在ISE中配置IP訪問限制

目錄

簡介

本文檔介紹在ISE 3.1、3.2和3.3中配置IP訪問限制的可用選項。

必要條件

需求

思科建議您瞭解以下主題：

- 思科身份服務引擎的基本知識

採用元件

- 思科身分辨識服務引擎版本3.1
- 思科身分辨識服務引擎版本3.2
- 思科身分辨識服務引擎版本3.3

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

IP訪問限制功能允許管理員控制哪些IP地址或範圍可以訪問ISE管理員門戶和服務。

此功能適用於各種ISE介面和服務，包括：

- 管理員門戶訪問和CLI
- ERS API訪問
- 訪客和發起人門戶訪問
- 我的裝置門戶訪問

啟用時，ISE僅允許來自指定IP地址或範圍的連線。從非指定IP訪問ISE管理介面的任何嘗試都會被阻止。

在意外鎖定情況下，ISE提供可以繞過IP訪問限制的「安全模式」啟動選項。這允許管理員重新獲得訪問許可權並糾正任何錯誤配置。

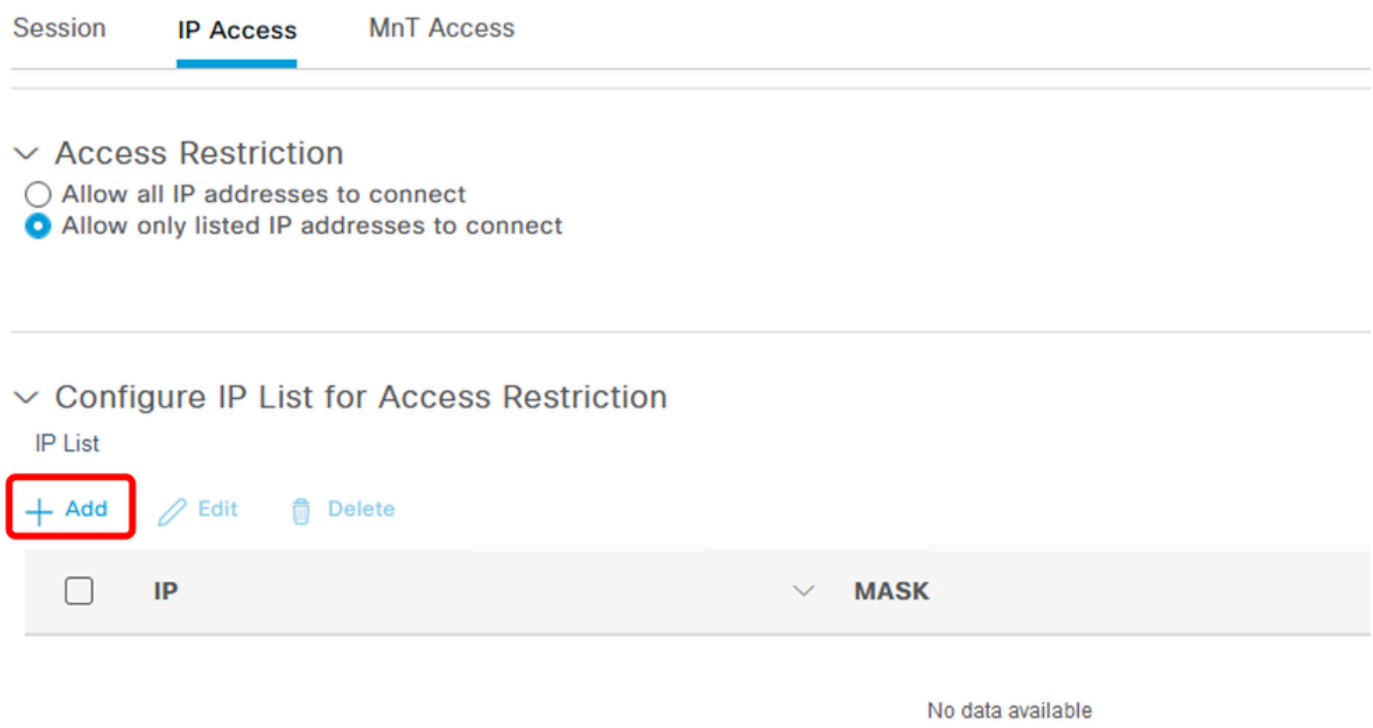
ISE 3.1及更低版本中的行為

導航到Administration > Admin Access > Settings > Access。您有以下選項：

- 工作階段
- IP存取
- MnT訪問

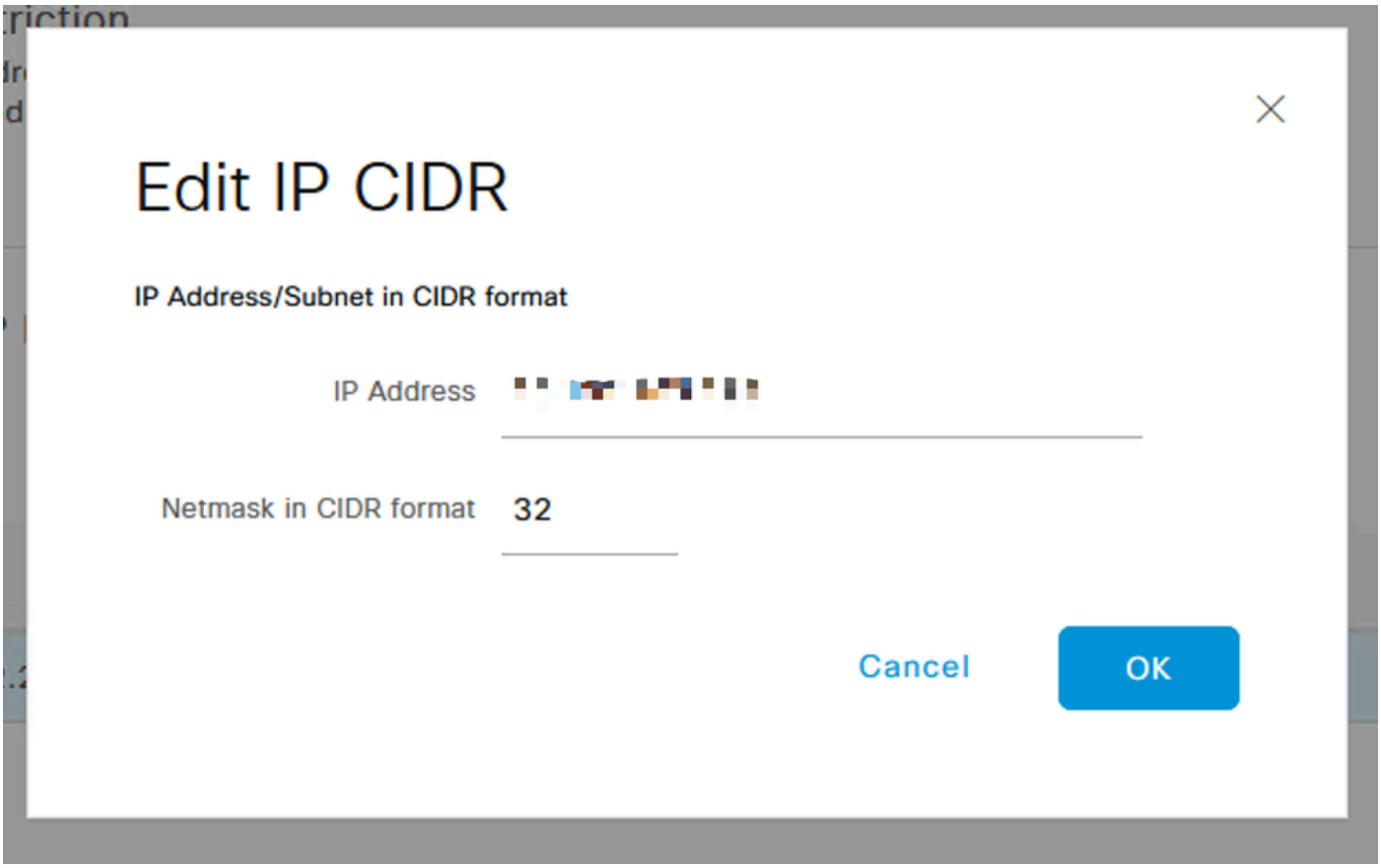
設定

- 選擇「僅允許列出的IP地址連線」
- 按一下「新增」

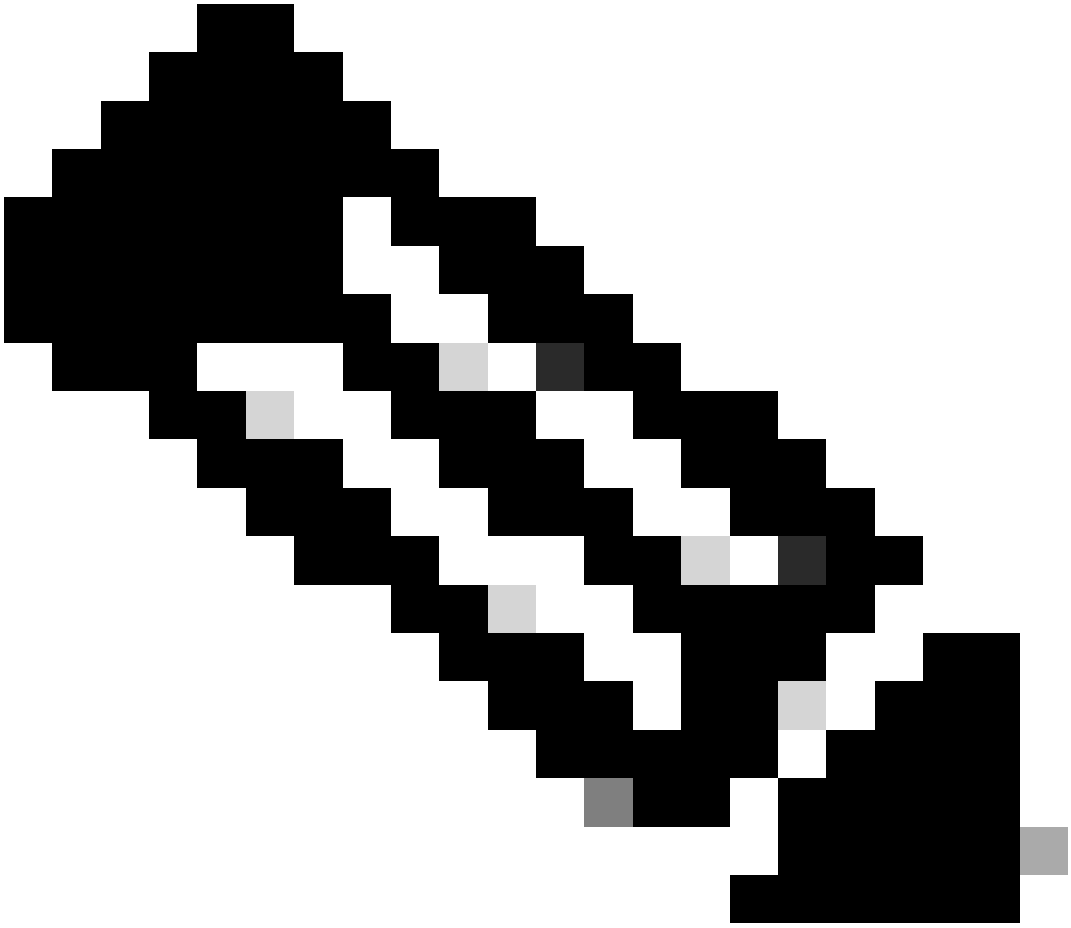


IP訪問配置

- 在ISE 3.1中，您沒有在「管理員」和「使用者」服務之間選擇的選項，啟用IP訪問限制阻止連線到：
  - GUI
  - CLI
  - SNMP
  - SSH
- 將打開一個對話方塊，您可以在其中輸入CIDR格式的IP地址IPv4或IPv6。
- 配置IP後，請以CIDR格式設定掩碼。


Edit IP CIDR
IP Address/Subnet in CIDR format
IP Address
Netmask in CIDR format
32
Cancel
OK

編輯IP CIDR

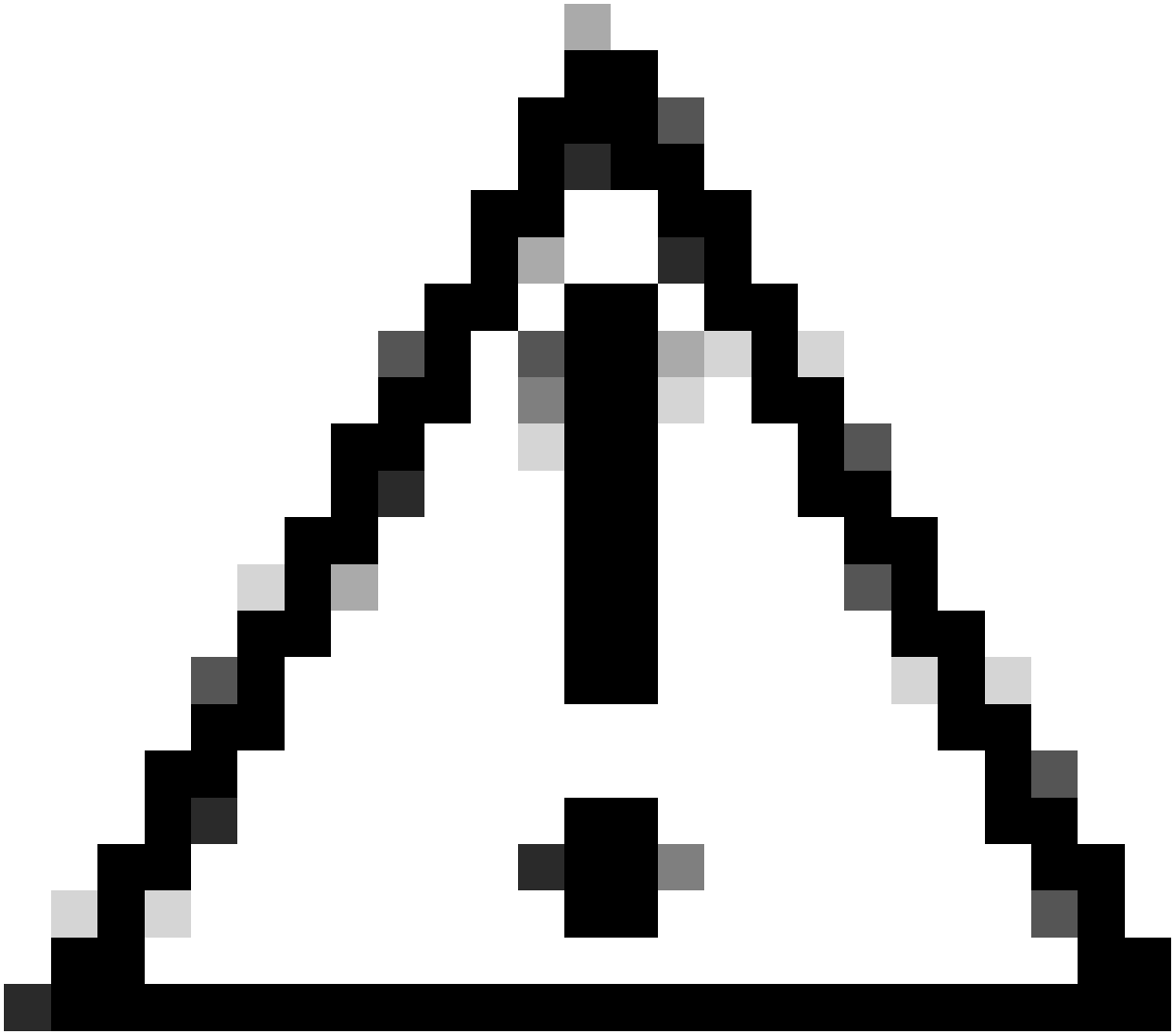


注意：IP CIDR（無類域間路由）格式是一種表示IP地址及其相關路由字首的方法。

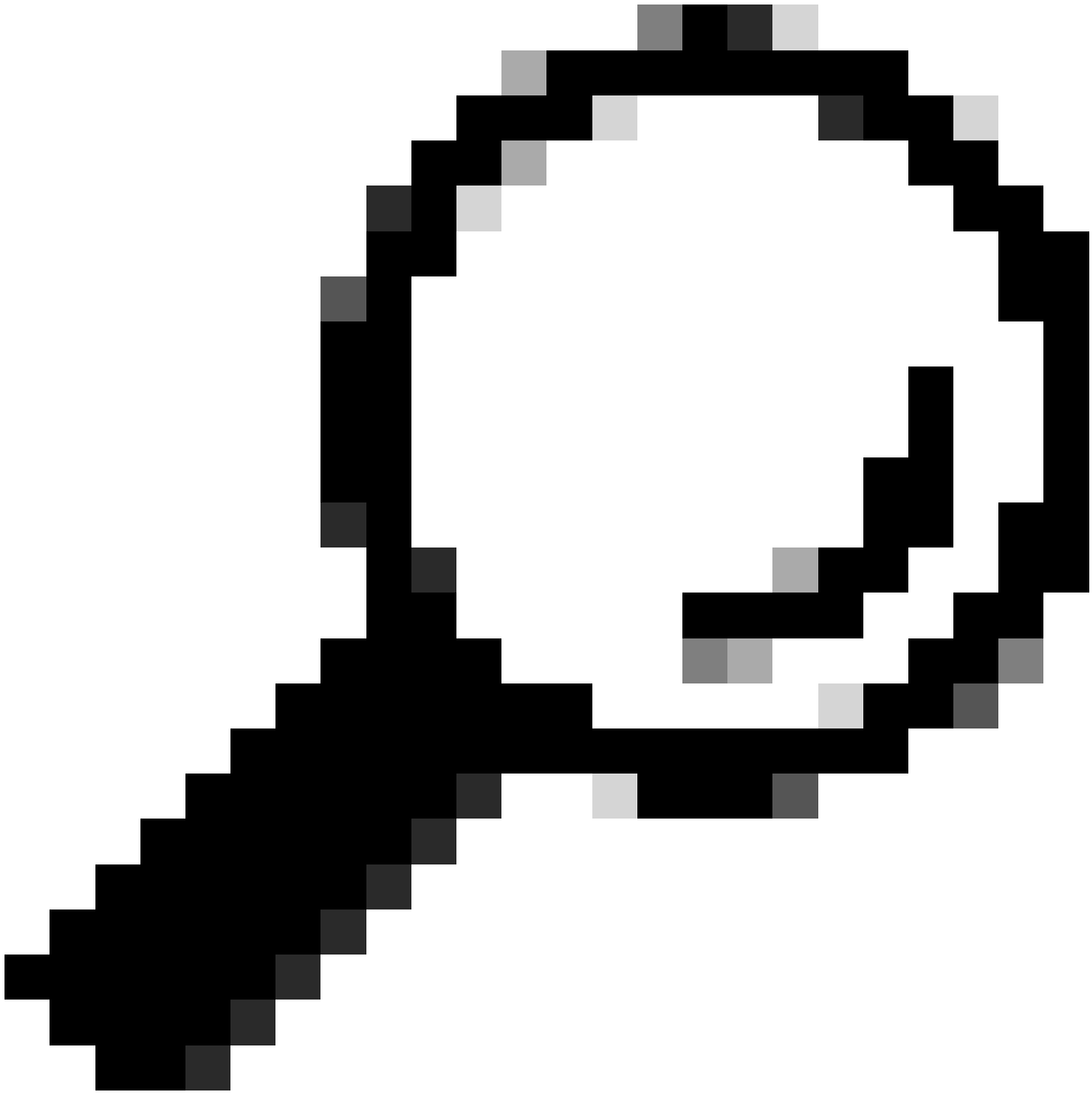
範例：

IP：10.8.16.32

遮罩： /32



注意：配置IP限制時必須小心，以免意外鎖定合法管理員訪問。Cisco建議在完全實施任何IP限制配置之前對其進行全面測試。



提示：對於IPv4地址：

- 對特定IP地址使用/32。
- 對於子網，請使用任何其他選項。範例： 10.26.192.0/18

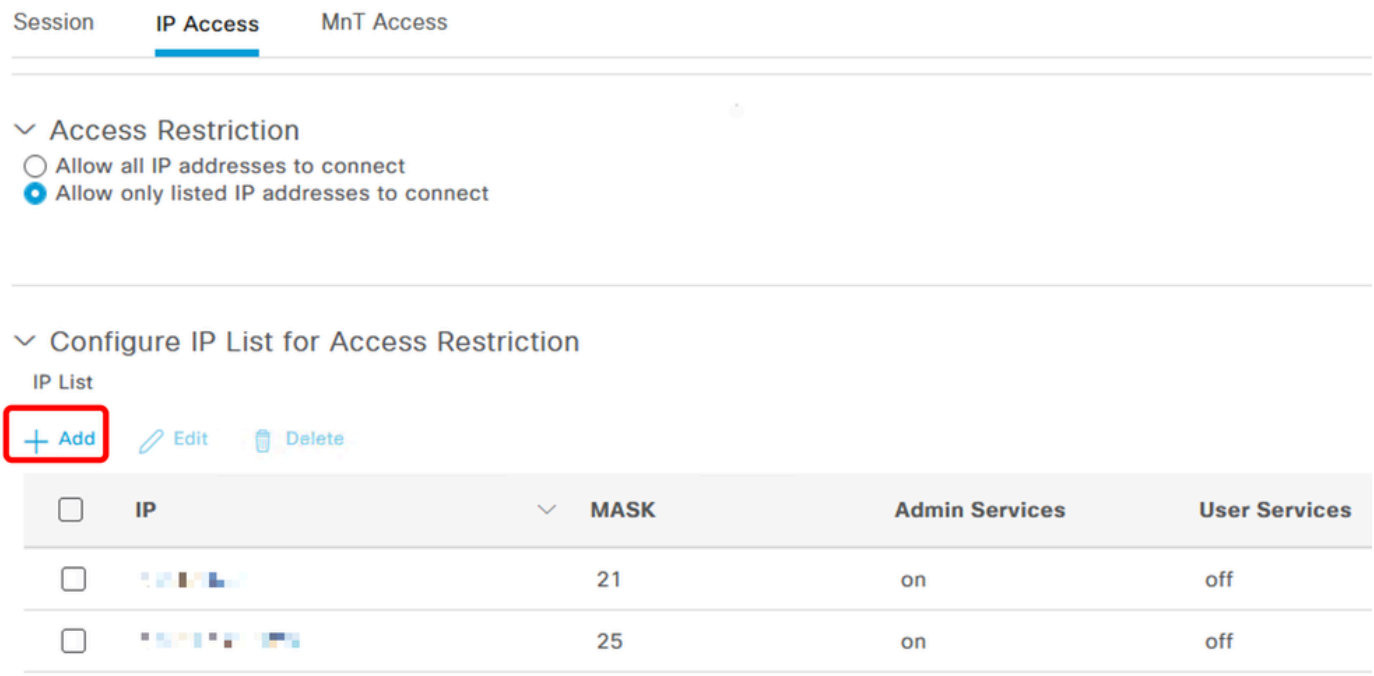
ISE 3.2中的行為

導航到Administration > Admin Access > Settings > Access。您可使用以下選項：

- 工作階段
- IP存取
- MnT訪問

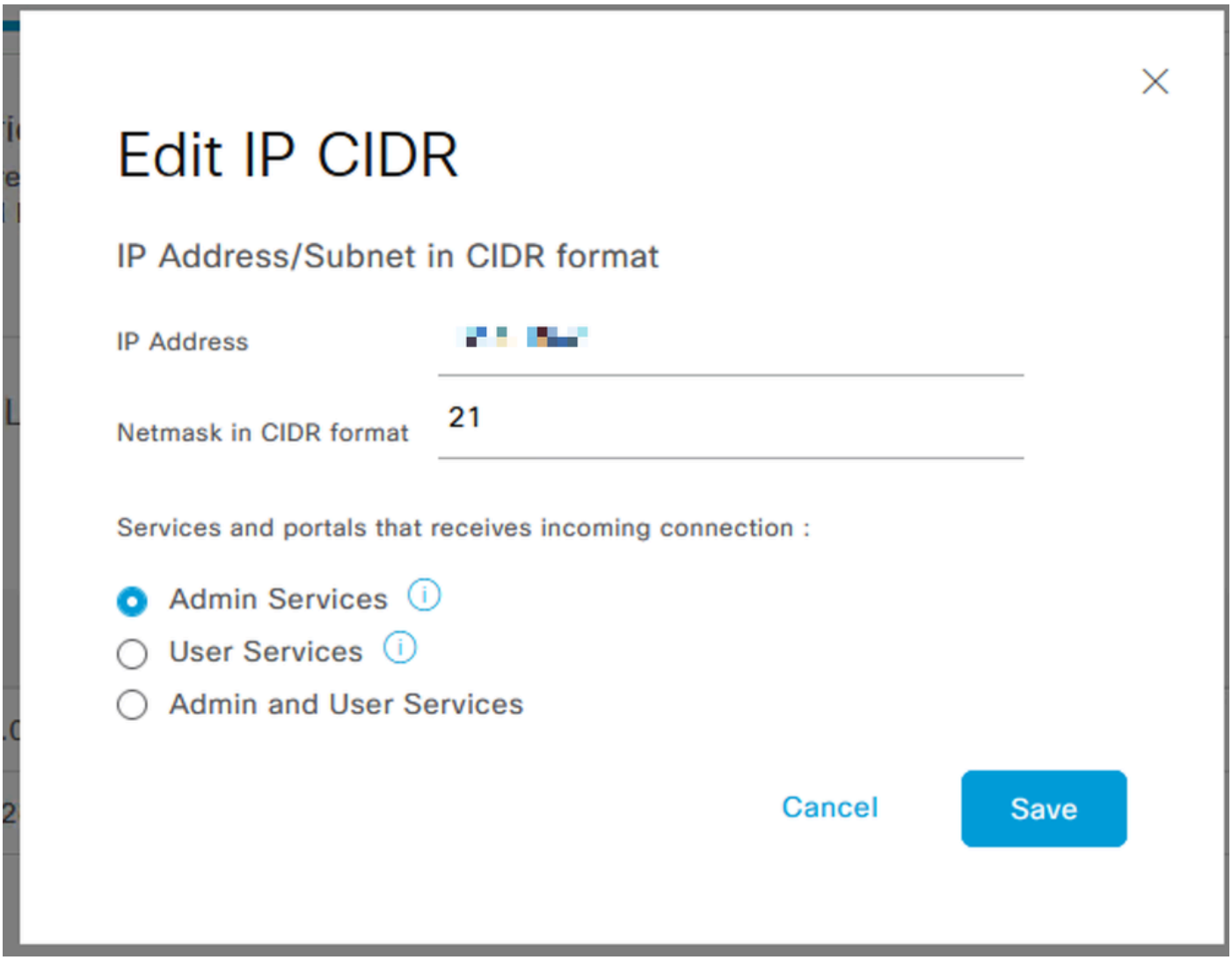
設定

- 選擇「僅允許列出的IP地址連線」
- 按一下「新增」



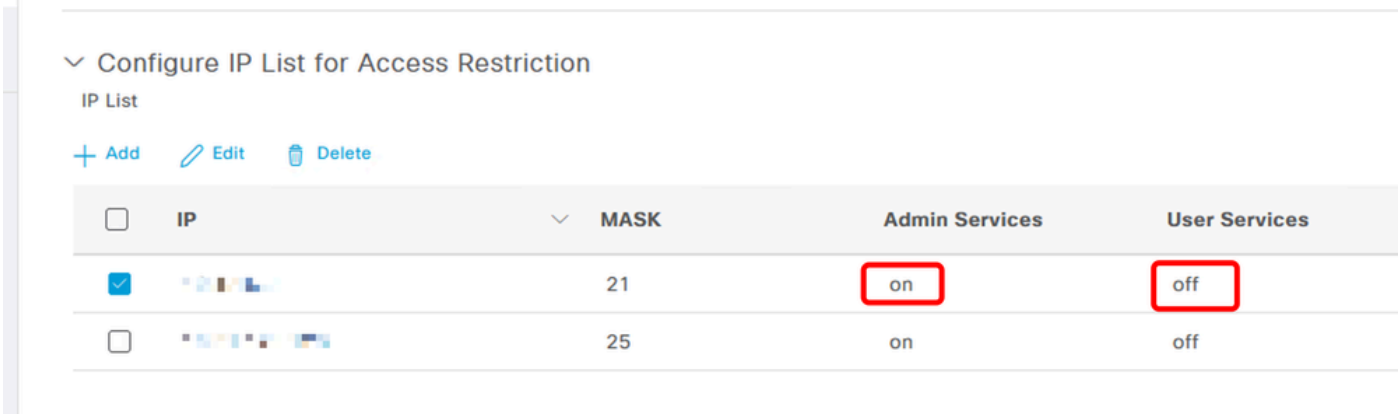
IP訪問配置

- 將打開一個對話方塊，您可以在其中輸入CIDR格式的IP地址IPv4或IPv6。
- 配置IP後，請以CIDR格式設定掩碼。
- 這些選項可用於IP訪問限制
  - 管理服務：GUI、CLI (SSH)、SNMP、ERS、OpenAPI、UDN、API網關、PxGrid（在修補2中停用）、MnT分析
  - 使用者服務：訪客、BYOD、狀態、分析
  - 管理員和使用者服務



編輯IP CIDR

- 點選「儲存」按鈕
- 「ON」表示啟用管理服務，「OFF」表示停用使用者服務。



3.2中的IP訪問配置

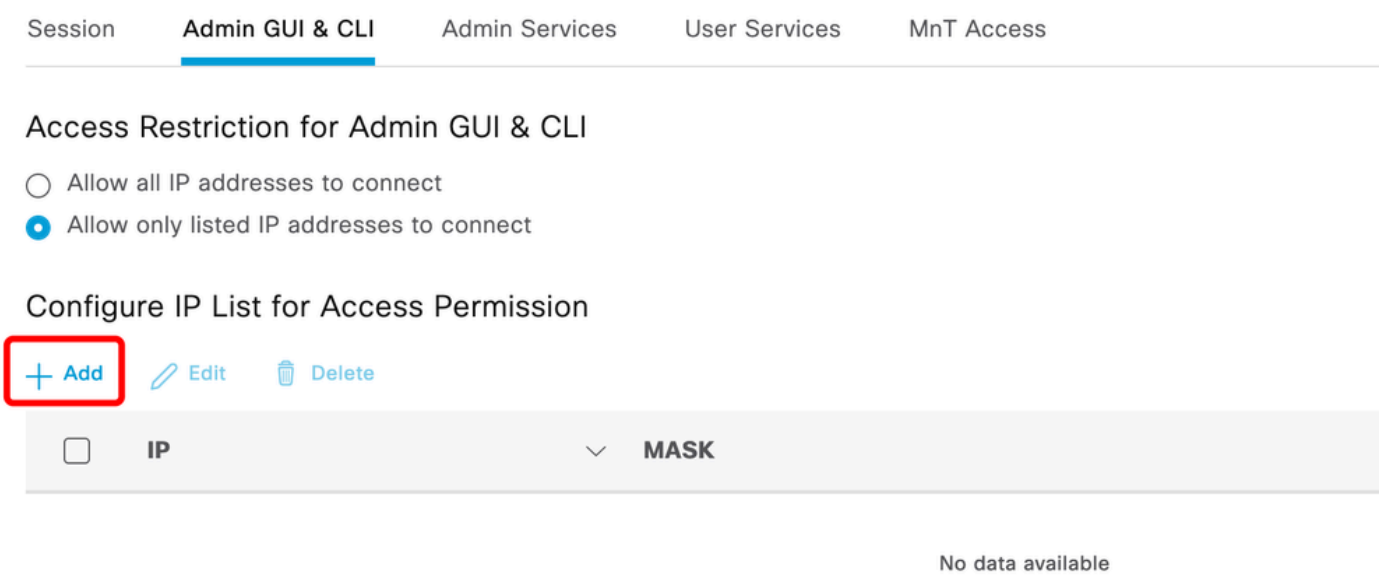
ISE 3.2 P4及更高版本中的行為

導航到Administration > Admin Access > Settings > Access。您可使用以下選項：

- 工作階段
- 管理GUI&CLI：ISE GUI (TCP 443)、ISE CLI (SSH TCP22)和SNMP。
- 管理服務：ERS API、Open API、pxGrid、DataConnect。
- 使用者服務：訪客、BYOD、安全評估。
- MNT訪問：使用此選項，ISE不使用從外部源傳送的系統日誌消息。

設定

- 選擇「僅允許列出的IP地址連線」
- 按一下「新增」



3.3中的IP訪問配置

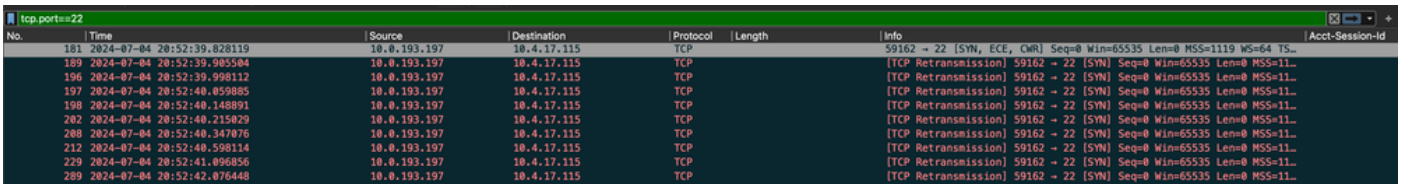
- 將打開一個對話方塊，您可以在其中輸入CIDR格式的IP地址IPv4或IPv6。
- 配置IP後，請以CIDR格式設定掩碼。
- 按一下「新增」

恢復ISE GUI/CLI

- 使用控制檯登入
- 使用應用停止ise停止ISE服務
- 使用應用啟動ise safe啟動ISE服務
- 從GUI中刪除IP訪問限制。

疑難排解

進行資料包捕獲，驗證ISE是否無響應或丟棄流量。



檢查ISE防火牆規則

- 對於3.1及更低版本，您只能在show tech中檢查此配置。
  - 您可以使用show tech-support file <filename>」將show tech檔案存入localdisk中
  - 然後，您可以使用「copy disk：/<filename> ftp://<ip_address>/path」將檔案傳輸到儲存庫，儲存庫url將根據您使用的儲存庫型別而變化
  - 您可以將檔案下載到您的電腦，以便讀取檔案並尋找「Running iptables -nvL」
  - show tech的初始規則不包含於下方。換句話說，您可以在此處找到附加到show tech by IP Access限制功能的最後規則。

<#root>

```
****************************************
Running iptables -nvL...
****************************************
.
.
Chain ACCEPT_22_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- eth0 * x.x.x.x/x 0.0.0.0/0
```

tcp dpt:22

Firewall rule permitting the SSH traffic from segment x.x.x.x/x

```
461 32052 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
65 4048 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain ACCEPT_161_udp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT udp -- * * x.x.x.x/x 0.0.0.0/0
```

udp dpt:161

Firewall rule permitting the SNMP traffic from segment x.x.x.x/x

```
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0
```

- 對於3.2及更高版本，您可以使用命令「show firewall」檢查防火牆規則。
- 3.2及更高版本可以更好地控制IP訪問限制所阻止的服務。

<#root>

gjuarezo-311/admin#show firewall

.

.

Chain ACCEPT_22_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
170 13492 ACCEPT tcp -- eth0 * x.x.x.x/x 0.0.0.0/0

tcp dpt:22

Firewall rule permitting the SSH traffic from segment x.x.x.x/x

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
13 784 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain ACCEPT_161_udp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT udp -- * * x.x.x.x/x 0.0.0.0/0

udp dpt:161

Firewall rule permitting the SNMP traffic from segment x.x.x.x/x

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain ACCEPT_8910_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- * * x.x.x.x/x 0.0.0.0/0

tcp dpt:8910

Firewall rule permitting the PxGrid traffic from segment x.x.x.x/x

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
90 5400 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain ACCEPT_8443_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- * * x.x.x.x/x 0.0.0.0/0

tcp dpt:8443 F

irewall rule permitting the HTTPS traffic from segment x.x.x.x/x

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain ACCEPT_8444_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- * * x.x.x.x/x 0.0.0.0/0

tcp dpt:8444 F

irewall rule permitting the Block List Portal traffic from segment x.x.x.x/x

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain ACCEPT_8445_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- * * x.x.x.x/x 0.0.0.0/0

tcp dpt:8445 F

irewall rule permitting the Sponsor Portal traffic from segment x.x.x.x/x

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

檢查調試日誌

警告：並非所有流量都會生成日誌。IP訪問限制可以在應用級別和使用Linux內部防火牆阻止流量。SNMP、CLI和SSH在防火牆級別被阻止，因此不會生成任何日誌。

- 在GUI的DEBUG中啟用「基礎架構」元件。
- 使用show logging application ise-psc.log tail

當IP訪問限制執行操作時，可以檢視以下日誌。

```
2024-07-04 18:19:11,339 DEBUG [admin-http-pool31][] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCa
2024-07-04 18:19:11,339 DEBUG [admin-http-pool31][] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCa
2024-07-04 18:19:11,339 DEBUG [admin-http-pool31][] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCa
2024-07-04 18:19:11,339 DEBUG [admin-http-pool31][] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCa
2024-07-04 18:19:11,339 DEBUG [admin-http-pool31][] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCa
```

相關資訊

- 思科技術支援與下載
- ISE 3.1管理指南
- ISE 3.2管理指南
- ISE 3.3管理指南

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。