Asegure las propiedades de los datos vulnerables (SSD) en los switches para pila de las Sx500 Series

Objetivo

Utilizan a la Administración segura de los datos vulnerables (SSD) para manejar los datos vulnerables tales como contraseñas y claves con seguridad en el Switch. Esta información debe ser asegurada cuando se envía a partir de un dispositivo a otro dispositivo. El nivel de acceso del usuario determina cómo los datos vulnerables se pueden ver, como el plaintext o datos encriptados. Las propiedades SSD son un conjunto de parámetros conjuntamente con las reglas SSD que controlan las configuraciones tales como cómo se cifran los datos vulnerables, la fuerza de la Seguridad en los archivos de configuración, y cómo los datos vulnerables se ven dentro de la sesión en curso.

El objetivo de este documento es ayudar a configurar las propiedades seguras de los datos vulnerables (SSD) en los switches para pila de las Sx500 Series.

Dispositivos aplicables

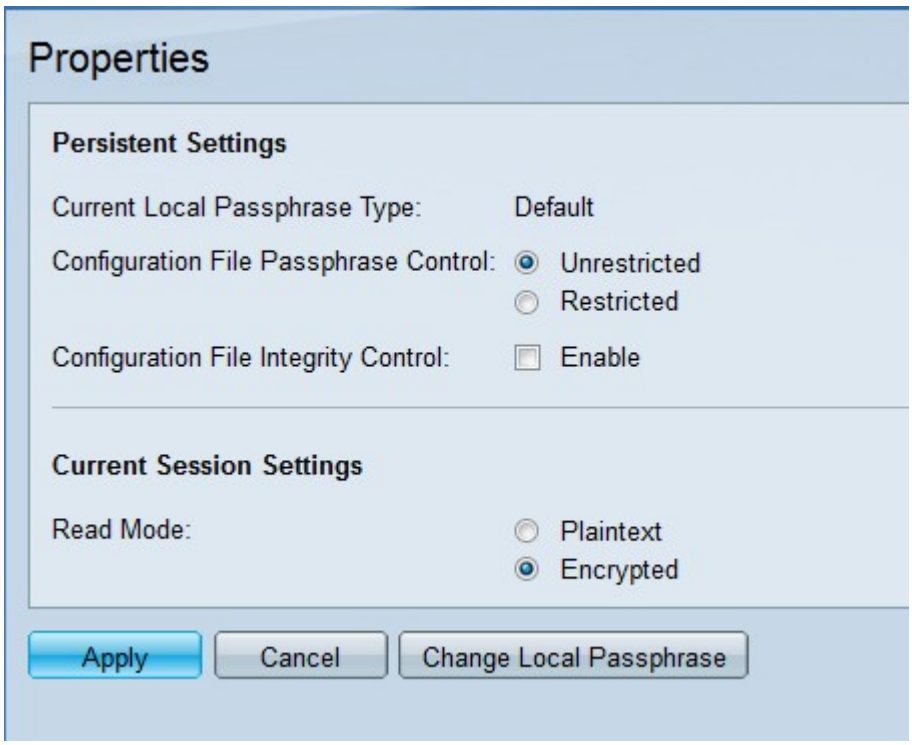
- Switches para pila de las Sx500 Series

Versión del software

- 1.3.0.62

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 campo local actual del tipo del passphrase visualiza el tipo de passphrase local fijado inicialmente.

Paso 2. En el Campo de control del passphrase del archivo de configuración, haga clic el botón de radio del tipo deseado de control del passphrase. El control del passphrase del archivo da la protección adicional al passphrase definido por el usario y a los datos cifrados con el passphrase definido por el usario.

- Sin restricción — El passphrase definido por el usario se incluye en el archivo de configuración que se envía a partir de un dispositivo a otro.
- Restricto — El passphrase definido por el usario no se incluye en el archivo de configuración.

El paso 3. (opcional) para habilitar el control de la integridad del archivo, marca la casilla de verificación del **permiso** en el Campo de control de la integridad del archivo de configuración. Esta opción protege el archivo de configuración contra la modificación.

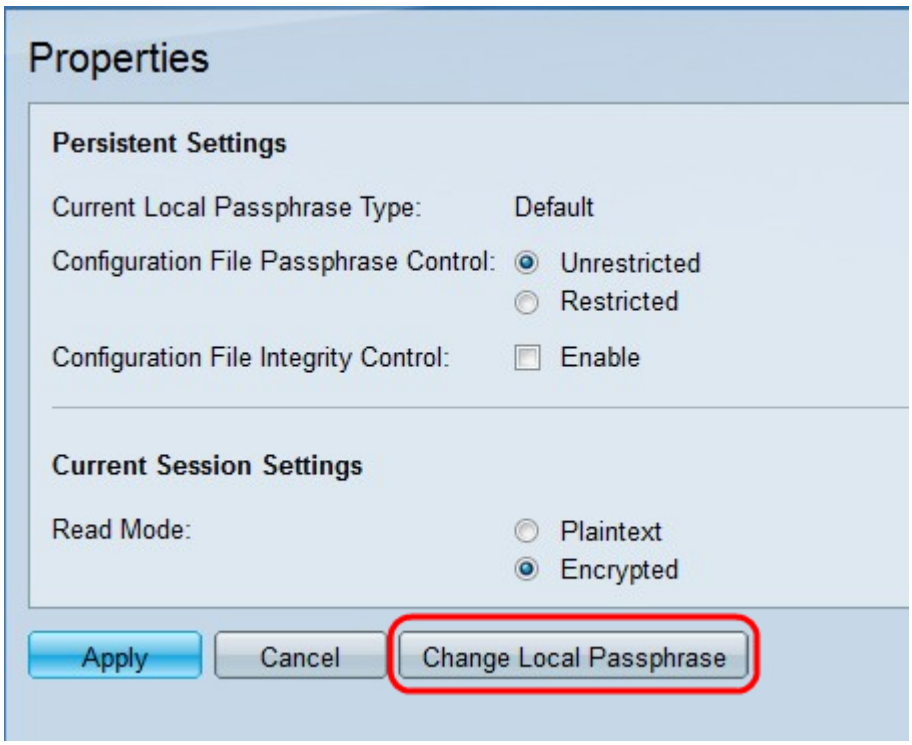
Paso 4. En el campo modo leído, haga clic el botón de radio deseado. Las opciones disponibles son:

- Texto simple — Los datos vulnerables se visualizan como texto simple.
- Cifrado — Los datos se visualizan en la forma encriptada.

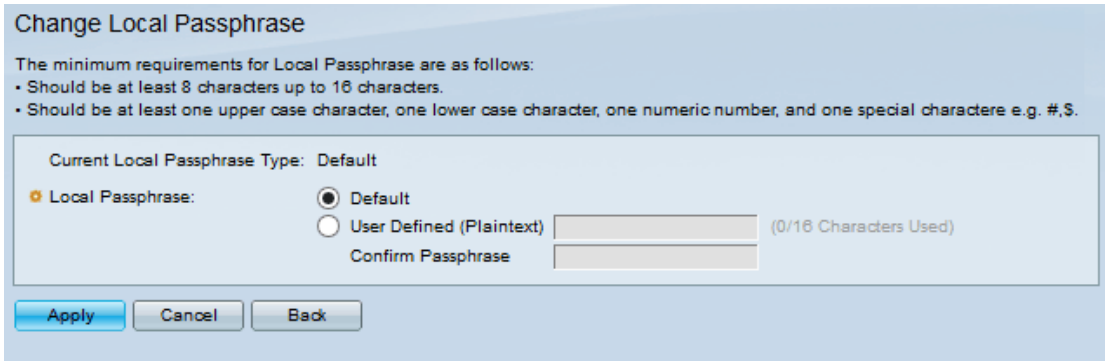
Paso 5. El tecleo **se aplica**.

Cambie el passphrase local

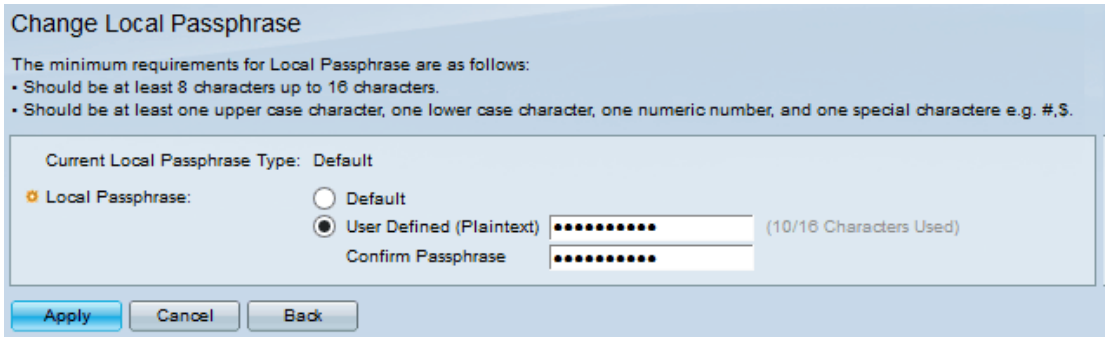
Paso 1. Inicie sesión a la utilidad de configuración de la red y elija la **Seguridad > Administración > las propiedades seguras de datos vulnerables.** La página de las *propiedades* se abre**:**



Paso 2. **Passphrase local del cambio del** tecleo para cambiar el passphrase local actual. La página *local del passphrase del cambio* se abre:



Nota: El campo local actual del tipo del passphrase visualiza el passphrase local actual.



Paso 3. En el campo local del passphrase, haga clic el botón de radio del passphrase local deseado:

- Valor por defecto — Esto asigna el passphrase predeterminado.
- Definido por el usario (Plaintext) — Ingrese el passphrase deseado. Debe estar entre 8 y 16 caracteres e incluir el mayúscula y los caracteres en minúscula, un número, y un carácter especial.

– Confirme el passphrase — Entre el passphrase de nuevo definido por el usario.

Paso 4. El tecleo **se aplica**.