Integrate Sophos UTM

EventTracker v7.x

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

Publication Date: April 6, 2015

Abstract

This guide provides instructions to configure Sophos UTM 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 Sophos UTM 9 and later.

Audience

Sophos UTM 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.

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.

Table of Contents

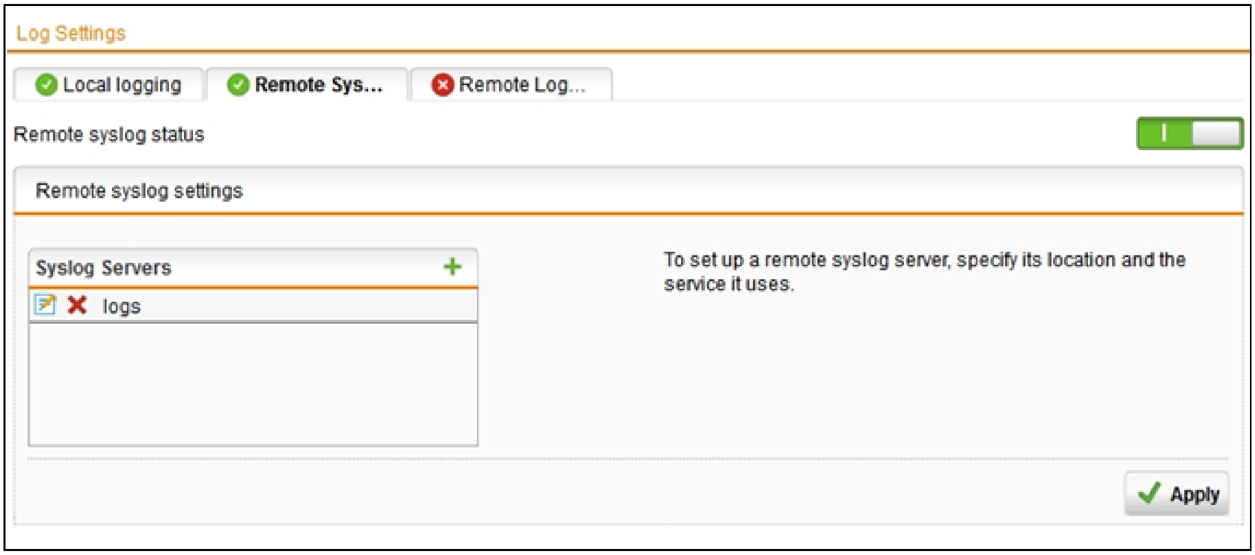
Prerequisites

- EventTracker should be installed
- Sophos UTM 9 and later should be installed and configured

Integrate EventTracker with Sophos UTM

To configure logging for Sophos UTM proceed as follows:

- Logon to the WebAdmin of the UTM
- Navigate to **Logging & Reporting > Log Settings > Remote Syslog Server**
- Activate the Remote Syslog status
- Configure a Syslog server
  - **Name:** freely selectable
  - **Server:** IP or hostname of your Syslog server EventTracker Enterprise
  - **Port:** UDP 514
- Click on Apply

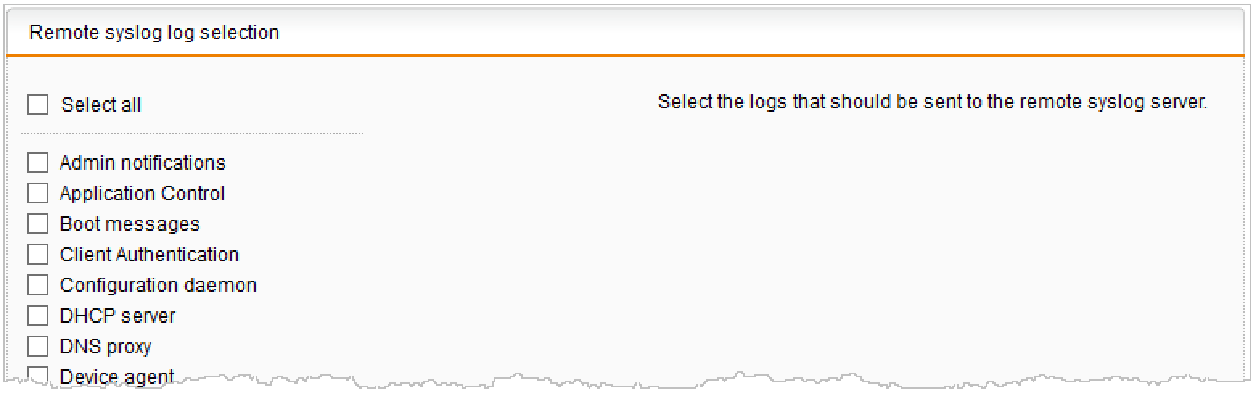


To set up a remote syslog server, specify its location and the service it uses.

Figure 01

If syslog messages cannot be delivered, they will be buffered, and re-send when possible. By default, up to 1000 logs will be buffered.

Once Syslog targets have been configured the logs to send via syslog must also be selected on the same screen. By default, none are selected. Select the desired logs, and click 'Apply'.



Remote syslog log selection

□ Select all

Select the logs that should be sent to the remote syslog server.

□ Admin notifications
□ Application Control
□ Boot messages
□ Client Authentication
□ Configuration daemon
□ DHCP server
□ DNS proxy
□ Device agent

Figure 01

To determine which logs are desired, you can view complete log contents and watch logs in real-time, under **'Logging & Reporting' > 'View Log Files'**.

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.x to support Sophos UTM monitoring:

Alerts:-

- **Sophos UTM: User authentication failure -** This alert is generated when user authentication failure occurs.
- **Sophos UTM: Shell password changed -** This alert is generated when shell password has been changed.
- **Sophos UTM: Object changed -** This alert is generated when object changed.
- **Sophos UTM: Object deleted -** This alert is generated when object deleted**.**
- **Sophos UTM: Node changed -** This alert is generated when node changed.

Reports:-

- **Sophos UTM: User Authentication Success -** This flex report provides information related to user authentication success.
- **Sophos UTM: Shell Password Changed -** This flex report provides information related to shell password changed by someone.
- **Sophos UTM: Packet Dropped -** This flex report provides information related to packet data dropped. It gives the information on which interface packet dropped.
- **Sophos UTM: Packet Accepted -** This flex report provides information related to packet data accepted. It gives the information on which interface packet accepted.
- **Sophos UTM: Object Created -** This flex report provides information related to object created .It gives the object name which has been created and who has created.
- **Sophos UTM: Object Changed -** This flex report provides information related to object changed. It gives information which object has been changed by who.
- **Sophos UTM: Object Deleted -** This flex report provides information related to object deleted. It gives information which object has been deleted by who.

- **Sophos UTM: Node Changed -** This flex report provides information related to node changed. It gives information what node has been changed by who.

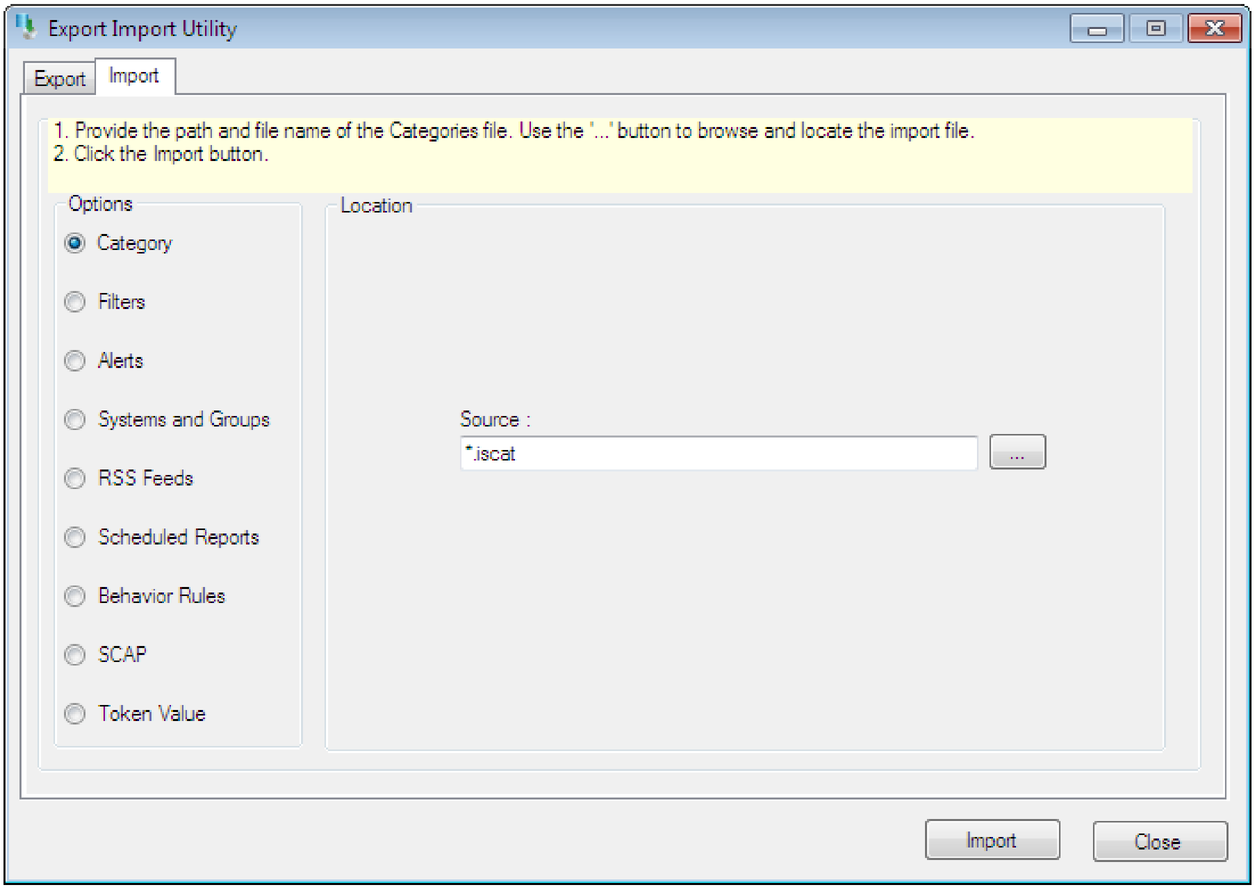
Import Sophos UTM Knowledge Pack into EventTracker

1. Launch **EventTracker Control Panel**.
2. Double click **Import Export Utility**, and then click the **Import** tab.

   Import **Category, Alert, Tokens** and **Flex Reports** as given below.

Import Category

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



1. Provide the path and file name of the Categories file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

● Category
○ Filters
○ Alerts
○ Systems and Groups
○ RSS Feeds
○ Scheduled Reports
○ Behavior Rules
○ SCAP
○ Token Value

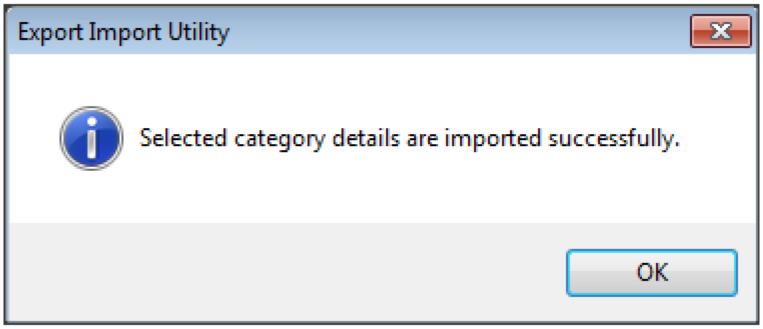
Source : *.iscat ...

Figure 03

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

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

   EventTracker displays success message.



Export Import Utility

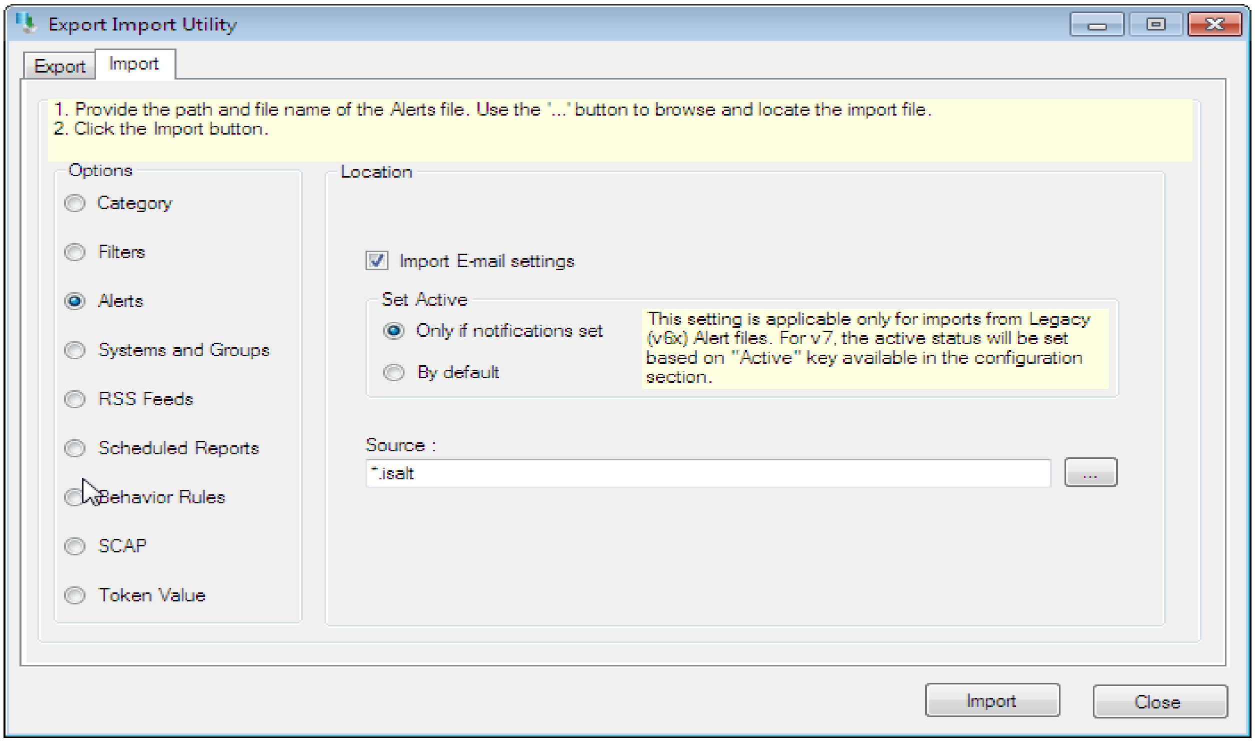
Selected category details are imported successfully.

Figure 04

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

Import Alerts

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



Export Import Utility

1. Provide the path and file name of the Alerts file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options

○ Category
○ Filters
● Alerts
○ Systems and Groups
○ RSS Feeds
○ Scheduled Reports
○ Behavior Rules
○ SCAP
○ Token Value

Location

☑ Import E-mail settings

Set Active

● Only if notifications set
○ By default

This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

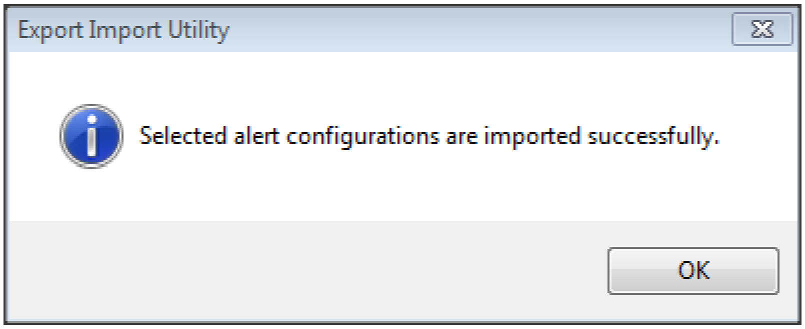
Source : *.isalt

Figure 05

2. Locate **All Sophos UTM group of Alerts.isalt** file, and then click the **Open** button.

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

   EventTracker displays success message.



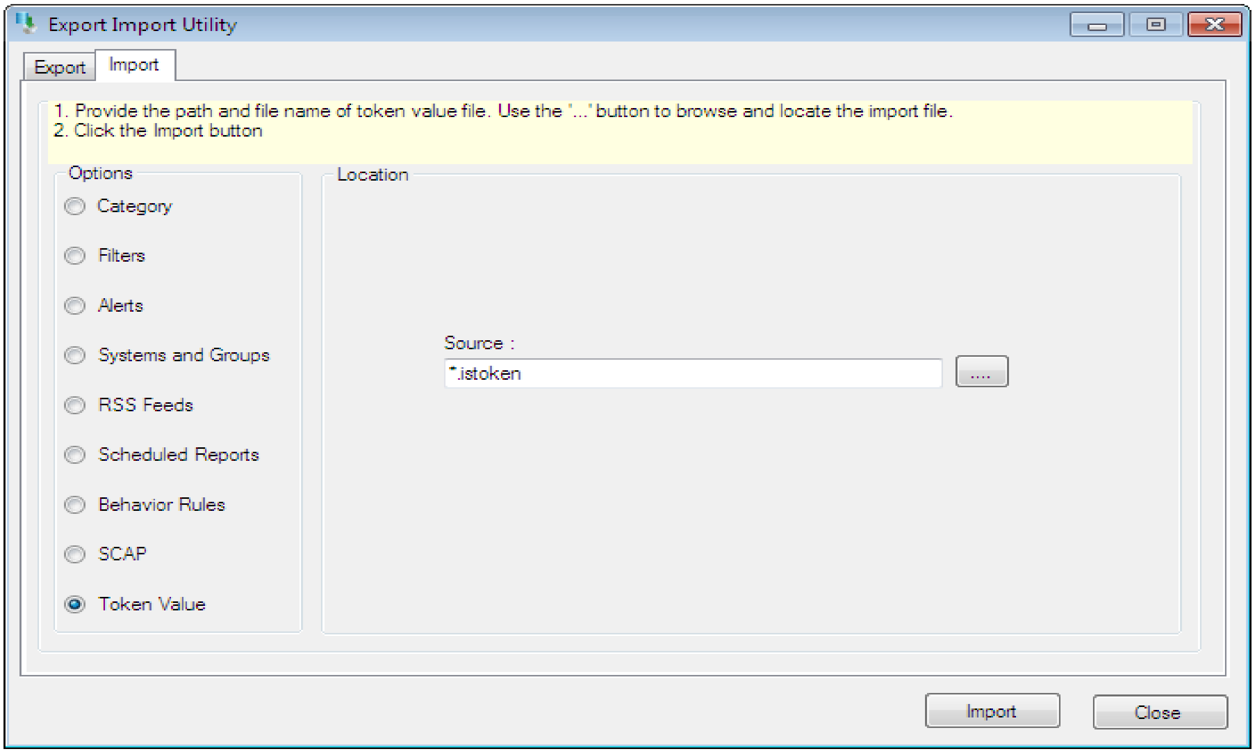
Selected alert configurations are imported successfully.

Figure 06

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

Import Tokens

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



1. Provide the path and file name of token value file. Use the '...' button to browse and locate the import file.
2. Click the Import button

○ Category
○ Filters
○ Alerts
○ Systems and Groups
○ RSS Feeds
○ Scheduled Reports
○ Behavior Rules
○ SCAP
● Token Value

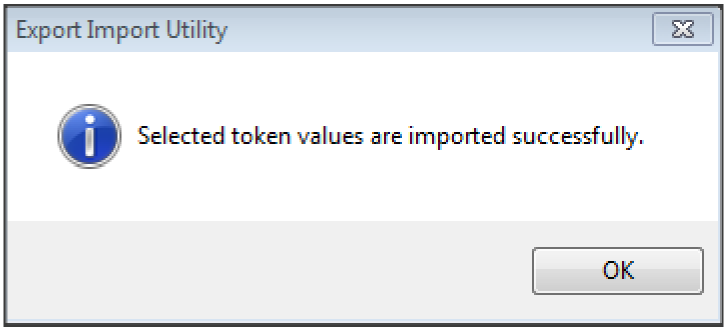
Source : *.istoken

Figure 07

2. Locate **All Sophos group of Tokens.istoken** file, and then click the **Open** button.

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

   EventTracker displays success message.



Export Import Utility

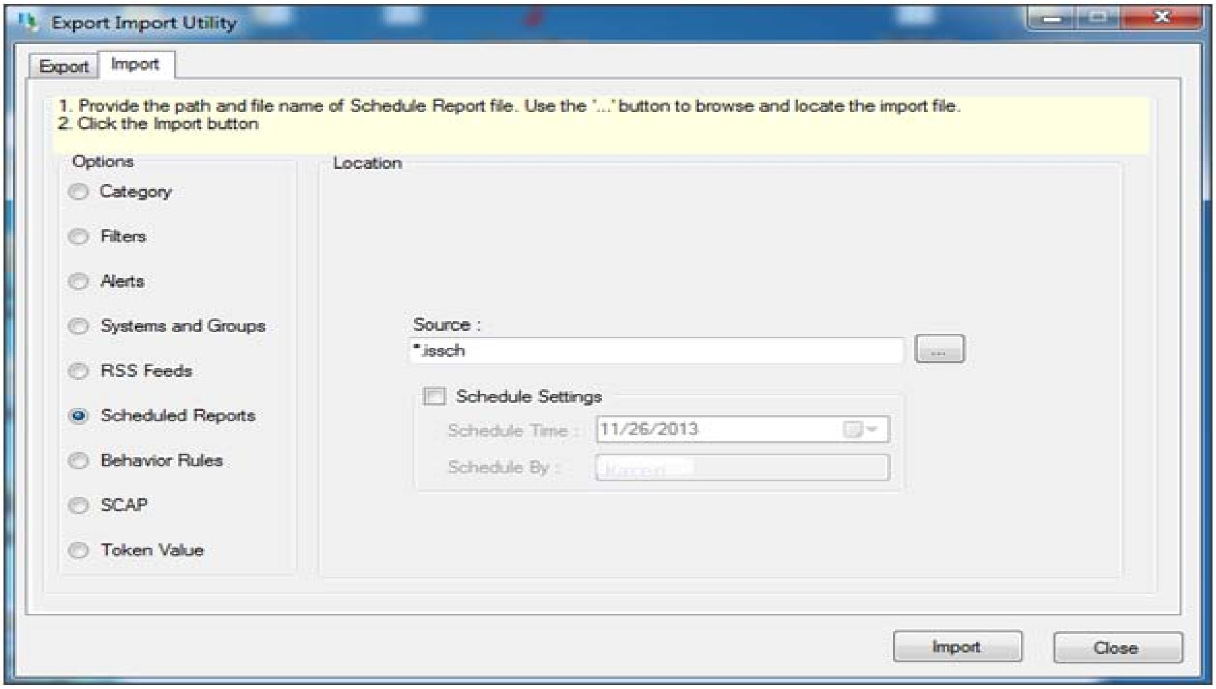
Selected token values are imported successfully.

Figure 08

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

Import Flex Reports

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



Export Import Utility

1. Provide the path and file name of Schedule Report file. Use the '...' button to browse and locate the import file.
2. Click the Import button

Options

○ Category

○ Filters

○ Alerts

○ Systems and Groups

○ RSS Feeds

● Scheduled Reports

○ Behavior Rules

○ SCAP

○ Token Value

Location

Source : *.issch

□ Schedule Settings

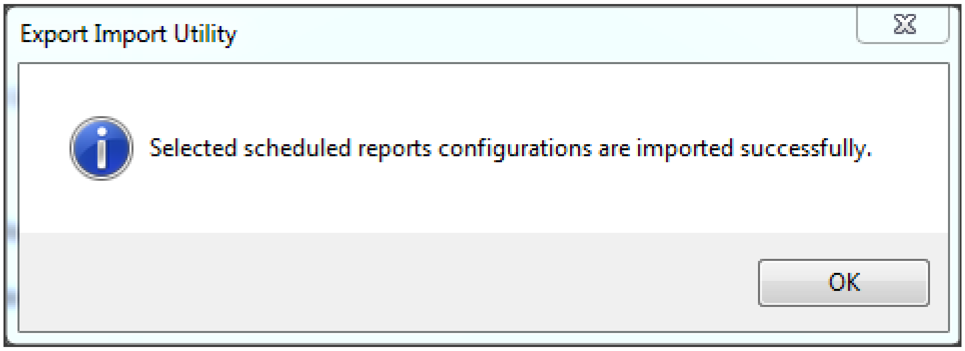
Schedule Time : 11/26/2013

Schedule By :

Figure 09

2. Locate **All Sophos UTM group of Flex Report.issch** file, and then click the **Open** button.
3. To import scheduled reports, click the **Import** button.

   EventTracker displays success message.



Selected scheduled reports configurations are imported successfully.

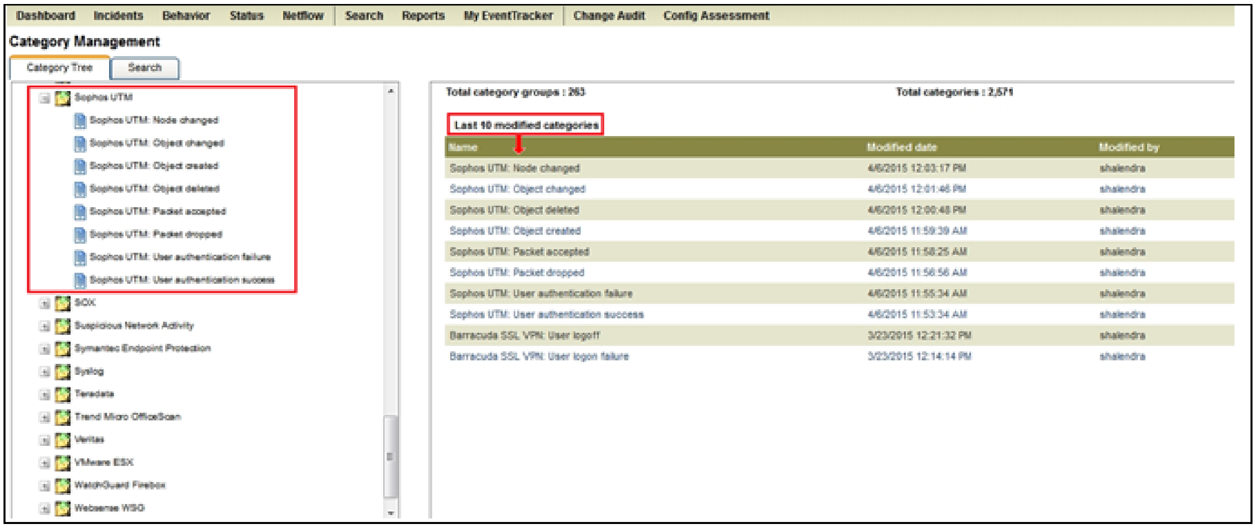
Figure 10

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

Verify Sophos UTM knowledge pack in EventTracker

Verify Sophos UTM Categories

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


Dashboard
Incidents
Behavior
Status
Netflow
Search
Reports
My EventTracker
Change Audit
Config Assessment
Category Management
Category Tree
Search
Sophos UTM
Sophos UTM: Node changed
Sophos UTM: Object changed
Sophos UTM: Object created
Sophos UTM: Object deleted
Sophos UTM: Packet accepted
Sophos UTM: Packet dropped
Sophos UTM: User authentication failure
Sophos UTM: User authentication success
SOX
Suspicious Network Activity
Symantec Endpoint Protection
Syslog
Teradata
Trend Micro OfficeScan
Veritas
VMware ESX
WatchGuard Firebox
Websense WSG

Total category groups : 263 Total categories : 2,571

Last 10 modified categories

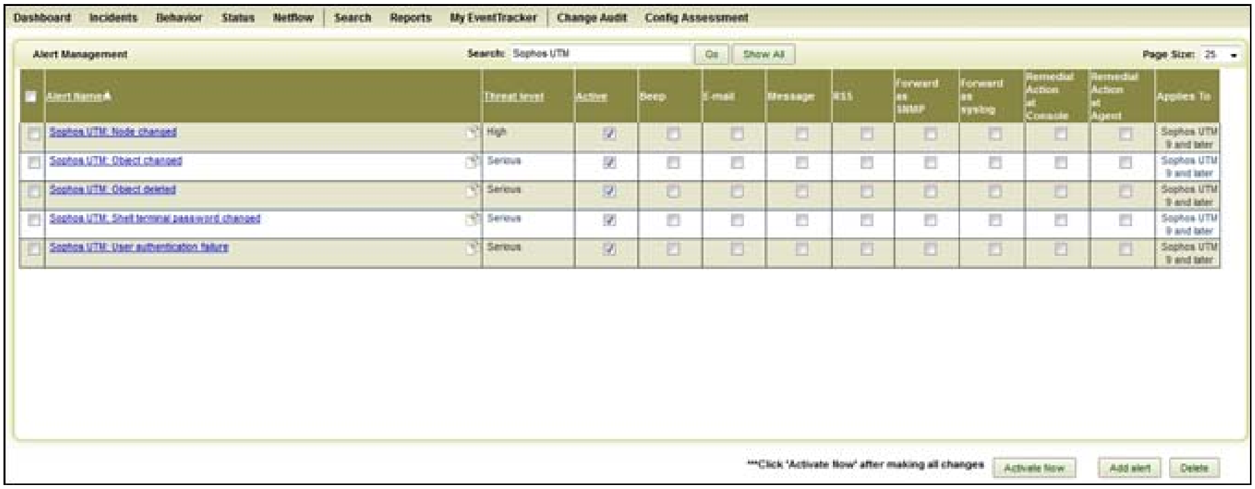
Name	Modified date	Modified by
Sophos UTM: Node changed	4/6/2015 12:03:17 PM	shalendra
Sophos UTM: Object changed	4/6/2015 12:01:46 PM	shalendra
Sophos UTM: Object deleted	4/6/2015 12:00:48 PM	shalendra
Sophos UTM: Object created	4/6/2015 11:59:39 AM	shalendra
Sophos UTM: Packet accepted	4/6/2015 11:58:25 AM	shalendra
Sophos UTM: Packet dropped	4/6/2015 11:56:56 AM	shalendra
Sophos UTM: User authentication failure	4/6/2015 11:55:34 AM	shalendra
Sophos UTM: User authentication success	4/6/2015 11:53:34 AM	shalendra
Barracuda SSL VPN: User logoff	3/23/2015 12:21:32 PM	shalendra
Barracuda SSL VPN: User logon failure	3/23/2015 12:14:14 PM	shalendra

Figure 11

Verify Sophos UTM Alerts

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

   Alert Management page will display all the imported Sophos UTM alerts.



Search: Sophos UTM

Page Size: 25

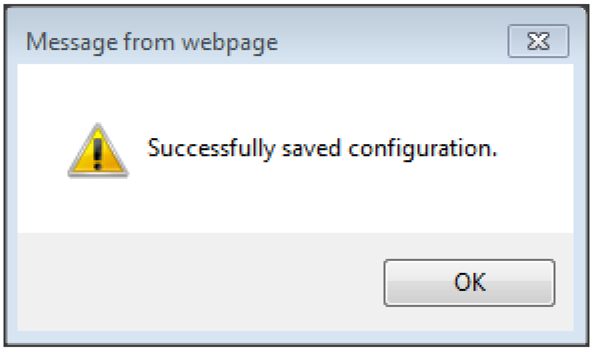
□	Alert Name▲	Threat level	Active	Beep	E-mail	Message	RSS	Forward as SNMP	Forward as syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
□	Sophos UTM: Node changed	High	☑	□	□	□	□	□	□	□	□	Sophos UTM 9 and later
□	Sophos UTM: Object changed	Serious	☑	□	□	□	□	□	□	□	□	Sophos UTM 9 and later
□	Sophos UTM: Object deleted	Serious	☑	□	□	□	□	□	□	□	□	Sophos UTM 9 and later
□	Sophos UTM: Shell terminal password changed	Serious	☑	□	□	□	□	□	□	□	□	Sophos UTM 9 and later
□	Sophos UTM: User authentication failure	Serious	☑	□	□	□	□	□	□	□	□	Sophos UTM 9 and later

**Click 'Activate Now' after making all changes

Figure 12

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

EventTracker displays message box.



Successfully saved configuration.

Figure 13

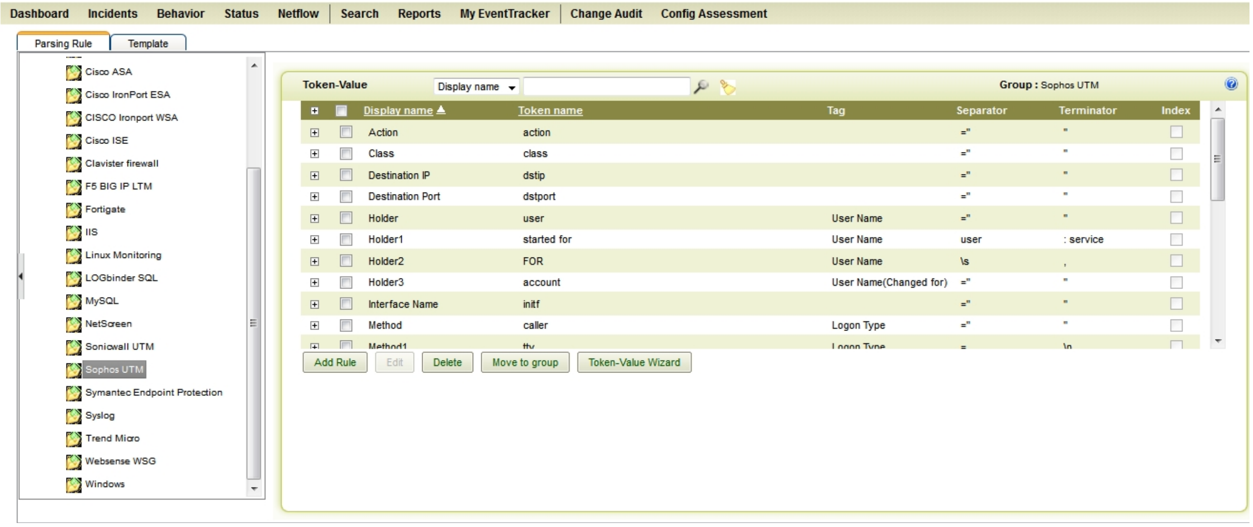
5. Click the **OK** button, and then click the **Activate now** button.

   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 Sophos UTM Tokens

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

   The imported Sophos UTM tokens are added in Token-Value Groups list. Please refer Figure 13.



Group : Sophos UTM

⊞	□	Display name ▲	Token name	Tag	Separator	Terminator	Index
⊞	□	Action	action		="	"	□
⊞	□	Class	class		="	"	□
⊞	□	Destination IP	dstip		="	"	□
⊞	□	Destination Port	dstport		="	"	□
⊞	□	Holder	user	User Name	="	"	□
⊞	□	Holder1	started for	User Name	user	: service	□
⊞	□	Holder2	FOR	User Name	\s	,	□
⊞	□	Holder3	account	User Name(Changed for)	="	"	□
⊞	□	Interface Name	initf		="	"	□
⊞	□	Method	caller	Logon Type	="	"	□
⊞	□	Method1	tty	Logon Type	=	\n	□

Figure 14

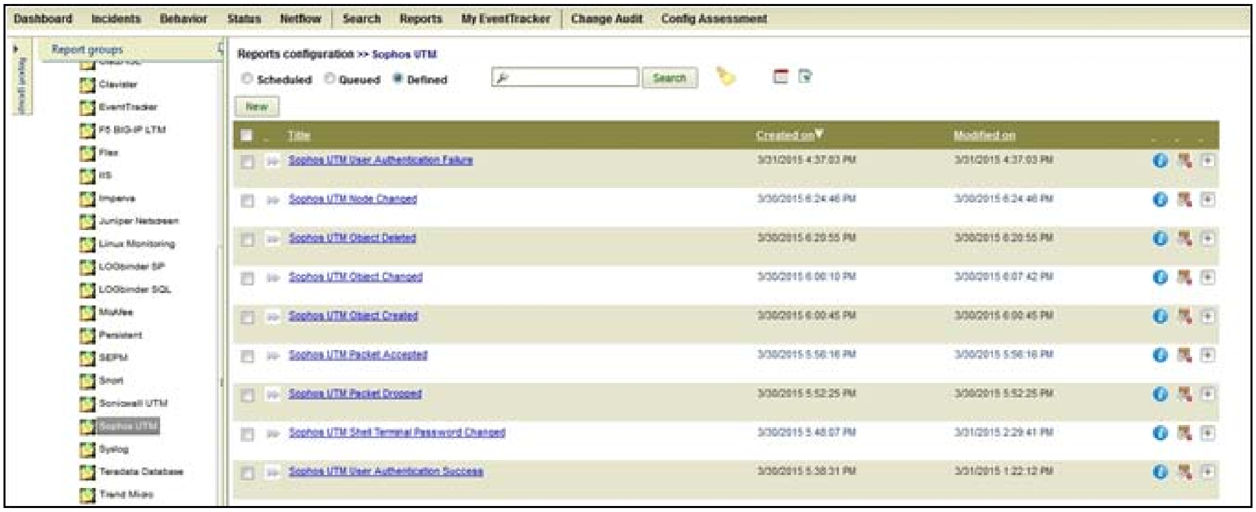
Verify Sophos UTM Flex Reports

1. Logon to **EventTracker Enterprise**.
2. Select the **Reports** menu, and then select **Configuration**.
3. In **Reports Configuration**, select **Defined** option.

   EventTracker displays **Defined** page.

4. In search box enter '**Sophos UTM**'.

   EventTracker displays Flex reports of Sophos UTM.



Reports configuration >> Sophos UTM

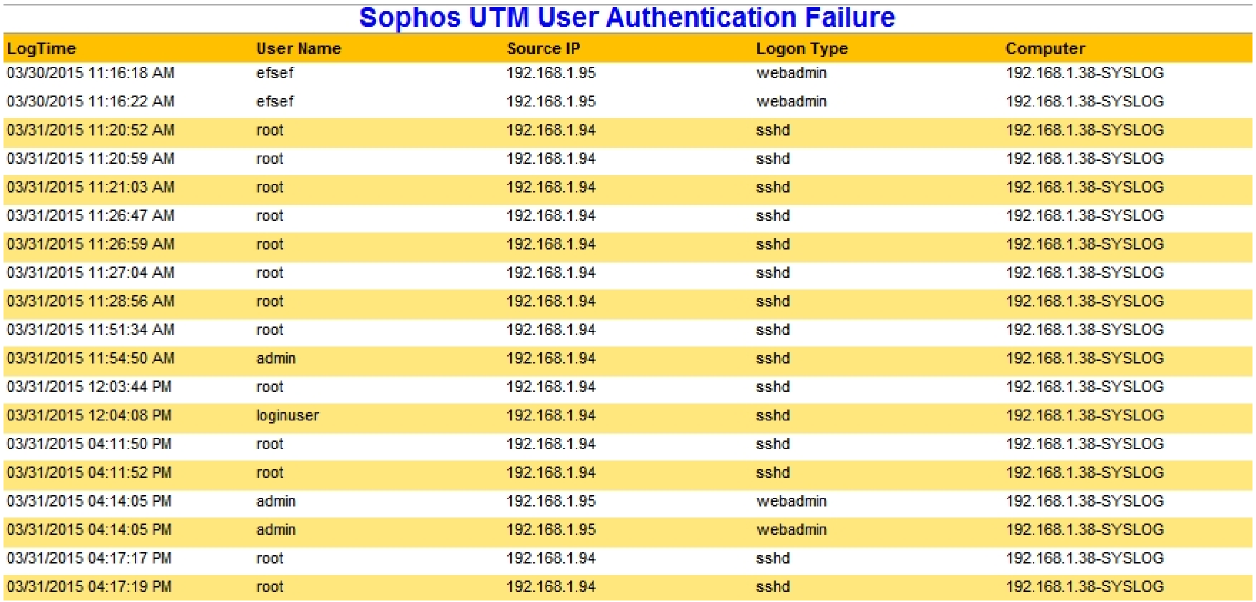
○ Scheduled ○ Queued ● Defined

Title	Created on	Modified on
Sophos UTM User Authentication Failure	3/31/2015 4:37:03 PM	3/31/2015 4:37:03 PM
Sophos UTM Node Changed	3/30/2015 6:24:46 PM	3/30/2015 6:24:46 PM
Sophos UTM Object Deleted	3/30/2015 6:20:55 PM	3/30/2015 6:20:55 PM
Sophos UTM Object Changed	3/30/2015 6:06:10 PM	3/30/2015 6:07:42 PM
Sophos UTM Object Created	3/30/2015 6:00:45 PM	3/30/2015 6:00:45 PM
Sophos UTM Packet Accepted	3/30/2015 5:56:16 PM	3/30/2015 5:56:16 PM
Sophos UTM Packet Dropped	3/30/2015 5:52:25 PM	3/30/2015 5:52:25 PM
Sophos UTM Shell Terminal Password Changed	3/30/2015 5:48:07 PM	3/31/2015 2:29:41 PM
Sophos UTM User Authentication Success	3/30/2015 5:38:31 PM	3/31/2015 1:22:12 PM

Figure 15

Sample Reports

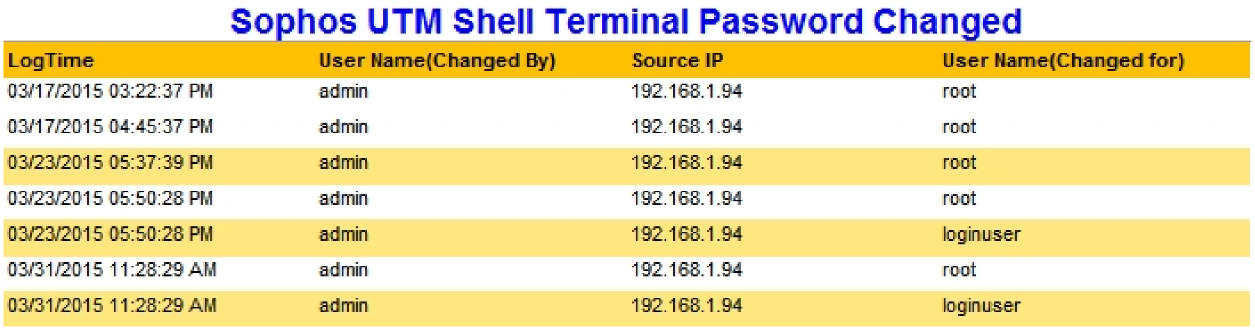
Some sample reports are given below.



Sophos UTM User Authentication Failure

LogTime	User Name	Source IP	Logon Type	Computer
03/30/2015 11:16:18 AM	efsef	192.168.1.95	webadmin	192.168.1.38-SYSLOG
03/30/2015 11:16:22 AM	efsef	192.168.1.95	webadmin	192.168.1.38-SYSLOG
03/31/2015 11:20:52 AM	root	192.168.1.94	sshd	192.168.1.38-SYSLOG
03/31/2015 11:20:59 AM	root	192.168.1.94	sshd	192.168.1.38-SYSLOG
03/31/2015 11:21:03 AM	root	192.168.1.94	sshd	192.168.1.38-SYSLOG
03/31/2015 11:26:47 AM	root	192.168.1.94	sshd	192.168.1.38-SYSLOG
03/31/2015 11:26:59 AM	root	192.168.1.94	sshd	192.168.1.38-SYSLOG
03/31/2015 11:27:04 AM	root	192.168.1.94	sshd	192.168.1.38-SYSLOG
03/31/2015 11:28:56 AM	root	192.168.1.94	sshd	192.168.1.38-SYSLOG
03/31/2015 11:51:34 AM	root	192.168.1.94	sshd	192.168.1.38-SYSLOG
03/31/2015 11:54:50 AM	admin	192.168.1.94	sshd	192.168.1.38-SYSLOG
03/31/2015 12:03:44 PM	root	192.168.1.94	sshd	192.168.1.38-SYSLOG
03/31/2015 12:04:08 PM	loginuser	192.168.1.94	sshd	192.168.1.38-SYSLOG
03/31/2015 04:11:50 PM	root	192.168.1.94	sshd	192.168.1.38-SYSLOG
03/31/2015 04:11:52 PM	root	192.168.1.94	sshd	192.168.1.38-SYSLOG
03/31/2015 04:14:05 PM	admin	192.168.1.95	webadmin	192.168.1.38-SYSLOG
03/31/2015 04:14:05 PM	admin	192.168.1.95	webadmin	192.168.1.38-SYSLOG
03/31/2015 04:17:17 PM	root	192.168.1.94	sshd	192.168.1.38-SYSLOG
03/31/2015 04:17:19 PM	root	192.168.1.94	sshd	192.168.1.38-SYSLOG

Figure 16



Sophos UTM Shell Terminal Password Changed

LogTime	User Name(Changed By)	Source IP	User Name(Changed for)
03/17/2015 03:22:37 PM	admin	192.168.1.94	root
03/17/2015 04:45:37 PM	admin	192.168.1.94	root
03/23/2015 05:37:39 PM	admin	192.168.1.94	root
03/23/2015 05:50:28 PM	admin	192.168.1.94	root
03/23/2015 05:50:28 PM	admin	192.168.1.94	loginuser
03/31/2015 11:28:29 AM	admin	192.168.1.94	root
03/31/2015 11:28:29 AM	admin	192.168.1.94	loginuser

Figure 17