Integrate TeamViewer
Abstract

TeamViewer is an intuitive, fast and secure application for remote control and meetings. This guide provides instructions to configure TeamViewer log to EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 7.X and later, and TeamViewer 10 or later.

Audience

Administrators who are responsible for Monitoring TeamViewer using EventTracker Manager.
# Table of Contents

Abstract .............................................................................................................................................. 1
Scope .................................................................................................................................................... 1
Audience .............................................................................................................................................. 1

Introduction ........................................................................................................................................ 4

Integration employing TeamViewer Management Console .............................................................. 4
Prerequisites ....................................................................................................................................... 4

Create access token from TeamViewer Management Console ......................................................... 5
Add access token to PowerShell script ............................................................................................... 9
Schedule PowerShell Script .............................................................................................................. 10

EventTracker DLA configuration ....................................................................................................... 13

Import EventTracker KP for TeamViewer ......................................................................................... 19
Parsing Rules .................................................................................................................................... 20
Flex Reports ..................................................................................................................................... 22
Knowledge Object ............................................................................................................................ 24

Verify EventTracker KP for TeamViewer .......................................................................................... 26
Parsing Rules .................................................................................................................................... 26
Flex Reports ..................................................................................................................................... 27
Knowledge Object ............................................................................................................................ 28

EventTracker Knowledge Pack for TeamViewer ............................................................................... 29
Report .............................................................................................................................................. 29
Knowledge Object ............................................................................................................................ 30

Integration employing TeamViewer native logging ........................................................................ 30
Prerequisites .................................................................................................................................... 30

Locate TeamViewer Log .................................................................................................................. 30
EventTracker LFM configuration ....................................................................................................... 31

Import EventTracker KP for TeamViewer ......................................................................................... 34
Token Templates ................................................................................................................................ 34
Flex Report ....................................................................................................................................... 37
Knowledge Object ............................................................................................................................ 39
Integrate TeamViewer

Verify EventTracker KP for TeamViewer .............................................................. 41
Token Template ........................................................................................................ 41
Flex Report .................................................................................................................. 42
Knowledge Object ....................................................................................................... 43
EventTracker Knowledge Pack for TeamViewer ...................................................... 45
Report .......................................................................................................................... 46
Knowledge Object ....................................................................................................... 46
Create Flex Dashboards in EventTracker ............................................................... 46
Schedule Reports ......................................................................................................... 46
Create Dashlets ............................................................................................................. 49
Sample Flex Dashboards ............................................................................................. 52
Introduction

TeamViewer is the popular Internet-based remote administration software. It provides an All-In-One solution to features such as remote control, desktop sharing, file transferring, messaging, meetings etc.

EventTracker utilizes TeamViewer’s reporting API to fetch connection reports from TeamViewer Management Console. For standalone installations, incoming connections are monitored on critical systems for suspicious activities using TeamViewer’s native logging.

Please select you preferred integration from above mentioned choices.

Integration employing TeamViewer Management Console

Prerequisites

- **EventTracker v7.x or later** must be installed.
- **Windows PowerShell 3.0 and later** must be installed.
- PowerShell script execution must be enabled and execution policy must be set to **bypass or unrestricted**.
- Administrator access to **TeamViewer Management Console**.
Create access token from TeamViewer Management Console

1. Login to your TeamViewer account at the TeamViewer Management Console website.

2. Select Edit Profile from profile drop-down in the top right of the website.
3. In Profile settings page, navigate to **Apps->Create script token**.
4. Enter **TeamViewerReporting** as the app name. Select **View connection entries** from **Connection reporting** drop-down. Other options can be configured as per user’s preference.

5. Click **Save**.
6. Please write down the **Token** generated.

7. Click **OK** and **Save** to apply changes.
Add access token to PowerShell script

1. Request TeamViewer script pack from EventTracker Support.
2. Download and extract the files provided to `<%EventTracker Installation Path%>\Prism Microsystems\EventTracker\ScheduledActionScripts`.

![Directory Structure](image)

Figure 7

3. Edit `ExportConnectionCSV.ps1` and add earlier generated API token as shown.
4. Save the script.

Schedule PowerShell Script


   ![Task Scheduler](image)

2. In Task scheduler windows, click on Import Task in Actions pane.
3. Browse and select the xml file named TeamViewerReporting.xml from earlier mentioned extraction location.
4. Double-click to edit the imported task named **TeamViewerReporting**.

5. Click **General** tab and change the user account settings in **Security options** section. Please ensure concerned user has the admin privileges.
6. Click **Triggers** tab and select edit. Please select an appropriate time for script execution.
7. Click **Actions** tab and select edit. Please edit expression provided in **Add arguments** as shown below.

```
-file "C:\Program Files (x86)\Prism Microsystems\EventTracker\ScheduledActionScripts\TeamViewerReporting\ExportConnectionsCSV.ps1"
```

- **Script Location**

8. Click **OK** to apply the changes.

9. When the script is executed, report named **ExportConnections.csv** will be generated in CSV format at the script location in **TVReportoutput** folder.

**EventTracker DLA configuration**

1. Open **EventTracker** in browser and logon.
2. In EventTracker Enterprise, select **Manager** from **Admin** drop-down.

3. Select **Direct Log Archiver/Netflow Receiver** tab and choose **Direct log file archiving from external sources** checkbox.
4. Click the **Add** button.
5. Compose Direct Archiver Configuration as suggested below:

- Select **Others** from **Type** dropdown.
- Type **csv** as **Logfile Extension**.
- Type an appropriate **Configuration Name**.
- Click the **Browse** button and select path of TeamViewer log folder (TVReportoutput).
- Select **Single Line** dialog box.
- Select **Comma - [Fields containing comma are wrapped in double quotes]** field separator dropdown.
- Type **1** as **Starting Line Offset**.
- Click the **Configure** button.
6. Compose Log File Configuration as suggested below:
   - Type TeamViewer as Log Source name.
   - Select appropriate Computer Name, Computer IP and System Type.
   - Select Formatted Description dialog box and choose Custom Log File Format from Log File Format drop-down.
   - Click Add button, type below mentioned Message Fields in following sequence:
     - Session ID
     - User ID
     - User Name
     - Device ID
- Device Name
- Group ID
- Group Name
- Start Time
- End Time
- Session Fee
- Fee Currency
- Session Billed
- Session Info

- Under **Event Date and Time Fields**, select 1 from **No of Fields** drop-down and select **Start Date** from **Date Field** drop-down.
- Under **Select Date Time Format Fields**, select **YYYY-MM-DD hh:mm** from **Format Value** drop-down.
- Scroll down and click **Save & Close** button.
7. On Manager Configuration page, click **Save** button to apply changes.

**Import EventTracker KP for TeamViewer**

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.
3. Import knowledge pack items in the following sequence:
   - Parsing Rules
   - Flex Reports

Parsing Rules

1. Select Import tab, choose Token value from Options dialog box.

2. Click the browse button in Location section.
3. Locate the TeamViewer Parsing Rules.istoken file, and then click the Open button.

4. To import tokens, click the Import button.

5. Click OK, and then click the Close button.
Flex Reports

1. Select **Import** tab, choose **Reports** from **Options** dialog box.

![Figure 23](image)

2. Select Legacy (*.issch) from Location dialog box, click the ‘**browse**’ button.
3. Locate TeamViewer Reports.issch file, and then click the Open button.
4. To import scheduled reports from selected file, click the **Import** button.

5. Click **OK** and **Close**.

**Knowledge Object**

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu and then click the **Knowledge Objects**.
3. Click the **Import** button.

4. Click browse and locate the file named **TeamViewer Knowledge Objects.etko**.
5. Click on **UPLOAD** button.

![Figure 29](image)

6. Select associated knowledge object and click on **Overwrite** button.

![Figure 30](image)

7. Click **OK**.

**Verify EventTracker KP for TeamViewer**

**Parsing Rules**

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Parsing rule**.
3. Scroll down and select **TeamViewer** from **Groups**. Imported Token-Values are shown in right pane.
Flex Reports

1. Logon to EventTracker Enterprise.

2. Navigate to Reports->Configuration.


5. **TeamViewer-Connection details** report is shown in the right pane.

**Knowledge Object**

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu and then click the **Knowledge Objects**.

![Image of TeamViewer-Connection details report](image-url)

![Image of EventTracker Enterprise Admin menu](image-url)
3. Scroll down and select **TeamViewer** from Groups section. Imported knowledge objects are shown in the right pane.

![Knowledge Objects](image)

**Figure 35**

**EventTracker Knowledge Pack for TeamViewer**

Once logs are received in to EventTracker, Reports can be configured into EventTracker.

The following Knowledge Pack are available in EventTracker to support TeamViewer monitoring:

**Report**

- **TeamViewer-Connection Details** – This report provides information related to users accessing remote systems through TeamViewer.

**Sample Report**

![Sample Report](image)

**Figure 36**
Integrate TeamViewer

Sample Log

<table>
<thead>
<tr>
<th>LOG TIME</th>
<th>EVENT ID</th>
<th>SITE / COMPUTER</th>
<th>USER</th>
<th>DOMAIN</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/19/2017 11:44:07 AM</td>
<td>12345</td>
<td>PHP, MySQL</td>
<td>SYSTEM</td>
<td>NT AUTHORITY</td>
<td>TeamViewer</td>
</tr>
</tbody>
</table>

Event Type: Information
Log Type: System
Category Id: 2

Description:
Session ID: 07a8b8c1-7c84-459b-9d32-1f788bc05a82
User ID: u65482389
User Name: Rajeshwori Raopatwad
Device ID: 871371966
Device Name: C:\Program Files\TeamViewer\TeamViewer.exe
Start Date: 2017-01-19 11:44:07
End Date: 2017-01-19 11:48:28
Session Fee: 0.00
Fee Currency: None
Session Billed: Yes
Session Info: Scheduled Monitoring.

Figure 37

Knowledge Object

- **TeamViewer Connections** – This KO aids an administrator to analyze and visualize all the TeamViewer remote connection related logs.

Integration employing TeamViewer native logging

Prerequisites

- **EventTracker v7.x or later** must be installed.
- Administrator access to TeamViewer installation path.

Locate TeamViewer Log

1. Logon to the workstation where TeamViewer is installed.
2. Navigate to TeamViewer installation directory. Default installation paths are given below:
   - **32-Bit (x86) Systems**: C:\Program Files\TeamViewer\TeamViewer.exe
   - **64-Bit (x64) Systems**: C:\Program Files (x86)\TeamViewer\TeamViewer.exe
3. Locate file named **Connections_incoming.txt**.
4. Sample Connections_incoming.txt file is shown below.

```
252398529  SOC-23  23-01-2017 10:00:01  23-01-2017 10:00:56  johnnyen  RemoteControl  {8984923-3318-4C4C-8588-F720C7EAB4B0}
```

**EventTracker LFM configuration**

1. Logon to the workstation where TeamViewer is installed.
2. Open **EventTracker Agent Configuration**, select **LogFile Monitor** tab and enable the same.
Integrate TeamViewer

3. Select Add File Name.

![Figure 40]

4. Choose TEXTLINE from Select Log File Type dropdown and select Get All Existing Log Files.

![Figure 41]

5. Click and browse to C:\Program Files\TeamViewer\Connections_incoming.txt.
6. Click **OK** and proceed.

7. Select **Text** from **Select Field Name** dropdown. Use “*” as the corresponding **Search String**.
8. Select **Current DateTime** checkbox and click **OK**.
9. Click **Save** to apply.

### Import EventTracker KP for TeamViewer

Import knowledge pack items in the following sequence:

- Templates
- Flex Reports

### Token Templates

1. Logon to EventTracker manager with appropriate credentials.
2. Click the **Admin** menu, and then click **Parsing rule**.

3. Select **Template** tab, and then click on ‘**Import**’ option.
4. Click on **Browse** button.

5. Locate **TeamViewer Token Template.ettld** file, and then click the **Open** button.

6. Now select the check box and then click on **Import** option.
7. Click on OK button.

**Flex Report**

1. Launch **EventTracker Control Panel**.

2. Double click **Export Import Utility**.
3. Select **Import** tab, choose **Reports** from **Options** dialog box.
4. Select Legacy (*.issch) from Location dialog box, click the ‘browse’ button.
5. Locate TeamViewer Connection Report.issch file, and then click the Open button.

![Figure 53](image)

6. To import scheduled reports from selected file, click the Import button.

![Figure 54](image)

7. Click OK and Close.

Knowledge Object

1. Logon to EventTracker Enterprise.
2. Click the Admin menu and then click the Knowledge Objects.
3. Click the **Import** button.

4. Click Browse and locate the file named **TeamViewer Knowledge Objects.etko**.
5. Click on **UPLOAD** button.

![Figure 57](image)

6. Select associated knowledge object and click on **Overwrite** button.

![Figure 58](image)

7. Click **OK**.

**Verify EventTracker KP for TeamViewer**

**Token Template**

1. Logon to **EventTracker Enterprise** web interface.

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

1. Logon to EventTracker Enterprise.

2. Navigate to Reports->Configuration.


5. **TeamViewer-Incoming connection details** report is shown in the right pane.

**Knowledge Object**

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu and then click the **Knowledge Objects**.
3. Click the **Import** button.

4. Click Browse and locate the file named **TeamViewer Knowledge Objects. etko**.
5. Click on **UPLOAD** button.

![Figure 64](image)

6. Select associated knowledge object and click on **Overwrite** button.

![Figure 65](image)

7. Click **OK**.

**EventTracker Knowledge Pack for TeamViewer**

Once logs are received in to EventTracker, Report can be configured into EventTracker.

The following Knowledge Pack are available in EventTracker to support TeamViewer monitoring:
Report

- **TeamViewer-Incoming connection details** – This report provides information related to remote users accessing monitored system through TeamViewer.

**Sample Report**

<table>
<thead>
<tr>
<th>Session Start Time</th>
<th>Session End Time</th>
<th>Source Device Name/ID</th>
<th>Source User Name</th>
<th>Destination User Name</th>
<th>Computer/Session Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>23-01-2017 12:00:00</td>
<td>23-01-2017 11:41:41</td>
<td>Support-05 252384574</td>
<td>johndoe</td>
<td>Test-SVR-40</td>
<td>RemoteControl</td>
</tr>
</tbody>
</table>

Sample Log

[Figure 66]

**Knowledge Object**

- **TeamViewer Incoming Connections** – This KO aids an administrator to analyze and visualize all the TeamViewer incoming connection related logs.

Create Flex Dashboards in EventTracker

**NOTE:** To configure the flex dashboards, schedule and generate the reports. Flex dashboard feature is available from EventTracker Enterprise v8.0.

**Schedule Reports**

1. Open EventTracker in browser and logon.
2. Navigate to **Reports>Configuration**.

3. Select **TeamViewer** in report groups. Check **Defined** dialog box.

4. Click on ‘schedule’ to plan a report for later execution.

5. Click Next button to proceed.

6. In review page, check Persist data in EventVault Explorer option.
7. In next page, check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.
8. Proceed to next step and click Schedule button.

9. Wait till the reports get generated.

Create Dashlets

1. Open EventTracker Enterprise in browser and logon.

![Figure 72]

2. Navigate to Dashboard>Flex.

![Figure 73]

10. Fill suitable title and description and click Save button.

11. Click 🛠️ to configure a new flex dashlet. Widget configuration pane is shown.
12. Locate earlier scheduled report in Data Source dropdown.
13. Select Chart Type from dropdown.
14. Select extent of data to be displayed in Duration dropdown.
15. Select computation type in Value Field Setting dropdown.
16. Select evaluation duration in As Of dropdown.
17. Select comparable values in X Axis with suitable label.
18. Select numeric values in Y Axis with suitable label.
19. Select comparable sequence in Legend.
20. Click Test button to evaluate. Evaluated chart is shown.
21. If satisfied, click **Configure** button.

22. Click ‘customize’ to locate and choose created dashlet.

23. Click **+** to add dashlet to earlier created dashboard.
Sample Flex Dashboards

1. **Widget Title:** TeamViewer Remote Connections  
   **Data Source:** TeamViewer-Connection details  
   **Chart Type:** Donut  
   **Axis Labels [X-AXIS]:** Destination Device Name  
   **Legend [SERIES]:** Source User Group
   
   ![TeamViewer Remote Connections](image1)

   **Figure 77**

2. **Widget Title:** TeamViewer Incoming Connections  
   **Data Source:** TeamViewer-Incoming connection details  
   **Chart Type:** Donut  
   **Axis Labels [X-AXIS]:** Source Device Name  
   **Legend [SERIES]:** Session Type
   
   ![TeamViewer Incoming Connections](image2)

   **Figure 78**