# ASA 8.2: Konfigurieren von Syslog mithilfe von ASDM

## Inhalt



## Einführung

Dieses Dokument enthält Informationen zum Konfigurieren von Syslog auf der Cisco Adaptive Security Appliance (ASA) 8.x mithilfe der ASDM-GUI (Adaptive Security Device Manager). Systemprotokollmeldungen sind Meldungen, die von der Cisco ASA generiert werden, um den Administrator über Änderungen an der Konfiguration, Änderungen in der Netzwerkeinrichtung oder Änderungen an der Geräteleistung zu informieren. Durch die Analyse der Systemprotokollmeldungen kann ein Administrator den Fehler problemlos beheben, indem er eine Ursachenanalyse durchführt.

Syslog-Meldungen werden hauptsächlich anhand ihres Schweregrads differenziert.

1. Schweregrad 0 - Notrufe - Ressource ist nicht verwendbar
2. Schweregrad 1 - Warnmeldungen - Sofortige Maßnahmen sind erforderlich
3. Schweregrad 2 - Kritische Nachrichten - Kritische Bedingungen
4. Schweregrad 3 - Fehlermeldungen - Fehlerbedingungen
5. Schweregrad 4 - Warnmeldungen - Warnbedingungen
6. Schweregrad 5 - Benachrichtigungsmeldungen - Normale, aber wesentliche Bedingungen
7. Schweregrad 6 - Informationsmeldungen - Nur Informationsmeldungen
8. Schweregrad 7 - Debugging-Meldungen - Nur Debugging-Meldungen**Hinweis:** Der höchste Schweregrad ist ein Notfall, der niedrigste Schweregrad ist das Debuggen.

Hier sehen Sie Beispiele für Syslog-Meldungen, die von der Cisco ASA generiert wurden:

- %ASA-6-106012: IP-Adressen von IP_Adresse zu IP_Adresse verweigern, IP-Optionen Hexadezimalziffer
- %ASA-3-211001: Speicherzuweisungsfehler
- %ASA-5-335003: Anwendung der NAC-Standardzugriffskontrollliste, ACL:ACL-Name - Hostadresse

Der in "%ASA-X-YYYYYY:" angegebene numerische Wert X gibt den Schweregrad der Nachricht an. Beispiel: "%ASA-6-106012" ist eine Informationsmeldung und "%ASA-5-335003" ist eine Fehlermeldung.

# Voraussetzungen

## Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ASA Version 8.2
- Cisco ASDM Version 6.2

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konventionen

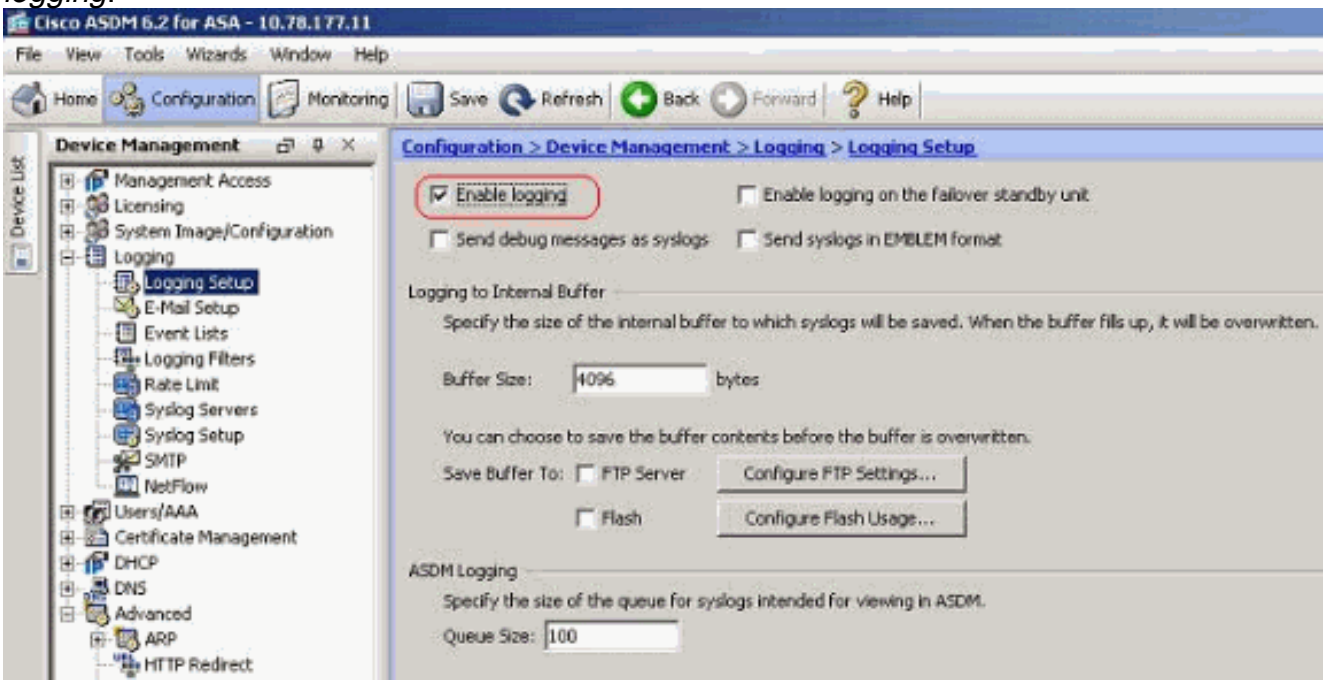
Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

# Grundlegende Syslog-Konfiguration mithilfe von ASDM

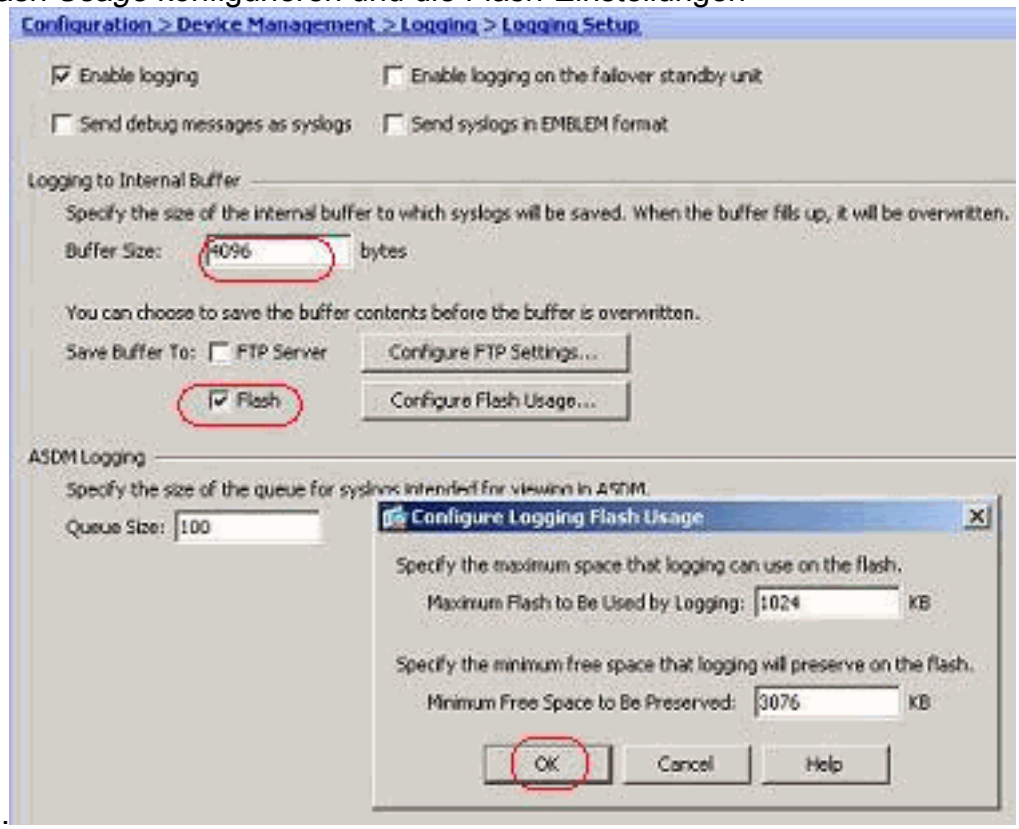
## Protokollierung aktivieren

Gehen Sie wie folgt vor:

1. Wählen Sie *Configuration > Device Management > Logging > Logging Setup* aus, und markieren Sie die Option *Enable logging*.

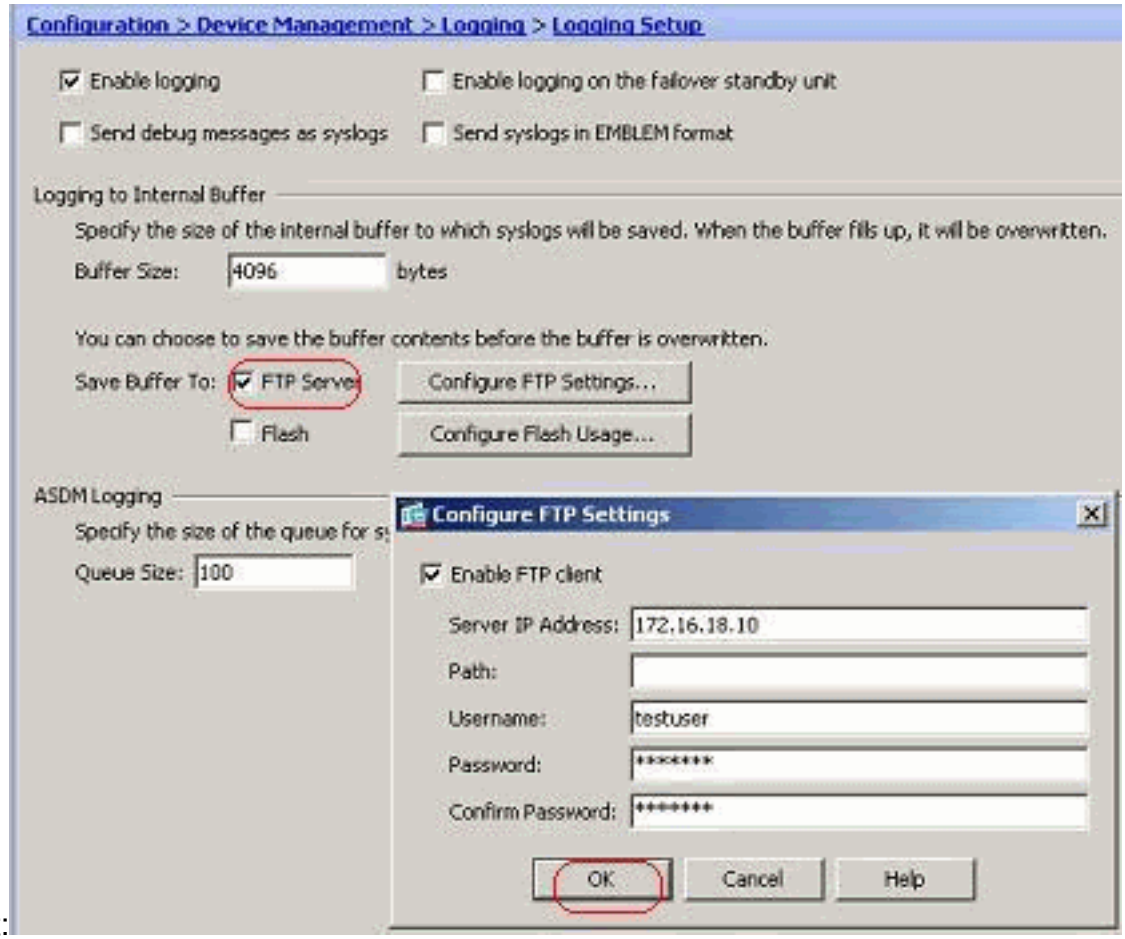



2. Sie können die Syslog-Meldungen in einem internen Puffer speichern, indem Sie die Puffergröße angeben. Sie können den Pufferinhalt auch in Flash-Speicher speichern, indem Sie auf *Flash Usage* konfigurieren und die Flash-Einstellungen definieren.




3. Pufferte Protokollmeldungen können an einen FTP-Server gesendet werden, bevor sie überschrieben werden. Klicken Sie auf *FTP-Einstellungen konfigurieren*, und geben Sie die FTP-Serverdetails an, wie hier

gezeigt:

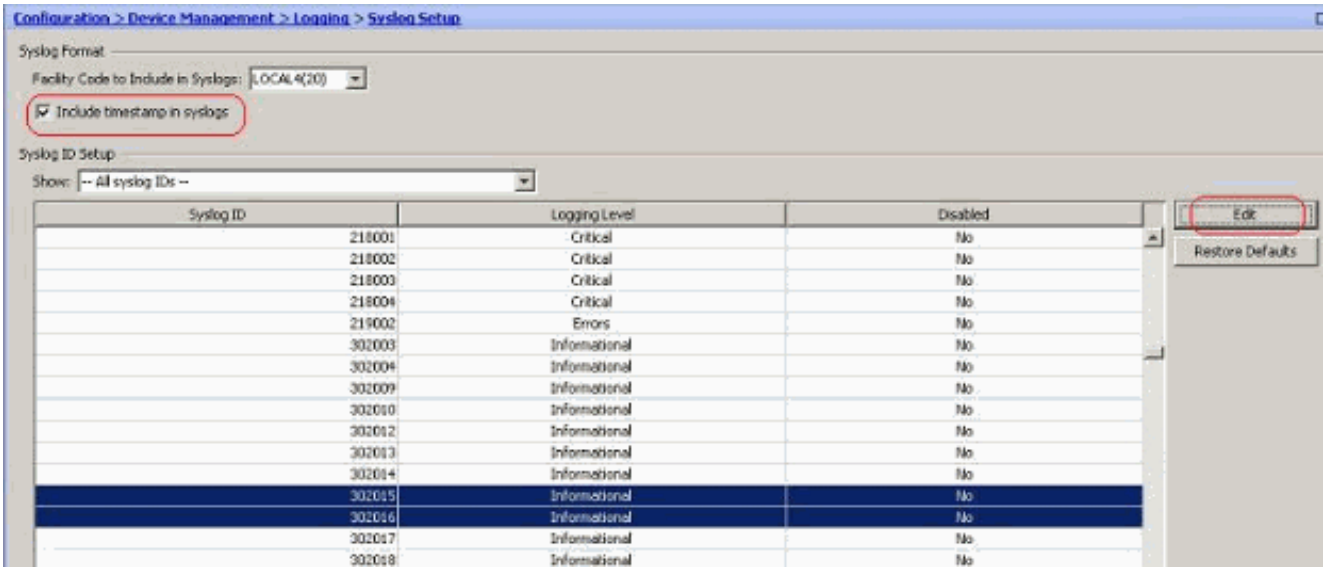



## Protokollierung deaktivieren

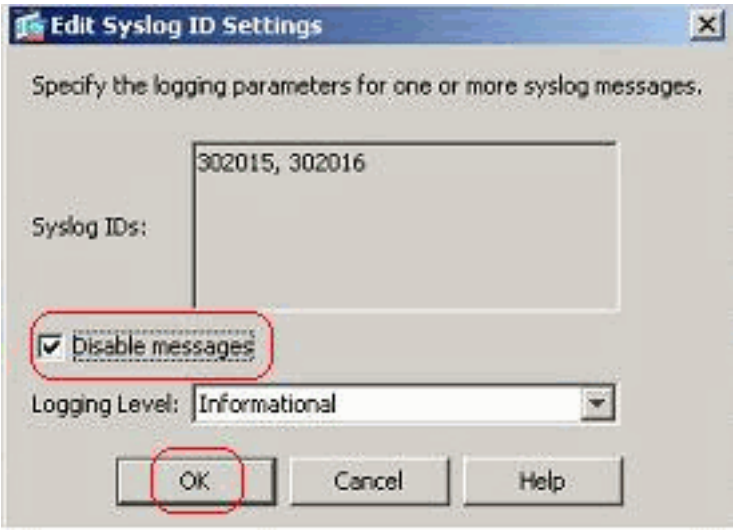
Sie können bestimmte Syslog-IDs je nach Ihren Anforderungen deaktivieren.

**Hinweis:** Durch Aktivieren des Kontrollkästchens für die Option *Zeitstempel in Syslogs einschließen* können Sie den Syslogs das Datum und die Uhrzeit hinzufügen, zu dem sie als Feld generiert wurden.

1. Wählen Sie die zu deaktivierenden Syslogs aus, und klicken Sie auf *Bearbeiten*.

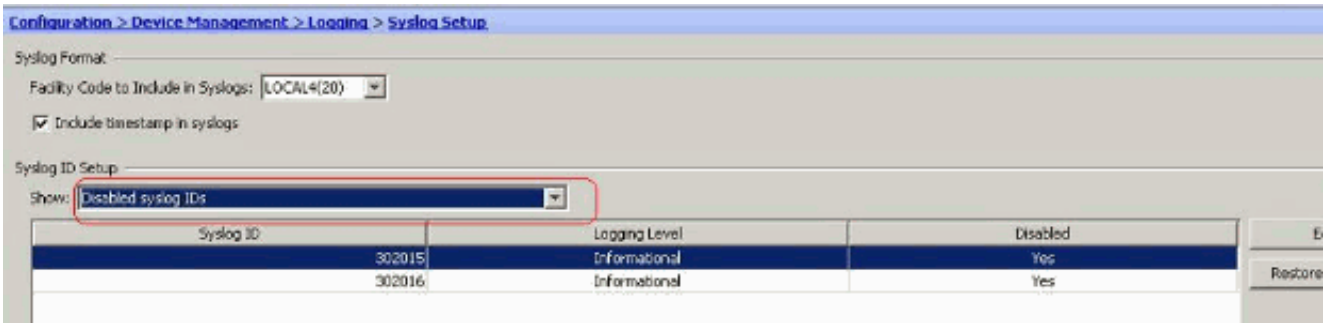



2. Aktivieren Sie im Fenster *Edit Syslog ID Settings (Syslog-ID-Einstellungen bearbeiten*) die Option *Disable messages (Nachrichten deaktivieren)*, und klicken Sie auf




*OK*.

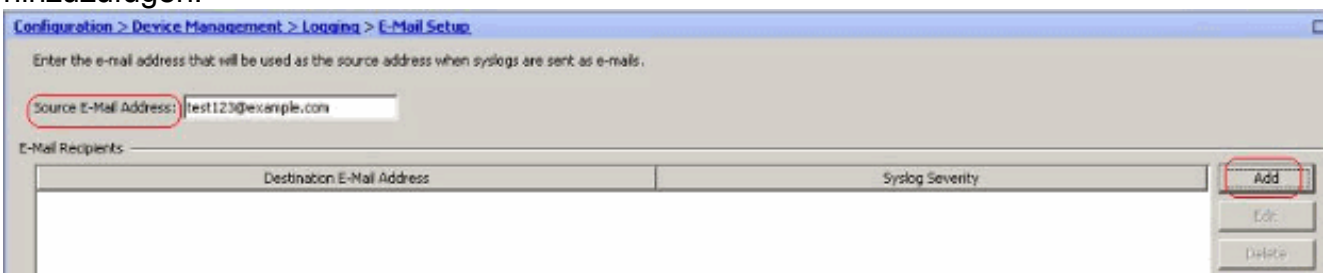
3. Die deaktivierten Syslogs können auf einer separaten Registerkarte angezeigt werden, indem Sie im Dropdown-Menü *Syslog-IDs* im *Syslog ID Setup*-Dropdown-Menü die Option *Disabled Syslog IDs* auswählen.




## Anmelden bei einer E-Mail

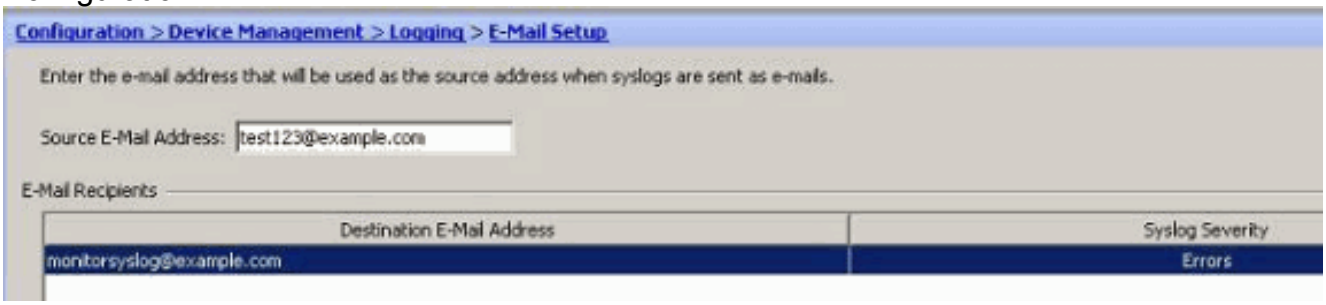
Gehen Sie wie folgt vor, um die Syslogs mithilfe von ASDM an eine E-Mail zu senden:

1. Wählen Sie *Konfiguration > Gerätemanagement > Protokollierung > E-Mail-Einrichtung aus*. Das Feld *Quell-E-Mail-Adresse* ist hilfreich, um eine E-Mail-ID als Quelle für die Syslogs zuzuweisen. Geben Sie die E-Mail-Quelladresse an. Klicken Sie jetzt auf *Hinzufügen*, um die E-Mail-Empfänger hinzuzufügen.

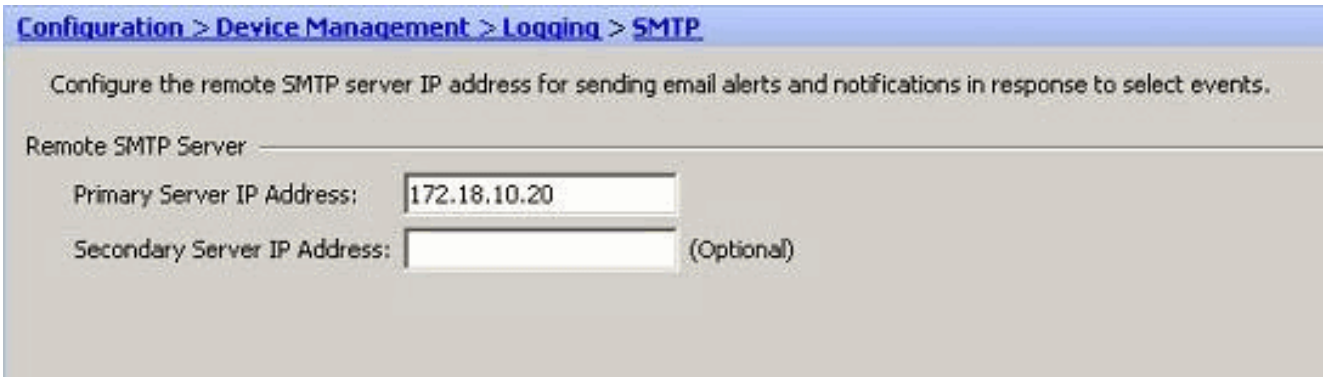



2. Geben Sie die *E-Mail-Zieladresse* an, und wählen Sie den *Schweregrad aus*. Je nach Schweregrad können Sie verschiedene E-Mail-Empfänger definieren. Klicken Sie auf *OK*, um zum Bereich *E-Mail-Setup*


zurückzukehren. Daraus ergibt sich folgende Konfiguration:



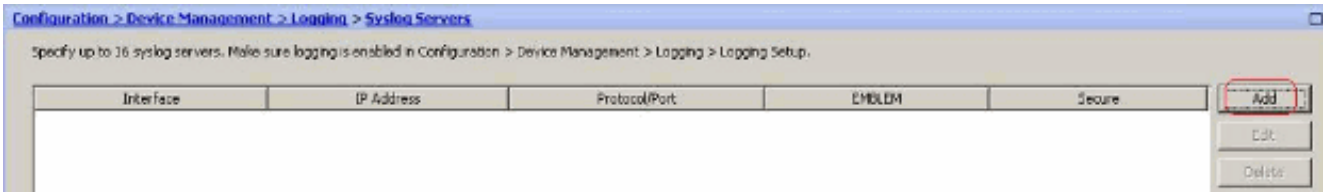

3. Wählen Sie *Configuration > Device Setup > Logging > SMTP* aus, und geben Sie den SMTP-Server an.




## Anmeldung bei einem Syslog-Server

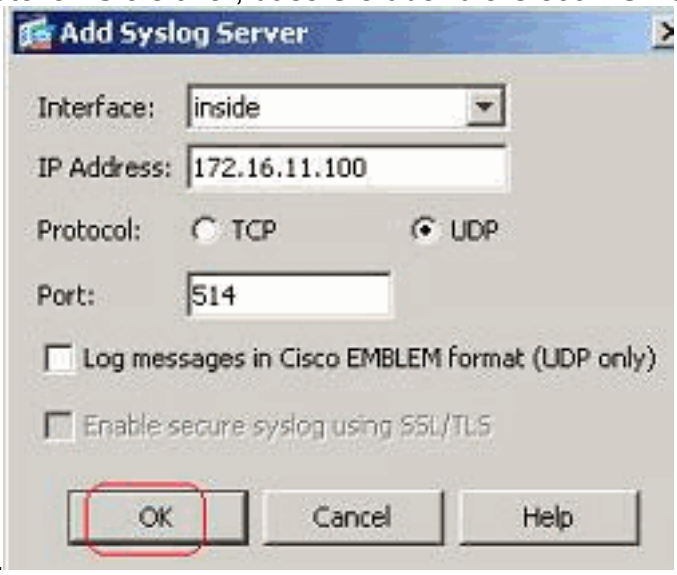
Sie können alle Syslog-Meldungen an einen dedizierten Syslog-Server senden. Führen Sie diese Schritte mit ASDM durch:

1. Wählen Sie *Konfiguration > Gerätemanagement > Protokollierung > Syslog-Server* aus, und klicken Sie auf *Hinzufügen*, um einen Syslog-Server hinzuzufügen.

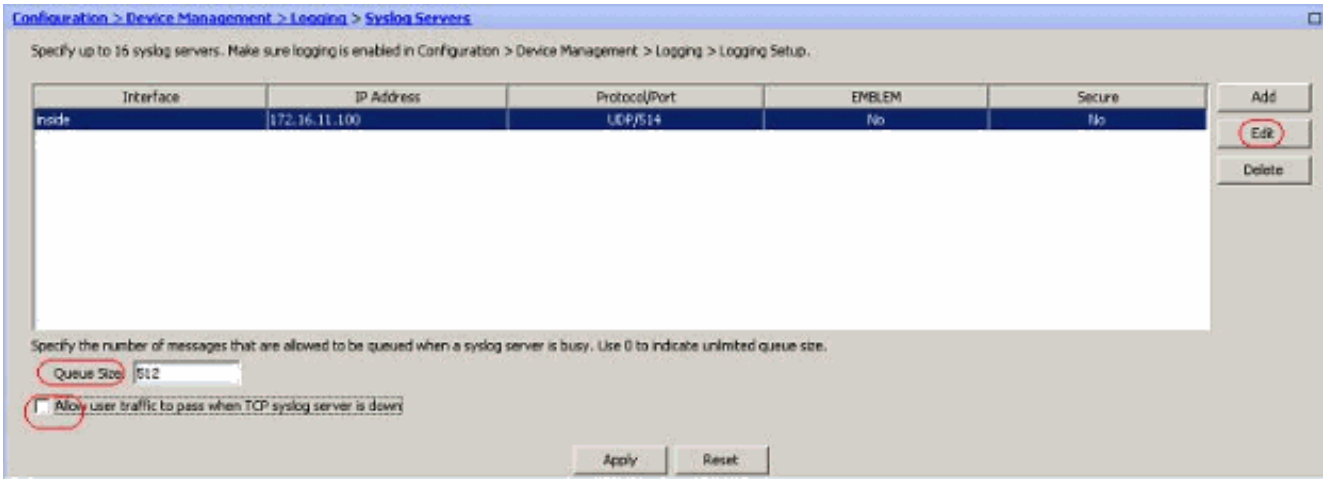



Das Fenster *Syslog-Server hinzufügen* wird angezeigt.

2. Geben Sie die Schnittstelle an, der der Server zugeordnet ist, sowie die IP-Adresse. Geben Sie die *Protokoll-* und *Port*-Details je nach Netzwerkeinrichtung an. Klicken Sie anschließend auf *OK*.**Hinweis:** Stellen Sie sicher, dass Sie über die Cisco ASA auf den Syslog-Server zugreifen können.




3. Der konfigurierte Syslog-Server wird wie hier gezeigt angezeigt. Änderungen können durchgeführt werden, wenn Sie diesen Server auswählen und dann auf *Bearbeiten* klicken.




**Hinweis:** Aktivieren Sie die Option *Benutzerdatenverkehr zum Weiterleiten zulassen, wenn der TCP-Syslog-Server ausgefallen ist*. Andernfalls werden die neuen Benutzersitzungen über die ASA abgelehnt. Dies gilt nur, wenn das Transportprotokoll zwischen ASA und dem Syslog-Server TCP ist. Standardmäßig werden neue Netzwerkzugriffssitzungen von der Cisco ASA verweigert, wenn ein Syslog-Server aus irgendeinem Grund ausfällt.Informationen zum Definieren des Typs von Syslog-Meldungen, die an den Syslog-Server gesendet werden sollen, finden Sie im Abschnitt Protokollierungsfilter.

## Erweiterte Syslog-Konfiguration mit ASDM

### Arbeiten mit Ereignislisten

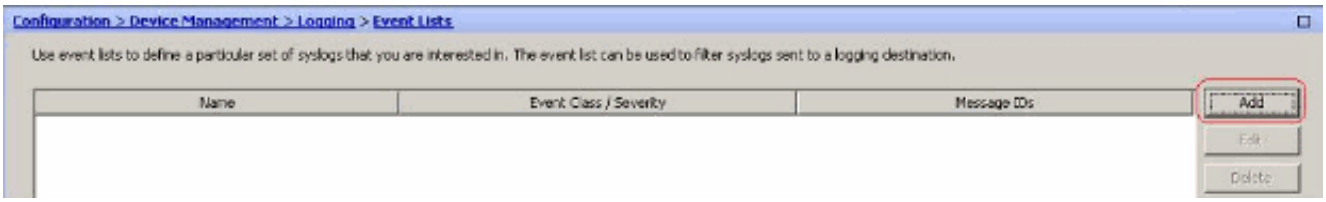
Mit Ereignislisten können wir benutzerdefinierte Listen erstellen, die die Gruppe von Syslog-Meldungen enthalten, die an ein Ziel gesendet werden sollen. Ereignislisten können auf drei verschiedene Arten erstellt werden:

- Nachrichten-ID oder Bereich der Nachrichten-IDs
- Schweregrad der Nachricht
- Message-Klasse

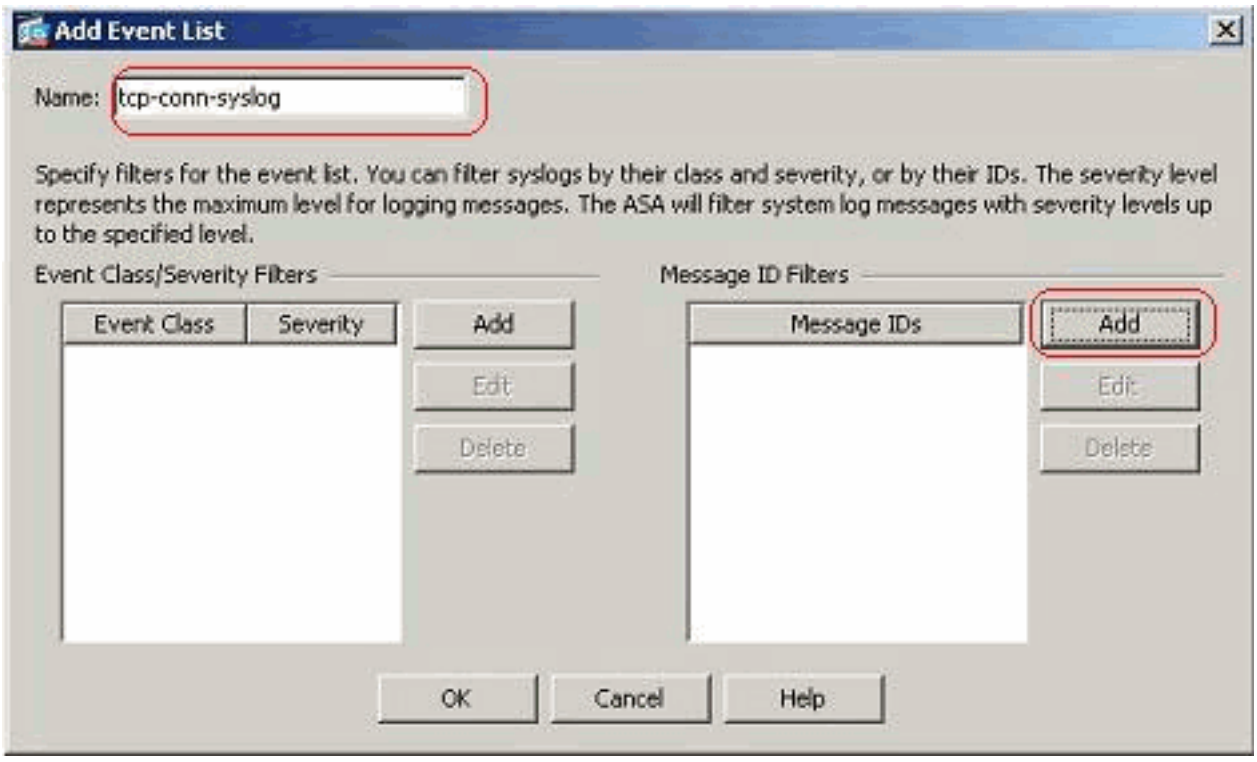
**Nachrichten-ID oder Bereich der Nachrichten-IDs**

Gehen Sie wie folgt vor:

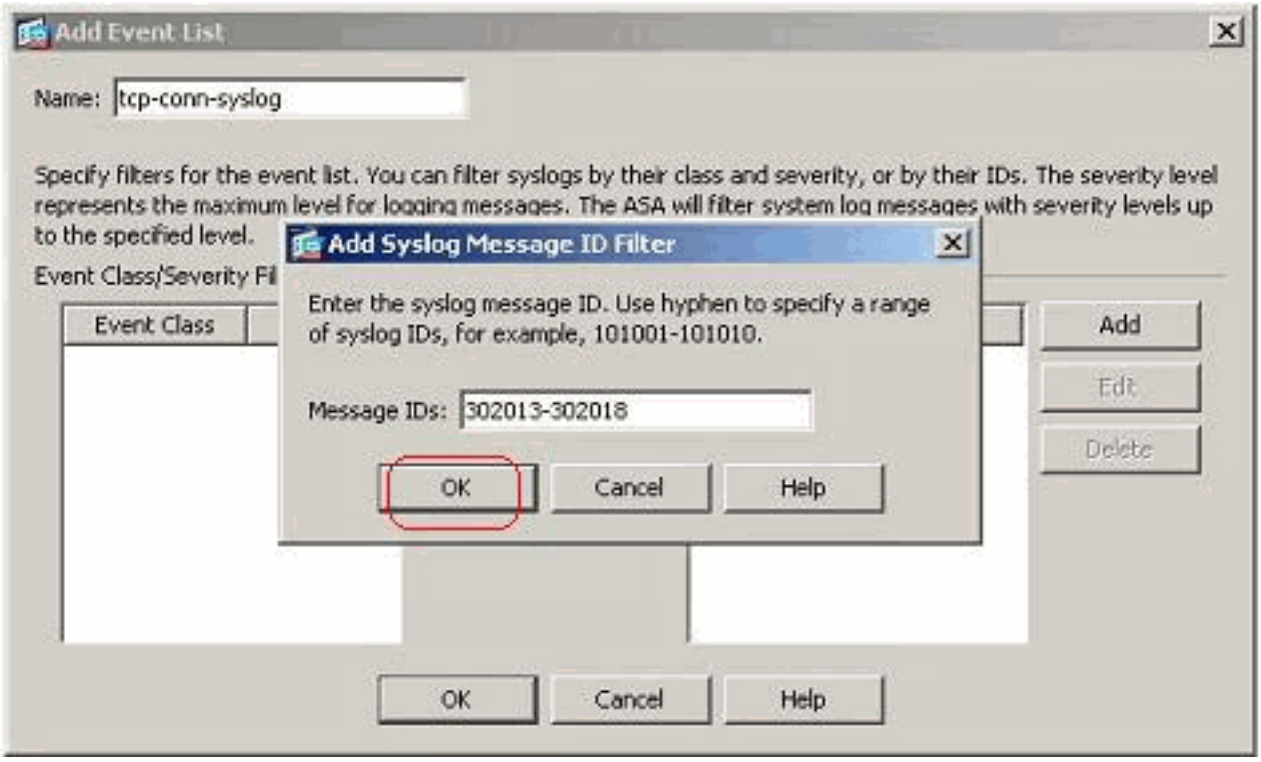
1. Wählen Sie *Configuration > Device Management > Logging > Event Lists (Konfiguration > Gerätemanagement > Protokollierung > Ereignislisten) aus,* und klicken Sie auf *Add*, um eine neue Ereignisliste zu
   erstellen.




2. Geben Sie im Feld *Name* einen Namen an. Klicken Sie im Bereich "*Nachrichten-ID-Filter" auf Hinzufügen*, um eine neue Ereignisliste zu
   erstellen.

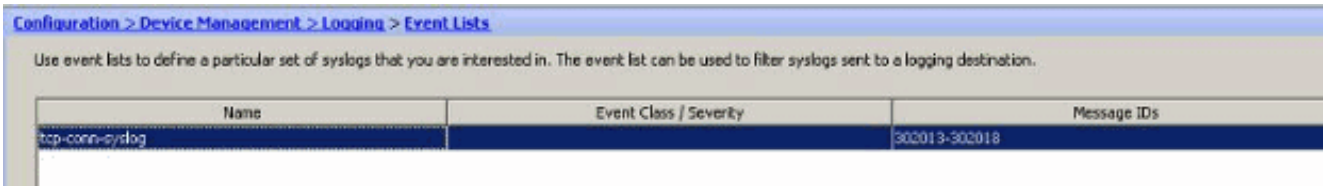



3. Geben Sie den Bereich der Syslog-Nachrichten-IDs an. Hier sind beispielsweise die TCP-Syslog-Meldungen enthalten. Klicken Sie zum Abschließen auf



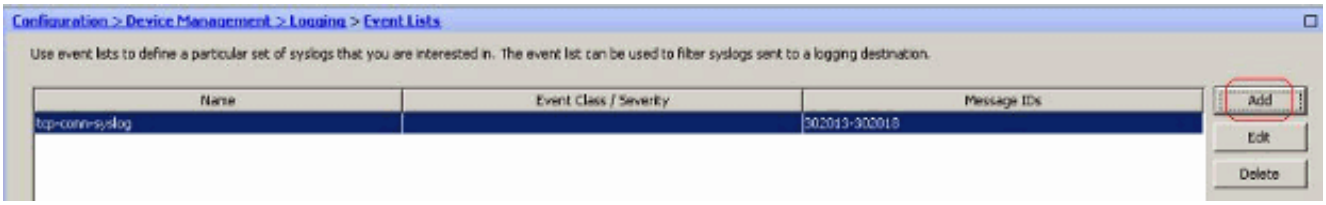

*OK*.

4. Klicken Sie erneut auf *OK*, um zum Fenster *Ereignislisten* zurückzukehren.



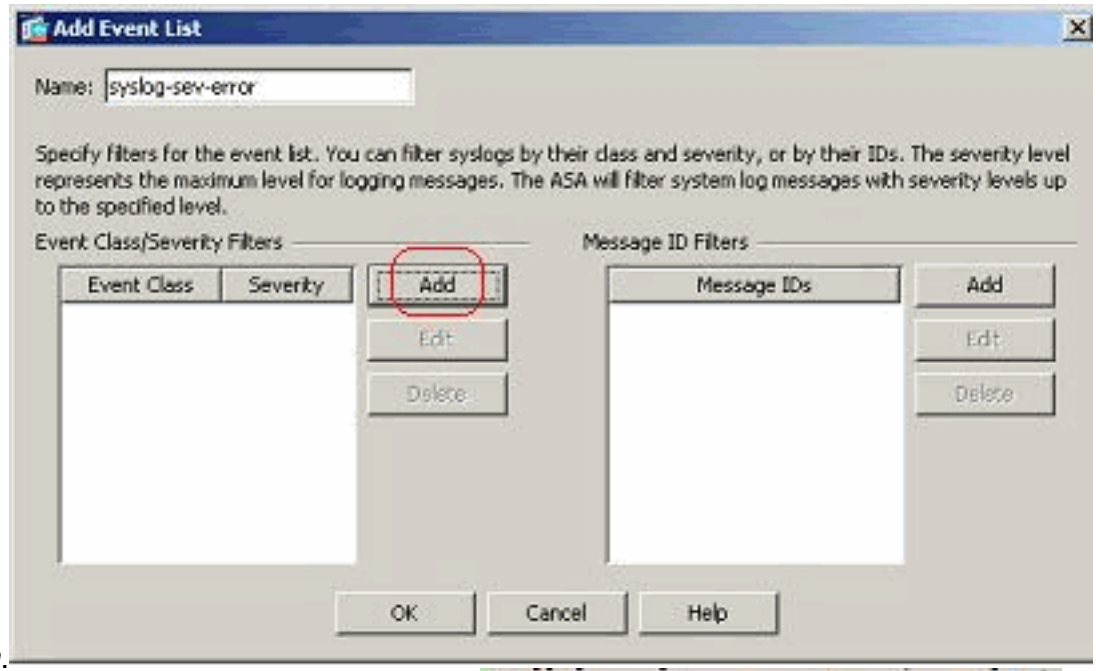

## Schweregrad der Nachricht

1. Ereignislisten können auch anhand des Schweregrads der Nachricht definiert werden. Klicken Sie auf *Hinzufügen*, um eine separate Ereignisliste zu erstellen.

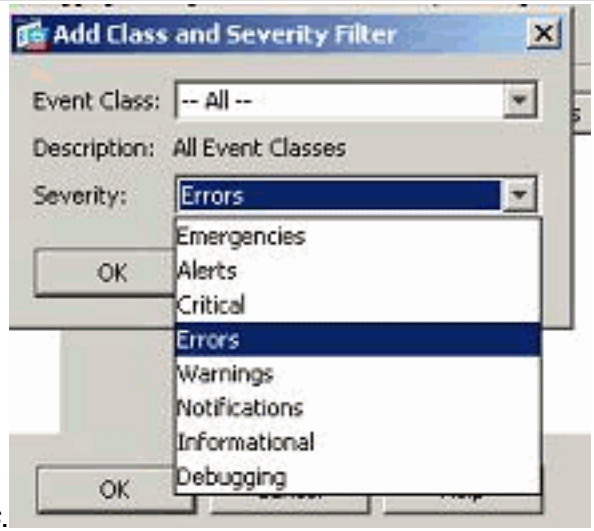



2. Geben Sie den Namen an, und klicken Sie auf

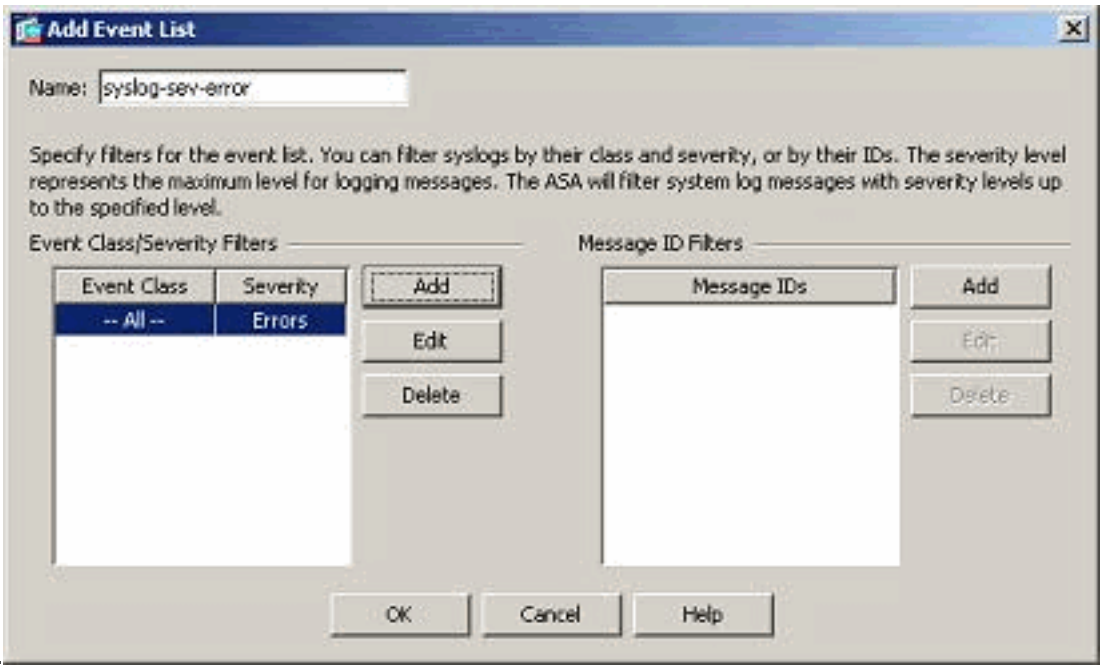
*Hinzufügen*.




3. Wählen Sie den Schweregrad als *Fehler aus*.




4. Klicken Sie auf *OK*.




**Message-Klasse**

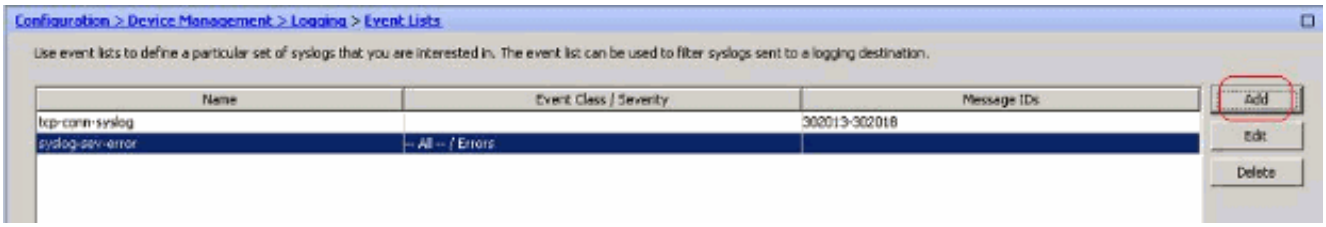
Ereignislisten werden auch basierend auf der Message Class konfiguriert. Eine Nachrichtenklasse

ist eine Gruppe von Syslog-Meldungen, die sich auf eine Sicherheitsanwendungsfunktion beziehen, mit der Sie eine ganze Nachrichtenklasse angeben können, anstatt für jede Nachricht einzeln eine Klasse anzugeben. Verwenden Sie z. B. die auth-Klasse, um alle Syslog-Meldungen auszuwählen, die mit der Benutzerauthentifizierung zusammenhängen. Einige verfügbare Nachrichtenklassen sind hier aufgeführt:

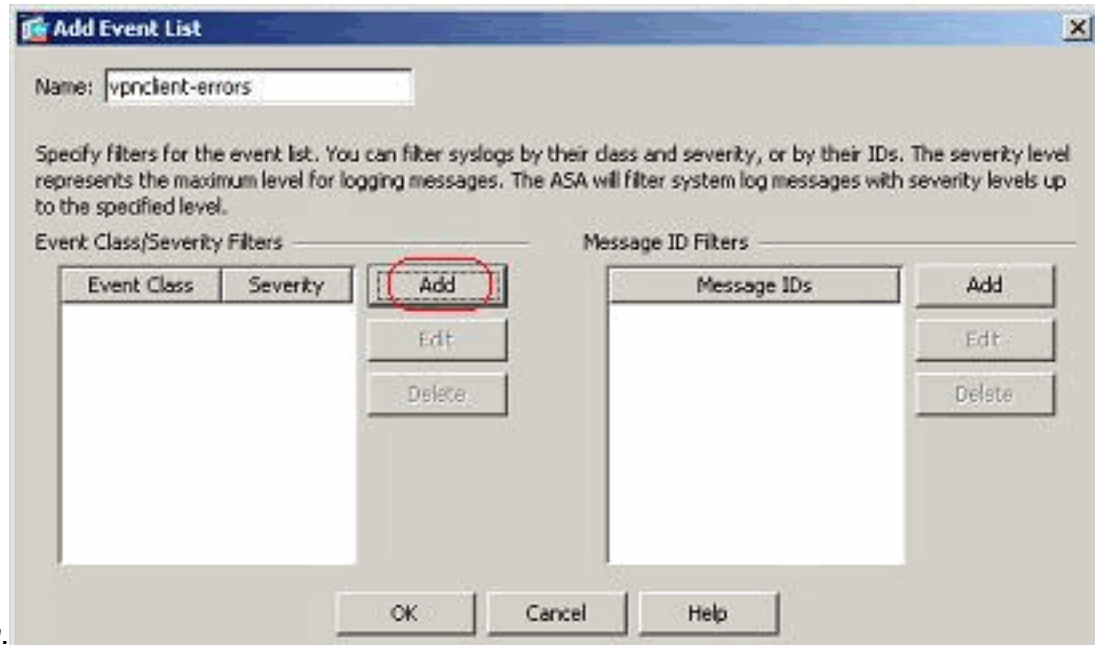
- Alle - Alle Ereignisklassen
- auth - Benutzerauthentifizierung
- Bridge - Transparente Firewall
- ca - PKI-Zertifizierungsstelle
- config - Befehlsschnittstelle
- ha - Failover
- ips - Intrusion Protection Service
- IP - IP-Stack
- np - Netzwerkprozessor
- ospf - OSPF-Routing
- RIP - RIP-Routing
- Sitzung - Benutzersitzung

Führen Sie diese Schritte aus, um eine Ereignisklasse zu erstellen, die auf der *vpnclient-errors*-Nachrichtenklasse basiert. Die Nachrichtenklasse *vpnc* kann alle Syslog-Meldungen kategorisieren, die sich auf den vpnclient beziehen. Der Schweregrad für diese Nachrichtenklasse wird als "Fehler" ausgewählt.

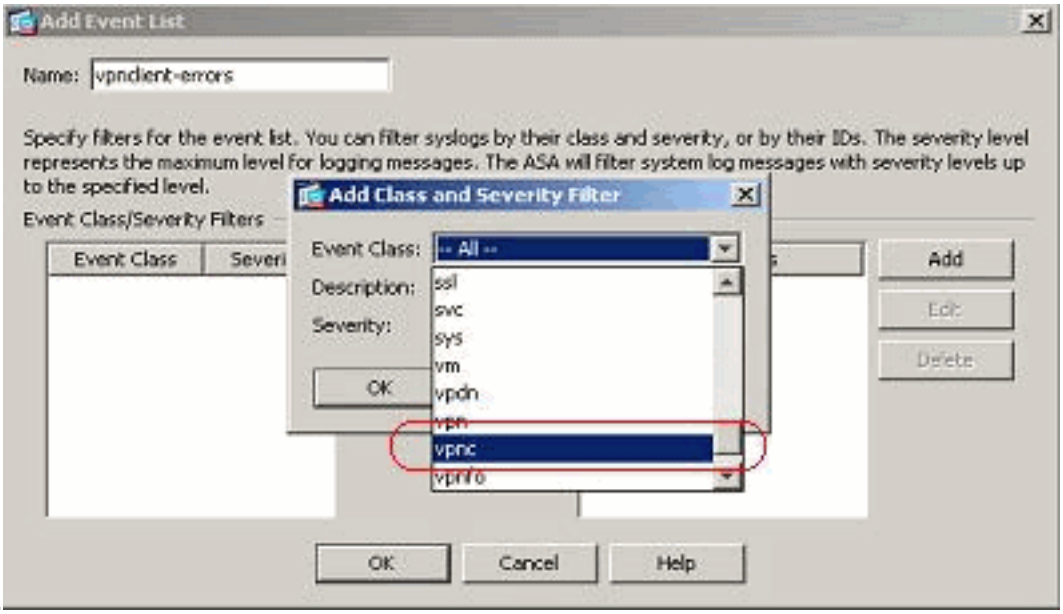
1. Klicken Sie auf Hinzufügen, um eine neue Ereignisliste zu erstellen.




2. Geben Sie den Namen an, der für die von Ihnen erstellte Nachrichtenklasse relevant sein soll, und klicken Sie auf *Hinzufügen*.

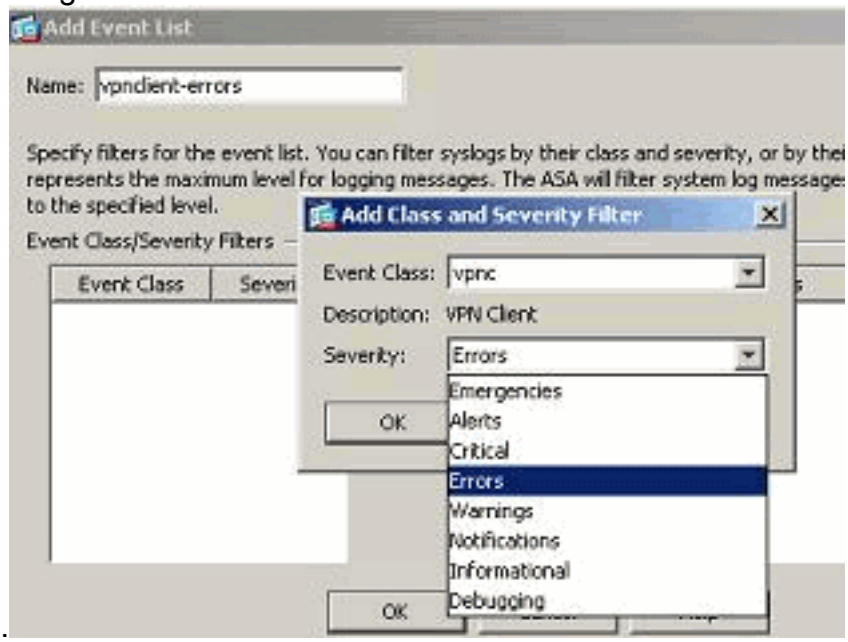



3. Wählen Sie *vpnc* aus der Dropdown-Liste



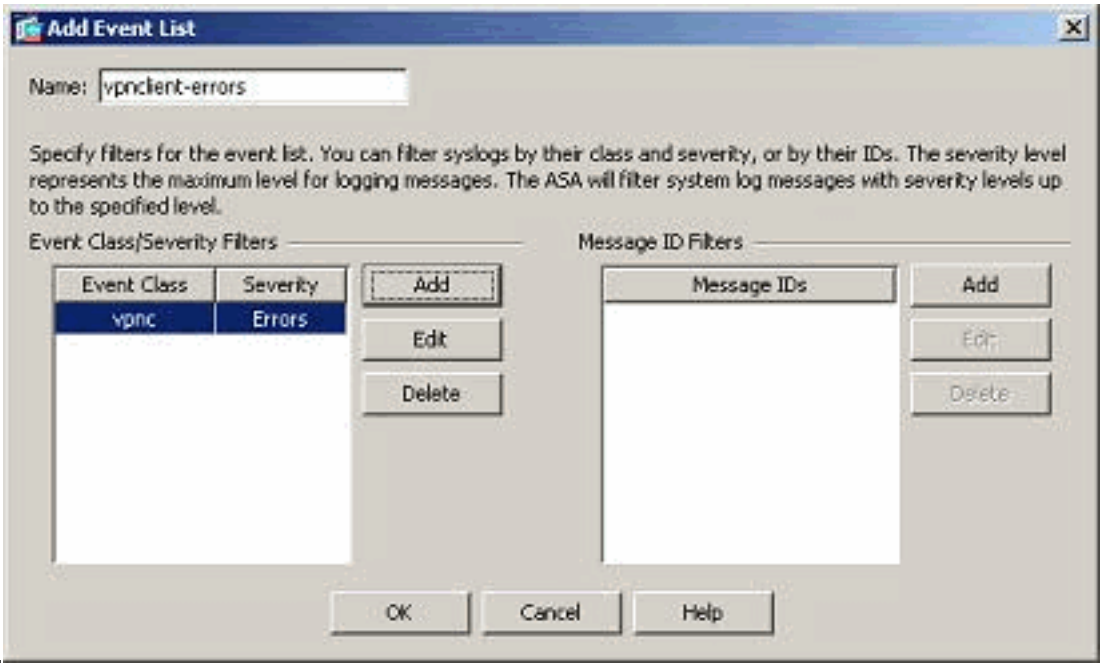
aus.

4. Wählen Sie den Schweregrad als *Fehler aus*. Dieser Schweregrad gilt nur für Nachrichten, die für diese Nachrichtenklasse protokolliert werden. Klicken Sie auf *OK*, um zum Fenster Ereignisliste hinzufügen



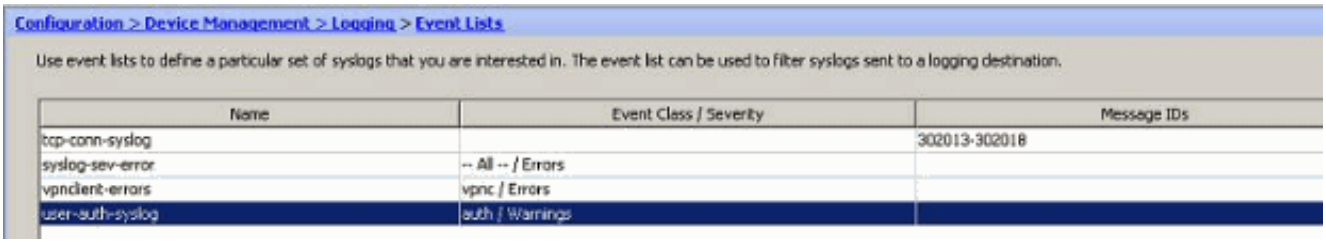
zurückzukehren.

5. Die Ereignisklasse/-schweregrad wird hier angezeigt. Klicken Sie auf *OK*, um die Konfiguration der Ereignisliste "vpnclient-errors"




abzuschließen.

Im nächsten Screenshot wird auch gezeigt, dass eine neue Ereignisliste, "user-auth-syslog", mit einer Nachrichtenklasse als "auth" und dem Schweregrad für die Syslogs dieser spezifischen Nachrichtenklasse als "Warnungen" erstellt wird. Durch diese Konfiguration gibt die Ereignisliste alle Syslog-Meldungen an, die sich auf die Authentifizierungsnachrichtenklasse beziehen, mit Schweregraden **bis zur** Stufe "Warnungen".**Hinweis:** Hier ist der Begriff "Bis" von Bedeutung. Beachten Sie bei der Angabe des Schweregrads, dass alle Syslog-Meldungen bis zu diesem Level protokolliert werden.**Hinweis:** Eine Ereignisliste kann mehrere Ereignisklassen enthalten. Die Ereignisliste "vpnclient-errors" wird durch Klicken auf **Bearbeiten** geändert und eine neue Ereignisklasse "ssl/error"
definiert.




## Arbeiten mit Protokollierungsfiltern

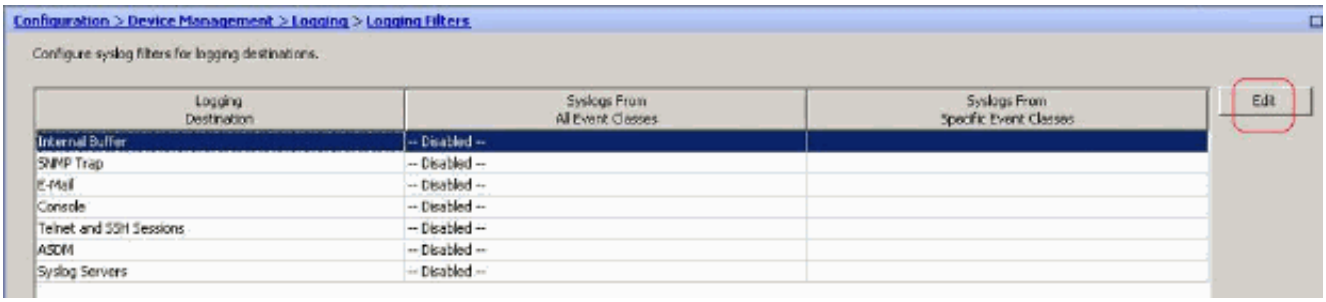
Protokollierungsfilter werden verwendet, um die Syslog-Meldungen an ein bestimmtes Ziel zu senden. Diese Syslog-Meldungen können auf dem Schweregrad oder den Listen "Selbst" basieren.

Diese Filter sind für die Bestimmungsorte geeignet:

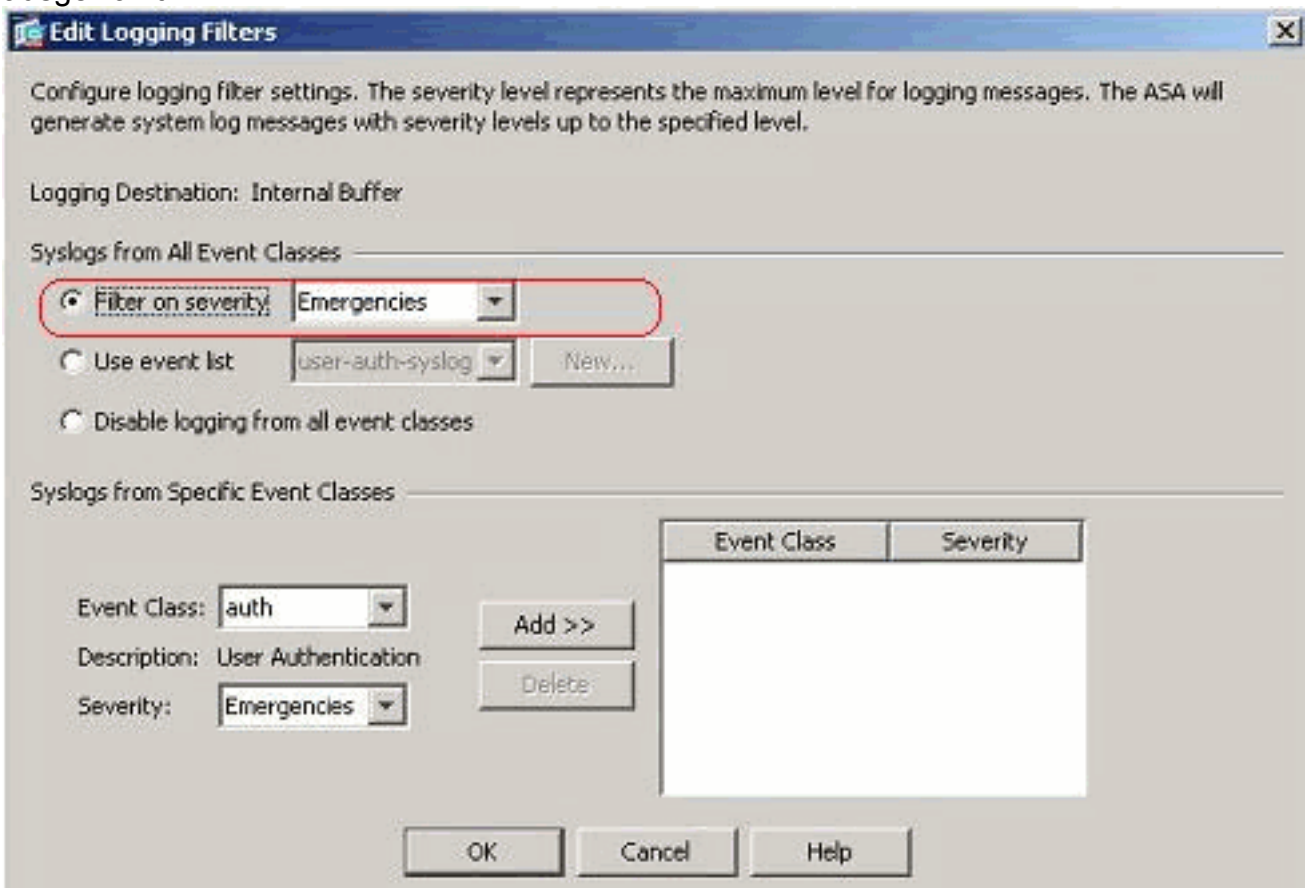
- Interner Puffer
- SNMP-Trap
- E-Mail
- Konsole
- Telnet-Sitzungen
- ASDM
- Syslog-Server

Gehen Sie wie folgt vor:

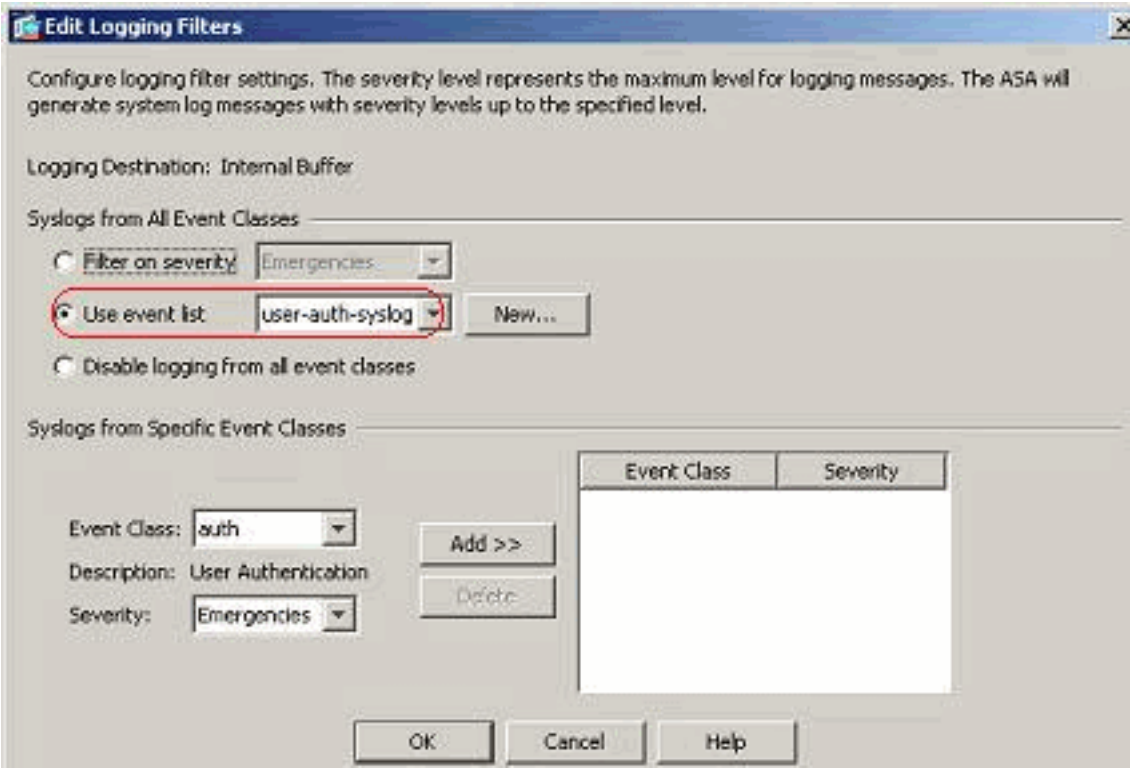
1. Wählen Sie **Konfiguration > Gerätemanagement > Protokollierung > Protokollierungsfilter** aus, und wählen Sie das Protokollierungsziel aus. Klicken Sie anschließend auf **Bearbeiten**, um die Einstellungen zu
   ändern.




2. Sie können die Syslog-Meldungen je nach Schweregrad senden. Hier wurde **Notfälle** als Beispiel
   ausgewählt.

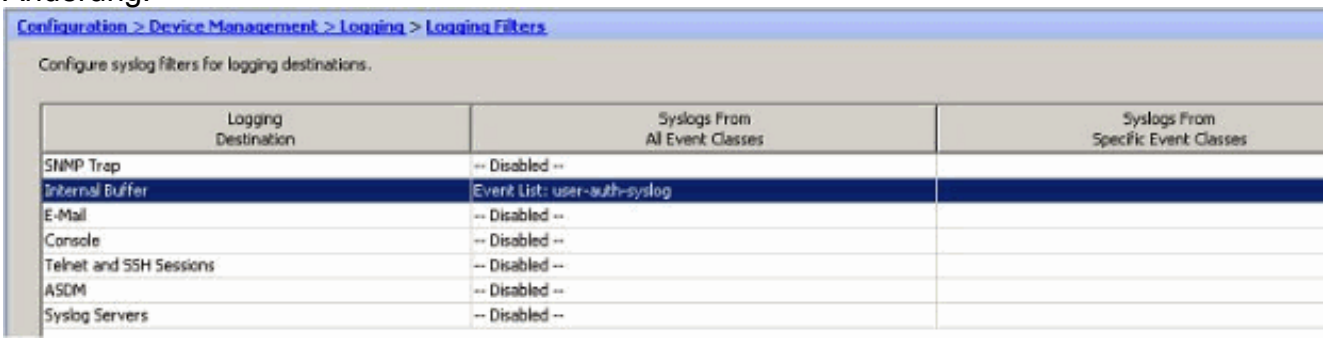



3. Eine Ereignisliste kann auch ausgewählt werden, um festzulegen, welche Arten von Nachrichten an ein bestimmtes Ziel gesendet werden sollen. Klicken Sie auf



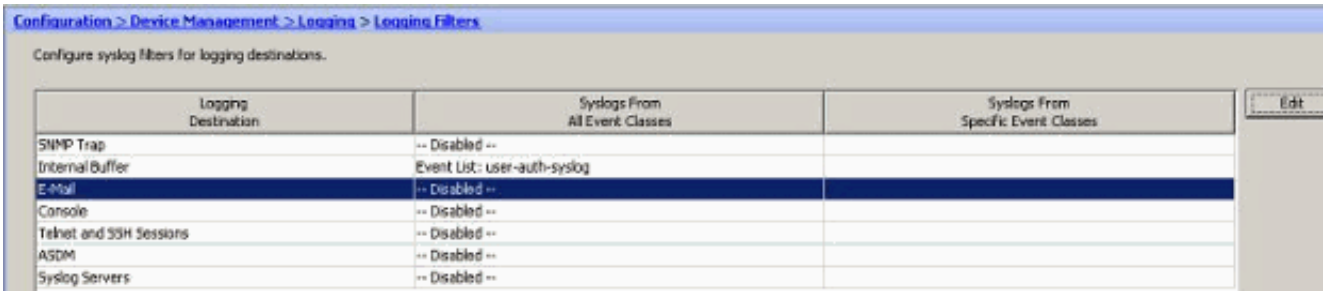

OK.

4. Überprüfen Sie die Änderung.

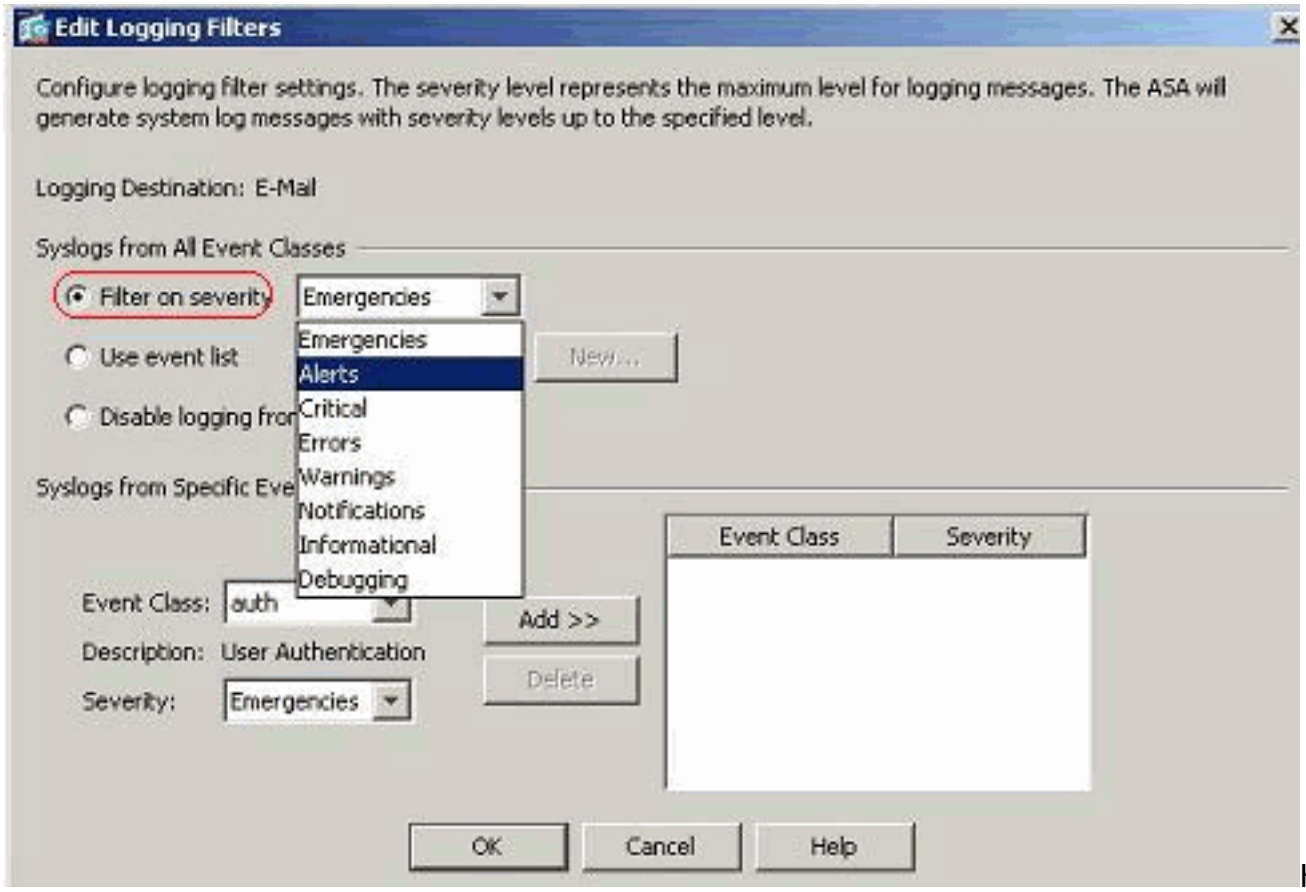



Dies sind die Schritte zum Senden einer Gruppe von Nachrichten (abhängig von ihrem Schweregrad) an den E-Mail-Server.

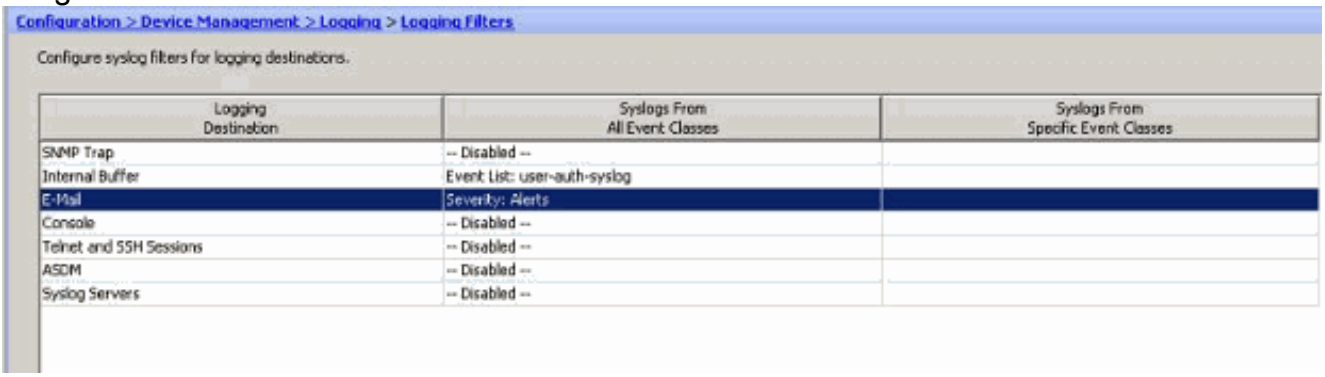
1. Wählen Sie **E-Mail** im Feld Logging Destination (Logging-Ziel) aus. Klicken Sie anschließend auf **Bearbeiten**.



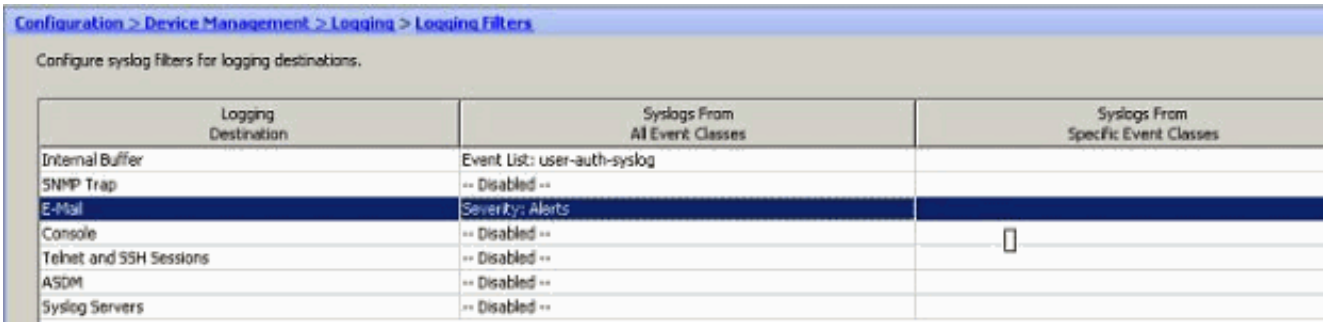

2. Wählen Sie die Option **Nach Schweregrad filtern**, und wählen Sie den gewünschten Schweregrad aus.




Hier wurde **Alerts** als Schweregrad ausgewählt.




Sie sehen, dass alle Alert-Syslog-Meldungen an die konfigurierte E-Mail gesendet werden sollen.

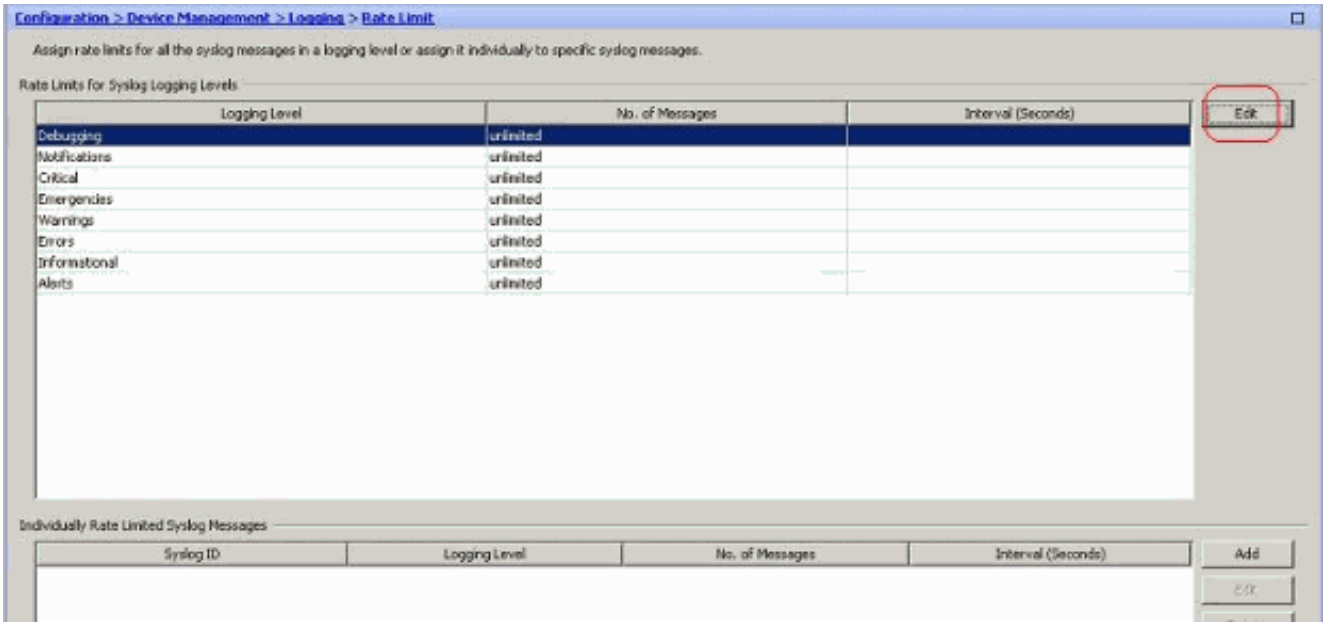



## Übertragungsratenlimit

Dieser Parameter gibt die Anzahl der Syslog-Meldungen an, die eine Cisco ASA innerhalb eines festgelegten Zeitraums an ein Ziel sendet. Sie wird in der Regel für den Schweregrad definiert.

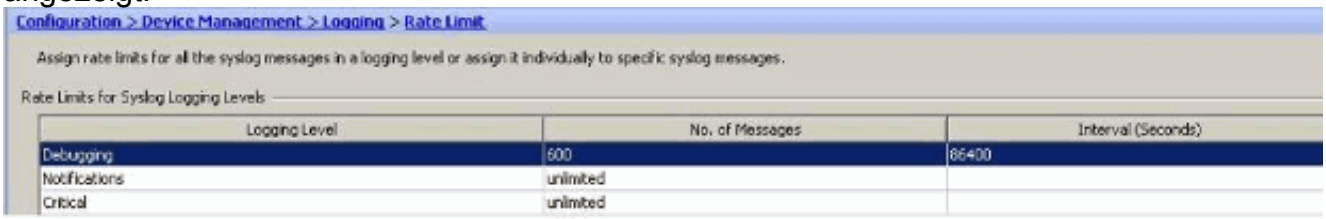
1. Wählen Sie **Configuration > Device Management > Logging > Rate Limit (Konfiguration >**

**Gerätemanagement > Protokollierung > Übertragungsratenlimit) aus,** und wählen Sie den gewünschten Schweregrad aus. Klicken Sie anschließend auf **Bearbeiten**.




2. Geben Sie die Anzahl der Nachrichten an, die zusammen mit dem Zeitintervall gesendet werden sollen. Klicken Sie auf **OK**.

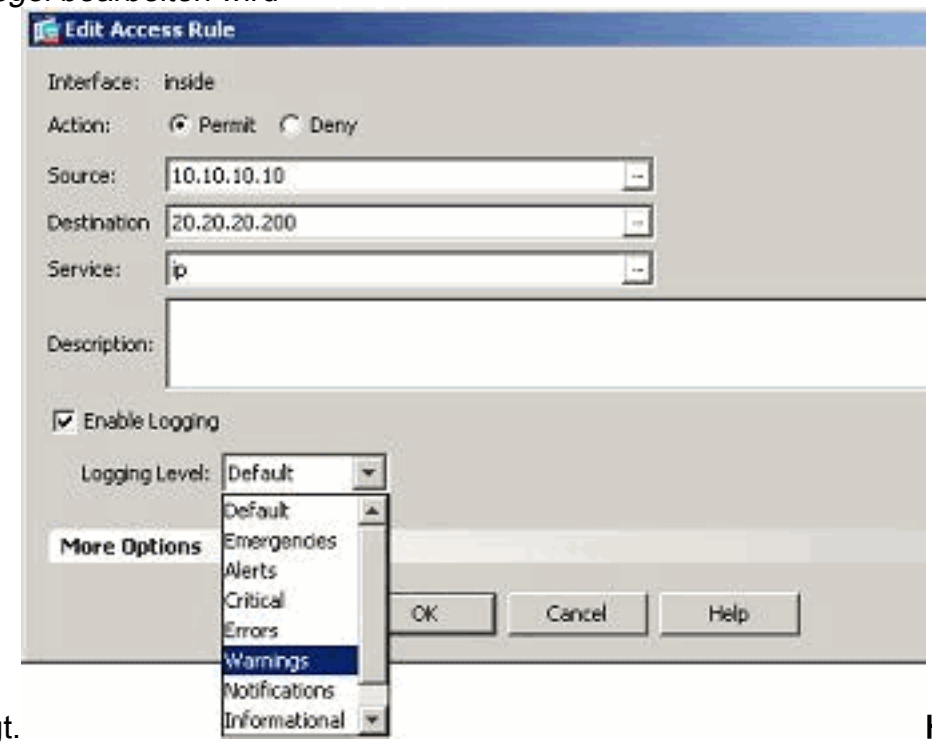

**Hinweis:** Diese Zahlen werden als Beispiel angegeben. Diese unterscheiden sich je nach Netzwerkumgebung.Geänderte Werte werden hier angezeigt:

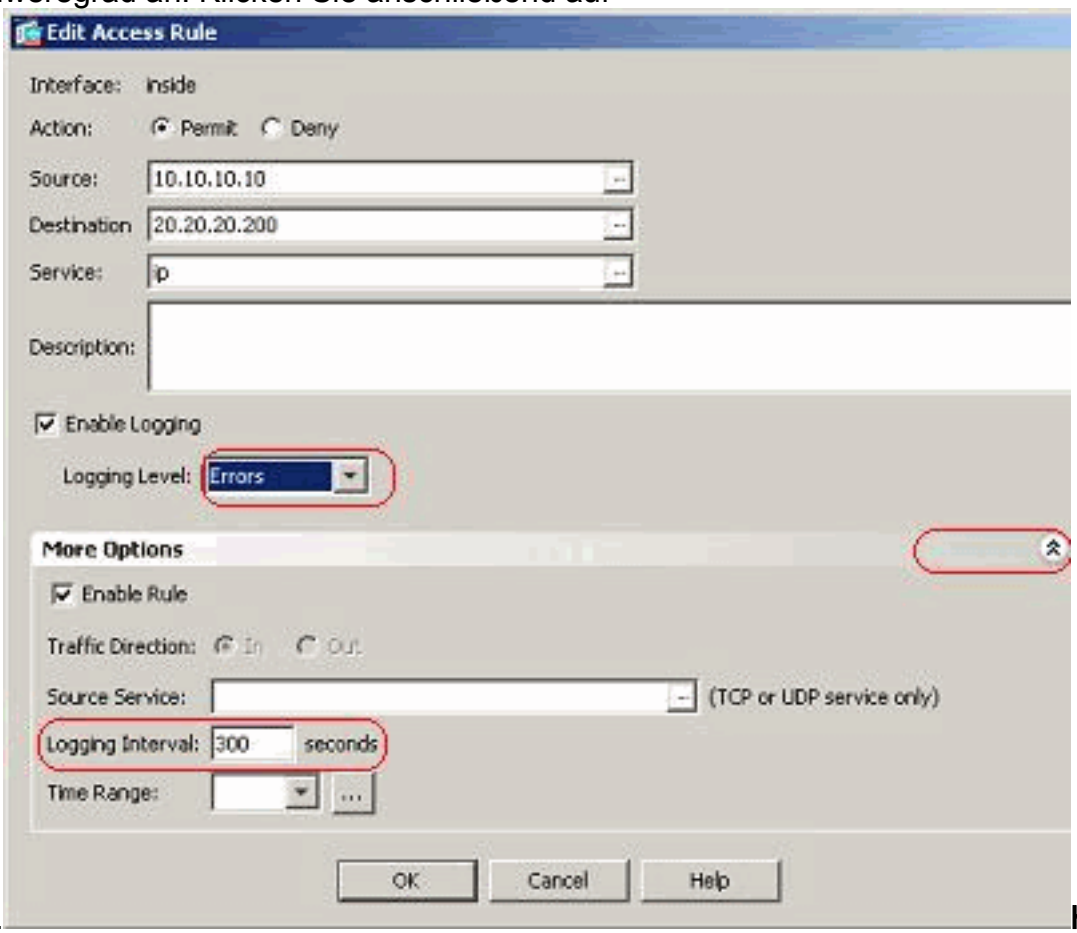



## Protokollieren der Hits einer Zugriffsregel

Sie können die Zugriffsregelhits mit dem ASDM protokollieren. Das Standardprotokollierungsverhalten besteht darin, eine Syslog-Meldung für alle abgelehnten Pakete zu senden. Für die zulässigen Pakete wird keine Syslog-Meldung angezeigt, und diese werden nicht protokolliert. Sie können jedoch eine benutzerdefinierte Protokollierungsschweregrad-Ebene für die Zugriffsregel definieren, um die Anzahl der Pakete zu verfolgen, die diese Zugriffsregel erreicht.

Gehen Sie wie folgt vor:

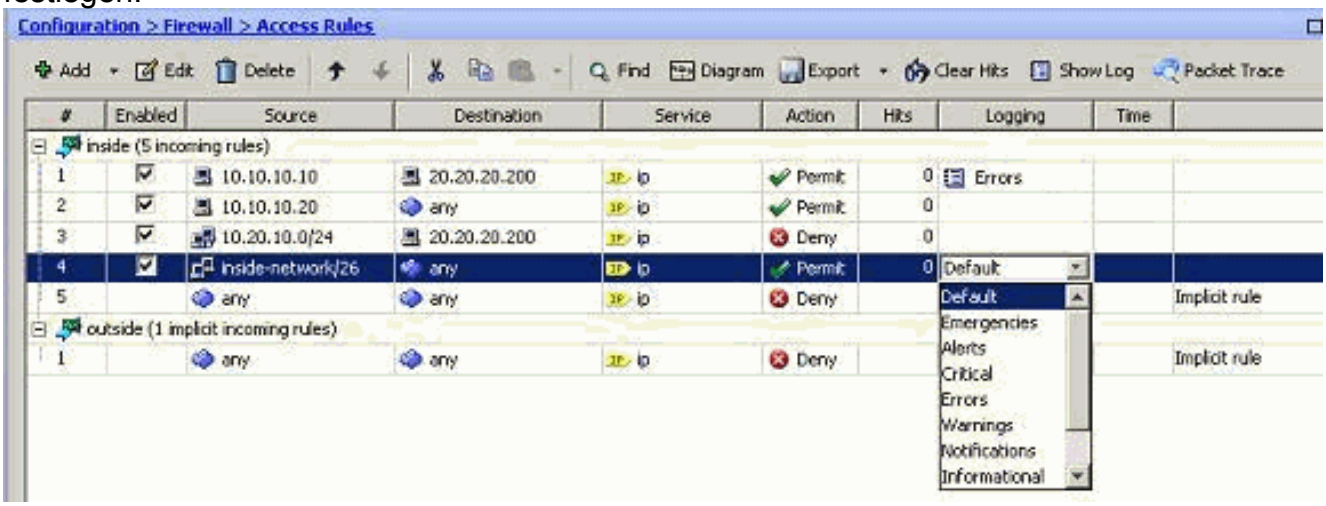
1. Wählen Sie die gewünschte Zugriffsregel aus, und klicken Sie auf *Bearbeiten*.Das Fenster *Zugriffsregel bearbeiten* wird angezeigt. 

**Hinweis:** In diesem Bild zeigt die *Standard*-Option im Feld *Protokollierungsebene* das Standardprotokollierungsverhalten der Cisco ASA an. Weitere Informationen hierzu finden Sie im Abschnitt "Logging Access List Activity" (Protokollzugriffslistenaktivität).
2. Aktivieren Sie die Option *Protokollierung aktivieren*, und geben Sie den gewünschten Schweregrad an. Klicken Sie anschließend auf *OK*. 

**Hinweis:**

Wenn Sie auf die Dropdown-Registerkarte *More options (Weitere Optionen*) klicken, wird die Option *Logging Interval (Protokollierungsintervall) angezeigt*. Diese Option wird nur hervorgehoben, wenn die Option *Protokollierung aktivieren* aktiviert aktiviert ist. Der Standardwert dieses Timers beträgt 300 Sekunden. Diese Einstellung ist hilfreich, um den Timeoutwert für die zu löschenden Flussstatistiken anzugeben, wenn für diese Zugriffsregel keine Übereinstimmung vorliegt. Bei Treffern wartet ASA bis zum Protokollierungsintervall und sendet diese an das Syslog.

3. Die Änderungen werden hier angezeigt. Alternativ können Sie auf das Feld *Protokollierung* der jeweiligen Zugriffsregel doppelklicken und dort den Schweregrad festlegen.




**Hinweis:** Diese alternative Methode zur Angabe des *Protokollierungsgrads* im gleichen Bereich *für* Zugriffsregeln durch Doppelklicken funktioniert nur für manuell erstellte Zugriffsregeleinträge, nicht jedoch für implizite Regeln.

# Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

**Hinweis:** Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

## Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

**CiscoASA**

```
: Saved
:
ASA Version 8.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
```

```
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 209.165.201.2 255.255.255.0
!
interface Ethernet0/2
 nameif inside
 security-level 100
 ip address 10.78.177.11 255.255.255.192
!
!!--- Output Suppressed ! access-list inside_access_in
extended permit ip host 10.10.10.10 host 20.20.20.200
log errors
access-list inside_access_in extended permit ip host
10.10.10.20 any
access-list inside_access_in extended deny ip 10.20.10.0
255.255.255.0 host 20.20.20.200
access-list inside_access_in extended permit ip
10.78.177.0 255.255.255.192 any log emergencies
pager lines 24
logging enable
logging list user-auth-syslog level warnings class auth
logging list TCP-conn-syslog message 302013-302018
logging list syslog-sev-error level errors
logging list vpnclient-errors level errors class vpnc
logging list vpnclient-errors level errors class ssl
logging buffered user-auth-syslog
logging mail alerts
logging from-address test123@example.com
logging recipient-address monitorsyslog@example.com
level errors
logging queue 1024
logging host inside 172.16.11.100
logging ftp-bufferwrap
logging ftp-server 172.16.18.10 syslog testuser ****
logging permit-hostdown
no logging message 302015
no logging message 302016
logging rate-limit 600 86400 level 7
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-623.bin
asdm history enable
arp timeout 14400
!!--- Output Suppressed ! timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00
mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00
sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00 timeout sip-provisional-media 0:02:00 uauth
0:05:00 absolute timeout TCP-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy ! !---
Output Suppressed ! ! telnet timeout 5 ssh timeout 5
console timeout 0 threat-detection basic-threat threat-
detection statistics access-list no threat-detection
statistics TCP-intercept ! !--- Output Suppressed !
username test password /FzQ9W6s1KjC0YQ7 encrypted
privilege 15 ! ! class-map inspection_default match
```

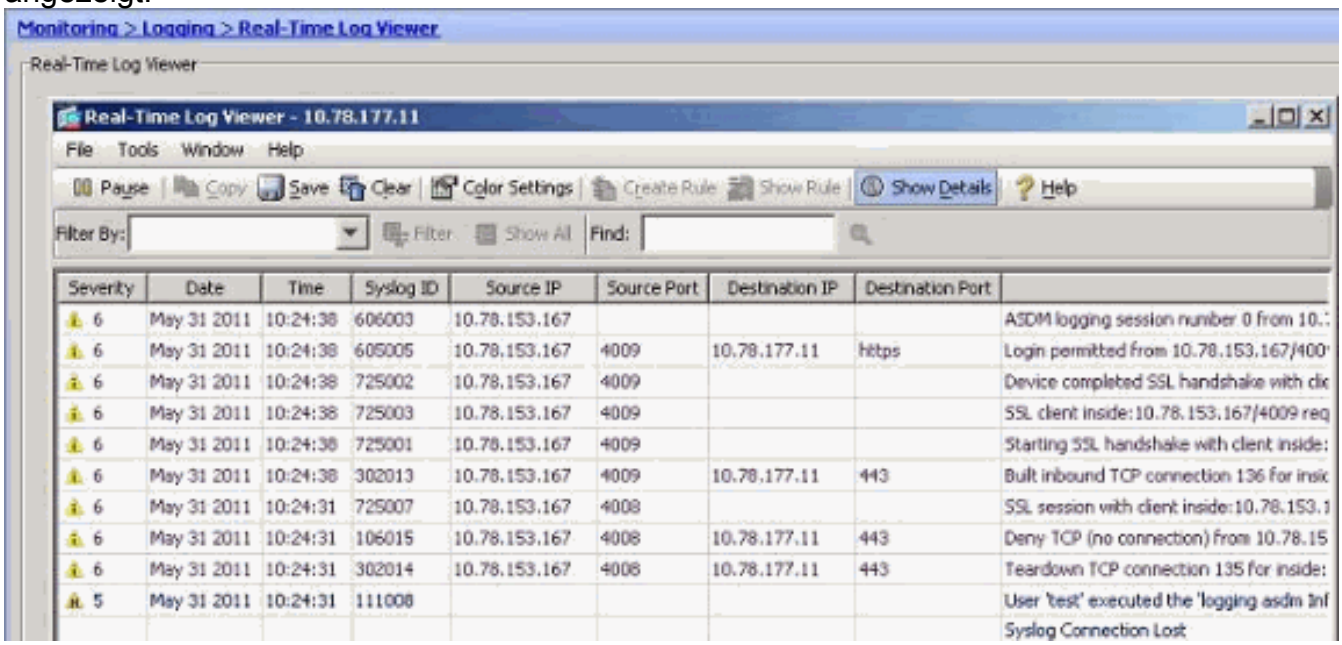
```
default-inspection-traffic ! ! policy-map type inspect
dns preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global smtp-server 172.18.10.20
prompt hostname context
Cryptochecksum:ad941fe5a2bbea3d477c03521e931cf4
: end
```

# Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- Sie können die Syslogs im ASDM anzeigen. Wählen Sie **Monitoring > Logging > Real Time Log Viewer aus**. Hier wird eine Beispielausgabe angezeigt:




# Fehlerbehebung

## Problem: Verbindung unterbrochen — Syslog-Verbindung beendet —

Dieser Fehler tritt auf, wenn versucht wird, die ASDM-Protokollierung für einen der Kontexte im Geräte-Dashboard zu aktivieren.

```
"Verbindung unterbrochen — Syslog-Verbindung beendet —"
```

Wenn ASDM für die direkte Verbindung mit dem Admin-Kontext verwendet wird und dort die ADSM-Protokollierung deaktiviert ist, wechseln Sie zu einem Subkontext, und aktivieren Sie die ASDM-Protokollierung. Die Fehler werden empfangen, aber die Syslog-Meldungen erreichen den Syslog-Server gut.

## Lösung

Dies ist ein bekanntes Verhalten von Cisco ASDM, das in der Cisco Bug ID CSCsd10699 dokumentiert ist (nur registrierte Kunden). Aktivieren Sie als Problemumgehung die ASDM-Protokollierung, wenn Sie sich im Admin-Kontext anmelden.

## Echtzeitprotokolle auf Cisco ASDM können nicht angezeigt werden.

Ein Problem besteht darin, dass die Echtzeitprotokolle nicht auf dem ASDM angezeigt werden können. Wie wird diese konfiguriert?

## Lösung

Konfigurieren Sie Folgendes auf der Cisco ASA:

```
ciscoasa(config)#logging monitor 6
ciscoasa(config)#terminal monitor
ciscoasa(config)#logging on
ciscoasa(config)#logging trap 6
```

# Zugehörige Informationen

- Unterstützung von Cisco Adaptive Security Appliances der Serie ASA 5500
- Technischer Support und Dokumentation - Cisco Systems