

Sx500系列堆疊式交換機上的安全敏感資料(SSD)屬性

目標

安全敏感資料(SSD)管理用於安全地管理交換機上的密碼和金鑰等敏感資料。當資訊從一台裝置傳送到另一台裝置時，應保護此資訊。使用者的訪問級別決定如何以純文字檔案或加密資料檢視敏感資料。SSD屬性是與SSD規則一起使用的一組引數，這些規則控制設定，例如如何加密敏感資料、配置檔案的安全強度，以及在當前會話中如何檢視敏感資料。

本文的目標是幫助在Sx500系列堆疊式交換機上配置安全敏感資料(SSD)屬性。

適用裝置

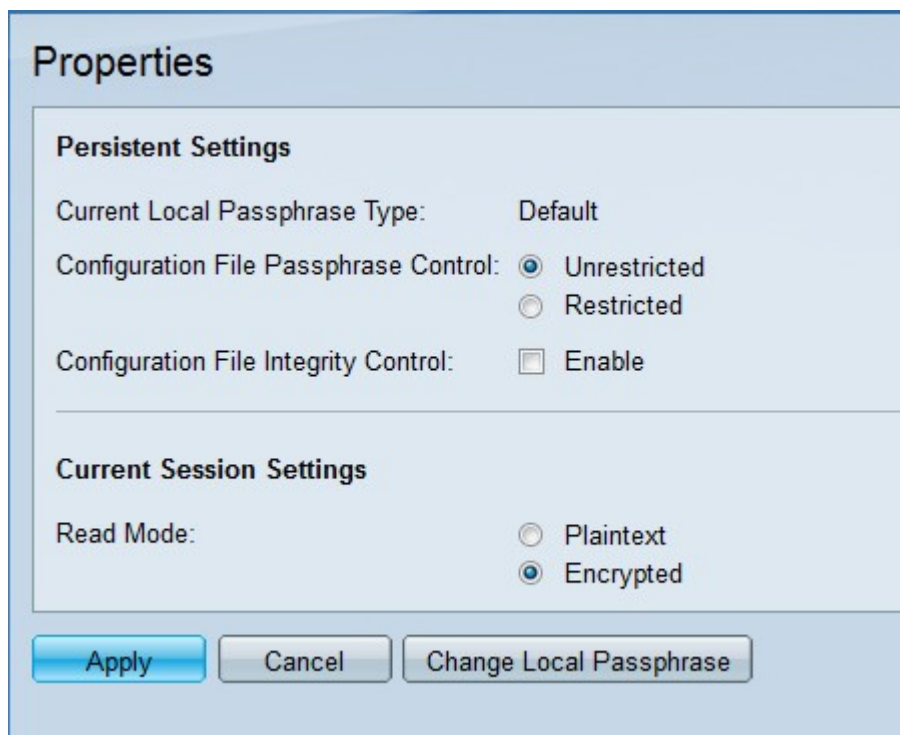
- Sx500系列堆疊式交換器

軟體版本

- 1.3.0.62

SSD屬性

步驟1.登入到Web配置實用程式，然後選擇**安全>安全敏感資料管理>屬性**。將開啟*Properties*頁面：



The screenshot shows a web-based configuration interface titled "Properties". It is divided into two main sections: "Persistent Settings" and "Current Session Settings".

Persistent Settings

- Current Local Passphrase Type: Default
- Configuration File Passphrase Control: Unrestricted, Restricted
- Configuration File Integrity Control: Enable

Current Session Settings

- Read Mode: Plaintext, Encrypted

At the bottom of the form, there are three buttons: "Apply", "Cancel", and "Change Local Passphrase".

附註： Current Local Passphrase Type欄位顯示最初設定的本地密碼的型別。

步驟2.在Configuration File Passphrase Control欄位中，按一下所需型別密碼控制的單選按鈕。檔案密碼控制為使用者定義的密碼和使用使用者定義的密碼加密的資料提供額外的保護。

·無限制 — 使用者定義的密碼包含在從一個裝置傳送到另一個裝置的配置檔案中。

·受限 — 配置檔案中不包含使用者定義的密碼。

步驟3. (可選) 要啟用檔案完整性控制，請選中Configuration File Integrity Control欄位中的Enable覆取方塊。此選項可保護配置檔案免於修改。

步驟4.在Read Mode欄位中，按一下所需的單選按鈕。可用選項包括：

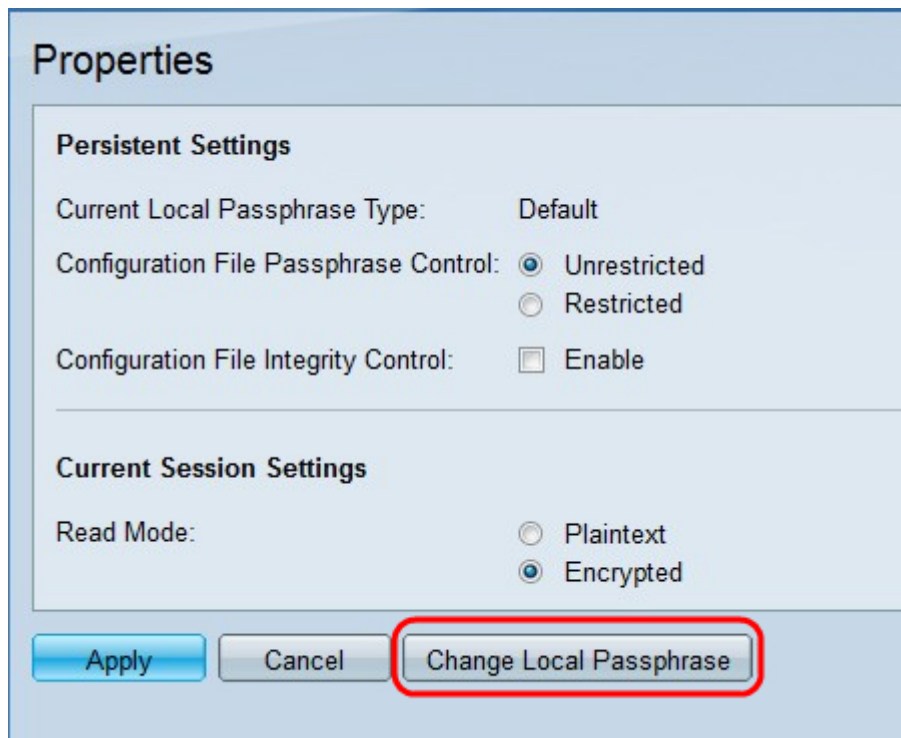
·純文字檔案 — 敏感資料顯示為純文字檔案。

·已加密 — 資料以加密形式顯示。

步驟5.按一下Apply。

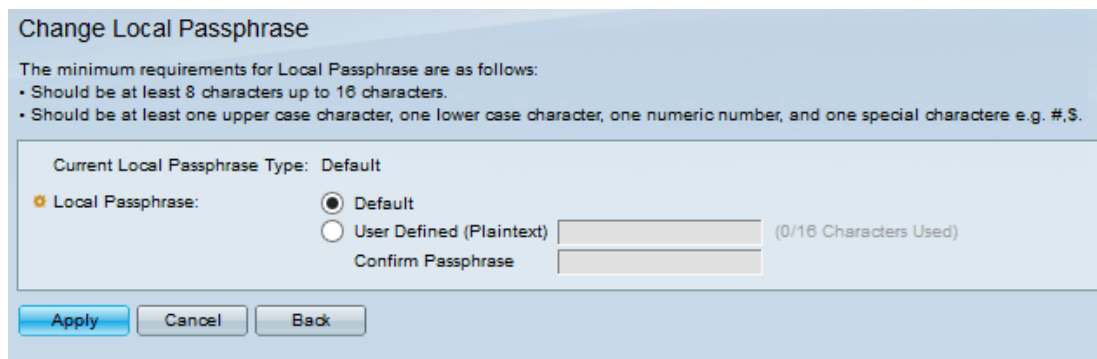
變更本機密碼短語

步驟1.登入到Web配置實用程式，然後選擇安全>安全敏感資料管理>屬性。將開啟Properties頁面：



The screenshot shows a 'Properties' dialog box with two sections: 'Persistent Settings' and 'Current Session Settings'. In 'Persistent Settings', 'Current Local Passphrase Type' is set to 'Default', 'Configuration File Passphrase Control' has 'Unrestricted' selected, and 'Configuration File Integrity Control' has 'Enable' unchecked. In 'Current Session Settings', 'Read Mode' has 'Encrypted' selected. At the bottom, there are three buttons: 'Apply', 'Cancel', and 'Change Local Passphrase', with the latter highlighted by a red rectangle.

步驟2.按一下更改本地密碼以更改當前的本地密碼。此時將開啟更改本地密碼頁：



The screenshot shows a 'Change Local Passphrase' dialog box. It lists minimum requirements for the local passphrase: at least 8 characters up to 16 characters, and at least one upper case character, one lower case character, one numeric number, and one special character (e.g., #, \$). Below this, 'Current Local Passphrase Type' is set to 'Default'. There are two radio buttons for 'Local Passphrase': 'Default' (selected) and 'User Defined (Plaintext)'. The 'User Defined' option has an input field showing '(0/16 Characters Used)' and a 'Confirm Passphrase' input field. At the bottom, there are three buttons: 'Apply', 'Cancel', and 'Back'.

附註：Current Local Passphrase Type欄位顯示當前的本地密碼短語。

Change Local Passphrase

The minimum requirements for Local Passphrase are as follows:

- Should be at least 8 characters up to 16 characters.
- Should be at least one upper case character, one lower case character, one numeric number, and one special character e.g. #,\$.

Current Local Passphrase Type: Default

Local Passphrase:

Default

User Defined (Plaintext) (10/16 Characters Used)

Confirm Passphrase

步驟3.在Local Passphrase欄位中，按一下所需本地密碼的單選按鈕：

·預設 — 此命令會分配預設密碼。

·使用者定義（明文） — 輸入所需的密碼。它應介於8到16個字元之間，並包含大寫和小寫字元、數字和特殊字元。

— 確認密碼短語 — 重新輸入使用者定義的密碼短語。

步驟4.按一下**Apply**。