Integrate Microsoft Exchange Server

EventTracker v8.x and above
Abstract

EventTracker allows you to effectively manage your systems and provides operational efficiencies – reducing IT costs and freeing resources for other duties that increase the business value of your organization. EventTracker’s built-in knowledge base enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 8.x and later, and Microsoft Exchange Server 2010, 2013 and 2016.

Audience

EventTracker users, who wish to monitor Microsoft Exchange Server.
# Table of Contents

Abstract .......................................................................................................................... 1  
Scope ............................................................................................................................... 1  
Audience .......................................................................................................................... 1  
Introduction ..................................................................................................................... 3  
Prerequisites ................................................................................................................... 3  
Enable Logging on Exchange Server ............................................................................. 3  
EventTracker Knowledge Pack ..................................................................................... 8  
   Flex Reports ................................................................................................................. 8  
   Categories .................................................................................................................... 16  
   Knowledge Objects .................................................................................................... 16  
Import Exchange Server knowledge pack into EventTracker ...................................... 17  
   Category .................................................................................................................... 18  
   Parsing Rules ............................................................................................................. 19  
   Knowledge Objects ................................................................................................... 19  
   Flex Reports ............................................................................................................. 21  
   Dashboards ............................................................................................................... 22  
Verify Exchange Server knowledge pack in EventTracker ......................................... 26  
   Categories ................................................................................................................. 26  
   Knowledge Objects .................................................................................................. 26  
   Flex Reports ............................................................................................................. 27  
   Dashboards ............................................................................................................... 28  
   Sample Flex Dashboards ......................................................................................... 29
Introduction

Microsoft Exchange Server is Microsoft's email, calendaring, contact, scheduling and collaboration platform deployed on the Windows Server operating system for use within a business or larger enterprise. Microsoft designed Exchange Server to give users access to the messaging platform on smartphones, tablets, desktops and web-based systems. Exchange users collaborate through calendar and document sharing. Storage and security features in the platform let organizations archive content, perform searches and execute compliance tasks.

With EventTracker you can monitor all your servers running Microsoft Exchange from a single view. EventTracker centrally consolidates all the event logs, SMTP logs and connectivity logs. Through consolidated logging you can monitor the performance, availability, and security of your Exchange servers. EventTracker can generate flex reports for mailbox access, mailbox changes, message tracking, audit activity, user permission and database changes by admin.

Prerequisites

- Exchange Server should be installed on Microsoft Windows Server 2010 R2 and later.
- EventTracker Agent should be installed on the respective server.
- PowerShell version 4.0 or later should be installed.
- PS session module should be installed.
- User Permissions needed.

Enable Logging on Exchange Server

1. Copy the MSExchange folder from <Installation Path>\Prism Microsystems\EventTracker\Knowledge Packs\Microsoft Exchange.
2. Save MSExchange folder to a desired location in exchange server, run executable file “MSExchange Integrator.exe” as Exchange Admin.
3. After launching integrator, a prerequisite check for Exchange server, EventTracker Agent and PowerShell 5.0 is done. If all the perquisites are available, then integrator will allow you to continue with the configuration.
4. Select the logs you want to monitor.
5. Under **Message Trace Logs**, you have an option of writing logs to either Default or Custom Location.

6. **Monitor Mailbox Operation** section gives you options to enable mailbox monitoring either for all users or selected users.
   - **All Users**: This option enables Mailbox Monitoring for all the users.
- **Selected Users**: This option enables Mailbox Monitoring for all specified set of users. You can specify this list of users in a text file and locate the file using the browse button on the integrator.

  **Note**: You should specify the text file as shown below.
7. **Administrator Audit Logging** enables logging for admin activities.

8. Once all the required logging are selected, click **Next**.
9. On clicking **Next**, the configuration will be applied and relevant information about successful configuration or any errors that occur are written in the console.

![Console](image)

**Figure 7**

10. Enter the **Exchange admin credentials**, this will create a task in task scheduler.

![Windows PowerShell credential request](image)

**Figure 8**

11. Once all the configuration are done, a **Configuration successful!** message is displayed.
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 Enterprise to support Exchange Server.

Flex Reports

- **Microsoft Exchange- Message tracking details** - This report gives the information about all mails sent or received through the exchange server.
Sample logs:

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
</table>

Figure 11

- **Microsoft Exchange- Mailbox changes by admin** - This report gives the information about mailbox changes by admin.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Server Name</th>
<th>Changed By</th>
<th>Object Changed</th>
<th>Command Executed</th>
<th>Command Parameters</th>
<th>Execution Status</th>
</tr>
</thead>
</table>

Figure 12
Sample logs:

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul 11 04:24 PM</td>
<td>ENTRY: RunDate: 7/2/2018 6:05:32 PM OriginatingServer: 192.168.10.10.50</td>
</tr>
<tr>
<td>event_log_type</td>
<td>Event Log Type: Application</td>
</tr>
<tr>
<td>event_type</td>
<td>Type: Information</td>
</tr>
<tr>
<td>event_id</td>
<td>ID: 3230</td>
</tr>
<tr>
<td>event_source</td>
<td>Source: EventTracker</td>
</tr>
<tr>
<td>event_user_domain</td>
<td>Domain: N/A</td>
</tr>
<tr>
<td>event_computer</td>
<td>Computer: Microsoft Exchange</td>
</tr>
<tr>
<td>event_user_name</td>
<td>User: N/A</td>
</tr>
<tr>
<td>event_description</td>
<td>Description: ENTER: RunDate: 7/2/2018 6:05:32 PM</td>
</tr>
</tbody>
</table>

**Figure 13**

- **Microsoft Exchange - Mailbox audit details** - This report gives the information about all mailbox audit activities.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Server Name</th>
<th>Changed By</th>
<th>Changed By Role</th>
<th>Operation Performed</th>
<th>Operation Status</th>
<th>User Changed</th>
<th>User Email Address</th>
<th>Folder Changed</th>
<th>User Workstation</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/6/2018 9:52:54 AM</td>
<td>contoso-server4dc</td>
<td>Carol</td>
<td>Delegate</td>
<td>SendAs</td>
<td>Succeeded</td>
<td>Tender HelpDesk</td>
<td><a href="mailto:tender.helpdesk@puto.com">tender.helpdesk@puto.com</a></td>
<td>Inbox</td>
<td>11.12.23.125</td>
</tr>
<tr>
<td>7/6/2018 2:07:46 PM</td>
<td>contoso-server5dc</td>
<td>Nazia</td>
<td>Delegate</td>
<td>Update</td>
<td>Succeeded</td>
<td>Tender HelpDesk</td>
<td><a href="mailto:nazia.C@puto.com">nazia.C@puto.com</a></td>
<td>Inbox</td>
<td>11.20.23.241</td>
</tr>
<tr>
<td>7/6/2018 2:06:03 PM</td>
<td>contoso-server5dc</td>
<td>Nazia</td>
<td>Delegate</td>
<td>Create</td>
<td>Succeeded</td>
<td>Tender HelpDesk</td>
<td><a href="mailto:nazia.C@puto.com">nazia.C@puto.com</a></td>
<td>Calendar</td>
<td>11.23.23.12</td>
</tr>
</tbody>
</table>

**Figure 14**
Sample logs:

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
</table>

- **Microsoft Exchange - Mailbox access by owner** - This report gives the information about mailbox activities by owner.

![Figure 15](image)

![Figure 16](image)
Sample logs:

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul 12 01:00:07 PM</td>
<td>ENTRY: LastAccessed: 7/9/2018 2:07:47 PM OriginatingServer: (14.03.0227.000) LogonUserDisplayName: <a href="mailto:nazia.C@judo.com">nazia.C@judo.com</a> LogonType: Owner</td>
</tr>
<tr>
<td>event_log_type</td>
<td>+ - Application</td>
</tr>
<tr>
<td>event_type</td>
<td>+ - Information</td>
</tr>
<tr>
<td>event_id</td>
<td>+ - 3230</td>
</tr>
<tr>
<td>event_source</td>
<td>+ - EventTracker</td>
</tr>
<tr>
<td>event_user_domain</td>
<td>+ - N/A</td>
</tr>
<tr>
<td>event_computer</td>
<td>+ - Microsoft Exchange</td>
</tr>
<tr>
<td>event_user_name</td>
<td>+ - N/A</td>
</tr>
</tbody>
</table>
| event_description     | ENTRY: LastAccessed: 7/9/2018 2:07:47 PM OriginatingServer: (14.03.0227.000) LogonUserDisplayName: nazia.C@judo.com LogonType: Owner Operation: SendAs OperationResult: Succeeded MailboxResolvedOwnerName: Tender HelpDesk MailboxOwnerUPN: nazia.C@judo.com FolderPathName: ClientIPAddress: F:\mail|"Figure 17

- **Microsoft Exchange- Mailbox access by non-owner** - This report gives the information about mailbox activities by non-owner.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Server Name</th>
<th>Changed By</th>
<th>Changed by Role</th>
<th>Operation Performed</th>
<th>Operation Status</th>
<th>User Changed</th>
<th>User Email Address</th>
<th>Folder Changed</th>
<th>User Workstation</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/9/2018 2:07:47 PM</td>
<td>contbco-server4dc (14.03.0227.000)</td>
<td>Nazia</td>
<td>Delegate</td>
<td>SendAs</td>
<td>Succeeded</td>
<td>Tender HelpDesk</td>
<td><a href="mailto:nazia.C@judo.com">nazia.C@judo.com</a></td>
<td>12.56.23.56</td>
<td></td>
</tr>
<tr>
<td>7/9/2018 2:08:34 AM</td>
<td>contbco-server2dc (14.03.0227.000)</td>
<td>Nazia</td>
<td>Delegate</td>
<td>Update</td>
<td>Succeeded</td>
<td>Tender HelpDesk</td>
<td><a href="mailto:tenderHelper@judo.com">tenderHelper@judo.com</a></td>
<td>12.56.23.45</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 18**
Sample logs:

- **Microsoft Exchange - Admin audit details** - This report gives the information about admin audit activities.
**Sample logs:**

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul 11 04:04:24 PM</td>
<td>ENTRY: RunDate: 7/2/2018 6:05:32 PM OriginatingServer: 15.00.0516.025 Caller: 15.1.128.105.105 ObjectModified: 15.1.128.105.105</td>
</tr>
<tr>
<td>event_log_type</td>
<td>+ Application</td>
</tr>
<tr>
<td>event_type</td>
<td>+ Information</td>
</tr>
<tr>
<td>event_id</td>
<td>+ 3230</td>
</tr>
<tr>
<td>event_source</td>
<td>+ EventTracker</td>
</tr>
<tr>
<td>event_user_domain</td>
<td>+ N/A</td>
</tr>
<tr>
<td>event_computer</td>
<td>+ Microsoft Exchange</td>
</tr>
<tr>
<td>event_user_name</td>
<td>+ N/A</td>
</tr>
<tr>
<td>event_description</td>
<td>ENTRY: RunDate: 7/2/2018 6:05:32 PM OriginatingServer: 15.00.0516.025 Caller: 15.1.128.105.105 ObjectModified: 15.1.128.105.105</td>
</tr>
</tbody>
</table>

**Figure 21**

- **Microsoft Exchange- Database changes by admin** - This report gives the information about database changes by admin.

**Figure 22**

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Server Name</th>
<th>Changed By</th>
<th>Object Changed</th>
<th>Command Executed</th>
<th>Command Parameters</th>
<th>Execution Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/4/2018 1:53:27 PM</td>
<td>contoso-server4dc (15.00.0516.025)</td>
<td>mtpko.com/Users/Joe Taylor</td>
<td>Mailbox Database 1365910500</td>
<td>Mount-Database</td>
<td>CmddParameters/Parameter/Name True e=[Identity]; CmddParameters/Parameter/Value e=[Mailbox Database 1365910500]</td>
<td></td>
</tr>
<tr>
<td>7/4/2018 3:39:18 PM</td>
<td>contoso-server3dc (15.00.0516.025)</td>
<td>mtpko.com/Users/Joe Taylor</td>
<td>Mailbox Database 1365910565</td>
<td>New-Database</td>
<td>CmddParameters/Parameter/Name True e=[Identity]; CmddParameters/Parameter/Value e=[Mailbox Database 1365910565]</td>
<td></td>
</tr>
<tr>
<td>7/4/2018 3:38:19 PM</td>
<td>contoso-server4dc (15.00.0516.025)</td>
<td>mtpko.com/Users/Joe Taylor</td>
<td>Mailbox Database 1365910500</td>
<td>Dismount-Database</td>
<td>CmddParameters/Parameter/Name True e=[Identity]; CmddParameters/Parameter/Value e=[Mailbox Database 1365910500]</td>
<td></td>
</tr>
</tbody>
</table>
Integrate Microsoft Exchange Server

**Sample logs:**

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
</table>

**Microsoft Exchange - User permission changes by admin** - This report gives the information about user permission changes by admin.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Server Name</th>
<th>Changed By</th>
<th>Object Changed</th>
<th>Command Executed</th>
<th>Command Parameters</th>
<th>Execution Status</th>
</tr>
</thead>
</table>

Figure 23

Figure 24

EventTracker
Actionable Security Intelligence
Sample logs:

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul 11 04:24</td>
<td>ENTRY: RunDate: 7/2/2018 6:05:32 PM OriginatingServer: \domain\domain (15.00.0516.025) Caller: \domain\domain\Users\Bill Smith, ObjectModified: \domain\domain\Users\Bill Smith Cm</td>
</tr>
</tbody>
</table>

Figure 25

Categories

- **Microsoft Exchange: Admin Audit** - This category provides information related to admin audit activities.
- **Microsoft Exchange: Mailbox Audit** - This category provides information related to mailbox audit activities.
- **Microsoft Exchange: Message Tracking** - This category provides information related to all mails traversing the exchange server.

Knowledge Objects

- **Microsoft Exchange: Admin Audit** - This knowledge object helps to analyze logs related to admin audit activities.
- **Microsoft Exchange: Mailbox Audit** - This knowledge object helps to analyze logs related to mailbox audit activities.
- **Microsoft Exchange: Message Tracking** - This knowledge object helps to analyze logs related to all mails traversing the exchange server.
Import Exchange Server knowledge pack into EventTracker

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

- Categories
- Parsing Rules
- Knowledge Objects
- Flex Reports
- Dashboards

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.
3. Click the **Import** tab.

![EventTracker Control Panel](image)

*Figure 26*
Category

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

![Figure 27](image1.png)

2. Locate **Category_Microsoft Exchange.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button. EventTracker displays success message.

![Figure 28](image2.png)
4. Click OK, and then click the Close button.

Parsing Rules

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

![Export Import Utility window](image)

Figure 29

2. Locate Token Value.Microsoft Exchange.istoken file, and then click the Open button.
3. To import alerts, click the Import button.

Knowledge Objects

1. Click Knowledge objects under Admin option in the EventTracker manager page.
2. Locate the KO.Microsoft Exchange.etko file.
3. Click the ‘Upload’ option.
4. Now select all the check box and then click on ‘Import’ option.
5. Knowledge objects are now imported successfully.

![Image of successful import message]

Figure 32

6. Click OK, and then click the Close button.

**Flex Reports**

On EventTracker Control Panel,

1. Click Reports option, and select new (*.etcrx) from the option.

![Image of EventTracker Control Panel with Reports option selected]

Figure 33

2. Locate the Reports_Microsoft Exchange.eetcrx file and select all the check box.
3. Click the **Import** button to import the reports. EventTracker displays success message.

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

**Dashboards**

**Note:** If you have EventTracker Enterprise version **v9.0**, you can import dashboards.
1. Open **EventTracker Enterprise**.

![Figure 36](image)

2. Navigate to **Dashboard>My Dashboard**.

3. Click the ‘**Import**’ button to import the dashlets.

![Figure 37](image)
4. Locate the **Dashboard_Microsoft Exchange.etwd** file.
5. Click the ‘**Upload**’ option.

![Image of Import dashlets - Mozilla Firefox](image)

6. Now select all the check boxes and then click on ‘**Import**’ option. Dashlets are now imported successfully.
7. Click the ‘**Add**’ button to create a new dashboard.
Integrate Microsoft Exchange Server

8. Fill suitable Title and Description and click **Save** button.

9. Click ‘**Customize**’ 📊 to locate **Microsoft Exchange** dashlets and choose all imported dashlets for **Microsoft Exchange Server**.

10. Click ‘**Add**’ to include dashlets in dashboard.
Verify Exchange Server knowledge pack in EventTracker

Categories

1. Logon to EventTracker Enterprise.
2. Click Admin dropdown, and then click Categories.
3. In Category Tree to view imported categories, scroll down and expand Microsoft Exchange group folder to view the imported categories.

![Category Tree](image)

Knowledge Objects

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Knowledge Objects.
2. In the Knowledge Object tree, expand Microsoft Exchange group folder to view the imported Knowledge objects.
Flex Reports

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

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

3. Click on the **Microsoft Exchange** group folder to view the imported Exchange Server reports.
Dashboards

1. Open EventTracker Enterprise in browser and logon.
2. Navigate to Dashboard>My Dashboard.
   My Dashboard pane is shown.
Sample Flex Dashboards

1. **Microsoft Exchange- Mailbox Changes by Admin**: This dashboard provides information related to mailbox changes by admin.

![Microsoft Exchange- Mailbox Changes by Admin](image)

*Figure 46*

2. **Microsoft Exchange- Admin Audit Activity**: This dashboard provides information related to admin audit activates.

![Microsoft Exchange- Admin Audit Activity](image)

*Figure 47*
3. **Microsoft Exchange - Mailbox Access by Non-Owner:** This dashboard provides information related to mailbox activities by non-owner.

![Microsoft Exchange - Mailbox Access by Non-Owner](image)

*Figure 48*