Configure Logging on FTD via FMC

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configure

- Configure Global Syslog Configuration
  - Logging Setup
  - Basic Logging Setup
  - VPN Logging Settings
  - FTP Server Information (Optional)
  - Flash Size (Optional)
  - Event Lists
  - Rate Limiting Syslog
  - Syslog Settings
- Configure Local Logging
- Configure the External Logging
  - Remote Syslog Server
  - Email Setup for Logging

Verify

Troubleshoot

Related Information

Introduction

This document describes the logging configuration for a FirePOWER Threat Defense (FTD) via Firepower Management Center (FMC).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- FirePOWER technology
- Adaptive Security Appliance (ASA)

- Syslog protocol

Components Used

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

- FMC Version 6.0.1 and later.
- ASA Firepower Threat Defense Image for ASA (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) that runs Software Version 6.0.1 and later.
- ASA Firepower Threat Defense Image for ASA (5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) that runs Software Version 6.0.1 and later.

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.

Background Information

The FTD system logs provide you with information to monitor and troubleshoot the FTD appliance. These logs are useful both in routine troubleshooting and in incident handling. FTD appliance supports both local and external logging.

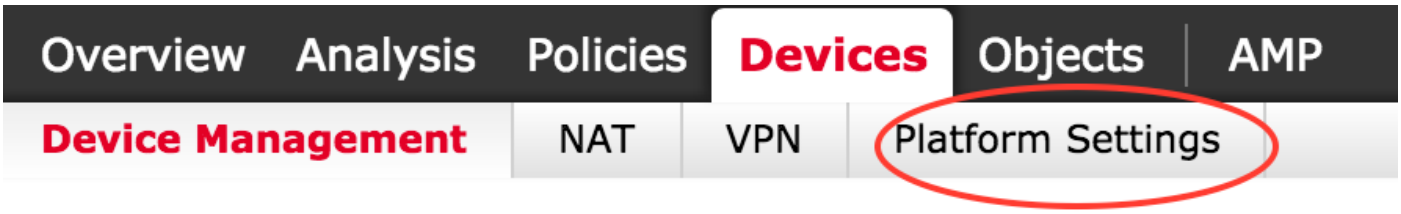
Local logging can help troubleshoot live issues, while external logging is a method of collection of logs from the FTD appliance to an external Syslog server. Logging to a central server helps in aggregation of logs and alerts. External logging can help in log correlation and incident handling.

For local logging, the FTD appliance supports console, internal buffer options, and the Secure Shell (SSH) session logging. For external logging, the FTD appliance supports the external Syslog server and Email Relay Server.

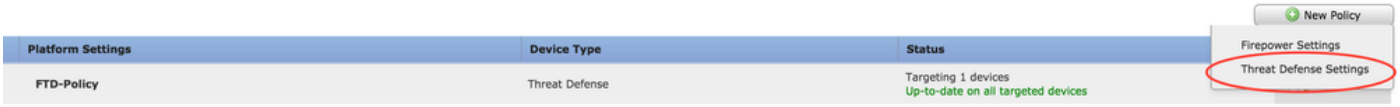
Note: If a high volume of traffic passes through the appliance, pay attention to the type of logging/severity/rate limiting. Do this in order to limit the number of logs, which avoids impact on the firewall.

Configure

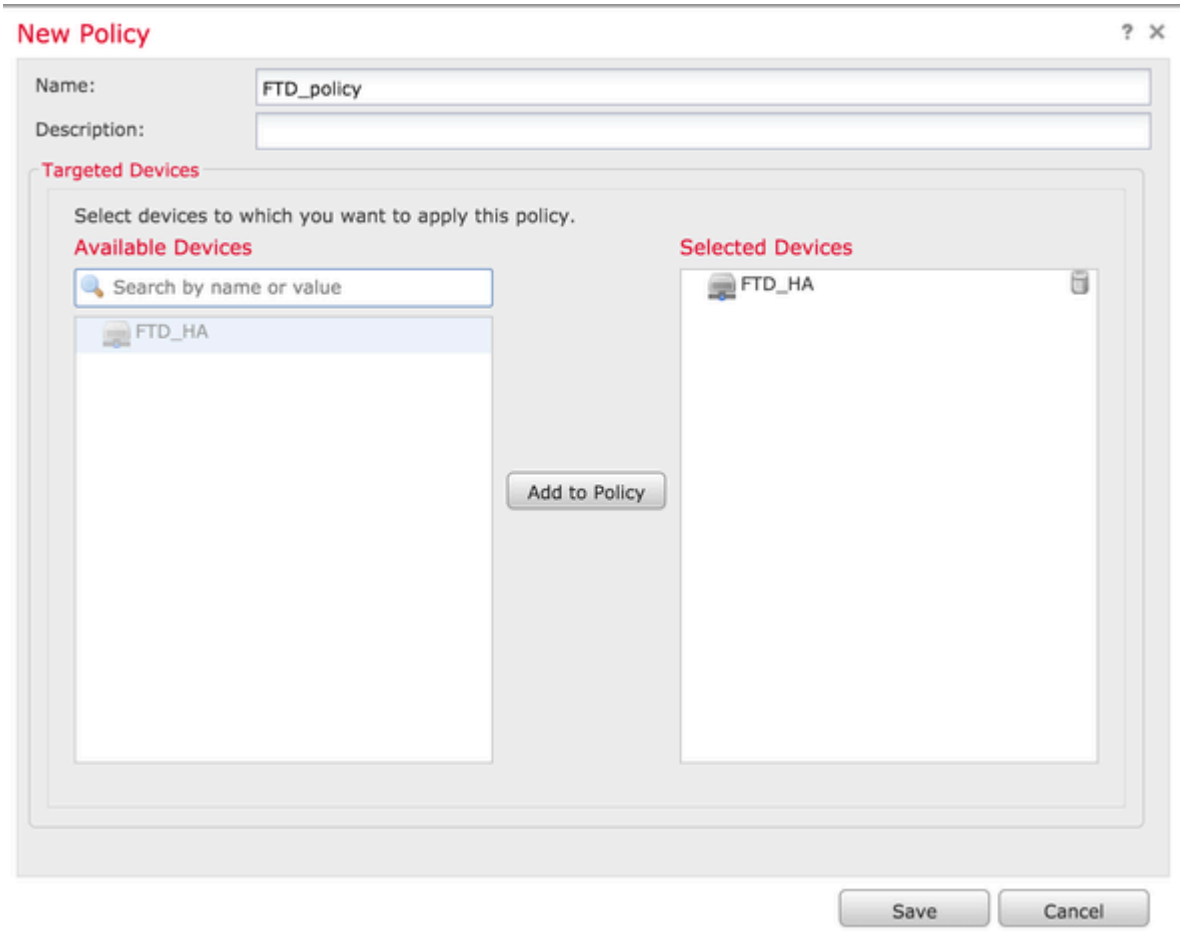
1. All logging related configurations can be configured when you navigate to the **Platform Settings** tab under the **Devices** tab. Choose **Devices > Platform Settings** as shown in this image:



2. Either click the pencil icon to edit the policy that exists or click **New Policy**, and then choose **Threat Defense Settings** to create a new FTD policy:



3. Choose the FTD appliance to apply the policy and click **Save**:



Configure Global Syslog Configuration

There are certain configurations which are applicable for both Local and External logging. This section details the mandatory and optional parameters that can be configured for Syslog.

Logging Setup

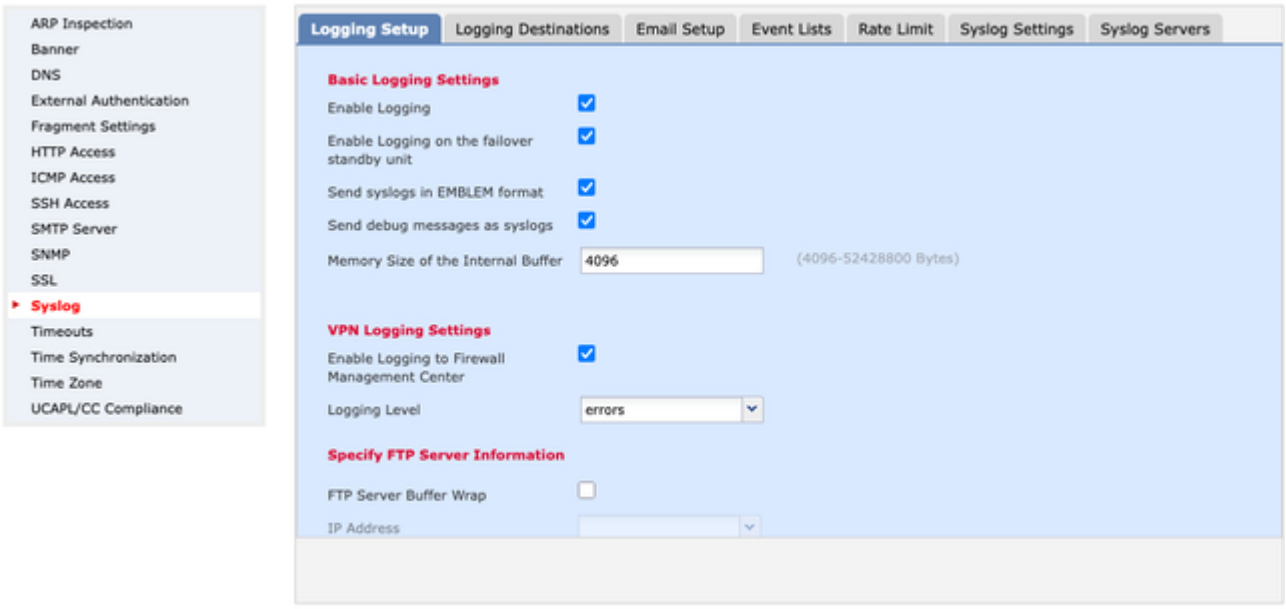
1. Logging setup options are applicable for Local and External logging. To configure the logging setup, choose **Devices > Platform Settings**.

---

2. Choose **Syslog > Logging Setup.**

Basic Logging Setup

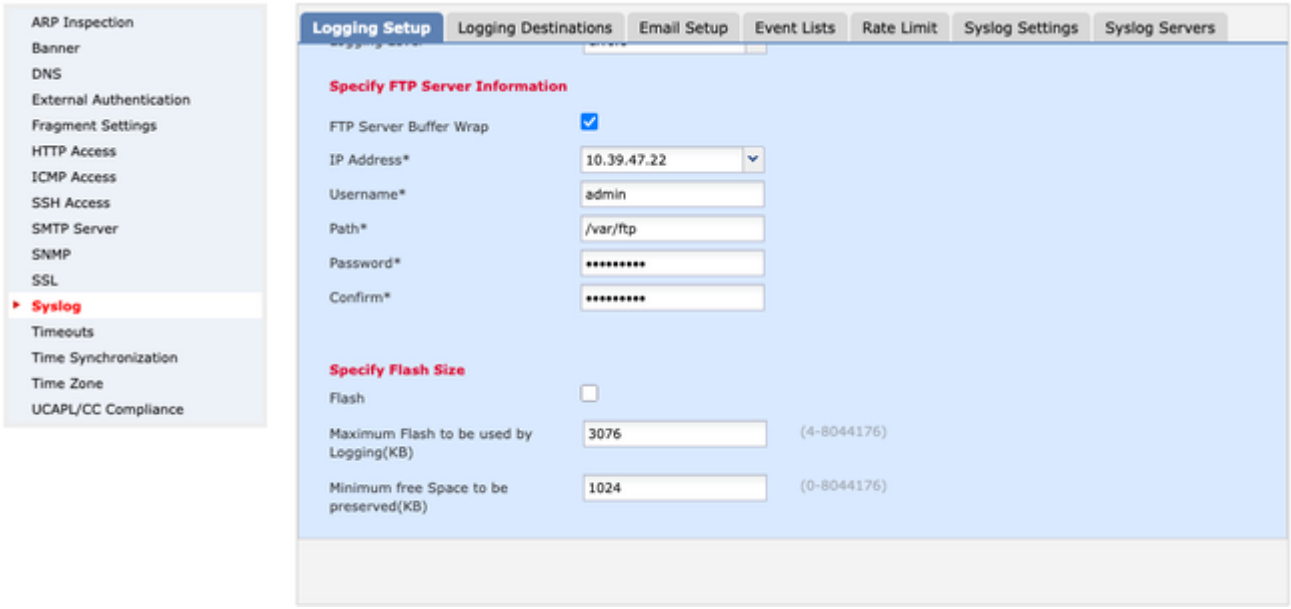
- **Enable Logging**: Check the **Enable Logging** checkbox to enable logging (this is a mandatory option.)
- **Enable Logging on the Failover Standby Unit**: Check the **Enable Logging on the failover standby unit** checkbox to configure logging on the standby FTD, which is part of the FTD High-Availability (HA) cluster.
- **Send Syslogs in EMBLEM Format**: Check the **Send syslogs in EMBLEM format** checkbox to enable the format Syslog as EMBLEM for each destination. The EMBLEM format is used primarily for the CiscoWorks Resource Manager Essentials (RME) Syslog analyzer. This format matches the Cisco IOS Software Syslog format produced by the routers and the switches. It is available only to UDP Syslog servers.
- **Send Debug Messages as Syslogs**: Check the **Send debug messages as syslogs** checkbox to send the debug logs as Syslog messages to the Syslog server.
- **Memory Size of the Internal Buffer**: Enter the internal memory buffer size where FTD can save the log data. The log data is rotated if its buffer limit is reached.



VPN Logging Settings

You can enable logging for VPN troubleshooting syslogs for FTD devices. All VPN syslogs appear with a default severity level of errors or a higher severity (unless changed). You can manage VPN logging through FTD platform settings and the message severity levels can be adjusted by editing the VPN Logging Settings for targeted devices. Setting the VPN logging level to level 4 and more (Warnings, Notifications, Informational or Debugging) can overload the FMC.

Note: When you configure a device with site-to-site or remote access VPN, it automatically enables sending VPN syslogs to the FMC by default.



FTP Server Information (Optional)

Specify FTP server details if you want to send log data to an FTP server before it overwrites the internal buffer.

- **FTP Server Buffer Wrap**: Check the **FTP Server Buffer Wrap** checkbox to send the buffer log data to the FTP server.
- **IP Address**: Enter the IP address of the FTP server.
- **Username**: Enter the username of the FTP server.
- **Path**: Enter the directory path of the FTP server.
- **Password**: Enter the password of the FTP server.
- **Confirm**: Enter the same password again.

Flash Size (Optional)

Specify the flash size to save log data to flash once the internal buffer is full.

- **Flash**: Check the **Flash** checkbox to send log data to the internal flash.
- **Maximum Flash to be used by Logging (KB)**: Enter the maximum size in KB of flash memory to be used for logging.
- **Minimum Free Space to be Preserved (KB)**: Enter the minimum size in KB of the flash memory to be preserved.

Click **Save** to save the platform setting. Choose the **Deploy** option, then select the FTD appliance where you want to apply the changes. Click **Deploy** to start the deployment of the platform setting.

Event Lists

The Configure Event Lists option allows you to create/edit an event list and specify which log data to include in the event list filter. Event Lists can be used when you configure Logging Filters under Logging destinations.

The system allows two options to use the functionality of custom event lists.

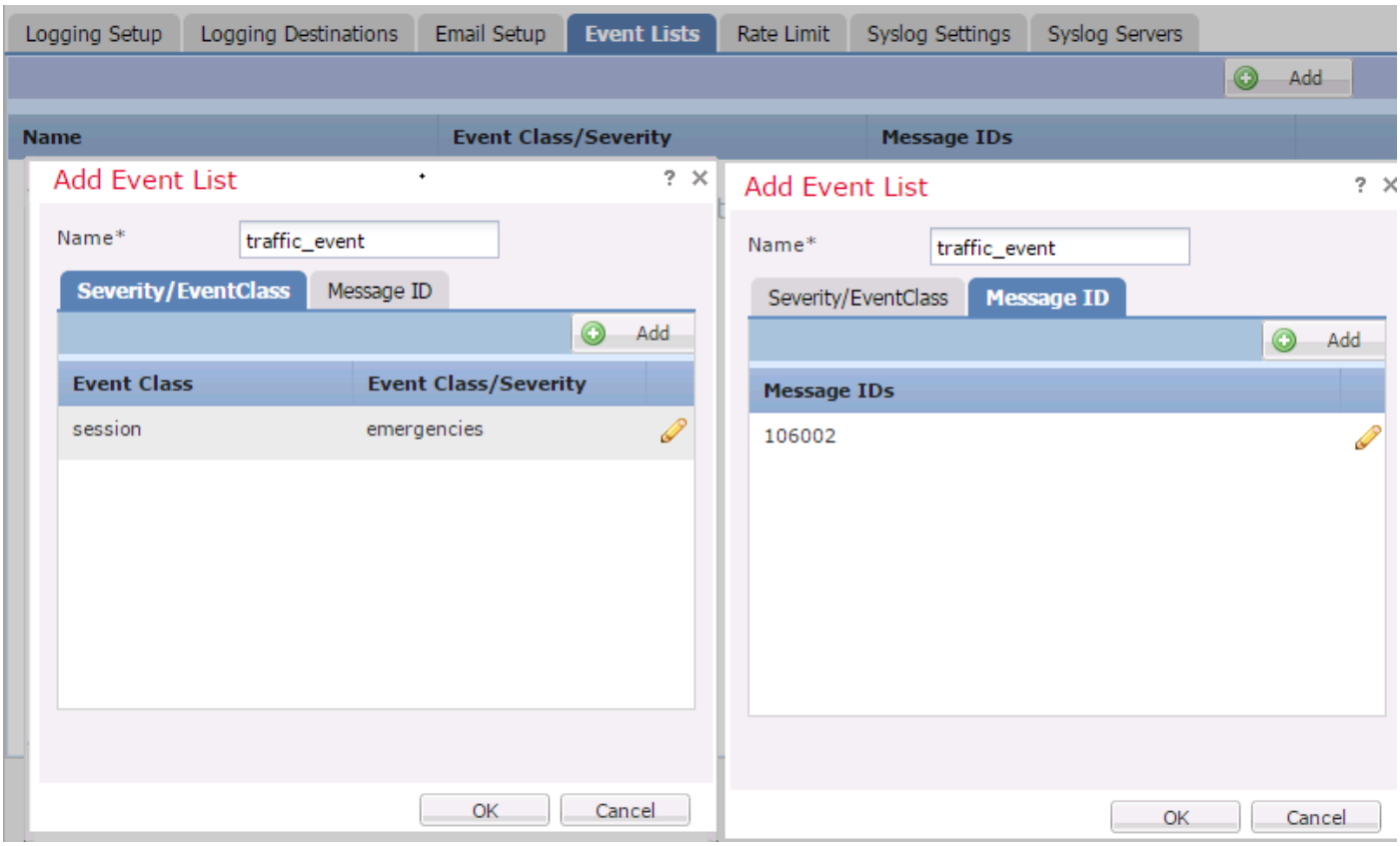
- Class and Severity
- Message ID

---

1. To configure custom event lists, choose **Device > Platform Setting > Threat Defense Policy > Syslog > Event List** and click **Add**. These are the options:

- **Name**: Enter the name of the event list.
- **Severity/Event Class:** In the Severity/Event Class section, click **Add**.
- **Event Class**: Choose the event class from the drop-down list for the type of log data you want. An Event Class defines a set of Syslog rules that represent the same features. For example, there is an Event Class for the session that includes all Syslogs that relate to that session.

- **Syslog Severity**: Choose the severity from the drop-down list for the selected Event Class. The severity can range from 0 (emergency) to 7 (debugging).
- **Message ID**: If you are interested in specific log data related to a message ID, click **Add** to put a filter based on the message ID.
- **Message IDs**: Specify the message ID as an individual/range format.



---

2. Click **OK** to save the configuration.

---

3. Click **Save** to save the platform setting. Choose to **Deploy**, select the FTD appliance where you want to apply the changes. Click **Deploy** to start deployment of the platform setting.

Rate Limiting Syslog

The Rate limit option defines the number of messages that can be sent to all configured destinations and defines the severity of the message you want to assign rate limits.

---

1. To configure rate limits for syslogs, choose **Device > Platform Setting > Threat Defense Policy > Syslog > Rate Limit**. You have two options where you can specify the rate limit:

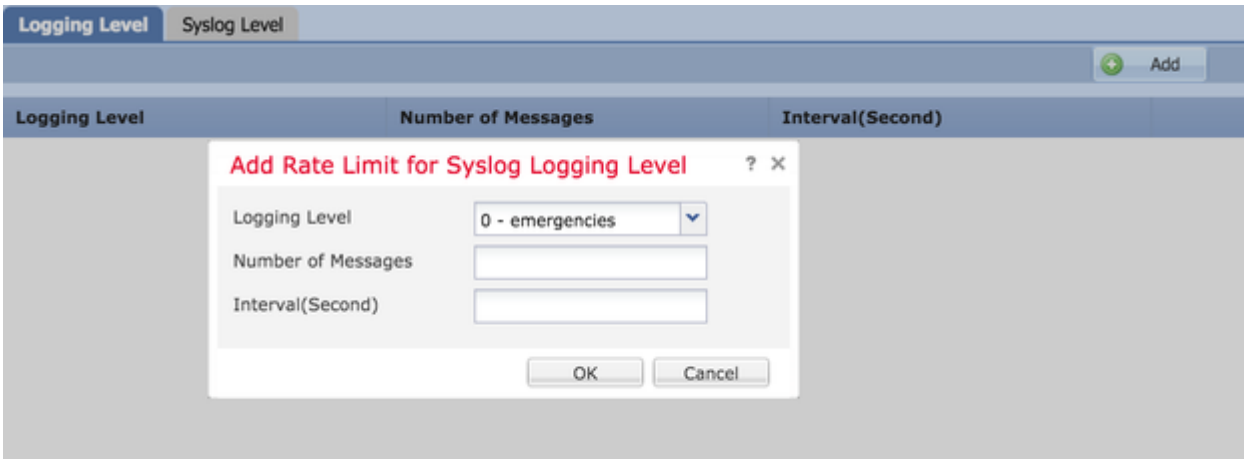
- Logging level
- Syslog levels

---

2. To enable the logging level-based rate limit, choose **Logging Level** and click **Add**.

- **Logging Level**: From the **Logging Level** drop-down list, choose the logging level you want to add rate-limiting.
- **Number of Messages**: Enter the maximum number of Syslog messages to receive within the specified interval.
- **Interval(Second)**: Based on the parameter Number of Messages configured previously, enter the time interval with a fixed set of Syslog messages to be received.

The rate of Syslog is the Number of Messages/Intervals.



---

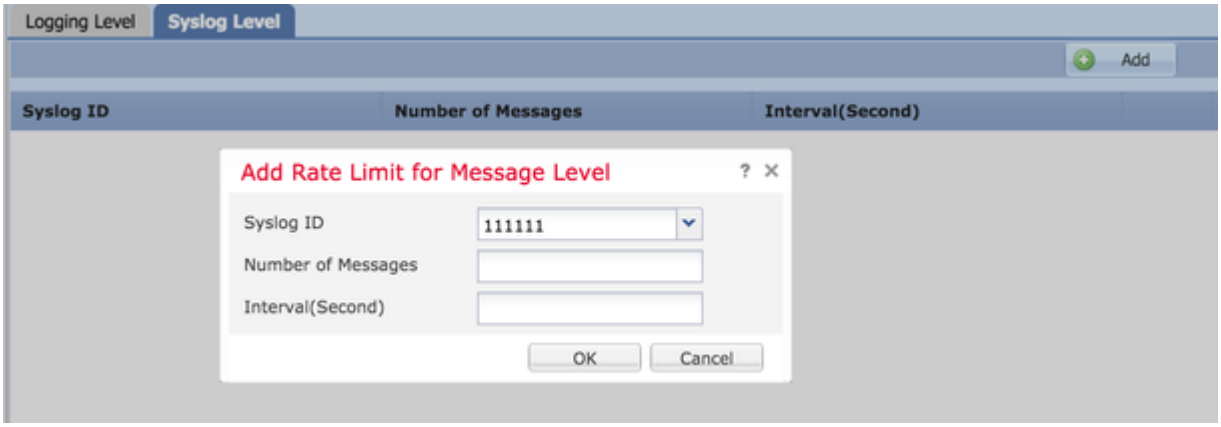
3. Click **OK** to save the logging level configuration.

---

4. To enable the Syslog level based rate limit, choose **Syslog Level** and click **Add**.

- **Syslog ID**: Syslog IDs are used to uniquely identify the Syslog messages. From the **Syslog ID** drop-down list, choose the **Syslog ID**.
- **Number of Messages**: Enter the maximum number of syslog messages to receive within the specified interval.
- **Interval(Second)**: Based on the parameter Number of Messages configured previously, enter the time interval with a fixed set of Syslog messages to be received.

The rate of Syslog is the Number of Messages/Interval.



---

5. Click **OK** in order to save the Syslog level configuration.

---

6. Click **Save** to save the platform setting. Choose to **Deploy**, then select the FTD appliance where you want to apply the changes. Click **Deploy** to start deployment of the platform setting.

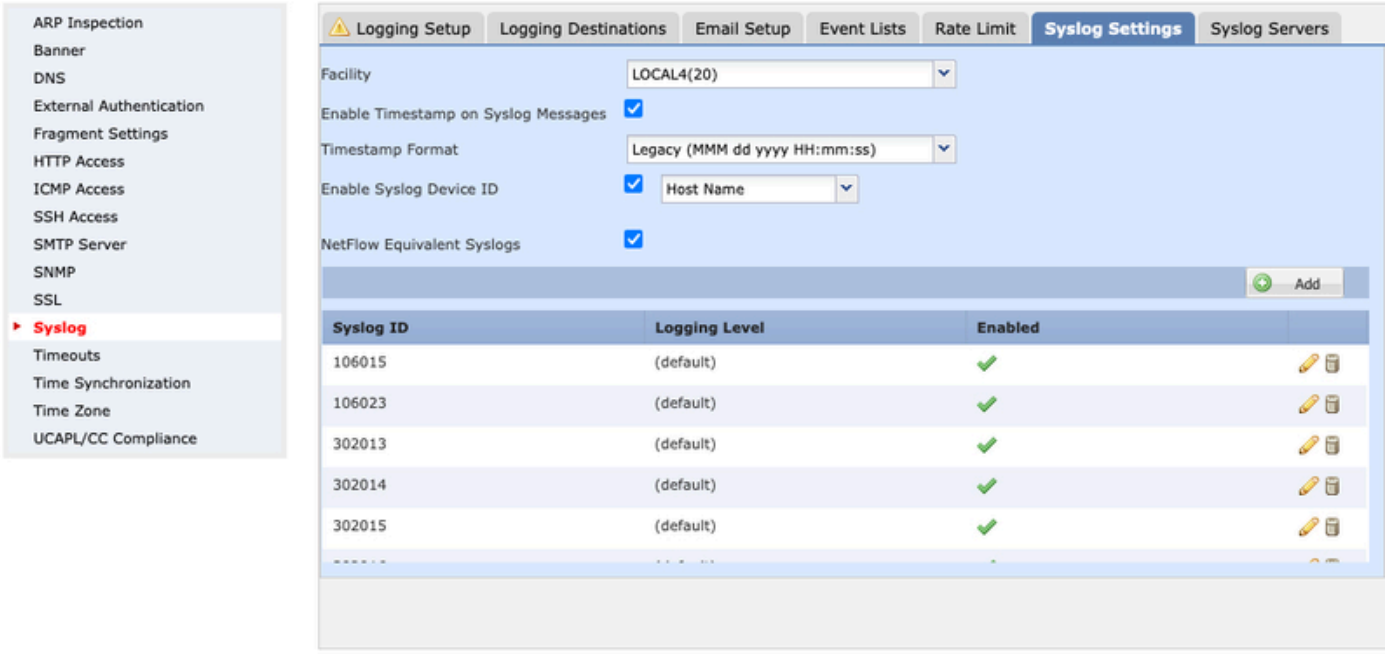
Syslog Settings

Syslog settings allow configuration of the Facility values to be included in the Syslog messages. You can include the timestamp in log messages and other Syslog server-specific parameters.

---

1. To configure custom event lists, choose **Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Settings**.

- **Facility**: A facility code is used to specify the type of program logging the message. Messages with different facilities can be handled differently. From the **Facility** drop-down list, choose the facility value.
- **Enable Timestamp on Syslog Messages**: Check the **Enable Timestamp on Syslog Messages** box to include the time stamp in Syslog messages. You can choose the **Timestamp Format** after enabling this option.
- **Enable Syslog Device ID**: Check the **Enable Syslog Device ID** checkbox to include a device ID in the non-EMBLEM-format Syslog messages.
- **Netflow Equivalent Syslogs**: Check the **Netflow Equivalent Syslogs** checkbox to send NetFlow equivalent Syslogs. It can affect the performance of the appliance.
- **Add Specific Syslog ID**: To specify the additional Syslog ID, click **Add** and specify the **Syslog ID/ Logging Level** checkbox.



---

2. Click **Save** to save the platform setting. Choose to **Deploy**, then select the FTD appliance where you want to apply the changes. Click **Deploy** to start deployment of the platform setting.

Configure Local Logging

The Logging Destination section can be used to configure logging to specific destinations.

The available internal logging destinations are:

- **Internal Buffer**: Logs to the internal logging buffer (logging buffered).
- **Console**: Sends logs to the console (logging console).
- **SSH Sessions**: Logs Syslog to SSH sessions (terminal monitor).

There are three steps to configure Local Logging.

1. Choose **Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations**.

---

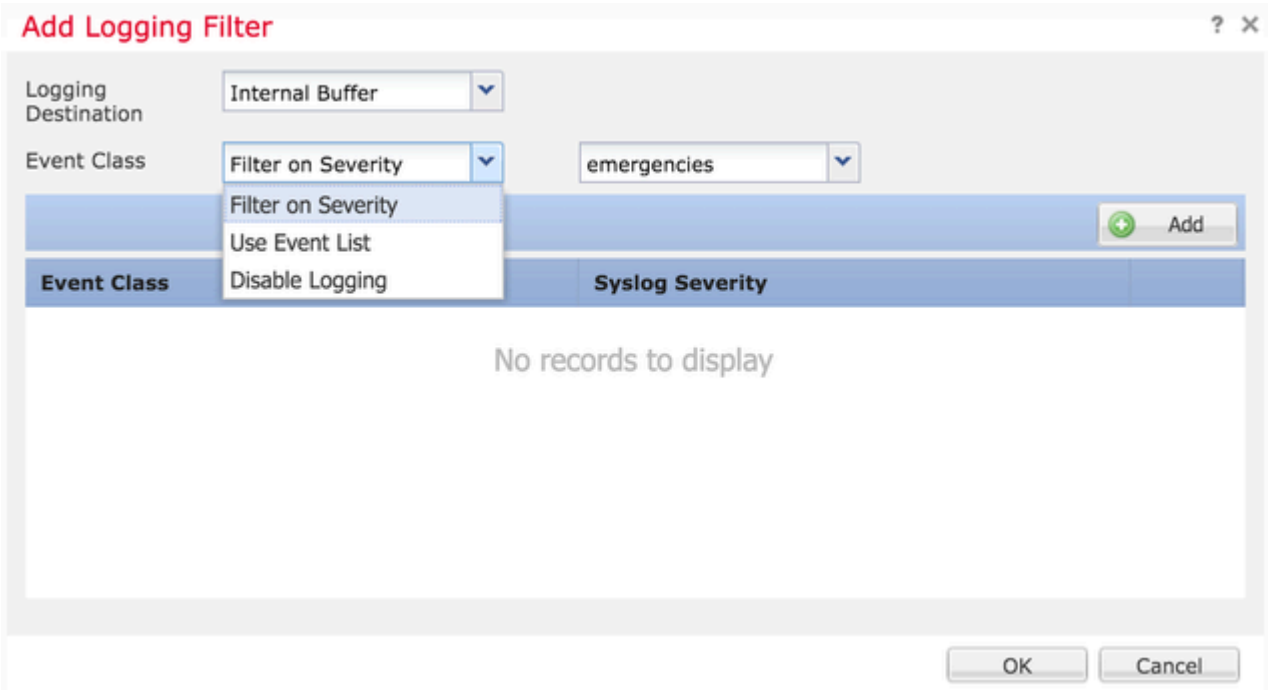
2. Click **Add** to add a Logging Filter for a specific **logging destination.**

3. **Logging Destination**: Choose the required logging destination from the **Logging Destination** drop-down list as Internal Buffer, Console, or SSH sessions.

Event Class: From the **Event Class** drop-down list, choose an Event class. Event Classes are a set of Syslogs that represent the same features. Event classes can be selected in three ways:

- **Filter on Severity**: Event Classes filter based on the severity of the Syslogs.
- **User Event List**: Administrators can create specific Event Lists with their own custom event classes and reference them in this section.
- **Disable Logging**: Use this option to disable logging for the chosen Logging Destination and Logging Level.

Logging Level: Choose the logging level from the drop-down list. The logging level range is from 0 (Emergencies) to 7 (debugging).

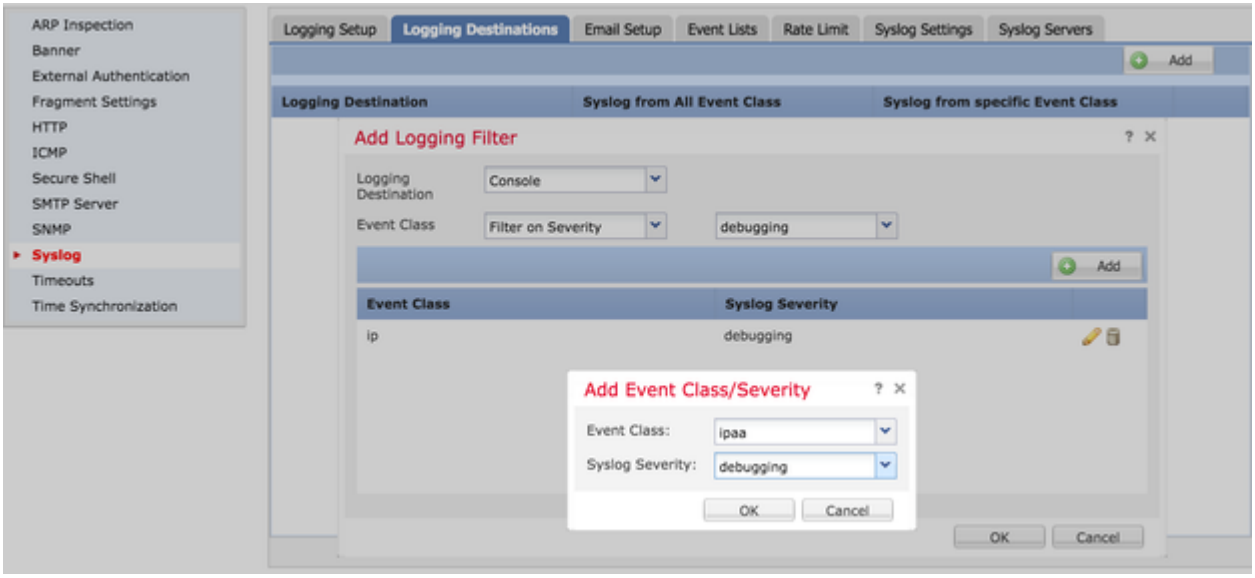


---

4. To add a separate Event class to this Logging filter, click **Add**.

Event Class: Choose the Event Class from the **Event Class** drop-down list.

Syslog Severity: Choose the Syslog severity from the **Syslog Severity** drop-down list.



---

5. Click **OK** once the filter is configured to add the filter for a specific logging destination.

---

6. Click **Save** to save the platform setting. Choose **Deploy**, choose the FTD appliance where you want to apply the changes. Click **Deploy** to start deployment of the platform setting.

Configure the External Logging

To configure external logging, choose **Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations**.

FTD supports these types of external logging.

- **Syslog Server**: Sends logs to the remote Syslog server.
- **SNMP Trap**: Sends logs out as an SNMP trap.
- **E-Mail**: Sends logs via email with a pre-configured mail relay server.

The configuration for the external logging and internal logging are the same. The selection of logging destinations decides the type of logging that is implemented. It is possible to configure Event Classes based on Custom Event lists to the remote server.

Remote Syslog Server

Syslog servers can be configured to analyze and store logs remotely from the FTD. There are three steps to

configure remote Syslog servers.

1. Choose **Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Servers**.

---

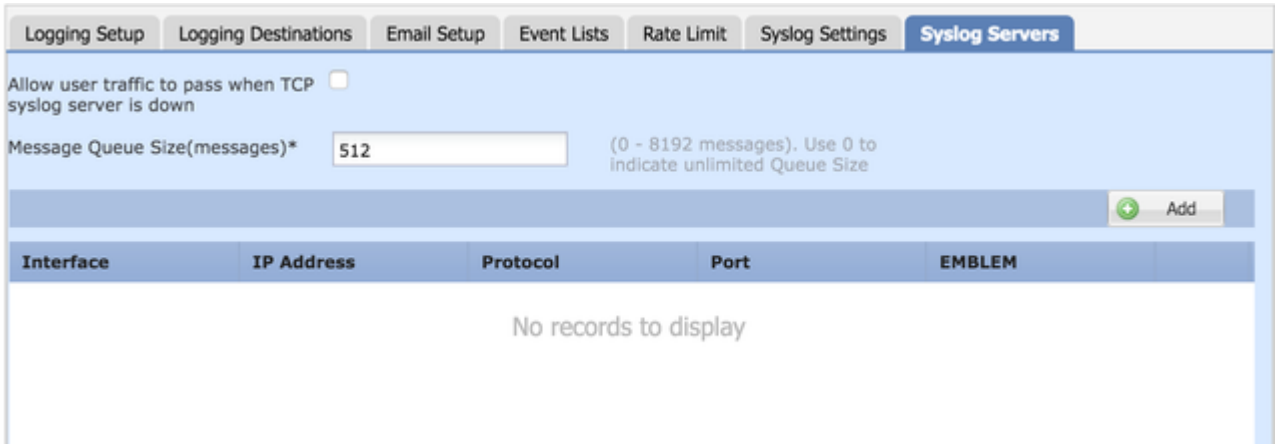
2. Configure the Syslog server related parameter.

---

3. Allow user traffic to pass when the TCP syslog server is down. If a TCP Syslog server has been deployed in the network and it is not reachable, the network traffic through the ASA is denied. This is applicable only when the transport protocol between the ASA and the Syslog server is TCP. Check the **Allow user traffic to pass when TCP syslog server is down** checkbox to allow traffic to pass through the interface when the Syslog server is down.

---

4. **Message Queue Size**: The message queue size is the number of messages that queues in the FTD when the remote Syslog server is busy and does not accept any log messages. The default is 512 messages and the minimum is 1 message. If 0 is specified in this option, the queue size is considered to be unlimited.



---

5. To add remote Syslog servers, click **Add**.

IP Address: From the **IP Address** drop-down list, choose a network object which has the Syslog servers listed. If you have not created a network object, click the plus (+) icon to create a new object.

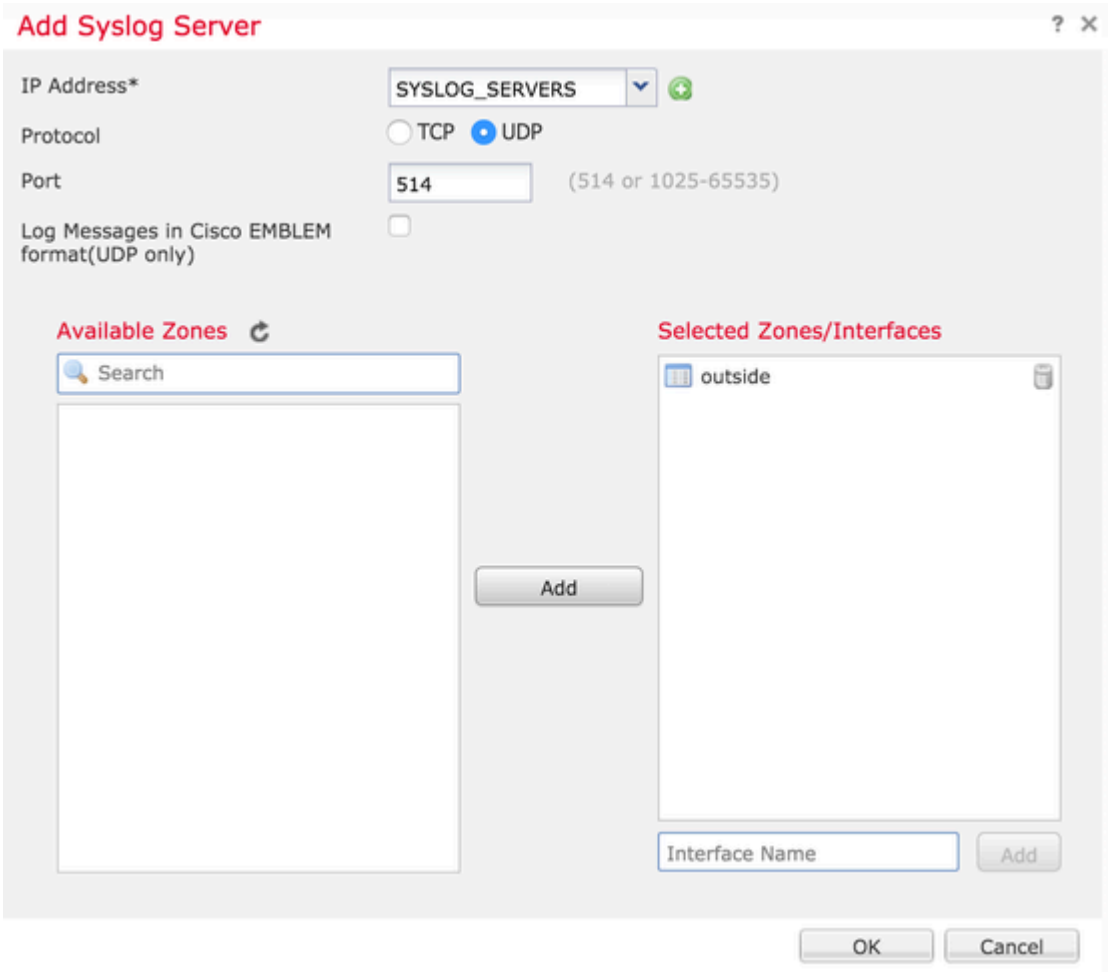
Protocol: Click either the **TCP** or **UDP** radio button for Syslog communication.

Port: Enter the Syslog server port number. By default, it is 514.

Log Messages in Cisco EMBLEM format(UDP only): Click the **Log Messages in Cisco EMBLEM format (UDP only)** checkbox to enable this option. If it is required to log messages in the Cisco EMBLEM

format (this is applicable for UDP-based Syslog only.)

Available Zones: Enter the security zones over which the Syslog server is reachable and move it to the Selected Zones/Interfaces column.



---

6. Click **OK** and **Save** to save the configuration.

---

7. Click **Save** to save the platform setting. Choose **Deploy** and select the FTD appliance where you want to apply the changes. Click **Deploy** to start deployment of the platform setting.

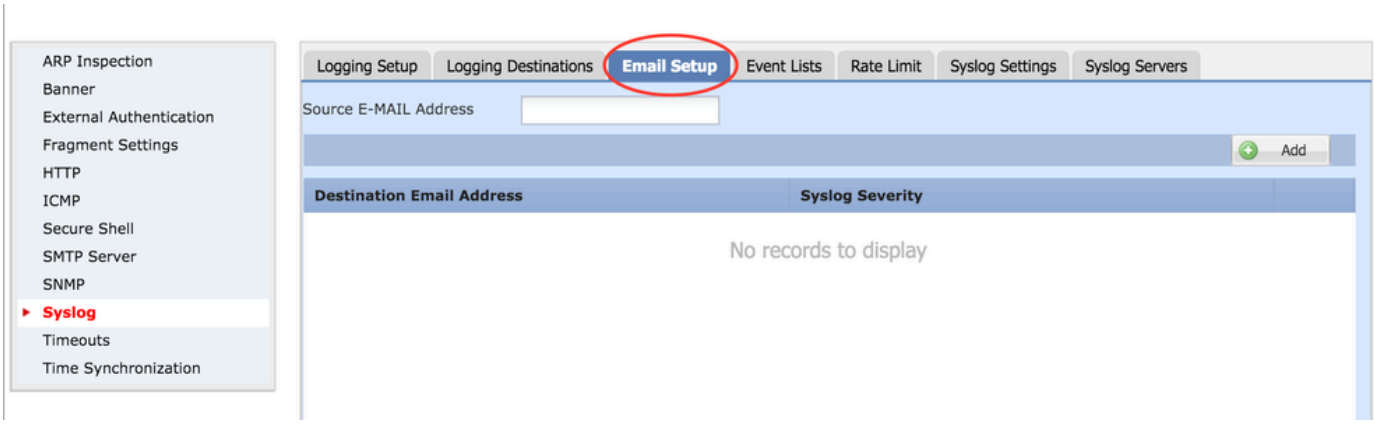
Email Setup for Logging

FTD allows you to send the Syslog to a specific email address. Email can be used as a logging destination only if an email relay server has already been configured.

There are two steps to configure email settings for the Syslogs.

1. Choose **Device > Platform Setting > Threat Defense Policy > Syslog >Email Setup**.

Source E-mail Address: Enter the source email address that appears on all emails sent from FTD that contains the Syslogs.

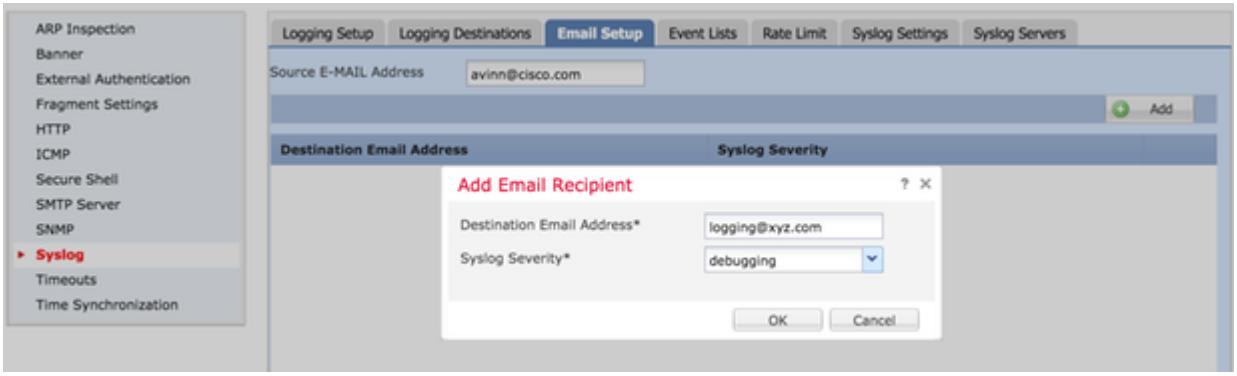


---

2. To configure the destination email address and the Syslog severity, click **Add**.

Destination Email Address: Enter the destination email address where Syslog messages are sent.

Syslog Severity: Choose the Syslog severity from the **Syslog Severity** drop-down list.



---

3. Click **OK** to save the configuration.

---

4. Click **Save** to save the platform setting. Choose **Deploy**, then select the FTD appliance where you want to apply the changes. Click **Deploy** to start deployment of the platform setting.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Verify the FTD Syslog configuration in the FTD CLI. Log in to the management interface of the FTD, and run the **system support diagnostic-cli** command to console into the diagnostic CLI.

```
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

><Press Enter>
firepower# sh run logging
logging enable
logging console emergencies
logging buffered debugging
logging host inside 192.168.0.192
logging flash-minimum-free 1024
logging flash-maximum-allocation 3076
logging permit-hostdown
```

Ensure the Syslog server is reachable from the FTD. Log in to the FTD management interface via SSH and verify the connectivity with the **ping** command.

```
Copyright 2004-2016, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.
Cisco Fire Linux OS v6.0.1 (build 37)
Cisco Firepower Threat Defense for VMWare v6.0.1 (build 1213)

> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> en
Password:
firepower# ping 192.168.0.192
```

You can take a packet capture to verify the connectivity between the FTD and the Syslog server. Log in to

the FTD management interface via SSH and run the **system support diagnostic-cli** command. For the packet capture commands, refer to ASA Packet Captures with CLI and ASDM Configuration Example.

Ensure that the policy deployment is applied successfully.

Related Information

- Technical Support & Documentation - Cisco Systems