ISEでのIPアクセス制限の設定

内容

はじめに

このドキュメントでは、ISE 3.1、3.2、および3.3でIPアクセス制限を設定するために使用できるオプションについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Identity Service Engine(ISE)の基礎知識

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

IPアクセス制限機能を使用すると、管理者は、どのIPアドレスまたは範囲がISE管理ポータルおよびサービスにアクセスできるかを制御できます。

この機能は、次のようなさまざまなISEインターフェイスおよびサービスに適用されます。

- 管理ポータルアクセスおよびCLI
- ERS APIアクセス
- ゲストおよびスポンサーポータルへのアクセス
- My Devicesポータルへのアクセス

有効にすると、ISEは指定されたIPアドレスまたは範囲からの接続のみを許可します。指定されていないIPからISE管理インターフェイスにアクセスしようとすると、ブロックされます。

誤ってロックアウトが発生した場合、ISEには、IPアクセス制限をバイパスできる「セーフモード」起動オプションが用意されています。これにより、管理者はアクセスを回復し、設定ミスを修正できます。

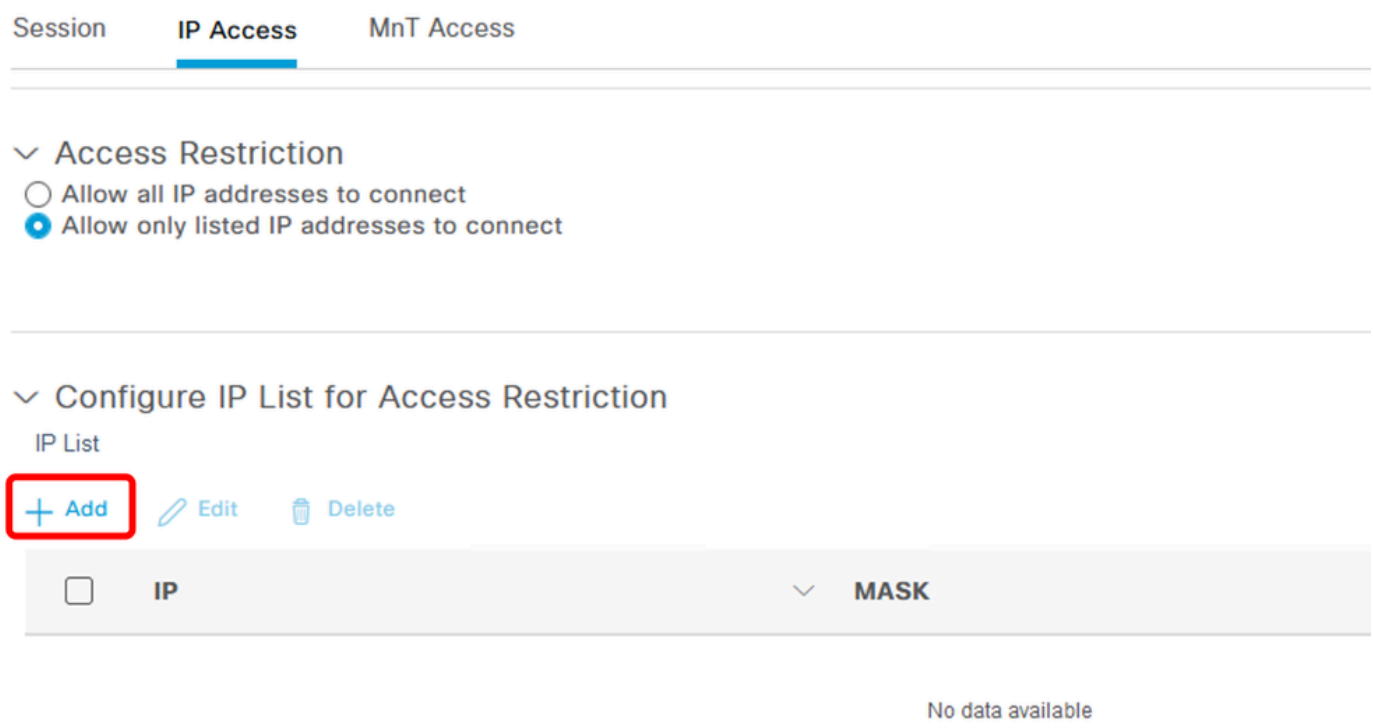
ISE 3.1以下での動作

「管理」>「管理アクセス」>「設定」>「アクセス」にナビゲートします。次のオプションがあります。

- セッション
- IPアクセス
- MnTアクセス

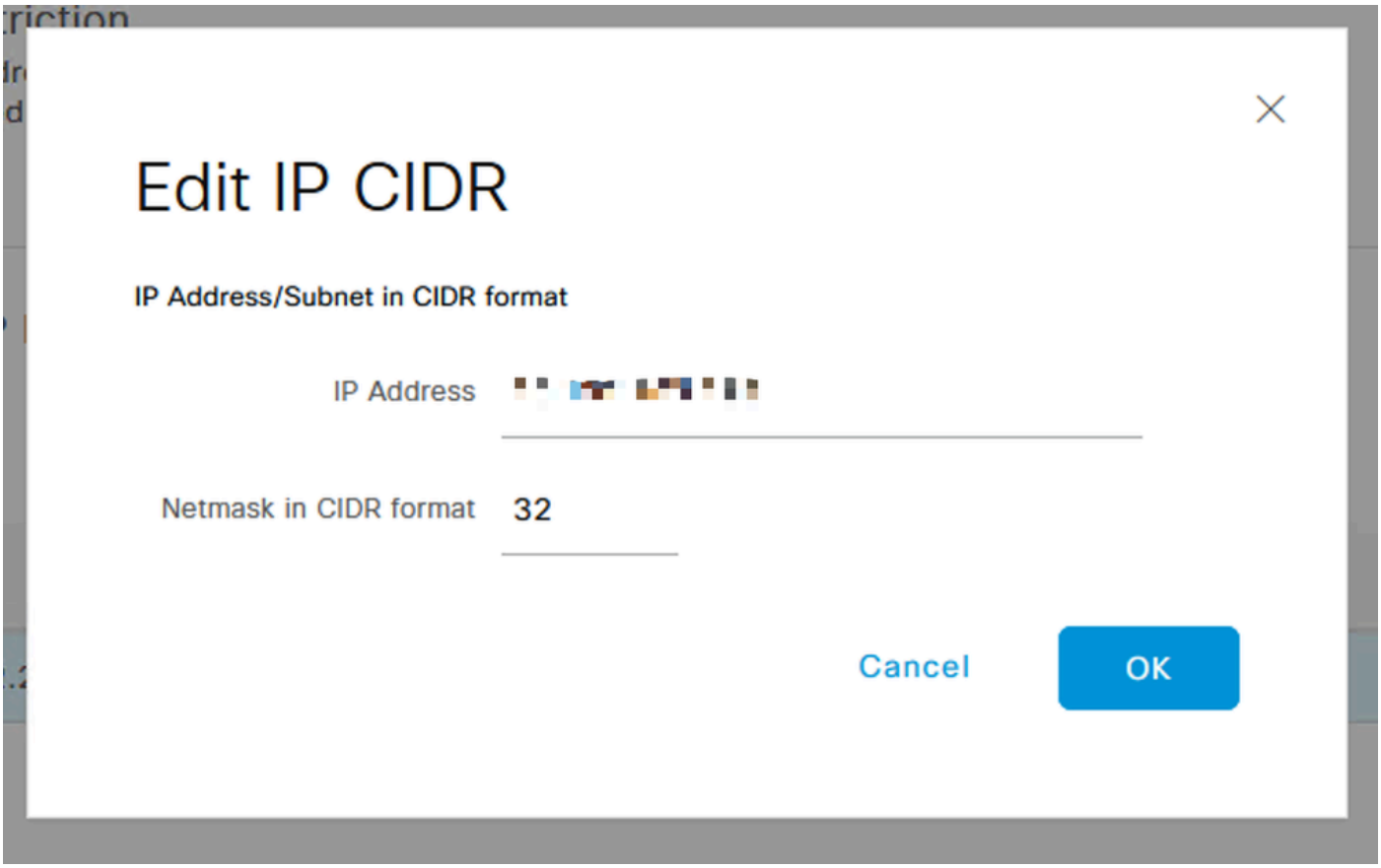
設定

- 「リストされているIPアドレスのみに接続を許可する」を選択します。
- [追加]をクリックします

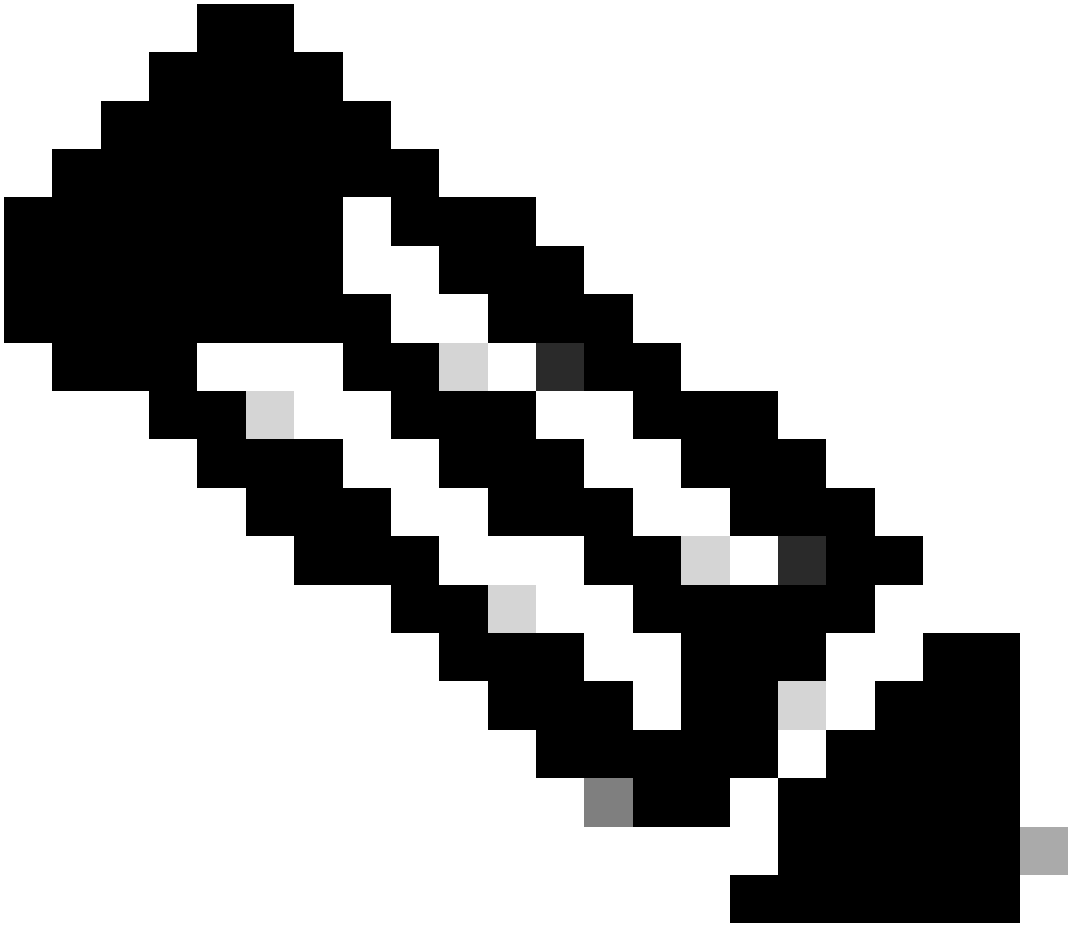


IPアクセスの設定

- ISE 3.1では、「Admin」サービスと「User」サービスの間で選択するオプションがないため、IPアクセス制限を有効にすると次の接続先がブロックされます。
  - GUI
  - CLI を使う場合：
  - SNMP
  - SSH
- ダイアログボックスが開き、IPアドレス（IPv4またはIPv6）をCIDR形式で入力できます。
- IPを設定したら、CIDR形式でマスクを設定します。


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

IP CIDRの編集

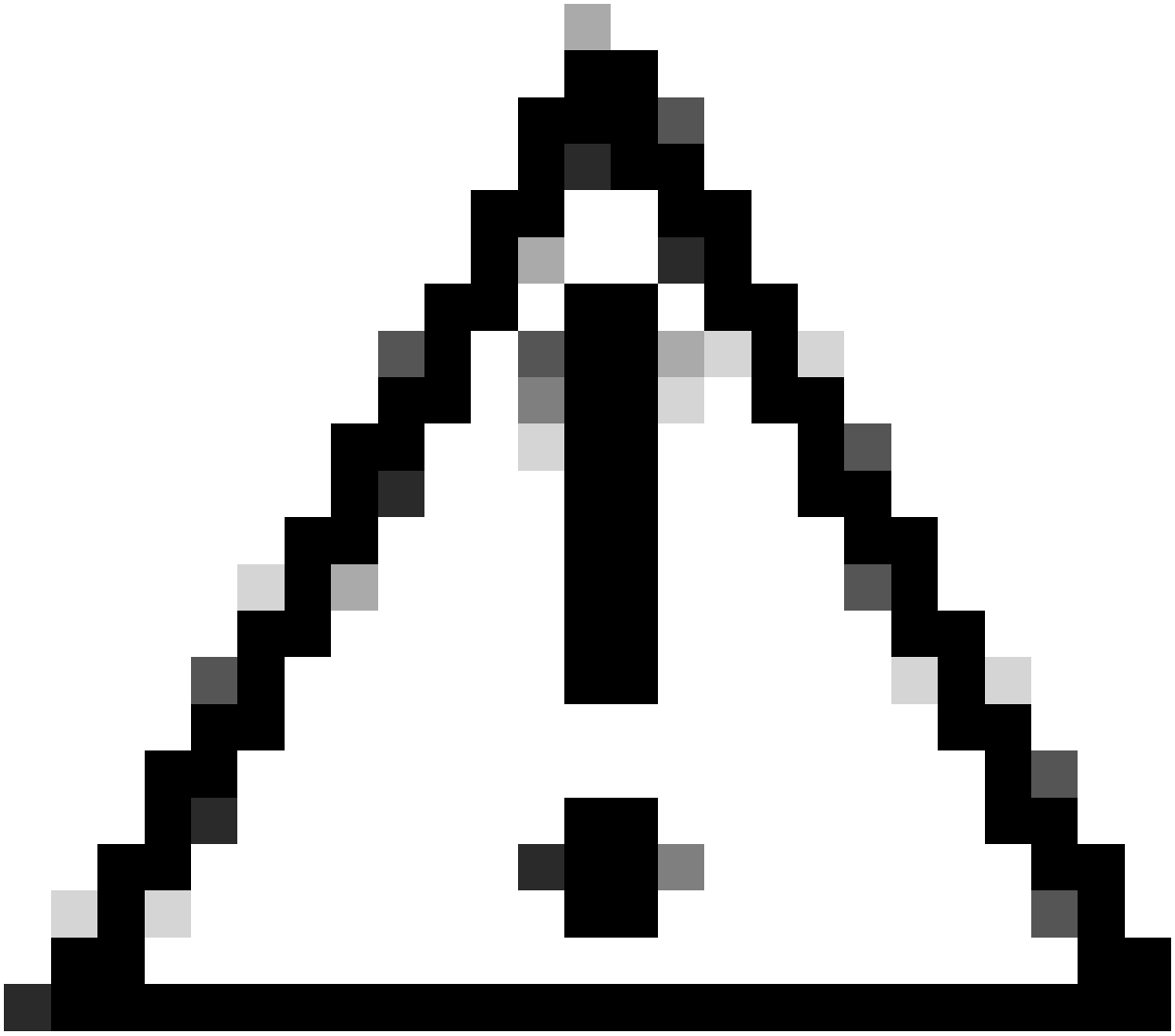


注:IP CIDR（クラスレスドメイン間ルーティング）形式は、IPアドレスとそれに関連付けられたルーティングプレフィックスを表す方法です。

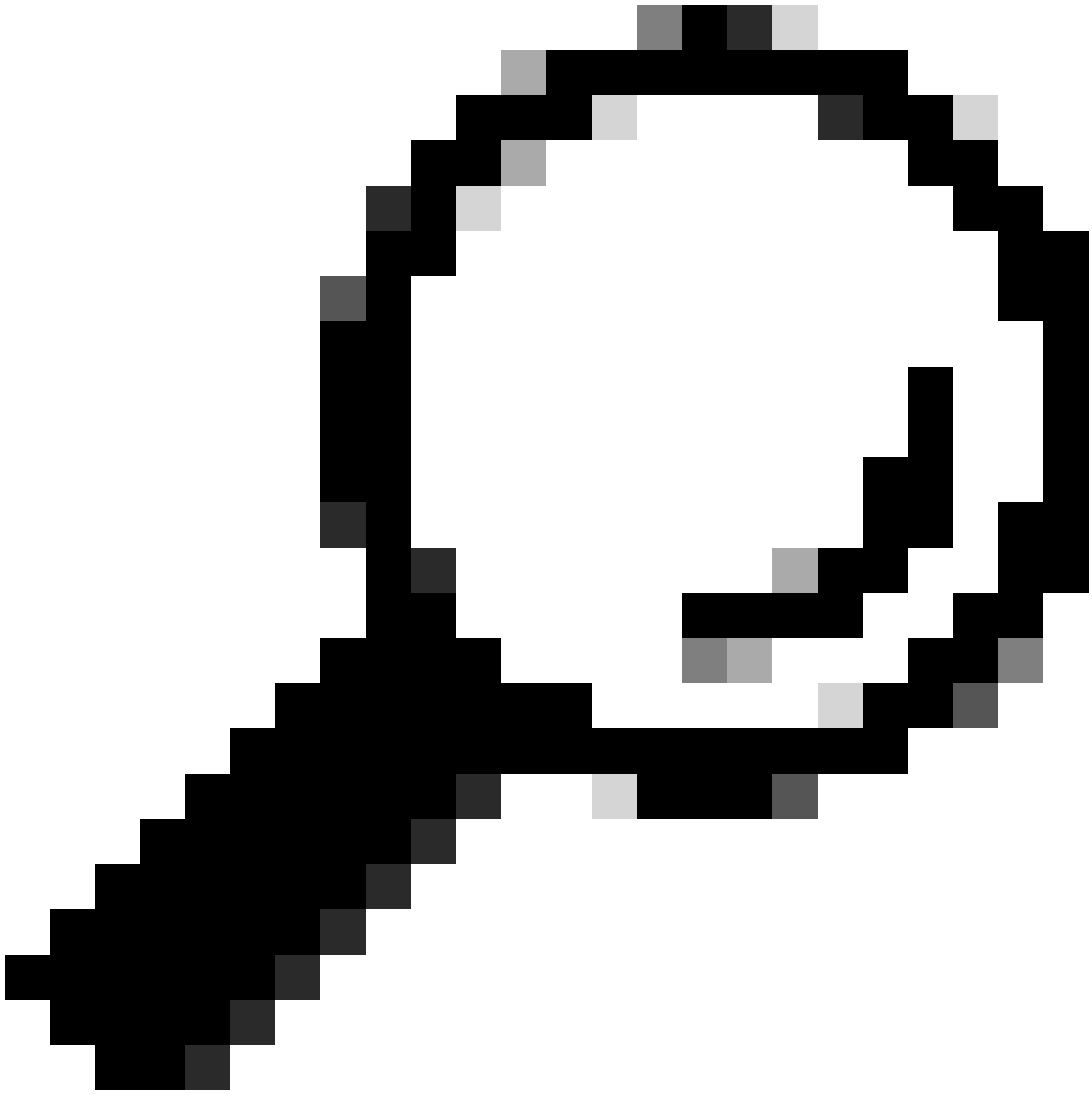
以下に例を挙げます。

IP:10.8.16.32

マスク：/32



注意:IP制限を設定する際は、正当な管理者アクセスが誤ってロックアウトされないように注意する必要があります。IP制限を完全に実装する前に、IP制限設定を徹底的にテストすることをお勧めします。



ヒント: IPv4アドレスの場合：

- 特定のIPアドレスに/32を使用します。
- サブネットの場合は、他のオプションを使用します。例： 10.26.192.0/18

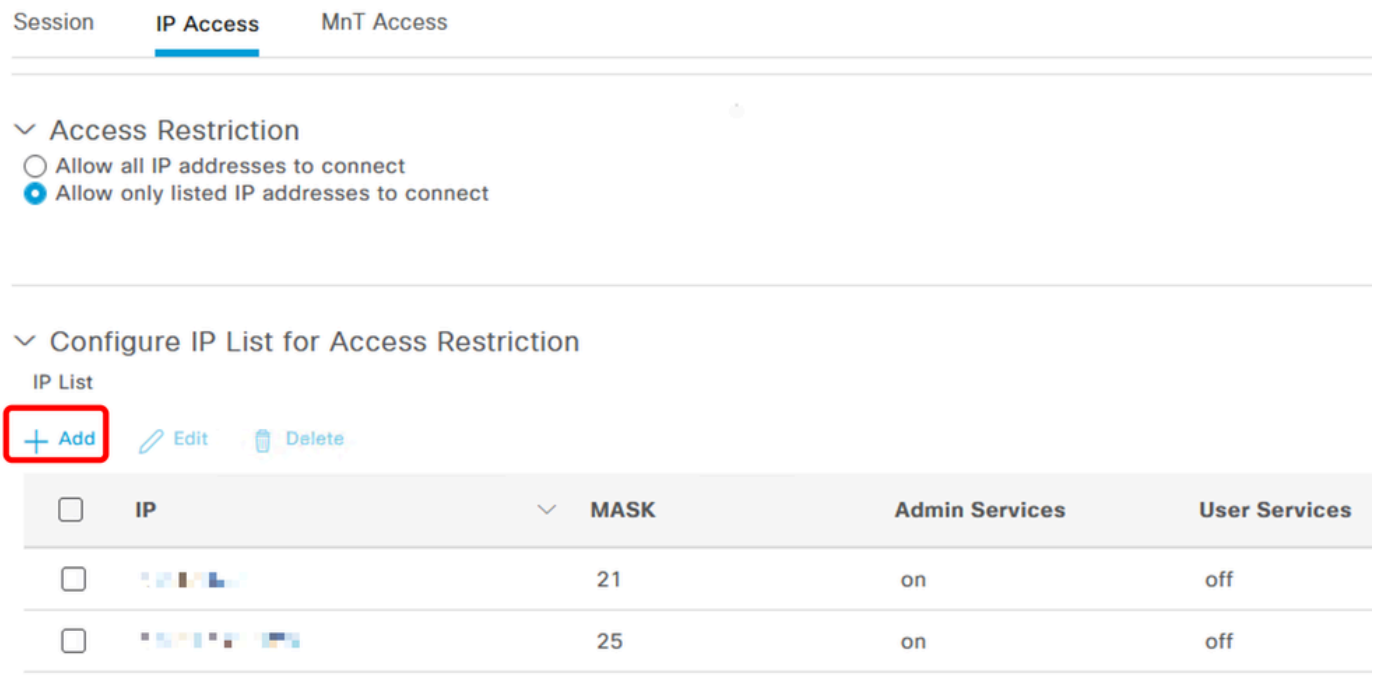
ISE 3.2の動作

「管理」>「管理アクセス」>「設定」>「アクセス」にナビゲートします。次のオプションを使用できます。

- セッション
- IPアクセス
- MnTアクセス

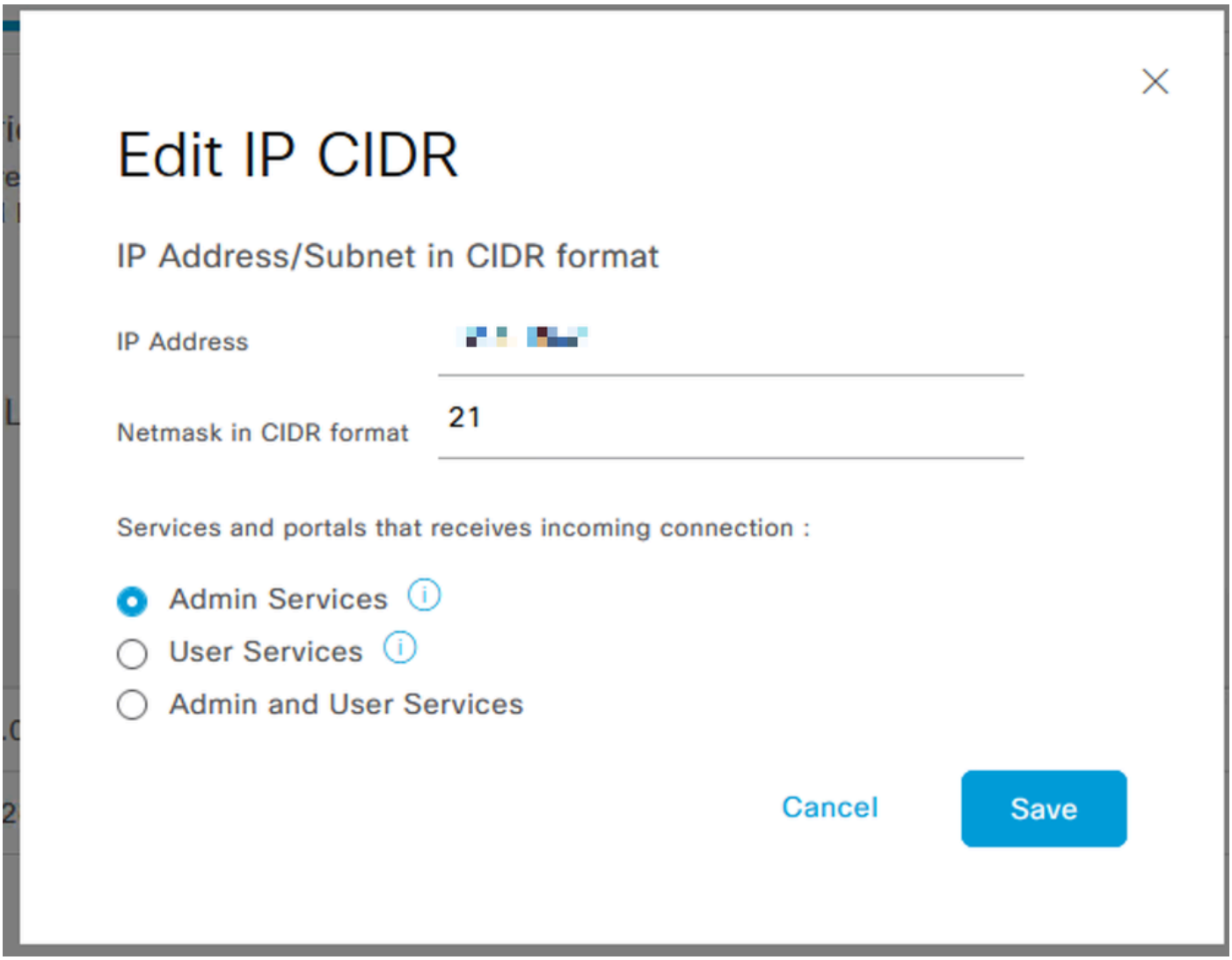
設定

- 「リストされているIPアドレスのみに接続を許可する」を選択します。
- [追加]をクリックします



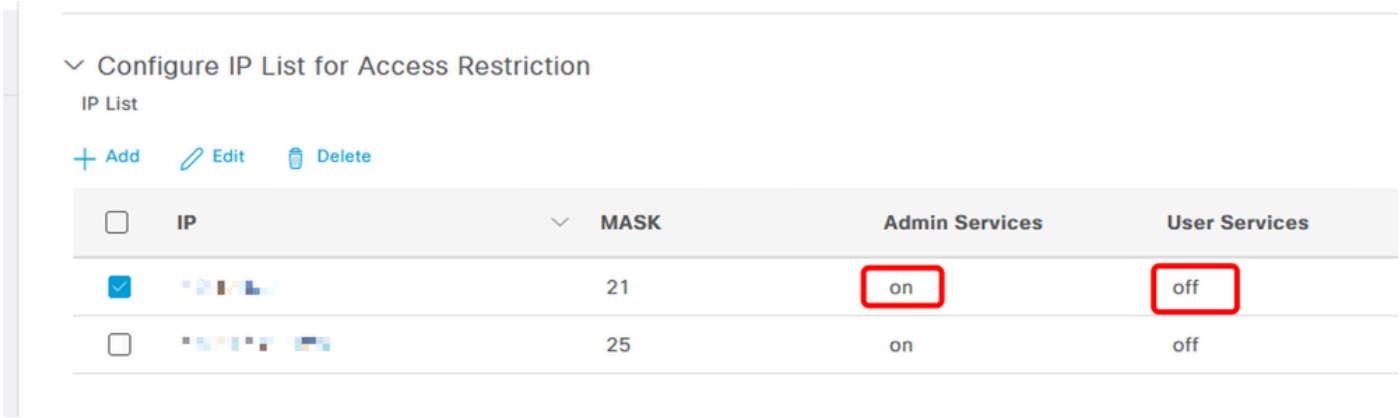
IPアクセスの設定

- ダイアログボックスが開き、IPアドレス（IPv4またはIPv6）をCIDR形式で入力できます。
- IPを設定したら、CIDR形式でマスクを設定します。
- IPアクセスの制限には、次のオプションを使用できます
  - Admin Services:GUI、CLI(SSH)、SNMP、ERS、OpenAPI、UDN、API Gateway、PxGrid（パッチ2では無効）、MnT Analytics
  - ユーザサービス：ゲスト、BYOD、ポスチャ、プロファイリング
  - 管理サービスとユーザサービス



IP CIDRの編集

- 「保存」ボタンをクリックします
- 「ON」は管理サービスが有効になっていることを意味し、「OFF」はユーザサービスが無効になっていることを意味します。



3.2のIPアクセス設定

ISE 3.2 P4以降での動作

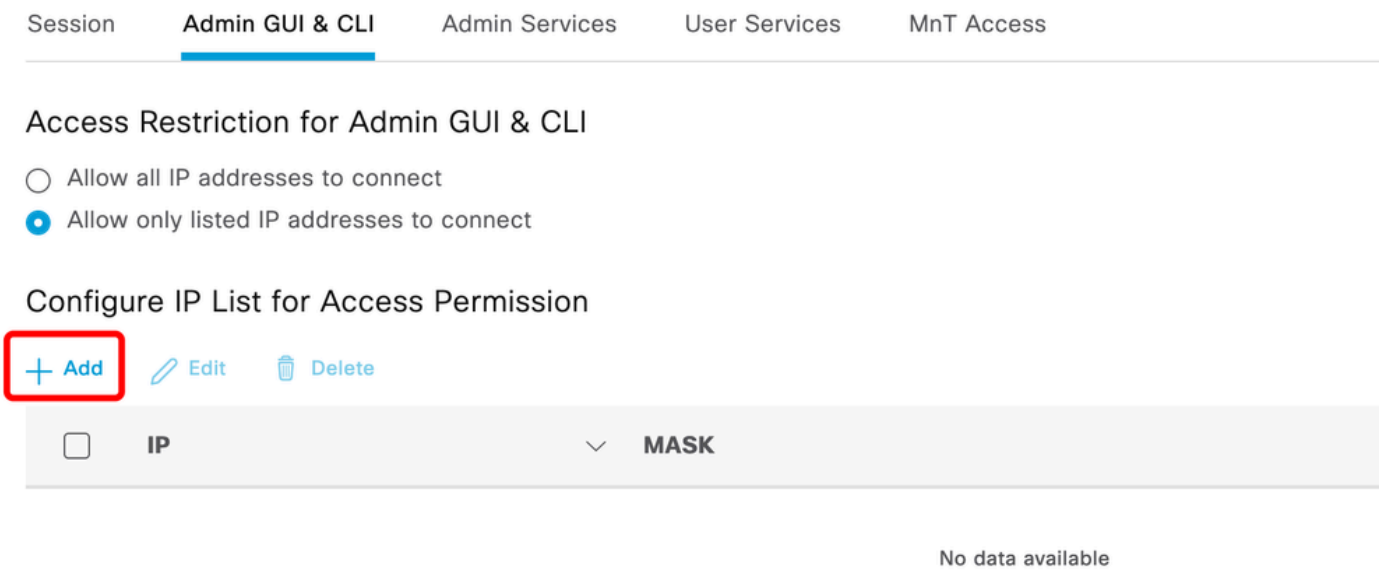
「管理」>「管理アクセス」>「設定」>「アクセス」にナビゲートします。次のオプションを使

用できます。

- セッション
- 管理GUI&CLI:ISE GUI(TCP 443)、ISE CLI(SSH TCP22)、およびSNMP。
- 管理サービス：ERS API、Open API、pxGrid、DataConnect
- ユーザサービス：ゲスト、BYOD、ポスチャ
- MNTアクセス：このオプションを使用すると、ISEは外部ソースから送信されるsyslogメッセージを消費しません。

設定

- 「リストされているIPアドレスのみに接続を許可する」を選択します。
- [追加]をクリックします



3.3のIPアクセス設定

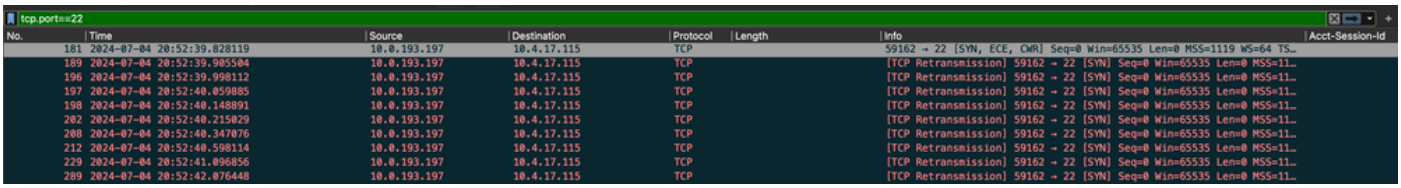
- ダイアログボックスが開き、IPアドレス（IPv4またはIPv6）をCIDR形式で入力できます。
- IPを設定したら、CIDR形式でマスクを設定します。
- [追加]をクリックします

ISE GUI/CLIの回復

- コンソールを使用したログイン
- application stop iseを使用してISEサービスを停止します。
- application start ise safeを使用したISEサービスの開始
- GUIからIPアクセス制限を削除します。

トラブルシューティング

ISEが応答していないか、またはトラフィックをドロップしているかを確認するために、パケットキャプチャを実行します。



No.	Time	Source	Destination	Protocol	Length	Info	Acct-Session-Id
181	2024-07-04 20:52:39.828119	10.0.193.197	10.4.17.115	TCP		59162 → 22 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1119 WS=64 TS…	
189	2024-07-04 20:52:39.905504	10.0.193.197	10.4.17.115	TCP		[TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11…	
196	2024-07-04 20:52:39.998112	10.0.193.197	10.4.17.115	TCP		[TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11…	
197	2024-07-04 20:52:40.059885	10.0.193.197	10.4.17.115	TCP		[TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11…	
198	2024-07-04 20:52:40.148891	10.0.193.197	10.4.17.115	TCP		[TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11…	
202	2024-07-04 20:52:40.215029	10.0.193.197	10.4.17.115	TCP		[TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11…	
208	2024-07-04 20:52:40.347076	10.0.193.197	10.4.17.115	TCP		[TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11…	
212	2024-07-04 20:52:40.598114	10.0.193.197	10.4.17.115	TCP		[TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11…	
229	2024-07-04 20:52:41.096856	10.0.193.197	10.4.17.115	TCP		[TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11…	
289	2024-07-04 20:52:42.076448	10.0.193.197	10.4.17.115	TCP		[TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11…	

ISEファイアウォールルールの確認

- 3.1以前の場合は、show techでだけ確認できます。
  - show techを実行し、「show tech-support file <filename>」を使用してlocaldiskに保存できます。
  - その後、「copy disk:/<filename> ftp://<ip_address>/path」を使用して、ファイルをリポジトリに転送できます。リポジトリのURLは、使用しているリポジトリタイプによって異なります
  - このファイルを自分のマシンにダウンロードして、ファイルを読み取り、「Running iptables -nvL」を探すことができます。
  - show techの最初のルールは次に含まれていません。つまり、show tech by IP Access restriction機能に最後のルールが追加されています。

<#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
```

- 3.2以降では、コマンド「show firewall」を使用してファイアウォールルールを確認できま

す。
- 3.2以降では、IPアクセス制限によってブロックされるサービスをより細かく制御できます。

<#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
```

デバッグログの確認

警告：すべてのトラフィックでログが生成されるわけではありません。IPアクセス制限は、アプリケーションレベルでLinux内部ファイアウォールを使用してトラフィックをブロックできます。SNMP、CLI、SSHはファイアウォールレベルでブロックされるため、ログは生成されません。

- GUIからのデバッグで「Infrastructure」コンポーネントを有効にします。
- show logging application ise-psc.log tailを使用します

次のログは、IPアクセス制限がいつ処理を実行しているかを確認できます。

```
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
```

関連情報

- シスコのテクニカルサポートとダウンロード
- ISE 3.1管理ガイド
- ISE 3.2管理ガイド
- ISE 3.3管理ガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。