

# Integrating Microsoft Forefront Unified Access Gateway (UAG)

---

*EventTracker v7.x*

# Abstract

This guide provides instructions to configure Microsoft Forefront Unified Access Gateway (UAG) to send the events to EventTracker Enterprise.

## Scope

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

## Audience

Microsoft Forefront Unified Access Gateway users, who wish to forward events to EventTracker Manager.

*The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.*

*This document is for informational purposes only. Prism Microsystems MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.*

*Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.*

*Prism Microsystems may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.*

*The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.*

*© 2014 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

# Contents

- About this Guide ..... 1
  - Scope ..... 1
  - Audience..... 1
- Overview..... 3
- Pre-requisite..... 3
- Integration of EventTracker with Forefront Unified Access Gateway ..... 3
- EventTracker Knowledge Pack (KP) ..... 4
  - Categories ..... 4
  - Alerts ..... 6
- Import UAG Knowledge pack into EventTracker..... 7
  - To import Category..... 7
  - To import Alerts..... 8
- Verify Forefront UAG knowledge pack in EventTracker ..... 10
  - Verify Forefront Unified Access Gateway Categories ..... 10
  - Verify Forefront Unified Access Gateway Alerts ..... 10

## Overview

Forefront UAG as a DirectAccess server, provide a seamless connection to internal resources for client devices that are running as DirectAccess clients. Client requests are securely directed to the internal network, without requiring a VPN connection. Forefront UAG DirectAccess extends the benefits of Windows DirectAccess by providing scalability, access to IPv4 resources, and simplified deployment.

## Pre-requisite

Prior to configuring Forefront Unified Access Gateway and the EventTracker Enterprise, ensure that you meet the following prerequisites:

- EventTracker V7.x should be installed.
- Forefront Unified Access Gateway 2010 should be installed and proper access permissions to make configuration changes.
- Administrative access on the EventTracker Enterprise.

## Integration of EventTracker with Forefront Unified Access Gateway

To configure Forefront Unified Access Gateway Firewall to forward the log to EventTracker Enterprise, deploy [EventTracker Agent](#).

# 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 V 7.x to support Forefront Unified Access Gateway (UAG) monitoring.

## Categories

- **Forefront UAG: Certificate activation failed** - This category based report provides information related to certificate activation failed.
- **Forefront UAG: Certificate cannot be installed** - This category based report provides information related to certificate cannot be installed.
- **Forefront UAG: Certificate requested** - This category based report provides information related to certificate requested.
- **Forefront UAG: Configuration changes** - This category based report provides information related to configuration changes.
- **Forefront UAG: Connection established** - This category based report provides information related to connection established.
- **Forefront UAG: DNS service restarted** - This category based report provides information related to DNS service restarted.
- **Forefront UAG: Filter shutdown** - This category based report provides information related to filter shutdown.
- **Forefront UAG: Filter startup** - This category based report provides information related to filter startup.
- **Forefront UAG: IP helper service error** - This category based report provides information related to IP helper service error.
- **Forefront UAG: KCD protocol transition failed** - This category based report provides information related to KCD protocol transition failed.
- **Forefront UAG: Network configuration error** - This category based report provides information related to network configuration error.

- **Forefront UAG: Network interface cannot disable** - This category based report provides information related to network interface cannot disable.
- **Forefront UAG: Network interface cannot enable** - This category based report provides information related to network interface cannot enable.
- **Forefront UAG: OTP certificate cannot be enrolled** - This category based report provides information related to OTP certificate cannot be enrolled.
- **Forefront UAG: OTP certificates cannot be deleted** - This category based report provides information related to OTP certificates cannot be deleted.
- **Forefront UAG: OTP configuration error** - This category based report provides information related to OTP configuration error.
- **Forefront UAG: Remote user request denied** - This category based report provides information related to remote user request denied.
- **Forefront UAG: Restricted URL access denied** - This category based report provides information related to restricted URL access denied.
- **Forefront UAG: Service down** - This category based report provides information related to service down.
- **Forefront UAG: Service up** - This category based report provides information related to service up.
- **Forefront UAG: Timeout error** - This category based report provides information related to timeout error.
- **Forefront UAG: Unable to send message** - This category based report provides information related to unable to send message.
- **Forefront UAG: Unable to start application** - This category based report provides information related to unable to start application.
- **Forefront UAG: URL changed** - This category based report provides information related to URL changed.
- **Forefront UAG: URL path not allowed** - This category based report provides information related to URL path not allowed.
- **Forefront UAG: User login failed** - This category based report provides information related to user login failed.

- **Forefront UAG: User login successful** - This category based report provides information related to user login successful.
- **Forefront UAG: User request denied** - This category based report provides information related to user request denied.

## Alerts

- **Forefront UAG: Certificate activation failed** - This alert is generated when certificate activation failed.
- **Forefront UAG: Configuration changes** - This alert is generated when configuration changes event occurs.
- **Forefront UAG: IP helper service error** - This alert is generated when IP helper service error event occurs.
- **Forefront UAG: Network configuration error** - This alert is generated when network configuration error event occurs.
- **Forefront UAG: OTP configuration error** - This alert is generated when OTP configuration error event occurs.
- **Forefront UAG: User login failed** - This alert is generated when user login failed.

# Import UAG Knowledge pack into EventTracker

1. Launch **EventTracker Control Panel**.
2. Double click **Import Export Utility**. Click the **Import** tab.  
Import **Category and Alert** as given below.

## To import Category

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

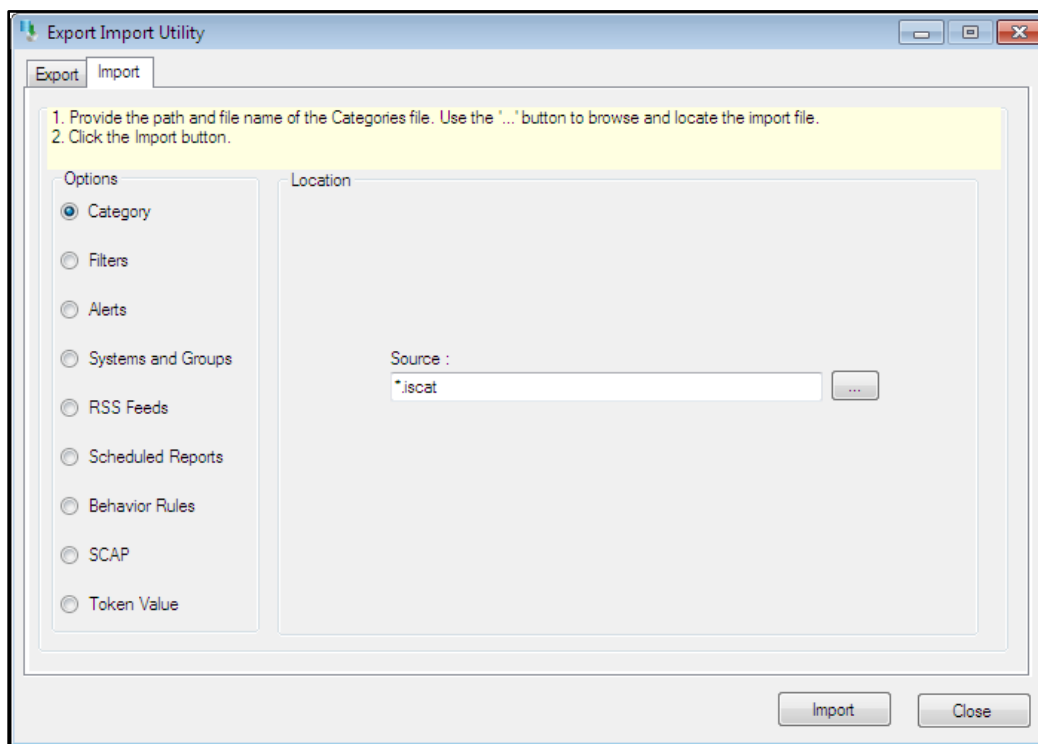


Figure 1

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



EventTracker displays success message.

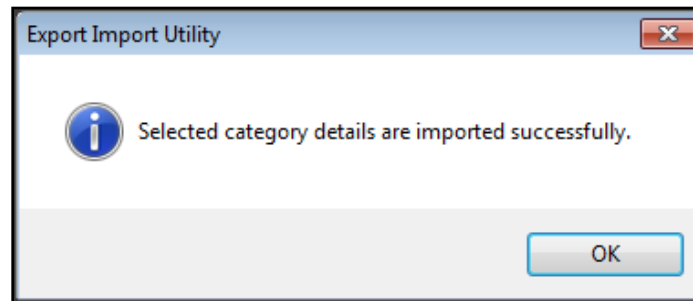



Figure 2

4. Click the **OK** button. Click the **Close** button.

## To import Alerts

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

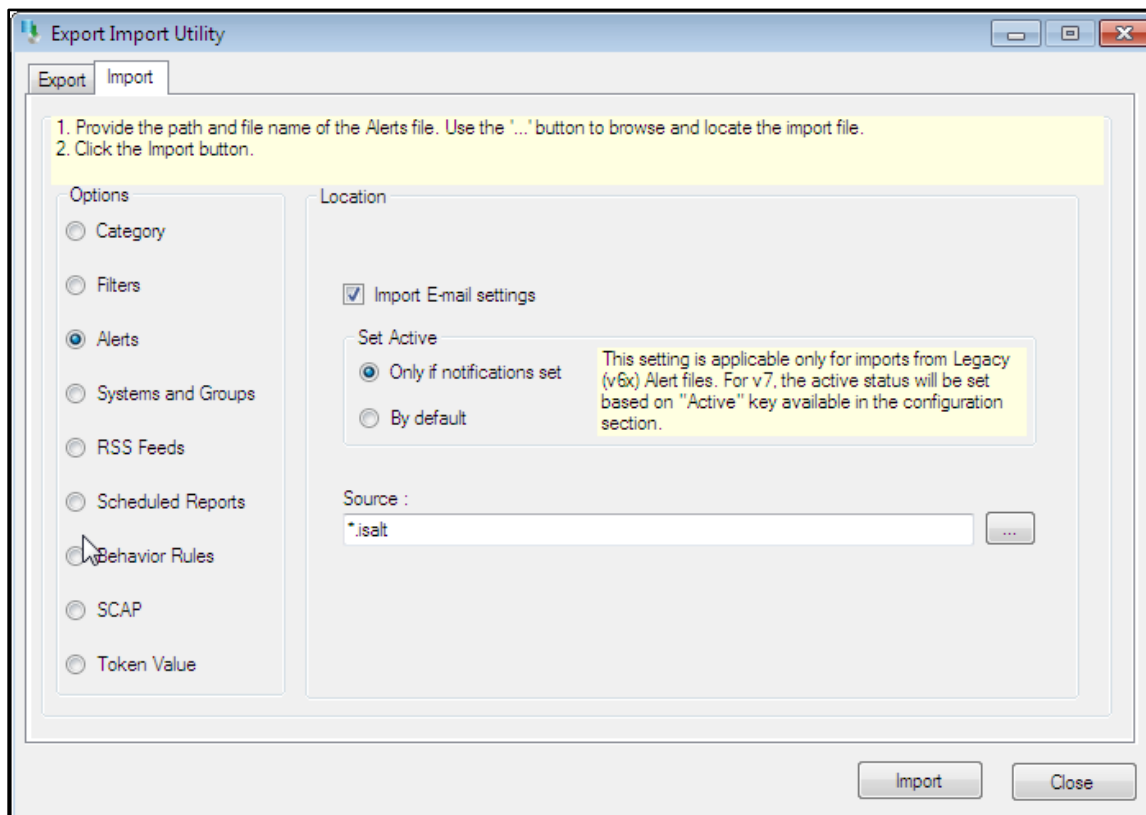


Figure 3

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

EventTracker displays success message.

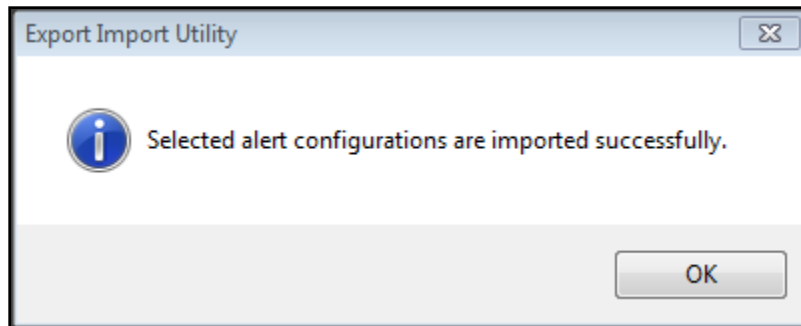


Figure 4

4. Click the **OK** button. Click the **Close** button.

# Verify Forefront UAG knowledge pack in EventTracker

## Verify Forefront Unified Access Gateway Categories

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Category**.
3. In the **Category Tree**, expand Microsoft Forefront group folder under this Unified Access Gateway, to see the imported categories.

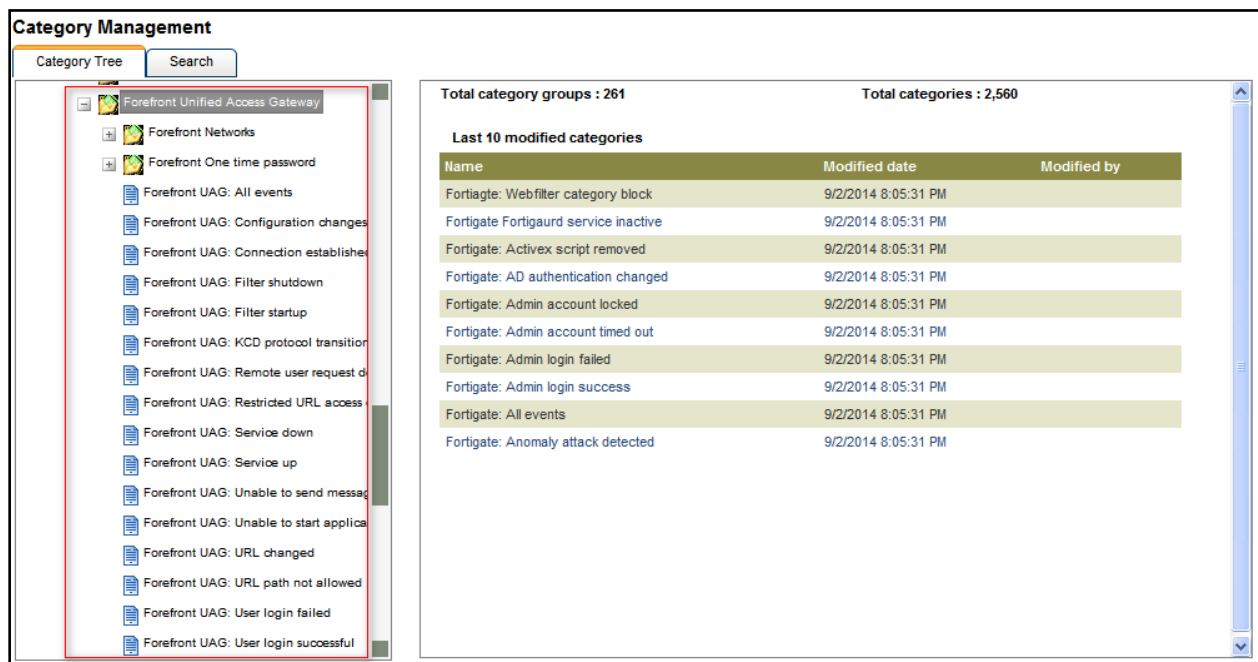


Figure 5

## Verify Forefront Unified Access Gateway Alerts

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

Alert Management page will display all the imported Forefront Unified Access Gateway alerts.

Alert Name	Threat level	Active	Beep	E-mail	Message	RSS	Forward as SNMP	Forward as syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
<a href="#">Forefront UAG. Certificate activation failed</a>	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forefront Client 2010 and later
<a href="#">Forefront UAG. Configuration changes</a>	Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forefront Client 2010 and later
<a href="#">Forefront UAG. IP helper service error</a>	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forefront Client 2010 and later
<a href="#">Forefront UAG. Network configuration error</a>	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forefront Client 2010 and later
<a href="#">Forefront UAG. OTP configuration error</a>	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forefront Client 2010 and later
<a href="#">Forefront UAG. User login failed</a>	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forefront Client 2010 and later

\*\*Click 'Activate Now' after making all changes

Figure 6

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

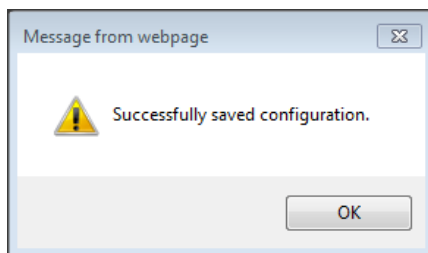


Figure 7

- 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.