

# Konfigurieren der IP-Zugriffsbeschränkung in der ISE

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Verhalten bei ISE 3.1 und niedriger](#)

[Konfigurieren](#)

[Verhalten in ISE 3.2](#)

[Konfigurieren](#)

[Verhalten bei ISE 3.2 P4 und höher](#)

[Konfigurieren](#)

[Wiederherstellen der ISE-GUI/CLI](#)

[Fehlerbehebung](#)

[ISE-Firewall-Regeln überprüfen](#)

[Debug-Protokolle überprüfen](#)

[Zugehörige Informationen](#)

---

## Einleitung

In diesem Dokument werden die verfügbaren Optionen zum Konfigurieren von IP-Zugriffsbeschränkungen in ISE 3.1, 3.2 und 3.3 beschrieben.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse der Cisco Identity Service Engine

### Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Hintergrundinformationen

Mit der Funktion für IP-Zugriffsbeschränkungen können Administratoren steuern, welche IP-Adressen oder IP-Adressbereiche auf das ISE-Admin-Portal und die ISE-Services zugreifen können.

Diese Funktion gilt für verschiedene ISE-Schnittstellen und -Services, darunter:

- Admin-Portalzugriff und CLI
- ERS API-Zugriff
- Zugriff auf das Gast- und Sponsorportal
- Zugriff auf das Geräteportal

Wenn diese Funktion aktiviert ist, lässt die ISE nur Verbindungen von den angegebenen IP-Adressen oder -Bereichen zu. Alle Versuche, von nicht angegebenen IPs auf ISE-Verwaltungsschnittstellen zuzugreifen, werden blockiert.

Im Falle einer versehentlichen Sperre bietet die ISE eine Startoption im "sicheren Modus", mit der IP-Zugriffsbeschränkungen umgangen werden können. Administratoren erhalten so wieder Zugriff und können Fehlkonfigurationen korrigieren.

## Verhalten bei ISE 3.1 und niedriger

Navigieren Sie zu Administration > Admin Access > Settings > Access. Folgende Optionen stehen zur Verfügung:

- Sitzung
- IP-Zugriff
- MnT-Zugriff

### Konfigurieren

- Wählen Sie Verbindungen nur mit aufgelisteten IP-Adressen zulassen aus.
- Klicken Sie auf "Hinzufügen"

∨ 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-Zugriffskonfiguration

- In ISE 3.1 haben Sie keine Option zur Auswahl zwischen "Admin"- und "User"-Services. Durch die Aktivierung von "IP Access Restriction" werden Verbindungen blockiert, um:
  - GUI
  - CLI
  - SNMP
  - SSH
- Es wird ein Dialogfeld geöffnet, in dem Sie die IP-Adressen IPv4 oder IPv6 im CIDR-Format eingeben.
- Sobald die IP konfiguriert ist, legen Sie die Maske im CIDR-Format fest.

restriction

in  
d



# Edit IP CIDR

IP Address/Subnet in CIDR format

IP Address 

Netmask in CIDR format

Cancel

OK

IP-CIDR bearbeiten.



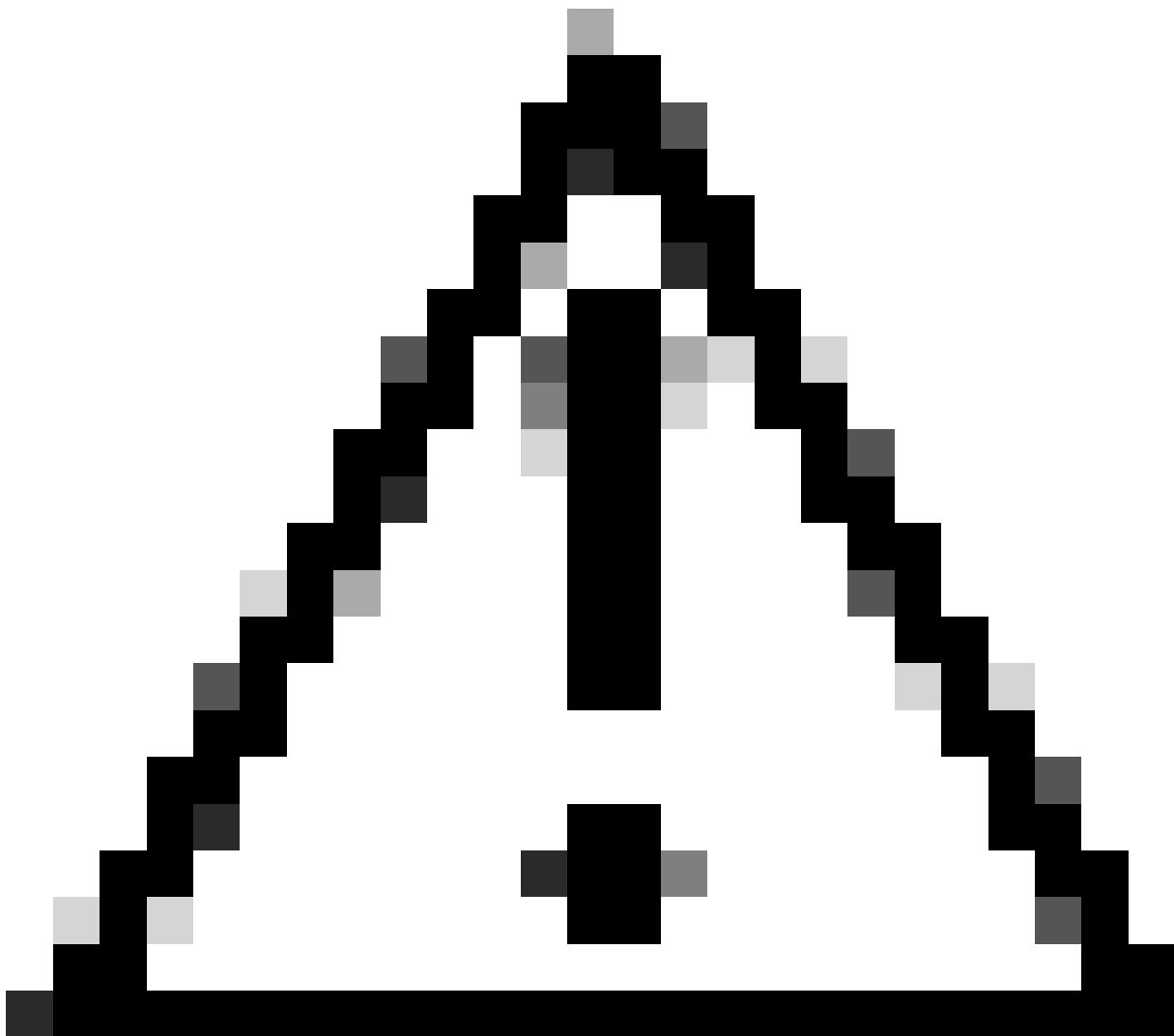
Hinweis: Das IP-CIDR-Format (Classless Inter-Domain Routing) ist eine Methode zur Darstellung von IP-Adressen und den zugehörigen Routing-Präfixen.

Beispiel:

IP: 10.8.16.32

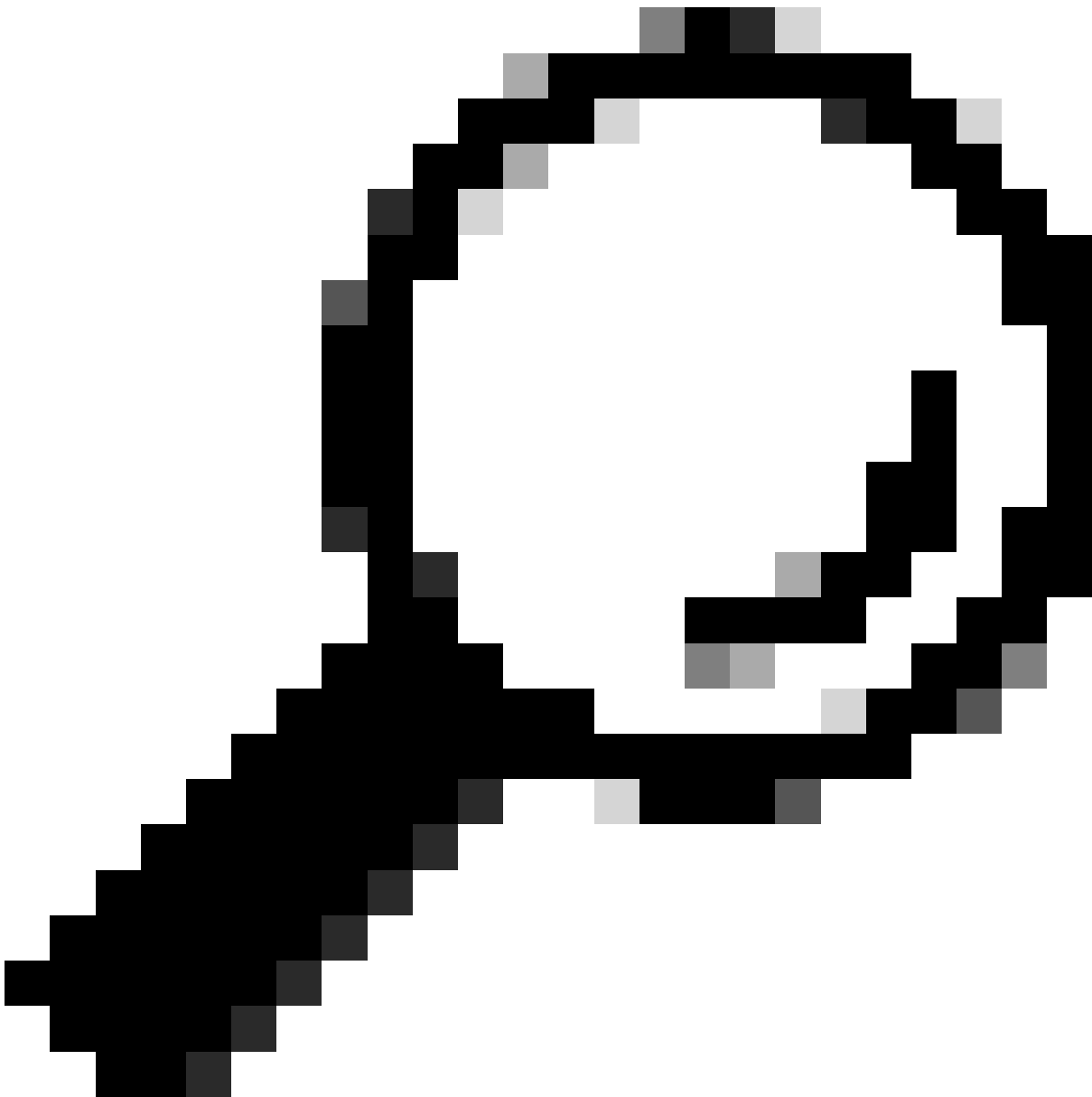
Maske: /32

---



Vorsicht: Bei der Konfiguration von IP-Einschränkungen muss sorgfältig vorgegangen werden, um zu verhindern, dass der legitime Administratorzugriff versehentlich gesperrt wird. Cisco empfiehlt, vor der vollständigen Implementierung alle Konfigurationen mit IP-Einschränkungen sorgfältig zu testen.

---



Tipp: Für IPv4-Adressen:

- Verwenden Sie /32 für bestimmte IP-Adressen.
- Verwenden Sie für Subnetze alle anderen Optionen. Beispiel: 10.26.192.0/18

---

## Verhalten in ISE 3.2

Navigieren Sie zu Administration > Admin Access > Settings > Access. Folgende Optionen stehen zur Verfügung:

- Sitzung
- IP-Zugriff
- MnT-Zugriff

## Konfigurieren

- Wählen Sie Verbindungen nur mit aufgelisteten IP-Adressen zulassen aus.
- Klicken Sie auf "Hinzufügen"

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"/>	192.168.1.0/21	21	on	off
<input type="checkbox"/>	192.168.1.0/25	25	on	off

### IP-Zugriffskonfiguration

- Es wird ein Dialogfeld geöffnet, in dem Sie die IP-Adressen IPv4 oder IPv6 im CIDR-Format eingeben.
- Sobald die IP konfiguriert ist, legen Sie die Maske im CIDR-Format fest.
- Diese Optionen sind für IP-Zugriffsbeschränkungen verfügbar.
  - Admin-Services: GUI, CLI (SSH), SNMP, ERS, OpenAPI, UDN, API-Gateway, PxGrid (in Patch 2 deaktiviert), MnT-Analysen
  - Benutzerservices: Gast, BYOD, Status, Profilerstellung
  - Admin- und Benutzerdienste



IP-CIDR bearbeiten.

- Klicken Sie auf die Schaltfläche "Speichern"
- "EIN" bedeutet, dass Admin-Dienste aktiviert sind, "AUS" bedeutet, dass Benutzerdienste deaktiviert sind.

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

IP-Zugriffskonfiguration in 3.2

## Verhalten bei ISE 3.2 P4 und höher

Navigieren Sie zu Administration > Admin Access > Settings > Access. Folgende Optionen stehen

zur Verfügung:

- Sitzung
- Admin-GUI&CLI: ISE-GUI (TCP 443), ISE-CLI (SSH TCP 22) und SNMP.
- Admin-Services: ERS-API, offene API, pxGrid, DataConnect
- Benutzerservices: Gast, BYOD, Status.
- MNT Access (MNT-Zugriff): Mit dieser Option verbraucht ISE keine Syslog-Meldungen, die von externen Quellen gesendet wurden.

## Konfigurieren

- Wählen Sie Verbindungen nur mit aufgelisteten IP-Adressen zulassen aus.
- Klicken Sie auf "Hinzufügen"

The screenshot shows the configuration page for 'Admin GUI & CLI' under the 'Access Restriction' section. The 'Allow only listed IP addresses to connect' option is selected. Below this, there is a section titled '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 at the bottom right of the table area.

IP-Zugriffskonfiguration in 3.3

- Es wird ein Dialogfeld geöffnet, in dem Sie die IP-Adressen IPv4 oder IPv6 im CIDR-Format eingeben.
- Sobald die IP konfiguriert ist, legen Sie die Maske im CIDR-Format fest.
- Klicken Sie auf "Hinzufügen"

## Wiederherstellen der ISE-GUI/CLI

- Anmeldung mit Konsole
- Stoppen von ISE-Services mithilfe der Anwendungsstoppanzeige
- Starten der ISE-Services mit sicherer Anwendungsstartanwendung
- Entfernen Sie die IP-Zugriffsbeschränkung aus der GUI.

## Fehlerbehebung

Überprüfen Sie anhand einer Paketerfassung, ob die ISE nicht reagiert oder den Datenverkehr

verwirft.

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, CW] 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...	

## ISE-Firewall-Regeln überprüfen

- Für 3.1 und niedriger können Sie dies nur in der Show-Tech überprüfen.
  - Sie können eine Show-Tech in der lokalen Festplatte speichern, indem Sie "show tech-support file <Dateiname>" verwenden.
  - Anschließend können Sie die Datei mithilfe von "copy disk: /<filename> ftp://<ip address>/path" in ein Repository übertragen. Die URL des Repositories ändert sich je nach dem von Ihnen verwendeten Repository-Typ.
  - Sie können die Datei auf Ihren Computer herunterladen, sodass Sie sie lesen können und nach "Running iptables -nvL" suchen
  - Die anfänglichen Regeln in der Show-Tech sind unten nicht aufgeführt. Mit anderen Worten, hier finden Sie die letzten Regeln, die der Show-Tech durch IP Access Restriktionsfunktion beigefügt sind.

```
<#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
```

- Für Version 3.2 und höher können Sie den Befehl "show firewall" verwenden, um die Firewall-Regeln zu überprüfen.
- 3.2 und höher bieten mehr Kontrolle über die Services, die durch die IP-Zugriffsbeschränkung blockiert werden.

```
<#root>
```

```
gjuarez-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
```

## Debug-Protokolle überprüfen



Warnung: Nicht der gesamte Datenverkehr generiert Protokolle. Die Einschränkung des IP-Zugriffs kann den Datenverkehr auf Anwendungsebene und mithilfe der internen Linux Firewall blockieren. SNMP, CLI und SSH werden auf Firewall-Ebene blockiert, sodass keine Protokolle generiert werden.

- 
- Aktivieren Sie die Komponente "Infrastruktur" in DEBUG über die GUI.
  - Verwenden Sie `show logging application ise-psc.log tail`

Die nächsten Protokolle werden angezeigt, wenn die IP-Zugriffsbeschränkung Maßnahmen ergreift.

```
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
```

## Zugehörige Informationen

- [Technischer Support und Downloads von Cisco](#)
- [ISE 3.1 - Administratorhandbuch](#)
- [ISE 3.2 - Administratorhandbuch](#)
- [ISE 3.3 - Administratorhandbuch](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.