Integrating Microsoft Forefront Client Security

EventTracker v7.x

Publication Date: Nov 27, 2014

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Abstract

This guide provides instructions to configure Microsoft Forefront Client Security to send events to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 7.X and later, and Microsoft Forefront Client Security 2010.

Audience

Microsoft Forefront Client Security users, who wish to forward syslog events to EventTracker Manager.

Contents

Overview

Forefront Client Security is a unified Internet security software package from Microsoft. Forefront Client Security provides business networks with protection from viruses, worms and other malware threats. The software can protect all of the machines on a Windows network infrastructure, including the servers and the client desktops and laptops.

EventTracker Supports Microsoft Forefront Client Security and monitors it and generates alerts and reports for critical events.

Prerequisites

Prior to configuring Microsoft Forefront Client Security and the EventTracker Enterprise, ensure that you meet the following prerequisites:

- EventTracker should be installed.
- Administrative access on the EventTracker Enterprise.
- Microsoft Forefront Client Security should be installed and proper access permissions to make configuration changes.
- EventTracker agent must be deployed on Microsoft Forefront Client Security machine.

Integration of EventTracker with Microsoft Forefront Client Security

To configure Microsoft Forefront Client Security to forward all the logs to EventTracker Enterprise, deploy EventTracker Agent. EventTracker will receive all Microsoft Forefront Client Security events. The detail procedure to deploy the Agent is available in EventTracker Agent Deployment Manual.

EventTracker Knowledge Pack (KP)

Once logs are received in to EventTracker, Alerts and reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker v7 to support Microsoft Forefront Client Security monitoring:

Categories:-

- **Forefront Client: Client security configuration change -** This category based report provides information related to client security configuration change.
- **Forefront Client: Client security engine failure -** This category based report provides information related to client security engine failure.
- **Forefront Client: Malware detected -** This category based report provides information related to malware detected.
- **Forefront Client: Malware protection action failed -** This category based report provides information related to malware protection action failed.
- **Forefront Client: Malware protection action success -** This category based report provides information related to malware protection action success.
- **Forefront Client: Malware protection engine update failed -** This category based report provides information related to malware protection engine update failed.
- **Forefront Client: Malware protection engine updated -** This category based report provides information related to malware protection engine updated.
- **Forefront Client: Malware protection signature reverted -** This category based report provides information related to malware protection signature reverted.
- **Forefront Client: Malware protection signature update failed -** This category based report provides information related to malware protection signature update failed.
- **Forefront Client: Malware protection signature updated -** This category based report provides information related to malware protection signature updated.
- **Forefront Client: Quarantined item restore failed -** This category based report provides information related to quarantined item restore failed.
- **Forefront Client: Quarantined item restore success -** This category based report provides information related to quarantined item restore success.

- **Forefront Client: Real time protection agent configuration change -** This category based report provides information related to real time protection agent configuration change.
- **Forefront Client: Real time protection agent status -** This category based report provides information related to real time protection agent status.
- **Forefront Client: Real time protection startup failed -** This category based report provides information related to real time protection startup failed.
- **Forefront Client: Scan canceled -** This category based report provides information related to scan canceled.
- **Forefront Client: Scan completed -** This category based report provides information related to scan completed.
- **Forefront Client: Scan disabled -** This category based report provides information related to **scan disabled**.
- **Forefront Client: Scan enabled -** This category based report provides information related to **scan enabled**.
- **Forefront Client: Scan failed -** This category based report provides information related to scan failed.
- **Forefront Client: Scan started-** This category based report provides information related to scan started.

Alerts:-

- **Forefront Client: Client security engine failed-** This alert is generated when client security engine failed.
- **Forefront Client: Configuration change-** This alert is generated when configuration change occurs.
- **Forefront Client: Malware detected-** This alert is generated when malware detected.
- **Forefront Client: Malware protection action failed-** This alert is generated when malware protection action failed occurs.
- **Forefront Client: Update failed-** This alert is generated when update failure occurs.

Import Forefront Client Security Knowledge Pack into EventTracker

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

   Import **Category/Alert** as given below.

To import Category

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

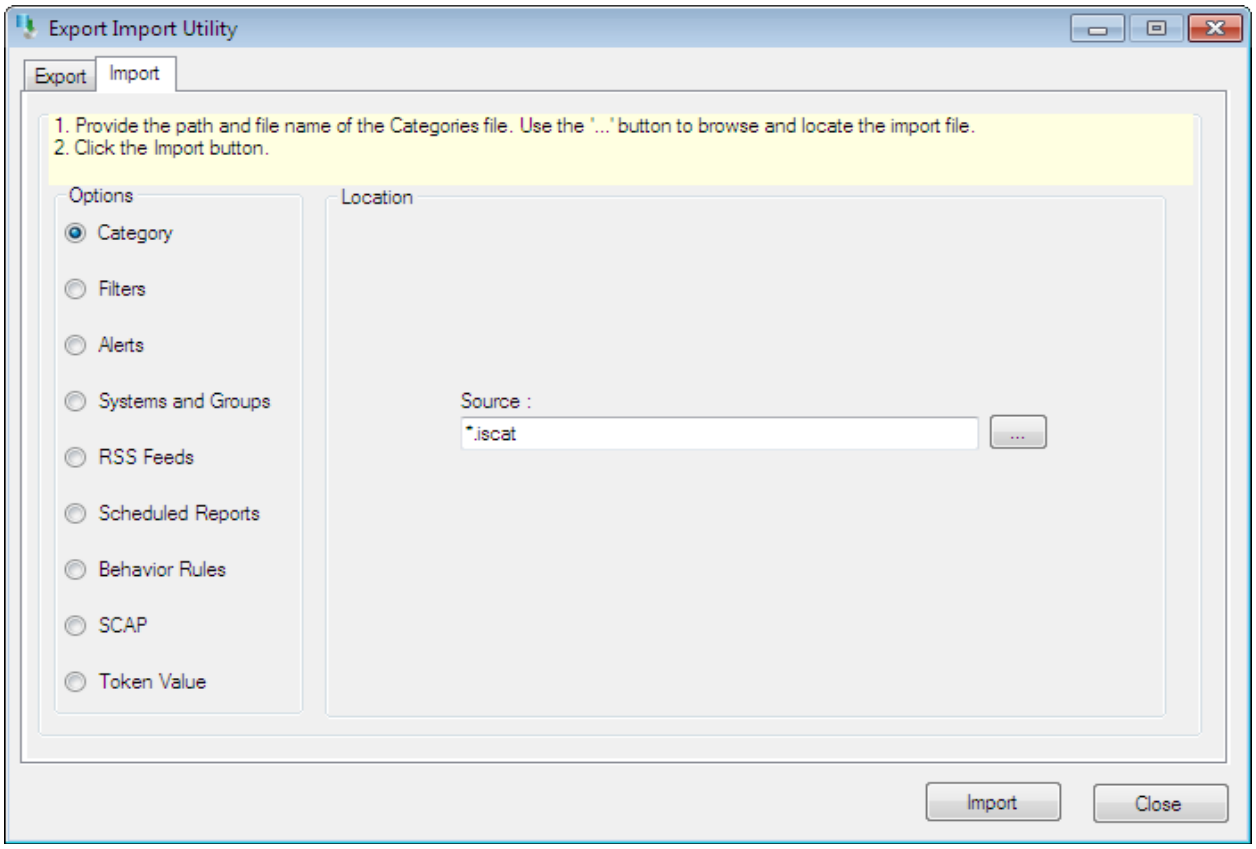

Figure 1

2. Locate **All Forefront Client Security group of Categories.iscat** file, and then click the **Open** button.
3. Click the **Import** button to import the categories.

   EventTracker displays success message.

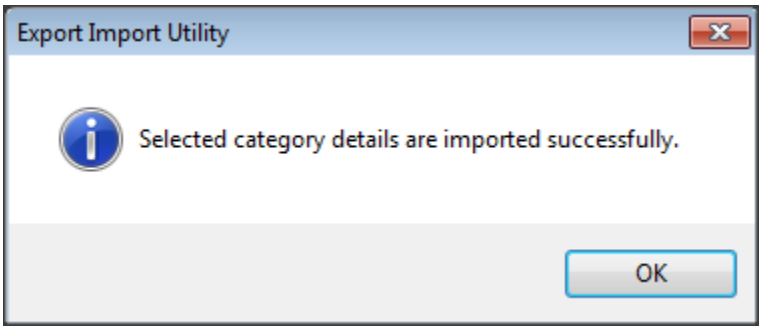

Figure 2

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

To import Alerts

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

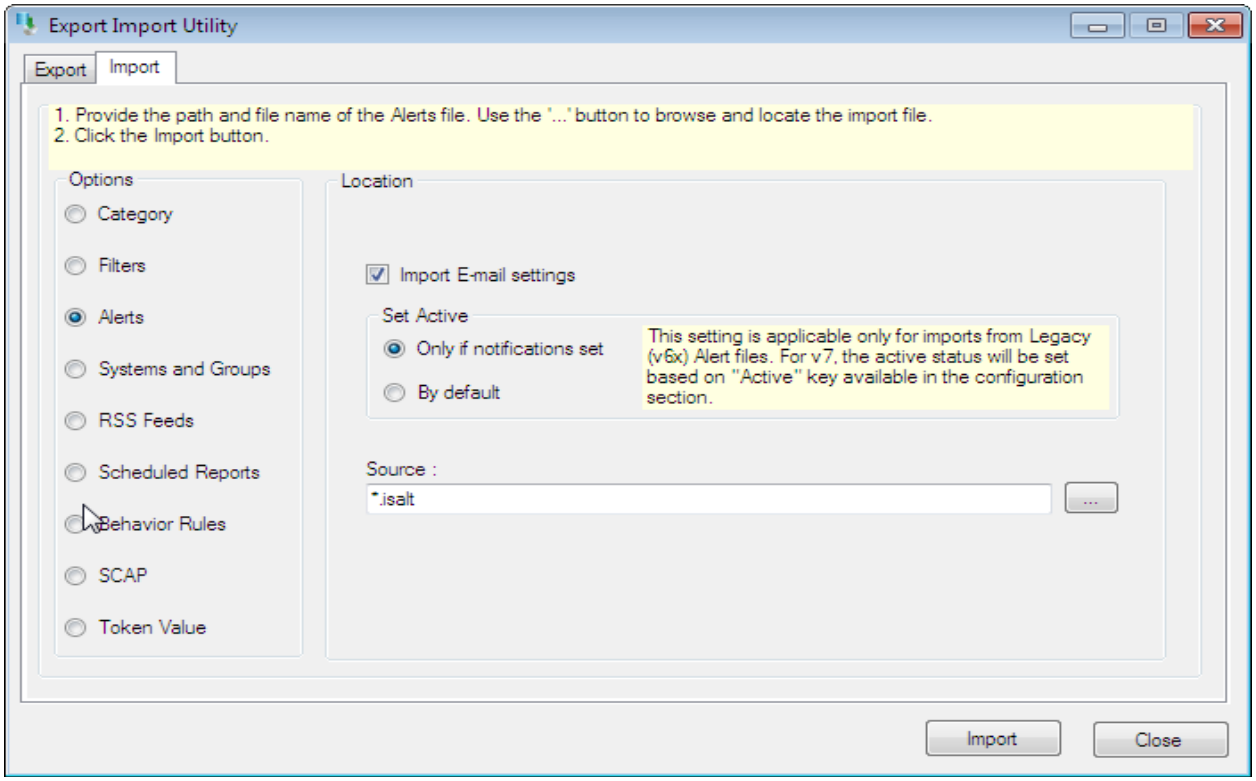

Figure 3

2. Locate **All Forefront Client Security group of Alerts.isalt** file, and then click the **Open** button.
3. Click the **Import** button to import the alerts.

   EventTracker displays success message.

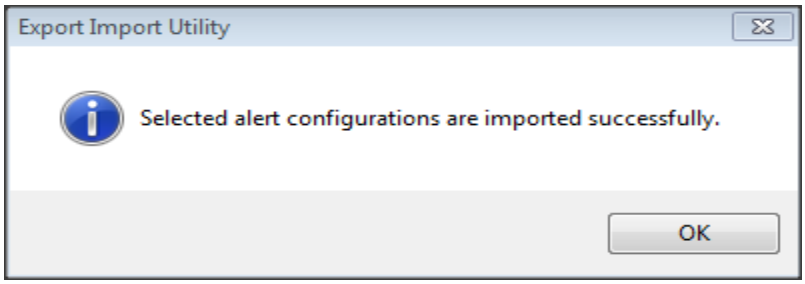

Figure 4

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

Verify Forefront Client Security Knowledge Pack in EventTracker

Verify Forefront Client Security Categories

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

Figure 5

Verify Forefront Client Security Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Alerts**.
3. In the **Search** field, type '**Forefront Client**', and then click the **Go** button.

   Alert Management page will display all the imported Microsoft Forefront Client Security device alerts.

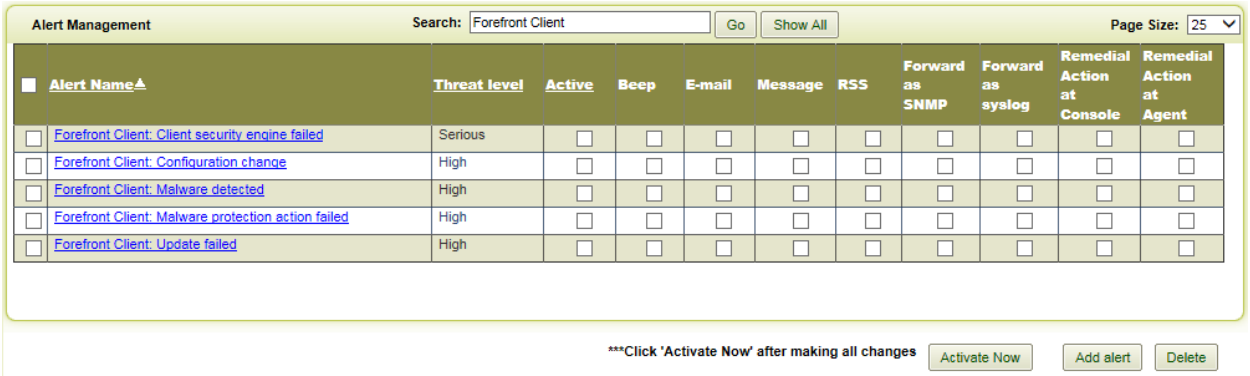

Figure 6

4. To activate the imported alerts, select the respective checkbox in the **Active** column.

   EventTracker displays message box.

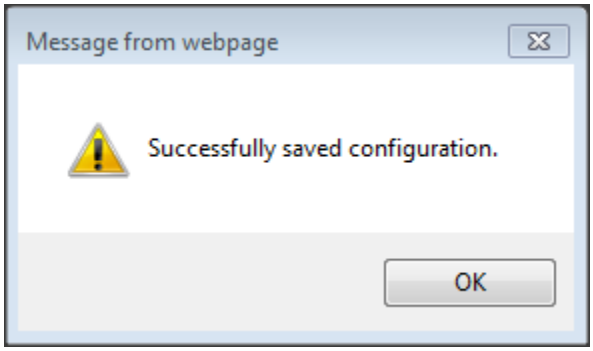

Figure 7

5. Click the **OK** button, 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.