Netsurion | EventTracker®

How to- Configure Defender MFA to forward logs to EventTracker

EventTracker v9.2 and later

Publication Date: September 28, 2020

Abstract

This guide provides instructions to retrieve the **Defender MFA (One Identity)** events via syslog. Once the logs starts coming into EventTracker, reports, dashboards, alerts and saved searches can be configured.

Scope

The configuration details in this guide are consistent with EventTracker version 9.2 or above and **Defender MFA 5.9 and above.**

Audience

Administrators who are assigned the task to monitor **Defender MFA** events using EventTracker.

Table of Contents

1. Overview

One Identity - Defender is a two-factor authentication or Multi-Factor Authentication (MFA) program. It uses your current identity store within Microsoft Active Directory to enable two-factor authentication, taking advantage of its inherent scalability and security, and eliminating the costs and time involved to set up and maintain proprietary databases.

Defender MFA integrates with EventTracker SIEM application to give security analytics with deep data context so that organizations can be confident in their data security strategy. Benefits include scheduled reports, integrated defender MFA dashboards and alerts for streamlined investigation.

Reports will allow users to keep records that is easy to read and to format. It is a detailed summary of events generated by Defender MFA. It includes successful or failed user sign in attempts using, user assigned tokens.

Alerts are best way to keep updated with critical events occurring in Defender MFA, such as, failed sign-in attempt using a token by a user, or when a token or defender password is assigned/unassigned to/from a user.

Dashboard provide a graphical representation of events generated by Defender MFA in the form of pie chart or bar graph, or force direction, and many more. Some of them are, top successful user authentications, user authentication failure reasons, top user authentication fails, etc.

2. Prerequisites

- EventTracker v9.2 and above should be installed.
- Administrative/root access to Defender Security Server (DSS).
- Syslog port (e.g. 514) should be allowed in firewall.
- EventTracker Manager IP address.

3. Integrating Defender MFA with EventTracker

3.1 Part 1: Configuring Syslog Message Forwarding

User can configure the syslog server address in DSS configuration wizard so that logs are sent to EventTracker.

1. Login to your Defender Security Server (DSS) with administrative account.

2. Navigate to **Start > Programs > Defender Active Directory Edition > Defender Security Server Configuration**.
3. In **Defender Security Server Configuration** wizard**,** select "**Audit Log**" tab and click on the "**Enable syslog**" checkbox.

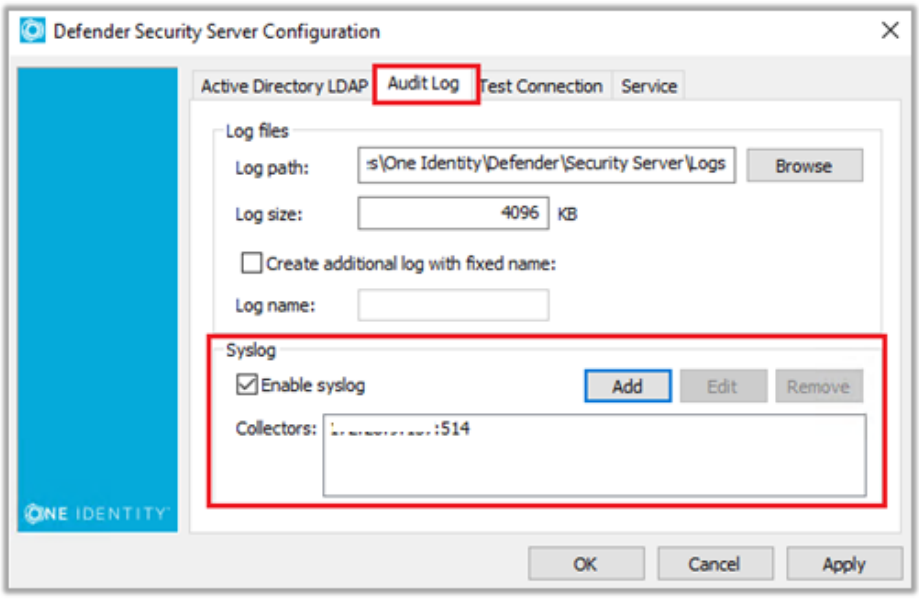

Figure 1

4. Next, click on "**Add**" button to add new syslog server. Enter the syslog server **IP address** and **port** number (default is 514) and click **OK**.

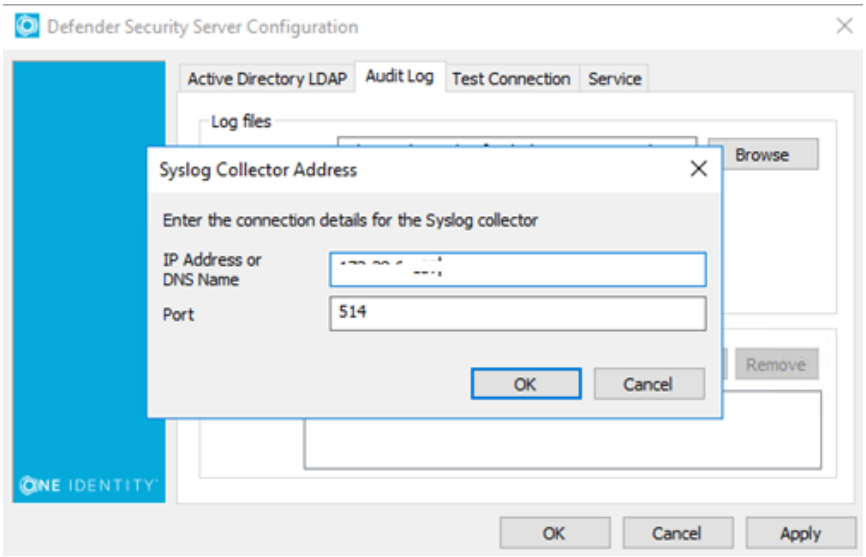

Figure 2

5. Finally click **Apply**, then **OK** to complete integration process.

3.2 Part 2: Configuring Defender Console event log forwarding

Defender MFA is also able to record events to the Windows Event Log. These logs are typically associated with token/defender password/ PIN management in Defender AD console. E.g. assigning a token to a user, assigning a Defender password to a user, setting a token PIN, etc.

By default, event logging is turned off in the Defender Console. To allow these events to be logged in windows event viewer and then forwarded to EventTracker, follow the below steps:

1. Set the following value in the registry on each desktop/server that is used to administer Defender tokens (i.e., wherever the Defender Console is installed.

x86: HKEY_LOCAL_MACHINE\Software\PassGo Technologies\Defender\Defender AD MMC

x64: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PassGo Technologies\Defender\Defender AD MMC

Value: LoggingEnabled (create the entry if it does not exist)

Type: DWORD

Data: 0 to disable logging, 1 to enable logging

Figure 3

2. Next, Configure EventTracker agent to pick up the Defender Console logs. For this, Open EventTracker agent configuration by navigating to path:
"**C:\Program Files (x86)\Prism Microsystems\EventTracker\Agent\"** or **"%et_install_path%\Agent**" and run "**etaconfig.exe**". EventTracker Agent Configuration wizard opens, select "**Event Filters**".

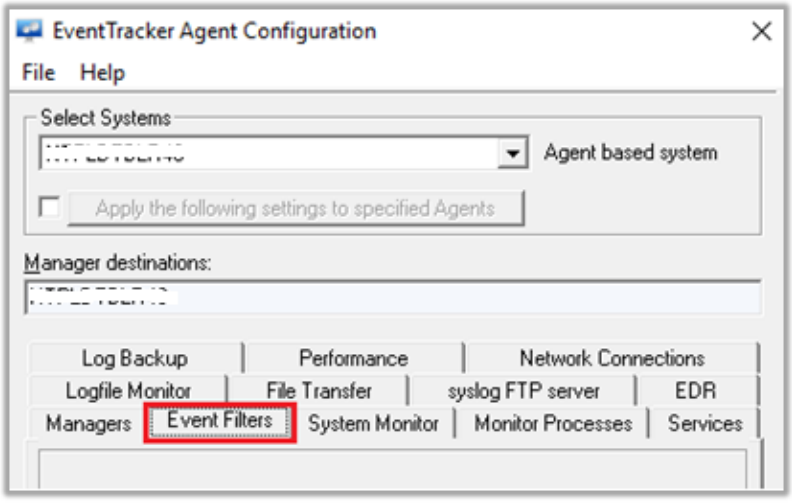

Figure 4

3. In "**Event Filters**", select "**Filter exception**" button:

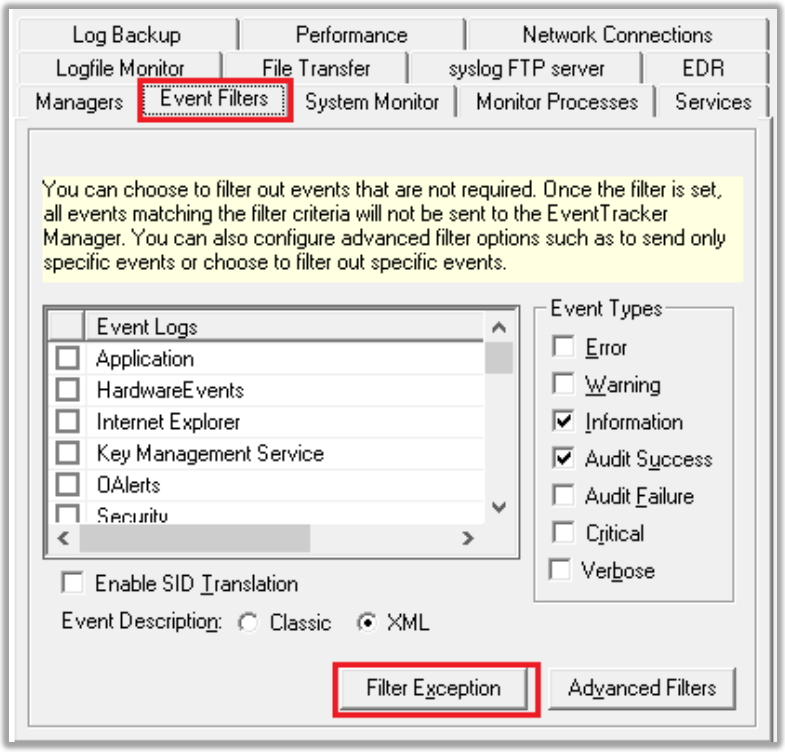

Figure 5

4. In "**Filter Exception**" wizard, click on "**New**" button:

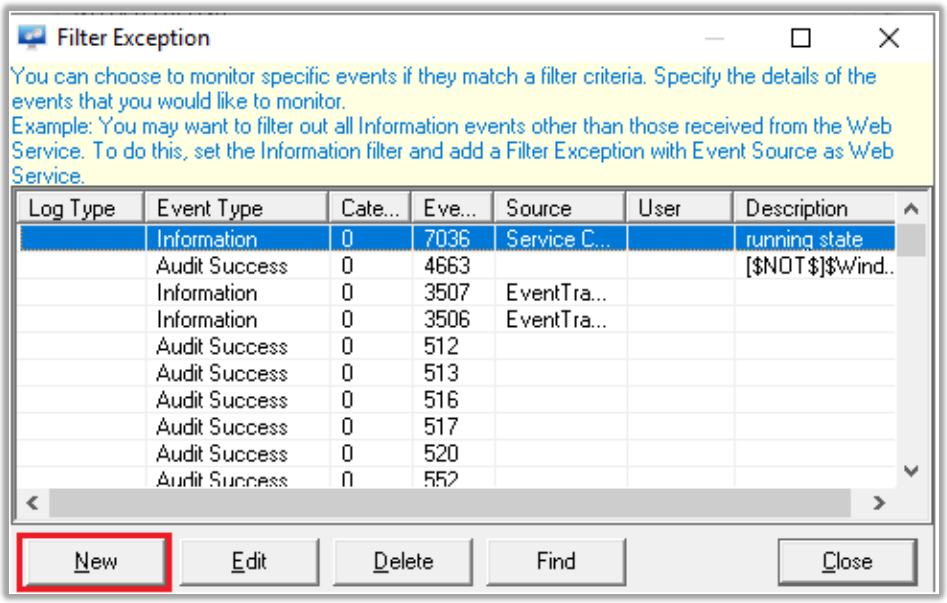

Figure 6

5. In "**New Event Details**" wizard, specify the values as give in the picture below and click "**OK**":

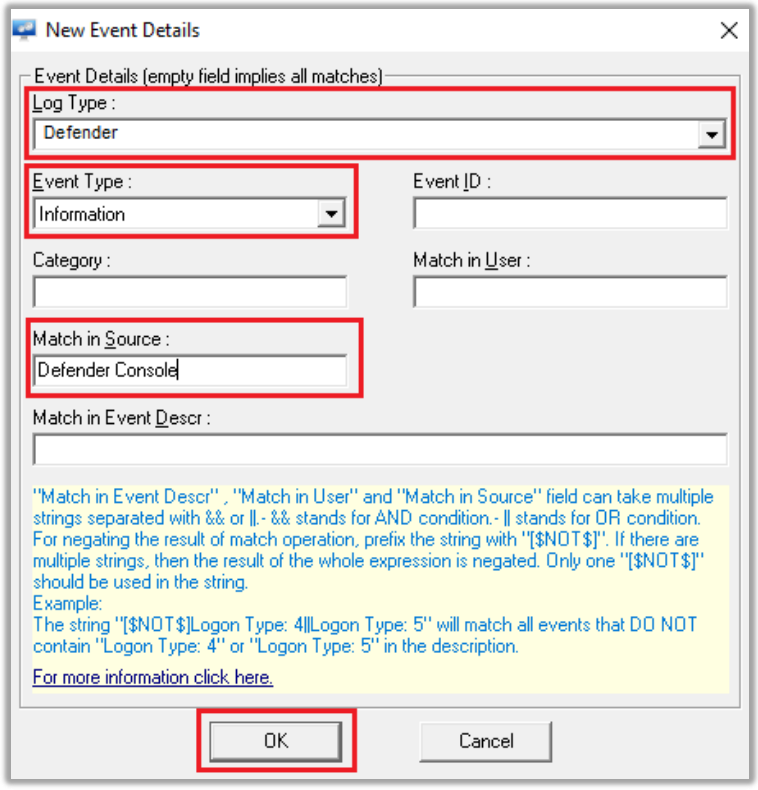

Figure 7

6. Next, click on "**Close**" button and then click on "**Save**":

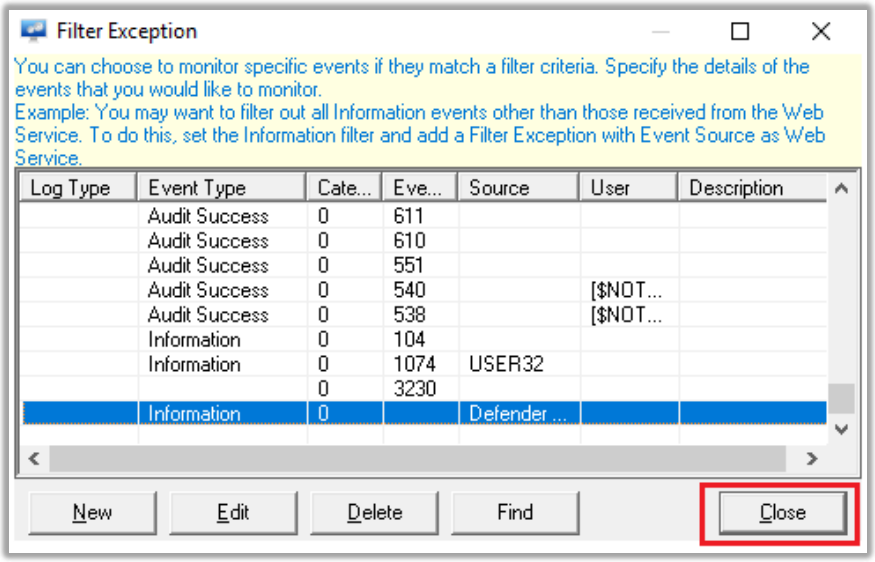

Figure 8

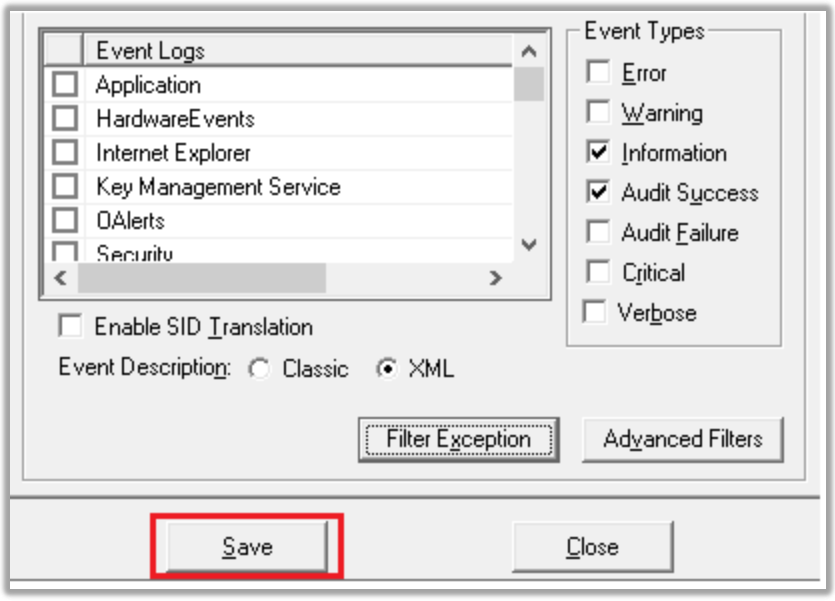

Figure 9

7. Finally, click on "**Close**" button to complete the integration process.