Dell Data Protection | Access. Inicio

La página de inicio de **Dell Data Protection | Access** es el punto inicial para acceder a las funciones de la aplicación. Desde esta ventana podrá acceder a lo siguiente:

System Access Wizard
Opciones de acceso
Self-Encrypting Drive
Opciones avanzadas

En la esquina inferior derecha de la ventana hay un enlace llamado **avanzadas**, que puede pulsar para acceder a las opciones avanzadas.

Desde las opciones avanzadas, puede hacer clic en el enlace **inicio**, situado en la esquina inferior derecha de la ventana, para volver a la página de inicio.

System Access Wizard

System Access Wizard se inicia automáticamente la primera vez que se abre la aplicación **Dell Data Protection | Access**. Este asistente le guiará a través de la configuración de todos los aspectos de la seguridad del sistema, incluyendo cómo (p.ej., contraseña solo o huella dactilar y contraseña) y cuándo (Windows, pre-Windows o ambos) desea iniciar sesión en el sistema. Además, si el sistema tiene una self-encrypting drive, puede configurarla a través de este asistente.

Funciones del administrador

Los usuarios configurados con privilegios de administrador de Windows en el sistema tienen derecho a utilizar las siguientes funciones en **Dell Data Access | Protection**, que los usuarios estándar no pueden:

- Establecer / cambiar la contraseña de sistema (Pre-Windows)
- Establecer / cambiar la contraseña del disco duro
- Establecer / cambiar la contraseña del administrador
- Establecer / cambiar la contraseña de propietario de TPM
- Establecer / cambiar la contraseña del administrador de ControlVault
- Restaurar el sistema
- Archivar y restaurar credenciales
- Establecer / cambiar el PIN del administrador de la smartcard
- Borrar / restaurar una smartcard
- Activar / Desactivar el inicio de sesión seguro de Dell en Windows
- Establecer la política de inicio de sesión en Windows
- Gestionar las self-encrypting drives, incluyendo:
    - Activar / Desactivar el bloqueo de self-encrypting drive
    - Activar / Desactivar la sincronización con contraseña de Windows (WPS)
    - Activar / Desactivar Single Sign On (SSO)
    - Realizar un borrado criptográfico

Gestión remota

Su organización puede configurar un entorno donde se gestionen centralmente las funciones de seguridad de la aplicación **Dell Data Protection | Access** en varias plataformas gestión remota). En este caso, puede utilizarse la infraestructura de seguridad de Windows, como Active Directory, para gestionar de forma segura las funciones específicas de **Dell Data Protection | Access**.

Cuando un ordenador se gestiona remotamente (es decir, cuando su propietario sea el administrador remoto), se desactivará la administración local de la función **Dell Data Protection | Access**; las ventanas de gestión de la aplicación no serán accesibles localmente. Es posible gestionar remotamente las siguientes funciones:

- Trusted Platform Module (TPM)
- ControlVault
- Inicio de sesión Pre-Windows
- Restaurar sistema
- Contraseñas de BIOS
- Política de inicio de sesión en Windows
- Self-Encrypting Drives
- Asociación de huellas dactilares y Smartcard

Para solicitar más información sobre cómo utilizar el servidor EMBASSY® Remote Administration Server (ERAS) de Wave Systems para la gestión remota, póngase en contacto con un comercial de Dell o visite dell.com.

Opciones de acceso

Desde la ventana Opciones de acceso, puede configurar cómo acceder a su sistema.

Si tiene alguna opción de **Dell Data Protection | Access** establecida, se mostrará en la página de inicio con las opciones disponibles (por ejemplo, cambiar contraseña para el inicio de sesión pre-Windows). Las opciones disponibles son accesos directos que, al hacer clic sobre ellos, le llevan a la ventana correspondiente para realizar una tarea específica (por ejemplo, cambiar su contraseña pre-Windows o asociar otra huella dactilar).

General
En primer lugar, puede especificar cuándo iniciar sesión (en Windows, pre-Windows o ambos) y cómo (por ejemplo, huella dactilar y contraseña). Puede elegir una o dos opciones sobre cómo iniciar sesión; estas incluyen combinaciones de huellas dactilares, smartcard y contraseña. Las opciones enumeradas se basan en las políticas de inicio de sesión aplicadas a su entorno y en lo que se admite en la plataforma.

Huella dactilar
Si su sistema tiene un lector de huella dactilar, puede asociar o actualizar las huellas dactilares y utilizarlas para iniciar sesión en su sistema. Cuando haya asociado las huellas dactilares, podrá pasar los dedos asociados sobre el lector de huellas del sistema para acceder a él en Windows, pre-Windows o ambos (dependiendo de lo que haya especificado en las opciones generales de acceso). Consulte Asociación de huellas dactilares del usuario para más información.

Inicio de sesión Pre-Windows
Si ha especificado que los usuarios deben iniciar sesión pre-Windows, debe establecer una contraseña del sistema (a veces llamada contraseña pre-Windows) para el acceso pre-Windows. Una vez establecida, el administrador podrá cambiarla en cualquier momento.

También puede desactivar el inicio de sesión pre-Windows desde esta pantalla; para ello, tendrá que introducir su contraseña de sistema actual, comprobar que la contraseña es correcta y después hacer clic en el botón **Desactivar**.

Smartcard
Si ha especificado que los usuarios deben utilizar una smartcard para iniciar sesión, es necesario que asocie una o más smartcards contactless (o con contacto). Haga clic en el enlace **Asociar otra SmartCard** para abrir el asistente de asociación de smartcard. "Asociar" significa configurar la smartcard para utilizarla en el inicio de sesión.

Una vez asociada la smartcard, podrá cambiar o establecer un PIN para esta tarjeta con el enlace **Cambiar o establecer mi PIN de smartcard**.

Inicio de sesión Pre-Windows

Si configura el inicio de sesión pre-Windows, debe autenticarse (contraseña, huella dactilar o smartcard) al encenderse el sistema, antes de que se cargue Windows. La función de inicio de sesión pre-Windows proporciona una seguridad adicional al sistema, ya que evita que usuarios autorizados comprometan Windows y accedan al ordenador (por ejemplo, si éste ha sido robado).

Desde la ventana Inicio de sesión pre-Windows, los administradores pueden configurar el inicio de sesión pre-Windows o crear y cambiar una contraseña (de sistema) de pre-Windows. Si ya se ha configurado la contraseña, puede desactivar el inicio de sesión pre-Windows desde esta ventana. Al configurar el inicio de sesión pre-Windows se abrirá un asistente que hará lo siguiente:

- Contraseña del sistema: configure una contraseña del sistema (también llamada contraseña pre-Windows) para el acceso pre-Windows. Esta contraseña se utiliza también como copia de seguridad en caso de que un usuario tenga factores de autenticación adicionales (por ejemplo, para acceder al sistema si hay algún problema con el sensor de huellas dactilares).
- Huella dactilar o Smartcard: configure una huella dactilar smartcard para utilizarla en el inicio de sesión pre-Windows y especifique si desea utilizar este factor de autenticación en lugar (o además) de la contraseña pre-Windows.
- Single Sign On: Por defecto, su autenticación pre-Windows (contraseña, huella dactilar o smartcard) se utilizará también para iniciar sesión automáticamente en Windows (a esto se le denomina "Single Sign On"). Para desactivar esta función, seleccione la casilla "Deseo iniciar sesión de nuevo en Windows".
- Si además de la contraseña pre-Windows, se ha establecido la contraseña del disco duro de la BIOS , también tendrá la opción de cambiar o desactivar la contraseña del disco duro.

NOTA: no todos los lectores de huellas dactilares sirven para la autenticación pre-Windows. Si el lector no es compatible, sólo podrá asociar huellas dactilares para el inicio de sesión de Windows. Para saber si un lector de huellas dactilares específico es compatible, póngase en contacto con el administrador de su sistema o visite support.dell.com, donde encontrará una lista de los lectores de huellas dactilares admitidos.

Desactivar inicio de sesión Pre-Windows
También puede desactivar el inicio de sesión pre-Windows desde esta ventana; para ello, tendrá que introducir su contraseña (de sistema) actual pre-Windows, comprobar que la contraseña es correcta y después hacer clic en el botón **Desactivar**. Recuerde que, al desactivar el inicio de sesión pre-Windows, las huellas dactilares o las smartcards que haya asociado seguirán estándolo.

Asociar y quitar huellas dactilares

Los usuarios pueden registrar o actualizar las huellas dactilares que les permiten autenticarse en el sistema bien al iniciar sesión en Windows, bien antes de Windows (pre-Windows). En la ficha Huella dactilar, las imágenes de las manos muestran los dedos que se han asociado (si los hubiera). Si hace clic en el enlace **Asociar otro**, se abrirá el asistente de asociación de huellas dactilares, que le guiará por todo el proceso de asociación. "Asociar" significa guardar una huella dactilar que se utilizará para el inicio de sesión. Para poder asociar huellas dactilares, debe tener un lector de huellas válido correctamente instalado y configurado.

NOTA: no todos los lectores de huellas dactilares sirven para el inicio de sesión pre-Windows. Aparecerá un mensaje de error si intenta asociar un lector incompatible con pre-Windows. Para saber si un dispositivo es compatible, póngase en contacto con el administrador de su sistema o visite support.dell.com, donde encontrará una lista de los lectores de huellas dactilares admitidos.

Al asociar las huellas dactilares, se le pedirá que introduzca su contraseña de Windows para verificar su identidad. Si así lo establece su política, se le pedirá que introduzca también su contraseña (del sistema) pre-Windows . La contraseña pre-Windows permite acceder al sistema en caso de que hubiera alguna incidencia con el lector de huellas.

NOTAS:

- Se recomienda que asocie al menos dos huellas dactilares durante el proceso de asociación.
- Deberá asociar las huellas dactilares con anterioridad a la activación de la autenticación de las huellas dactilares.
- Si cambia los lectores de huellas dactilares del sistema, deberá volver a asociar las huellas con el nuevo lector. No se recomienda alternar entre dos lectores de huellas dactilares distintos.
- Si, al asociar huellas dactilares, le aparecen mensajes repetidos relacionados con una "pérdida del enfoque del sensor" , puede significar que el ordenador no reconoce el lector de huellas. Si se trata de un lector externo, puede que solucione el problema desconectándolo y volviéndolo a conectar.

Borrar huellas dactilares asociadas
Para quitar las huellas dactilares asociadas, haga clic en el enlace **Quitar huellas dactilares** o haga clic en un dedo asociado (para desmarcarlo) en el asistente de asociación de huellas dactilares.

Para quitar un usuario específico que haya asociado huellas dactilares para la autenticación pre-Windows, el administrador puede desmarcar todas las huellas asociadas para ese usuario.

NOTA: si aparecen errores durante el proceso de asociación de las huellas dactilares, puede visitar wave.com/support/Dell para más detalles.

Asociación de Smart Cards

Dell Data Protection | Access le ofrece la posibilidad de utilizar una smartcard contactless (o con contacto) para iniciar sesión en su cuenta de Windows o para autenticarse antes de Windows. En la ficha Smartcard, haga clic en el enlace **Asociar otra SmartCard** para abrir el asistente de asociación de Smartcard, que le guiará a través del proceso de asociación. "Asociar" significa configurar la smartcard para utilizarla en el inicio de sesión.

Para poder realizar la asociación, debe tener un dispositivo de autenticación de smartcards válidas correctamente instalado o configurado.

NOTA: Para saber si un dispositivo específico es compatible, póngase en contacto con el administrador de su sistema o visite support.dell.com, donde encontrará una lista de las smartcards admitidas.

Asociación
Al asociar una smartcard, se le pedirá que introduzca su contraseña de Windows para verificar su identidad. Si así lo establece su política, se le pedirá que introduzca también su contraseña (del sistema) pre-Windows . La contraseña pre-Windows permite acceder al sistema en caso de que hubiera alguna incidencia con el lector.

Durante la asociación, se le pedirá el PIN de la smartcard, si está establecido. Si su política requiere un PIN y no hay ninguno establecido, se le pedirá que cree uno.

NOTAS:

- Una vez se asocie un usuario para utilizar smartcard antes que Windows, no podrá eliminarse a este usuario.
- Los usuarios estándar pueden cambiar el PIN de usuario de una smartcard, mientras que el administrador puede cambiar tanto el PIN de administrador como el PIN de los usuarios.
- El administrador también puede restaurar una smartcard; después de restaurada, la smartcard no podrá utilizarse para la autenticación en el inicio de sesión de Windows o antes de Windows hasta que vuelva a asociarse.

NOTA:Para la autenticación de certificados TPM, los administradores pueden asociar los certificados TPM mediante el proceso de asociación de smartcards de Microsoft Windows. Los administradores deben seleccionar "Wave TCG-Enabled CSP" como proveedor de servicios criptográficos en lugar de SmartCard CSP para que sea compatible con esta aplicación. Además, el inicio de sesión seguro de Dell debe activarse con la política del tipo de autenticación adecuado para el cliente..

NOTA: Si le aparece un error indicando que el servicio de Smartcard no funciona, puede iniciar o reiniciar este servicio siguiendo estos pasos:

- Navegue hasta la ventana Herramientas administrativas del Panel de control, seleccione Servicio, haga clic derecho en Smartcard y seleccione Iniciar o Reiniciar.
- Si desea información más detallada sobre algún mensaje de error específico, vaya a wave.com/support/Dell.

Self-Encrypting Drive

Dell Data Protection | Access gestiona las funciones de seguridad basadas en hardware de las Self-Encrypting Drives (unidades de autocifrado), que tienen cifrado de datos incrustado en el hardware de la unidad. Esta funcionalidad garantiza que sólo los usuarios autorizados accedan a los datos cifrados (cuando el bloqueo de la unidad está activado).

Para acceder a la ventana de la unidad de autocifrado, se hace clic en la ficha inferior **Self-Encrypting Drive**. Esta ficha muestra solo la unidad o unidades self-encrypting drives (SED) que se encuentran en el sistema.

Haga clic en el enlace **Configurar** para iniciar el asistente de configuración de Self-Encrypting Drive. En este asistente, creará la contraseña del administrador de la unidad, hará una copia de seguridad de esta contraseña y aplicará su configuración de cifrado de la unidad. Sólo los administradores del sistema pueden acceder al asistente de configuración de Self-Encrypting Drive.

Importante: Una vez configurada la unidad, la protección de datos y el bloqueo de la unidad estarán "habilitados". Al bloquearse, la unidad presentará el siguiente comportamiento:

- La unidad entra en modo *bloqueado* cada vez que se apague.
- La unidad no arrancará a menos que el usuario introduzca el nombre de usuario y la contraseña (o su huella dactilar) en la pantalla de inicio de sesión pre-Windows. Antes de que se active el bloqueo de la unidad, los datos de la unidad serán accesibles para cualquier usuario del ordenador.
- La unidad será segura aunque se inserte en otro ordenador como unidad secundaria, ya que para acceder a sus datos se necesitará la autenticación.

Una vez configurada la unidad, la ventana Self-Encrypting Drive mostrará la unidad o unidades y un enlace para que los usuarios cambien su contraseña. Si es usted el administrador de la unidad, también podrá añadir o quitar usuarios de esta ventana. Si hay una unidad externa que se ha configurado, aparecerá en esta ventana y podrá desbloquearla.

NOTA: Para bloquear una unidad secundaria o externa, la unidad debe apagarse independientemente desde el ordenador.

El administrador de la unidad puede gestionar sus ajustes en **Dispositivos > avanzados**. Para más información, consulte Gestión del dispositivo: Self-Encrypting Drives.

Configuración de la unidad

El asistente de configuración de Self-Encrypting Drive le guiará a través del proceso de configuración de la unidad. Para este proceso, es importante que tenga en mente los siguientes conceptos:

Administrador de la unidad
El primer usuario con derechos de administrador del sistema que configura el acceso a la unidad (y que establece la contraseña del administrador) se convierte en el administrador de la unidad. Es el único usuario que puede hacer cambios en el acceso de ésta. Para confirmar que desea realmente establecer el primer usuario como administrador de la unidad, debe seleccionar la casilla "Entiendo" para continuar con este paso.

Contraseña del administrador de la unidad
Este asistente le mostrará una pantalla para que cree la contraseña del administrador de la unidad y para que vuelva a escribirla para confirmarla. Antes de crear la contraseña del administrador de la unidad, debe introducir su contraseña de Windows para identificarse. El

actual usuario de Windows debe tener derechos de administrador para poder crear esta contraseña.

Hacer una copia de seguridad de las credenciales de la unidad
Escriba una ubicación (o haga clic en el botón **Examinar** para seleccionar una) y guarde una copia de seguridad de sus credenciales de administrador de la unidad.

IMPORTANTE

- Le recomendamos hacer una copia de seguridad de estas credenciales y guardarla en una unidad que no sea el disco duro principal (por ejemplo, en un soporte extraíble). De lo contrario, si pierde el acceso al disco, no podrá acceder a la copia de seguridad.
- Una vez completada la configuración de la unidad, todos losusuarios tendrán que introducir el nombre de usuario y la contraseña (o huella dactilar) correctos antes de que Windows se cargue, para poder acceder al sistema la próxima vez que se encienda.

Agregar un usuario de la unidad
El administrador de la unidad puede agregar otros usuarios a la unidad que sean usuarios válidos de Windows. Al agregar usuarios a la unidad, el administrador puede obligar al usuario a restablecer la contraseña la primera vez que inicie sesión. El usuario deberá restablecer su contraseña en la pantalla de autenticación pre-Windows para poder desbloquear la unidad.

Configuración avanzada

- *Single Sign On*: Por defecto, la contraseña de Self-Encrypting Drive, que introduce antes de Windows para autenticar la unidad, se utilizará también para que inicie sesión en Windows (recibe el nombre de "Single Sign On"). Para desactivar esta función, seleccione la casilla "Quiero iniciar sesión de nuevo cuando se inicie Windows" al configurar la unidad.
- *Inicio de sesión con huella dactilar*: en las plataformas admitidas, puede especificar si desea autenticarse en su self-encrypting drive con una huella dactilar en lugar de con una contraseña.
- *Compatibilidad con reposo/suspensión (S3)* (si es compatible con la plataforma): si activa esta opción, la self-encrypting drive podrá entrar en modo de reposo o de suspensión (también llamado modo S3) de forma segura. Para salir de este modo, será necesaria la autenticación pre-Windows.

NOTAS:

- Cuando la compatibilidad con S3 está activada, las contraseñas de cifrado de la unidad estarán supeditadas a cualquier límite de contraseñas BIOS que exista. Consulte al fabricante del hardware del sistema para obtener más información sobre cualquier límite específico de las contraseñas BIOS que pudiera tener ese sistema.
- No todas las self-encrypting drives son compatibles con el modo S3. Durante la configuración de la unidad, se le informará sobre si la unidad es compatible o no con el modo de reposo o suspensión. Para unidades que no admiten este modo, las solicitudes de S3 a Windows se convertirán en solicitudes de hibernación, siempre que este modo este activado (le recomendamos que active el modo de hibernación en su ordenador).
- La primera vez que inicie sesión después de configurar la opción Single Sign On (SSO) , el proceso se detendrá en el mensaje de inicio de sesión de Windows. Se le pedirá que introduzca su tipo de autenticación de Windows, que estará guardada a buen recaudo por si se produjeran futuros intentos de iniciar sesión en Windows. La próxima vez que arranque el sistema, SSO le conectará directamente con Windows. También se requiere el mismo proceso cada vez que cambien los datos de autenticación en Windows de un usuario (contraseña, huella dactilar, PIN de Smartcard). Si el ordenador se encuentra en un dominio y ese dominio tiene una política que obliga a pulsar ctrl+alt+supr para iniciar sesión en Windows, se respetará esta política.

PRECAUCIÓN: Si desinstala la aplicación **Dell Data Protection | Access**, deberá primero desactivar la protección de datos de self-encrypting drive y desbloquear la unidad.

Funciones de usuario de SED

Los administradores de Self-encrypting drive se encargan de gestionar todo lo relacionado con la seguridad y los usuarios de las unidades. Los usuarios de la unidad que no sean administradores sólo pueden realizar las siguientes tareas:

- Cambiar su contraseña de la unidad
- Desbloquear una unidad

Es posible acceder a estas tareas desde la ficha **Self-Encrypting Drive** en **Dell Data Protection | Access**.

Cambiar contraseña
Permite a los usuarios asociados crear una nueva contraseña de autenticación de la unidad. Debe introducir su contraseña actual de Self-Encrypting Drive para poder cambiar la contraseña de la unidad.

NOTAS:

- La aplicación hace respetar las políticas de longitud y complejidad de contraseña de Windows si están activadas. Si las políticas de contraseña de Windows no están activadas, la longitud máxima de una contraseña de Self-Encrypting Drive es de 32 caracteres. Recuerde que esta longitud máxima es de 127 caracteres si S3 (Reposo/Suspensión) no está activado.
- La contraseña de Self-Encrypting Drive de un usuario es distinta de su contraseña de Windows. Cuando se cambia o restablece la contraseña de Windows de un usuario, no se ve afectada la contraseña de la unidad de ese usuario, a menos que se haya activado la sincronización con contraseña de Windows. Consulte Dispositivos: Self-Encrypting Drives para más detalles.
- En algunos teclados no ingleses, hay un conjunto de caracteres restringidos que no se pueden usar en la contraseña de la self-encrypting drive. Si la contraseña de Windows contiene alguno de los caracteres restringidos que se muestran a continuación, y la sincronización con la contraseña de Windows está activada, la sincronización no se llevará a cabo y aparecerá un mensaje de error.

Desbloqueo de la unidad
Desbloqueo de la unidad permite a los usuarios de la unidad asociados desbloquear la unidad bloqueada. Si el bloqueo de la unidad está activado, la unidad cambia al estado de bloqueo siempre que se desconecte la alimentación del ordenador. Cuando se vuelva a encender el sistema, deberá autenticarse en la unidad introduciendo su contraseña en la ventana de autenticación pre-Windows.

NOTAS:

- Es posible que no se pueda pasar al modo de ahorro de energía (por ejemplo, Reposo/Suspensión o Hibernación) si en el ordenador hay activas simultáneamente varias cuentas de usuario de self-encrypting drive.
- En la pantalla de autenticación pre-Windows, "User 1", "User 2", etc. se sustituyen por los nombres de usuario de unidad en las versiones de la aplicación que están localizadas a los siguientes idiomas: chino, japonés, coreano y ruso.

Opciones avanzadas

Las opciones avanzadas de **Dell Data Protection | Access** permiten al usuario con privilegios de administrador gestionar los siguientes aspectos de la aplicación:

Mantenimiento
Contraseñas
Dispositivos

NOTA: sólo los usuarios con privilegios de administrador pueden hacer modificaciones en las opciones avanzadas; los usuarios estándar pueden ver las opciones, pero no cambiarlas.

Mantenimiento

Los administradores utilizan la ventana Mantenimiento para configurar las preferencias de inicio de sesión de Windows, restaurar el sistema para reabastecerlo o archivar y restaurar las credenciales de los usuarios, guardadas en el hardware de seguridad del sistema. Para más información, consulte los siguientes temas:

Preferencias de acceso
Restaurar sistema
Archivar y restaurar & credenciales

Preferencias de acceso

La ventana Preferencias de acceso permite a los administradores especificar las preferencias de inicio de sesión de Windows de todos los usuarios del sistema.

Activar inicio de sesión seguro de Dell
La opción de sustituir la pantalla ctrl-alt-suprimir estándar de Windows le permite utilizar factores distintos de autenticación en lugar de la contraseña de Windows (o además de ella) para acceder a este sistema operativo. Puede elegir añadir una huella dactilar como segundo factor de autenticación para reforzar la seguridad del proceso de inicio de sesión de Windows. También pueden añadirse factores de autenticación adicionales para iniciar sesión en Windows, incluyendo una smartcard o un certificado de TPM.

NOTAS:

- la activación del inicio de sesión seguro de Dell afecta a todos los usuarios del sistema.
- Se recomienda activar esta opción DESPUÉS de que los usuarios hayan asociado sus huellas dactilares o su smartcard.
- La primera vez que inicie sesión tras activar esta opción, se le pedirá que se autentique en Windows de conformidad con su política estándar; después necesitará utilizar sus nuevos factores de autenticación en el inicio siguiente.

Desactivar el inicio de sesión seguro de Dell
Esta opción desactiva todas las funciones de **Dell Data Protection | Access** para iniciar sesión en Windows. Si la selecciona, volverá a su política estándar de inicio de sesión de Windows.

NOTAS:

- Si, cuando intenta iniciar sesión, le aparece un error relacionado con el inicio de sesión seguro en Windows, desactive y vuelva a activar la opción de inicio de sesión seguro de Dell.
- Si desea información más detallada sobre algún mensaje de error específico, vaya a wave.com/support/Dell.

Restaurar sistema

La función Restaurar sistema se utiliza para borrar los datos de todos los usuarios del hardware de seguridad de la plataforma. Se utiliza, por ejemplo, para reabastecer un ordenador. Esta opción eliminará todas las contraseñas del sistema, excepto las contraseñas de usuario de Windows, así como los datos de los dispositivos de hardware (es decir, ControlVault, TPM y los lectores de huellas dactilares). Para las self-encrypting drives, esta función desactiva también la protección de datos, de manera que éstos sean accesibles.

Debe confirmar que sabe que está a punto de restaurar el sistema; después pulse en **Siguiente**. Para restaurar el sistema, necesitará introducir la contraseña de cada dispositivo de seguridad, si la ha establecido:

- Propietario de TPM
- Administrador de ControlVault
- Administrador de la BIOS
- Sistema BIOS (pre-Windows)
- Disco duro (BIOS)
- Administrador de Self-Encrypting Drive

NOTA: En el caso de las self-encrypting drives, solo se necesita la contraseña del administrador de la unidad, no las contraseñas de los usuarios.

Importante La única forma de recuperar los datos borrados al restaurar el sistema es restaurarlos de un archivo previamente guardado. Si no tiene este archivo, los datos serán irrecuperables. En el caso de la self-encrypting drive, sólo se eliminan los datos de la configuración (no se eliminará la información personal de la unidad).

Archivar y restaurar credenciales

La función Archivar y restaurar credenciales se utiliza para hacer copias de seguridad y restaurar todas las credenciales (información de inicio de sesión y cifrado) guardadas en ControlVault y en Trusted Platform Module (TPM). Las copias de seguridad son importantes para reabastecer a un ordenador y para restaurar los datos en caso de fallo del hardware. En este caso, puede simplemente restaurar todas las credenciales en su nuevo ordenador desde el fichero guardado en el archivo.

Puede elegir si archivar o restaurar las credenciales de un solo usuario o de todos los usuarios del sistema.

Las credenciales del usuario son datos utilizados antes de Windows, como las huellas asociadas y los datos de Smartcard, así como las claves guardadas en TPM. TPM creará las claves según lo soliciten las aplicaciones de seguridad; por ejemplo, al generar un certificado digital se crearán claves en TPM.

NOTA: Para saber si las claves TPM pueden ser archivadas por **Dell Data Protection | Access**, consulte la documentación de la aplicación de seguridad. En general, las aplicaciones que utilizan “Wave TCG-Enabled CSP” para generar claves son compatibles.

Archivar credenciales
Para archivar credenciales debe hacer lo siguiente:

- Especifique si está archivando credenciales para usted o para todos los usuarios del sistema.
- Autentíquese en el hardware de seguridad introduciendo la contraseña del sistema (pre-Windows) , la contraseña de administrador de ControlVault y la contraseña de propietario de TPM .
- Cree una contraseña para la copia de seguridad de credenciales.
- Especifique la ubicación del archivo con el botón **Examinar**. La ubicación del archivo debería ser un soporte extraíble, como un lápiz USB o una unidad de red, para protegerlo contra los fallos del disco duro.

Notas importantes:
- Tome note de la ubicación del archivo, ya que el usuario necesitará esta información para restaurar los datos de las credenciales.
- Tome note de la contraseña de la copia de seguridad de las credenciales para asegurarse de poder restaurar los datos. Es importante, ya que la contraseña no puede recuperarse.
- Si no conoce la contraseña del propietario TPM, póngase en contacto con el administrador del sistema o consulte las instrucciones de configuración del TPM del ordenador.

Restaurar credenciales
Para restaurar credenciales, debe hacer lo siguiente:

- Especifique si está restaurando credenciales para usted o para todos los usuarios del sistema.
- Navegue hasta la ubicación del archivo y seleccione el fichero de su interior.
- Introduzca la contraseña de la copia de seguridad de las credenciales que se creó al configurar el archivo.
- Autentíquese en el hardware de seguridad introduciendo la contraseña del sistema (pre-Windows), la contraseña de administrador de ControlVault y la contraseña de propietario de TPM .

NOTAS:

- Si le aparece un error indicando que no se ha podido realizar la restauración de las credenciales y lo ha intentado ya varias veces, intente restaurar un fichero distinto del archivo. Si no funciona, cree otro archivo de credenciales e intente restaurar desde este nuevo archivo.
- Si le aparece un error indicando que no se pudieron restaurar las claves de TPM , cree un archivo de credenciales y después borre TPM de la BIOS. Para borrar TPM, vuelva a arrancar el ordenador, pulse la tecla **F2** al iniciarse para volver a acceder a la configuración de la BIOS y navegue hasta Seguridad>TPM Seguridad. Después, reestablezca la propiedad del TPM e intente de nuevo restaurar las credenciales.
- Si desea información más detallada sobre algún mensaje de error específico, vaya a wave.com/support/Dell.

Administración de contraseñas

Desde la ventana Administración de contraseñas, un administrador puede crear o cambiar todas las contraseñas de seguridad del sistema:

- Sistema (también llamada Pre-Windows)*
- Administrador*
- Disco duro*
- ControlVault
- Propietario de TPM
- Maestra TPM
- Cripta de contraseñas TPM
- Self-Encrypting Drive

NOTAS:

- Sólo se mostrarán las contraseñas que sean aplicables a la configuración actual de la plataforma; por tanto, esta ventana cambiará en función de la configuración y el estado del sistema.
- Las contraseñas que en la lista anterior aparecen junto a un * son contraseñas BIOS y también pueden cambiarse a través de la BIOS del sistema.
- Las contraseñas de nivel de BIOS no pueden crearse ni cambiarse si el administrador de la BIOS ha denegado los cambios de contraseñas.
- Al hacer clic en el enlace **configurar** de una self-encrypting drive, se abre el asistente de configuración de Self-Encrypting Drive. Si hace clic en **administrar**, el usuario podrá cambiar una o más contraseñas de Self-Encrypting Drive.
- Al hacer clic en el enlace **administrar** de la cripta de contraseñas de TPM, se abrirá una ventana donde podrá ver o cambiar las contraseñas que protegen sus claves de TPM. Cuando se crea una clave de TPM que requiere una contraseña, la contraseña se genera al azar y se guarda en la cripta. No podrá administrar la cripta de contraseñas TPM hasta que cree la contraseña maestra de TPM.

Reglas de complejidad de contraseñas de Windows

Dell Data Protection | Access comprueba que la siguiente contraseña cumpla con las normas de complejidad de contraseñas de Windows para la máquina:

- Contraseña del propietario de TPM

Para determinar la política de complejidad de contraseñas de Windows para una máquina, siga estos pasos:

1. Acceda al Panel de control.
2. Haga doble clic en Herramientas Administrativas.
3. Haga doble clic en Directiva de seguridad local.
4. Expanda Directivas de cuenta y seleccione Directiva de contraseñas.

Dispositivos

Los administradores utilizan la ventana Dispositivos para gestionar todos los dispositivos de seguridad instalados en su sistema. Por cada dispositivo, es posible ver el estado e información adicional detallada, como la versión de firmware. Haga clic en **mostrar** para ver la información de cada dispositivo o en **ocultar** para contraer la sección. Los dispositivos que pueden gestionarse son los siguientes, dependiendo de lo que contenga la plataforma:

Trusted Platform Module (TPM)
ControlVault®
Self-Encrypting Drive(s)
Información de dispositivo de autenticación

Trusted Platform Module (TPM)

Es necesario habilitar el chip de seguridad de y establecer la propiedad de TPM para poder utilizar las funciones de seguridad avanzadas disponibles con **Dell Data Protection | Access** y el TPM.

La ventana de Trusted Platform Module en **Gestión de dispositivos** sólo se muestra cuando se detecta un TPM en el sistema.

Gestión de TPM

Estas funciones permiten al administrador del sistema gestionar el TPM.

Estado
Muestra el estado de TPM: *activo* o *inactivo*. "Activo" significa que el TPM ha sido activado en la BIOS y que está listo para ser configurado (puede establecerse su propiedad, por ejemplo). Si el TPM no está activo (habilitado), no será posible administrarlo ni acceder a sus funciones de seguridad .

Si se detecta TPM en el sistema pero no está activo (habilitado), puede activarlo haciendo clic en el enlace **activar** de esta ventana, sin entrar en la BIOS del sistema. Después de activar el TPM con esta función, será necesario volver a arrancar el ordenador. Durante el arranque, aparecerá un mensaje en algunos casos preguntándole si acepta los cambios.

NOTA: es posible que no todas las plataformas admitan la activación (habilitación) de TPM desde esta aplicación. Si no se admite, deberá activarlo en la BIOS del sistema. Para ello, reinicie el sistema, pulse la tecla **F2** antes de que se cargue Windows para entrar en la configuración de la BIOS , navegue hasta Seguridad>TPM Seguridad y active TPM.

También puede *desactivar* TPM desde aquí haciendo clic en el enlace **desactivar**; al desactivar TPM dejará de estar disponible para las funciones de seguridad avanzadas. Sin embargo, la desactivación no cambiará ninguno de los ajustes de TPM ni eliminará o modificará los datos o las claves guardadas en él.

Con propietario
Muestra el estado de propiedad (es decir, "con propietario") y le permite especificar el propietario de TPM . Es necesario establecer la propiedad de TPM para que sus funciones de seguridad estén disponibles. Para poder establecer la propiedad, es necesario activar (habilitar) TPM.

El proceso de establecer la propiedad consiste en la creación por parte del usuario (con privilegios de administrador) de una contraseña de propietario de TPM. Una vez que se ha definido la contraseña, se establece la propiedad y el TPM está preparado para utilizarse.

NOTA: la contraseña del propietario de TPM debe cumplir con las normas de complejidad de contraseñas de Windows de su sistema.

Importante: procure no perder ni olvidar la contraseña de propietario de TPM , ya que es necesaria para poder acceder a las funciones de seguridad avanzadas de TPM en **Dell Data Protection | Access**.

Bloqueado
Muestra el estado de TPM: *bloqueado* o *desbloqueado*. El "Bloqueo" es una función de seguridad de TPM; TPM entrará en estado de bloqueo después de realizarse el número especificado de introducciones incorrectas de contraseña de propietario de TPM . El propietario de TPM puede desbloquearlo desde aquí; deberá introducir la contraseña de propietario de TPM.

NOTAS:

- Si le aparece un error indicando que no se pudo establecer el propietario de TPM , borre el TPM en la BIOS del sistema e intente establecerlo de nuevo. Para borrar TPM, vuelva a arrancar el ordenador, pulse la tecla **F2** al iniciarse para volver a acceder a la configuración de la BIOS y navegue hasta Seguridad>TPM Seguridad.
- Si le aparece un error indicando que no se pudo modificar la contraseña del propietario de TPM, archive los datos de TPM (archivo de credenciales), borre el TPM de la BIOS, reestablezca la propiedad de TPM y restaure los datos de TPM (restaurar credenciales).
- Si desea información más detallada sobre algún mensaje de error específico, vaya a wave.com/support/Dell.

Dell ControlVault®

Dell ControlVault® (CV) es un almacén seguro para guardar las credenciales del usuario utilizadas durante el inicio de sesión pre-Windows (por ejemplo, las contraseñas del usuario o los datos de huella dactilar asociados). La ventana de ControlVault en **Gestión de dispositivos** sólo se muestra cuando se detecta ControlVault en el sistema.

Gestión de ControlVault

Estas funciones permiten al administrador del sistema gestionar ControlVault..

Estado
Muestra el estado de ControlVault: *activo* o *inactivo*. "Inactivo" significa que ControlVault no está disponible en su sistema para almacenar. Consulte la documentación del sistema Dell para saber si contiene un ControlVault.

Contraseña
Indica si se ha establecido la contraseña de administrador de ControlVault y le permite establecer o cambiar la contraseña (esto último, en caso de que haya una establecida). Sólo los administradores del sistema pueden configurar o cambiar esta contraseña. Es necesario establecer una contraseña de administrador de ControlVault para poder hacer lo siguiente:

- Realizar el archivado y la restauración de credenciales.
- Borrar los datos de usuario (de todos).

NOTA: Si intenta archivar o restaurar cuando no hay ninguna contraseña de administrador de ControlVault establecida, se le pedirá que cree una (si es administrador).

Usuarios asociados
Indica si algún usuario tiene credenciales de inicio de sesión asociadas (por ejemplo, contraseñas, huellas dactilares o datos de smartcard) y guardadas actualmente en el ControlVault.

Borrar datos de usuario
Es posible que necesite borrar los datos de ControlVault en algún momento; por ejemplo, si los usuarios tienen problemas para utilizar o asociar las credenciales anteriores a Windows para la autenticación. Desde esta ventana pueden borrarse todos los datos guardados en ControlVault, ya sean de un usuario individual o de todos los usuarios.

Para borrar los datos de todos los usuarios de la plataforma, debe introducirse la contraseña de administrador de ControlVault. También se le pedirá cualquier contraseña del sistema (pre-Windows) si se han asociado credenciales anteriores a Windows. Al borrar los datos de todos los usuarios, la contraseña de administrador de ControlVault y la contraseña del sistema se restablecen. Recuerde también que esta es la única forma de borrar la contraseña de administrador de ControlVault.

NOTA: Después de borrar los datos de todos los usuarios, se le pedirá que reinicie el ordenador. Es importante que lo reinicie para que el sistema funcione correctamente.

Para borrar las credenciales de un solo usuario, no es necesario establecer la contraseña de administrador de ControlVault. Al hacer clic en **borrar datos de usuario**, se le pedirá que seleccione el usuario cuyas credenciales de ControlVault desea borrar. Una vez seleccionado el usuario, se le pedirá la contraseña del sistema (solo si hay credenciales anteriores a Windows asociadas).

NOTAS:

- Si le aparece un error indicando que no se pudo crear la contraseña de administrador de ControlVault, debería archivar sus credenciales, borrar los datos de todos los usuarios de ControlVault, reiniciar el ordenador y volver a intentar crear la contraseña.
- Si le aparece un error indicando que no se pudieron eliminar las credenciales de ControlVault de un solo usuario, debería archivar sus credenciales, intentar borrar los datos de todos los usuarios y reintentar después borrar los datos de ese usuario.
- Si le aparece un error indicando que no se pudieron borrar las credenciales de ControlVault de todos los usuarios, tal vez debería hacer una restauración del sistema. **Importante** Antes de proceder con la restauración, repase el tema de ayuda sobre la restauración del sistema, ya que al hacerlo se borrarán TODOS los datos de seguridad de los usuarios.
- Si le aparece un error indicando que no se pudo hacer una copia de seguridad de los datos de ControlVault y TPM , desactive TPM de la BIOS del sistema. Para ello, debe volver a arrancar el ordenador, pulsar la tecla **F2** al iniciarse para volver a acceder a la configuración de la BIOS y navegar hasta Seguridad>TPM Seguridad. Después, vuelva a activar TPM e intente de nuevo archivar sus datos de ControlVault.
- Si desea información más detallada sobre algún mensaje de error específico, vaya a wave.com/support/Dell.

Self-Encrypting Drives: Avanzadas

Dell Data Protection | Access gestiona las funciones de seguridad basadas en hardware de las Self-Encrypting Drives (unidades de autocifrado), que tienen cifrado de datos incrustado en el hardware de la unidad. Esta función garantiza que sólo los usuarios autorizados accedan a los datos cifrados (cuando el bloqueo de la unidad está activado).

La ventana Self-Encrypting Drive de **Gestión del dispositivo** muestra solo la unidad o unidades self-encrypting drives (SED) que se encuentran en el sistema.

Importante: Una vez configurada la unidad, la protección de datos y el bloqueo de la unidad de la self-encrypting drive estarán "habilitados".

Gestión de la unidad

Estas funciones permiten al administrador de la unidad gestionar la configuración de seguridad de la unidad. Los cambios en la configuración de seguridad de la unidad surten efecto después de que se ha desactivado la unidad.

Protección de datos

Aparece el estado de la protección de datos de la self-encrypting drive: *activado* o *desactivado*. "Activado" significa que se ha habilitado la seguridad de la unidad; sin embargo, hasta que se active el *bloqueo* de la unidad, los usuarios no tendrán que autenticarse en la unidad antes de Windows para acceder a ella.

Puede desactivar la protección de los datos de la self-encrypting drive desde aquí. Al desactivarla, todas las funciones de seguridad avanzadas de la self-encrypting drive se deshabilitarán y la unidad actuará de manera estándar. Al deshabilitar la protección de los datos también se elimina la configuración completa de seguridad, incluyendo las credenciales de los administradores y usuarios de la unidad. Sin embargo, esta función no altera ni elimina los datos del usuario que haya en la unidad.

Bloqueo

Aparece el estado de las self-encrypting drives: *activado* o *desactivado*. Consulte el apartado sobre Self-Encrypting Drive para más información sobre el comportamiento de las unidades bloqueadas.

Es posible que deba desactivar temporalmente el bloqueo de las unidades, y podrá hacerlo desde aquí. No se lo recomendamos, ya que cuando está desactivado el bloqueo, no se necesitan credenciales para acceder a la unidad, de manera que cualquier usuario de la plataforma podrá acceder a sus datos. Al desactivar el bloqueo de la unidad no seelimina ningún ajuste de seguridad, ni las credenciales del administrador o los usuarios de la unidad ni ningún dato de usuario sobre ella.

PRECAUCIÓN: Si desinstala la aplicación **Dell Data Protection | Access**, deberá primero desactivar la protección de datos de self-encrypting drive y desbloquear la unidad.

Administrador de unidad

Muestra el administrador actual de la unidad. Este administrador puede cambiar desde aquí el usuario que debe ser administrador de la unidad. El nuevo administrador debe ser un usuario de Windows válido en el sistema, con derechos de administrador. Sólo puede haber un administrador de unidad en el sistema.

Usuarios de la unidad

Muestra los usuarios de unidad asociados y el número de usuarios actualmente asociados. El número máximo de usuarios admitidos depende de la self-encrypting drive (en la actualidad, cuatro usuarios para unidades Seagate y 24 para unidades Samsung).

Sincronización con contraseña de Windows

La función "Sincronización con contraseña de Windows" (WPS) establece automáticamente las contraseñas de usuarios de Self-Encrypting Drive para que coincidan con las de Windows. Esta función no se aplica al administrador, sólo es aplicable a los usuarios de la unidad. La función WPS puede utilizarse en empresas que deben cambiar las contraseñas en intervalos de tiempo específicos (por ejemplo, cada 90 días); con esta opción activada, todas las contraseñas de los usuarios de la self-encrypting drive se actualizarán automáticamente cada vez que se modifiquen sus contraseñas de Windows.

NOTA: Si la sincronización con la contraseña de Windows (WPS) está activada, la contraseña de un usuario de Self-Encrypting Drive no podrá modificarse; será necesario cambiar la contraseña de Windows para que se actualice automáticamente la contraseña de la unidad.

Recordar último nombre de usuario

Cuando esta opción está activada, el último nombre de usuario introducido aparecerá por defecto en el campo **Nombre de usuario** de la pantalla de autenticación pre-Windows.

Selección del nombre de usuario

Cuando esta opción está activada, los usuarios pueden ver todos los nombres de usuario de la unidad en el campo **Nombre de usuario** de la pantalla de autenticación pre-Windows.

Borrado criptográfico

Esta opción puede utilizarse para "borrar" todos los datos de la self-encrypting drive. Realmente no se borran los datos, sino las claves utilizadas para cifrarlos, lo que hace que los datos sean inutilizables. Después del borrado criptográfico, no es posible recuperar los datos de la unidad; también quedará desactivada la protección de los datos de la unidad y ésta estará lista para utilizarla de nuevo.

NOTAS:

- Si aparece algún error relacionado con las funciones de gestión de la self-encrypting drive, apague completamente el ordenador (no haga un rearranque) y reinícielo de nuevo.
- Si desea información más detallada sobre un mensaje de error específico, vaya a wave.com/support/Dell.

Información de dispositivo de autenticación

La ventana Información del dispositivo de autenticación en **Gestión de dispositivos** muestra la información y el estado de todos los dispositivos de autenticación conectados (por ejemplo, el lector de huellas dactilares o el lector de smartcard tradicional o contactless) al sistema.

Asistencia técnica

Encontrará asistencia técnica del software **Dell Data Protection | Access** en http://www.wave.com/support.dell.com.

Wave TCG-Enabled CSP

El proveedor de servicios criptográficos (CSP) Wave Systems Trusted Computing Group (TCG)-enabled se incluye con la aplicación **Dell Data Protection | Access** y está disponible para ser utilizado cuando se requiera un CSP, ya sea invocado directamente desde una aplicaicón o seleccionable desde una lista de CSP instalados. Cuando sea posible, seleccione “Wave TCG-Enabled CSP” para asegurarse de que TPM genere las claves y que éstas y sus contraseñan sean gestionadas por **Dell Data Protection | Access**.

El CSP de Wave Systems TCG-enabled permite a las aplicaciones utilizar funciones disponibles en plataformas compatibles con TCG directamente a través de MSCAPI. Es un módulo CSP MSCAPI de TCG mejorado que proporciona funcionalidad asimétrica de claves en TPM y aumenta la seguridad mejorada de TPM, independientemente de los requisitos específicos del proveedor en lo que se refiere al proveedor de Trusted Software Stack (TSS).

NOTA: Si las claves de TPM generadas por el CSP de Wave TCG-enabled requieren una contraseña y el usuario ha creado una contraseña maestra de TPM, las contraseñas de claves individuales se generarán al azar y se guardarán en la cripta de contraseñas de TPM.