FMCでsyslogのトラブルシューティングを送信および表示するためのデバイスの設定

内容

はじめに

このドキュメントでは、FMCに診断syslogメッセージを送信し、Unified Event Viewerで表示するように管理対象デバイス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。
•syslog メッセージ
•Firepower Management Center（FMC）
•Firepower Threat Defense（FTD）

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。
・ このドキュメントは、すべてのFirepowerプラットフォームに適用されます。
・ ソフトウェアバージョン7.6.0を実行するSecure Firewall Threat Defense Virtual(FTD)
・ ソフトウェアバージョン7.6.0が稼働するSecure Firewall Management Center Virtual(FMC)
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。

機能の概要

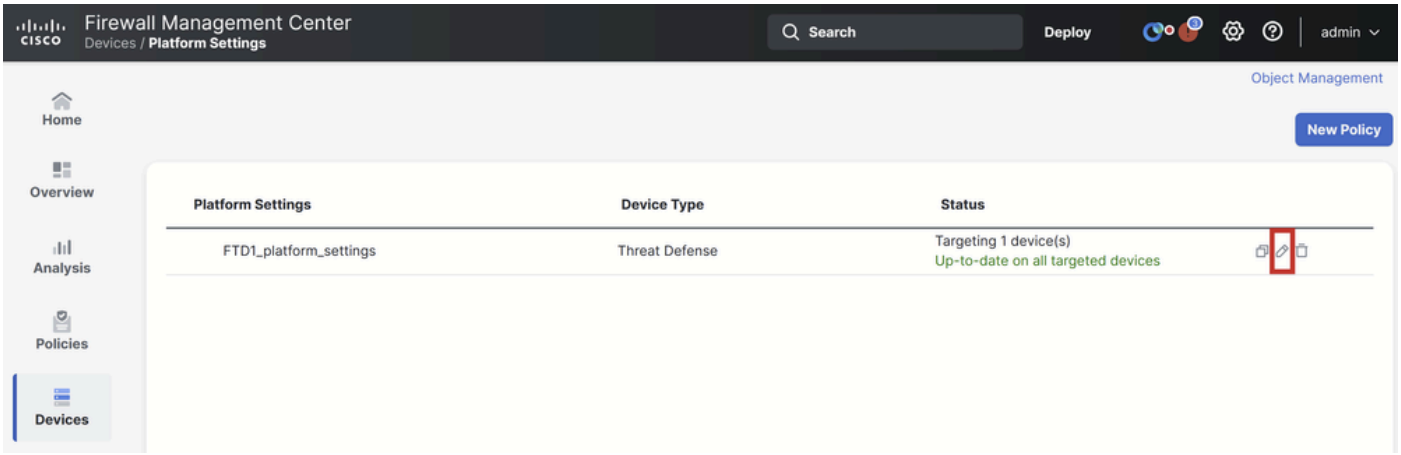
Secure Firewall 7.6では、新しいトラブルシューティングイベントタイプがUnified Event Viewerテーブルに追加されました。プラットフォーム設定のsyslog口ギング設定が拡張され、VPN口グだけでなく、LINAによって生成された診断syslogメッセージのFMCへの送信がサポート

されるようになりました。この機能は、FMC 7.6.0と互換性のあるソフトウェアバージョンを実行しているすべてのFTDで設定できます。cdFMCには分析ツールがないため、cdFMCはサポートされていません。

- [すべてのログ]オプションは、イベント・ボリュームによる緊急、アラート、重大のログ・レベルに制限されています。
- これらのトラブルシューティングログには、デバイス（ASAを含む）からFMC（VPNまたはその他）に送信されたsyslogが表示されます。
- トラブルシューティングログはFMCに送信され、Unified Event ViewおよびDevices > Troubleshoot > Troubleshooting Logsに表示されます。

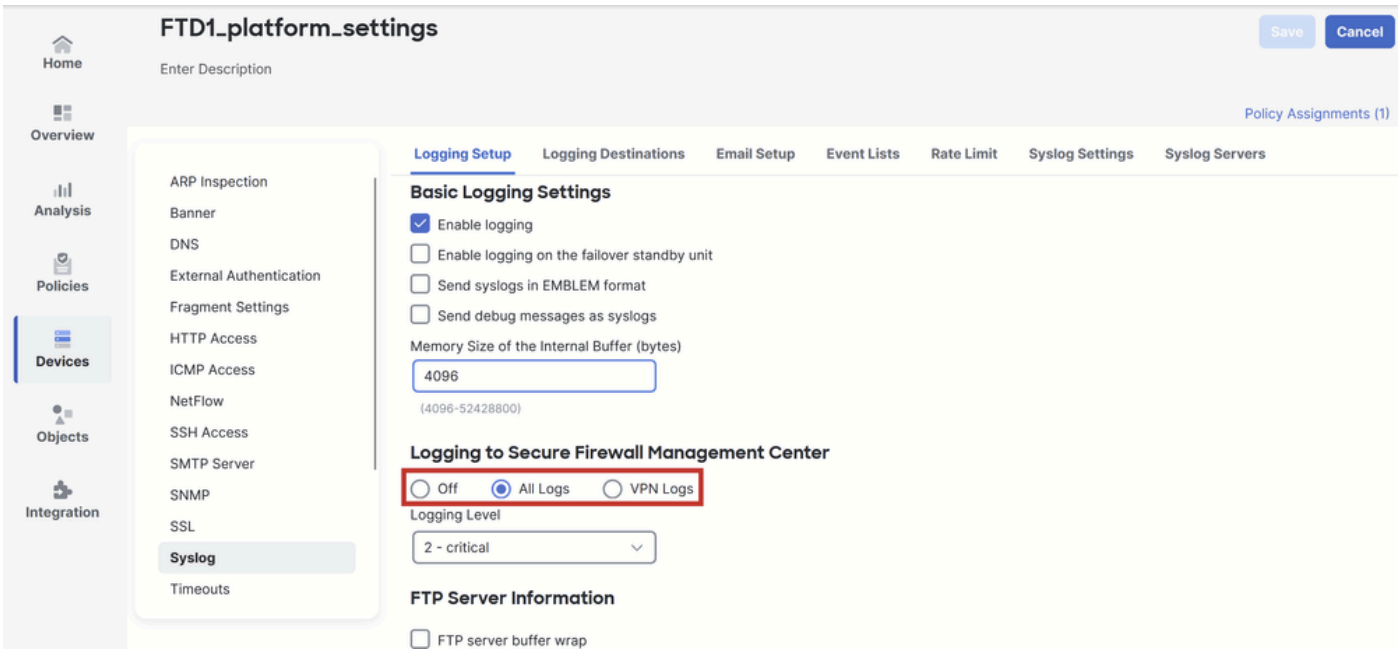
設定

FMC Devices > Platform Settingsの順に移動し、ポリシーの右上隅にあるEditアイコンをクリックします。



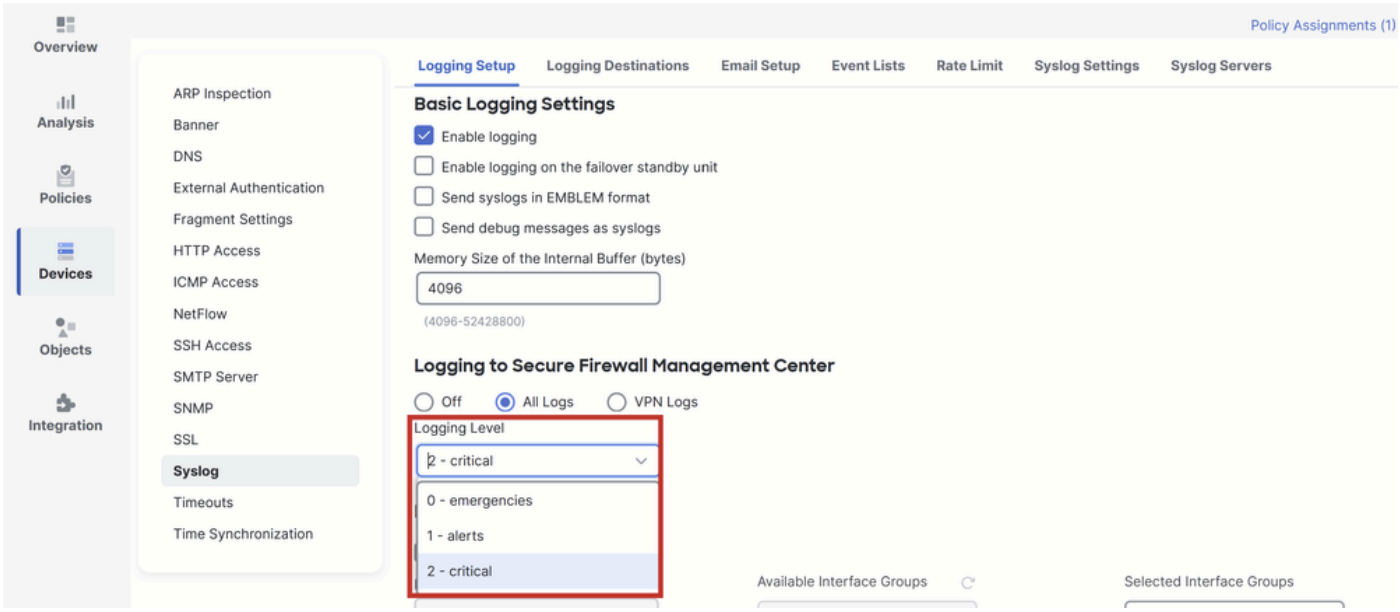
プラットフォーム設定ポリシー

Syslog > Logging Setupの順に進みます。Logging to Secure Firewall Management Centerの下に3つのオプションが表示されます。



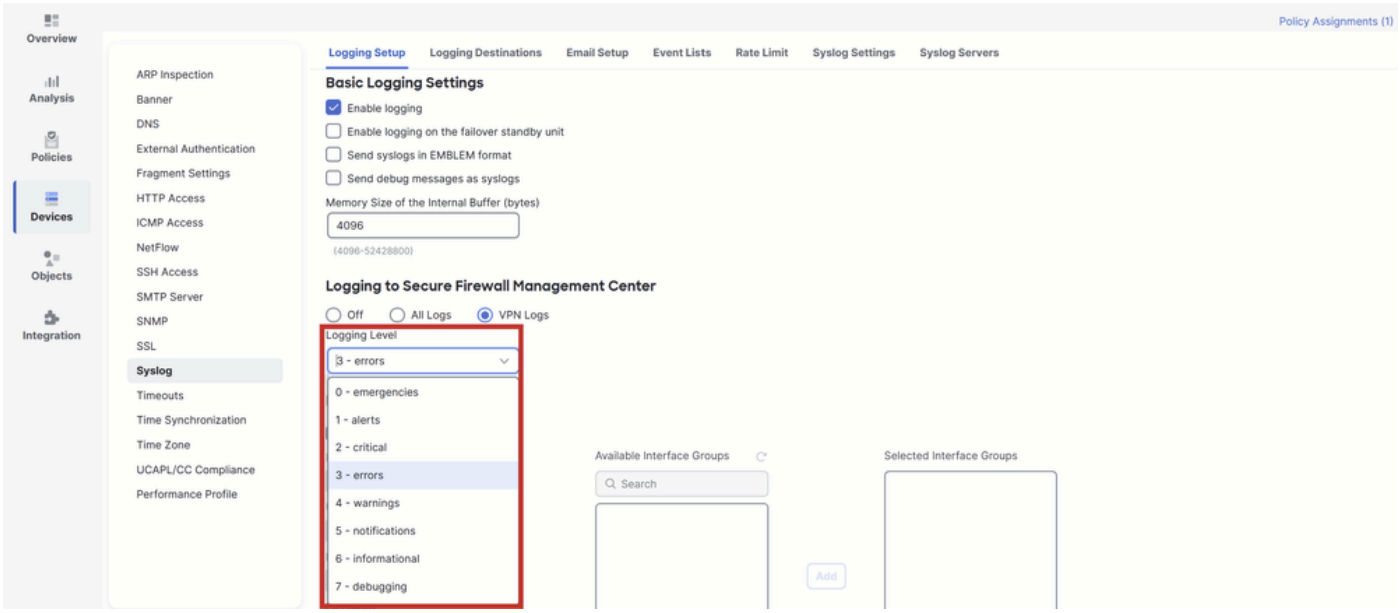
3つのロギングオプション

All Logsを選択した場合、使用可能な3つのログレベル（緊急、アラート、重大）のいずれかを選択して、すべての診断syslogメッセージをFMC（VPNを含む）に送信できます。

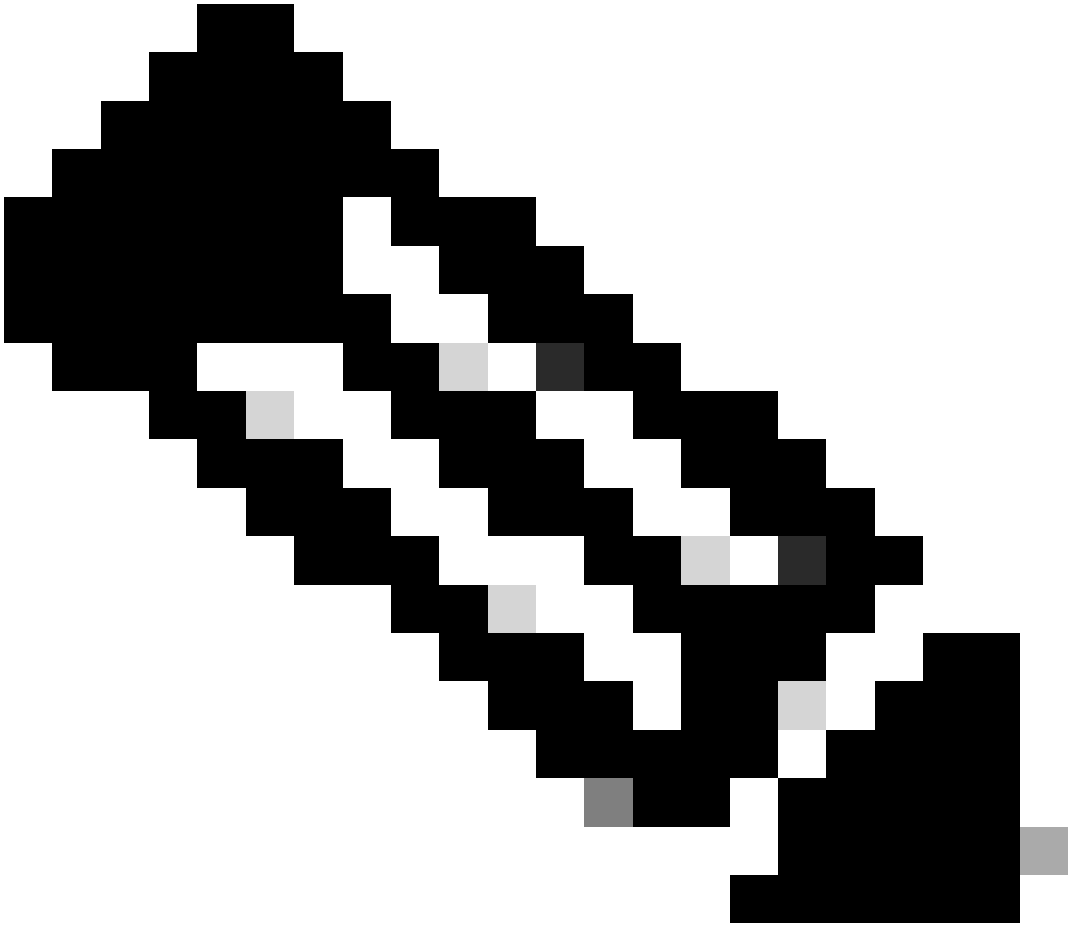


使用可能なログレベル

VPN Logsを選択すると、すべてのログレベルが使用可能になり、その中の1つを選択できます。

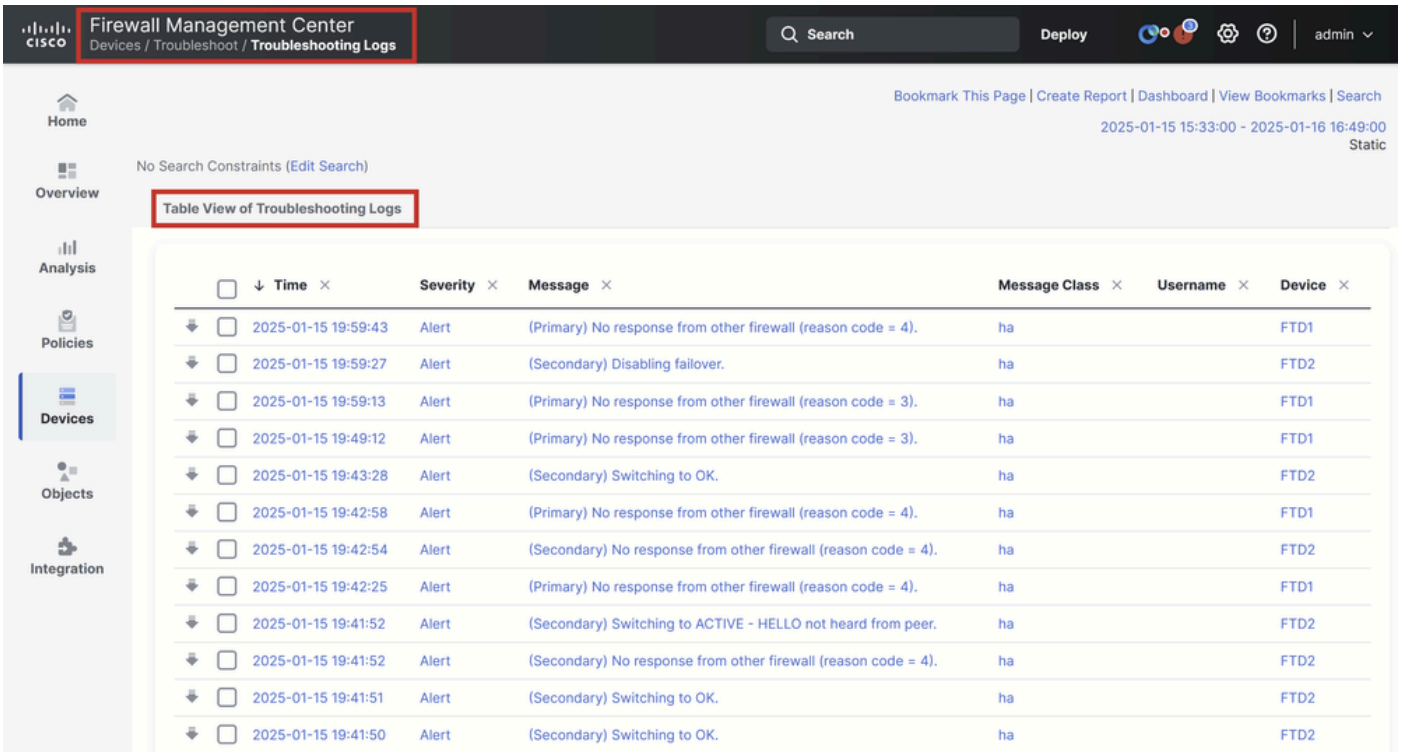


使用可能なログレベル



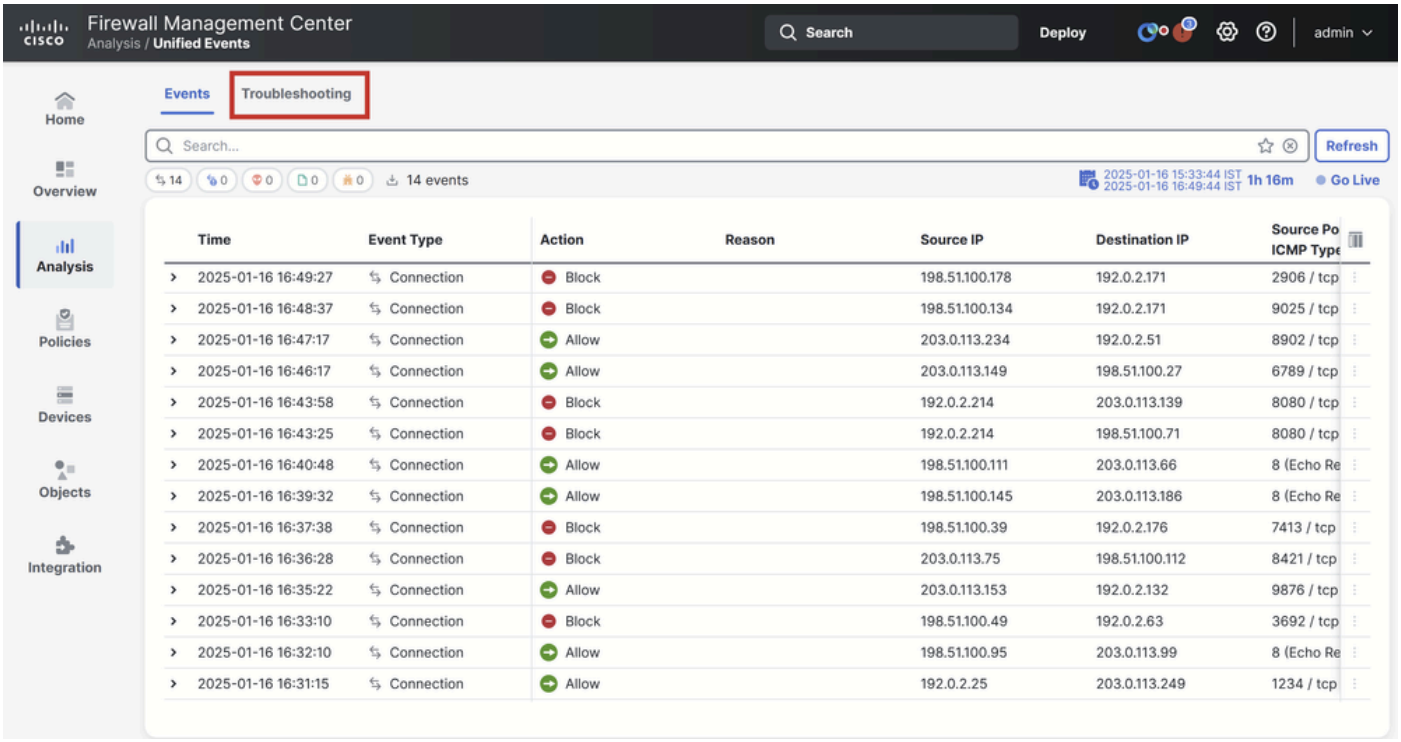
注：デバイスにサイト間VPNまたはリモートアクセスVPNを設定すると、デフォルトでVPN syslogの管理センターへの送信が自動的に有効になります。これをAll Logsに変更すると、VPNログ以外のすべてのsyslogをFMCに送信できます。

これらの口グには、Devices > Troubleshoot > Troubleshooting Logsからアクセスできます。



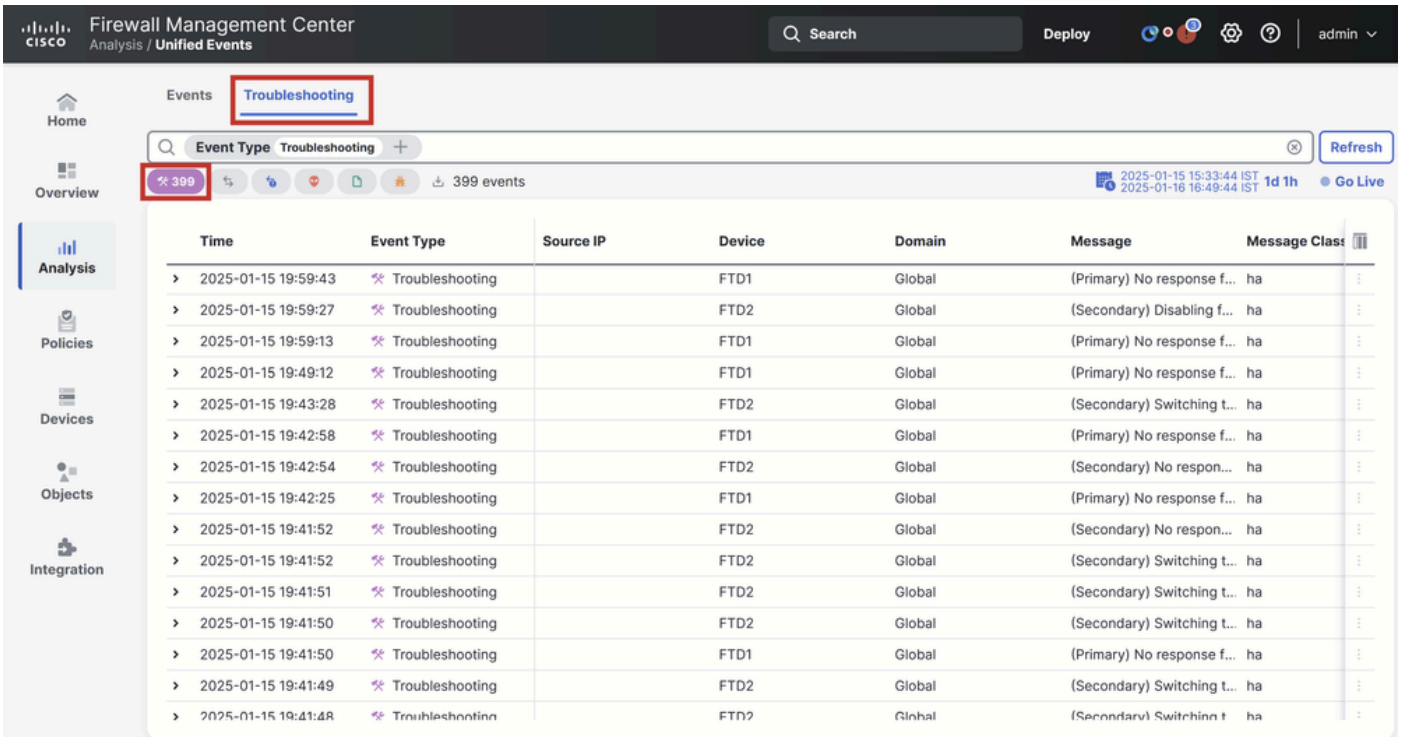
トラブルシューティングログのテーブルビュー

新しい[Troubleshooting view]タブが[Unified Event Viewer]ページで使用できるようになりました。これらのイベントを表示するには、Analysis > Unified Events > Troubleshootingの順に選択します。



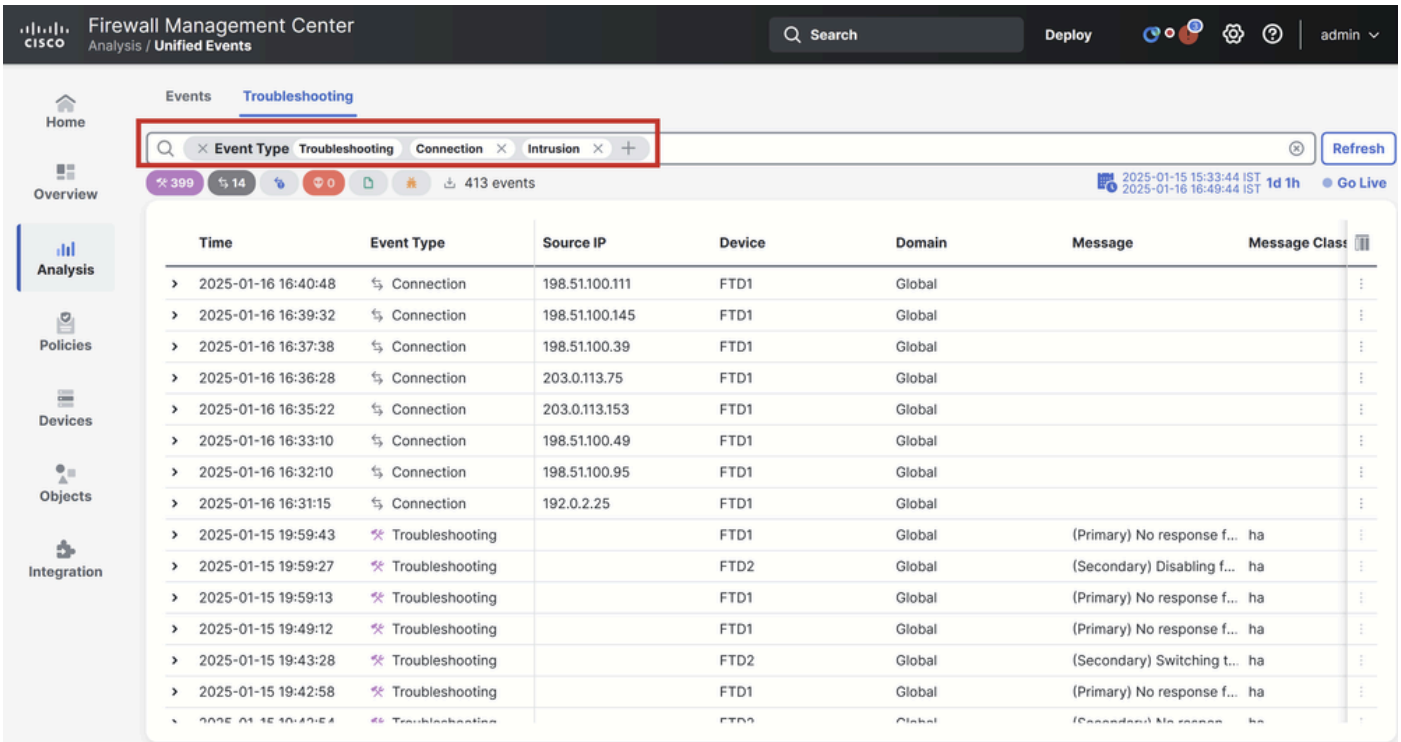
トラブルシューティングビュー

このタブに切り替えると、新しいイベントタイプがテーブル内に表示されます。これはトラブルシューティングビューの中心であるため、他のタイプのようにビューに追加したりビューから削除したりすることはできません。



トラブルシューティングのイベントの種類

このトラブルシューティングビューでは、他のイベントタイプの追加や削除も可能です。これにより、他のイベントデータとともに診断ログを表示できます。



その他のイベントタイプ

設定を検証する

FMCのGUIから設定を行ったら、CLISHモードまたはLINAモードでshow running-config loggingコマンドとshow loggingコマンドを実行することにより、FTD CLIから設定を確認できます。

```
FTD1# show running-config logging
logging enable
logging timestamp
logging list MANAGER_ALL_SYSLOG_EVENT_LIST level critical
logging buffered errors
logging FMC MANAGER_ALL_SYSLOG_EVENT_LIST
logging device-id hostname
logging permit-hostdown
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
no logging message 302016
no logging message 302021
no logging message 302020
```

FTD CLIコマンド

```
FTD1# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: enabled
    Timezone: disabled
    Logging Format: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level errors, 45 messages logged
    Trap logging: disabled
    Permit-hostdown logging: enabled
    History logging: disabled
    Device ID: hostname "FTD1"
    Mail logging: disabled
    ASDM logging: disabled
    FMC logging: list MANAGER_ALL_SYSLOG_EVENT_LIST, 45 messages logged
```

FTD CLIコマンド

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。