FMC を介して FTD にロギングを設定

内容

はじめに

このドキュメントでは、Firepower Management Center （ FMC ）から Firepower Threat Defense のロギングを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- FirePOWER 技術
- 適応型セキュリティ アプライアンス (ASA)
- Syslogプロトコル

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェアバージョン6.0.1以降が稼働するASA(5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)用のASAFirepower脅威対策イメージ

- ソフトウェアバージョン6.0.1以降が稼働するASA(5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、ASA 5585-X)用のASAFirepower脅威対策イメージ
- FMCバージョン6.0.1以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

FTD システム ログは、FTD アプライアンスを監視およびトラブルシューティングするための情報を提供します。

ログは、日常的なトラブルシューティングとインシデント処理の両方で役立ちます。FTDアプライアンスは、ローカルと外部の両方のロギングをサポートしています。

ローカル ロギングを使用すると、発生中の問題のトラブルシューティングに役立ちます。外部ロギングとは、FTD 機器から外部の syslog サーバにログを収集する方法です。

中央管理サーバへのロギングは、ログおよびアラートの集約に役立ちます。外部ログは、ログの相関およびインシデント処理に役立ちます。

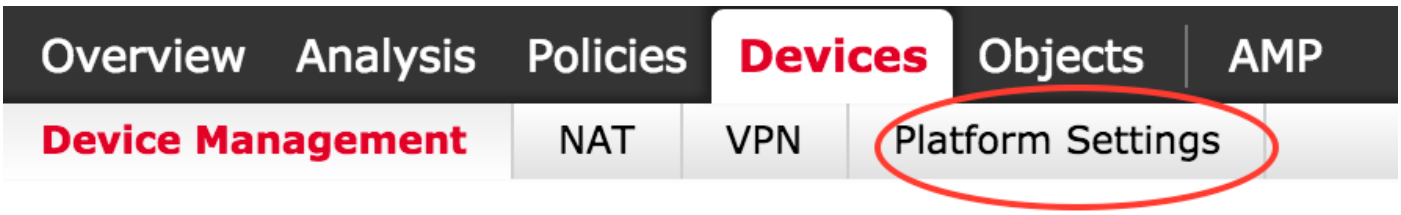
ローカル ロギングに関して、FTD アプライアンスがコンソール、内部バッファ オプション、およびセキュア シェル（SSH）セッション ロギングをサポートしています。

外部ロギングの場合、FTDアプライアンスは外部syslogサーバとEメールリレーサーバをサポートします。

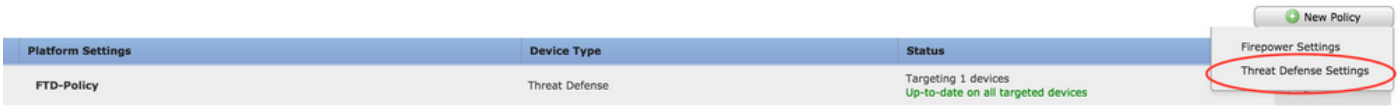
注：大量のトラフィックがアプライアンスを通過する場合は、ロギング/重大度/レート制限のタイプに注意してください。ログの数を制限し、ファイアウォールへの影響を回避するには、次の手順を実行します。

設定

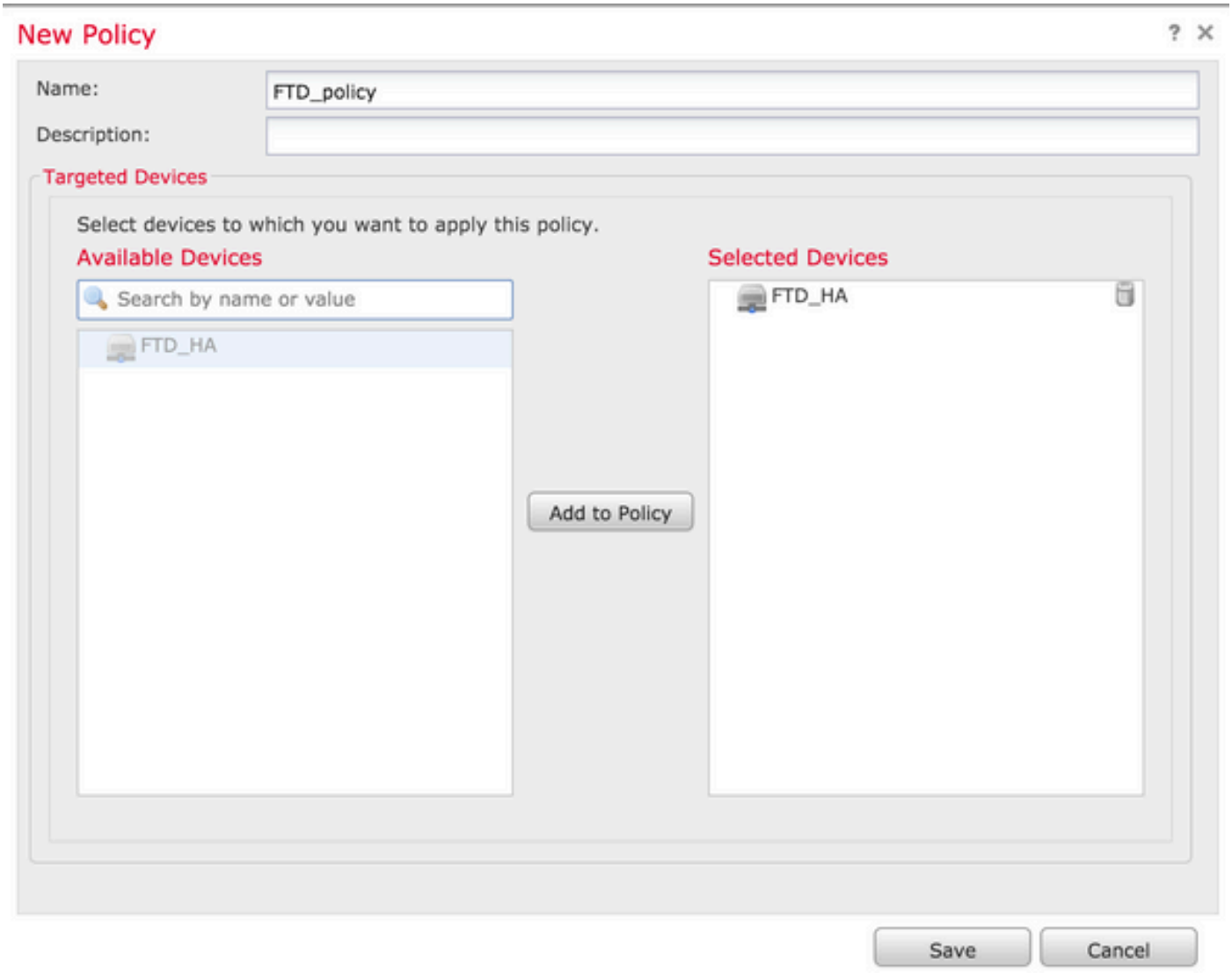
すべてのロギング関連の設定は、 Platform Settings タブを Devices tab.選択 Devices > Platform Settings 以下の図に、出力例を示します。



鉛筆アイコンをクリックして既存のポリシーを編集するか、 **New Policy**を選択し、 **Threat Defense Settings**新しいFTDポリシーを作成します。



このポリシーを適用するFTDアプライアンスを選択し、 **Save** 以下の図に、出力例を示します。



グローバル syslog 設定の編集

ローカルおよび外部両方のロギングに適用される特定の設定があります。この項では、syslog のために設定できる必須パラメータとオプション パラメータについて説明します。

ロギングの設定

ロギング設定のオプションは、ローカルおよび外部のロギングに適用されます。ロギングの設定を行うには、 **Devices > Platform Settings**を参照。

選択 **Syslog > Logging Setup**を参照。

ロギングの基本的な設定

- Enable Logging：次を確認します。 **Enable Logging** チェックボックスをオンにして、ロギングを有効にします。これは必須オプションです。
- Enable Logging on the failover standby unit：次を確認します。 **Enable Logging on the failover standby unit** チェックボックスをオンにして、FTDハイアベイラビリティクラスタの一部であるスタンバイFTDのロギングを設定します。
- Send syslogs in EMBLEM format：次を確認します。 **Send syslogs in EMBLEM format** チェックボックスをオンにして、すべての宛先に対してSyslogの形式をEMBLEMとして有効にします。EMBLEM形式は、主に CiscoWorks Resource Manager Essentials（RME）の syslog アナライザに使用されます。この形式は、ルータとスイッチで生成されるCisco IOSソフトウェアのSyslog形式と一致します。これは、UDP syslog サーバでのみ利用できます。
- Send debug messages as syslogs：次を確認します。 **Send debug messages as syslogs** syslogメッセージとしてデバッグログをsyslogサーバに送信します。
- Memory size of the Internal Buffer:FTDがログデータを保存できる内部メモリバッファサイズを入力します。ログ データは、そのバッファの上限に達するとローテーションされます。

FTP サーバ情報（オプション）

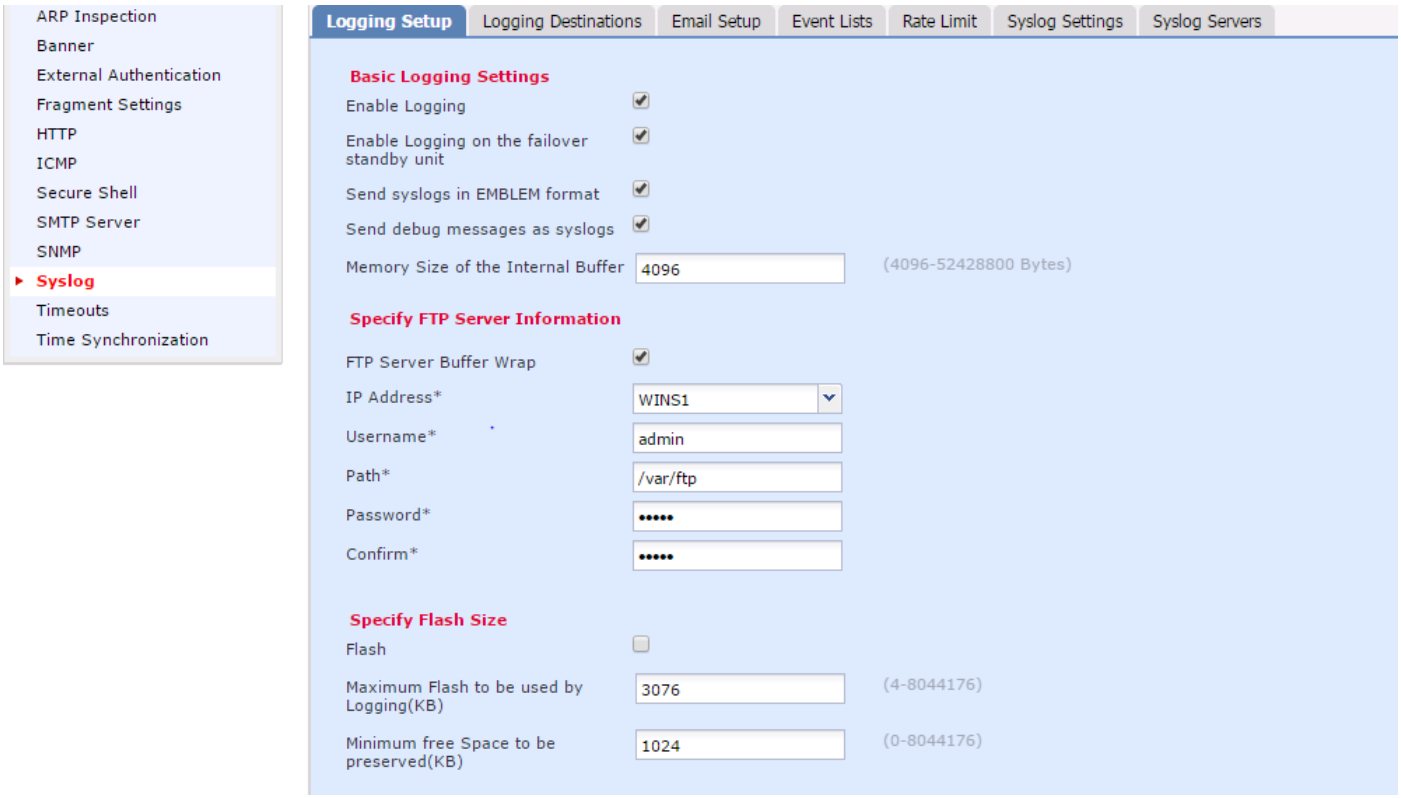
ログデータをFTPサーバに送信してから内部バッファを上書きする場合は、FTPサーバの詳細を指定します。

- FTP Server Buffer Wrap：次を確認します。 **FTP Server Buffer Wrap** チェックボックスをオンにして、バッファログデータをFTPサーバに送信します。
- IP Address: FTPサーバのIPアドレスを入力します。
- Username:FTPサーバのユーザ名を入力します。
- Path: FTPサーバのディレクトリパスを入力します。
- Password:FTPサーバのパスワードを入力します。
- Confirm：同じパスワードをもう一度入力します。

フラッシュ サイズ（オプション）

内部バッファがいっぱいになった場合、フラッシュする前にログ データを保存するには、フラッシュ サイズを指定します。

- Flash：次を確認します。 **Flash** チェックボックスをオンにして、ログデータを内部フラッシュに送信します。
- Maximum Flash to be used by Logging(KB)：ロギングに使用できるフラッシュメモリの最大サイズをKB単位で入力します。
- Minimum free Space to be preserved(KB)：保存する必要があるフラッシュメモリの最小サイズをKB単位で入力します。



クリック **Save** プラットフォーム設定を保存します。次のいずれかを選択します **Deploy** オプションで、変更を適用するFTDアプライアンスを選択し、 **Deploy** プラットフォーム設定の導入を開始します。

イベントリスト

Configure Event Listsオプションを使用すると、イベントリストを作成/編集し、イベントリストフィルタに含めるログデータを指定できます。イベントリストは、ロギングの宛先でロギングフィルタを設定するときに使用できます。

カスタム イベント リストの機能を使用するには、2 つのオプションを使用できます。

- クラスと重大度
- メッセージ ID

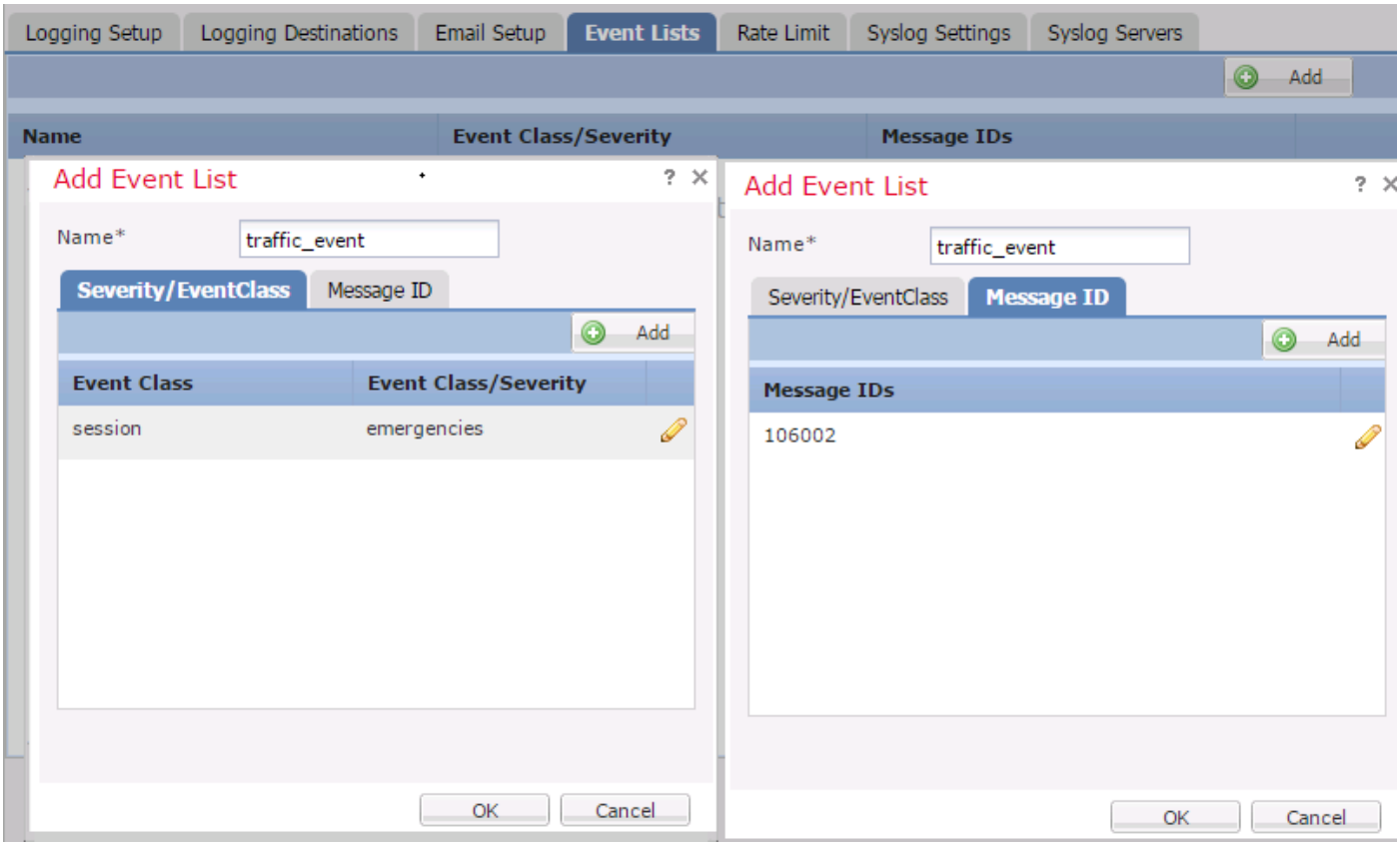
カスタムイベントリストを設定するには、 **Device > Platform Setting > Threat Defense Policy > Syslog > Event List** クリックして **Add**を参照。オプションは次のとおりです。

- Name：イベントリストの名前を入力します。
- Severity/Event Class：重大度/イベントクラスのセクションで、 **Add**を参照。
- Event Class：ドロップダウンリストから、必要なログデータのタイプに対応するイベントクラスを選択します。イベント クラスは、同じ機能を示す一連の syslog ルールを定義します。

たとえば、セッションに関連するすべてのSyslogを含むセッションのイベントクラスがあります。

- Syslog Severity：選択したイベントクラスのドロップダウンリストから重大度を選択します。重大度は 0 （緊急）~ 7 （デバッグ）の範囲で指定できます。

- Message ID：メッセージIDに関連する特定のログデータを確認するには、 **Add** メッセージIDに基づいてフィルタを適用します。
- Message IDs：メッセージIDを個別/範囲形式で指定します。



クリック **OK** 設定を保存します。

クリック **Save** プラットフォーム設定を保存します。次のいずれかを選択 **Deploy**変更を適用するFTDアプライアンスを選択し、 **Deploy**プラットフォーム設定の導入を開始します。

レート制限 syslog

Rate limitオプションは、設定されたすべての宛先に送信できるメッセージの数を定義し、レート制限を割り当てるメッセージの重大度を定義します。

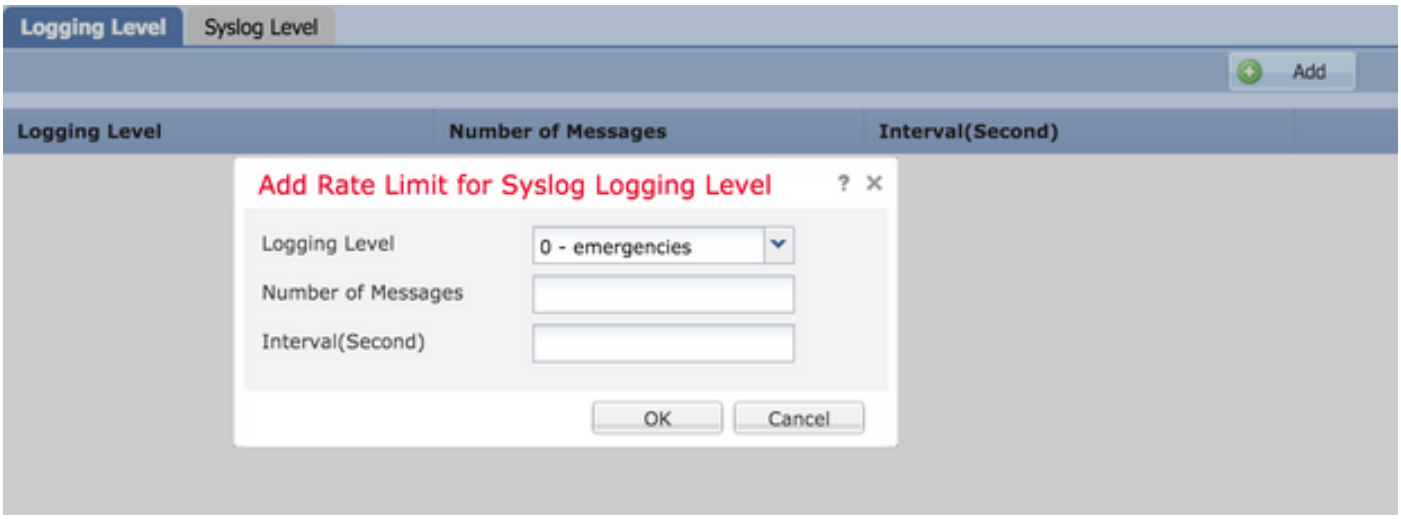
カスタムイベントリストを設定するには、 **Device > Platform Setting > Threat Defense Policy > Syslog > Rate Limit**を参照。次の 2 つのオプションに基づいてレート制限を指定できます。

- Logging level
- Syslog levels

ロギングレベルに基づくレート制限を有効にするには、 **Logging Level** クリックして **Add**を参照。

- Logging Level: **Logging Level** ドロップダウンリストから、レート制限を実行するログレベルを選択します。
- Number of Messages:指定された間隔内に受信できる syslog メッセージの最大数を入力します。
- Interval(Second)：以前に設定したNumber of Messagesパラメータに基づいて、Syslogメッセージの固定セットを受信できる時間間隔を入力します。

Syslogのレートは、メッセージ/間隔の数です。

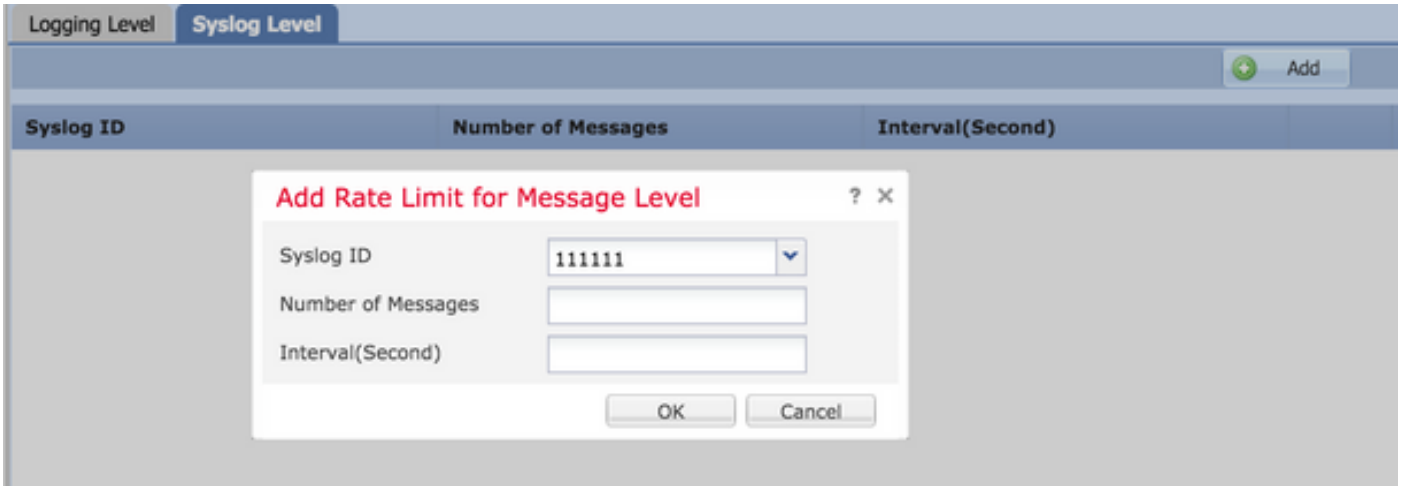


クリック **OK** ロギングレベルの設定を保存します。

ロギングレベルに基づくレート制限を有効にするには、 **Logging Level** クリックして **Add**を参照。

- Syslog ID:syslog ID は、syslog メッセージを一意に識別するのに使用されます。 **Syslog ID** ドロップダウンリストから、Syslog IDを選択します。
- Number of Messages:指定された間隔内に受信できる syslog メッセージの最大数を入力します。
- Interval(Second)：以前に設定したNumber of Messagesパラメータに基づいて、Syslogメッセージの固定セットを受信できる時間間隔を入力します。

Syslogのレートは、メッセージ数/インターバルです。



クリック **OK** syslogレベルの設定を保存します。

クリック **Save** プラットフォーム設定を保存します。次のいずれかを選択 **Deploy**変更を適用するFTDアプライアンスを選択し、 **Deploy** プラットフォーム設定の導入を開始します。

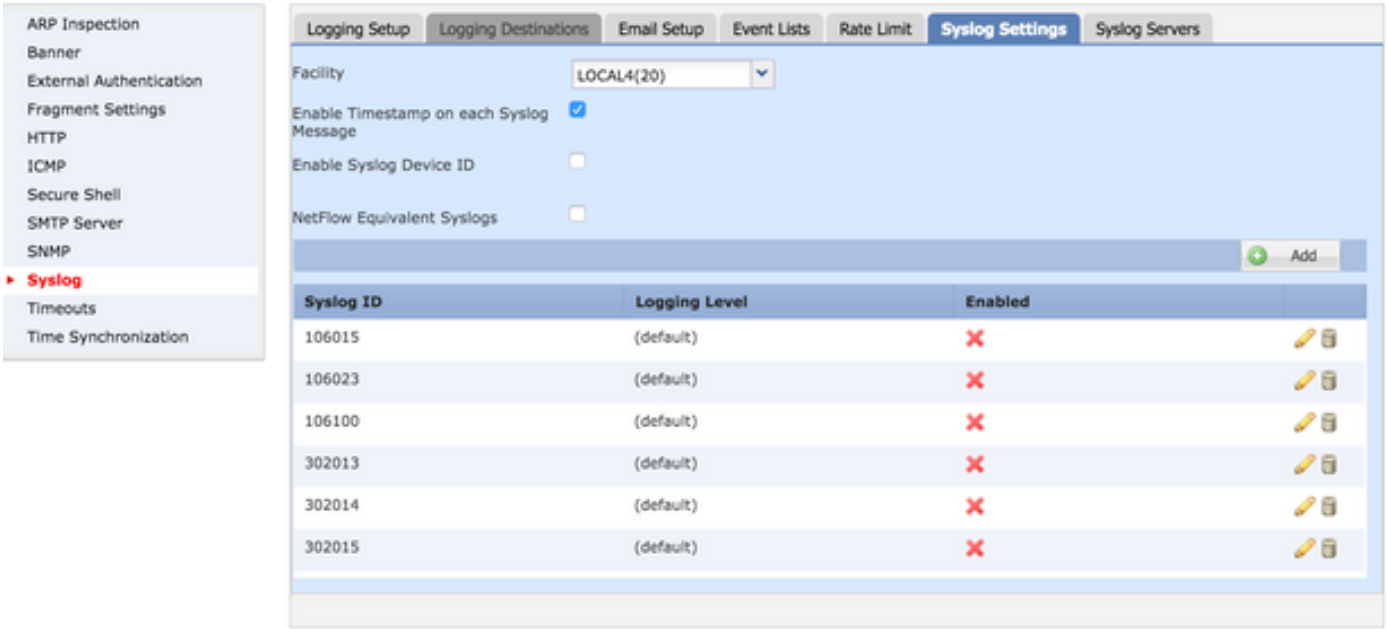
Syslog Settings

Syslog設定では、Facility値をSyslogメッセージに含めるように設定できます。また、ログ メッセ

ージやその他の syslog サーバ固有のパラメータにタイムスタンプを含めることができます。

カスタムイベントリストを設定するには、 **Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Settings**を参照。

- Facility:ファシリティ コードは、メッセージをロギングするプログラムの種類を指定するのに使用されます。異なるファシリティを持つメッセージは、異なる方法で処理できます。 **Facility** ドロップダウンリストから、ファシリティ値を選択します。
- Enable Timestamp on each Syslog Message：次を確認します。 **Enable Timestamp on each Syslog Message** syslogメッセージにタイムスタンプを含めるには、このチェックボックスをオンにします。
- Enable Syslog Device ID：次を確認します。 **Enable Syslog Device ID** チェックボックスをオンにして、非EMBLEM形式のsyslogメッセージにデバイスIDを含めます。
- Netflow Equivalent Syslogs：次を確認します。 **Netflow Equivalent Syslogs** netflowの同等のSyslogを送信する場合に使用します。アプライアンスのパフォーマンスに影響を与える可能性があります。
- 特定のSyslog IDの追加：追加のSyslog IDを指定するには、 **Add** を入力し、 **Syslog ID/ Logging Level** チェックボックスをオンにします。



クリック **Save** プラットフォーム設定を保存します。次のいずれかを選択 **Deploy**変更を適用するFTDアプライアンスを選択し、 **Deploy** プラットフォーム設定の導入を開始します。

ローカル ロギングの設定

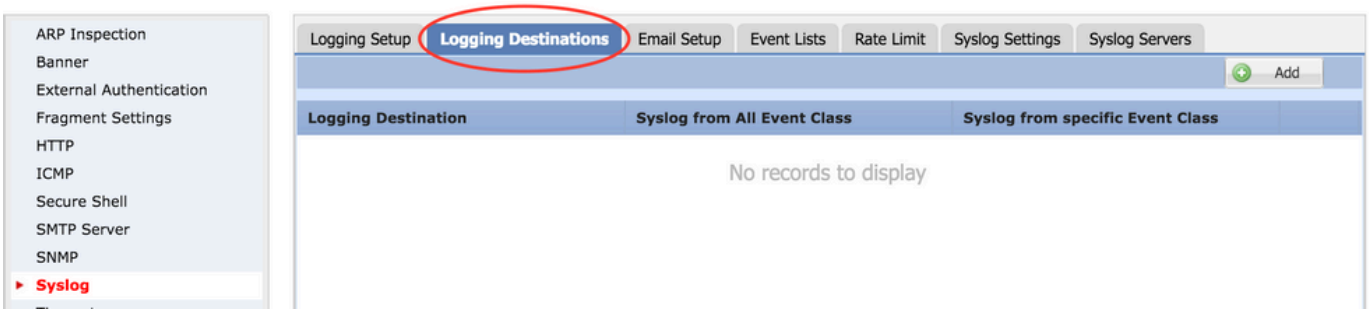
Logging Destinationセクションは、特定の宛先へのロギングを設定するために使用できます。

利用可能な内部ロギングの宛先は次のとおりです。

- 内部バッファ：内部ロギングバッファ（ロギングバッファ）にログを記録します。
- コンソール：ログをコンソール（ロギングコンソール）に送信します。
- SSHセッション：SSHセッションにSyslogを記録（ターミナルモニタ）

ローカル ロギングの設定には、次の 3 つの手順があります。

ステップ 1：選択 **Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations**を参照。



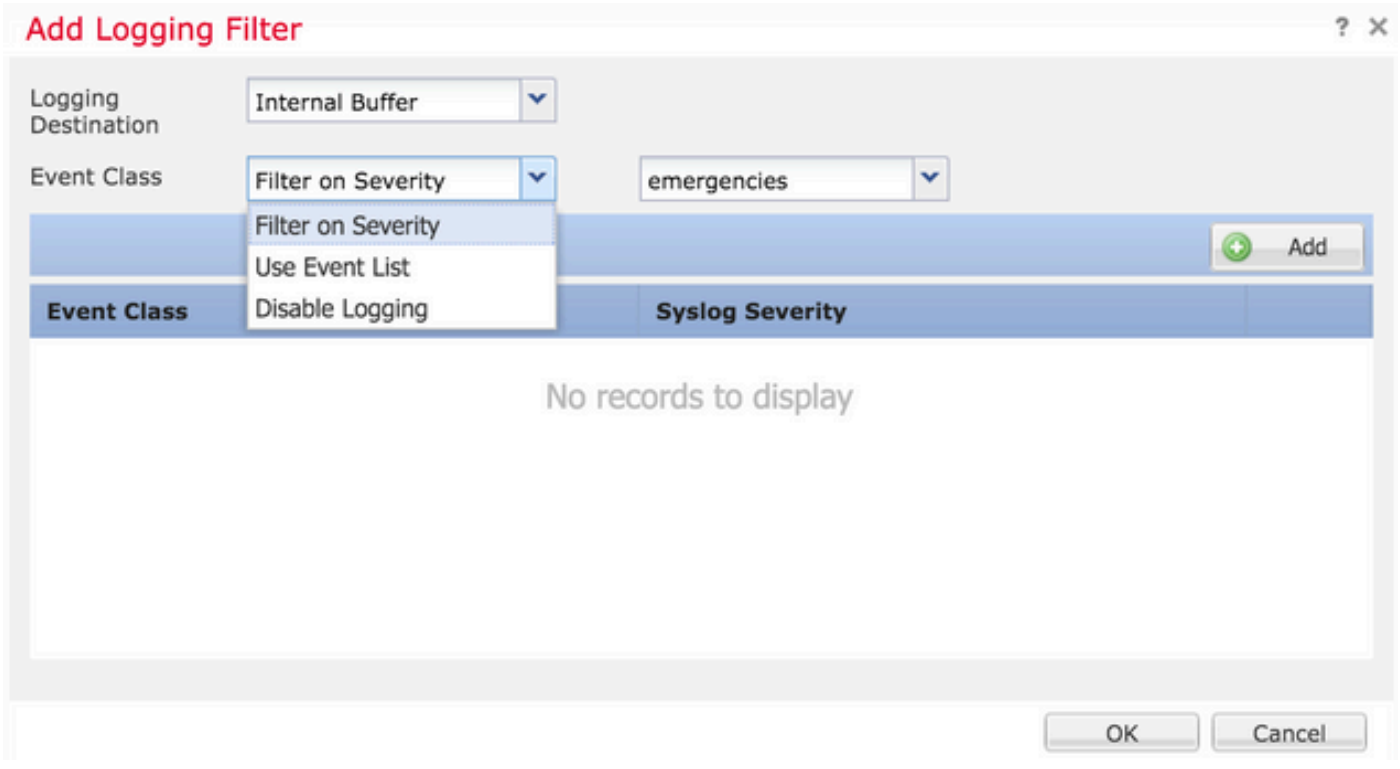
ステップ 2：クリック **Add** 特定のインターフェイスのロギングフィルタを **logging destination**を参照。

ロギングの宛先：必要なロギングの宛先を **Logging Destination** 「内部バッファ」、「コンソール」、または「SSHセッション」のドロップダウンリスト。

イベントクラス： **Event Class** ドロップダウンリストから、イベントクラスを選択します。前述したように、イベントクラスは同じ機能を表すsyslogのセットです。イベントクラスは次の方法で選択できます。

- Filter on Severity：イベントクラスは、Syslogの重大度に基づいてフィルタリングします。
- User Event List：管理者は、独自のカスタムイベントクラスを使用して特定のイベントリスト（前述）を作成し、このセクションで参照できます。
- Disable Logging：選択したロギング先およびログレベルのロギングを無効にするには、このオプションを使用します。

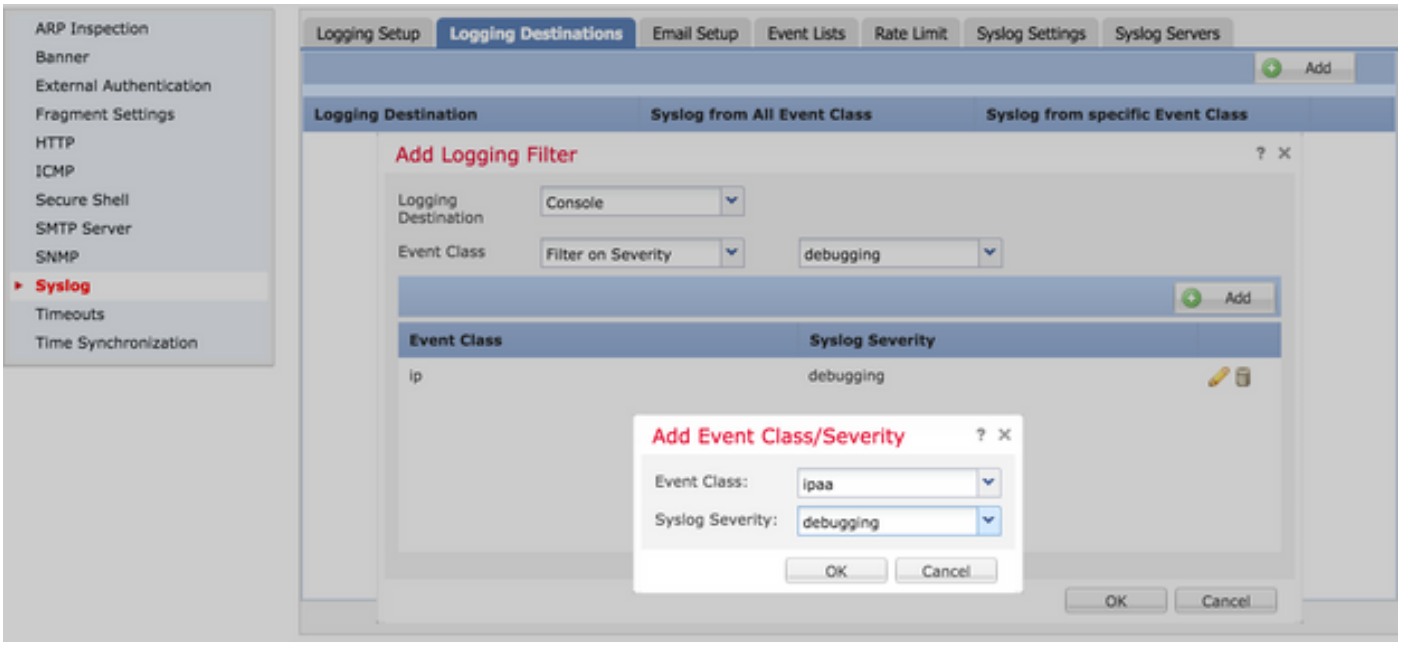
ログレベル：ドロップダウンリストからログレベルを選択します。ログレベルの範囲は0（緊急）から7（デバッグ）です。



ステップ 3：このロギングフィルタに個別のイベントクラスを追加するには、 **Add**を参照。

Event Class：次の中からイベントクラスを選択します。 **Event Class** 選択します。

Syslog Severity：次のリストからSyslog重大度を選択します。 **Syslog Severity** 選択します。



クリック **OK** 特定のロギング宛先に対してフィルタを追加するようにフィルタを設定したら、

クリック **Save** プラットフォーム設定を保存します。選択 **Deploy**変更を適用するFTDアプライアンスを選択し、 **Deploy** プラットフォーム設定の導入を開始します。

外部ロギングの設定

外部ロギングを設定するには、 **Device > Platform Setting > Threat Defense Policy > Syslog > Logging Destinations**を参照。

FTDは、これらのタイプの外部ロギングをサポートします。

- Syslogサーバ：リモートSyslogサーバにログを送信します。
- SNMPトラップ：ログをSNMPトラップとして送信します。
- Eメール：事前に設定されたメールリレーサーバを使用して、ログをEメールで送信します。

外部ロギングと内部ロギングの設定は同じです。ロギングの宛先を選択することで、実装されるロギングのタイプが決まります。カスタム イベント リストに基づいて、リモート サーバにイベント クラスを設定することができます。

リモートSyslogサーバ

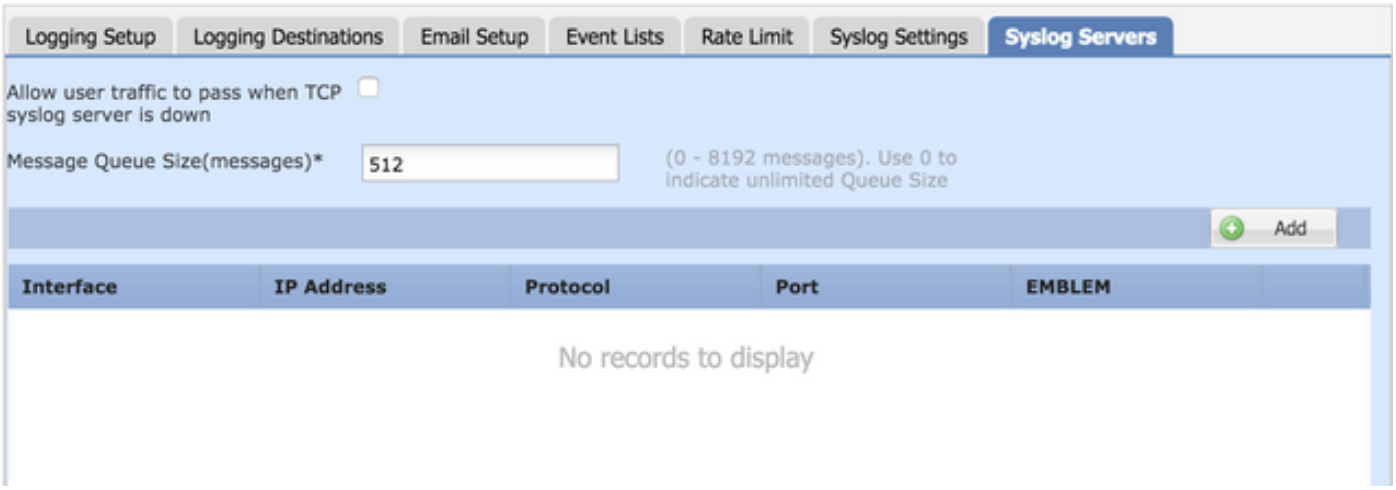
FTD からリモートでログを分析および保存するように syslog サーバを設定できます。

リモート syslog サーバの設定には、次の 3 つの手順があります。

ステップ 1：選択 **Device > Platform Setting > Threat Defense Policy > Syslog > Syslog Servers**を参照。

ステップ 2：Syslogサーバ関連のパラメータを設定します。

- TCP syslogサーバがダウンしているときにユーザトラフィックが通過することを許可する：TCP syslogサーバがネットワークに導入されており、到達不能な場合、ASAを通過するネットワークトラフィックは拒否されます。これは、ASA と syslog サーバ間のトランスポート プロトコルが TCP の場合だけ適用されます。次の項目を確認します。 **Allow user traffic to pass when TCP syslog server is down** syslogサーバがダウンしたときにトラフィックがインターフェイスを通過できるようにするチェックボックスをオンにします。
- Message Queue Size：メッセージキューサイズは、リモートSyslogサーバがビジーでログメッセージを受け付けない場合に、FTDでキューイングされるメッセージの数です。デフォルトは512メッセージで、最小値は1メッセージです。このオプションに 0 を指定すると、キュー サイズは無制限とみなされます。



ステップ 3：リモートSyslogサーバを追加するには、 **Add**を参照。

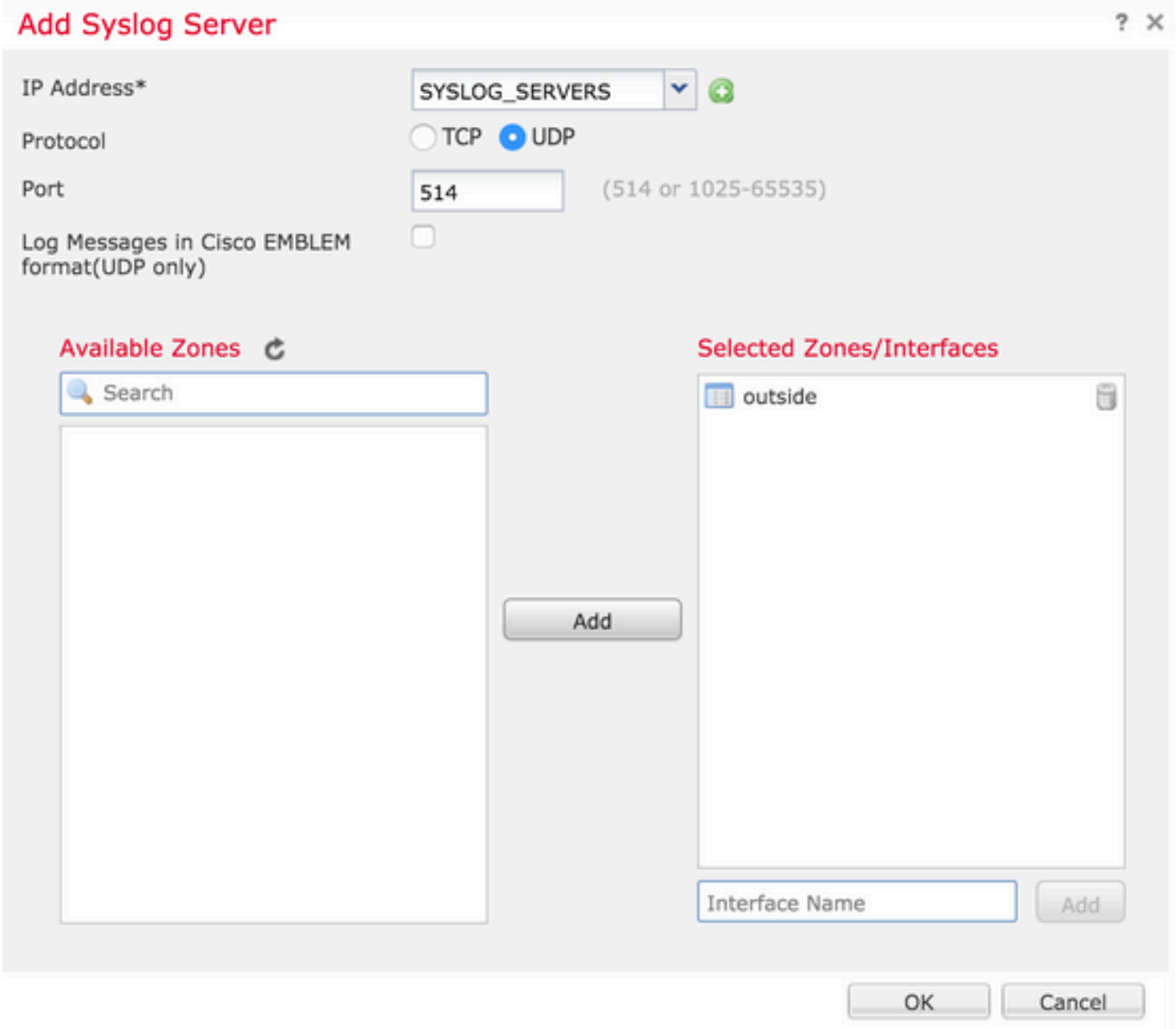
IP Address: **IP Address** ドロップダウンリストから、Syslogサーバがリストされているネットワークオブジェクトを選択します。ネットワークオブジェクトを作成していない場合は、プラス(+)アイコンをクリックして新しいオブジェクトを作成します。

Protocol：次のいずれかをクリック **TCP** または **UDP** Syslog通信用のオプションボタンです。

Port:Syslogサーバのポート番号を入力します。デフォルトでは 514 です。

Log Messages in Cisco EMBLEM format(UDP only):ポリシーの横の [レポート（Report）] **Log Messages in Cisco EMBLEM format (UDP only)** チェックボックスをオンにして、Cisco EMBLEM形式でメッセージをログに記録する必要がある場合にこのオプションを有効にします。これは、UDP ベースの syslog のみに適用されます。

Available Zones:Syslogサーバが到達可能なセキュリティゾーンを入力し、それをSelected Zones/Interfaces列に移動します。



クリック **OK** と **Save** 設定を保存します。

クリック **Save** プラットフォーム設定を保存します。選択 **Deploy**変更を適用するFTDアプライアンスを選択し、 **Deploy** プラットフォーム設定の導入を開始します。

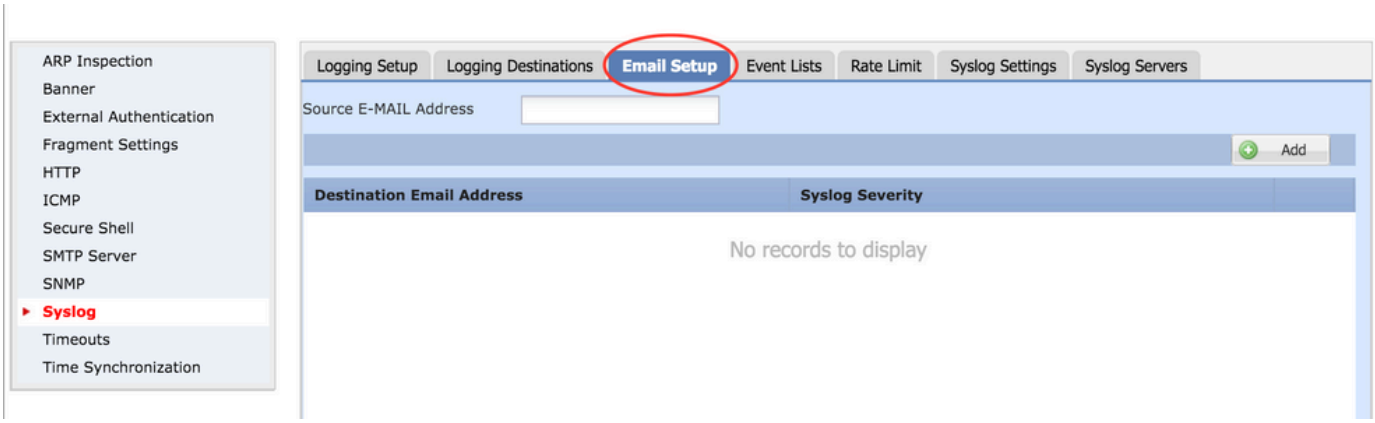
ロギングの電子メール設定

FTDでは、特定の電子メールアドレスにSyslogを送信できます。電子メールは、電子メールリレーサーバがすでに設定されている場合にのみ、ロギングの宛先として使用できます。

Syslogの電子メール設定を設定するには、2つの手順があります。

ステップ 1：選択 **Device** > **Platform Setting** > **Threat Defense Policy** > **Syslog** >**Email Setup**を参照。

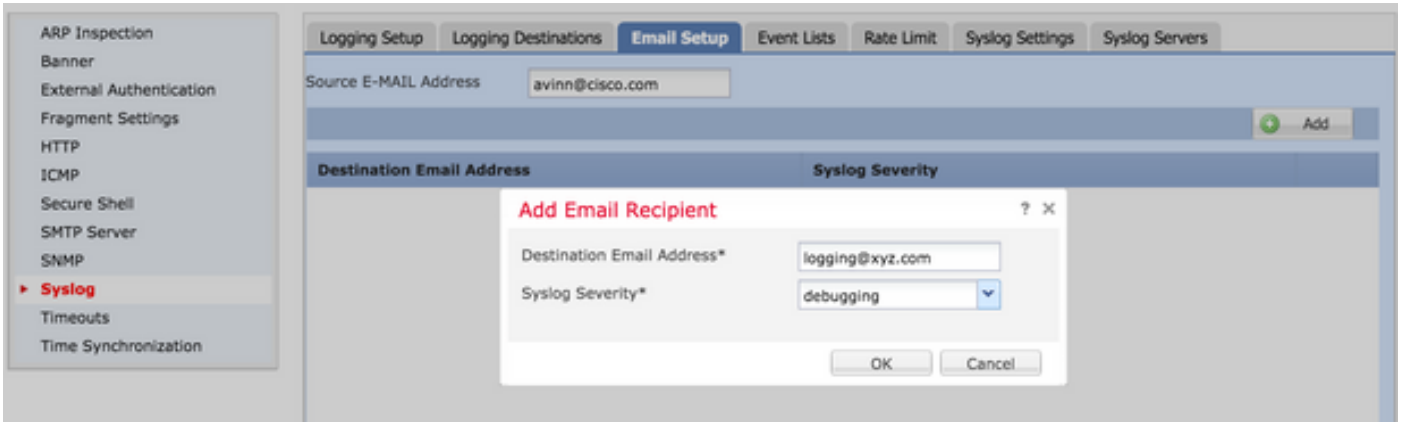
Source E-MAIL Address:FTDから送信され、Syslogを含むすべての電子メールに表示される送信元の電子メールアドレスを入力します。



ステップ 2：宛先の電子メールアドレスとSyslogの重大度を設定するには、 **Add**を参照。

Destination Email Address:Syslogメッセージの送信先の電子メールアドレスを入力します。

Syslog Severity：次のリストからSyslog重大度を選択します。 **Syslog Severity** 選択します。



クリック **OK** 設定を保存します。

クリック **Save** プラットフォーム設定を保存します。選択 **Deploy**変更を適用するFTDアプライアンスを選択し、 **Deploy** プラットフォーム設定の導入を開始します。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

- FTD CLIでFTD Syslog設定を確認します。FTDの管理インターフェイスにログインし、 **system support diagnostic-cli** コマンドを発行して、診断CLIにコンソール接続します。

```
> 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
```

- FTD から syslog サーバに到達可能であることを確認します。SSH経由でFTD管理インターフェイスにログインし、 **ping** コマンドを使用して、アップグレードを実行します。

```
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
```

- FTDとSyslogサーバ間の接続を確認するために、パケットキャプチャを取得できます。SSH経由でFTD管理インターフェイスにログインし、コマンドを入力します。 **system support diagnostic-cli**を参照。パケットキャプチャコマンドについては、『CLIおよびASDMでのASAパケットキャプチャの設定例』を参照してください。
- ポリシーの展開が正常に適用されていることを確認します。

関連情報

- ASA 向け Cisco Firepower Threat Defense クイック スタート ガイド
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。