ManageEngine
Password Manager Pro

GUÍA DE INICIO

Para los administradores de Password Manager Pro

www.passwordmanagerpro.com

Índice

Introducción

Gracias por elegir Password Manager Pro de ManageEngine para gestionar las identidades privilegiadas de su organización. Esta guía le proporcionará la información básica necesaria para ayudarle a empezar.

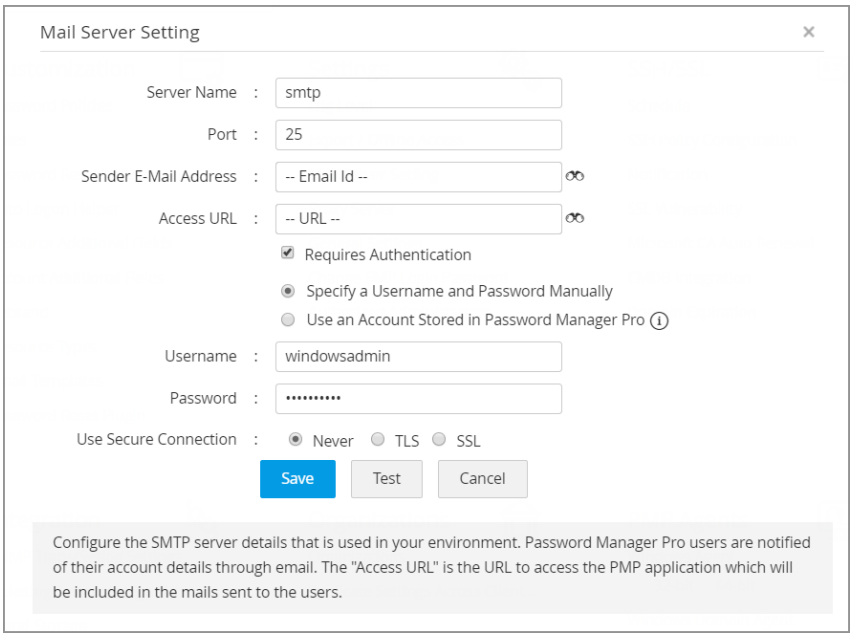
Instalación

Si aún no ha instalado Password Manager Pro, siga los pasos detallados en el manual de usuario e instálelo. Esta guía le ayudará a iniciar el servidor y a conectarse a la interfaz web.

Configuraciones básicas

Configure el servidor de correo

Después de la instalación, es necesario configurar algunos ajustes básicos. En primer lugar, configure el servidor de correo para que Password Manager Pro pueda enviar correos electrónicos directamente desde la aplicación, sin necesidad de un cliente de correo externo. Aquí también necesita configurar los detalles del servidor SMTP. Los usuarios de Password Manager Pro son notificados de los detalles de su cuenta y de las acciones de la contraseña sólo a través del correo electrónico, por lo que es importante que esto se ajuste correctamente.

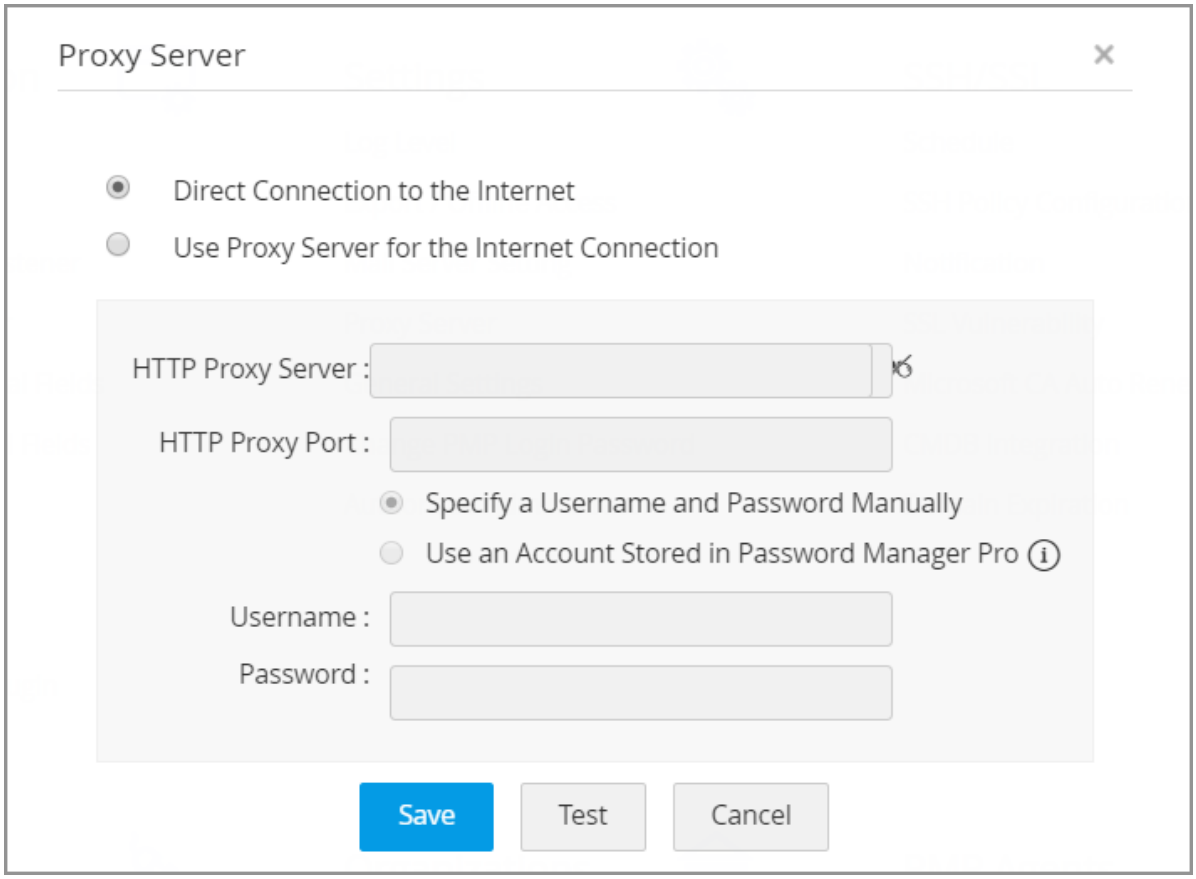


Introduzca todos los detalles, incluido el nombre del servidor, el puerto, el ID de correo electrónico del remitente, la URL de acceso y el tipo de autenticación. A continuación, guarde la configuración.

R|{qus£ p px } |¦§

A continuación, especifique cómo se va a conectar a Internet: directamente o a través de un proxy. Configure este ajuste yendo a la pestaña **Admin**, en **Settings** > **Proxy Server.**
Aquí verá dos opciones:

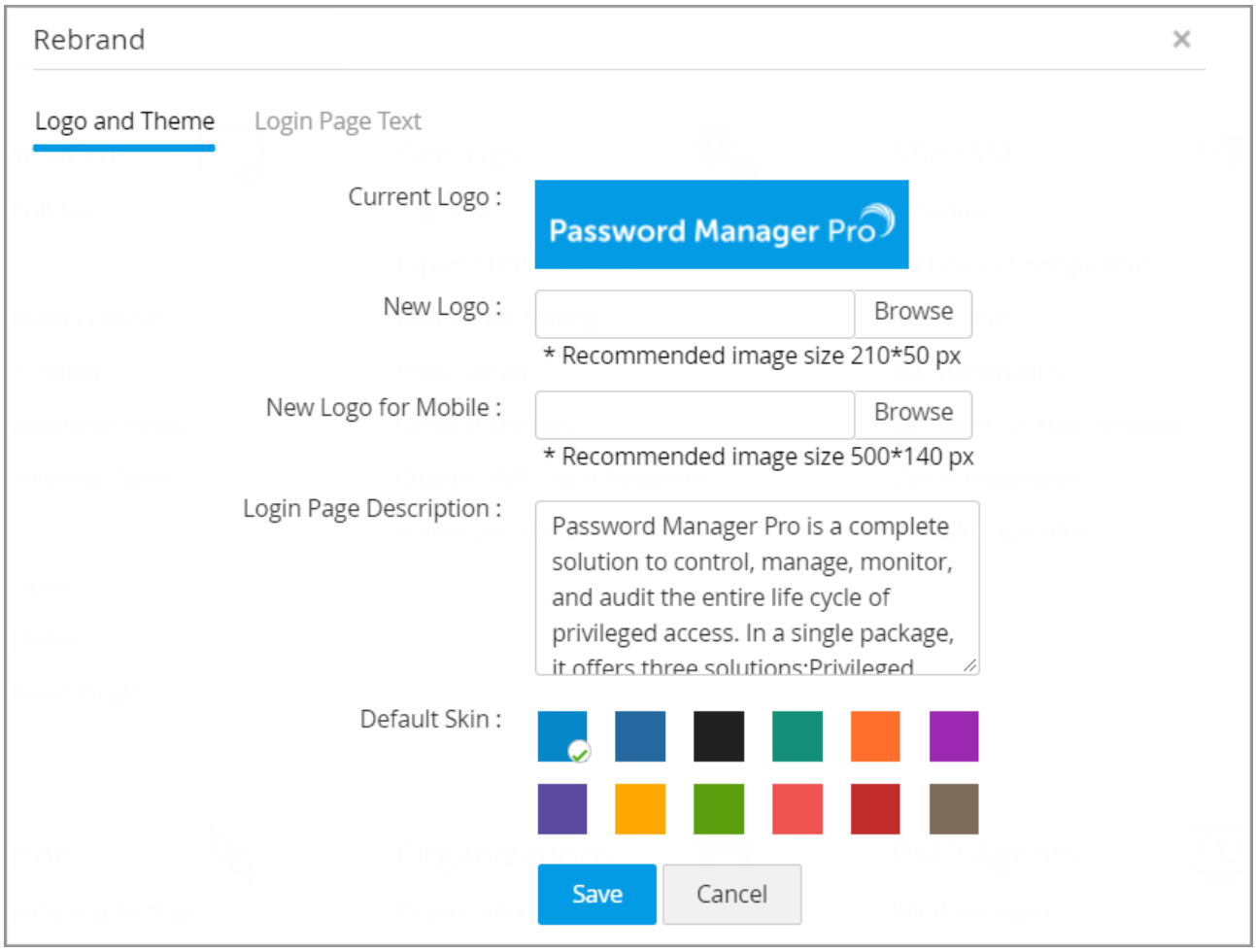
- Conexión directa a Internet
- Utilizar un servidor proxy para la conexión a Internet

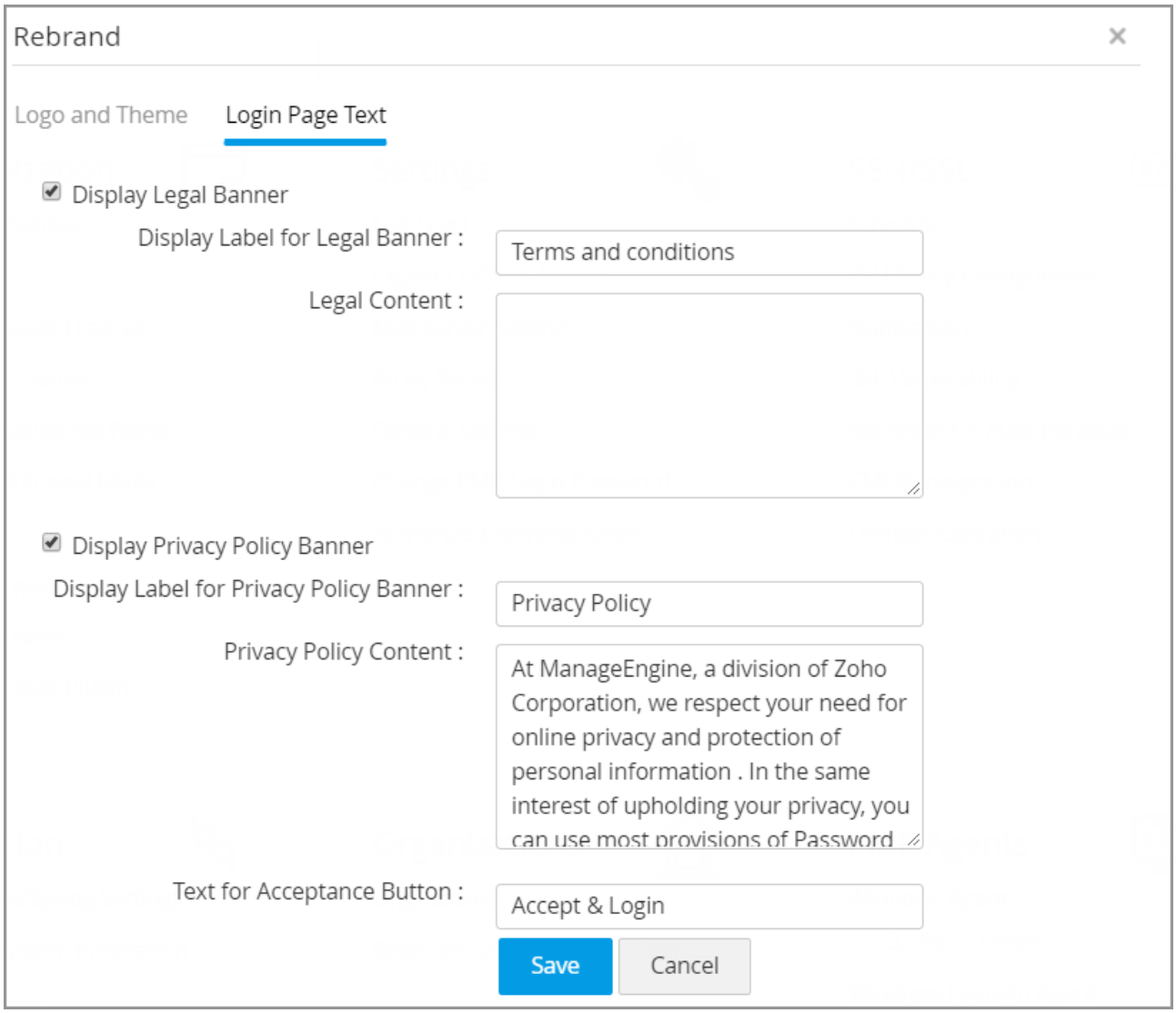


Si su conexión a Internet es a través de un proxy, configure los ajustes del servidor proxy, como el nombre del servidor proxy HTTP, el puerto proxy, el tipo de autenticación y el nombre de usuario y la contraseña utilizados para la conexión.

Cambie el logotipo

Si desea sustituir el logotipo de Password Manager Pro en la GUI por el de su empresa, puede hacerlo con un simple cambio en los ajustes. El tamaño recomendado del logotipo es de 210 x 50 píxeles. Para efectuar el cambio, vaya a la pestaña **Admin** y haga clic en **Rebrand** en la sección **Customize**.





Además del cambio de logotipo, se pueden realizar otras personalizaciones, como cambiar la descripción de la página de inicio de sesión y el color del aspecto de la GUI, o mostrar un banner específico de la empresa para la política de privacidad y los fines legales.

Para obtener instrucciones detalladas sobre el cambio de marca, puede consultar este documento de ayuda.

Aprovisionamiento y gestión de usuarios

Después de configurar los ajustes básicos, el siguiente paso es crear cuentas para sus usuarios en Password Manager Pro.

Agregue usuarios

Hay varias formas de agregar usuarios a Password Manager Pro. Password Manager Pro ofrece la opción de importar usuarios desde almacenes de identidades corporativas como AD, LDAP o Azure AD a través de la integración. También puede importar usuarios de forma masiva desde un CSV o agregar usuarios manualmente. Para obtener información detallada sobre la adición de usuarios, consulte los documentos que figuran a continuación:

- Importe usuarios desde AD o LDAP
- Importe usuarios desde LDAP
- Importe usuarios desde Azure AD
- Importe usuarios desde CSV
- Agregue usuarios manualmente

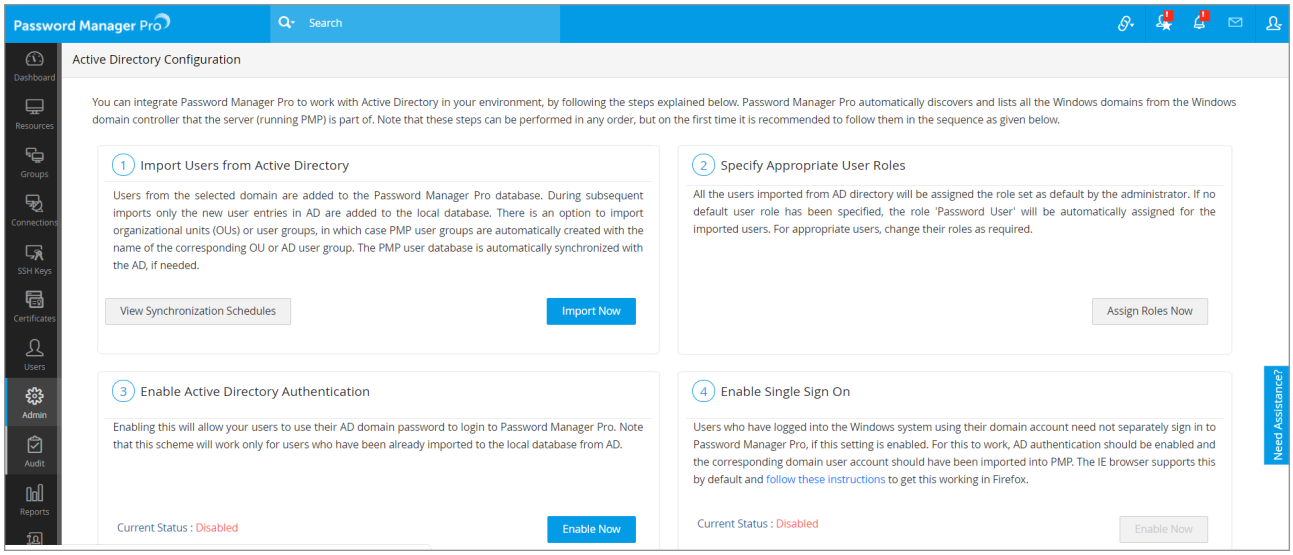
Establezca una autenticación de primer nivel

Dado que Password Manager Pro sirve como bóveda para las contraseñas sensibles, es esencial tener un mecanismo de autenticación sólido para conceder el acceso al software. Password Manager Pro ofrece varias opciones de autenticación y los usuarios pueden elegir las que mejor se adapten a su entorno. Aparte de la autenticación local de Password Manager Pro, está la opción de aprovechar la autenticación de almacenes de identidad externos como Active Directory/LDAP.

Autenticación a través de AD

Para permitir que los usuarios inicien sesión en Password Manager Pro utilizando sus contraseñas de dominio de AD, vaya a **Admin** > **Authentication** > **Active Directory** y active la opción de autenticación de Active Directory.

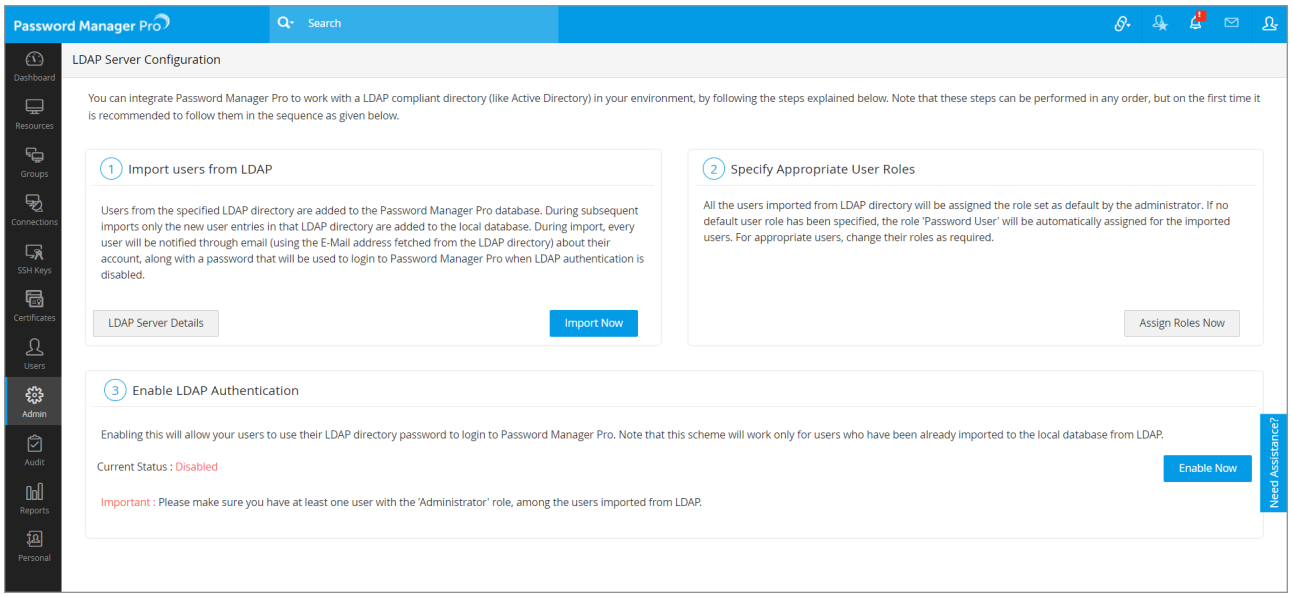
> **Nota:** Este esquema de autenticación sólo funcionará para los usuarios que ya han sido importados a la base de datos local desde Active Directory.



Autenticación a través de LDAP

Para permitir que los usuarios inicien sesión en Password Manager Pro utilizando sus contraseñas del directorio LDAP, vaya a **Admin** > **Authentication** > **LDAP** y active la opción de autenticación LDAP.

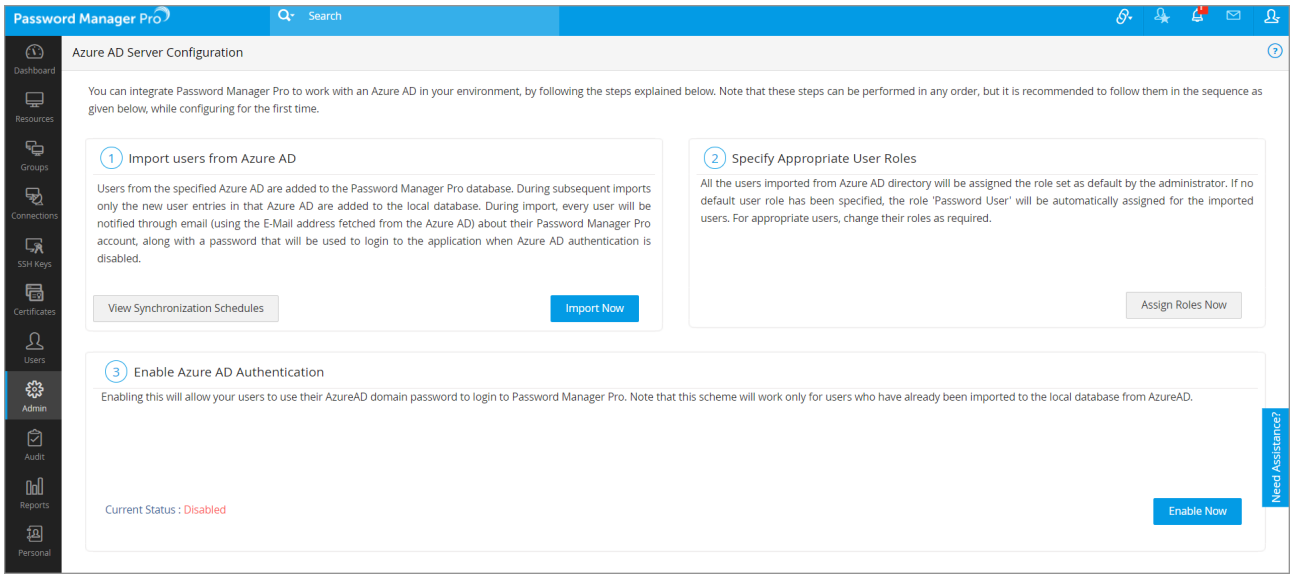
> **Nota:** Este esquema de autenticación sólo funcionará para los usuarios que ya han sido importados a la base de datos local desde LDAP.



Autenticación a través de Azure AD

Para permitir que los usuarios inicien sesión en Password Manager Pro utilizando sus contraseñas de dominio de Azure AD, vaya a **Admin** > **Authentication** > **Azure AD** y active la opción de autenticación de Azure AD.

> **Nota:** Este esquema de autenticación sólo funcionará para los usuarios que ya han sido importados a la base de datos local desde Azure AD.



Además de esto, Password Manager Pro también ofrece los siguientes mecanismos de autenticación de primer nivel:

Autenticación con smart-card

Si tiene un sistema de autenticación con tarjeta inteligente en su entorno, puede configurar Password Manager Pro para autenticar a los usuarios con sus tarjetas inteligentes y su número de identificación personal (PIN), evitando otros métodos de autenticación de primer factor como AD, LDAP o autenticación local.

Para activar esta configuración, vaya a la pestaña **Admin** > **Authentication** > y seleccione **Smart card /PKI / Certificate** en la interfaz web. Para obtener instrucciones detalladas para configurar la autenticación con tarjeta inteligente, consulte esta sección de la documentación de ayuda.

RADIUS

Puede integrar Password Manager Pro con el servidor RADIUS en su entorno y aprovechar la autenticación RADIUS para el acceso de los usuarios, evitando la autenticación local proporcionada por PMP.

Para activar esta configuración, vaya a la pestaña **Admin** > **Authentication** > y seleccione **RADIUS** en la interfaz web. Para obtener instrucciones detalladas sobre la integración del servidor RADIUS, consulte esta sección de la documentación.

SAML SSO

Password Manager Pro ofrece compatibilidad con SAML 2.0, que facilita la integración con soluciones de gestión de identidades federadas para el inicio de sesión único. PMP actúa como proveedor de servicios (SP) y se integra con los proveedores de identidad (IdP) utilizando SAML 2.0. La integración implica el suministro de detalles sobre el SP al IdP y viceversa. Una vez que se integra PMP con un IdP, los usuarios sólo tienen que iniciar sesión en el IdP y, a continuación, pueden iniciar sesión automáticamente en PMP desde la GUI del respectivo proveedor de identidad sin tener que volver a proporcionar las credenciales.

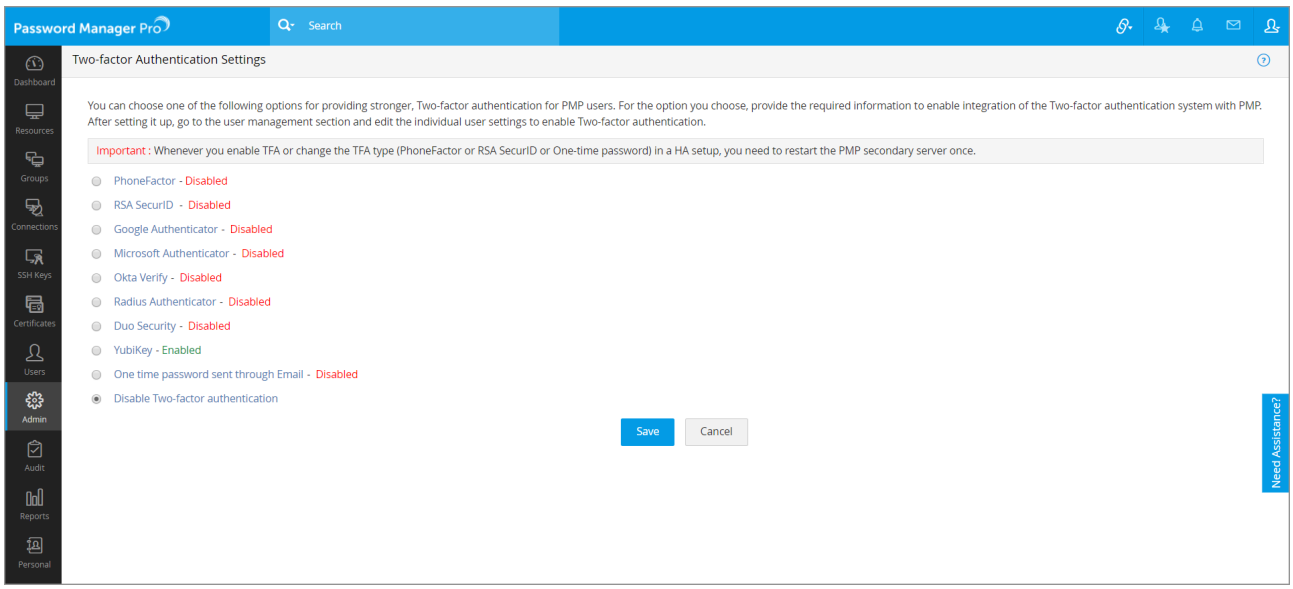
Para activar esta configuración, vaya a la pestaña **Admin** > **Authentication** > y seleccione **SAML Single Sign On** en la interfaz web. Para obtener instrucciones detalladas sobre la autenticación SAML Single Sign On, consulte esta sección de la documentación.

Configure la autenticación de dos factores (recomendado)

Si su organización requiere una capa adicional de seguridad, puede configurar la autenticación de dos factores (TFA) y obligar a los usuarios a pasar por dos etapas sucesivas de autenticación antes de iniciar la sesión. Una vez configurado, sus usuarios tendrán que pasar por dos pasos:

1. Autenticación de primer nivel a través de AD, LDAP, o nativo.
2. Autenticación de segundo nivel a través de alguno de los siguientes mecanismos:
    - PhoneFactor
    - RSA SecurID
    - Google Authenticator
    - Microsoft Authenticator

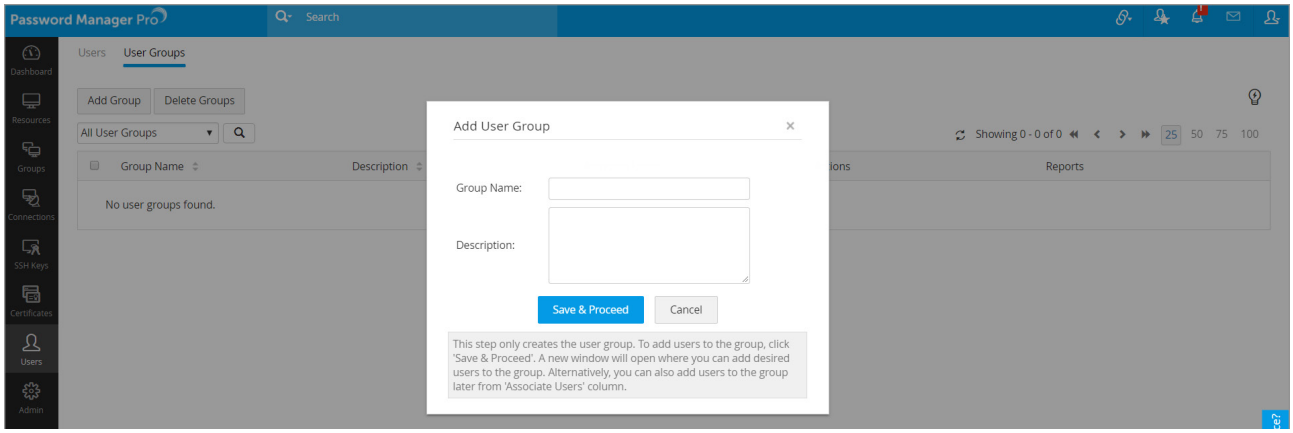
- Okta Verify
- RADIUS Authenticator
- Duo Security
- Yubikey
- A unique one time password through email



Para activar esta configuración, vaya a la pestaña **Admin** > **Authentication** > **Two-factor Authentication** en la interfaz web.

Cree grupos de usuarios

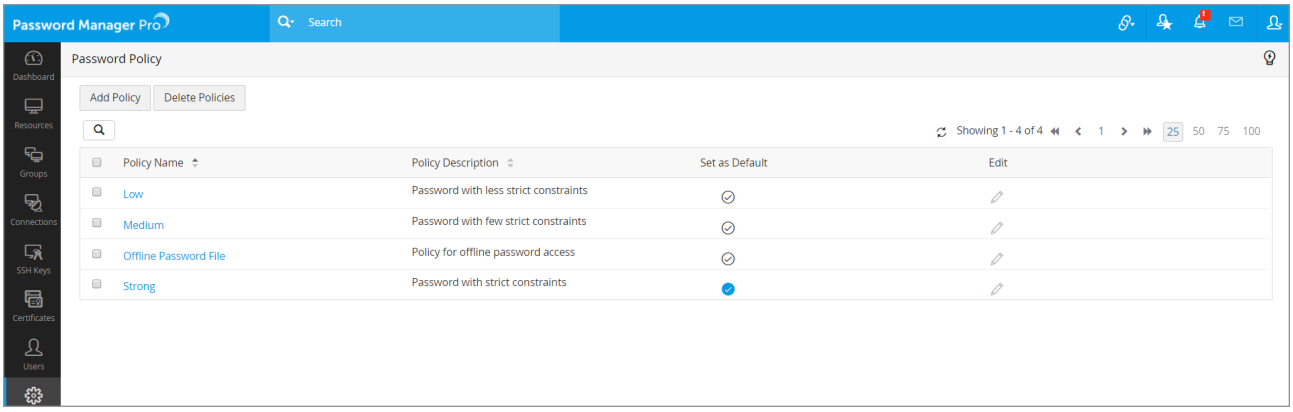
Después de agregar usuarios, puede agruparlos para realizar operaciones de forma masiva. Por ejemplo, puede crear un grupo de usuarios para todos los administradores de Windows y luego asignar contraseñas de forma masiva a este grupo de usuarios en particular. Para crear un grupo de usuarios, vaya a la pestaña **Users** > **User Groups** y haga clic en **"Add Group"**. Encontrará información detallada sobre la creación de grupos de usuarios en esta sección de nuestra documentación de ayuda.



Establezca la política de contraseñas

Password Manager Pro ayuda a aplicar políticas de contraseñas sólidas a todos los niveles, ya sean las contraseñas de autenticación local de los usuarios o las contraseñas de los recursos de TI gestionados. Password Manager Pro viene con un generador de contraseñas integrado que puede generar contraseñas basadas en el nivel de complejidad definido en las políticas de contraseñas.

Puede especificar varias condiciones, como la longitud mínima, los caracteres mixtos, los números, etc., y el generador creará las contraseñas según sea necesario. Por defecto, Password Manager Pro ofrece tres tipos de políticas: baja, media y sólida. Puede elegir una de ellas o crear su propia política personalizada. Puede crear nuevas políticas de contraseñas desde la sección **Admin** > **Customize** > **Password Policies**.



Puede encontrar instrucciones detalladas sobre la configuración de las políticas de contraseñas en esta sección de nuestra documentación de ayuda.

Gestión de contraseñas

Agregue sus recursos

El término "recurso" se refiere a todos los dispositivos y aplicaciones cuyas cuentas privilegiadas deben ser gestionadas por Password Manager Pro. Hay varias formas de añadir sus recursos a Password Manager Pro:

- Analice su red y descubra versiones de Windows, Linux, Vmware y dispositivos de red, junto con sus cuentas privilegiadas asociadas.
- Importe los recursos de Windows desde su dominio.
- Importe recursos dispares de forma masiva desde un archivo CSV o archivo separado por tabulaciones.

Cuando se carga la información de los recursos a través de un archivo CSV o archivo separado por tabulaciones, se puede compartir de dos maneras

1. Como un archivo normal
2. Como archivo ZIP protegido por contraseña

Archivo normal: Esta opción se puede utilizar para cargar directamente un archivo de texto plano CSV o archivo separado por tabulaciones en el que los datos se guardan como valores separados por comas o por tabulaciones.

Archivo ZIP protegido por contraseña: Esta opción se puede utilizar si desea cargar una carpeta ZIP protegida por contraseña que contenga el archivo CSV o archivo separado por tabulaciones. Si elige este formato de archivo, también debe proporcionar la contraseña y especificar el nombre del archivo CSV o archivo separado por tabulaciones de destino, en el campo "File Name". Si el campo "File Name" se deja vacío, PMP importará automáticamente la información del primer archivo CSV o archivo separado por tabulaciones, al que haya accedido en la carpeta descomprimida.

- Agregue los recursos uno a uno, manualmente.

Puede encontrar información detallada sobre las opciones anteriores en las siguientes secciones de nuestra documentación de ayuda.

- Descubrimiento de cuentas privilegiadas
- Importación de recursos desde Active Directory y a través de un archivo CSV o archivo separado por tabulaciones o KeePass
- Agregar recursos manualmente

Cree grupos de recursos

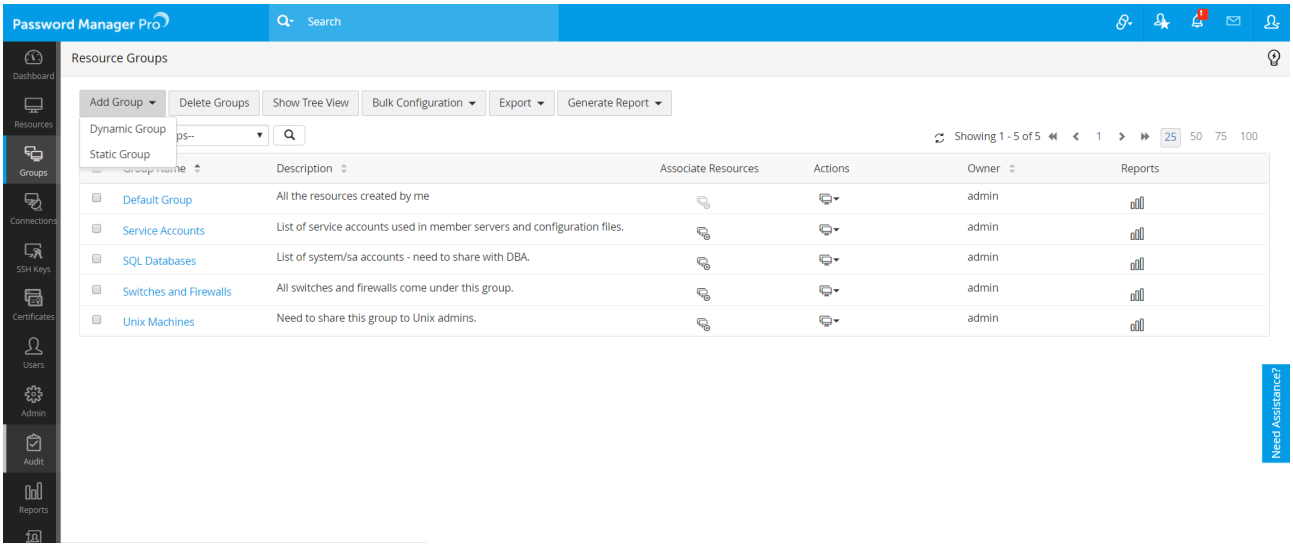
Después de agregar recursos, puede agruparlos para organizarlos mejor y facilitar su gestión. Los recursos pueden agruparse especificando un conjunto de criterios o seleccionando recursos individuales.

En el caso de los grupos estáticos, los recursos deben agregarse y eliminarse manualmente, según sea necesario. Mientras que en el caso de un grupo dinámico, es decir, basado en criterios, cada vez que un recurso recién añadido coincide con los criterios de un grupo existente, pasa a formar parte automáticamente de ese grupo.

Cuando se añade o se elimina un recurso de un grupo, esto afecta al acceso con contraseña compartido a través del grupo. Es decir, cuando se comparte un determinado grupo de recursos con los usuarios, éstos pueden ver las contraseñas sólo de los recursos que forman parte del grupo en el momento de compartirlo.

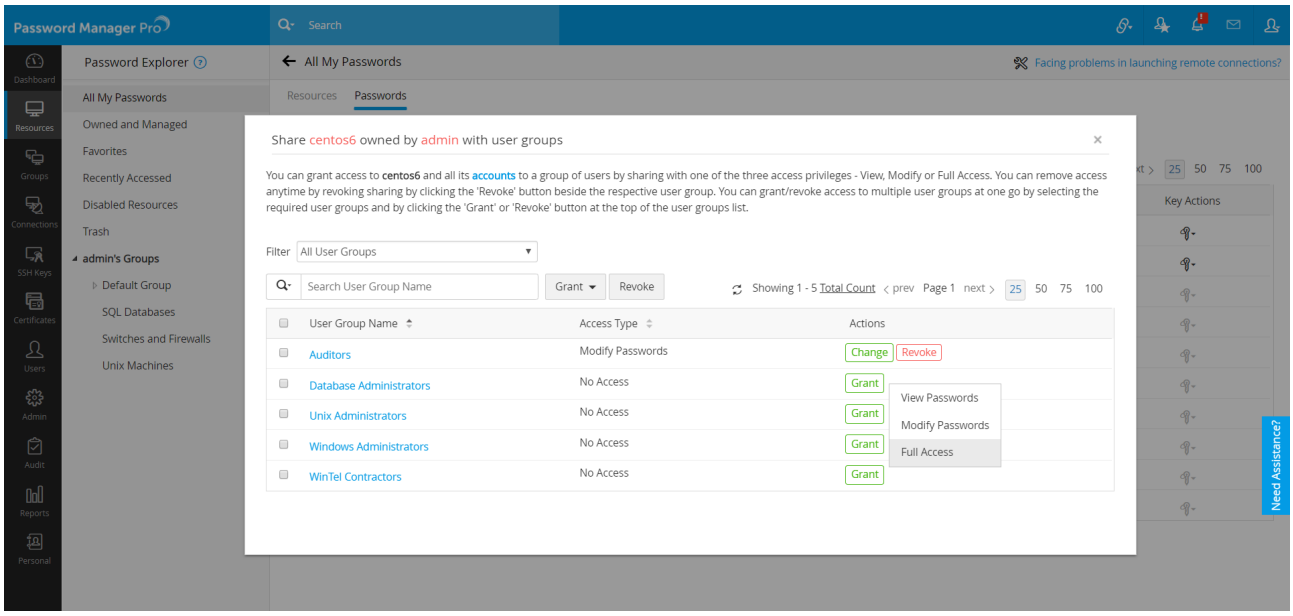
Para crear un grupo(s) de recursos, navegue hasta **Groups,** haga clic en **Add Group** y luego seleccione **Dynamic Group** o **Static Group.**

Encontrará instrucciones detalladas para crear grupos de recursos en esta sección de nuestra documentación.



Comparta cuentas, recursos y grupos de recursos

Con un solo clic, puede compartir una cuenta individual o todas las cuentas de un recurso o un grupo de recursos con cualquier usuario o grupo de usuarios. Al compartir recursos con otros usuarios, también puede establecer diferentes privilegios de acceso:



Ver contraseñas: Los usuarios y grupos de usuarios sólo pueden acceder a las contraseñas.

Modificación de contraseñas: Los usuarios y grupos de usuarios pueden ver y editar las contraseñas de los recursos compartidos. Sin embargo, este privilegio no les permite acceder a la sección "Resource Actions" (Acciones del recurso), que restringe a los usuarios la posibilidad de cambiar cualquier otro atributo del recurso.

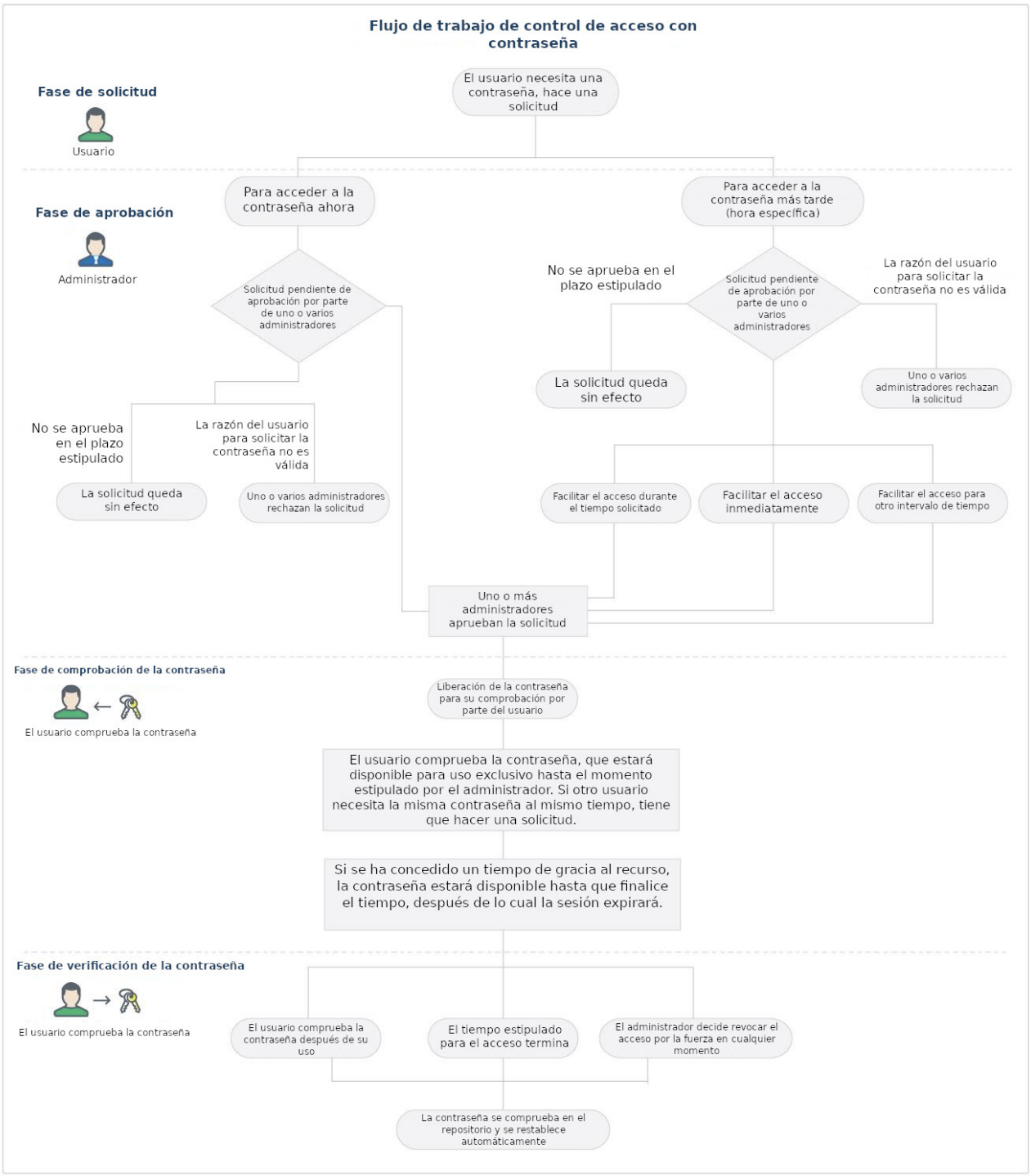
Acceso completo: Los usuarios y los grupos de usuarios tienen una gestión completa del recurso/grupo de recursos. Incluso pueden volver a compartir el recurso o la contraseña con otros usuarios.

Puede encontrar información detallada sobre cómo compartir recursos en esta sección de nuestra documentación.

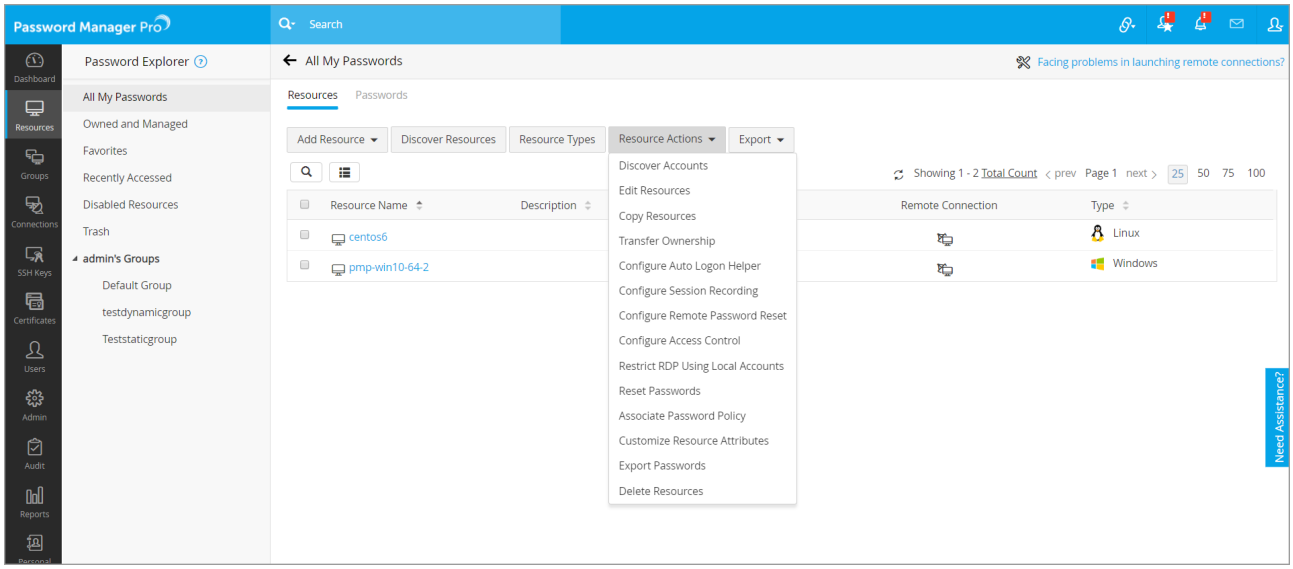
Nota: Password Manager Pro permite a los usuarios compartir contraseñas sin revelarlas en texto plano en la GUI. Esto se puede hacer desde **Admin** > **General Settings** > **Password Retrieval**. La casilla de verificación de la opción **"Allow plain text view of passwords, if auto logon is configured"** no debe ser seleccionada para ejercer esta opción.

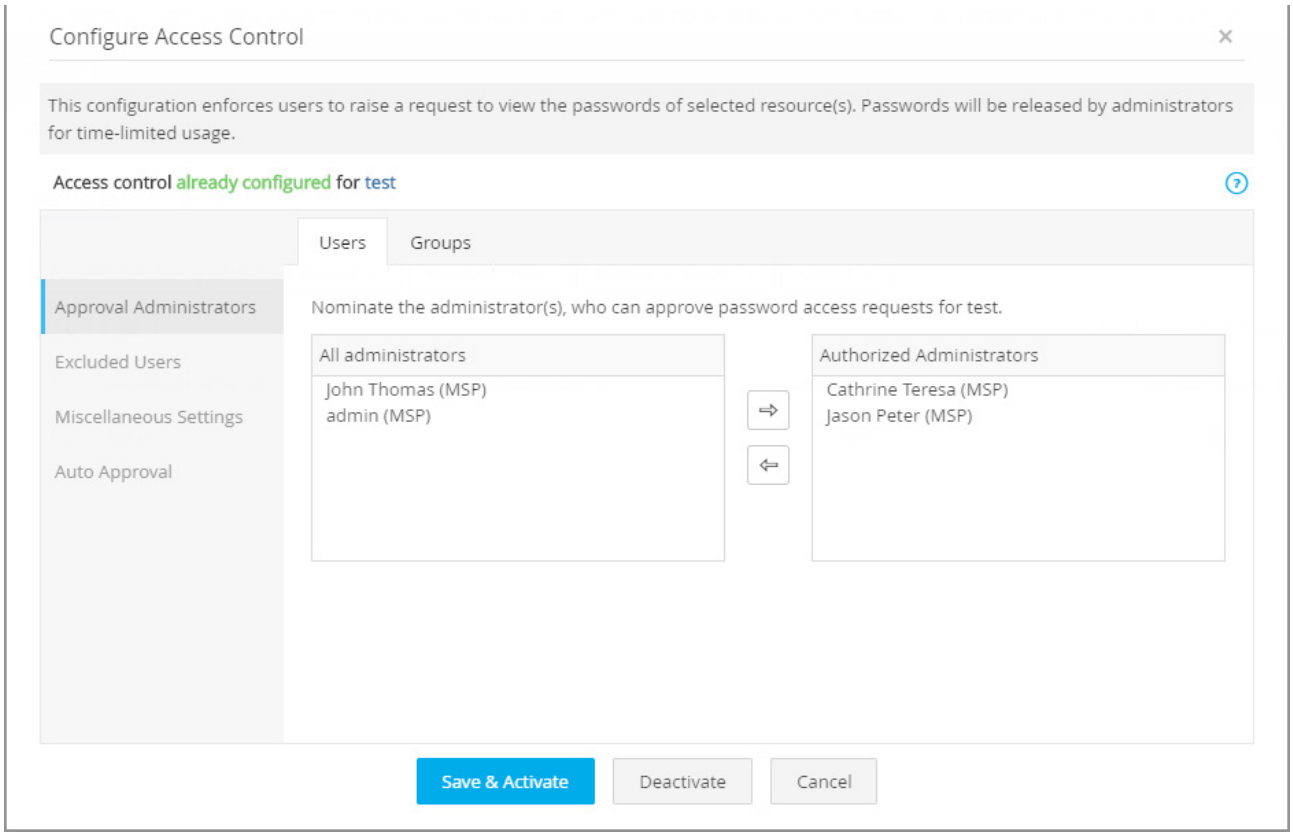
Configure el flujo de trabajo de control de acceso

Después de un inicio de sesión exitoso en Password Manager Pro, los usuarios obtienen acceso instantáneo a las contraseñas que son de su propiedad o compartidas con ellos. Si es necesario, puede añadir una capa adicional de seguridad exigiendo a sus usuarios que pasen por una aprobación de solicitud y liberación. Este mecanismo sigue un flujo de trabajo bien definido: los usuarios sólo obtienen acceso tras la aprobación administrativa. La contraseña puede ser liberada por un período de tiempo limitado, al final del cual se restablecerá automáticamente.



Para configurar los controles de acceso, vaya a la pestaña de **Resource**, seleccione los recursos para los que desea configurar los controles de acceso y haga clic en **Configure Access Control** en el menú desplegable de **Resource Actions**.





Puede encontrar instrucciones detalladas y casos de uso para configurar los flujos de trabajo de control de acceso en esta sección de nuestra documentación.

Configure el restablecimiento remoto de la contraseña

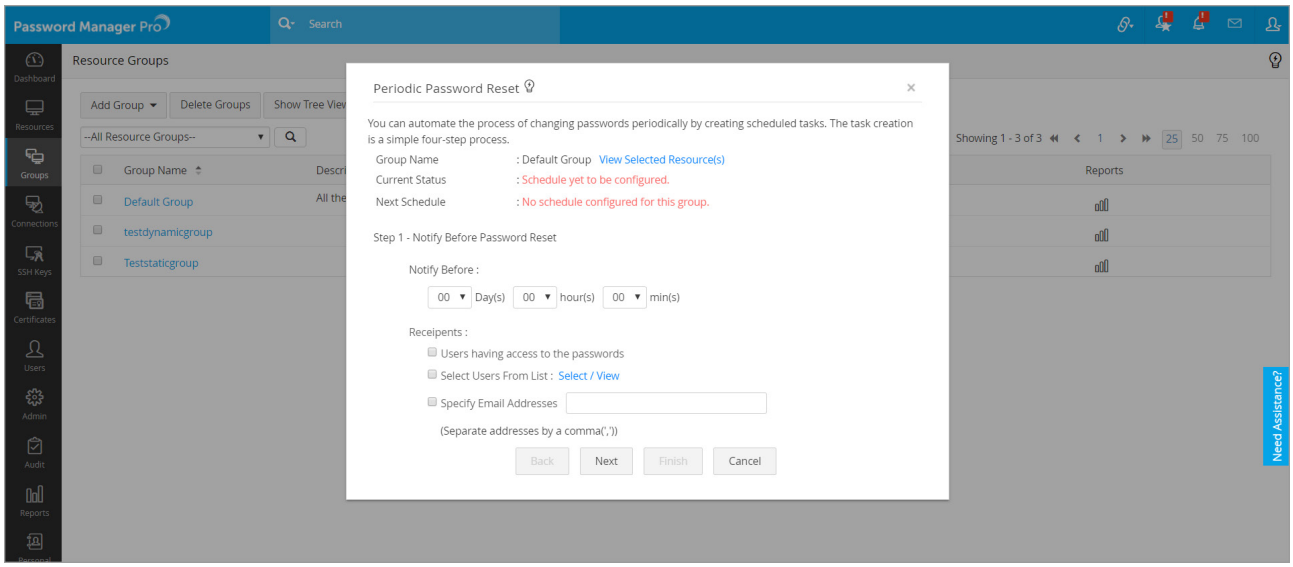
Password Manager Pro le ayuda a restablecer las contraseñas de una amplia gama de sistemas de destino bajo demanda en cualquier momento o automáticamente a intervalos periódicos en múltiples plataformas a través de infraestructuras físicas, virtuales y en la nube. El restablecimiento de la contraseña puede hacerse de dos maneras:

Con agentes	Los restablecimientos basados en agentes resultan útiles cuando hay que restablecer las contraseñas de recursos sin conectividad directa, como los que se encuentran en ubicaciones DMZ o con restricciones de firewall. Para llevar a cabo estos restablecimientos de contraseña, Password Manager Pro implementa un agente en el host remoto para ejecutar la tarea. Toda la comunicación entre el agente y el servidor de aplicaciones es unidireccional y a través de HTTPS.
Sin agentes	Password Manager Pro se conecta directamente al sistema de destino y cambia la contraseña.

Se pueden enviar notificaciones a los usuarios antes y después del proceso de restablecimiento remoto de la contraseña. La configuración básica necesaria para el restablecimiento remoto de la contraseña puede llevarse a cabo como parte de la adición de recursos. En el caso de los recursos ya añadidos, esto también se puede llevar a cabo editando los recursos. Esta configuración depende del tipo de recurso que se añada. En esta sección de nuestra documentación encontrará instrucciones detalladas para configurar el restablecimiento remoto de la contraseña para diferentes tipos de recursos.

Configure el restablecimiento periódico de la contraseña

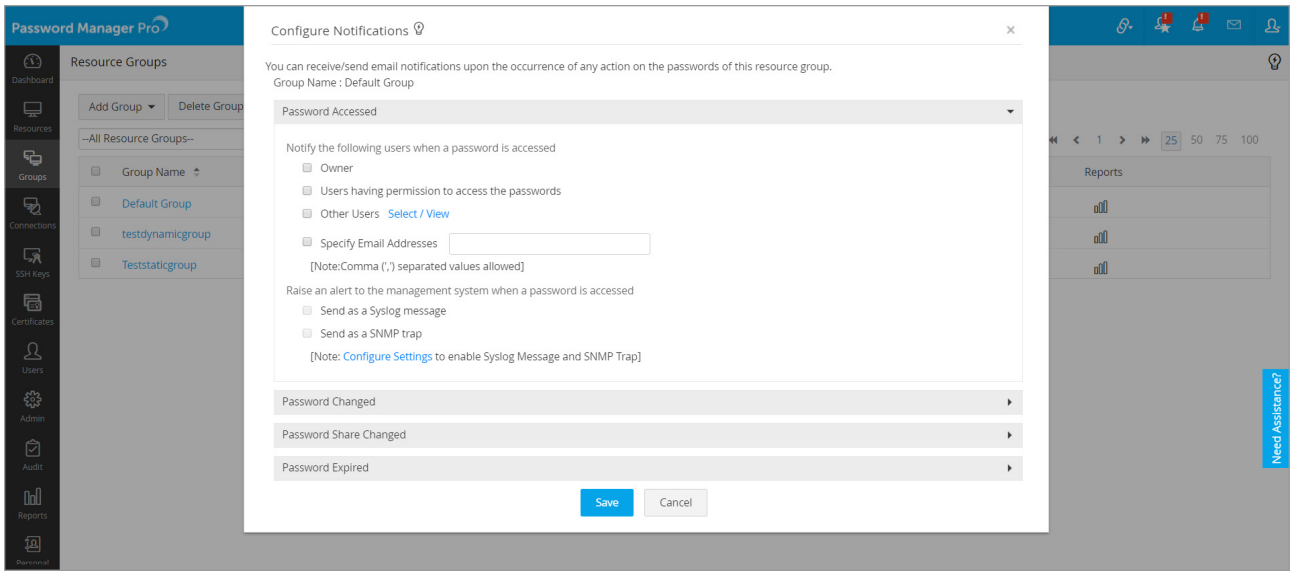
Puede restablecer periódicamente las contraseñas de los recursos remotos creando programas de restablecimiento. Esto puede hacerse a nivel de grupo de recursos. Password Manager Pro asignará una contraseña sólida y única a cada cuenta perteneciente al grupo de recursos. Para configurar el restablecimiento periódico de la contraseña, vaya a la pestaña Grupos, haga clic en el icono **"Actions"** frente al grupo de recursos requerido y seleccione Periodic Password Reset en el menú desplegable.



En esta sección de nuestra documentación encontrará información detallada sobre la configuración de los calendarios de restablecimiento de contraseñas.

Configure las notificaciones para las acciones de contraseña

Cuando se realiza cualquier acción sobre una contraseña -ya sea un acceso a la misma, una modificación, o el cambio del permiso de compartición cuando la contraseña caduca o cuando se infringe la política de contraseñas- se envían notificaciones a los propietarios de las contraseñas, a los que tienen acceso a las mismas, y/o a cualquier otro usuario que deseen los administradores. La función de notificación de acción de contraseña le ayuda a conseguirlo.



Estos ajustes pueden configurarse a nivel de grupo de recursos. Vaya a la pestaña de Grupos, haga clic en el icono de **"Actions"** frente al grupo para el que necesita activar las notificaciones de acciones y seleccione **"Configure Notifications"** en la lista desplegable. Puede encontrar información detallada sobre la configuración de las notificaciones de acciones de contraseña en esta sección de nuestra documentación.

Funciones avanzadas

Conexión directa a sitios web y aplicaciones

Al configurar el inicio de sesión automático, puede lanzar una conexión directa a sitios web y aplicaciones desde la interfaz web de Password Manager Pro. Esto puede hacerse mediante el uso de extensiones nativas del navegador.

Puede encontrar información detallada sobre las extensiones de los navegadores Chrome, Firefox e IE en las siguientes secciones de nuestra documentación.

- Extensión del navegador para Chrome
- Extensión del navegador para Firefox
- Extensión del navegador para IE

Conexión directa a sistemas remotos

Password Manager Pro le permite iniciar automáticamente la sesión en sistemas de destino remotos directamente desde su interfaz web con la opción de gateway de inicio de sesión automático. El gateway de inicio de sesión automático es útil para iniciar sesiones RDP, VNC, SSH y SQL de Windows. En esta sección de nuestra documentación de ayuda encontrará información detallada sobre cómo utilizar esta función.

API para eliminar las credenciales codificadas

Varias aplicaciones necesitan acceder a bases de datos y otras aplicaciones con frecuencia para consultar información relacionada con el negocio. Este proceso de comunicación se suele automatizar incrustando las credenciales de la aplicación en texto plano dentro de los archivos de configuración y los scripts. Aunque la codificación de las credenciales facilita el trabajo de los técnicos, también es un punto de partida fácil para los hackers.

Gestión de contraseñas entre aplicaciones

Password Manager Pro elimina las contraseñas codificadas con API seguras para la gestión de contraseñas de aplicación a aplicación (A-to-A). Password Manager Pro proporciona API de gestión de contraseñas, a través de las cuales cualquier aplicación empresarial o script puede consultar y recuperar contraseñas para conectarse con otras aplicaciones o bases de datos. De este modo, las contraseñas A-to-A también están sujetas a las mejores prácticas de seguridad, como la rotación periódica de contraseñas, sin necesidad de realizar actualizaciones manuales en múltiples lugares.

Para configurar las API, vaya a **Admin** > **Configuration** >**Password Management API.**

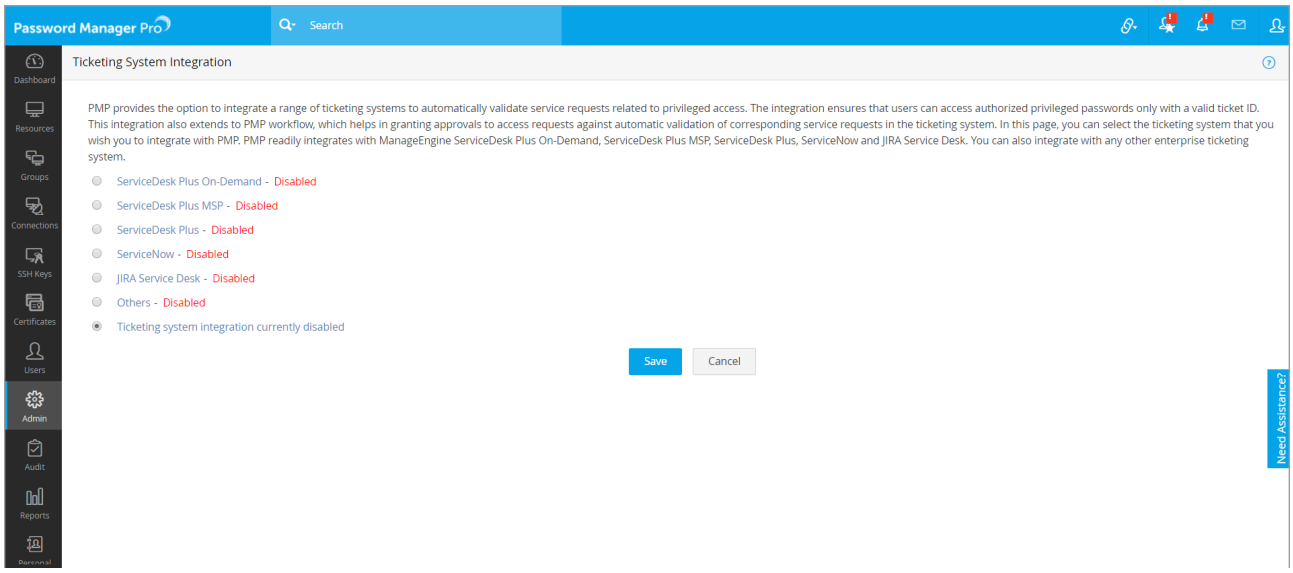
Para obtener instrucciones detalladas sobre la configuración de la API de gestión de contraseñas, consulte esta sección de nuestra documentación.

Rest API

La API más utilizada en Password Manager Pro es la REpresentational State Transfer (REST) o la API RESTful. Las API que pertenecen a esta categoría permiten añadir recursos, cuentas, recuperar contraseñas, detalles de recursos/cuentas y actualizar contraseñas mediante programación. El primer paso en el proceso de configuración de las API de gestión de contraseñas implica la creación de cuentas de usuario de la API en Password Manager Pro. Para obtener instrucciones detalladas al respecto, consulte esta sección de la documentación de ayuda.

Integración del sistema de generación de tickets

Password Manager Pro le permite integrar una serie de sistemas de generación de tickets para validar automáticamente las solicitudes de servicio relacionadas con el acceso privilegiado. La integración garantiza que los usuarios puedan acceder a las contraseñas privilegiadas autorizadas sólo con un ID de ticket válido. Esta integración también se extiende al flujo de trabajo de Password Manager Pro, que le ayuda a conceder aprobaciones a las solicitudes de acceso con la validación automática de las correspondientes solicitudes de servicio en el sistema de tickets.



Para configurar esta opción, vaya a la pestaña **Admin** > **Integration** > **Ticketing System Integration**. En esta sección de nuestra documentación de ayuda encontrará instrucciones detalladas sobre la integración del servicio de asistencia.

Configuración de alta disponibilidad

Para un acceso ininterrumpido a las contraseñas, Password Manager Pro ofrece una arquitectura de alta disponibilidad que utiliza instancias redundantes del servidor y la base de datos de Password Manager Pro. La configuración de alta disponibilidad varía según la base de datos back-end utilizada. Las siguientes secciones de nuestra documentación de ayuda le guiarán a través del proceso de establecimiento de la alta disponibilidad.

- Alta disponibilidad (PostgreSQL)
- Alta disponibilidad (MS SQL)
- Servicio Fail Over

Configuración de la recuperación ante desastres

También puede configurar una copia de seguridad de la base de datos de Password Manager Pro para recuperarla en caso de desastre. Password Manager Pro ofrece dos opciones para configurar la copia de seguridad de la base de datos:

- Copia de seguridad en tiempo real
- Copia de seguridad programada.

Para configurar una copia de seguridad de los datos, vaya a **Admin** > **Configuration** > **Database Backup**. Puede consultar esta sección de nuestra documentación para obtener más información.

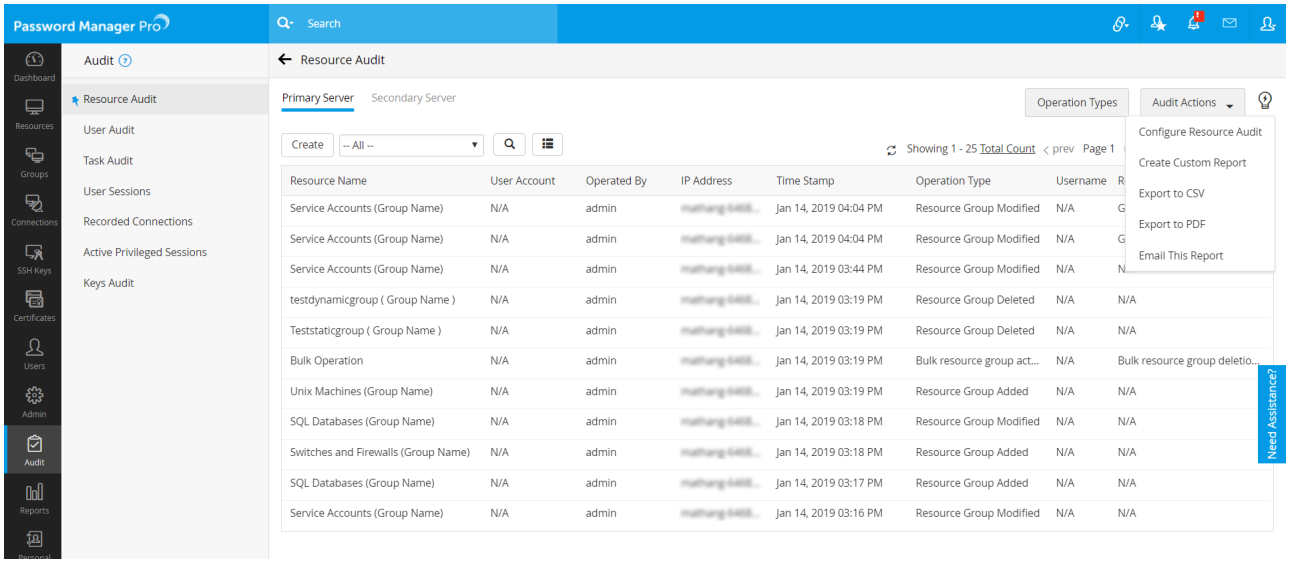
Configuración de la auditoría

Password Manager Pro viene con un mecanismo de auditoría efectivo para registrar las pistas de cada acción realizada por cada usuario. Todas las operaciones realizadas por los usuarios en la GUI se auditan con la marca de tiempo de cada operación y la dirección IP desde la que el usuario accedió a la aplicación. La auditoría en Password Manager Pro se puede clasificar en tres tipos:

- **Auditoría de recursos:** Todas las operaciones relativas a los recursos, grupos de recursos, cuentas, contraseñas, recursos compartidos y políticas.
- **Auditoría de usuarios:** Todas las operaciones realizadas en Password Manager Pro por un usuario de Password Manager Pro se registran en la auditoría de usuario.

- **Auditoría de tareas:** Registros de la creación de varias tareas programadas.

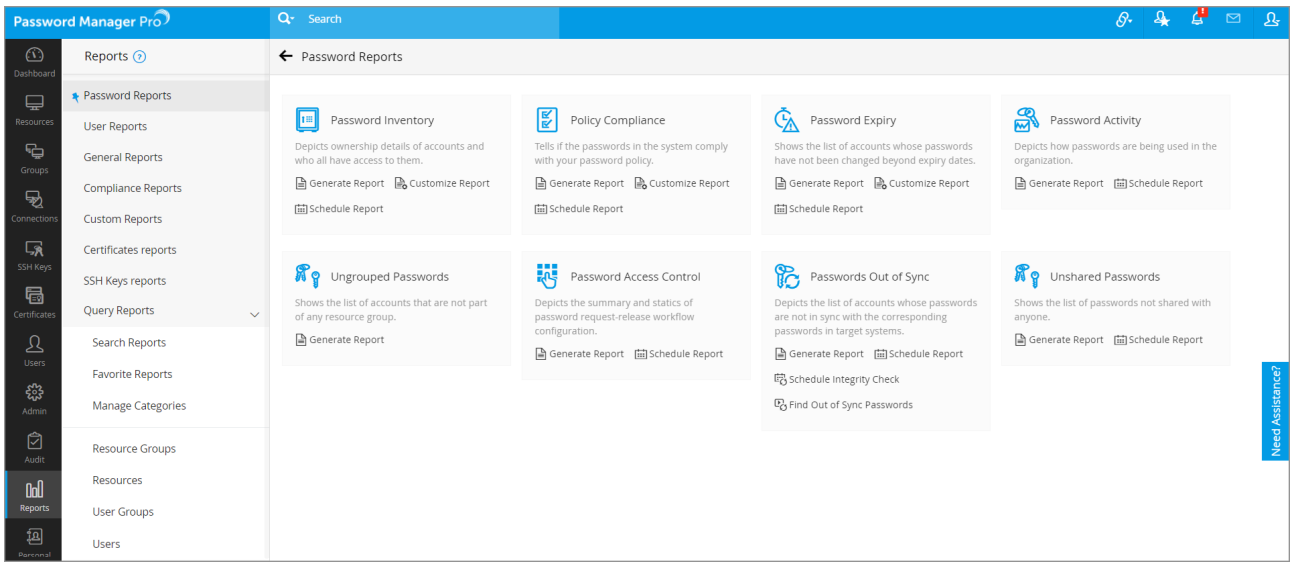
Las auditorías de Password Manager Pro son bastante completas, casi todas las acciones son auditadas. Si sólo desea auditar operaciones específicas, puede especificarlas en función del tipo de operación de auditoría. También puede enviar notificaciones a los destinatarios requeridos cada vez que se produzca un evento elegido (pista de auditoría de su elección).



Puede configurar cada una de estas auditorías en la pestaña Audit de la interfaz web. Puede encontrar más instrucciones sobre la configuración de las auditorías en esta sección de nuestra documentación.

Informes

La información sobre todo el proceso de gestión de cuentas privilegiadas en su empresa se presenta en forma de informes completos en Password Manager Pro. El estado y los resúmenes de diferentes actividades, como el inventario de contraseñas, el cumplimiento de las políticas, la caducidad de las contraseñas, la actividad de los usuarios, etc., se proporcionan en forma de tablas y gráficos que ayudan a los administradores de TI a tomar decisiones bien informadas sobre la gestión de contraseñas. Password Manager Pro proporciona informes en varias categorías y también le permite crear sus propios informes.



Para ver y configurar los informes, vaya a la pestaña **Reports** de la interfaz web. Puede encontrar instrucciones detalladas en esta sección de nuestra documentación.

Acceso sin conexión

Password Manager Pro ofrece múltiples opciones para el acceso seguro sin conexión y la conservación de la información de las contraseñas.

- La opción más básica es exportar el nombre del recurso, el nombre de la cuenta y las contraseñas en texto plano en una hoja de cálculo.
- La opción más segura es exportar las contraseñas en un archivo HTML cifrado.
- También puede sincronizar automáticamente el archivo HTML exportado a los dispositivos móviles de los usuarios a través de sus cuentas en la nube de Dropbox, Box y Amazon S3.

Los casos típicos de uso de esta opción incluyen:

1. Un proveedor de servicios gestionados (MSP) que utiliza Password Manager Pro para almacenar las contraseñas compartidas de sus clientes y de los técnicos que visitan a los clientes, los cuales no tienen acceso a Password Manager Pro instalado en su red.
2. Técnicos que trabajan en DMZ sin acceso a la interfaz web de Password Manager Pro. Los administradores pueden decidir qué opción (HTML cifrado o sincronización automática con los dispositivos móviles) debe utilizarse en su organización. Además, la exportación puede activarse o desactivarse para usuarios o grupos de usuarios específicos, según sea necesario.

Puede encontrar más información sobre la exportación de contraseñas en esta sección de nuestra documentación.

Acceso móvil

La aplicación móvil nativa es útil para recuperar las contraseñas de forma segura desde cualquier lugar. A continuación se ofrece la lista de plataformas móviles compatibles y las instrucciones detalladas para cada plataforma.

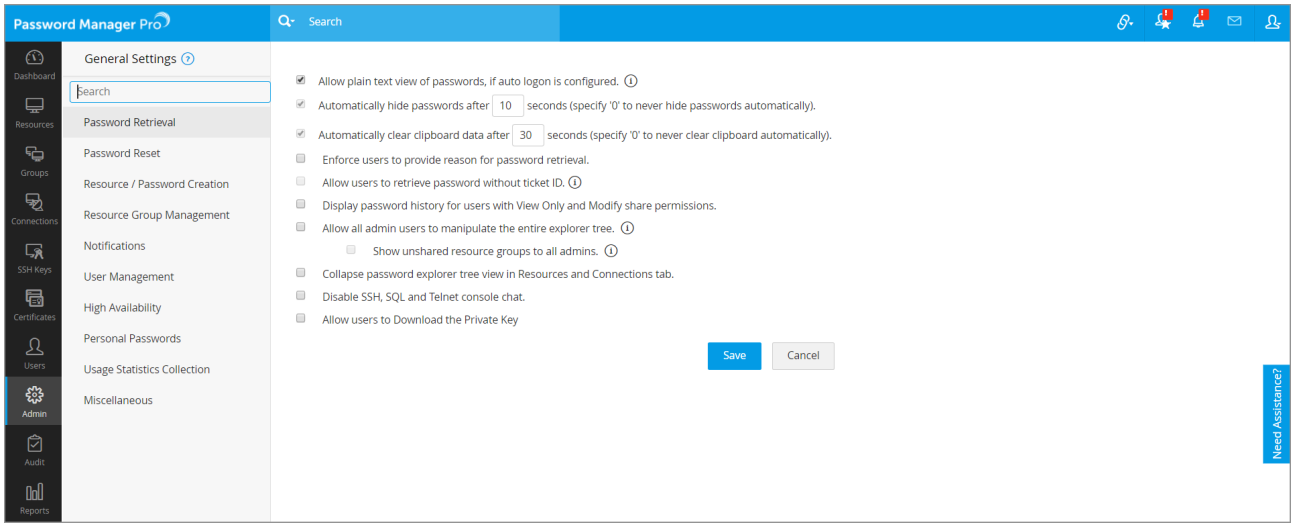
- Android
- iOS

Extensiones del navegador

Para facilitar el proceso de gestión de contraseñas y el inicio de sesión automático, Password Manager Pro le ofrece la opción de sincronizar de forma segura las contraseñas entre los navegadores a través de extensiones nativas del navegador. Las extensiones podrán autocompletar las contraseñas de los sitios y aplicaciones web y también iniciar sesiones RDP y SSH. Además, las extensiones permiten ver todas las contraseñas, los grupos de recursos, los favoritos y los utilizados recientemente, y ofrecen una opción de búsqueda. Una vez implementada la extensión, podrá realizar la mayoría de las operaciones de gestión de contraseñas directamente desde la extensión del navegador, mientras Password Manager Pro se ejecuta en segundo plano. Actualmente, las extensiones están disponibles para Chrome, Firefox e IE.

Ajustes generales

Password Manager Pro le permite habilitar o deshabilitar selectivamente varias configuraciones en función de las necesidades específicas de su organización. A través de estos ajustes, puede optar por aplicar o desactivar diversas políticas. Vaya a **Admin** > **Settings** > **General Settings** para personalizar sus opciones.



Especificaciones de seguridad para su revisión

Password Manager Pro ha sido diseñado para ofrecer la máxima seguridad desde la instalación de la aplicación hasta la autenticación del usuario, la transmisión de datos, el almacenamiento y todo el flujo de trabajo de uso. Puede revisar las especificaciones de seguridad de Password Manager Pro aquí y decidir las configuraciones de seguridad adecuadas para su organización.

Mejores prácticas a seguir

Puede seguir ciertas prácticas recomendadas en todas las etapas -instalación, configuración, instalación e implementación del producto- con especial atención a la seguridad de los datos. Consulte la guía de buenas prácticas para más detalles.

Datos de contacto para la asistencia técnica

Si tiene problemas para empezar a utilizar el producto o si necesita más ayuda, nuestro equipo de asistencia técnica está a sólo un correo electrónico o una llamada telefónica de distancia.

Correo electrónico: **passwordmanagerpro-support@manageengine.com**
Número de línea gratuita: **+1-408-454-4014**