Dell Data Protection

Guía de recuperación v8.13/v1.7/v1.4/v1.2

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 de recuperación de Dell Data Protection

2017 - 04

Rev. A01

Tabla de contenido

1

Introducción a la recuperación

En esta sección se describe lo necesario para crear un entorno de recuperación.

- Una copia descargada del software del entorno de recuperación ubicada en la carpeta Kit de recuperación de Windows en los medios de instalación de Dell Data Protection.
- Medios CD-R, DVD-R o medios USB formateados
  - Si va a grabar un CD o DVD, consulte Grabar la ISO del entorno de recuperación en CD/DVD para obtener más información.
  - Si va a utilizar un medio USB, consulte Grabar el entorno de recuperación en un medio extraíble para obtener más información.
- Paquete de recuperación para dispositivos en error
  - Para clientes administrados remotamente, las instrucciones siguientes explican cómo recuperar un paquete de recuperación desde su Dell Data Protection Server.
  - Para clientes administrados localmente, el paquete de recuperación se creó durante la configuración en una unidad de red compartida o en un medio externo. Localice este paquete antes de continuar.

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

Recuperación de cifrado basado en la política o de archivo/carpeta

Con la recuperación de cifrado basado en la política o cifrado de archivo/carpeta (FFE), puede recuperar el acceso a lo siguiente:

- A un equipo que no se inicia y que muestra una petición para realizar recuperación de SDE.
- A un equipo en el que no se pueden editar políticas ni acceder a los datos cifrados.
- A un servidor que ejecuta Dell Data Protection | Server Encryption que cumple con las condiciones anteriores.
- A un equipo en el que se debe sustituir la tarjeta de Hardware Crypto Accelerator o la placa base/TPM.

Descripción general del proceso de recuperación

Para recuperar un sistema defectuoso:

1 Grabe el entorno de recuperación en un CD/DVD o cree una unidad USB de arranque. Consulte Apéndice A - Grabar el entorno de recuperación.
2 Obtenga el archivo de recuperación.
3 Realice la recuperación.

Realizar el cifrado basado en la política o la recuperación de FFE

Siga estos pasos para realizar el cifrado basado en la política o la recuperación de FFE.

Obtener el archivo de recuperación - Equipo administrado de forma remota

Para descargar el archivo **<machinename_domain.com>.exe**:

1 Abra la Remote Management Console y, desde el panel izquierdo, seleccione **Administración** > **Recuperar extremo**.
2 En el campo Nombre de host, introduzca el nombre de dominio completo del extremo y haga clic en **Buscar**.
3 En la ventana Recuperación mejorada, introduzca una Contraseña de recuperación y haga clic en **Descargar**.

> **NOTA:**
> Debe recordar esta contraseña para acceder a las claves de recuperación.

4 Copie el archivo **<machinename_domain.com** > **.exe** en una ubicación a la que se pueda acceder al iniciar en WinPE.

Obtener el archivo de recuperación - Equipo administrado localmente

Para obtener el archivo de recuperación de Personal Edition:

1 Localice el archivo de recuperación denominado **LSARecovery_<systemname>** > **.exe**. Este archivo fue almacenado en una unidad de red o unidad de almacenamiento extraíble al hacerse la instalación de Personal Edition por medio del asistente de configuración.

2 Copie **LSARecovery_<systemname>** > **.exe** en el equipo de destino (el equipo que tiene los datos que desea recuperar).

Realizar una recuperación

1 Con los medios de arranque creados anteriormente, realice el inicio con dichos medios en un sistema de recuperación o en el dispositivo con la unidad que está intentando recuperar. Se abre un entorno WinPE.

2 Introduzca **x** y pulse **Intro** para acceder al símbolo del sistema.

3 Vaya al archivo de recuperación e inícielo.

4 Seleccione una opción:

- Mi sistema no se inicia y muestra un mensaje que me pide que ejecute la recuperación SDE.

  Esto le permitirá volver a crear las comprobaciones de hardware que realiza el cliente Encryption cuando lo inicia en el SO.

- Mi sistema no me permite el acceso a la información cifrada, ni modificar las políticas, o se está reinstalando.

  Utilícelo si se debe sustituir la tarjeta de Hardware Crypto Accelerator o la placa base/TPM.

5 En el cuadro de diálogo Backup and Recovery Information (Información de recuperación y copia de seguridad), confirme que es correcta la información acerca del equipo cliente que se debe recuperar y haga clic en **Next** (Siguiente).

Al recuperar equipos que no sean de Dell, los campos Número de serie y Etiqueta de activos se dejarán en blanco.

6 En el cuadro de diálogo que muestra los volúmenes del equipo, seleccione todas las unidades correspondientes y haga clic en **Next** (Siguiente).

Haga clic en Mayús o Ctrl para resaltar varias unidades.

Si la unidad seleccionada no tiene cifrado basado en la política o FFE, no se realizará la recuperación.

7 Introduzca su contraseña de recuperación y haga clic en **Next** (Siguiente).

Con un cliente administrado de forma remota, esta es la contraseña proporcionada en el paso 3 en Obtener el archivo de recuperación - Equipo administrado de forma remota.

En Personal Edition, la contraseña es la Contraseña del administrador de cifrado que estableció el sistema al custodiar las claves.

8 En el cuadro de diálogo Recuperar, haga clic en **Recover** (Recuperar). Se inicia el proceso de recuperación.

9 Una vez completada la recuperación, haga clic en **Finish** (Finalizar).

> **NOTA:**
> Asegúrese de extraer cualquier medio USB o CD\DVD que utilizó para iniciar la máquina. Si no hace esto, es posible que se vuelva a iniciar al entorno de recuperación.

10 Después de reiniciar el equipo, debe tener un equipo en pleno funcionamiento. Si los problemas continúan, póngase en contacto con Dell ProSupport.

Recuperación de datos con unidad de cifrado

Si el equipo de destino no puede iniciarse y no hay ningún error de hardware, la recuperación de datos se puede realizar en un equipo iniciado en un entorno de recuperación. Si el equipo de destino no puede iniciarse y ha fallado el hardware o es un dispositivo USB, la recuperación de datos se puede realizar iniciando en una unidad secundaria. Cuando utiliza una unidad, verá el sistema de archivos y podrá navegar por los directorios. Sin embargo, si intenta abrir o copiar un archivo, se producirá un error *Access denied* (Acceso denegado).

Recuperar datos con unidad de cifrado

Para recuperar datos con unidad de cifrado:

1 Para obtener la Id. de recuperación/DCID del equipo, seleccione una opción:
   a Ejecute WSScan en cualquier carpeta donde se almacenan los datos cifrados comunes.
   Se muestra el ID de recuperación/DCID de ocho caracteres después de "Common" (Común).

   b Abra la Remote Management Console y selecciona la pestaña **Details & Actions** (Detalles y acciones) del extremo.
   c En la sección Detalle de Shield de la pantalla Detalles de extremo, localice la Id. de recuperación/DCID.

2 Para descargar la clave desde el servidor, vaya a la utilidad Dell Administrative Unlock (**CMGAu**).
   La utilidad Dell Administrative Unlock se puede obtener desde Dell ProSupport.

3 En el cuadro de diálogo Dell Administrative Utility (CMGAu), introduzca la siguiente información (algunos campos se rellenan previamente) y haga clic en **Next** (Siguiente).
   Server (Servidor): nombre del host completo del servidor, por ejemplo:

   Servidor de dispositivos: **https://<server.organization.com>:8081/xapi**

   Servidor de seguridad: **https://<server.organization.com>:8443/xapi/**

   Dell Admin (Administrador de Dell): el nombre de la cuenta del administrador forense (habilitado en el servidor)

   Dell Admin Password (Contraseña del administrador de Dell): la contraseña de la cuenta del administrador forense (habilitado en el servidor)

   MCID: borre el campo MCID

   DCID: el ID de recuperación/DCID que ha obtenido antes.

4 En el cuadro de diálogo Dell Administrative Utility, seleccione **No, perform a download from a server now** (No, realizar una descarga desde un servidor ahora) y haga clic en **Next** (Siguiente).

   NOTA:
   Si no tiene instalado el cliente Encryption, se muestra el mensaje *Unlock failed* (Error de desbloqueo). Muévalo a un equipo que tenga instalado cliente Encryption.

5 Cuando la descarga y el desbloqueo se hayan completado, copie los archivos que necesite recuperar de esta unidad. Se pueden leer todos los archivos. ***No haga clic en Finish (Finalizar) hasta que haya recuperado los archivos***.

6 Cuando haya recuperado los archivos y ya pueda volver a bloquearlos, haga clic en **Finish** (Finalizar).
   Después de hacer clic en Finish (Finalizar), los archivos cifrados ya no estarán disponibles.

Recuperación de Hardware Crypto Accelerator

Con la recuperación de Hardware Crypto Accelerator (HCA) de Dell Data Protection, puede recuperar el acceso a lo siguiente:

- Archivos en una unidad cifrada de HCA: este método descifra la unidad mediante las claves proporcionadas. Puede seleccionar la unidad específica que necesita descifrar durante el procesado de recuperación.
- Una unidad cifrada de HCA después de la sustitución del hardware: este método se utiliza después de sustituir la tarjeta de Hardware Crypto Accelerator o la placa base/TPM. Puede ejecutar una recuperación para volver a tener acceso a los datos cifrados sin tener que descifrar la unidad.

Requisitos de recuperación

Para la recuperación de HCA, necesita lo siguiente:

- Acceso a la ISO de entorno de recuperación
- CD\DVD o medios USB de arranque

Descripción general del proceso de recuperación

Para recuperar un sistema defectuoso:

1 Grabe el entorno de recuperación en un CD/DVD o cree una unidad USB de arranque. Consulte Apéndice A - Grabar el entorno de recuperación.
2 Obtenga el archivo de recuperación.
3 Realice la recuperación.

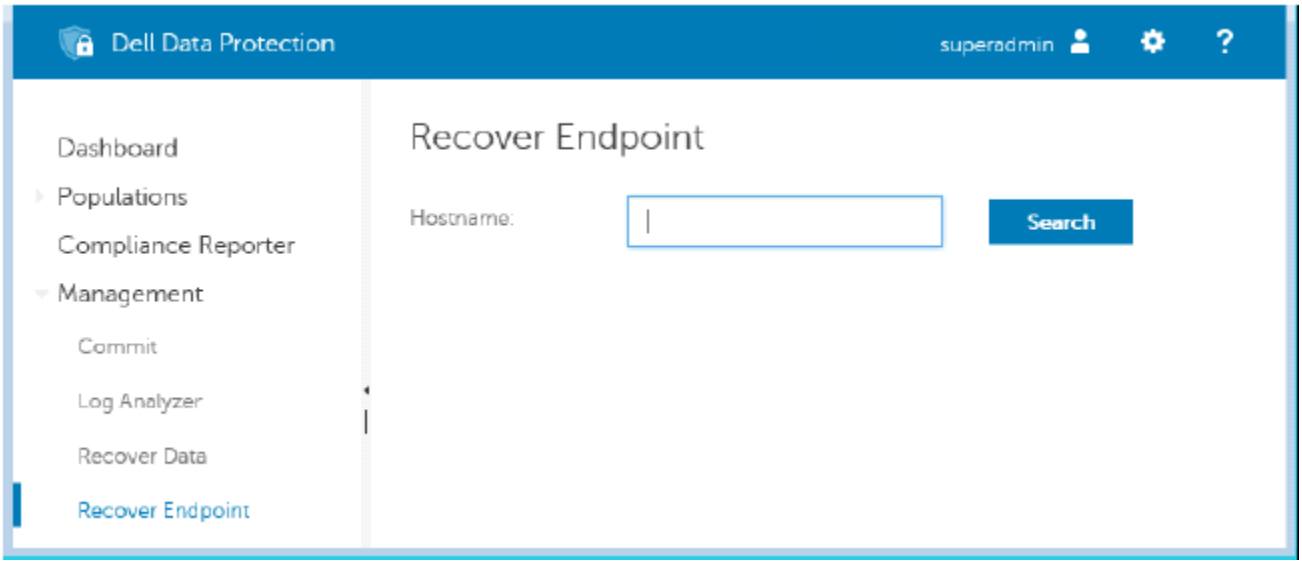
Realizar la recuperación de HCA

Siga estos pasos para realizar la recuperación de HCA.

Obtener el archivo de recuperación - Equipo administrado de forma remota

Para descargar el archivo **<machinename_domain.com>.exe** que se generó al instalar Dell Data Protection:

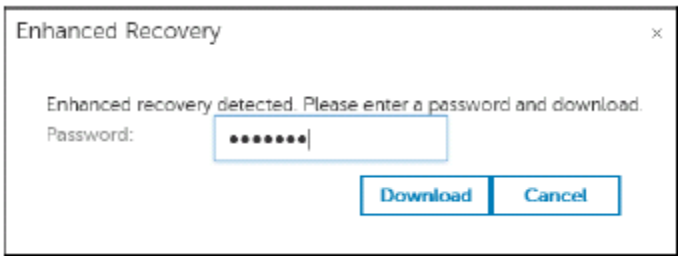
1 Abra la Remote Management Console y, desde el panel izquierdo, seleccione **Administración** > **Recuperar extremo**.



2 En el campo Nombre de host, introduzca el nombre de dominio completo del extremo y haga clic en **Buscar**.

3 En la ventana Recuperación mejorada, introduzca una Contraseña de recuperación y haga clic en **Descargar**.

NOTA:
Debe recordar esta contraseña para acceder a las claves de recuperación.



Obtener el archivo de recuperación - Equipo administrado localmente

Para obtener el archivo de recuperación de Personal Edition:

1 Localice el archivo de recuperación denominado **LSARecovery_<systemname> > .exe**. Este archivo fue almacenado en una unidad de red o unidad de almacenamiento extraíble al hacerse la instalación de Personal Edition por medio del asistente de configuración.

2 Copie **LSARecovery_<systemname> > .exe** en el equipo de destino (el equipo que tiene los datos que desea recuperar).

Realizar una recuperación

1 Con los medios de arranque creados anteriormente, realice el inicio con dichos medios en un sistema de recuperación o en el dispositivo con la unidad que está intentando recuperar.

Se abre un entorno WinPE.

2 Escriba **x** y pulse **Intro** para acceder al símbolo del sistema.

3 Vaya al archivo de recuperación guardado e inícielo.

4 Seleccione una opción:

- Deseo descifrar mi unidad HCA cifrada.

- Deseo restaurar el acceso a mi unidad HCA cifrada.

5 En el cuadro de diálogo Backup and Recovery Information (Información de recuperación y copia de seguridad), confirme que el número de activo o la etiqueta de servicio son correctos y haga clic en **Next** (Siguiente).

6 En el cuadro de diálogo que muestra los volúmenes del equipo, seleccione todas las unidades correspondientes y haga clic en **Next** (Siguiente).

Haga clic en Mayús o Ctrl para resaltar varias unidades.

Si la unidad seleccionada no está cifrada con HCA, no se realizará la recuperación.

7 Introduzca su contraseña de recuperación y haga clic en **Next** (Siguiente).

En un equipo administrado de forma remota, esta es la contraseña proporcionada en el paso 3 in Obtener el archivo de recuperación - Equipo administrado de forma remota.

En un equipo administrado localmente, la contraseña es la Contraseña del administrador de cifrado que estableció el sistema en Personal Edition al custodiar las claves.

8 En el cuadro de diálogo Recuperar, haga clic en **Recover** (Recuperar). Se inicia el proceso de recuperación.

9 Cuando se le solicite, vaya al archivo de recuperación guardado y haga clic en **OK** (Aceptar).

Si está realizando un descifrado completo, el siguiente cuadro de diálogo mostrará el estado. Este proceso puede tardar un poco.

10 Cuando se muestre el mensaje para indicar que la recuperación ha finalizado correctamente, haga clic en **Finish** (Finalizar). Se reinicia el equipo.

Después de reiniciar el equipo, debe tener un equipo en pleno funcionamiento. Si los problemas continúan, póngase en contacto con Dell ProSupport.

Recuperación de la unidad de cifrado automático (SED)

Con la recuperación de SED, puede recuperar el acceso a los archivos en una SED mediante los siguientes métodos:

- Realice un desbloqueo de una sola vez de la unidad para omitir y quitar la Autenticación previa al inicio (PBA).
  - En un cliente SED administrado remotamente, la PBA se puede volver a habilitar más tarde mediante la Remote Management Console.
  - En un cliente SED administrado localmente, la PBA se puede volver a habilitar mediante la Consola del administrador de Security Tools.
- Desbloquéela y, a continuación, quite de forma permanente la PBA de la unidad. El inicio de sesión único no funcionará con la PBA quitada.
  - En un cliente SED administrado remotamente, para quitar la PBA, tendrá que desactivar el producto desde la Remote Management Console si es necesario para volver a habilitar la PBA en un futuro.
  - En un cliente SED administrado localmente, para quitar la PBA, tendrá que desactivar el producto del SO si es necesario para volver a habilitar la PBA en un futuro.

Requisitos de recuperación

Para la recuperación de SED, necesita lo siguiente:

- Acceso a la ISO de entorno de recuperación
- CD\DVD o medios USB de arranque

Descripción general del proceso de recuperación

Para recuperar un sistema defectuoso:

1 Grabe el entorno de recuperación en un CD/DVD o cree una unidad USB de arranque. Consulte Apéndice A - Grabar el entorno de recuperación.
2 Obtenga el archivo de recuperación.
3 Realice la recuperación.

Realizar la recuperación de SED

Siga estos pasos para realizar la recuperación de SED.

Obtener el archivo de recuperación - Cliente SED administrado remotamente

Obtenga el archivo de recuperación.

El archivo de recuperación se puede descargar desde la Remote Management Console. Para descargar el archivo *<hostname>-sed-recovery.dat* que se generó al instalar Dell Data Protection:

a Abra la Remote Management Console y, en el panel izquierdo, seleccione **Management > Recover Data** (Administración > Recuperar datos). A continuación, seleccione la pestaña **SED**.
b En la pantalla Recover Data (Recuperar datos), en el campo Hostname (Nombre de host), introduzca el nombre de dominio completo del extremo y, a continuación, haga clic en **Search** (Buscar).
c En el campo SED, seleccione una opción.
d Haga clic en **Create Recovery File** (Crear archivo de recuperación).

El archivo **<hostname>-sed-recovery.dat** se descarga.

Obtener el archivo de recuperación - Cliente SED administrado localmente

Obtenga el archivo de recuperación.

Se ha generado el archivo y se puede acceder a él desde la ubicación de la copia de seguridad que seleccionó al instalar Dell Data Protection | Security Tools en el equipo. El nombre de archivo es *OpalSPkey<systemname>.dat*.

Realizar una recuperación

1 Con los medios de arranque creados anteriormente, realice el inicio con dichos medios en un sistema de recuperación o en el dispositivo con la unidad que está intentando recuperar. Se abre un entorno de WinPE con la aplicación de recuperación.
2 Elija una opción y pulse **Intro**.
3 Seleccione **Browse** (Examinar), localice el archivo de recuperación y, a continuación, haga clic en **Open** (Abrir).
4 Seleccione una opción y haga clic en **OK** (Aceptar).
   - **One-time unlock of the drive** (Desbloqueo de una sola vez de la unidad): este método ignora y elimina la PBA. Después, se puede volver a habilitar a través de la Remote Management Console (para un cliente SED administrado remotamente) o a través de la Consola del administrador de Security Tools (para un cliente SED administrado localmente).
   - **Unlock drive and remove PBA** (Desbloquear unidad y eliminar la PBA): este método desbloquea y luego elimina permanentemente la PBA de la unidad. Si quiere quitar la PBA tendrá que desactivar el producto desde la Remote Management Console (para un cliente SED administrado remotamente) o en el SO (para un cliente SED administrado localmente) si es necesario para volver a habilitar la PBA en el futuro. El inicio de sesión único no funcionará con la PBA quitada.
5 La recuperación está ahora completada. Presione cualquier tecla para volver al menú.
6 Pulse **r** para reiniciar el equipo.

> **NOTA:**
> Asegúrese de extraer cualquier medio USB o CD\DVD que utilizó para iniciar el equipo. Si no hace esto, es posible que se vuelva a iniciar al entorno de recuperación.

7 Después de reiniciar el equipo, debe tener un equipo en pleno funcionamiento. Si los problemas continúan, póngase en contacto con Dell ProSupport.

Recuperación de la clave de propósito general

Se utiliza la Clave de propósito general (GPK) para cifrar una parte del registro para los usuarios de dominio. Sin embargo, raras veces, durante el proceso de inicio se vuelve inutilizable y no se puede abrir. Si ocurre esto, se muestran los siguientes errores en el archivo CMGShield.log en el equipo cliente:

```
[12.06.13 07:56:09:622 GeneralPurposeK: 268] GPK - Failure while unsealing data [error = 0xd]

[12.06.13 07:56:09:622 GeneralPurposeK: 631] GPK - Unseal failure

[12.06.13 07:56:09:622 GeneralPurposeK: 970] GPK - Failure to get keys for the registry driver
```

Si no se puede abrir la GPK, ésta se debe recuperar. Para ello, extráigala del paquete de recuperación que se ha descargado del servidor.

Recuperar la GPK

Obtener el archivo de recuperación

Para descargar el archivo **<machinename_domain.com>.exe** que se generó al instalar Dell Data Protection:

1 Abra la Remote Management Console y, desde el panel izquierdo, seleccione **Administración** > **Recuperar extremo**.

2 En el campo Nombre de host, introduzca el nombre de dominio completo del extremo y haga clic en **Buscar**.

3 En la ventana Recuperación mejorada, introduzca una Contraseña de recuperación y haga clic en **Download** (Descargar).

> **NOTA:**
> Debe recordar esta contraseña para acceder a las claves de recuperación.

El archivo **<machinename_domain.com>.exe** se descarga.

Realizar una recuperación

1 Cree un medio de inicio del entorno de recuperación. Para obtener instrucciones, consulte Apéndice A - Grabar el entorno de recuperación.

2 Realice el inicio con dichos medios en un sistema de recuperación o en el dispositivo con la unidad que está intentando recuperar.
Se abre un entorno WinPE.

3 Introduzca **x** y pulse **Intro** para acceder al símbolo del sistema.

4 Vaya al archivo de recuperación e inícielo.
Se abre el cuadro de diálogo de diagnóstico del cliente Encryption y se genera el archivo de recuperación en segundo plano.

5 En el símbolo del sistema de administrador, ejecute **<machinename_domain.com** > **.exe** > **-p <password** > **-gpk**
Devuelve el archivo GPKRCVR.txt para su equipo.

6 Copie el archivo **GPKRCVR.txt** en la raíz de la unidad del sistema operativo del equipo.

7 Reinicie el equipo.

El sistema operativo consumirá el archivo GPKRCVR.txt y volverá a generar la GPK en ese equipo.

8 Si se le solicita, reinicie de nuevo.

6

Recuperación de BitLocker Manager

Para recuperar datos, obtenga una contraseña de recuperación o paquete de claves de la Remote Management Console, que le permitan desbloquear los datos en el equipo.

Recuperar datos

1 Inicie sesión como administrador de Dell en la Remote Management Console.

2 En el panel izquierdo, haga clic en **Management** > **Recover Data** (Administración > Recuperar datos).

3 Haga clic en la pestaña **Manager** (Administrador).

4 Para *BitLocker*:

Introduzca el **Recovery ID** (ID de recuperación) recibido de BitLocker. De manera opcional, si introduce el Nombre de host y el Volumen, se completará la Id. de recuperación.

Haga clic en **Get Recovery Password** (Obtener contraseña de recuperación) o **Create Key Package** (Crear paquete de claves).

En función de la manera en que desee realizar la recuperación, utilizará la contraseña de recuperación o el paquete de claves para recuperar datos.

Para el *TPM*:

Introduzca el **Hostname** (Nombre de host).

Haga clic en **Get Recovery Password** (Obtener contraseña de recuperación) o **Create Key Package** (Crear paquete de claves).

En función de la manera en que desee realizar la recuperación, utilizará la contraseña de recuperación o el paquete de claves para recuperar datos.

5 Para completar la recuperación, consulte las Instrucciones de recuperación de Microsoft.

NOTA:

Si BitLocker Manager no es "propietario" de TPM, la contraseña y el paquete de claves de TPM no estarán disponibles en la base de datos de Dell. Recibirá un mensaje de error indicando que Dell no puede encontrar la clave, que es el comportamiento esperado.

Para recuperar un TPM "con propietario" de una entidad distinta de BitLocker Manager, deberá seguir el proceso de recuperación del TPM de ese propietario específico o seguir su propio proceso existente para la recuperación del TPM.

7

Recuperación de contraseña

Normalmente, los usuarios olvidan su contraseña. Afortunadamente, existen varios métodos para que los usuarios puedan volver a acceder a un equipo con autenticación previa al inicio cuando lo hagan.

- La función Recovery Questions (Preguntas de recuperación) ofrece autenticación basada en preguntas y respuestas.
- Los códigos de desafío/respuesta permiten a los usuarios trabajar con su administrador para volver a tener acceso a sus equipos. Esta función solo está disponible para usuarios con equipos administrados por su organización.

Preguntas de recuperación

La primera vez que un usuario inicia sesión en un equipo, se le solicita que responda a un conjunto estándar de preguntas que el administrador ha configurado. Después de inscribir sus respuestas a estas preguntas, la próxima vez que olvide su contraseña, se le solicitarán las respuestas. Suponiendo que responda correctamente a las preguntas, podrá iniciar sesión y volver a acceder a Windows.

Requisitos previos

- Las preguntas de recuperación debe configurarlas el administrador.
- El usuario debe haber inscrito sus respuestas a las preguntas.
- Antes de hacer clic en la opción de menú **Trouble Signing In** (Problema de inicio de sesión), el usuario debe introducir un nombre de usuario y un dominio válidos.

Para acceder a las preguntas de recuperación desde la pantalla de inicio de sesión de PBA:

1 Introduzca un nombre de dominio y un nombre de usuario válidos.
2 En el lado inferior izquierdo de la pantalla, haga clic en **Options** > **Trouble Signing In** (Opciones > Problema de inicio de sesión).
3 Cuando aparezca el cuadro de diálogo Q&A (Preguntas y respuestas), introduzca las respuestas que proporcionó al inscribirse en las preguntas de recuperación por primera vez.

Códigos de desafío/respuesta

La recuperación con desafío/respuesta se puede utilizar para autenticarse a través de PBA para accede a Windows. La opción de desafío/respuesta se puede usar en los casos siguientes:

- Cuando un usuario no recuerda las respuestas proporcionadas en el momento de la inscripción en Recovery Questions (Preguntas de recuperación).
- El administrador no ha activado la función Recovery Questions (Preguntas de recuperación).
- Un usuario es remoto sin conectividad de red y no puede recibir un comando de desbloqueo del servidor de seguridad a través de los controles de dispositivos SED.

Un usuario puede acceder a la pantalla Challenge/Response (Desafío/respuesta) haciendo clic en la opción **Trouble Signing In** (Problema de inicio de sesión) o introduciendo su contraseña de forma incorrecta, si se supera el límite de errores de contraseña sin el cable de red conectado. Si se ha desactivado la función Recovery Questions (Preguntas de seguridad), la opción **Trouble Signing In** (Problema de inicio de sesión) abre directamente la pantalla Challenge/Response (Desafío/respuesta).

Requisito

- La recuperación con desafío/respuesta está disponible únicamente para equipos del dominio administrados de forma remota por su organización o empresa.

Requisitos previos

- Desconecte el equipo de la red antes de responder a las preguntas de recuperación o introducir los códigos de desafío/respuesta.
- Antes de hacer clic en Trouble Signing In (Problema de inicio de sesión), introduzca un nombre de usuario y un dominio válidos.

Para utilizar la recuperación con desafío/respuesta

1 El usuario hace clic en el enlace **Options** (Opciones) para mostrar el menú.

2 El usuario hace clic en **Trouble Signing In** > **Challenge/Response** (Problema de inicio de sesión > Desafío/respuesta).

> **NOTA:**
> La opción Challenge/Response (Desafío/respuesta) solo está disponible en equipos administrados por una empresa. Si el equipo no es del dominio, la opción Challenge/Response (Desafío/respuesta) no aparece en el menú.

3 Cuando se solicite, el usuario contacta con el departamento de soporte técnico y proporciona al administrador el nombre de dispositivo (nombre de host) y el código de desafío.

4 El administrador abre la Remote Management Console, hace clic en **Management** > **Recover Data** (Administración > Recuperar datos) y, a continuación, hace clic en **SED** en el menú superior.

5 En Recover SED User Access (Recuperar acceso de usuario SED), el administrador introduce el **Host Name** (Nombre de host) obtenido del usuario y hace clic en **Search** (Buscar).

6 El administrador selecciona el nombre del usuario que está pidiendo ayuda:

7 Introduzca el código del dispositivo obtenido del usuario en el campo **Challenge** (Desafío) y haga clic en **Generate Response** (Generar respuesta).

8 Proporcione el código de respuesta generado al usuario.

> **NOTA:**
> Estos códigos no distinguen entre mayúsculas y minúsculas. Los números se muestran en rojo y las letras en azul.

9 El usuario introduce el código de respuesta en el campo **Response code** (Código de respuesta) de la pantalla de inicio de sesión de PBA. Este es un ejemplo de un código de respuesta introducido por el usuario:

10 Haga clic en la flecha derecha para continuar y para superar la autenticación en la pantalla PBA.

11 Haga clic en **Submit** (Enviar).

Un usuario puede superar la autenticación de PBA mediante la función Challenge/Response (Desafío/respuesta) solo una vez. Después de que se reinicie el equipo, el nivel de PBA reactivará la protección del equipo y volverá a solicitar al usuario que inicie sesión en la pantalla PBA.

> **NOTA:**
> Después de que el usuario visualice el cuadro de diálogo Challenge/Response (Desafío/respuesta), debe completar la secuencia de desafío/respuesta para volver a acceder al sistema. Si el usuario apaga el equipo e intenta volver a iniciar sesión (incluso con la contraseña correcta), la PBA volverá a mostrar al usuario el cuadro de diálogo Challenge/Response (Desafío/respuesta).

Recuperación de la contraseña de External Media Shield

External Media Shield (EMS) le ofrece la capacidad de proteger los medios de almacenamiento extraíbles dentro y fuera de la organización, permitiendo a los usuarios cifrar las unidades flash USB y otros medios de almacenamiento extraíbles. El usuario asigna una contraseña a cada medio extraíble que desea proteger. Esta sección describe el proceso de recuperación del acceso a un dispositivo de almacenamiento USB cifrado cuando un usuario olvida la contraseña de un dispositivo.

Recuperar el acceso a los datos

Cuando un usuario escribe de forma incorrecta su contraseña tantas veces que se supera el número permitido de intentos de contraseña, el dispositivo USB entra en modo de autenticación manual.

Autenticación manual es un proceso que consiste en proporcionar códigos del cliente a un administrador que ha iniciado sesión en el servidor.

En modo de autenticación manual, el usuario tiene dos opciones para restablecer su contraseña y recuperar el acceso a sus datos.

El administrador proporciona un código de acceso al cliente, que permite al usuario restablecer su contraseña y recuperar el acceso a sus datos cifrados.

1 Cuando se le solicite su contraseña, haga clic en el botón **I Forgot** (La he olvidado).

Se abrirá el cuadro de diálogo de confirmación.

2 Haga clic en **Sí** para confirmar. Después de la confirmación, el dispositivo entra en modo de autenticación manual.

3 Póngase en contacto con el administrador del departamento de soporte técnico y proporciónele los códigos que aparecen en el cuadro de diálogo.

4 Como administrador del departamento de soporte técnico, inicie sesión en la Remote Management Console. La cuenta del administrador del departamento de soporte técnico debe tener los privilegios correspondientes.

5 Vaya a la opción de menú **Recover Data** (Recuperar datos) en el panel izquierdo.

6 Introduzca los códigos proporcionados por el usuario final.

7 Haga clic en el botón **Generate Response** (Generar respuesta) en la esquina inferior izquierda de la pantalla.

8 Proporcione al usuario el código de acceso.

> **NOTA:**
> Asegúrese de autenticar manualmente al usuario antes de proporcionarle el código de acceso. Por ejemplo, plantee al usuario una serie de preguntas por teléfono que solo sabría él, como: "¿cuál es su número de ID de empleado?". Otro ejemplo: solicite al usuario que vaya al departamento de soporte técnico para que proporcione una identificación que garantice que es el propietario del medio. Si no se autentica a un usuario antes de proporcionarle un código de acceso por teléfono, un atacante podría obtener acceso al medio extraíble cifrado.

9 Restablezca su contraseña para el medio cifrado.

Se solicitará al usuario que restablezca su contraseña para el medio cifrado.

Recuperación automática

La recuperación automática es el proceso de restablecimiento de la contraseña para un medio extraíble cifrado mediante la inserción de la unidad de nuevo en un equipo protegido en el que el propietario del medio ha iniciado sesión. Siempre que el propietario del medio se autentique en el Mac o PC protegido, el cliente detecta la pérdida del material de claves y solicita al usuario que vuelva a iniciar el dispositivo. En ese momento, el usuario puede restablecer su contraseña y volver a acceder a sus datos cifrados.

1 Inicie sesión en una estación de trabajo cifrada con Dell Data Protection como propietario del medio.
2 Introduzca el dispositivo de almacenamiento extraíble cifrado.
3 Cuando se le solicite, introduzca una nueva contraseña para volver a iniciar el dispositivo de almacenamiento extraíble.

   Si se realiza correctamente, aparece una pequeña notificación para indicar que se ha aceptado.
4 Navegue al dispositivo de almacenamiento y confirme el acceso a los datos.

9

Recuperación de Dell Data Guardian

La herramienta de recuperación permite:

- Descifrar los archivos de Office protegidos

  Esto incluye los archivos hasta con cifrado triple: con más de una forma de cifrar archivos, ocasionalmente un archivo cuenta con cifrado doble o triple. Si el usuario abre el archivo, un mensaje de error indica que debe ponerse en contacto con el administrador para recuperarlo.
- Custodiar el material de claves
- Capacidad para comprobar archivos manipulados
- Capacidad para forzar el cifrado de documentos de Office protegidos en los que alguien ha manipulado el contenedor del archivo, por ejemplo, la portada del archivo de Office protegido en la nube o en un dispositivo que no cuenta con Data Guardian

Requisitos de recuperación

Los requisitos incluyen:

- Microsoft .NET Framework 4.5.2 en ejecución en el extremo que se va a recuperar.
- El rol de administrador forense se debe asignar en la Remote Management Console al administrador que lleve a cabo la recuperación.

Realizar recuperación de Data Guardian

Siga estos pasos para realizar la recuperación de documentos de Office protegidos con Data Guardian.

Realizar una recuperación desde Windows, una unidad flash USB o una unidad de red

Para realizar una recuperación:

1 Desde el medio de instalación de Dell, copie **RecoveryTools.exe** en una de estas ubicaciones:

   - Equipo: copie el archivo .exe en el equipo en el que se van a recuperar los documentos de Office.
   - USB: copie el archivo .exe en la unidad flash USB y ejecútelo desde esta.
   - Unidad de red

2 Haga doble clic en **RecoveryTools.exe** para iniciar la herramienta de recuperación.

3 En la ventana Data Guardian, introduzca la URL del servidor de Dell en este formato:

   https://<server.domain.com>:8443/cloud

   NOTA:
   Sustituya <server.domain.com> con el nombre de host completo del servidor de Dell que gestiona Data Guardian en ese extremo. Para localizar la URL del servidor de Dell, haga clic en el icono de Data Guardian en la bandeja del sistema y haga clic en **Detalles**. La esquina superior izquierda de la pantalla Detalles mostrará la URL del servidor.

4 Introduzca su nombre de usuario y su contraseña y haga clic en **Iniciar sesión**.

NOTA:
No desmarque la casilla *Activar confianza en SSL* a menos que lo indique el administrador.

NOTA:
Si no es administrador forense e introduce las credenciales, se mostrará un mensaje que indica que no tiene derechos de inicio de sesión.

Si es administrador forense, se abrirá la herramienta de recuperación.

5 Seleccione **Origen**.

NOTA:
Debe navegar a un origen y un destino, aunque puede seleccionarlos en cualquier orden.

6 Haga clic en **Examinar** para seleccionar la carpeta o unidad que se va a recuperar.

7 Haga clic en **Aceptar**.

8 Haga clic en **Destino**.

9 Haga clic en **Examinar** para seleccionar un destino; por ejemplo, un dispositivo externo, la ubicación de un directorio o el escritorio.

10 Haga clic en **Aceptar**.

11 Seleccione una o más casillas en función de lo que desee recuperar.

Opciones	Descripción
Custodia	• Recupere las claves generadas sin conexión que no se pudieron custodiar en el servidor de Dell. • Si una unidad de disco duro falla mientras el usuario está desconectado de la red, utilice la unidad secundaria para recuperar los datos y las claves no custodiadas del equipo.
Descifrado	Navegue con la herramienta de recuperación a un directorio que contenga los documentos de Office protegidos para descifrarlos. De manera opcional, si se ha producido manipulación, seleccione una de estas opciones o las dos (consulte más abajo para obtener información): • **Comprobación de manipulación**: comprueba los archivos manipulados, pero no los descifra. • **Comprobación de manipulación** y **Forzar descifrado incluso si está manipulado**: comprueba si hay archivos manipulados y, si el contenedor de un documento de Office protegido se ha manipulado, Data Guardian repara el contenedor y descifra el documento de Office.
Comprobación de manipulación	Detecta los archivos que se han manipulado, los registra y se lo notifica. Registra el autor de la manipulación del archivo. No descifra los archivos.
Forzar descifrado incluso si está manipulado	Para seleccionar esta opción, debe también seleccionar **Comprobación de manipulación**. Si una persona autorizada ha manipulado el contenedor de un documento de Office protegido, como la portada, ya sea en la nube o en un dispositivo que no cuenta con Data Guardian, seleccione esta opción para reparar el contenedor y forzar el descifrado del archivo de Office protegido.

Opciones	Descripción
	Nota: Si alguien ha manipulado el archivo .xen de Office cifrado dentro del contenedor, el archivo no se podrá recuperar.

Cada archivo de Office protegido tiene una marca de agua oculta que contiene el historial del usuario original y el nombre de equipo, y cualquier otro nombre de equipo que haya modificado el archivo. De manera predeterminada, la herramienta de recuperación comprueba las marcas de agua ocultas y registra la información.

12 Una vez que se hayan completado las selecciones, haga clic en **Explorar**.

El área de registro muestra:

- Las carpetas encontradas y exploradas dentro del origen seleccionado
- Si el cifrado se ha realizado correctamente o no

La herramienta de recuperación añade los archivos recuperados al destino seleccionado. Puede abrir y ver los archivos.

Apéndice A - Grabar el entorno de recuperación

Puede descargar Master Installer.

Grabar la ISO del entorno de recuperación en CD/DVD

El siguiente enlace contiene el proceso necesario para utilizar Microsoft Windows 7, Windows 8 o Windows 10 para crear un CD o DVD de arranque para el entorno de recuperación.

http://windows.microsoft.com/en-us/windows7/burn-a-cd-or-dvd-from-an-iso-file

Grabar el entorno de recuperación en un medio extraíble

Para crear un USB de arranque, siga las instrucciones de este artículo de Microsoft:

https://technet.microsoft.com/en-us/library/jj200124(v=ws.11).aspx