Netsurion | EventTracker®

How to-Configure Azure MFA On-Premise to forward logs to EventTracker

EventTracker v9.x and above

Publication Date: May 18, 2020

Abstract

This guide provides instructions to configure Microsoft Azure Multi-Factor Authentication (MFA) to send logs to EventTracker.

Scope

The configuration details in this guide are consistent with EventTracker version v9.x or above and **Azure MFA On-Premise**

Audience

Administrators who are assigned the task to monitor Azure MFA On-Premise events using EventTracker.

Table of Contents

1. Overview

Microsoft Azure Multi-Factor Authentication (MFA) prompts the users during the sign-in process for an additional form of identification, such as to enter a code on cellphone or to provide a fingerprint scan.

EventTracker helps to monitor events from **Azure MFA On-Premise**. Its dashboard and reports will help you to detect authentication activities.

EventTracker's built-in knowledge pack enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

Through alerts, knowledge base solutions, and reports, EventTracker helps you correct problems long before a disastrous failure occurs.

2. Prerequisites

- Admin privileges for **Azure MFA** and should be installed.
- **EventTracker agent** should be installed in the system.

3. Integration of Azure MFA On-Premise with EventTracker

3.1 Integrating via syslog configuration

Follow the below steps to configure syslog.

1. Log on to the server running the Multi-Factor Authentication Server with administrative privileges.
2. Open the Multi-Factor Authentication Server Management console by searching for it on the Start Screen.
3. In the left pane, click **Logging**-> **syslog** tab.

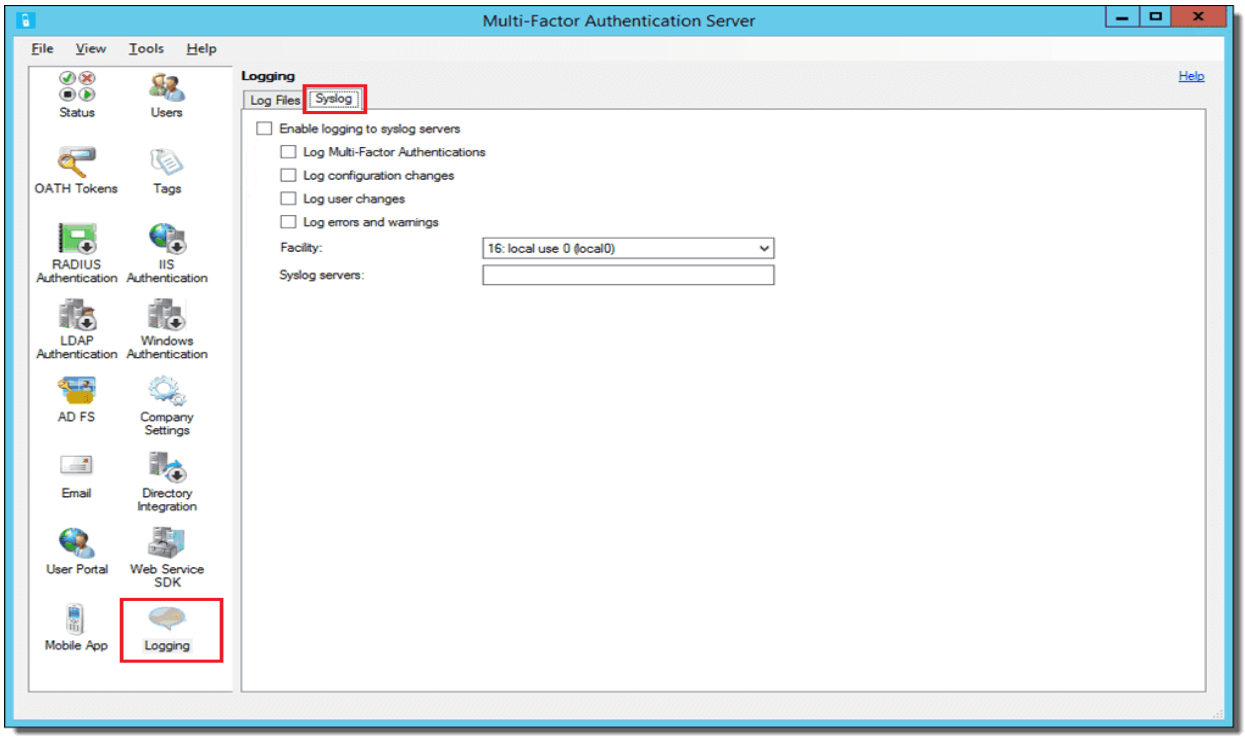

Figure 1

4. Check the “Enable logging to syslog server” box.
5. Enter the EventTracker Manager IP in the syslog server field.

Integration is complete, EventTrackser will receive Azure MFA logs.