

Integrate F-Secure Client Security

EventTracker v9.x and above

Abstract

This guide provides instructions to configure an **F-Secure Client Security** to send its syslog to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version v9.x or above and F-Secure Client Security 12.x or 13.x.

Audience

Administrators who are assigned the task to monitor F-Secure Client Security events using EventTracker.

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

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

EventTracker 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 EventTracker, 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.

© 2018 EventTracker Security LLC. 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
Integration of F-Secure Client Security with EventTracker manager.....	3
EventTracker Knowledge Pack	4
Alerts	4
Categories.....	5
Knowledge Objects.....	5
Flex Reports.....	6
Import F-Secure Client Security knowledge pack into EventTracker.....	8
Alerts	9
Categories.....	10
Knowledge Objects.....	11
Token Templates	12
Flex Reports.....	13
Dashlets	15
Verify F-Secure Client Security knowledge pack in EventTracker.....	17
Alerts	17
Categories.....	17
Knowledge Objects.....	18
Token Templates	19
Flex Reports.....	19
Dashlets	20

Overview

F-Secure Client Security is much more than anti-malware – it offers next-gen protection elements such as threat intelligence, behavioral analysis and proactive protection against all the latest threats.

EventTracker helps to monitor events from F-Secure Client Security. Its knowledge objects and flex reports will help you to analyze firewall, application control, threat and spyware related details.

Prerequisites

- EventTracker v9.x or above should be installed.
- **F-Secure Client Security 12.x or 13.x** should be installed.
- Required Access to the **F-Secure Policy Manager** Console.
- Firewall Exception to the port 514 should be configured.

Integration of F-Secure Client Security with EventTracker manager

To forward **F-Secure Client Security** alerts through **F-Secure Policy Manger**, configure as shown below:

1. Logon to **F-Secure Policy Manger**.
2. Select **Server configuration** in **Tools** from the menu.

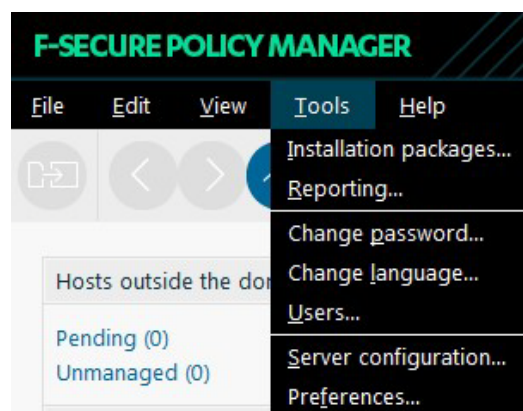


Figure 1

3. Click **Syslog**.
4. Select **Forward alerts to syslog** and enter the **EventTracker Manager** address.
By default, alerts are forwarded to syslog using UDP port number 514.
5. Select the message format **Syslog (RFC 3614)**.

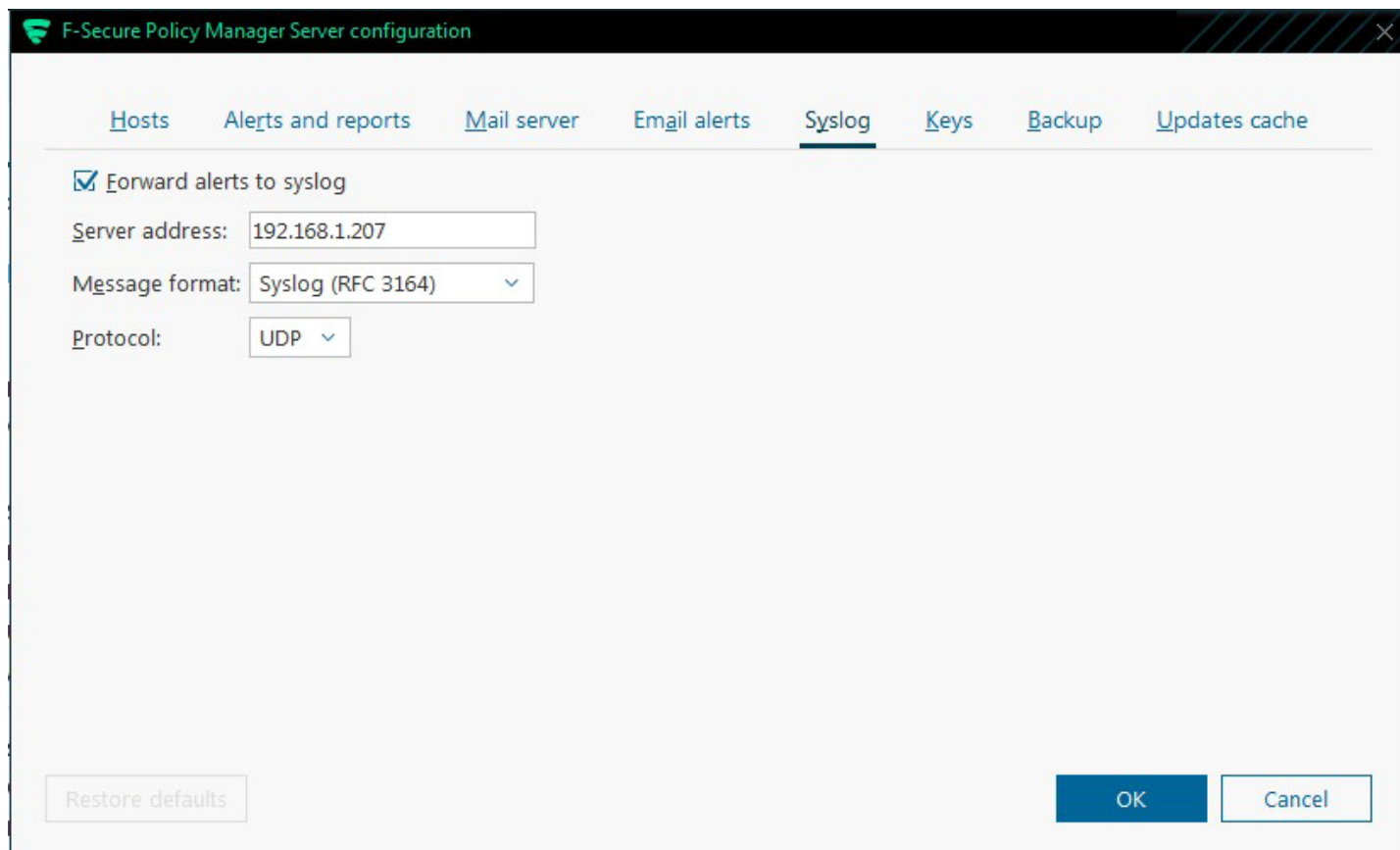


Figure 2

6. Click **OK**.

EventTracker Knowledge Pack

Once logs are received by EventTracker manager, knowledge packs can be configured into EventTracker. The following Knowledge Packs are available in EventTracker Enterprise to support F-Secure Client Security.

Alerts

- **F-Secure Client Security - Application blocked** – This alert will be generated when a suspicious application is blocked.

- **F-Secure Client Security - Spyware detected** – This alert will be generated when a spyware is detected at the endpoints.
- **F-Secure Client Security - Virus detected** – This alert will be generated when a virus is detected at the endpoints.
- **F-Secure Client Security: Malware blocked** – This alert will be generated when a malware execution is blocked.

Categories

- **F-Secure Client Security: Application Blocked**-This category provides information related to the suspicious applications or processes blocked at the endpoints and its attributes.
- **F-Secure Client Security: Web Traffic Scanning** - This category provides information related to the websites blocked at the endpoints.
- **F-Secure Client Security: Virus detected** - This category provides information related to the threats or malicious file contents detected at the endpoints and its attributes.
- **F-Secure Client Security: Spyware detected** - This category provides information related to the spywares detected at the endpoints and its attributes.

Knowledge Objects

- **F-Secure Client Security Application Blocked** - This knowledge object will help us to analyze logs related to the suspicious applications or processes blocked at the endpoints and its attributes.
- **F-Secure Client Security Web Traffic Scanning** - This knowledge object will help us to analyze logs related to websites blocked at the endpoints.
- **F-Secure Client Security Virus detected** - This knowledge object will help us to analyze threats or malicious file contents detected at the endpoints and its attributes.
- **F-Secure Client Security Spyware detected** - This knowledge object will help us to analyze logs related to the spywares detected at the endpoints and its attributes.

Flex Reports

- **F-Secure Client Security - Application blocked** – This report gives the information about suspicious applications or processes blocked at the endpoints and its attributes.

LogTime	Computer	Object ID	Host Name	Domain Tree Path	User ID	Application Path	File Hash	Message
07/05/2018 02:22:44 PM	FSECURE	1.3.6.1.4.1.2213.53.2147483647.101	Contoso-pc	root/Desktops/Desktops\Windows 10\Contoso-pc	60c8f0c8-2808-11e6-b998-7013d1562400	\\?\c:\users\ksr\downloads\slight client 84241228 (1).exe	c7d8a707a3dcc9f9e5bc505481486a54e945d468	Application was blocked. This was determined to be a high-risk application by system control heuristics. Application path: \\?\c:\users\ksr\downloads\slight client 84241228 (1).exe File hash: c7d8a707a3dcc9f9e5bc505481486a54e945d468
07/05/2018 02:22:44 PM	FSECURE	1.3.6.1.4.1.2213.53.2147483647.101	Contoso-pc	root/Desktops/Desktops\Windows 10\Contoso-pc	60c8f0c8-2808-11e6-b998-7013d1562400	\\?\c:\users\ksr\downloads\slight client 84241228.exe	c7d8a707a3dcc9f9e5bc505481486a54e945d468	Application was blocked. This was determined to be a high-risk application by system control heuristics. Application path: \\?\c:\users\ksr\downloads\slight client 84241228.exe File hash: c7d8a707a3dcc9f9e5bc505481486a54e945d468

Figure 3

Sample logs:

```

Jul 09 05:29:59 PM Jul 09 13:38:53 580f-secure02 May 28 08:00:47 fsecure Dangerous application blocked [alertMeta@0 oid="1.3.6.1.4.1.2213.53.2147483647.101" shost="dsk-s...

checksum      +- 1d8a646e3828c37a875570d92ccace3cee329cf
event_computer +- Fsecure
event_description Jul 09 13:38:53 580f-secure02 May 28 08:00:47 fsecure Dangerous application blocked [alertMeta@0 oid="1.3.6.1.4.1.2213.53.2147483647.101" shost="dsk-s-4f58192" uid="3ada24a4-8a33-11e5-919e-9a540eaf1400" domainTreePath=" Desktops/Desktops\Windows 10/" * message="Application was blocked. This was determined to be a high-risk application by system control heuristics. Application path: \\?\c:\users\jkl\appdata\local\apps\2.0-c4jh9e.w@\lokg3ege.wyg\libr..tion_3dfe2efc282aafa8_0001.0004_ab1afde63804386e\libraryadministrationazure nordic.exe File hash: 1d8a646e3828c37a875570d92ccace3cee329cf"]
event_id      +- 3333
event_log_type +- Application
event_source   +- syslog
  
```

Figure 4

- **F-Secure Client Security Web Traffic Scanning** – This report gives the information about websites blocked at the endpoints.

Computer	Object ID	User Name	User ID	Host Name	Domain Tree Path	Object Name	Threat Detail	Action	Message
FSECURE	1.3.6.1.4.1.2213.12.2147483647.722		095a73d4-a9d7-955a-e0a4-5ac10b2d5aed	Contoso-pc	root/Desktops/Desktops\Windows 10\Contoso-pc	http://www.google.dk/?sa=t&rc=j&q=3esrc=s&source=web&cd=1&ved=2ahUKEwlllM_7nbAhVHh6YKHGtVDOYQFJAeegQIARAv&url=http://Trojan.Script.745076F Trojan.Script.745076F Trojan.Script.745076F@gmail.com Trojan.Script.745076F&usq=AOvVaw3dxE3SBiHsk78gNuS2x8Wx	Trojan.Script.745076	Malicious content was blocked	Web Traffic Scanning Alert Infection: Trojan.Script.745076 Object name: http://www.google.dk/?sa=t&rc=j&q=3esrc=s&source=web&cd=1&ved=2ahUKEwlllM_7nbAhVHh6YKHGtVDOYQFJAeegQIARAv&url=http://Trojan.Script.745076F Trojan.Script.745076F@gmail.com Trojan.Script.745076F&usq=AOvVaw3dxE3SBiHsk78gNuS2x8Wx Action: Malicious content was blocked.

Figure 5

Sample logs:

Jul 09 05:29:55 PM	Jul 03 13:38:53 580f-secure02 Jun 4 14:19:27 fsecure Web Traffic Scanning Alert: Malicious Content Blocked [alertMeta@0 oid="1.3.6.1.4.1.2213.12.2147483647.207" shost="dsk-s4bkex1" uid="095a73d4-a9d7-955a-e0a4-5ac10b2d5aed" domainTreePath="Desktops/Desktops Windows 10/47.722" message="Web Traffic Scanning Alert Infection: Trojan.Script.745076 Object name: http://www.google.dk/url?sa=t&rc=tj&q=&esrc=s&source=web&cd=1&ved=2ahLUKEwiliilIM_7nbAhVHh6YKHQtvDOYQFjAAegQIARAv&url=httpATrojan.Script.745076FTrojan.Script.745076Fgmai.comTrojan.Script.745076F&usg=AOvWaw3dxE3SBiHsK78gNuS2x8Wx Action: Malicious content was blocked."]
action	+-- Malicious content was blocked
event_computer	+-- Fsecure
event_description	Jul 03 13:38:53 580f-secure02 Jun 4 14:19:27 fsecure Web Traffic Scanning Alert: Malicious Content Blocked [alertMeta@0 oid="1.3.6.1.4.1.2213.12.2147483647.207" shost="dsk-s4bkex1" uid="095a73d4-a9d7-955a-e0a4-5ac10b2d5aed" domainTreePath="Desktops/Desktops Windows 10/47.722" message="Web Traffic Scanning Alert Infection: Trojan.Script.745076 Object name: http://www.google.dk/url?sa=t&rc=tj&q=&esrc=s&source=web&cd=1&ved=2ahLUKEwiliilIM_7nbAhVHh6YKHQtvDOYQFjAAegQIARAv&url=httpATrojan.Script.745076FTrojan.Script.745076Fgmai.comTrojan.Script.745076F&usg=AOvWaw3dxE3SBiHsK78gNuS2x8Wx Action: Malicious content was blocked."]
event_id	+-- 3333
event_log_type	+-- Application
event_source	+-- syslog

Figure 6

- **F-Secure Client Security - Virus detected** – This report gives the information about threats or malicious file contents detected at the endpoints and its attributes.

Computer	Object ID	Host Name	Domain Tree Path	File Name	User Name	User ID	Action	Message	File Path
FSECURE	1.3.6.1.4.1.2213.12.2147483647.207	Contoso2-pc	root\Member Servers\Contoso2-pc	BehavesLike:BAT.Delete	williams	e6c01642-ae95-9a22-1bf4-075797350b2f	The file was quarantined	Malicious code found in file E:\cp\start\start.bat. Infection: BehavesLike:BAT.Delete Action: The file was quarantined.	E:\cp\start\start.bat.
FSECURE	1.3.6.1.4.1.2213.12.2147483647.207	Contoso-pc	root\Laptops\Laptops Windows 10\Contoso-pc	JS:Trojan.Cryxos.1623	sam	c3006ccc-2f9d-11b2-a85c-fd261fba95af	The file was quarantined	Malicious code found in file C:\Users\hnb\AppData\Local\Packa ges\Microsoft.MicrosoftEdge_8we kyb3d8bbwe\AC#\001\MicrosoftEd ge\Cache\CSZ4R4XD\index4.htm. Infection: JS:Trojan.Cryxos.1623 Action: The file was quarantined.	C:\Users\hnb\AppData\Local\Packa ges\Microsoft.MicrosoftEdge_8we kyb3d8bbwe\AC#\001\MicrosoftEd ge\Cache\CSZ4R4XD\index4.htm.

Figure 7

Sample logs:

Jul 09 05:29:54 PM	Jul 03 13:38:53 580f-secure02 Jun 11 10:19:53 fsecure Virus Alert: Quarantined [alertMeta@0 oid="1.3.6.1.4.1.2213.12.2147483647.207" shost="c3006ccc-2f9d-11b2-a85c-fd261fba95af" domainTreePath="Laptops/Laptops Windows 10/" message="Malicious code found in file C:\Users\hnb\AppData\Local\Packa ges\Microsoft.MicrosoftEdge_8we kyb3d8bbwe\AC#\001\MicrosoftEdge\Cache\BOCIZVGC\index2.htm. Infection: JS:Trojan.Cryxos.1623 Action: The file was quarantined. "]
action	+-- The file was quarantined
event_computer	+-- Fsecure
event_description	Jul 03 13:38:53 580f-secure02 Jun 11 10:19:53 fsecure Virus Alert: Quarantined [alertMeta@0 oid="1.3.6.1.4.1.2213.12.2147483647.207" shost="c3006ccc-2f9d-11b2-a85c-fd261fba95af" domainTreePath="Laptops/Laptops Windows 10/" message="Malicious code found in file C:\Users\hnb\AppData\Local\Packa ges\Microsoft.MicrosoftEdge_8we kyb3d8bbwe\AC#\001\MicrosoftEdge\Cache\BOCIZVGC\index2.htm. Infection: JS:Trojan.Cryxos.1623 Action: The file was quarantined. "]
event_id	+-- 3333
event_log_type	+-- Application
event_source	+-- syslog

Figure 8

- **F-Secure Client Security Spyware detected** – This report gives the information about spywares detected at the endpoints and its attributes.

LogTime	Computer	Host Name	User ID	Object ID	Action	Domain Tree Path	Threat Name	Threat Family	Threat Type	Object Name	Message
07/05/2018 02:22:41 PM	FSECURE	Contoso-pc	e6c01642-ae95-9a22-1bf4-075797350b2f	1.3.6.1.4.1.2213.12.2147483647.290	none	root/Member Servers/Contoso-pc	Gen:Application.Bundle.r.InstallIQ	riskware		E:\oc\FinalMediaPlayer2011Setup.exe	Spyware detected: Type: riskware Family: Name: Gen: Application.Bundler.InstallIQ Object: E:\oc\FinalMediaPlayer2011Setup.exe Action: none.
07/05/2018 02:22:42 PM	FSECURE	Contoso-pc	e6c01642-ae95-9a22-1bf4-075797350b2f	1.3.6.1.4.1.2213.12.2147483647.290	none	root/Member Servers/Contoso-pc	Application.Bundler.AHN	riskware		E:\kellu\Downloads\Setup_FileViewPro_2016.exe	Spyware detected: Type: riskware Family: Name: Application.Bundler.AHN Object: E:\kellu\Downloads\Setup_FileViewPro_2016.exe Action: none.

Figure 9

Sample logs:

Jul 09 05:30:18 PM	Jul 03 13:38:53 580f-secure02 May 6 08:48:31 fsecure Spyware Alert [alertMeta@0 oid="1.3.6.1.4.1.2213.12.2147483647.290" shost=" " uid="e6c01642...
action	+-- none
event_computer	+-- Fsecure
event_description	Jul 03 13:38:53 580f-secure02 May 6 08:48:31 fsecure Spyware Alert [alertMeta@0 oid="1.3.6.1.4.1.2213.12.2147483647.290" shost=" " uid="e6c01642-ae95-9a22-1bf4-075797350b2f" domainTreePath=" /Member Servers/ " message="Spyware detected: Type: riskware Family: Name: Gen: Application.Bundler.InstallIQ Object: E:\bc\FinalMediaPlayer2011Setup.exe Action: none. "]
event_id	+-- 3333
event_log_type	+-- Application
event_source	+-- syslog

Figure 10

Import F-Secure Client Security knowledge pack into EventTracker

NOTE: Import the knowledge pack items in the following sequence:

- Alerts
- Categories
- Knowledge Objects
- Flex Reports
- Dashlets

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

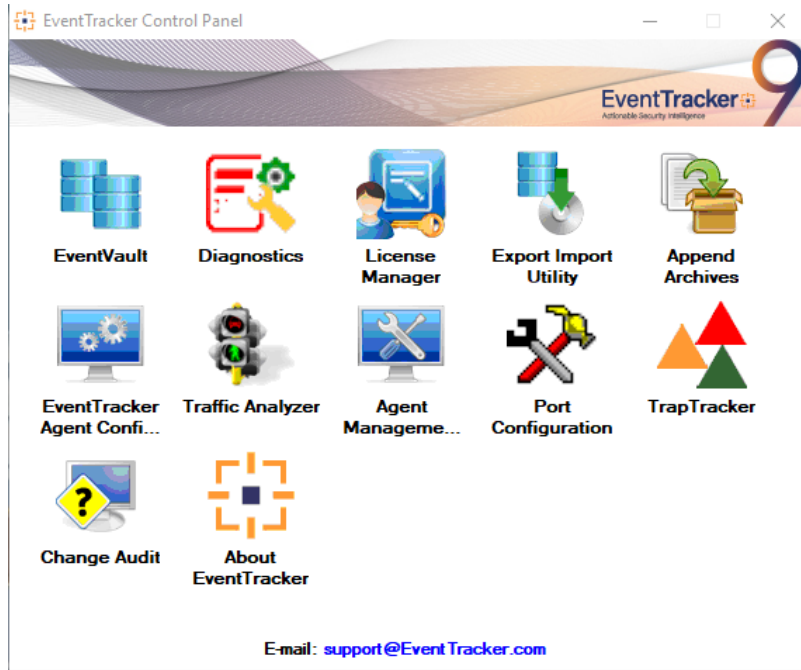



Figure 11

- 3. Click the **Import** tab.

Alerts

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

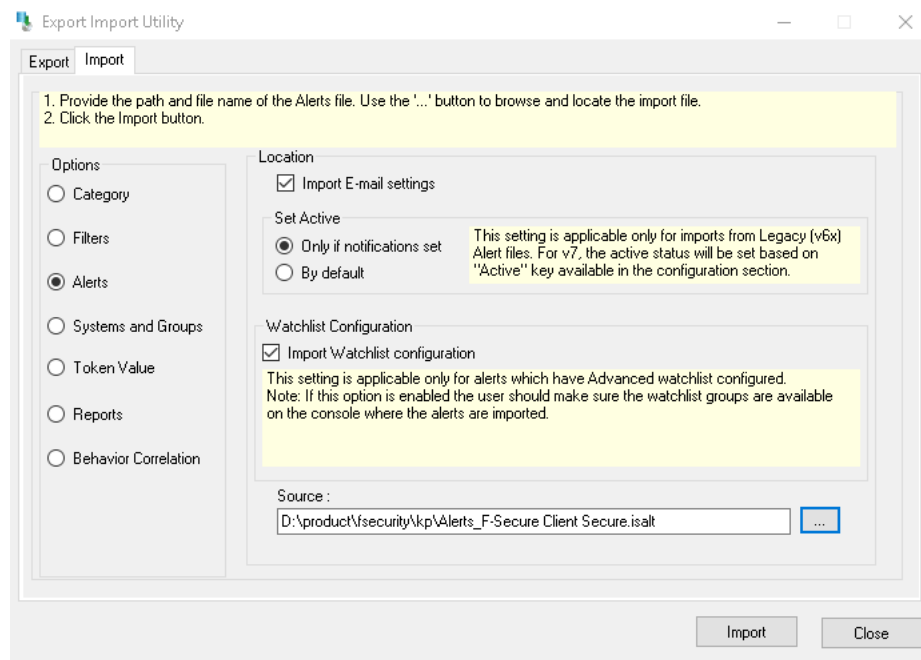


Figure 12

1. Locate **Alert_F-Secure Client Secure.isalt** file, and then click the **Open** button.
2. To import alerts, click the **Import** button.

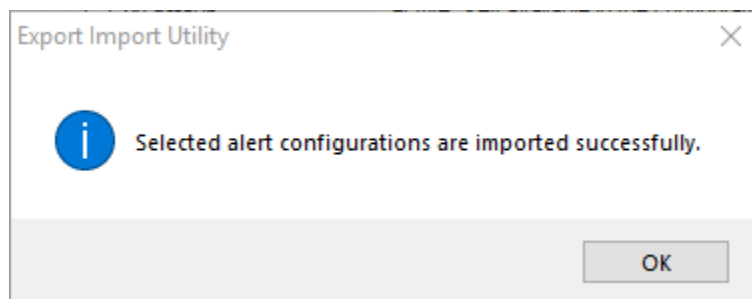


Figure 13

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

Categories

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

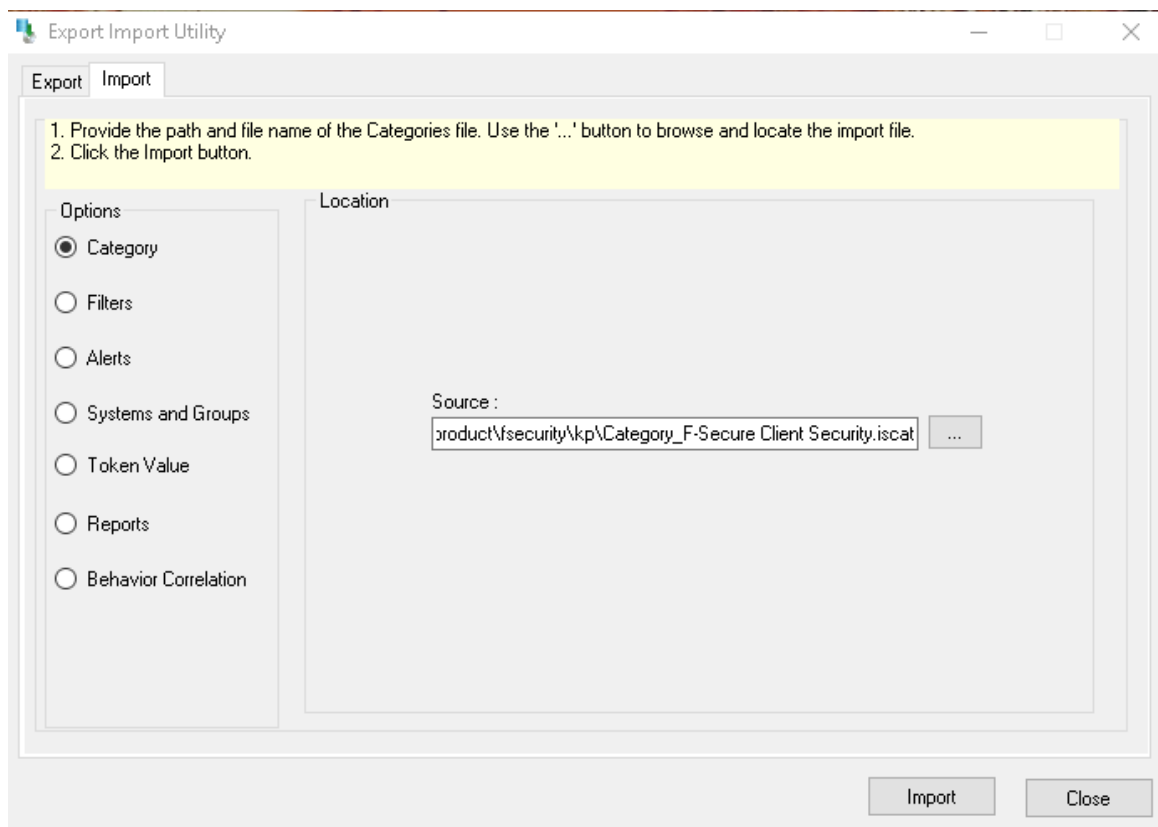


Figure 14

2. Locate **Category_F-Secure Client Security.iscat** file, and then click the **Open** button.

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

EventTracker displays a success message.

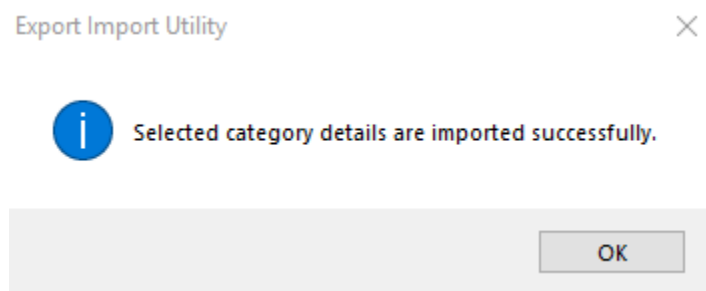


Figure 15

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

Knowledge Objects

- Click **Knowledge objects** under Admin option in the EventTracker manager page.
- Locate the file named **KO_F-Secure Client Security .etko**.

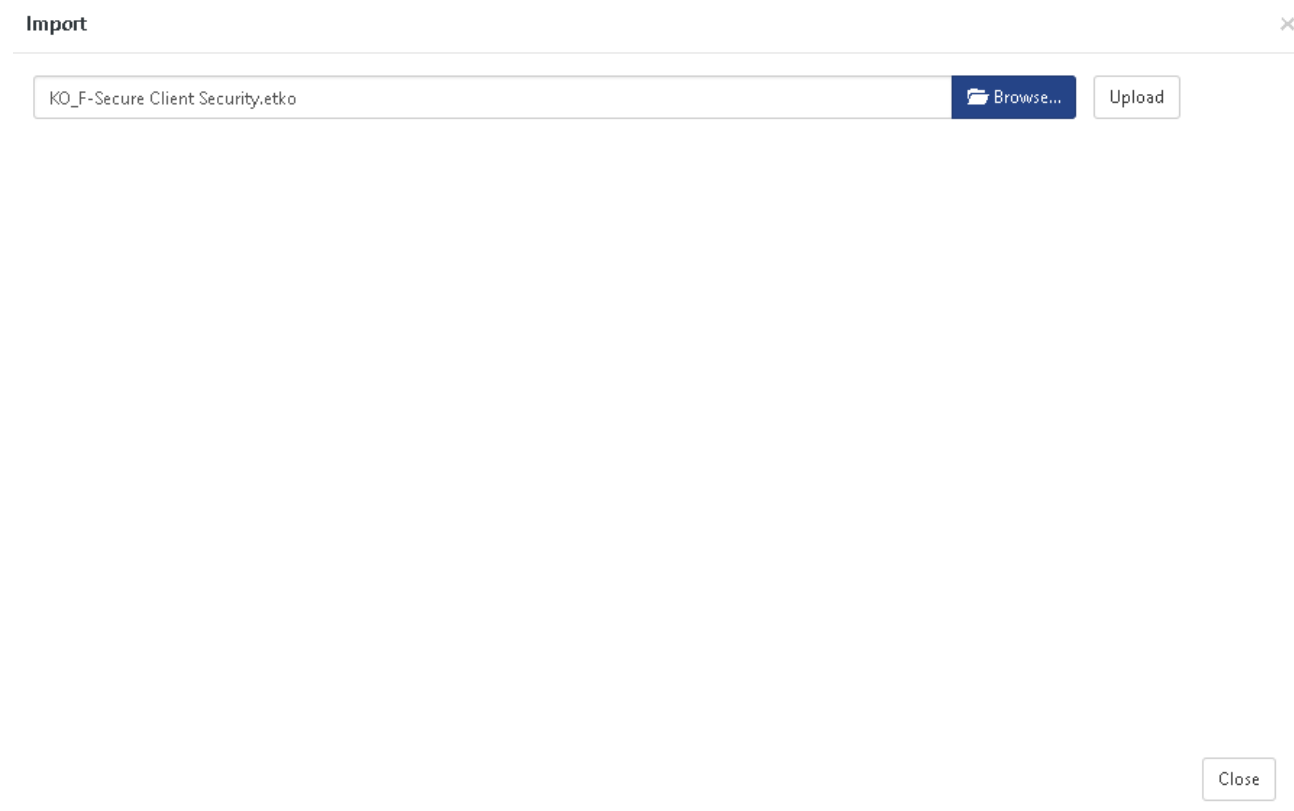


Figure 16

- Now select all the checkbox and then click on '**Import**' option.

Import



Select file...

<input checked="" type="checkbox"/> Object name	Applies to	Group name
<input checked="" type="checkbox"/> F-Secure Client Security Application Blocked	F-Secure Client Security 12.x and above	F-Secure Client Security
<input checked="" type="checkbox"/> F-Secure Client Security Spyware Detected	F-Secure Client Security 12.x and above	F-Secure Client Security
<input checked="" type="checkbox"/> F-Secure Client Security Virus Detected	F-Secure Client Security 12.x and above	F-Secure Client Security
<input checked="" type="checkbox"/> F-Secure Client Security Web Traffic Scanning	F-Secure Client Security 12.x and above	F-Secure Client Security

Figure 17

- Knowledge objects are now imported successfully.

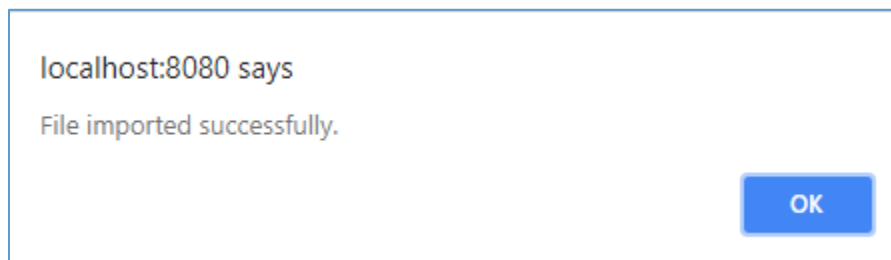




Figure 18

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 **Token_F-Secure Client.ettd**.

<input checked="" type="checkbox"/>	Template name	Separator	Template description	Added date	Added by	Group Name
<input checked="" type="checkbox"/>	F-Secure Client Security-Application blocked	\n	Jul 03 13:38:53 580f-secure02 Jun 29 11:50:49 580F-SECURE02.aabenraa.local Dangerous application blocked [alertMeta@0 oid="1.3.6.1.4.1.2213.53.2147483647.101" shost=" " uid="60c8f0c8-2808-11e6-b998-7013d1562400" domainTreePath="aa/Desktops/Desktops Windows 10/dsk-s4w31594" message="Application was blocked. This was determined to be a high-risk application by system control heuristics. Application path: \\?\c:\users\ksr\downloads\isl light client 84241228 (1).exe File hash: c7d8a707a3dcc9f9e5bc505481486a54e945d468"]	Jul 05 02:52:47 PM		F-Secure Client Security
<input checked="" type="checkbox"/>	F-Secure Client Security-Spyware Detected	\n	Jul 03 13:38:53 580f-secure02 May 4 11:13:33 580F-SECURE02.aabenraa.local Spyware Alert [alertMeta@0 oid="1.3.6.1.4.1.2213.12.2147483647.290" shost=" " uid="e6c01642-ae95-9a22-1bf4-075797350b2f" domainTreePath=" /Member Servers/580f i101" message="Spyware detected: Type: riskware Family: Malware Name: Gen:Application.Bundler.InstallIQ Object: E:\bc\FinalMedia Player2011Setup.exe Action: none. "]	Jul 05 03:39:30 PM		F-Secure Client Security
<input checked="" type="checkbox"/>	F-Secure Client Security-Virus detected	\n	Jul 04 18:44:31 NTPLDTBLR47 Jul 4 18:44:26 10.0.2.15 Virus Alert: File deleted [alertMeta@0 oid="1.3.6.1.4.1.2213.12.2147483647.202" shost="contoso-pc" uid="contoso-pc" domainTreePath="Root/contoso-pc" suser="contoso-PC\contoso" message="Malicious code found in file C:\Users\contoso\AppData\Local\Temp\537d898a-9fcf-4236-9625-1973ce5d31e5.tmp. Infection: EICAR_Test_File Action: The file was deleted. "]	Jul 05 04:23:15 PM		F-Secure Client Security
<input checked="" type="checkbox"/>	F-Secure Client Security-Web Traffic Scanning	\n	Jul 04 18:44:31 NTPLDTBLR47 Jul 4 18:44:30 10.0.2.15 Web Traffic Scanning Alert: Malicious Content Blocked [alertMeta@0 oid="1.3.6.1.4.1.2213.12.2147483647.722" shost="contoso-pc" uid="contoso-pc" domainTreePath="Root/contoso-pc" suser="contoso-PC\contoso" message="Web Traffic Scanning Alert Infection: http://www.eicar.org/download/eicarcom2.zip Object name: EICAR_Test_File Action: Malicious content was blocked."]	Jul 05 04:58:20 PM		F-Secure Client Security

Figure 19

4. Now select all the checkbox and then click on  Import option.

Flex Reports

On the EventTracker Control Panel,

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

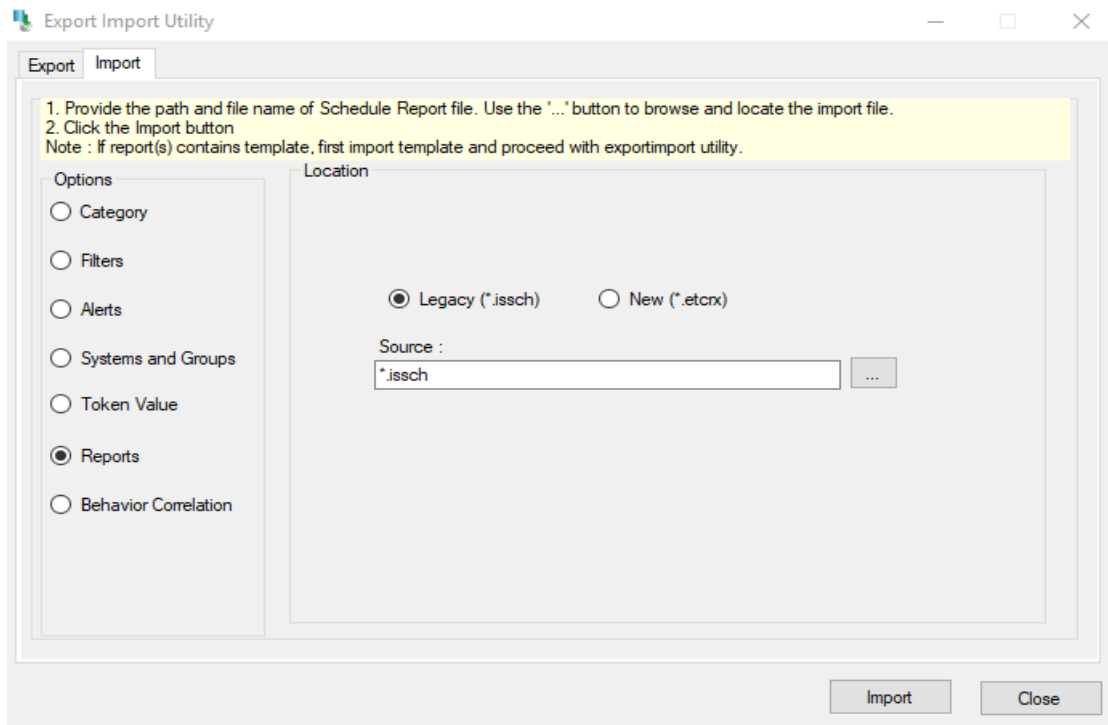


Figure 20

2. Locate the file named **Reports_ F-Secure Client Security. etcrx**, and select all the checkbox.

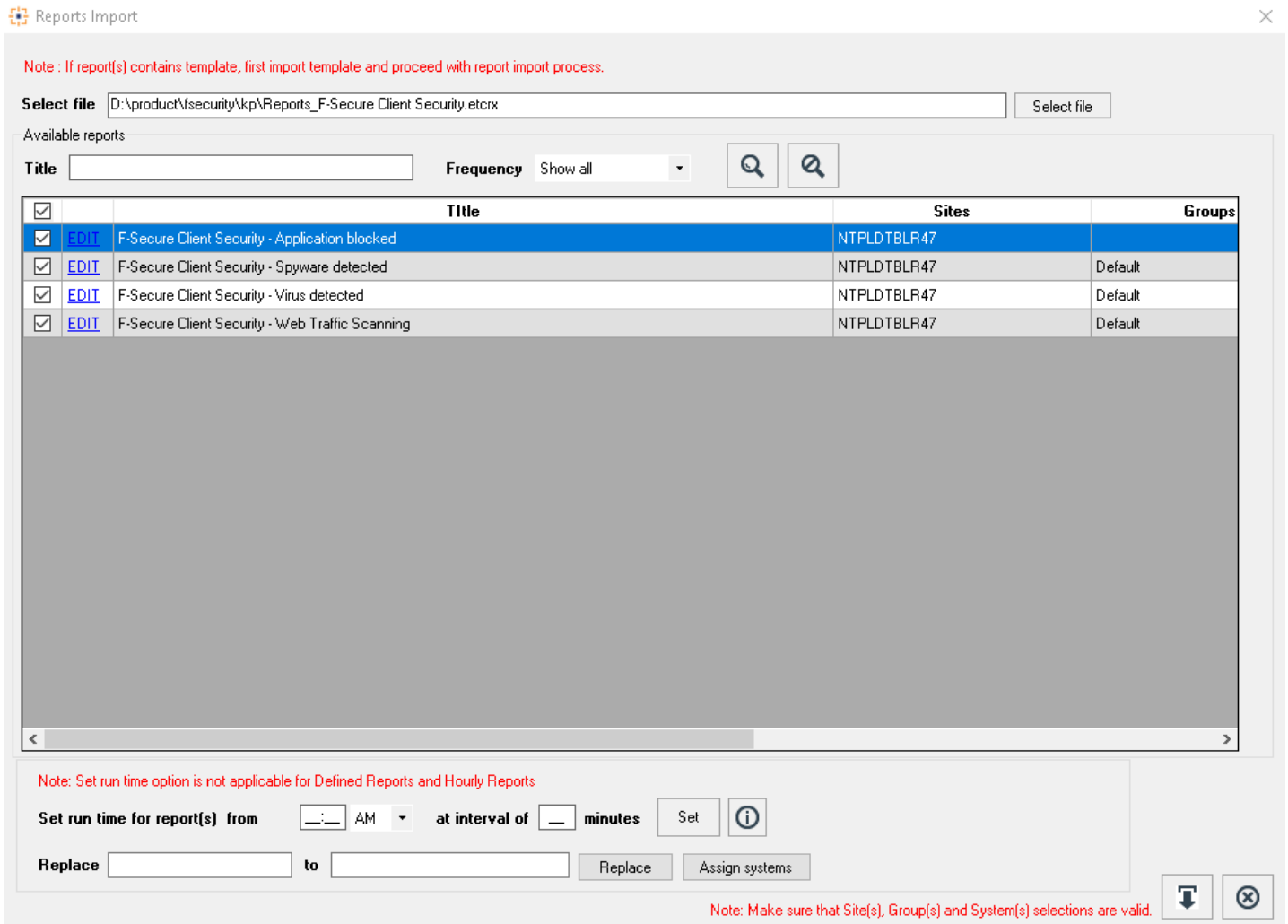


Figure 21

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

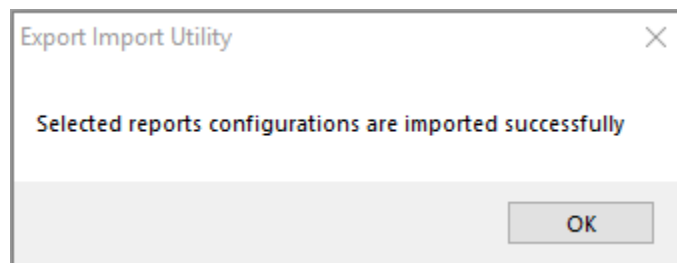


Figure 22

Dashlets

1. Open **EventTracker Enterprise** in the browser and log in.

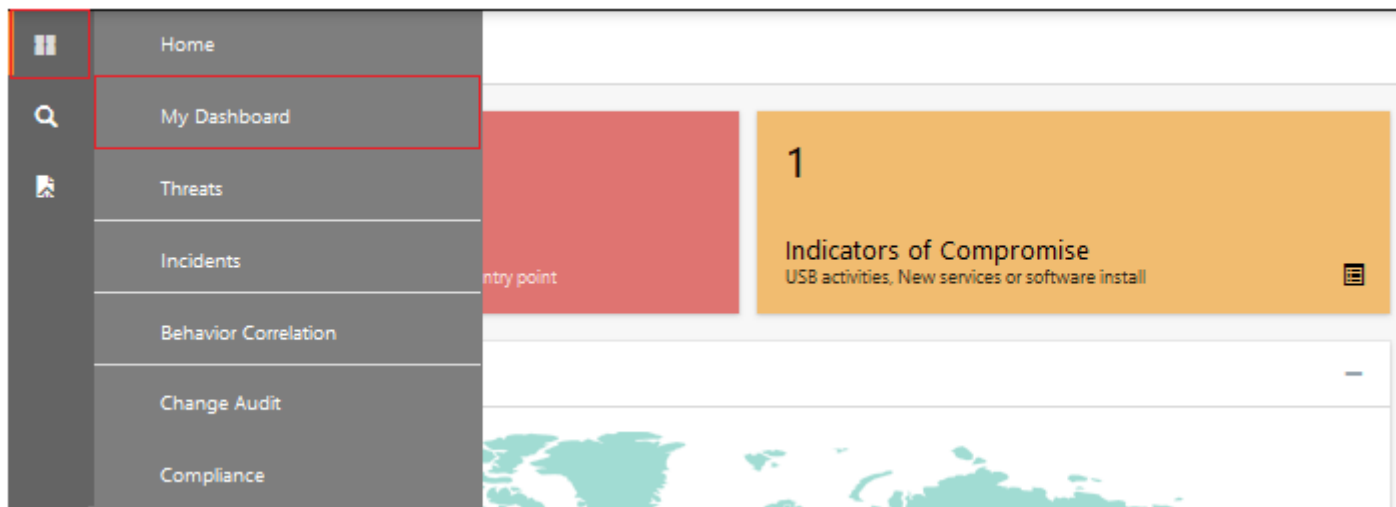



Figure 23

2. Navigate to **My Dashboard**
3. Click on import configuration  icon on the top right corner.
4. In the popup window browse the file named **Dashboard_F-Secure Client Security .etwd**.

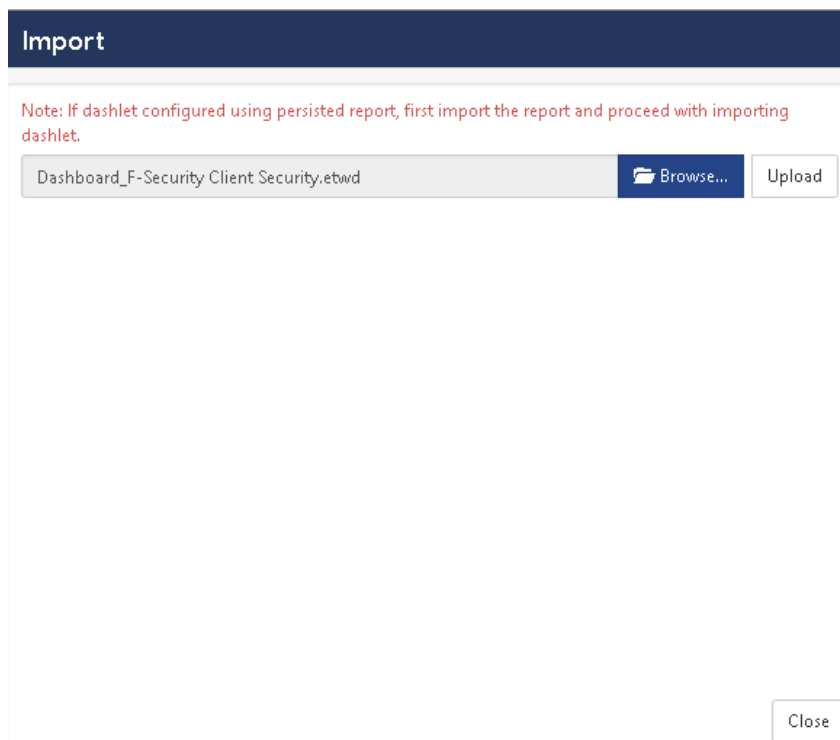


Figure 24

5. Now select all the available checkboxes and then click on **Import** option.

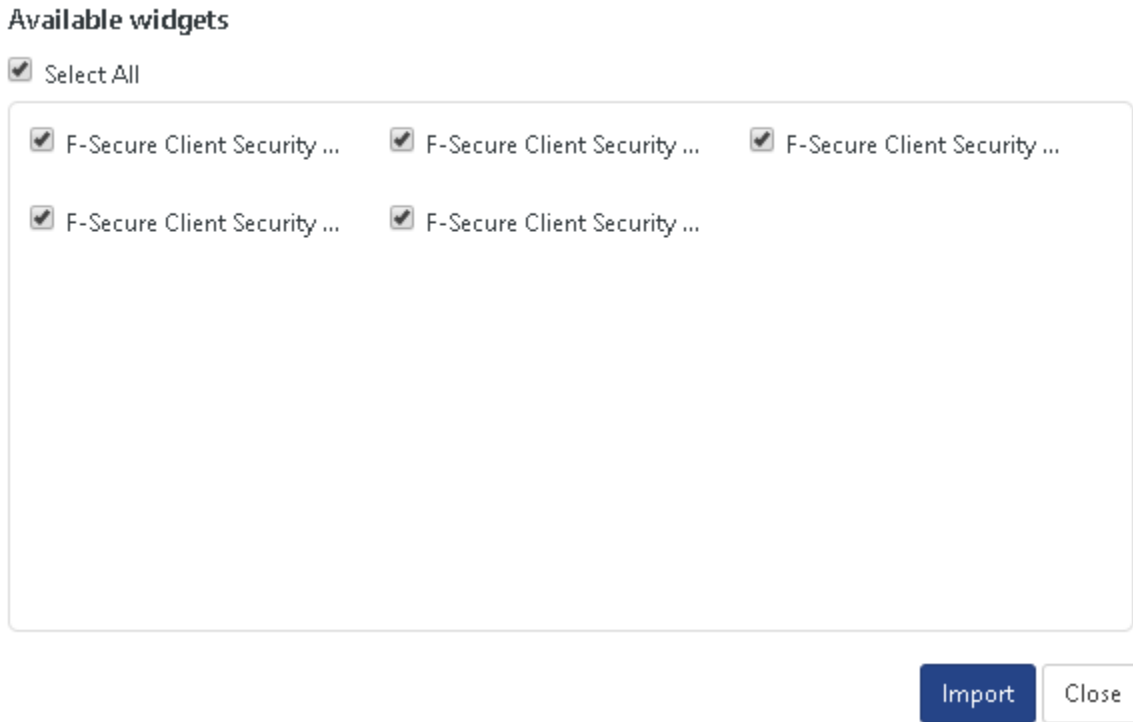



Figure 25

6. Click 'customize'  to locate and choose created dashlet.

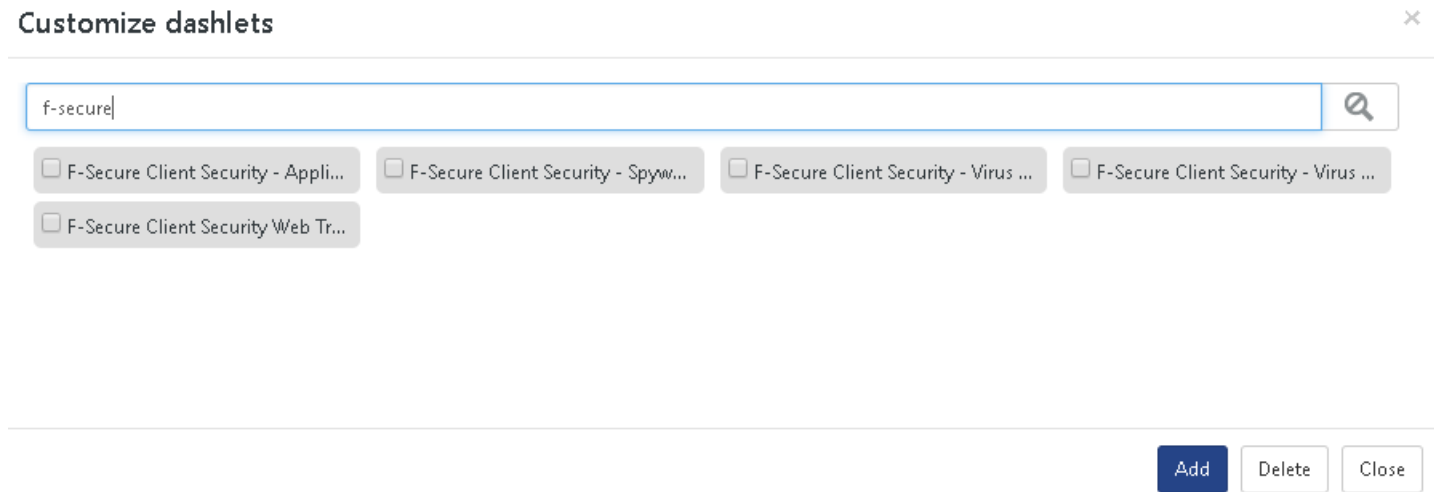


Figure 26

7. Click **Add** to add dashlet to the dashboard.

Verify F-Secure Client Security knowledge pack in EventTracker

Alerts

1. In the **EventTracker Enterprise** web interface, click the **Admin** drop-down, and then click **Alerts**.
2. In the search box, enter **F-Secure** and then click the **Search** button.
3. EventTracker displays alert of **F-secure**.

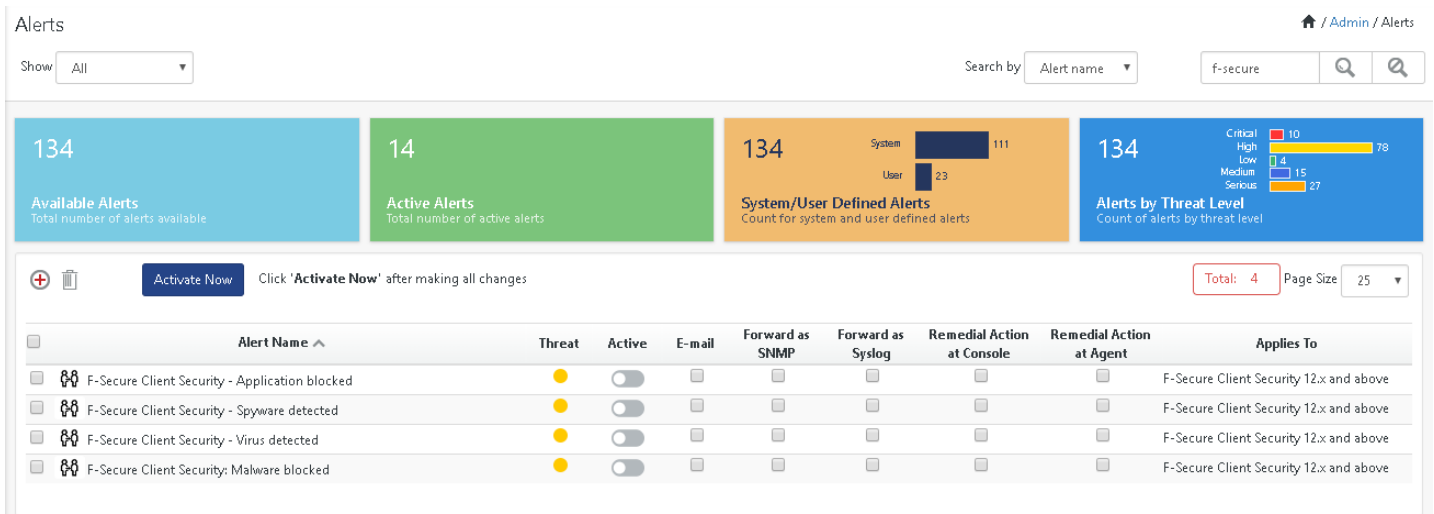


Figure 27

Categories

1. Login to **EventTracker Enterprise**.
2. Click the **Admin** drop-down, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand the F-Secure Client Security group folder to view the imported categories.

Category

Total category groups: 20 Total categories: 405

Last 10 modified categories

Name	Modified date
F-Secure Client Security - Virus Detected	Jul 09 05:27:16 PM
F-Secure Client Security - Spyware Detected	Jul 09 05:26:51 PM
F-Secure Client Security - Application Blocked	Jul 09 05:26:36 PM
F-Secure Client Security Web Traffic Scanning	Jul 06 12:27:49 PM
MS RRAS: Request Discard	Jun 26 06:56:44 PM
MS RRAS: Authentication Failure	Jun 26 06:55:56 PM
MS RRAS: Accounting Type	Jun 26 06:55:42 PM
MS RRAS: Access Reject	Jun 26 06:55:27 PM
MS RRAS: Access Accept	Jun 26 06:55:14 PM
MS RRAS: Accept-Request	Jun 26 06:55:00 PM

Figure 28

Knowledge Objects

1. In the **EventTracker Enterprise** web interface, click the **Admin** drop-down, and then click **Knowledge Objects**.
2. In the **Knowledge Object** tree, expand the **F-Secure Client Security** group folder to view the imported Knowledge objects.

Knowledge Objects

Search objects... Objects

Object name: F-Secure Client Security Application Blocked

Applies to: F-Secure Client Security 12.x and above

Rules

Title	Log type	Event source	Event id	Event type
F-Secure Client Security Application Blocked		syslog*		

Message Signature: oid=.*?shost=.*?uid=.*?domainTreePath=.*?message=\\"(Application\s+|Action\s+|by\s+malware\s+|was\s+|blocked

Message Exception:

Expressions

Expression type	Expression 1	Expression 2	Format string
Regular Expression	(?<key>\w+)\.=\"(?<value>.*?)\"		
Regular Expression	(?<=File\s+hash\);.*?(?=\\"))		1:File Hash
Regular Expression	(?<=Application\s+path\ Malware\s+path\);.*?(?=\\"))		1:Application Path

Figure 29

Token Templates

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

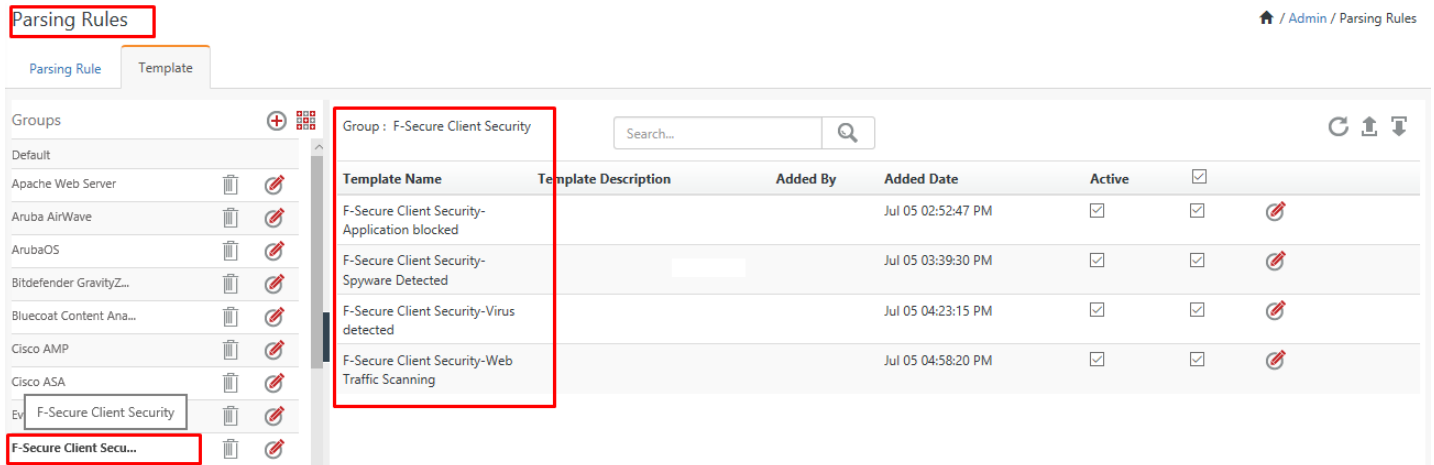


Figure 30

Flex Reports

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

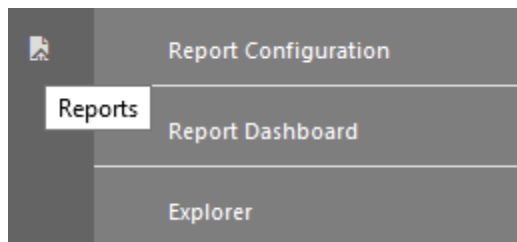


Figure 31

2. In **Reports Configuration** pane, select a **Defined** option.
3. Click on the **F-Secure Client Security** group folder to view the imported F-Secure Client Security reports.

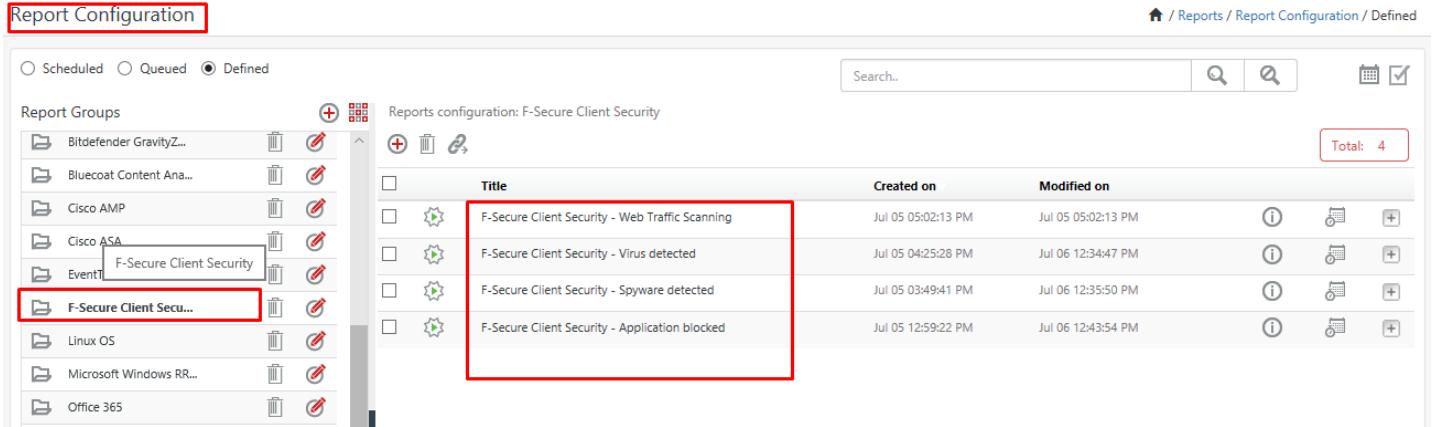


Figure 32

Dashlets

Title: F-Secure Client -Application Blocked

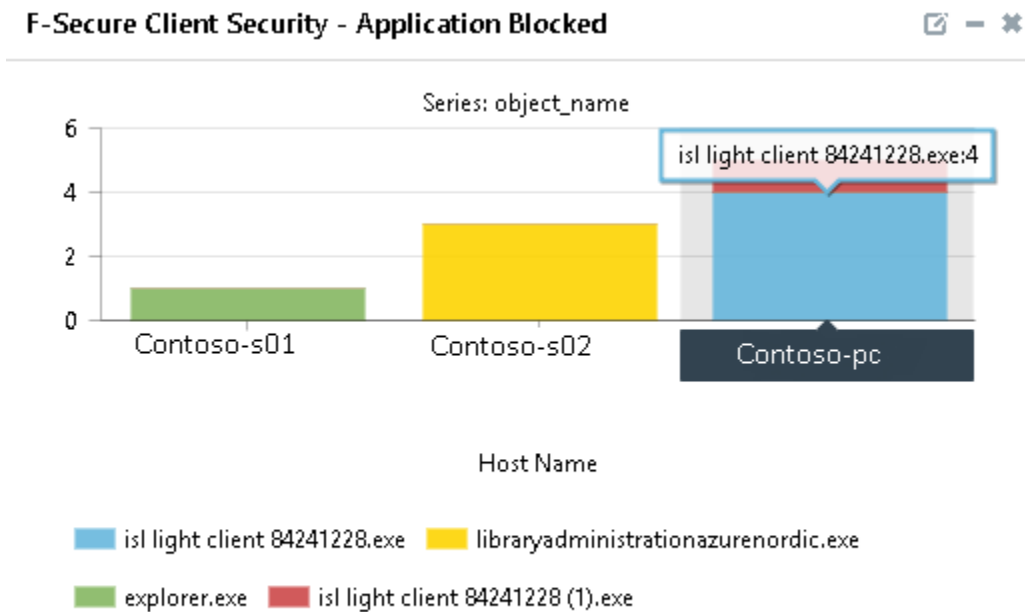


Figure 33

Title: F-Secure Client Security – Spyware Detected

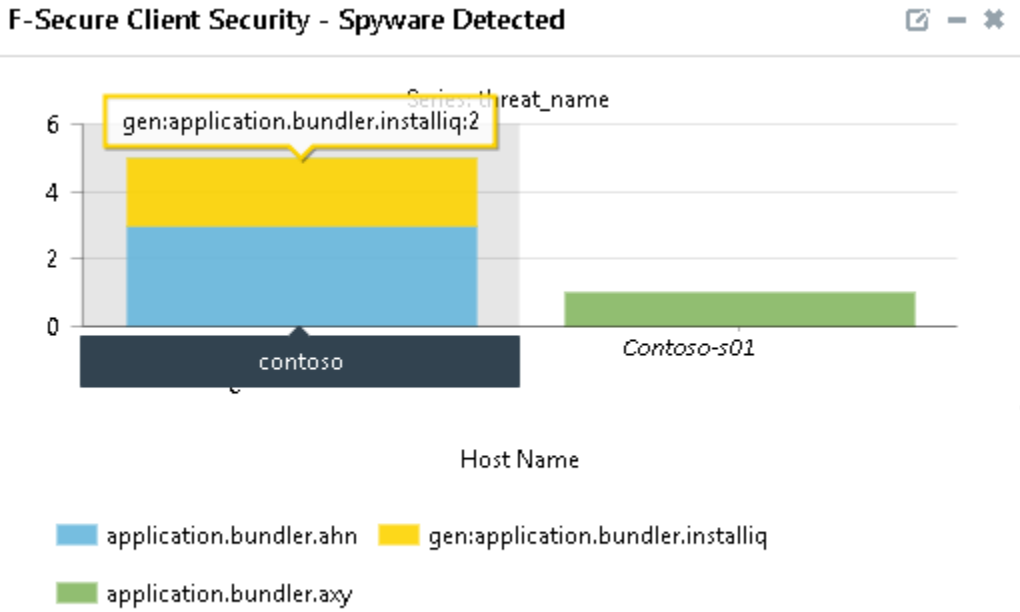


Figure 34

Title: F-Secure Client Security -Virus Detected

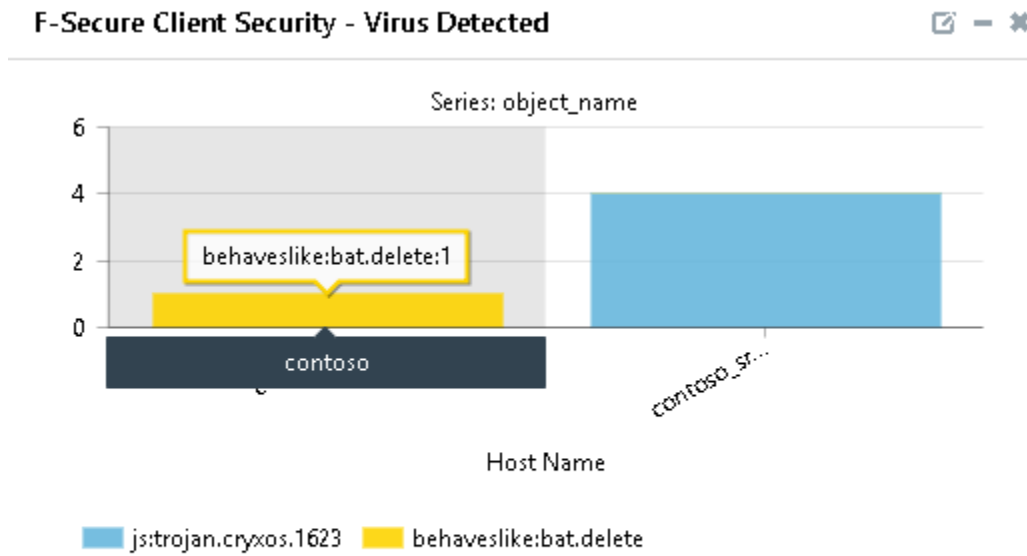


Figure 35

Title: F-Secure Client Security - Virus Detected Action

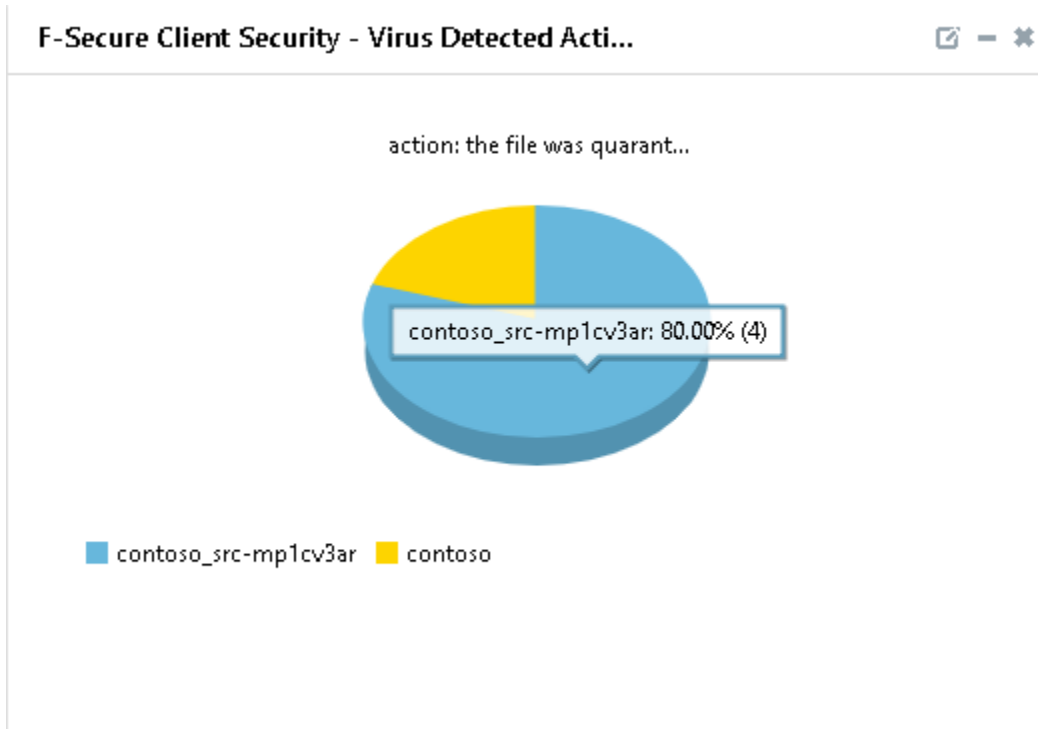


Figure 36