

Configuración de las propiedades seguras de los datos vulnerables (SSD) en el Switches manejado 200/300 Series

Objetivo

Los datos vulnerables seguros (SSD) protegen la información vulnerable tal como contraseñas, permiten o niegan el acceso de usuarios a los datos vulnerables, y evitan que los archivos de configuración sean corrompidos por los usuarios malintencionados. El SSD utiliza las frases de contraseña a los datos seguros. Las frases de contraseña son similares a una contraseña que se salve en el Switch y se utilice como clave de encriptación. Los dispositivos que no conocen el passphrase no podrán a los datos del unencrypt que utilizan el passphrase.

El objetivo de este documento es explicar las características disponibles en la página de las *propiedades SSD*.

Dispositivos aplicables

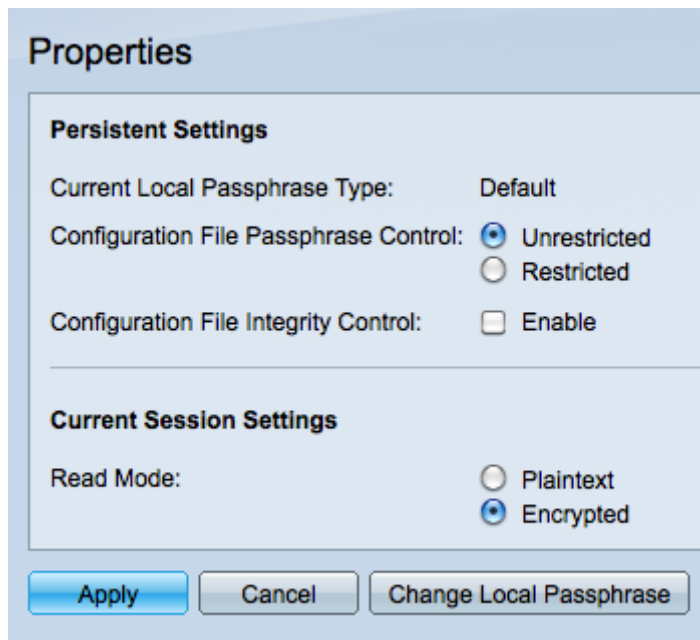
- Switches manejado 300 Series SF/SG 200 y SF/SG

Versión del software

- 1.3.0.62

Configuración de las propiedades SSD

Paso 1. Inicie sesión a la utilidad de configuración de la red y elija la **Seguridad > Administración > las propiedades seguras de datos vulnerables**. La página de las *propiedades* se abre:



Nota: El control local actual del passphrase describe si el dispositivo utiliza el passphrase predeterminado o un passphrase definido por el usuario.

Paso 2. Haga clic el botón de radio deseado en el *Campo de control del passphrase del archivo de configuración*.

- Sin restricción — Envía el passphrase en el archivo de configuración, que permite que los otros dispositivos conozcan el passphrase.
- Restringido — Restringe el passphrase del envío en el archivo de configuración, que guarda los otros dispositivos de aprender el passphrase.

Paso 3. Marque la casilla de verificación del control de la integridad del archivo de configuración para habilitar la protección contra las modificaciones indeseadas al archivo de configuración.

Paso 4. Haga clic el botón de radio deseado en el *campo modo leído* para fijar cómo se lee el archivo.

- Texto simple — Utiliza el texto simple para mostrar la información de sesión en curso.
- Cifrado — Cifra el archivo antes de que muestre la información de la sesión.

Paso 5. El teclado **se aplica** para guardar los cambios o la **cancelación** actuales para deshacer los cambios realizados dentro de la página.

Cambie el passphrase local

Paso 1. Inicie sesión a la utilidad de configuración de la red y elija la **Seguridad > Administración > las propiedades seguras de datos vulnerables**. Haga clic el **passphrase del Local del cambio**. La página *local del passphrase del cambio* se abre:

Nota: El tipo local actual del passphrase describe qué passphrase es funcionando.

Paso 2. Haga clic el botón de radio deseado del campo *local del passphrase*.

- Valor por defecto — Utiliza el passphrase predeterminado.
- Definido por el usuario — El usuario define se utiliza qué passphrase.

Paso 3. Si es definido por el usuario fue hecho clic, ingresan el passphrase deseado en el campo, y después ingresan el mismo passphrase en el campo de *contraseña del confirmar*.

Paso 4. Elija **se aplican** para mantener los cambios realizados o **cancelación** para deshacer todos los cambios en esto página.

Paso 5. Elija **de nuevo a la** vuelta a la página de las *propiedades*.