

# Integrating McAfee IntruShield IPS

---

*EventTracker v7.x*

# Abstract

This guide provides instructions to configure McAfee IntruShield Intrusion Prevention Sensor (IPS) to send the syslog events to EventTracker Enterprise.

## Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 7.X and later, McAfee IntruShield Security Manager Version 4.1 and later.

## Audience

McAfee IntruShield IPS users, who wish to forward syslog 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.*

*© 2015 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

# Table of Contents

- Abstract..... 1
  - Scope ..... 1
  - Audience..... 1
- Overview..... 3
- Prerequisites..... 3
- Integration of EventTracker with McAfee IntruShield IPS..... 3
- EventTracker Knowledge Pack (KP)..... 6
  - Categories ..... 6
  - Alerts ..... 7
- Import McAfee IntruShield IPS Knowledge pack into EventTracker ..... 8
  - Import Category..... 8
  - Import Alerts..... 10
  - Import Tokens..... 11
  - Import Flex Reports ..... 12
- Verify McAfee IntruShield IPS knowledge pack in EventTracker ..... 13
  - Verify McAfee IntruShield IPS Categories ..... 13
  - Verify McAfee IntruShield IPS Alerts ..... 13
  - Verify McAfee IntruShield IPS Tokens ..... 15
  - Verify McAfee IntruShield IPS Flex Reports..... 15
- Sample Report..... 17

## Overview

EventTracker is designed to delve into the operational and machine data an organization's IT infrastructure collects as it operates, and quickly identify patterns, isolate problems, and make it possible to diagnose potential security and other problems. EventTracker provides tools that address SIEM, real-time log management change and configuration management.

## Prerequisites

- EventTracker v7.x should be installed.
- McAfee IntruShield Security Manager Version 4.1 and later should be installed and configured.

## Integration of EventTracker with McAfee IntruShield IPS

1. To configure McAfee IntruShield IPS to forward logs to EventTracker Enterprise, open the IntruShield Manager Console.
2. Select **Alert Notification** tab, and then select **Syslog Forwarder**.

Alert Syslog Forwarder pane is displayed.

Figure 1

3. Select **Yes** next to **Enable Syslog Forwarder**.
4. Enter the **IP address** or **hostname** of EventTracker Enterprise in the appropriate **Syslog Server** field.
5. Enter '**514**' in the **Port** field.
6. Select **Local user 0 (local0)** from the **Facilities** list.
7. Complete the **Severity Mapping** section as follows:
  - **Informational to:** Select **Informational: informational messages**.
  - **Low to:** Select **Notice: normal but significant condition**.
  - **Medium to:** Select **Critical: critical conditions**.
  - **High to:** Select **Alert: action must be taken immediately**.
8. Select **Informational and above** from the **With severity** list in the **Forward Alerts** section.
9. Click **Apply**.

10. Select **Customized** in the **Message Preference** section, and then click **Edit**.
11. Copy and paste the following text into the Message field on the Customize Syslog Forwarder Message window.

**SyslogAlertForwarder format string:**

```
|$IV_ATTACK_TIME|$IV_ATTACK_ID|$IV_ATTACK_NAME|$IV_SOURCE_IP|$IV_SOURCE_PORT|$IV_DESTINATION_IP|$IV_DESTINATION_PORT|$IV_NETWORK_PROTOCOL|$IV_INTERFACE|$IV_APPLICATION_PROTOCOL|$IV_RESULT_STATUS|$IV_DIRECTION|$IV_CATEGORY|$IV_SUB_CATEGORY|$IV_ATTACK_SEVERITY|$IV_ATTACK_CONFIDENCE|$IV_ADMIN_DOMAIN|$IV_SENSOR_NAME|$IV_ALERT_TYPE|$IV_DETECTION_MECHANISM|$IV_ATTACK_SIGNATURE$
```

**SyslogAuditLogForwarder format string:**

```
|$IV_AUDIT_ACTION|$IV_AUDIT_RESULT|$IV_AUDIT_TIME|$IV_AUDIT_MESSAGE|$IV_AUDIT_USER|$IV_AUDIT_CATEGORY|$IV_AUDIT_DOMAIN|$IV_AUDIT_DETAIL_COMMENT|$IV_AUDIT_DETAIL_DELTA$
```

**SyslogACLLogForwarder format string:**

```
|$ACL_NAME|$ACL_ACTION|$SOURCE_IP|$SOURCE_PORT|$TARGET_IP|$TARGET_PORT|$APPLICATION_PROTOCOL|$SENSOR_NAME|$INTERFACE|$ALERT_DIRECTION$
```

**SyslogFaultForwarder format string:**

```
|$IV_FAULT_TYPE|$IV_FAULT_NAME|$IV_DESCRIPTION|$IV_FAULT_SOURCE|$IV_FAULT_COMPONENT|$IV_FAULT_LEVEL|$IV_FAULT_TIME|$IV_SEVERITY|$IV_ADMIN_DOMAIN|$IV_OWNER_NAME|$IV_OWNER_ID|$IV_ACK_INFORMATION$
```

12. Click **Save** and then click **Apply**.

# EventTracker Knowledge Pack (KP)

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

The following Knowledge Packs are available in EventTracker v7.x to support McAfee IntruShield IPS monitoring.

## Categories

- **McAfee IntruShield IPS: Brute-force attack** - This category based report provides information related to the Brute-force attack activity.
- **McAfee IntruShield IPS: Exploit attack** - This category based report provides information related to exploit attack.
- **McAfee IntruShield IPS: Fingerprinting attack** - This category based report provides information related to fingerprinting attack.
- **McAfee IntruShield IPS: Host sweep attack** - This category based report provides information related to host sweep attack.
- **McAfee IntruShield IPS: Policy Violation attack** - This category based report provides information related to policy violation attack.
- **McAfee IntruShield IPS: Port-scan attack** - This category based report provides information related to port-scan attack.
- **McAfee IntruShield IPS: Service-sweep attack** - This category based report provides information related to service-sweep attack.
- **McAfee IntruShield IPS: Volume DoS** - This category based report provides information related to volume DoS.

## Alerts

- **McAfee IntruShield IPS: Brute-force** - This alert is generated when Brute-force attack occurs.
- **McAfee IntruShield IPS: BACKDOOR attack** - This alert is generated when BACKDOOR attack occurs.
- **McAfee IntruShield IPS: Back Orifice Trojan** - This alert is generated when Back Orifice Trojan detected.
- **McAfee IntruShield IPS: Exploit** - This alert is generated when exploitation attack occurs.
- **McAfee IntruShield IPS: Fingerprinting** - This alert is generated when fingerprinting attack occurs.
- **McAfee IntruShield IPS: FTP login alert** - This alert is generated when FTP login occurs.
- **McAfee IntruShield IPS: Host sweep** - This alert is generated when host sweep event occurs.
- **McAfee IntruShield IPS: MSSQL user login failed** - This alert is generated when MSSQL user login failure occurs.
- **McAfee IntruShield IPS: NBTSTAT scan** - This alert is generated when NBTSTAT scan occurs.
- **McAfee IntruShield IPS: Port-scan** - This alert is generated when port-scan activity occurs.
- **McAfee IntruShield IPS: RADIUS attack** - This alert is generated when RADIUS attack occurs.
- **McAfee IntruShield IPS: SITE EXEC exploit** - This alert is generated when SITE EXEC exploit occurs.
- **McAfee IntruShield IPS: SMTP worm spread via attachment** - This alert is generated when SMTP worm spreads by attachment.
- **McAfee IntruShield IPS: SQL system alert** - This alert is generated when SQL system activity occurs.
- **McAfee IntruShield IPS: Telnet login Brute force** - This alert is when generated telnet login occurs by brute force.




- **McAfee IntruShield IPS: Virus/worm file share spread** - This alert is generated when virus/worm is spread by shared file.

## Import McAfee IntruShield IPS Knowledge pack into EventTracker

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

Import **Category/Alerts/Tokens/Flex Reports** as given below.

### Import Category

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

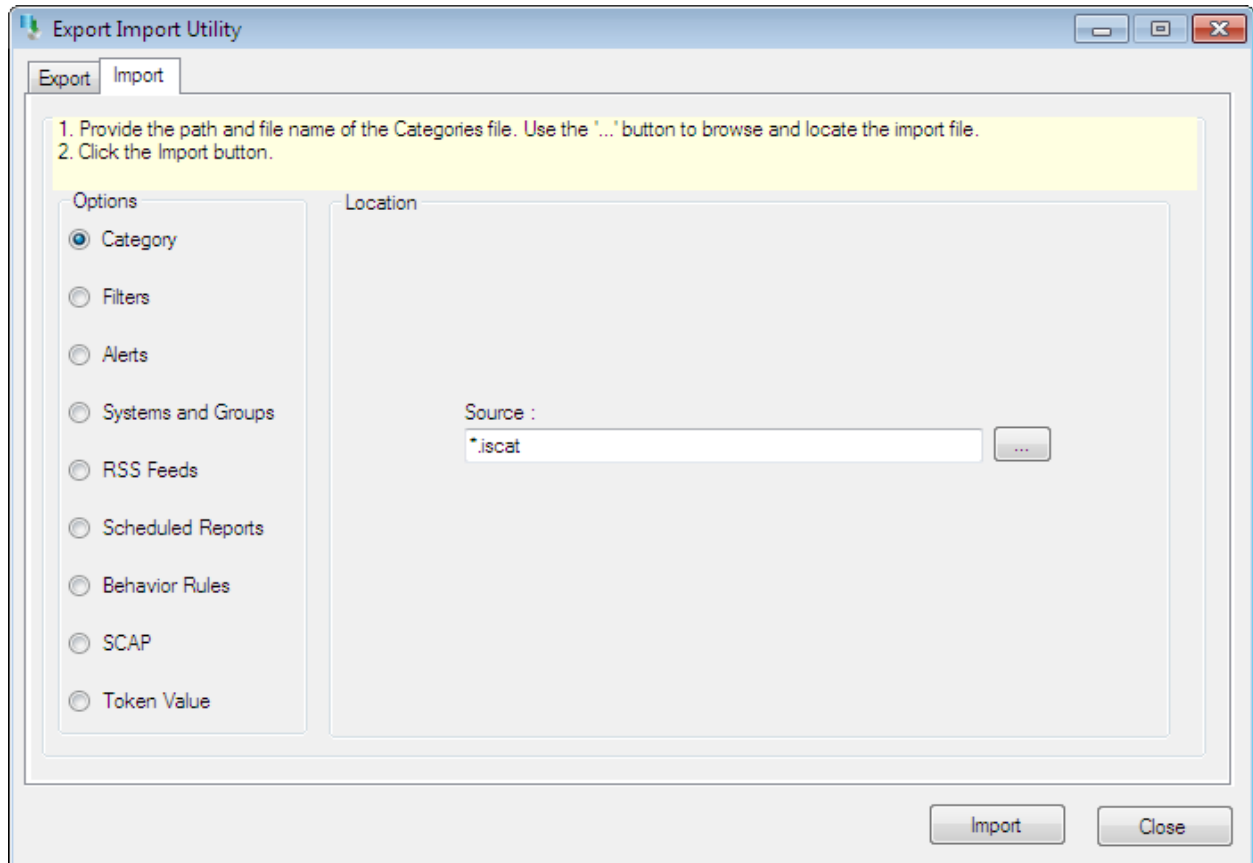


Figure 2

2. Locate **All McAfee IntruShield IPS group of Categories.iscat** file, and then click the **Open** button.
3. To import the categories, click the **Import** button.

EventTracker displays success message.

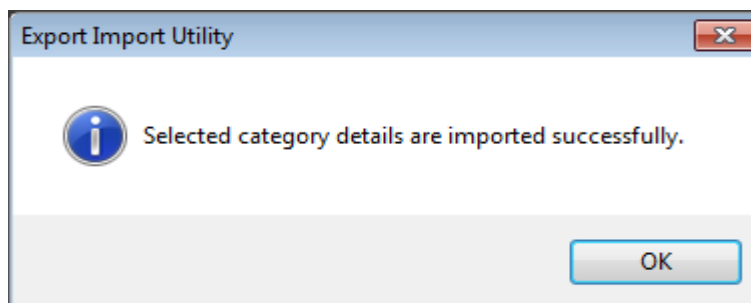



Figure 3

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

# Import Alerts

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

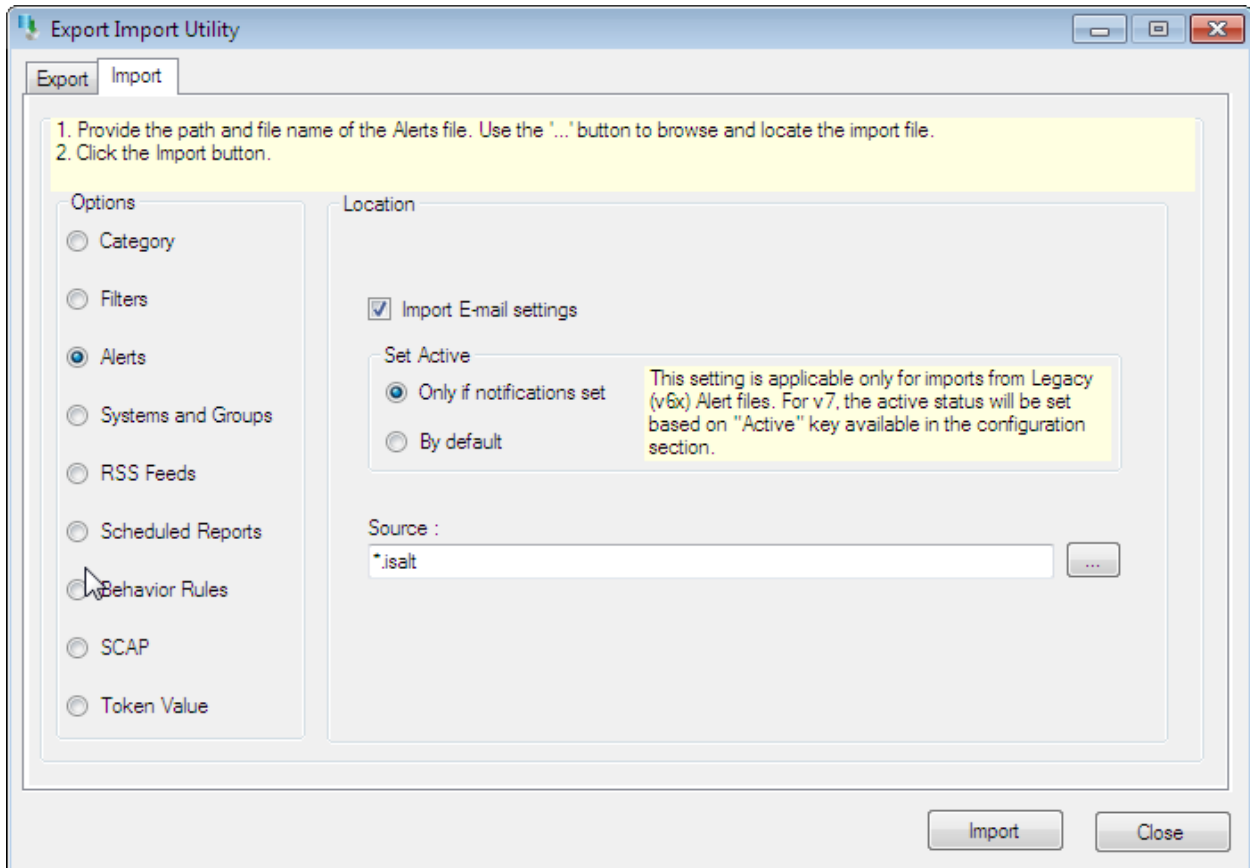


Figure 4

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

EventTracker displays success message.

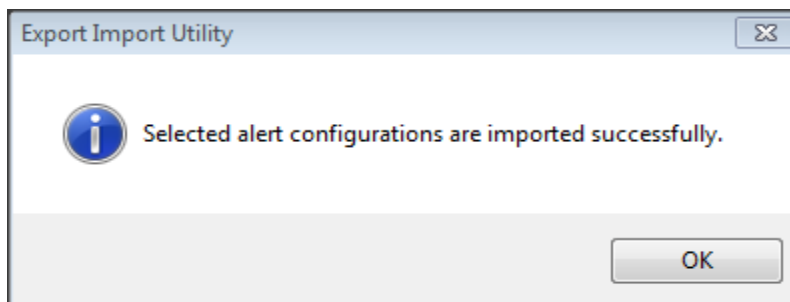



Figure 5

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

## Import Tokens

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

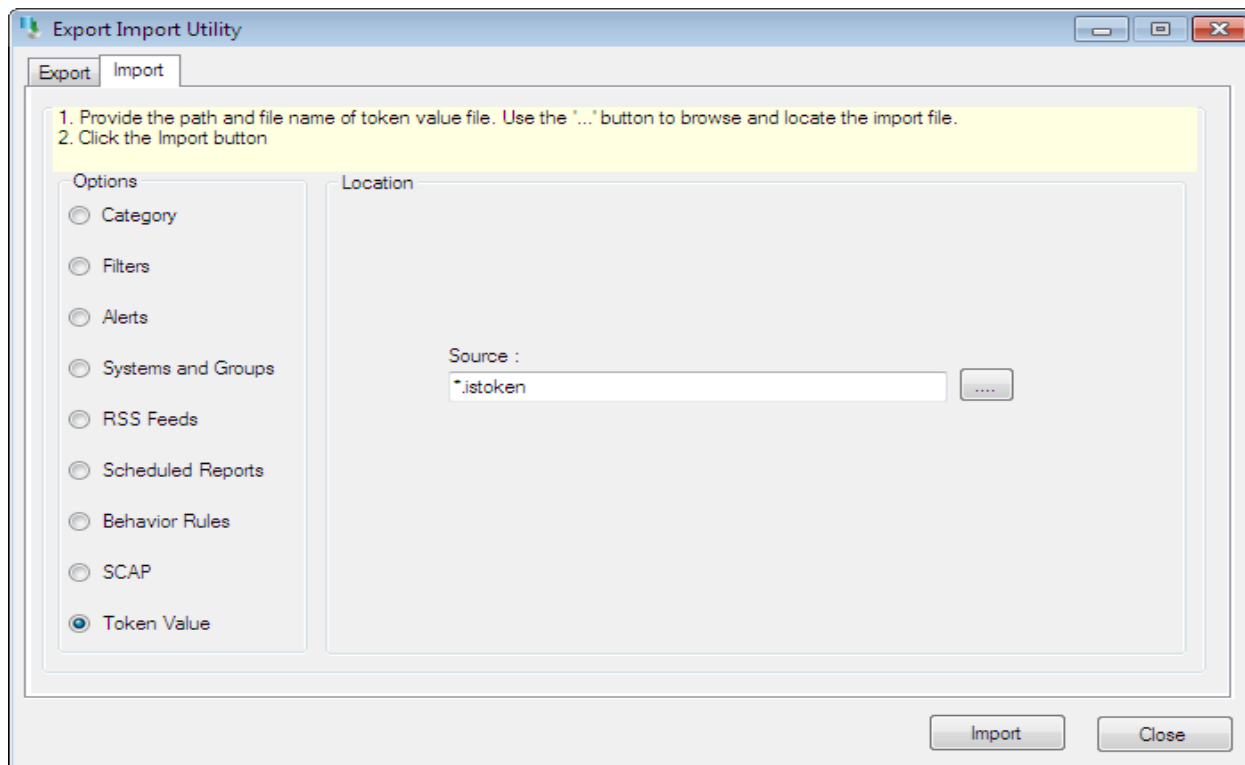


Figure 6

2. Locate **All McAfee IntruShield IPS group of Tokens.istoken** file, and then click the **Open** button.
3. To import tokens, click the **Import** button.

EventTracker displays success message.

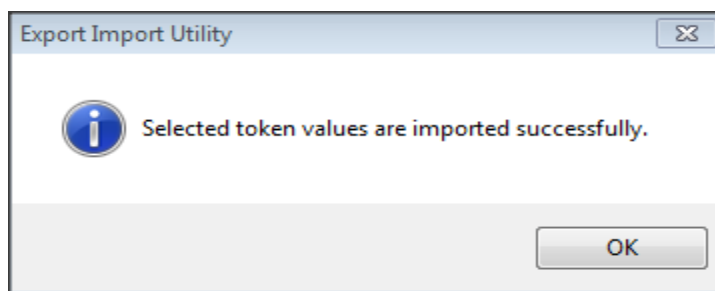



Figure 7

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

## Import Flex Reports

1. Click **Scheduled Reports** option and then click the browse  button.
2. Locate **All McAfee IntruShield IPS group of reports.issch** file and then click the **Open** button.

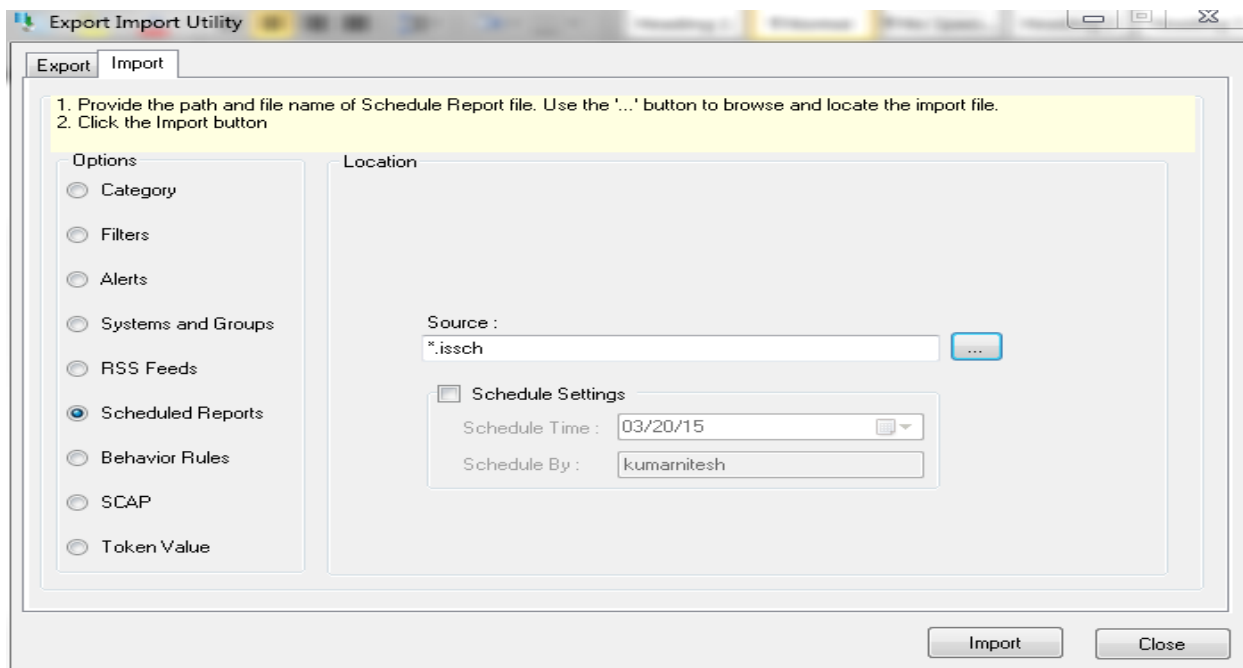


Figure 8

3. To import scheduled reports, click the **Import** button.

EventTracker displays success message.

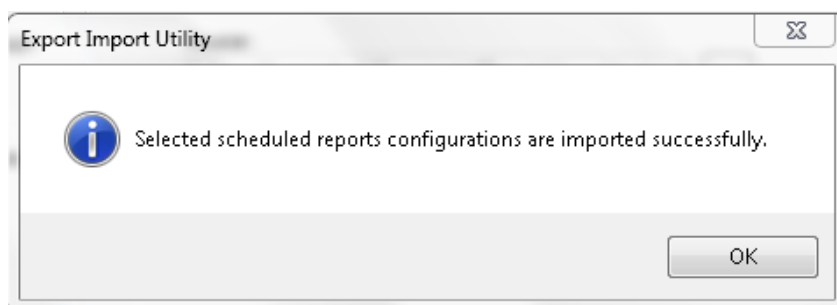


Figure 9

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

# Verify McAfee IntruShield IPS knowledge pack in EventTracker

## Verify McAfee IntruShield IPS Categories

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

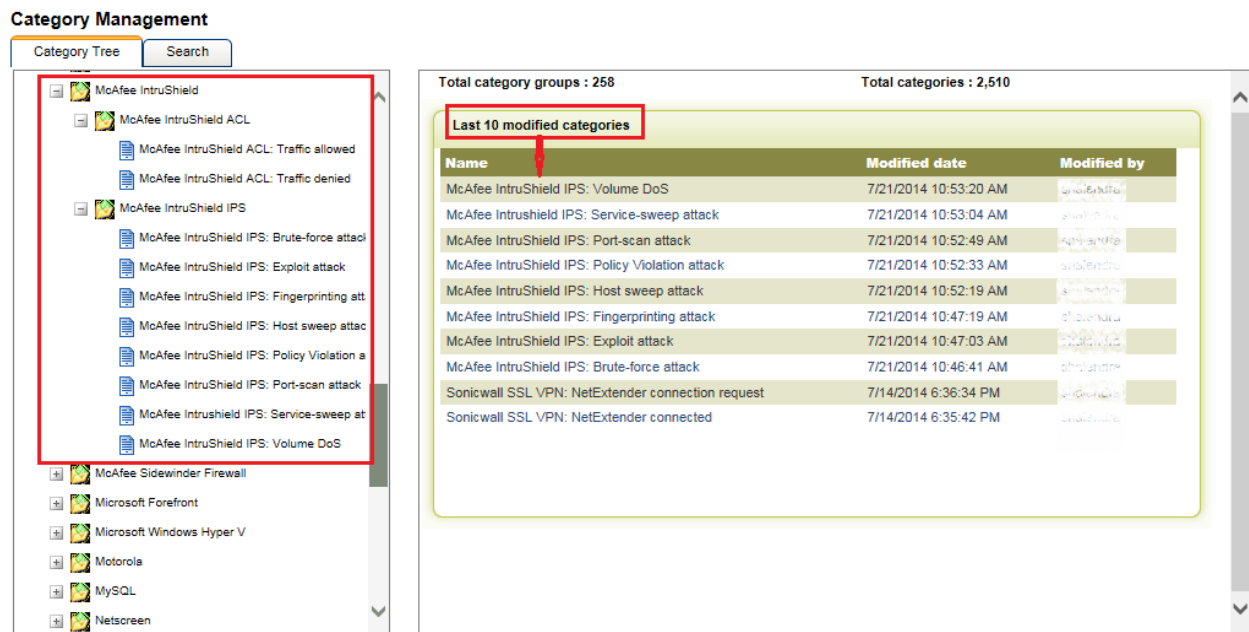


Figure 10

## Verify McAfee IntruShield IPS Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Alerts**.
3. In the **Search** field, enter '**McAfee IntruShield IPS**', and then click the **Go** button.

Alert Management page displays all the imported McAfee IntruShield IPS alerts.

Alert Management Search: McAfee Go Show All Page Size: 25

Alert Name	Threat level	Active	Beep	E-mail	Message	RSS	Forward as SNMP	Forward as syslog	Remedial Action at Console	Remedial Action at Agent
<input type="checkbox"/> McAfee EPO: Activity log error	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"/>
<input type="checkbox"/> McAfee EPO: Buffer overflow detected	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"/>
<input type="checkbox"/> McAfee EPO: Disk I/O errors	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"/>
<input type="checkbox"/> McAfee EPO: File I/O errors	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"/>
<input type="checkbox"/> McAfee EPO: Memory allocation error	Medium	<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"/>
<input type="checkbox"/> McAfee EPO: Scan error	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"/>
<input type="checkbox"/> McAfee EPO: Virus detected	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"/>
<input type="checkbox"/> McAfee HIPS: Application blocked	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"/>
<input type="checkbox"/> McAfee HIPS: Host intrusion detected	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"/>
<input type="checkbox"/> McAfee HIPS: Network intrusion detected	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"/>
<input type="checkbox"/> McAfee HIPS: Quarantine check failed	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"/>
<input checked="" type="checkbox"/> McAfee IntruShield IPS: Back office Trojan	Medium	<input checked="" 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"/>
<input checked="" type="checkbox"/> McAfee IntruShield IPS: BACKDOOR Attack	High	<input checked="" 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"/>

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

Activate Now Add alert Delete

Figure 11

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

EventTracker displays message box.

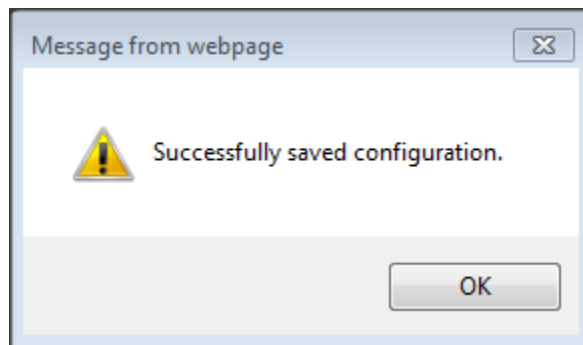


Figure 12

- 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.

## Verify McAfee IntruShield IPS Tokens

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Parsing rules**.

Imported McAfee IntruShield tokens are added in Token-Value Groups list. Refer Figure 14.

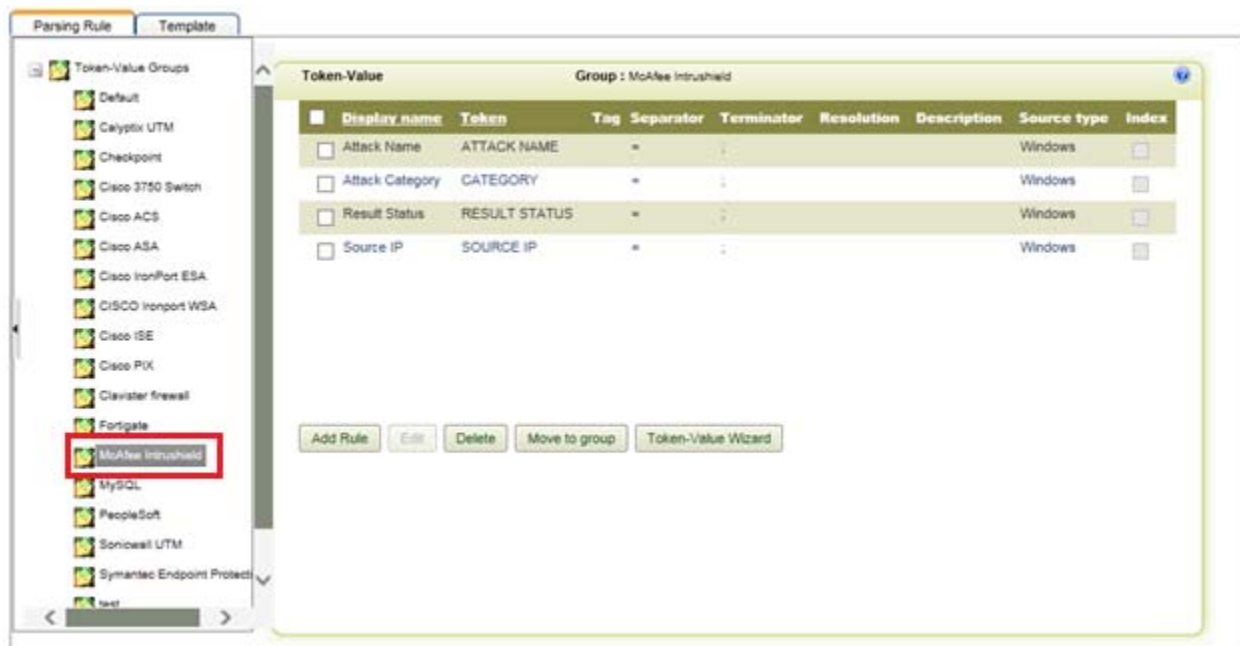


Figure 13

## Verify McAfee IntruShield IPS Flex Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports** menu and then **Configuration**.
3. Select **Defined** in report type.
4. In **Report groups Tree** to view imported Scheduled Reports, scroll down and click **McAfee** group folder. Scheduled Reports are displayed in the Reports configuration pane.



Report groups

- Cisco IronPort WSA
- Cisco ISE
- Clavister
- Dell FORCE 10 Switch
- EventTracker
- Flex
- Imperva
- Juniper JUNOS
- LOGbinder SP
- LOGbinder SQL
- McAfee**
- OKTA SSO
- Persistent
- SEPM
- Snort
- Sonitwall UTM
- Teradata Database
- Trend Micro
- Trend Micro
- VMware
- WebSense WSG

Reports configuration >> McAfee

Scheduled  Queued  Defined

Search

New

Title	Created on	Modified on
<a href="#">McAfee Intrushield-IPS attack detail report</a>	04/17/12 4:47:26 PM	04/17/12 4:47:26 PM
<a href="#">McAfee HPS threat detail report</a>	11/21/11 5:35:04 PM	11/21/11 5:35:04 PM
<a href="#">McAfee VirusScan analysis report</a>	11/21/11 4:42:02 PM	11/21/11 4:42:02 PM

Delete Move to group

Figure 24

# Sample Report

## McAfee Intrushield - Attack activity

### User Selection :

From Date: 7/17/2014 6:05:43 PM

To Date: 7/17/2014 7:05:43 PM

Limit Time Range: None

Refine: None

Filter: None

Categories Selected: N/A

Computers Selected: CONTOSO-MCAFEIIPS-SYSLOG, CONTOSO-MCAFEIIPS

Description: None

### Detail:

LogTime	Source IP	Attack Name	Attack Category	Result Status
07/17/2014 06:05:52 PM	45.67.2.6	NETBIOS-SS: Virus/Worm File Share Spread	Service Sweep	Blocked
07/17/2014 06:05:52 PM	23.45.68.82	RADIUS: Authentication Brute Force	Brute Force	Blocked
07/17/2014 06:05:52 PM	34.67.98.54	NETBIOS-NS: NBTSTAT Scan	Service Sweep	Blocked
07/17/2014 06:05:52 PM	56.27.92.34	MSSQL: Password Brute Force	Brute Force	Blocked
07/17/2014 06:05:52 PM	53.6.24.25	IMAP: Password Brute Force	Brute Force	Blocked
07/17/2014 06:05:52 PM	67.24.46.34	ICMP: Host Sweep	Host sweep	Blocked
07/17/2014 06:05:52 PM	58.12.34.23	FTP: Login Brute Force	Brute Force	Blocked
07/17/2014 06:05:52 PM	23.67.34.34	MSSQL: SQL Server Worm Slammer	Exploit	Blocked
07/17/2014 06:05:52 PM	23.78.67.32	Over Threshold	DDos	Blocked
07/17/2014 06:05:53 PM	36.36.25.25	BACKDOOR: Injector Trojan	Exploit	Blocked
07/17/2014 06:05:53 PM	57.23.24.75	RLOGIN: Password Brute Force	Brute Force	Blocked