Configuration of the Secure Sensitive Data (SSD) Properties on 200/300 Series Managed Switches

Objective

Secure Sensitive Data (SSD) protects sensitive information such as passwords, allows or denies users access to sensitive data, and prevents configuration files from being corrupted by malicious users. SSD utilizes passphrases to secure data. Passphrases are similar to a password that is stored in the switch and used as an encryption key. Devices that do not know the passphrase will not be able to unencrypt data that uses the passphrase.

The objective of this document is to explain the features available in the *SSD Properties* page.

Applicable Devices

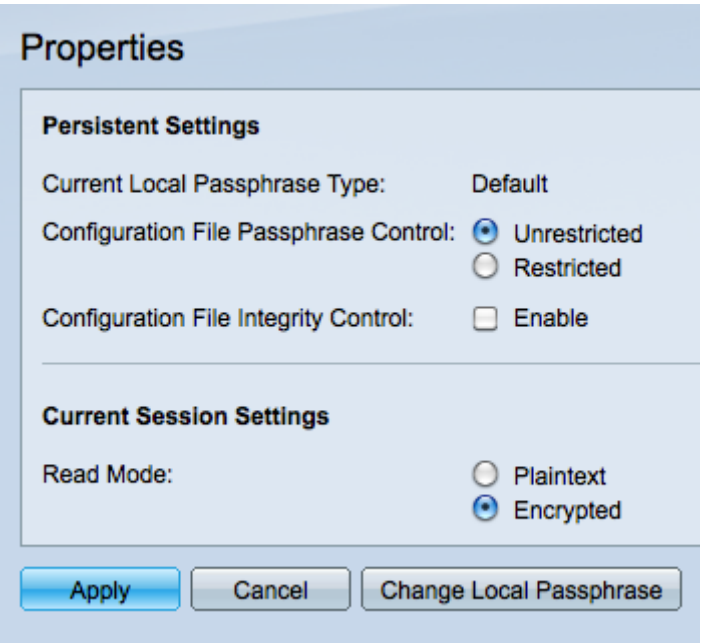
- SF/SG 200 and SF/SG 300 Series Managed Switches

Software Version

- 1.3.0.62

Configuration of the SSD Properties

Step 1. Log in to the web configuration utility and choose **Security** > **Secure Sensitive Data Management** > **Properties**. The *Properties* page opens:



Note: The Current Local Passphrase Control describes whether the device uses the default passphrase or a user defined passphrase.

Step 2. Click the desired radio button in the *Configuration File Passphrase Control* field.

- Unrestricted — Sends the passphrase into the configuration file, which allows other devices to know the passphrase.
- Restricted — Restricts the passphrase from being sent into the configuration file, which keeps other devices from learning the passphrase.

Step 3. Check the Configuration File Integrity Control check box to enable protection from unwanted modifications to the configuration file.

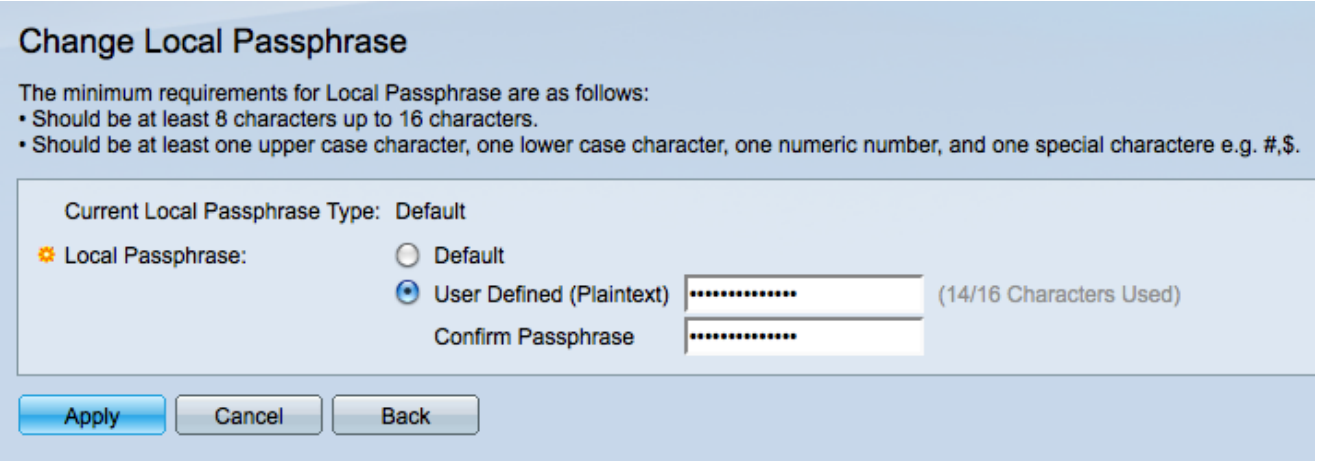
Step 4. Click the desired radio button in the *Read Mode* field to set how the file is read.

- Plaintext — Uses plaintext to show the current session information.
- Encrypted — Encrypts the file before it shows the session information.

Step 5. Click **Apply** to keep the current changes or **Cancel** to undo changes made within the page.

Change Local Passphrase

Step 1. Log in to the web configuration utility and choose **Security** > **Secure Sensitive Data Management** > **Properties**. Click **Change Local Passphrase**. The *Change Local Passphrase* page opens:



Note: The Current Local Passphrase Type describes which passphrase is in use.

Step 2. Click the desired radio button from the *Local Passphrase* field.

- Default — Uses the default passphrase.
- User Defined — User defines what passphrase is used.

Step 3. If User Defined was clicked, enter the desired passphrase into the field, and then enter the same passphrase in the *Confirm Password* field.

Step 4. Choose **Apply** to keep the changes made or **Cancel** to undo all changes on this page.

Step 5. Choose **Back** to return to the *Properties* page.