Konfiguration der SSD-Eigenschaften (Secure Sensitive Data) auf Managed Switches der Serien 200 und 300

Ziel

SSD (Secure Sensitive Data) schützt vertrauliche Informationen wie Kennwörter, ermöglicht oder verweigert Benutzern den Zugriff auf vertrauliche Daten und verhindert, dass Konfigurationsdateien durch böswillige Benutzer beschädigt werden. SSD verwendet Passphrasen zum Sichern von Daten. Passphrasen ähneln einem Passwort, das im Switch gespeichert und als Verschlüsselungsschlüssel verwendet wird. Geräte, die die Passphrase nicht kennen, können die Daten, die die Passphrase verwenden, nicht entschlüsseln.

In diesem Dokument sollen die Funktionen erläutert werden, die auf der Seite *SSD-Eigenschaften* verfügbar sind.

Unterstützte Geräte

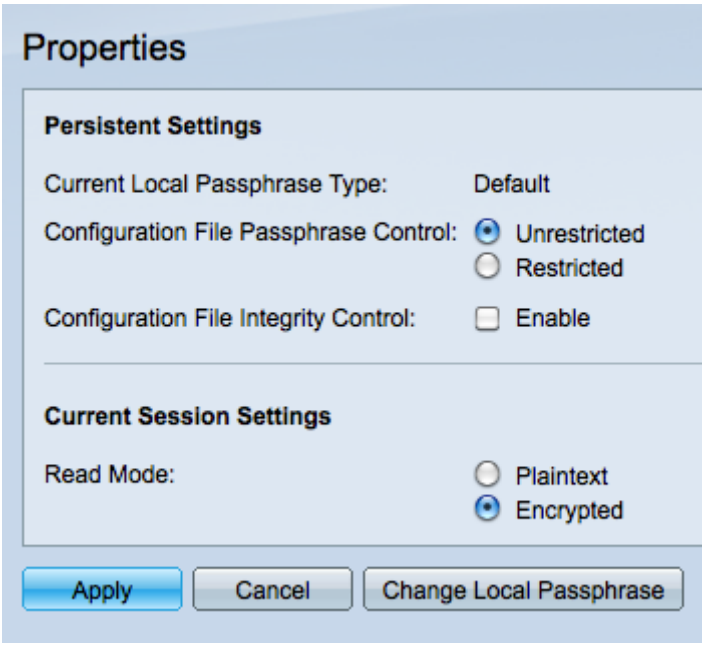
- Managed Switches der Serien SF/SG 200 und SF/SG 300

Software-Version

•1.3.0.62

Konfiguration der SSD-Eigenschaften

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > Secure Sensitive Data Management > Properties**. Die Seite *Eigenschaften* wird geöffnet:



Hinweis: Das aktuelle lokale Passphrase-Steuerelement beschreibt, ob das Gerät die Standard-Passphrase oder eine benutzerdefinierte Passphrase verwendet.

Schritt 2: Klicken Sie im Feld "*Passphrase-Steuerung* der *Konfigurationsdatei" auf das* gewünschte Optionsfeld.

- Unrestricted (Unbeschränkt): Sendet die Passphrase in die Konfigurationsdatei, sodass andere Geräte die Passphrase kennen können.
- Restricted (Eingeschränkt) - Verhindert, dass die Passphrase in die Konfigurationsdatei gesendet wird, wodurch andere Geräte die Passphrase nicht lernen können.

Schritt 3: Aktivieren Sie das Kontrollkästchen Integritätskontrolle der Konfigurationsdatei, um den Schutz vor unerwünschten Änderungen an der Konfigurationsdatei zu aktivieren.

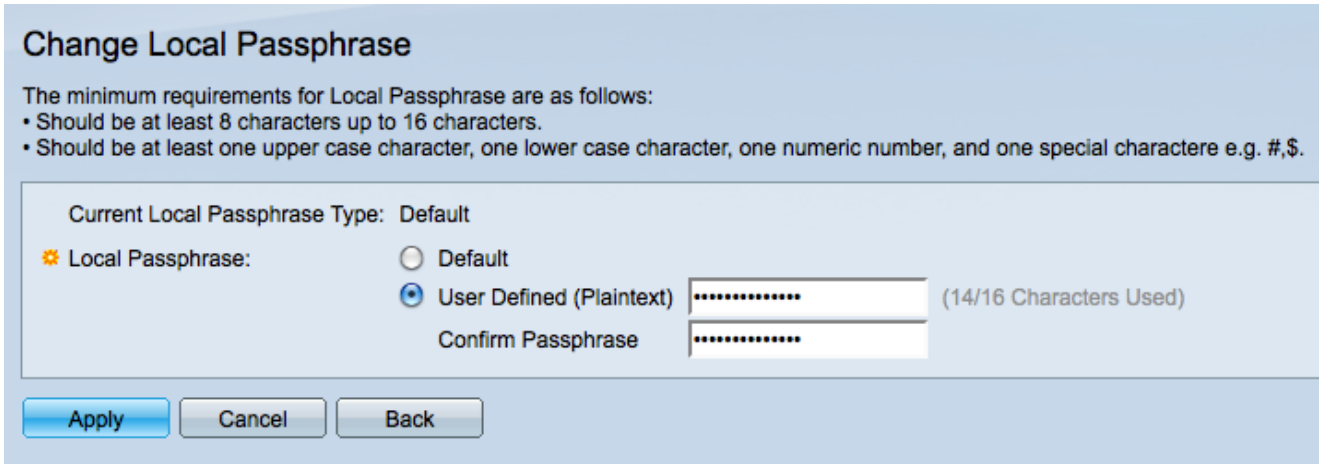
Schritt 4: Klicken Sie auf das gewünschte Optionsfeld im Feld *Lesemodus*, um festzulegen, wie die Datei gelesen wird.

- Klartext — Verwendet Klartext, um die aktuellen Sitzungsinformationen anzuzeigen.
- Verschlüsselt — Verschlüsselt die Datei, bevor sie die Sitzungsinformationen anzeigt.

Schritt 5: Klicken Sie auf **Anwenden**, um die aktuellen Änderungen beizubehalten, oder auf **Abbrechen**, um die auf der Seite vorgenommenen Änderungen rückgängig zu machen.

Lokale Passphrase ändern

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > Secure Sensitive Data Management > Properties**. Klicken Sie auf **Lokale Passphrase ändern** . Die Seite *Lokale Passphrase ändern* wird geöffnet:



Hinweis: Der aktuelle lokale Passphrasentyp beschreibt, welche Passphrase verwendet wird.

Schritt 2: Klicken Sie im Feld "*Lokale Passphrase"* auf das gewünschte Optionsfeld.

- Standard — Verwendet die Standard-Passphrase.
- Benutzerdefiniert — Der Benutzer definiert, welche Passphrase verwendet wird.

Schritt 3: Wenn Sie auf Benutzerdefiniert geklickt haben, geben Sie die gewünschte Passphrase in das Feld ein, und geben Sie diese dann im Feld *Passwort bestätigen* ein.

Schritt 4: Wählen Sie **Anwenden**, um die Änderungen beizubehalten, oder **Abbrechen**, um

alle Änderungen auf dieser Seite rückgängig zu machen.

Schritt 5: Wählen Sie **Zurück**, um zur Seite *Eigenschaften* zurückzukehren.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.