

Configuración del inicio de sesión en FTD mediante el FMC

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Configuración de Syslog global](#)

[Configuración de registros](#)

[Listas de eventos](#)

[Registro del sistema de limitación de velocidad](#)

[Configuración de Syslog](#)

[Configurar registro local](#)

[Configuración del registro externo](#)

[Servidor Syslog remoto](#)

[Configuración de correo electrónico para registro](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

En este documento se describe la configuración de registro para Firepower Threat Defense (FTD) a través del centro de administración Firepower (FMC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Tecnología FirePOWER
- Dispositivo de seguridad adaptable (ASA)
- protocolo Syslog

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Imagen de defensa frente a amenazas ASA Firepower para ASA (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) que ejecuta la versión de software 6.0.1 y posteriores
- Imagen de defensa frente a amenazas ASA Firepower para ASA (5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) que ejecuta la versión de software 6.0.1 y posteriores
- FMC versión 6.0.1 y posteriores

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Los registros del sistema FTD le proporcionan la información necesaria para supervisar y solucionar los problemas del dispositivo FTD.


Los registros son útiles tanto en la resolución de problemas rutinaria como en la gestión de incidentes. El dispositivo FTD admite el registro local y externo.

El registro local puede ayudarle a solucionar los problemas en directo. El registro externo es un método de recolección de registros desde el dispositivo FTD a un servidor Syslog externo.

El registro en un servidor central ayuda en la agregación de registros y alertas. El registro externo puede ayudar en la correlación de registros y la gestión de incidentes.

Para el registro local, el dispositivo FTD admite la consola, la opción de búfer interno y el registro de sesiones de Secure Shell (SSH).

Para el registro externo, el dispositivo FTD admite el servidor Syslog externo y el servidor de retransmisión de correo electrónico.

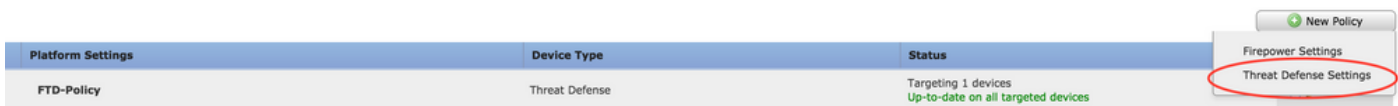
 Nota: Si el dispositivo atraviesa un gran volumen de tráfico, preste atención al tipo de registro/gravedad/límite de velocidad. Haga esto para limitar el número de registros, lo que evita el impacto en el firewall.

Configurar

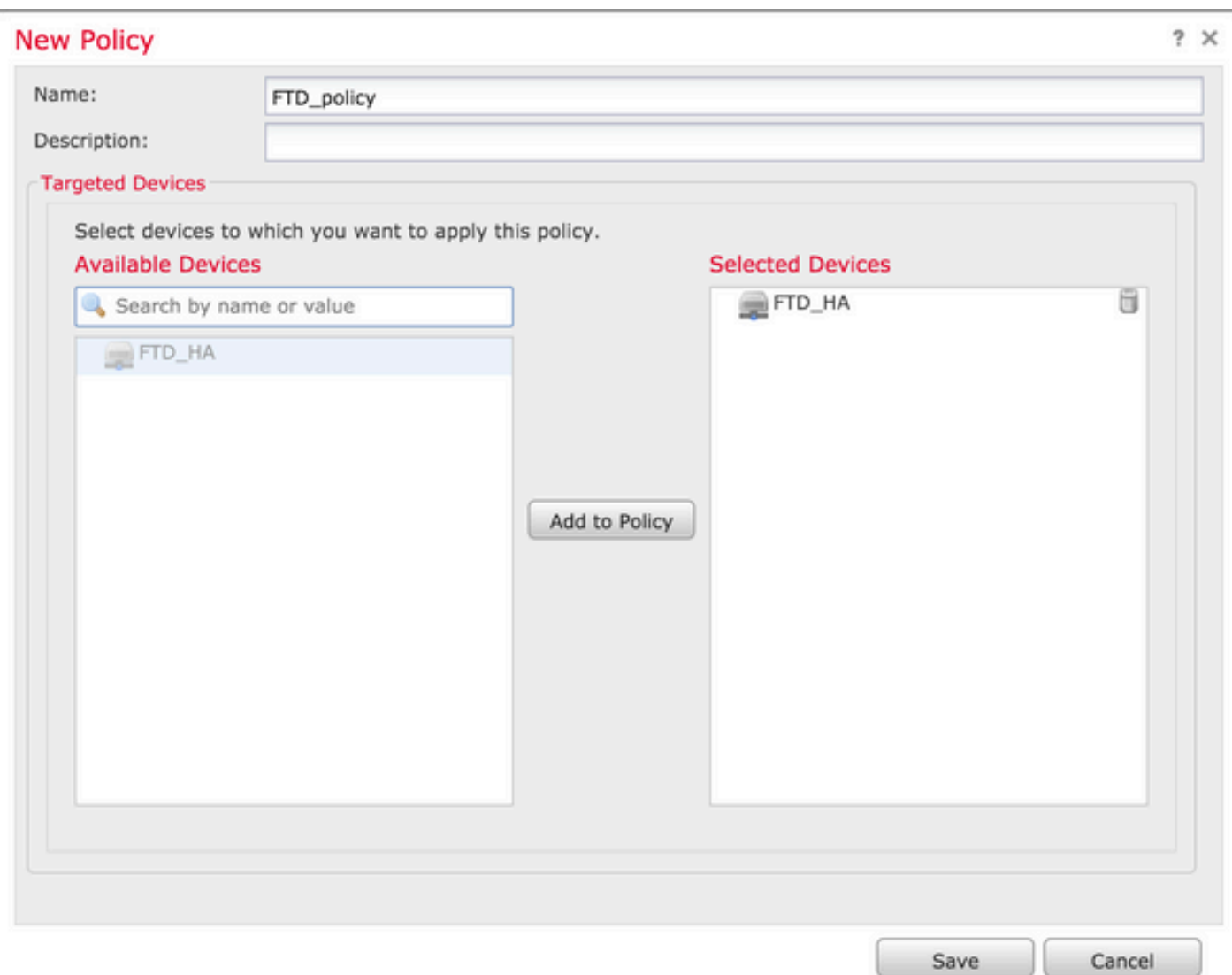
Todas las configuraciones relacionadas con el registro se pueden configurar al desplazarse a la [Platform Settings](#) debajo de la ficha [Devices](#) ficha. Elegir [Devices](#) > [Platform Settings](#) como se muestra en esta imagen.



Haga clic en el icono del lápiz para editar la política que existe o haga clic en **New Policy**, a continuación, elija **Threat Defense Settings** para crear una nueva política de FTD como se muestra en esta imagen.



Elija el dispositivo FTD para aplicar esta política y haga clic en **save** como se muestra en esta imagen.



Configuración de Syslog global

Existen ciertas configuraciones que son aplicables para el registro local y externo. Esta sección trata sobre los parámetros obligatorios y opcionales que se pueden configurar para Syslog.

Configuración de registros

Las opciones de configuración de registro se aplican al registro local y externo. Para configurar la configuración de registro, elija **Devices > Platform Settings**.

Elegir **Syslog > Logging Setup**.

Configuración básica de registro

- **Enable Logging**: consulte la **Enable Logging** para habilitar el registro. Esta es una opción obligatoria.
- **Enable Logging on the failover standby unit**: consulte la **Enable Logging on the failover standby unit** para configurar el registro en el FTD en espera que forma parte de un clúster de alta disponibilidad de FTD.
- **Send syslogs in EMBLEM format**: consulte la **Send syslogs in EMBLEM format** para habilitar el formato de Syslog como LOGOTIPO para cada destino. El formato EMBLEM se utiliza principalmente para el analizador Syslog de CiscoWorks Resource Manager Essentials (RME). Este formato coincide con el formato Syslog del software del IOS de Cisco producido por los routers y los switches. Sólo está disponible para servidores UDP Syslog.
- **Send debug messages as syslogs**: consulte la **Send debug messages as syslogs** para enviar los registros de depuración como mensajes Syslog al servidor Syslog.
- **Memory size of the Internal Buffer**: introduzca el tamaño del búfer de memoria interna en el que el FTD puede guardar los datos de registro. Los datos del registro giran si se alcanza el límite del búfer.

Información del servidor FTP (opcional)

Especifique los detalles del servidor FTP si desea enviar los datos de registro al servidor FTP antes de que sobrescriba el búfer interno.

- **FTP Server Buffer Wrap**: consulte la **FTP Server Buffer Wrap** para enviar los datos del registro del búfer al servidor FTP.
- **IP Address**: introduzca la dirección IP del servidor FTP.
- **Username**: Introduzca el nombre de usuario del servidor FTP.
- **Path**: introduzca la ruta del directorio del servidor FTP.
- **Password**: introduzca la contraseña del servidor FTP.
- **Confirm**: vuelva a introducir la misma contraseña.

Tamaño de flash (opcional)

Especifique el tamaño de flash si desea guardar los datos de registro en flash una vez que el búfer interno esté lleno.

- **Flash**: consulte la **Flash** para enviar los datos del registro a la memoria flash interna.
- **Maximum Flash to be used by Logging(KB)**: introduzca el tamaño máximo en KB de memoria flash que se puede utilizar para el registro.
- **Minimum free Space to be preserved(KB)**: introduzca el tamaño mínimo en KB de la memoria flash que

debe conservarse.

Haga clic en **Save** para guardar la configuración de la plataforma. Elija el **Deploy** seleccione el dispositivo FTD en el que desea aplicar los cambios y haga clic en **Deploy** para iniciar la implementación de la configuración de la plataforma.

Listas de eventos

La opción Configurar listas de eventos le permite crear/editar una lista de eventos y especificar qué datos de registro incluir en el filtro de lista de eventos. Las listas de eventos se pueden utilizar al configurar los filtros de registro en Destinos de registro.

El sistema permite dos opciones para utilizar la funcionalidad de las listas de eventos personalizadas.

- Clase y gravedad
- ID del mensaje

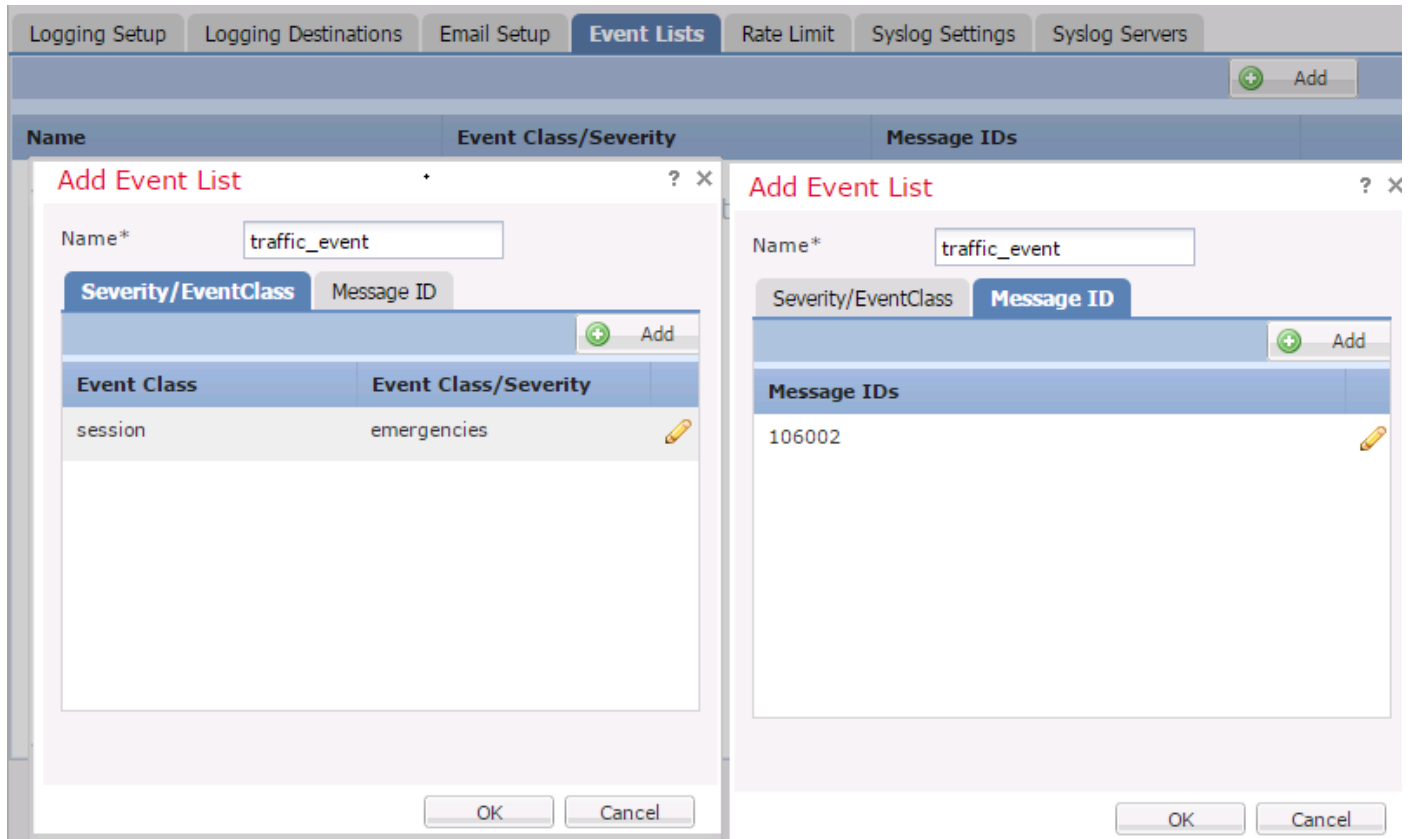
Para configurar listas de eventos personalizadas, elija **Device > Platform Setting > Threat Defense Policy > Syslog > Event List** y haga clic en **Add**. Estas son las opciones:

- **Name:** introduzca el nombre de la lista de eventos.
- **Severity/Event Class:** en la sección Gravedad/Clase de evento, haga clic en **Add**.
- **Event Class:** elija la clase de evento de la lista desplegable para el tipo de datos de registro que desee. Una clase de evento define un conjunto de reglas de Syslog que representan las mismas características.

Por ejemplo, hay una clase de evento para la sesión que incluye todos los registros del sistema

relacionados con la sesión.

- Syslog Severity: elija la gravedad en la lista desplegable para la clase de evento seleccionada. La gravedad puede oscilar entre 0 (emergencia) y 7 (depuración).
- Message ID: si está interesado en datos de registro específicos relacionados con una ID de mensaje, haga clic en **Add** para colocar un filtro basado en el ID del mensaje.
- Message IDs: especifique el ID del mensaje como formato individual/ de rango.



Haga clic en **OK** para guardar la configuración.

Haga clic en **Save** para guardar la configuración de la plataforma. Elija entre **Deploy**, seleccione el dispositivo FTD donde desea aplicar los cambios y haga clic en **Deploy** para iniciar la implementación de la configuración de la plataforma.

Registro del sistema de limitación de velocidad

La opción de límite de velocidad define el número de mensajes que se pueden enviar a todos los destinos configurados y define la gravedad del mensaje al que desea asignar límites de velocidad.

Para configurar listas de eventos personalizadas, elija **Device > Platform Setting > Threat Defense Policy > Syslog > Rate Limit**. Dispone de dos opciones en función de las cuales puede especificar el límite de velocidad:

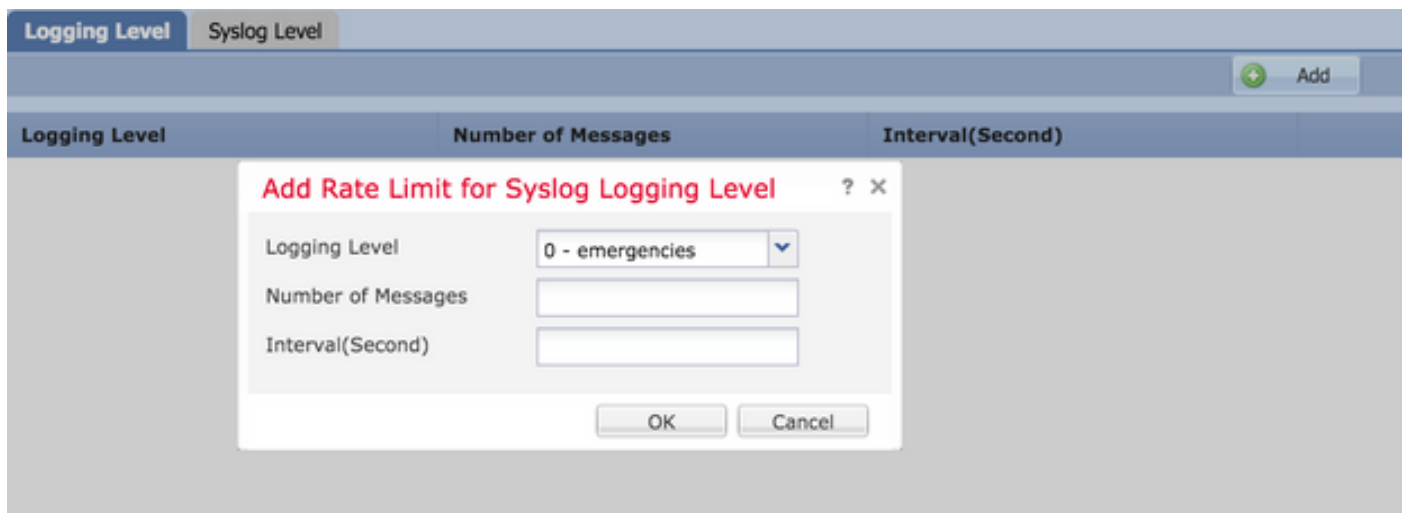
- Nivel de Registro
- Niveles de Syslog

Para habilitar el límite de velocidad basado en el nivel de registro, elija **Logging Level** y haga clic en

Add.

- **Logging Level:** Desde **Logging Level** , seleccione el nivel de registro para el que desea realizar la limitación de velocidad.
- **Number of Messages:** introduzca el número máximo de mensajes de Syslog que se recibirán dentro del intervalo especificado.
- **Interval(Second):** en función del parámetro Número de mensajes configurado anteriormente, introduzca el intervalo de tiempo en el que se puede recibir un conjunto fijo de mensajes Syslog.

La velocidad de Syslog es el número de mensajes/intervalos.

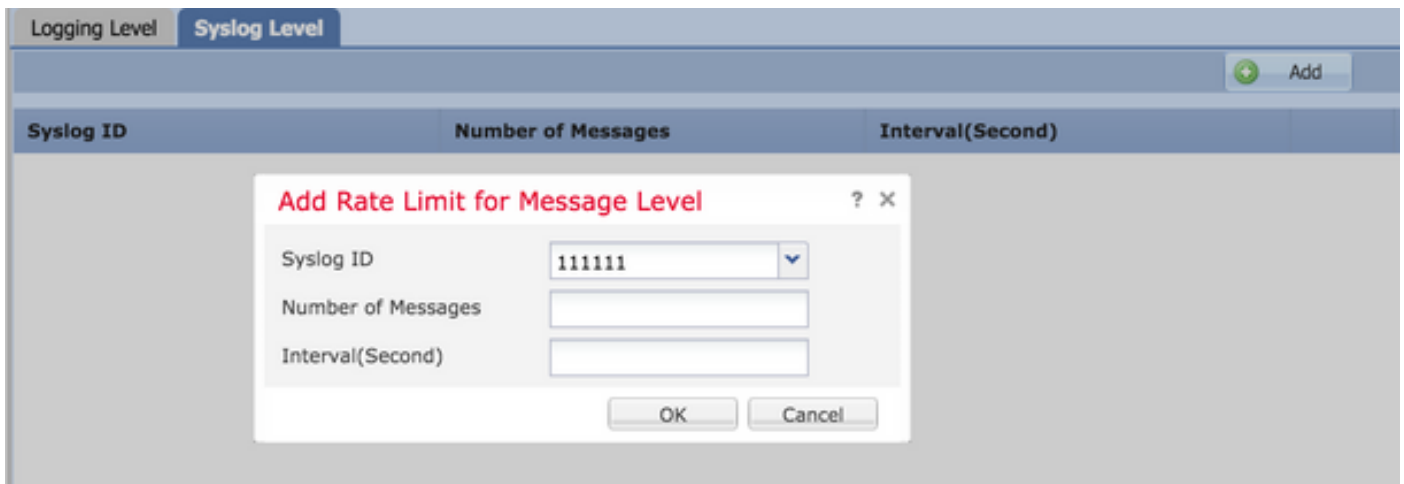


Haga clic en **OK** para guardar la configuración del nivel de registro.

Para habilitar el límite de velocidad basado en el nivel de registro, elija **Logging Level** y haga clic en **Add**.

- **Syslog ID:** los ID de Syslog se utilizan para identificar de forma única los mensajes de Syslog. Desde **Syslog ID** , seleccione la ID de Syslog.
- **Number of Messages:** introduzca el número máximo de mensajes de syslog que se recibirán dentro del intervalo especificado.
- **Interval(Second):** en función del parámetro Número de mensajes configurado anteriormente, introduzca el intervalo de tiempo en el que se puede recibir un conjunto fijo de mensajes Syslog.

La velocidad de Syslog es el número de mensajes/intervalo.



Haga clic en **OK** para guardar la configuración de nivel de Syslog.

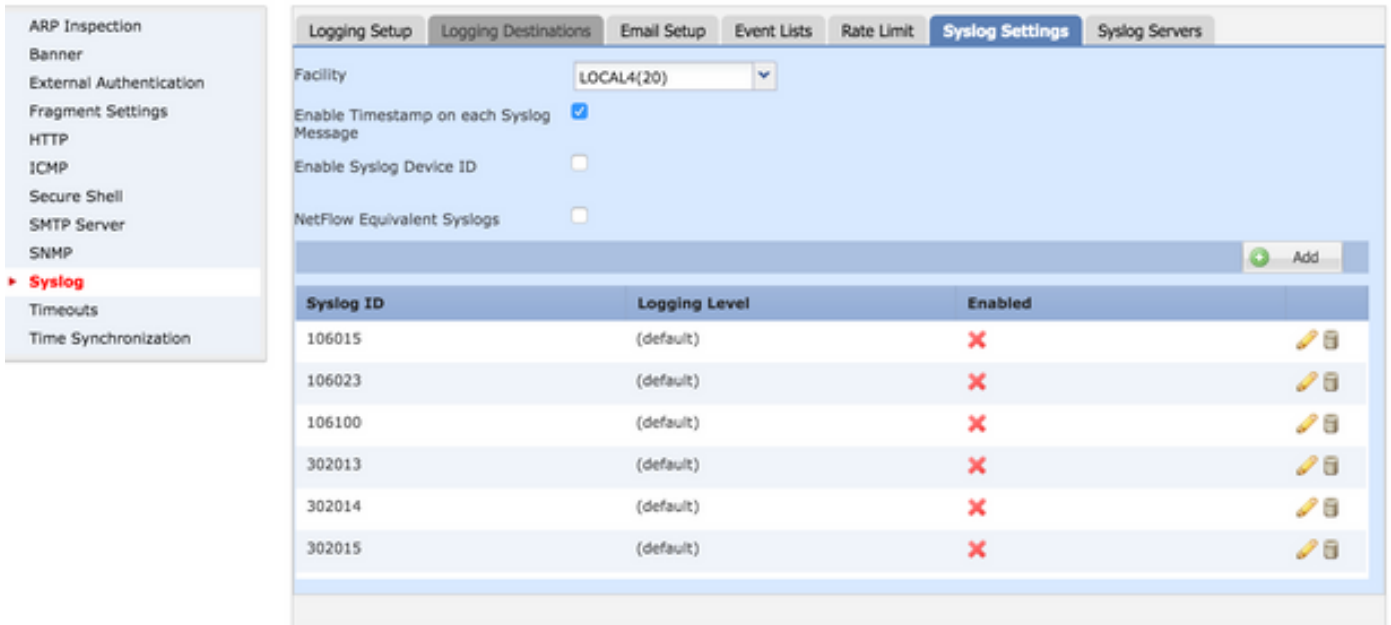
Haga clic en **Save** para guardar la configuración de la plataforma. Elija entre **Deploy**, seleccione el dispositivo FTD donde desea aplicar los cambios y haga clic en **Deploy** para iniciar la implementación de la configuración de la plataforma.

Configuración de Syslog

La configuración de Syslog permite incluir la configuración de los valores de Facility en los mensajes de Syslog. También puede incluir la marca de tiempo en los mensajes de registro y otros parámetros específicos del servidor Syslog.

Para configurar listas de eventos personalizadas, elija **Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Settings**.

- **Facility:** se utiliza un código de servicio para especificar el tipo de programa que registra el mensaje. Los mensajes con diferentes recursos se pueden gestionar de forma diferente. Desde **Facility** seleccione el valor del recurso en la lista desplegable.
- **Enable Timestamp on each Syslog Message:** consulte la **Enable Timestamp on each Syslog Message** para incluir la marca de tiempo en los mensajes de Syslog.
- **Enable Syslog Device ID:** consulte la **Enable Syslog Device ID** para incluir un ID de dispositivo en los mensajes Syslog sin formato EMBLEM.
- **Netflow Equivalent Syslogs:** consulte la **Netflow Equivalent Syslogs** para enviar registros del sistema equivalentes de NetFlow. Puede afectar al rendimiento del dispositivo.
- **Add Specific Syslog ID (Agregar ID específica de Syslog):** Para especificar la ID adicional de Syslog, haga clic en **Add** y especifique el **Syslog ID/ Logging Level** casilla de verificación.



Haga clic en **Save** para guardar la configuración de la plataforma. Elija entre **Deploy**, seleccione el dispositivo FTD donde desea aplicar los cambios y haga clic en **Deploy** para iniciar la implementación de la configuración de la plataforma.

Configurar registro local

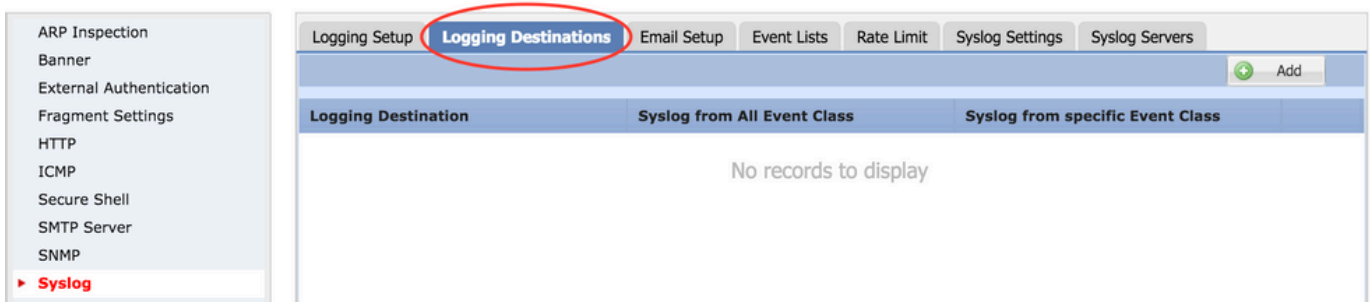
La sección Logging Destination se puede utilizar para configurar el registro en destinos específicos.

Los destinos de registro internos disponibles son:

- **Búfer interno:** registra en el búfer de registro interno (registro almacenado en búfer)
- **Consola:** envía registros a la consola (consola de registro)
- **Sesiones SSH:** Registra Syslog en sesiones SSH (monitor de terminal)

Hay tres pasos para configurar el registro local.

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



Paso 2. Haga clic en **Add** para agregar un filtro de registro para un logging destination.

Destino de registro: seleccione el destino de registro necesario en el **Logging Destination** lista

desplegable como memoria intermedia interna, consola o sesiones SSH.

Clase de evento: desde el **Event Class** seleccione una clase de evento en la lista desplegable. Como se ha descrito anteriormente, las clases de eventos son un conjunto de registros del sistema que representan las mismas características. Las clases de eventos se pueden seleccionar de las siguientes maneras:

- **Filter on Severity:** las clases de eventos filtran según la gravedad de los registros del sistema.
- **User Event List:** los administradores pueden crear listas de eventos específicas (descritas anteriormente) con sus propias clases de eventos personalizadas y hacer referencia a ellas en esta sección.
- **Disable Logging:** utilice esta opción para inhabilitar el registro para el destino de registro y el nivel de registro seleccionados.

Nivel de registro: seleccione el nivel de registro en la lista desplegable. El rango del nivel de registro va de 0 (Emergencias) a 7 (depuración).

Add Logging Filter

Logging Destination: Internal Buffer

Event Class: Filter on Severity

Syslog Severity: emergencias

Filter on Severity

Use Event List

Disable Logging

Add

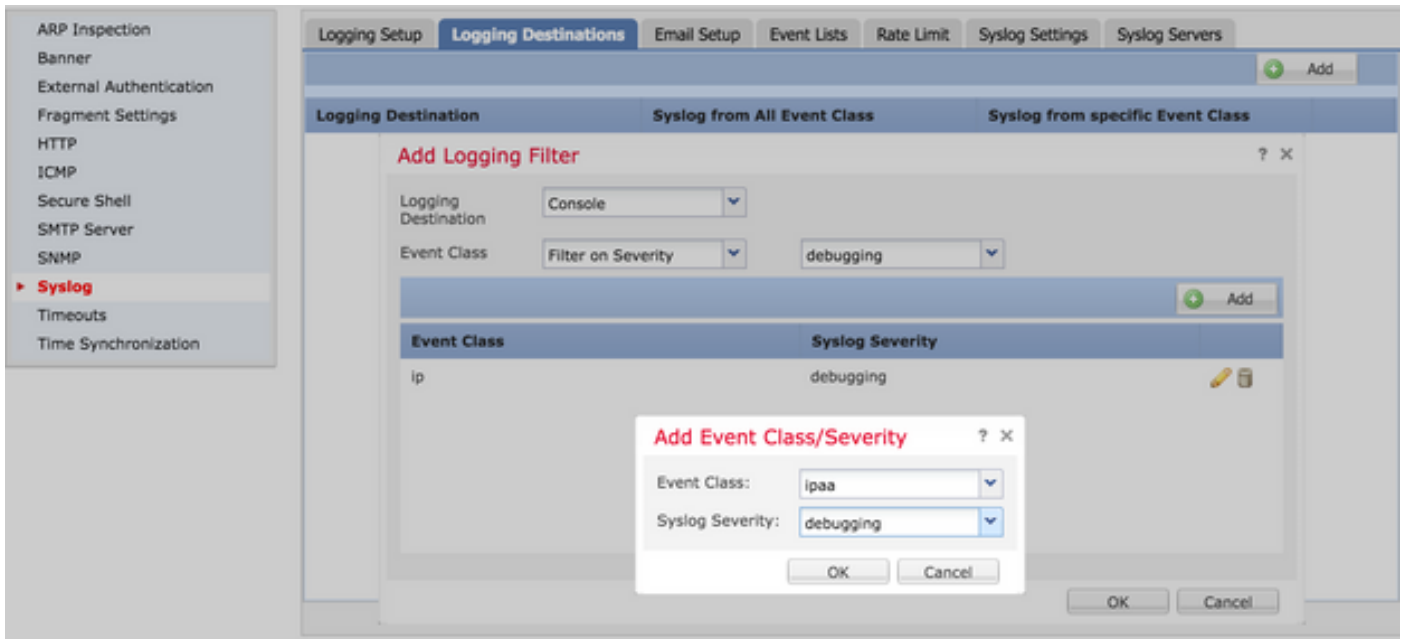
No records to display

OK Cancel

Paso 3. Para agregar una clase de evento independiente a este filtro de registro, haga clic en **Add**.

Event Class: elija la clase de evento de la **Event Class** lista desplegable.

Syslog Severity: elija la gravedad de Syslog en la **Syslog Severity** lista desplegable.



Haga clic en **OK** una vez configurado el filtro para agregar el filtro para un destino de registro específico.

Haga clic en **Save** para guardar la configuración de la plataforma. Elegir **Deploy**, seleccione el dispositivo FTD donde desea aplicar los cambios y haga clic en **Deploy** para iniciar la implementación de la configuración de plataforma.

Configuración del registro externo

Para configurar el registro externo, elija **Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations**.

FTD admite estos tipos de registro externo.

- Servidor Syslog: envía registros al servidor Syslog remoto.
- Captura SNMP: envía los registros como una captura SNMP.
- Correo electrónico: envía los registros por correo electrónico con un servidor de retransmisión de correo preconfigurado.

La configuración para el registro externo y el registro interno son iguales. La selección de destinos de registro decide el tipo de registro que se implementa. Es posible configurar las clases de eventos basadas en listas de eventos personalizados para el servidor remoto.

Servidor Syslog remoto

Los servidores Syslog se pueden configurar para analizar y almacenar registros de forma remota desde el FTD.

Hay tres pasos para configurar servidores Syslog remotos.

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

Paso 2. Configure el parámetro relacionado con el servidor Syslog.

- Permitir que el tráfico de usuario pase cuando el servidor syslog TCP está inactivo: si un servidor Syslog TCP se ha implementado en la red y no es accesible, se niega el tráfico de red a través del ASA. Esto sólo se aplica cuando el protocolo de transporte entre el ASA y el servidor Syslog es TCP. Compruebe el **Allow user traffic to pass when TCP syslog server is down** para permitir que el tráfico pase a través de la interfaz cuando el servidor Syslog está inactivo.
- Tamaño de cola de mensajes: el tamaño de cola de mensajes es el número de mensajes que se ponen en cola en el FTD cuando el servidor Syslog remoto está ocupado y no acepta ningún mensaje de registro. El valor predeterminado es 512 mensajes y el mínimo es 1 mensaje. Si se especifica 0 en esta opción, el tamaño de la cola se considera ilimitado.

The screenshot shows the 'Syslog Servers' configuration page. At the top, there are tabs for 'Logging Setup', 'Logging Destinations', 'Email Setup', 'Event Lists', 'Rate Limit', 'Syslog Settings', and 'Syslog Servers'. Below the tabs, there is a checkbox labeled 'Allow user traffic to pass when TCP syslog server is down' which is currently unchecked. Below this, there is a text input field for 'Message Queue Size(messages)*' with the value '512' entered. To the right of the input field, there is a note: '(0 - 8192 messages). Use 0 to indicate unlimited Queue Size'. At the bottom right of the configuration area, there is a green '+ Add' button. Below the configuration area, there is a table with the following columns: 'Interface', 'IP Address', 'Protocol', 'Port', and 'EMBLEM'. The table is currently empty, and the text 'No records to display' is centered below the table header.

Paso 3. Para agregar servidores Syslog remotos, haga clic en Add.

IP Address: Desde **IP Address** seleccione un objeto de red que contenga los servidores Syslog en la lista. Si no ha creado un objeto de red, haga clic en el icono más (+) para crear un nuevo objeto.

Protocol: haga clic en el **TCP** or **UDP** botón de opción para la comunicación Syslog.

Port: introduzca el número de puerto del servidor Syslog. De forma predeterminada, es 514.

Log Messages in Cisco EMBLEM format(UDP only): haga clic en el **Log Messages in Cisco EMBLEM format (UDP only)** para habilitar esta opción si es necesario registrar mensajes en el formato del LOGOTIPO de Cisco. Esto es aplicable solamente para el Syslog basado en UDP.

Available Zones: introduzca las zonas de seguridad a través de las cuales se puede acceder al servidor Syslog y muévelo a la columna Zonas/Interfaces seleccionadas.

Add Syslog Server

IP Address*

Protocol TCP UDP

Port (514 or 1025-65535)

Log Messages in Cisco EMBLEM format(UDP only)

Available Zones

Selected Zones/Interfaces

Haga clic en **OK** y **Save** para guardar la configuración.

Haga clic en **Save** para guardar la configuración de la plataforma. Elegir **Deploy**, seleccione el dispositivo FTD donde desea aplicar los cambios y haga clic en **Deploy** para iniciar la implementación de la configuración de la plataforma.

Configuración de correo electrónico para registro

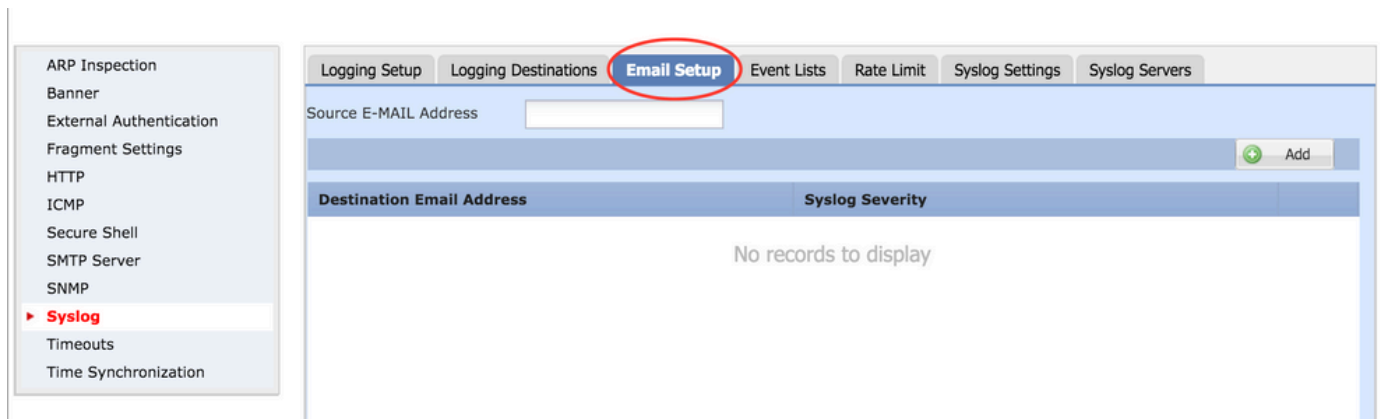
FTD permite enviar el registro del sistema a una dirección de correo electrónico específica. El correo electrónico se puede utilizar como destino de registro sólo si ya se ha configurado un servidor de retransmisión de correo electrónico.

Hay dos pasos para configurar los ajustes de correo electrónico para los registros del sistema.

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

Source E-MAIL Address: introduzca la dirección de correo electrónico de origen que aparece en todos

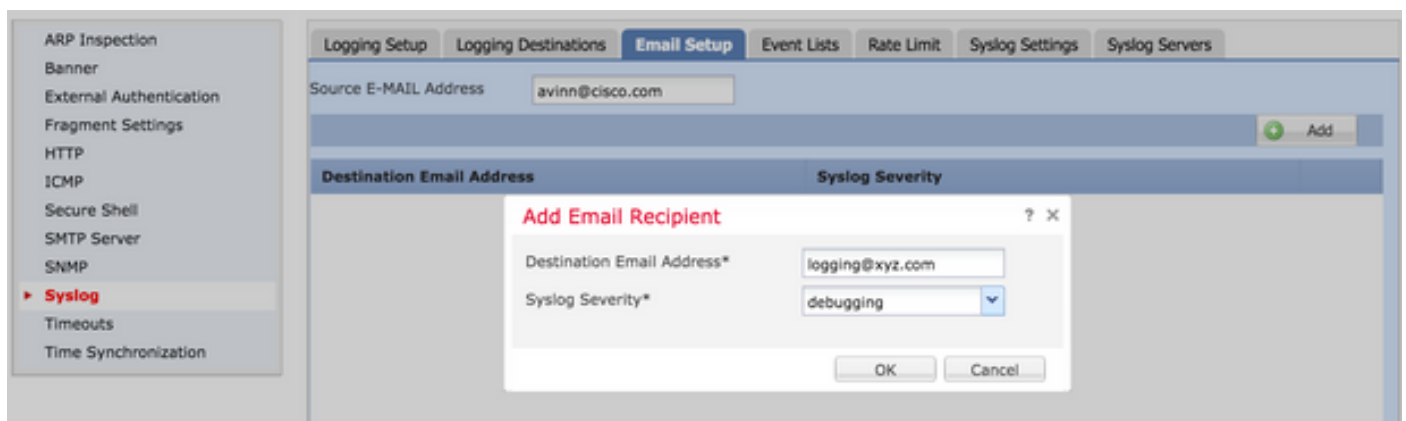
los correos electrónicos enviados desde el FTD que contienen los registros del sistema.



Paso 2. Para configurar la dirección de correo electrónico de destino y la gravedad de Syslog, haga clic en **Add**.

Destination Email Address: introduzca la dirección de correo electrónico de destino donde se envían los mensajes de Syslog.

Syslog Severity: elija la gravedad de Syslog en la Syslog Severity lista desplegable.



Haga clic en **OK** para guardar la configuración.

Haga clic en **Save** para guardar la configuración de la plataforma. Elegir **Deploy**, seleccione el dispositivo FTD donde desea aplicar los cambios y haga clic en **Deploy** para iniciar la implementación de la configuración de la plataforma.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

- Verifique la configuración de FTD Syslog en la CLI de FTD. Inicie sesión en la interfaz de gestión del FTD e introduzca el `system support diagnostic-cli` para iniciar la consola en la CLI de diagnóstico.

```
> 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
```

- Asegúrese de que el servidor Syslog es accesible desde el FTD. Inicie sesión en la interfaz de gestión de FTD a través de SSH y verifique la conectividad con el `ping` comando.

```
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
```

- Puede tomar una captura de paquetes para verificar la conectividad entre el FTD y el servidor Syslog. Inicie sesión en la interfaz de administración de FTD a través de SSH e ingrese el comando `system support diagnostic-cli`. Para ver los comandos de captura de paquetes, consulte [Ejemplo de Configuración de Capturas de Paquetes ASA con CLI y ASDM](#).
- Asegúrese de que la implementación de directivas se aplica correctamente.

Información Relacionada

- [Guía de inicio rápido de Cisco Firepower Threat Defence para ASA](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).