Guía del usuario de Dell Data Protection Console

Protección frente a amenazas/Estado de cifrado/
Inscripción de autenticación/Password Manager v. 1.7

Notas, precauciones y avisos

NOTA: Una NOTA indica información importante que le ayuda a hacer un mejor uso de su producto.

PRECAUCIÓN: Una PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos, y le explica cómo evitar el problema.

AVISO: Un mensaje de AVISO indica el riesgo de daños materiales, lesiones corporales o incluso la muerte.

Guía del usuario de Dell Data Protection Console

2017 - 04

Rev. A01

Tabla de contenido

1

Introducción a la DDP Console

Dell Data Protection | Endpoint Security Suite le ofrece herramientas intuitivas y fáciles de usar para aumentar la seguridad del equipo.

Las siguientes características están disponibles a través de la DDP Console, en el sistema operativo de una estación de trabajo:

- Registre las credenciales para su uso con Endpoint Security Suite
- Sáquele partido a sus credenciales de factor múltiple, como las contraseñas, huella digitales y tarjetas inteligentes
- Recupere el acceso a su equipo si ha olvidado la contraseña sin llamadas al servicio de asistencia o la ayuda del administrador
- Realice una copia de seguridad de sus datos de programa y restáurelos
- Cambie fácilmente su contraseña de Windows
- Establezca preferencias personales
- Vea el estado de cifrado (en equipos con unidades de cifrado automático)

  Vea el estado de Threat Protection

DDP Console

La DDP Console es una interfaz a través de la que puede registrar y administrar sus credenciales, y configurar las preguntas de recuperación automática más frecuentes.

Puede acceder a estas aplicaciones:

- El panel de Protección frente a amenazas muestra el estado de protección del equipo, en función de las políticas de protección de amenazas.La herramienta Estado de cifrado le permite ver el estado de cifrado de las unidades del equipo.
- La herramienta de Registros le permite establecer y administrar las credenciales, configurar las preguntas de autorecuperación y ver el estado del registro de sus credenciales. El administrador establece su capacidad de registrar cada tipo de credencial.
- Password Manager le permite rellenar y enviar automáticamente los datos necesarios para iniciar sesión en los sitios webs, aplicaciones de Windows y recursos de red. Password Manager también le permite cambiar sus contraseñas de inicio de sesión a través de la aplicación, con lo que se asegura que las contraseñas de Password Manager se mantengan sincronizadas con las del recurso en cuestión.

Esta guía describe cómo utilizar cada una de estas aplicaciones.

Compruebe periódicamente las actualizaciones de la documentación en la página dell.com/support.

Cómo ponerse en contacto con Dell ProSupport

Llame al 877-459-7304, extensión 4310039 para obtener soporte telefónico sobre su producto Dell Data Protection 24 horas al día 7 días a la semana.

De manera adicional, puede obtener soporte en línea para su producto Dell Data Protection en dell.com/support. El soporte en línea incluye controladores, manuales, recomendaciones técnicas, P+F y posibles problemas.

Asegúrese de ayudarnos a conectarle rápidamente con el experto técnico adecuado teniendo su Código de servicio disponible cuando realice la llamada.

Para obtener los números de teléfono fuera de los Estados Unidos, consulte Números de teléfono internacionales de Dell ProSupport .

2

DDP Console

La DDP Console proporciona acceso a aplicaciones que garantizan la seguridad de todos los usuarios del equipo a la hora de ver y administrar el estado de cifrado de las unidades y particiones del equipo y, en función de política establecida por el administrador, administrar sus inicios de sesión en sitios web, programas y recursos de red, y registrar fácilmente sus credenciales de autenticación.

Para abrir la DDP Console, en el *escritorio*, haga doble clic en el icono de **DDP Console**.

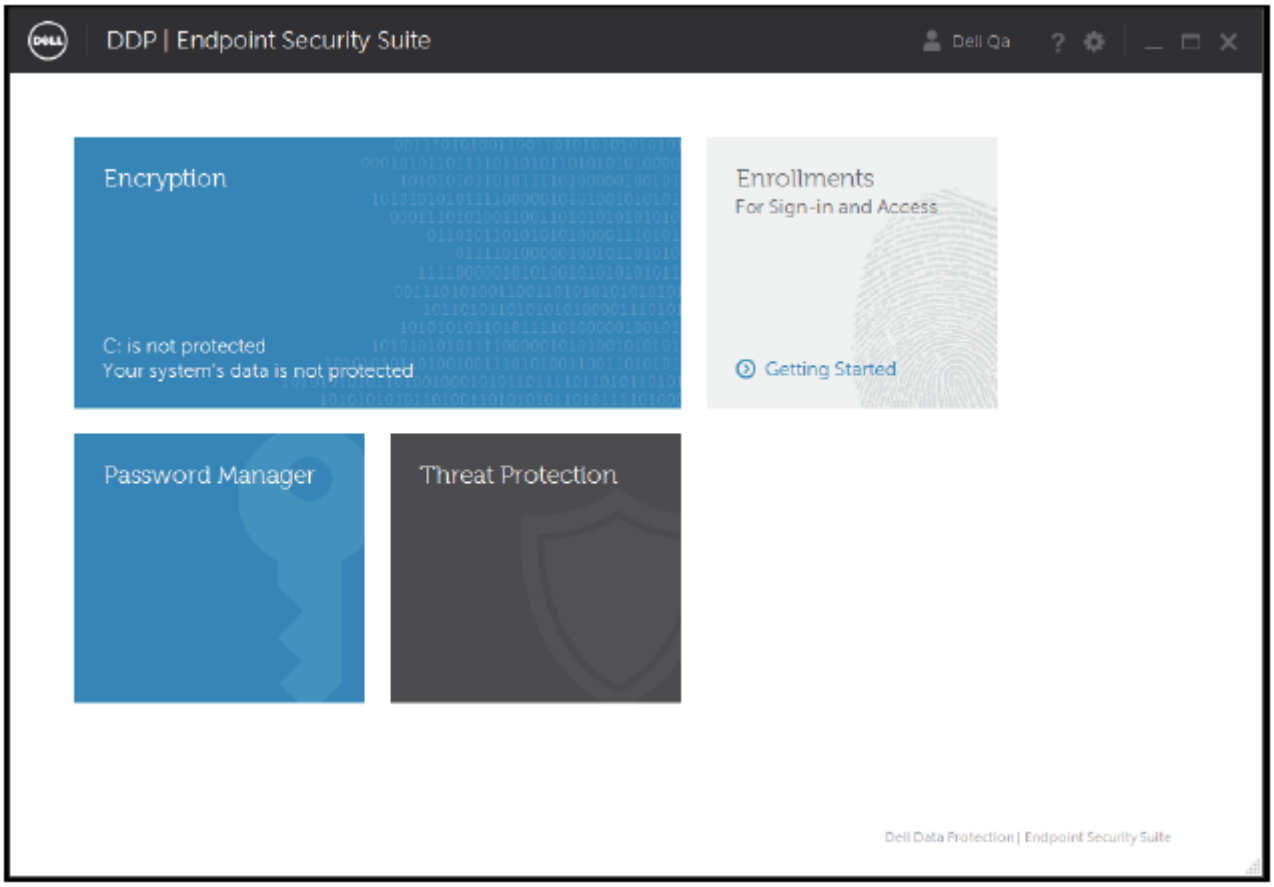
Cuando se inicie la DDP Console, las aplicaciones Endpoint Security Suite aparecerán en la página principal:

- Threat Protection
- Estado del cifrado
- Registros
- Password Manager

  Para configurar las credenciales por primera vez, seleccione el vínculo **Introducción** en el mosaico de registros. Un asistente le guiará a través del proceso de registro corto. Para obtener más información, consulte Registro de credenciales por primera vez.

Navegación

Para acceder a una aplicación, haga clic sobre el mosaico correspondiente.



Barra de título

Para volver a la página de inicio desde dentro de una aplicación, haga clic en la flecha Atrás situada en la esquina izquierda de la barra del título, próxima al nombre de la aplicación activa.

Para desplazarse directamente a otra aplicación, haga clic en la flecha abajo situada junto al nombre de la aplicación activa y seleccione una aplicación.

Para minimizar, maximizar o cerrar la DDP Console, haga clic en el icono correspondiente situado en la esquina derecha de la barra de título.

Para restaurar la DDP Console después de minimizar, haga doble clic en el icono de bandeja del sistema.

Para abrir la ayuda, haga clic en **?** en la barra de título.

Detalles de la DDP Console

Para ver detalles sobre la DDP Console, políticas, servicios en ejecución y registros, haga clic en el icono de engranaje situado en la parte izquierda de la barra de título. Es posible que esta información sea necesaria para que el administrador pueda proporcionar asistencia técnica.

Seleccione un elemento del menú.

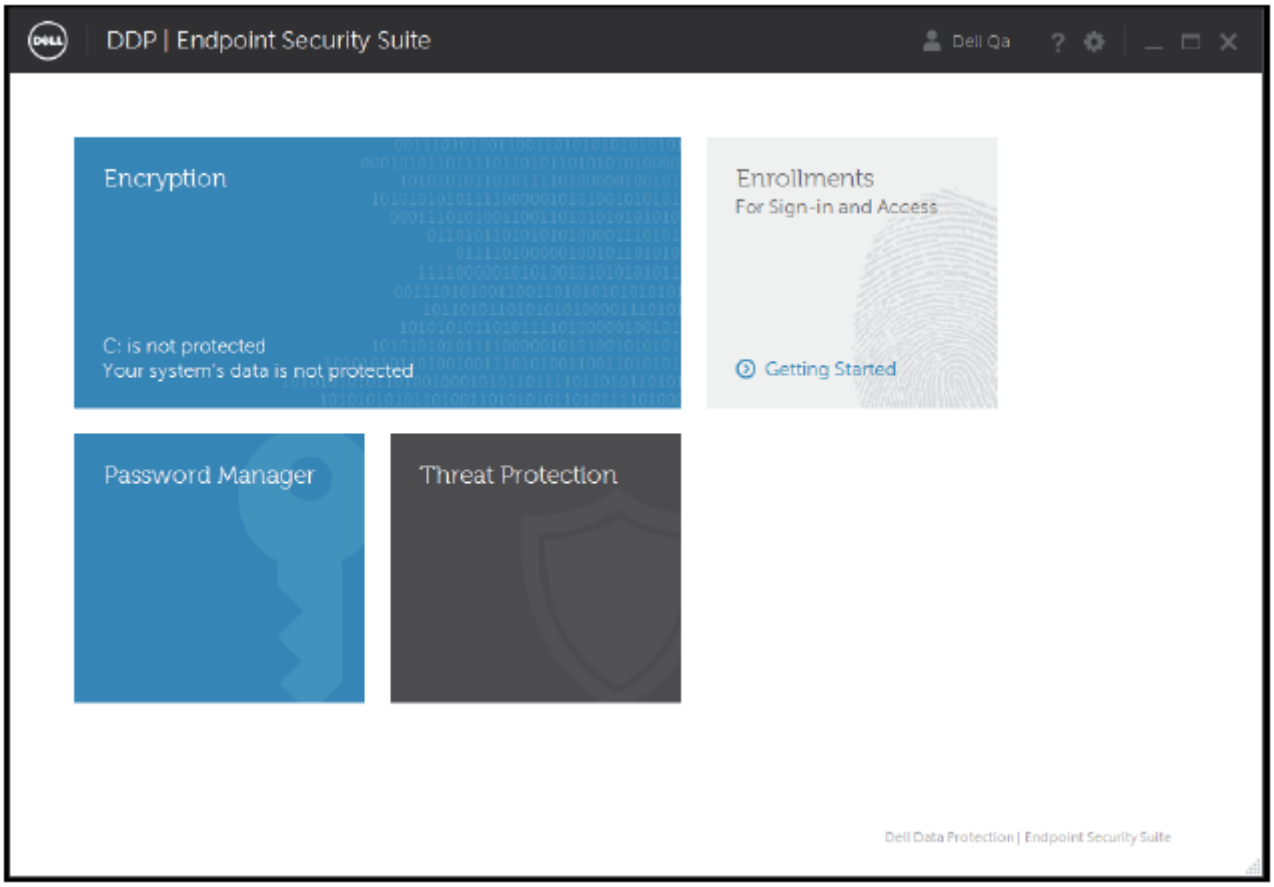
Elemento del menú	Propósito
Acerca de	Contiene información de los derechos de autor y de la versión.
Mostrar información	Contiene lo siguiente: • información sobre la fecha y la versión del producto • si la empresa o un administrador local administra la DDP Console en este equipo • los números de versión del sistema operativo, el BIOS, la placa base y el módulo de plataforma de confianza (TPM).
Información de MS	Ejecuta la utilidad de Información del sistema de Microsoft Windows para mostrar información detallada sobre el entorno de software, los componentes y el hardware.
Copiar información	Copia toda la información del sistema en el portapapeles para pegarla en un correo electrónico dirigido a su administrador o a Dell ProSupport.
Comentarios	Muestra un formulario donde puede proporcionar comentarios a Dell sobre este producto. (En equipos que no son del dominio, esta opción está siempre disponible. En equipos del dominio, esta opción está determinada por la política de empresa).
Políticas	Muestra una jerarquía de las políticas que se aplican a este equipo.
Servicios	Muestra detalles sobre los servicios que están en ejecución.
Compatibilidad	Conecta con el sitio web de Dell ProSupport.
Registro	Muestra una lista detallada de eventos registrados para la solución de problemas.
Iniciar seguimiento	Le permite iniciar y detener la grabación de las actividades de inicio de sesión, para la solución de problemas.

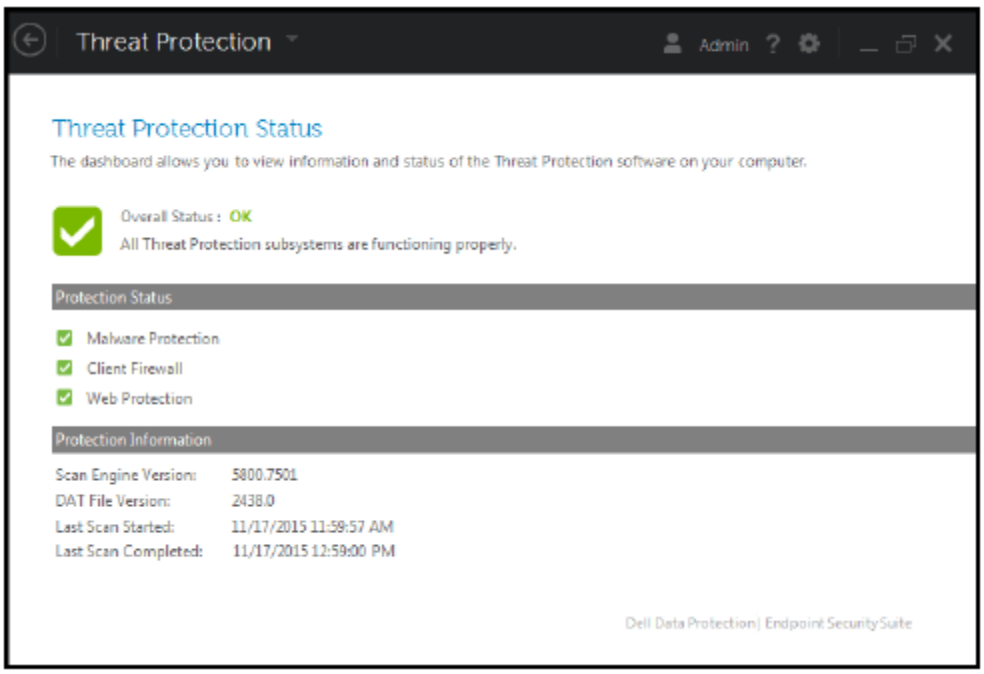
3

Threat Protection

Panel de Threat Protection

Los usuarios acceden al panel Estado de Threat Protection desde el mosaico Threat Protection de la DDP Console.





- Protegido: el estado general es protegido si las políticas de *Protección de acceso*, *Protección de explotación* y **Protección siempre activa** se establecen en verdadero (habilitado).

  O bien

  Si la política de *Protección a petición: exploración completa* o *Protección a petición: exploración rápida* se ha establecido en verdadero (habilitado) y se han configurado sus correspondientes políticas de programación.

- Vulnerable: el estado general es vulnerable si alguna de las siguientes políticas se establece en falso (deshabilitado): *Protección de acceso*, *Protección de explotación* y **Protección siempre activa**.

  y

  Tanto la política de *Protección a petición: exploración completa*, como la de *Protección a petición: exploración rápida* se establecen en falso (deshabilitado) o verdadero (habilitado) cuando no se han configurado sus políticas de programación correspondientes.

  Estado de protección

  El campo Estado de protección muestra el estado individual de Protegido (indicado mediante una marca de comprobación verde) o Vulnerable (indicado por una X roja) en función de si las políticas maestras están establecidas en Verdadero (habilitada):

- Protección de malware
- Servidor de seguridad del cliente
- Protección web

  Información de protección

  El campo Información de protección proporciona la siguiente información:

- Versión de motor de exploración: versión de motor de exploración utilizada. El motor de exploración compara el contenido de los archivos analizados con las amenazas conocidas.
- Versión de archivo DAT: versión del archivo DAT de Threat Protection que el motor utiliza para detectar malware durante una exploración.
- Última exploración iniciada: marca de tiempo de inicio de la última exploración correcta.
- Última exploración completada: marca de tiempo de finalización de la última exploración.

  Menú de engranaje

  El menú de engranaje proporciona acceso a lo siguiente:

- Acerca de: proporciona información sobre la versión de Endpoint Security Suite y la configuración del equipo cliente.
- Políticas: muestra varias políticas de agente. Actualmente y debido a que hay un gran número de políticas de Threat Protection, éstas no se muestran.
- Servicios: muestra el estado del complemento de administración antimalware y la comunicación con el agente de administración de Dell.
- Comentarios: proporciona un vínculo al sitio web de asistencia de Dell.
- Registros: muestra los eventos relacionados con los servicios, incluido el complemento de administración antimalware.
- Iniciar supervisión: le permite iniciar y detener la grabación de actividades del sistema para la solución de problemas.

Notificaciones emergentes

Según la política, las notificaciones emergentes pueden informar al usuario de amenazas que impliquen lo siguiente:

- Carpetas y archivos
- Registro
- Procesos de Endpoint Security Suite
- Sitios web no verificados o maliciosos
- Páginas de phishing

No es necesario que el usuario emprenda ninguna acción. Endpoint Security Suite se ocupa de todas las correcciones.

Supresión de todas las notificaciones emergentes

Para suprimir mensajes que avisan el usuario de las amenazas, establezca la siguiente clave del registro:

[HKLM\Software\Dell\Dell Data Protection]

"DDPTPHideToasters"=dword:1

0=(Default) Deshabilitado, no ocultar las notificaciones emergentes al usuario

1=Habilitado, ocultar las notificaciones emergentes al usuario

Filtrado de notificaciones emergentes

Para mostrar notificaciones de un nivel de gravedad mínimo, establezca esta clave de registro:

[HKLM\Software\Dell\Dell Data Protection]

"DDPTPEventSeverityFilter"=dword:3

0=Información (muestra todos los eventos), 1=Aviso, 2=Leve, 3=Grave (predeterminado, mostrar solo Grave y Crítico), 4=Crítico

Si "DDPTPHideToasters" está establecido en 1, se ignora la configuración para "DDPTPEventSeverityFilter".

4

Estado del cifrado

La página Cifrado muestra el estado de cifrado del equipo. Si un disco, unidad o partición aparece sin cifrar, su estado indicará *Sin proteger*. Si una unidad o partición aparece como cifrada, su estado indicará *Protegida*.

Para actualizar el estado de cifrado, haga clic con el botón derecho del ratón en el disco, unidad o partición correspondiente y, a continuación, seleccione **Actualizar**.

5

Registros

La herramienta Registros le permite registrar, modificar y comprobar el estado del registro en función de la política establecida por el administrador.

La primera vez que registra sus credenciales con la DDP Console, un asistente le guía por el proceso de registrar un cambio de contraseña, Preguntas de recuperación, huellas digitales, dispositivos móviles y tarjetas inteligentes. Según la política, puede registrar u omitir cada credencial. Después del registro inicial, puede hacer clic en el mosaico Registros para agregar o modificar las credenciales.

Registro de credenciales por primera vez

Para registrar credenciales por primera vez:

1 En la página principal de la DDP Console, haga clic en el vínculo **Introducción** del mosaico de registros.
2 En la página de Bienvenida, haga clic en **Siguiente**.
3 En el cuadro de diálogo Se requiere autenticación, inicie sesión con su contraseña de Windows, y haga clic en **Aceptar**.
4 En la página de contraseña, para cambiar la contraseña de Windows, introduzca y confirme la nueva contraseña y haga clic en **Siguiente**.
   Si no desea cambiar la contraseña, haga clic en **Omitir**. El asistente le permite omitir una credencial si no desea registrarla. Para volver a la página, haga clic en **Atrás**.
5 Siga las instrucciones de cada página y haga clic en el botón correspondiente: **Siguiente**, **Omitir**, o **Atrás.**
6 En la página de Resumen, confirme las credenciales registradas y, cuando se haya terminado con el proceso de registro, haga clic en **Aplicar**.
   Para volver a la página de registro de credenciales para hacer un cambio, haga clic en **Atrás** hasta llegar a la página que desea cambiar.

Para obtener más información detallada acerca de cómo registrar o cambiar una credencial, consulte Agregar, modificar o ver registros.

Agregar, modificar o ver los registros

Para agregar, modificar o ver registros, haga clic en el mosaico **Registros**.

Las pestañas de la lista del panel izquierdo están disponibles en Registros. Esto varía en función de su plataforma o tipo de hardware.

La página Estado muestra las credenciales admitidas, su configuración de política (Necesaria o N/A) y su estado de registro. Desde esta página, los usuarios pueden administrar sus registros, según la política establecida por el administrador:

- Para registrar una credencial por primera vez, en la línea con la credencial, haga clic en **Registrar**.
- Para eliminar una credencial registrada existente, haga clic en **Eliminar**.
- En caso de que la política no le permita registrarse o modificar sus credenciales, los vínculos **Registrar** y **Eliminar** de la página de estado estarán inactivos.
- Para cambiar un registro existente, haga clic en la pestaña correspondiente del panel izquierdo.

  Si la política no permite el registro o la modificación de una credencial, aparecerá un mensaje en la página de registro de credenciales, "La política no permite la modificación de credenciales".

Contraseña

Para cambiar su contraseña de Windows:

1 Haga clic en la pestaña **Contraseña**.
2 Introduzca la contraseña actual de Windows.
3 Introduzca la nueva contraseña y vuelva a hacerlo para confirmarla; a continuación, haga clic en **Cambiar**.
Los cambios de contraseña se efectúan de forma inmediata.

4 En el cuadro de diálogo Registro correcto, haga clic en **Aceptar**.

NOTA:
Solo debe cambiar la contraseña de Windows en la DDP Console, en lugar de en Windows. Si se cambia la contraseña de Windowas fuera de la DDP Console, se producirá una falta de coincidencia, lo que requiere una operación de recuperación.

Preguntas de recuperación

La página Preguntas de recuperación le permite crear, eliminar o cambiar las preguntas de recuperación y las respuestas. Las Preguntas de recuperación proporcionan un método basado en pregunta y respuesta para que pueda acceder a sus cuentas de Windows si, por ejemplo, la contraseña ha caducado o se ha olvidado.

NOTA:
Las preguntas de recuperación se utilizan para recuperar el acceso a solo un equipo. Las preguntas y respuestas no se pueden utilizar para iniciar sesión.

Si no tiene registradas Preguntas de recuperación anteriores:

1 Haga clic en la pestaña **Preguntas de recuperación**.
2 Seleccione de una lista de preguntas predefinidas y, a continuación, introduzca y confirme las respuestas.
3 Haga clic en **Registrar**.

NOTA:
Haga clic en el botón **Restablecer** para desmarcar las opciones seleccionadas en esta página y empezar de nuevo.

Preguntas de recuperación ya registradas

Si las preguntas de recuperación ya han sido registradas, puede borrarlas o volver a registrarlas.

1 Haga clic en la pestaña **Preguntas de recuperación**.
2 Haga clic en el botón correspondiente:
- Para eliminar las preguntas de recuperación por completo, haga clic en **Eliminar**.
- Para volver a definir las preguntas de recuperación y las respuestas, haga clic en **Volver a registrar**.

Huellas digitales

NOTA:
Para utilizar esta función, el equipo debe contar con un lector de huellas digitales.

Para registrar huellas digitales, siga estas instrucciones:

1 Haga clic en la pestaña **Huellas digitales**.
2 En la página Huellas digitales, haga clic en el dedo que desea registrar.
3 Siga las instrucciones que aparecen en la pantalla para registrar su huella digital.

> **NOTA:**
> El dedo debe escanearse correctamente cuatro veces para poder registrarse. El número de lecturas necesarias para completar el registro de una huella digital depende de la calidad obtenida en cada lectura. El administrador define el número mínimo y máximo de huellas digitales.

4 Haga clic en cada dedo subsiguiente para escanearlo hasta que se haya registrado el número mínimo de huellas digitales que la política exige.
Un cuadro de diálogo le informará si ha registrado o no el número mínimo de huellas digitales. Haga clic en **Aceptar** para continuar.
5 Realice la lectura de cada número de huellas digitales requeridas y haga clic en **Guardar**.
Para eliminar una huella digital escaneada, en la página de registro de huellas digitales, haga clic en la huella digital resaltada para eliminar el registro; haga clic en **Sí** para confirmar la eliminación y, a continuación, en **Guardar**.

Dispositivo móvil

El registro del dispositivo móvil proporciona la función Contraseña de un solo uso (OTP). Con OTP, el usuario puede iniciar sesión en Windows utilizando una contraseña generada por la aplicación Security Tools Mobile, en un dispositivo móvil que está asociado al equipo. De manera alternativa, si la política lo permite, la función OTP se puede utilizar para recuperar acceso al equipo en caso de olvido o vencimiento de contraseña.

> **NOTA:**
> Si la pestaña Dispositivo móvil no se muestra en la DDP Console, la configuración de su equipo no la admite, o la política establecida por su administrador no lo permite.

> **NOTA:**
> Los valores de configuración de la política determinan la manera de utilizar la función OTP: mediante el inicio de sesión o mediante la recuperación de acceso al equipo si la contraseña se venció o se olvidó. No se puede utilizar para el inicio de sesión y la recuperación.

Para utilizar la función OTP, debe registrar o asociar su dispositivo móvil al equipo. En un equipo con varios usuarios, cada usuario puede registrar un dispositivo móvil con el equipo. Es posible registrar los dispositivos móviles en varios equipos.

Cuando un dispositivo ya se ha registrado, al registrar un nuevo dispositivo, se desasocia automáticamente el dispositivo anterior.

Registro del dispositivo móvil

1 En la página de registros de la DDP Console, haga clic en la pestaña **Dispositivo móvil**.
2 En la parte superior derecha, haga clic en **Registrar**.
Se abre la página Registrar contraseña de un solo uso.
3 Si este es el primer equipo que va a emparejar, seleccione **Sí**.

a En el dispositivo móvil, descargue la aplicación Dell Data Protection | Security Tools Mobile desde su tienda de aplicaciones.
b En el equipo, haga clic en **Siguiente**.

Configuración de Security Tools Mobile

1 Abra la aplicación Security Tools Mobile.

2 Cree e introduzca un PIN para acceder a la aplicación Security Tools Mobile.

> **NOTA:**
> Cuando el dispositivo móvil no está bloqueado, es posible que la política requiera el PIN. Si no utiliza un PIN para desbloquear el dispositivo móvil, necesitará uno para acceder a la aplicación Security Tools Mobile.

3 Seleccione **Registrar un ordenador**. (Si fuera necesario, presione sobre la esquina superior izquierda de su pantalla móvil para acceder a los comandos).

El dispositivo móvil mostrará un código. La longitud del código y la combinación de caracteres alfanuméricos están basados en la configuración de la política establecida por el administrador.

Asociación del dispositivo móvil al equipo

1 En el equipo, en la página Código móvil de la DDP Console:
   a Introduzca el código del dispositivo móvil en el campo.
   b Haga clic en **Siguiente**.
   c En la página Asociar dispositivo, seleccione uno de los siguientes:
   Código QR: se muestra un código QR.

   O bien

   Entrada manual: se muestra un código de emparejamiento de 24 dígitos.
2 En el dispositivo móvil:
   a Toque **Emparejar dispositivos**.
   b Seleccione la misma opción de emparejamiento (**Escanear código QR** o **Entrada manual**) que haya seleccionado en el equipo.
   c Seleccione uno:
   - Para **Código QR**, coloque el dispositivo móvil frente a la pantalla del equipo de modo que pueda escanear el código QR.
     Anote el código numérico de comprobación que se muestra en el dispositivo móvil; a continuación, haga clic en **Siguiente**.

     > **NOTA:**
     > Si se muestra la barra *¿Problemas para escanear?*, inténtelo de nuevo o seleccione **Entrada manual**.

   - Para **Entrada manual**, introduzca el código de emparejamiento de 24 dígitos en el equipo y toque **Listo**.
     Anote el código numérico de comprobación que se muestra en el dispositivo móvil; a continuación, haga clic en **Siguiente**.
3 En el equipo, en la DDP Console:
   a Haga clic en **Siguiente**.
   b Introduzca el código de comprobación que se muestra en el dispositivo móvil y haga clic en **Siguiente**.
   c Si lo desea, modifique el nombre del dispositivo móvil.
   d Haga clic en **Aplicar**.
   Los dispositivos están emparejados.
4 En el dispositivo móvil:
   a Toque **Continuar**.
   b De manera opcional, modifique el nombre del equipo y toque **Listo**.
   c Toque **Finalizar**.

Registro de otro dispositivo móvil

El registro de un nuevo dispositivo automáticamente desasocia el anterior. No es necesario realizar ningún paso adicional para desasociar.

Desasociación de un equipo y un dispositivo móvil

Para desasociar un equipo y dispositivo móvil sin registrar otro dispositivo, seleccione uno:

- En la DDP Console: en la página de estado de los registros, junto a la credencial Dispositivo móvil, haga clic en **Eliminar**.
- En el dispositivo móvil: consulte los pasos que se indican a continuación.

1 En el dispositivo móvil, complete las siguientes acciones:
   a Ejecute la aplicación Security Tools Mobile.
   b En la parte izquierda superior, presione las barras de menú para abrir el cajón.
   c Toque **Eliminar equipos**.
   d Seleccione el equipo a desasociar.
   e Seleccione **Eliminar** (Android) o toque **Listo** (iOS).
   Aparece un mensaje de confirmación.
   f Seleccione **Eliminar todos** para eliminar todos los equipos registrados del dispositivo.
   La opción Quitar todo aparece cuando quite varios equipos y cuando quite el único equipo asociado.

   - Seleccione **Restaurar configuración predeterminada** para eliminar los equipos registrados y el PIN. Si restaura los valores predeterminados, se eliminarán todos los equipos registrados y el PIN que utiliza para acceder a la aplicación Security Tools Mobile.
   - Seleccione **Cancelar** para que el equipo siga registrado.

Inicio de sesión con contraseña de un solo uso

NOTA:
La autenticación OTP solamente se puede utilizar con inicios de sesión de Windows.

OTP se puede utilizar para la recuperación, para volver a tener acceso al equipo que le bloqueó ese acceso, o para el inicio de sesión de Windows. No se puede utilizar para ambos fines.

Si la política lo permite y el símbolo OTP  se muestra en la pantalla de inicio de sesión, puede iniciar sesión en Windows con OTP.

Para iniciar sesión con OTP:

1 En el equipo, en la pantalla de inicio de sesión de Windows, seleccione el icono OTP  .
2 En el dispositivo móvil, abra la aplicación Security Tools Mobile e introduzca el PIN.
3 Seleccione el equipo al que desea acceder.
   Si el nombre del equipo no aparece en el dispositivo móvil, es posible que se deba a una de las siguientes situaciones:

   - El dispositivo móvil no está registrado o asociado con el equipo al que está intentando acceder.
   - Si tiene más de una cuenta de usuario de Windows, o bien Endpoint Security Suite no está instalado en el equipo al que intenta acceder o bien que está intentando iniciar sesión en una cuenta de usuario distinta a la que se utilizó para emparejar el equipo y el dispositivo móvil.

4 Presione **Contraseña de un solo uso**.
   Aparece una contraseña en la pantalla del dispositivo móvil.

NOTA:

Si es necesario, haga clic en el símbolo Actualizar  para obtener un nuevo código. Después de las dos primeras actualizaciones de OTP, habrá un retraso de treinta segundos antes de que se genere otra OTP.

El equipo y el dispositivo móvil deben estar sincronizados para que ambos puedan reconocer la misma contraseña al mismo tiempo. Intentar generar rápidamente contraseña tras contraseña hará que el equipo y el dispositivo móvil pierdan la sincronización y que falle la función OTP. Si se produjera este problema, espere treinta segundos para que los dos dispositivos vuelvan a sincronizarse y, a continuación, vuelva a intentarlo.

5 En el equipo, en la pantalla de inicio de sesión de Windows, escriba la contraseña que se muestra en el dispositivo móvil y presione **Intro**.

Si ha utilizado OTP para la recuperación, una vez obtenido el acceso al equipo, siga las instrucciones en pantalla para restablecer la contraseña.

Tareas de administración de Security Tools Mobile

Estas tareas se ejecutan mediante la aplicación Security Tools Mobile en el dispositivo móvil.

Restablecimiento del PIN de la aplicación Security Tools Mobile

Para restablecer el PIN de la aplicación Security Tools Mobile:

1 En la parte superior derecha, presione las opciones de menú.
2 Seleccione **Restablecer PIN**.
3 Introduzca y confirme el nuevo PIN.

Desinstalación de la aplicación Security Tools Mobile

En el dispositivo móvil:

1 Desasocie el dispositivo del equipo.
2 Elimine o desinstale la aplicación Security Tools Mobile del mismo modo que elimina una aplicación de su dispositivo móvil.

Tarjetas inteligentes

NOTA:
Para utilizar esta función, el equipo debe contar con un lector de tarjetas inteligentes.

Para registrar tarjetas inteligentes, siga estas instrucciones:

1 Haga clic en la pestaña **Tarjeta inteligente**.
2 Registre la tarjeta inteligente en función del tipo de tarjeta:
   - Introduzca la tarjeta inteligente en el lector de tarjetas.
   - Con la ayuda de una tarjeta sin contacto, coloque y mantenga la tarjeta en el lector o cerca de él.
3 Cuando se detecte la tarjeta, aparecerá una casilla de verificación verde y se mostrará la opción *Registrar la tarjeta*. Seleccione **Registrar la tarjeta**.
4 En el cuadro de diálogo Registro correcto, haga clic en **Aceptar**.

Para anular el registro de todas las tarjetas inteligentes asociadas al usuario, en la página de registro de tarjetas inteligentes, seleccione **Eliminar tarjetas registradas de la cuenta**.

6

Password Manager

Password Manager le permite iniciar sesión automáticamente en sitios web, programas de Windows y recursos de red y administrar las credenciales de inicio de sesión en una herramienta única. Password Manager también permite a los usuarios cambiar sus contraseñas de inicio de sesión a través de la aplicación, con lo que se asegura que las contraseñas de Password Manager se mantengan sincronizadas con las del recurso en cuestión.

Password Manager es compatible con Internet Explorer y Mozilla Firefox. Password Manager no es compatible con las cuentas de Microsoft (anteriormente Windows Live ID).

NOTA:
Si ejecuta Password Manager en Firefox, debe instalar y registrar la extensión de Password Manager. Para obtener instrucciones sobre la instalación de extensiones en Mozilla Firefox, consulte https://support.mozilla.org/.

NOTA:
El uso de iconos de Password Manager (iconos entrenados previamente y entrenados) en Mozilla Firefox difiere de Microsoft Internet Explorer:

- La función de doble clic en iconos de Password Manager no está disponible.
- La acción predeterminada no se muestra en negrita en el menú contextual desplegable.
- Si una página tiene varios formularios de inicio de sesión, podría ver más de un icono de Password Manager.

NOTA:
Debido al cambio continuo en la estructura de las páginas de inicio de sesión de la web, es posible que Password Manager no sea compatible con todos los sitios web en todo momento.

Introducción a Password Manager

Password Manager recopila y almacena sus credenciales de inicio de sesión a medida que trabaja. Puede comenzar a utilizar Password Manager inmediatamente después de instalar Endpoint Security Suite. Cuando introduce las credenciales en una página de inicio de sesión, Password Manager detecta el

formulario de inicio de sesión y le permite elegir si desea que Password Manager guarde sus credenciales.

Tiene tres opciones:

- Haga clic en **Guardar inicio de sesión** para almacenar sus credenciales de inicio de sesión en Password Manager.
- Si ***no*** desea guardar su inicio de sesión, se le solicitará que guarde las credenciales de inicio de sesión cada vez que inicie sesión en el sitio web o el programa. Si prefiere que el sistema deje de preguntarle, seleccione **Nunca para este sitio**. Se creará un registro en la lista de Exclusiones del sitio web. Consulte Excluir sitios web para obtener más detalles.
- Si no desea guardar las credenciales, haga clic en **No guardar inicio de sesión**.

Este cuadro de diálogo también se muestra cuando ha guardado las credenciales anteriormente para un sitio web o un programa, pero introduce un nombre de usuario o una contraseña diferentes. Al usar un nuevo nombre de usuario, si selecciona **Guardar inicio de sesión**, se almacenará un nuevo conjunto de credenciales. Con el nombre de usuario guardado anteriormente y la nueva contraseña, si selecciona **Guardar inicio de sesión**, las credenciales originales se actualizarán con la nueva contraseña.

Administración de inicios de sesión

El Administrador de inicio de sesión simplifica y centraliza la administración de todos los inicios de sesión en sitios web, programas de Windows y recursos de red.

Para abrir el Administrador de inicio de sesión:

1 En la página principal de la DDP Console, haga clic en el mosaico **Password Manager**.
2 Haga clic en la pestaña **Administrador de inicio de sesión**.

Puede agregar inicios de sesión y categorías y ordenarlos y filtrarlos:

Agregar inicio de sesión: le permite agregar un nuevo conjunto de credenciales de inicio de sesión. En función de la política, es posible que se le pida proporcionar credenciales almacenadas en para agregar un inicio de sesión.

Agregar categoría: le permite agregar una nueva categoría (como correo electrónico, almacenamiento, noticias, recursos corporativos, redes sociales), para su uso a la hora de ordenar y filtrar.

Ordenar: ordene los inicios de sesión por cuenta, nombre de usuario o categoría. Haga clic en el encabezado de la columna para ordenar por columna.

Filtro: seleccione una categoría de la lista *Ver* para ocultar todos los inicios de sesión mediante huella dactilar, excepto los de la categoría seleccionada. Para eliminar el filtro, seleccione *Todos*.

Puede administrar los inicios de sesión:

Iniciar: abre el sitio web o el programa y envía las credenciales de inicio de sesión, de acuerdo con la configuración del usuario.

Editar: le permite cambiar los datos de inicio de sesión guardados de un sitio web o de un programa.

Eliminar: le permite eliminar los datos de inicio de sesión guardados de Password Manager.

Agregar: le permite agregar un inicio de sesión nuevo, una categoría o datos de inicio de sesión nuevos.

Agregación de categoría

Antes de agregar inicios de sesión, cree categorías (como Correo electrónico, Noticias, Recursos corporativos y Redes sociales) para que pueda categorizar sus inicios de sesión conforme los cree. A continuación puede ordenar y filtrar sus inicios de sesión por categoría.

Para agregar una categoría, en la página de administrador de inicio, haga clic en **Agregar categoría**, escriba un nombre de categoría y haga clic en **Guardar**.

Agregación de inicio de sesión

1 En la página de administrador de inicio de sesión, haga clic en **Agregar inicio de sesión**.
En función de la política, es posible que se le pida proporcionar autenticación para agregar un inicio de sesión.
2 Abra el sitio web o el programa para iniciar sesión.
3 En el cuadro de diálogo para agregar inicio de sesión, haga clic en **Continuar**.
4 En el siguiente diálogo, introduzca lo siguiente:

- **Categoría**: elija una categoría para el inicio de sesión del sitio web o el programa que va a guardar. Si no ha agregado categorías, esta lista estará vacía.
- **Nombre de la cuenta**: déjelo tal cual para aceptar el nombre completado automáticamente, o escriba el nombre del sitio web o el programa.
- **Título sin detectar**: Password Manager detecta estos campos como los campos en la página de inicio de sesión en los que introduce su información de inicio de sesión. Estos campos incluyen normalmente el Nombre de usuario o Correo electrónico y la Contraseña.

5 Si se muestra un nombre de campo como título sin detectar o si se han incluido los campos erróneos como campos de inicio de sesión, haga clic en el botón **Más campos** para editar los nombres de campo o eliminar los campos.

6 En el cuadro de diálogo de más campos, haga clic en **Título sin detectar** e introduzca el nombre de campo correcto para cada uno.

Cuando aparece el cuadro de diálogo Más campos, el campo que estaba activo en el cuadro de diálogo Agregar inicio de sesión se resalta para ayudarle a renombrar los campos.

Si un campo no es necesario para iniciar sesión, para excluirlo de la información de inicio de sesión, desactive su casilla de verificación.

7 Para guardar los cambios, haga clic en **Aceptar**.

8 En el cuadro de diálogo Agregar inicio de sesión, complete los campos necesarios para el inicio de sesión.

> **NOTA:**
> Debido a que está guardando un inicio de sesión existente, solo puede cambiar la contraseña en la función Cambiar contraseña del sitio web o programa.

9 Si desea que Password Manager rellene automáticamente y envíe la información de inicio de sesión, seleccione **Enviar datos de inicio de sesión automáticamente**.

10 Haga clic en **Guardar**.

El inicio de sesión de la página web o del programa se muestra en la página del Administrador de inicio de sesión.

Importación de credenciales

Puede importar credenciales guardadas en navegadores web en Password Manager.

1 En la herramienta Password Manager, seleccione **Importar credenciales**.

2 Seleccione el explorador en el que desea importaras y haga clic en **Escanear**.

3 Cuando se le indique, introduzca la contraseña del explorador seleccionado.

> **NOTA:**
> Si la importación no contiene contraseñas importadas, compruebe si el explorador ha almacenado los datos que desea importar. Si está utilizando Firefox, inicie sesión en Sync. Intente importar las credenciales una vez más.

Menú contextual del icono

Cuando visita un sitio web o abre un programa, aparece el icono de Password Manager.

indica que el formulario de inicio de sesión se puede entrenar.

Cuando no se encuentra presente, el formulario de inicio de sesión ya ha sido entrenado. Haga doble clic en el icono para iniciar sesión en el programa o sitio web.

Cuando haga clic en el icono, un menú contextual muestra diferentes opciones, dependiendo de si el formulario de inicio de sesión está o no capacitado.

Cuando los campos de inicio de sesión actuales todavía no han sido capacitados, el menú contextual muestra las siguientes opciones:

Agregar a Password Manager: abre el cuadro de diálogo para agregar el inicio de sesión.

Configuración del icono: permite que el usuario configure la visualización del icono de Password Manager en las páginas de inicio de sesión entrenables.

Abrir Password Manager: inicia la herramienta de *administración de Password Manager* y abre la página de administrador de inicio de sesión.

Ayuda: abre la ayuda en pantalla.

Cuando los campos de inicio de sesión actuales han sido capacitados, el menú contextual muestra las siguientes opciones:

Rellenar datos de inicio de sesión: en función de las opciones que haya seleccionado al entrenar el formulario de inicio de sesión, iniciará sesión de forma automática o rellenará los campos de nombre de usuario y contraseña, permitiéndole enviar los datos de inicio de sesión.

Editar inicio de sesión: abre el cuadro de diálogo para editar el inicio de sesión.

Agregar inicio de sesión: abre el cuadro de diálogo para agregar el inicio de sesión.

Abrir Password Manager: abre la página de administrador de inicio de sesión.

Ayuda: abre la ayuda en pantalla.

Si los iconos de Password Manager no aparecen con formularios de inicio de sesión, desactive la función de guardado de contraseña de su explorador:

- En Mozilla Firefox: icono de menú > Opciones > Seguridad > desmarque la casilla de verificación **Recordar credenciales de sitios**.
- En Internet Explorer: icono del engranaje > Opciones de Internet > pestaña Contenido > Configuración de Autocompletar > desmarque la casilla de verificación **Nombres de usuario y contraseñas en formularios**.

Inicio de sesión en páginas de inicio de sesión capacitadas

Cuando abre un inicio de sesión en un sitio web o de un programa, Password Manager detecta si la página está capacitada. Si lo está, el icono de Password Manager aparece en el área de inicio de sesión. Si no lo está, se muestra el icono de Password Manager, a menos que se hayan deshabilitado las solicitudes para formularios no entrenados.

Para iniciar sesión, seleccione uno:

- Explore las credenciales registradas. Si ha registrado una huella digital o tarjeta inteligente, puede tocar el lector de huellas digitales con una huella digital registrada o presentar una tarjeta registrada al lector de tarjetas.
- Haga clic en el icono de Password Manager y seleccione **Completar datos de inicio** en el menú contextual.
- Pulse la combinación de teclas de acceso rápido de Password Manager: **Ctrl+Win+H**. El elemento emergente de Password Manager muestra sus sitios capacitados, lo que le permite iniciar uno rápidamente.

NOTA:
Puede modificar la combinación de teclas de acceso rápido en la DDP Console > Password Manager > Configuración.

En caso de que se haya almacenado más de un inicio de sesión para el sitio web o el programa, se le solicita que seleccione la cuenta que desea utilizar.

Compatibilidad con dominios web

Si ha capacitado una página de inicio de sesión para un dominio web específico pero desea acceder a la cuenta en ese dominio web desde una página de inicio de sesión diferente, vaya hasta la nueva página de inicio de sesión. Se le pide que utilice un inicio de sesión existente o agregue uno nuevo a Password Manager.

- Si hace clic en *Utilizar inicio de sesión*, se iniciará sesión en la cuenta que ha creado anteriormente. La próxima vez que acceda a la cuenta desde la nueva página de inicio de sesión, automáticamente se iniciará sesión en la cuenta anteriormente creada.
- Al hacer clic en *Agregar inicio de sesión*, aparecerá el cuadro de diálogo Agregar inicio de sesión.

Introducción de credenciales de Windows

Algunos programas le permiten utilizar las credenciales de Windows para iniciar sesión.

En lugar de escribir el nombre de usuario y la contraseña, puede elegir sus credenciales de Windows en los menús desplegables disponibles en los cuadros de diálogo *Agregar inicio de sesión* y *Editar inicio de sesión*.

Para el nombre de usuario, puede elegir entre los siguientes tipos:

- Nombre de usuario de Windows
- Nombre principal del usuario de Windows
- Nombre de usuario\Dominio de Windows
- Dominio de Windows

Para la contraseña, utilice su contraseña de Windows.

No se pueden modificar estas opciones.

Uso de una contraseña antigua

Es posible que se haya cambiado una contraseña en Password Manager, por lo que el programa rechaza la nueva contraseña. En este caso, el programa le permite utilizar una contraseña anterior (una contraseña que se haya introducido previamente para esta página de inicio) en lugar de la más reciente.

Seleccione **Historial de contraseñas**. Tras la autenticación, se le solicitará que elija una contraseña antigua de la lista Historial de contraseñas. La lista incluye siete contraseñas.

Excluir sitios web

Para evitar que Password Manager administre sitios web, haga clic en la pestaña **Exclusiones de sitios web**.

Los sitios web excluidos tienen las siguientes características:

- No hacen que se abra un icono de Password Manager.
- No inician sesión automáticamente para los usuarios.
- No muestran recordatorios de contraseña.

Para agregar un nuevo sitio web a la lista de exclusiones:

1 Haga clic en la pestaña **Exclusiones de sitios web**.
2 Haga clic en **Agregar sitio web**.

3 Introduzca la URL del sitio web a excluir.
4 Haga clic en **Guardar**.

Una vez que haya excluido un sitio web, Password Manager no administrará el sitio web. Simplemente elimine el sitio web de la lista de Exclusiones de sitios web para revertir la exclusión. Para eliminar un sitio web de la lista de exclusiones: haga clic en X.

Después de agregar varios sitios web, puede:

- Para ordenar la lista por sitio web, en orden ascendente o descendente, haga clic en el encabezado de columna Sitio web.
- Para buscar en la lista, introduzca parte de la URL en el campo de búsqueda. La lista se filtra al escribir.

Deshabilitación de las solicitudes para capacitar los formularios de inicio de sesión

Puede conservar los inicios de sesión capacitados existentes y deshabilitar las solicitudes para capacitar nuevos formularios de inicio de sesión.

Para deshabilitar los avisos de nuevos inicios de sesión:

1 Abra la DDP Console.
2 Haga clic en el mosaico de **Password Manager**.
3 Haga clic en la pestaña **Configuración**.
4 Desmarque la casilla de verificación **Preguntar si desea añadir un inicio de sesión en la pantalla de inicio**.

Cómo hacer una copia de seguridad y restaurar las credenciales de Password Manager

Password Manager le permite realizar una copia de seguridad de forma segura de los datos de inicio de sesión administrados por Password Manager. Estos datos se pueden restaurar en cualquier equipo protegido por Password Manager.

NOTA:
La información de Password Manager no incluye las credenciales del sistema operativo ni del inicio de sesión de autenticación de prearranque (PBA), ni tampoco información específica de credenciales, como las huellas digitales.

Credenciales de copia de seguridad

Para realizar copias de seguridad de las credenciales:

1 Haga clic en la pestaña **Credenciales de copia de seguridad** para configurar el proceso de copia de seguridad.
2 Haga clic en **Examinar** y navegue hasta la ubicación de la copia de seguridad deseada.
Si intenta realizar una copia de seguridad de los datos en una unidad local, aparecerá una advertencia con la recomendación de realizar la copia de seguridad en un dispositivo de almacenamiento portátil o una unidad de red.
3 Introduzca y confirme una contraseña. Se debe utilizar esta contraseña si se tienen que restaurar las credenciales con copia de seguridad.
4 Haga clic en **Copia de seguridad**.
5 Introduzca su contraseña de Windows.
6 En el cuadro de diálogo correcto, haga clic en **Aceptar**.

NOTA:

Para ver un registro de texto de la operación de copia de seguridad realizada, haga clic en y seleccione **Registro**.

Restauración de credenciales

La ubicación de copia de seguridad debe estar disponible para restaurar las credenciales.

Para restaurar credenciales:

1 Haga clic en la pestaña **Restaurar credenciales**.
2 Haga clic en **Examinar** para acceder al archivo de copia de seguridad y, a continuación, introducir la contraseña del archivo.
3 Haga clic en **Restaurar**.

AVISO:

La restauración de los datos de Password Manager sobreescribirá datos existentes. Se perderán los inicios de sesión y otros datos agregados después de la creación de la copia de seguridad.

4 Haga clic en **Siguiente**.

NOTA:

Para ver un registro de texto de la operación de restauración realizada en este equipo, haga clic en el icono y seleccione **Registro**.

7

Glosario

Credencial: una credencial es algo que demuestra la identidad de una persona, como sus huellas dactilares o su contraseña de Windows.

Contraseña de un solo uso (OTP): una Contraseña de un solo uso es una contraseña que se puede utilizar solamente una vez y es válida durante un periodo de tiempo limitado. OTP requiere que haya un TMP presente, habilitado y con propietario. Para habilitar OTP, se asocia un dispositivo móvil con el equipo mediante la Security Console y la aplicación Security Tools Mobile. La aplicación Security Tools Mobile genera la contraseña en el dispositivo móvil que se utiliza para iniciar sesión en el equipo en la pantalla de inicio de sesión de Windows. En función de la política, es posible que la función OTP se utilice para recuperar el acceso al equipo si la contraseña ha caducado o se ha olvidado, si la OTP no ha sido utilizada para iniciar sesión en el equipo. La función OTP se puede utilizar para la autenticación o la recuperación, pero no para ambas cosas. La seguridad OTP supera la de otros métodos de autenticación ya que la contraseña generada se puede utilizar una sola vez y se vence en un periodo corto de tiempo.

Autenticación previa al inicio (PBA): la autenticación previa al inicio sirve como una extensión del BIOS o del firmware de arranque y garantiza un entorno seguro, a prueba de manipulaciones y externo al sistema operativo como un nivel de autenticación fiable. La PBA impide la lectura de la unidad de disco duro, incluido el sistema operativo, hasta que el usuario haya confirmado que tiene las credenciales correctas.

Protegido: para una unidad de disco con autocifrado (SED), un ordenador se encuentra protegido una vez que el SED se ha activado y la autenticación de prearranque (PBA) se ha implementado.

Unidades de cifrado automático (SED): una unidad de disco duro con un mecanismo de cifrado integrado que cifra todos los datos almacenados en el soporte y descifra todos los datos que abandonan el soporte de manera automática. Este tipo de cifrado es completamente claro par el usuario.

Inicio de sesión único (SSO): El inicio de sesión único simplifica el proceso de inicio de sesión cuando está habilitada la autenticación multifactor tanto antes del arranque como al inicio de sesión en Windows. Si está habilitada, la autenticación se requiere solo en el preinicio, y los usuarios inician sesión en Windows automáticamente. Si está deshabilitada, la autenticación puede requerirse varias veces.

Trusted Platform Module (TPM): el TPM es un chip de seguridad que cumple tres funciones importantes: atestación, medición y almacenamiento seguro. El cliente Encryption utiliza el TPM por su función de almacenamiento seguro. El TPM también sirve para proporcionar contenedores cifrados al almacén de software. El TPM también es necesario para utilizarlo con la función de Contraseña de un solo uso.