

# IP-toegangsbeperking configureren in ISE

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Gedrag in ISE 3.1 en lager](#)

[Configureren](#)

[Gedrag in ISE 3.2](#)

[Configureren](#)

[Gedrag in ISE 3.2 P4 en hoger](#)

[Configureren](#)

[ISE-GUI/CLI herstellen](#)

[Probleemoplossing](#)

[Controleer ISE-firewallregels](#)

[Logboeken voor debuggen controleren](#)

[Gerelateerde informatie](#)

---

## Inleiding

In dit document worden de beschikbare opties beschreven om IP-toegangsbeperking in ISE 3.1, 3.2 en 3.3 te configureren.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van Cisco Identity Service Engine

### Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

Met de functie voor IP-toegangsbeperking kunnen beheerders bepalen welke IP-adressen of bereiken toegang kunnen krijgen tot het ISE-beheerportal en de services.

Deze optie is van toepassing op verschillende ISE-interfaces en -services, waaronder:

- Admin-poorttoegang en CLI
- ERS API-toegang
- Toegang tot gast- en sponsorportal
- Toegang tot mijn apparaatportal

Als deze optie is ingeschakeld, maakt ISE alleen verbindingen mogelijk vanaf de opgegeven IP-adressen of bereiken. Alle pogingen om toegang te krijgen tot ISE-beheerinterfaces van niet-gespecificeerde IP's worden geblokkeerd.

In het geval van accidentele lock-out biedt ISE een opstartoptie 'safe mode' die IP-toegangsbeperkingen kan omzeilen. Hiermee kunnen beheerders toegang verkrijgen en eventuele fouten corrigeren.

## Gedrag in ISE 3.1 en lager

Navigeer naar Beheer>Admin Access>Instellingen>Toegang. U hebt de volgende opties:

- Sessie
- IP-toegang
- MnT-toegang

### Configureren

- Selecteer "Alleen genoemde IP-adressen toestaan om verbinding te maken"
- Klik op "Toevoegen"

∨ 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

IP-toegangsconfiguratie

- In ISE 3.1 hebt u geen optie om te kiezen tussen "Admin" en "User" services, waardoor IP Access Restriction blokkeert verbindingen om:
  - GUI
  - CLI
  - SNMP
  - SSH
- Er wordt een dialoogvenster geopend waar u de IP-adressen, IPv4 of IPv6, in CIDR-indeling kunt invoeren.
- Zodra IP is geconfigureerd, stelt u het masker in CIDR-indeling in.

restriction

in  
d



# Edit IP CIDR

IP Address/Subnet in CIDR format

IP Address 

Netmask in CIDR format

Cancel

OK

IP CIDR bewerken



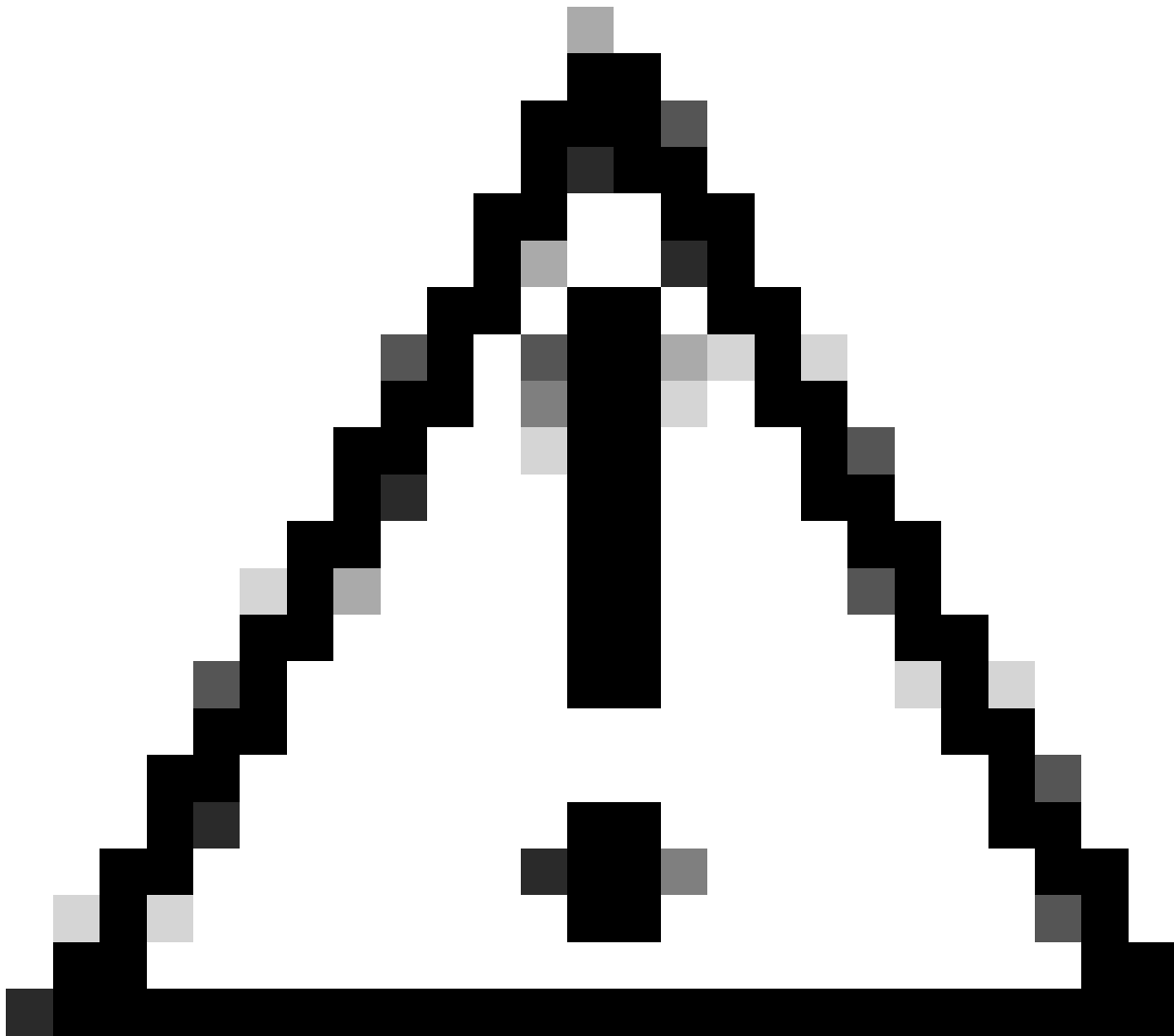
Opmerking: het formaat IP CIDR (Classless Inter-Domain Routing) is een methode om IP-adressen en het bijbehorende routingprefix weer te geven.

Voorbeeld:

IP: 10.8.16.32

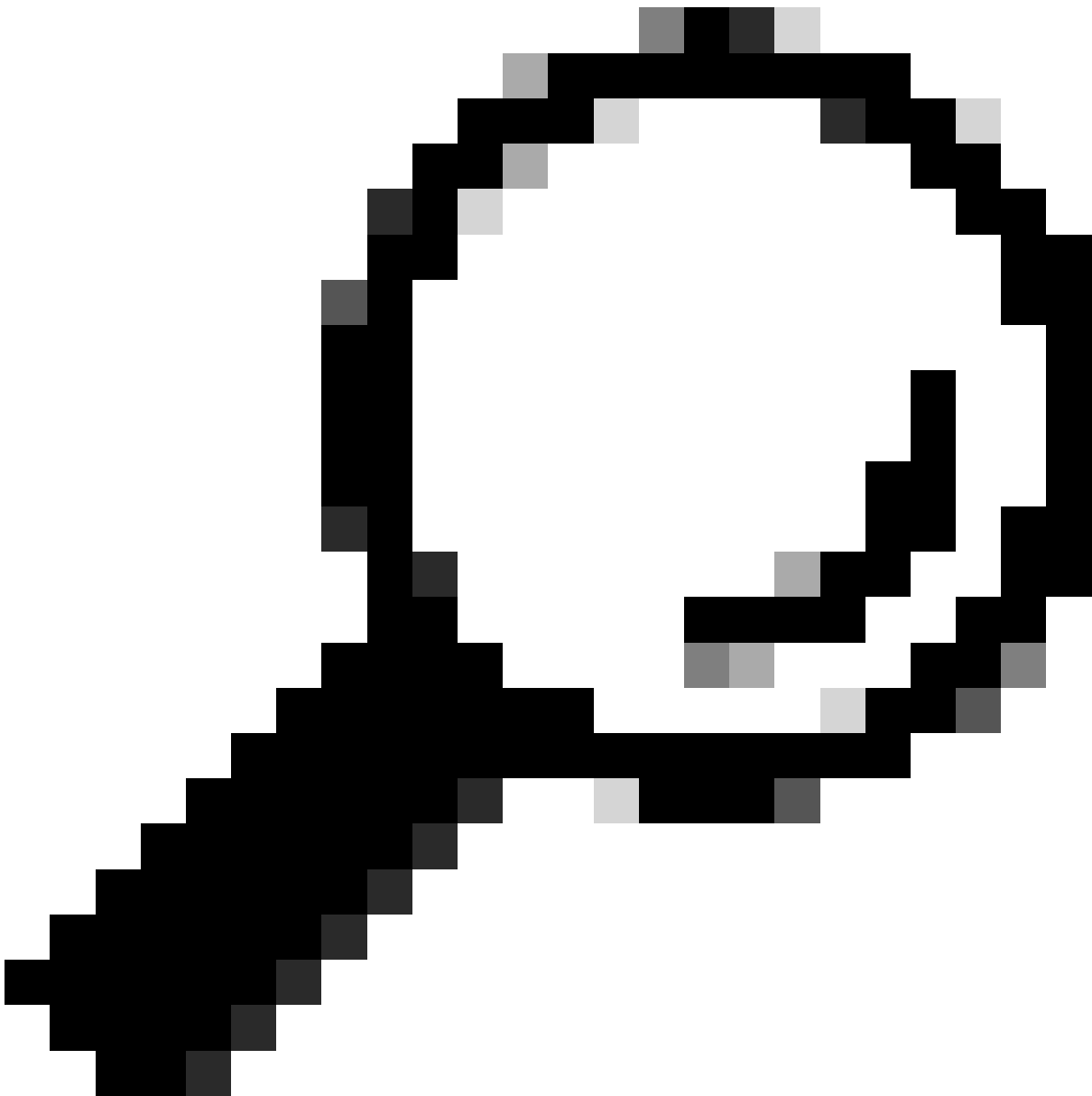
Masker: /32

---



Waarschuwing: bij het configureren van IP-beperkingen moet u voorzichtig zijn om te voorkomen dat legitieme beheerderstoegang per ongeluk wordt uitgesloten. Cisco adviseert het grondig testen van elke configuratie van IP-beperkingen voordat deze volledig wordt geïmplementeerd.

---



Tip: voor IPv4-adressen:

- Gebruik /32 voor specifieke IP-adressen.
- Gebruik voor subnetten een andere optie. Voorbeeld: 10.26.192.0/18

---

## Gedrag in ISE 3.2

Navigeer naar [Beheer](#)>[Admin Access](#)>[Instellingen](#)>[Toegang](#). U hebt de volgende opties beschikbaar:

- Sessie
- IP-toegang
- MnT-toegang

## Configureren

- Selecteer "Alleen genoemde IP-adressen toestaan om verbinding te maken"
- Klik op "Toevoegen"

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"/>		21	on	off
<input type="checkbox"/>		25	on	off

### IP-toegangsconfiguratie

- Er wordt een dialoogvenster geopend waar u de IP-adressen, IPv4 of IPv6, in CIDR-indeling kunt invoeren.
- Zodra IP is geconfigureerd, stelt u het masker in CIDR-indeling in.
- Deze opties zijn beschikbaar voor IP-toegangsbeperking
  - Admin Services: GUI, CLI (SSH), SNMP, ERS, OpenAPI, UDN, API-gateway, PxGrid (uitgeschakeld in Patch 2), MnT Analytics
  - Gebruikersservices: Gast, BYOD, Positie, Profiling
  - Beheer- en gebruikersservices



✕

## Edit IP CIDR

IP Address/Subnet in CIDR format

IP Address

Netmask in CIDR format

Services and portals that receives incoming connection :

Admin Services ⓘ

User Services ⓘ

Admin and User Services

Cancel
Save

IP CIDR bewerken

- Klik op de knop "Opslaan"
- "AAN" staat voor Admin-services ingeschakeld en "OFF" staat voor gebruikersservices die zijn uitgeschakeld.

∨ Configure IP List for Access Restriction

IP List

[+ Add](#) [Edit](#) [Delete](#)

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

IP-toegangsconfiguratie in 3.2

## Gedrag in ISE 3.2 P4 en hoger

Navigeer naar Beheer>Admin Access>Instellingen>Toegang. U hebt de volgende opties

beschikbaar:

- Sessie
- Admin GUI&CLI: ISE GUI (TCP 43), ISE CLI (SSH TCP22) en SNMP.
- Beheerservices: ERS API, Open API, pxGrid, DataConnect.
- Gebruikersdiensten: Gast, BYOD, Positie.
- MNT Access: met deze optie neemt ISE geen Syslog-berichten uit externe bronnen in beslag.

## Configureren

- Selecteer "Alleen genoemde IP-adressen toestaan om verbinding te maken"
- Klik op "Toevoegen"

The screenshot shows the configuration page for 'Admin GUI & CLI' under the 'Access Restriction' section. The 'Admin GUI & CLI' tab is selected. The configuration is set to 'Allow only listed IP addresses to connect'. Below this, there is a section for 'Configure IP List for Access Permission' with a '+ Add' button highlighted in a red box, along with 'Edit' and 'Delete' buttons. A table header is visible with columns for 'IP' and 'MASK'. The table is currently empty, and the text 'No data available' is displayed below it.

IP-toegangsconfiguratie in 3.3

- Er wordt een dialoogvenster geopend waar u de IP-adressen, IPv4 of IPv6, in CIDR-indeling kunt invoeren.
- Zodra IP is geconfigureerd, stelt u het masker in CIDR-indeling in.
- Klik op "Toevoegen"

## ISE-GUI/CLI herstellen

- Aanmelden met console
- Stop ISE-services met applicatie stop ise
- Start ISE-services met applicatie start ise safe
- Verwijder de IP-toegangsbeperking uit de GUI.

## Probleemoplossing

Neem een pakketopname om te controleren of ISE niet reageert of het verkeer laat vallen.

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 20:52:39.985504	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...	

## Controleer ISE-firewallregels

- Voor 3.1 en lager kun je dit alleen controleren in de show tech.
  - U kunt een show tech nemen en opslaan in de localdisk met behulp van "show tech-support bestand <filename>"
  - Vervolgens kunt u het bestand overbrengen naar een repository met behulp van "copy disk:./<filename> ftp://<ip\_address>/path" de repository URL verandert afhankelijk van het type repository dat u gebruikt
  - U kunt het bestand downloaden naar uw computer, zodat u het kunt lezen en op zoek kunt naar "Running iptables -nvL"
  - De eerste regels in de show tech zijn niet hieronder opgenomen. Met andere woorden, hier kunt u de laatste regels vinden die aan de showtech zijn toegevoegd door de beperkingsfunctie van IP Access.

<#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

- Voor 3.2 en hoger kunt u de opdracht "Toon firewall" gebruiken om de firewallregels te controleren.
- 3.2 en hoger bieden meer controle over de services die worden geblokkeerd door IP-toegangsbeperking.

<#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
```

## Logboeken voor debuggen controleren



Waarschuwing: niet al het verkeer genereert logs. IP Access-bepanking kan het verkeer op toepassingsniveau blokkeren met behulp van Linux Internal Firewall. SNMP, CLI en SSH zijn op firewallniveau geblokkeerd, zodat er geen logs worden gegenereerd.

- 
- Schakel de component "Infrastructuur" in DEBUG vanuit GUI in.
  - Gebruik show logging applicatie ise-psc.log tail

De volgende logbestanden kunnen worden weergegeven wanneer er actie wordt ondernomen tegen de beperking van IP-toegang.

```
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
```

## Gerelateerde informatie

- [Cisco Technical Support en downloads](#)
- [ISE 3.1 beheerdershandleiding](#)
- [ISE 3.2 beheerdershandleiding](#)
- [ISE 3.3 beheerdershandleiding](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.