Configurazione delle regole Secure Sensitive Data (SSD) sugli switch serie Sx500 impilabili

Obiettivo

La gestione Secure Sensitive Data (SSD) viene utilizzata per gestire in modo sicuro dati sensibili quali password e chiavi sullo switch, popolare questi dati con altri dispositivi e proteggere la configurazione automatica. L'accesso per la visualizzazione dei dati sensibili come testo normale o crittografato viene fornito in base al livello di accesso configurato dall'utente e al metodo di accesso dell'utente. Questo articolo spiega come gestire le regole SSD sugli switch impilabili serie Sx500.

Nota: È inoltre possibile sapere come gestire le proprietà SSD. Per ulteriori informazioni, consultare l'articolo *Proprietà Secure Sensitive Data (SSD) sugli switch impilabili serie Sx500* .

Dispositivi interessati

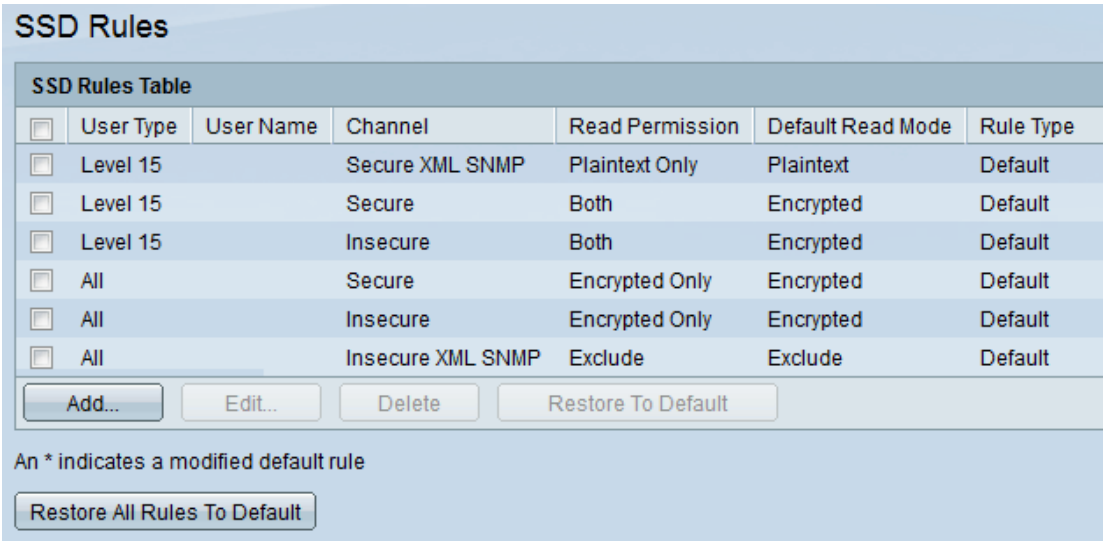
·Switch Stack Serie Sx500

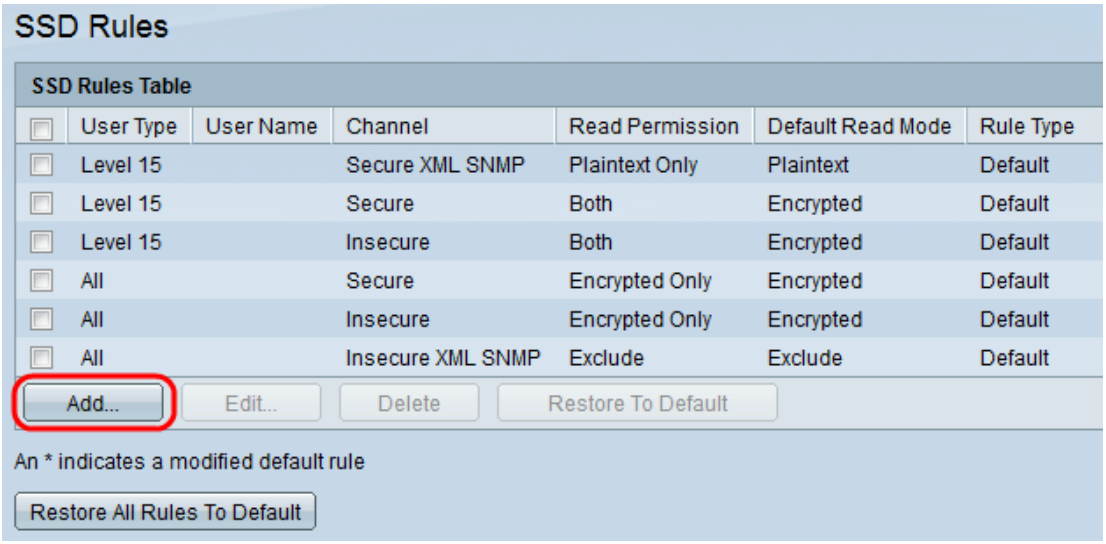
Versione del software

·v1.2.7.76

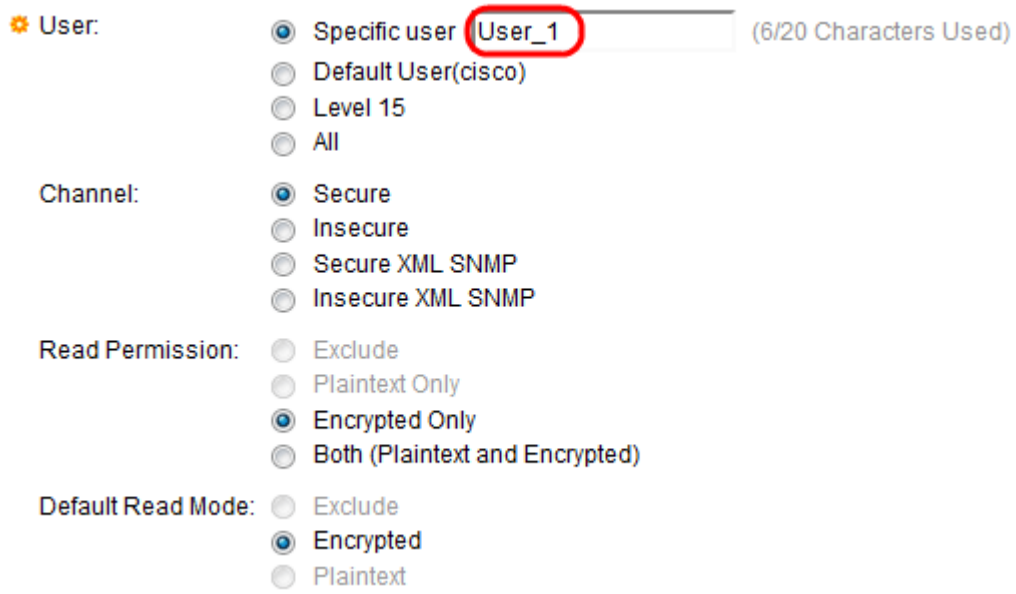
Configurazione regole SSD

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





Passaggio 2. Fare clic su **Add** per aggiungere una nuova regola SSD. Viene visualizzata la finestra *Aggiungi regola SSD*.



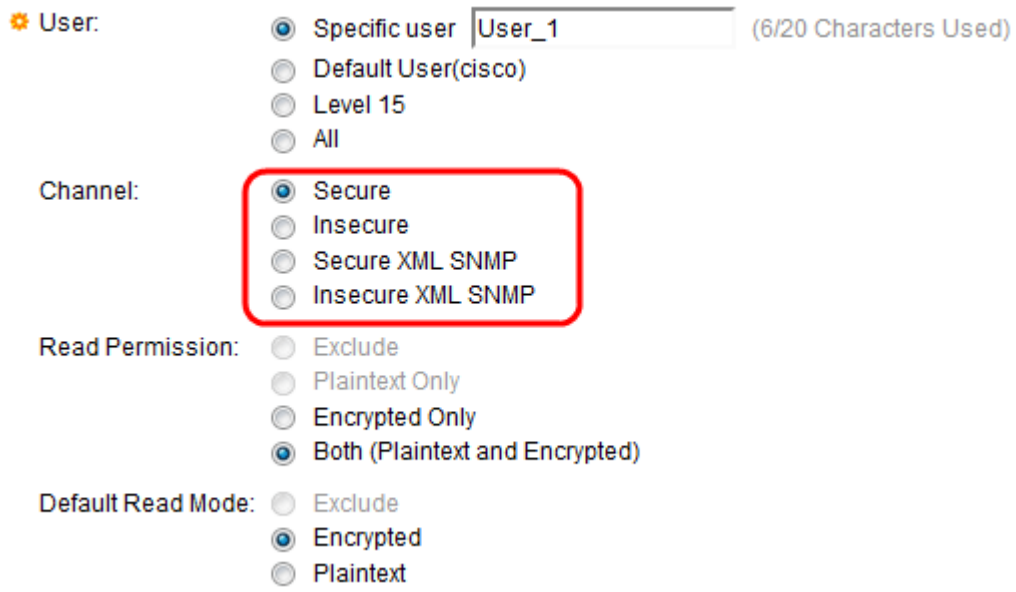
Passaggio 3. Fare clic sul pulsante di opzione Utente desiderato in cui viene visualizzata la regola SSD. Le opzioni disponibili sono:

·Utente specifico - Immettere il nome utente specifico a cui applicare la regola (non è necessario definire l'utente).

·Utente predefinito (cisco): la regola viene applicata all'utente predefinito.

·Livello 15: la regola viene applicata a tutti gli utenti con il livello di privilegio 15. In questa posizione l'utente può accedere alla GUI e configurare lo switch. Per modificare le impostazioni dei privilegi, consultare l'articolo *Configurazione dell'account utente sugli switch impilabili serie Sx500*.

·Tutti: la regola viene applicata a tutti gli utenti.



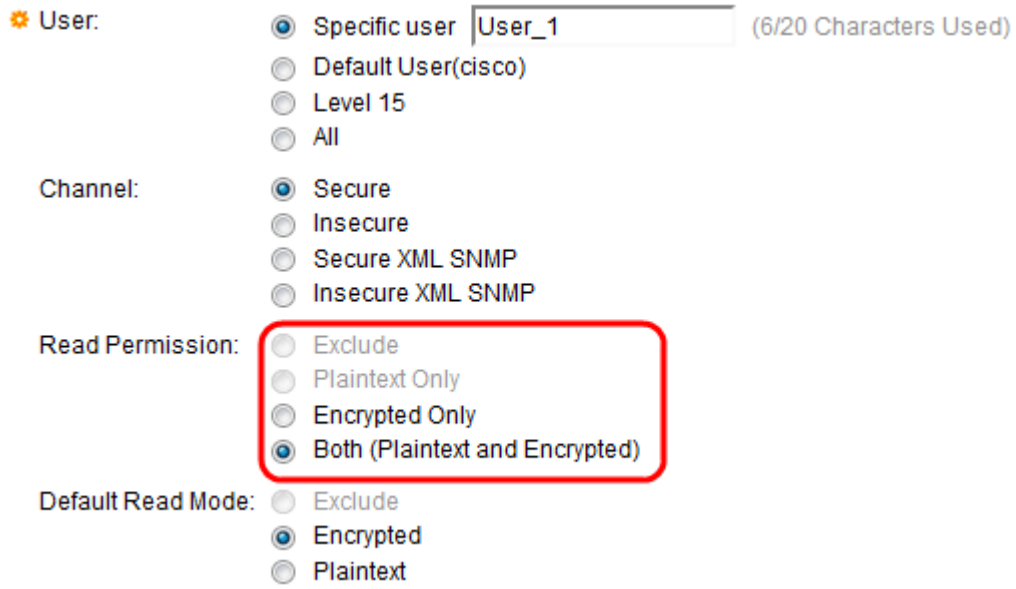
Passaggio 4. Fare clic sul pulsante di opzione corrispondente al livello di sicurezza del canale di input a cui si applica la regola nel campo Canale. Le opzioni disponibili sono:

·Protetto: questa regola si applica solo ai canali protetti (console, SCP, SSH e HTTPS), esclusi i canali SNMP e XML.

·Non sicuro: questa regola si applica solo ai canali non sicuri (Telnet, TFTP e HTTP), esclusi i canali SNMP e XML.

·Secure XML SNMP: questa regola si applica solo a XML su HTTPS e SNMPv3 con privacy.

·SNMP XML non sicuro: questa regola si applica solo a XML su HTTP o SNMPv1/v2 e SNMPv3 senza privacy.



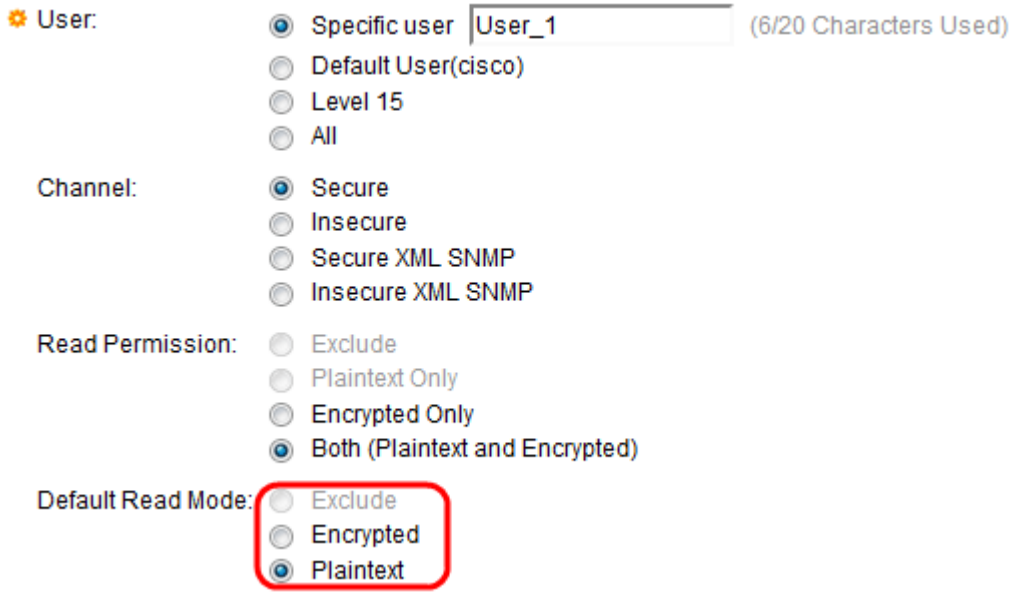
Passaggio 5. Fare clic sul pulsante di opzione desiderato per definire le autorizzazioni di lettura associate alla regola nel campo Autorizzazione lettura. Le opzioni disponibili sono:

·Escludi: il livello più basso di autorizzazione di lettura e gli utenti non sono autorizzati a ricevere dati riservati in alcun formato. Questa opzione è disponibile solo se si fa clic su Non sicuro nel passaggio 4.

·Solo testo normale: un livello più elevato di autorizzazioni di lettura rispetto a Escludi. Questa opzione consente agli utenti di ricevere dati riservati solo in formato testo normale. Questa opzione è disponibile solo se si fa clic su Non sicuro nel passaggio 4.

·Solo crittografati: il livello intermedio delle autorizzazioni di lettura. Questa opzione consente agli utenti di ricevere solo i dati sensibili crittografati.

·Entrambi (testo normale e crittografato): il livello più alto di autorizzazioni di lettura. Questa opzione consente agli utenti di ricevere autorizzazioni sia crittografate che di testo normale e di ottenere dati riservati in forma crittografata e non crittografata.



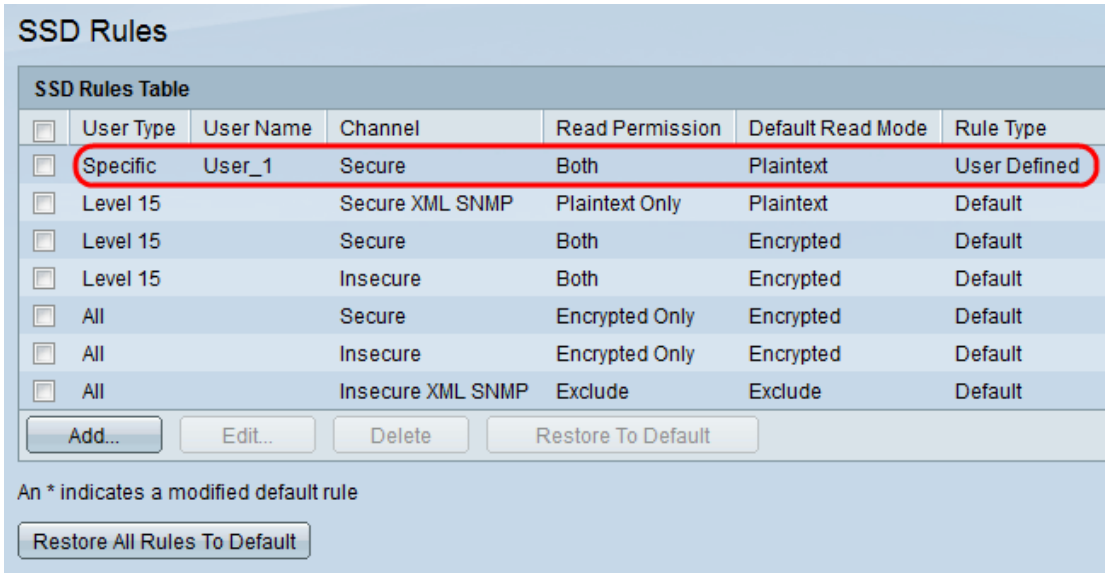
Passaggio 6. Fare clic sul pulsante di opzione corrispondente alla modalità di lettura desiderata nel campo Modalità di lettura predefinita. Definisce l'autorizzazione predefinita assegnata a tutti gli utenti. L'opzione Modalità lettura predefinita non ha una priorità più alta del campo Autorizzazione lettura. Le opzioni disponibili sono:

·Escludi: non consente la lettura dei dati riservati. Questa opzione è disponibile solo se si fa clic su Non protetto nel passaggio 4.

·Crittografia: i dati sensibili vengono presentati crittografati.

·Testo normale: i dati sensibili vengono presentati come testo normale.

Passaggio 7. Fare clic su **Salva** nella finestra *Aggiungi regola SSD*. Le modifiche vengono visualizzate nella tabella Regole SSD come illustrato di seguito:


SSD Rules
SSD Rules Table
User Type
User Name
Channel
Read Permission
Default Read Mode
Rule Type
Specific
User_1
Secure
Both
Plaintext
User Defined
Level 15
Secure XML SNMP
Plaintext Only
Plaintext
Default
Level 15
Secure
Both
Encrypted
Default
Level 15
Insecure
Both
Encrypted
Default
All
Secure
Encrypted Only
Encrypted
Default
All
Insecure
Encrypted Only
Encrypted
Default
All
Insecure XML SNMP
Exclude
Exclude
Default
Add...
Edit...
Delete
Restore To Default
An * indicates a modified default rule
Restore All Rules To Default