在ISE中配置IP访问限制

目录

简介

本文档介绍在ISE 3.1、3.2和3.3中配置IP访问限制的可用选项。

先决条件

要求

思科建议您了解思科身份服务引擎(ISE)。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科ISE版本3.1
- 思科ISE版本3.2
- 思科ISE版本3.3

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

IP访问限制功能允许管理员控制哪些IP地址或范围可以访问ISE管理员门户和服务。

此功能适用于各种ISE接口和服务，包括：

- 管理员门户访问和CLI
- ERS API访问
- 访客和发起人门户访问
- 我的设备门户访问

启用时，ISE仅允许来自指定IP地址或范围的连接。阻止从非指定IP访问ISE管理接口的任何尝试。

在意外锁定情况下，ISE提供可绕过IP访问限制的“安全模式”启动选项。这样，管理员可以重新获得访问权限并纠正任何错误配置。

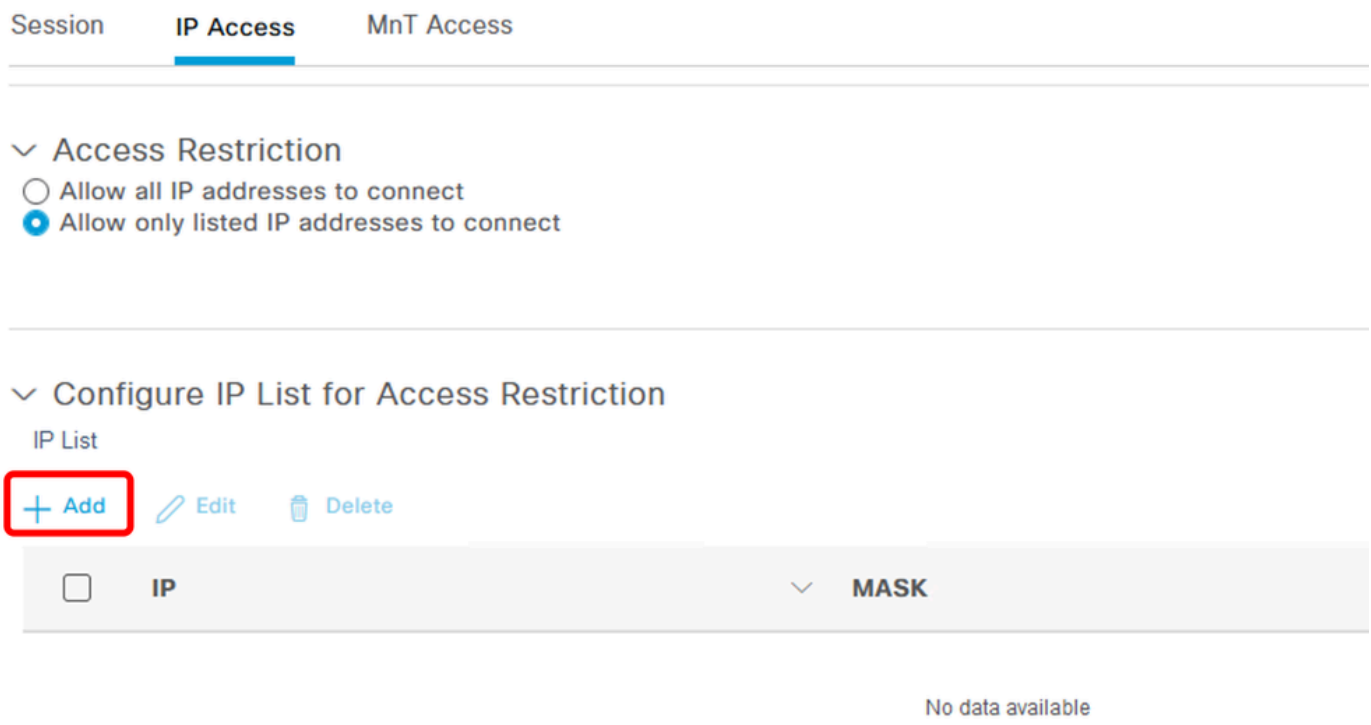
ISE 3.1及更低版本中的行为

导航到Administration > Admin Access > Settings > Access。您有以下选项：

- 会话
- IP访问
- MnT访问

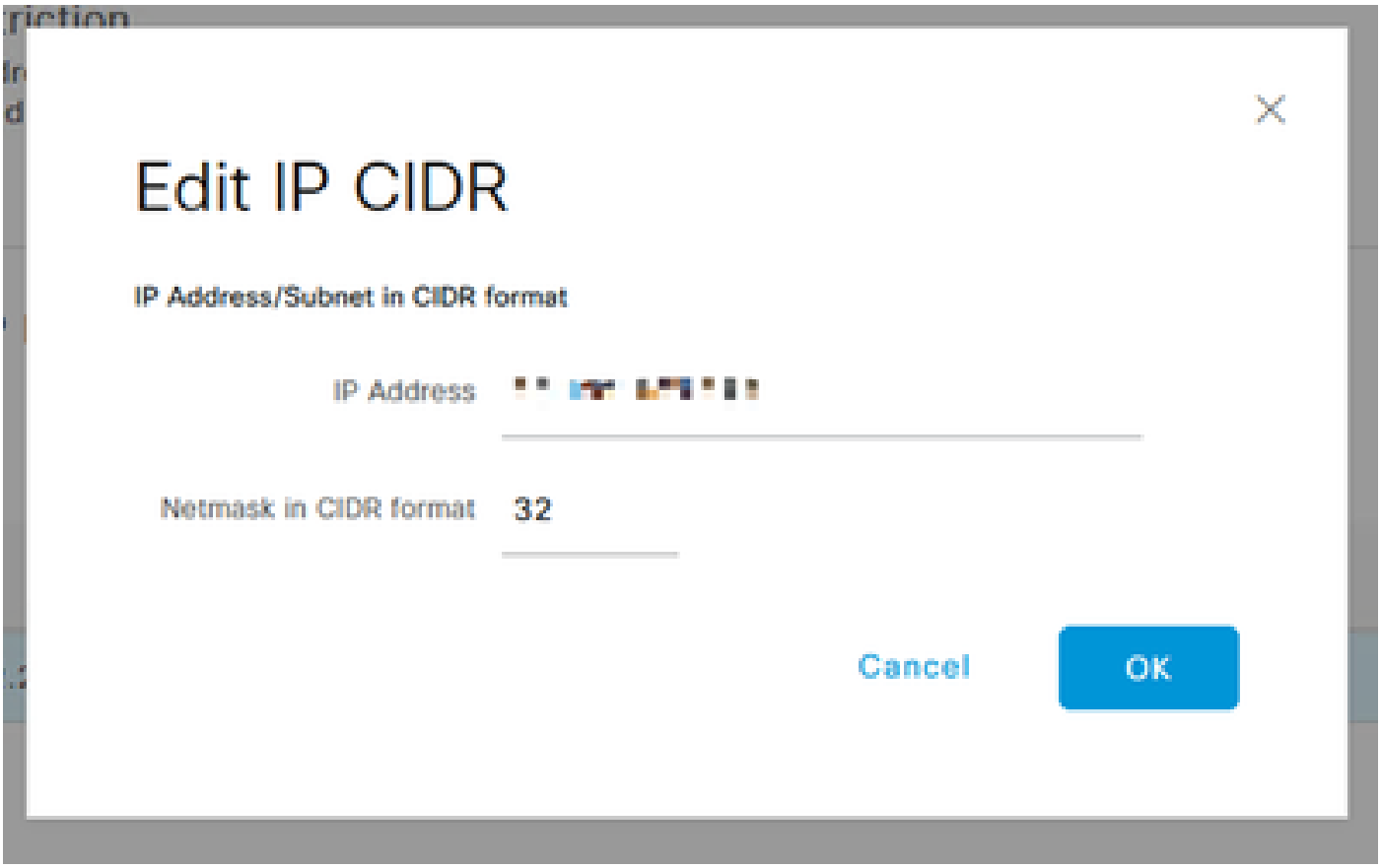
配置

- 选择. **Allow only listed IP addresses to connect**
- 单击。Add

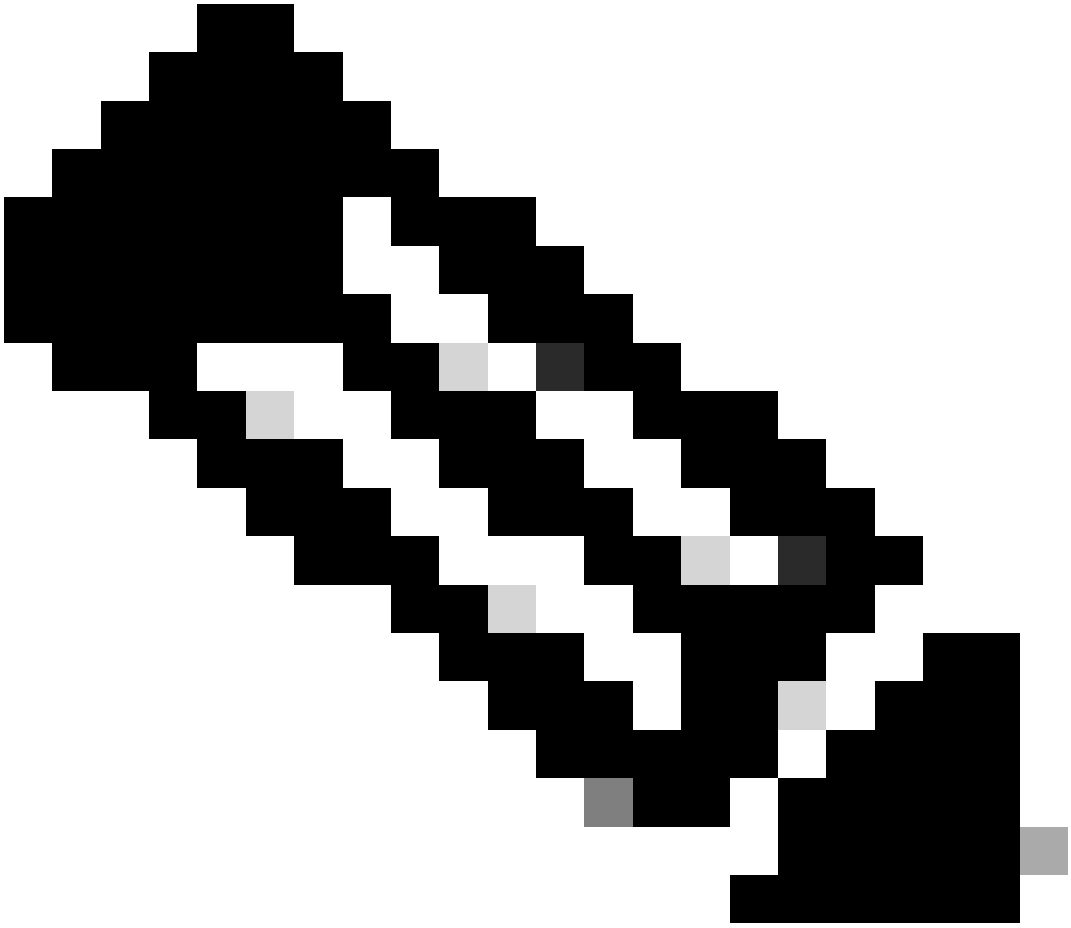


*IP*访问配置

- 在ISE 3.1中，您没有在Admin和**User** 服务之间选择的选项，启用IP访问限制阻止连接到：
  - GUI
  - CLI
  - SNMP
  - SSH
- 将打开一个对话框，您可以在其中输入CIDR格式的IP地址（IPv4或IPv6）。
- 配置IP后，以CIDR格式设置掩码。


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

编辑*IP CIDR*

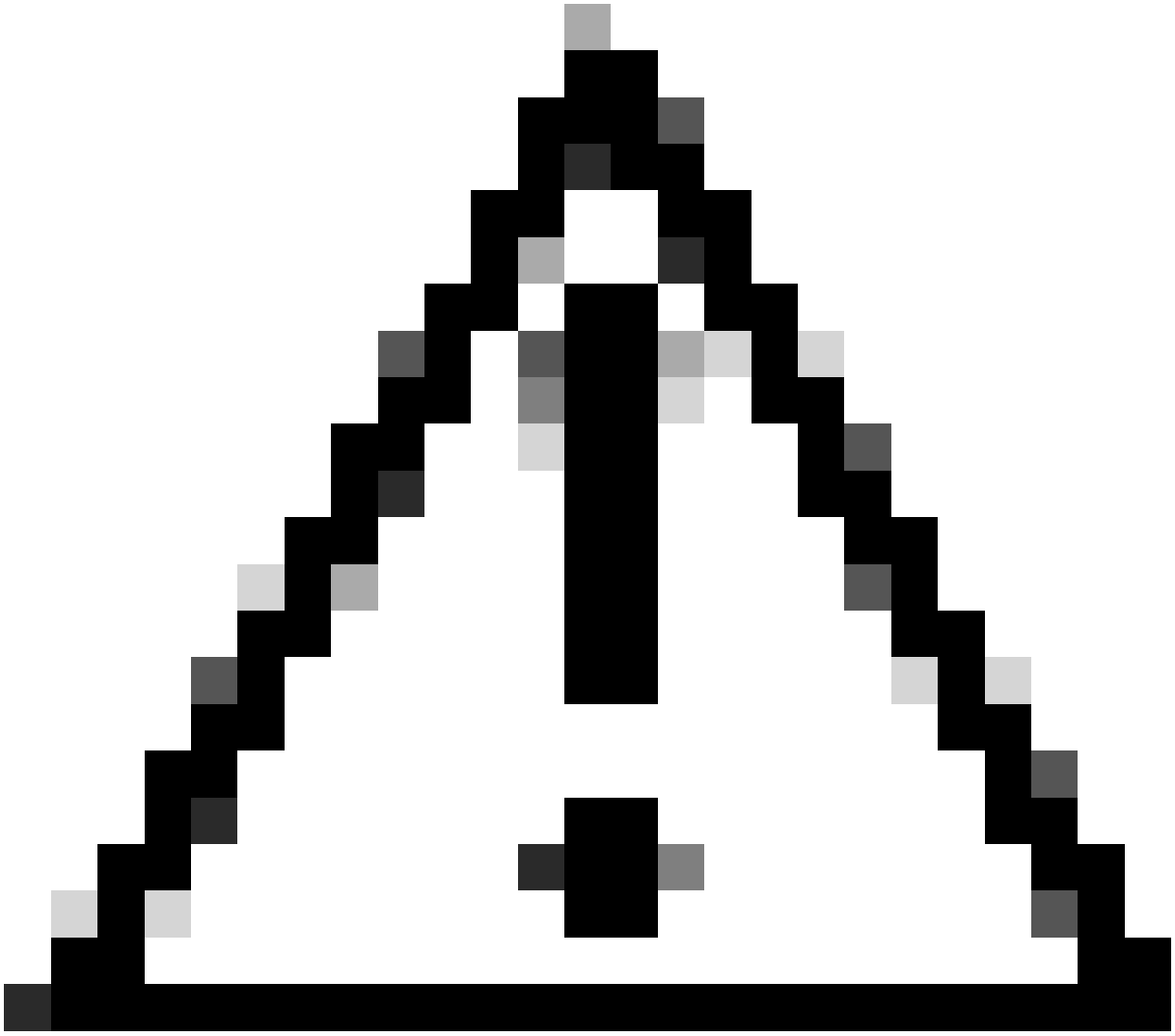


注意：IP无类域间路由(CIDR)格式是表示IP地址及其相关路由前缀的方法。

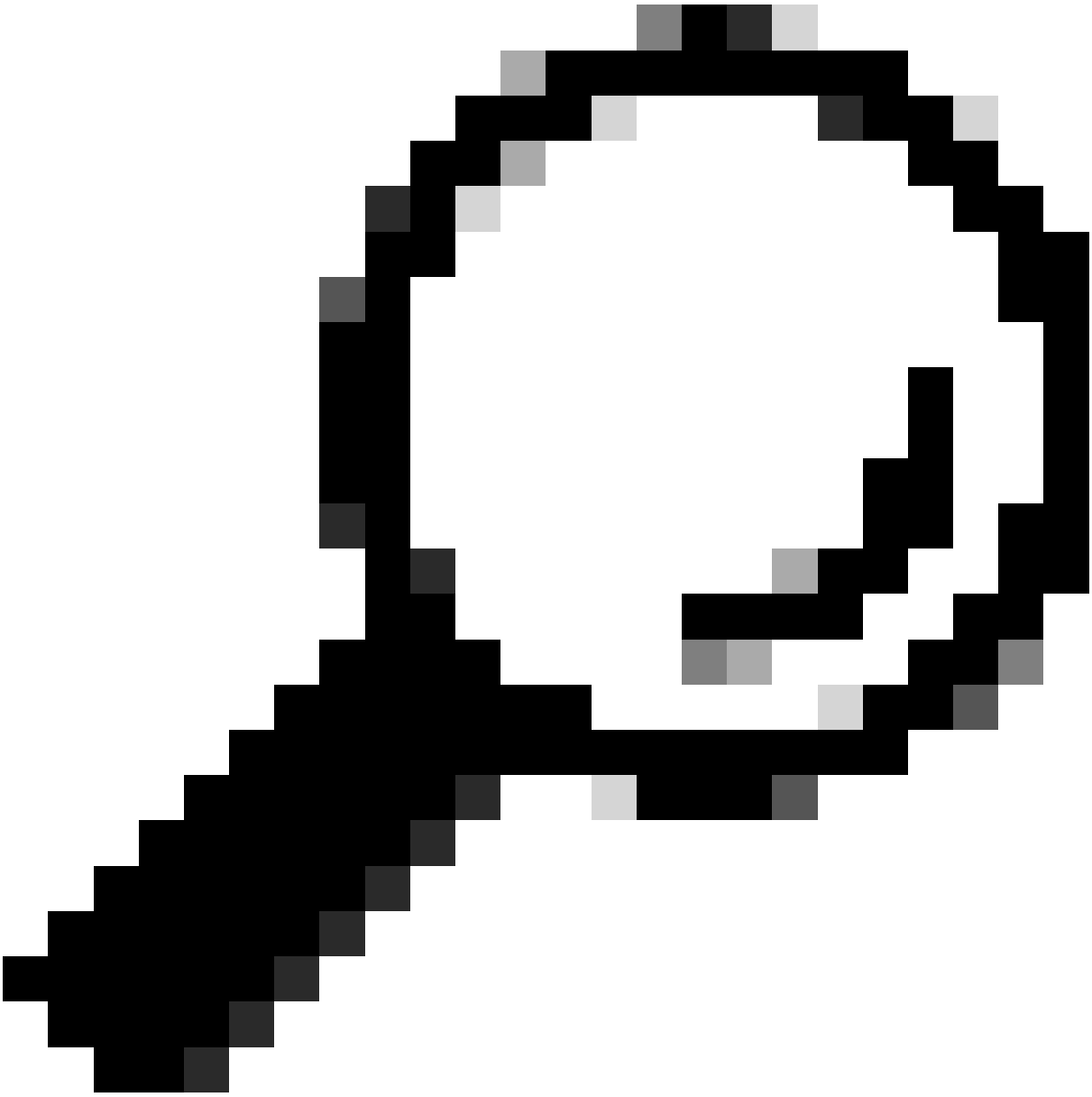
示例：

IP：10.8.16.32

掩码： /32



注意：配置IP限制时必须小心，以免意外锁定合法管理员访问权限。Cisco建议在完全实施任何IP限制配置之前对其进行全面测试。



提示：对于IPv4地址：

- 对特定IP地址使用/32。
- 对于子网，请使用任何其他选项。示例：10.26.192.0/18

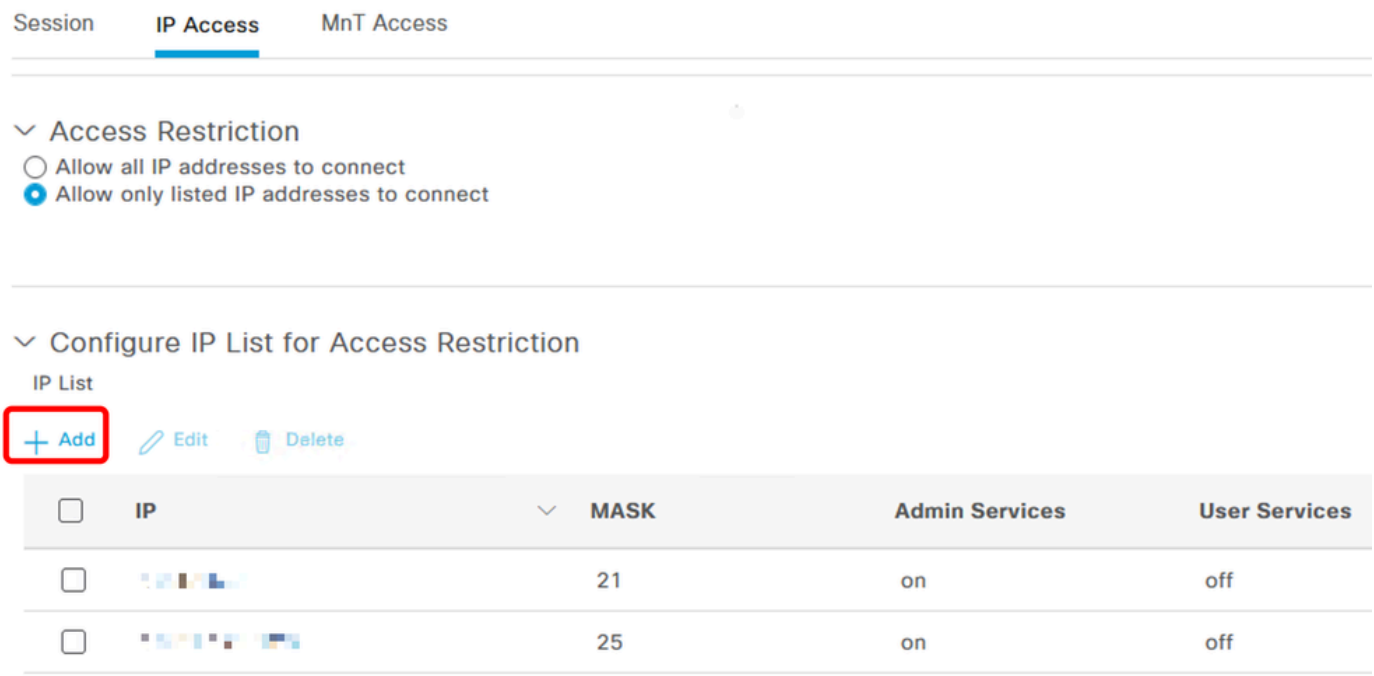
ISE 3.2中的行为

导航至Administration > Admin Access > Settings > Access. 您有以下可用选项：

- 会话
- IP访问
- MnT访问

配置

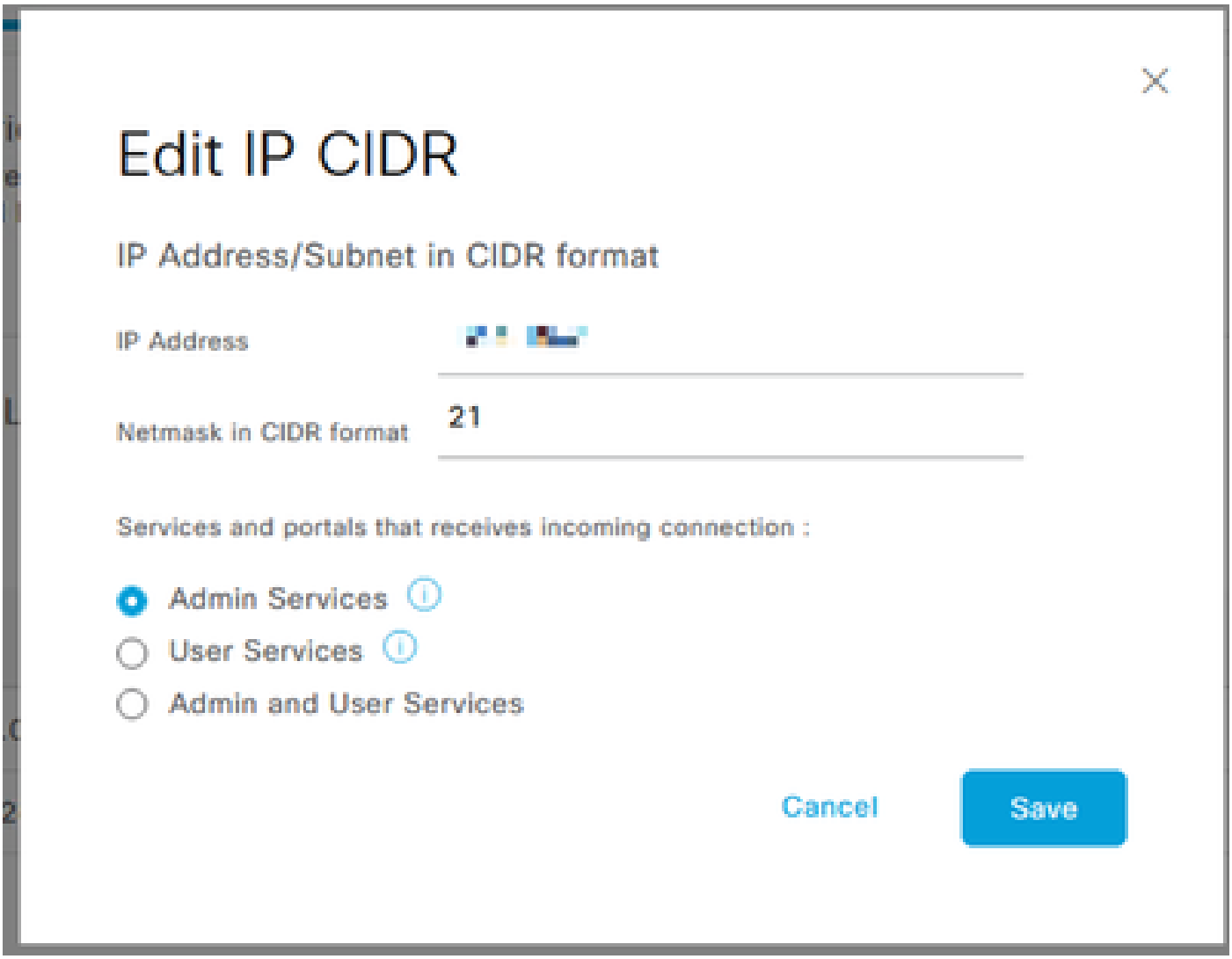
- 选择 **Allow only listed IP addresses to connect**.
- 单击。Add



*IP*访问配置

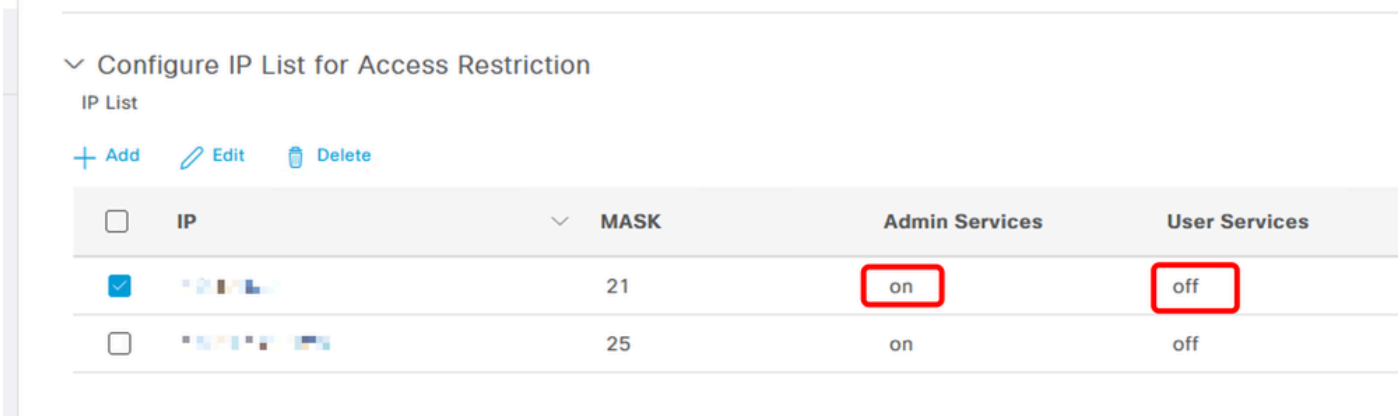
- 将打开一个对话框，您可以在其中输入CIDR格式的IP地址（IPv4或IPv6）。
- 配置IP后，以CIDR格式设置掩码。
- 以下选项可用于IP访问限制：

- 管理服务：GUI、CLI (SSH)、SNMP、ERS、OpenAPI、UDN、API网关、PxGrid（在补丁2中已禁用）、MnT分析
- 用户服务：访客、BYOD、状态、分析
- 管理员和用户服务



编辑*IP CIDR*

- 点击Save按钮。
- ON 表示启用管理服务，OFF表示禁用用户服务。

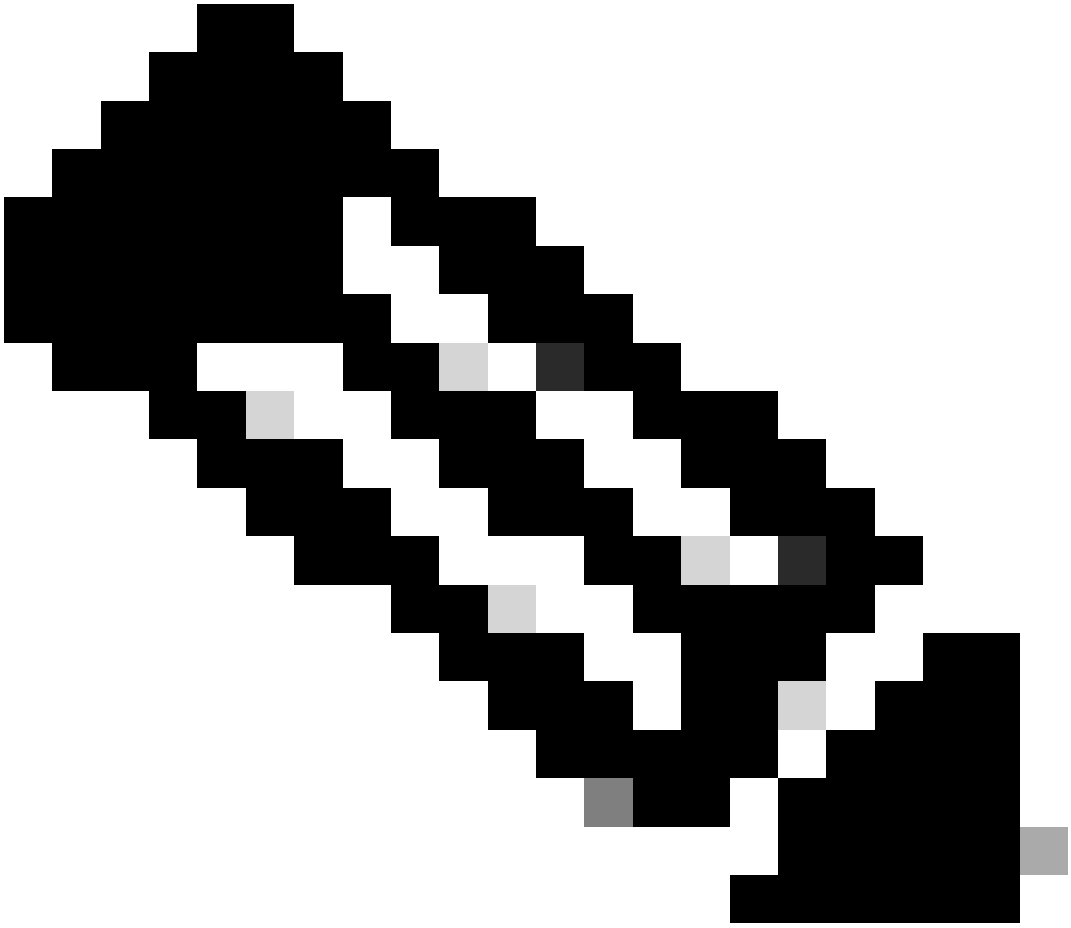


*3.2*中的*IP*访问配置

ISE 3.2 P4及更高版本中的行为

导航到Administration > Admin Access > Settings > Access。您可以使用以下选项：

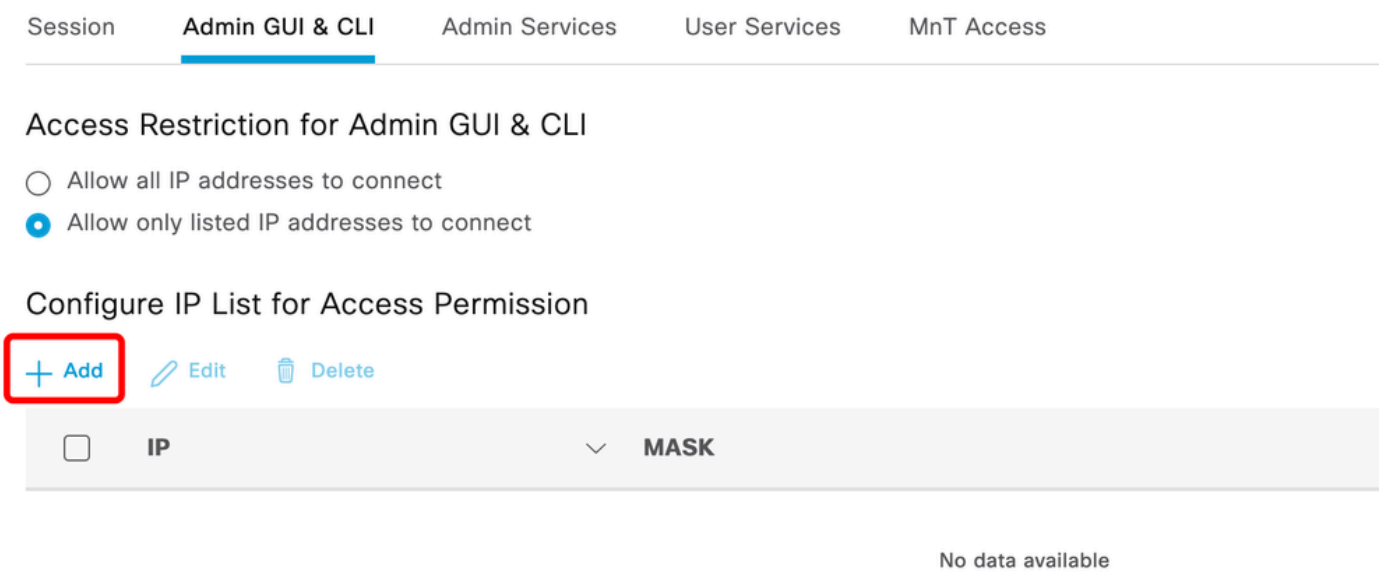
- 会话
- 管理GUI和CLI：ISE GUI (TCP 443)、ISE CLI (SSH TCP22)和SNMP。
- 管理服务：ERS API、Open API、pxGrid、DataConnect。
- 用户服务：访客、BYOD、状态。
- MNT访问：使用此选项，ISE不使用从外部源发送的系统日志消息。



注意：pxGrid和Data Connect访问限制适用于ISE 3.3+，但不适用于ISE 3.2 P4+。

配置

- 选择 Allow only listed IP addresses to connect.
- 点击 **Add**.



*3.3*中的*IP*访问配置

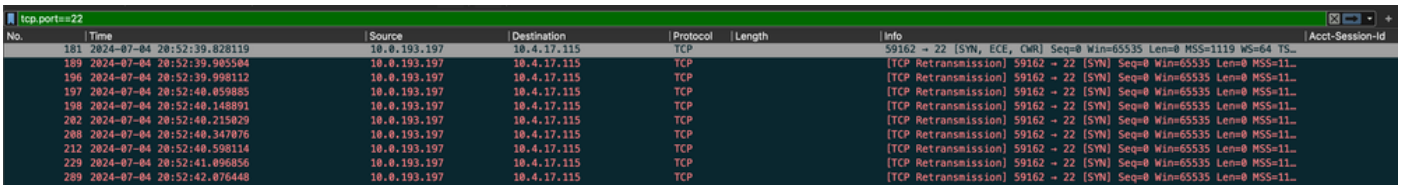
- 将打开一个对话框，您可以在其中输入CIDR格式的IP地址（IPv4或IPv6）。
- 配置IP后，以CIDR格式设置掩码。
- 单击。Add

恢复ISE GUI/CLI

- 使用控制台登录。
- 停止ISE服务 application stop ise
- 使用ISE启动服务 application start ise safe
- 从GUI中删除IP访问限制。

故障排除

执行数据包捕获，验证ISE是否不响应或丢弃流量。



检查ISE防火墙规则

- 对于3.1及更低版本，只能在show tech中检查。

    - 您可使用show tech将其存储在本地磁盘中 show tech-support file <filename>

        - 然后可以使用存储库URL更改将copy disk:/<filename> ftp://<ip_address>/path. 该文件传输到存储库，具体取决于您使用的存储库类型。
        - 您可以将该文件下载到您的计算机，以便读取并查找 **Running iptables -nvL**.
        - 此处不包括show tech中的初始规则。换句话说，在这里可以找到附加到show tech by IP Access限制功能的最后规则。

```
****************************************
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
```

- 对于3.2及更高版本，您可以使用命令show firewall检查防火墙规则。
- 3.2及更高版本可以更好地控制被IP访问限制阻止的服务。

```
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

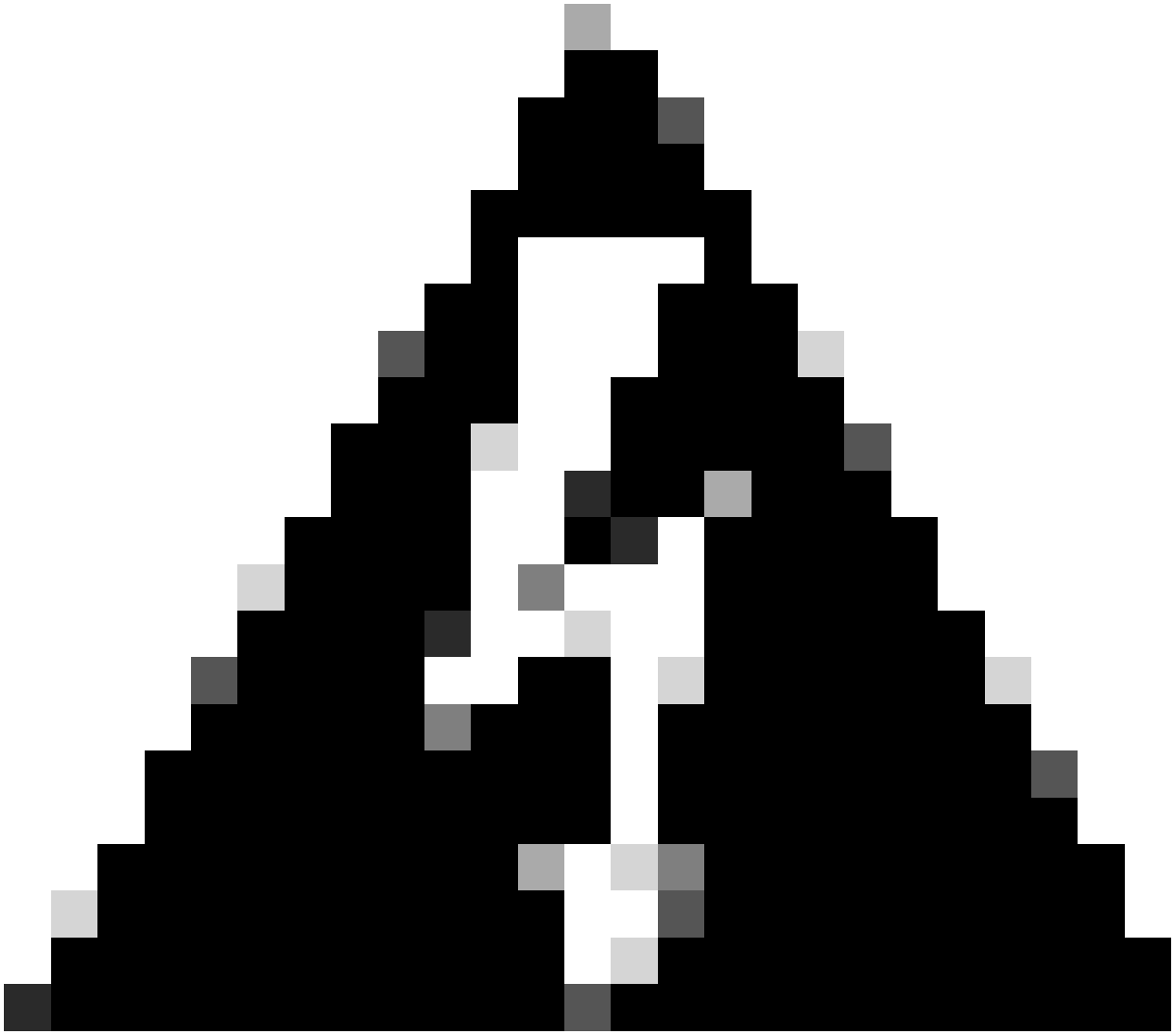
Chain ACCEPT_8910_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- * * x.x.x.x/x 0.0.0.0/0 tcp dpt:8910 Firewall rule permitting the PxGrid traffic from segment x.x.x.x/x
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
90 5400 DROP all -- * * 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 Firewall 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 Firewall 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 Firewall 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

检查调试日志



警告：并非所有流量都生成日志。IP访问限制可以在应用级别使用Linux内部防火墙阻止流量。SNMP、CLI和SSH在防火墙级别被阻止，因此不会生成任何日志。

- 启用Infrastructure 组件以从GUI进行调试。
- 启用**Admin-infra** 组件以从GUI进行调试。
- 启用**NSF** 组件以从GUI进行调试。
- 使用show logging application ise-psc.log tail。

当ISE管理员WebUI访问受限时，可以查看示例日志条目，其中允许的子网为198.18.133.0/24，而ISE管理员来自198.18.134.28。

```
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCache -:::::- IpList -> 198.18.133.0/24/basicS
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCache -:::::- Low ip address198.18.133.0
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCache -:::::- High ip address198.18.133.255
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.nsf.impl.NetworkElement -:::::- The ip address to check is v4 198.18.134.28
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCache -:::::- Checkin Ip In ipList returned Fin
```

相关信息

- ISE 3.1管理员指南
- ISE 3.2管理指南
- ISE 3.3管理指南
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。