Dell Data Security Console

User Guide v3.9

January 2024
Rev. A01

DELL Technologies

Notas, precauciones y advertencias

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

PRECAUCIÓN: CAUTION indica la posibilidad de daños en el hardware o la pérdida de datos y le informa cómo evitar el problema.

AVISO: WARNING indica la posibilidad de daños en la propiedad, lesiones personales o la muerte.

Contents

1

Introducción

Data Security Console brinda 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 registrar fácilmente su contraseña de PBA y sus preguntas de recuperación.

Las siguientes funciones se encuentran disponibles:

- Registre las credenciales que se utilizarán con PBA
- Aproveche sus credenciales de factor múltiple, incluidas las contraseñas 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
- Cambie fácilmente su contraseña de Windows
- Establezca preferencias personales
- Ver estado de cifrado
- Revise el estado de la protección web y del Firewall (en caso de estar instalados).
- Revise el estado de Advanced Threat Prevention.

Las siguientes características están disponibles a través de Data Security Console, en el sistema operativo de un servidor:

- Vea el estado de cifrado (en equipos con unidades de cifrado automático)
- Vea Advanced Threat Prevention

Data Security Console

Para abrir Data Security Console desde el escritorio, haga doble clic en el icono de Dell Data Security Console 

.

Puede acceder a estas aplicaciones:

- Estado de cifrado permite ver el estado del cifrado de las unidades y las particiones del equipo.
- El panel de Advanced Threat Prevention muestra el estado de protección del equipo, según las políticas de Advanced Threat Prevention.
- En la página de estado de Firewall y protección web se muestra el estado de protección general e individual de las computadoras (Protección web y Firewall).
- La herramienta de acceso mediante inicio de sesión le permite configurar y administrar contraseñas de PBA, configurar las preguntas de autorecuperación de PBA y visualizar el estado del registro de sus credenciales.

Esta guía describe cómo utilizar cada una de estas aplicaciones.

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

Comuníquese con el equipo de Dell ProSupport for Software

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

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

Tenga su Código de servicio rápido o Etiqueta de servicio a mano cuando realice la llamada para asegúrese de ayudarnos a conectarle rápidamente con el experto técnico adecuado.

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

2

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 Data Security Console, haga clic en el ícono correspondiente situado en la esquina derecha de la barra de título.

Para restaurar la Data Security Console después de minimizar, haga doble clic en el icono del área de notificación.

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

Detalles de Data Security Console

Para ver detalles sobre la Data Security Console, políticas, servicios en ejecución y registros, haga clic en el ícono de engranaje situado en el lado izquierdo 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 la versión.
Mostrar información	Contiene lo siguiente: • información sobre la fecha y la versión del producto • si Dell Encryption o la autenticación avanzada de PBA es administrada por la empresa o por un administrador local • 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).
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.
Advanced Threat Prevention	Habilita la interfaz de usuario estándar para el panel de Advanced Threat Prevention.
Registro	Muestra una lista detallada de eventos registrados para la solución de problemas.

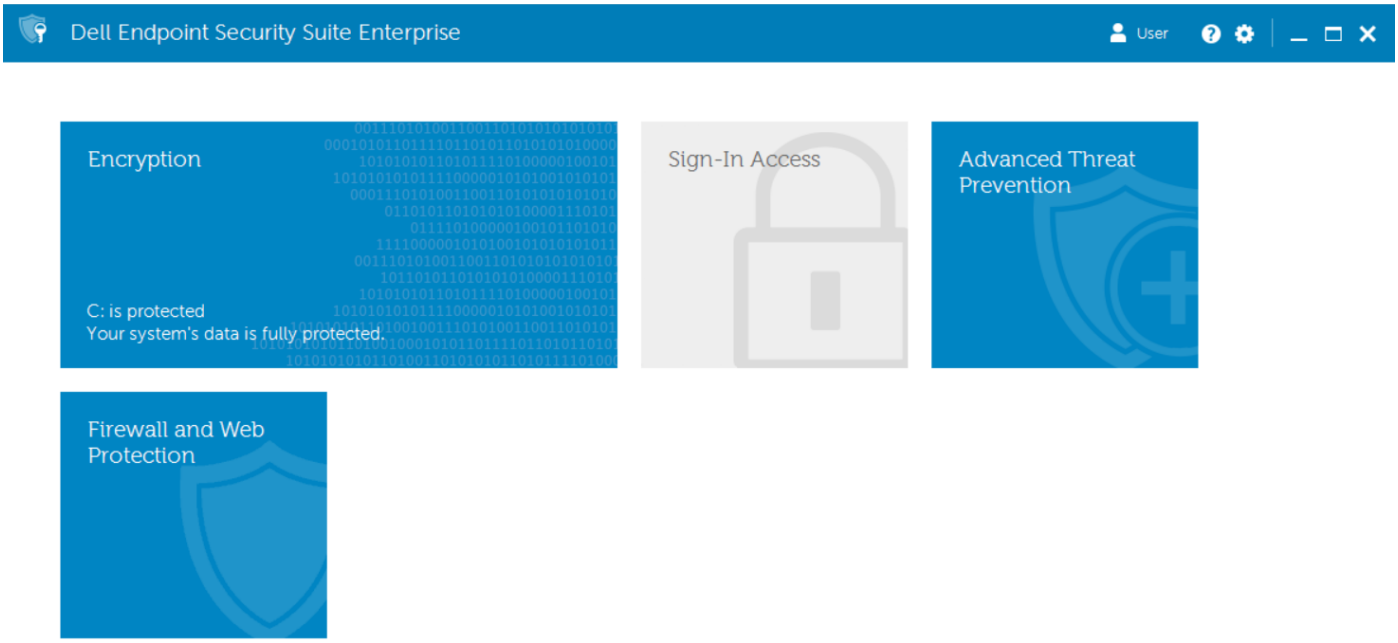
3

Advanced Threat Prevention

Advanced Threat Prevention protege su equipo contra malware mediante la supervisión de todos los procesos que se intentan ejecutar en su equipo o dentro del espacio de memoria y marcando cualquier proceso que se considere anómalo o no seguro.

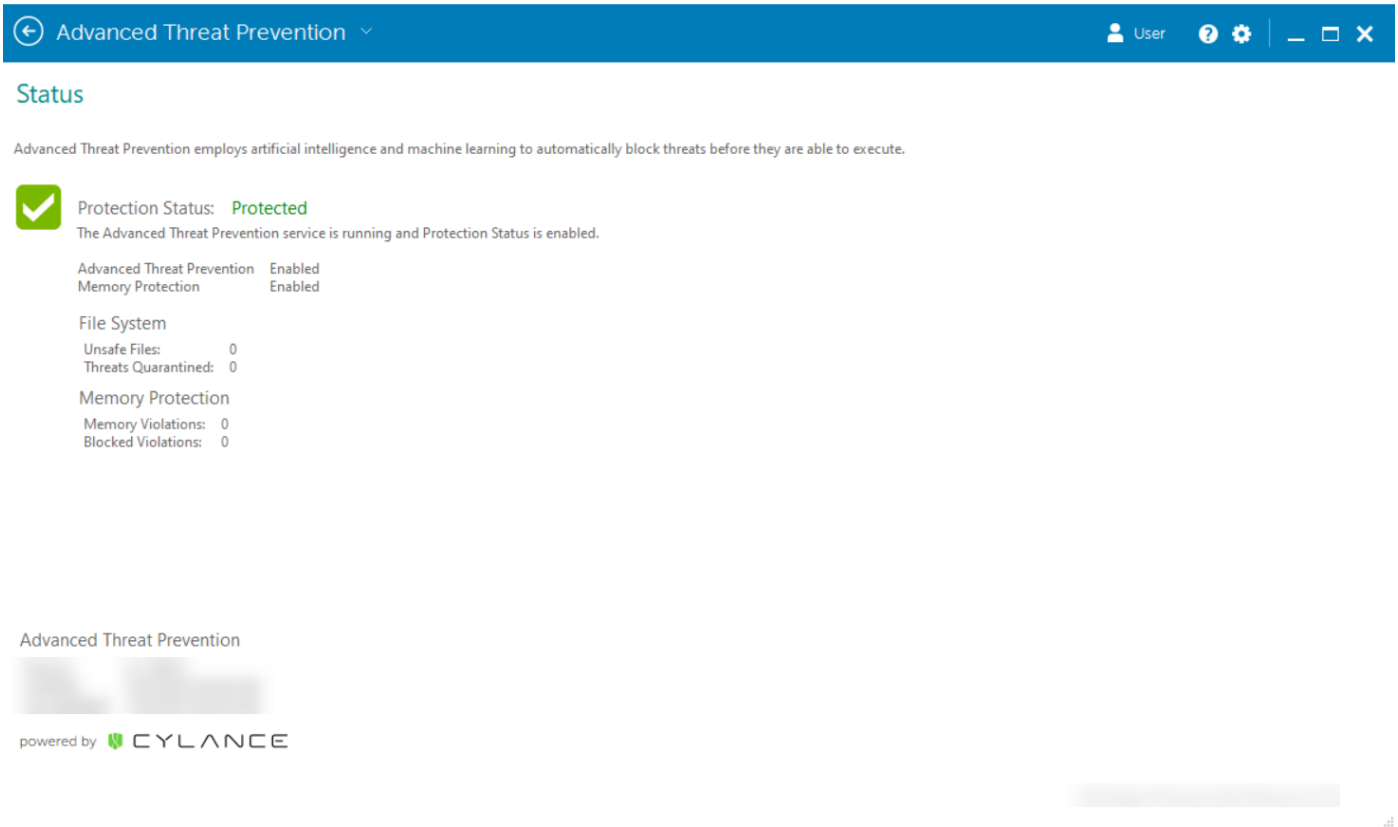
De forma predeterminada, Advanced Threat Prevention se instala con Endpoint Security Suite Enterprise. El servidor de seguridad y protección web tiene la opción de instalarse como parte de Endpoint Security Suite Enterprise.

Seleccione el mosaico de Advanced Threat Prevention para ver las estadísticas del equipo tras el análisis y la supervisión avanzada.



Estado de Advanced Threat Prevention

Acceda a la página de estado de Advanced Threat Prevention desde el mosaico **Advanced Threat Prevention** en Data Security Console.



Estado de protección

El estado de protección indica si el equipo está protegido (indicado mediante una marca de verificación verde) o desprotegido (indicado mediante una X roja), según si el servicio Advanced Threat Prevention se está ejecutando y si Advanced Threat Prevention está activado en el Dell Server.

- Advanced Threat Prevention: indica si Advanced Threat Prevention está activado en el Dell Server.
- Protección de memoria: indica si la protección de memoria está activada en el Dell Server.

Sistema de archivos

- Archivos no seguros: número de archivos del equipo que probablemente sean malware.
- Amenazas en cuarentena: número de archivos que se han movido de su ubicación original en el equipo y se impide su ejecución.

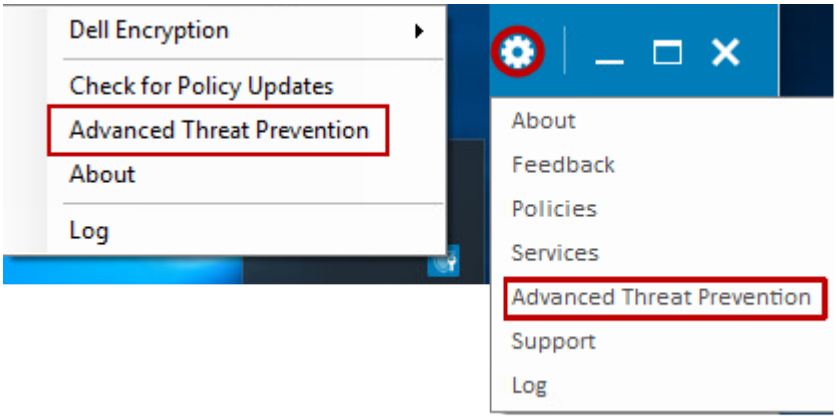
Protección de memoria

- Violaciones de memoria: número de intentos de conectarse a la memoria del ordenador por parte de aplicaciones.
- Violaciones bloqueadas: número de intentos bloqueados de conectarse a la memoria del ordenador por parte de aplicaciones.

Interfaz de usuario estándar

Mediante la interfaz de usuario estándar, se habilita una nueva función en el menú de engranaje o el menú de bandeja de sistema en la Data Security Console que muestra información detalla sobre los eventos que se han capturado en un terminal específico. La interfaz de usuario estándar **solo** se puede activar si su política está habilitada en la Remote Management Console. Para obtener información adicional, consulte *AdminHelp* seleccionando **?** en la esquina superior derecha de la Remote Management Console.

La interfaz de usuario estándar se puede activar en la Data Security Console con el icono de la bandeja de sistema o de engranaje que se encuentra en el lado izquierdo de la barra de título.



Seleccione una de las siguientes opciones para mostrar los detalles extensos de Advanced Threat Prevention:

- **Mostrar amenazas**

  Mediante la opción **Mostrar amenazas**, podrá obtener las amenazas que se han mitigado con Advanced Threat Prevention y los siguientes detalles:

  Identificador de hash del archivo: muestra la información de hash SHA256 de la amenaza.

  MD5 del archivo: el hash MD5.

  ¿Se está ejecutando actualmente? - ¿Se está ejecutando la amenaza actualmente en su dispositivo? Ejecución en curso o no.

  Ruta de archivo: la ruta en la que se encontró la amenaza. Incluye el nombre del archivo.

  Puntuación: clasificación de la amenaza.

- **Mostrar vulnerabilidades**

  Mediante la opción **Mostrar vulnerabilidades**, podrá obtener las vulnerabilidades que se han mitigado con Advanced Threat Prevention y los siguientes detalles:

  Id. de evento: número exclusivo asignado a cada evento de amenaza.

  Identificador de proceso: muestra el identificador del proceso de la aplicación que encontró la Protección de memoria.

  Etiqueta de proceso: un identificador único con el que se categorizan los procesos según el ciclo de arranque.

  Hash de imagen: muestra la información de hash SHA256 de la vulnerabilidad.

  Ruta de imagen: la ruta en la que se origina la vulnerabilidad. Incluye el nombre del archivo.

  Versión de archivo: muestra el número de versión del archivo de vulnerabilidad.

- **Mostrar scripts**

  Mediante la opción **Mostrar scripts**, podrá obtener los scripts que se han mitigado con Advanced Threat Prevention y los siguientes detalles:

  Ruta de script: la ruta en la que se origina el script. Incluye el nombre del archivo.

  Identificador de evento: un número único asignado a cada evento de script.

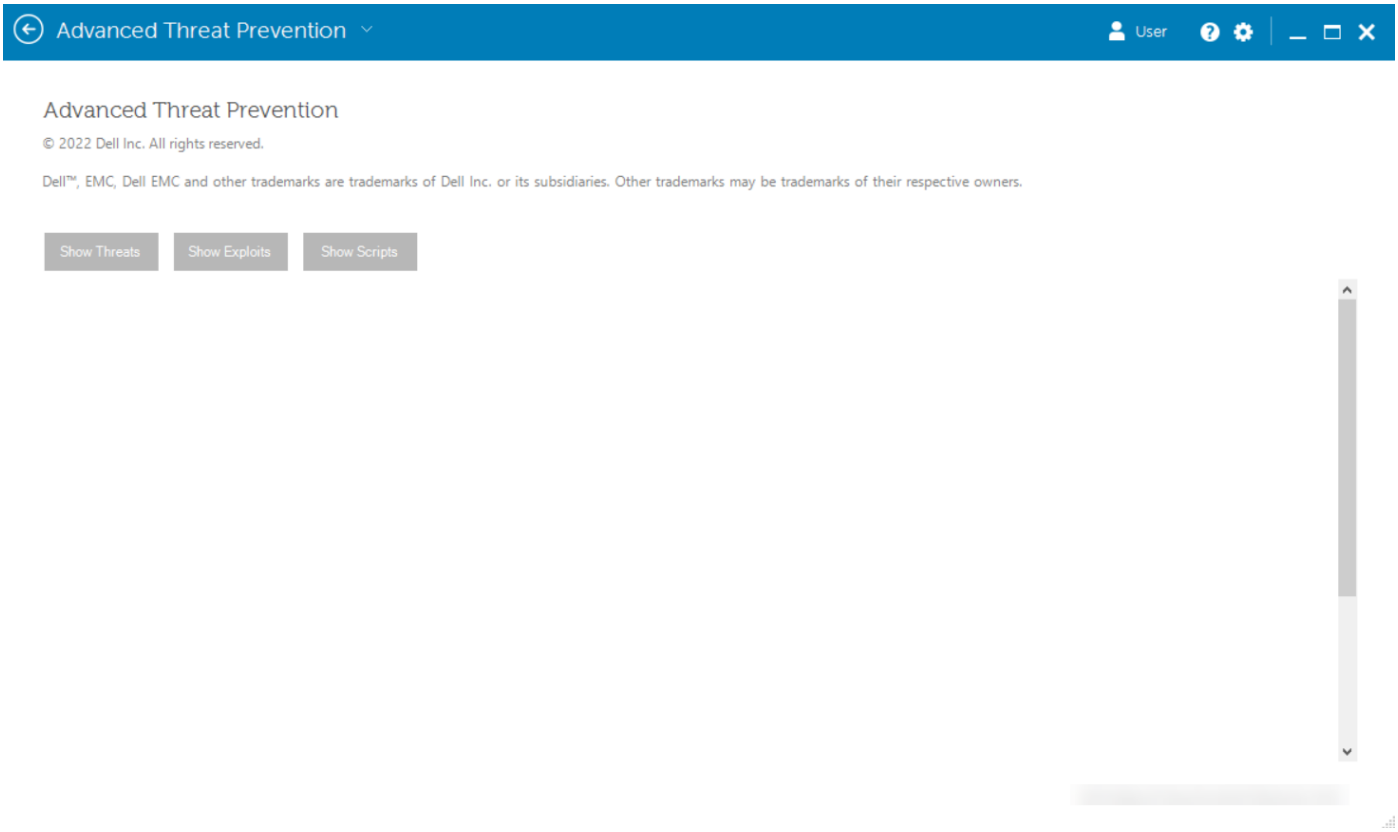
  Identificador de hash del archivo: muestra la información de hash SHA256 del script.

  MD5 del archivo: el hash MD5.

  Tipo de unidad: información acerca de si la unidad es interna o externa.

  Nombre de intérprete: el nombre de la función de control de script con la que se identificó el script malicioso.

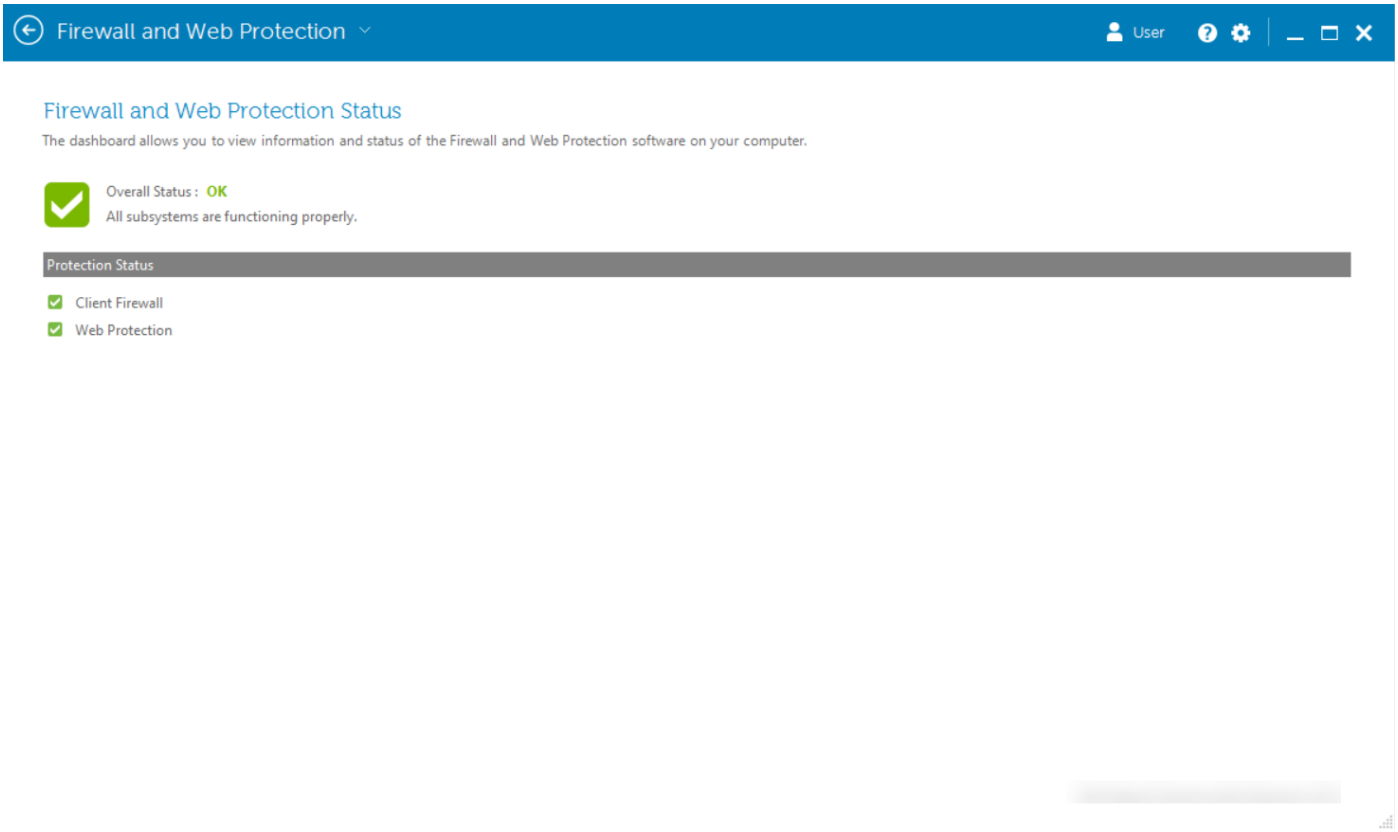
  Versión de intérprete: el número de versión de la función de control de script.



La lista de eventos mostrada se recopila cuando se inicia esa sesión de Data Security Console. Para recuperar eventos nuevos, cierre Data Security Console y vuelva a iniciarla.

Estado de servidor de seguridad y protección

Acceda a la página de estado del servidor de seguridad y protección web desde el mosaico **Servidor de seguridad y protección web** de Data Security Console.



Estado general

El estado general indica si el equipo está protegido o es vulnerable, según la configuración de la política del servidor de seguridad y protección web en el Dell Server.

- Protegido: el estado general está protegido si las políticas de *protección web* o de *firewall del cliente* están activadas.
- Vulnerable: el estado general es Vulnerable si las políticas de servidor de seguridad de cliente y la protección web están desactivadas.

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 siguientes políticas están activadas en el Dell Server:

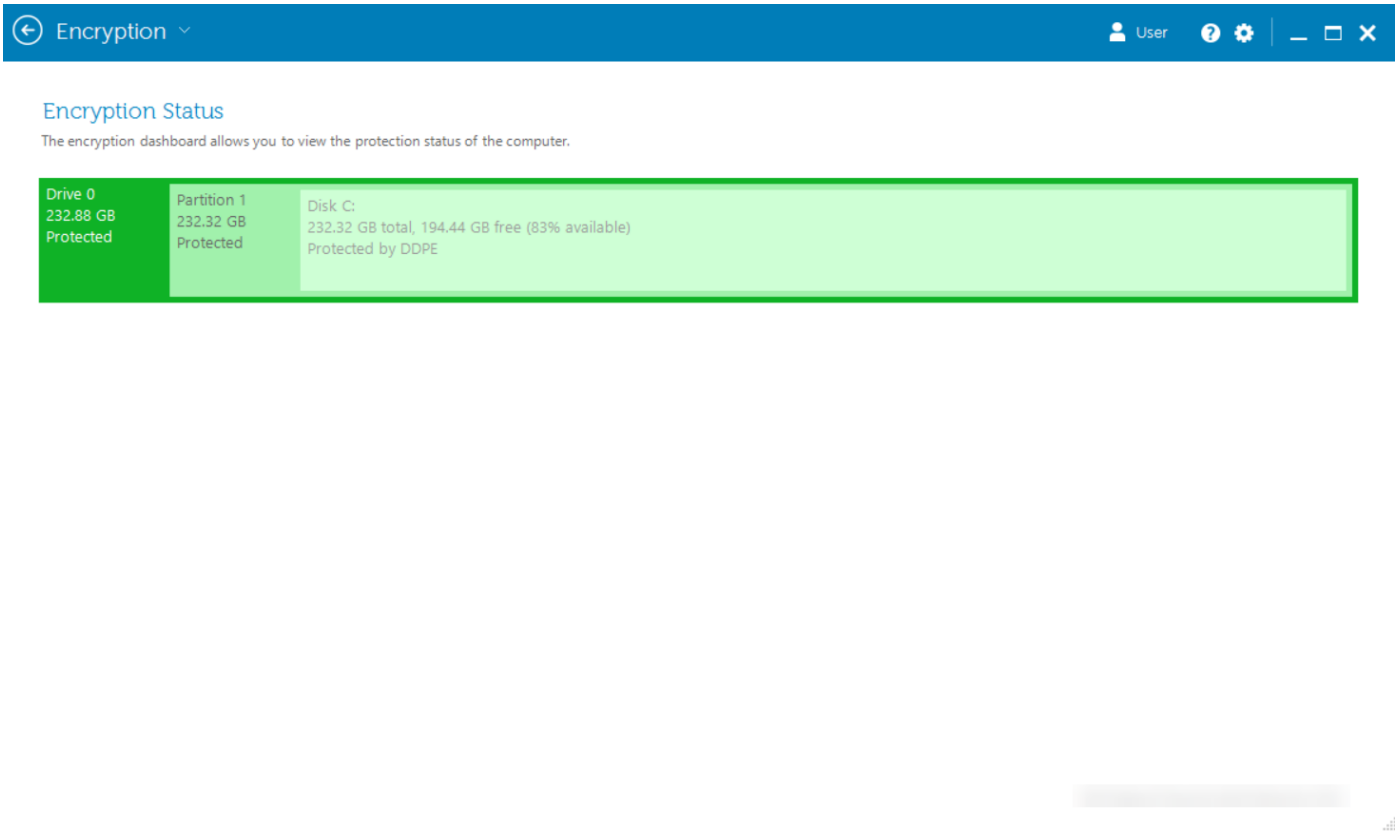
- Servidor de seguridad del cliente: el estado general es Protegido si la política del servidor de seguridad del cliente está activada.
- Protección web: el estado general es Protegido si la política de protección web está activada.

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

Acceso mediante inicio de sesión

Acceso mediante inicio de sesión le permite registrar, modificar y comprobar su estado de registro, según la política que configuró el administrador.

Después del registro inicial, puede hacer clic en el mosaico Acceso mediante inicio de sesión para agregar o modificar las credenciales.

NOTA: El mosaico Acceso mediante inicio de sesión solo se mostrará si el PBA está activo.

Registro de credenciales por primera vez

Para registrar credenciales por primera vez:

1. En la página de inicio de Data Security Console, haga clic en el mosaico **Acceso mediante inicio de sesión**.
2. Para cambiar su contraseña de Windows, vaya a la página Contraseña, ingrese su contraseña actual y luego su contraseña nueva, confírmela y haga clic en **Cambiar**.
3. En la página Pregunta de recuperación, responda tres preguntas de recuperación, luego haga clic en **Registrar**.

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 **Acceso mediante inicio de sesión**.

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 Acceso mediante inicio de sesión 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 Data Security Console, en lugar de en Windows. Si se cambia la contraseña de Windows fuera de la Data Security 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 de PBA 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 **Restablecer** para desmarcar las opciones seleccionadas en esta página y empezar de nuevo.

Preguntas de recuperación ya registradas

Si las preguntas de recuperación de PBA 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 de PBA por completo, haga clic en **Eliminar**.
   - Para volver a definir las preguntas de recuperación de PBA y las respuestas, haga clic en **Volver a registrar**.

6

Glosario

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

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.