

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

EventTracker v9.x and above

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.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

1. Overview	3
2. Prerequisites	3
3. Integration of Azure MFA On-Premise with EventTracker	3
3.1 Integrating via syslog configuration	3

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.

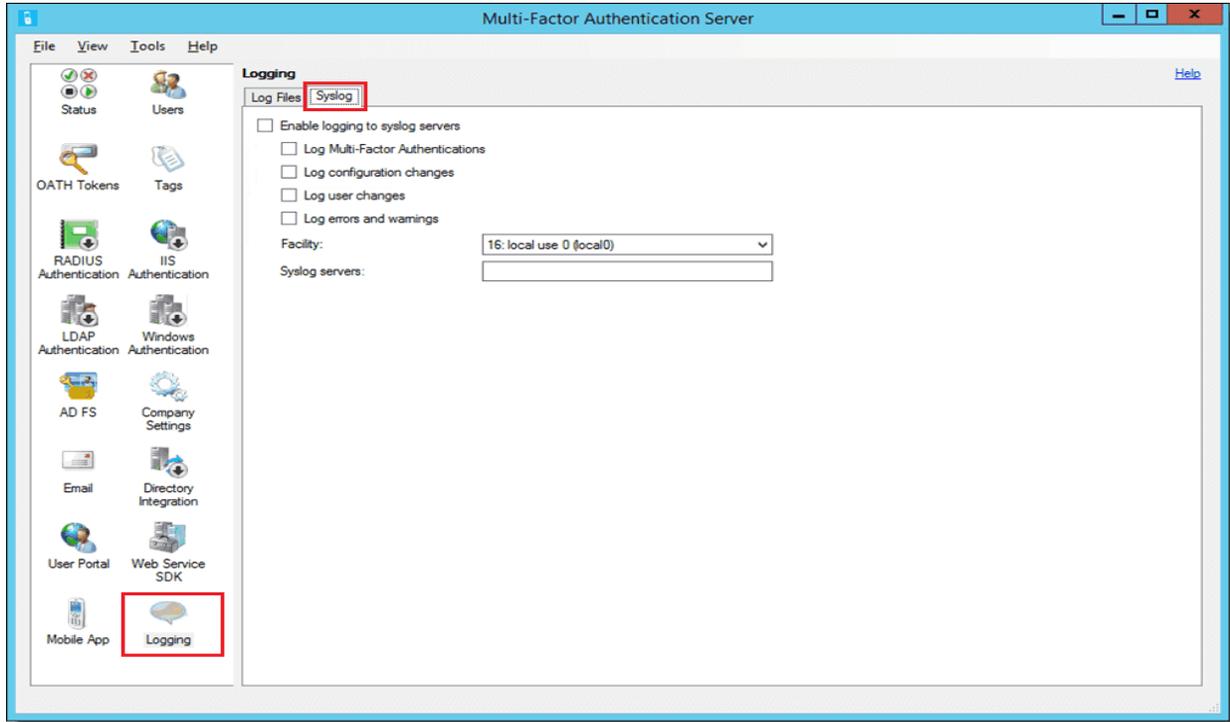


Figure 1

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

Integration is complete, EventTracker will receive Azure MFA logs.