

Configurazione delle proprietà SSD (Secure Sensitive Data) sugli switch gestiti serie 200/300

Obiettivo

Secure Sensitive Data (SSD) protegge le informazioni riservate, ad esempio le password, consente o nega l'accesso degli utenti ai dati riservati e impedisce che i file di configurazione vengano danneggiati da utenti malintenzionati. SSD utilizza le passphrase per proteggere i dati. Le passphrase sono simili a una password memorizzata nello switch e utilizzata come chiave di crittografia. I dispositivi che non conoscono la passphrase non saranno in grado di decrittografare i dati che la utilizzano.

L'obiettivo di questo documento è spiegare le funzioni disponibili nella pagina *Proprietà SSD*.

Dispositivi interessati

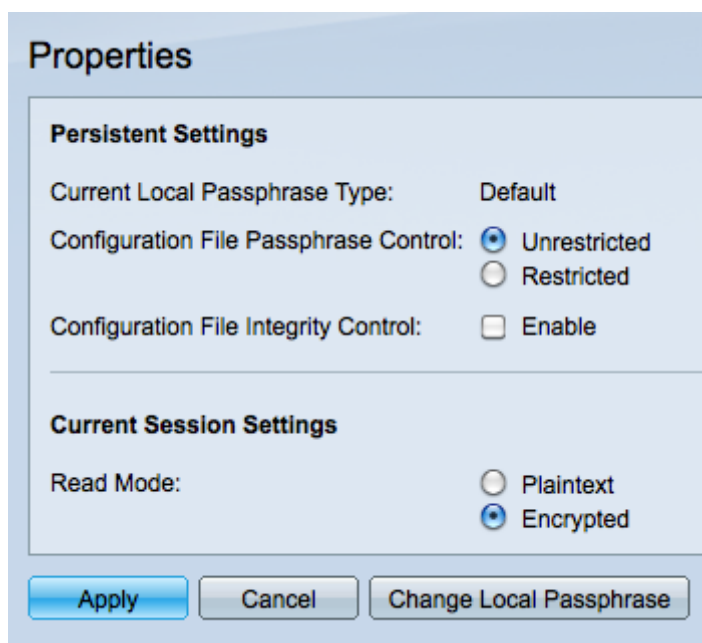
•SF/SG serie 200 e SF/SG serie 300 Managed Switch

Versione del software

•1.3.0.62

Configurazione delle proprietà SSD

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Sicurezza > Gestione sicura dei dati sensibili > Proprietà**. Viene visualizzata la pagina *Proprietà*:



The screenshot shows a web interface titled "Properties" with two 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, there are three buttons: "Apply", "Cancel", and "Change Local Passphrase".

Nota: il Controllo passphrase locale corrente descrive se il dispositivo utilizza la passphrase predefinita o una passphrase definita dall'utente.

Passaggio 2. Fare clic sul pulsante di scelta desiderato nel campo *Controllo passphrase del file di configurazione*.

·Senza restrizioni - Invia la passphrase nel file di configurazione, consentendo ad altri dispositivi di conoscere la passphrase.

·Limitato — impedisce l'invio della passphrase nel file di configurazione, impedendo così ad altri dispositivi di apprendere la passphrase.

Passaggio 3. Selezionare la casella di controllo Controllo dell'integrità del file di configurazione per attivare la protezione da modifiche indesiderate al file di configurazione.

Passaggio 4. Fare clic sul pulsante di opzione desiderato nel campo *Modalità lettura* per impostare la modalità di lettura del file.

·Testo normale — utilizza testo normale per visualizzare le informazioni sulla sessione corrente.

·Crittografato - esegue la crittografia del file prima di visualizzare le informazioni sulla sessione.

Passaggio 5. Fare clic su **Applica** per mantenere le modifiche correnti o su **Annulla** per annullare le modifiche apportate nella pagina.

Cambia passphrase locale

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Sicurezza > Gestione sicura dei dati sensibili > Proprietà**. Fare clic su **Cambia passphrase locale**. Viene visualizzata la pagina *Modifica passphrase locale*:

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) (14/16 Characters Used)

Confirm Passphrase

Apply **Cancel** **Back**

Nota: il tipo di passphrase locale corrente descrive la passphrase in uso.

Passaggio 2. Fare clic sul pulsante di scelta desiderato nel campo *Passphrase locale*.

·Predefinito — utilizza la passphrase predefinita.

·Definita dall'utente: la passphrase viene definita dall'utente.

Passaggio 3. Se è stato fatto clic su Definita dall'utente, immettere la passphrase desiderata nel campo, quindi immettere la stessa passphrase nel campo *Conferma password*.

Passaggio 4. Scegliere **Applica** per mantenere le modifiche apportate o **Annulla** per annullare tutte le modifiche apportate in questa pagina.

Passaggio 5. Scegliere **Indietro** per tornare alla pagina *Proprietà*.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).