Dell Data Protection | Security Tools

Guía de instalación

v 1.9

01/2016

Contenido

1

Introducción

Dell Data Protection | Security Tools (DDP|ST) proporciona seguridad y protección de identidades a los administradores y usuarios de equipos Dell. DDP|ST viene preinstalado en todos los equipos Dell Latitude, Optiplex y Precision, así como en algunos equipos portátiles Dell XPS. En caso de que tenga que *reinstalar* DDP|ST, siga las instrucciones de esta guía. Para obtener ayuda adicional, consulte www.dell.com/support > Endpoint Security Solutions.

Descripción general

DDP|ST es una solución de seguridad integral diseñada para proporcionar asistencia de autenticación avanzada, así como compatibilidad para Autenticación previa al inicio y administración de las unidades de cifrado automático.

DDP|ST proporciona compatibilidad multifactor en la autenticación de Windows con contraseñas, lectores de huellas digitales y tarjetas inteligentes, tanto de contacto como sin contacto, así como autoregistro, Inicio de sesión en un solo paso (Inicio de sesión único [SSO]) y Contraseñas de un solo uso (OTP).

Antes de poner Security Tools a la disposición de los usuarios finales, puede que los administradores deseen configurar las funciones de Security Tools, utilizando la herramienta Configuración del administrador de DDP Security Console, por ejemplo, con el fin de habilitar la Autenticación previa al inicio y las políticas de autenticación. Sin embargo, la configuración predeterminada permite que los administradores y usuarios comiencen a utilizar Secutiry Tools inmediatamente después de la instalación y activación.

DDP Security Console

La DDP Security Console es la interfaz de Security Tools mediante la que los usuarios pueden registrarse y administrar sus credenciales y pueden configurar las preguntas de autorecuperación, según sea la política que haya establecido el administrador. Los usuarios pueden acceder a estas aplicaciones de Security Tools:

- La herramienta de Cifrado permite que los usuarios vean el estado del cifrado de las unidades del equipo.
- La herramienta de Registros permite que los usuarios establezcan y administren las credenciales, configuren las preguntas de autorecuperación y vean el estado del registro de sus credenciales. Estos privilegios están basados en la política establecida por el administrador.
- Password Manager permite a los usuarios rellenar y enviar automáticamente los datos necesarios para iniciar sesión en los sitios webs, aplicaciones de Windows y recursos de red. Password Manager también ofrece la posibilidad de que el usuario cambie sus contraseñas de inicio de sesión a través de la aplicación, con lo que se asegura de que las contraseñas conservadas por Password Manager se mantengan sincronizadas con las del recurso en cuestión.

Configuración del administrador

La herramienta Configuración del administrador se utiliza para configurar Security Tools para todos los usuarios del equipo, lo cual permite al administrador establecer las políticas de autenticación, administrar a usuarios y configurar las credenciales que se utilizarán en el inicio de sesión de Windows.

Con la herramienta Configuración del administrador, el administrador puede habilitar el cifrado y la Autenticación previa al inicio (PBA), así como configurar las políticas de la PBA y personalizar el texto en pantalla de la PBA.

Vaya a Requisitos.

2

Requisitos

- DDP|ST viene preinstalado en todos los equipos Dell Latitude, Optiplex y Precision, así como en algunos equipos portátiles Dell XPS, y cumple con los siguientes requisitos mínimos. En caso de que necesite reinstalar DDP|ST, asegúrese de que su equipo aún cumpla estos requisitos. Consulte www.dell.com/support > Endpoint Security Solutions para obtener más información.
- Windows 8.1 no debe estar instalado en la unidad 1 de unidades de cifrado automático. Esta configuración de sistema operativo no es compatible porque Windows 8.1 crea una partición de recuperación de la unidad 0 que, a su vez, anula la Autenticación previa al inicio. No obstante, puede instalar Windows 8.1 en la unidad configurada como unidad 0, o restaurar Windows 8.1 como imagen en cualquiera de las unidades.
- DDP|ST no admite discos dinámicos.
- Los equipos que están equipados con unidades de autocifrado no pueden ser utilizados con Hardware Crypto Accelerators. Existen incompatibilidades que impiden el aprovisionamiento del HCA. Tenga en cuenta que Dell no vende equipos que tengan unidades de autocifrado compatibles con el módulo HCA. Esta configuración incompatible será una configuración realizada poscompra.
- DDP|ST no admite la configuración de discos de arranques múltiples.
- Antes de instalar un sistema operativo nuevo en el cliente, borre el Trusted Platform Module (TPM) del BIOS.
- Una SED no requiere un TPM para proporcionar autenticación avanzada o cifrado.
- **Intel RAID integrado en los equipos portátiles** es compatible con PBA al utilizar el DDP|Hardware Crypto Accelerator. RAID no está admitido en sistemas con unidades de cifrado automático. Para obtener más información, consulte Controladores.

Controladores

- Las SED admitidas que cumplen con la norma de Opal necesitan controladores actualizados Intel Rapid Storage Technology, que se pueden encontrar en http://www.dell.com/support/drivers/us/en/19/DriverDetails/Product/latitude-e6440-laptop?driverId=1KX2H&osCode=W764&fileId=3356216042&languageCode=en&categoryId=SA.

IMPORTANTE: Debido a la naturaleza de RAID y SED, SED Management no es compatible con RAID. El problema que presenta "RAID=On" con respecto a SED es que RAID requiere acceso al disco para leer y escribir los datos relacionados con RAID en un sector de alto nivel que no se encuentra disponible desde el inicio en un SED bloqueado, y RAID no puede esperar a leer estos datos hasta que el usuario inicie sesión. Para resolver este problema, cambie el funcionamiento de SATA en el BIOS de "RAID=On" a "AHCI". Si el sistema operativo no tiene controladores de la controladora AHCI instalados previamente, el sistema operativo mostrará una pantalla azul al realizar el cambio de "RAID=On" a "AHCI."

Requisitos previos del cliente

- La versión completa de Microsoft .Net Framework 4.0 (o posterior) es obligatoria para Security Tools. Todos los equipos enviados desde la fábrica de Dell vienen con la versión completa de Microsoft .Net Framework 4.0 previamente instalada. Sin embargo, si no está instalando en hardware Dell o si está actualizando Security Tools en hardware Dell más antiguo, debería comprobar qué versión de Microsoft .Net tiene instalada y actualizar la versión, antes de instalar Security Tools, con el fin de evitar errores durante la instalación/actualización. Para instalar la versión completa de Microsoft .Net Framework 4.0, vaya a http://www.microsoft.com/en-us/download/details.aspx?id=17851.

  Para comprobar qué versión de .Net tiene instalada, siga estas instrucciones en el equipo en el que se va a realizar la instalación: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx.
- Los controladores y el firmware de su hardware de autenticación deben estar actualizados en su equipo. Para obtener controladores y firmware para equipos Dell, vaya a http://www.dell.com/support/home/us/en/19/Products/?app=drivers y seleccione su modelo de equipo. Según su hardware de autenticación, descargue lo siguiente:
  - Controlador de huellas digitales NEXT Biometrics
  - Controlador de lector de huellas digitales Validity 495
  - Controlador de tarjetas inteligentes O2Micro
  - Dell ControlVault

  Es posible que otros proveedores de hardware requieran sus propios controladores.

El instalador agrega este componente si no se encuentra instalado en el equipo.

Requisitos previos
• Paquete redistribuible de Microsoft Visual C++ 2012 actualización 4 o posterior (x86/x64)

Software

Sistemas operativos Windows

La tabla a continuación muestra qué software es compatible.

Sistemas operativos Windows (de 32 y 64 bits)
• Microsoft Windows 7 SP0 - SP1 - Enterprise - Professional
NOTA: El modo de inicio heredado es compatible con Windows 7. UEFI no es compatible con Windows 7.
• Microsoft Windows 8 - Enterprise - Pro - Windows 8 (Consumer)

NOTA: Windows 8 es compatible con el modo UEFI cuando se utiliza con SED que cumplen con la norma de Opal y Modelos de equipos Dell - Compatibilidad con UEFI.

Sistemas operativos Windows (de 32 y 64 bits)
• Microsoft Windows 8.1 - 8.1 Actualización 1 - Enterprise Edition - Pro Edition

NOTA: Windows 8.1 es compatible con el modo UEFI cuando se utiliza con SED que cumplen con la norma de Opal y Modelos de equipos Dell - Compatibilidad con UEFI.

• Microsoft Windows 10 - Education Edition - Enterprise Edition - Pro Edition

NOTA: Windows 10 es compatible con el modo UEFI cuando se utiliza con SED que cumplen con la norma de Opal y Modelos de equipos Dell - Compatibilidad con UEFI.

Sistemas operativos de dispositivos móviles

Los siguientes sistemas operativos para móviles son compatibles con la función de Contraseña de un solo uso de Security Tools.

Sistemas operativos Android
• 4.0 - 4.0.4 Ice Cream Sandwich
• 4.1 - 4.3.1 Jelly Bean
• 4.4 - 4.4.4 KitKat
• 5.0 - 5.1.1 Lollipop
Sistemas operativos iOS
• iOS 7.x
• iOS 8.x
Sistemas operativos Windows Phone
• Windows Phone 8.1
• Windows 10 Mobile

Hardware

Autenticación

La siguiente tabla detalla el hardware de autenticación compatible.

Lectores de huellas digitales
• Validity VFS495 en modo seguro
• Lector magnético Broadcom Control Vault
• Lector UPEK TCS1 FIPS 201 Secure 1.6.3.379
• Lectores USB Authentec Eikon y Eikon To Go

NOTA: Al utilizar un lector de huellas digitales externo, debe descargar e instalar la última versión de los controladores que requiera su lector.

Tarjetas sin contacto
• Tarjetas sin contacto con lectores compatibles sin contacto integrados en equipos portátiles específicos de Dell
Tarjetas inteligentes
• Tarjetas inteligentes PKCS n.º 11 que utilizan el cliente ActivIdentity **NOTA:** El cliente ActivIdentity no se carga previamente y debe instalarse por separado.
• Tarjetas de acceso común (CAC) **NOTA:** Con las CAC de varios certificados, el usuario selecciona el certificado correcto de una lista durante el inicio de sesión.
• Tarjetas CSP
• Tarjetas SIPR Net/Clase B

La siguiente tabla muestra qué modelos de equipos Dell admiten tarjetas SIPR Net.

Modelos de equipos Dell - Compatibilidad con la tarjeta SIPR Net/Clase B
• Latitude E6440
• Latitude E6540
• Precision M2800
• Precision M4800
• Precision M6800
• Latitude 14 Rugged Extreme
• Latitude 12 Rugged Extreme
• Latitude 14 Rugged

Modelos de equipos Dell - Compatibilidad con UEFI

Las funciones de autenticación son compatibles con el modo UEFI en determinados equipos Dell que ejecutan Microsoft Windows 8, Microsoft Windows 8.1 y Microsoft Windows 10 con SED que cumplen con la norma de Opal cualificadas. Otros equipos que ejecutan Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 8.1 y Microsoft Windows 10 admiten el modo de inicio heredado.

La siguiente tabla muestra qué modelos de equipos Dell admiten UEFI.

Modelos de equipos Dell - Compatibilidad con UEFI
• Latitude E7240
• Latitude E7250
• Latitude E7350
• Latitude E7440
• Latitude E7450
• Precision M4800
• Precision M6800
• Precision T7810
• OptiPlex 7020
• OptiPlex 9020 Micro
• Venue Pro 11 (Modelo 7139)

NOTA: En un equipo compatible con UEFI, después de seleccionar **Reiniciar** desde el menú principal, el equipo se reinicia y a continuación muestra una de las dos posibles pantallas de inicio. La pantalla de inicio que aparece la determinan las diferencias en la arquitectura de la plataforma del equipo. Algunos modelos muestran una pantalla de inicio de sesión PBA; otros modelos muestran la pantalla de inicio de sesión de Windows. Ambas pantallas son seguras.

NOTA: Asegúrese de que la configuración Habilitar las ROM de opción heredadas está deshabilitada en el BIOS.

Para deshabilitar las ROM de opción heredadas:

1. Reinicie el equipo.
2. Mientras se reinicia, pulse **F12** varias veces para que aparezca la configuración de inicio del equipo UEFI.
3. Pulse la flecha Abajo, resalte la opción **Configuración del BIOS** y pulse **Intro**.
4. Seleccione **Configuración > General > Opciones de inicio avanzadas**.
5. Borre la casilla de verificación **Habilitar las ROM de opción heredadas** y haga clic en **Aplicar**.

SED que cumplen con la norma de Opal

Las unidades con "X" son compatibles pero no son adecuadas ni se entregan con los sistemas Dell.

Unidad	Disponibilidad	Estándar
Seagate ST320LT009 (FIPS Julius 320 GB)	✓	Opal 1
Seagate ST320LT014 (Julius 320 GB)	✓	Opal 1
Seagate ST500LM001 (Kahuna 500 GB)	✓	Opal 2/eDrive
Seagate ST1000LM015 (Kahuna 1000 GB)	✓	Opal 2/eDrive
Seagate ST500LT012 (Yarra 1D non-FIPS 500 GB)	✓	Opal 2/eDrive
Seagate ST500LT015 (Yarra 1D FIPS 500 GB)	✓	Opal 2/eDrive
Seagate ST500LM020 (Kahuna V FIPS 500 GB)	✓	Opal 2/eDrive
Seagate ST1000LM028 (Kahuna V FIPS 1000 GB)	✓	Opal 2/eDrive
Seagate ST500LM023 (Yarra X)	✓	Opal 2/eDrive
Seagate ST500LM024 (Yarra X FIPS 500 GB)	✓	Opal 2/eDrive
Seagate ST500LT025 (Yarra R)	✓	Opal 2/eDrive
Seagate ST500LT033 (Asagana)	✓	Opal 2/eDrive
Seagate ST1000DM004 (Desktop 3,5 pulgadas 1000 GB)	X	Opal 2/eDrive
Seagate ST1000DM004 (Desktop 3,5 pulgadas 2000 GB)	X	Opal 2/eDrive
Seagate ST1000DM004 (Desktop 3,5 pulgadas 3000 GB)	X	Opal 2/eDrive
Travelstar serie 5K750	X	Opal 1
Travelstar serie 7K750	X	Opal 1
Travelstar serie Z5K320	X	Opal 1
Toshiba serie MKxx61GSYD	X	Opal 1
Toshiba serie MKxx61GSYG	X	Opal 1
Samsung SM840 EVO MZ-MTEXXXBW	X	Opal 2
SSD Samsung SM841 OPAL	✓	Opal 2
SSD Samsung SM841N OPAL	✓	Opal 2
Samsung SM850 PRO de 2,5 pulgadas MZ-7KE128 – MZ-7KE2T0 (SSD SED de 2,5 pulgadas de 128 GB a 2000 GB)	X	Opal 2/eDrive
Samsung SM850 EVO de 2,5 pulgadas MZ-75E120 – MZ-75E2T0 (SSD SED de 2,5 pulgadas de 120 GB a 2000 GB)	X	Opal 2/eDrive
Samsung SM850 EVO mSATA MZ-M5E120 – MZ-M5E1T0 (SSD mSATA SED de 120 GB a 1000 GB)	X	Opal 2/eDrive
Samsung SM850 EVO M.2 MZ-N5E120 – MZ-N5E500 (M.2. SSD SED de 120 GB a 500 GB)	X	Opal 2/eDrive
SSD Samsung PM851 OPAL – 2,5 pulgadas (2,5 pulgadas de 128 GB - 512 GB)	✓	Opal 2/eDrive
SSD Samsung PM851 OPAL – mSATA (mSATA de 128 GB - 512 GB)	✓	Opal 2/eDrive

Unidad	Disponibilidad	Estándar
SSD Samsung PM851 OPAL - M.2. (M.2. de 128 GB - 512 GB)	✓	Opal 2/eDrive
SSD Samsung PM871 OPAL - 2,5 pulgadas (2,5 pulgadas de 256 GB - 512 GB)	✓	Opal 2/eDrive
SSD Samsung PM871 OPAL - mSATA (mSATA de 256 GB - 512 GB)	✓	Opal 2/eDrive
SSD Samsung PM871 OPAL - M.2. (M.2. de 256 GB - 512 GB)	✓	Opal 2/eDrive
SanDisk X300s	X	Opal 2
SSD OPAL LiteOn L9M	✓	Opal 2
SSD LiteOn serie M3	✓	Opal 1
SSD LiteOn serie M6	✓	Opal 2
SSD LiteOn serie V2M	✓	Opal 2
SSD Crucial RealSSD C400	X	Opal 1
SSD Micron RealSSD C400	X	Opal 1
SSD Micron M500 de 2,5 pulgadas (120 GB - 960 GB)	X	Opal 2/eDrive
SSD Micron M500 mSATA (120 GB - 480 GB)	X	Opal 2/eDrive

Compatibilidad de idiomas

DDP|ST es una Interfaz de usuario multilingüe (MUI) que cumple los requisitos del sector y se puede configurar en los siguientes idiomas.

NOTA: La localización de PBA no está disponible en ruso, chino tradicional y chino simplificado.

Compatibilidad de idiomas	
• Inglés (EN)	• Coreano (KO)
• Francés (FR)	• Chino simplificado (ZH-CN)
• Italiano (IT)	• Chino tradicional /Taiwán (ZH-TW)
• Alemán (DE)	• Portugués brasileño (PT-BR)
• Español (ES)	• Portugués europeo (PT-PT)
• Japonés (JA)	• Ruso (RU)

Opciones de autenticación

Las opciones de autenticación siguientes requieren hardware específico: Huellas digitales, Tarjetas inteligentes, Tarjetas sin contacto, Tarjetas SIPR Net/Clase B y Autenticación en equipos UEFI.

La función de la contraseña de un solo uso requiere que haya un TPM presente, habilitado y con propietario. Para obtener más información, consulte Borrar la propiedad y activar el TPM.

Las tablas siguientes muestran opciones de autenticación disponibles con Security Tools, por sistema operativo, cuando se cumplan los requisitos de hardware y de configuración.

Sin UEFI

	PBA					Autenticación de Windows				
	Contraseña	Huellas digitales	Tarjeta inteligente con contacto	OTP	Tarjeta SIPR	Contraseña	Huellas digitales	Tarjeta inteligente	OTP	Tarjeta SIPR
Windows 7 SP0-SP1	X[1]					X	X	X	X	X
Windows 8	X[1]					X	X	X	X	X
Windows 8.1-Windows 8.1 Actualización 1	X[1]					X	X	X	X	X
Windows 10	X[1]					X	X	X	X	X

1. Disponible con un SED Opal compatible.

UEFI

	PBA - en equipos Dell compatibles					Autenticación de Windows				
	Contraseña	Huellas digitales	Tarjeta inteligente con contacto	OTP	Tarjeta SIPR	Contraseña	Huellas digitales	Tarjeta inteligente	OTP	Tarjeta SIPR
Windows 7										
Windows 8	X[2]					X	X	X	X	X
Windows 8.1-Windows 8.1 Actualización 1	X[2]					X	X	X	X	X
Windows 10	X[2]					X	X	X	X	X

2. Disponible con un SED OPAL compatible en equipos UEFI admitidos.

Interoperabilidad

Desaprovisionamiento y desinstalación de Dell Data Protection | Access

Si se ha instalado ahora DDP|A o ya se había instalado previamente en su equipo, **antes** de instalar Security Tools deberá desaprovisionar el hardware administrado por DDP|A y desinstalar DDP|A. Si DDP|A no ha sido utilizado, puede simplemente desinstalarlo y reiniciar el proceso de instalación.

El desaprovisionamiento de hardware administrado por DDP|A incluye los lectores de huellas digitales, los lectores de tarjetas inteligentes, contraseñas de BIOS, TPM y la unidad de cifrado automático.

NOTA: Si se ejecutan productos de cifrado DDP|E, detenga o pause el barrido de cifrado. Si está ejecutando Microsoft BitLocker, suspenda la política de cifrado. Una vez que se haya instalado DDP|A y suspendido la política de Microsoft BitLocker, inicialice el TPM siguiendo las instrucciones que se encuentran en http://technet.microsoft.com/en-us/library/cc753140.aspx.

Desaprovisionamiento de hardware administrado por DDP|A

1. Inicie DDP|A y haga clic en la pestaña *Avanzado*.
2. Seleccione **Restablecer sistema**. Esto requiere que introduzca cualquier credencial proporcionada para comprobar su identidad. Una vez que DDP|A compruebe las credenciales, DDP|A realizará las siguientes acciones:

   - Eliminará todas las credenciales proporcionadas de Dell ControlVault (si está presente)
   - Eliminará la contraseña de propietario de Dell ControlVault (si está presente)
   - Eliminará todas las huellas digitales proporcionadas del lector integrado de huellas digitales (si está presente)
   - Eliminará todas las contraseñas del BIOS (contraseñas del sistema BIOS, administrador BIOS y unidad de disco duro)
   - Limpiará el Trusted Platform Module
   - Eliminará el proveedor de credenciales de DDP|A.

   Una vez desaprovisionado el equipo, DDP|A lo reiniciará para restaurar el proveedor de credenciales predeterminado de Windows.

Desinstalación de DDP|A

Una vez que el hardware de autenticación esté desaprovisionado, desinstale DDP|A.

1. Inicie DDP|A y restablezca el sistema.

   Esto hará que se eliminen todas las credenciales y contraseñas administradas por DDP|A y que se limpie el Trusted Platform Module (TPM).
2. Haga clic en **Desinstalar** para iniciar el instalador.
3. Cuando finalice la desinstalación, haga clic en **Sí** para reiniciar.

NOTA: Al eliminar DDP|A también se desbloqueará el SED y se eliminará la Autenticación previa al inicio.

Inicialización del TPM

1. Siga las instrucciones que se explican en http://technet.microsoft.com/en-us/library/cc753140.aspx.

Borrar la propiedad y activar el TPM

Para borrar y establecer la propiedad del TPM, consulte https://technet.microsoft.com/en-us/library/cc749022%28v=ws.10%29.aspx#BKMK_S2.

Continúe con Instalación y activación.

3

Instalación y activación

Esta sección describe cómo instalar DDP|ST en un equipo local. Para instalar y activar DDP|ST, debe haber iniciado sesión en el equipo como administrador.

PRÁCTICA RECOMENDADA: Durante la instalación, no realice cambios en el equipo, incluida la inserción o extracción de las unidades (USB) externas.

Instalación de DDP|ST

Para instalar Security Tools:

1. Localice el archivo de instalación en el medio de instalación de DDP|ST. Cópielo al equipo local.

NOTA: El medio de instalación se puede encontrar en www.dell.com/support > Endpoint Security Solutions.

2. Haga doble clic en el archivo para iniciar el instalador.
3. Seleccione el idioma adecuado y haga clic en **Aceptar**.
4. Haga clic en **Siguiente** cuando aparezca la pantalla de Bienvenida.
5. Lea el contrato de licencia, acepte las condiciones y haga clic en **Siguiente**.
6. Haga clic en **Siguiente** para instalar Security Tools en la ubicación predeterminada de C:\Program Files\Dell\Dell Data Protection. Seleccione **Siguiente** en la página de selección de características.
7. Haga clic en **Instalar** para iniciar la instalación.
8. Cuando la instalación haya finalizado, deberá reiniciar el equipo. Seleccione **Sí** para reiniciar y, a continuación, haga clic en **Finalizar**.

   La instalación ha finalizado.

Activación de DDP|ST

La primera vez que ejecute la DDP Security Console y seleccione Configuración del administrador, el asistente de Activación le guiará durante el proceso de Activación.

Aunque no esté activada todavía la DDP Security Console, todavía puede ser ejecutada por un usuario final. Cuando un usuario final es la primera persona en utilizar la DDP Security Console antes de que un administrador active DDP|ST y personalice la configuración, se utilizarán los valores predeterminados.

Para activar Security Tools:

1. Como administrador, inicie Security Tools desde el acceso directo de su escritorio.

NOTA: Si ha iniciado sesión como un usuario normal (utilizando una cuenta estándar de Windows), la herramienta Configuración del administrador requiere elevación de UAC para iniciarse. El usuario normal escribirá en primer lugar las credenciales del administrador para iniciar sesión en la herramienta y, en segundo lugar, cuando se le solicite, escribirá la contraseña del administrador (la contraseña almacenada en Configuración del administrador).

2. Haga clic en el mosaico **Configuración de administrador**.
3. En la página de Bienvenida, haga clic en **Siguiente**.
4. Cree la contraseña para DDP|ST y haga clic en **Siguiente**.

   Debe crear la contraseña de administrador para DDP|ST antes de configurar Security Tools. La contraseña será necesaria cada vez que ejecute la herramienta Configuración del administrador. La contraseña debe tener 8-32 caracteres e incluir al menos una letra, un número y un carácter especial.
5. En **Ubicación de la copia de seguridad**, especifique la ubicación en la que se escribirá el archivo de copia de seguridad y haga clic en **Siguiente**.
   El archivo de copia de seguridad debe guardarse en una unidad de red o en un soporte extraíble. El archivo de copia de seguridad contiene las claves necesarias para recuperar datos en este equipo. Dell Support debe tener acceso a este archivo para ayudarle a recuperar los datos.

   Se realizará automáticamente una copia de seguridad de los datos de recuperación en la ubicación determinada. Si la ubicación no está disponible (por ejemplo, si no se ha introducido su unidad USB de copia de seguridad), DDP|ST solicitará una ubicación para realizar la copia de seguridad de los datos. Será necesario tener acceso a los datos de recuperación para comenzar el cifrado.
6. En la página de Resumen, haga clic en **Aplicar**.

La activación de Security Tools ha sido completada.

Los administradores y los usuarios pueden empezar a utilizar las funciones de Security Tools inmediatamente, dependiendo de la configuración predeterminada.

4

Tareas de configuración para administradores

La configuración predeterminada de Security Tools permite que los administradores y usuarios utilicen Security Tools inmediatamente después de la activación y sin necesidad de realizar ninguna configuración adicional. Los usuarios son automáticamente agregados como usuarios de Security Tools cuando inician sesión en el equipo con sus contraseñas de Windows pero, de forma predeterminada, no se habilita la autenticación multifactor de Windows. De forma predeterminada, tampoco se habilitan el cifrado y la Autenticación previa al inicio.

Para configurar las funciones de Security Tools debe ser un administrador en el equipo.

Cambio de la Contraseña del administrador y de la Ubicación de las copias de seguridad

Después de la activación de Security Tools, se puede cambiar la Contraseña del administrador y la Ubicación de las copias de seguridad si es necesario.

1. Como administrador, inicie Security Tools desde el acceso directo de su escritorio.
2. Haga clic en el mosaico **Configuración de administrador**.
3. En el diálogo Autenticación, introduzca la contraseña del administrador que fue establecida durante la activación, y haga clic en **Aceptar**.
4. Haga clic en la pestaña **Configuración de administrador**.
5. En la página Cambiar contraseña del administrador, si desea cambiar la contraseña, introduzca una nueva que contenga entre 8-32 caracteres e incluya al menos una letra, un número y un carácter especial.
6. Introduzca la contraseña una segunda vez para confirmarla, a continuación haga clic en **Aplicar**.
7. Para cambiar la ubicación donde se ha almacenado la clave de recuperación, en el panel izquierdo, seleccione **Cambiar ubicación de copia de seguridad**.
8. Seleccione una nueva ubicación para la copia de seguridad y haga clic en **Aplicar**.

   El archivo de copia de seguridad debe guardarse en una unidad de red o un soporte extraíble. El archivo de copia de seguridad contiene las claves necesarias para recuperar datos en este equipo. Dell ProSupport debe tener acceso a este archivo para ayudarle a recuperar los datos.

   Se realizará automáticamente una copia de seguridad de los datos de recuperación en la ubicación determinada. Si la ubicación no está disponible (por ejemplo, si no se ha introducido su unidad USB de copia de seguridad), DDP|ST solicitará una ubicación para realizar la copia de seguridad de los datos. Será necesario tener acceso a los datos de recuperación para comenzar el cifrado.

Configuración de cifrado y Autenticación previa al inicio

El cifrado y la Autenticación previa al inicio (PBA) están disponibles si su equipo tiene una unidad de cifrado automático (SED). Ambas funciones están configuradas mediante la pestaña Cifrado, que se puede ver solamente si el equipo tiene una unidad de cifrado automático (SED). Cuando se habilita la función de cifrado o la de PBA, se habilitará también la otra.

Antes de activar el cifrado y la PBA por primera vez, Dell recomienda que registre y habilite las Preguntas de recuperación como una Opción de recuperación para poder recuperar la contraseña en caso de que se pierda. Para obtener más información, consulte Configuración de las opciones de inicio de sesión.

Para configurar el cifrado y la Autenticación previa al inicio:

1. En la DDP Security Console, haga clic en el mosaico **Configuración del administrador**.
2. Asegúrese de que se puede acceder a la ubicación de copia de seguridad desde el equipo.

NOTA: Si aparece un mensaje cuando se está habilitando la función de cifrado, "No se encuentra ubicación de copia de seguridad", y la ubicación de la copia de seguridad está en una unidad USB, su unidad no está conectada o está conectada en una ranura diferente a la que utilizó durante la copia de seguridad. Si se muestra el mensaje y la ubicación de copia de seguridad se encuentra en una unidad de red, no se podrá acceder a esta unidad desde el equipo. Si es necesario cambiar la ubicación de copia de seguridad, desde la pestaña **Configuración del administrador**, seleccione **Cambiar ubicación de copia de seguridad** para cambiar la ubicación a la ranura actual o a una unidad accesible. Transcurridos unos segundos tras la reasignación de la ubicación, se podrá continuar con el proceso de habilitación del cifrado.

3. Haga clic en la pestaña **Cifrado** y, a continuación, en **Cifrar**.
4. En la página de Bienvenida, haga clic en Siguiente.
5. En la página Política de preinicio, cambie o confirme los siguientes valores, y haga clic en **Siguiente**.

Intentos de inicio de sesión de usuario sin caché	Número de veces que un usuario desconocido puede intentar iniciar sesión (un usuario que no ha iniciado sesión en el equipo anteriormente [no se han guardado sus credenciales en la memoria caché]).
Intentos de inicio de sesión de usuario en caché	Número de veces que un usuario conocido puede intentar iniciar sesión.
Intentos en responder a preguntas de recuperación	Número de veces que el usuario puede intentar escribir la respuesta correcta.
Habilitar contraseña para eliminar cifrado	Seleccionar para habilitar
Introducir contraseña para eliminar cifrado	Una palabra o código de hasta 100 caracteres utilizado como mecanismo de seguridad a prueba de errores. Introducir esta palabra o código en el nombre del usuario o en la contraseña durante la autenticación PBA borra el dispositivo de forma permanente. Si no se introduce texto en este campo no estará disponible ninguna contraseña para borrar cifrado en caso de emergencias.

6. En la página Personalización de preinicio, introduzca el texto personalizado que aparecerá en la pantalla de Autenticación previa al inicio (PBA), y haga clic en **Siguiente.**

Texto del título de preinicio	Este texto aparece en la parte superior de la pantalla de PBA. Si deja este campo vacío, no se mostrará ningún título. El texto no hace salto de línea, por lo que es posible que los textos de más de 17 caracteres aparezcan cortados.

Texto de información de soporte	Este texto se muestra en la página de información sobre soporte de PBA. Dell recomienda personalizar el mensaje para incluir instrucciones específicas sobre cómo comunicarse con el Servicio de asistencia o el Administrador de seguridad. Si no se introduce texto en este campo no se mostrará la información de contacto de soporte para el usuario. El ajuste de texto se produce a nivel de las palabras y no de los caracteres. Por ejemplo, si hay una sola palabra que tiene más de aproximadamente 50 caracteres, esta no hará salto de línea y no habrá una barra de desplazamiento presente, por lo tanto el texto se cortará.
Texto de aviso legal	Este texto se muestra antes de que se permita al usuario iniciar sesión en el dispositivo. Por ejemplo: "Al hacer clic en Aceptar, acepta cumplir con la política de uso aceptable del equipo". Si no se introduce texto en este campo, no aparecerá ningún tipo de texto ni los botones Aceptar/Cancelar. El ajuste de texto se produce a nivel de las palabras y no de los caracteres. Por ejemplo, si hay una sola palabra que tiene más de aproximadamente 50 caracteres, esta no hará salto de línea y no habrá una barra de desplazamiento presente, por lo tanto el texto se cortará.

7 En la página de Resumen, haga clic en **Aplicar**.

8 Cuando se le solicite, haga clic en **Apagar**.

Es necesario un apagado completo antes de que pueda darse inicio al proceso de cifrado.

9 Después del apagado, reinicie el equipo.

La Autenticación será ahora administrada por Security Tools. Los usuarios deben iniciar sesión en la pantalla de Autenticación previa al inicio con sus contraseñas de Windows.

Cambiar cifrado y Configuración de la Autenticación previa al inicio

Una vez que primeramente se haya habilitado la función de cifrado y configuración de la Política de preinicio y Personalización, la pestaña Cifrado presentará las siguientes acciones como disponibles:

- Cambiar la Política de preinicio o Personalización: haga clic en la pestaña **Cifrado** y, a continuación, haga clic en **Cambiar**.
- Descifrar la SED, por ejemplo para la desinstalación: haga clic en **Descifrar**.

Una vez habilitados el cifrado y la configuración de la Política de preinicio y Personalización, la pestaña Configuración de preinicio presentará las siguientes acciones como disponibles:

- Cambiar la Política de preinicio o Personalización: haga clic en la pestaña **Configuración de preinicio** y seleccione **Personalización del preinicio** o **Políticas de inicio de sesión del preinicio**.

  Para obtener instrucciones sobre la desinstalación, consulte el apartado Tareas de desinstalación.

Configuración de las opciones de autenticación

Los controles de la pestaña Autenticación de la configuración del administrador le permiten definir opciones de inicio de sesión para los usuarios y personalizar la configuración de cada uno de ellos.

NOTA: La opción Contraseña de un solo uso no aparece en Opciones de recuperación si el TPM no está presente, con propietario ni habilitado.

Configuración de las opciones de inicio de sesión

En la página Opciones de inicio de sesión, puede configurar las políticas de inicio de sesión. De manera predeterminada, todas las credenciales admitidas aparecen en la lista de Opciones disponibles.

Para configurar las opciones de inicio de sesión:

1. En el panel izquierdo, en Autenticación, seleccione **Opciones de inicio de sesión**.
2. Para elegir el rol que desea definir, selecciónelo en la lista **Aplicar opciones de inicio de sesión a**: **Usuarios** o **Administradores**. Todos los cambios que realice en esta página se aplicarán únicamente a la función que haya seleccionado.
3. Defina las Opciones disponibles para la autenticación.

   De manera predeterminada, cada método de autenticación se configura para ser utilizado individualmente, no en combinación con otros métodos de autenticación. Puede cambiar los valores predeterminados de la siguiente manera:

   - Para especificar una combinación de opciones de autenticación, bajo Opciones disponibles haga clic en el icono para seleccionar el primer método de autenticación. En el cuadro de diálogo Opciones disponibles, seleccione el segundo método de autenticación y, a continuación, haga clic en **Aceptar**.

     Por ejemplo, puede solicitar una huella digital y una contraseña como credenciales de inicio de sesión. En el cuadro de diálogo, seleccione el segundo método de autenticación que se debe utilizar con la autenticación de huella digital.
   - Para permitir que cada método de autenticación pueda usarse individualmente, en el cuadro diálogo Opciones disponibles, establezca el segundo método de autenticación en **Ninguno** y haga clic en **Aceptar**.
   - Para eliminar una opción de inicio de sesión, en Opciones disponibles de la página Opciones de inicio de sesión, haga clic en **X** para eliminar este método.
   - Para agregar una nueva combinación de métodos de autenticación, haga clic en **Agregar una opción**.
4. Establezca las Opciones de recuperación para que los usuarios recuperen el acceso a sus equipos, en el caso de que estén bloqueados.

   - Para permitir que los usuarios definan un conjunto de preguntas y respuestas que puedan utilizar para recuperar el acceso al equipo, seleccione **Preguntas de recuperación**.

     Para evitar que se utilicen las Preguntas de recuperación, desactive la opción.
   - Para permitir que los usuarios recuperen el acceso mediante un dispositivo móvil, seleccione **Contraseña de un solo uso**. Cuando se selecciona la Contraseña de un solo uso (OTP) como un método de recuperación, no estará disponible como opción de inicio de sesión en la pantalla de inicio de sesión de Windows.

     Para utilizar la función OTP para el inicio de sesión, deseleccione la opción en Opciones de recuperación. Cuando se ha deseleccionado como método de recuperación, la opción OTP aparecerá en una página de inicio de Windows siempre que al menos se haya registrado un usuario en OTP.

NOTA: Como administrador, usted controla cómo utilizar la Contraseña de un solo uso, ya sea para la autenticación o para la recuperación. La función OTP se puede utilizar para la autenticación o la recuperación, pero no para ambas cosas. La configuración afectará a todos los usuarios del equipo o a todos los administradores, en función de la selección en el campo Opciones de inicio de sesión, **Aplicar opciones de inicio de sesión a**.

Si la opción de Contraseña de un solo uso no aparece en la lista, la configuración de su equipo no la admite. Para obtener más información, consulte Requisitos.

- Para solicitar al usuario que haga una llamada al soporte técnico si pierde u olvida las credenciales de inicio de sesión, desactive Preguntas de recuperación y Contraseña de un solo uso.

5 Para establecer un período de tiempo durante el que los usuarios puedan registrar sus credenciales de autenticación, seleccione **Período de gracia**.

La función Período de gracia le permite establecer la fecha en la que se empezará a hacer cumplir la Opción de inicio de sesión configurada. Puede configurar una Opción de inicio de sesión antes de la fecha en la que se hará cumplir y establecer un período de tiempo durante el que puedan registrarse los usuarios. De forma predeterminada, la política se hace cumplir inmediatamente.

Para cambiar la fecha en la que se hará cumplir la Opción de inicio de sesión de *Inmediatamente* a otra opción, vaya al cuadro de diálogo Período de gracia y haga clic en el menú desplegable para seleccionar **Fecha especificada**. Haga clic en la flecha abajo situada en el lateral derecho del campo de la fecha para mostrar un calendario y, a continuación, seleccione la fecha en el calendario. La aplicación de la política comienza aproximadamente a las 00:01 en la fecha seleccionada.

A los usuarios se les puede recordar que registren las credenciales que serán necesarias en su próximo inicio de sesión de Windows (de manera predeterminada), o puede especificar recordatorios periódicos. Seleccione el intervalo de aviso desde la lista desplegable *Recordar al usuario*.

NOTA: Al activarse, el recordatorio que se muestra al usuario en la pantalla de inicio de sesión o en una sesión de Windows es ligeramente diferente. Los recordatorios no aparecen en las pantallas de inicio de sesión de Autenticación previa al inicio.

Funcionalidad durante el período de gracia

Durante un Período de gracia determinado, después de cada inicio de sesión, la notificación Credenciales adicionales se mostrará cuando el usuario aún no esté registrado con las credenciales mínimas necesarias para cumplir con la Opción de inicio de sesión que haya cambiado. El contenido del mensaje es: *Se encuentran disponibles credenciales adicionales para el registro.*

Si hay credenciales adicionales disponibles que no son necesarias, el mensaje aparece solo una vez después de modificar la política.

Hacer clic en la notificación tiene los siguientes efectos, según el contexto:

- Si no se han registrado credenciales, aparecerá el asistente de Configuración, lo que permite a los Usuarios administrativos configurar los valores relacionados con el equipo, y ofrece a los usuarios la posibilidad de registrar las credenciales más comunes.
- Después del registro de credenciales inicial, al hacer clic en la notificación aparecerá el asistente de Configuración dentro de la DDP Security Console.

Funcionalidad posterior al vencimiento del período de gracia

En todos los casos, una vez vencido el Período de gracia, los usuarios no podrán iniciar sesión si no han registrado las credenciales que exige la Opción de inicio de sesión. Si un usuario intenta iniciar sesión con una credencial o combinación de credenciales que no cumplan con la Opción de inicio de sesión, el asistente de Configuración aparece en la parte superior de la pantalla de inicio de sesión de Windows.

- Si el usuario registra con éxito las credenciales necesarias, podrá iniciar sesión en Windows.
- Si un usuario no registra correctamente las credenciales necesarias o cancela el asistente, será llevado de nuevo a la pantalla de inicio de sesión en Windows.

6 Para guardar la configuración de la función seleccionada, haga clic en **Aplicar**.

Configuración de la autenticación en Password Manager

En la página de Password Manager, puede configurar la manera en la que los usuarios se autentican en Password Manager.

Para configurar la autenticación en Password Manager:

1 En el panel izquierdo, en Autenticación, seleccione **Password Manager**.

2 Para elegir el rol que desea definir, selecciónelo en la lista **Aplicar opciones de inicio de sesión a**: **Usuarios** o **Administradores**. Todos los cambios que realice en esta página se aplicarán únicamente a la función que haya seleccionado.

3 De manera opcional, seleccione la casilla de verificación **No requerir autenticación** para dejar que el rol del usuario seleccionado inicie sesión automáticamente en todas las aplicaciones de software y sitios web de Internet con credenciales guardadas en Password Manager.

4 Defina las Opciones disponibles para la autenticación.

De manera predeterminada, cada método de autenticación se configura para ser utilizado individualmente, no en combinación con otros métodos de autenticación. Puede cambiar los valores predeterminados de la siguiente manera:

- Para especificar una combinación de opciones de autenticación, bajo Opciones disponibles haga clic en el icono para seleccionar el primer método de autenticación. En el cuadro de diálogo Opciones disponibles, seleccione el segundo método de autenticación y, a continuación, haga clic en **Aceptar**.

  Por ejemplo, puede solicitar una huella digital y una contraseña como credenciales de inicio de sesión. En el cuadro de diálogo, seleccione el segundo método de autenticación que se debe utilizar con la autenticación de huella digital.

- Para permitir que cada método de autenticación pueda usarse individualmente, en el cuadro diálogo Opciones disponibles, establezca el segundo método de autenticación en **Ninguno** y haga clic en **Aceptar**.
- Para eliminar una opción de inicio de sesión, en Opciones disponibles de la página Opciones de inicio de sesión, haga clic en **X** para eliminar este método.
- Para agregar una nueva combinación de métodos de autenticación, haga clic en **Agregar una opción**.

5 Para guardar la configuración de la función seleccionada, haga clic en **Aplicar.**

NOTA: Seleccione el botón Valores predeterminados para restaurar la configuración a sus valores originales.

Configuración de preguntas de recuperación

En la página Preguntas de recuperación, puede seleccionar las preguntas que se presentarán a los usuarios cuando definan las Preguntas de recuperación personales y las respuestas. Las Preguntas de recuperación permiten a los usuarios recuperar el acceso a sus equipos si las contraseñas han caducado o se han olvidado.

Para configurar las preguntas de recuperación:

1. En el panel izquierdo, en Autenticación, seleccione **Preguntas de recuperación**.
2. En la página Preguntas de recuperación, seleccione, como mínimo, tres Preguntas de recuperación predefinidas.
3. De manera opcional, puede agregar hasta tres preguntas personalizadas a la lista de selección para el usuario.
4. Para guardar las Preguntas de recuperación, haga clic en **Aplicar**.

Configuración de la autenticación mediante lectura de huellas digitales

Para configurar la autenticación mediante lectura de huellas digitales:

1. En el panel izquierdo, bajo **Autenticación,** seleccione **Huellas digitales**.
2. En Registros, defina el número mínimo y máximo de huellas digitales que el usuario puede registrar.
3. Defina la sensibilidad de la lectura de huella digital.

   Una baja sensibilidad admite una desviación más alta y aumenta las probabilidades de aceptar una lectura falsa. En la configuración más alta, el sistema puede rechazar huellas digitales legítimas. La configuración de Más sensibilidad baja el índice de aceptaciones de lecturas falsas a 1 en 10 000.
4. Haga clic en **Borrar lector** para eliminar todas las lecturas de huellas y registros de credenciales del búfer del lector de huellas digitales De esta manera solamente se eliminan datos que actualmente se están agregando. No elimina lecturas y registros almacenados de sesiones previas.
5. Para guardar los valores de configuración, haga clic en **Aplicar**.

Configuración de autenticación mediante contraseña de un solo uso

Para utilizar la función Contraseña de un solo uso, el usuario genera una contraseña de un solo uso con la aplicación Dell Data Protection | Security Tools Mobile en su dispositivo móvil y, a continuación, introduce la contraseña en el equipo. La contraseña solo se puede utilizar una vez y solo es válida durante un periodo de tiempo limitado.

Para mejorar más la seguridad, el administrador puede garantizar que la aplicación móvil es segura solicitando un PIN.

En la página Dispositivo móvil, puede configurar los valores que mejoran la seguridad del dispositivo móvil y de la Contraseña de un solo uso.

Para configurar la autenticación mediante la Contraseña de un solo uso:

1. En el panel izquierdo, en Autenticación, seleccione **Dispositivo móvil**.
2. Para solicitar al usuario que introduzca un PIN para acceder a la aplicación Security Tools Mobile en el dispositivo móvil, seleccione **Solicitar PIN**.

NOTA: Si se habilita la política *Solicitar PIN* después de que los dispositivos móviles se hayan registrado con un equipo, se cancelará el registro de dichos dispositivos móviles. Se solicitará a los usuarios que vuelvan a registrar sus dispositivos móviles una vez que se haya habilitado la política.

Cuando la casilla de verificación **Solicitar PIN** esté seleccionada, los usuarios deberán desbloquear su dispositivo móvil para acceder a la aplicación Security Tools Mobile. Si el dispositivo móvil no cuenta con un bloqueo de dispositivo, será necesario un PIN.

3. Para seleccionar la longitud de la Contraseña de un solo uso (OTP), en **Longitud de la contraseña de un solo uso**, seleccione el número de caracteres de la contraseña que se necesitan.
4. Para seleccionar el número de intentos que el usuario tiene hasta introducir la Contraseña de un solo uso correctamente, seleccione un número del 5 al 30 en **Intentos de inicio de sesión del usuario permitidos**.

   Cuando se ha alcanzado el número máximos de intentos, se deshabilitará la función OTP hasta que el usuario vuelva a registrar el dispositivo móvil.

PRÁCTICA RECOMENDADA: Dell recomienda la configuración de al menos otro método de autenticación además de la Contraseña de un solo uso.

Configuración del registro de tarjetas inteligentes

DDP|Security Tools es compatible con dos tipos de tarjetas inteligentes: con contacto y sin contacto.

Las tarjetas con contacto requieren un lector de tarjeta inteligente donde se introducirá la tarjeta. Las tarjetas con contacto son solamente compatibles con equipos de dominio. Las tarjetas CAC y SIPRNet son ambas tarjetas con contacto. Debido a la naturaleza avanzada de estas tarjetas, el usuario necesitará escoger un certificado después de introducir su tarjeta para iniciar sesión.

- Las tarjetas sin contacto son compatibles con equipos que no pertenecen a un dominio y con equipos configurados con especificaciones de dominio.
- Los usuarios pueden registrar una tarjeta inteligente con contacto por cuenta de usuario, o varias tarjetas sin contacto por cuenta.
- Las tarjetas inteligentes no son compatibles con la Autenticación previa al inicio.

NOTA: Al eliminar el registro de una tarjeta inteligente de una cuenta con varias tarjetas registradas, se anulará el registro de todas las tarjetas al mismo tiempo.

Para configurar el registro de tarjetas inteligentes

1. En la pestaña de Autenticación de la herramienta Configuración del administrador, seleccione **Tarjeta inteligente**.

Configuración de permisos avanzados

1. Haga clic en **Avanzado** para modificar las opciones de usuario final avanzadas. En *Avanzado*, puede permitir de manera opcional a los usuarios el registro automático de credenciales o permitir a los usuarios que modifiquen sus credenciales registradas y habilitar el inicio de sesión en un paso.
2. Active o desactive las siguientes casillas de verificación:

   Permitir a los usuarios registrar credenciales: esta casilla de verificación está activada por defecto. Se permite a los usuarios registrar credenciales sin la intervención de un administrador. Si desmarca la casilla de verificación, el administrador será el encargado de registrar las credenciales.

   Permitir a los usuarios modificar sus credenciales registradas: de manera predeterminada, se selecciona la casilla de verificación. Cuando está seleccionada, se permite a los usuarios modificar o eliminar sus credenciales registradas sin la intervención de un administrador. Si desmarca la casilla de verificación, las credenciales no podrán ser modificadas ni eliminadas por un usuario normal. Deberá modificarlas o eliminarlas el administrador.

NOTA: Para registrar las credenciales de un usuario, vaya a la página *Usuarios* de la herramienta Configuración del administrador, seleccione un usuario y haga clic en **Registrar**.

   Permitir inicio de sesión de un solo paso: el inicio de sesión de un solo paso es un Inicio de sesión único (SSO). De manera predeterminada, se selecciona la casilla de verificación. Cuando esta función está habilitada, los usuarios deben introducir sus credenciales solamente en la pantalla Autenticación previa al inicio. Los usuarios inician sesión en Windows automáticamente. Si desmarca la casilla de verificación, el usuario tendrá que iniciar sesión varias veces.

NOTA: Esta opción no se puede seleccionar a menos que se seleccione también el valor **Permitir a los usuarios registrar credenciales**.

3. Haga clic en **Aplicar** cuando termine.

Servicios biométricos y de tarjetas inteligentes (opcional)

Si no desea que Security Tools cambie los servicios asociados con los dispositivos biométricos y las tarjetas inteligentes a un inicio "automático", entonces se puede deshabilitar la función de inicio de servicios.

Cuando esté deshabilitado, Security Tools no tratará de iniciar estos tres servicios:

- SCardSvr: administra el acceso a las tarjetas inteligentes leídas por el equipo. Si el servicio se detiene, el equipo no podrá leer tarjetas inteligentes. Si el servicio se deshabilita, no podrán iniciarse los servicios que dependan explícitamente de él.
- SCPolicySvc: permite que el sistema se configure para bloquear el escritorio del usuario cuando se retire la tarjeta inteligente.
- WbioSrvc: el servicio biométrico de Windows otorga a las aplicaciones de cliente la capacidad de capturar, comparar, manipular y almacenar datos biométricos sin obtener acceso directo a ningún hardware o muestras biométricos. El servicio está alojado en un proceso SVCHOST privilegiado.

La deshabilitación de esta función también suprime los avisos asociados con el mal funcionamiento de los servicios necesarios.

Deshabilitación del inicio automático de servicios

De manera predeterminada, si la clave de registro no existe o si el valor está establecido en 0, se habilita esta función.

1. Ejecute **Regedit**.
2. Busque la siguiente entrada de registro:

   [HKEY_LOCAL_MACHINE\SOFTWARE\DELL\Dell Data Protection]

   SmartCardServiceCheck=REG_DWORD:0

   Establezca en 0 para habilitar.
   Establezca en 1 para deshabilitar.

Administración de la autenticación de usuarios

Los controles en la pestaña de Autenticación de la Configuración del administrador le permiten establecer opciones para el inicio de sesión del usuario y personalizar la configuración de cada uno.

Para administrar la autenticación de usuarios:

1. Como administrador, haga clic en el mosaico **Configuración del administrador**.
2. Haga clic en la pestaña **Usuarios** para administrar usuarios y ver el estado del registros de los usuarios. Desde esta pestaña, puede:
   - Registrar nuevos usuarios
   - Agregar o modificar credenciales
   - Quitar las credenciales de un usuario

NOTA: Inicio de sesión y **Sesión** muestran el estado de registro de un usuario.

Cuando el estado **Inicio de sesión** aparece como **OK**, significa que se han realizado todos los registros que el usuario necesita para poder iniciar sesión.
Cuando el estado **Sesión** aparece como **OK**, significa que se han realizado todos los registros que el usuario necesita para utilizar el Password Manager.

Si alguno de estos dos estados aparece como **No**, el usuario tendrá que realizar más registros. Para saber qué registros faltan, seleccione la herramienta **Configuración de administrador** y abra la pestaña **Usuarios.** Cuando hay casillas que tienen una marca de verificación gris, significa que hay registros que están incompletos. Como alternativa, haga clic en el mosaico **Registros** y revise la columna **Política** de la pestaña **Estado**, en la que se indican los registros necesarios.

Cómo agregar nuevos usuarios

NOTA: Los nuevos usuarios de Windows se agregan automáticamente cuando inician sesión en Windows o registran credenciales.

1. Haga clic en **Agregar usuario** para iniciar el proceso de registro para un usuario de Windows existente.
2. Cuando se muestre el cuadro de diálogo *Seleccionar usuario*, seleccione **Tipos de objeto.**
3. Introduzca un nombre de objeto de usuario en el cuadro de texto y haga clic en **Comprobar nombres**.
4. Haga clic en **Aceptar** cuando termine.

   Se abre el Asistente de registro.

   Vaya a Registro o cambio de las credenciales del usuario para obtener instrucciones.

Registro o cambio de las credenciales del usuario

El administrador puede registrar o cambiar las credenciales de un usuario en nombre del usuario, pero algunas actividades de registro requieren la presencia del usuario; por ejemplo, para responder a las preguntas de recuperación y leer las huellas digitales del usuario.

Para registrar o cambiar las credenciales de un usuario:

1. En Configuración del administrador, haga clic en la pestaña **Usuarios**.
2. En la página Usuarios, haga clic en **Registrar**.
3. En la página de Bienvenida, haga clic en **Siguiente**.
4. En el cuadro de diálogo Se requiere autenticación, inicie sesión con la contraseña de Windows del usuario, y haga clic en **Aceptar**.

5 En la página Contraseña, para cambiar la contraseña de Windows del usuario, introduzca y confirme la nueva contraseña y haga clic en **Siguiente**.

   Si no desea cambiar la contraseña, haga clic en **Omitir**. El asistente le permite omitir una credencial si no desea registrarla. Para volver a la página, haga clic en **Atrás**.

6 Siga las instrucciones de cada página y haga clic en el botón correspondiente: **Siguiente**, **Omitir** o **Atrás**.

7 En la página de Resumen, confirme las credenciales registradas y, cuando se haya terminado con el proceso de registro, haga clic en **Aplicar**.

   Para volver a la página de registro de credenciales para hacer un cambio, haga clic en **Atrás** hasta llegar a la página que desea cambiar.

Para obtener información más detallada sobre cómo registrar o cambiar una credencial, consulte la *Dell Data Protection | Console User Guide* (Guía del usuario de Dell Data Protection | Console).

Cómo quitar una credencial registrada

1 Haga clic en el mosaico **Configuración de administrador**.

2 Haga clic en la pestaña **Usuarios** y busque el usuario que desea cambiar.

3 Desplácese sobre la marca de verificación verde de la credencial que desea eliminar. Se convierte en ⊗.

4 Haga clic en el símbolo ⊗ y, a continuación, haga clic en **Sí** para confirmar la eliminación.

NOTA: No es posible eliminar una credencial de este modo si es la única credencial registrada que tiene el usuario. Además, no es posible eliminar la contraseña de este modo. Utilice el comando Quitar para eliminar completamente el acceso de un usuario al equipo.

Cómo quitar todas las credenciales registradas de un usuario

1 Haga clic en el mosaico **Configuración de administrador**.

2 Haga clic en la pestaña **Usuarios** y busque el usuario que desea eliminar.

3 Haga clic en **Quitar**. (El comando Quitar aparece en rojo en la parte inferior de la configuración del usuario).

Tras la eliminación, el usuario no podrá iniciar sesión en el equipo a menos que se vuelva a registrar.

5

Tareas de desinstalación

Para desinstalar DDP|ST, debe ser como mínimo un usuario **Administrador local**.

Desinstalación de DDP|ST

Debe desinstalar las aplicaciones en este orden:

1. DDP | Client Security Framework
2. DDP | Security Tools Authentication
3. DDP | Security Tools

Si tiene un equipo con una unidad de cifrado automático, siga las siguientes instrucciones para desinstalar:

1. Desaprovisione la SED:
   a. En Configuración del administrador > haga clic en la pestaña **Cifrado**.
   b. Haga clic en **Descifrar** para deshabilitar el cifrado.
   c. Una vez descifrada la SED, reinicie el equipo.
2. En el Panel de control de Windows, vaya a **Desinstalar un programa**.

NOTA: Inicio > Panel de control > Programas y características > Desinstalar un programa.

3. Desinstale **Client Security Framework** y reinicie el equipo.
4. Desde el Panel de control de Windows, desinstale **Security Tools Authentication**.
   Aparece un mensaje que le pregunta si desea conservar los datos de usuario.
   Haga clic en **Sí** si su intención es volver a instalar Security Tools. En caso contrario, haga clic en **No**.
   Una vez finalizada la desinstalación, reinicie el equipo.
5. Desde el Panel de control de Windows, desinstale **Security Tools**.
   Aparece un mensaje que le pregunta si desea desinstalar completamente esta aplicación y sus componentes.
   Haga clic en **Sí**.
   Aparece el cuadro de diálogo *Desinstalación completada*.
6. Haga clic en **Sí, deseo reiniciar ahora mi equipo** y, a continuación, haga clic en **Finalizar**.
7. El equipo se reinicia y finaliza la desinstalación.

6

Recuperación

Hay opciones de recuperación disponibles en caso de que caduquen o se pierdan las credenciales:

- **Contraseña de un solo uso (OTP):** El usuario genera una OTP con la aplicación Security Tools Mobile en un dispositivo móvil registrado e introduce la OTP en la pantalla de inicio de sesión de Windows para recuperar acceso. Esta opción está disponible solo si el usuario ha registrado un dispositivo móvil con Security Tools en el equipo. Para utilizar la función OTP para la recuperación, el usuario no puede haber utilizado la OTP para iniciar sesión en el equipo.

NOTA: La característica Contraseña de un solo uso (OTP) requiere que el TPM esté presente, habilitado y con propietario. Siga las instrucciones descritas en Borrar la propiedad y activar el TPM.
Se puede utilizar la OTP para la autenticación o la recuperación, pero no para ambas cosas. Para obtener detalles, consulte Configuración de las opciones de inicio de sesión.

- **Preguntas de recuperación:** El usuario responde correctamente a varias preguntas personales para recuperar el acceso al equipo. Esta opción solo está disponible si el administrador ha configurado y habilitado las Preguntas de recuperación y si el usuario ha registrado las Preguntas de recuperación. Esta opción se puede utilizar para recuperar acceso al equipo mediante la pantalla de Autenticación previa al inicio y la pantalla de inicio de sesión de Windows.

Ambos métodos de recuperación requieren que se haya preparado para la recuperación, registrando las Preguntas de recuperación o un dispositivo móvil con Security Tools en el equipo.

Recuperación automática, Preguntas de recuperación de inicio de sesión de Windows

Para responder a las Preguntas de recuperación para recuperar acceso a la pantalla de inicio de sesión de Windows:

1. Para utilizar las Preguntas de recuperación, haga clic en **¿No puede acceder a su cuenta?**

   Se muestran las Preguntas de recuperación que seleccionó durante el registro.

2. Introduzca las respuestas y haga clic en **Aceptar**.

   Tras introducir correctamente las respuestas a las preguntas, entrará en el modo de Recuperación de acceso. Lo que suceda a continuación dependerá de la credencial que haya fallado.

   - Si no ha introducido la contraseña de Windows correcta, aparecerá la pantalla de cambio de contraseña.
   - Si no se ha reconocido una huella digital, aparecerá la página de registro de huellas digitales para que pueda volver a registrar la huella digital.

Recuperación automática, Preguntas de recuperación de PBA

Para responder a las Preguntas de recuperación para recuperar acceso a la pantalla de Autenticación previa al inicio:

1. En la pantalla de Autenticación previa al inicio, introduzca su nombre.
2. En la esquina inferior izquierda de la pantalla, seleccione **Opciones**.
3. En el menú Opciones, seleccione **¿Olvidó la contraseña?**
4. Responda las Preguntas de recuperación y haga clic en **Iniciar sesión**.

Recuperación automática, Contraseña de un solo uso

Este procedimiento describe cómo utilizar la función de Contraseña de un solo uso (OTP) para recuperar acceso al equipo si, por ejemplo, la contraseña de Windows ha caducado o se ha olvidado o se ha superado el número máximo de intentos de inicio de sesión permitidos. La opción de Contraseña de un solo uso (OTP) está disponible solo si el usuario ha registrado el dispositivo móvil y si no se utilizó la OTP la última vez que inició sesión en Windows.

NOTA: La característica Contraseña de un solo uso requiere que el TPM esté presente, habilitado y con propietario. Se puede utilizar la OTP para la autenticación de Windows o la recuperación, pero no para ambas cosas. El administrador puede establecer una política para permitir la OTP para la recuperación o la autenticación o puede deshabilitar la función.

Para utilizar la OTP para recuperar acceso al equipo:

1. Seleccione el icono de OTP en la pantalla de inicio de sesión de Windows.
2. En el dispositivo móvil, abra la aplicación Security Tools Mobile e introduzca el PIN.
3. Seleccione el equipo al que desea acceder.

   Si el nombre del equipo no aparece en el dispositivo móvil, es posible que se deba a una de las siguientes situaciones:

   - El dispositivo móvil no está registrado o asociado con el equipo al que está intentando acceder.
   - Si tiene más de una cuenta de usuario de Windows, puede ser que DDP | Security Tools no esté instalado en el equipo al que intenta acceder o bien que está intentando iniciar sesión en una cuenta de usuario que no es la misma que se utilizó para asociar el equipo y el dispositivo móvil.
4. Presione **Contraseña de un solo uso**.

   Aparece una contraseña en la pantalla del dispositivo móvil.

   NOTA: Si es necesario, haga clic en el símbolo Actualizar para obtener un nuevo código. Después de las dos primeras actualizaciones de OTP, habrá un retraso de treinta segundos antes de que se genere otra OTP.
   El equipo y el dispositivo móvil deben estar sincronizados para que ambos puedan reconocer la misma contraseña al mismo tiempo. Intentar generar rápidamente contraseña tras contraseña hará que el equipo y el dispositivo móvil pierdan la sincronización y que falle la función OTP. Si se produjera este problema, espere treinta segundos para que los dos dispositivos vuelvan a sincronizarse y, a continuación, vuelva a intentarlo.
5. En el equipo, en la pantalla de inicio de sesión de Windows, escriba la contraseña que se muestra en el dispositivo móvil y presione **Intro**.
6. En el equipo, en la pantalla Modo de recuperación, seleccione **He olvidado mi contraseña de Windows** y siga las instrucciones que se muestran en pantalla para restablecer su contraseña.

Glosario

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.

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

Desaprovisionamiento: el desaprovisionamiento elimina la base de datos de PBA y desactiva la PBA. Para que un desaprovisionamiento entre en vigor, hay que reiniciar el equipo.

Inicio de sesión único (SSO): el Inicio de sesión único simplifica el proceso de inicio de sesión cuando está habilitada la autenticación multifactor tanto en la Autenticación previa al inicio como en el 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. DDP|E utiliza el TPM por su función de almacenamiento seguro. El TPM también sirve para proporcionar contenedores cifrados al almacén de software de DDP|E y para proteger la clave de cifrado del HCA de DDP|E. Dell recomienda el aprovisionamiento del TPM. El TPM es necesario para el HCA de DDP|E y la función de Contraseña de un solo uso.


0XXXXXA0X