Erstellung und Management von SSD-Regeln (Secure Sensitive Data) für Managed Switches der Serien 200 und 300

Ziel

In diesem Artikel wird erläutert, wie Sie Regeln für Secure Sensitive Data (SSD) auf Switches der Serien 200 und 300 einrichten und verwalten.

Unterstützte Geräte

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

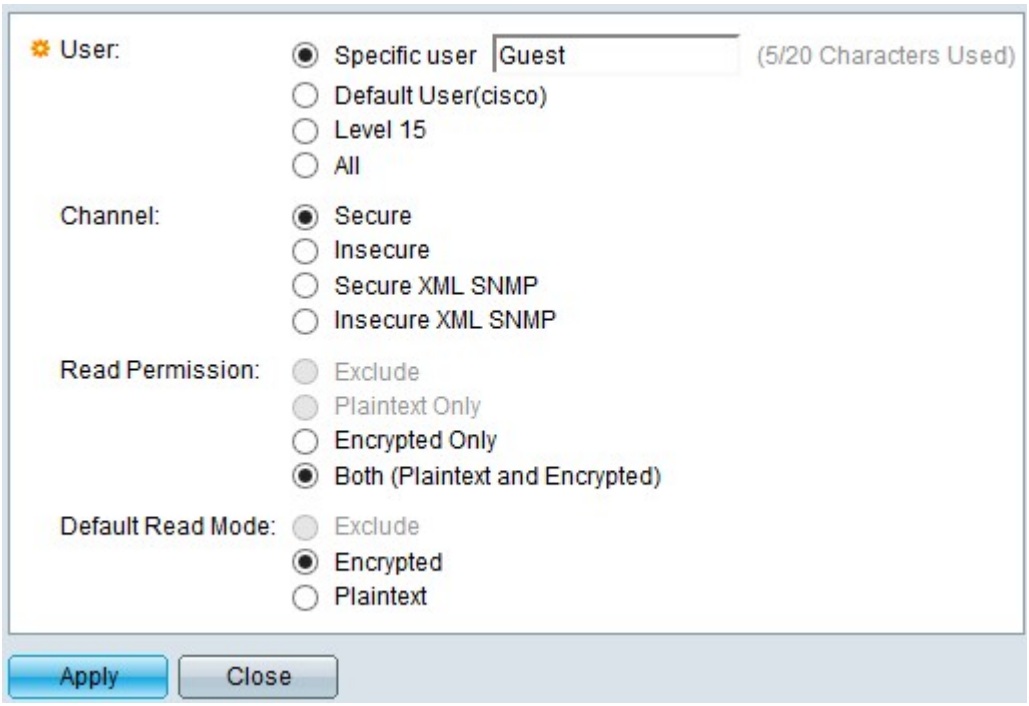
Software-Version

- v1.2.7.76

SSD-Regeln

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

Schritt 2: Klicken Sie zum Erstellen einer neuen Regel auf **Hinzufügen**. Die Seite *Regeldefinition* wird geöffnet.



Schritt 3: Wählen Sie im Feld *Benutzer* ein Optionsfeld aus, um festzulegen, auf welche Benutzer die Regel angewendet werden soll.

- Spezifischer Benutzer — Geben Sie den spezifischen Benutzernamen in das Feld ein, wenn die Regel für einen einzelnen Benutzer gilt.
- Standardbenutzer —. Diese Regel gilt für den Standardbenutzer, der auf "cisco" festgelegt ist.
- Ebene 15 — Diese Regel gilt für alle Benutzer mit Berechtigungen der Ebene 15.
- Alle — Diese Regel gilt für alle Benutzer.

Schritt 4: Wählen Sie im Feld *Channel* (Kanal) ein Optionsfeld aus, um zu bestimmen, auf welche Kanäle die Regel angewendet werden soll.

- Sicher - Diese Regel gilt nur für sichere Kanäle. Dies schließt Konsole, SSH und HTTPS ein, jedoch keine XML-Kanäle.
- Unsicher — Diese Regel gilt nur für unsichere Kanäle. Dies schließt Telnet-, TFTP- und HTTP-, aber keine XML-Kanäle ein.
- Sicheres XML-SNMP — Diese Regel gilt nur für XML über HTTPS mit Datenschutz.
- Unsicheres XML-SNMP - Diese Regel gilt nur für XML über HTTP oder ohne Datenschutz.

Schritt 5: Wählen Sie im Feld *Leseberechtigung* je nach Ihrer vorherigen Auswahl ein Optionsfeld aus.

- Wenn Sie in Schritt 3 Ebene 15 oder Alle ausgewählt haben, klicken Sie entweder auf **Ausschließen** oder auf **Nur Klartext.**
- Wenn Sie in Schritt 4 Secure XML SNMP oder Insecure XML SNMP ausgewählt haben, klicken Sie entweder auf **Exclude (Ausschließen)** oder auf **Plaintext Only (Nur Klartext).**

- Wenn Sie in Schritt 4 Sicher oder Unsicher ausgewählt haben, klicken Sie entweder auf **Nur verschlüsselt** oder auf **Beide (Nur Text und Verschlüsselt).**

Schritt 6: Klicken Sie im Feld *Standard-Lesemodus* auf **Ausschließen**, **Verschlüsselt** oder **Nur-Text.**

Schritt 7. Klicken Sie zum Aktivieren der Regel auf **Anwenden**. Zum Abbrechen der Regelerstellung klicken Sie auf **Schließen.**

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.