

Configurar a restrição de acesso IP no ISE

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Comportamento no ISE 3.1 e versões anteriores](#)

[Configurar](#)

[Comportamento no ISE 3.2](#)

[Configurar](#)

[Comportamento no ISE 3.2 P4 e posterior](#)

[Configurar](#)

[Recuperar GUI/CLI do ISE](#)

[Troubleshooting](#)

[Verificar regras de firewall do ISE](#)

[Verificar logs de depuração](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve as opções disponíveis para configurar a restrição de acesso IP no ISE 3.1, 3.2 e 3.3.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico do Cisco Identity Service Engine

Componentes Utilizados

- Cisco Identity Services Engine versão 3.1
- Cisco Identity Services Engine versão 3.2
- Cisco Identity Services Engine versão 3.3

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

Informações de Apoio

O recurso de restrição de acesso IP permite que os administradores controlem quais endereços IP ou intervalos podem acessar o portal e os serviços do administrador do ISE.

Esse recurso se aplica a várias interfaces e serviços do ISE, incluindo:

- Acesso ao portal do administrador e CLI
- Acesso à API ERS
- Acesso ao portal de convidados e patrocinadores
- Acesso ao portal Meus dispositivos

Quando ativado, o ISE permite apenas conexões dos endereços IP ou intervalos especificados. Todas as tentativas de acessar as interfaces de administração do ISE a partir de IPs não especificados são bloqueadas.

Em caso de bloqueio acidental, o ISE fornece uma opção de inicialização de 'modo de segurança' que pode ignorar as restrições de acesso IP. Isso permite que os administradores recuperem o acesso e corrijam quaisquer configurações incorretas.

Comportamento no ISE 3.1 e versões anteriores

Navegue até Administração>Acesso de administrador>Configurações>Acesso. Você tem estas opções:

- Sessão
- Acesso IP
- Acesso MnT

Configurar

- Selecione "Permitir que somente os endereços IP listados se conectem"
- Clique em "Adicionar"

∨ Access Restriction

- Allow all IP addresses to connect
- Allow only listed IP addresses to connect

∨ Configure IP List for Access Restriction

IP List

+ Add Edit Delete

<input type="checkbox"/>	IP	▼	MASK
--------------------------	----	---	------

No data available

Configuração de acesso IP

- No ISE 3.1, você não tem uma opção para selecionar entre os serviços "Admin" e "Usuário", habilitando a Restrição de acesso IP para bloquear conexões a:
 - GUI
 - CLI
 - SNMP
 - SSH
- Uma caixa de diálogo é aberta onde você insere os endereços IP, IPv4 ou IPv6, no formato CIDR.
- Depois que o IP estiver configurado, defina a máscara no formato CIDR.

restriction

in
d



Edit IP CIDR

IP Address/Subnet in CIDR format

IP Address 

Netmask in CIDR format

Cancel

OK

Editor CIDR IP

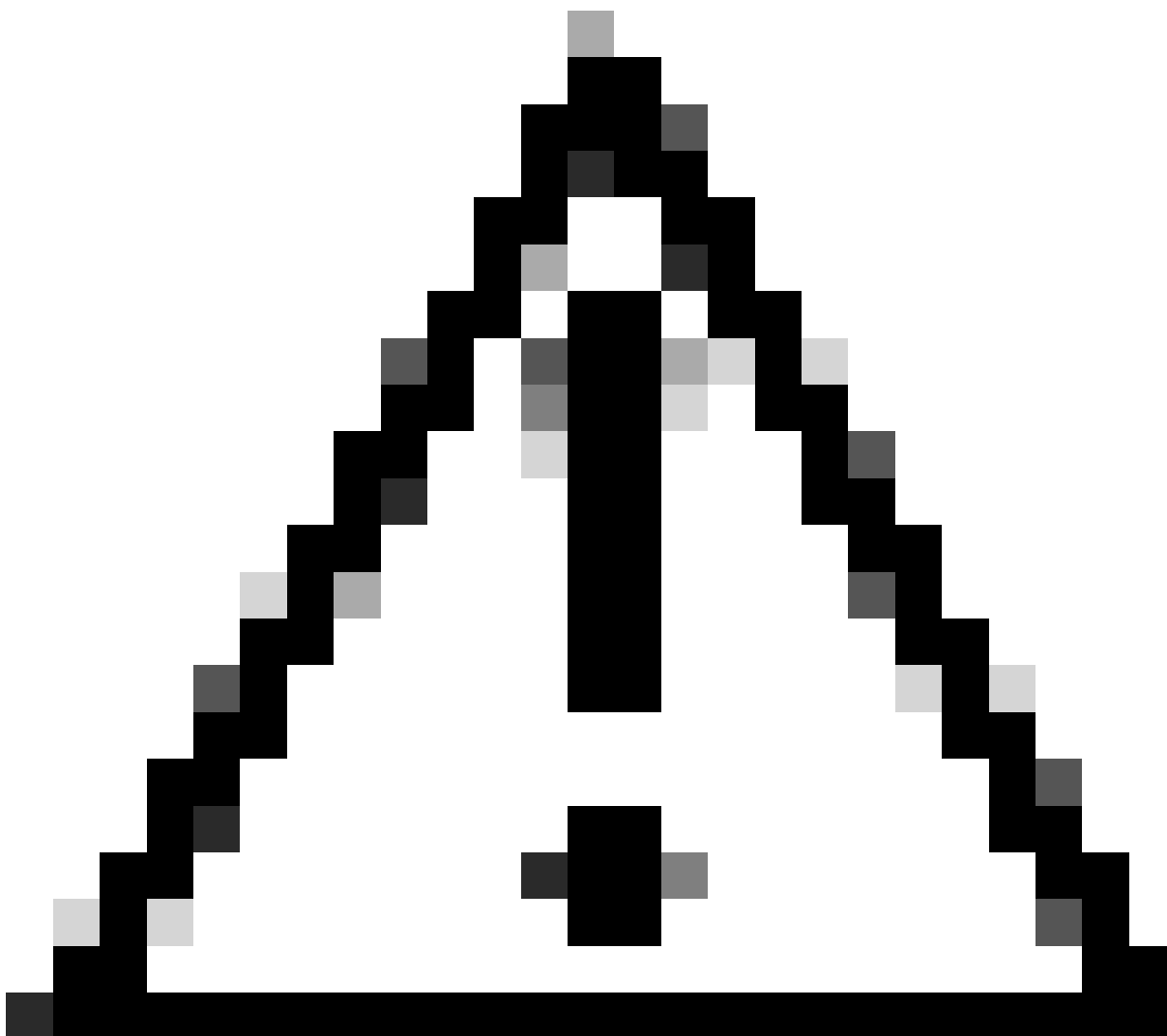


Observação: o formato IP CIDR (Classless Inter-Domain Routing) é um método de representação de endereços IP e seu prefixo de roteamento associado.

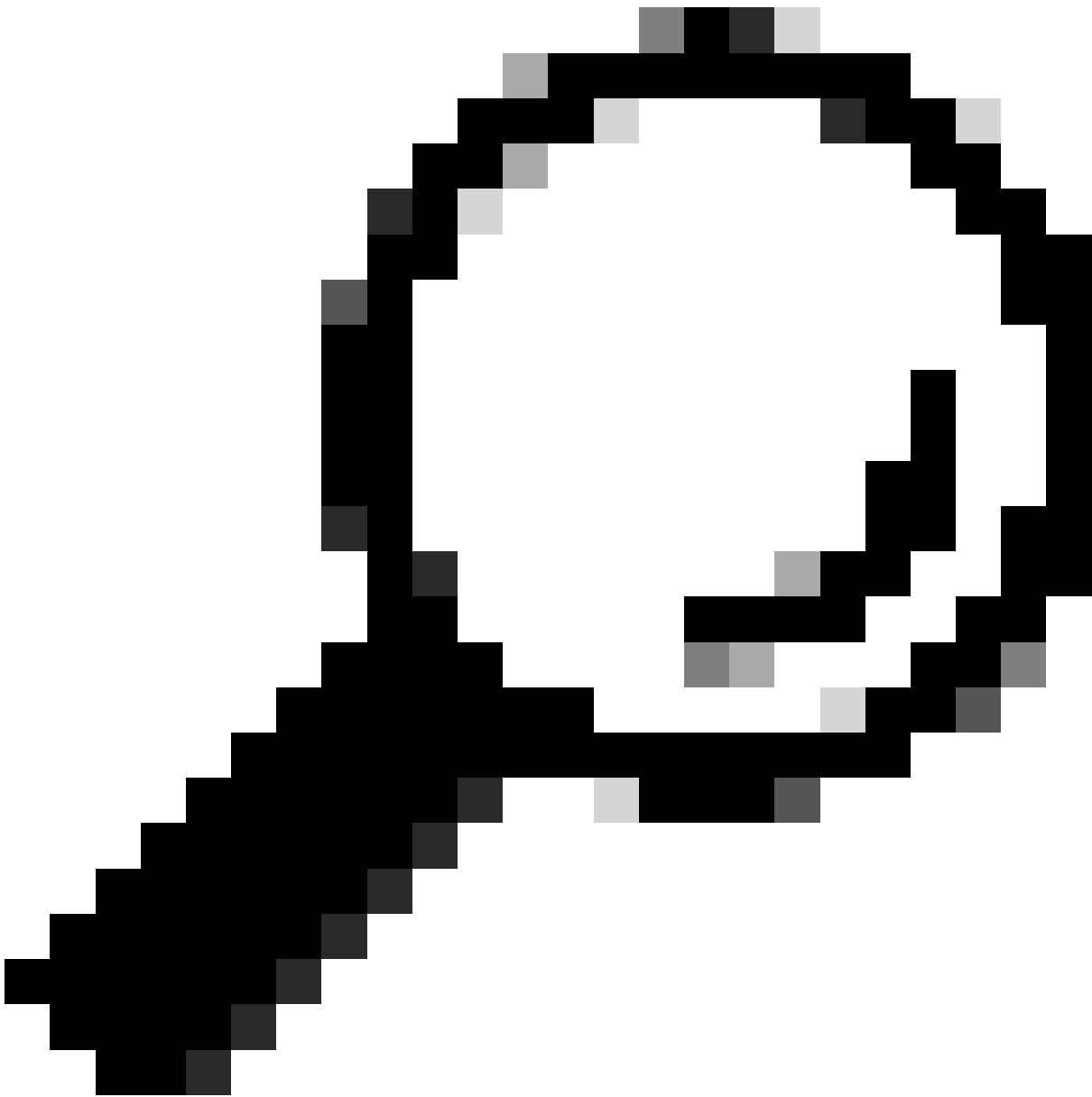
Exemplo:

IP: 10.8.16.32

Máscara: /32



Cuidado: deve-se tomar cuidado ao configurar restrições de IP para evitar o bloqueio acidental do acesso legítimo do administrador. A Cisco recomenda testar completamente qualquer configuração de restrição de IP antes de implementá-la completamente.



Dica: para endereços IPv4:

- Use /32 para endereços IP específicos.
- Para sub-redes, use qualquer outra opção. Exemplo: 10.26.192.0/18

Comportamento no ISE 3.2

Navegue até [Administração](#)>[Acesso de administrador](#)>[Configurações](#)>[Acesso](#). Você tem estas opções disponíveis:

- Sessão
- Acesso IP
- Acesso MnT

Configurar

- Selecione "Permitir que somente os endereços IP listados se conectem"
- Clique em "Adicionar"

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

+ Add  Edit  Delete

<input type="checkbox"/>	IP	MASK	Admin Services	User Services
<input type="checkbox"/>	10.10.10.10	21	on	off
<input type="checkbox"/>	10.10.10.10	25	on	off

Configuração de acesso IP

- Uma caixa de diálogo é aberta onde você insere os endereços IP, IPv4 ou IPv6, no formato CIDR.
- Depois que o IP estiver configurado, defina a máscara no formato CIDR.
- Essas opções estão disponíveis para restrição de acesso IP
 - Serviços de administração: GUI, CLI (SSH), SNMP, ERS, OpenAPI, UDN, API Gateway, PxGrid (desabilitado no Patch 2), MnT Analytics
 - Serviços de usuário: convidado, BYOD, postura, criação de perfis
 - Serviços de administrador e usuário

Editar CIDR IP

- Clique no botão "Salvar"
- "ATIVADO" significa que os serviços do administrador estão ativados, "DESATIVADO" significa que os serviços do usuário estão desativados.

Configure IP List for Access Restriction

IP List

+ Add Edit Delete

<input type="checkbox"/>	IP	MASK	Admin Services	User Services
<input checked="" type="checkbox"/>		21	on	off
<input type="checkbox"/>		25	on	off

Configuração de acesso IP no 3.2

Comportamento no ISE 3.2 P4 e posterior

Navegue até Administração>Acesso de administrador>Configurações>Acesso. Você tem estas

opções disponíveis:

- Sessão
- GUI e CLI do administrador: GUI do ISE (TCP 443), CLI do ISE (SSH TCP22) e SNMP.
- Serviços de administração: ERS API, Open API, pxGrid, DataConnect.
- Serviços ao usuário: convidado, BYOD, postura.
- Acesso MNT: com essa opção, o ISE não consome mensagens de Syslog enviadas de fontes externas.

Configurar

- Selecione "Permitir que somente os endereços IP listados se conectem"
- Clique em "Adicionar"

The screenshot shows the configuration page for "Admin GUI & CLI" access restriction. The page has a navigation bar with tabs: "Session", "Admin GUI & CLI" (selected), "Admin Services", "User Services", and "MnT Access". Below the navigation bar, the title is "Access Restriction for Admin GUI & CLI". There are two radio button options: "Allow all IP addresses to connect" (unselected) and "Allow only listed IP addresses to connect" (selected). Below this, the section is titled "Configure IP List for Access Permission". There are three buttons: "+ Add" (highlighted with a red box), "Edit", and "Delete". Below the buttons is a table with two columns: "IP" and "MASK". The table is currently empty, and the text "No data available" is displayed at the bottom right of the table area.

Configuração de acesso IP no 3.3

- Uma caixa de diálogo é aberta onde você insere os endereços IP, IPv4 ou IPv6, no formato CIDR.
- Depois que o IP estiver configurado, defina a máscara no formato CIDR.
- Clique em "Adicionar"

Recuperar GUI/CLI do ISE

- Fazer login com o console
- Interrompa os serviços do ISE usando o comando stop do aplicativo
- Inicie os serviços do ISE usando o application start ise safe
- Remova a restrição de acesso IP da GUI.

Troubleshooting

Faça uma captura de pacote para verificar se o ISE não está respondendo ou se está

descartando o tráfego.

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, CWB] Seq=0 Win=65535 Len=0 MSS=1119 WS=64 TS...	
189	2024-07-04 20:52:39.985584	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 20:52:40.215829	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...	

Verificar regras de firewall do ISE

- Para 3.1 e inferior, você pode verificar isso apenas no show tech.
 - Você pode pegar um show tech e armazená-lo no disco local usando "show tech-support file <filename>"
 - Em seguida, você pode transferir o arquivo para um repositório usando "copy disk:<filename> ftp://<ip_address>/path" as alterações de url do repositório, dependendo do tipo de repositório que você está usando
 - Você pode fazer o download do arquivo para sua máquina para poder lê-lo e procurar "Running iptables -nvL"
 - As regras iniciais do show tech não estão incluídas abaixo. Em outras palavras, aqui você pode encontrar as últimas regras anexadas ao recurso 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 a versão 3.2 e posterior, você pode usar o comando "show firewall" para verificar as regras de firewall.
- 3.2 e superiores fornecem mais controle sobre os serviços que estão sendo bloqueados pela Restrição de Acesso 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
```

iptables 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
```

iptables 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
```

iptables 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
```

Verificar logs de depuração



Aviso: nem todo o tráfego gera logs. A restrição de acesso IP pode bloquear o tráfego no nível do aplicativo e usando o firewall interno do Linux. SNMP, CLI e SSH são bloqueados no nível do firewall para que nenhum registro seja gerado.

-
- Ative o componente "Infraestrutura" em DEBUG a partir da GUI.
 - Use `show logging application ise-psc.log tail`

Os próximos logs podem ser vistos quando a restrição de acesso IP está agindo.

```
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
```

Informações Relacionadas

- [Suporte técnico e downloads da Cisco](#)
- [Guia do administrador do ISE 3.1](#)
- [Guia do administrador do ISE 3.2](#)
- [Guia do administrador do ISE 3.3](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.