Konfiguration von SSD-Regeln (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 Daten auf andere Geräte zu übertragen und die automatische Konfiguration zu sichern. Der Zugriff auf die Anzeige vertraulicher Daten als unverschlüsselt oder verschlüsselt erfolgt auf der Grundlage der vom Benutzer konfigurierten Zugriffsebene und der Zugriffsmethode des Benutzers. In diesem Artikel wird die Verwaltung von SSD-Regeln für Stackable Switches der Serie Sx500 erläutert.

Hinweis: Möglicherweise möchten Sie auch wissen, wie die SSD-Eigenschaften verwaltet werden. Weitere Informationen finden Sie im Artikel *Secure Sensitive Data (SSD) Properties (SSD-Eigenschaften) auf Stackable Switches der Serie Sx500*.

Anwendbare Geräte

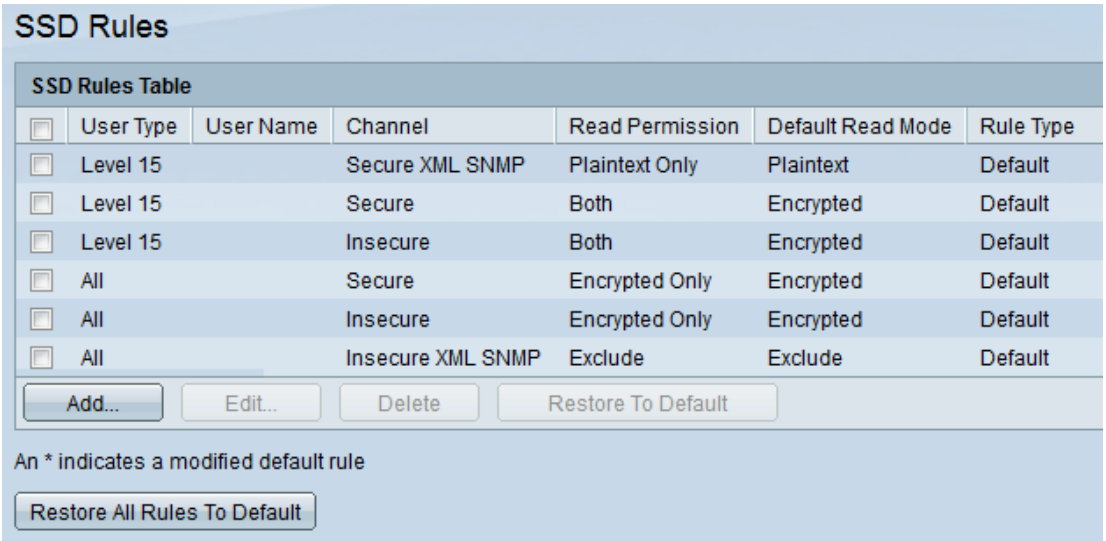
·Stackable Switches der Serie Sx500

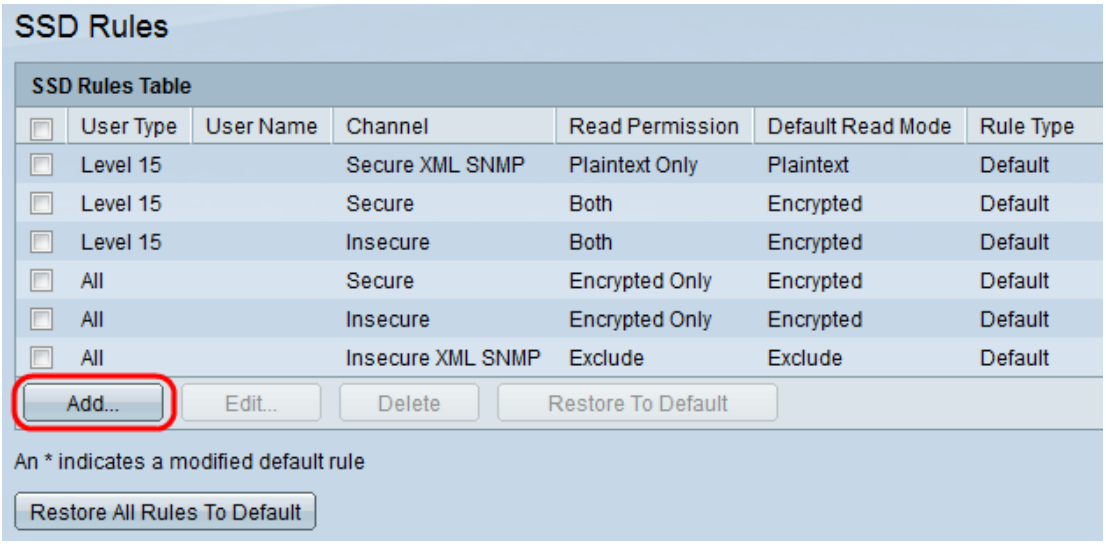
Softwareversion

·v1.2.7.76

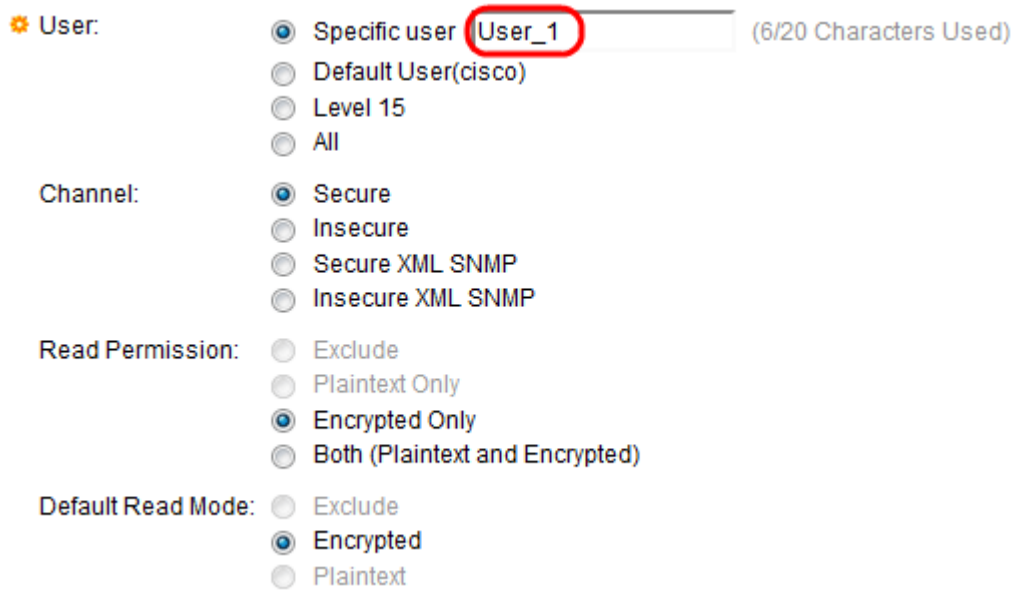
Konfiguration der SSD-Regeln

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





Schritt 2: Klicken Sie auf **Hinzufügen**, um eine neue SSD-Regel hinzuzufügen. Das Fenster *SSD-Regel hinzufügen* wird angezeigt.



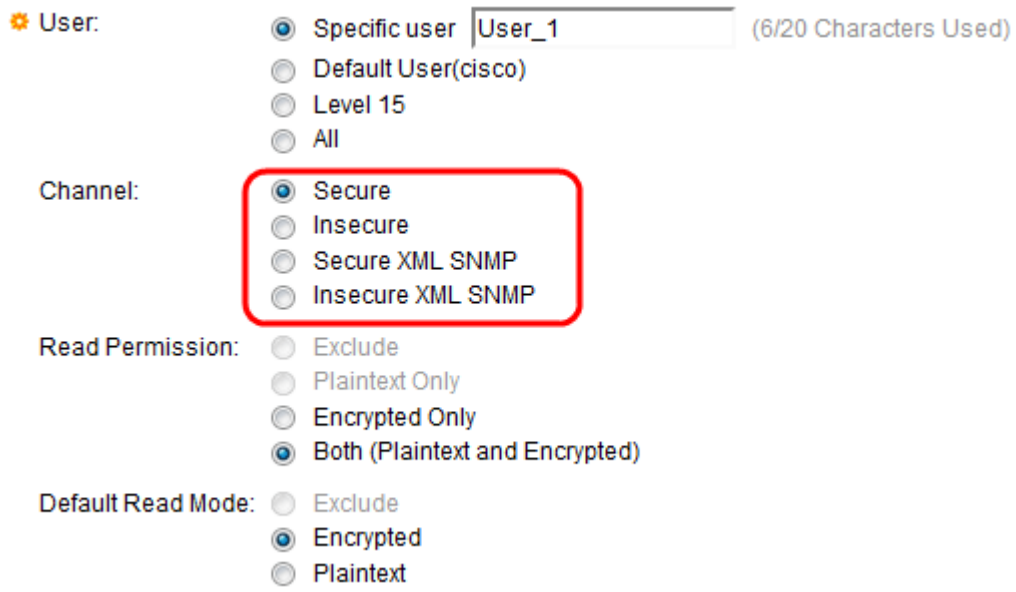
Schritt 3: Klicken Sie auf das Optionsfeld für den gewünschten Benutzer, in dem die SSD-Regel angezeigt wird. Folgende Optionen stehen zur Verfügung:

·Bestimmter Benutzer: Geben Sie den spezifischen Benutzernamen ein, für den diese Regel gilt (dieser Benutzer muss nicht unbedingt definiert werden).

·Standardbenutzer (cisco) - Die Regel gilt für den Standardbenutzer.

·Stufe 15 - Die Regel gilt für alle Benutzer mit der Berechtigungsstufe 15. Hier kann der Benutzer auf die GUI zugreifen und den Switch konfigurieren. Informationen zum Ändern der Berechtigungseinstellungen finden Sie im Artikel *Benutzerkontenkonfiguration auf stapelbaren Switches der Serie Sx500*.

·All (Alle): Die Regel gilt für alle Benutzer.



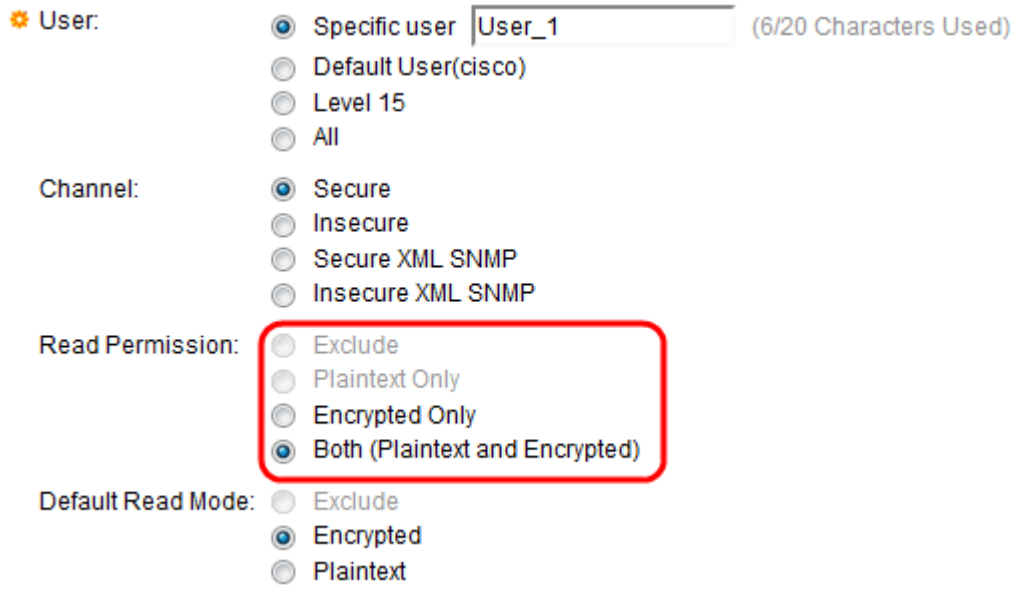
Schritt 4: Klicken Sie auf das Optionsfeld, das der Sicherheitsstufe des Eingangskanals entspricht, für den die Regel im Feld "Channel" gilt. Folgende Optionen stehen zur Verfügung:

·Sicher - Diese Regel gilt nur für sichere Kanäle (Konsole, SCP, SSH und HTTPS), nicht jedoch für SNMP- und XML-Kanäle.

·Unsicher - Diese Regel gilt nur für unsichere Kanäle (Telnet, TFTP und HTTP), nicht jedoch für SNMP- und XML-Kanäle.

·Sicheres XML-SNMP - Diese Regel gilt nur für XML über HTTPS und SNMPv3 mit Datenschutz.

·Unsicheres XML-SNMP - Diese Regel gilt nur für XML über HTTP oder SNMPv1/v2 und SNMPv3 ohne Datenschutz.



Schritt 5: Klicken Sie auf das gewünschte Optionsfeld, um die Leseberechtigungen festzulegen, die der Regel im Feld Leseberechtigung zugeordnet sind. Folgende Optionen stehen zur Verfügung:

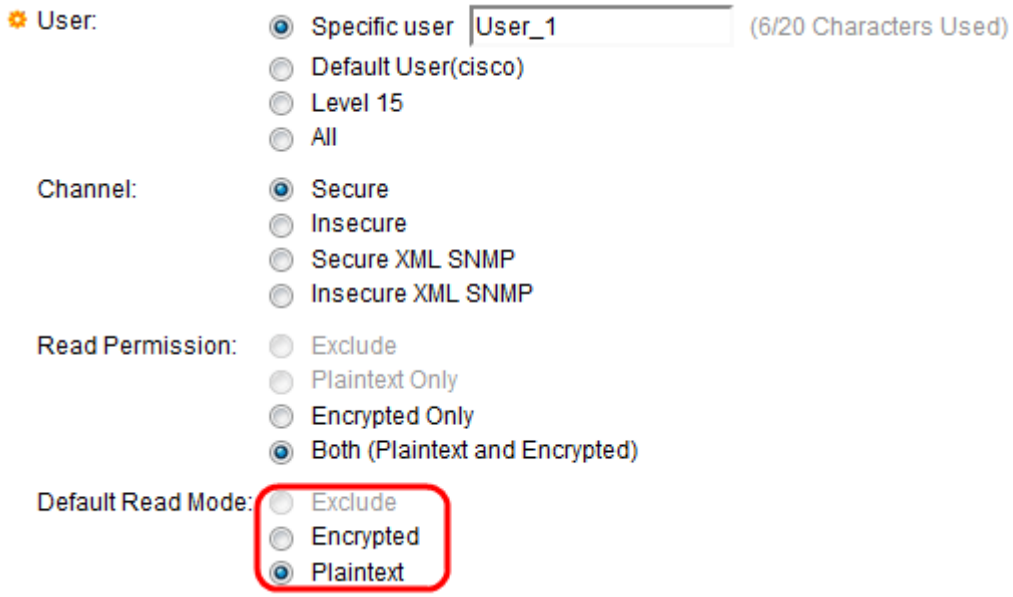
·Exclude (Ausschließen) - Die niedrigste Stufe der Leseberechtigung und die Benutzer

dürfen keine vertraulichen Daten in irgendeiner Form empfangen. Diese Option ist nur verfügbar, wenn Sie in Schritt 4 auf Unsicher klicken.

·Nur Klartext: Eine höhere Leserechtigkeit im Vergleich zu Exclude. Mit dieser Option können Benutzer vertrauliche Daten nur im Klartextformat empfangen. Diese Option ist nur verfügbar, wenn Sie in Schritt 4 auf Unsicher klicken.

·Nur verschlüsselt - Die mittlere Ebene der Leseberechtigung. Mit dieser Option können Benutzer vertrauliche Daten nur als verschlüsselt empfangen.

·Both (Plaintext und Encrypted) (Beide) - Die höchste Ebene der Leseberechtigung. Diese Option ermöglicht es Benutzern, sowohl verschlüsselte als auch Klartextberechtigungen zu erhalten und vertrauliche Daten als verschlüsseltes und unverschlüsseltes Formular abzurufen.



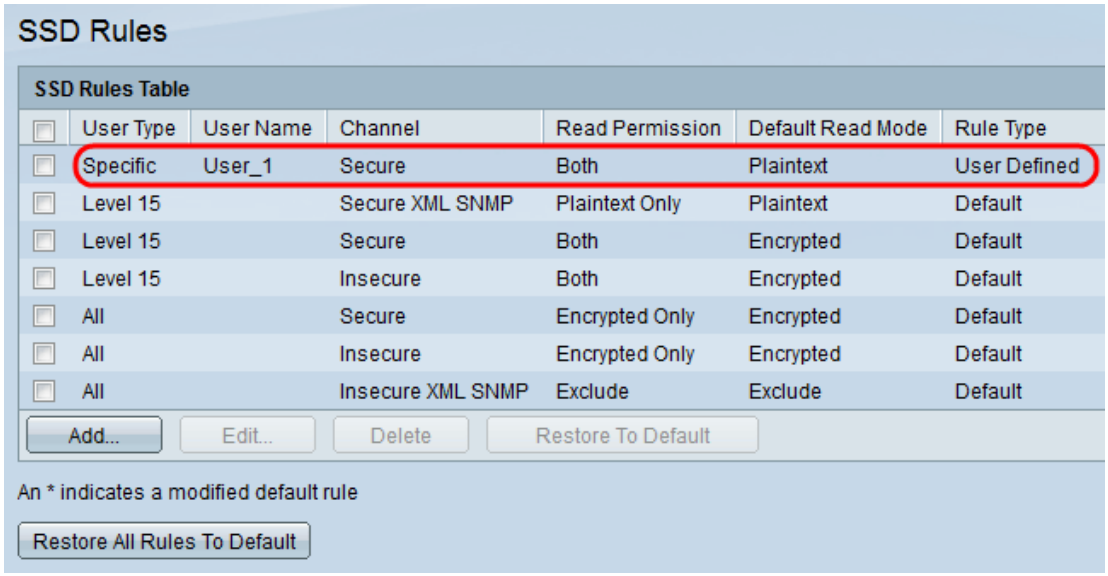
Schritt 6: Klicken Sie im Feld Standardschreibmodus auf das Optionsfeld für den gewünschten Lesemodus. Sie definiert die Standardberechtigung, die allen Benutzern erteilt wird. Die Option Standardschreibmodus hat keine höhere Priorität als das Feld Leseberechtigung. Folgende Optionen stehen zur Verfügung:

·Exclude (Ausschließen): Lese der vertraulichen Daten nicht. Diese Option ist nur verfügbar, wenn in Schritt 4 auf Unsicher geklickt **wird**.

·Verschlüsselt - Vertrauliche Daten werden verschlüsselt dargestellt.

·Klartext: Vertrauliche Daten werden als Klartext dargestellt.

Schritt 7: Klicken Sie im Fenster *SSD-Regel hinzufügen auf* **Speichern**. Die Änderungen werden wie folgt in der Tabelle mit den SSD-Regeln angezeigt:


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