

Integrate McAfee Sidewinder Firewall

EventTracker v7.x

Abstract

This guide provides instructions to configure McAfee Sidewinder Firewall 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, and McAfee Sidewinder Firewall 6.1 and later.

Audience

McAfee Sidewinder Firewall 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.

© 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

- Abstract..... 1
 - Scope 1
 - Audience..... 1
- Overview..... 3
- Prerequisites..... 3
- Integrate EventTracker with McAfee Sidewinder Firewall 4
 - Configure McAfee Sidewinder Firewall to forward logs to EventTracker..... 4
 - Configure Sidewinder v6.1 4
 - Configure Sidewinder v 6.2.x 5
 - Configure Sidewinder version 7.0 6
- EventTracker Knowledge Pack (KP) 8
 - Categories 8
 - Alerts 10
- Import McAfee Sidewinder Knowledge Pack in EventTracker 11
 - Import Category..... 11
 - Import Alerts..... 12
- Verify McAfee Sidewinder knowledge pack in EventTracker..... 14
 - Verify McAfee Sidewinder Firewall Categories 14
 - Verify McAfee Sidewinder Firewall Alerts..... 14

Overview

McAfee Sidewinder (also known as Secure Firewall) is a hardware appliance that contains the following features:

- Application-layer firewall
- VPN functionality
- Web filtering
- Anti-spam/Anti-fraud functionality
- Anti-virus/Anti-spyware filtering engines

The logs produced by Sidewinder include events from all of its application functions (i.e., firewall, VPN, Web filtering, etc.) as well as local auditing of the Sidewinder appliance itself (e.g., appliance configuration changes, logins, daemon errors, etc.). Sidewinder appliances can generate audit log messages via Syslog using a variety of log formats.

The EventTracker Enterprise supports Syslog Sidewinder firewall events using the Sidewinder Export Format (SEF). EventTracker acts as the Syslog Server for Sidewinder, and Sidewinder sends SEF-formatted Syslog messages via UDP or TCP to the EventTracker's Syslog Listener. The configuration procedures for Sidewinder and the EventTracker depend upon your environment.

Prerequisites

Prior to configuring Sidewinder and the EventTracker Enterprise, ensure that you meet the following prerequisites:

- EventTracker v7.x should be installed
- Secure Computing Sidewinder appliances running version 6.1, 6.2.x, 7.0
- Proper access permissions to make configuration changes
- Administrative access on the EventTracker Enterprise
- McAfee Firewall Enterprise (Sidewinder) appliances running version 7.0

Integrate EventTracker with McAfee Sidewinder Firewall

Configure McAfee Sidewinder Firewall to forward logs to EventTracker

Configure Sidewinder v6.1

1. Make sure that the auditing and syslog daemons are stopped on the Sidewinder host machine.
2. On Sidewinder, navigate to the location **/etc/sidewinder/**
3. Open **auditd.conf** file in a text editor and add the following line to end of the file:**syslog(facilityfilters["filter"] format)**

where,

- **facility** - Facility level associated with the Syslog message (e.g., local0-local7)
 - **filter** - Name of the sacap filter to use for all the events. If this parameter is set to NULL, then all audit events are reported to the log.
 - **format** - Event output format. Make sure this is set to SEF (Sidewinder Export Format used by Sidewinder G2 Security Reporter). For example, syslog(local0 filters["NULL"] SEF)
4. Open the **syslogd.conf** file in a text editor and modify the default burb entry (log_burb[0]) to the correct burb.
 5. Navigate to the location **/etc/**.
 6. Open the **syslog.conf** file in a text editor and add the following line to the file:

facility.* @x.x.x.x

where,

- **facility** - Facility level you specified in same facility as mentioned above
- **x.x.x.x** - IP address of the remote Syslog Server (i.e., EventTracker's Machine IP)

For example, *local0.* @10.2.1.149*

7. Restart the auditing and syslog daemons by completing the following steps:
 - a. Find the **Syslog Process Identifier** (PID) using the **pss syslog** command.
 - b. Restart the syslogd and audit processes by using the following commands:

```
kill syslogpid
```

```
ind Slog /usr/sbin/syslogd -l
```

```
cf server restart auditd
```

Configure Sidewinder v 6.2.x

1. Make sure that the auditing and syslog daemons are stopped on the Sidewinder host machine.
2. Navigate to the location **/etc/sidewinder/**.
3. Open **auditd.conf** file in a text editor and add the following line to the end of the file: **syslog(facilityfilters["filter"] format)** where,
 - **facility** - Facility level associated with the Syslog message (e.g., local0-local7)
 - **filter** - Name of the sacap filter to use for all the events. If this parameter is set to NULL, then all audit events are reported to the log.
 - **format** - Event output format. Make sure this is set to SEF (Sidewinder Export Format used by Sidewinder G2 Security Reporter).

For example, *syslog(local0 filters["NULL"] SEF)*

4. Navigate to the location **/etc/**.
5. Open the **syslog.conf** file in a text editor and add the following line to the file:

facility. @x.x.x.x* where,

- **facility** - Facility level you specified in same facility as mentioned above
- **x.x.x.x** - IP address of the remote Syslog Server (i.e., EventTracker's Machine IP)

For example, *local0.* @10.2.1.149*

6. Restart the auditing and syslog daemons by completing the following steps:
 - a. Find the **Syslog Process Identifier (PID)** using the **pss** syslog command.
 - b. Restart the **syslogd** and audit processes by using the following commands:

```
kill -HUP syslogpid
```

```
nd Slog /usr/sbin/syslogd -l
```

```
cf server restart auditd
```

Configure Sidewinder version 7.0

1. Make sure that auditing and syslog daemons are stopped on Sidewinder host machine.
2. Navigate to the location **/secureos/etc/**.
3. Open **auditd.conf** file in a text editor and add the following line to the end of the file **syslog(*facility*filters["*filter*"] *format*)** where,
 - **facility** - Facility level associated with the Syslog message (e.g., local0-local7)
 - **filter** - Name of the sacap filter to use for all the events. If this parameter is set to NULL, then all audit events are reported to the log.
 - **format** - Event output format. Make sure this is set to SEF (Sidewinder Export Format used by Sidewinder G2 Security Reporter). For example, syslog(local0 filters["NULL"] SEF)
4. Navigate to the location **/etc/**.
5. Open the **syslog.conf** file in a text editor and add the following line to the file:

```
facility.* @x.x.x.x where,
```

- **facility** - Facility level you specified in same facility as mentioned above
- **x.x.x.x** - IP address of the remote Syslog Server (i.e., EventTracker's Machine IP)

For example, *local0.* @10.2.1.149*

6. Within the **syslog.conf** file by changing this line from

```
*.notice;auth,...uucp.none /var/logmessages
```

to

```
*.notice;auth,...uucp,facility.none /var/logmessages
```

Changing this line prevents redundant logging.

7. Restart auditing and syslog daemons using the following commands:

```
cf daemon restart agent=syslog
```

```
cf daemon restart agent=auditd
```


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 Sidewinder Firewall monitoring.

Categories

- **McAfee Sidewinder: Access violation** - This category based report provides information related to the access violation.
- **McAfee Sidewinder: ACL modifications** - This category based report provides information related to ACL modifications.
- **McAfee Sidewinder: Application defense log** - This category based report provides information related to application defense log.
- **McAfee Sidewinder: Attack detection** - This category based report provides information related to attack detection.
- **McAfee Sidewinder: Blackhole message detection** - This category based report provides information related to blackhole message detection.
- **McAfee Sidewinder: DNS requests log** - This category based report provides information related to DNS requests log.
- **McAfee Sidewinder: Generic messages** - This category based report provides information related to generic messages.
- **McAfee Sidewinder: Hardware/Software failure** - This category based report provides information related to Hardware/Software failure.
- **McAfee Sidewinder: Health monitoring** - This category based report provides information related to the health monitoring.
- **McAfee Sidewinder: HTTP requests** - This category based report provides information related to HTTP requests.
- **McAfee Sidewinder: IP filter traffic** - This category based report provides information related to IP filter traffic.

- **McAfee Sidewinder: License exceeded** - This category based report provides information related to license exceeded.
- **McAfee Sidewinder: Log overflow** - This category based report provides information related to log overflow.
- **McAfee Sidewinder: Mail messages rejected** - This category based report provides information related to mail messages rejected.
- **McAfee Sidewinder: MIME/Virus detected** - This category based report provides information related to MIME/Virus detected.
- **McAfee Sidewinder: Network access control allowed** - This category based report provides information related to network access control being allowed or not.
- **McAfee Sidewinder: Network access control violation** - This category based report provides information related to network access control violation.
- **McAfee Sidewinder: Network traffic log** - This category based report provides information related to network traffic log.
- **McAfee Sidewinder: Protocol violation** - This category based report provides information related to protocol violation.
- **McAfee Sidewinder: Proxy flooded** - This category based report provides information related to proxy flooded.
- **McAfee Sidewinder: Proxy/Server authentication** - This category based report provides information related to Proxy/Server authentication.
- **McAfee Sidewinder: SNMP trap alert log** - This category based report provides information related to SNMP trap alert log.
- **McAfee Sidewinder: SWEDE configuration change** - This category based report provides information related to SWEDE configuration change.
- **McAfee Sidewinder: UDP traffic dropped** - This category based report provides information related to UDP traffic dropped.
- **McAfee Sidewinder: UPS logs** - This category based report provides information related to UPS logs.
- **McAfee Sidewinder: User database modifications** - This category based report provides information related to User database modifications.

- **McAfee Sidewinder: VPN traffic log** - This category based report provides information related to VPN traffic log.

Alerts

- **McAfee Sidewinder: Access violation** - This alert is generated when access violation occurs.
- **McAfee Sidewinder: ACL modifications** - This alert is generated when ACL modifications occur.
- **McAfee Sidewinder: Attack detection** - This alert is generated when attack detection occurs.
- **McAfee Sidewinder: Hardware/Software failure** - This alert is generated when Hardware/Software failure occurs.
- **McAfee Sidewinder: License exceeded** - This alert is generated when license is exceeded.

Import McAfee Sidewinder Knowledge Pack in EventTracker

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

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

Import Category

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

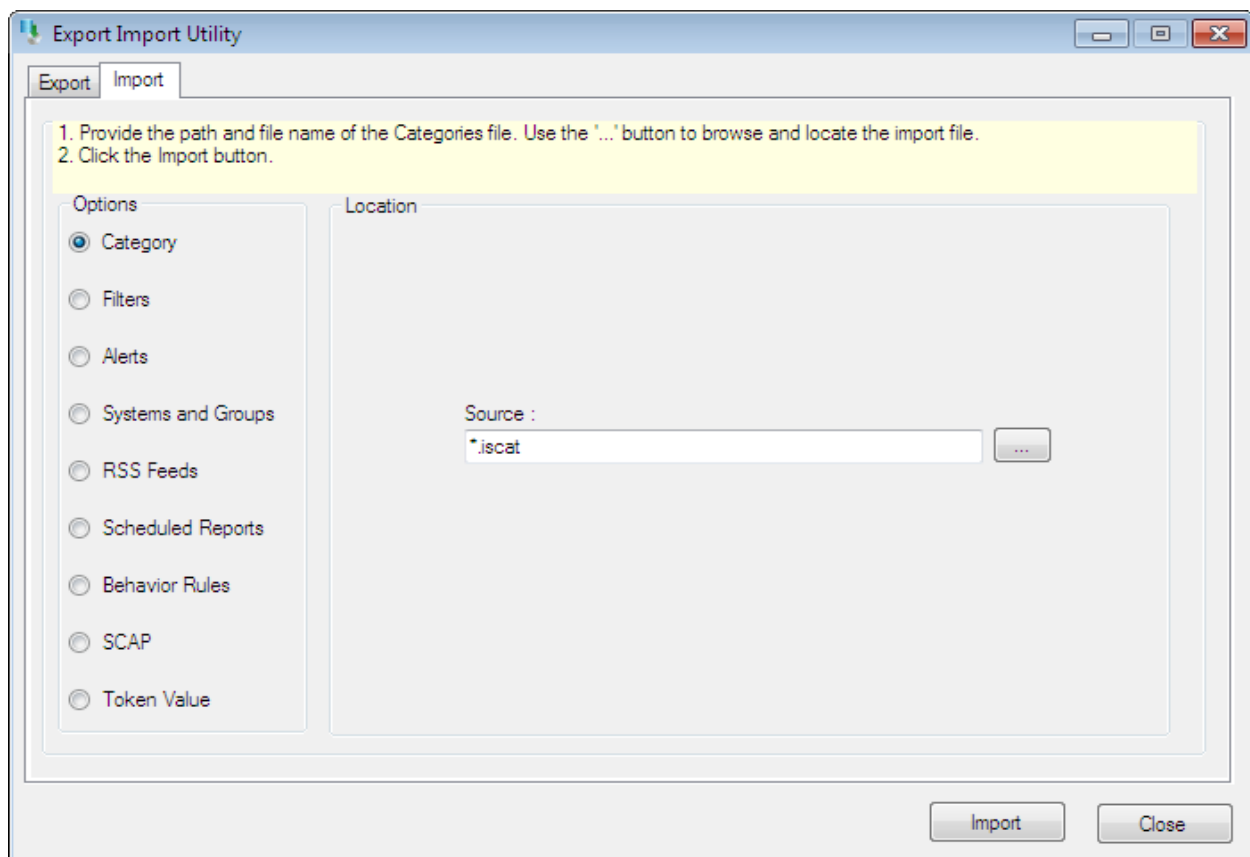


Figure 1

2. Locate **All McAfee Sidewinder group of Categories.iscat** file, and then click the **Open** button.

3. To import the categories, click the **Import** button.

EventTracker displays success message.

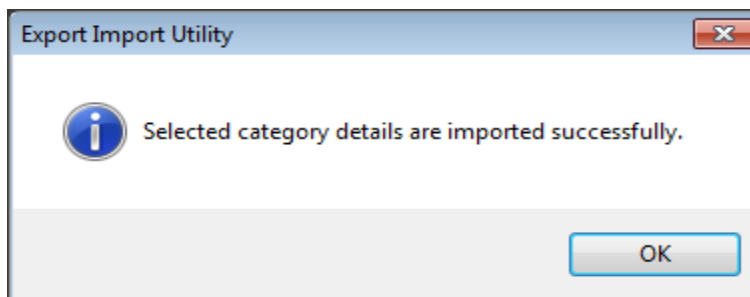


Figure 2

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

Import Alerts

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

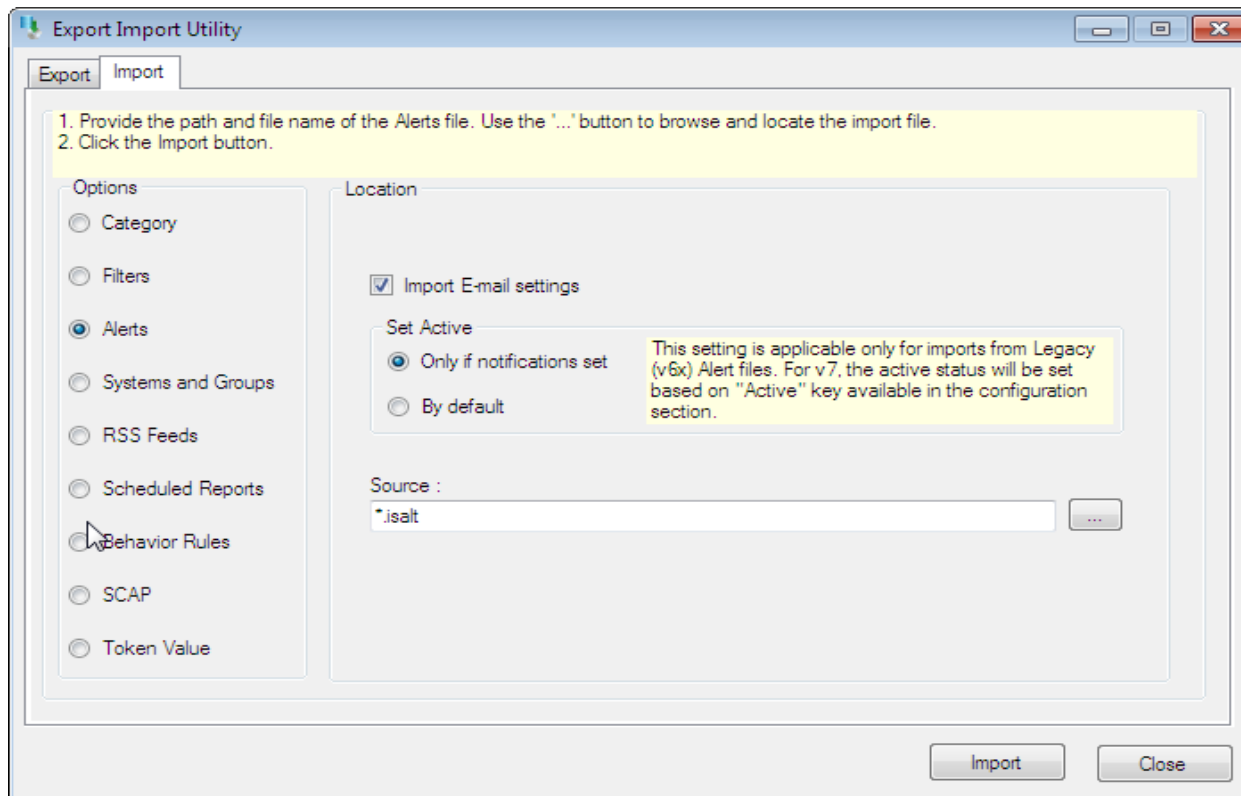


Figure 3

2. Locate **All McAfee Sidewinder group of Alerts.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

EventTracker displays success message.

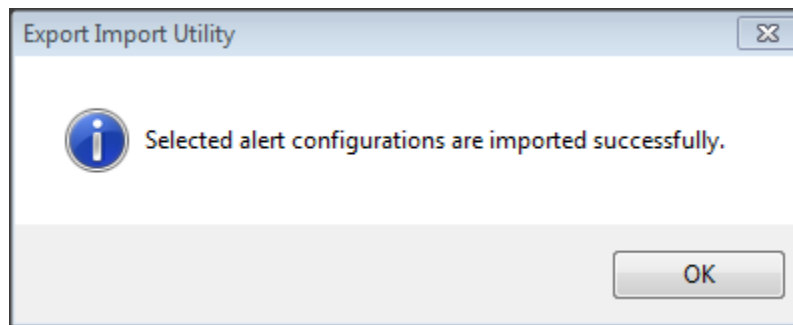


Figure 4

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

Verify McAfee Sidewinder knowledge pack in EventTracker

Verify McAfee Sidewinder Firewall Categories

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

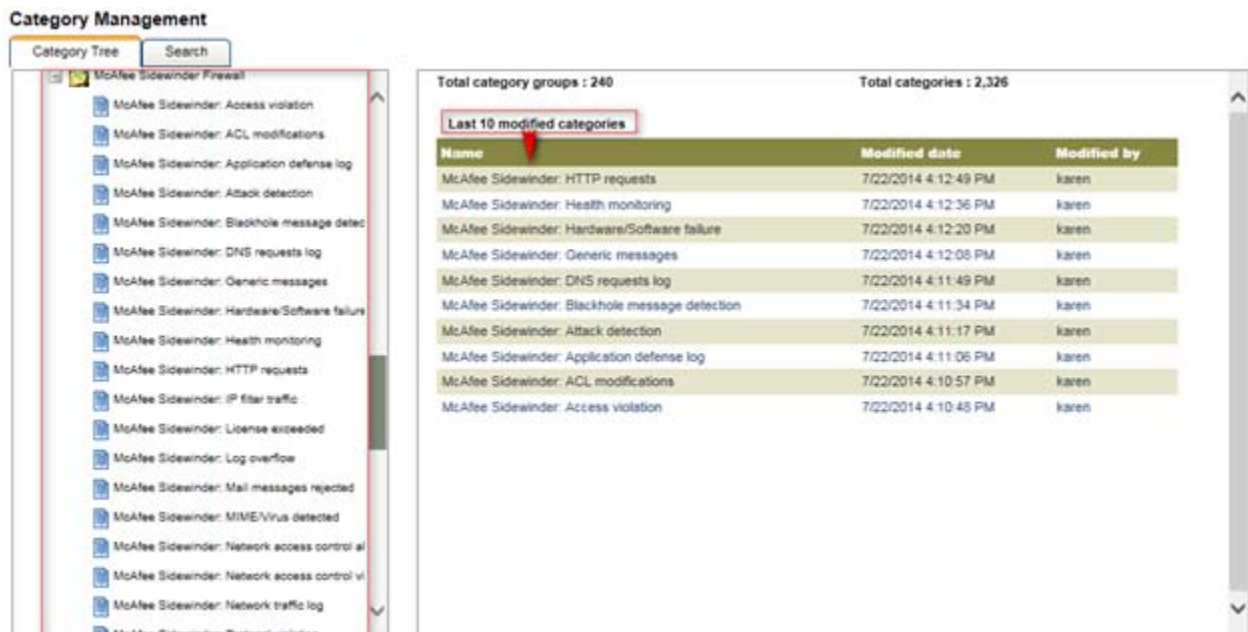
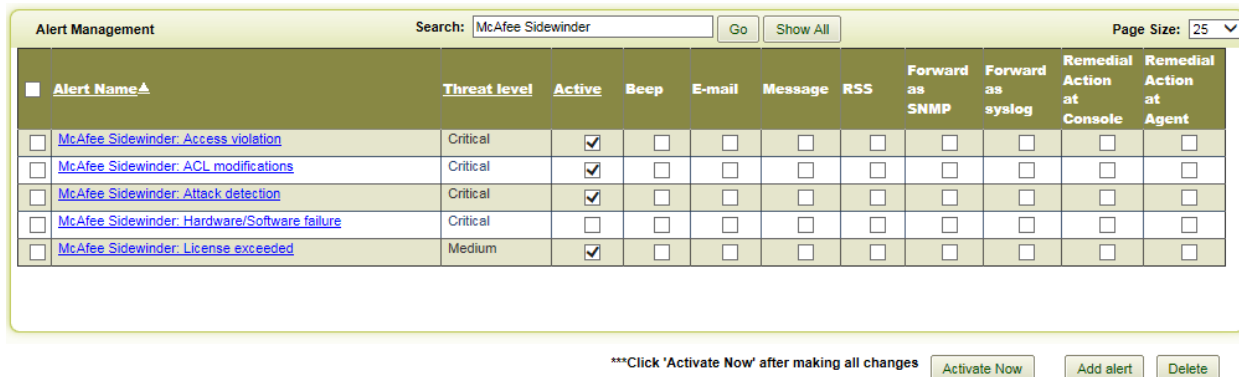


Figure 7

Verify McAfee Sidewinder Firewall Alerts

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

Alert Management page will display all the imported McAfee Sidewinder Firewall alerts.



Alert Management Search: McAfee Sidewinder 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 Sidewinder: Access violation	Critical	<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 type="checkbox"/> McAfee Sidewinder: ACL modifications	Critical	<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 type="checkbox"/> McAfee Sidewinder: Attack detection	Critical	<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 type="checkbox"/> McAfee Sidewinder: Hardware/Software failure	Critical	<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 Sidewinder: License exceeded	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"/>

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

Activate Now Add alert Delete

Figure 8

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

EventTracker displays message box.

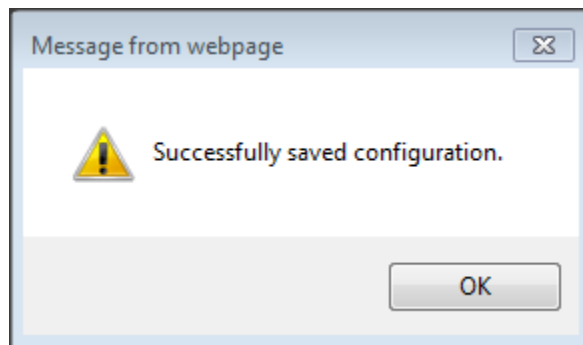


Figure 9

- Click **OK**, 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.