

# Sx500系列堆疊式交換機上的管理訪問方法配置檔案規則配置

## 目標

訪問配置檔案充當交換機的另一安全層。訪問配置檔案最多可包含128條規則以提高安全性。每個規則都包含一個操作和標準。如果傳入的資料包匹配該規則，並且訪問方法匹配該管理方法，則會執行該操作。如果資料包與訪問配置檔案中的規則不匹配，則丟棄該資料包。如果訪問方法與管理方法不匹配，交換機將生成SYSLOG消息以通知網路管理員嘗試失敗。

本文說明如何在Sx500系列堆疊式交換機上配置配置檔案規則。

**附註：**要配置訪問配置檔案規則，您需要配置訪問配置檔案，請參閱Sx500系列交換機上的管理訪問身份驗證設定。

## 適用裝置

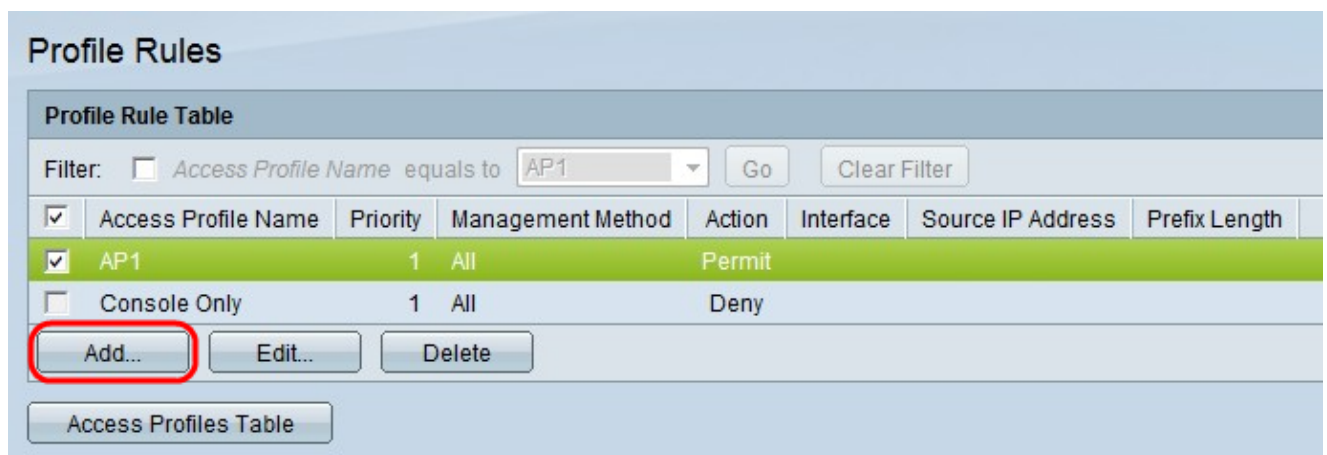
·Sx500系列堆疊式交換器

## 軟體版本

•1.3.0.62

## 配置檔案規則

步驟1.登入到Web配置實用程式，然後選擇**Security > Mgmt Access Method > Profile Rules**。將開啟*Profile Rules*頁面：



The screenshot displays the 'Profile Rules' configuration page. At the top, there is a filter section with a checkbox for 'Access Profile Name equals to' and a dropdown menu set to 'AP1'. Below this is a table with the following data:

<input checked="" type="checkbox"/>	Access Profile Name	Priority	Management Method	Action	Interface	Source IP Address	Prefix Length
<input checked="" type="checkbox"/>	AP1	1	All	Permit			
<input type="checkbox"/>	Console Only	1	All	Deny			

Below the table are three buttons: 'Add...' (highlighted with a red circle), 'Edit...', and 'Delete'. At the bottom of the page, there is a button labeled 'Access Profiles Table'.

步驟2.選中與所需訪問配置檔名稱對應的覈取方塊，然後點選**Add**以新增新的配置檔案規則。出現「Add Profile Rule」視窗。

Access Profile Name: **AP1** ▼

---

\* Rule Priority:  (Range: 1 - 65535)

Management Method:

- All
- Telnet
- Secure Telnet (SSH)
- HTTP
- Secure HTTP (HTTPS)
- SNMP

Action:

- Permit
- Deny

---

Applies to Interface:  All  User Defined

Interface:  Unit/Slot  Port   LAG   VLAN

---

Applies to Source IP Address:  All  User Defined

IP Version:  Version 6  Version 4

\* IP Address:

\* Mask:

- Network Mask
- Prefix Length  (Range: 0 - 32)

步驟3. ( 可選 ) 從Access Profile Name下拉選單中選擇要新增規則的訪問配置檔案。

Access Profile Name: AP1

---

\* Rule Priority: 1 (Range: 1 - 65535)

Management Method:

- All
- Telnet
- Secure Telnet (SSH)
- HTTP
- Secure HTTP (HTTPS)
- SNMP

Action:

- Permit
- Deny

---

Applies to Interface:  All  User Defined

Interface:  Unit/Slot 1/2 Port FE1  LAG 1  VLAN 1

---

Applies to Source IP Address:  All  User Defined

IP Version:  Version 6  Version 4

\* IP Address:

\* Mask:

- Network Mask
- Prefix Length  (Range: 0 - 32)

步驟4.在「規則優先順序」欄位中輸入規則優先順序的值。規則優先順序將資料包與規則相匹配。首先檢查優先順序較低的規則。如果資料包與規則匹配，則執行所需的操作。

Access Profile Name:

---

✳ Rule Priority:  (Range: 1 - 65535)

Management Method:

- All
- Telnet
- Secure Telnet (SSH)
- HTTP
- Secure HTTP (HTTPS)
- SNMP

Action:

- Permit
- Deny

---

Applies to Interface:  All  User Defined

Interface:  Unit/Slot  Port   LAG   VLAN

---

Applies to Source IP Address:  All  User Defined

IP Version:  Version 6  Version 4

✳ IP Address:

✳ Mask:  Network Mask   Prefix Length  (Range: 0 - 32)

步驟5.在Management Method欄位中點選與所需管理方法對應的單選按鈕。使用者使用的訪問方法必須與管理方法匹配才能執行操作。

Access Profile Name: AP1

---

✱ Rule Priority: 1 (Range: 1 - 65535)

Management Method:

- All
- Telnet
- Secure Telnet (SSH)
- HTTP
- Secure HTTP (HTTPS)
- SNMP

Action:

- Permit
- Deny

---

Applies to Interface:  All  User Defined

Interface:  Unit/Slot 1/2 Port FE1  LAG 1  VLAN 1

---

Applies to Source IP Address:  All  User Defined

IP Version:  Version 6  Version 4

✱ IP Address:

✱ Mask:  Network Mask   Prefix Length  (Range: 0 - 32)

步驟6.點選與「操作」欄位中所需操作對應的單選按鈕。

- Permit — 允許使用者使用步驟5中選擇的訪問方法訪問交換機。
- 拒絕 — 拒絕使用者通過步驟5中選擇的存取方法存取交換器。

Access Profile Name: AP1

✱ Rule Priority: 1 (Range: 1 - 65535)

Management Method:

- All
- Telnet
- Secure Telnet (SSH)
- HTTP
- Secure HTTP (HTTPS)
- SNMP

Action:

- Permit
- Deny

Applies to Interface:  All  User Defined

Interface:  Unit/Slot 1/2 Port FE1  LAG 1  VLAN 1

Applies to Source IP Address:  All  User Defined

IP Version:  Version 6  Version 4

✱ IP Address: [ ]

✱ Mask:

- Network Mask [ ]
- Prefix Length [ ] (Range: 0 - 32)

Apply Close

步驟7.在Apply to Interface欄位中點選與所需介面對應的單選按鈕。

- 所有 — 適用於交換機上的所有埠、LAG和VLAN ( 上述步驟5和步驟6規則 )。
- 使用者定義 — 僅應用於交換機上所選埠、LAG或VLAN的上述步驟5和步驟6規則。

Access Profile Name: AP1

---

✱ Rule Priority: 1 (Range: 1 - 65535)

Management Method:

- All
- Telnet
- Secure Telnet (SSH)
- HTTP
- Secure HTTP (HTTPS)
- SNMP

Action:

- Permit
- Deny

---

Applies to Interface:  All  User Defined

Interface:  Unit/Slot 1/2  Port FE1  LAG 1  VLAN 1

---

Applies to Source IP Address:  All  User Defined

IP Version:  Version 6  Version 4

✱ IP Address:

✱ Mask:  Network Mask   Prefix Length  (Range: 0 - 32)

步驟8.如果在上一步中選擇了User Defined (使用者定義)，則點選與Interface (介面) 欄位中的所需介面對應的單選按鈕。從Unit/Slot and Port下拉選單中選擇埠，從LAG下拉選單中選擇LAG，或者從VLAN下拉選單中選擇VLAN。

Access Profile Name:

---

✱ Rule Priority:  (Range: 1 - 65535)

Management Method:

- All
- Telnet
- Secure Telnet (SSH)
- HTTP
- Secure HTTP (HTTPS)
- SNMP

Action:

- Permit
- Deny

---

Applies to Interface:  All  User Defined

Interface:  Unit/Slot  Port   LAG   VLAN

---

Applies to Source IP Address:  All  User Defined

IP Version:  Version 6  Version 4

✱ IP Address:

✱ Mask:

- Network Mask
- Prefix Length  (Range: 0 - 32)

步驟9.點選與Apply to Source IP Address欄位中所需的IP地址對應的單選按鈕。

·所有 — 適用於所有型別的IP地址。

·使用者定義 — 僅適用於此處定義的允許或拒絕上述規則的IP地址型別。

**Timesaver:**如果在步驟9中選擇了All，請跳到步驟13。



Access Profile Name:

---

**Rule Priority:**  (Range: 1 - 65535)

**Management Method:**

- All
- Telnet
- Secure Telnet (SSH)
- HTTP
- Secure HTTP (HTTPS)
- SNMP

**Action:**

- Permit
- Deny

---

**Applies to Interface:**  All  User Defined

**Interface:**  Unit/Slot  Port   LAG   VLAN

---

**Applies to Source IP Address:**  All  User Defined

**IP Version:**  Version 6  Version 4

**IP Address:**

**Mask:**

- Network Mask
- Prefix Length  (Range: 0 - 32)

步驟10.如果選擇了「使用者定義」，則點選與「IP版本」欄位中支援的IP版本對應的單選按鈕。

Access Profile Name: AP1

Rule Priority: 1 (Range: 1 - 65535)

Management Method:  
 All  
 Telnet  
 Secure Telnet (SSH)  
 HTTP  
 Secure HTTP (HTTPS)  
 SNMP

Action:  
 Permit  
 Deny

Applies to Interface:  All  User Defined

Interface:  Unit/Slot 1/2 Port FE1  LAG 1  VLAN 1

Applies to Source IP Address:  All  User Defined

IP Version:  Version 6  Version 4

IP Address: 192.168.0.1

Mask:  
 Network Mask  
 Prefix Length (Range: 0 - 32)

Apply Close

步驟11.在「IP地址」欄位中輸入源IP地址。

Access Profile Name: AP1

Rule Priority: 1 (Range: 1 - 65535)

Management Method:
 

- All
- Telnet
- Secure Telnet (SSH)
- HTTP
- Secure HTTP (HTTPS)
- SNMP

Action:
 

- Permit
- Deny

Applies to Interface:
 

- All
- User Defined

Interface:
 

- Unit/Slot 1/2 Port FE1
- LAG 1
- VLAN 1

Applies to Source IP Address:
 

- All
- User Defined

IP Version:
 

- Version 6
- Version 4

IP Address: 192.168.0.1

Mask:
 

- Network Mask 255.255.255.0
- Prefix Length (Range: 0 - 32)

Apply Close

步驟12.點選與Mask欄位中的網路掩碼對應的單選按鈕。

·網路掩碼 — 在網路掩碼欄位中輸入網路掩碼。這將定義源IP地址的子網掩碼。

·字首長度(Prefix Length) — 在「字首長度」(Prefix length)欄位中輸入字首長度 ( 介於0到32之間的整數 )。這將通過源IP地址的字首長度定義子網掩碼。

步驟13.按一下Apply。

Profile Rules

Profile Rule Table

Filter:  Access Profile Name equals to AP1 Go Clear Filter

<input checked="" type="checkbox"/>	Access Profile Name	Priority	Management Method	Action	Interface	Source IP Address	Prefix Length
<input checked="" type="checkbox"/>	AP1	1	All	Permit			
<input type="checkbox"/>	Console Only	1	All	Deny			

Add... Edit... Delete

Access Profiles Table

步驟14。(可選)要編輯配置檔案規則，請選中所需的訪問配置檔案覈取方塊，然後按一下Edit。

步驟15。(可選)要從配置檔案規則表中刪除訪問配置檔案規則，請選中所需的訪問配置檔案覈取方塊，然後按一下Delete。