Configuración de la restricción de acceso IP en ISE

Contenido

Introducción

Este documento describe las opciones disponibles para configurar la restricción de acceso IP en ISE 3.1, 3.2 y 3.3.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de Cisco Identity Service Engine

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La función de restricción de acceso a IP permite a los administradores controlar qué rangos o direcciones IP pueden acceder al portal de administración y a los servicios de ISE.

Esta función se aplica a varias interfaces y servicios de ISE, entre los que se incluyen:

- Acceso al portal de administración y CLI
- Acceso a API ERS
- Acceso al portal de invitados y patrocinadores
- Acceso al portal Mis dispositivos

Cuando está habilitado, ISE solo permite conexiones de los rangos o direcciones IP especificados. Se bloquea cualquier intento de acceder a las interfaces de administración de ISE desde IP no especificadas.

En caso de bloqueo accidental, ISE proporciona una opción de inicio de 'modo seguro' que puede eludir las restricciones de acceso IP. Esto permite a los administradores recuperar el acceso y corregir cualquier configuración incorrecta.

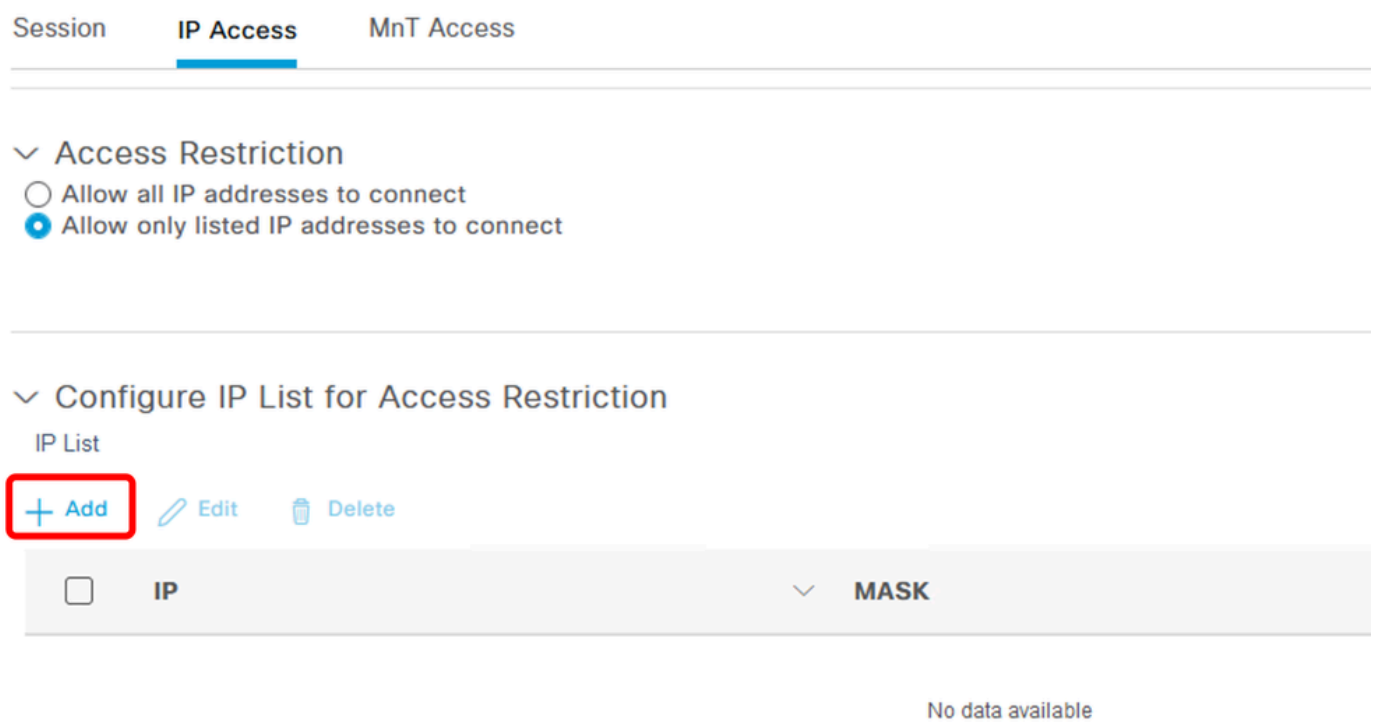
Comportamiento en ISE 3.1 y versiones anteriores

Vaya a Administración>Acceso de administrador>Configuración>Acceso. Tiene estas opciones:

- Sesión
- Acceso IP
- Acceso MnT

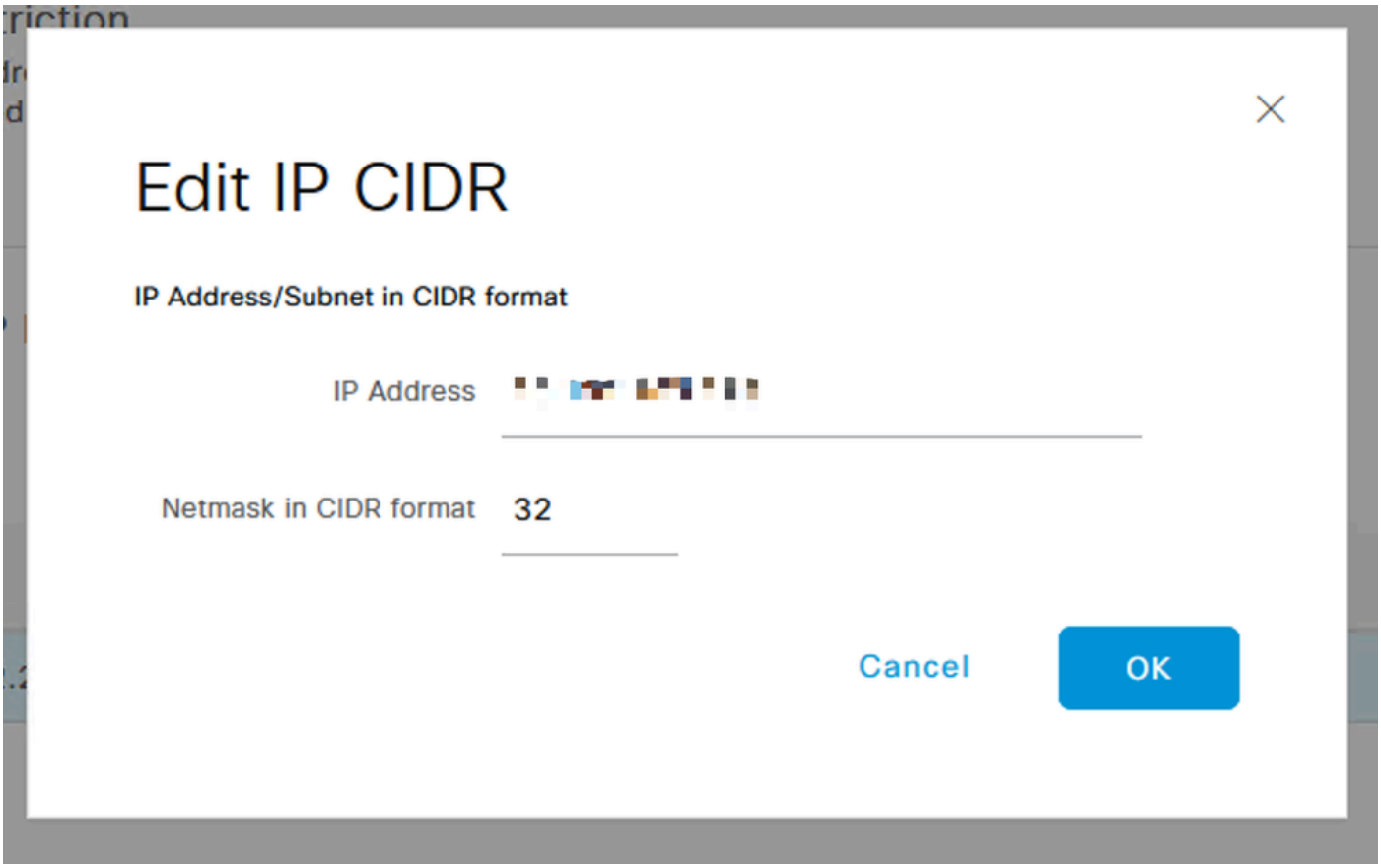
Configurar

- Seleccione "Permitir que sólo se conecten las direcciones IP de la lista"
- Haga clic en "Agregar"

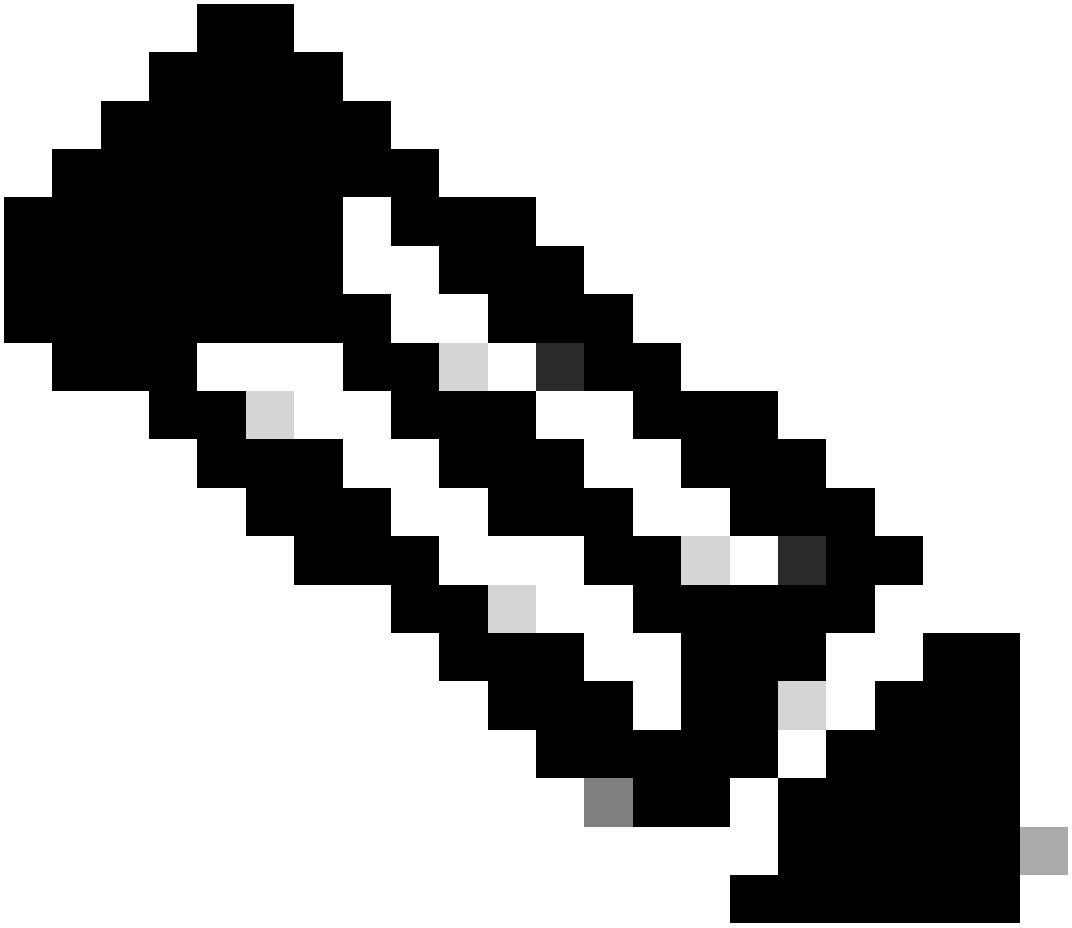


Configuración de acceso IP

- En ISE 3.1 no tiene la opción de seleccionar entre los servicios "Admin" y "User", por lo que la activación de la restricción de acceso IP bloquea las conexiones a:
  - GUI
  - CLI
  - SNMP (Protocolo de administración de red simple)
  - SSH
- Se abre un cuadro de diálogo en el que se introducen las direcciones IP, IPv4 o IPv6, en formato CIDR.
- Una vez configurada la IP, establezca la máscara en formato CIDR.



Editar CIDR IP

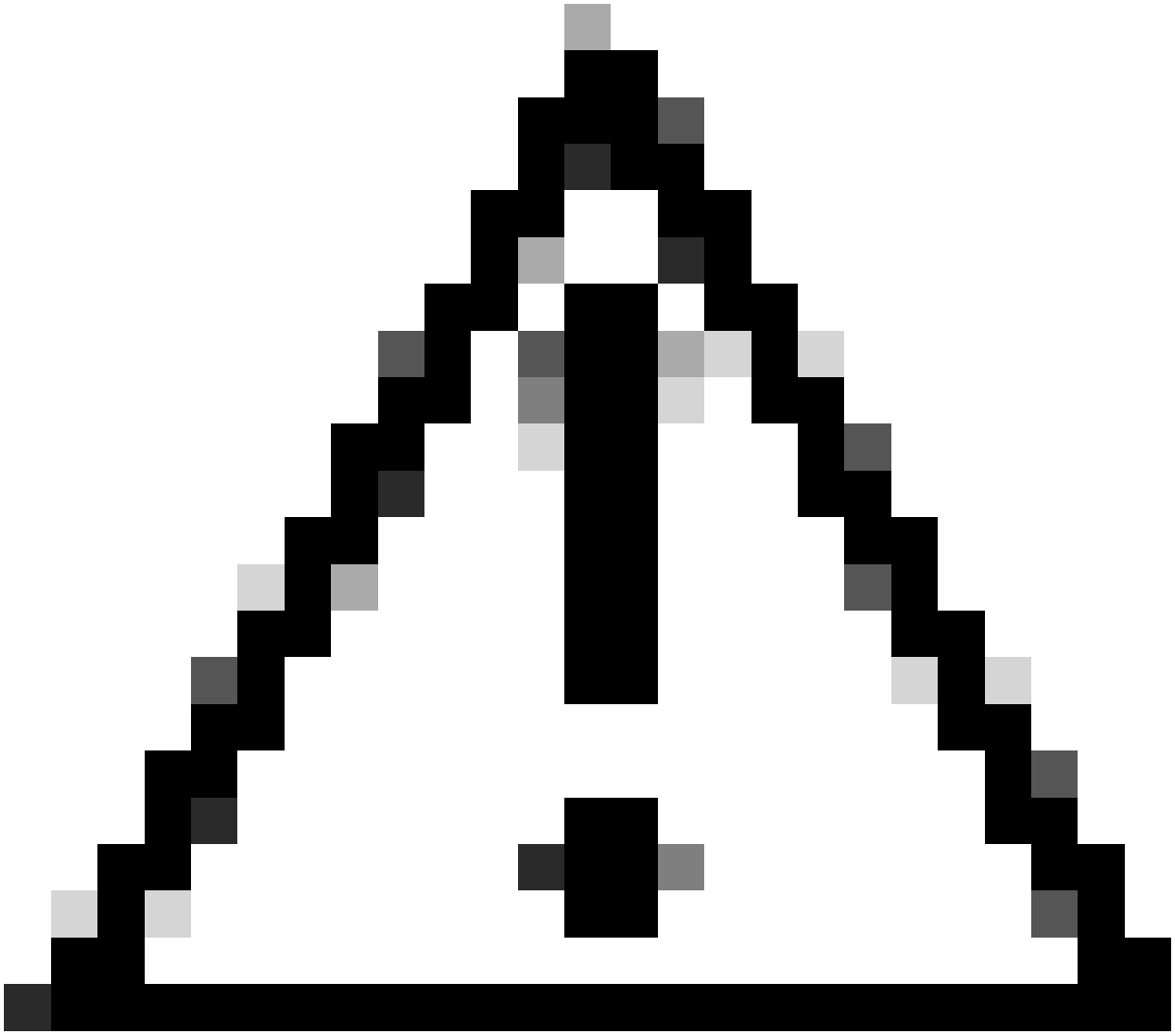


Nota: El formato IP CIDR (enrutamiento entre dominios sin clase) es un método para representar direcciones IP y su prefijo de enrutamiento asociado.

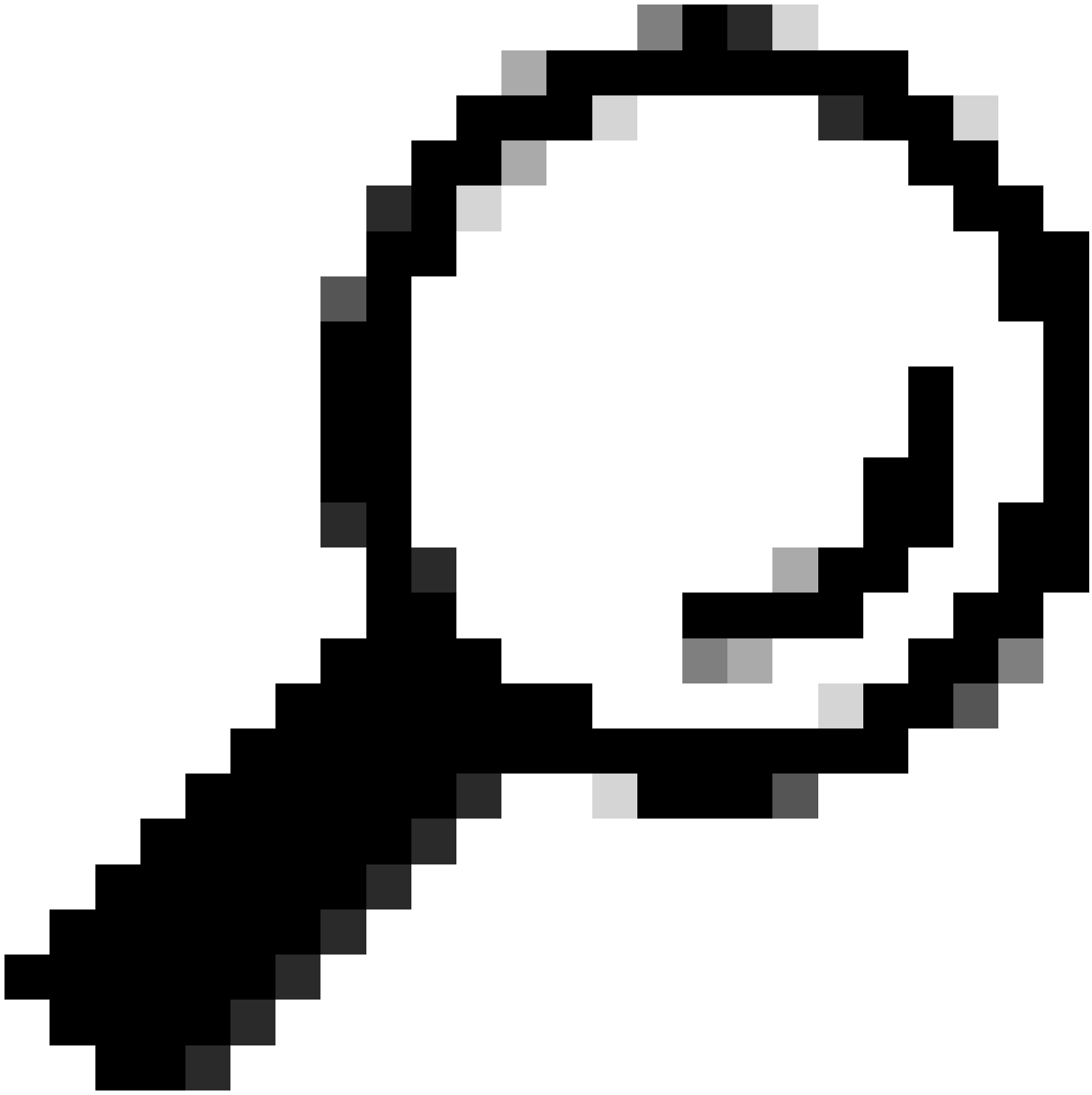
Ejemplo:

IP: 10.8.16.32

Máscara: /32



Precaución: se debe tener cuidado al configurar las restricciones IP para evitar bloquear accidentalmente el acceso de administrador legítimo. Cisco recomienda probar exhaustivamente cualquier configuración de restricción de IP antes de implementarla por completo.



Sugerencia: para direcciones IPv4:

- Utilice /32 para direcciones IP específicas.
- Para subredes, utilice cualquier otra opción. Ejemplo: 10.26.192.0/18

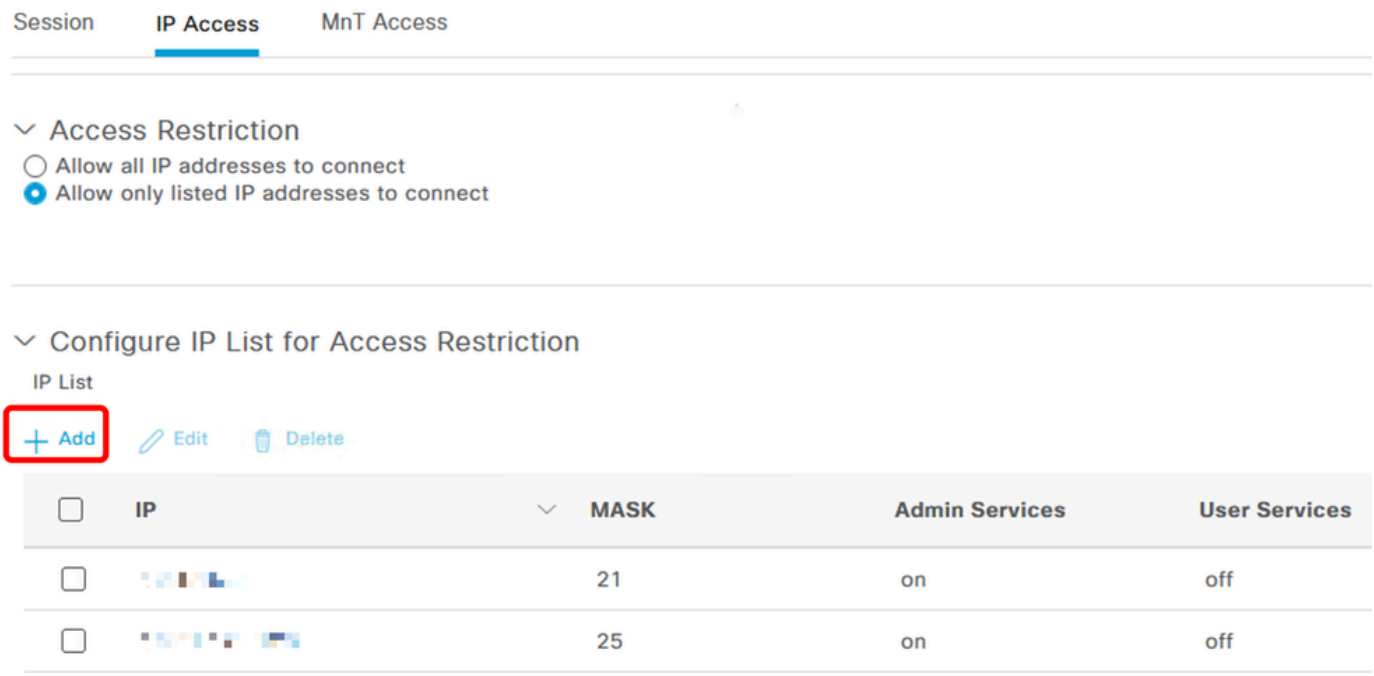
Comportamiento en ISE 3.2

Vaya a Administración>Acceso de administrador>Configuración>Acceso. Tiene estas opciones disponibles:

- Sesión
- Acceso IP
- Acceso MnT

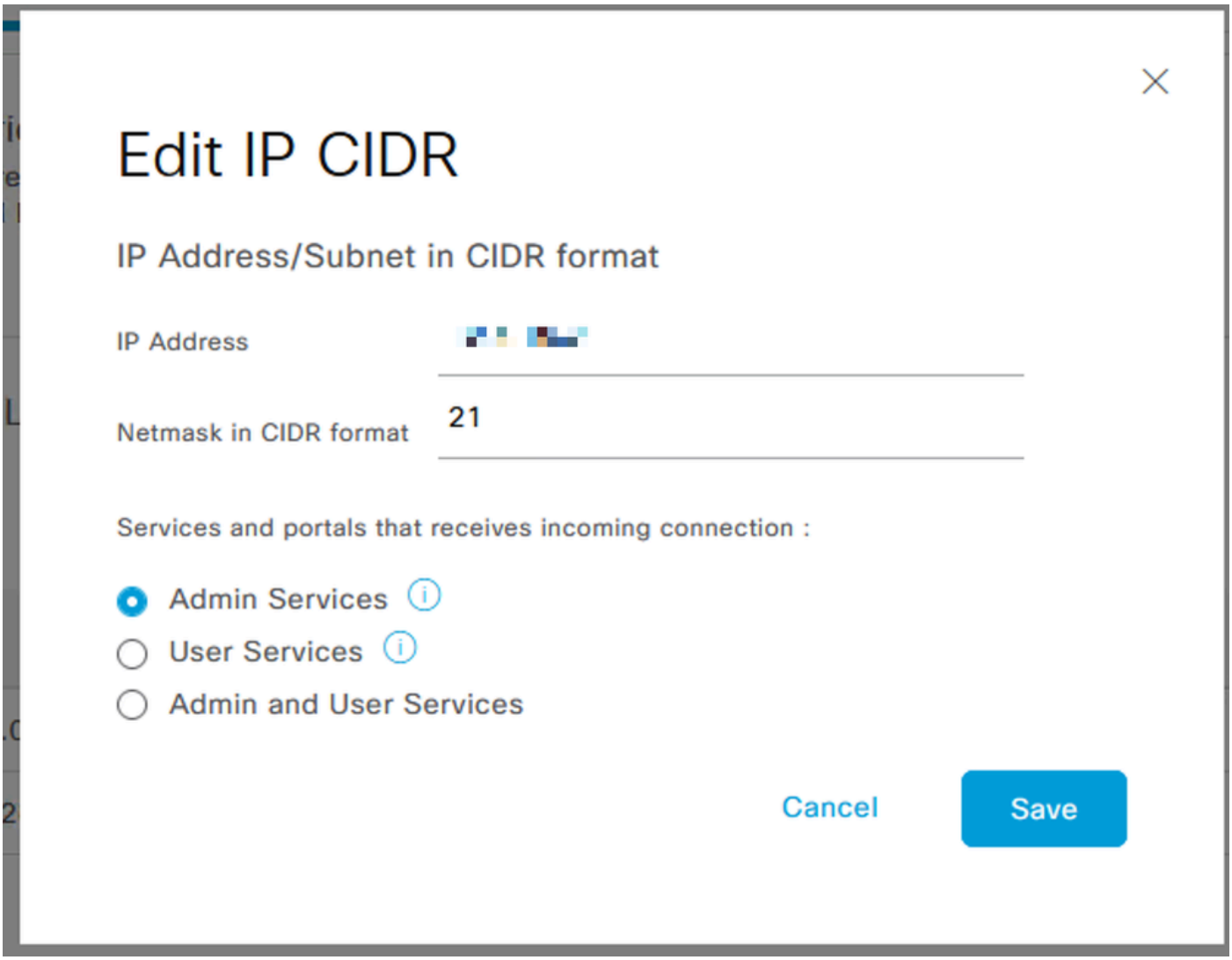
Configurar

- Seleccione "Permitir que sólo se conecten las direcciones IP de la lista"
- Haga clic en "Agregar"



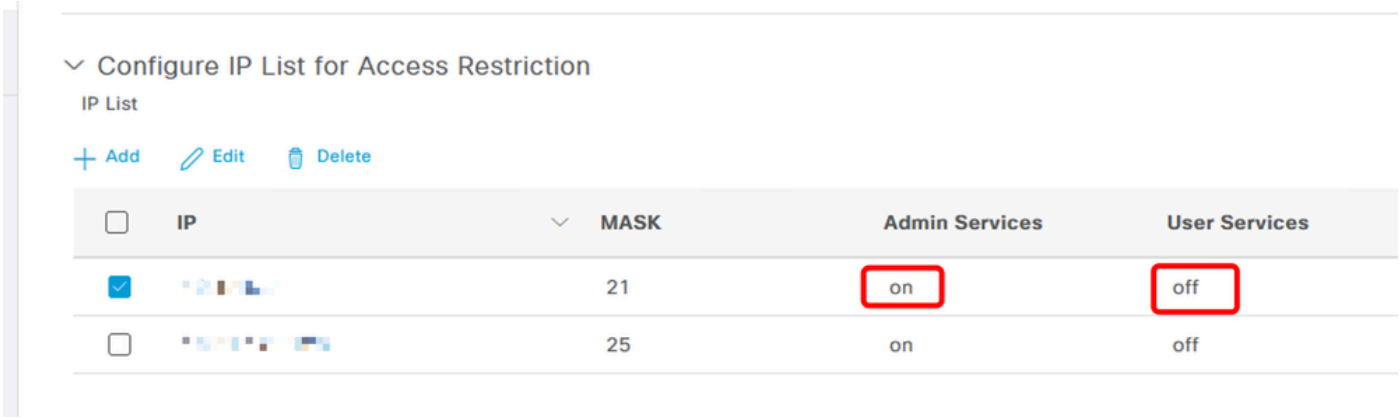
Configuración de acceso IP

- Se abre un cuadro de diálogo en el que se introducen las direcciones IP, IPv4 o IPv6, en formato CIDR.
- Una vez configurada la IP, establezca la máscara en formato CIDR.
- Estas opciones están disponibles para la restricción de acceso IP
  - Servicios de administración: GUI, CLI (SSH), SNMP, ERS, OpenAPI, UDN, API Gateway, PxGrid (deshabilitado en el parche 2), MnT Analytics
  - Servicios para usuarios: invitados, BYOD, estado, definición de perfiles
  - Servicios de administración y de usuario



Editar CIDR IP

- Haga clic en el botón "Guardar"
- "ON" significa que los servicios de administración están activados, "OFF" significa que los servicios de usuario están desactivados.



Configuración del acceso IP en 3.2

Comportamiento en ISE 3.2 P4 y versiones posteriores

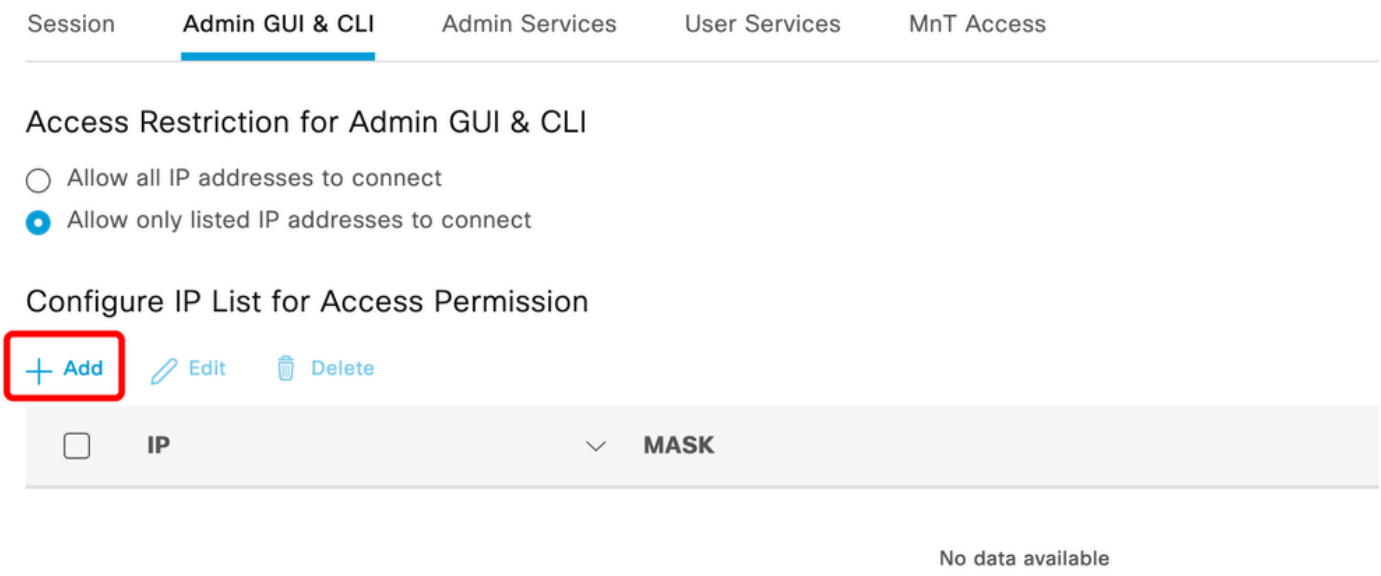
Vaya a Administración>Acceso de administrador>Configuración>Acceso. Tiene estas opciones

disponibles:

- Sesión
- GUI y CLI de administración: GUI de ISE (TCP 443), CLI de ISE (SSH TCP22) y SNMP.
- Servicios de administración: API ERS, API abierta, pxGrid, DataConnect.
- Servicios para usuarios: invitado, BYOD, estado.
- Acceso MNT: con esta opción, ISE no consume mensajes de Syslog enviados desde fuentes externas.

Configurar

- Seleccione "Permitir que sólo se conecten las direcciones IP de la lista"
- Haga clic en "Agregar"



Configuración de acceso IP en 3.3

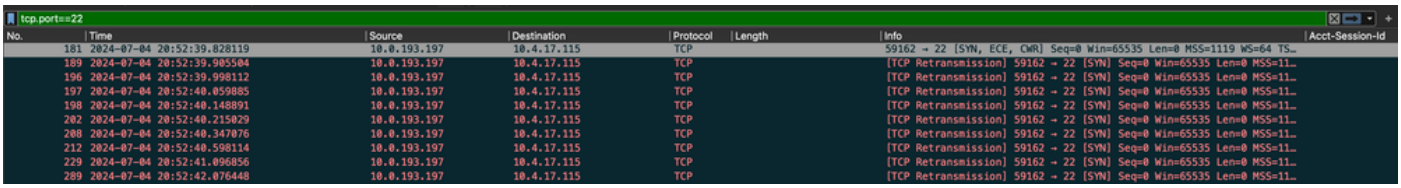
- Se abre un cuadro de diálogo en el que se introducen las direcciones IP, IPv4 o IPv6, en formato CIDR.
- Una vez configurada la IP, establezca la máscara en formato CIDR.
- Haga clic en "Agregar"

Recuperar GUI/CLI de ISE

- Iniciar sesión con la consola
- Detener los servicios de ISE mediante application stop ise
- Inicio de servicios ISE mediante inicio de aplicación ise seguro
- Elimine la restricción de acceso IP de la GUI.

Resolución de problemas

Realice una captura de paquetes para verificar si ISE no responde o si está descartando el tráfico.



Comprobar las reglas del firewall ISE

- Para 3.1 y versiones inferiores puede verificar esto solamente en el show tech.
  - Puede tomar un show tech y almacenarlo en el disco local usando "show tech-support file <filename>"
  - Luego puede transferir el archivo a un repositorio usando "copy disk:/<filename> ftp://<ip_address>/path" la url del repositorio cambia dependiendo del tipo de repositorio que esté utilizando
  - Puede descargar el archivo en su máquina para que pueda leerlo y buscar "Running iptables -nvL"
  - Las reglas iniciales del show tech no se incluyen a continuación. En otras palabras, aquí puede encontrar las últimas reglas añadidas a la función show tech by IP Access restricted.

<#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
```

- Para la versión 3.2 y posteriores, puede utilizar el comando "show firewall" para verificar las reglas del firewall.
- Las versiones 3.2 y superiores proporcionan un mayor control sobre los servicios que están siendo bloqueados por la Restricción de acceso IP.

<#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
```

Comprobar los registros de depuración

Advertencia: no todo el tráfico genera registros. La restricción de acceso IP puede bloquear el tráfico en el nivel de aplicación y mediante el firewall interno de Linux. SNMP, CLI y SSH se bloquean en el nivel de firewall, por lo que no se generan registros.

- Habilite el componente "Infraestructura" en DEBUG desde la GUI.
- Utilice show logging application ise-psc.log tail

Los siguientes registros se pueden ver cuando la restricción de acceso IP está tomando medidas.

```
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
```

Información Relacionada

- Soporte técnico y descargas de Cisco
- Guía de administración de ISE 3.1
- Guía de administración de ISE 3.2
- Guía de administración de ISE 3.3

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).