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.
# 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.
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:**

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

**SyslogAuditLogForwarder format string:**

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

**SyslogACLLogForwarder format string:**

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

**SyslogFaultForwarder format string:**

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

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 generated when 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.
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.

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

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

![Figure 4](image)

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](image)
4. Click **OK**, and then click the **Close** button.

**Import Tokens**

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

![Figure 6](image)

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](image)
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.

3. To import scheduled reports, click the **Import** button. EventTracker displays success message.

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.

![Category Management](image)

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

   EventTracker displays message box.

![Message from webpage](image)

**Figure 12**

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.
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](image)

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.
EventTracker: Integrating McAfee IntruShield IPS

![Image of EventTracker interface]

**Figure 24**

<table>
<thead>
<tr>
<th>Title</th>
<th>Created on</th>
<th>Modified on</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee IntruShield IPS attack detail report</td>
<td>01/27/13 4:47:26 PM</td>
<td>01/27/13 4:47:26 PM</td>
</tr>
<tr>
<td>McAfee IPS threat detail report</td>
<td>11/01/11 5:56:34 PM</td>
<td>11/01/11 5:56:34 PM</td>
</tr>
<tr>
<td>McAfee virus scan malware report</td>
<td>11/02/11 4:42:02 PM</td>
<td>11/02/11 4:42:02 PM</td>
</tr>
</tbody>
</table>
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-MCAFEEIPS-SYSLOG, CONTOSO-MCAFEEIPS
- Description: None

**Detail:**

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Source IP</th>
<th>Attack Name</th>
<th>Attack Category</th>
<th>Result Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>07/17/2014 06:05:52 PM</td>
<td>45.87.2.8</td>
<td>NETBIOS-SS: Virus/Worm File Share Spread</td>
<td>Service Sweep</td>
<td>Blocked</td>
</tr>
<tr>
<td>07/17/2014 06:05:52 PM</td>
<td>21.46.68.02</td>
<td>RADIUS: Authentication Brute Force</td>
<td>Brute Force</td>
<td>Blocked</td>
</tr>
<tr>
<td>07/17/2014 06:05:52 PM</td>
<td>24.57.82.54</td>
<td>NETBIOS-NS: NETSTAT Scan</td>
<td>Service Sweep</td>
<td>Blocked</td>
</tr>
<tr>
<td>07/17/2014 06:05:52 PM</td>
<td>50.27.92.34</td>
<td>MSSQL: Password Brute Force</td>
<td>Brute Force</td>
<td>Blocked</td>
</tr>
<tr>
<td>07/17/2014 06:05:52 PM</td>
<td>53.8.24.25</td>
<td>MAP: Password Brute Force</td>
<td>Brute Force</td>
<td>Blocked</td>
</tr>
<tr>
<td>07/17/2014 06:05:52 PM</td>
<td>67.24.46.34</td>
<td>ICMP: Host Sweep</td>
<td>Host Sweep</td>
<td>Blocked</td>
</tr>
<tr>
<td>07/17/2014 06:05:52 PM</td>
<td>56.12.34.23</td>
<td>FTP: Login Brute Force</td>
<td>Brute Force</td>
<td>Blocked</td>
</tr>
<tr>
<td>07/17/2014 06:05:52 PM</td>
<td>23.67.34.34</td>
<td>MSSQL: SQL Server Worm/Scanner</td>
<td>Exploit</td>
<td>Blocked</td>
</tr>
<tr>
<td>07/17/2014 06:05:52 PM</td>
<td>23.78.67.32</td>
<td>Over Threshold</td>
<td>DDoS</td>
<td>Blocked</td>
</tr>
<tr>
<td>07/17/2014 06:05:53 PM</td>
<td>26.36.25.28</td>
<td>BACKDOOR: Injector Trojan</td>
<td>Exploit</td>
<td>Blocked</td>
</tr>
<tr>
<td>07/17/2014 06:05:53 PM</td>
<td>57.23.24.75</td>
<td>ALOGN: Password Brute Force</td>
<td>Brute Force</td>
<td>Blocked</td>
</tr>
</tbody>
</table>