

Integrate Meraki Firewall

EventTracker v8.x and above

Abstract

This guide provides instructions to configure a Meraki Firewall to report its logs to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 8.X and later, and **Meraki security appliance MX series**.

Audience

Administrators, who wish to monitor Meraki Firewall using EventTracker Enterprise.

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

This document is for informational purposes only. Netsurion 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 Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion 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 Netsurion, 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.

© 2019 Netsurion. 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
Configure Meraki Firewall to forward logs to EventTracker	3
To configure the Meraki Firewall to forward logs to a syslog server	3
EventTracker Knowledge Pack	5
Flex Reports	5
Alerts	9
Categories and Saved searches	9
Knowledge Objects	10
Import Meraki Firewall knowledge pack into EventTracker	10
Category	11
Alerts	13
Knowledge Objects	14
Flex Reports	16
Verify Meraki Firewall knowledge pack in EventTracker	18
Categories	18
Alerts	18
Token Templates	19
Knowledge Objects	19
Flex Reports	20

Overview

Meraki Firewalls are cloud-managed network security appliances designed to make distributed networks fast, secure, manageable by employing stateful inspection and auto-configuring VPN options.

EventTracker amasses and examines logs generated by Meraki Firewall to help an administration to monitor ids, alerts, VPN sessions, web traffic etc.

Prerequisites

- Administrative access to Meraki Dashboard.

Configure Meraki Firewall to forward logs to EventTracker

To configure the Meraki Firewall to forward logs to a syslog server

In your Meraki Dashboard:

1. Go to **Network-wide**.
2. On **Configure** tab, click on **General**.

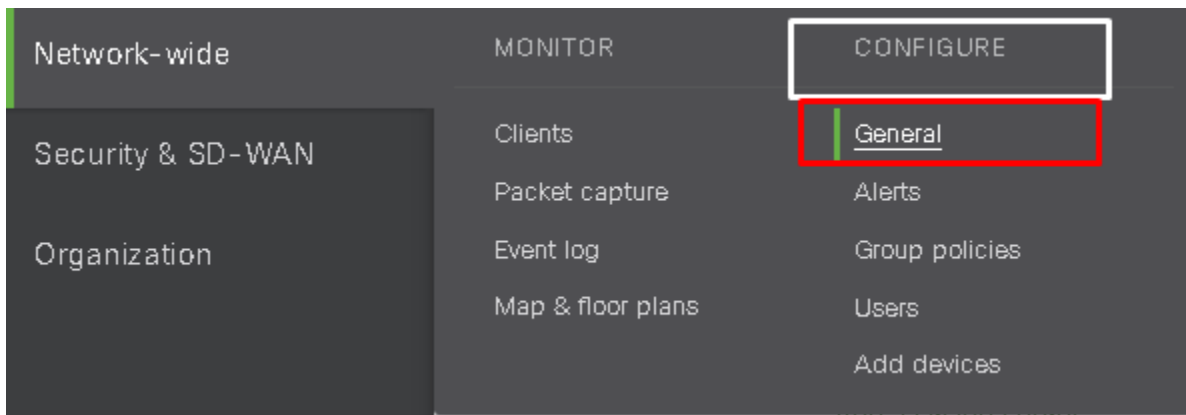


Figure 1

3. At the **General** page, scroll down to the Logging section.

Logging

Syslog servers

Server IP	Port	Roles	Actions
logger2.etagent.com	514	Flows x Appliance event log x	X
		Flows	
		URLs	
		Appliance event log	

[Add a syslog server](#)

Figure 2

- Click the **Add a syslog server** link to define a new server.
- Click on the **Add a syslog server** link and type the IP address or name of **EventTracker Manager** in **Server IP** field.
- Type **Eventtracker Manager Port** in the **Port** field.
- Choose **Appliance event Log, Security events, IDS Alerts, Flows and URLs**; in **Roles** field. Mentioned log types are detailed below:

Reporting

Syslog servers

Server IP	Port	Roles	Actions
logger2.etagent.com	514	Flows x URLs x Security events x Appliance event log x	X

Figure 3

- Click **Save Changes** at the bottom of the page.

Save Changes or [cancel](#)

(Please allow 1-2 minutes for changes to take effect.)

Figure 4

Integrated device can be verified in the Systems pane of EventTracker advanced log search.

EventTracker Knowledge Pack

Once logs are received into EventTracker Categories, Alerts, Reports and Dashboards can be configured into EventTracker. The following Knowledge Packs are available in EventTracker to support Meraki Firewall monitoring.

Flex Reports

- **Meraki Firewall- Blocked web content details:** This report provides information related to web content blocked by content filter.

Report Sample:

LogTime	Device Name	Server Address	Server Port	Blocked Category	Blocked URL
03/30/2016 07:53:40 PM	MX64	174.76.226.93	80	User-defined Blacklist	http://img2.imagesbn.com/p/2940043877833_p0_v2_s600_e404.png;
03/30/2016 07:53:49 PM	MX64	184.105.82.3	443	User-defined Blacklist	https://*.cloudmosa.com/...
03/30/2016 07:54:01 PM	MX64	67.215.65.130	80	Proxy Avoidance and Anonymizers	http://q99.info/wp-content/uploads/2013/12/posted-the-wizard-saturday-july-48090.jpg;
04/01/2016 04:54:48 PM	MX64	52.86.88.235	443	Dating	https://api.gotinder.com/...
04/04/2016 10:30:07 AM	MX64	174.76.226.93	80	User-defined Blacklist	http://img2.imagesbn.com/p/2940043877833_p0_v2_s600_e404.png;

Figure 5

Sample Log:

Mar 05 01:14:43 PM	<134>1 1392859398.201435382 Meraki_Security_Appliance events content_filtering_block url="https://*.contosooserver.com/..." category0="User-defined Blacklist" server="100.17.82.3:443"
event_computer	+ meraki2019
event_description	<134>1 1392859398.201435382 Meraki_Security_Appliance events content_filtering_block url="https://*.contosooserver.com/..." category0="User-defined Blacklist" server="100.17.82.3:443"
event_id	+ 3399
event_log_type	+ Application
event_source	+ syslog
event_type	+ Information
event_user_domain	+ N/A
event_user_name	+ N/A
log_source	+ Meraki Firewall Content Filter
rule_name	+ User-defined Blacklist
src_device_name	+ Meraki_Security_Appliance
src_ip_address	+ 100.17.82.3
src_port_no	+ 443
url_name	+ https://*.contosooserver.com/...
tags	+ Meraki Firewall
tags	+ Content Filter

Figure 6

- **Meraki Firewall- VPN session details:** This report provides information related to VPN sessions establishment, connection or disconnection.

Report Sample:

LogTime	Device Name	VPN Type	VPN Status	User Name	Source IP	Source Port	Destination IP	Destination Port
03/30/2016 07:10:26 PM	MX60	Site-to-site VPN	established		24.249.102.115	4500	70.168.64.32	4500
03/30/2016 07:10:36 PM	MX60	client_vpn	vpn_connect	astaubin	70.168.64.32		192.168.251.122	
03/30/2016 07:10:45 PM	MX60	client_vpn	vpn_disconnect	astaubin	70.168.64.32		192.168.251.122	

Figure 7

Sample Log:

Mar 05 01:14:43 PM	<134>1 1392808395.669667263 Meraki_Security_Appliance events Site-to-site VPN: IPsec-SA established: ESP/Transport 24.249.102.115[4500]->70.168.64.32[4500]
dest_ip_address	+ 70.168.64.32
dest_port_no	+ 4500
event_computer	+ meraki2019
event_description	<134>1 1392808395.669667263 Meraki_Security_Appliance events Site-to-site VPN: IPsec-SA established: ESP/Transport 24.249.102.115[4500]->70.168.64.32[4500]
event_id	+ 3399
event_log_type	+ Application
event_source	+ syslog
event_type	+ Information
event_user_domain	+ N/A
event_user_name	+ N/A
log_action	+ established
log_source	+ Meraki Firewall VPN
object_type	+ Site-to-site VPN
src_device_name	+ Meraki_Security_Appliance
src_ip_address	+ 24.249.102.115
src_port_no	+ 4500
tags	+ Meraki Firewall
tags	+ VPN Activities

Figure 8

- **Meraki Firewall- User authentication details:** This report provides information related to local user authentication attempt.

Report Sample:

LogTime	Device Name	Host MAC	User Name	User Details	Group Details
03/30/2016 03:36:30 PM	MX64	00:1E:0B:3E:42:DD	TTobey	CN=Tami Tobey,OU=Teachers,OU=Users - Domain,DC=eagles,DC=ocacademy,DC=org	CN=Teachers,OU=Teachers,OU=Users - Domain,DC=eagles,DC=ocacademy,DC=org
03/30/2016 03:36:43 PM	MX64	90:B1:1C:79:1C:50	JWolfe	CN=Janet Wolfe,OU=Administration,OU=Users - Domain,DC=eagles,DC=ocacademy,DC=org	CN=Administration,OU=Administration,OU=Users - Domain,DC=eagles,DC=ocacademy,DC=org
03/30/2016 03:36:54 PM	MX64	00:0B:DB:73:F1:78	student	CN=Student Guest,OU=Students,OU=Users - Domain,DC=eagles,DC=ocacademy,DC=org	CN=Students,OU=Students,OU=Users - Domain,DC=eagles,DC=ocacademy,DC=org

Figure 9

Sample Log:

Mar 05 01:24:49 PM	<134>1 1392792900.051011956 Meraki_Security_Appliance events authentication on 00:1E:0B:3E:42:DD for user Tmark as CN=ted mark,OU=lab,OU=Users - Domain,DC=contoso,DC=domain,DC=org with policy for grou...
event_computer	meraki2019
event_description	<134>1 1392792900.051011956 Meraki_Security_Appliance events authentication on 00:1E:0B:3E:42:DD for user Tmark as CN=ted mark,OU=lab,OU=Users - Domain,DC=contoso,DC=domain,DC=org with policy for grou...
event_id	3399
event_log_type	Application
event_source	syslog
event_type	Information
event_user_domain	N/A
event_user_name	N/A
log_source	Meraki Firewall Authentication Details
src_device_name	Meraki_Security_Appliance
src_mac_address	00:1E:0B:3E:42:DD
src_user_info	CN=ted mark,OU=lab,OU=Users - Domain,DC=contoso,DC=domain,DC=org
src_user_name	Tmark
tags	Meraki Firewall
tags	Authentication Activities

Figure 10

- **Meraki Firewall- DHCP IP lease details:** This report provides information related to IPs leased by DHCP.

Report Sample:

LogTime	Device Name	Server MAC	Client MAC	Leased IP	Allocated DNS	Router IP
03/31/2016 06:03:47 PM	MX60	00:18:0A:02:85:88	00:18:0A:76:F9:79	172.16.37.220	172.16.1.200, 172.16.1.1	172.16.1.2
03/31/2016 06:08:20 PM	MX60	00:18:0A:02:85:88	00:18:08:06:9F:88	172.16.37.210	172.16.1.200, 172.16.1.1	172.16.1.2

Figure 11

- **Meraki Firewall- IDS alert details:** This report provides information related to threats detected by IDS.

Report Sample:

LogTime	Device Name	Source MAC	Source IP	Source Port	Destination MAC	Destination IP	Destination Port	Protocol Type	Alert Priority	Alert Direction	Alert Details	
03/29/2016 05:45:12 PM	MX60	03:99:9D:3B:F7:C5	192.168.251.122	61724		172.16.1.90	22	tcp/ip	2	egress	(spp_ssh) Protocol mismatch	
03/29/2016 05:45:23 PM	MX60		70.168.64.32	64697	00:1B:21:A2:73:C9	172.16.1.70	6690	tcp/ip	3	ingress	Data sent on stream not accepting data	
03/29/2016 05:45:34 PM	MX60		24.249.102.115	46865		6.0.0.2	3128	tcp/ip	2		(http_inspect) NON-RFC DEFINED CHAR	
03/29/2016 05:45:43 PM	MX60		72.246.55.50	80	04:15:52:5B:60:CC	172.16.25.241	50449	tcp/ip	2	ingress	Bad segment, adjusted size <= 0	
03/29/2016 05:45:53 PM	MX60	20:C9:D0:BC:66:A3							34525	3	egress	(spp_frag3) Fragmentation overlap

Figure 12

Sample Log:

Mar 05 01:24:49 PM	1490031971.951780201 ANB_MX80 security_event ids_alerted signature=1:39867:3 priority=3 timestamp=1490031971.693691 shost=00:15:5D:1E:08:04 direction=egress protocol=udp/ip src=192.168.30.10:49243 dst=210.15....
dest_ip_address	+- 210.15.216.1:53
event_computer	+- meraki2019
event_description	1490031971.951780201 ANB_MX80 security_event ids_alerted signature=1:39867:3 priority=3 timestamp=1490031971.693691 shost=00:15:5D:1E:08:04 direction=egress protocol=udp/ip src=192.168.30.10:49243 dst=210.15.... 216.1:53 message: INDICATOR-COMPROMISE Suspicious .tk dns query
event_id	+- 3399
event_log_type	+- Application
event_source	+- syslog
event_type	+- Information
event_user_domain	+- N/A
event_user_name	+- N/A
log_datetime	+- 1490031971.693691
log_direction	+- egress
log_priority	+- 3
log_source	+- Meraki Firewall IDS
protocol_type	+- udp/ip
src_ip_address	+- 192.168.30.10:49243
src_mac_address	+- 00:15:5D:1E:08:04
threat_id	+- 1:39867:3
threat_info	+- INDICATOR-COMPROMISE Suspicious .tk dns query
tags	+- Intrusion Detected
tags	+- Intrusion Detected
tags	+- Meraki Firewall

Figure 13

- **Meraki Firewall- Web traffic details:** This report provides information related to web traffic.

Report Sample:

LogTime	Device Name	Source MAC	Source IP	Source Port	Destination IP	Destination Port	Request Type	Requested URI
03/29/2016 12:40:56 PM	MX60	00:18:0A:77:1B:D7	172.16.0.1	1	192.168.0.1	80	GET	http://192.168.3.12/fog/service/ser vicemodule- active.php?mac=00:0F:20:FE:CA:A 8&moduleid=snapin' nc -v -u -w 0 172.16.1.90 552; done
03/29/2016 12:41:07 PM	MX60	00:18:0A:77:1B:D7	172.16.4.6	52436	173.194.115.45	80	GET	http://testuser:testpassword@pag ead2.googleadsyndication.com/simga d/2675983589122411580
03/29/2016 12:41:18 PM	MX60	00:18:0A:82:4E:26	172.16.4.3	41805	74.50.59.38	443	UNKNOWN	http://dsfsd.sdf

Figure 14

Sample Log:

Mar 05 01:24:49 PM	1374543213.342705328 MX84 url=src=192.168.1.186:63735 dst=69.58.23.25:80 mac=58:1F:AA:CE:61:F2 request: GET http://bit.ly/17zTvl agent=""Go-http-client/1.1""
dest_ip_address	+- 69.58.23.25
dest_port_no	+- 80
event_computer	+- meraki2019
event_description	1374543213.342705328 MX84 url=src=192.168.1.186:63735 dst=69.58.23.25:80 mac=58:1F:AA:CE:61:F2 request: GET http://bit.ly/17zTvl agent=""Go-http-client/1.1""
event_id	+- 3399
event_log_type	+- Application
event_source	+- syslog
event_type	+- Information
event_user_domain	+- N/A
event_user_name	+- N/A
http_type	+- GET
log_source	+- Meraki Firewall Web Traffic
src_ip_address	+- 192.168.1.186
src_mac_address	+- 58:1F:AA:CE:61:F2
src_port_no	+- 63735
url_name	+- http://bit.ly/17zTvl agent=""Go-http-client/1.1""
tags	+- Web Traffic
tags	+- Meraki

Figure 15

- **Meraki Firewall- Traffic flow details:** This report provides information related to inbound and outbound traffic flow.

Report Sample:

LogTime	Device Name	Source MAC	Source IP	Source Port	Destination IP	Destination Port	Protocol Type	Rule Name
03/29/2016 11:56:40 AM	MX10		17.173.254.223	16387	24.249.102.115	1072	udp	1 all
03/29/2016 11:56:50 AM	MX10	00:18:0A:77:1B:D7	172.16.4.21	53336	74.125.193.138	443	tcp	allow all
03/29/2016 11:57:00 AM	MX60		39.41.41.56	13943	114.18.74.11	16329	udp	1 all
03/29/2016 11:57:08 AM	MX60	00:18:0A:98:L9:U7	192.168.10.254	9562	8.8.8.8	53	udp	allow all

Figure 16

Sample Log:

Mar 05 01:24:49 PM	192.168.10.1 1 948136486.721741837 MX60 flows src=192.168.10.254 dst=8.8.8.8 mac=00:18:0A:XX:XX:XX protocol=udp sport=9562 dport=53 pattern: allow all
action	+ allow all
dest_ip_address	+ 8.8.8.8
dest_port_no	+ 53
event_computer	+ meraki2019
event_description	192.168.10.1 1 948136486.721741837 MX60 flows src=192.168.10.254 dst=8.8.8.8 mac=00:18:0A:XX:XX:XX protocol=udp sport=9562 dport=53 pattern: allow all
event_id	+ 3399
event_log_type	+ Application
event_source	+ syslog
event_type	+ Information
event_user_domain	+ N/A
event_user_name	+ N/A
log_source	+ Meraki Firewall Traffic Flow
protocol_type	+ udp
src_ip_address	+ 192.168.10.254
src_mac_address	+ 00:18:0A:XX:XX:XX
src_port_no	+ 9562
tags	+ Traffic Activities
tags	+ Meraki Firewall

Figure 17

Alerts

- **Meraki Firewall: IDS alert detected** - This alert is generated when unusual traffic is detected by IDS.
- **Meraki Firewall: Suspicious content blocked** - This alert is generated when suspicious content is blocked by content filter.

Categories and Saved searches

- **Meraki Firewall: Content Filter** - This category provides information related to web content blocked by content filter.
- **Meraki Firewall: IDS** - This category provides information related to threats detected by IDS.
- **Meraki Firewall: Traffic flow** - This category provides information related to ingress and egress traffic flow.

- **Meraki Firewall: Web traffic** - This category provides information related to inbound and outbound web traffic.
- **Meraki Firewall: Authentication Details** - This category provides information related to local user authentication attempt.
- **Meraki Firewall: VPN session** - This category provides information related to VPN sessions establishment, connection or disconnection.
- **Meraki Firewall: AMP** – This category provides information related to meraki firewall advance malware protection and detection details.

Knowledge Objects

- **Meraki Firewall Advanced Malware Protection** - This knowledge object helps to analyze logs related to meraki firewall advanced malware protection.
- **Meraki Firewall Authentication Details** - This knowledge object helps to analyze logs related to user authentication and authorization activities.
- **Meraki Firewall Content Filter** - This knowledge object helps to analyze logs related to web content blocked by content filter.
- **Meraki Firewall IDS**- This knowledge object helps to analyze logs related to threats detected by IDS.
- **Meraki Firewall Traffic Flow**- This knowledge object helps to analyze logs related to network traffic flow details.
- **Meraki Firewall VPN**- This knowledge object helps to analyze logs related to VPN sessions establishment, connection or disconnection.

Import Meraki Firewall knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
 - Alerts
 - Token Templates
 - Knowledge Objects
 - Flex Reports
 - Dashboards
1. Launch **EventTracker Control Panel**.
 2. Double click **Export Import Utility**.

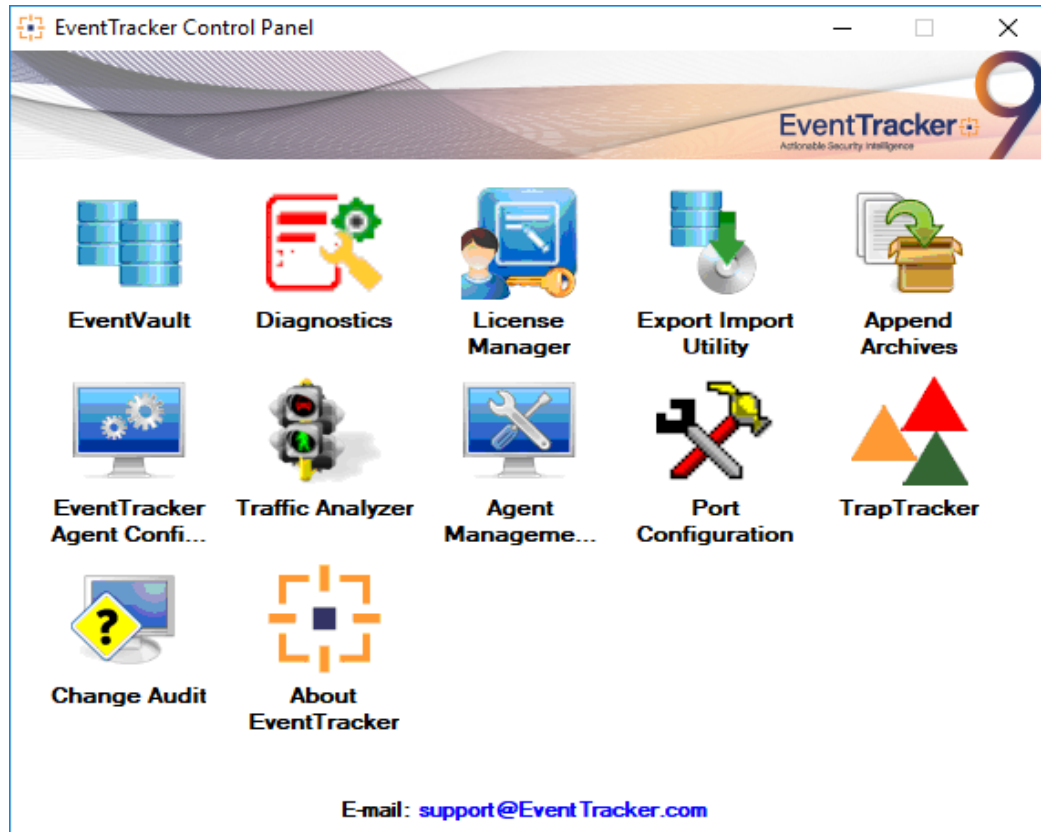



Figure 18

3. Click the **Import** tab.

Category

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

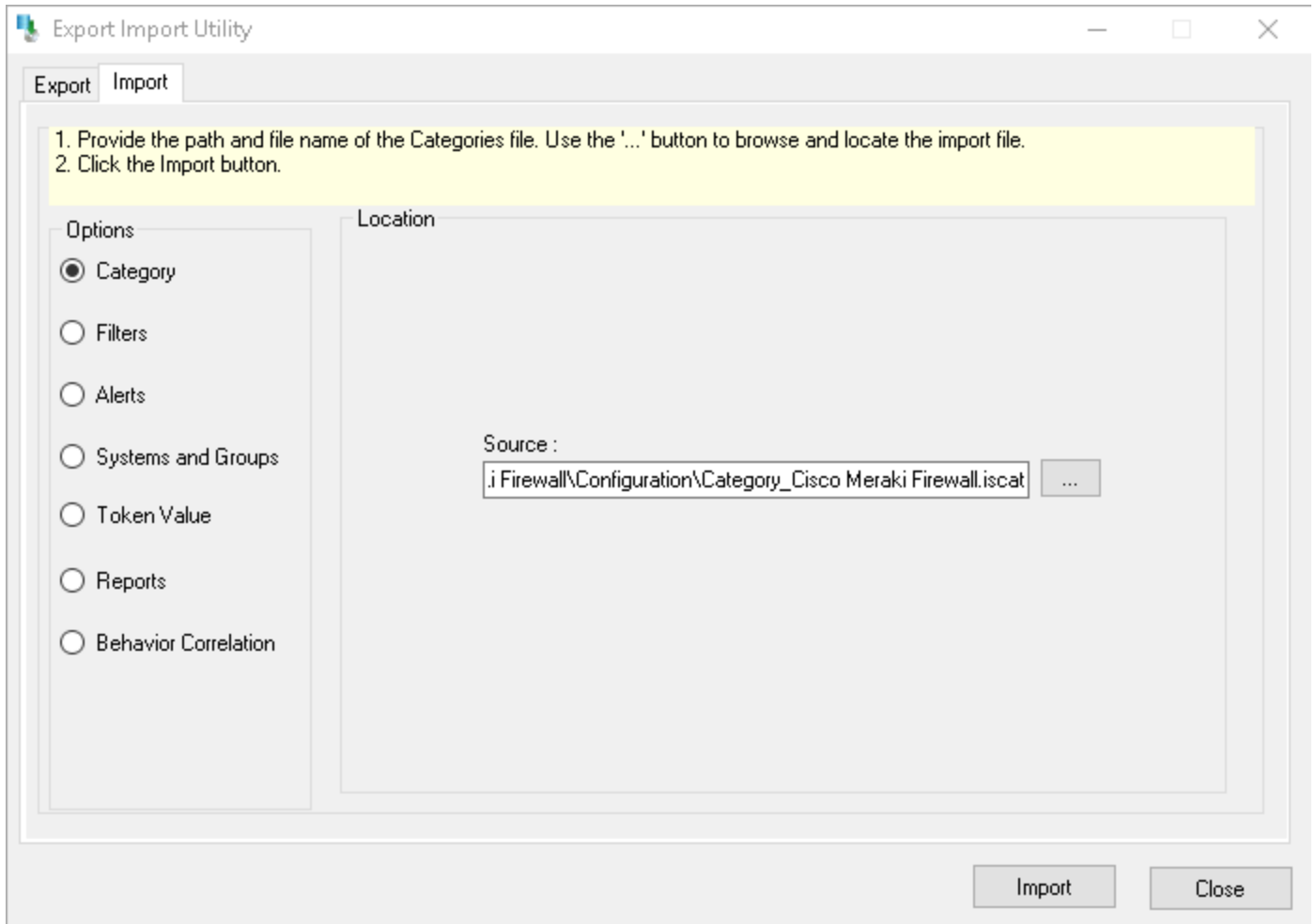


Figure 19

2. Locate **Category_Cisco Meraki Firewall.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button. EventTracker displays success message.

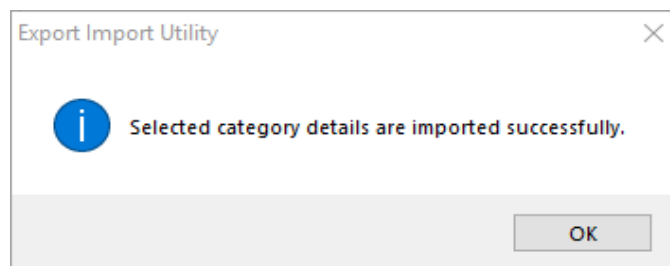


Figure 20

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

Alerts

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

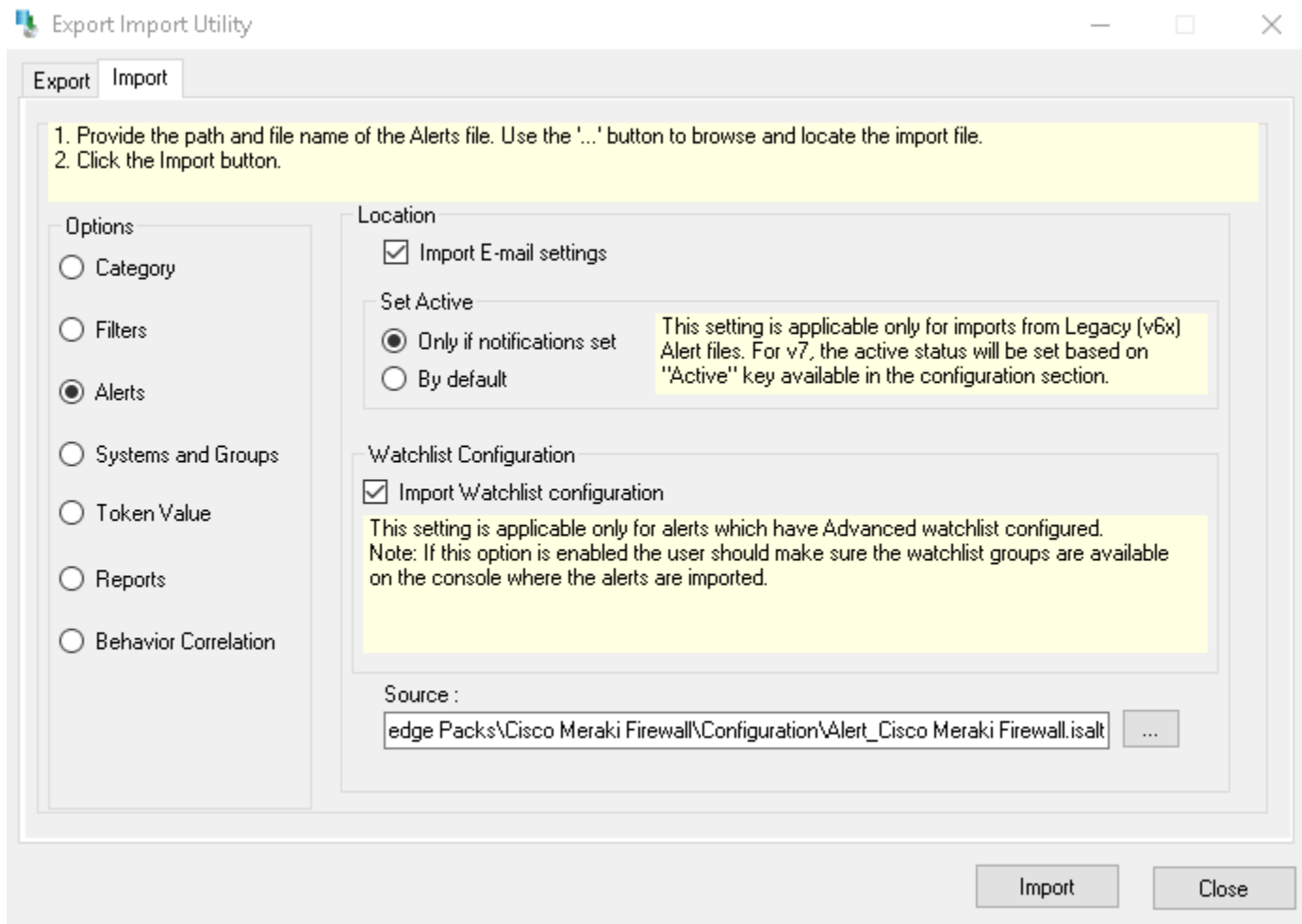


Figure 21

2. Locate **Alert_Cisco Meraki Firewall.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

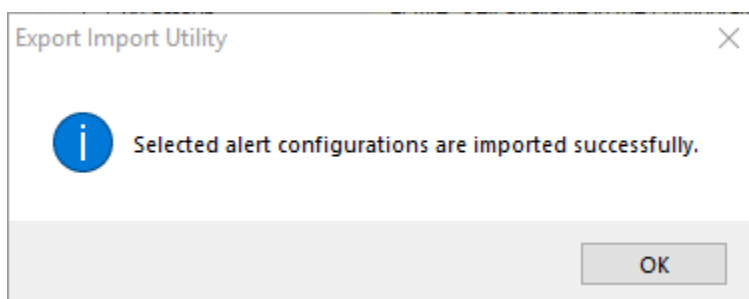



Figure 22

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

Token Templates

- Click **Parsing rules** under **Admin** option in the EventTracker manager page.
- Move to **Template** and click on import configuration  icon on the top right corner.
- In the popup window browse the file named **Template_Cisco Meraki Firewall.ettd**.



Import						
selected file is: Template_Cisco Meraki Firewall.ettd 						
<input checked="" type="checkbox"/>	Template name	Separator	Template description	Added date	Added by	Group Name
<input checked="" type="checkbox"/>	Meraki Firewall- Blocked content details	\t	<134>1 139285998.201435382 Meraki_Security_Appliance events content_filtering_block url='https://*.cloudmosa.com/...' category='User-defined Blacklist' server='184.105.82.3443'	Mar 31 06:17:55 PM	ETAdmin	Cisco Meraki Firewall
<input checked="" type="checkbox"/>	Meraki Firewall- DHCP IP lease details	\t	<134>1 1392793111.469320128 Meraki_Security_Appliance events dhcp lease of ip 172.16.37.220 from server mac 0018:0A:02:85:88 for client mac 0018:0A:76:F9:79 from router 172.16.1.2 on subnet 255.255.0.0 with dns 172.16.1.200, 172.16.1.1	Mar 31 06:17:55 PM	ETAdmin	Cisco Meraki Firewall
<input checked="" type="checkbox"/>	Meraki Firewall- IDS alert details	\t	<134>1 1392812405.977854011 Meraki_Security_Appliance ids-alerts signature=128/4/1 priority=2 timestamp=1392812405.977656 shorts=09:39:30/3 B4F7C5 direction=egress protocol=udp src=192.168.251.122/61724 dst=172.16.1.90/22 message: (ppp_ssh) Protocol mismatch	Mar 31 06:17:55 PM	ETAdmin	Cisco Meraki Firewall
<input checked="" type="checkbox"/>	Meraki Firewall- Traffic flow details	\t	<134>1 1392793163.700257235 Meraki_Security_Appliance flows src=17.173.254.223 dst=24.249.102.115 protocol=udp sport=16387 dport=1072 pattern: 1 all	Mar 31 06:17:55 PM	ETAdmin	Cisco Meraki Firewall
<input checked="" type="checkbox"/>	Meraki Firewall- User authentication details	\t	<134>1 1392875022.027478864 Meraki_Security_Appliance events authentication on 00:08:0B:73:F1:78 for user student as CN=Student Guest,OU=Students,OU=Users - Domain,DC=eagles,DC=ocacademy,DC=org with policy for group CN=Students,OU=Students,OU=Users - Domain,DC=eagles,DC=ocacademy,DC=org	Mar 31 06:17:55 PM	ETAdmin	Cisco Meraki Firewall
<input checked="" type="checkbox"/>	Meraki Firewall- VPN session details	\t	<134>1 1392808395.669667263 Meraki_Security_Appliance events Site-to-site VPN: IPsec-SA established: ESP/Transport 24.249.102.115[4500]->70.16	Mar 31 06:17:55 PM	ETAdmin	Cisco Meraki Firewall

Figure 23

- Now select all the check box and then click on  Import option. EventTracker displays success message.

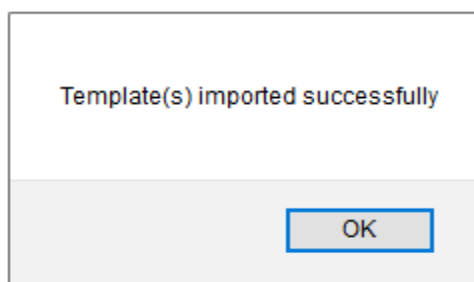


Figure 24

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

Knowledge Objects

- Click **Knowledge objects** under **Admin** option in the EventTracker manager page.
- Locate the **KO_Cisco Meraki Firewall.etko** file.

3. Click the **'Upload'** option.
4. Now select all the check box and then click on **'Import'** option.

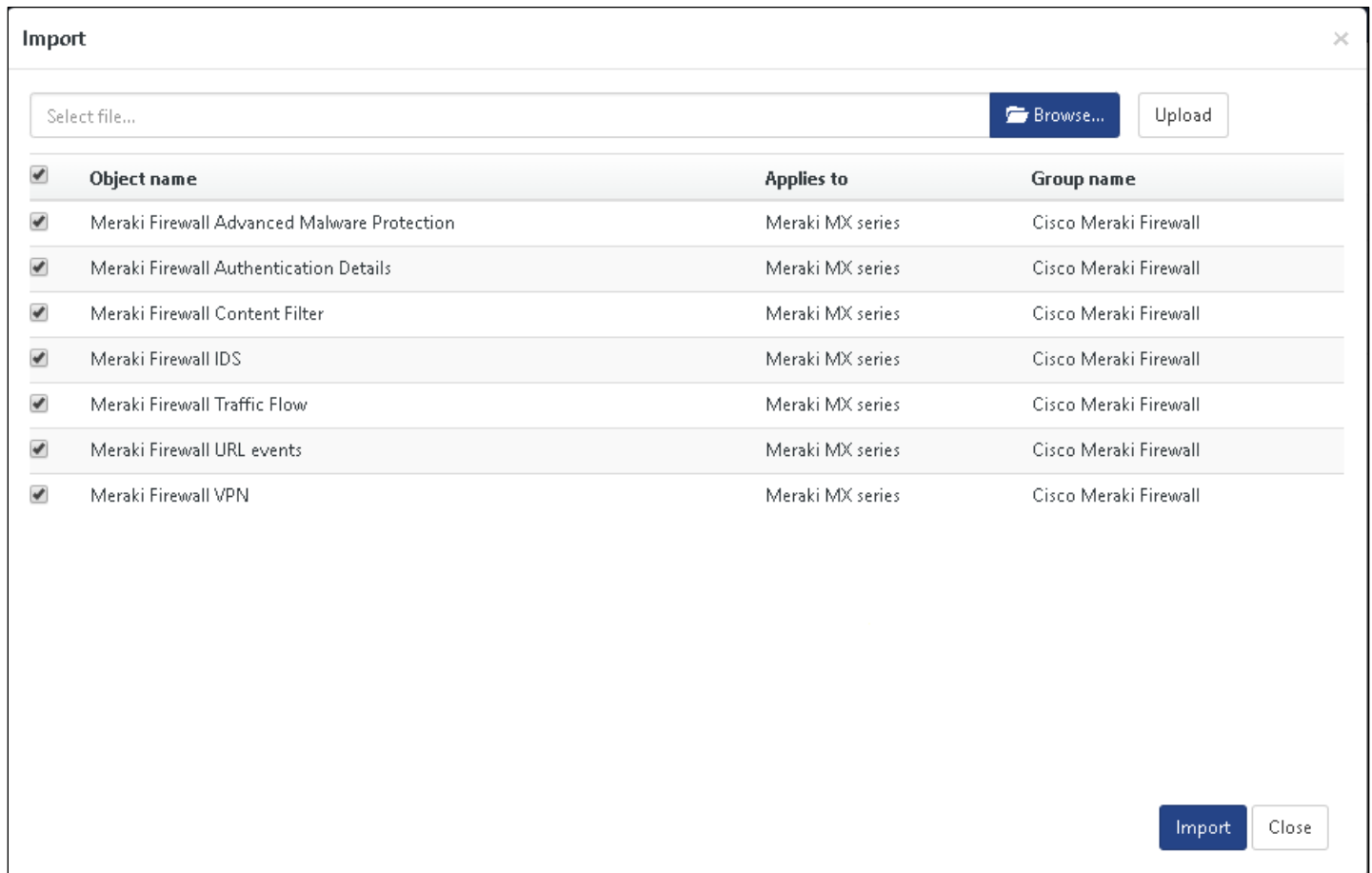


Figure 25

5. Knowledge objects are now imported successfully.

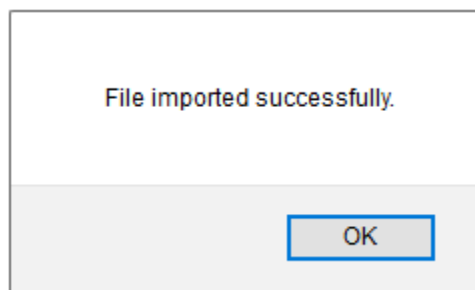


Figure 26

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

Flex Reports

On EventTracker Control Panel,

1. Click **Reports** option, and select new (*.etcrx) from the option.

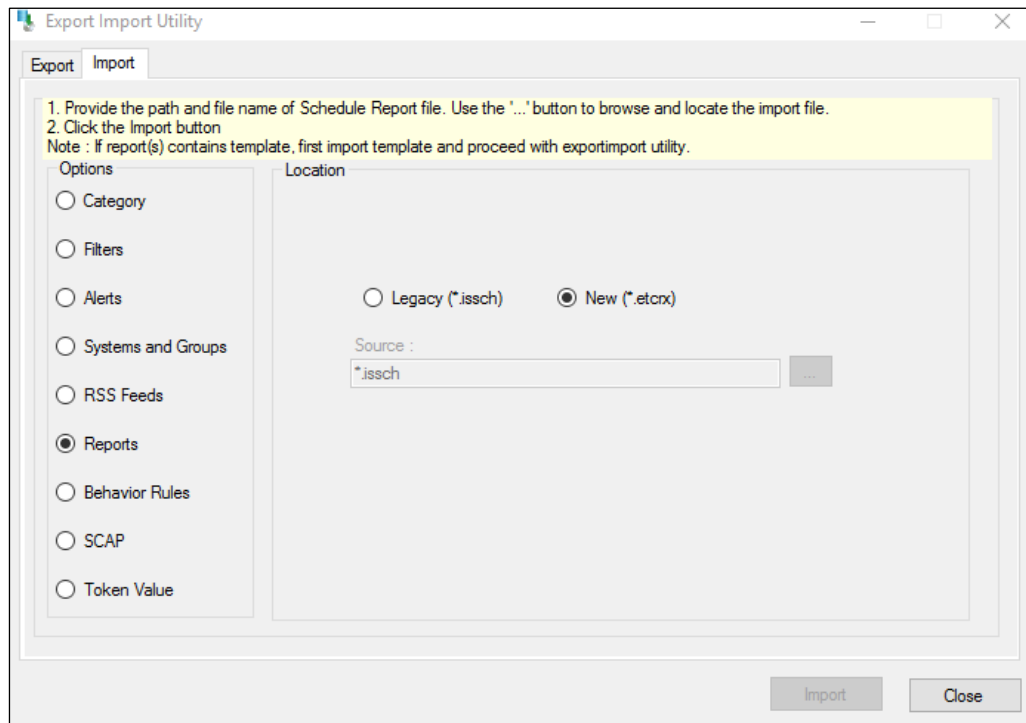


Figure 27

2. Locate the Flex **Report_Cisco Meraki Firewall.etcrx** file and select all the check box.

Reports Import

Note : If report(s) contains template, first import template and proceed with report import process.

Select file C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs\Cisco Meraki Firewall\Configuration\Flex Report_Cisco Meraki Firewa Select file

Available reports

Title Frequency Show all Q Q

<input checked="" type="checkbox"/>	Title	Sites	Groups	Systems	Frequency
<input checked="" type="checkbox"/> EDIT	Meraki Firewall- Blocked content details	NTPLDTBLR40	EventTracker	meraki	Undefined
<input checked="" type="checkbox"/> EDIT	Meraki Firewall- IDS alert details	NTPLDTBLR40	EventTracker	meraki	Undefined
<input checked="" type="checkbox"/> EDIT	Meraki Firewall- Traffic flow details	NTPLDTBLR40	EventTracker	meraki	Undefined
<input checked="" type="checkbox"/> EDIT	Meraki Firewall- User authentication de...	NTPLDTBLR40	EventTracker	meraki	Undefined
<input checked="" type="checkbox"/> EDIT	Meraki Firewall- VPN session details	NTPLDTBLR40	EventTracker	meraki	Undefined
<input checked="" type="checkbox"/> EDIT	Meraki Firewall- Web traffic details	NTPLDTBLR40	EventTracker	meraki	Undefined

Note: Set run time option is not applicable for Defined Reports and Hourly Reports

Set run time for report(s) from AM at interval of minutes Set i

Replace to Replace Assign systems

Note: Make sure that Site(s), Group(s) and System(s) selections are valid. ↓ ⊗

Figure 28

- Click the **Import** button to import the reports. EventTracker displays success message.

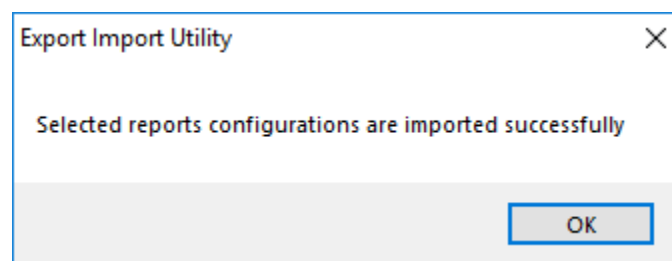


Figure 29

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

Verify Meraki Firewall knowledge pack in EventTracker

Categories

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

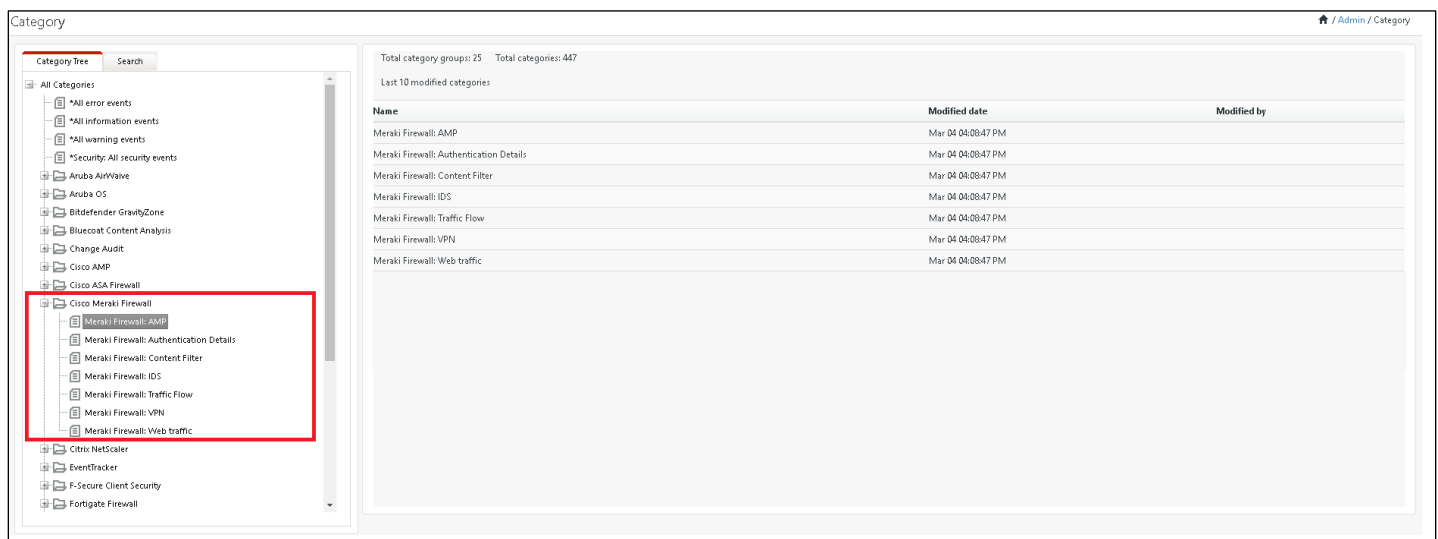


Figure 30

Alerts

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Alerts**.
 2. In search box, enter **Meraki firewall** and then click the **Search** button.
- EventTracker displays alert of Meraki Firewall.

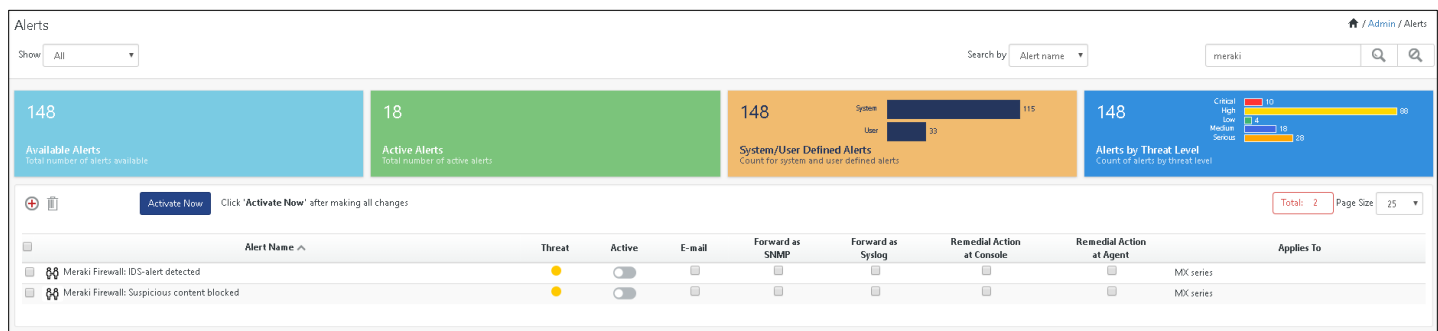


Figure 31

Token Templates

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Parsing rules**.
2. On **Template** tab, click on the **Cisco Meraki Firewall** group folder to view the imported Token Values.

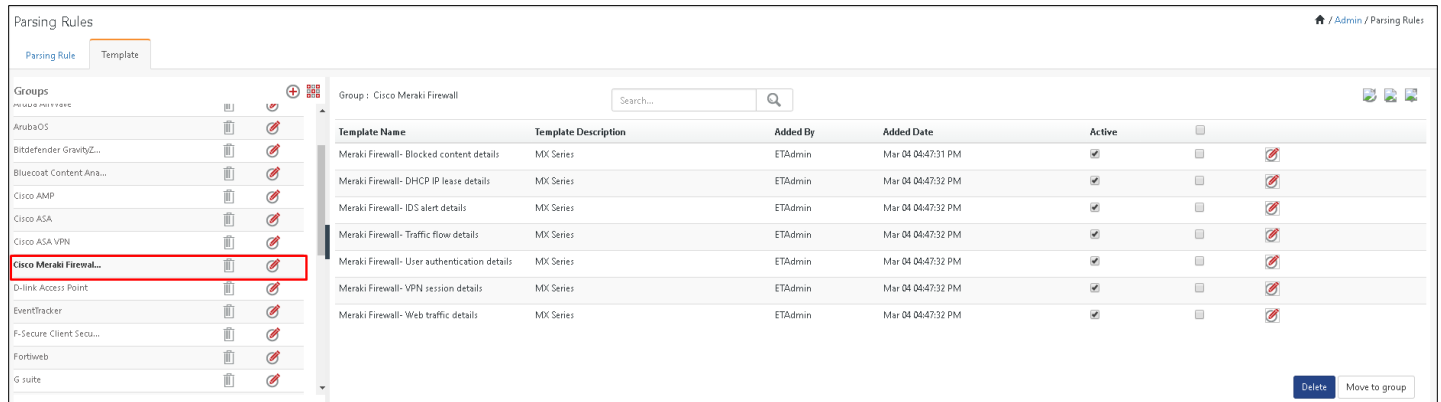


Figure 32

Knowledge Objects

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Knowledge Objects**.
2. In the **Knowledge Object** tree, expand **Meraki Firewall** group folder to view the imported Knowledge objects.

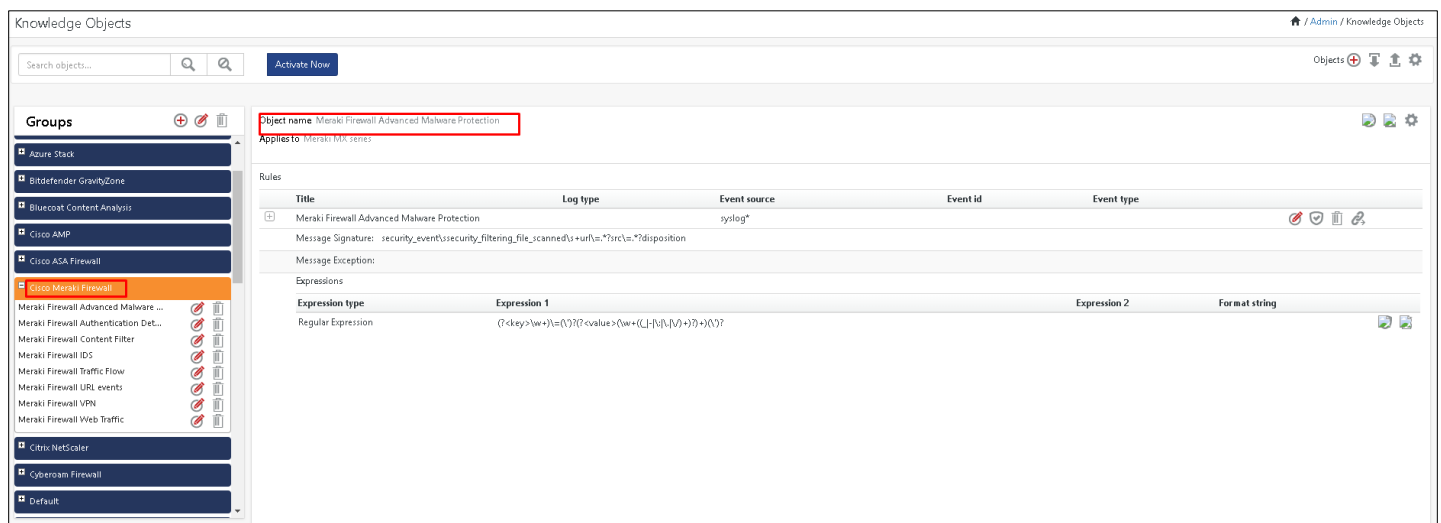


Figure 33

Flex Reports

1. In the **EventTracker Enterprise** web interface, click the **Reports** menu, and then select **Report Configuration**.

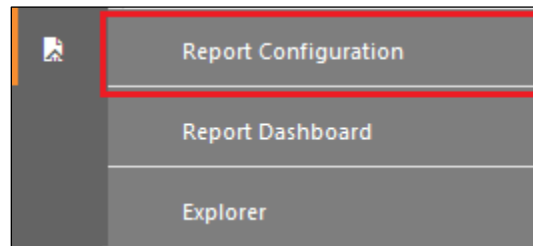


Figure 34

2. In **Reports Configuration** pane, select **Defined** option.
3. Click on the **Meraki Firewall** group folder to view the imported **Meraki Firewall** reports.

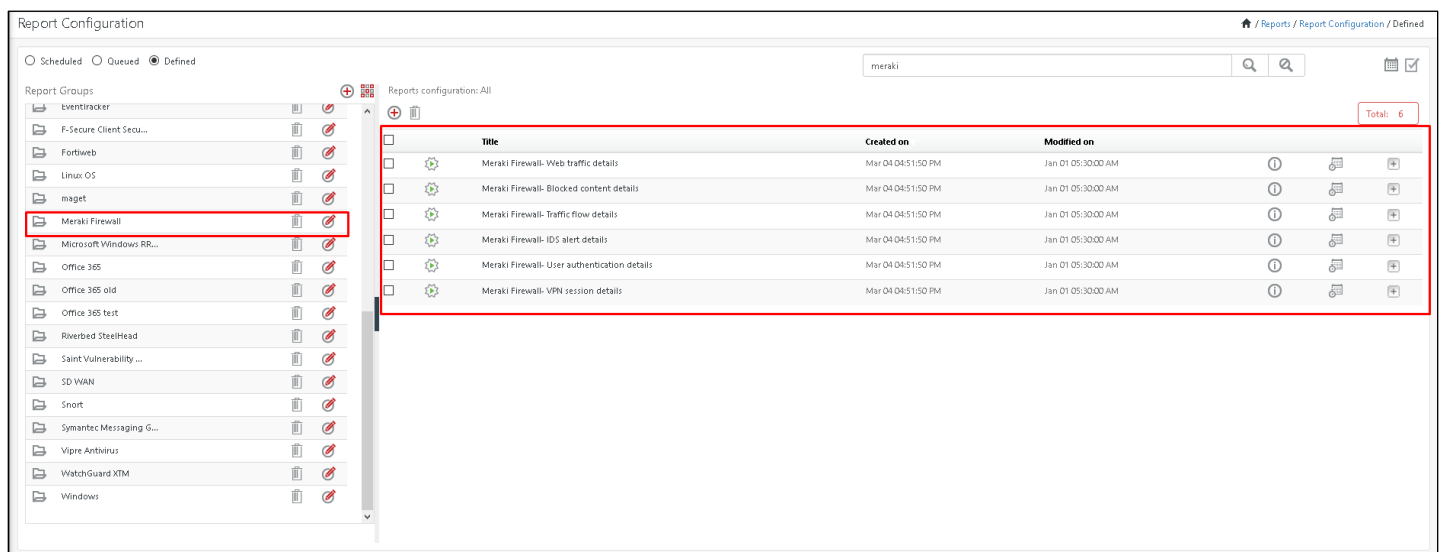


Figure 35