

# Integrate Meraki Firewall

EventTracker v8.x and above

Publication Date: March 6, 2019

### 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 To configure the Meraki Firewall to forward logs to a syslog server	3 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 Category	10 11
Alerts	13
Knowledge Objects	14
Flex Reports	16
Verify Meraki Firewall knowledge pack in EventTracker Categories	18 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**.

Network-wide	MONITOR	CONFIGURE
Security & SD-WAN	Clients	General
	Packet capture	Alerts
Organization	Event log	Group policies
	Map & floor plans	Users
		Add devices



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	×
	Add a syslog server		Flows	
			URLs	
			Appliance event log	



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

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



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



#### 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/294004 3877833_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/294004 3877833_p0_v2_s600_e404.png';

#### Figure 5

#### Sample Log:

- Mar 05 01:14:43 PM	<134>1 1392859398.201435382 Meraki_Security_Applicance events content_filtering_block url="https://".contososerver.com/" category0="User-defined Blacklist" server="100.17.82.3:443"
event_computer	+- meraki2019
event_description	<134>1 1392859398.201435382 Meraki_Security_Applicance events content_filtering_block url="https://*.contososerver.com/" category0="User-defined Blacklist" server="100.17.82.3443"
event_id	<b>↓-</b> 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_Applicance
src_ip_address	+- 100.17.82.3
src_port_no	+- 443
url_name	+- https://*.contososerver.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 Туре	VPN Status	User Name	Source IP	Source Port	Destination IP	<b>Destination Port</b>
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_Applicance events Site-to-site VPN: IPsec-SA established: ESP/Transport 24.249.102.115[4500]->70.168.64.32[4500]
dest_ip_address	<b>+</b> - 70.168.64.32
dest_port_no	<b>★</b> - 4500
event_computer	← merski2019
event_description	<134>1 1392808395.669667263 Meraki_Security_Applicance 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	<b>★</b> - 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_Applicance
src_ip_address	+- 24,249,102,115
src_port_no	<b>★</b> - 4500
tags	+- Meraki Firewall
tags	

#### 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=U sers - Domain,DC=eagles,DC=ocacademy ,DC=org
03/30/2016 03:36:43 PM	MX64	90:B1:1C:79:1C:50	J/Volfe	CN=Janet Wolfe,OU=Administration,OU=User s - Domain,DC=eagles,DC=ocacademy ,DC=org	CN=Administration,OU=Administrati on,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=Us ers - Domain,DC=eagles,DC=ocacademy ,DC=org



#### Sample Log:

- Mar 05 01:24:49 PM	<134>1 1392792900.051011956 Meraki_Security_Applicance events authentication on 00.1E:08:3E: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_Applicance events authentication on 00:1E:08:3E:42:DD for user Tmark as CN=ted mark,OU=lab, OU=Users - Domain,DC=contoso,DC=domain,DC=org with policy for grou
	p CN=lab,OU=lab,OU=lab,OU=Users - Domain,DC=contoso,DC=domain,DC=org
event_id	+- 3399
event_log_type	+- Application
event_source	← syslog
event_type	+ Information
event_user_domain	★- N/A
event_user_name	<b>+</b> - ₩A
log_source	+- Meraki Firewall Authentication Details
src_device_name	← Meraki_Security_Applicance
src_mac_address	+- 00.1E:08:3E42: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	top/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	top/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	tep/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



#### 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	<b>↓</b> - 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	<b>+</b> -3
log_source	+- Meraki Firewall IDS
protocol_type	+- udp/ip
src_ip_address	+- 192.768.30.10.49243
src_mac_address	+- 00:15:50:1E:08:04
threat_id	+- 1:39867:3
threat_info	+- INDICATOR-COMPROMISE Suspicious :tk dns query
tags	+- Intrusion Detected
tags	+- Intrusion Detected
tags	+- Merski 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	<b>Destination IP</b>	<b>Destination Port</b>	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.googlesyndication.com/singa 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



#### Sample Log:

- Mar 05 01:24:49 PM	1374543213.342705328 MX84 urls src=192.168.1.186:63735 dst=69.58.23.25:80 mac=58:1F:AA:CE:61:F2 request: GET http://bit.ly/17zJTvJ agent=""Go-http-client/1.1""
dest_ip_address	+- 69.58.23.25
dest_port_no	+- 60
event_computer	+- meraki2019
event_description	1374543213.342705328 MX84 urls src=192.168.1.18&65735 dst=69.58.23.25:80 mac=58:1F:AA:CE:61:F2 request: GET http://bit.ly/17zJTvJ 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	<b>+-</b> 192.168.1.186
src_mac_address	+- 58:1F:-AA:CE:61:F2
src_port_no	+- 63735
url_name	+- http://bit.ly/17zJTvJ agent="Go-http-client/1.1"
tags	+- Web Traffic
taar	▶ Mershi



• 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	<b>Destination Port</b>	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=8.8.88 mac=00:18:0A:>OC>OC>OC>OC protocol=udp sport=9562 dport=53 pattern: allow all
action	+- allow all
dest_ip_address	<b>+-</b> 8888
dest_port_no	<b>+-</b> 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=00:18:0A0000000 protocol=udp sport=9562 dport=53 pattern: allow all
event_id	<b>+-</b> 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	<b>+-</b> 192.168.10.254
src_mac_address	+- 00:18:0AD000000
src_port_no	<b>+-</b> 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.



3. Click the **Import** tab.

### Category

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

button.



•	Export Import Utility					$\times$
E	xport Import					
	<ol> <li>Provide the path and file na</li> <li>Click the Import button.</li> </ol>	e of the Categories file. Use the '' button	to browse and locate the import file.			
	Options	Location				
	Category					
	O Filters					
	<ul> <li>Alerts</li> </ul>					
	O Systems and Groups	Source : _i Firewall\Configuration\0	Category_Cisco Meraki Firewall.iscat			
	🔘 Token Value					
	O Reports					
	O Behavior Correlation					
			Impo	ort	Close	9



- 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.

Export Import Utility	×
Selected categ	ory details are imported successfully.
	ОК



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

 $\times$ 

### Alerts

🐁 Export Import Utility		
Export Import		
1. Provide the path and file na 2. Click the Import button.	ame of the Alerts file. Use the '' butt	on to browse and locate the import
Options O Category	Location Import E-mail settings	
<ul> <li>Filters</li> </ul>	Set Active	This setting is applicable only for

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

<ul> <li>Filters</li> <li>Alerts</li> <li>Systems and Groups</li> <li>Token Value</li> <li>Reports</li> <li>Behavior Correlation</li> </ul>	Uptions	Location Import E-mail settings	
Systems and Groups       Watchlist Configuration         Token Value       Import Watchlist configuration         Reports       This setting is applicable only for alerts which have Advanced watchlist configured. Note: If this option is enabled the user should make sure the watchlist groups are available on the console where the alerts are imported.         Source :	) Filters ) Alerts	<ul> <li>Only if notifications set</li> <li>By default</li> </ul>	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.
<ul> <li>Token Value</li> <li>Token Value</li> <li>Reports</li> <li>Behavior Correlation</li> <li>Source :</li> </ul>	Systems and Groups	Watchlist Configuration	
O Reports       Note: If this option is enabled the user should make sure the watchlist groups are available on the console where the alerts are imported.         O Behavior Correlation       Source :	) Token Value	<ul> <li>Import Watchlist configurat</li> <li>This setting is applicable only f</li> </ul>	ion for alerts which have Advanced watchlist configured.
Behavior Correlation     Source :	) Reports	Note: If this option is enabled i on the console where the aleri	the user should make sure the watchlist groups are available ts are imported.
Source :	Behavior Correlation		
edge Packs\Cisco Meraki Firewall\Configuration\Alert_Cisco Meraki Firewall.isalt		Source : edge Packs\Cisco Meraki F	irewall\Configuration\Alert_Cisco Meraki Firewall.isalt

button.

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



Figure 22



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

### **Token Templates**

- 1. Click Parsing rules under Admin option in the EventTracker manager page.
- 2. Move to **Template** and click on import configuration  $\mathbb{T}$  icon on the top right corner.
- 3. In the popup window browse the file named Template\_Cisco Meraki Firewall.ettd.

Impo	port					
selecte	d file is: Template_Cisco Meraki Firewall.ettd 🖉 Browse 📮	8				
	Template name	Separator	Template description	Added date	Added by	Group Name
	Meraki Firewall- Blocked content details	\t	<134>1 1392659398.201435382 Meraki_Security_Applicance events conten t_filtering_block url='https://*.cloudmosa.com/' category0='User-define d Blacklist' server='184.105.82.3:443'	Mar 31 06:17:55 PM	ETAdmin	Cisco Meraki Firewall
*	Meraki Firewall-DHCP IP lease details	/t	$<\!134\!>\!11392793111.469320128Meraki_Security_Applicance events dhcp le ase of ip 172.1637.220from server mac 0018.04.02:85:89 for client mac 0 0.18:04.02:87979 from router 172.16.1.2 on subnet 255.255.0.0 with dns 172.16.1.2 log 172.16.1.1$	Mar 31 06:17:55 PM	ETAdmin	Cisco Meraki Firewall
×	Meraki Firewall- IDS əlert details	\t	<134>1 1392812405.977894011 Meraki_Security_Applicance ids-alerts sign ature=128:4:1 priority=2 timestamp=1392812405.977656 shost=03:99:90.3 B:F7C5 direction=egress protocol=tcp/ip src=192.168.251.122.61724 dst= 172.161.302.22 message: (pp_sth) Protocol mismatch	Mar 31 06:17:55 PM	ETAdmin	Cisco Meraki Firewall
۲	Meraki Firewall- Traffic flow details	\t	<134>1 1392793163.700257235 Meraki_Security_Applicance flows src=17.1 73.254.223 dst=24.249.102.115 protocol=udp sport=16387 dport=1072 patt ern: 1 all	Mar 31 06:17:55 PM	ETAdmin	Cisco Meraki Firewall
•	Meraki Firewall- User authentication details	ζt.	<134>11392875022.027478864 Meraki_Security_Applicance events authen tication on 00.081087.9731738 for user student as CN=Student Guest,OU=S tudents,OU=Users - Domain,DC=eagles,DC=occademy,DC=org with pol icy 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
•	Meraki Firewall- VPN session details	\t	<134>1 1392808395.669667263 Meraki_Security_Applicance 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

4. Now select all the check box and then click on  $\mathbb{T}$  Import option. EventTracker displays success message.



Figure 24

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

### Knowledge Objects

- 1. Click Knowledge objects under Admin option in the EventTracker manager page.
- 2. 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.

Impo	t		×
Sele	ct file		Browse Upload
	Object name	Applies to	Group name
1	Meraki Firewall Advanced Malware Protection	Meraki MX series	Cisco Meraki Firewall
1	Meraki Firewall Authentication Details	Meraki MX series	Cisco Meraki Firewall
*	Meraki Firewall Content Filter	Meraki MX series	Cisco Meraki Firewall
<b>«</b>	Meraki Firewall IDS	Meraki MX series	Cisco Meraki Firewall
1	Meraki Firewall Traffic Flow	Meraki MX series	Cisco Meraki Firewall
1	Meraki Firewall URL events	Meraki MX series	Cisco Meraki Firewall
*	Meraki Firewall VPN	Meraki MX series	Cisco Meraki Firewall
			Import Close

Figure 25

5. Knowledge objects are now imported successfully.

File	e imported successfully.
	ОК



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.

ote : If report(s) contains templa Options	ate, first import template and proce Location	ed with exportimport utility.	
Category			
) Filters			
) Alerts	O Legacy (*.issch)	New (*.etcrx)	
Systems and Groups	Source :		
RSS Feeds	issch		
Reports			
Behavior Rules			
⊖ SCAP			
🔿 Token Value			

#### Figure 27

2. Locate the Flex **Report\_Cisco Meraki Firewall.etcrx** file and select all the check box.



Reports Ir	mport ort(s) contains template, first import template a	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     Image: Constraint of the state of the sta										
	Title	Sites	Groups	Systems	Frequency					
	Meraki Firewall- Blocked content details	NTPLDTBLR40	EventTracker	meraki	Undefined					
EDIT	Meraki Firewall- IDS alert details	NTPLDTBLR40	EventTracker	meraki	Undefined					
EDIT	Meraki Firewall- Traffic flow details	NTPLDTBLR40	EventTracker	meraki	Undefined					
EDIT	Meraki Firewall- User authentication de	NTPLDTBLR40	EventTracker	meraki	Undefined					
EDIT	Meraki Firewall- VPN session details	NTPLDTBLR40	EventTracker	meraki	Undefined					
EDIT	Meraki Firewall- Web traffic details	NTPLDTBLR40	EventTracker	meraki	Undefined					
٢					>					
Note: Set	run time option is not applicable for Defined F	Reports and Hourly Reports								
Set run	time for report(s) from	4 ▼ at interval of minut	es Set 🚺							
Replace	to	Rep	olace Assign systems							
			Note: Make sure that Site(s	), Group(s) and System(s) selections are va	alid. 📕 🛞					



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

Export Import Utility	$\times$
Selected reports configurations are imported successfully	
ОК	



4. 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.

itegory			Admin / Category
Category Tree Search	Total category groups: 25 Total categories: 447		
- All Categories	Last 10 modified categories		
All error events	Name	Modified date	Modified by
*All information events	Meraki Firewall: AMP	Mar 04 04:08:47 PM	
- E *Security All security events	Meraki Firewall: Authentication Details	Mar 04 04:08:47 PM	
Calify Walke	Meraki Firewall: Content Filter	Mar 04 04:08:47 PM	
Aruba OS	Meraki Firewall: IDS	Mar 04 04:08:47 PM	
🗟 🔁 Bitdefender GravityZone	Meraki Firewall: Traffic Flow	Mar 04 04:08:47 PM	
🐵 🔁 Bluecoat Content Analysis	Meraki Firewall: VPN	Mar 04 04:08:47 PM	
Change Audit	Meraki Firewall: Web traffic	Mar 04 04:08:47 PM	
Clica ASA Firewall  Clica			

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.

Alerts										Admin / Alerts
Show All T							Search by Alert name	•	meraki	ଦ୍ ଦ୍
148	18				148	System	115	148	Critical High Low 4 Medium	10 88
Available Alerts Total number of alerts available	Active Alerts Total number of active alerts				System/User Define Count for system and us	d Alerts er defined alerts		Alerts by Thre Count of alerts b	Serious at Level y threat level	28
The Activate Now Click 'Activate Now' after making a	all changes									Total: 2 Page Size 25 V
Alert Name A	Th	ireat <i>i</i>	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent		Applies To
☐ දී්‍ਰੈ Meraki Firewall: IDS-alert detected		•							MX series	
Bo Meraki Firewall: Suspicious content blocked		•							MX series	





### **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.

Parsing Rules									ŧ	/ Admin / Parsing Rules
Parsing Rule Template										
Groups	L	<i>.</i> ⊕ ₩	Group : Cisco Meraki Firewall	Search	Q					22
ArubaOS	Ü	1	Template Name	Template Description	Added By	Added Date	Active			
Bitdefender GravityZ	Ü	1	Meraki Firewall- Blocked content details	MX Series	ETAdmin	Mar 04 04:47:31 PM			Ø	
Bluecoat Content Ana	Ű	1	Meraki Firewall- DHCP IP lease details	MX Series	ETAdmin	Mar 04 04:47:32 PM			0	
Cisco AMP	Û	0	Meraki Firewall- IDS alert details	MX Series	ETAdmin	Mar 04 04:47:32 PM			Ø	
Cisco ASA	Ü	0	Meraki Firewalla Traffic flow details	MY Series	FTAdmin	Mar 04 04:47-32 PM			2	
Cisco ASA VPN	Ü	0		The same	2.0530100	ind of one local in		-	<b>U</b>	
Cisco Meraki Firewal	Ü	۲	Meraki Firewall- User authentication details	MX Series	ETAdmin	Mar 04 04:47:32 PM	×		Ø	
D-link Access Point	Û	Ø	Meraki Firewall- VPN session details	MDC Series	ETAdmin	Mar 04 04:47:32 PM	×.		Ø	
EventTracker	Ű	1	Meraki Firewall- Web traffic details	MX Series	ETAdmin	Mar 04 04:47:32 PM	₹		0	
F-Secure Client Secu	Ű	1								
Fortiweb	Ű	1								
G suite	Ü	0							Delete	Move to group



### 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.

					Admin / Knowledge Objects
ctivate Now					Objects 🕀 ፒ 🏦 🌣
t name Meraki Firewall Advanced Malware Protectio as to Meraki MX series	n				ې 🗟 🕏
Tal-	Las hora	F	Event M	Freed down	
Merski Eirawall Advanced Maharare Protection	Log type	svilaa*	Eventia	Event type	<b>(注 回 前 2</b>
Message Signature: security event/ssecurity filts	ering file scanned\s+url\=.*?src\=.*?dispo	sition			
Message Exception:	2				
Expressions					
Expression type	Expression 1			Expression 2	Format string
Regular Expression	$(?<\!$	\.[\/]+)?)+)(\')?			2
	thate Now  Transe Merski Firewall Advanced Makware Protection  Title  Merski Firewall Advanced Makware Protection Mersage Signature: security,event/security_filt Mersage Exception: Expression Expression Expression	ttynte Now  Traine Maraki Pirewall Advanced Malware Profection  Title Log type  Mesias Firewall Advanced Malware Protection  Mesiage Signature: security_event/security_filtering_file_scannedus+urls=??rrchs=?dispo Mesiage Exception: Expression Expression Expression (?c4ep2/wr+)\=(1)?(? cvalue>(wr+(L+N))	toote Now The New Protection The Leg type Event source Messis Firewall Advanced Malware Protection Messis Firewall Advanced Malware Protection Messis Signature: security_event/ssecurity_filtering_file_cannedUs=urls=*?rdisposition Message Exception: Expression Expression Expression (rdkey>Uw+)=(0?1?Cvalue>(w+(C_H\gL\[/\)+)?)+(0)?	ttvin Nov Time Manki Pireali Advanced Malvare Protection Time Consult Prevail Advanced Malvare Protection Time Consult Prevail Advanced Malvare Protection Meriage Signature : econty_event/siscurity_filtering_file_scanned/s=url.e="rint="	ttvis Nor Time Maski Presil Advanced Makare Protection Time Maski Presil Advanced Makare Protection Time Maski Bresil Advanced Makare Protection Maski Bresil Advanced Makare Protection Maski Bresil Signature record Company Signature Signature Signature Signature Recent Signature Recent Signature Recent Signature Signature Recent Signature Signature Recent Signature Signature Recent Signature Recent Signature Signature Recent Signat



### Flex Reports

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





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

Report Configuration							🔶 / Reports / Rep	ort Configur	ation / Defined
O Scheduled O Queued      O Defined					meraki		ଦ୍ ଦ୍		
Report Groups		+	Reports configura	tion: All					
Les Eventiracker		<ul> <li>^</li> </ul>	🕂 🗓					ſ	Total: 6
F-Secure Client Secu	<u>ii</u> (	0		Title	Created on	Modified on			
D Fortiweb	<u></u>	0	- D &	Meraki Firewall- Web traffic details	Mar 04 04:51:50 PM	Jan 01 05:30:00 AM	Û	周	Ŧ
Linux OS	<u></u>	0					0	0	
🕞 maget	Ű (	1		Meraki Firewali- blocked content details	Mar 04 04:5 1:50 PM	Jan DT 05:5000 AM	0	0 <sup>11</sup>	+
🔁 Meraki Firewall	Ű (	0		Meraki Firewall- Traffic flow details	Mar 04 04:51:50 PM	Jan 01 05:30:00 AM	(i)	8	+
Microsoft Windows RR	<u>Î</u> (	1	D 🔅	Meraki Firewall- IDS alert details	Mar 04 04:51:50 PM	Jan 01 05:30:00 AM	(i)	<i>5</i>	+
Office 365	Ê (	0	- 🔅	Meraki Firewall- User authentication details	Mar 04 04:51:50 PM	Jan 01 05:30:00 AM	()	5	+
Coffice 365 old	1	0	D 🔅	Meraki Firewall- VPN session details	Mar 04 04:51:50 PM	Jan 01 05:30:00 AM	()	8	+
Office 365 test	1	0							
Riverbed SteelHead	Î (	1							
🕞 Saint Vulnerability	<u>i</u> (	1							
D SD WAN	<u>ii</u> (	1							
🕞 Snort	<u>ii</u> (	1							
Symantec Messaging G	Ű (	1							
Vipre Antivirus	<u></u>	1							
🕞 WatchGuard XTM	Ű (	1							
🔁 Windows	Ű (	Ø							

