SSD-Eigenschaften (Secure Sensitive Data) auf Stackable Switches der Serie Sx500

Ziel

Secure Sensitive Data (SSD) Management wird verwendet, um vertrauliche Daten wie Kennwörter und Schlüssel sicher auf dem Switch zu verwalten. Diese Informationen müssen gesichert werden, wenn sie von einem Gerät an ein anderes Gerät gesendet werden. Die Zugriffsebene des Benutzers legt fest, wie die vertraulichen Daten entweder als Klartext oder als verschlüsselte Daten angesehen werden können. SSD-Eigenschaften sind eine Reihe von Parametern in Verbindung mit SSD-Regeln, die Einstellungen steuern, wie z. B. die Verschlüsselung vertraulicher Daten, die Sicherheit von Konfigurationsdateien und die Anzeige vertraulicher Daten innerhalb der aktuellen Sitzung.

Dieses Dokument soll Ihnen helfen, SSD-Eigenschaften (Secure Sensitive Data) auf Stackable Switches der Serie Sx500 zu konfigurieren.

Anwendbare Geräte

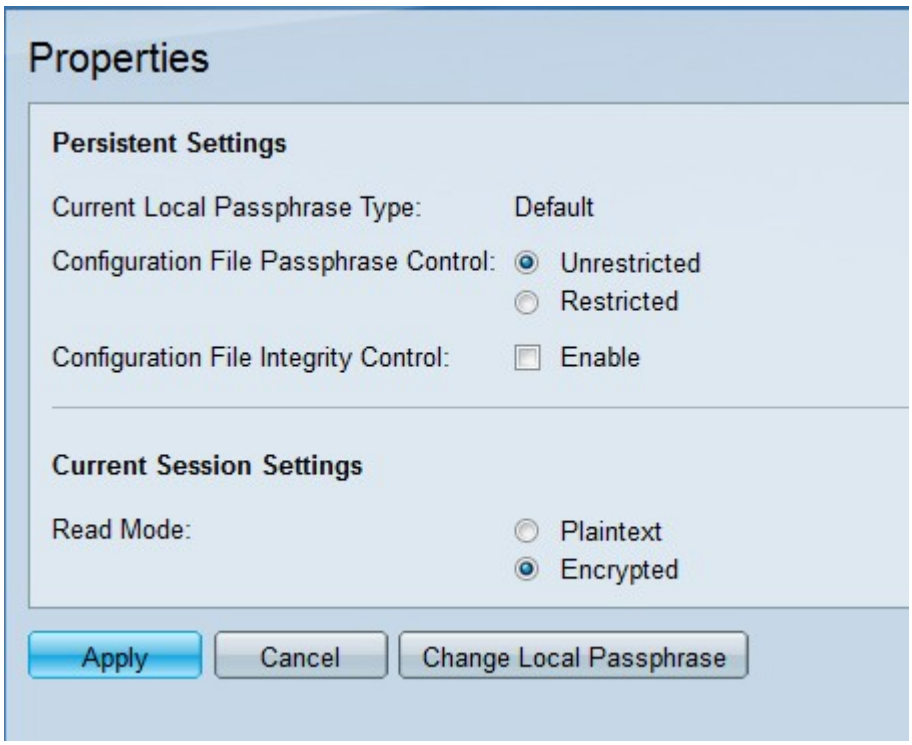
·Stackable Switches der Serie Sx500

Softwareversion

·1.3.0.62

SSD-Eigenschaften

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



Hinweis: Das Feld Aktueller lokaler Passphrasentyp zeigt den anfänglich festgelegten Typ der lokalen Passphrase an.

Schritt 2: Klicken Sie im Feld Passphrase-Steuerelement für die Konfigurationsdatei auf das Optionsfeld des gewünschten Typs von Passphrase-Steuerelement. Die Passphrasenkontrolle für Dateien bietet zusätzlichen Schutz für die vom Benutzer definierte Passphrase und die mit der vom Benutzer definierten Passphrase verschlüsselten Daten.

·Unrestricted - Die benutzerdefinierte Passphrase ist in der Konfigurationsdatei enthalten, die von einem Gerät an ein anderes gesendet wird.

·Restricted (Eingeschränkt): Die benutzerdefinierte Passphrase ist nicht in der Konfigurationsdatei enthalten.

Schritt 3: (Optional) Um die Dateiintegritätskontrolle zu aktivieren, aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld Konfigurationsdateiintegritätskontrolle. Diese Option schützt die Konfigurationsdatei vor Änderungen.

Schritt 4: Klicken Sie im Feld Lesemodus auf das gewünschte Optionsfeld. Folgende Optionen stehen zur Verfügung:

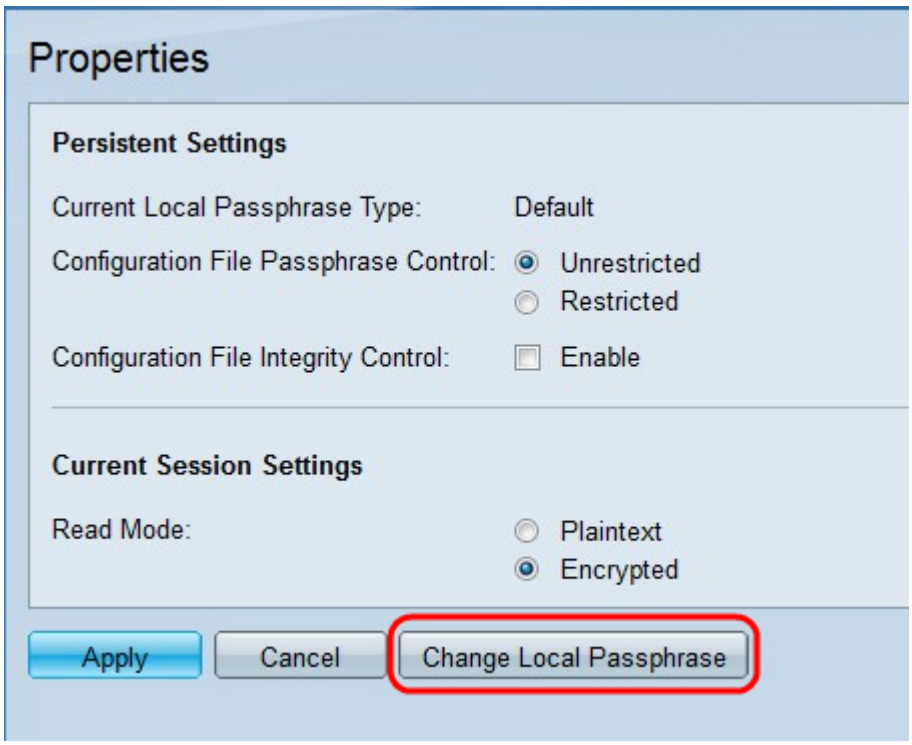
·Nur Text: Die vertraulichen Daten werden als Klartext angezeigt.

·Verschlüsselt - Die Daten werden verschlüsselt angezeigt.

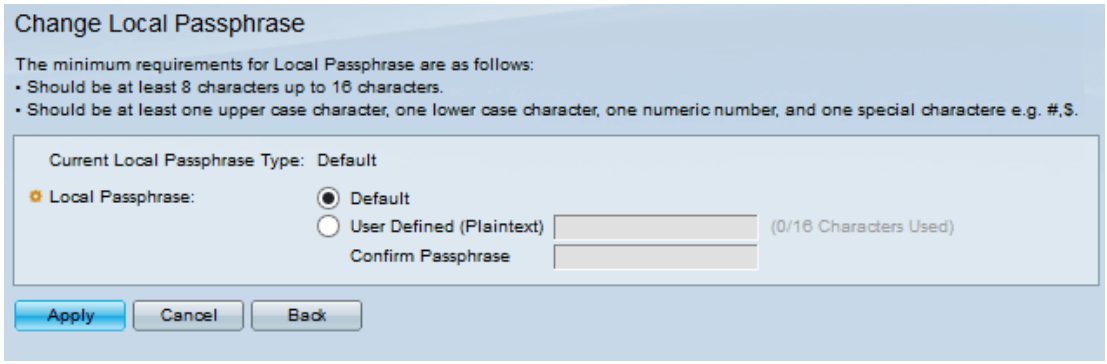
Schritt 5: Klicken Sie auf **Übernehmen**.

Lokale Passphrase ändern

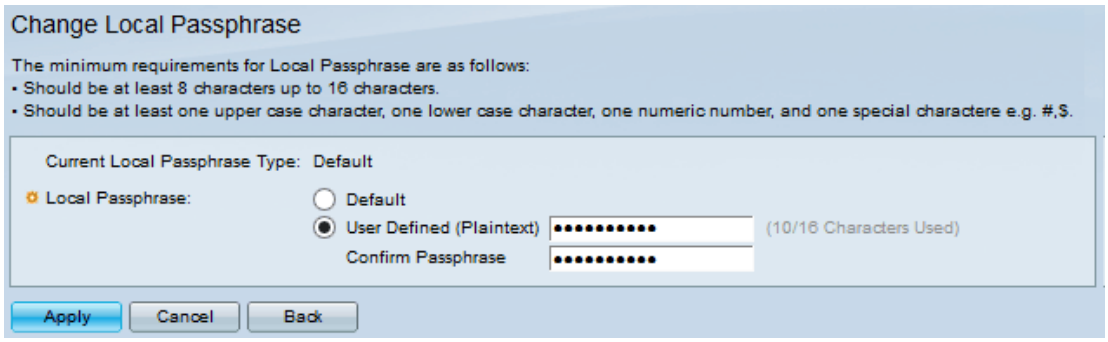
Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > Secure Sensitive Data Management > Properties aus.** Die Seite *Eigenschaften* wird geöffnet**:**



Schritt 2: Klicken Sie auf **Lokale Passphrase ändern**, um die aktuelle lokale Passphrase zu ändern. Die Seite *Lokale Passphrase ändern* wird geöffnet:



Hinweis: Im Feld Aktueller lokaler Passphrasentyp wird die aktuelle lokale Passphrase angezeigt.



Schritt 3: Klicken Sie im Feld Lokale Passphrase auf das Optionsfeld der gewünschten lokalen Passphrase:

·Default (Standard): Diese Zuweisung weist die Standard-Passphrase zu.

·Benutzerdefiniert (Nur-Text) - Geben Sie die gewünschte Passphrase ein. Sie muss zwischen 8 und 16 Zeichen umfassen und Groß- und Kleinbuchstaben, eine Zahl und ein Sonderzeichen enthalten.

- Passphrase bestätigen - Geben Sie die benutzerdefinierte Passphrase erneut ein.

Schritt 4: Klicken Sie auf **Übernehmen**.