

# Configurar o registro no FTD usando o FMC

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Configuração global do syslog](#)

[Configuração de registro](#)

[Listas de eventos](#)

[Syslog de limitação de taxa](#)

[Configurações de Syslog](#)

[Configurar registro local](#)

[Configurar o registro externo](#)

[Servidor Syslog Remoto](#)

[Configuração de e-mail para registro](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve a configuração de registro para um FirePOWER Threat Defense (FTD) via Firepower Management Center (FMC).

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Tecnologia FirePOWER
- Conhecimento básico do Adaptive Security Appliance (ASA)
- protocolo Syslog

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Imagem do ASA Firepower Threat Defense para ASA (5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X ) que executa a versão de software 6.0.1 e posterior
- Imagem do ASA Firepower Threat Defense para ASA (5515-X, ASA 5525-X, ASA 5545-X,

ASA 5555-X, ASA 5585-X) que executa a versão de software 6.0.1 e posterior

- FMC Versão 6.0.1 e posterior

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

Os registros do sistema FTD fornecem informações para monitorar e solucionar problemas do dispositivo FTD. Os registros são úteis na solução de problemas de rotina e no tratamento de incidentes. O dispositivo FTD suporta registro local e externo.

O registro local pode ajudá-lo a solucionar problemas ao vivo. O registro externo é um método de coleta de logs do dispositivo FTD para um servidor Syslog externo. Fazer login em um servidor central ajuda na agregação de logs e alertas. O registro externo pode ajudar na correlação de registros e no tratamento de incidentes.

Para o registro local, o dispositivo FTD suporta console, opção de buffer interno e o registro de sessão Secure Shell (SSH).

Para o registro externo, o dispositivo FTD suporta o servidor Syslog externo e o servidor do Email Relay.

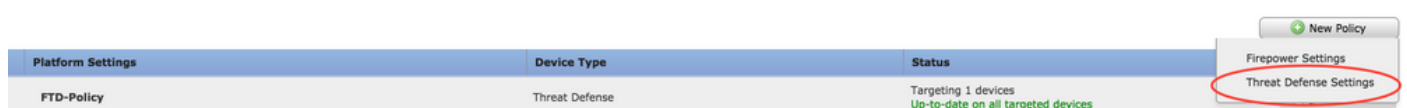
**Note:** Se um alto volume de tráfego passar pelo dispositivo, preste atenção ao tipo de registro/gravidade/limitação de taxa. Faça isso para limitar o número de registros, o que evita o impacto no firewall.

## Configurar

Todas as configurações relacionadas ao registro podem ser configuradas quando você navega para o Platform Settings na guia Devices . Escolher Devices > Platform Settings como mostrado nesta imagem.



Clique no ícone do lápis para editar a política existente ou clique em **New Policy**, em seguida, selecione **Threat Defense Settings** para criar uma nova política de FTD como mostrado nesta imagem.



Escolha o dispositivo FTD para aplicar essa política e clique em **Save** como mostrado nesta imagem.

**New Policy** ? X

Name:

Description:

**Targeted Devices**

Select devices to which you want to apply this policy.

**Available Devices**

- FTD\_HA

**Selected Devices**

- FTD\_HA

## Configuração global do syslog

Há algumas configurações aplicáveis para registro local e externo. Esta seção trata dos parâmetros obrigatórios e opcionais que podem ser configurados para Syslog.

### Configuração de registro

As opções de configuração de registro aplicam-se ao registro local e externo. Para configurar a configuração de registro, escolha **Devices > Platform Settings**.

Escolher **Syslog > Logging Setup**.

### Configuração básica de registro em log

- **Enable Logging:** Verifique a **Enable Logging** para ativar o registro. Esta é uma opção obrigatória.
- **Enable Logging on the failover standby unit:** Verifique a **Enable Logging on the failover standby unit** para configurar o registro no FTD em standby, que faz parte de um cluster de alta disponibilidade do FTD.
- **Send syslogs in EMBLEM format:** Verifique a **Send syslogs in EMBLEM format** para habilitar o formato de Syslog como EMBLEM para cada destino. O formato EMBLEM é usado principalmente para o analisador de Syslog do CiscoWorks Resource Manager Essentials (RME). Esse formato corresponde ao formato Syslog do software Cisco IOS produzido pelos roteadores e pelos

switches. Ele está disponível somente para servidores Syslog UDP.

- Send debug messages as syslogs: Verifique a **Send debug messages as syslogs** para enviar os logs de depuração como mensagens de Syslog ao servidor Syslog.
- Memory size of the Internal Buffer: Insira o tamanho do buffer de memória interno no qual o FTD pode salvar os dados de log. Os dados de log serão girados se seu limite de buffer for atingido.

### Informações do servidor FTP (opcional)

Especifique os detalhes do servidor FTP se desejar enviar os dados de log para o servidor FTP antes que ele substitua o buffer interno.

- FTP Server Buffer Wrap: Verifique a **FTP Server Buffer Wrap** para enviar os dados de log de buffer ao servidor FTP.
- IP Address: Insira o endereço IP do servidor FTP.
- Username: Digite o nome de usuário do servidor FTP.
- Path: Digite o caminho do diretório do servidor FTP.
- Password: Digite a senha do servidor FTP.
- Confirm: Digite a mesma senha novamente.

### Tamanho da memória flash (opcional)

Especifique o tamanho da flash se desejar salvar os dados de log na memória flash quando o buffer interno estiver cheio.

- Flash: Verifique a **Flash** para enviar os dados de log à flash interna.
- Maximum Flash to be used by Logging(KB): Digite o tamanho máximo, em KB, da memória flash que pode ser usada para o registro.
- Minimum free Space to be preserved(KB): Digite o tamanho mínimo em KB da memória flash que precisa ser preservada.

The screenshot shows the 'Syslog' configuration page in the Cisco FTD web interface. The left sidebar contains a menu with 'Syslog' selected. The main content area is divided into three sections: 'Basic Logging Settings', 'Specify FTP Server Information', and 'Specify Flash Size'. In the 'Basic Logging Settings' section, 'Enable Logging', 'Enable Logging on the failover standby unit', 'Send syslogs in EMBLEM format', 'Send debug messages as syslogs', and 'Memory Size of the Internal Buffer' (set to 4096) are all checked or configured. The 'Specify FTP Server Information' section has 'FTP Server Buffer Wrap' checked, and fields for 'IP Address\*' (WINS1), 'Username\*' (admin), 'Path\*' (/var/ftp), 'Password\*', and 'Confirm\*'. The 'Specify Flash Size' section has 'Flash' unchecked, 'Maximum Flash to be used by Logging(KB)' set to 3076, and 'Minimum free Space to be preserved(KB)' set to 1024.

Section	Setting	Value	Range/Default
Basic Logging Settings	Enable Logging	<input checked="" type="checkbox"/>	
	Enable Logging on the failover standby unit	<input checked="" type="checkbox"/>	
	Send syslogs in EMBLEM format	<input checked="" type="checkbox"/>	
	Send debug messages as syslogs	<input checked="" type="checkbox"/>	
	Memory Size of the Internal Buffer	4096	(4096-52428800 Bytes)
Specify FTP Server Information	FTP Server Buffer Wrap	<input checked="" type="checkbox"/>	
	IP Address*	WINS1	
	Username*	admin	
	Path*	/var/ftp	
	Password*	.....	
Specify Flash Size	Flash	<input type="checkbox"/>	
	Maximum Flash to be used by Logging(KB)	3076	(4-8044176)
	Minimum free Space to be preserved(KB)	1024	(0-8044176)

Clique em **save** para salvar a configuração da plataforma. Escolha o **Deploy**, escolha o dispositivo FTD no qual deseja aplicar as alterações e clique em **Deploy** para iniciar a implantação da

configuração da plataforma.

## Listas de eventos

A opção Configurar listas de eventos permite criar/editar uma lista de eventos e especificar quais dados de log incluir no filtro da lista de eventos. As listas de eventos podem ser usadas ao configurar os filtros de registro em destinos de registro.

O sistema permite que duas opções usem a funcionalidade de listas de eventos personalizadas.

- Classe e Gravidade
- ID da mensagem

Para configurar listas de eventos personalizadas, escolha **Device > Platform Setting > Threat Defense Policy > Syslog > Event List** e clique em **Add**. Estas são as opções:

- Name: Digite o nome da lista de eventos.
- Severity/Event Class: Na seção Gravidade/Classe de Evento, clique em **Add**.
- Event Class: Escolha a classe de evento na lista suspensa para o tipo de dados de log desejado. Uma classe de evento define um conjunto de regras de Syslog que representam os mesmos recursos. Por exemplo, há uma Classe de Evento para a sessão que inclui todos os Syslogs relacionados à sessão.
- Syslog Severity: Escolha a gravidade na lista suspensa para a classe de evento escolhida. A gravidade pode variar de 0 (emergência) a 7 (depuração).
- Message ID: Se você estiver interessado em dados de log específicos relacionados a uma ID de mensagem, clique em **Add** para colocar um filtro com base na ID da mensagem.
- Message IDs: Especifique a ID da mensagem como formato individual/ de intervalo.

The screenshot shows the 'Add Event List' configuration interface. The interface is divided into two main sections: 'Severity/EventClass' and 'Message ID'. Both sections have a table with an 'Add' button and an 'OK' button.

**Severity/EventClass Section:**

Event Class	Event Class/Severity
session	emergencies

**Message ID Section:**

Message IDs
106002

Clique em **OK** para salvar a configuração.

Clique em **Save** para salvar a configuração da plataforma. Escolher para **Deploy**, escolha o dispositivo FTD no qual deseja aplicar as alterações e clique em **Deploy** para iniciar a implantação da configuração da plataforma.

## Syslog de limitação de taxa

A opção Limite de taxa define o número de mensagens que podem ser enviadas a todos os destinos configurados e define a gravidade da mensagem à qual você deseja atribuir limites de taxa.

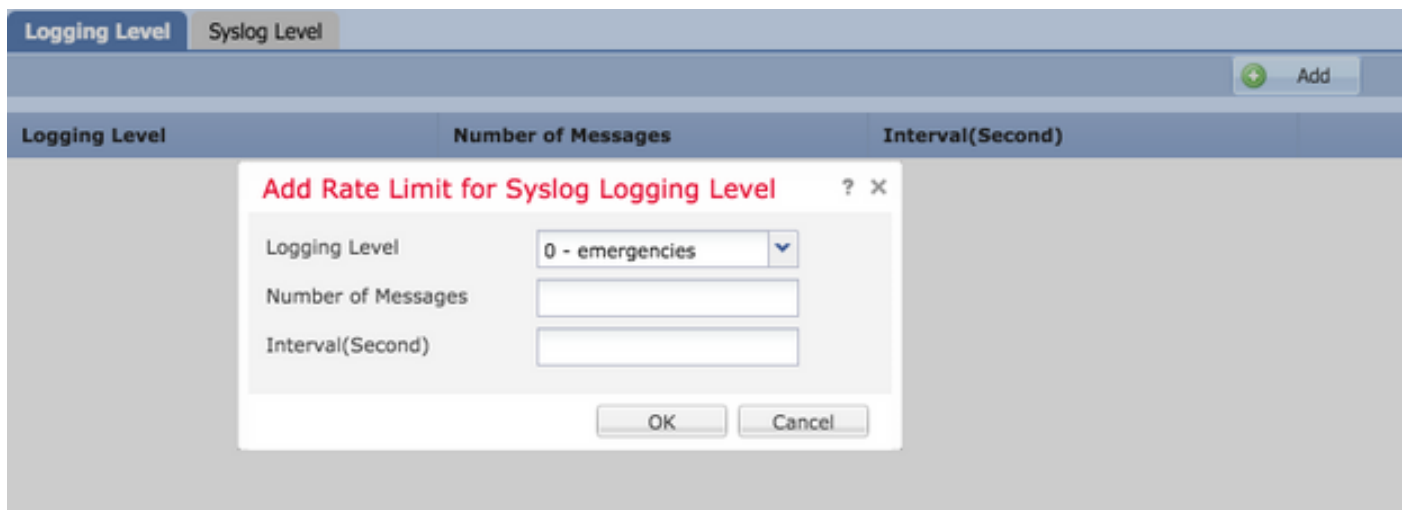
Para configurar listas de eventos personalizadas, escolha **Device > Platform Setting > Threat Defense Policy > Syslog > Rate Limit**. Você tem duas opções com base nas quais pode especificar o limite de taxa:

- Nível de registro
- Níveis de syslog

Para ativar o limite de taxa baseado no nível de registro, escolha **Logging Level** e clique em **Add**.

- **Logging Level**: Nos **Logging Level** selecione o nível de registro para o qual deseja executar a limitação de taxa.
- **Number of Messages**: Insira o número máximo de mensagens de Syslog a serem recebidas no intervalo especificado.
- **Interval(Second)**: Com base no parâmetro Número de mensagens configuradas anteriormente, insira o intervalo de tempo no qual um conjunto fixo de mensagens de Syslog pode ser recebido.

A taxa de syslog é o número de mensagens/intervalos.



The screenshot shows a web interface with two tabs: 'Logging Level' (selected) and 'Syslog Level'. An 'Add' button is visible in the top right. Below the tabs is a table with columns for 'Logging Level', 'Number of Messages', and 'Interval(Second)'. A modal dialog box titled 'Add Rate Limit for Syslog Logging Level' is open, containing three input fields: 'Logging Level' (a dropdown menu showing '0 - emergencies'), 'Number of Messages' (an empty text box), and 'Interval(Second)' (an empty text box). At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Clique em **OK** para salvar a configuração de nível de registro.

Para ativar o limite de taxa baseado no nível de registro, escolha **Logging Level** e clique em **Add**.

- **Syslog ID**: As IDs de Syslog são usadas para identificar exclusivamente as mensagens de Syslog. Nos **Syslog ID** selecione a ID do Syslog.
- **Number of Messages**: Insira o número máximo de mensagens de syslog a serem recebidas no intervalo especificado.
- **Interval(Second)**: Com base no parâmetro Número de mensagens configuradas anteriormente,

insira o intervalo de tempo no qual um conjunto fixo de mensagens de Syslog pode ser recebido.

A taxa de syslog é o número de mensagens/intervalo.



Clique em **OK** para salvar a configuração de nível Syslog.

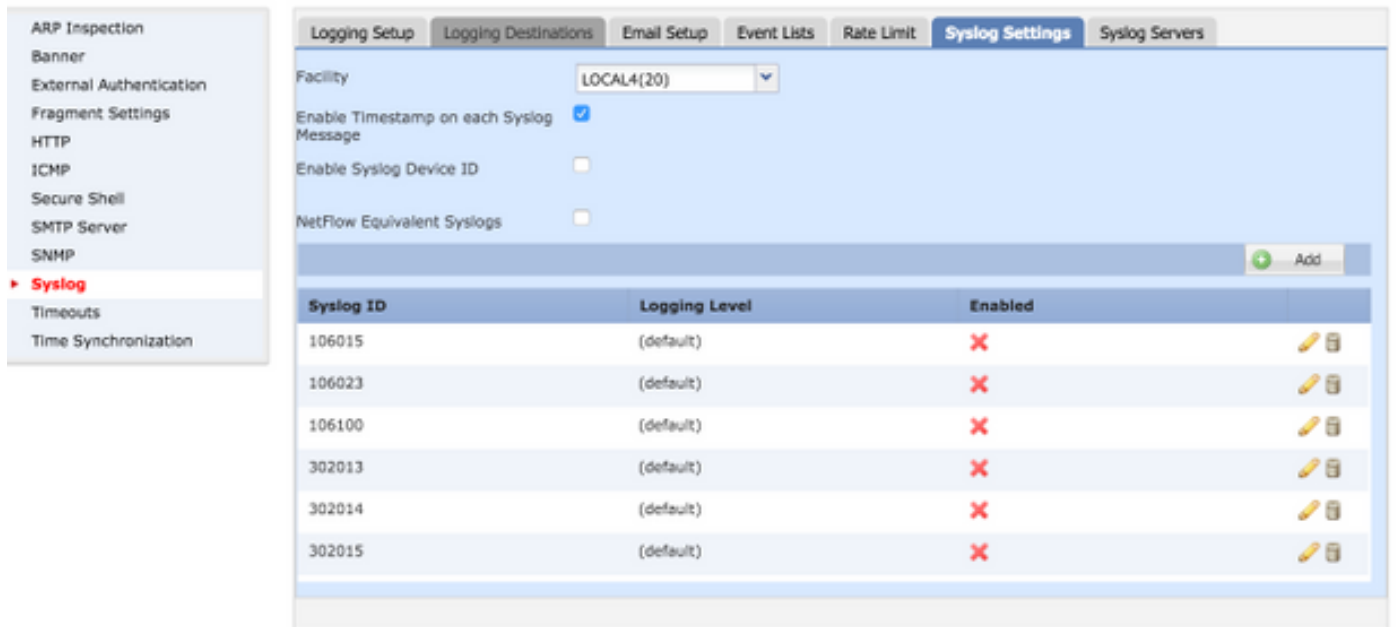
Clique em **save** para salvar a configuração da plataforma. Escolher para **Deploy**, escolha o dispositivo FTD no qual deseja aplicar as alterações e clique em **Deploy** para iniciar a implantação da configuração da plataforma.

## Configurações de Syslog

As configurações de syslog permitem que a configuração dos valores de Facility sejam incluídos nas mensagens de Syslog. Você também pode incluir o timestamp em mensagens de log e outros parâmetros específicos do servidor Syslog.

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

- **Facility:** Um código de recurso é usado para especificar o tipo de programa que está registrando a mensagem. Mensagens com diferentes recursos podem ser tratadas de forma diferente. Nos **Facility** selecione o valor do recurso.
- **Enable Timestamp on each Syslog Message:** Verifique a **Enable Timestamp on each Syslog Message** para incluir o datador de hora nas mensagens do Syslog.
- **Enable Syslog Device ID:** Verifique a **Enable Syslog Device ID** para incluir uma ID de dispositivo em mensagens Syslog não-EMBLEM-format.
- **Netflow Equivalent Syslogs:** Verifique a **Netflow Equivalent Syslogs** para enviar Syslogs equivalentes do NetFlow. Isso pode afetar o desempenho do dispositivo.
- **Adicionar ID de Syslog Específico:** Para especificar a ID de Syslog adicional, clique em **Add** e especificar **Syslog ID/ Logging Level** caixa de seleção.



Clique em **Save** para salvar a configuração da plataforma. Escolher para **Deploy**, escolha o dispositivo FTD no qual deseja aplicar as alterações e clique em **Deploy** para iniciar a implantação da configuração da plataforma.

## Configurar registro local

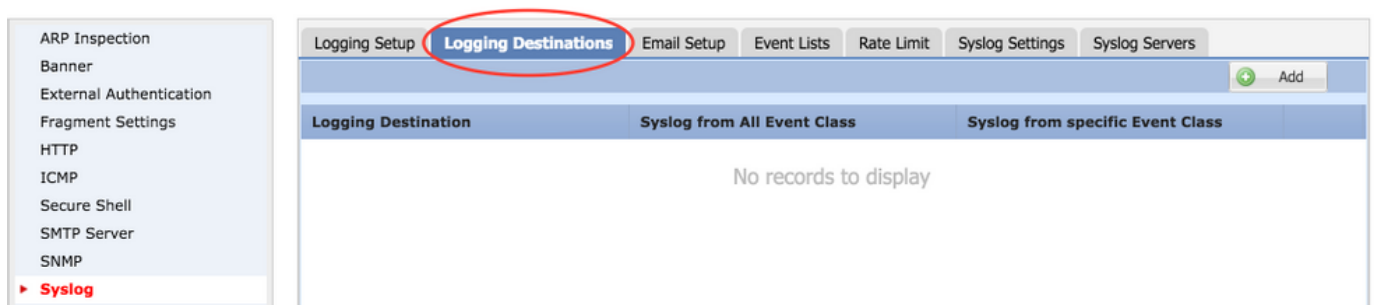
A seção de destino de registro pode ser usada para configurar o registro em destinos específicos.

Os destinos de registro interno disponíveis são:

- Buffer interno: Registra no buffer de registro interno (logging buffered)
- Console: Envia registros para o console (console de registro)
- Sessões SSH: Registra Syslog em sessões SSH (monitor de terminal)

Há três etapas para configurar o registro local.

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



Etapa 2. Clique em **Add** para adicionar um filtro de registro para um logging destination.

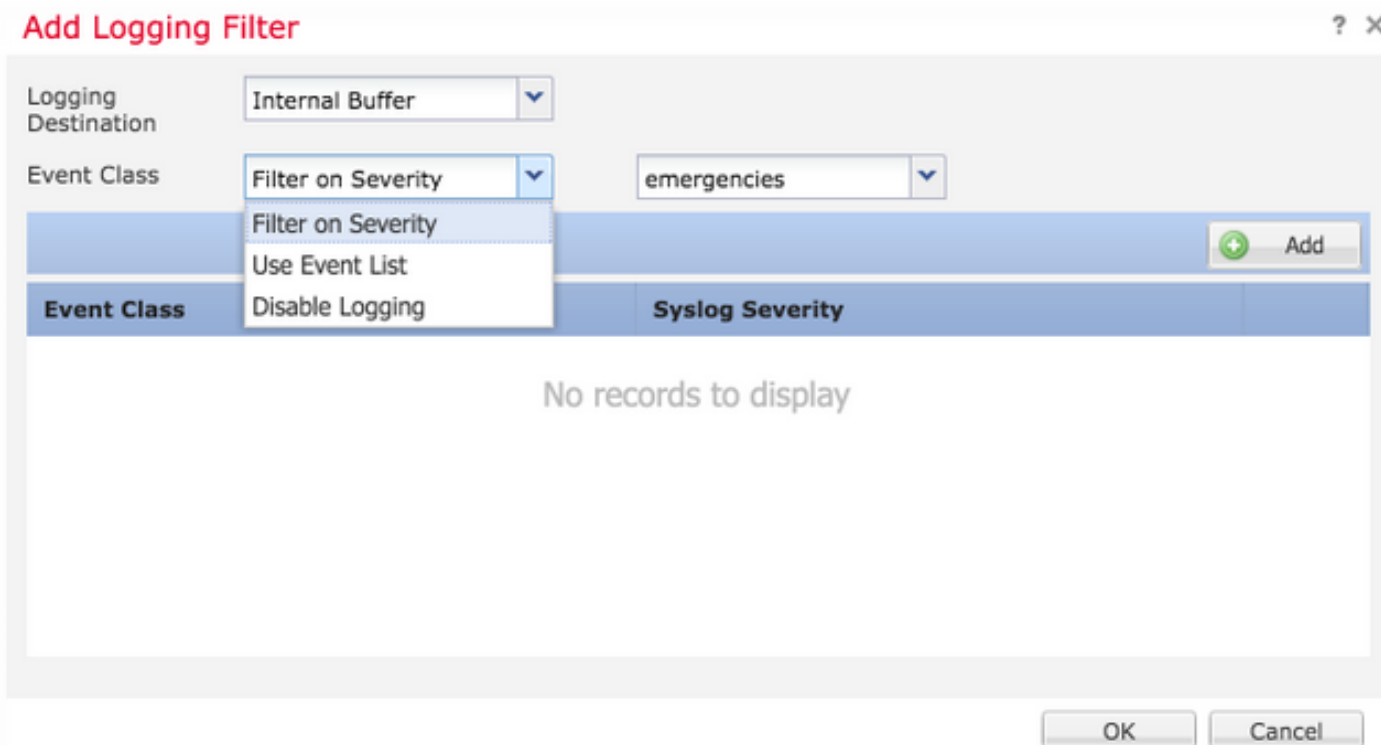
Destino de registro: Escolha o destino de registro obrigatório no **Logging Destination** lista suspensa como sessões de buffer interno, console ou SSH.

Classe de evento: Nos **Event Class** selecione uma classe Evento. Conforme descrito anteriormente, as classes de eventos são um conjunto de syslogs que representam os mesmos recursos. As classes de eventos podem ser selecionadas das seguintes maneiras:



- Filter on Severity: As classes de evento filtram com base na gravidade dos Syslogs.
- User Event List: Os administradores podem criar listas de eventos específicas (descritas anteriormente) com suas próprias classes de eventos personalizadas e referenciá-las nesta seção.
- Disable Logging: Use esta opção para desabilitar o registro para o destino de registro e o nível de registro escolhidos.

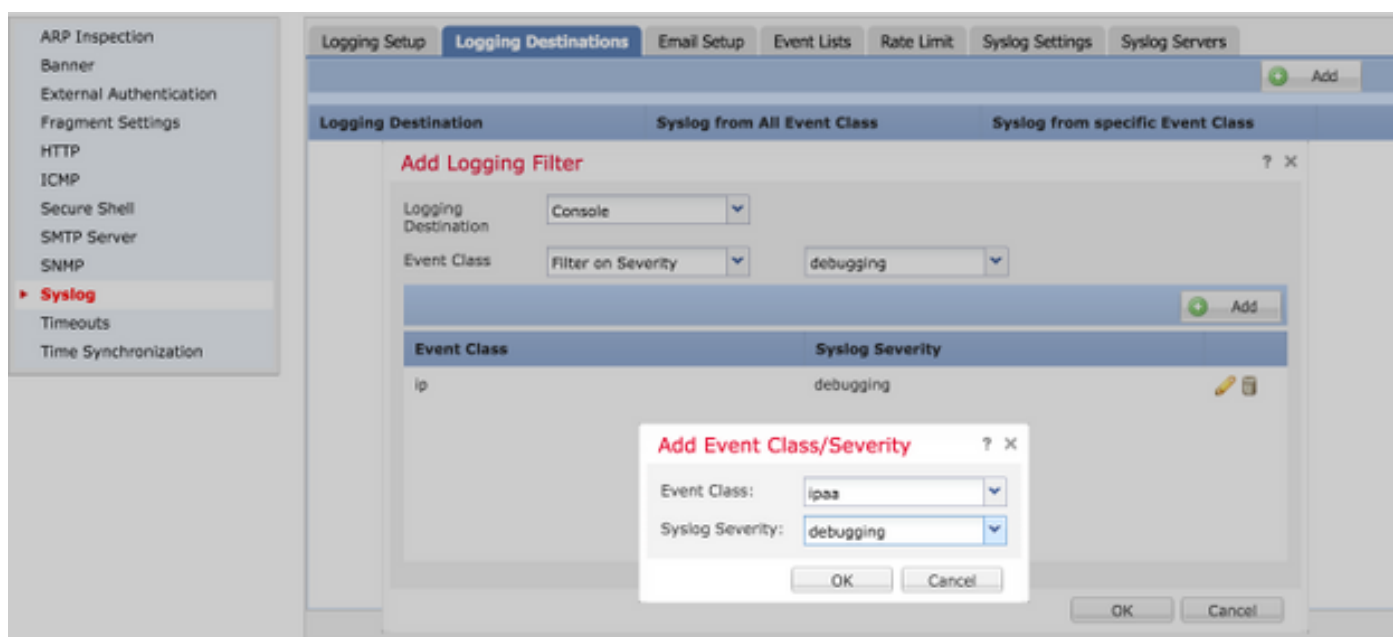
Nível de registro: Escolha o nível de registro na lista suspensa. O intervalo do nível de registro é de 0 (Emergências) a 7 (depuração).



Etapa 3. Para adicionar uma classe de Evento separada a este filtro de Log, clique em Add.

Event Class: Escolha a classe de evento no Event Class lista suspensa.

Syslog Severity: Escolha a gravidade do Syslog no Syslog Severity lista suspensa.



Clique em **OK** quando o filtro estiver configurado para adicionar o filtro para um destino de registro específico.

Clique em **save** para salvar a configuração da plataforma. Escolher **Deploy**, escolha o dispositivo FTD no qual deseja aplicar as alterações e clique em **Deploy** para iniciar a implantação da configuração da plataforma.

## Configurar o registro externo

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

O FTD suporta estes tipos de registro externo.

- Servidor Syslog: Envia registros para o servidor Syslog remoto.
- interceptação SNMP: Envia os logout como uma armadilha SNMP.
- e-mail: Envia os registros por e-mail com um servidor de retransmissão de e-mail pré-configurado.

A configuração para o registro externo e o registro interno são iguais. A seleção de destinos de registro decide o tipo de registro que é implementado. É possível configurar Classes de Evento com base em Listas de Evento Personalizadas para o servidor remoto.

## Servidor Syslog Remoto

Os servidores syslog podem ser configurados para analisar e armazenar logs remotamente a partir do FTD.

Há três etapas para configurar servidores Syslog remotos.

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

Etapa 2. Configure o parâmetro relacionado ao servidor Syslog.

- Permitir que o tráfego do usuário passe quando o servidor syslog TCP estiver inoperante: Se um servidor Syslog TCP tiver sido implantado na rede e não estiver acessível, o tráfego de rede através do ASA será negado. Isso é aplicável somente quando o protocolo de transporte entre o ASA e o servidor Syslog é TCP. Verifique a **Allow user traffic to pass when TCP syslog server is down** para permitir que o tráfego passe pela interface quando o servidor Syslog estiver inoperante.
- Tamanho da fila de mensagens: O tamanho da fila de mensagens é o número de mensagens que são enfileiradas no FTD quando o servidor Syslog remoto está ocupado e não aceita nenhuma mensagem de log. O padrão é 512 mensagens e o mínimo é 1 mensagem. Se 0 for especificado nesta opção, o tamanho da fila será considerado ilimitado.

Logging Setup Logging Destinations Email Setup Event Lists Rate Limit Syslog Settings **Syslog Servers**

Allow user traffic to pass when TCP syslog server is down

Message Queue Size(messages)\*  (0 - 8192 messages). Use 0 to indicate unlimited Queue Size

Interface	IP Address	Protocol	Port	EMBLEM
No records to display				

Etapa 3. Para adicionar servidores Syslog remotos, clique em **Add**.

**IP Address:** Nos **IP Address** selecione um objeto de rede que tenha os servidores Syslog listados. Se você não criou um objeto de rede, clique no ícone de mais (+) para criar um novo objeto.

**Protocol:** Clique no botão **TCP** or **UDP** para comunicação Syslog.

**Port:** Digite o número da porta do servidor Syslog. Por padrão, é 514.

**Log Messages in Cisco EMBLEM format(UDP only):** Clique no botão **Log Messages in Cisco EMBLEM format (UDP only)** para habilitar essa opção se for necessário registrar mensagens no formato Cisco EMBLEM. Isso se aplica somente a Syslog baseado em UDP.

**Available Zones:** Insira as zonas de segurança sobre as quais o servidor Syslog pode ser alcançado e mova-o para a coluna Zonas/ interfaces selecionadas.

## 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**

Clique em **OK** e **save** para salvar a configuração.

Clique em **save** para salvar a configuração da plataforma. Escolher **Deploy**, escolha o dispositivo FTD no qual deseja aplicar as alterações e clique em **Deploy** para iniciar a implantação da configuração da plataforma.

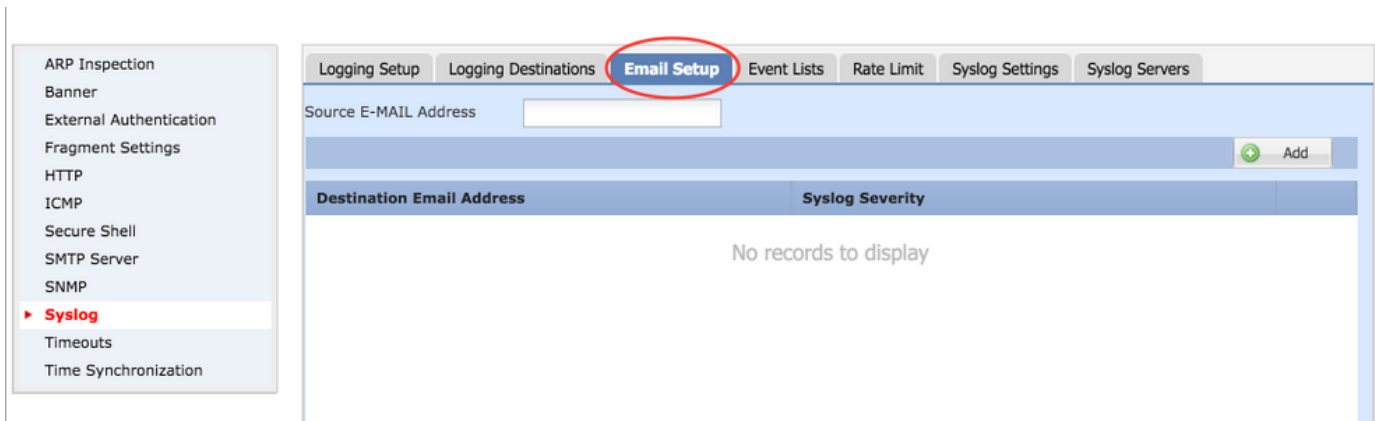
### Configuração de e-mail para registro

O FTD permite enviar o Syslog para um endereço de e-mail específico. O e-mail pode ser usado como um destino de registro somente se um servidor de e-mail relay já tiver sido configurado.

Há duas etapas para definir as configurações de e-mail para os Syslogs.

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

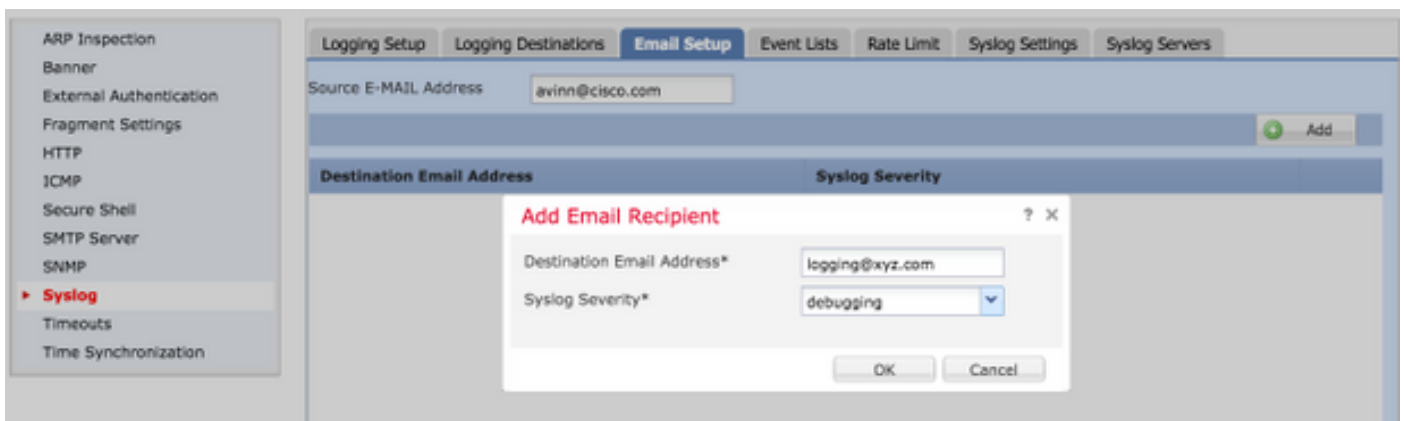
Source E-MAIL Address: Insira o endereço de e-mail de origem que aparece em todos os e-mails enviados do FTD que contêm os Syslogs.



Etapa 2. Para configurar o endereço de e-mail de destino e a gravidade do Syslog, clique em **Add**.

Destination Email Address: Insira o endereço de e-mail de destino para onde as mensagens de Syslog são enviadas.

Syslog Severity: Escolha a gravidade do Syslog no **Syslog Severity** lista suspensa.



Clique em **OK** para salvar a configuração.

Clique em **save** para salvar a configuração da plataforma. Escolher **Deploy**, escolha o dispositivo FTD no qual deseja aplicar as alterações e clique em **Deploy** para iniciar a implantação da configuração da plataforma.

## Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

## Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

- Verifique a configuração do Syslog FTD na CLI do FTD. Faça login na interface de gerenciamento do FTD e insira o comando `system support diagnostic-cli` para usar o console na 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
```

- **Certifique-se de que o servidor Syslog esteja acessível no FTD. Faça login na interface de gerenciamento FTD via SSH e verifique a conectividade com o 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
```

- Você pode capturar um pacote para verificar a conectividade entre o FTD e o servidor Syslog. Faça login na interface de gerenciamento FTD via SSH e insira o comando `system support diagnostic-cli`. Para os comandos de captura de pacotes, consulte [Exemplo de Configuração de Capturas de Pacotes ASA com CLI e ASDM](#).
- Verifique se a implantação da política foi aplicada com êxito.

## Informações Relacionadas

- [Guia de início rápido do Cisco Firepower Threat Defense para o ASA](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)