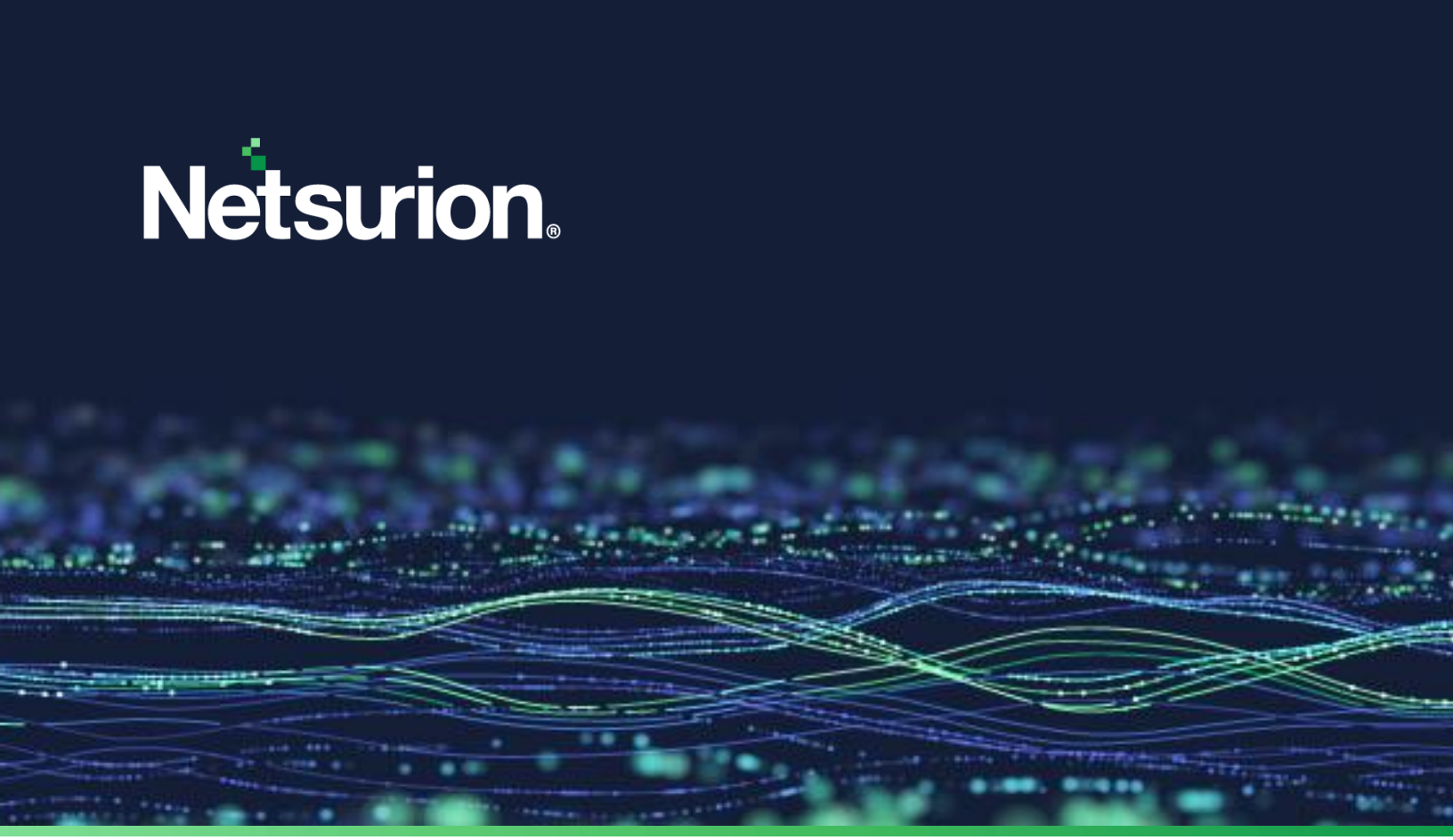


Integration Guide

Integrate Cisco FTD with the Netsurion Open XDR platform

Publication Date:

April 05, 2023

Abstract

This guide provides instructions to configure and retrieve the Cisco FTD events via syslog and then forward the logs to the Netsurion Open XDR platform.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with Cisco FTD and the Netsurion Open XDR platform version 9.3 or later.

Audience

This guide is for the administrators responsible for configuring the Cisco FTD in the Netsurion Open XDR platform.

Product Terminology

The following terms are used throughout this guide:

- The term “Netsurion’s Open XDR platform” or “the Netsurion Open XDR platform” or “the Open XDR platform” refers to EventTracker.
- The term “Data Source Integrations” refers to Knowledge Packs.

Table of Contents

1 Overview

Cisco Firepower Threat Defense (FTD) is an integrative software image combining CISCO Adaptive Security Appliance (ASA) and Firepower features into one hardware and software inclusive system, majorly responsible for handling network traffic and complies with defined security policies.

Netsurion's Open XDR platform seamlessly combines SIEM, Log Management, File Integrity Monitoring, machine analytics, and user behavior monitoring. The dashboard, category, alerts, and reports in Netsurion's Open XDR platform benefit in tracking critical activities, security warning activities, and others.

2 Prerequisite

- The user must have Device Administrator privileges for Firepower management console (FMC).
- Port 514 must be open and dedicated to syslog communication.
- The Data Source Integrator package.

Note:

To get the Data Source Integrator package, contact your Netsurion Account Manager.

3 Configuring Cisco FTD to forward logs to the Netsurion Open XDR platform.

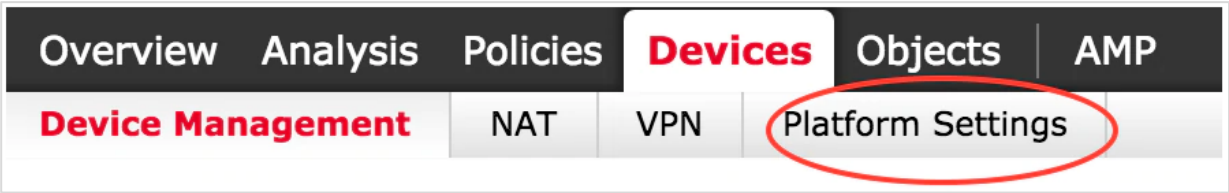
Syslog integration facilitates exporting the events to a Syslog Server or a Security Information and Events Management (SIEM) System.

Note:

Ensure the Netsurion Open XDR Manager's FQDN and Port are reachable.

Perform the following steps to configure the syslog integration.

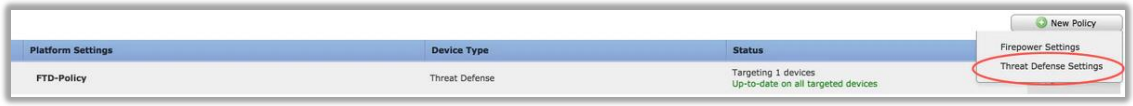
1. Log in to the **Cisco FMC** web UI.
2. In the menu bar, navigate to **Devices > Platform Settings.**



3. Go to the existing **Netsurion syslog** policy (created earlier) and click **Edit**.

Refer the below steps to create a New Policy.

a. Click **New Policy** and select **Threat Defense Policy**

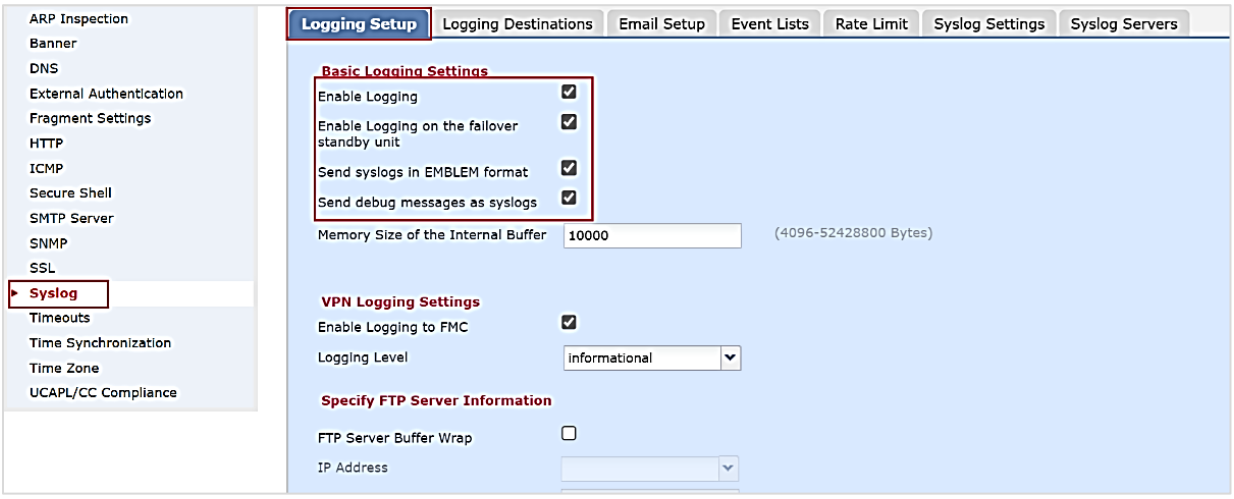


b. Provide a policy name (like **Netsurion syslog)**, followed by selecting all the FTD device from the **Available Devices** list, and click **Add to Policy**.

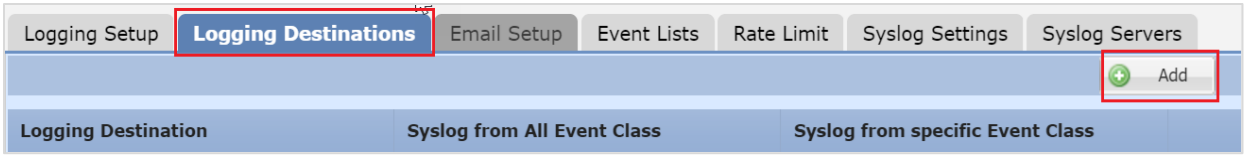
c. Click **Save** to save and close the dialog box.

4. In the navigation panel on the left, select **Syslog.**

5. In the **Logging Setup** tab, select the specified check boxes (as illustrated in the following image).

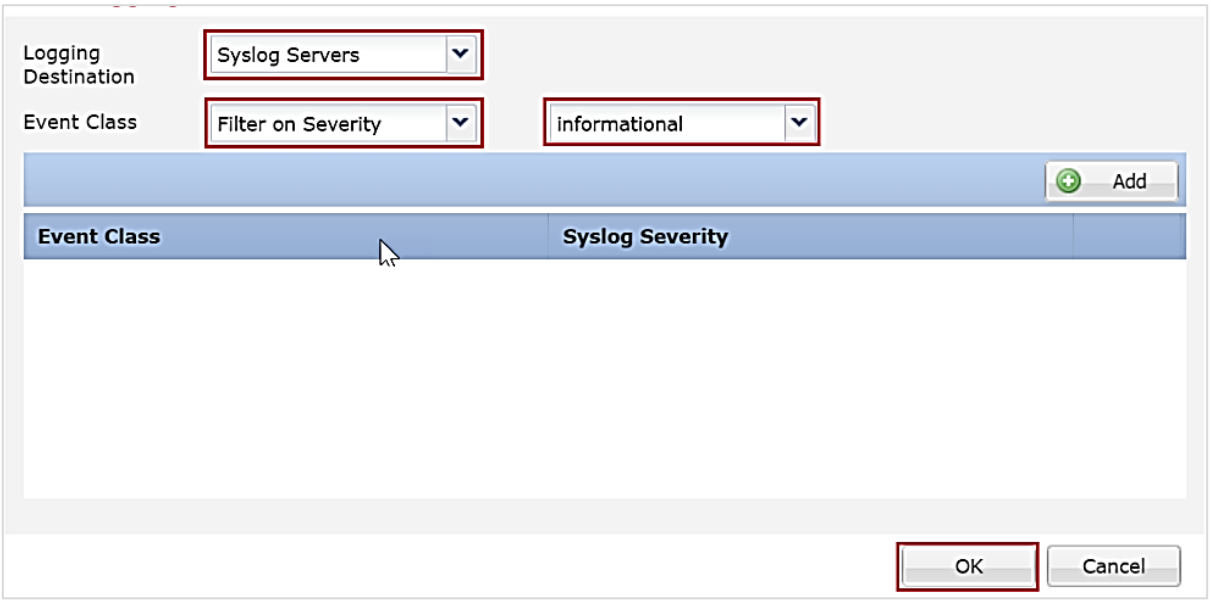


6. Then, in the **Logging Destinations** tab, click **Add** to configure the details.

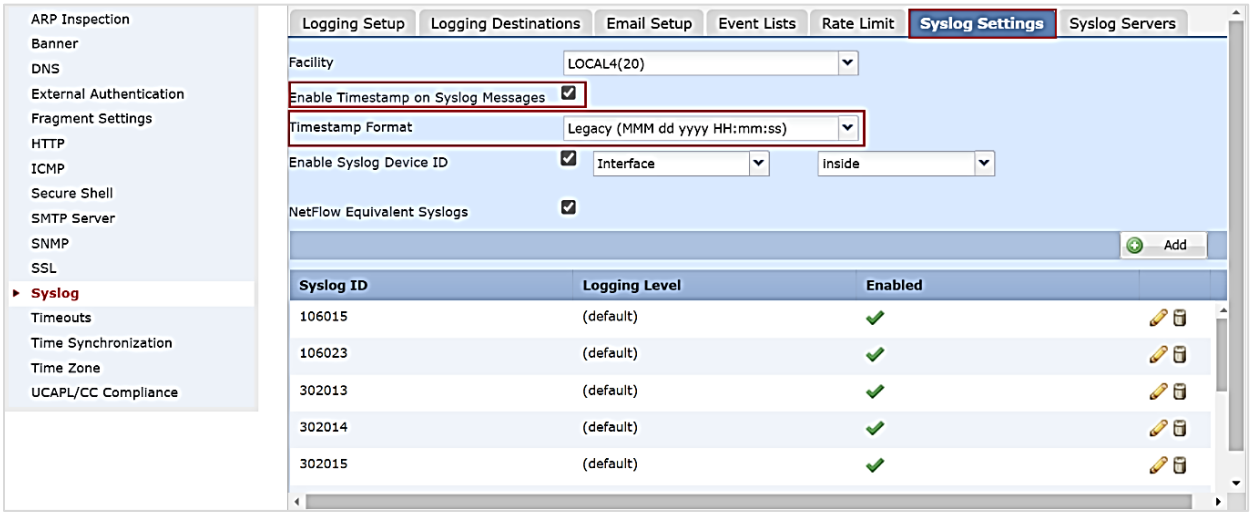


In the Logging Filter interface, specify the following details.

- **Logging Destination** - Select **Syslog Servers** from the drop-down list.
- **Event Class** - Select **Filter on Severity** from the drop-down list.
- **Severity** - Select **Informational** from the drop-down list.



7. Then, click the **Syslog Settings** tab and specify the following.
   - Select the **Enable Timestamp on Syslog Messages** check box.
   - Select **Timestamp Format** as **Legacy** from the drop-down list.

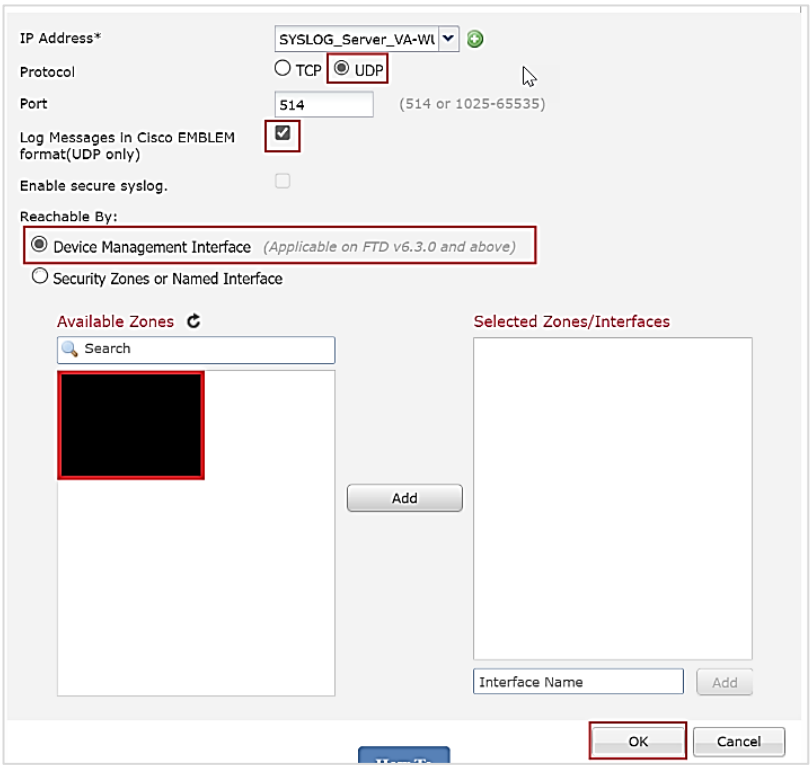


8. In the **Syslog Servers**, click **Add** and specify the following details.

- **IP Address** - Enter the Open XDR Manager's **FQDN** or the **IP address**.

> **Note:**
>
> Recommended using the FQDN.

- **Protocol** - Choose **UDP**.
- **Port** – Type in **514**.
- Select the **Log Message in Cisco EMBLEM format (UDP only)** check box.
- **Reachable By** - Choose **Device Management Interface.**



9. After providing the details, click **OK**, and then click **Save**.
10. To activate, go to **Deploy** > **Deployment** and deploy the policies assigned to the devices.

4 Data Source Integrations (DSIs) in the Netsurion Open XDR platform

After receiving the logs in the Netsurion Open XDR platform, configure the Data Source Integrations in the Netsurion Open XDR platform.

The Data Source Integrations package contains the following files for the Cisco FTD.

- Categories_Cisco FTD.iscat
- Alerts_ Cisco FTD.isalt
- Flex_Reports_ Cisco FTD.etcrx
- KO_ Cisco FTD.etko
- Dashboards_ Cisco FTD.etwd
- Templates_Cisco FTD.ettd

Note:

Refer the How To Configure DSI guide for the procedures to configure the above DSIs in the Netsurion Open XDR platform.

Data Source Integrations Details

4.1 Alerts

Name	Description
Cisco FTD - NGIPS has blocked a suspicious connection	This alert gets triggered when the Cisco Firepower NGIPS detects a suspicious connection event.
Cisco FTD - NGIPS has detected a Malware	This alert gets triggered when the Cisco Firepower NGIPS detects a File Malware Event.
Cisco FTD - NGIPS has blocked an intrusion event	This alert gets triggered when the Cisco Firepower NGIPs detects and blocks an intrusion event.
Cisco FTD - Authorization fail detected for admin user	This alert gets triggered when Cisco FTD login fails for the admin user.
Cisco FTD - Authorization fail detected for network user	This alert gets triggered when Cisco FTD detects a login failure for network user.
Cisco FTD - Device console 'enable' password incorrect	This alert gets triggered when Cisco FTD receives incorrect credentials for device console, which is ‘enable’.

Name	Description
Cisco FTD - Device console login failed	This alert gets triggered when there is an incorrect login attempt or a failed login to FTD to the console.
Cisco FTD - Intrusion detection event has been detected	This alert gets triggered when the IDS engine discovers a potential attack or scanning on the network.
Cisco FTD - SSL-VPN invalid client tried to login	This alert gets triggered when an invalid or unknown SSL VPN Client or AnyConnect client tries to login.
Cisco FTD - SSL-VPN login fail detected	This alert gets triggered when the SSL handshake with remote device fails.
Cisco FTD - User session request with IP options has been discarded	This alert gets triggered when an IP packet is seen with IP options. The incoming packet is discarded as the IP options are considered as security risk.
Cisco FTD - User session with possible ARP poisoning in progress	This alert gets triggered when the FTD device receives an ARP packet, where the MAC address in the packet differs from the ARP cache entry.
Cisco FTD - User session with possible footprint/port scanning in progress	This alert gets triggered when a real IP packet is denied by ACL. When this event is reoccurring, it becomes suspicious for port scanning or footprint attempt.
Cisco FTD - User session with possible IP address spoof detected	This alert gets triggered when there is an attack in progress where an adversary is attempting to spoof an IP address on an inbound connection.
Cisco FTD - user session with possible spoofing attack in progress	This alert gets triggered when FTD device receives a packet with the same IP but, a different MAC address from one of its uauth entries. Or FTD device receives a packet with exempt MAC address, but, a different IP address from the corresponding uauth entries.
Cisco FTD - User session with teardrop signature detected	This alert gets triggered when FTD device discards a packet with a teardrop signature containing either a small offset or fragment overlapping.
Cisco FTD - VPN session failed	This alert gets triggered when a VPN client authentication fails.
Cisco FTD - WebVPN/AnyConnect session login failed	This alert gets triggered when a WebVPN or AnyConnect authentication is rejected.

Name	Description
Cisco FTD - High memory utilization detected on FTD device	This alert gets triggered when the FTD system reports high memory utilization.
Cisco FTD - Device configuration erased	This alert gets triggered when the device configuration is erased by any user.
Cisco FTD - SSL-VPN unsupported client has been rejected	This alert gets triggered when an unsupported AnyConnect client connection is rejected.
Cisco FTD - WebVPN/AnyConnect session file access denied	This alert gets triggered when a file access via a WebVPN or AnyConnect session denied for any user.

4.2 Reports

Name	Description
Cisco FTD - NGIPS (Intrusion Events)	This report provides a summary of intrusion events detected by the Cisco Firepower NGIPS. It includes, date, time, the type of exploit, and contextual information about the source of the attack and its target.
Cisco FTD - IDS scanning report	This report provides a summary of IDS events when a host is targeted or attacked. It includes the destination subnet, or endpoint IP address with action that is performed on the target system.
Cisco FTD - SSLVPN failed connections	This report provides a summary of failed SSLVPN handshakes. This includes source IP or Source port, destination IP or destination port, and type of peer type, that is, ‘client’ or ‘server’.
Cisco FTD - VPN client failed connections	This report provides a summary of failed VPN client connections. It includes source Ip address and username.
Cisco FTD - WebVPN failed connections	This report provides a summary of failed login attempt from WebVPN/ AnyConnect client. This includes, the user group name, username, and session type, for example ‘WebVPN’ or ‘admin’.

Name	Description
Cisco FTD - NGIPS (Network connection)	This report provides a summary of network connections at the beginning and at the end of a session. This includes SSL flow status, access control rule action, URL accessed, and more.
Cisco FTD - User command execution	This report provides a summary of commands executed by the user, like show config, or run diagnostics.
Cisco FTD – System login success	This report provides a summary of successful login by a user to FTD device. It includes, username, source IP/ source port, destination IP/ destination port, and event timestamp.
Cisco FTD – Allowed traffic activities	This report provides a detailed summary of allowed traffic connection, like TCP, UDP, or ICMP. It includes, protocol type, source IP or source port, destination IP or destination port, and event timestamp.
Cisco FTD - SSLVPN successful connections	This report provides a detailed summary of successful SSLVPN handshake with client. This includes, the protocol version used to establish connection, along with peer type, source IP or source port, and destination Ip or destination port.
Cisco FTD - VPN client successful connections	This report provides a summary of successful VPN client connections. It includes username and source IP address.
Cisco FTD - WebVPN successful connections	This report provides a summary of successful WebVPN/AnyConnect client connections or sessions. This includes the username, user group name, and source IP address.
Cisco FTD - Device configuration changes	This report provides a summary of the configuration changes on the FTD device by any user.

Name	Description
	This includes username, time of command execution, and the actual command that was executed to make any changes in device configuration.
Cisco FTD – User privilege changed	This report provides a summary of user privilege change. It includes, username, old privilege level, new privilege level and event timestamp.
Cisco FTD – User management	This report provides a detailed summary of event which includes new user creation in FTD database, and user deletion from FTD database. It includes, username and privilege level assigned to that user.
Cisco FTD – System login failed	This report provides a detailed summary of failed login attempt in Cisco FTD device. It includes, username, source IP or source port, destination IP or destination port, and event timestamp.
Cisco FTD – Traffic activity (TCP denied)	This report provides a detailed summary of failed TCP connections. It includes source IP or source port, destination IP or destination port, and event timestamp.
Cisco FTD – Traffic activity (UDP denied)	This report provides a detailed summary of failed UDP connections. It includes source IP or source port, destination IP or destination port, and event timestamp.

4.3 Dashboard

Name	Description
Cisco FTD: Device configuration changes	This dashlet displays device configuration changes with their sender and recipient address.
Cisco FTD: Top Message IDs	This dashlet displays the activities with their message id.

Name	Description
Cisco FTD: User command execution	This dashlet displays the user command execution with their username.
Cisco FTD: Console enable password incorrect	This dashlet displays the console enable password incorrect with their source IP address.
Cisco FTD: IDS scanning	This dashlet displays the IDS scanning by source IP address.
Cisco FTD: SSLVPN events by Message IDs	This dashlet displays the SSLVPN events by message IDs.
Cisco FTD: login success by Source IP	This dashlet displays the login success by source IP address.
Cisco FTD: login failed by Source IP	This dashlet displays the login failed by source IP address.
Cisco FTD: System Memory utilization	This dashlet displays the system memory utilization.
Cisco FTD Traffic Activities	This dashlet displays the traffic activities by message id.
Cisco FTD - SSL Handshake failure by Destination IP	This dashlet displays the SSL handshake failure by destination IP.
Cisco FTD - SSL Handshake failure by Source IP	This dashlet displays the SSL handshake failure by source IP address.

4.4 Saved Search

Name	Description
Cisco FTD: Device Configuration events	This saved search provides the information about any device configuration events including the details of severity, message id, and username.
Cisco FTD: Intrusion detection events	This saved search provides the information about any Intrusion detection events, including the details of severity, message id, source IP address, and more.
Cisco FTD: IP stacks events	This saved search provides the information about any IP stacks events, including the details of severity, message id, source IP address, and more.

Name	Description
Cisco FTD: SSL VPN Client (SVC) events	This saved search provides the information about any SSL VPN Client (SVC) events, including the details of severity, message id, source IP address, source port, destination IP address, destination port, and more.
Cisco FTD: System events	This saved search provides the information about any system events, including the details of severity, message id, source IP address, source port, username, and more.
Cisco FTD: User authentication events	This saved search provides the information about any user authentication events, including the details of severity, message id, source IP address, source port, username, and more.
Cisco FTD: User session events	This saved search provides the information about any user session events, including the details of severity, message id, source IP address, and more.
Cisco FTD: WebVPN/AnyConnect client events	This saved search provides the information about any WebVPN/AnyConnect client events, including the details of severity, message id, source IP address, group name, username, and more.
Cisco FTD: NGIPS Events logged at beginning of connection	This saved search provides the information about any NGIPS Events logged at beginning of connection, including the details of severity, message id, source IP address, and more.
Cisco FTD: NGIPS Events logged at end of connection	This saved search provides the information about any NGIPS Events logged at end of connection, including the details of severity, message id, source IP address, and more.
Cisco FTD: NGIPS File events	This saved search provides the information about any NGIPS File events, including the details of severity, message id, file name, action, and more.
Cisco FTD: NGIPS File malware events	This saved search provides the information about any NGIPS File malware events, including the details of severity, message id, file name, and more.
Cisco FTD: NGIPS Intrusion events	This saved search provides the information about any NGIPS Intrusion events, including the details of severity, message id, file name, source IP address, and more.

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers Managed Threat Protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection and Response (MDR) and a Top 25 Global MSSP. Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Use the form to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials-Support@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support