Configure Adaptive Security Appliance (ASA) Syslog

Contents

Introduction

This document describes sample configuration that demonstrates how to configure different logging options on ASA that runs code Version 8.4 or later.

Background Information

ASA Version 8.4 has introduced very granular filtering techniques in order to allow only certain specified syslog messages to be presented. The Basic Syslog section of this document demonstrates a traditional syslog configuration. The Advanced Syslog section of this document shows the new syslog features in Version 8.4. Refer to Cisco Security Appliance System Log Messages Guides for the complete system log messages guide.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- ASA 5515 with ASA Software Version 8.4
- Cisco Adaptive Security Device Manager (ASDM) Version 7.1.6

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Note: Refer to ASA 8.2: Configure Syslog using ASDM for more information for similar configuration details with ASDM version 7.1 and later.

Basic Syslog

Enter these commands in order to enable logging, view logs, and view configuration settings.

- **logging enable** - Enables the transmission of syslog messages to all output locations.
- **no logging enable -** Disables logging to all output locations.
- **show logging -** Lists the contents of the syslog buffer as well as information and statistics that pertain to the current configuration.

The ASA can send syslog messages to various destinations. Enter the commands in these sections in order to specify the locations you would like the syslog information to be sent:

Send Logging Information to the Internal Buffer

<#root>

```
logging buffered
```

```
 severity_level
```

External software or hardware is not required when you store the syslog messages in the ASA internal buffer. Enter the **show logging** command in order to view the stored syslog messages. The internal buffer has a maximum size of 1 MB (configurable with the **logging buffer-size** command). As a result, it can wrap very quickly. Keep this in mind when you choose a logging level for the internal buffer as more verbose levels of logging can quickly fill, and wrap, the internal buffer.

Send Logging Information to a Syslog Server

<#root>

```
logging host

 interface_name ip_address [tcp[/port] | udp[/port]] [format emblem]

logging trap

 severity_level

logging facility

 number
```

A server that runs a syslog application is required in order to send syslog messages to an external host. ASA sends syslog on UDP port 514 by default, but protocol and port can be chosen. If TCP is chosen as the logging protocol, this causes the ASA to send syslogs via a TCP connection to the syslog server. If the server is inaccessible, or the TCP connection to the server cannot be established, the ASA, by default, blocks ALL new connections. This behavior can be disabled if you enable **logging permit-hostdown**. See the configuration guide for more information about the **logging permit-hostdown** command.

Note: The ASA only allows ports that range from 1025-65535. Use of any other ports results in this error:
ciscoasa(config)# logging host tftp 192.168.1.1 udp/516
WARNING: interface Ethernet0/1 security level is 0.
ERROR: Port '516' is not within the range 1025-65535.

Send Logging Information as E-mails

<#root>

```
logging mail

 severity_level

logging recipient-address

 email_address

logging from-address

 email_address

smtp-server
```

```
 ip_address
```

An SMTP server is required when you send the syslog messages in e-mails. Correct configuration on the SMTP server is necessary in order to ensure that you can successfully relay e-mails from the ASA to the specified e-mail client. If this logging level is set to a very verbose level, such as debug or informational, you can generate a significant number of syslogs since each e-mail sent by this logging configuration causes upwards of four or more additional logs to be generated.

Send Logging Information to the Serial Console

<#root>

```
logging console

 severity_level
```

Console logging enables syslog messages to display on the ASA console (tty) as they occur. If console logging is configured, all log generation on the ASA is ratelimited to 9800 bps, the speed of the ASA serial console. This can cause syslogs to be dropped to all destinations, which include the internal buffer. Do not use console logging for verbose syslogs for this reason.

Send Logging Information to a Telnet/SSH Session

<#root>

```
logging monitor

 severity_level

terminal monitor
```

Logging monitor enables syslog messages to display as they occur when you access the ASA console with Telnet or SSH and the command **terminal monitor** is executed from that session. In order to stop the printing of logs to your session, enter the **terminal no monitor** command.

Display Log Messages on the ASDM

<#root>

```
logging asdm

 severity_level
```

ASDM also has a buffer that can be used to store syslog messages. Enter the **show logging asdm** command in order to display the content of the ASDM syslog buffer.

Send Logs to an SNMP Management Station

<#root>

```
logging history

 severity_level

snmp-server host

 [if_name] ip_addr

snmp-server location

 text

snmp-server contact

 text

snmp-server community

 key

snmp-server enable traps
```

Users need an existing functional Simple Network Management Protocol (SNMP) environment in order to send syslog messages with SNMP. See Commands for Setting and Managing Output Destinations for a complete reference on the commands you can use to set and manage output destinations. See Messages Listed by Severity Level for messages listed by severity level.

Add Timestamps to Syslogs

In order to help align and order events, timestamps can be added to syslogs. This is recommended in order to help trace issues based on time. In order to enable timestamps, enter the **logging timestamp** command. Here are two syslog examples, one without the timestamp and one with:

```
%ASA-6-302016: Teardown UDP connection 806353 for outside:172.18.123.243/24057 to
 identity:172.18.124.136/161 duration 0:02:01 bytes 313

Jul 03 2014 14:33:09: %ASA-6-302014: Teardown TCP connection 806405 for
 inside:10.0.0.100/50554 to identity:172.18.124.136/51358 duration 0:00:00 bytes
 442 TCP Reset-I
```

Example 1

This output shows a sample configuration for logging into the **buffer** with the severity level of **debugging**.

<#root>

```
logging enable
logging buffered debugging
```

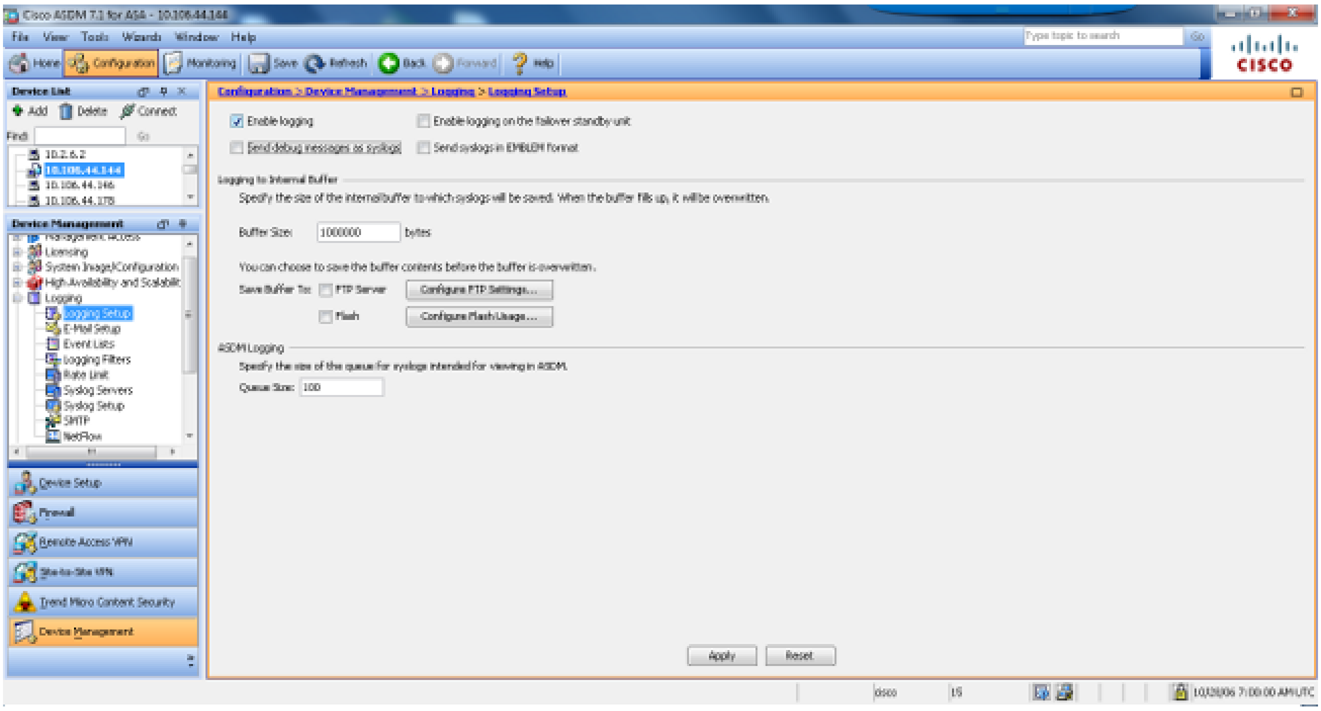
This is sample output.

```
%ASA-6-308001: console enable password incorrect for number tries (from 10.1.1.15)
```

Configure Basic Syslog with ASDM

This procedure demonstrates the ASDM configuration for all available syslog destinations.

1. In order to enable logging on the ASA, first configure the basic logging parameters. Choose **Configuration > Features > Properties > Logging > Logging Setup**. Check the **Enable logging** check box in order to enable syslogs.



Configuration > Device Management > Logging > Logging Setup

☑ Enable logging □ Enable logging on the failover standby unit

□ Send debug messages as syslogs □ Send syslogs in EMBLEM format

Logging to Internal Buffer

Specify the size of the internal buffer to which syslogs will be saved. When the buffer fills up, it will be overwritten.

Buffer Size: 1000000 bytes

You can choose to save the buffer contents before the buffer is overwritten.

Save Buffer To: □ FTP Server [Configure FTP Settings...]

□ Flash [Configure Flash Usage...]

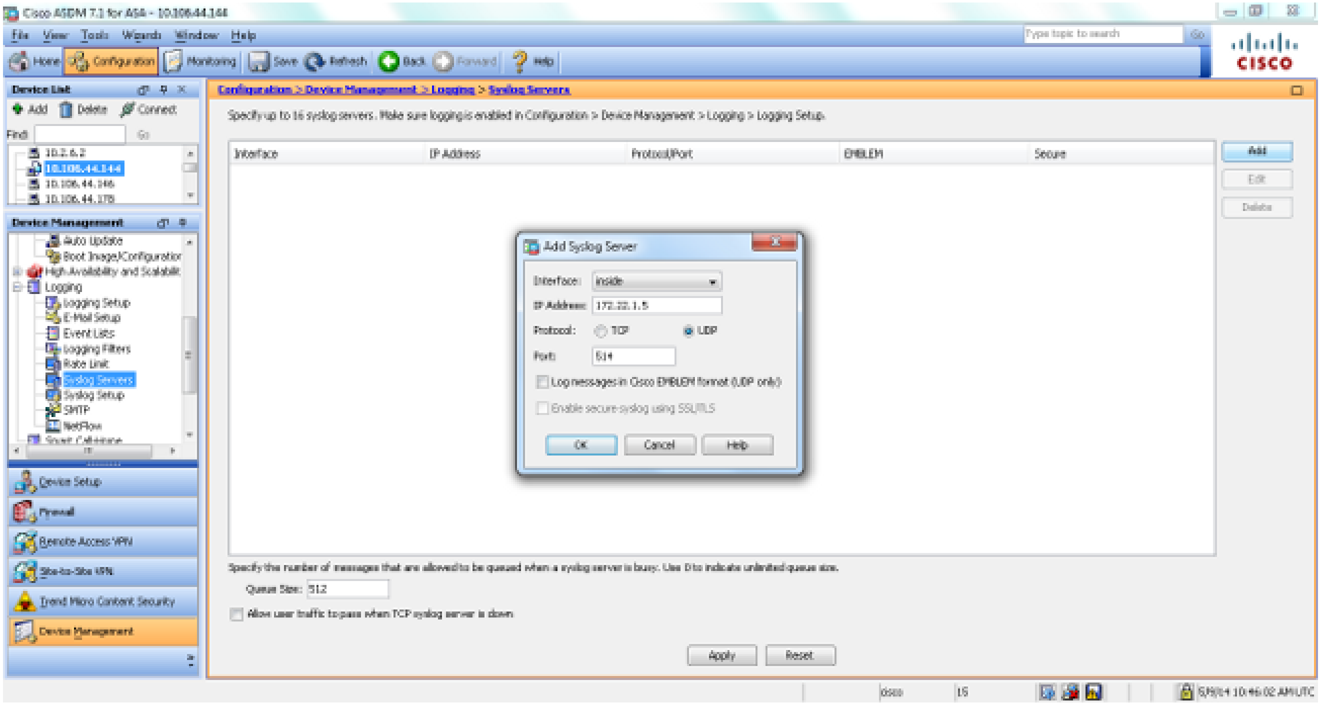
ASDM Logging

Specify the size of the queue for syslogs intended for viewing in ASDM.

Queue Size: 100

[Apply] [Reset]

2. In order to configure an external server as the destination for syslogs, choose **Syslog Servers** in Logging and click **Add** in order to add a syslog server. Enter the syslog server details in the Add Syslog Server box and choose **OK** when you are done.



Configuration > Device Management > Logging > Syslog Servers

Specify up to 16 syslog servers. Make sure logging is enabled in Configuration > Device Management > Logging > Logging Setup.

Interface	IP Address	Protocol/Port	EMBLEM	Secure

Add Syslog Server

Interface: inside

IP Address: 172.22.1.5

Protocol: ○ TCP ● UDP

Port: 514

□ Log messages in Cisco EMBLEM format (UDP only)

□ Enable secure syslog using SSL/TLS

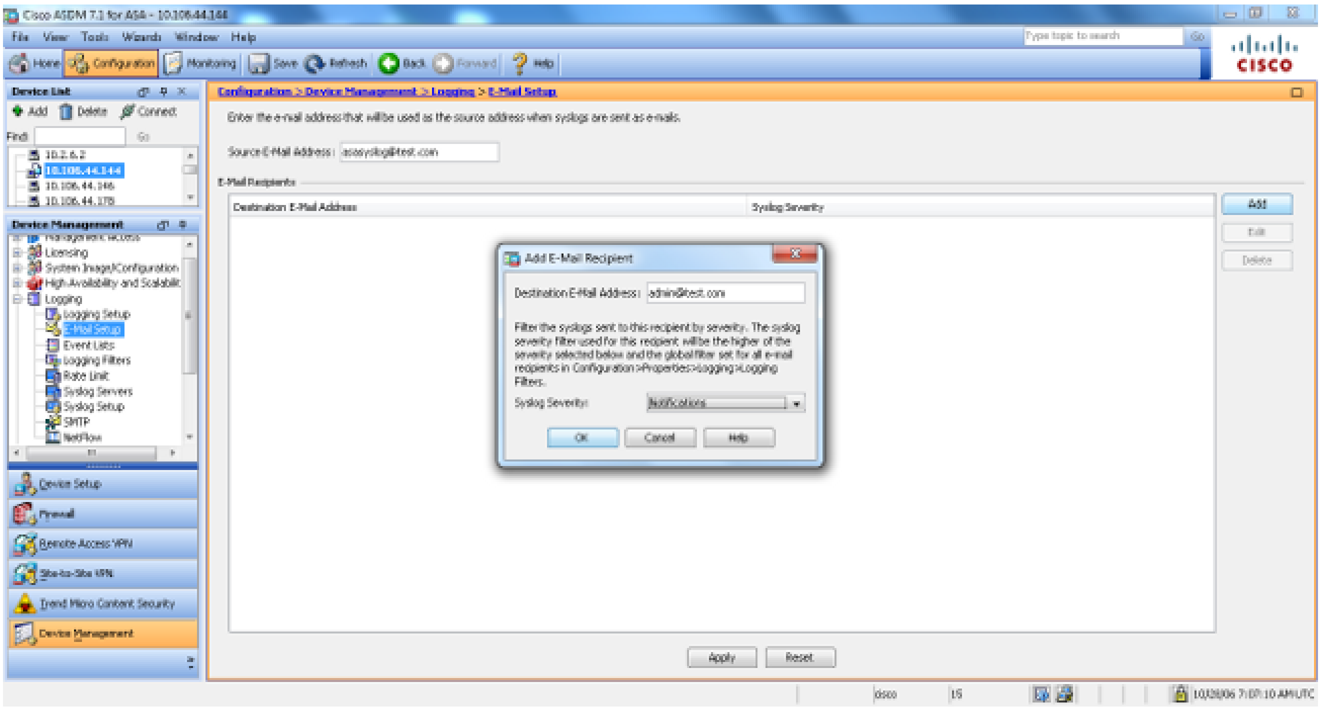
Specify the number of messages that are allowed to be queued when a syslog server is busy. Use 0 to indicate unlimited queue size.

Queue Size: 512

□ Allow user traffic to pass when TCP syslog server is down

Cisco ASDM 7.1 for ASA - 10.106.44.144
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Device Management
Add
Edit
Delete
OK
Cancel
Help
Apply
Reset

3. Choose **E-Mail Setup** in Logging in order to send syslog messages as e-mails to specific recipients. Specify the source e-mail address in the Source E-Mail Address box and choose **Add** in order to configure the destination e-mail address of the e-mail recipients and the message severity level. Click **OK** when you are done.



Configuration > Device Management > Logging > E-Mail Setup

Enter the e-mail address that will be used as the source address when syslogs are sent as e-mails.

Source E-Mail Address: asasyslog@test.com

E-Mail Recipients

Destination E-Mail Address	Syslog Severity

Add E-Mail Recipient

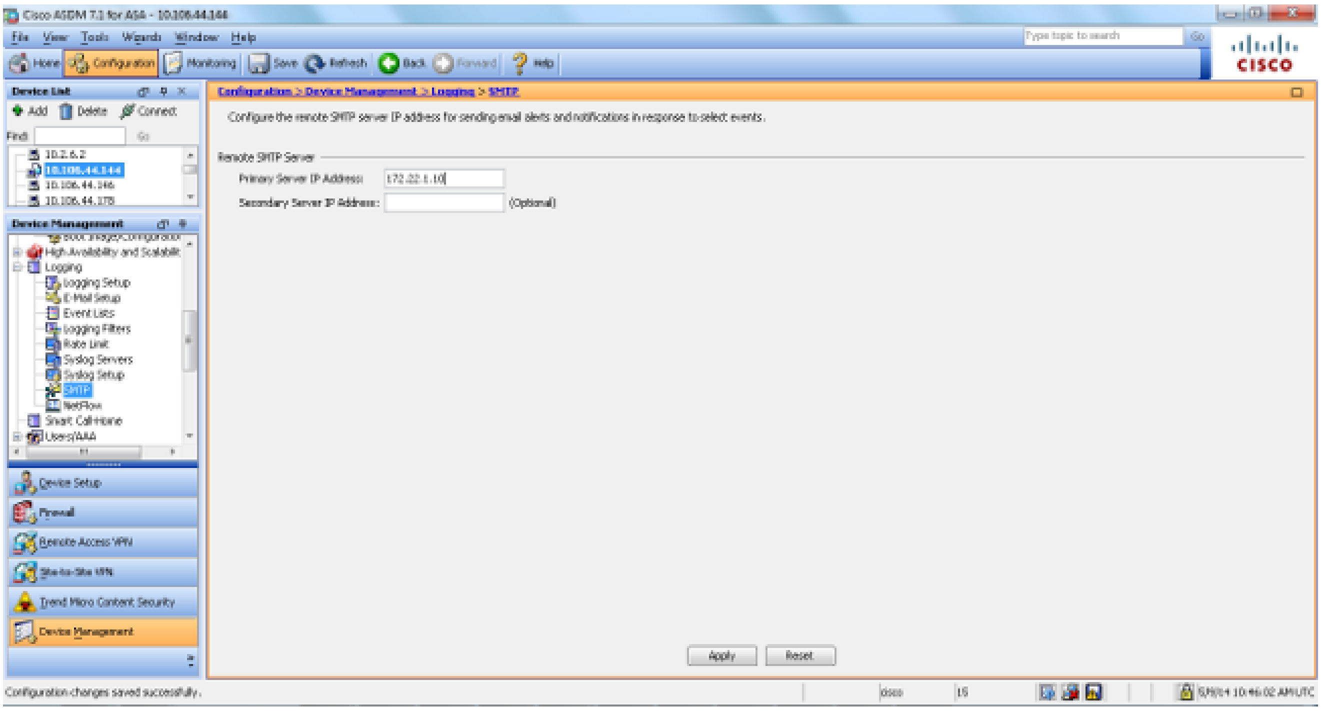
Destination E-Mail Address: admin@test.com

Filter the syslogs sent to this recipient by severity. The syslog severity filter used for this recipient will be the higher of the severity selected below and the global filter set for all e-mail recipients in Configuration >Properties>Logging>Logging Filters.

Syslog Severity: Notifications

Cisco ASDM 7.1 for ASA - 10.106.44.144
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Device Management
Add
Edit
Delete
OK
Cancel
Help
Apply
Reset

4. Choose **Device Administration**, **Logging**, choose **SMTP**, and enter the Primary Server IP Address in order to specify the SMTP server IP address.



Configuration > Device Management > Logging > SMTP

Configure the remote SMTP server IP address for sending email alerts and notifications in response to select events.

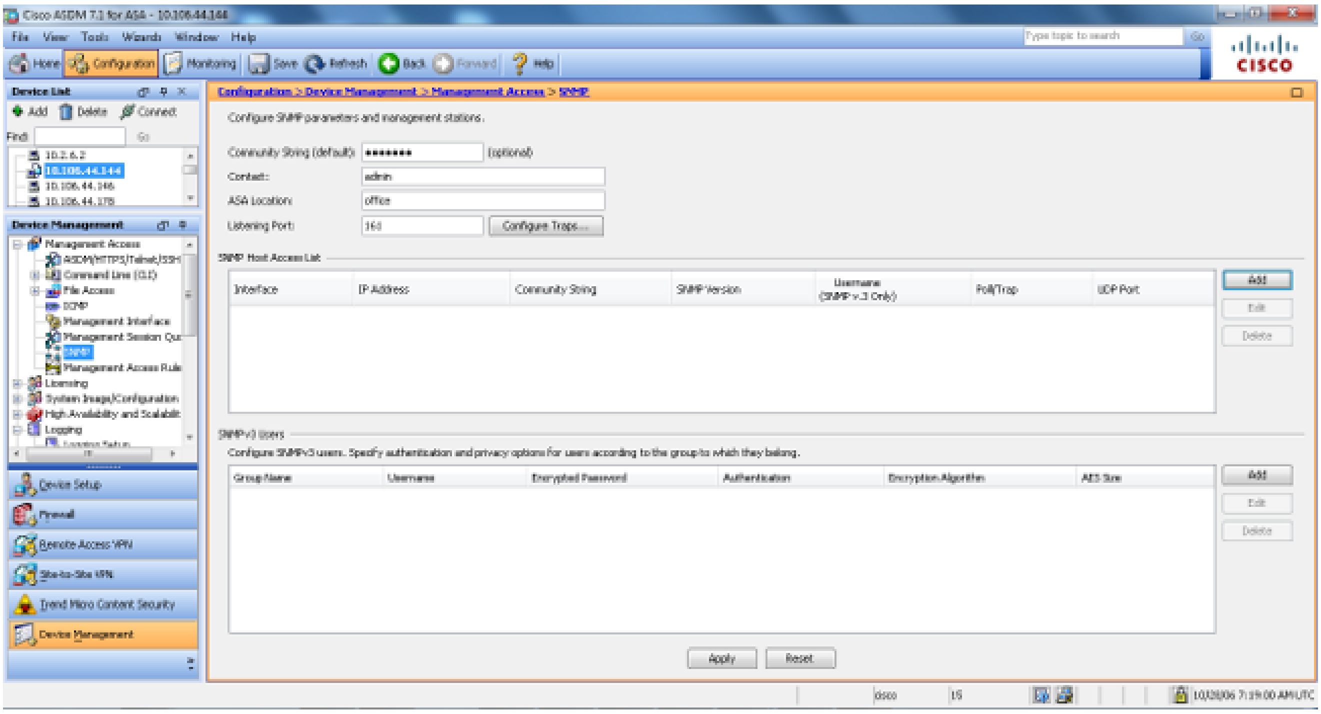
Remote SMTP Server

Primary Server IP Address: 172.22.1.10

Secondary Server IP Address: (Optional)

Configuration changes saved successfully.

5. If you want to send syslogs as SNMP traps, you must first define an SNMP server. Choose **SNMP** in in the **Management Access** menu in order to specify the address of the SNMP management stations and their specific properties.



Configuration > Device Management > Management Access > SNMP

Configure SNMP parameters and management stations.

Community String (default): ******** (optional)

Contact: admin

ASA Location: office

Listening Port: 161

SNMP Host Access List

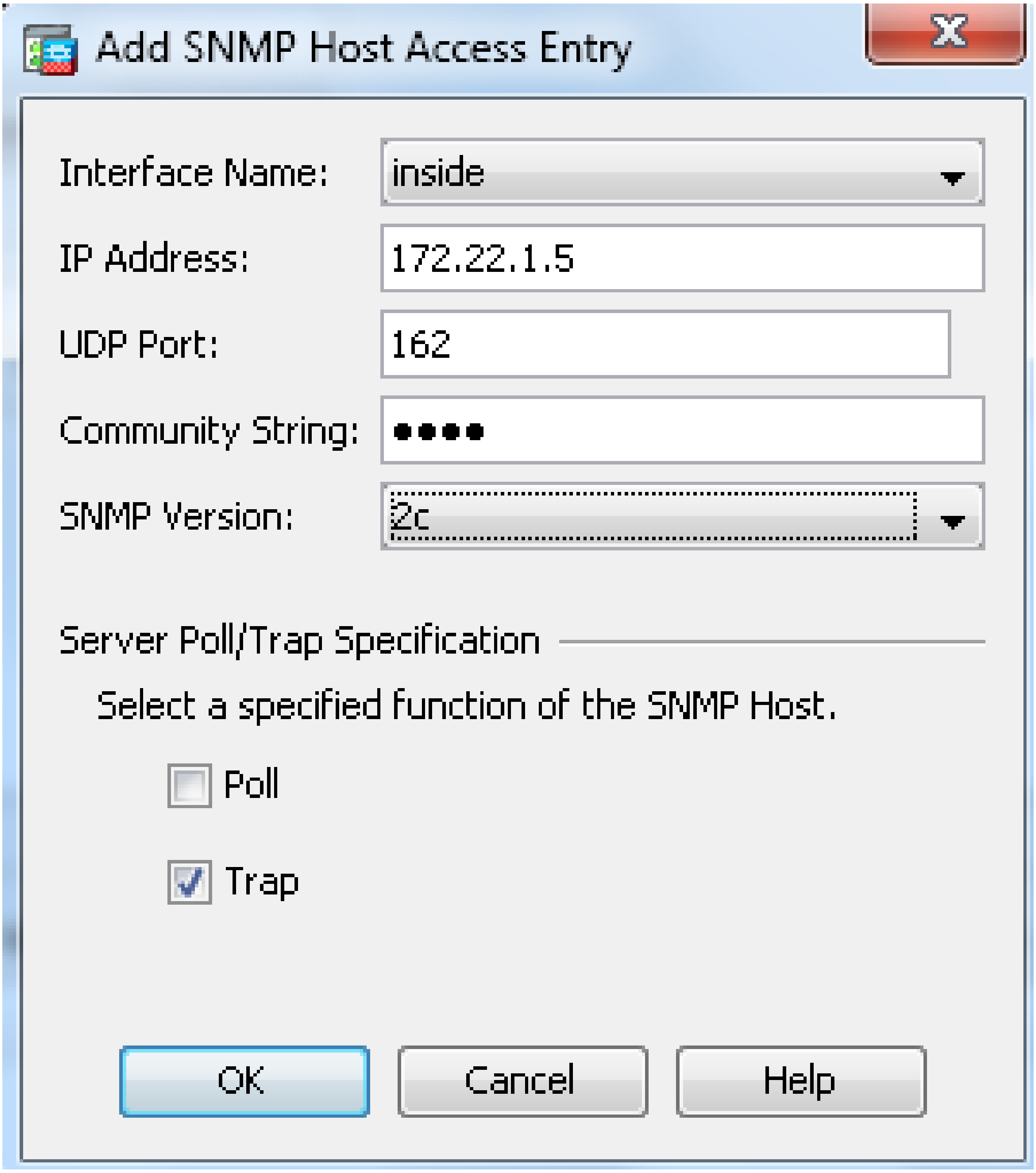
Interface	IP Address	Community String	SNMP Version	Username (SNMP v.3 Only)	Poll/Trap	UDP Port

SNMPv3 Users

Configure SNMPv3 users. Specify authentication and privacy options for users according to the group to which they belong.

Group Name	Username	Encrypted Password	Authentication	Encryption Algorithm	AES Size

6. Choose **Add** in order to add an SNMP management station. Enter the SNMP host details and click **OK**.


Add SNMP Host Access Entry

Interface Name: inside

IP Address: 172.22.1.5

UDP Port: 162

Community String: ●●●●

SNMP Version: 2c

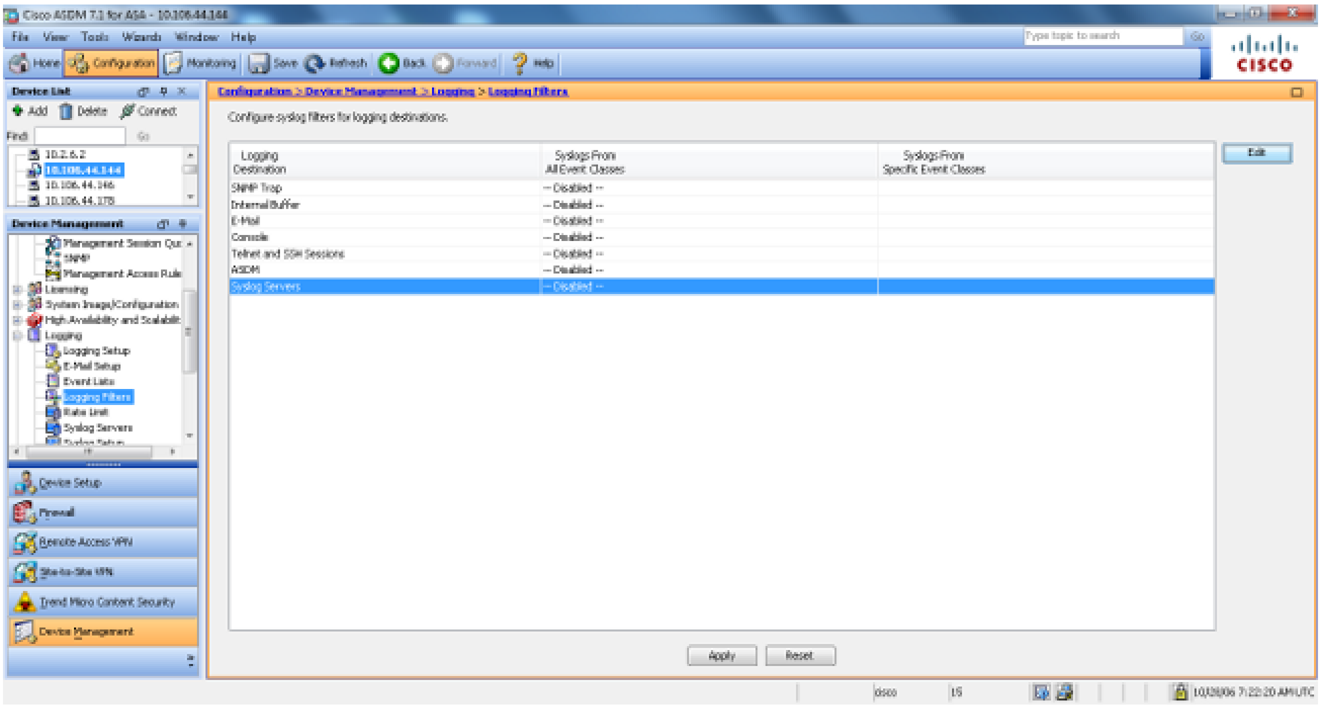
Server Poll/Trap Specification

Select a specified function of the SNMP Host.

□ Poll

☑ Trap

7. In order to enable logs to be sent to any of the prior mentioned destinations, choose **Logging Filters** in the logging section. This presents you with each possible logging destination and the current level of logs that are sent to those destinations. Choose the desired Logging Destination and click **Edit**. In this example, the 'Syslog Servers' destination is modified.

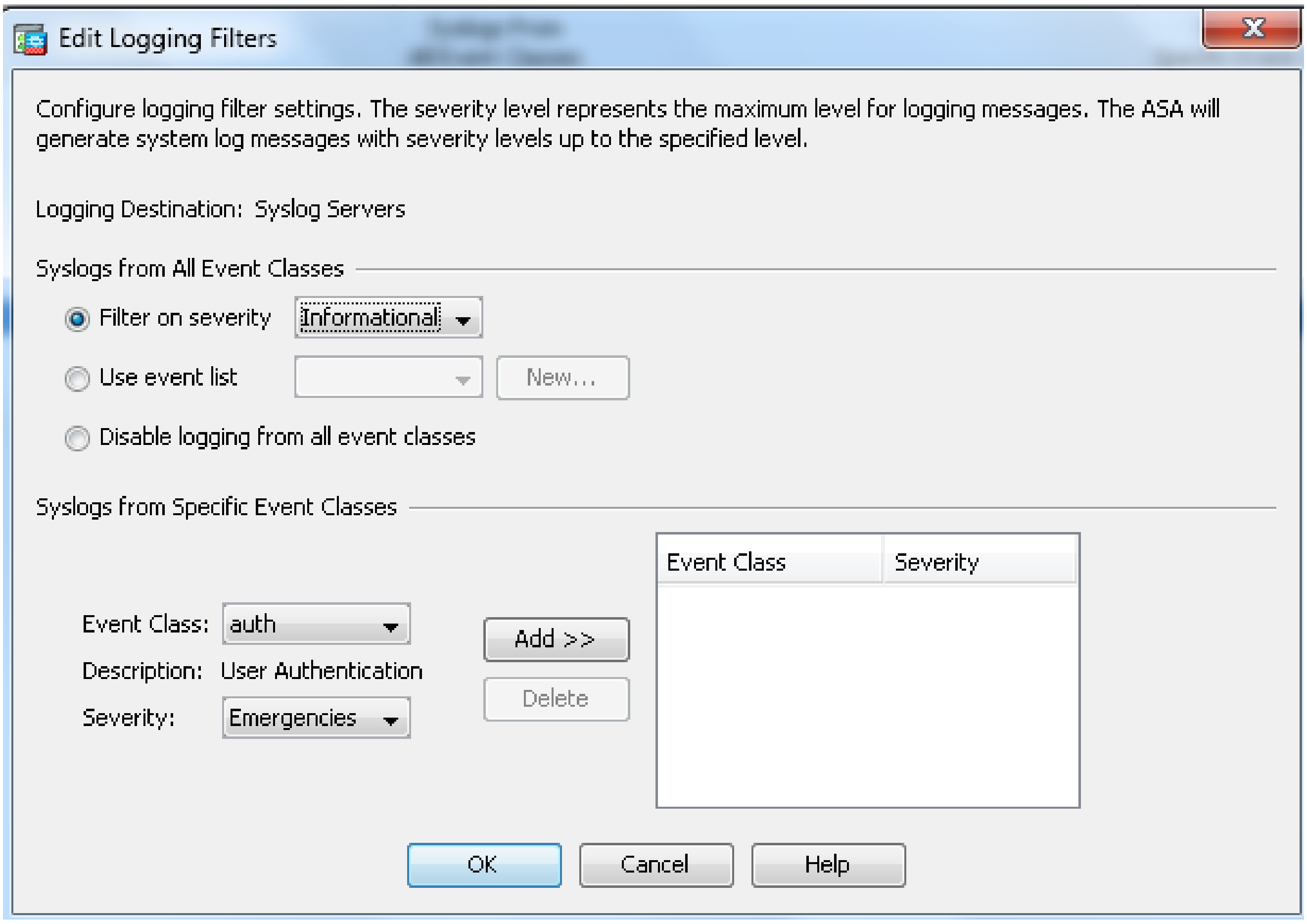


Configuration > Device Management > Logging > Logging Filters

Configure syslog filters for logging destinations.

Logging Destination	Syslogs From All Event Classes	Syslogs From Specific Event Classes
SNMP Trap	-- Disabled --	
Internal Buffer	-- Disabled --	
E-Mail	-- Disabled --	
Console	-- Disabled --	
Telnet and SSH Sessions	-- Disabled --	
ASDM	-- Disabled --	
Syslog Servers	-- Disabled --	

8. Choose an appropriate severity, in this case **Informational,** from the **Filter on severity** drop-down list. Click **OK** when you are done.



Edit Logging Filters

Configure logging filter settings. The severity level represents the maximum level for logging messages. The ASA will generate system log messages with severity levels up to the specified level.

Logging Destination: Syslog Servers

Syslogs from All Event Classes

● Filter on severity: Informational

○ Use event list

○ Disable logging from all event classes

Syslogs from Specific Event Classes

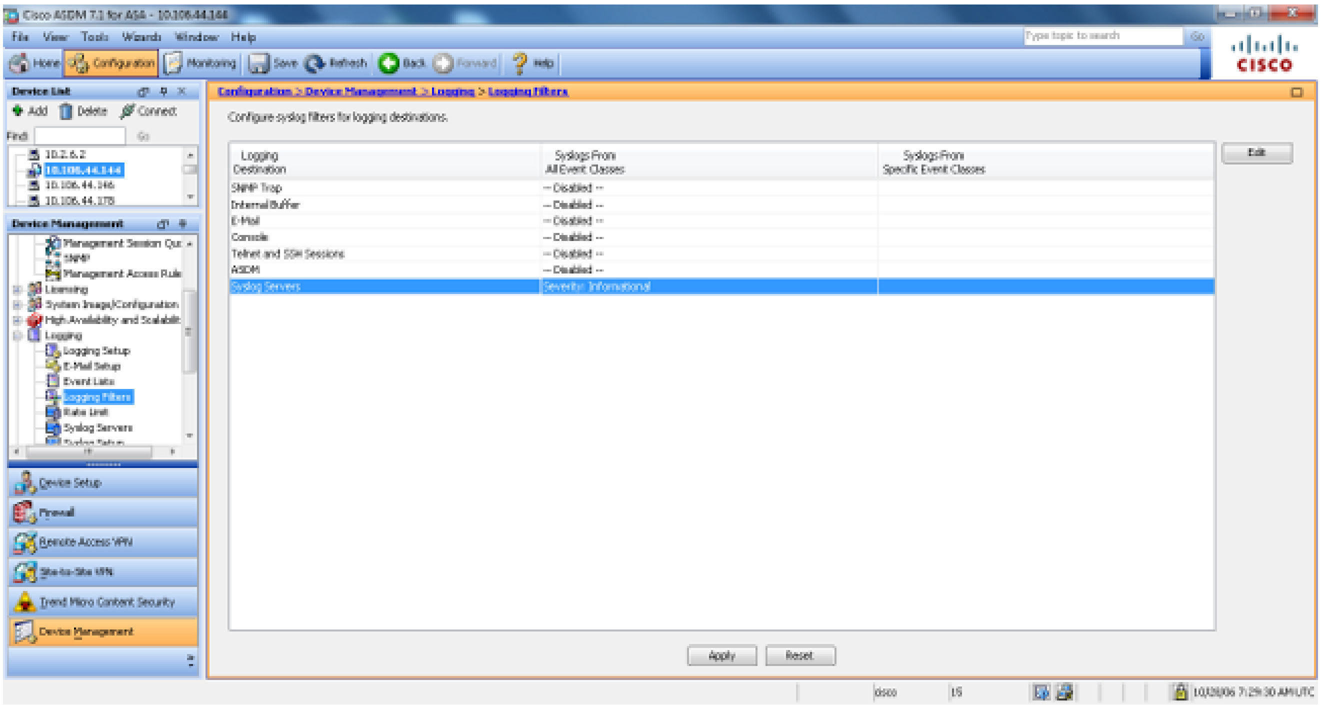
Event Class: auth

Description: User Authentication

Severity: Emergencies

Event Class	Severity

9. Click **Apply** after you return to the Logging Filters window.



Configuration > Device Management > Logging > Logging Filters

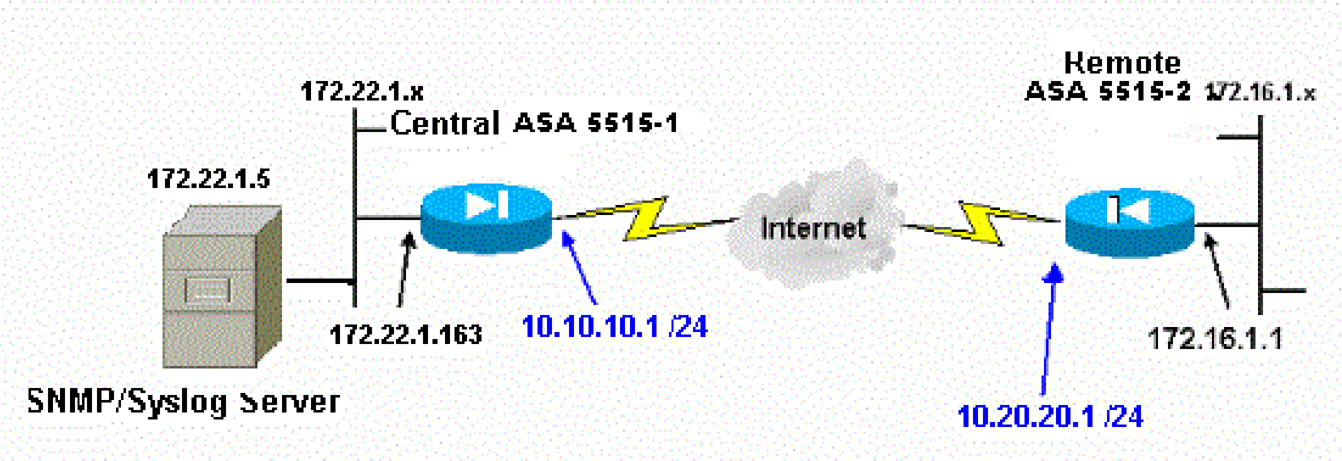
Configure syslog filters for logging destinations.

Logging Destination	Syslogs From All Event Classes	Syslogs From Specific Event Classes
SNMP Trap	-- Disabled --	
Internal Buffer	-- Disabled --	
E-Mail	-- Disabled --	
Console	-- Disabled --	
Telnet and SSH Sessions	-- Disabled --	
ASDM	-- Disabled --	
Syslog Servers	Severity: Informational	

Send Syslog Messages Over a VPN to a Syslog Server

In either the simple site-to-site VPN design or the more complicated hub-and-spoke design, administrator could want to monitor all remote ASA Firewalls with the SNMP server and syslog server located at a central site.

In order to configure the site-to-site IPsec VPN configuration, refer to PIX/ASA 7.x and above: PIX-to-PIX VPN Tunnel Configuration Example. Apart from the VPN configuration, you have to configure the SNMP and the interesting traffic for the syslog server in both the central and local site.



Central ASA Configuration

<#root>

```
!--- This access control list (ACL) defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two ASA.
!--- It also includes the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind the ASA 5515.
```

```
access-list 101 permit ip 172.22.1.0 255.255.255.0 172.16.1.0 255.255.255.0



!--- This lines covers SNMP (TCP/UDP port - 161), SNMP TRAPS(TCP/UDP port - 162)
!--- and syslog traffic (UDP port - 514) from SNMP/syslog server
!--- to the outside interface of the remote ASA.


access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 161
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 161
access-list 101 permit tcp host 172.22.1.5 host 10.20.20.1 eq 162
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 162
access-list 101 permit udp host 172.22.1.5 host 10.20.20.1 eq 514




logging enable
logging trap debugging


!--- Define logging host information.

logging facility 16
logging host inside 172.22.1.5



!--- Define the SNMP configuration.

snmp-server host inside 172.22.1.5 community ***** version 2c



snmp-server community *****
```

Remote ASA Configuration

<#root>

```
!--- This ACL defines IPsec interesting traffic.
!--- This line covers traffic between the LAN segment behind two ASA.
!--- It also covers the SNMP/syslog traffic between the SNMP/syslog server
!--- and the network devices located on the Ethernet segment behind ASA 5515.

access-list 101 permit ip 172.16.1.0 255.255.255.0 172.22.1.0 255.255.255.0



!--- This lines covers SNMP (TCP/UDP port - 161), SNMP TRAPS (TCP/UDP port - 162) and
!--- syslog traffic (UDP port - 514) sent from this ASA outside
!--- interface to the SYSLOG server.

access-list 101 permit tcp host 10.20.20.1 host 172.22.1.5 eq 161
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 161
access-list 101 permit tcp host 10.20.20.1 host 172.22.1.5 eq 162
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 162
access-list 101 permit udp host 10.20.20.1 host 172.22.1.5 eq 514
```

```
!--- Define syslog server.

logging facility 23
logging host outside 172.22.1.5



!--- Define SNMP server.

snmp-server host outside 172.22.1.5 community ***** version 2c
snmp-server community *****
```

Refer to Monitoring Cisco Secure ASA Firewall Using SNMP and Syslog Through VPN Tunnel for more information on how to configure ASA Version 8.4

Advanced Syslog

ASA Version 8.4 provides several mechanisms that enable you to configure and manage syslog messages in groups. These mechanisms include message severity level, message class, message ID, or a custom message list that you create. With the use of these mechanisms, you can enter a single command that applies to small or large groups of messages. When you set up syslogs this way, you are able to capture the messages from the specified message group and no longer all the messages from the same severity.

Use the Message List

Use the message list in order to include only the interested syslog messages by severity level and ID into a group, then associate this message list with the desired destination.

Complete these steps in order to configure a message list:

1. Enter the **logging list *message_list* | *level severity_level [class message_class]*** command in order to create a message list that includes messages with a specified severity level or message list.

2. Enter the **logging list *message_list* message *syslog_id-syslog_id2*** command in order to add additional messages to the message list just created.

3. Enter the **logging *destination message_list*** command in order to specify the destination of the message list created.

Example 2

Enter these commands in order to create a message list, which includes all the severity 2 (critical) messages with the addition of message 611101 to 611323, and also have them sent to the console:

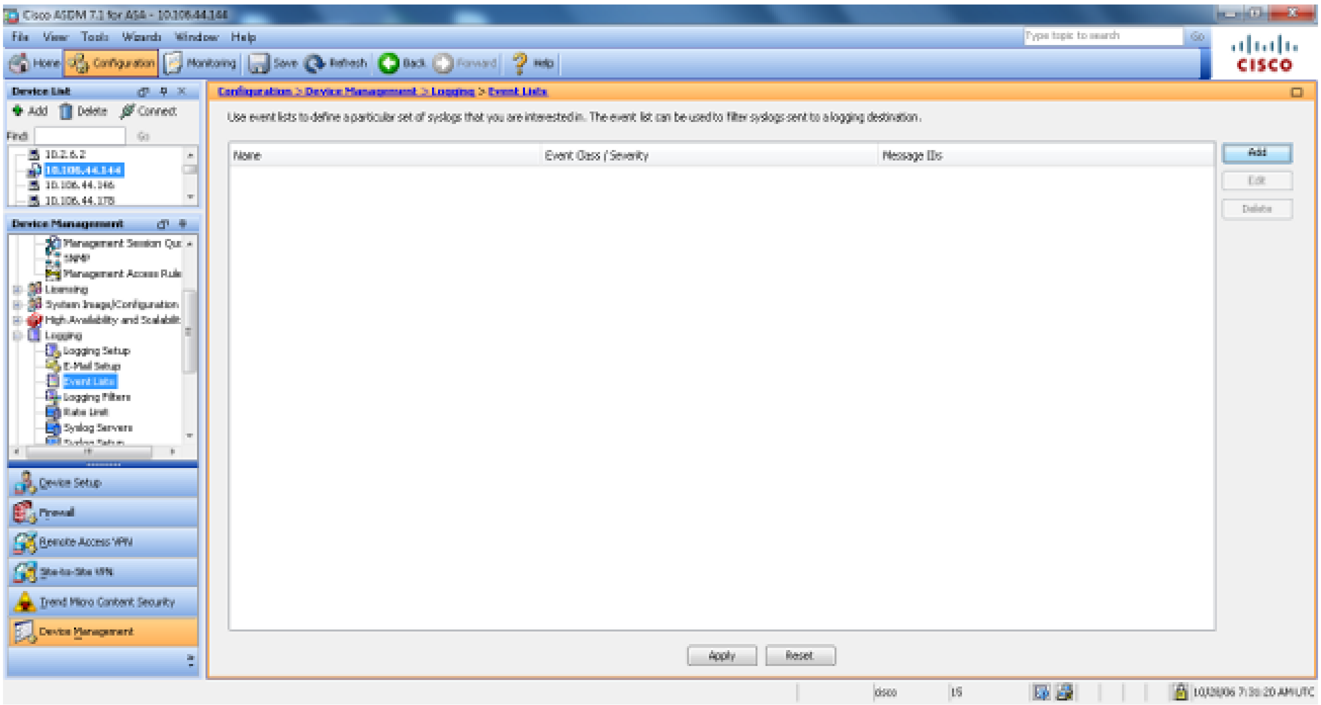
<#root>

```
logging list my_critical_messages level 2
logging list my_critical_messages message 611101-611323
logging console my_critical_messages
```

ASDM Configuration

This procedure shows an ASDM configuration for Example 2 with the use of the message list.

1. Choose **Event Lists** under Logging and click **Add** in order to create a message list.

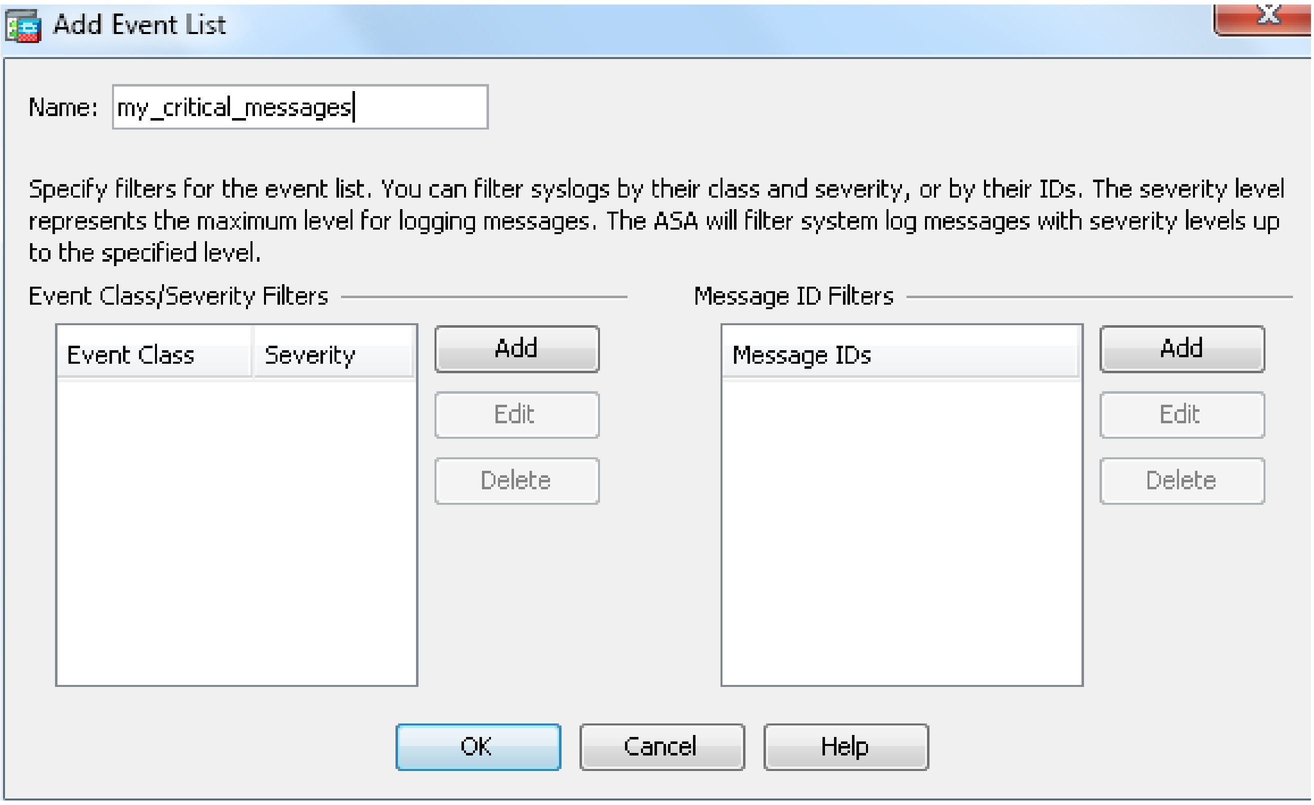


Cisco ASDM 7.1 for ASA - 10.106.44.144

Configuration > Device Management > Logging > Event Lists

Use event lists to define a particular set of syslogs that you are interested in. The event list can be used to filter syslogs sent to a logging destination.

2. Enter the name of the message list in the Name box. In this case **my_critical_messages** is used. Click **Add** under Event Class/Severity Filters.

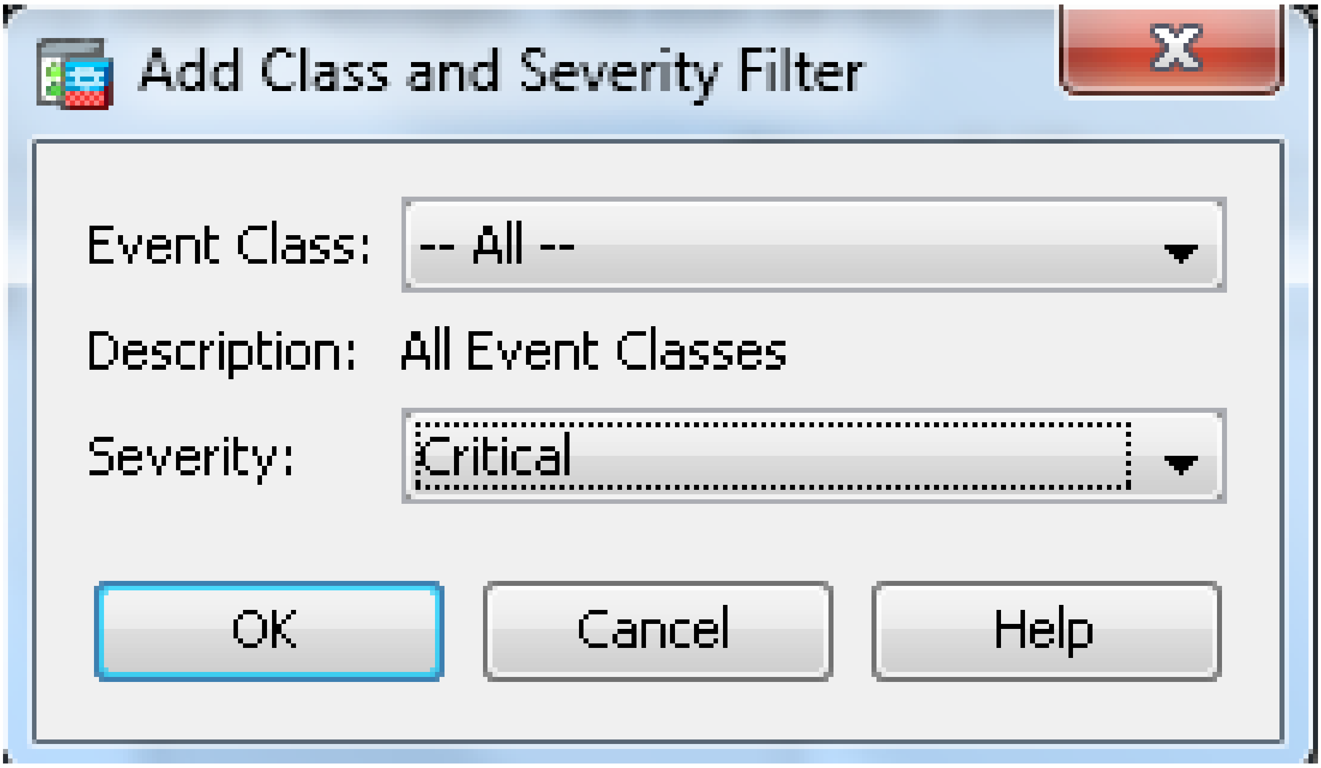


Add Event List

Name: my_critical_messages

Specify filters for the event list. You can filter syslogs by their class and severity, or by their IDs. The severity level represents the maximum level for logging messages. The ASA will filter system log messages with severity levels up to the specified level.

3. Choose **All** from the Event Class drop-down list. Choose **Critical** from the Severity drop-down list. Click **OK** when you are done.



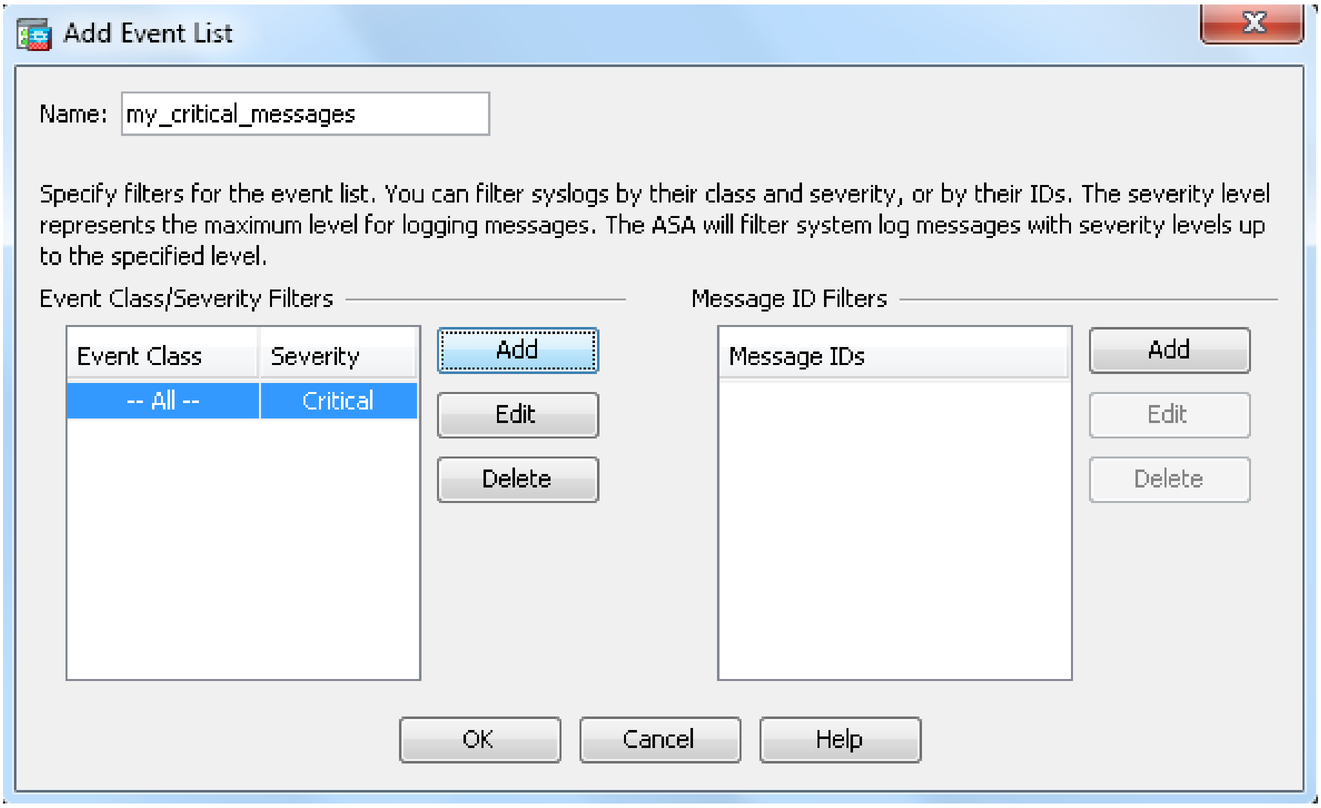
Add Class and Severity Filter

Event Class: -- All --

Description: All Event Classes

Severity: Critical

4. Click **Add** under the Message ID Filters if additional messages are required. In this case, you need to put in messages with ID 611101-611323.



Add Event List

Name: my_critical_messages

Specify filters for the event list. You can filter syslogs by their class and severity, or by their IDs. The severity level represents the maximum level for logging messages. The ASA will filter system log messages with severity levels up to the specified level.

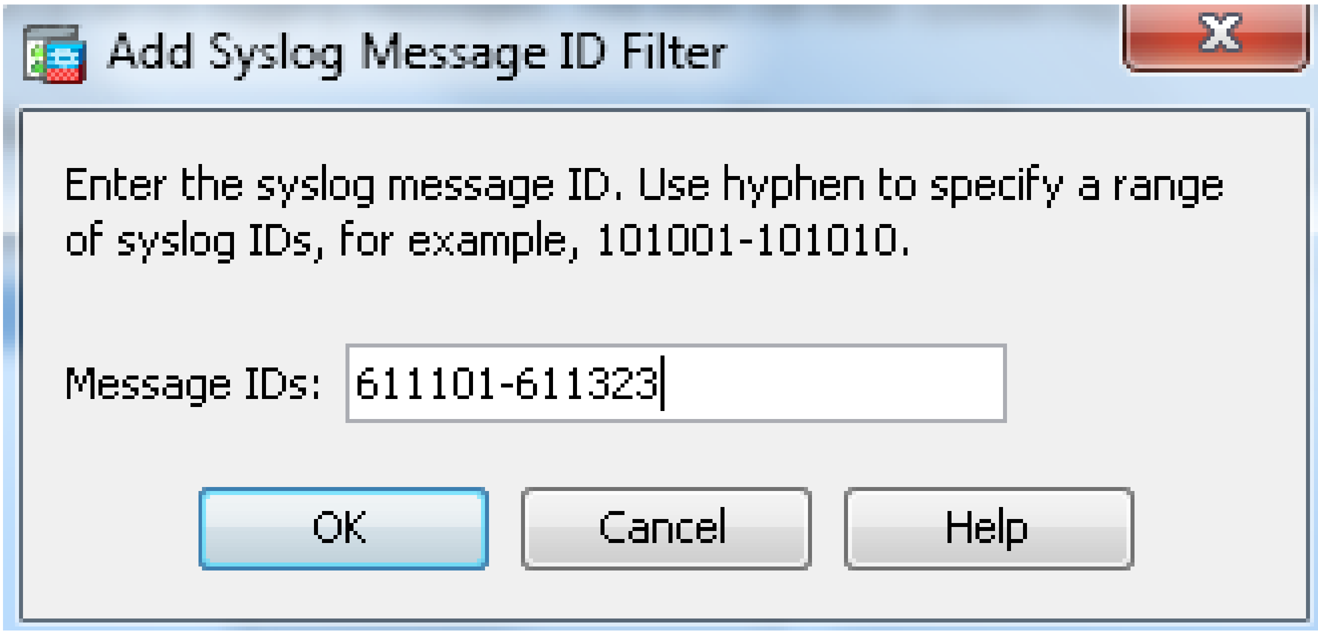
Event Class/Severity Filters

Event Class	Severity
-- All --	Critical

Message ID Filters

Message IDs

5. Put in the ID range in the Message IDs box and click **OK**.



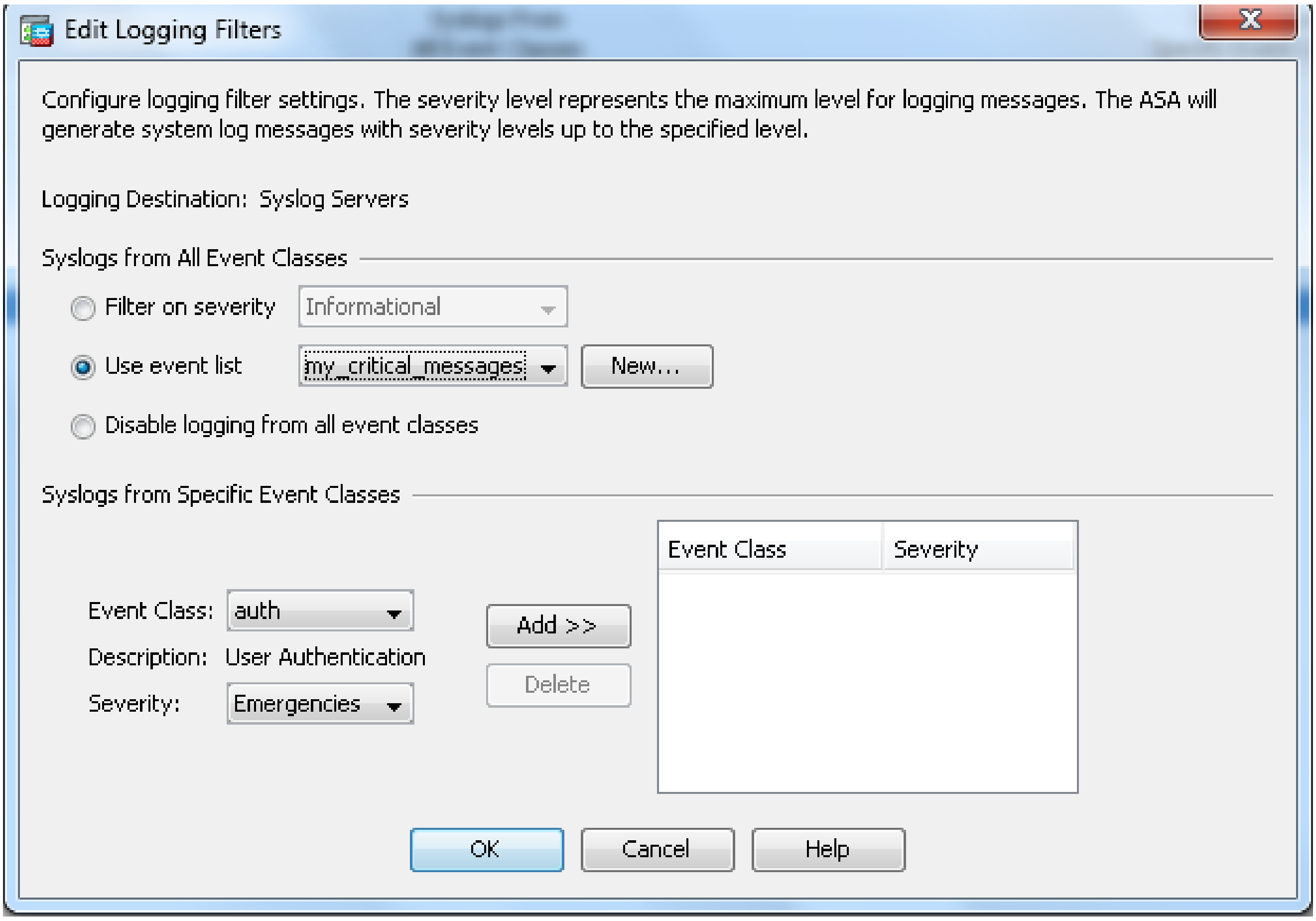
Add Syslog Message ID Filter

Enter the syslog message ID. Use hyphen to specify a range of syslog IDs, for example, 101001-101010.

Message IDs: 611101-611323

6. Go back to the **Logging Filters** menu and choose **Console** as the destination.

7. Choose **my_critical_messages** from the **Use event list** drop-down list. Click **OK** when you are done.



Edit Logging Filters

Configure logging filter settings. The severity level represents the maximum level for logging messages. The ASA will generate system log messages with severity levels up to the specified level.

Logging Destination: Syslog Servers

Syslogs from All Event Classes

○ Filter on severity: Informational

● Use event list: my_critical_messages

○ Disable logging from all event classes

Syslogs from Specific Event Classes

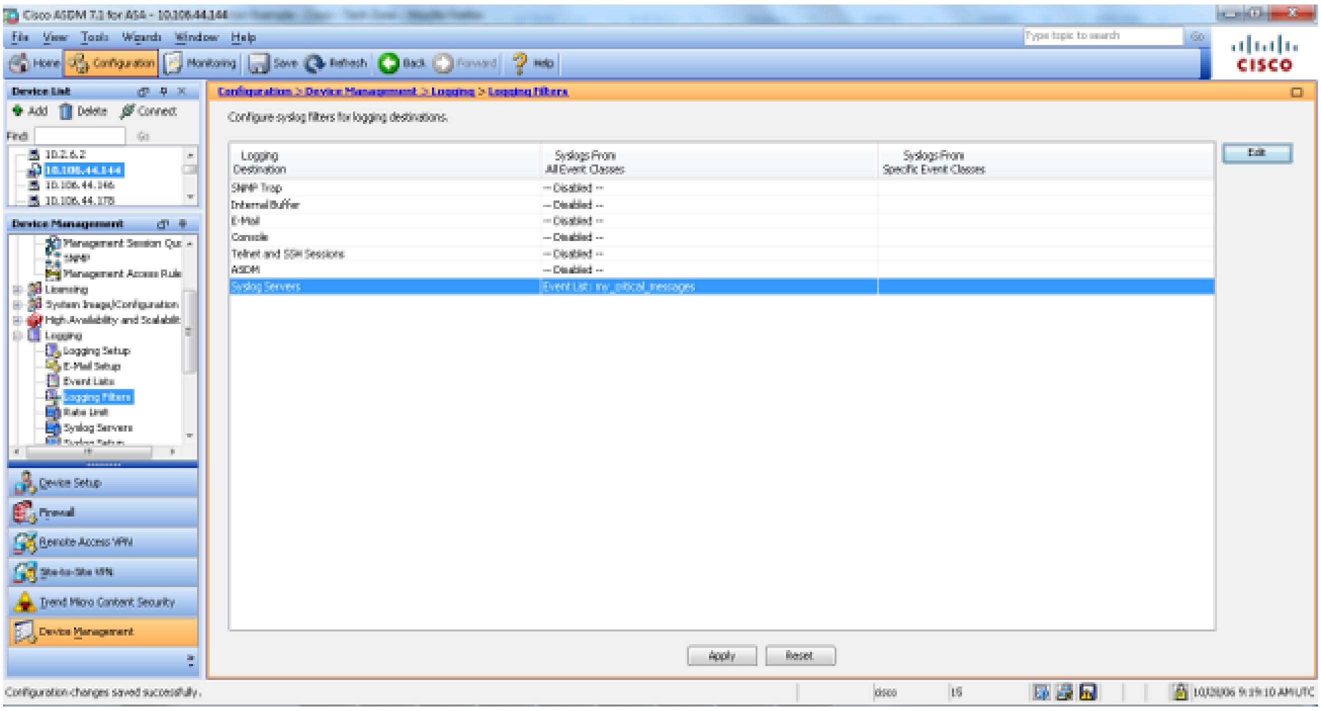
Event Class: auth

Description: User Authentication

Severity: Emergencies

Event Class	Severity

8. Click **Apply** after you return to the Logging Filters window.



Cisco ASDM 7.1 for ASA - 10.106.44.144
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Device Management
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Trend Micro Content Security
Device Management
Apply
Reset
Edit

Configuration > Device Management > Logging > Logging Filters

Configure syslog filters for logging destinations.

Logging Destination	Syslogs From All Event Classes	Syslogs From Specific Event Classes
SNMP Trap	-- Disabled --	
Internal Buffer	-- Disabled --	
E-Mail	-- Disabled --	
Console	-- Disabled --	
Telnet and SSH Sessions	-- Disabled --	
ASDM	-- Disabled --	
Syslog Servers	Event List: my_critical_messages	

Configuration changes saved successfully.

This completes the ASDM configurations with the use of a message list as shown in Example 2.

Use the Message Class

Use the message class in order to send all messages associated with a class to the specified output location. When you specify a severity level threshold, you can limit the number of messages sent to the output location.

<#root>

```
logging class
```

```
 message_class destination | severity_level
```

Example 3

Enter this command in order to send all ca class messages with a severity level of emergencies or higher to the console.

<#root>

```
logging class ca console emergencies
```

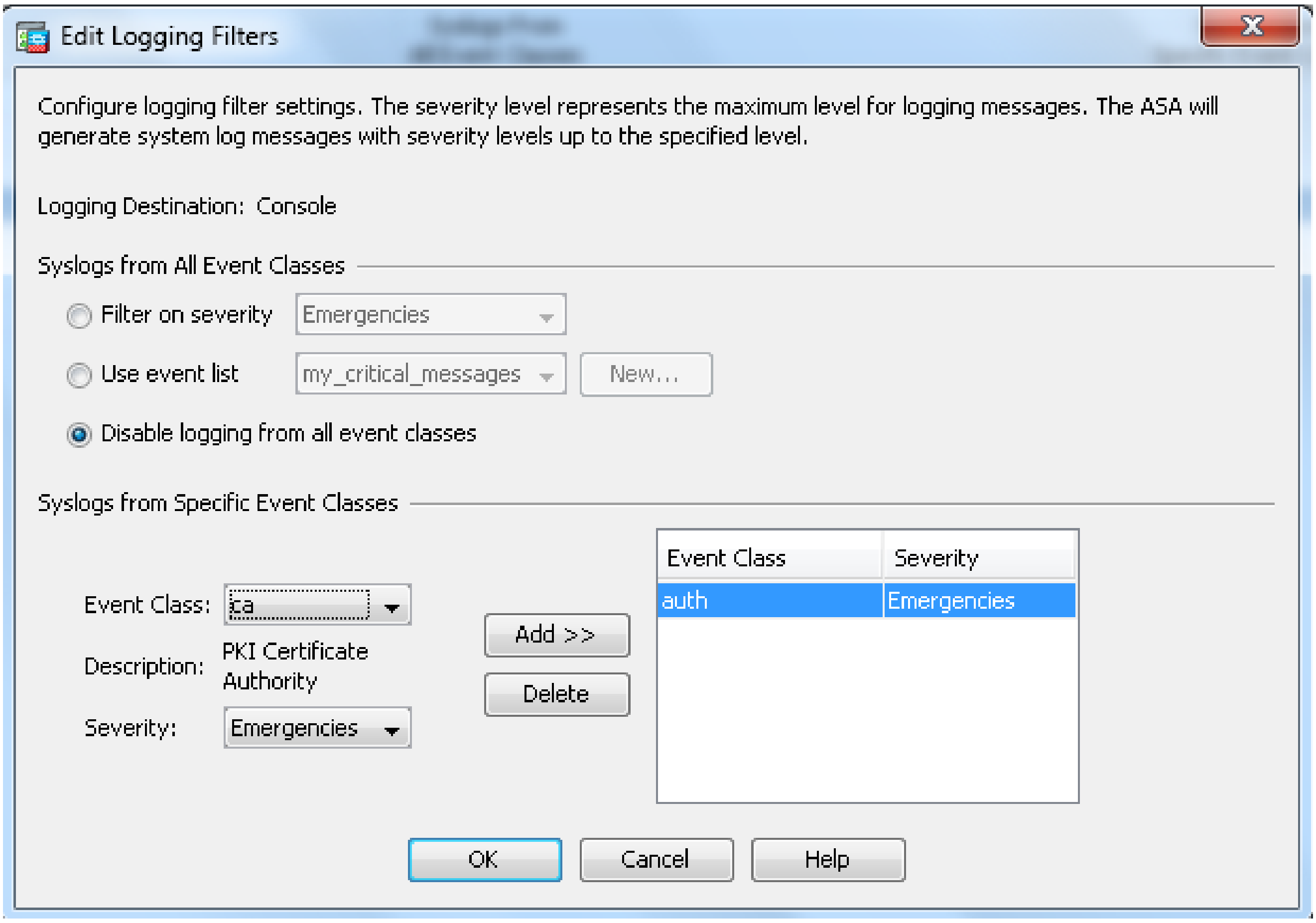
ASDM Configuration

This procedure shows the ASDM configurations for Example 3 with the use of the message list.

1. Choose the **Logging Filters** menu and choose **Console** as the destination.

2. Click **Disable logging from all event classes**.
3. Under the Syslogs from Specific Event Classes, choose the Event Class and Severity you want to add.

   This procedure uses **ca** and **Emergencies** respectively.
4. Click **Add** in order to add this into the message class and click **OK**.



Edit Logging Filters

Configure logging filter settings. The severity level represents the maximum level for logging messages. The ASA will generate system log messages with severity levels up to the specified level.

Logging Destination: Console

Syslogs from All Event Classes

○ Filter on severity: Emergencies

○ Use event list: my_critical_messages

● Disable logging from all event classes

Syslogs from Specific Event Classes

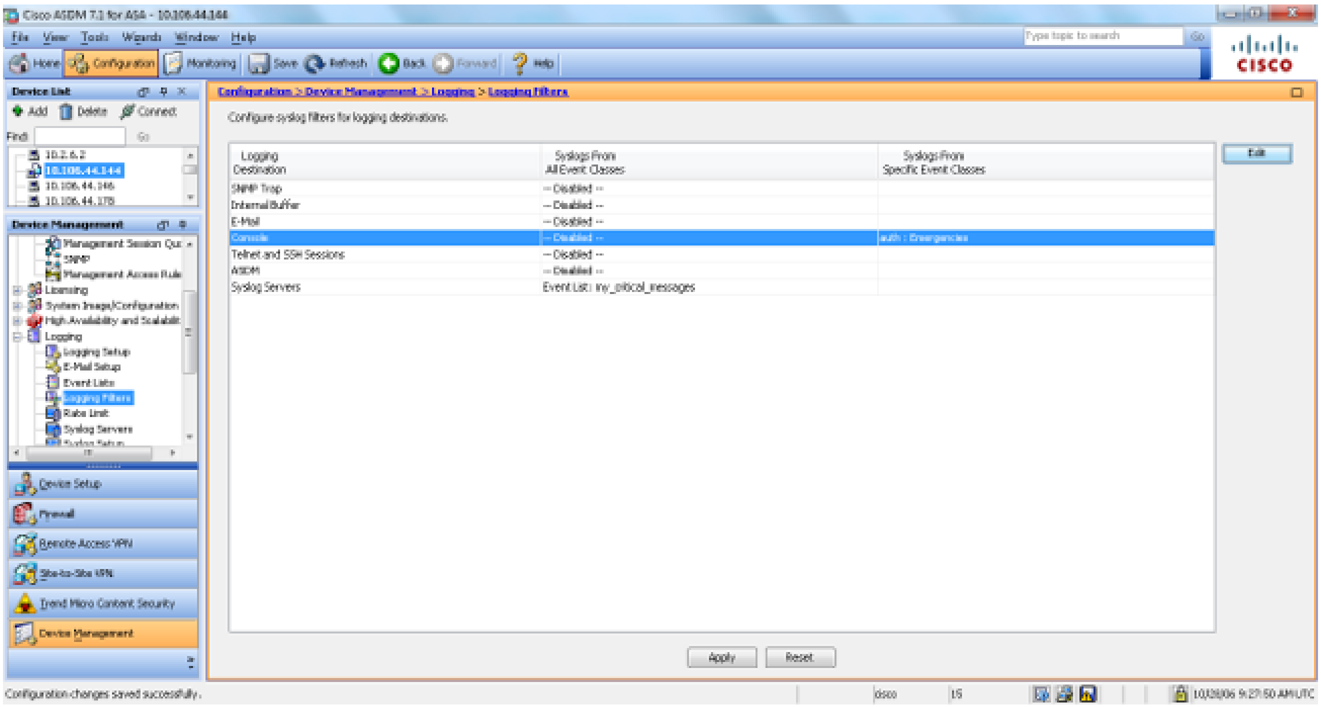
Event Class: ca

Description: PKI Certificate Authority

Severity: Emergencies

Event Class	Severity
auth	Emergencies

5. Click **Apply** after you return to the Logging Filters window. The console now collects the ca class message with severity level Emergencies as shown on the Logging Filters window.



Cisco ASDM 7.1 for ASA - 10.106.44.144
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Device Management
Configuration > Device Management > Logging > Logging Filters
Edit
Apply
Reset

Configure syslog filters for logging destinations.

Logging Destination	Syslogs From All Event Classes	Syslogs From Specific Event Classes
SNMP Trap	-- Disabled --	
Internal Buffer	-- Disabled --	
E-Mail	-- Disabled --	
Console	-- Disabled --	auth : Emergencies
Telnet and SSH Sessions	-- Disabled --	
ASDM	-- Disabled --	
Syslog Servers	Event List: my_critical_messages	

Configuration changes saved successfully.

This completes the ASDM configuration for Example 3. Refer to Messages Listed by Severity Level for a list of the log message severity levels.

Send Debug Log Messages to a Syslog Server

For advanced troubleshooting, feature/protocol specific debug logs are required. By default, these log messages are displayed on terminal (SSH/Telnet). Dependent on the type of debug, and the rate of debug messages generated, use of the CLI can prove difficult if debugs are enabled. Optionally, debug messages can be redirected to the syslog process and generated as syslogs. These syslogs can be sent to any syslog desination as would any other syslog. In order to divert debugs to syslogs, enter the **logging debug-trace** command. This configuration sends debug output, as syslogs, to a syslog server.

```
logging trap debugging
logging debug-trace
logging host inside 172.22.1.5
```

Use of Logging List and Message Classes Together

Enter the **logging list** command in order to capture the syslog for LAN-to-LAN and Remote access IPsec VPN messages alone. This example captures all VPN (IKE and IPsec) class system log messages with debugging level or higher.

Example

<#root>

```
hostname(config)#
```

```
logging enable
```

```
hostname(config)#

logging timestamp


hostname(config)#

logging list my-list level debugging class vpn


hostname(config)#

logging trap my-list


hostname(config)#

logging host inside 192.168.1.1
```

Log ACL Hits

Add **log** to each access list element (ACE) you wish in order to log when an access list is hit. Use this syntax:

<#root>

```
access-list id {deny | permit protocol} {source_addr source_mask}
{destination_addr destination_mask} {operator port} {log}
```

Example

<#root>

```
ASAfirewall(config)#

access-list 101 line 1 extended permit icmp any any log
```

ACLs, by default, log every denied packet. There is no need to add the log option to **deny** ACLs to generate syslogs for denied packets. When the **log** option is specified, it generates syslog message `106100` for the ACE to which it is applied. Syslog message `106100` is generated for every matching permit or deny ACE flow that passes through the ASA Firewall. The first-match flow is cached. Subsequent matches increment the hit count displayed in the **show access-list** command. The default access list logging behavior, which is the **log** keyword not specified, is that if a packet is denied, then message `106023` is generated, and if a packet is permitted, then no syslog message is generated.

An optional syslog level (0 - 7) can be specified for the generated syslog messages (`106100`). If no level is specified, the default level is 6 (informational) for a new ACE. If the ACE already exists, then its current log level remains unchanged. If the **log disable** option is specified, access list logging is completely disabled. No syslog message, which includes message `106023`, is generated. The **log** default option restores the default access list logging behavior.

Complete these steps in order to enable the syslog message `106100` to view in the console output:

1. Enter the **logging enable** command in order to enable transmission of system log messages to all output locations. You must set a logging output location in order to view any logs.

2. Enter the **logging message <message_number> level <severity_level>** command in order to set the severity level of a specific system log message.

   In this case, enter the **logging message 106100** command in order to enable the message `106100`.

3. Enter the **logging console message_list | severity_level** command in order to enable system log messages to display on the Security Appliance console (tty) as they occur. Set the `severity_level` from 1 to 7 or use the level name. You can also specify which messages are sent with the `message_list` variable.

4. Enter the **show logging message** command in order to display a list of system log message messages that have been modified from the default setting, which are messages that have been assigned a different severity level and messages that have been disabled.

   This is sample output of the **show logging message** command:

   <#root>

   ```
   ASAfirewall#
   ```

   ```
   show logging message 106100
   ```

   ```
   syslog 106100: default-level informational (enabled)
   ASAfirewall# %ASA-7-111009: User 'enable_15' executed cmd: show logging mess 106
   100
   ```

Blocking syslog generation on a standby ASA

Start from ASA software release 9.4.1 onwards and you can block specific syslogs from being generated on a standby unit and use this command:

```
no logging message syslog-id standby
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

If you want to suppress a specific syslog message to be sent to syslog server, then you must enter the command as shown.

<#root>

```
hostname(config)#
```

```
no logging message
```

<syslog_id>

Refer to the logging message command for more information.

%ASA-3-201008: Disallowing New Connections

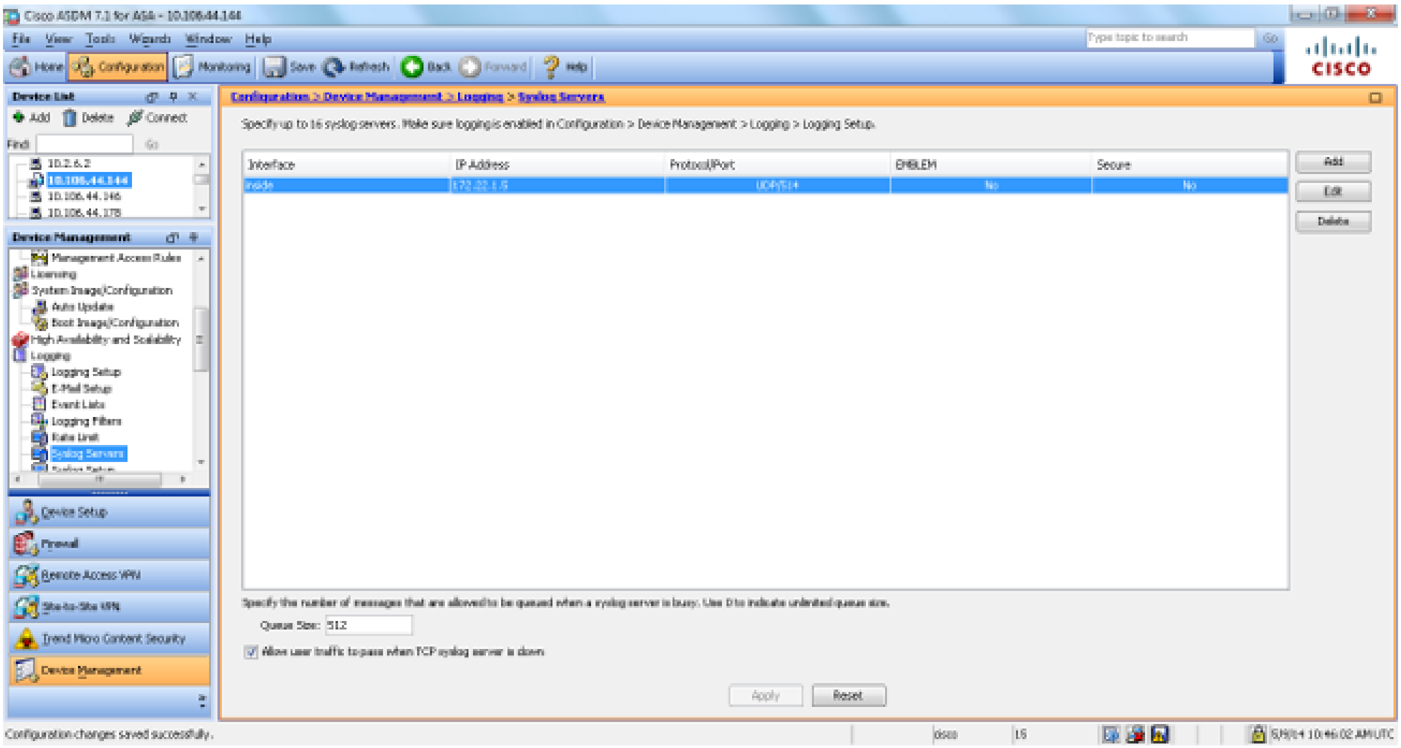
The `%ASA-3-201008: Disallowing new connections.` error message is seen when an ASA is unable to contact the syslog server and no new connections are allowed.

Solution

This message appears when you have enabled TCP system log messaging and the syslog server cannot be reached, or when you use Cisco ASA Syslog Server (PFSS) and the disk on the Windows NT system is full. Complete these steps in order to resolve this error message:

- Disable TCP system log messaging if it is enabled.
- If you use PFSS, free up space on the Windows NT system where PFSS resides.
- Ensure that the syslog server is up and you can ping the host from the Cisco ASA console.
- Restart TCP system message logging in order to allow traffic.

If the syslog server goes down and the TCP logging is configured, either use the logging permit-hostdown command or switch to UDP logging.



Cisco ASDM 7.1 for ASA - 10.106.44.144
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Device Management
Logging Setup
Syslog Servers
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Trend Micro Content Security
Device Management

Configuration > Device Management > Logging > Syslog Servers

Specify up to 16 syslog servers. Make sure logging is enabled in Configuration > Device Management > Logging > Logging Setup.

Interface	IP Address	Protocol/Port	EMBLEM	Secure
inside	172.22.1.5	UDP/514	No	No

Specify the number of messages that are allowed to be queued when a syslog server is busy. Use 0 to indicate unlimited queue size.

Queue Size: 512

☑ Allow user traffic to pass when TCP syslog server is down

Apply Reset

Configuration changes saved successfully.

Related Information

- Cisco Secure PIX Firewall Command References

- **Requests for Comments (RFCs)**
- **Technical Support & Documentation - Cisco Systems**