Konfigurieren von Geräten zum Senden und Anzeigen von Fehlerbehebungs-Syslogs auf FMC

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie verwaltete Geräte so konfiguriert werden, dass sie Syslog-Diagnosemeldungen an FMC senden und diese in der Unified Event Viewer anzeigen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:
- Syslog-Meldungen
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:
- Dieses Dokument gilt für alle Firepower-Plattformen.
- Secure Firewall Threat Defense Virtual (FTD) mit der Softwareversion 7.6.0
- Secure Firewall Management Center Virtual (FMC) mit der Softwareversion 7.6.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

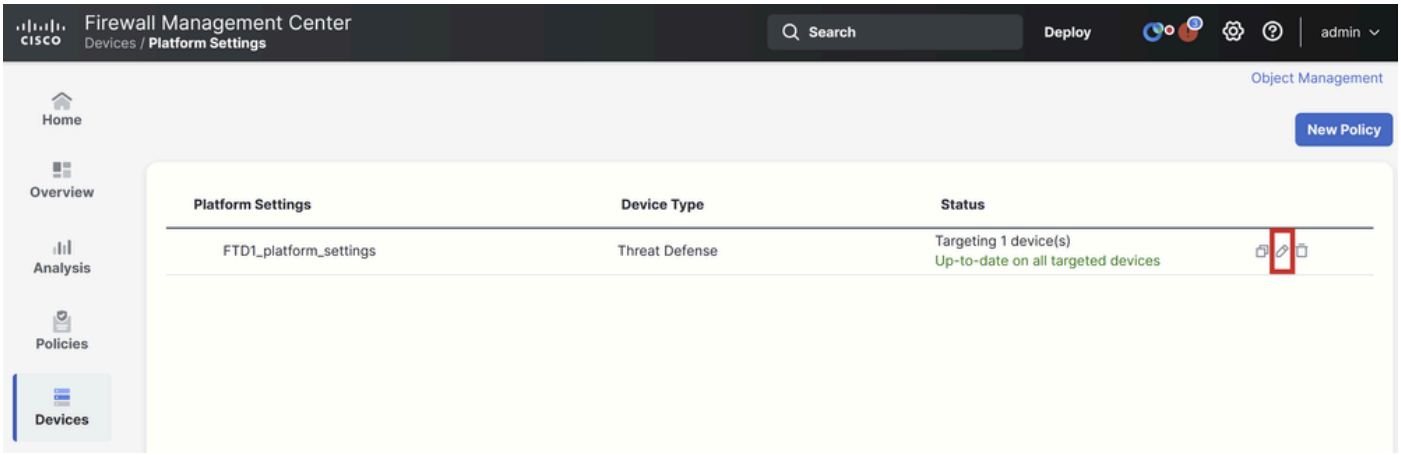
Funktionsüberblick

In Secure Firewall 7.6 wird der neue Fehlerbehebungsereignistyp in der Tabelle Unified Event Viewer hinzugefügt. Die Syslog-Protokollierungskonfiguration für die Plattformeinstellungen wurde erweitert. Sie unterstützt das Senden von LINA-generierten Syslog-Diagnosemeldungen an das FMC anstelle von VPN-Protokollen. Diese Funktion kann auf jedem FTD konfiguriert werden, auf dem eine mit FMC 7.6.0 kompatible Softwareversion ausgeführt wird. cdFMC wird nicht unterstützt, da cdFMC nicht über Analysetools verfügt.

- Die Option "Alle Protokolle" ist aufgrund des Ereignisvolumens auf Notruf-, Alarm- und kritische Protokollstufen beschränkt.
- Diese Fehlerbehebungsprotokolle zeigen alle Syslog-Protokolle an, die vom Gerät an das FMC (VPN oder andere) gesendet wurden.
- Die Fehlerbehebungsprotokolle werden an das FMC übertragen und sind in der einheitlichen Ereignisansicht und unter Geräte > Fehlerbehebung > Fehlerbehebungsprotokolle sichtbar.

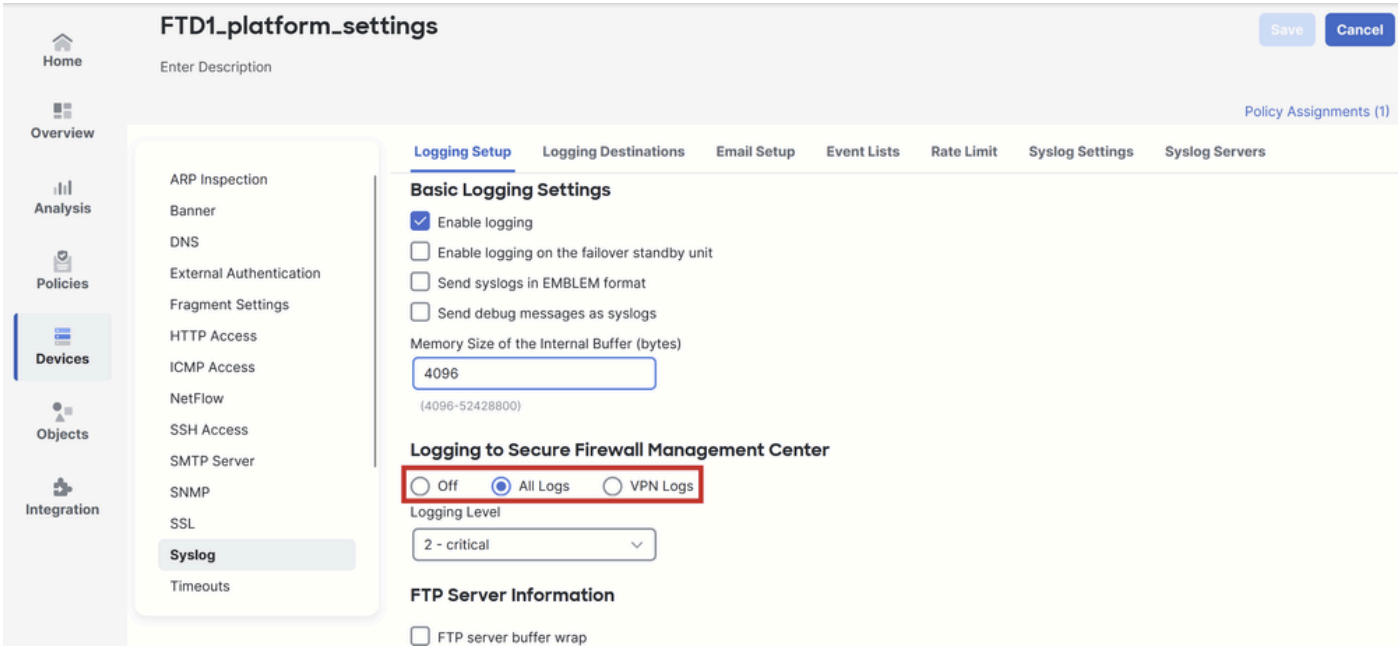
Konfigurieren

Navigieren Sie zu FMC Devices > Platform Settings, und klicken Sie oben rechts in der Richtlinie auf das Symbol Edit (Bearbeiten).



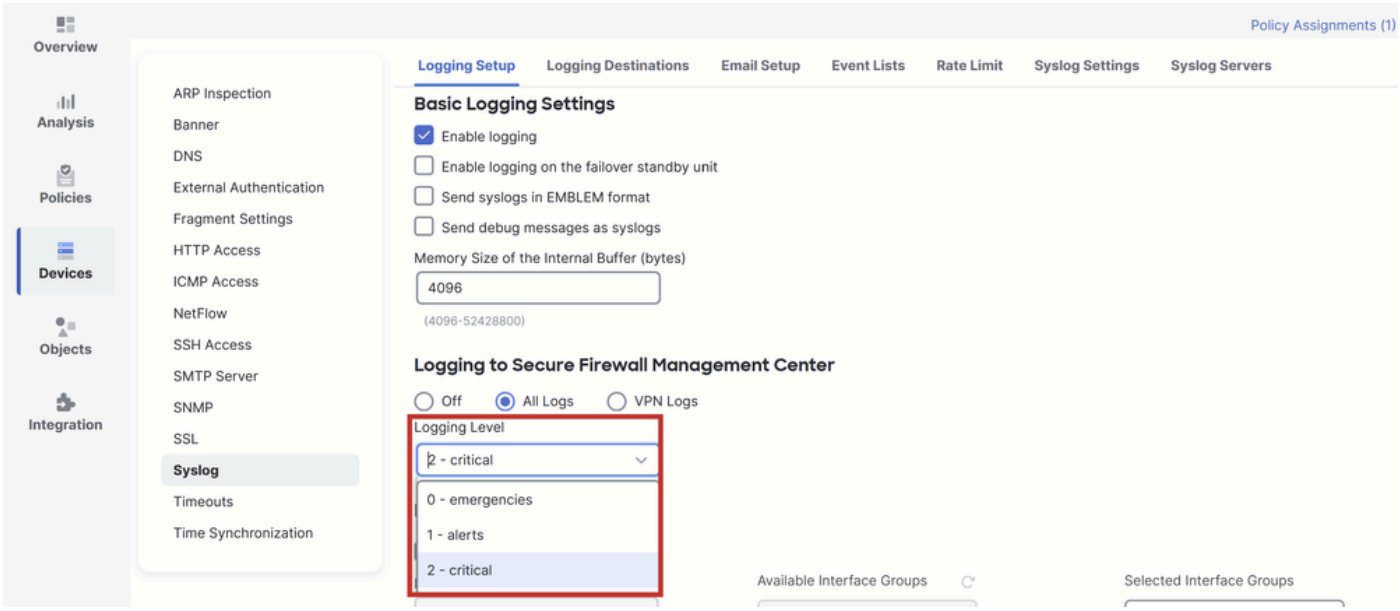
Richtlinie für Plattformeinstellungen

Wechseln Sie zu Syslog > Logging Setup. Unter Protokollierung beim sicheren Firewall-Management-Center werden drei Optionen angezeigt.



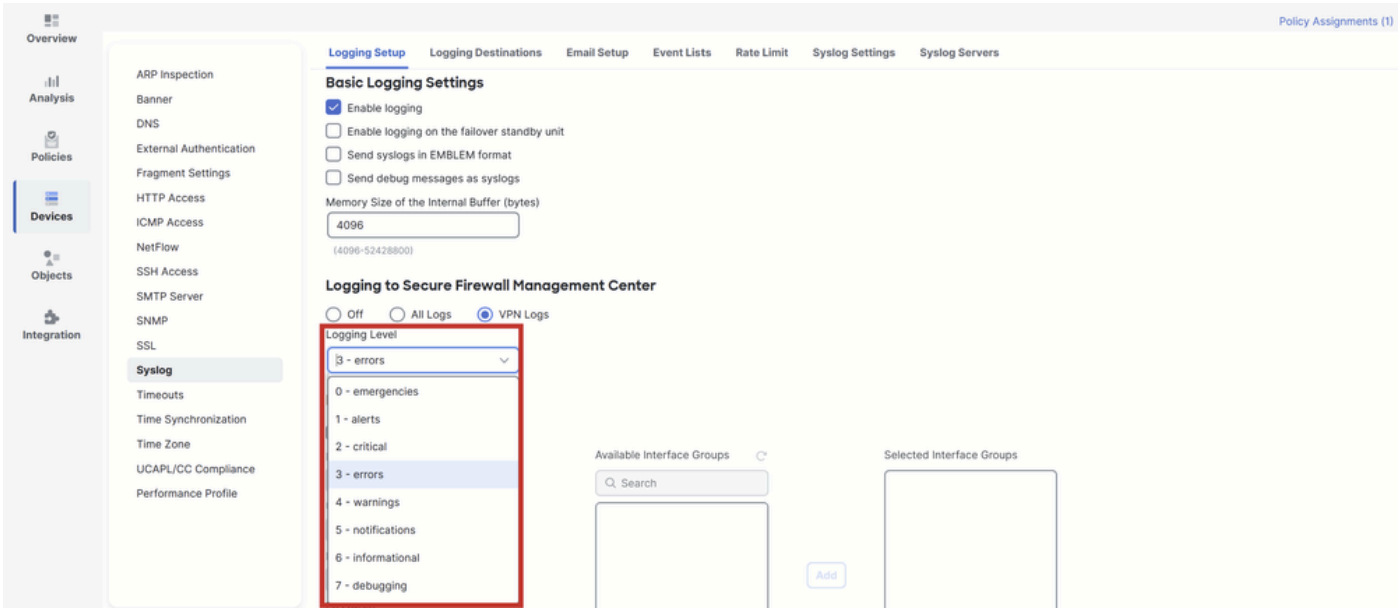
Drei Protokollierungsoptionen

Wenn Sie Alle Protokolle auswählen, können Sie eine der drei verfügbaren Protokollierungsebenen auswählen: Notfälle, Warnungen und kritische Meldungen aus und senden alle Syslog-Diagnosemeldungen an FMC (einschließlich VPN).

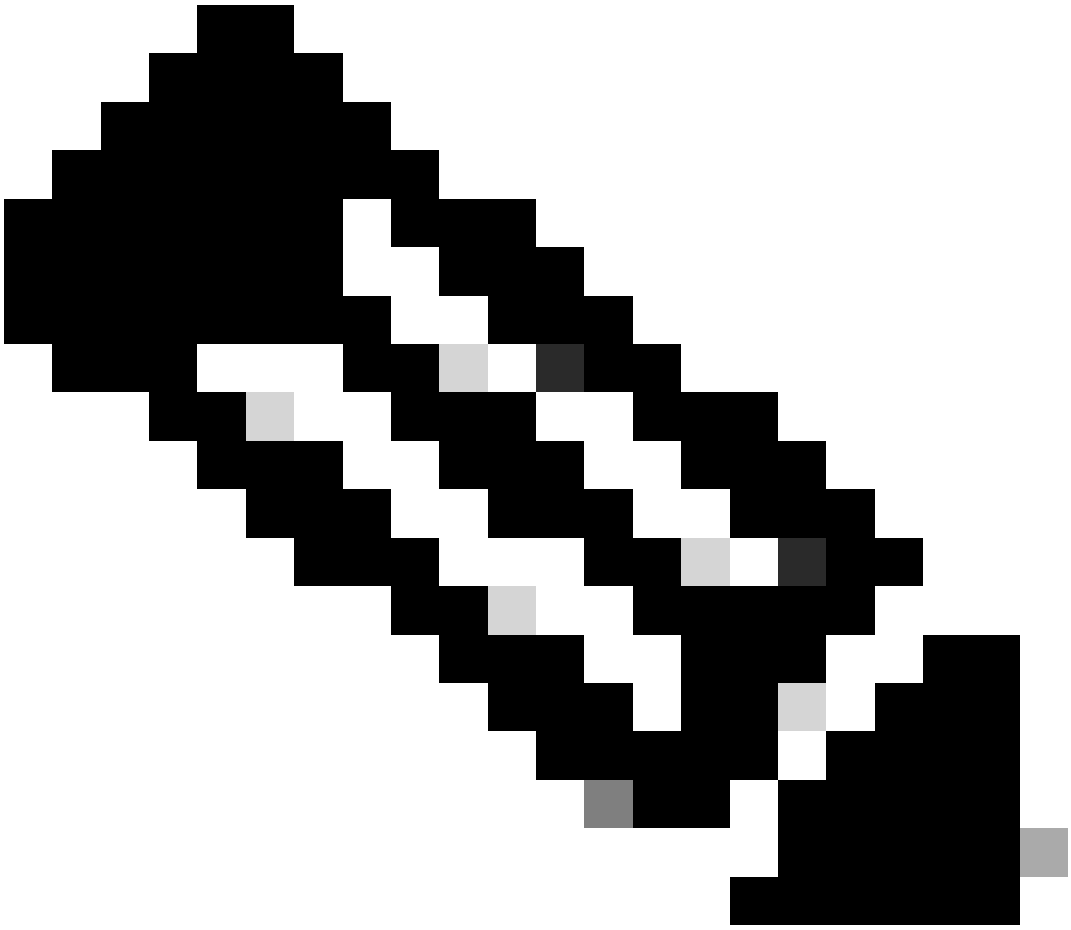


Verfügbare Protokollierungsebenen

Wenn Sie VPN-Protokolle auswählen, sind alle Protokollierungsebenen verfügbar, und eine davon kann ausgewählt werden.



Verfügbare Protokollierungsebenen

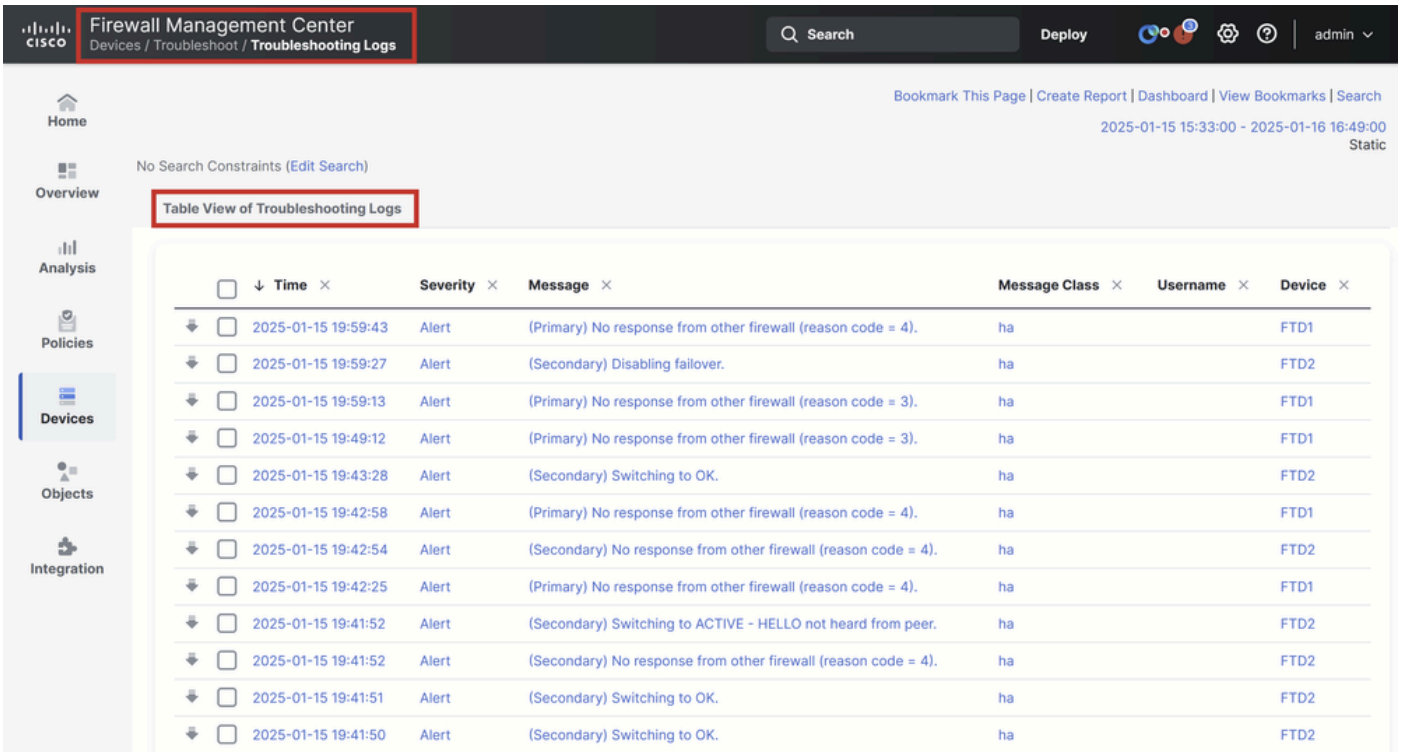


Anmerkung: Wenn Sie ein Gerät mit Site-to-Site- oder Remote Access-VPN konfigurieren,

---

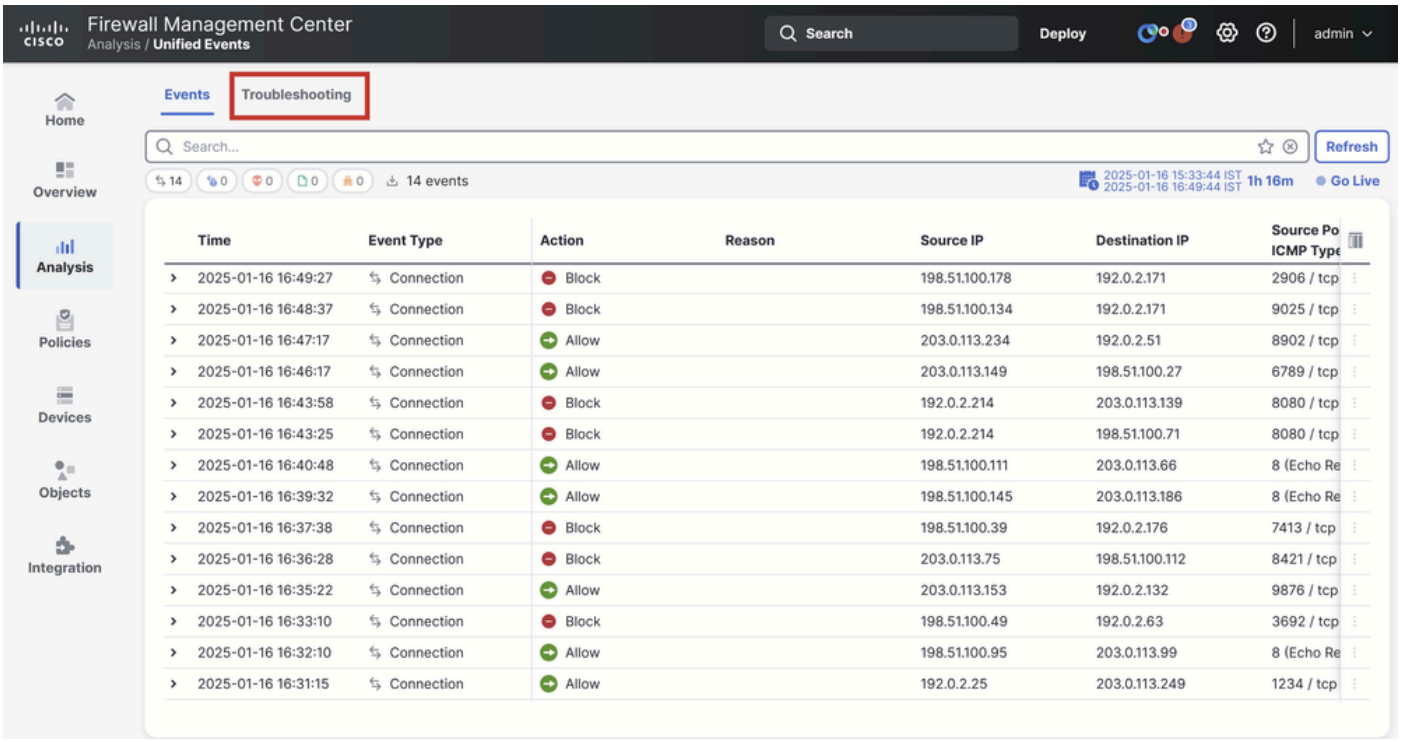
aktiviert es standardmäßig automatisch das Senden von VPN-Syslogs an das Management Center. Sie können sie in All Logs (Alle Protokolle) ändern, um alle Syslogs außer den VPN-Protokollen an FMC zu senden.

Auf diese Protokolle kann von Devices (Geräte) > Troubleshoot (Fehlerbehebung) > Troubleshooting Logs (Fehlerbehebungsprotokolle) zugegriffen werden.



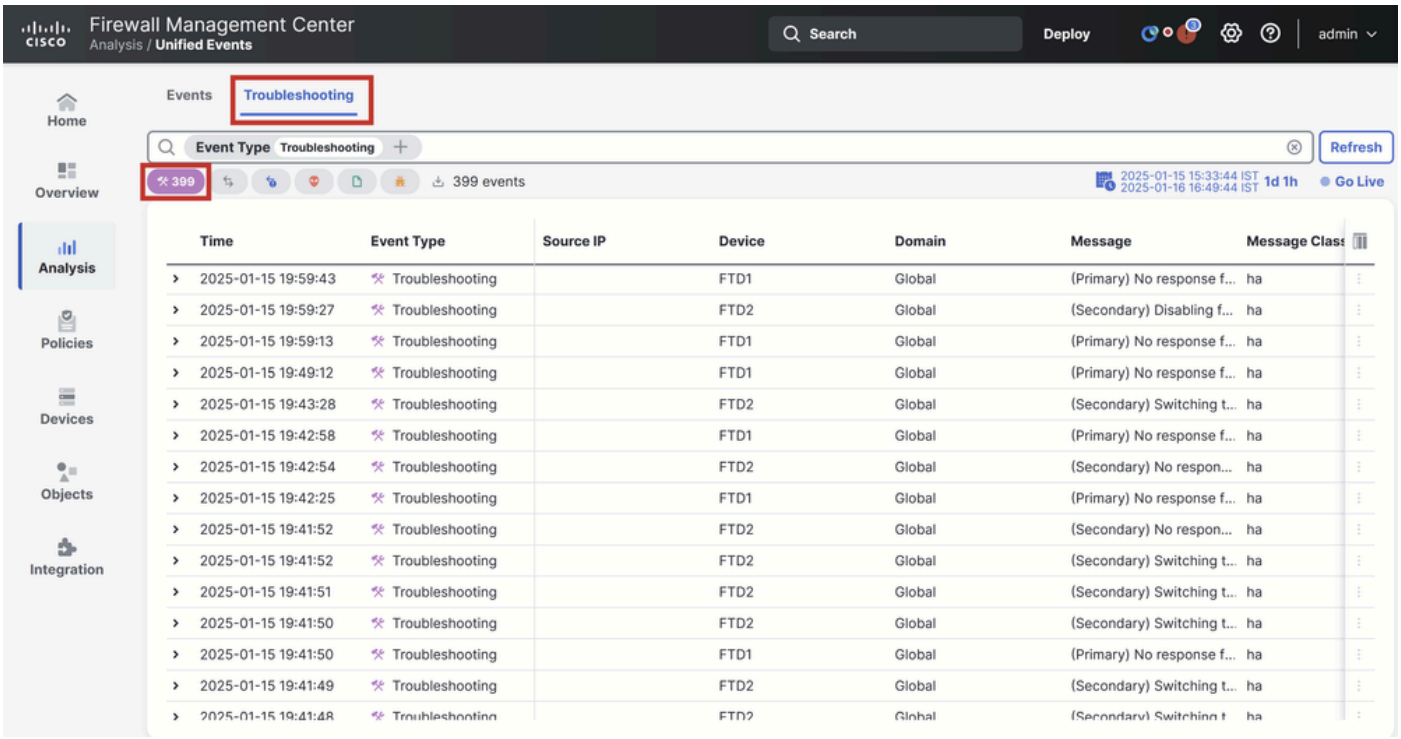
Tabellenansicht der Fehlerbehebungsprotokolle

Eine neue Registerkarte für die Fehlerbehebungsansicht ist jetzt auf der Seite Unified Event Viewer verfügbar. Um diese Ereignisse anzuzeigen, navigieren Sie zu Analyse > Vereinheitlichte Ereignisse > Problembehandlung.



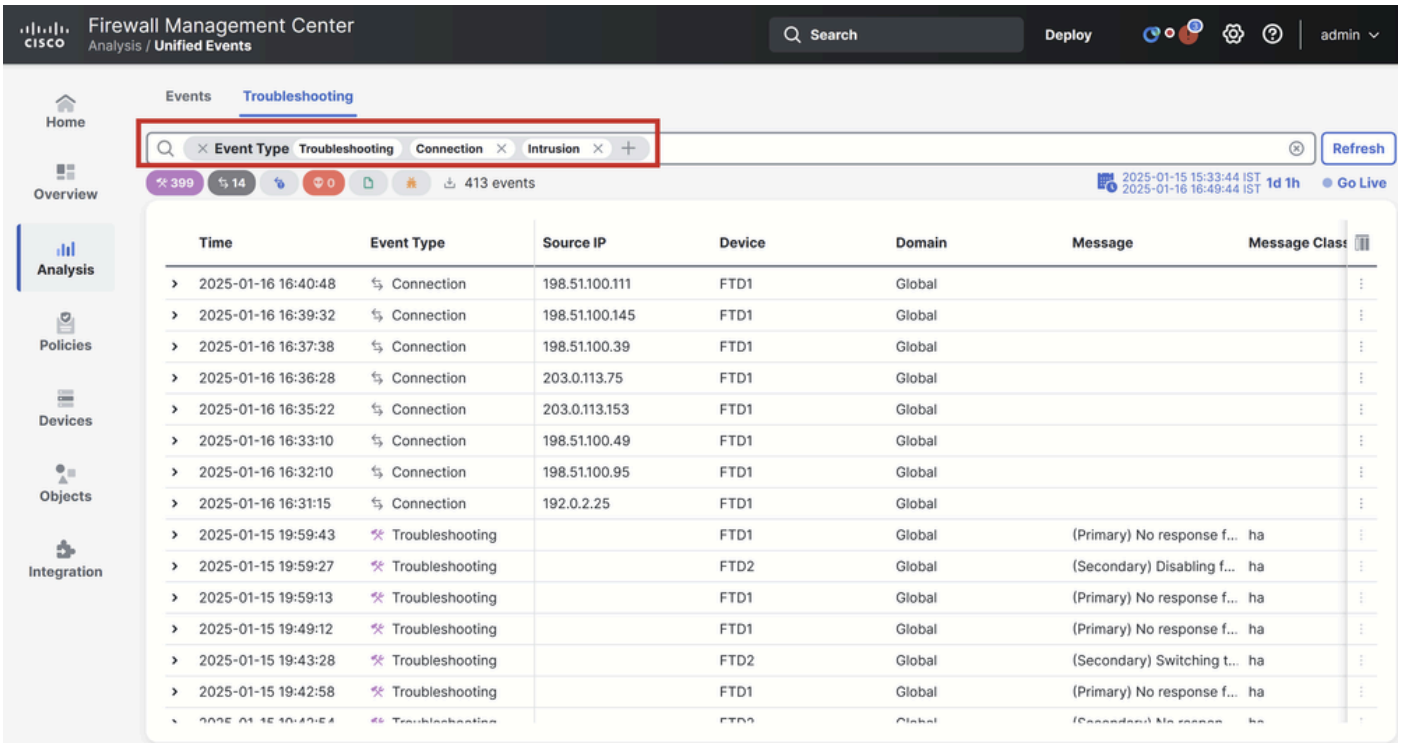
Fehlerbehebungsansicht

Sobald Sie zu dieser Registerkarte wechseln, wird ein neuer Ereignistyp in der Tabelle angezeigt. Sie kann nicht wie die anderen Typen zur Ansicht hinzugefügt oder daraus entfernt werden, da sie für die Fehlerbehebungsansicht von zentraler Bedeutung ist.



Fehlerbehebung Ereignistyp

Andere Ereignistypen können weiterhin in dieser Fehlerbehebungsansicht hinzugefügt und entfernt werden. Dadurch können Sie Diagnoseprotokolle zusammen mit anderen Ereignisdaten anzeigen.



Andere Ereignistypen

Überprüfen der Konfiguration

Nachdem die Konfiguration über die FMC-GUI vorgenommen wurde, kann sie über die FTD-CLI überprüft werden, indem die Befehle show running-config logging und show logging entweder im CLISH- oder im LINA-Modus ausgeführt werden.

```
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-Befehl

```
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-Befehl

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.