Integrate Azure MFA On-Premise

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 ........................................................................................................................................... 3
2. Prerequisites ......................................................................................................................................... 3
3. Integration of Azure MFA On-Premise with EventTracker ................................................................. 3
   3.1 Integrating via syslog configuration ............................................................................................... 3
4. EventTracker Knowledge Pack .......................................................................................................... 5
   4.1 Category .......................................................................................................................................... 5
   4.2 Alert ................................................................................................................................................ 5
   4.3 Report ............................................................................................................................................ 5
   4.4 Dashboards ..................................................................................................................................... 6
5. Importing Azure MFA On-Premise knowledge pack into EventTracker ............................................ 9
   5.1 Category .......................................................................................................................................... 9
   5.2 Alert ................................................................................................................................................ 10
   5.3 Token template .................................................................................................................................. 11
   5.4 Knowledge Object .......................................................................................................................... 13
   5.5 Report ............................................................................................................................................ 15
   5.6 Dashboards ..................................................................................................................................... 16
6. Verifying Azure MFA On-Premise knowledge pack in EventTracker ................................................. 19
   6.1 Category .......................................................................................................................................... 19
   6.2 Alert ................................................................................................................................................ 20
   6.3 Token templates .............................................................................................................................. 21
   6.4 Knowledge Object .......................................................................................................................... 21
   6.5 Report ............................................................................................................................................ 22
   6.6 Dashboards ..................................................................................................................................... 23
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.
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.
4. EventTracker Knowledge Pack

Once logs are received by EventTracker manager, knowledge packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support Azure MFA.

4.1 Category

- **Azure MFA: Authentication Success** - This category provides information related to successful authentication.
- **Azure MFA: Authentication Failure** – This category provides information related to all authentication failure.

4.2 Alert

- **Azure MFA: Authentication Failure** - This alert is generated when any authentication failure is detected by Azure MFA.

4.3 Report

- **Azure MFA – Authentication Failure** - This report gives information about all the authentication failure detected by Azure MFA. Report contains username, source IP, guide, call status along with other useful information for further analysis.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Call Status</th>
<th>Guid</th>
<th>IP Address</th>
<th>Message</th>
<th>Username</th>
<th>EventDescription</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/07/2021 12:09:16 PM</td>
<td>172.xx.xx.xx:51810</td>
<td>FAIL3_PHONE_BUSY</td>
<td>686e306-964d-41f8-ae78-407829229498</td>
<td>Auth Already In Progress</td>
<td>encecm</td>
<td>May 07 12:09:16 172.27.188.13 Apr 30 16:47-20 RAAMAF1032 Apr 19 15:47-20 remoteMFA pfvc</td>
<td><img src="image" alt="Figure 2" /></td>
</tr>
<tr>
<td>05/07/2021 12:09:16 PM</td>
<td>172.xx.xx.xx:51810</td>
<td>FAIL3_PHONE_APP_RESPON</td>
<td>634741-c863-4b0b-66f7-595cb4b4a1f8</td>
<td>Unable App Response</td>
<td>encecm</td>
<td>May 07 12:09:16 172.27.188.13 Apr 30 16:47-20 RAAMAF1032 Apr 19 15:47-20 remoteMFA pfvc</td>
<td><img src="image" alt="Figure 2" /></td>
</tr>
<tr>
<td>05/07/2021 12:10:18 PM</td>
<td>172.xx.xx.xx:51810</td>
<td>FAIL3_PHONE_APP_NO_RESPON</td>
<td>50bac017-4d5a-4745-9036-b9558be08a78</td>
<td>Unable App No Response</td>
<td>encecm</td>
<td>May 07 12:10:18 172.27.188.13 Apr 30 16:47-20 RAAMAF1032 Apr 19 15:47-20 remoteMFA pfvc</td>
<td><img src="image" alt="Figure 2" /></td>
</tr>
</tbody>
</table>

- **Azure MFA – Authentication Success** - This report gives information about all the successful authentication detected by Azure MFA. Report contains username, source IP, guide, call status along with other useful information for further analysis.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Call Status</th>
<th>Guid</th>
<th>IP Address</th>
<th>Message</th>
<th>Username</th>
<th>EventDescription</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/07/2021 12:09:23 PM</td>
<td>172.xx.xx.xx:51810</td>
<td>SUCCESS_PHONE_APP_AUTHENTICATED</td>
<td>71bebf3-3f8a-409b-a9d7-3e7f9029f097</td>
<td>Mobile App Authenticated</td>
<td><a href="mailto:johncole@converseenergy.com">johncole@converseenergy.com</a></td>
<td>May 07 12:09:23 172.27.188.13 Apr 30 16:47-20 RAAMAF1032 Apr 19 15:47-20 remoteMFA pfvc</td>
<td><img src="image" alt="Figure 3" /></td>
</tr>
<tr>
<td>05/07/2021 12:09:23 PM</td>
<td>172.xx.xx.xx:51810</td>
<td>SUCCESS_PHONE_APP_AUTHENTICATED</td>
<td>33d9fac1-3846-4c77-b369-65850be5885e</td>
<td>Mobile App Authenticated</td>
<td>johncole</td>
<td>May 07 12:09:23 172.27.188.13 Apr 30 16:47-20 RAAMAF1032 Apr 19 15:47-20 remoteMFA pfvc</td>
<td><img src="image" alt="Figure 3" /></td>
</tr>
<tr>
<td>05/07/2021 12:09:23 PM</td>
<td>172.xx.xx.xx:51810</td>
<td>SUCCESS_PHONE_APP_AUTHENTICATED</td>
<td>27be90b-2a89-4e8a-b2d5-c85d04eb278c</td>
<td>Mobile App Authenticated</td>
<td>notaday</td>
<td>May 07 12:09:23 172.27.188.13 Apr 30 16:47-20 RAAMAF1032 Apr 19 15:47-20 remoteMFA pfvc</td>
<td><img src="image" alt="Figure 3" /></td>
</tr>
</tbody>
</table>
**Logs Considered**

<table>
<thead>
<tr>
<th>action</th>
<th>succeeded</th>
</tr>
</thead>
<tbody>
<tr>
<td>event_category</td>
<td>0</td>
</tr>
<tr>
<td>event_computer</td>
<td>172.27.100.13-syslog</td>
</tr>
<tr>
<td>event_datetime</td>
<td>5/7/2020 5:16:17 PM</td>
</tr>
<tr>
<td>event_datetime_utc</td>
<td>1588851977</td>
</tr>
<tr>
<td>event_description</td>
<td>May 07 17:16:17 172.27.100.13 Apr 29 06:47:28 RAMADYS02 Apr 29 06:47:28 ramaedh02 pfOSC iAppsvouTc8l9 succeeded for user ‘davejohn’. Call status: SUCCESS_PHONE_APP_AUTHENTICATED - ‘Mobile App Authentication’ succeeded for user ‘davejohn’.</td>
</tr>
<tr>
<td>event_group_name</td>
<td>Default</td>
</tr>
<tr>
<td>event_id</td>
<td>128</td>
</tr>
<tr>
<td>event_log_type</td>
<td>Application</td>
</tr>
<tr>
<td>event_source</td>
<td>SYSLOG local0</td>
</tr>
<tr>
<td>event_type</td>
<td>Error</td>
</tr>
<tr>
<td>event_user_domain</td>
<td>N/A</td>
</tr>
<tr>
<td>event_user_name</td>
<td>N/A</td>
</tr>
<tr>
<td>log_source</td>
<td>Azure MFA</td>
</tr>
<tr>
<td>log_type</td>
<td>SUCCESS_PHONE_APP_AUTHENTICATED</td>
</tr>
<tr>
<td>object_id</td>
<td>7e835a4-b738-45fe-9e4d-6a15660a43d1</td>
</tr>
<tr>
<td>reason</td>
<td>Mobile App Authenticated</td>
</tr>
<tr>
<td>source_type</td>
<td>Azure MFA</td>
</tr>
<tr>
<td>src_user_name</td>
<td>davejohn</td>
</tr>
<tr>
<td>tags</td>
<td>Authentication Success</td>
</tr>
<tr>
<td>tags</td>
<td>Authentication Activities</td>
</tr>
</tbody>
</table>

Figure 4

### 4.4 Dashboards

- **Azure MFA: Authentication Success**

![Azure MFA: Authentication Success](image)

Figure 5
• **Azure MFA: Authentication Failure**

![Figure 6](image)

• **Azure MFA: User Location**

![Figure 7](image)
• **Azure MFA: Authentication Failed with Method Used**

![](image)

**Figure 8**

• **Azure MFA: Authentication Request Mode**

![](image)

**Figure 9**
5. Importing Azure MFA On-Premise knowledge pack into EventTracker

**NOTE:** Import knowledge pack items in the following sequence.

- Category
- Alert
- Token template
- Knowledge Object
- Report
- Dashboard

1. Launch EventTracker Control Panel.

2. Double click Export Import Utility.

3. Click the Import tab.

### 5.1 Category

1. Click **Category** option, and then click **Browse**.
2. Locate `Categories_Azure MFA.iscat` file, and then click **Open**.

3. To import categories, click **Import**.

   EventTracker displays success message.

![Figure 12](image)

4. Click **OK**, and then click **Close**.

### 5.2 Alert

1. Click **Alert** option, and then click **Browse ...**.
2. Locate **Alerts_Azure MFA.isalt** file, and then click **Open**.
3. To import alerts, click **Import**.
   EventTracker displays success message.

4. Click **OK**, and then click **Close**.

### 5.3 Token template

1. Click **Parsing rule** under **Admin** option in the EventTracker manager page.
2. Click **Template**.

3. To import token template, click **Import**.

4. Locate the **Templates_Azure MFA.ettd** type file by clicking **Browse**, enable all the templates and click **import**.
5. Click **OK**.

### 5.4 Knowledge Object

1. Click **Knowledge objects** under Admin option in the EventTracker manager page.

2. Click **Import** as highlighted in the below image:

3. Click **Browse**.
4. Locate the file named KO_Azure MFA.etko.
5. Now select the check box and then click **Import**.

6. Knowledge objects are now imported successfully.
5.5 Report

1. Click Reports option and select New (*.etcrx) option.

![Export Import Utility](image)

Figure 24

2. Locate the file named Reports_Azure MFA.etcrx and select the check box.

![Report Details](image)

Figure 25
3. Click Import to import the report. EventTracker displays success message.

5.6 Dashboards

**NOTE**: Below steps given are specific to EventTracker 9 and later.

1. Open **EventTracker** in browser and logon.

2. Navigate to **My Dashboard** option as shown above.

3. Click **Import** as show below:
4. Import dashboard file **Dashboard_Azure MFA.etwd** and select **Select All** checkbox.
5. Click **Import** as shown below.

![Import dashboard](image)

**Figure 29**

6. Import is now completed successfully.

![Import completed successfully](image)

**Figure 30**

7. In **My Dashboard** page select to add dashboard.

![My Dashboard](image)

**Figure 31**

8. Choose appropriate name for **Title** and **Description**. Click **Save**.

10. Select imported dashlets and click Add.
6. Verifying Azure MFA On-Premise knowledge pack in EventTracker

6.1 Category

1. Logon to EventTracker.

2. Click Admin dropdown, and then click Category.

3. In Category Tree to view imported category, scroll down and expand Azure MFA group folder to view the imported category.
6.2 Alert

1. Logon to EventTracker.
2. Click the Admin menu, and then click Alerts.

![EventTracker](image)

Figure 37

3. In the Search box, type ‘Azure MFA’, and then click Go. Alert Management page will display the imported alert.

![Alert Management](image)

Figure 38

4. To activate the imported alert, toggle the Active switch. EventTracker displays message box.

![Message Box](image)

Figure 39

5. Click OK, and then click Activate Now.

**NOTE:** Specify appropriate system in alert configuration for better performance.
6.3 Token templates

1. In the EventTracker web interface, click the Admin dropdown, and then click Parsing rules.

![Figure 40](image)

2. On Template tab, click on the Azure MFA group folder to view the imported token values.

![Figure 41](image)

6.4 Knowledge Object

1. In the EventTracker web interface, click the Admin dropdown, and then select Knowledge Objects.

![Figure 42](image)

2. In the Knowledge Object tree, expand Azure MFA group folder to view the imported knowledge object.
3. Click **Activate Now** to apply imported knowledge objects.

### 6.5 Report

1. In the **EventTracker** web interface, click the **Reports** menu, and then select **Report Configuration**.

2. In **Reports Configuration** pane, select **Defined** option.

3. Click on the **Azure MFA** group folder to view the imported reports.
6.6 Dashboards

1. In the EventTracker web interface, Click **Home** and select “**My Dashboard**”.

2. In the “**Azure MFA**” dashboard you should be now able to see something like this.

![Dashboard image](image2.png)

![My Dashboard image](image1.png)

![Azure MFA: Authentication Request Mode](image3.png)