuentra en la sección de informes de contraseña, le permite personalizar un informe predeterminado. Después de establecer los criterios necesarios, puede generar un informe al instante haciendo clic en *Generar informe*, o guardar el informe para su uso futuro haciendo clic en *Guardar*.

Una vez guardado, el informe estará disponible en la sección de Informes personalizados.

c) Programar informes: Envíe el informe por correo electrónico en formato PDF y/o Excel a los usuarios requeridos de forma diaria, mensual o puntual. Puede elegir los destinatarios como un conjunto (todos los administradores/auditores), seleccionar usuarios individuales de la lista o proporcionar las direcciones de correo electrónico de los usuarios requeridos.

Nota: *Las programaciones que se creen aquí se someten a auditoría y los resultados estarán disponibles en la sección de Auditoría de tareas en la pestaña de Auditoría.*

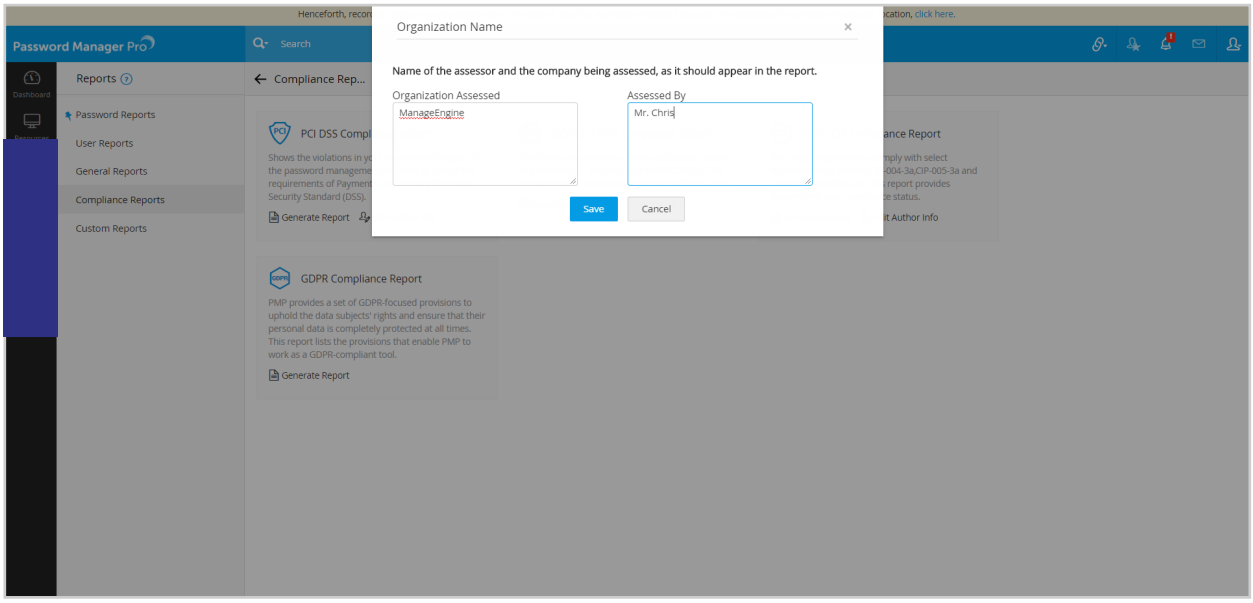


d) Programar la verificación de la integridad: Disponible en la categoría de informe de *Contraseñas no sincronizadas*, esta opción le ayuda a programar una verificación de la integridad diaria o mensualmente para averiguar qué cuentas tienen contraseñas almacenadas en Password Manager Pro que no están sincronizadas con las contraseñas correspondientes en los sistemas de destino. Para comprobar la integridad de las contraseñas, Password Manager Pro intentará iniciar sesión en los recursos de destino para los que se ha habilitado el restablecimiento remoto de contraseñas utilizando las credenciales almacenadas en la base de datos de Password Manager Pro. Si el inicio de sesión falla, Password Manager Pro concluye que la contraseña no está sincronizada.

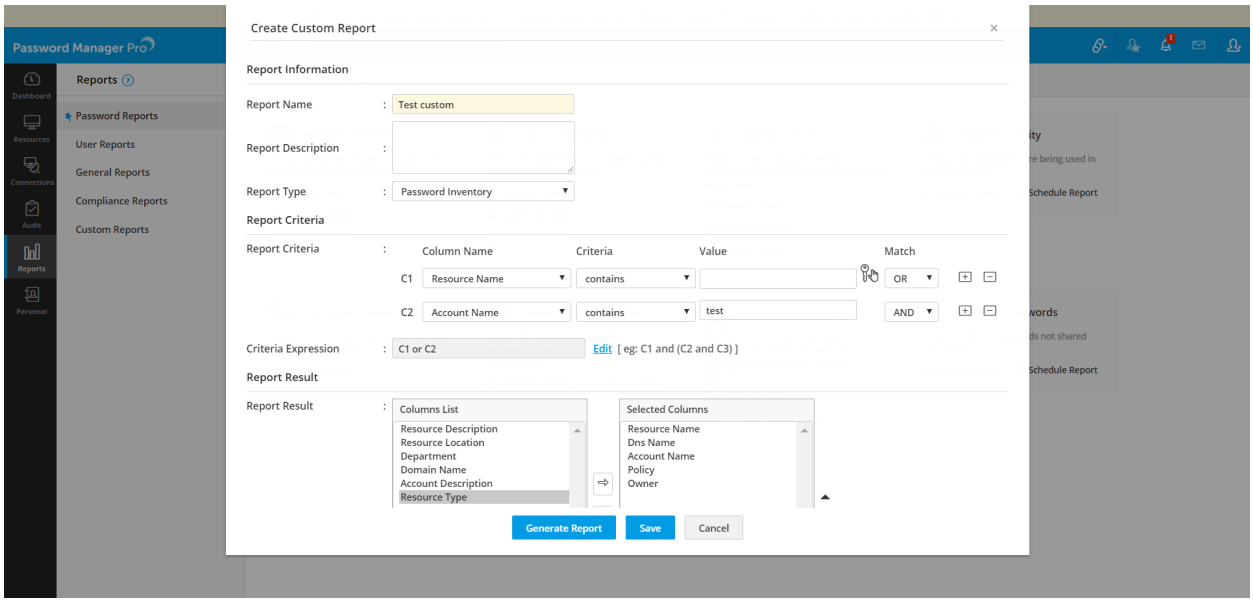
Nota: *Las programaciones que se creen aquí se someten a auditoría y los resultados estarán disponibles en la sección de Auditoría de tareas en la pestaña de Auditoría.*

e) Encontrar las contraseñas no sincronizadas: Esta opción de la categoría de informe de Contraseñas no sincronizadas proporciona una lista detallada de las contraseñas. Menciona qué contraseñas no están sincronizadas, a quién pertenecen y su tipo de recurso.

f) Editar la información del autor: Esta opción, que se encuentra bajo el informe de cumplimiento, le permite proporcionar el nombre de la organización que se está evaluando y el nombre del evaluador que quiere que aparezca en la *Información de contacto* en el informe generado.



g) Crear informe personalizado: Este botón bajo *Informes personalizados* le ayuda a generar un informe personalizado al instante, o a guardarlo para el futuro. El menú desplegable de la esquina superior derecha le ayuda a filtrar los informes personalizados en función del tipo de informe que haya proporcionado al crearlo.



Nota: *No se puede acceder a las pestañas Dashboard, Informes y Auditoría desde las aplicaciones móviles.*

www.passwordmanagerpro.com

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.passwordmanagerpro.com

ManageEngine
Password Manager Pro

For queries: hello@passwordmanagerpro.com
For demo: demo.passwordmanagerpro.com