Integrating Trend Micro OfficeScan 10

*EventTracker v7.x*
Abstract

This guide will help you in configuring Trend Micro OfficeScan events and EventTracker to receive Trend Micro OfficeScan events. You will find the detailed procedures required for monitoring Trend Micro OfficeScan.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 7.X and later, and Trend Micro OfficeScan 10 and later.

Intended audience

Administrators who are assigned the task to monitor and manage Trend Micro OfficeScan events using EventTracker.
# Table of Contents

Abstract ........................................................................................................................................................ 1  
Scope ........................................................................................................................................................ 1  
Intended audience ................................................................................................................................... 1  
About Trend Micro OfficeScan .................................................................................................................... 3  
Overview ....................................................................................................................................................... 3  
Prerequisites ................................................................................................................................................ 3  
Configuration ............................................................................................................................................... 4  
Configure Syslog and Windows Event for Trend Micro Control Manager ................................................. 9  
EventTracker Agent configuration ........................................................................................................... 12  
EventTracker Knowledge Pack .................................................................................................................. 15  
Categories .............................................................................................................................................. 15  
Alerts ...................................................................................................................................................... 16  
Reports ................................................................................................................................................... 16  
Import Trend Micro OfficeScan knowledge pack into EventTracker ..................................................... 17  
Import Category........................................................................................................................................ 17  
Import Alerts............................................................................................................................................ 18  
Import Tokens.......................................................................................................................................... 20  
Import Flex Reports ............................................................................................................................... 21  
Verify Trend Micro OfficeScan knowledge pack in EventTracker .......................................................... 23  
Verify Trend Micro OfficeScan Categories ............................................................................................ 23  
Verify Trend Micro OfficeScan Alerts .................................................................................................... 24  
Verify Trend Micro OfficeScan Tokens .................................................................................................... 25  
Verify Trend Micro OfficeScan Reports ................................................................................................... 26  
Sample Report ........................................................................................................................................... 27
About Trend Micro OfficeScan

OfficeScan is a powerful endpoint security solution and is a combination of on premise and in-the-cloud security technologies to protect file servers, desktops, laptops, and virtualized desktops.

This application is a well supervised antivirus service providing enhanced support for antivirus / anti spyware / firewall protection for endpoint and mobile security.

Overview

In order to monitor Trend Micro OfficeScan 10.5 in EventTracker, you need to perform the configurations as below.

- Configure Trend Micro OfficeScan to log all client events.
- Configure Trend Micro OfficeScan to send all events as Windows event and Syslog to EventTracker System.

Prerequisites

Prior to configuring Trend Micro OfficeScan Server and EventTracker, ensure that you meet the following prerequisites:

- Trend Micro OfficeScan Server 10 is running on Microsoft Windows 2003 Enterprise Edition R2 and later with proper access permissions to make configuration changes.
- Install Trend Micro Control Manager 6 on Microsoft Windows 2003 and later.
- EventTracker Agent should be installed.
- Administrative access on EventTracker.
Configuration

Trend Micro OfficeScan logs are generated in Windows Event Log format on the Windows host machine configured for OfficeScan Server.

To configure Trend Micro OfficeScan:

1. Log in to the Trend Micro OfficeScan interface.

![Login page of Trend Micro OfficeScan Web Console displays.](image)

Login page of Trend Micro OfficeScan Web Console displays.
2. Enter valid **User name:** and **Password,** and then click the **Log On** button.

Summary Page of Trend Micro OfficeScan displays.
3. Click **Notifications** tab on the left hand side.

4. Expand the **Administrator Notifications** section.

5. Select **Standard Notifications**, and then select **NT Event Log** tab.

6. Select **Enable notification via NT Event Log** option.

7. Leave the Message box as default, and then click the **Save** button.
In Standard Notifications pane, Criteria tab displays by default.

8. Select **Send notifications when virus/malware is detected** and **Send notifications when spyware/grayware is detected** option.

9. Click the **Save** button.
EventTracker: Integrating Trend Micro OfficeScan 10

Figure 5
Configure Syslog and Windows Event for Trend Micro Control Manager

1. Log in to the Trend Micro Control Manager device.
2. Select Administration > Settings > Event Center Settings.
3. Click General Event Settings.

![Control Manager](image)

4. In SysLog Settings pane, enter EventTracker Server IP address*: and Server port*: as 514.
5. Click Save.

To configure events in the Event Center.

1. Select Administration > Event Center.
2. From the Event Category list, expand Alert.
3. Click Recipients for an alert.
Recipients page displays.

4. In Notification methods, select Syslog and Windows event log Notification option.
5. Click the **Save** button.

   The Edit Recipients Result window is displayed.

6. Click the **OK** button.
EventTracker Agent configuration

1. Select the **Start** button, select **All Programs**, and then select **Prism Microsystems**.

2. Select **EventTracker**, select **EventTracker Control Panel**, and then select **EventTracker Agent Configuration**.

3. Select **Event Filters** tab, and then select the **Filter Exception** button.

---

**Figure 10**

---

**EventTracker**

Filter Exception window displays.

4. Click the **New** button.

![Filter Exception window](image)

**Figure 11**

Event Details window displays.

5. In **Match in Source** box, enter *Trend Micro OfficeScan Server*.
6. Click the **OK** button.
EventTracker Knowledge Pack

Once Trend Micro OfficeScan events are enabled and Trend Micro OfficeScan events are received in EventTracker, Alerts and Reports can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker to support Trend Micro OfficeScan monitoring:

Categories

- **Trend Micro OfficeScan: Virus Detected**: This category based report provides information related to Virus Detected from Trend Micro OfficeScan.

- **Trend Micro OfficeScan: Virus Quarantine**: This category based report provides information related to Virus in Quarantine.

- **Trend Micro OfficeScan: Web Security Violation**: This category based report provides information related to Web Security Violation in Organization.

- **Trend Micro OfficeScan: Spyware Detected**: This category based report provides information related to Spyware Detected from Trend Micro OfficeScan.

- **Trend Micro OfficeScan: Administrator Password changed**: This category based report provides information related to Administrator Password changed in Trend Micro OfficeScan.

- **Trend Micro OfficeScan: Firewall policy added**: This category based report provides information related to Firewall policy added in Trend Micro OfficeScan.

- **Trend Micro OfficeScan: Firewall policy deleted**: This category based report provides information related to deleted Firewall policy from Trend Micro OfficeScan.

- **Trend Micro OfficeScan: Firewall policy modified**: This category based report provides information related to modified Firewall policy from Trend Micro OfficeScan.

- **Trend Micro OfficeScan: User account created**: This category based report provides information related to User account created in Trend Micro OfficeScan.

- **Trend Micro OfficeScan: User account deleted**: This category based report provides information related to User account deleted in Trend Micro OfficeScan.
EventTracker: Integrating Trend Micro OfficeScan 10

- **Trend Micro OfficeScan: User account modified:** This category based report provides information related to User account modified in Trend Micro OfficeScan.

- **Trend Micro OfficeScan: User Roles created:** This category based report provides information related to User Roles created in Trend Micro OfficeScan.

- **Trend Micro OfficeScan: User Roles Deleted:** This category based report provides information related to User Roles Deleted in Trend Micro OfficeScan.

**Alerts**

- **Trend Micro OfficeScan: Virus Detected:** This alert is generated when any virus are detected from Trend Micro OfficeScan.

- **Trend Micro OfficeScan: Virus Quarantine:** This alert is generated when any virus is unable to delete or move to Quarantine from Trend Micro OfficeScan.

- **Trend Micro OfficeScan: Spyware Detected:** This alert is generated when any Spyware are detected from Trend Micro OfficeScan.

- **Trend Micro OfficeScan: Web Security Violation:** This alert is generated when any user accesses blocked websites in Organization.

**Reports**

- **Trend Micro: User Authentication Success** - This report provides information related to user which authenticated with firewall successfully which includes user details and its role

- **Trend Micro: User Account Management** - This report provides information related with account creation, deletion and modification which include user by whom creation, deletion or modification happens and details of changes happen in accounts.

- **Trend Micro: Firewall Policy Management** - This report provides information related to changes happen in Firewall policy of Trend Micro officescan which includes User by whom changes happens and what changes happen (added, deleted or modified).
Import Trend Micro OfficeScan knowledge pack into EventTracker

1. Launch EventTracker Control Panel.
2. Double click Export Import Utility, and then click Import tab.
   Import Category/Alert/Tokens/ Flex Reports as given below.

Import Category

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

![Image of Export Import Utility window](Figure 13)
2. Locate All TREND MICRO OFFICESCAN group of Categories.iscat file, and then click the Open button.

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

   ![Import Success Message](Figure 14)

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

Import Alerts

1. Click Alerts option, and then click the browse button.
2. Locate All TREND MICRO OFFICESCAN group of Alerts.salt file, and then click the Open button.

3. To import alerts, click the Import button.

   EventTracker displays success message.

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

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

2. Locate **Trend Micro OfficeScan tokens.istoken** file, and then click the Open button.

3. To import tokens, click the **Import** button.
   EventTracker displays success message.
4. Click **OK**, and then click the **Close** button.

### Import Flex Reports

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

2. Locate **Trend Micro OfficeScan Flex Report.issch** file, and then click the **Open** button.
3. To import scheduled reports, click the **Import** button.

   EventTracker displays success message.

   ![Image](image.png)

   **Figure 20**

4. Click **OK**, and then click the **Close** button.
Verify Trend Micro OfficeScan knowledge pack in EventTracker

Verify Trend Micro OfficeScan Categories

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Categories.
3. In Category Tree to view imported categories, scroll down and expand Trend Micro OfficeScan group folder to view the imported categories.

Figure 21
Verify Trend Micro OfficeScan Alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Alerts.
3. In Search field, type 'Trend Micro', and then click the Go button.
   Alert Management page will display all the imported Trend Micro OfficeScan alerts.

   ![Alert Management Page](image)
   
   Figure 22

4. To activate the imported alerts, select the respective checkbox in the Active column.
   EventTracker displays message box.

   ![Message Box](image)
   
   Figure 23

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

You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.

Verify Trend Micro OfficeScan Tokens

1. Logon to **EventTracker Enterprise**.

2. Click the **Admin** menu, and then click **Parsing Rules**.

   The imported Trend Micro OfficeScan tokens are added in Token-Value Groups list. Please refer Figure 24.
Verify Trend Micro OfficeScan Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports menu, and then select Configuration.
3. In Reports Configuration pane, select Defined option.
   EventTracker displays Defined page.
4. In search box enter Trend Micro, and then click the Search button.
   EventTracker displays Flex reports of Trend Micro.

Figure 25
## Sample Report

### Trend Micro-Account Management Test

<table>
<thead>
<tr>
<th>Time</th>
<th>Computer</th>
<th>Account</th>
<th>User</th>
<th>Action</th>
<th>Role</th>
<th>Status</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>08/21/2015 10:26:04 AM</td>
<td>CONTOSO-TMOS</td>
<td>'joeb'</td>
<td>joeb</td>
<td>modifies</td>
<td>Administrator (Built-in)</td>
<td>Enabled</td>
<td>changed.</td>
</tr>
<tr>
<td>08/21/2015 10:26:04 AM</td>
<td>CONTOSO-TMOS</td>
<td>'joeb'</td>
<td>joeb</td>
<td>modifies</td>
<td>Administrator (Built-in)</td>
<td>Enabled</td>
<td>changed.</td>
</tr>
<tr>
<td>08/21/2015 10:26:08 AM</td>
<td>CONTOSO-TMOS</td>
<td>'David'</td>
<td>Mark</td>
<td>adds</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>08/21/2015 10:26:09 AM</td>
<td>CONTOSO-TMOS</td>
<td>'James'</td>
<td>Mark</td>
<td>adds</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>08/21/2015 10:26:09 AM</td>
<td>CONTOSO-TMOS</td>
<td>'James'</td>
<td>Mark</td>
<td>removes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>08/21/2015 10:26:09 AM</td>
<td>CONTOSO-TMOS</td>
<td>'Matt'</td>
<td>root</td>
<td>removes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>08/21/2015 10:26:09 AM</td>
<td>CONTOSO-TMOS</td>
<td>'Smith'</td>
<td>root</td>
<td>adds</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>08/21/2015 10:26:09 AM</td>
<td>CONTOSO-TMOS</td>
<td>'Smith'</td>
<td>root</td>
<td>adds</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>08/21/2015 10:26:09 AM</td>
<td>CONTOSO-TMOS</td>
<td>'David'</td>
<td>Mark</td>
<td>adds</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>08/21/2015 10:26:09 AM</td>
<td>CONTOSO-TMOS</td>
<td>'John'</td>
<td>Smith</td>
<td>adds</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Trend Micro-Authentication Success

<table>
<thead>
<tr>
<th>Time</th>
<th>Computer</th>
<th>User</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>08/13/2015 12:17:47 PM</td>
<td>CONTOSO-TMOS</td>
<td>root</td>
<td>Administrator (Built-in)</td>
</tr>
<tr>
<td>08/13/2015 12:17:47 PM</td>
<td>CONTOSO-TMOS</td>
<td>John</td>
<td>Guest User (Built-in)</td>
</tr>
<tr>
<td>08/13/2015 12:17:47 PM</td>
<td>CONTOSO-TMOS</td>
<td>Smith</td>
<td>Trend Power User (Built-in)</td>
</tr>
</tbody>
</table>

---

**Figure 26**

**Figure 27**