Integration of Phonefactor or Multi-Factor Authentication
Abstract

This guide provides instructions to configure phonefactor to send the event logs to EventTracker. Once events are configured to send to EventTracker Manager, alerts, dashboards and reports can be configured into EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 7.X and later, and phonefactor or Multifactor Authentication 6.3.1.1 and later.

Audience

Phonefactor users, who wish to forward event logs to EventTracker Manager and monitor events using EventTracker.

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

This document is for informational purposes only. EventTracker 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 EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker 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 EventTracker, 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.

© 2017 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
# Table of Contents

Abstract .......................................................................................................................... 1
Overview .......................................................................................................................... 3
Prerequisites .................................................................................................................... 3
Integration of Phonefactor with Event Tracker ............................................................ 3
  Logging: ....................................................................................................................... 3
EventTracker Knowledge Pack (KP) ............................................................................... 5
  Categories ................................................................................................................... 5
  Alerts ............................................................................................................................ 5
  Reports ......................................................................................................................... 5
Import Knowledge Pack into EventTracker ................................................................. 6
  Import Categories ....................................................................................................... 7
  Import Alerts .............................................................................................................. 8
  Import Flex Reports ................................................................................................. 9
  Import Token Templates ......................................................................................... 10
Verify Knowledge Pack in EventTracker ................................................................. 11
  Verify Categories ..................................................................................................... 11
  Verify Alerts ............................................................................................................. 11
  Verify Flex Reports ................................................................................................ 12
  Verify Token Templates ......................................................................................... 13
Create Dashboards in EventTracker ......................................................................... 14
  Schedule Reports .................................................................................................... 14
  Create Dashlets ....................................................................................................... 16
Sample Reports ........................................................................................................... 19
Overview

Phonefactor is a multi-factor authentication system which uses the phone calls to verify identity. It provides a second factor of authentication through a call, text message or even voice recognition.

EventTracker aggregates and deduces informative events to provide an insight on user configuration changes and authentication information.

Prerequisites

- EventTracker v7.x and later should be installed.
- phonefactor must be connected to EventTracker server.

Integration of Phonefactor with Event Tracker

Logging:

Following are the steps for configuring the integration of EventTracker with PhoneFactor, with the help of syslog:

1. Open Multi-Factor Authentication Server or Phone-Factor Authentication.
2. Click on logging tab.
3. Click on Log Files tab and select the logs which you want.
4. Once you select the logs which you want, then click on **Syslog** tab

![Figure 1](image)

5. Select type of logs you want and select syslog **Facility** for logs
6. In **Syslog servers** option, enter the **EventTracker IP address** (e.g. 192.168.X.X).
7. Once it is done, you can check the logs in Log search.
EventTracker Knowledge Pack (KP)

Once logs are received in EventTracker; categories, alerts, reports and dashboards can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker v7 and later to support phonefactor Version 6.3.1.1 and later.

Categories

- **Phonefactor Authentication Failure** - This category based report provides information related to authentication failed activity.
- **Phonefactor Authentication Success** - This category based report provides information related to authentication succeded activity.
- **Phonefactor user configuration** - This category based report provides information related to phonefactor user configuration changes.

Alerts

- **Phonefactor Authentication Fails** - This alert is generated when user is unable to pass the authentication.
- **Phonefactor User configuration** - This alert is generated when user modifies the configuration on phonefactor authentication server.

Reports

- **phonefactor Authentication failed** - This report provides information related to user, source address and reason for authentication failure.
- **Phonefactor Authentication Succeeded** - This report provides information related to user, source address and reason for authentication success.
- **Phonefactor user configuration changes** - This report provides information related to user configuration modifies.
Import Knowledge Pack into EventTracker

1. Launch EventTracker Control Panel.
2. Double click Export/Import Utility, and then click the Import tab.
3. Import Categories/Alerts/Templates/Flex Reports/Knowledge Objects as given below.
Import Categories

1. Click **Category** option, and then click the ‘**browse**’ button.

2. Locate applicable ‘**phonefactor category.iscat**’ file, and then click the **Open** button.

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

   EventTracker displays success message.

4. Click **OK**, and then click the **Close** button.
Import Alerts

1. Click **Alert** option, and then click the ‘browse’ button.

![Figure 6](Image)

2. Locate applicable ‘phonefactor alerts.isalt’ file, and then click the **Open** button.

3. To import alerts, click the **Import** button.
   
   EventTracker displays success message.

![Figure 7](Image)

4. Click **OK**, and then click the **Close** button.
Import Flex Reports

1. Click **Reports** option, and then click the ‘**browse**’ button.

2. Locate applicable ‘**phonefactor reports.issch**’ file, and then click the **Open** button.

![Export Import Utility](image)

**Figure 8**

3. To import reports, click the **Import** button.
   EventTracker displays success message.

![Export Import Utility](image)

**Figure 9**

4. Click **OK**, and then click the **Close** button.
Import Token Templates

1. Click the **Token Value** option, and then click the ‘**browse**’ button.

   ![Figure 10](image1)

2. Locate applicable ‘**phonefactor token.istoken**’ file, and then click the **Import** button. EventTracker displays success message.

   ![Figure 11](image2)

3. Click on **OK** button.
Verify Knowledge Pack in EventTracker

Verify Categories

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Categories**.
3. To view the imported categories, in the **Category Tree**, expand the **phonefactor** group folder.

![Category Tree](image)

**Figure 12**

Verify Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In the **Search** box, type **phonefactor**, and then click the ‘**search**’ button.
   Alert Management page will display all the imported alerts.
To activate the imported alerts, select the respective checkbox in the Active column and then click the Activate Now button.

EventTracker displays message box.

![Message Box Image]

4. Click OK.

**NOTE:** Please specify appropriate systems in alert configuration for better performance.

### Verify Flex Reports

1. Logon to **EventTracker Enterprise**.
2. Click the Reports menu, and then select **Configuration**.
4. In **Report Groups Tree** to view imported Scheduled Reports, scroll down and click **phonefactor** group folder.
   
   Scheduled Reports are displayed in the Reports configuration pane.
NOTE: Please specify appropriate systems in Report wizard for better performance.

Verify Token Templates

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab.
3. Scroll and find imported **phonefactor** token templates.
Create Dashboards in EventTracker

Schedule Reports

1. Open EventTracker in browser and logon.

![Figure 17](image)

2. Navigate to Reports>Configuration.

![Figure 18](image)

3. Select phonefactor in report groups. Check Defined option.

4. Click on ‘schedule’ to plan a report for later execution.
5. Choose appropriate time for report execution and in Step 8 check Persist data in Eventvault explorer box.
6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.
7. Proceed to next step and click **Schedule** button.
8. Wait for scheduled time or generate report manually.

## Create Dashlets

1. **EventTracker 8** is required to configure flex dashboard.
2. Open **EventTracker** in browser and logon.

![Figure 21](image)

3. Navigate to **Dashboard>Flex**.

   Flex Dashboard pane is shown.

![Figure 22](image)

4. Click **+** to add a new dashboard.

   Flex Dashboard configuration pane is shown.
5. Fill fitting title and description and click **Save** button.
6. Click ✉ to configure a new flex dashlet.

Widget configuration pane is shown.
7. Locate earlier scheduled report in **Data Source** dropdown.
8. Select **Chart Type** from dropdown.
9. Select extent of data to be displayed in **Duration** dropdown.
10. Select computation type in **Value Field Setting** dropdown.
11. Select evaluation duration in **As Of** dropdown.
12. Select comparable values in **X Axis** with suitable label.
13. Select numeric values in **Y Axis** with suitable label.
14. Select comparable sequence in **Legend**.
15. Click **Test** button to evaluate.

Evaluated chart is shown.

*Figure 25*

16. Click ‘customize’ icon to locate and choose created dashlet.
17. Click icon to add dashlet to earlier created dashboard.
Sample Reports

1. Phonefactor Authentication succeeded

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Computer</th>
<th>User</th>
<th>Source Address</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/28/2015 11:27:37 AM</td>
<td>PHONEFACTOR</td>
<td>Coreym</td>
<td>68.83.142.12.</td>
<td>SUCCESS_WITH_PIN - &quot;PIN Entered&quot;</td>
</tr>
<tr>
<td>09/28/2015 11:27:37 AM</td>
<td>PHONEFACTOR</td>
<td>Coreym</td>
<td>68.83.142.12.</td>
<td>SUCCESS_WITH_PIN - &quot;PIN Entered&quot;</td>
</tr>
<tr>
<td>09/20/2015 11:27:37 AM</td>
<td>PHONEFACTOR</td>
<td>marwel</td>
<td>66.03.142.15.</td>
<td>SUCCESS_WITH_PIN - &quot;PIN Entered&quot;</td>
</tr>
<tr>
<td>09/20/2015 11:27:37 AM</td>
<td>PHONEFACTOR</td>
<td>marwel</td>
<td>66.03.142.15.</td>
<td>SUCCESS_WITH_PIN - &quot;PIN Entered&quot;</td>
</tr>
<tr>
<td>09/28/2015 11:27:37 AM</td>
<td>PHONEFACTOR</td>
<td>jenny</td>
<td>68.83.142.18.</td>
<td>SUCCESS_WITH_PIN - &quot;PIN Entered&quot;</td>
</tr>
<tr>
<td>09/28/2015 11:27:37 AM</td>
<td>PHONEFACTOR</td>
<td>jenny</td>
<td>68.83.142.18.</td>
<td>SUCCESS_WITH_PIN - &quot;PIN Entered&quot;</td>
</tr>
<tr>
<td>09/28/2015 11:27:37 AM</td>
<td>PHONEFACTOR</td>
<td>Coreym</td>
<td>66.03.142.12.</td>
<td>SUCCESS_WITH_PIN - &quot;PIN Entered&quot;</td>
</tr>
<tr>
<td>09/28/2015 11:27:37 AM</td>
<td>PHONEFACTOR</td>
<td>Coreym</td>
<td>66.03.142.12.</td>
<td>SUCCESS_WITH_PIN - &quot;PIN Entered&quot;</td>
</tr>
</tbody>
</table>

Figure 26
2. Phonefactor Authentication Failed

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>User</th>
<th>Source Address</th>
<th>reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/28/2015 11:06:22 AM</td>
<td>PHONEFACTOR</td>
<td>Donna2</td>
<td>107.217.32.235.</td>
<td>FAILED_PHONE_BUSY - “Call Already In Progress”</td>
</tr>
<tr>
<td>09/28/2015 11:06:22 AM</td>
<td>PHONEFACTOR</td>
<td>jennifer</td>
<td>107.217.32.236.</td>
<td>FAILED_PHONE_BUSY - “Call Already In Progress”</td>
</tr>
<tr>
<td>09/28/2015 11:06:22 AM</td>
<td>PHONEFACTOR</td>
<td>juliet</td>
<td>107.217.32.236.</td>
<td>FAILED_PHONE_BUSY - “Call Already In Progress”</td>
</tr>
<tr>
<td>09/28/2015 11:06:22 AM</td>
<td>PHONEFACTOR</td>
<td>kalf</td>
<td>107.217.32.238.</td>
<td>FAILED_PHONE_BUSY - “Call Already In Progress”</td>
</tr>
<tr>
<td>09/28/2015 11:06:22 AM</td>
<td>PHONEFACTOR</td>
<td>margret</td>
<td>107.217.32.239.</td>
<td>FAILED_PHONE_BUSY - “Call Already In Progress”</td>
</tr>
</tbody>
</table>

Figure 27

3. Phonefactor user configuration changes

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>User</th>
<th>change settings</th>
<th>changed value</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/28/2015 03:59:26 PM</td>
<td>PHONEFACTOR</td>
<td>AMFIRSTave_Monitor</td>
<td>Syslog value &quot;logErrorsWarnings&quot;</td>
<td>false to true</td>
</tr>
<tr>
<td>09/28/2015 03:59:26 PM</td>
<td>PHONEFACTOR</td>
<td>AMFIRSTave_Monitor</td>
<td>Syslog value &quot;logErrorsWarnings&quot;</td>
<td>false to true</td>
</tr>
<tr>
<td>09/28/2015 03:59:26 PM</td>
<td>PHONEFACTOR</td>
<td>AMFIRSTave_Monitor</td>
<td>Syslog value &quot;logErrorsWarnings&quot;</td>
<td>false to true</td>
</tr>
<tr>
<td>09/28/2015 03:59:26 PM</td>
<td>PHONEFACTOR</td>
<td>AMFIRSTave_Monitor</td>
<td>Syslog value &quot;logErrorsWarnings&quot;</td>
<td>false to true</td>
</tr>
<tr>
<td>09/28/2015 03:59:26 PM</td>
<td>PHONEFACTOR</td>
<td>AMFIRSTave_Monitor</td>
<td>Syslog value &quot;logErrorsWarnings&quot;</td>
<td>false to true</td>
</tr>
<tr>
<td>09/28/2015 03:59:26 PM</td>
<td>PHONEFACTOR</td>
<td>AMFIRSTave_Monitor</td>
<td>Syslog value &quot;logErrorsWarnings&quot;</td>
<td>false to true</td>
</tr>
<tr>
<td>09/28/2015 03:59:26 PM</td>
<td>PHONEFACTOR</td>
<td>AMFIRSTave_Monitor</td>
<td>Syslog value &quot;logErrorsWarnings&quot;</td>
<td>false to true</td>
</tr>
<tr>
<td>09/28/2015 03:59:26 PM</td>
<td>PHONEFACTOR</td>
<td>AMFIRSTave_Monitor</td>
<td>Syslog value &quot;logErrorsWarnings&quot;</td>
<td>false to true</td>
</tr>
<tr>
<td>09/28/2015 03:59:26 PM</td>
<td>PHONEFACTOR</td>
<td>AMFIRSTave_Monitor</td>
<td>Syslog value &quot;logErrorsWarnings&quot;</td>
<td>false to true</td>
</tr>
</tbody>
</table>

Figure 28