Integration Guide

Integrate TeamViewer with EventTracker

Publication Date:

November 19, 2021

Abstract

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

Scope

The configuration details in this guide are consistent with **EventTracker** version 9.2X and later, and **TeamViewer 10 or later**.

Audience

Administrators who are responsible for monitoring TeamViewer using EventTracker.

Table of Contents

1. Overview

TeamViewer is a 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 the TeamViewer Management Console. For standalone installations, incoming connections are monitored on critical systems for suspicious activities using TeamViewer's native logging.

Please select your preferred integration from the above-mentioned choices.

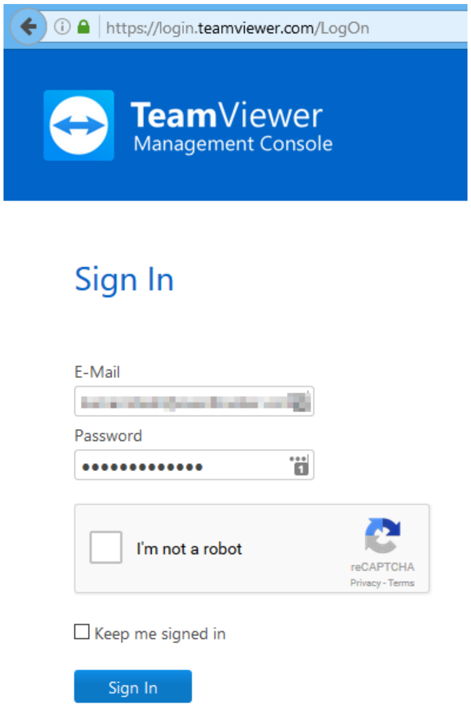
2. Prerequisites

- **EventTracker** v9.2x or later must be installed.
- **Windows PowerShell** 5.0 and later must be installed.
- PowerShell script execution must be enabled, and execution policy must be set to bypass or unrestrict.
- Administrator access to the TeamViewer Management Console.

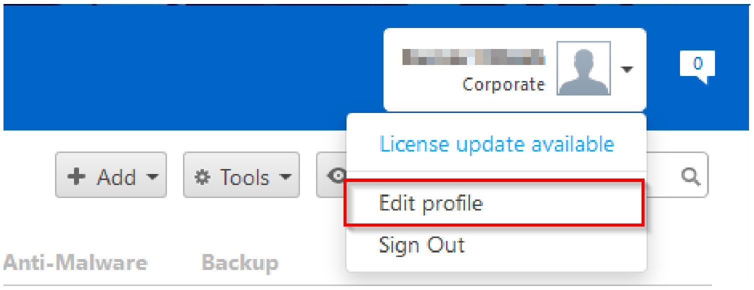
3. Configuring TeamViewer to send logs to EventTracker

This use case describes example steps to create an access token for the API integration with EventTracker.

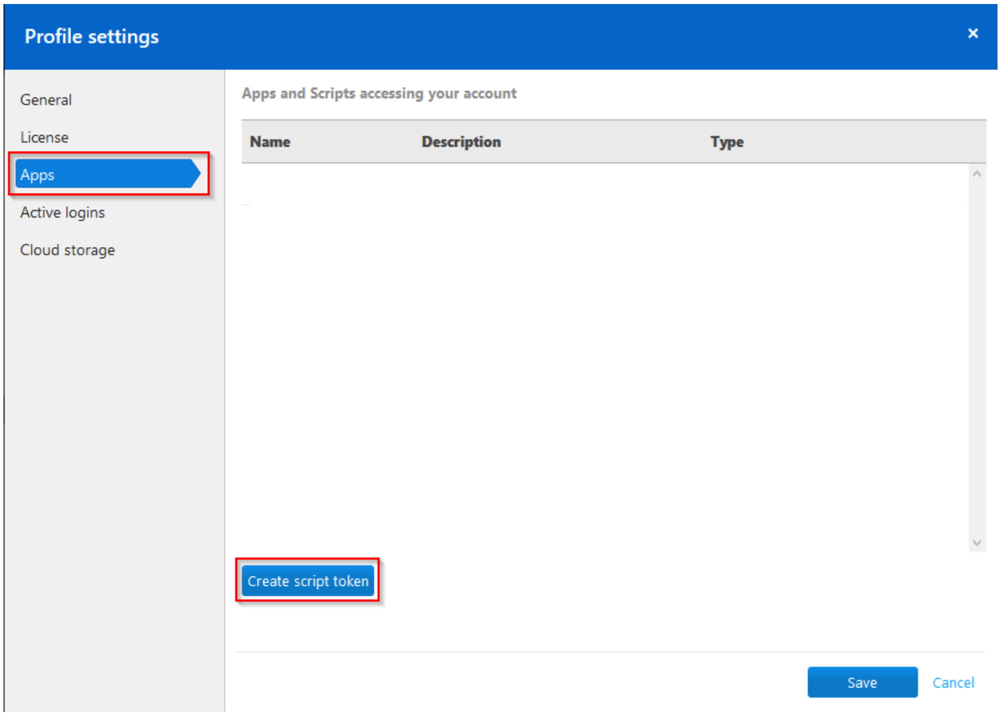
3.1 Create access token from TeamViewer Management Console



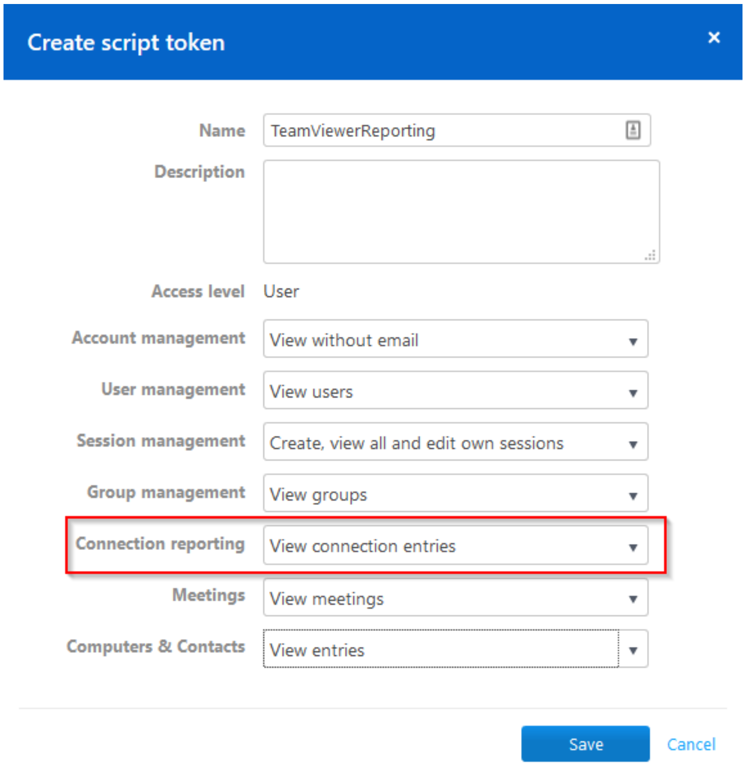
1. Log in to your TeamViewer account on the TeamViewer Management Console website.



2. Select **Edit Profile** from the **Profile** drop-down in the top right of the website.



3. In the Profile settings page, navigate to **Apps >> Create script token**.



Create script token

Name: TeamViewerReporting

Description:

Access level: User

Account management: View without email

User management: View users

Session management: Create, view all and edit own sessions

Group management: View groups

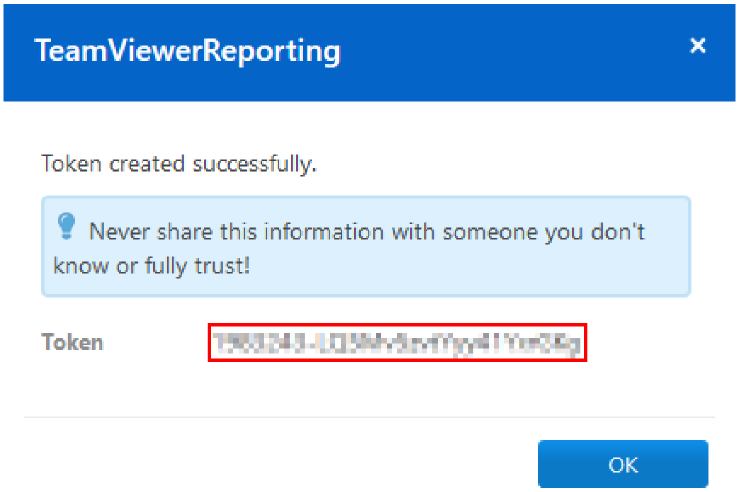
Connection reporting: View connection entries

Meetings: View meetings

Computers & Contacts: View entries

4. Enter **TeamViewerReporting** as the app name. Select **View connection entries** from the **Connection reporting** drop-down. Other options can be configured as per the user's preference.

5. Click **Save**.



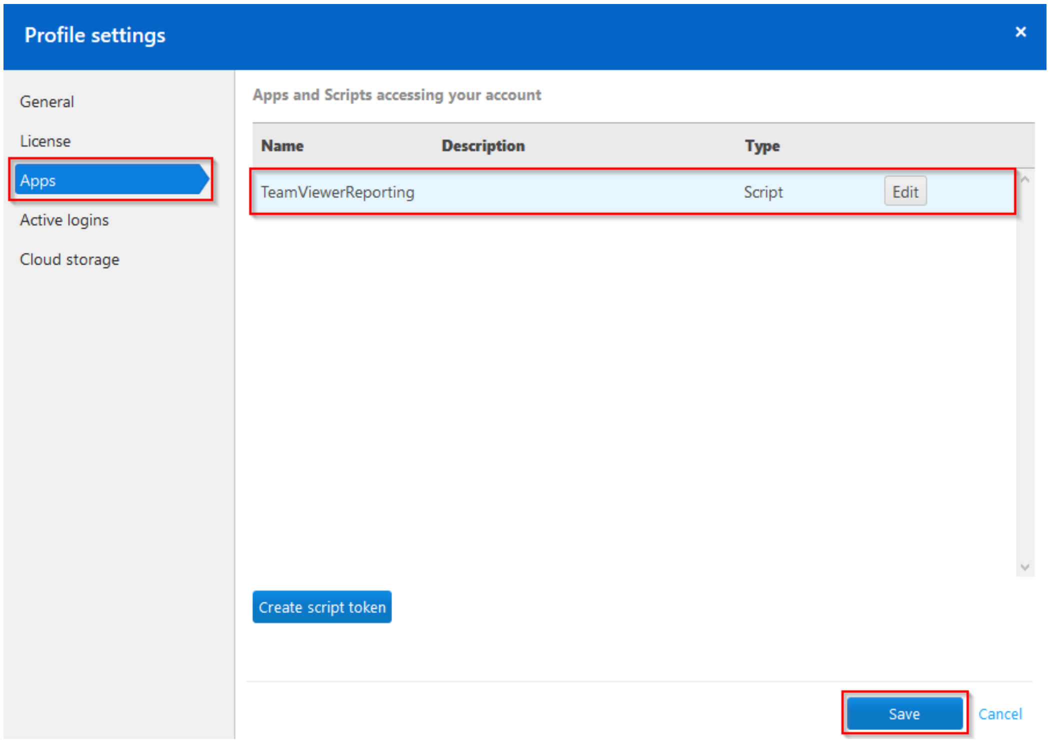
TeamViewerReporting

Token created successfully.

Never share this information with someone you don't know or fully trust!

Token: [redacted]

6. Please write down the **Token** generated for future use.

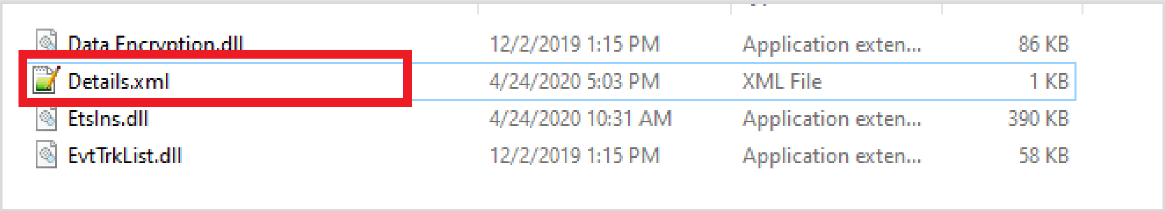


Name	Description	Type	
TeamViewerReporting		Script	Edit

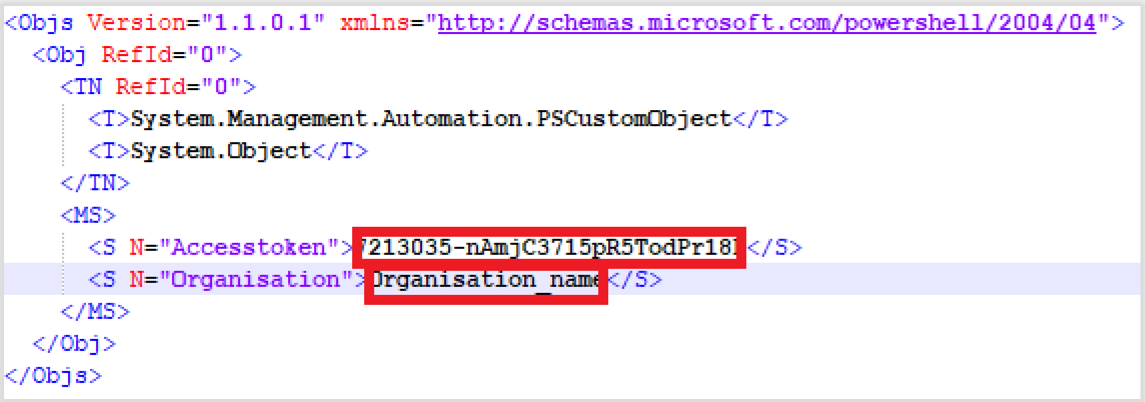
7. Click **OK** and **Save** to apply changes.

3.2 TeamViewer Logfetch

1. Please contact the EventTracker support team for the Integrator files.
2. Extract the files and navigate to the TeamViewer Integrator support folder location.
   Example: Folder_location\KP-TeamViewer\Integrator\Support
3. Open the **Details.xml** file for entering the token and organization name.

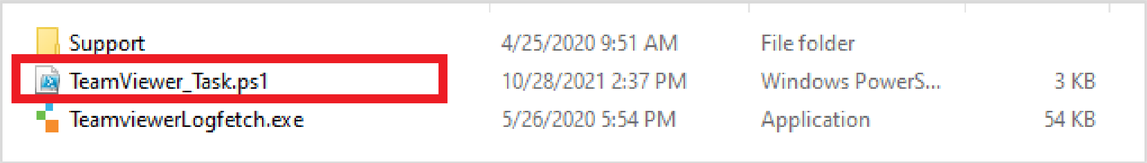


Data Encryption.dll	12/2/2019 1:15 PM	Application exten...	86 KB
Details.xml	4/24/2020 5:03 PM	XML File	1 KB
EtsIns.dll	4/24/2020 10:31 AM	Application exten...	390 KB
EvtTrkList.dll	12/2/2019 1:15 PM	Application exten...	58 KB



```
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04">
  <Obj RefId="0">
    <TN RefId="0">
      <T>System.Management.Automation.PSCustomObject</T>
      <T>System.Object</T>
    </TN>
    <MS>
      <S N="Accesstoken">7213035-nAmjC3715pR5TodPr18I</S>
      <S N="Organisation">Organisation_name</S>
    </MS>
  </Obj>
</Objs>
```

4. Run the **TeamViewer_Task.ps1** file in the Windows Powershell with admin privileges. It will create a task in the Task Scheduler.



Support	4/25/2020 9:51 AM	File folder	
TeamViewer_Task.ps1	10/28/2021 2:37 PM	Windows PowerS...	3 KB
TeamviewerLogfetch.exe	5/26/2020 5:54 PM	Application	54 KB

3.3 EventTracker Knowledge Pack for TeamViewer

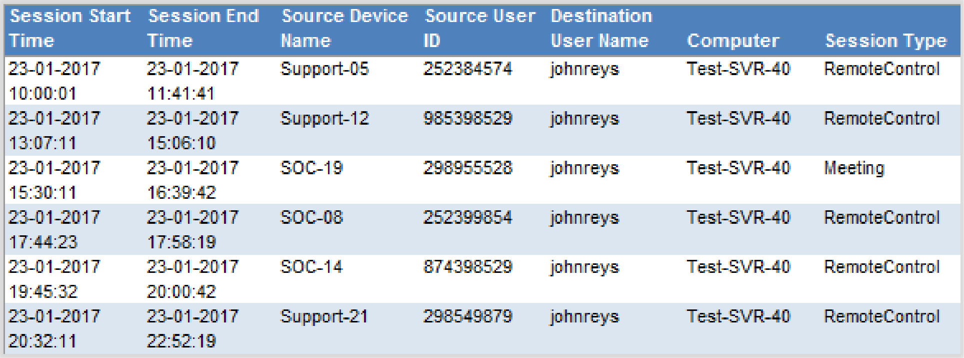
After the logs are received into EventTracker, the Report can be configured into EventTracker.

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

3.3.1 Reports

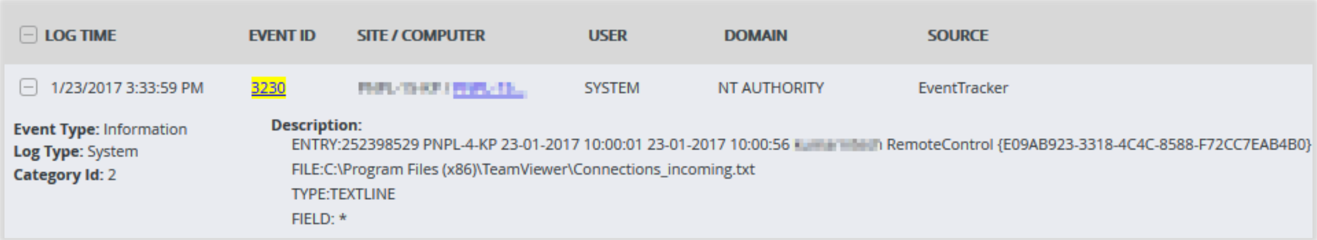
- **TeamViewer-Incoming connection details –** This report provides information related to the remote users accessing the monitored system through TeamViewer.

Sample Report



Session Start Time	Session End Time	Source Device Name	Source User ID	Destination User Name	Computer	Session Type
23-01-2017 10:00:01	23-01-2017 11:41:41	Support-05	252384574	johnreys	Test-SVR-40	RemoteControl
23-01-2017 13:07:11	23-01-2017 15:06:10	Support-12	985398529	johnreys	Test-SVR-40	RemoteControl
23-01-2017 15:30:11	23-01-2017 16:39:42	SOC-19	298955528	johnreys	Test-SVR-40	Meeting
23-01-2017 17:44:23	23-01-2017 17:58:19	SOC-08	252399854	johnreys	Test-SVR-40	RemoteControl
23-01-2017 19:45:32	23-01-2017 20:00:42	SOC-14	874398529	johnreys	Test-SVR-40	RemoteControl
23-01-2017 20:32:11	23-01-2017 22:52:19	Support-21	298549879	johnreys	Test-SVR-40	RemoteControl

Sample Log



LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
1/23/2017 3:33:59 PM	3230	[redacted]	SYSTEM	NT AUTHORITY	EventTracker

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

Description:

```
ENTRY:252398529 PNPL-4-KP 23-01-2017 10:00:01 23-01-2017 10:00:56 [redacted] RemoteControl {E09AB923-3318-4C4C-8588-F72CC7EAB4B0}
FILE:C:\Program Files (x86)\TeamViewer\Connections_incoming.txt
TYPE:TEXTLINE
FIELD: *
```

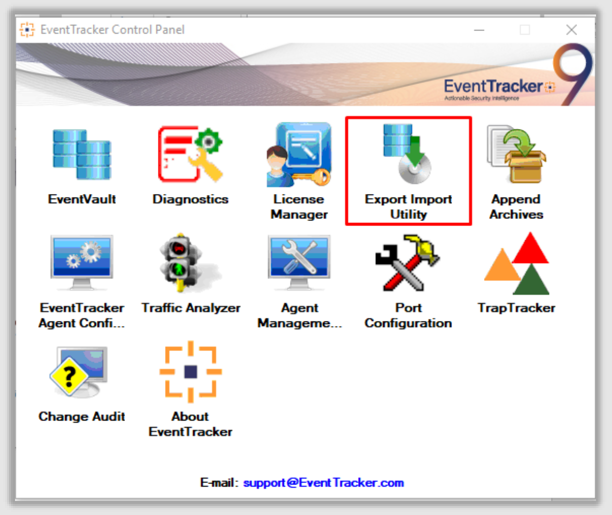
4. Importing TeamViewer Knowledge Pack into EventTracker

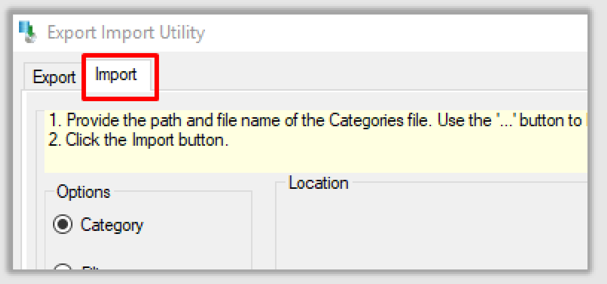
NOTE: Import the Knowledge Pack items in the following sequence:

- Templates
- Flex Reports
- Knowledge Objects

1. Launch the **EventTracker Control Panel**.

2. Double click the **Export-Import Utility**.





1. Provide the path and file name of the Categories file. Use the '...' button to
2. Click the Import button.

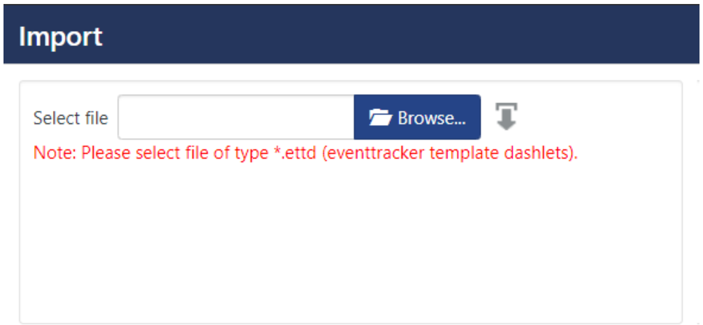
3. Click the **Import** tab.

4.1 Token Templates

1. Click the **Admin** menu, and then click the **Parsing rule**.

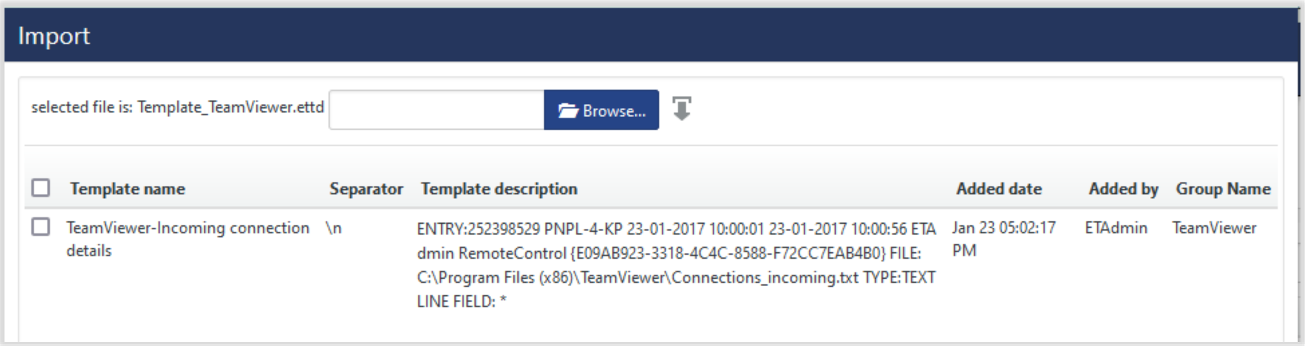
2. Select the **Template** tab, and then click the ⤓ **Import** option.

3. Click the **Browse** button.



Note: Please select file of type *.ettd (eventtracker template dashlets).

4. Locate the **Template_TeamViewer.ettd** file, and then click the **Open** button.

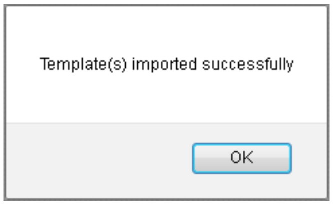


Import

selected file is: Template_TeamViewer.ettd

□	Template name	Separator	Template description	Added date	Added by	Group Name
□	TeamViewer-Incoming connection details	\n	ENTRY:252398529 PNPL-4-KP 23-01-2017 10:00:01 23-01-2017 10:00:56 ETA dmin RemoteControl {E09AB923-3318-4C4C-8588-F72CC7EAB4B0} FILE: C:\Program Files (x86)\TeamViewer\Connections_incoming.txt TYPE:TEXT LINE FIELD: *	Jan 23 05:02:17 PM	ETAdmin	TeamViewer

5. Select the check box and then click the **Import** option.
   EventTracker displays a success message.

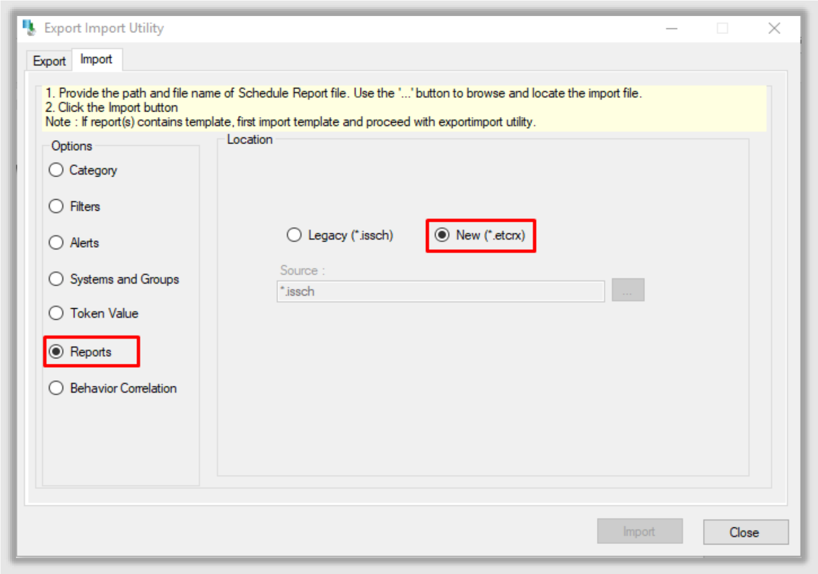


Template(s) imported successfully

6. Click the **OK** button.

4.2 Reports

1. In the EventTracker Control Panel, select the **Export/ Import utility** and select the **Import tab**. Then, click the **Reports** option, and choose **New (*.etcrx)**.



Export Import Utility

1. Provide the path and file name of Schedule Report file. Use the '...' button to browse and locate the import file.
2. Click the Import button
Note : If report(s) contains template, first import template and proceed with exportimport utility.

Options

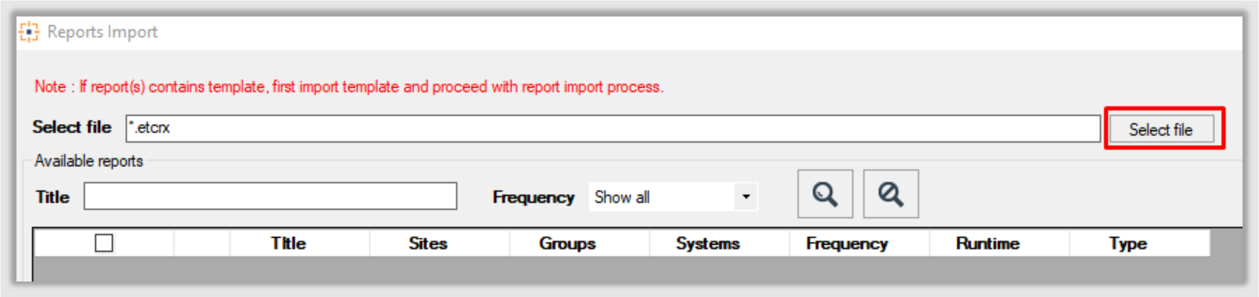
○ Category
○ Filters
○ Alerts
○ Systems and Groups
○ Token Value
● Reports
○ Behavior Correlation

Location

○ Legacy (*.issch) ● New (*.etcrx)

Source : *.issch

2. A new pop-up window appears. Click the **Select File** button and navigate to the file path with a file having the extension "**.etcrx", e.g., Reports_ TeamViewer.etcrx.**



Reports Import

Note : If report(s) contains template, first import template and proceed with report import process.

Select file: *.etcrx

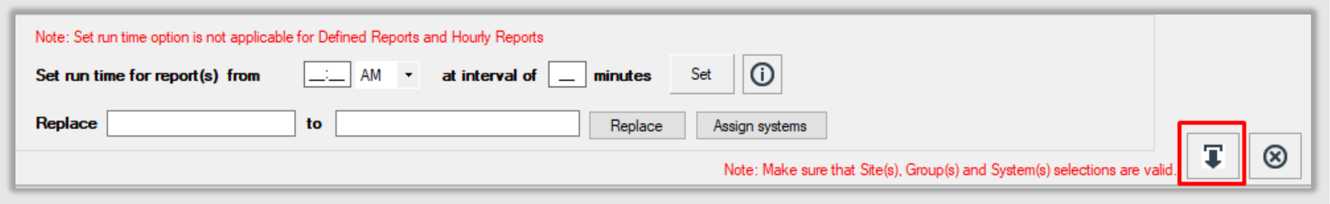
Available reports

Title:

Frequency: Show all

□	Title	Sites	Groups	Systems	Frequency	Runtime	Type

3. Wait while the reports populate in the below tables. Now, select all the relevant reports and then click the **Import** ⤓ button.



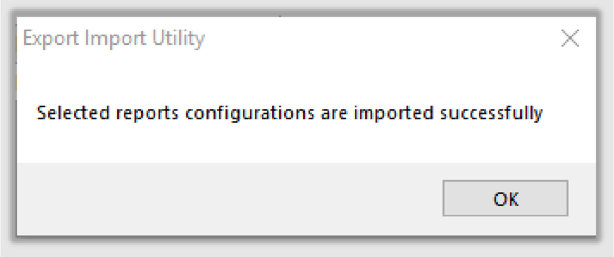
Note: Set run time option is not applicable for Defined Reports and Hourly Reports

Set run time for report(s) from __:__ AM at interval of __ minutes

Replace ______ to ______

Note: Make sure that Site(s), Group(s) and System(s) selections are valid.

EventTracker displays a success message.

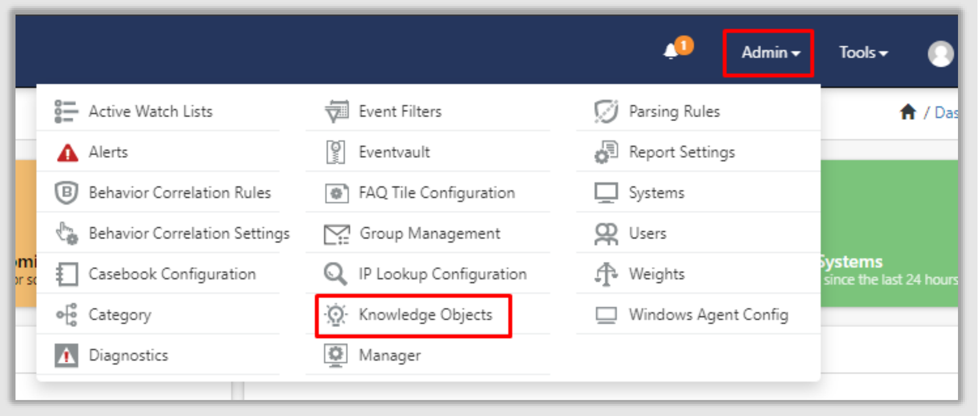


Export Import Utility

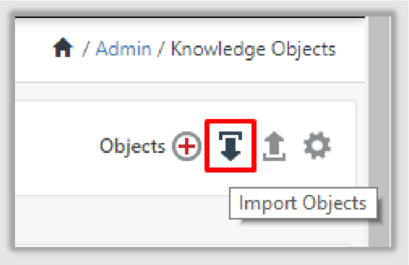
Selected reports configurations are imported successfully

4.3 Knowledge Objects

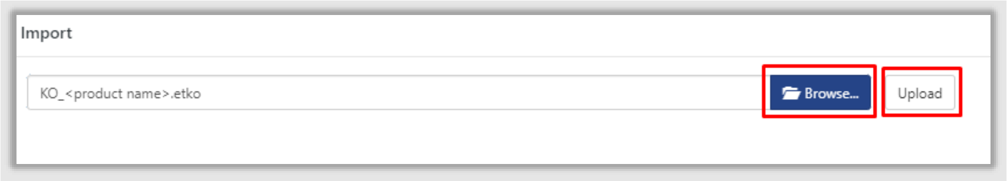
1. Click **Knowledge Objects** under the **Admin** option on the EventTracker page.



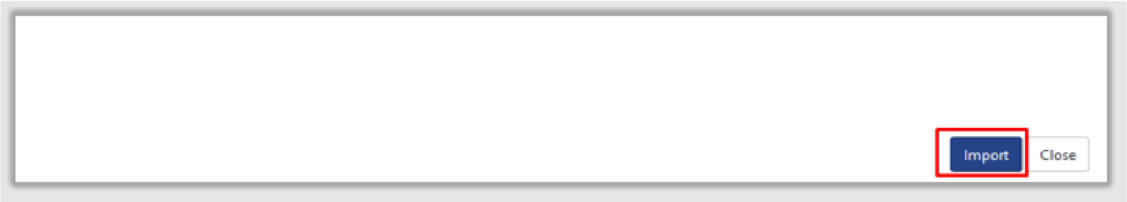
2. Click the **Import Objects** icon.



3. A pop-up box appears, click **Browse** and navigate to the Knowledge Packs folder (type **%et_install_path%\Knowledge Packs** in the navigation bar) with the extension **".etko", e.g., KO_TeamViewer.etko,** and then click **Upload**.



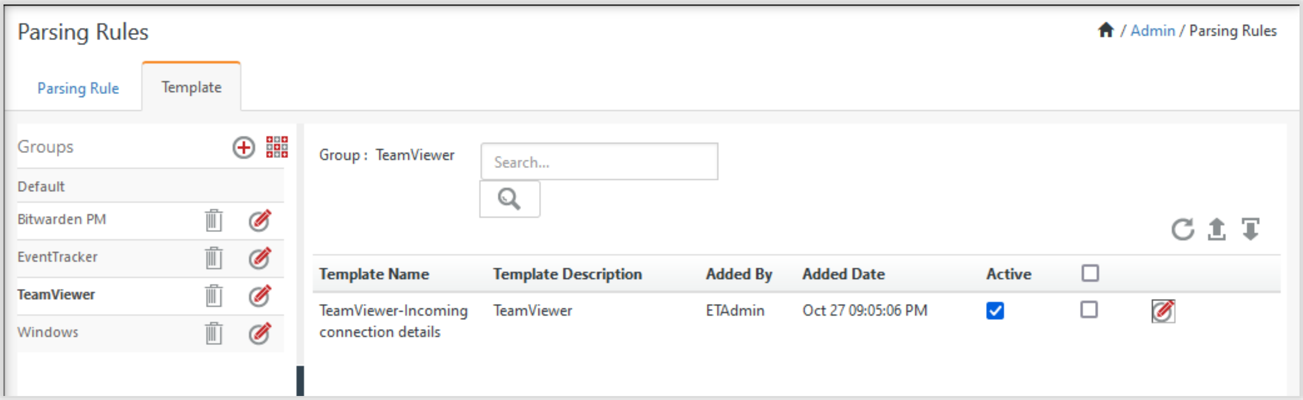
4. A list of available Knowledge Objects will appear. Select the relevant files and click the **Import** button.



5. Verifying TeamViewer Knowledge Pack in the EventTracker

5.1 Token Templates

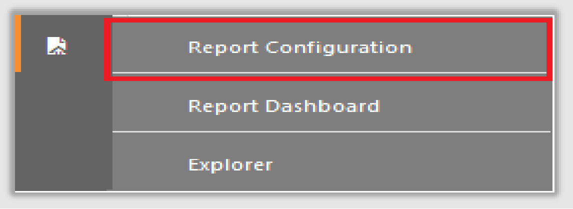
1. Log on to the **EventTracker** web interface.
2. Click the **Admin** menu, and then click **Parsing Rules** and click **Template**.
3. Click the **TeamViewer** group option.



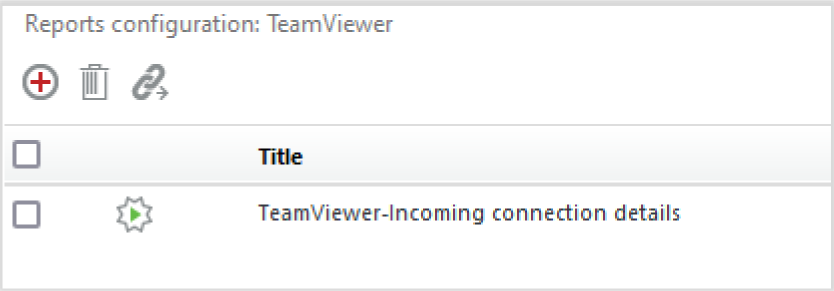
Template Name	Template Description	Added By	Added Date	Active	□	
TeamViewer-Incoming connection details	TeamViewer	ETAdmin	Oct 27 09:05:06 PM	☑	□	

5.2 Reports

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



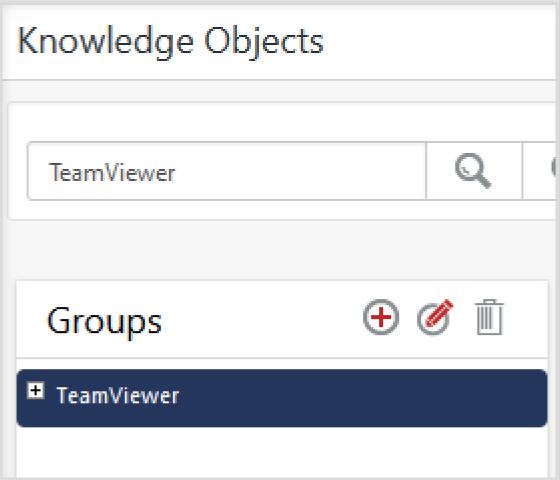
2. In the **Reports Configuration** pane, select the **Defined** option.
3. Click the **TeamViewer** group folder to view the imported reports.



□		Title
□		TeamViewer-Incoming connection details

5.3 Knowledge Objects

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Knowledge Objects.**
2. In the **Knowledge Object** tree, expand the **TeamViewer** group folder to view the imported Knowledge Objects.



Knowledge Objects

TeamViewer

Groups

⊞ TeamViewer

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's EventTracker cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #23 among MSSP Alert's 2021 Top 250 MSSPs.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)
EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3)
EventTracker Essentials SOC: 877-333-1433 (Option 4)
EventTracker Software Support: 877-333-1433 (Option 5)
https://www.netsurion.com/eventtracker-support