

Sx500系列堆疊式交換機上的安全敏感資料(SSD)規則配置

目標

安全敏感資料(SSD)管理用於安全地管理交換機上的密碼和金鑰等敏感資料、將此資料填充到其他裝置以及保護自動配置。基於使用者配置的訪問級別和使用者的訪問方法提供以明文或加密方式檢視敏感資料的訪問。本文說明如何在Sx500系列堆疊式交換機上管理SSD規則。

附註：您可能還想瞭解如何管理SSD屬性。有關詳細資訊，請參閱Sx500系列堆疊式交換機上的安全敏感資料(SSD)屬性一文。

適用裝置

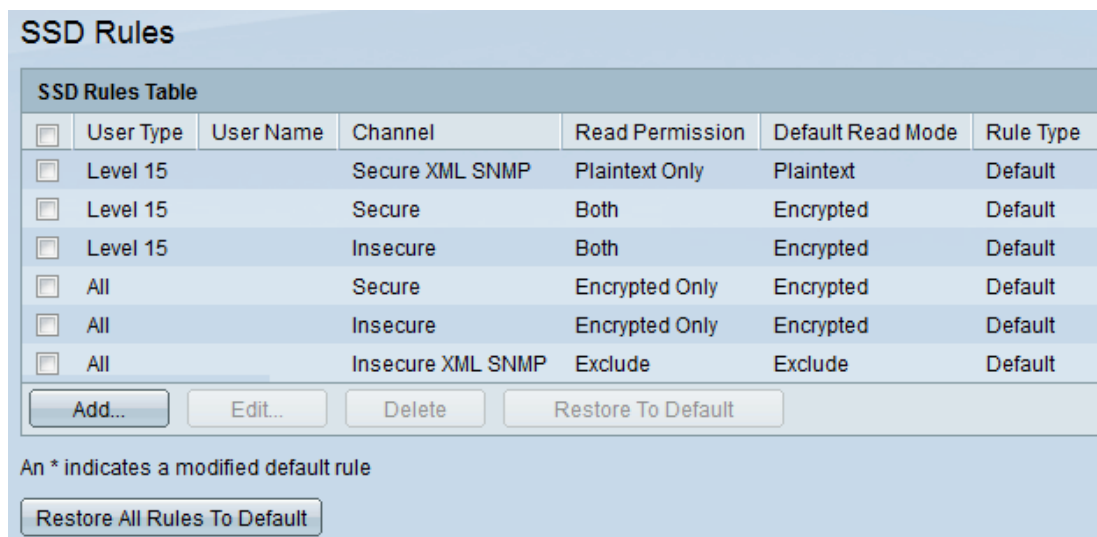
·Sx500系列堆疊式交換器

軟體版本

·v1.2.7.76

SSD規則配置

步驟1.登入到Web配置實用程式並選擇安全>安全敏感資料管理> SSD規則。將開啟SSD Rules頁面：



| SSD Rules Table | | | | | | |
|--------------------------|-----------|-----------|-------------------|-----------------|-------------------|-----------|
| <input type="checkbox"/> | User Type | User Name | Channel | Read Permission | Default Read Mode | Rule Type |
| <input type="checkbox"/> | Level 15 | | Secure XML SNMP | Plaintext Only | Plaintext | Default |
| <input type="checkbox"/> | Level 15 | | Secure | Both | Encrypted | Default |
| <input type="checkbox"/> | Level 15 | | Insecure | Both | Encrypted | Default |
| <input type="checkbox"/> | All | | Secure | Encrypted Only | Encrypted | Default |
| <input type="checkbox"/> | All | | Insecure | Encrypted Only | Encrypted | Default |
| <input type="checkbox"/> | All | | Insecure XML SNMP | Exclude | Exclude | Default |

An * indicates a modified default rule

SSD Rules

| SSD Rules Table | | | | | | |
|--------------------------|-----------|-----------|-------------------|-----------------|-------------------|-----------|
| <input type="checkbox"/> | User Type | User Name | Channel | Read Permission | Default Read Mode | Rule Type |
| <input type="checkbox"/> | Level 15 | | Secure XML SNMP | Plaintext Only | Plaintext | Default |
| <input type="checkbox"/> | Level 15 | | Secure | Both | Encrypted | Default |
| <input type="checkbox"/> | Level 15 | | Insecure | Both | Encrypted | Default |
| <input type="checkbox"/> | All | | Secure | Encrypted Only | Encrypted | Default |
| <input type="checkbox"/> | All | | Insecure | Encrypted Only | Encrypted | Default |
| <input type="checkbox"/> | All | | Insecure XML SNMP | Exclude | Exclude | Default |

An * indicates a modified default rule

步驟2.按一下**Add**新增新的SSD規則。出現*Add SSD Rule*視窗。

User:
 Specific user (6/20 Characters Used)

Default User(cisco)

Level 15

All

Channel:
 Secure

Insecure

Secure XML SNMP

Insecure XML SNMP

Read Permission:
 Exclude

Plaintext Only

Encrypted Only

Both (Plaintext and Encrypted)

Default Read Mode:
 Exclude

Encrypted

Plaintext

步驟3.點選顯示SSD規則的所需使用者單選按鈕。可用選項包括：

- 特定使用者 — 輸入應用此規則的特定使用者名稱（不必定義此使用者）。
- 預設使用者(cisco) — 規則適用於預設使用者。
- 第15級 — 該規則適用於具有許可權級別15的所有使用者。在此，使用者可以訪問GUI並配置交換機。要更改許可權設定，請參閱*Sx500系列堆疊式交換機上的使用者帳戶配置一文*。
- 全部 — 規則適用於所有使用者。

User: Specific user (6/20 Characters Used)
 Default User(cisco)
 Level 15
 All

Channel: Secure
 Insecure
 Secure XML SNMP
 Insecure XML SNMP

Read Permission: Exclude
 Plaintext Only
 Encrypted Only
 Both (Plaintext and Encrypted)

Default Read Mode: Exclude
 Encrypted
 Plaintext

步驟4.在Channel欄位中點選與應用規則的輸入通道的安全級別對應的單選按鈕。可用選項包括：

·安全 — 此規則僅適用於安全通道（控制檯、SCP、SSH和HTTPS），不包括SNMP和XML通道。

·不安全 — 此規則僅適用於不安全的通道（Telnet、TFTP和HTTP），不包括SNMP和XML通道。

·安全XML SNMP — 此規則僅適用於具有隱私性的HTTPS和SNMPv3上的XML。

·不安全的XML SNMP — 此規則僅適用於使用HTTP或SNMPv1/v2和SNMPv3的XML，且沒有隱私性。

User: Specific user (6/20 Characters Used)
 Default User(cisco)
 Level 15
 All

Channel: Secure
 Insecure
 Secure XML SNMP
 Insecure XML SNMP

Read Permission: Exclude
 Plaintext Only
 Encrypted Only
 Both (Plaintext and Encrypted)

Default Read Mode: Exclude
 Encrypted
 Plaintext

步驟5.按一下所需的單選按鈕，在Read Permission欄位中定義與規則關聯的讀取許可權。可用選項包括：

·排除 — 最低級別的讀取許可權，不允許使用者以任何形式接收敏感資料。僅當在步驟4中按了一下Insecure時，此選項才可用。

·純文字檔案 — 與「排除」相比，讀取許可權級別更高。此選項允許使用者以純文字檔案格

式接收敏感資料。僅當在步驟4中按一下了Insecure時，此選項才可用。

·僅加密 — 中間級別的讀取許可權。此選項允許使用者接收僅加密的敏感資料。

·兩者（明文和加密） — 最高級別的讀取許可權。此選項允許使用者接收加密和明文許可權，並允許獲取敏感資料（以加密和明文形式）。

User: Specific user (6/20 Characters Used)
 Default User(cisco)
 Level 15
 All

Channel: Secure
 Insecure
 Secure XML SNMP
 Insecure XML SNMP

Read Permission: Exclude
 Plaintext Only
 Encrypted Only
 Both (Plaintext and Encrypted)

Default Read Mode: Exclude
 Encrypted
 Plaintext

步驟6.從Default Read Mode欄位按一下與所需讀取模式對應的單選按鈕。它定義賦予所有使用者的預設許可權。預設讀取模式選項的優先順序不高於「讀取許可權」欄位。可用選項包括：

·排除 — 不允許讀取敏感資料。僅當在步驟4中按一下Insecure時，此選項才可用。

·已加密 — 敏感資料以加密方式顯示。

·純文字檔案 — 敏感資料顯示為純文字檔案。

步驟7.在Add SSD Rule視窗中按一下**Save**。這些更改顯示在SSD規則表中，如下所示：

| SSD Rules | | | | | | |
|--------------------------|-----------|-----------|-------------------|-----------------|-------------------|--------------|
| SSD Rules Table | | | | | | |
| <input type="checkbox"/> | User Type | User Name | Channel | Read Permission | Default Read Mode | Rule Type |
| <input type="checkbox"/> | Specific | User_1 | Secure | Both | Plaintext | User Defined |
| <input type="checkbox"/> | Level 15 | | Secure XML SNMP | Plaintext Only | Plaintext | Default |
| <input type="checkbox"/> | Level 15 | | Secure | Both | Encrypted | Default |
| <input type="checkbox"/> | Level 15 | | Insecure | Both | Encrypted | Default |
| <input type="checkbox"/> | All | | Secure | Encrypted Only | Encrypted | Default |
| <input type="checkbox"/> | All | | Insecure | Encrypted Only | Encrypted | Default |
| <input type="checkbox"/> | All | | Insecure XML SNMP | Exclude | Exclude | Default |

An * indicates a modified default rule