Integrate Microsoft Office 365
EventTracker v9.x and above

Publication Date: May 27, 2019
Abstract

This guide provides instructions to configure Office 365 to generate logs for critical events. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor Office 365 usage.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 9.x and later, and Microsoft Office 365.

Audience

IT admins, Office 365 administrators and EventTracker users who wish to forward logs to EventTracker Manager and monitor events using EventTracker Enterprise.
# Table of Contents

Abstract ............................................................................................................................................. 1  
Scope .................................................................................................................................................. 1  
Audience ............................................................................................................................................. 1  
Overview ........................................................................................................................................... 3  
Prerequisites ...................................................................................................................................... 3  
Configuring Office 365 to forward logs to EventTracker ................................................................. 3  
  User and Application Creation using Office 365 Integrator .............................................................. 3  
  Granting permission to App .................................................................................................................. 7  
  User and Application Creation without Integrator ............................................................................. 9  
  Assigning Compliance Management Permission to an Office 365 User ....................................... 11  
  Registering Application with your Azure Active Directory Tenant ................................................. 14  
Verifying Office 365 Integration ......................................................................................................... 21  
Office 365 Error .................................................................................................................................. 22  
EventTracker Knowledge Pack (KP) .................................................................................................... 23  
  Alert .................................................................................................................................................. 23  
  Reports ............................................................................................................................................ 24  
Importing Knowledge Pack into EventTracker .................................................................................. 26  
  Alerts .............................................................................................................................................. 26  
  Knowledge Objects ........................................................................................................................... 27  
  Flex Reports ................................................................................................................................... 29  
  Dashlets ......................................................................................................................................... 32  
Verifying Knowledge Pack in EventTracker ....................................................................................... 35  
  Alerts .............................................................................................................................................. 35  
  Knowledge Object ............................................................................................................................ 36  
  Flex Reports ................................................................................................................................... 37  
  Dashlets ......................................................................................................................................... 38  
Sample Dashboards ............................................................................................................................. 38
Overview

EventTracker Knowledge pack for Office 365 captures important and critical activities in Exchange and Azure Active Directory. Monitoring these activities is critical from a security aspect and is required for compliance and operational reasons. The dashboards, reports will help you in getting deeper insights to analyze various security use cases like login activities from different countries, changes in user permission, spam and malicious email detection and mailbox auditing. EventTracker detects and alerts a spoofed email from the received emails.

EventTracker helps you to monitor day to day activities of Office 365 Exchange like mailbox storage usage and summary of mail traffic.

Prerequisites

- **EventTracker v9.x or above** should be installed.
- **PowerShell 5.0** should be installed on the EventTracker Manager.
- Office 365 service account should have “Report Reader Role” and **Compliance Management** permission. Instructions are mentioned [here](#).
- Make sure **Auditing** is enabled on your Tenant. Instructions are mentioned [here](#).
- The App should be registered in Azure AD with **Office 365 Management API** and **Microsoft graph API** permission. Instructions are mentioned [here](#).
- Enable the following URL, if there is any web filter or firewall in between:
  - https://graph.microsoft.com
  - https://login.windows.net
  - https://manage.office.com

Configuring Office 365 to forward logs to EventTracker

User and Application Creation using Office 365 Integrator

2. Save **Office365Integrator.exe** and run the executable file “**Office365Integrator.exe**”.
3. Click on **Browse** and navigate to EventTracker Agent folder and click **Install**.
(After launching an integrator, it will check for PowerShell compatibility. If found compatible, the integrator will allow you to configure office 365. Otherwise, update PowerShell on the machine.)

4. We can create a user with "**Compliance Management** and **Report Reader**" permission through an integrator also. Click on **Create User** and provide the appropriate password for it and then click **OK**. On clicking **OK** provide global administrator credentials for creating a user.
5. If you want to create a “Compliance Management and Report Reader” user manually, follow the step mentioned here.

6. Click on Create Application to create “Microsoft graph and Office 365 Management API” enabled the app in Azure AD and then click OK. If you want to create a “Microsoft Graph” app manually, follow the step mentioned here.

7. Grant the permission on the application before click on “Test Credential”. Follow the step mentioned here.

8. After successful creation of user and application. Click on Next to review configuration.
9. Click on “Test Credential” button to verify credential are proper. If a credential is proper, then the Finish button will be enabled, to complete the integration otherwise, it will show error in “<Office 365 installation folder>/Logs/Office 365 Integrator.logs”. View the details of the error here.

![Office 365 Integrator](image)

**Figure 7**

Granting permission to App

1. Sign in with global administrator to the Azure portal.
2. In the left-hand navigation pane, click the Azure Active Directory service, click App registrations.
3. Click on “All Applications” and navigate to ETSIEMConnector > API permissions and click on “Grant Admin Consent”.

---

7

Integrate Microsoft Office 365

Neturion™ EventTracker
Figure 8

ETSIEMConnection - API permissions

- Permissions have changed. Users and/or admins will have to consent even if they have already done so previously.

<table>
<thead>
<tr>
<th>User.Read</th>
<th>Delegated</th>
<th>Sign-in and read user profile</th>
<th>-</th>
<th>Granted for EventTracker</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuditLogs.ReadAll</td>
<td>Application</td>
<td>Read all audit log data</td>
<td>Yes</td>
<td>Granted for EventTracker</td>
</tr>
<tr>
<td>Reports.Read.All</td>
<td>Application</td>
<td>Read all usage reports</td>
<td>Yes</td>
<td>Granted for EventTracker</td>
</tr>
<tr>
<td>SecurityEvents.Read.All</td>
<td>Application</td>
<td>Read your organization’s security events</td>
<td>Yes</td>
<td>Granted for EventTracker</td>
</tr>
<tr>
<td>SecurityEvents.ReadWithAllAb</td>
<td>Application</td>
<td>Read and update your organization’s security events</td>
<td>Yes</td>
<td>Not granted for EventTracker</td>
</tr>
<tr>
<td>Office 365 Management APIs (7)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ActivityFeed.Read</td>
<td>Application</td>
<td>Read activity data for your organization</td>
<td>Yes</td>
<td>Granted for EventTracker</td>
</tr>
<tr>
<td>ActivityFeed.ReadDlp</td>
<td>Application</td>
<td>Read DLP policy events including detected sensitive data</td>
<td>Yes</td>
<td>Granted for EventTracker</td>
</tr>
<tr>
<td>ActivityReports.Read</td>
<td>Application</td>
<td>Read activity reports for your organization</td>
<td>Yes</td>
<td>Granted for EventTracker</td>
</tr>
<tr>
<td>ActivityReports.Read</td>
<td>Application</td>
<td>Read activity reports for your organization</td>
<td>Yes</td>
<td>Granted for EventTracker</td>
</tr>
<tr>
<td>ServiceHealth.Read</td>
<td>Application</td>
<td>Read service health information for your organization</td>
<td>Yes</td>
<td>Granted for EventTracker</td>
</tr>
<tr>
<td>ThreatIntelligence.Read</td>
<td>Application</td>
<td>Read threat intelligence data for your organization</td>
<td>Yes</td>
<td>Granted for EventTracker</td>
</tr>
<tr>
<td>ThreatIntelligence.Read</td>
<td>Application</td>
<td>Read threat intelligence data for your organization</td>
<td>Yes</td>
<td>Granted for EventTracker</td>
</tr>
</tbody>
</table>

These are the permissions that the application requests statically. You may also request user consentable permissions dynamically through the [API](https://www.eventtracker.com). See best practices for requesting permissions.

Grant consent

To consent to permissions that require admin consent, please sign in with an account that is an administrator for this directory.

Grant admin consent for EventTracker Security LLC

Figure 9
User and Application Creation without Integrator

You need to follow these steps if you want to create User and application without integrator. If you have followed the above steps, then ignore these steps.

1. Contact EventTracker Support for Office 365 Integration package.
2. Save Office365Integrator.exe and run the executable file “Office365Integrator.exe”.

(After launching the integrator, it will check for PowerShell compatibility. If it is found compatible, the integrator will allow you to configure office 365. Otherwise, update PowerShell on the EventTracker Manager machine.)
3. Follow the Registering Application section, Assigning Compliance Management permission sections for application and user creation respectively. Fill the details of User details and Application details.
4. Fill Office 365 service account details having Compliance Management permission. Service account with administrative access is not required to fetch the logs and a normal service account with “Compliance Management” permission would suffice. For creating a service account with Compliance Management permissions, follow the instructions mentioned here.

5. Fill the details of the app registered in Azure AD with Microsoft graph and Office 365 Management API permission. If the user does not have an app registered in Azure AD, follow the instructions mentioned here.

6. Provide the tenant ID for the enterprise. Follow the instruction mentioned here, if tenant ID is not known.

7. Also, fill EventTracker Manager textbox with EventTracker manager system IP or hostname. Provide EventTracker Group details under which office 365 system should reside.

8. Once you provide all details in the Integrator “Test Credential” button will be enabled. Click on “Test Credential” to validate the details provided. If the credential is proper, then the Finish button will be enabled otherwise, it will show error in <Office 365 installation folder>/Logs/Office 365 Integrator.logs. View the details of the error here.

9. Click on the Finish button to Complete the Integration.

Assigning Compliance Management Permission to an Office 365 User

For creating Office 365 service account with “Reports Reader and Compliance Management” role permission, please follow the below procedure. This procedure should be carried out by a user having Administrator rights in Office365.

1. Create the user (ETreports@contoso.com) with the “Reports Reader” role. Follow the instructions mentioned here.

2. Click here to go to the Office 365 admin center.

3. Go to the Office 365 admin center by selecting the app launcher icon Office 365 app launcher in the upper-left and choose Admin.

![Office 365 app launcher](image)

Figure 13
4. On the left, select Admin Centers and then select Exchange.

![Figure 14](image)

5. On the left pane, select **Permissions**.

![Figure 15](image)
6. On the right pane, click on **Compliance Management** and click on **+**.

![Figure 16](image)

7. Scroll to **Members** and Click **+**.

![Figure 17](image)
8. Select the **User Name** (e.g. ETreports@contoso.com) and click **Ok**.

![Select Members - Mozilla Firefox](image)

Figure 18

9. Save the changes.

**Registering Application with your Azure Active Directory Tenant**

If the application has not been registered in Azure AD, follow the below procedure. This procedure should be carried out by a user having **Global Administrator** rights in Office365.

2. If your account gives you access to more than one, click your account in the top right corner, and set your portal session to the desired Azure AD tenant.  
3. In the left-hand navigation pane, click the **Azure Active Directory** service, click **App registrations**, and click **New registration**.
4. When the **Create** page appears, enter your application's registration information:
   - **Name**: Enter an appropriate application name (e.g. ETSIEMConnector).
   - **Supported account types**: Select **Accounts in this organizational directory only**.
   - **Redirect URI**: Select **Web** and Enter **http://localhost**.
Register an application

* Name
The user-facing display name for this application (this can be changed later).

ETSIEEMConnector

Supported account types
Who can use this application or access this API?

- [ ] Accounts in this organizational directory only
- [ ] Accounts in any organizational directory
- [ ] Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

Help me choose...

Redirect URI (optional)
We’ll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

[ ] Web

http://localhost

By proceeding, you agree to the Microsoft Platform Policies

Register

Figure 20
5. When finished, click **Register**. Azure AD assigns a unique Application ID to your application, and you are taken to your application’s main registration page. Note down the **Application ID**.

6. To add permission(s) to access resource APIs from your client,

   - Click the **API Permissions** section.
   - Click the **Add a Permission** button.
   - Click the **Microsoft API** tab to select the type of resources you want to pick from and select the **Microsoft Graph**.

   ![Request API permissions](image)

   **Commonly used Microsoft APIs**

   - **Microsoft Graph**
     
     Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

   - **Azure Data Catalog**
     
     Programmatic access to Data Catalog resources to register, annotate and search data assets.

   - **Azure Data Explorer**
     
     Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions.

   - **Azure Key Vault**
     
     Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults.

   - **Azure Rights Management Services**
     
     Allow validated users to read and write protected content.

   - **Azure Service Management**
     
     Programmatic access to much of the functionality available through the Azure portal.

   - **Data Export Service for Microsoft Dynamics 365**
     
     Export data from Microsoft Dynamics CRM organization to an external destination.

   - **Dynamics 365 Business Central**
     
     Programmatic access to data and functionality in Dynamics 365 Business Central.

   - **Dynamics CRM**
     
     Access the capabilities of CRM business software and ERP systems.

   - **Flow Service**
     
     Embed flow templates and manage flows.

   - **Intune**
     
     Programmatic access to Intune data.

   - **Office 365 Management APIs**
     
     Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity.

   - **OneNote**
     
     Create and manage notes, lists, pictures, files, and more in OneNote notebooks.

   - **Power BI Service**
     
     Programmatic access to Dashboard resources such as Datasets, Tables, and Rows in Power BI.

   - **PowerApps Runtime Service**
     
     Powerful data storage, modeling, security and integration capabilities.

   - **SharePoint**
     
     Interact remotely with SharePoint data.

   ![Figure 21](image)
7. After selecting the Microsoft Graph, add following application permissions:
   - Read your organization’s security events.
   - Read all usage reports.
   - Read all audit log data.

8. Now, we need to select “Office 365 Management API” in the required permissions and select all application permission.
## Request API permissions

<table>
<thead>
<tr>
<th>All APIs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office 365 Management APIs</td>
</tr>
<tr>
<td><a href="https://manage.office.com/">https://manage.office.com/</a> Docs</td>
</tr>
</tbody>
</table>

What type of permissions does your application require?

- **Delegated permissions**
  - Your application needs to access the API as the signed-in user.
- **Application permissions**
  - Your application runs as a background service or daemon without a signed-in user.

### Select permissions

<table>
<thead>
<tr>
<th>PERMISSION</th>
<th>ADMIN CONSENT REQUIRED</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ActivityFeed (2)</strong></td>
<td></td>
</tr>
<tr>
<td>ActivationFeed.Read</td>
<td>Read activity data for your organization</td>
</tr>
<tr>
<td>ActivationFeed.ReadDlp</td>
<td>Read DLP policy events including detected sensitive data</td>
</tr>
<tr>
<td><strong>ActivityReports (2)</strong></td>
<td></td>
</tr>
<tr>
<td>ActivationReports.Read</td>
<td>Read activity reports for your organization</td>
</tr>
<tr>
<td>ActivationReports.ReadDlp</td>
<td>Read activity reports for your organization</td>
</tr>
<tr>
<td><strong>ServiceHealth (1)</strong></td>
<td></td>
</tr>
<tr>
<td>ServiceHealth.Read</td>
<td>Read service health information for your organization</td>
</tr>
<tr>
<td><strong>ThreatIntelligence (2)</strong></td>
<td></td>
</tr>
<tr>
<td>ThreatIntelligence.Read</td>
<td>Read threat intelligence data for your organization</td>
</tr>
<tr>
<td>ThreatIntelligence.ReadDlp</td>
<td>Read threat intelligence data for your organization</td>
</tr>
</tbody>
</table>

Add permissions | Discard

---

**Figure 23**

9. Click **Grant admin consent** after selecting permission. For granting permissions, the user(s) with “**Global Administrator**” privileges are required.
You are taken to the application's main registration page, to add a secret key for your web application's credentials:

- Click the **Certificates & secrets** section on the **Settings** page.
- Add a description for your key (e.g. ETKey).
- Select **Never** from the **expires** section.
- Click **Add**. The right-most column will contain the key value after you save the configuration. Make note of value generated, this will be used in integrator as **client secret**.
Client secrets
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>EXPIRES</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETKey</td>
<td>12/31/2299</td>
<td>F6j1RtmMHInDyQyFSpkc_d/8+BYWdnc05y</td>
</tr>
</tbody>
</table>

Figure 26

11. Note down Application ID and Tenant ID after completing app configuration.

<table>
<thead>
<tr>
<th>Display name</th>
<th>ETSIEMConnector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application (client) ID</td>
<td>bu5f36b5-ad0e-428d-aada-bb1d5f419016</td>
</tr>
<tr>
<td>Directory (tenant) ID</td>
<td>af6e1548-8f43-41d3-ae27-2b0b6c2c0d67a</td>
</tr>
<tr>
<td>Object ID</td>
<td>03146be-8a7a-4496-93fe-bd400d519196</td>
</tr>
</tbody>
</table>

Figure 27

Verifying Office 365 Integration
After providing details in Office 365 Integrator, follow the steps to verify the office 365 integration.

1. Check if the following task is created in Task Scheduler.
# Office 365 Error

Following are the error table for office 365:

<table>
<thead>
<tr>
<th>Code</th>
<th>Message</th>
<th>Troubleshooting</th>
</tr>
</thead>
<tbody>
<tr>
<td>AF10001</td>
<td>The permission set ({0}) sent in the request did not include the expected permission ActivityFeed.Read.</td>
<td>Check the permission on application registered</td>
</tr>
<tr>
<td></td>
<td>{0} = the permission set in the access token.</td>
<td></td>
</tr>
<tr>
<td>AF20001</td>
<td>Missing parameter: {0}.</td>
<td>Contact the EventTracker support team</td>
</tr>
<tr>
<td></td>
<td>{0} = the name of the missing parameter.</td>
<td></td>
</tr>
<tr>
<td>AF20002</td>
<td>Invalid parameter type: {0}. Expected type: {1}</td>
<td>Contact the EventTracker support team</td>
</tr>
<tr>
<td></td>
<td>{0} = the name of the invalid parameter.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>{1} = the expected type (int, datetime, guid).</td>
<td></td>
</tr>
<tr>
<td>AF20003</td>
<td>Expiration {0} provided is set to past date and time.</td>
<td>Contact the EventTracker support team</td>
</tr>
<tr>
<td></td>
<td>{0} = the expiration passed in the API call.</td>
<td></td>
</tr>
<tr>
<td>AF20010</td>
<td>The tenant ID passed in the URL ({0}) does not match the tenant ID passed in the access token ({1}).</td>
<td>Check the tenant Id provided in Office 365 form</td>
</tr>
<tr>
<td></td>
<td>{0} = tenant ID passed in the URL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>{1} = tenant ID passed in the access token</td>
<td></td>
</tr>
<tr>
<td>AF20011</td>
<td>Specified tenant ID ({0}) does not exist in the system or has been deleted.</td>
<td>Contact the Microsoft Support for troubleshooting the issue</td>
</tr>
<tr>
<td></td>
<td>{0} = tenant ID passed in the URL</td>
<td></td>
</tr>
<tr>
<td>AF20012</td>
<td>Specified tenant ID ({0}) is incorrectly configured in the system.</td>
<td>Contact the Microsoft support for troubleshooting the issue</td>
</tr>
<tr>
<td></td>
<td>{0} = tenant ID passed in the URL</td>
<td></td>
</tr>
<tr>
<td>AF20013</td>
<td>The tenant ID passed in the URL ({0}) is not a valid GUID.</td>
<td>Check the tenant Id provided in Office 365 form</td>
</tr>
<tr>
<td></td>
<td>{0} = tenant ID passed in the URL</td>
<td></td>
</tr>
<tr>
<td>AF20020</td>
<td>The specified content type is not valid.</td>
<td>Contact the EventTracker support team</td>
</tr>
<tr>
<td>AF20021</td>
<td>The webhook endpoint {{0}) could not be validated. {1}</td>
<td>Contact the EventTracker support team</td>
</tr>
<tr>
<td></td>
<td>{0} = webhook address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>{1} = &quot;The endpoint did not return HTTP 200.&quot; or &quot;The address must begin with HTTPS.&quot;</td>
<td></td>
</tr>
<tr>
<td>AF20022</td>
<td>No subscription found for the specified content type.</td>
<td>Contact the Microsoft support for troubleshooting the issue</td>
</tr>
</tbody>
</table>
| AF20023 | The subscription was disabled by {0}.  
{0} = "a tenant admin" or "a service admin" | |
| AF20030 | Start time and end time must both be specified (or both omitted) and must be less than or equal to 24 hours apart, with the start time no more than 7 days in the past. | Contact the EventTracker support team |
| AF20031 | Invalid nextPage Input: {0}.  
{0} = the next page indicator passed in the URL | Contact the EventTracker support team |
| AF20050 | The specified content ({{0}}) does not exist.  
{0} = resource id or resource URL | Contact the EventTracker support team |
| AF20051 | Content requested with the key {0} has already expired. Content older than 7 days cannot be retrieved.  
 • {0} = resource id or resource URL | Contact the EventTracker support team |
| AF20052 | Content ID {0} in the URL is invalid.  
{0} = resource id or resource URL | Contact the EventTracker support team |
| AF20053 | Only one language may be present in the Accept-Language header. | Contact the EventTracker support team |
| AF20054 | Invalid syntax in Accept-Language header. | |
| AF429 | Too many requests. Method={0}, PublisherId={1}  
{0} = HTTP Method  
{1} = Tenant GUID used as PublisherIdentifier | Contact the EventTracker support team |
| AF50000 | An internal error occurred. Retry the request. | Contact the EventTracker support team |

**EventTracker Knowledge Pack (KP)**

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

The following Knowledge Packs are available in EventTracker v8.x and later to support Office 365 monitoring:

**Alert**

- **Office 365 - Azure active directory login failure**: This alert will trigger whenever Azure AD user is trying to login but fails.
Integrate Microsoft Office 365

- **Office 365 - Exchange mailbox login failure**: This alert will trigger whenever the mailbox user is trying to login and but fails.
- **Office 365 - Malicious email detected**: This alert will trigger whenever some malicious mail is detected in office 365 exchange.
- **Office 365 - Spam email detected**: This alert will trigger whenever spam mail is detected in office 365 exchange.
- **Office 365 - Threat detection**: This alert will trigger whenever the office 365 ATP module detects malicious/suspicious activity in exchange.

**Reports**

- **Office 365 - Activated user detail**: This report will provide you information related to office 365 activated user, with what kind of OS is used to access office 365.
- **Office 365 - Activation counts**: This report will provide you an overall summary of office 365 activated license with what kind of OS is being used to access office 365.
- **Office 365 - Active user counts**: This report will provide you an overall summary of the user who is active on Exchange, OneDrive, SharePoint, Skype for business, Teams, and Yammer.
- **Office 365 - Azure active directory admin activities**: This report will provide information related to azure active directory admin activities like user management, group management, permission assigning, etc.
- **Office 365 - Azure active directory login activities**: This report will provide information for user login activities from various Office 365 application which are using the azure active directory as the authentication server.
- **Office 365 - Email activity user counts**: This report will provide an overall summary for email activities happening in the Office 365 exchange server. (receive, send, read)
- **Office 365 - Email app usage user counts**: This report will provide an overall summary for application; which user is using for send/receiving the mail. (outlook, imap, pop3, etc)
- **Office 365 - Email app usage user detail**: This report will provide information related to the user using application for sending/receiving the mail.
- **Office 365 - Email app usage version user counts**: This report will provide an overall summary for version usage of email client by a user. (outlook 2016, outlook 2013, etc)
- **Office 365 - Exchange admin activities**: This report will provide detailed information for admin activities done for office 365 exchange like permission changes on a mailbox, mailbox creation, deletion or modification, etc.
- **Office 365 - Exchange mail Traffic Details**: This report will provide you an overall summary related to mail which matches transport rules (BCL0, BCL1, bad mail, good mail, spam mail, etc) of exchange.
- **Office 365 - Exchange mailbox login activities**: This report will provide detailed information related to mailbox login activities.
• **Office 365 - Exchange message trace details**: This report will provide detailed information of mail received/sending by exchange users. If some mail failed to send, then this report will provide a reason for failure.

• **Office 365 - Exchange spam mail traffic details**: This report will provide detailed information on spam mail received by exchange users.

• **Office 365 - Mailbox storage usage**: This report will provide an overall summary for storage used by office 365 exchange mailbox.

• **Office 365 - Mailbox usage detail**: This report will provide information for storage used by office 365 exchange mailbox for each user.

• **Office 365 - Mailbox usage mailbox counts**: This report will provide information for active mailbox count.

• **Office 365 - Mailbox usage quota status mailbox counts**: This report will provide an overall summary for mailbox who reached their mailbox usage quota.

• **Office 365 - Office 365 activation user counts**: This report will provide a summary for office 365 license usage.

• **Office 365 - OneDrive activity file counts**: This report will provide a count of OneDrive activities (viewed or edited, shared externally, synced, shared internally) done on files.

• **Office 365 - OneDrive activity user counts**: This report will provide a count of OneDrive activities (viewed or edited, shared externally, synced, shared internally) done by the user.

• **Office 365 - OneDrive file operations**: This report will provide details information of activities that happened on OneDrive like file uploaded, downloaded, edited, accessed, shared, etc.

• **Office 365 - OneDrive usage account counts**: This report will provide a summary of users who are actively using OneDrive.

• **Office 365 - OneDrive usage account detail**: This report will provide a summary of users who are using OneDrive and count of activities they are doing.

• **Office 365 - OneDrive usage file counts**: This report will provide the total file used by user on OneDrive.

• **Office 365 - OneDrive usage storage**: This report will provide summary of storage used by OneDrive.

• **Office 365 - SharePoint activity user details**: This report will provide activities count done by a user in Office 365 SharePoint.

• **Office 365 - SharePoint site operations**: This report will provide details information on activities happening on Office 365 SharePoint.

• **Office 365 - SharePoint site storage usage**: This report will provide a summary of storage used by SharePoint sites.

• **Office 365 - Skype for business activity user detail**: This report will provide a summary for the activities (peer to peer, conference session, etc) happening in Skype of Business.
Integrate Microsoft Office 365

- **Office 365 - Skype for business device usage user detail**: This report will provide a summary of devices used by a user for doing Skype for business activities.
- **Office 365 - Skype for business peer to peer activity user counts**: This report will provide a summary for peer to peer activities (IM, audio, video, file transfer, app sharing) happening in Skype for business.
- **Office 365 - Threat intelligence activities**: This report will provide detailed information related to threats detected by Office 365 ATP.

**Importing Knowledge Pack into EventTracker**

1. Launch the **EventTracker Control Panel**.
2. Double click **Export/Import Utility**, and then click the **Import** tab.

![EventTracker Control Panel](image)

Figure 29

3. Import **Tokens/Flex Reports** as given below.

**Alerts**

1. Click the **Alert** option, and then click the **browse** button.
2. Locate **Alerts.Office 365.isalt** file, and then click the **Open** button.

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

   EventTracker displays a success message.

   ![Import successful message]

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

**Knowledge Objects**

1. Click **Knowledge objects** under the Admin option in the EventTracker manager page.
2. Locate the file named **KO.Office365 Exchange.etko**.

   ![Knowledge objects page]
3. Now select all the checkbox and then click on the **Import** option.
4. Knowledge objects are now imported successfully.

Flex Reports

1. Click **Reports** option and select new (.etcrx) from the option.
2. Locate the file named **Flex Reports_Office 365.etcrx** and select all the checkbox.
3. Click the **Import** button to import the reports. EventTracker displays a success message.

![Figure 36](image1.png)

![Figure 37](image2.png)
Dashlets

In EventTracker 9.0, we have added a new feature which will help to import/export of dashlet. Following is the procedure to do that:

1. Login into EventTracker Enterprise Web console.

2. Go to My Dashboard option.
3. Click on the **import** button and select `.etwd` File.
4. Click upload and select **Dashboard** which you want to import.
5. Click on the **Import** button. It will upload all selected dashboards.

### Verifying Knowledge Pack in EventTracker

**Alerts**

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

3. In the **Search** box, type ‘**Office 365**’, and then click the **Go** button. Alert Management page will display all the imported alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column.

   EventTracker displays a message box.

   ![Successfully saved configuration](image)

5. Click **OK**, and then click the **Activate Now** button.

   **NOTE:** Specify appropriate **systems** in an **alert configuration** for better performance.

**Knowledge Object**

1. Logon to **EventTracker Enterprise**.

2. Click the **Admin** menu, and then click the **Knowledge Object**.

3. In **Knowledge Object Group Tree** to view imported knowledge object, scroll down and click the **Office 365** group folder.

4. Knowledge Object is displayed in the pane.
Flex Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports menu, and then Configuration.
4. In Report Groups Tree to view imported Scheduled Reports, scroll down and click the Office 365 group folder.
5. Reports are displayed in the Reports configuration pane.
Dashlets

1. Logon to EventTracker Enterprise.
2. Click the Dashboard menu, and then My Dashboard.
3. Then click on Customize Dashlet button and search for “Office 365”

![Customize dashlets]

Sample Dashboards

- Office 365 – Exchange Top Spam mail by sender

![Office 365 – Exchange Top Spam mail by Sender]
- **Office 365 – Exchange Top Spam mail by Recipient**

  ![Office 365 - Exchange Top Spam mail by Recipient](image)

  **Figure 50**

- **Office 365 – Exchange Malicious Email by Threat Name**

  ![Office 365 – Exchange Malicious Email by Threat Name](image)

  **Figure 51**
- **Office 365 – Exchange Malicious Email by Sender**

![Pie chart showing email distribution by sender.](image)

*Figure 52*

- **Office 365 – Exchange Malicious Email by Recipient**

![Pie chart showing email distribution by recipient.](image)

*Figure 53*
• **Office 365 – Exchange Admin Activities by Operation**

![Graph showing Exchange Admin Activities by Operation]

*Figure 54*

• **Office 365 – Exchange Admin Activities by User**

![Graph showing Exchange Admin Activities by User]

*Figure 55*
• **Office 365 – Exchange Activities by User Type**

![Exchange Activities by User Type](figure56)

Figure 56

• **Office 365 – Azure Active Directory Login failed by Reason**

![Azure Active Directory Login failed by Reason](figure57)

Figure 57
• **Office 365 – Azure Active Directory login by user**

![Office 365 - Azure Active Directory login by user](image)

Figure 58

• **Office 365 - Azure Active Directory Login by Status**

![Office 365 - Azure Active Directory login by status](image)

Figure 59
- **Office 365 – Azure Active Directory login failed by Country**

  ![Figure 60](image)

- **Office 365 – Azure Active Directory login Activities by Client IP**

  ![Figure 61](image)
• **Office 365 – Azure Active Directory Events**

![Figure 62](image1.png)

• **Office 365 – SharePoint Activities by Operation**

![Figure 63](image2.png)
• **Office 365 – SharePoint Activities by User**

![Office 365 - Sharepoint Activities by User](image)

**Figure 64**

• **Office 365 – SharePoint Activities by User Agent**

![Office 365 - Sharepoint Activities by User Agent](image)

**Figure 65**
• **Office 365 – SharePoint Activities by File Type**

![Pie chart showing file, page, and web activities](image)

*Figure 66*

• **Office 365 – SharePoint Activities by File Extension**

![Pie chart showing mp4, jpg, xlsx, and png activities](image)

*Figure 67*
- **Office 365 – OneDrive Activities**

![Graph showing Office 365 - OneDrive Activities](image1)

Figure 68

- **Office 365 – OneDrive Activities by Operation**

![Pie chart showing Office 365 - OneDrive Activities by Operation](image2)

Figure 69
• **Office 365 – OneDrive Activities by User**

![Pie chart showing OneDrive activities by user](image)

**Figure 70**

• **Office 365 – OneDrive Activities by User Agent**

![Pie chart showing OneDrive activities by user agent](image)

**Figure 71**
• **Office 365 – OneDrive Activities by Resource**

![Figure 72](image)

• **Office 365 – OneDrive Activities by File Extension**

![Figure 73](image)
• **Office 365 – Exchange Top Sender**

![Office 365 - Exchange Top Sender](image)

Figure 74

• **Office 365 – Exchange Top Recipient**

![Office 365 - Exchange Top Recipient](image)

Figure 75
• Office 365 – SharePoint Activities

![Office 365 - SharePoint Activities chart](image)

**Figure 76**