Configure IP Access Restriction in ISE

Contents

Introduction

This document describes the available options to configure IP access restriction in ISE 3.1, 3.2 and 3.3.

Prerequisites

Requirements

Cisco recommends that you have knowledge of Cisco Identity Service Engine (ISE).

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ISE Version 3.1
- Cisco ISE Version 3.2
- Cisco ISE Version 3.3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

IP access restriction feature allows administrators to control which IP addresses or ranges can access the ISE admin portal and services.

This feature applies to various ISE interfaces and services, including:

- Admin portal access adn CLI
- ERS API access
- Guest and sponsor portal access
- My Devices portal access

When enabled, ISE only allows connections from the specified IP addresses or ranges. Any attempts to access ISE admin interfaces from non-specified IPs are blocked.

In case of accidental lockout, ISE provides a 'safe mode' startup option that can bypass IP access restrictions. This allows administrators to regain access and correct any misconfigurations.

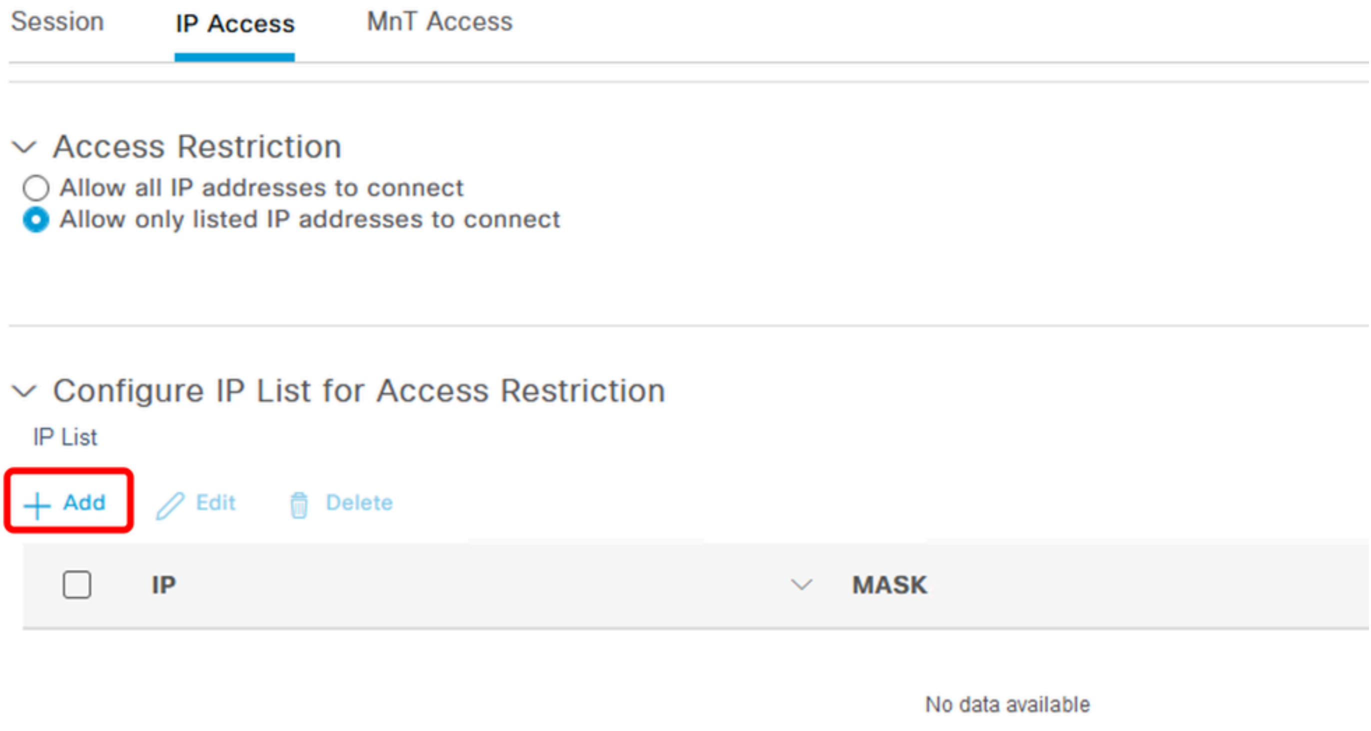
Behaviour in ISE 3.1 and Lower

Navigate to Administration > Admin Access > Settings > Access . You have these options:

- Session
- IP Access
- MnT Access

Configure

- Select **Allow only listed IP addresses to connect** .
- Click Add.



Session | IP Access | MnT Access

Access Restriction

○ Allow all IP addresses to connect
● Allow only listed IP addresses to connect

Configure IP List for Access Restriction

IP List

□	IP	MASK

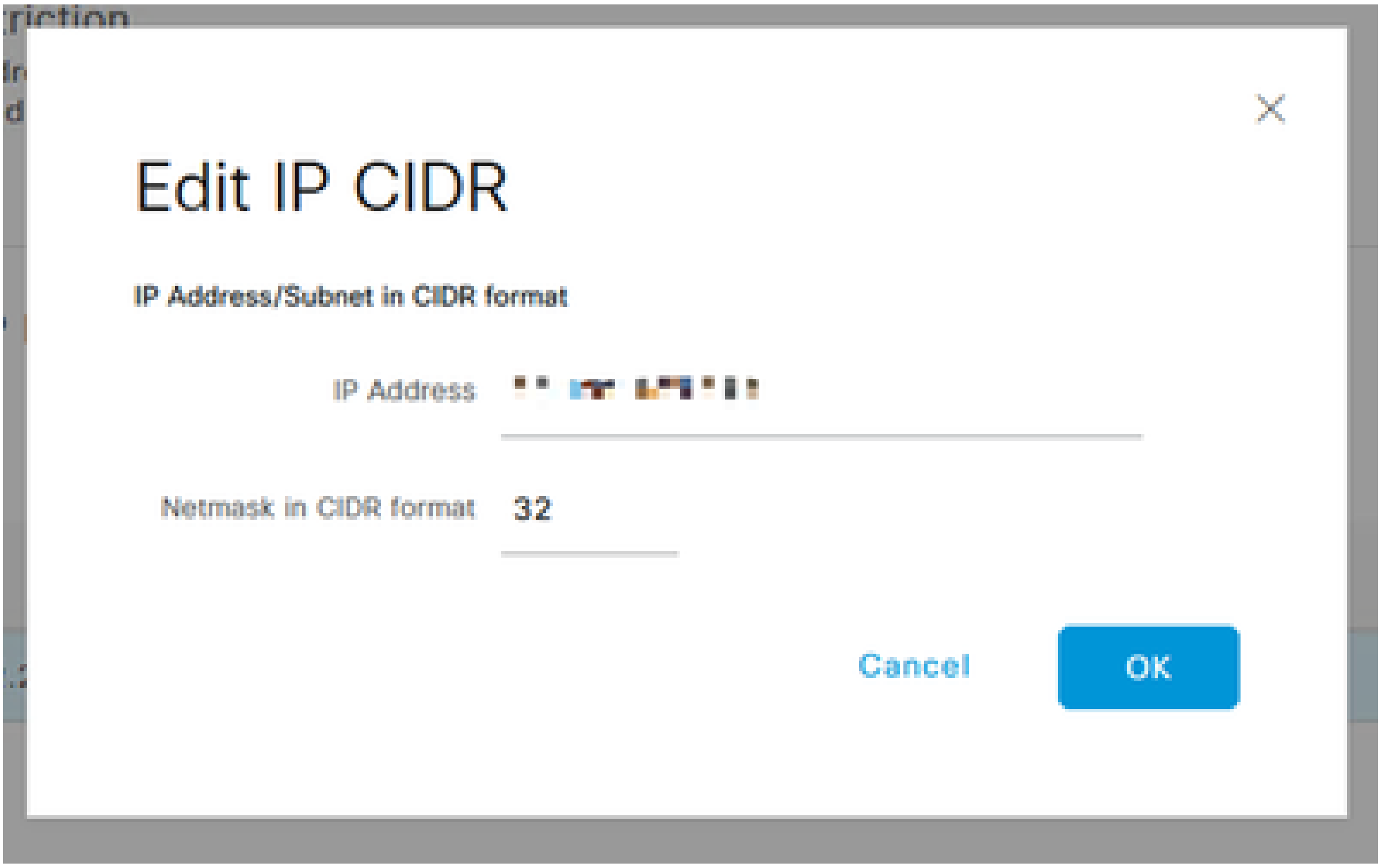
No data available

IP Access configuration

- In ISE 3.1 you do not have an option to select bewteen Admin and **User** services, enabling IP Access

Restriction blocks connections to:

  - GUI
  - CLI
  - SNMP
  - SSH
- A dialog box opens where you enter the IP addresses, IPv4 or IPv6, in CIDR format.
- Once the IP is configured, set the mask in CIDR format.



Edit IP CIDR

IP Address/Subnet in CIDR format

IP Address [redacted]

Netmask in CIDR format 32

Edit IP CIDR

Note: IP Classless Inter-Domain Routing (CIDR) format is a method of representing IP addresses and their associated routing prefix.

Example:

IP: 10.8.16.32

Mask: /32

Caution: Care must be taken when configuring IP restrictions to avoid accidentally locking out legitimate admin access. Cisco recommends thoroughly testing any IP restriction configuration before fully implementing it.

Tip: For IPv4 addresses:

- Use /32 for specific IP addresses.
- For subnets use any other option. Example: 10.26.192.0/18

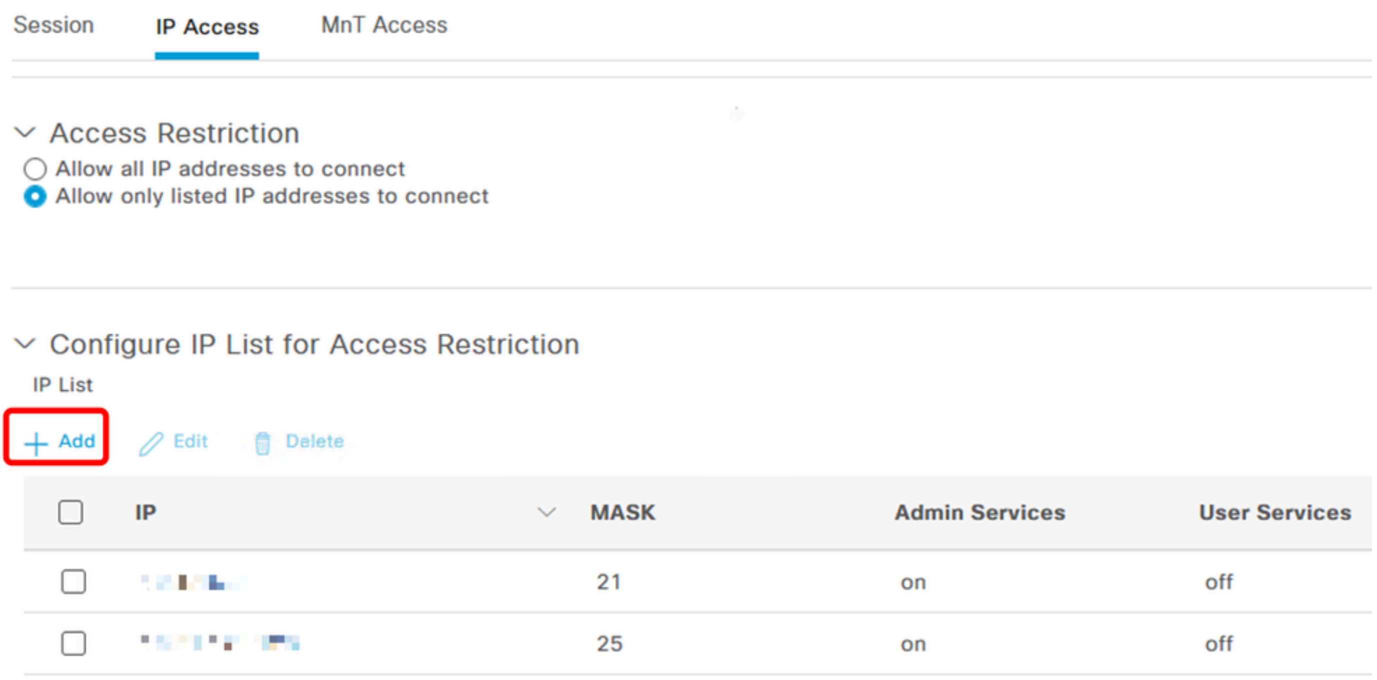
Behaviour in ISE 3.2

Navigate to Administration > Admin Access > Settings > Access. You have these options available:

- Session
- IP Access
- MnT Access

Configure

- Select **Allow only listed IP addresses to connect**.
- Click Add.



Session | **IP Access** | MnT Access

Access Restriction

○ Allow all IP addresses to connect
● Allow only listed IP addresses to connect

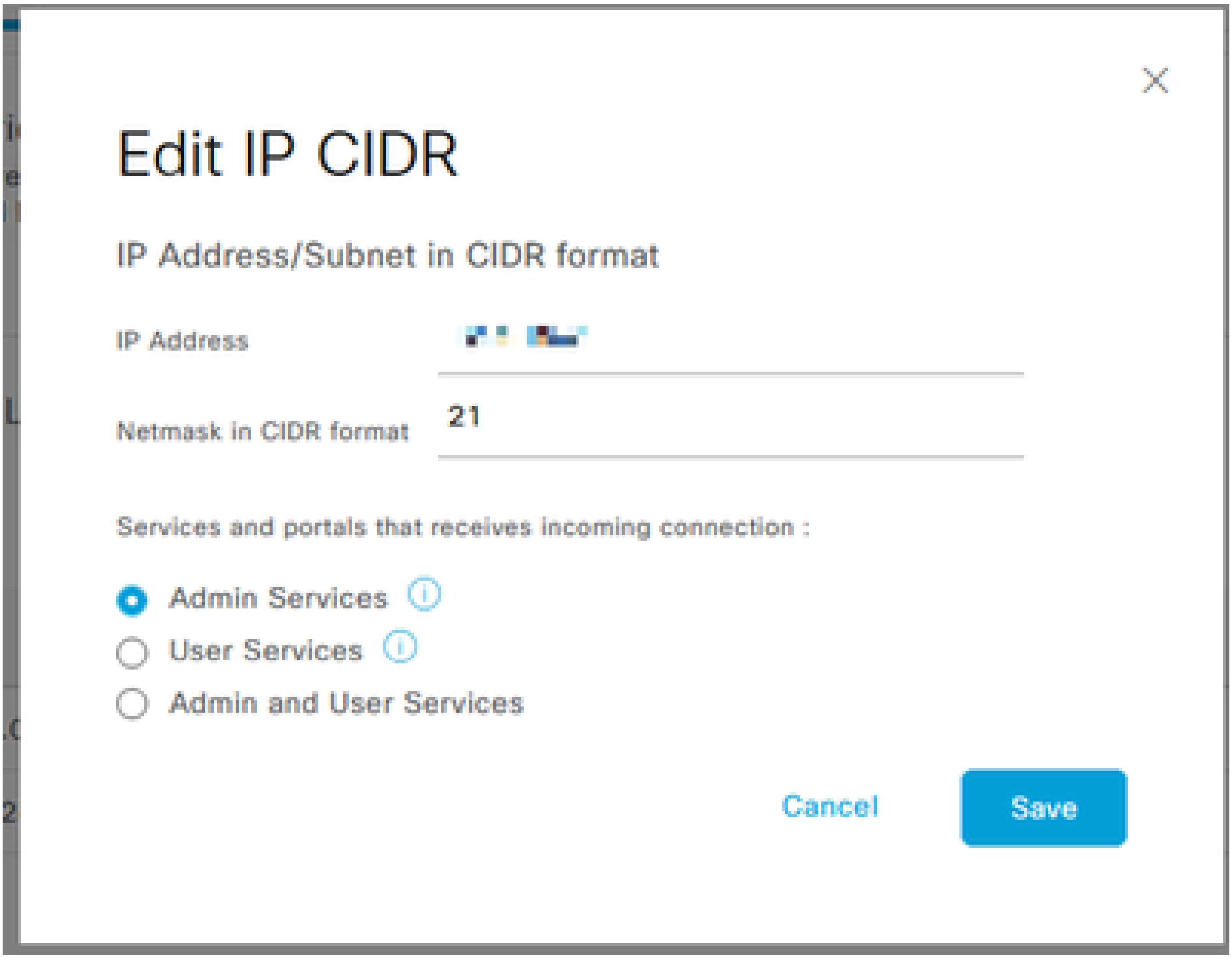
Configure IP List for Access Restriction

IP List

□	IP	MASK	Admin Services	User Services
□	[redacted]	21	on	off
□	[redacted]	25	on	off

IP Acess configuration

- A dialog box opens where you enter the IP addresses, IPv4 or IPv6, in CIDR format.
- Once the IP is configured, set the mask in CIDR format.
- These options are available for IP Access restriction:
  - Admin Services: GUI, CLI (SSH), SNMP, ERS, OpenAPI, UDN, API Gateway, PxGrid (disabled in Patch 2), MnT Analytics
  - User Services: Guest, BYOD, Posture, Profiling
  - Admin and User Services



Edit IP CIDR

IP Address/Subnet in CIDR format

IP Address [redacted]

Netmask in CIDR format 21

Services and portals that receives incoming connection :

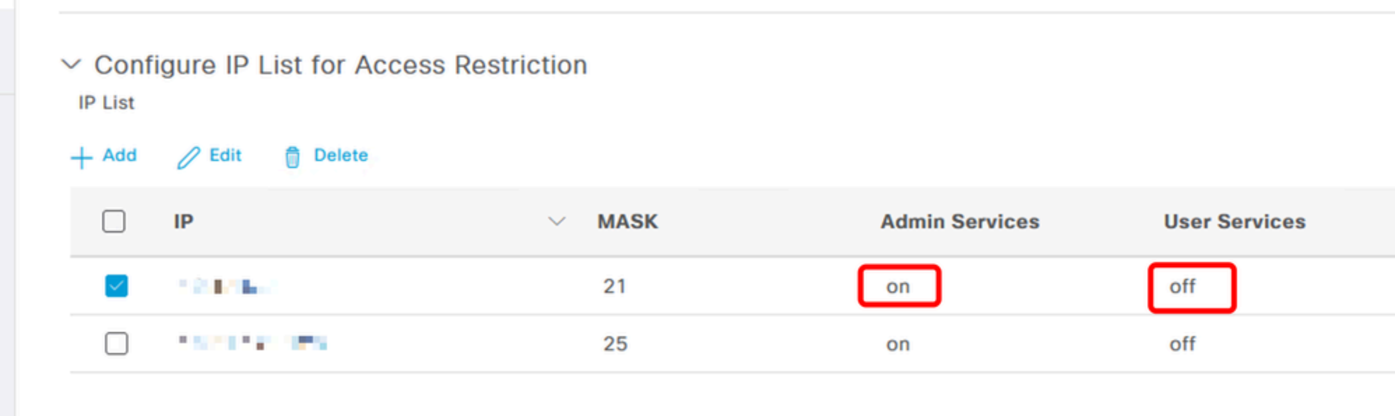
● Admin Services ⓘ

○ User Services ⓘ

○ Admin and User Services

Edit IP CIDR

- Click on Save button.
- ON means Admin services are enabled, OFF means user services are disabled.



Configure IP List for Access Restriction

IP List

□	IP	MASK	Admin Services	User Services
☑	[redacted]	21	on	off
□	[redacted]	25	on	off

IP Access configuration in 3.2

Behaviour in ISE 3.2 P4 and Greater

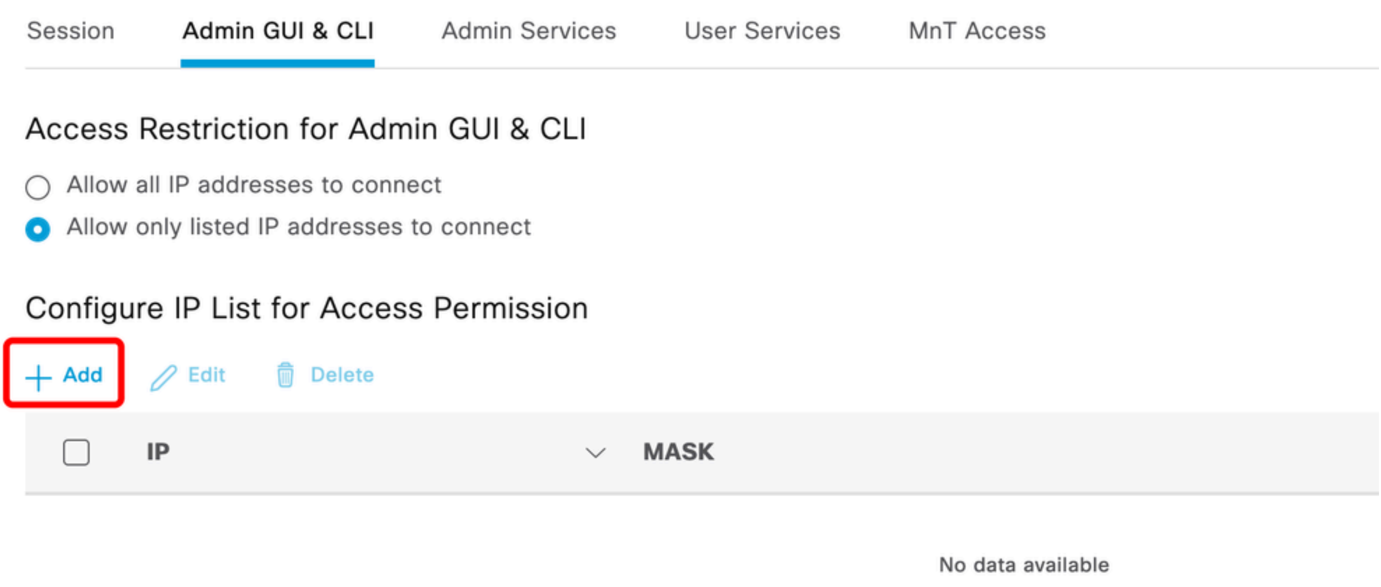
Navigate to Administration > Admin Access > Settings > Access . You have these options available:

- Session
- Admin GUI & CLI: ISE GUI (TCP 443), ISE CLI (SSH TCP22) and SNMP.
- Admin Services: ERS API, Open API, pxGrid, DataConnect.
- User Services: Guest, BYOD, Posture.
- MNT Access: With this option, ISE does not consume Syslog messages sent from external sources.

Note: pxGrid and Data Connect access restriction is for ISE 3.3+, but not for ISE 3.2 P4+.

Configure

- Select Allow only listed IP addresses to connect.
- Click **Add**.



Session | Admin GUI & CLI | Admin Services | User Services | MnT Access

Access Restriction for Admin GUI & CLI

○ Allow all IP addresses to connect

● Allow only listed IP addresses to connect

Configure IP List for Access Permission

+ Add | Edit | Delete

□	IP	MASK

No data available

IP Access configuration in 3.3

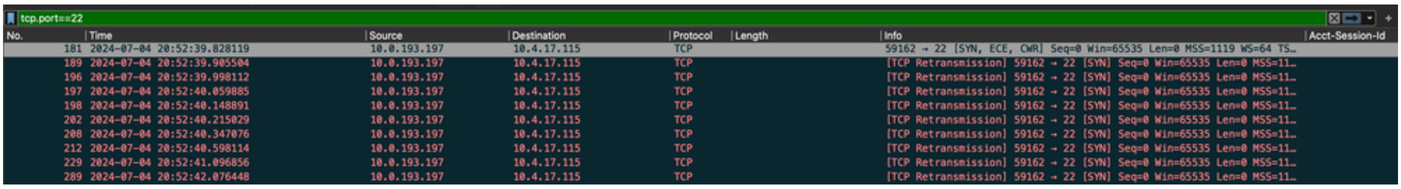
- A dialog box opens where you enter the IP addresses, IPv4 or IPv6, in CIDR format.
- Once the IP is configured, set the mask in CIDR format.
- Click Add.

Recover ISE GUI/CLI

- Login with console.
- Stop ISE services using application stop ise
- Start ISE services using application start ise safe
- Remove the IP access restriction from the GUI.

Troubleshooting

Take a packet capture to verify if ISE is not responding or it is dropping the traffic.



tcp.port==22

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…	

Check ISE Firewall Rules

- For 3.1 and lower, you can check this only in the show tech.
  - You can take a show tech and store it in the localdisk using show tech-support file <filename>
  - Then you can transfer the file to a repository using copy disk:/<filename> ftp://<ip_address>/path. The repository URL changes depending on the repository type you are using.
  - You can download the file to your machine so you can read it and look for **Running iptables -nvL**.
  - The initial rules in the show tech are not included here. In other words, here you can find the last rules appended to the show tech by IP Access restriction feature.

```
*****************************************
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 se
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 se
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
```

- For 3.2 and higher you can use the command `show firewall` to check the firewall rules.
- 3.2 and higher provide more control over the services being blocked by IP Access Restriction.

```
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 f
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 se
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
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 Firewall rule permitting the HTTPS traffic from s
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 Firewall rule permitting the Block List Portal t
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 Firewall rule permitting the Sponsor Portal traf
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
```

Check Debug Logs

Warning: Not all the traffic generates logs. IP Access restriction can block the traffic at the application level and using Linux Internal Firewall. SNMP, CLI, and SSH is blocked at firewall level so no logs are generated.

- Enable Infrastructure component to DEBUG from GUI.
- Enable **Admin-infra** component to DEBUG from GUI.
- Enable **NSF** component to DEBUG from GUI.
- Use show logging application ise-psc.log tail.

The sample log entries can be see when the ISE admin webUI access is restricted, where the allowed subnet is 198.18.133.0/24 while the ISE admin comes from 198.18.134.28.

```
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.infrastructure.systemconfig.CpmIpFilterC
```

```
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.infrastructure.systemconfig.CpmIpFilterC
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.infrastructure.systemconfig.CpmIpFilterC
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.nsf.impl.NetworkElement -:::::- The ip a
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.infrastructure.systemconfig.CpmIpFilterC
```

Related Information

- ISE 3.1 Admin Guide
- ISE 3.2 Admin Guide
- ISE 3.3 Admin Guide
- Cisco Technical Support & Downloads