EventTracker:

Actionable Security Intelligence

Integrate F-Secure Client Security

EventTracker v9.x and above

Publication Date: July 13, 2018

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 Alerts	
Categories	5
Knowledge Objects	5
Flex Reports	6
Import F-Secure Client Security knowledge pack into EventTracker Alerts	
Categories	10
Knowledge Objects	11
Token Templates	12
Flex Reports	13
Dashlets	15
Verify F-Secure Client Security knowledge pack in EventTracker Alerts	
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).

Secure Policy Man	ager Server configurat	tion					
<u>H</u> osts Al	e <u>r</u> ts and reports	<u>M</u> ail server	Em <u>a</u> il alerts	Syslog	<u>K</u> eys	<u>B</u> ackup	<u>U</u> pdates cache
Forward alerts	s to syslog						
<u>S</u> erver address:	192.168.1.207						
M <u>e</u> ssage format:	Syslog (RFC 3164)	~					
Protocol:	UDP V						
							OK Cancel
						C C	OK Cancel

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	1.3.6.1.4.1.2213.53.2147483647.1 01		root/Desktops/Desktops Windows 10/Contoso-pc	60c8f0c8-2808-11e6- b998-7013d1562400	(?lo:'users'ksrldownloads'isl light client 84241228 (1).exe	c7d8a707a3dcc9f9e5bc50548148 6a54e945d468	Application was blocked. This was determined to be a high-risk application by system control heuristics. Application path: 170::users/widownloads/skilight client 84241228 (1).exe File hash: c7d8a707a3dcs99e5bc50548148 6a54e945468
07/05/2018 02:22:44 PM	FSECURE	1.3.6.1.4.1.2213.53.2147483647.1 01		root/Desktops/Desktops Windows 10/Contoso-pc	60c8f0c8-2808-11e6- b998-7013d1562400	(?)c:\usersiksn\downloads\isl light client 84241228.exe	c7d8a707a3dcc9f9e5bc50548148 6a54e945d468	Application was blocked. This was determined to be a high-risk application by system control heuristics. Application path: 170c/users/ksr/downloads/isl light client 64241226 exe File hash: c7d8a707a3dcc919e5bc50548148 6a54e945d468

Figure 3

Sample logs:

 Jul 09 05:29:59 PM 	Jul 03 13:38:53 580F-secure02 May 28 08:00:47 fsecure Dangerous application bloc	ked [alertMeta@0 oid="1.3.6.1.4.1.2213.53.214	47483647.101" shost="dsk-s
hecksum	+- 1d8a646e3828c37a875570d92ccace3ceea329cf		
event_computer	+- Facure		
event_description	Jul 03 13:38:53 580F-secure02 May 28 08:00:47 fsecure Dangerous application bloc	ked [alertMeta@0 oid="1.3.6.1.4.1.2213.53.21	47483647.101" shost="dsk-s
	4r58192" uid="3ada24a4-8a33-11e5-919e-9a540eaf1400" domainTreePath="	Desktops/Desktops Windows 10/	" message="Applicati
	on was blocked. This was determined to be a high-risk application by system cor	trol heuristics. Application path: \?\c:\users\	jkl\appdata\local\apps\2.0
	c4jh9le.w8r\lokg3ege.wyg\librtion_3dfe2efc282aafa8_0001.0004_ab1afde6380438	96e\libraryadministrationazurenordic.exe File	hash: 1d8a646e3828c37a875
	570d92ccace3ceea329cf"]		
vent_id	+- 3333		
vent_log_type	+- Application		
went source	+- syslog		

Figure 4

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

Compute	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 7 22		095a73d4-e907-955a-e0a4- 5ac10b2d5aed	Contoso-pc	root/Desktops Windows 10/Contoso-pc	http://www.google.dk/u17sa-45rd =)&q=&erc=s&surce=web&cd=t =&ved=zahu/EK-willim/_ThoAhV1thgV KHGtVDOYQFJAAegQIARAv&uth ttpATrojan_SCript.745076F7orjan_S cript.745076Fgmai.comTrojan_Scrip t.745076F&usg=AQvVaw3dxE3SB IHsK78ghUsS2x8Wx	Trojan.Script.745076		Web Traffic Scanning Alert Infection: Trojan.Script.745076 Object name: http://www.google.dk/url?sa=t&rct 3&red=2ahUKEwilliM_7nbAhVH6V KHGtVDOYGFJAAeg0IARAv&url+ tgATrojan.Script.745076FTrojan.S cript.745076Fgmai.comTrojan.Script 1.745076F8usg=AAOVTvav3dx2535 Hist/T8g1uS2x8Wx.Action: Malicious content was blocked.
					Figure	E			



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="1.3.6.1.4.1.2213.12.21474836.
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="1.3.6.1.4.1.2213.12.21474836
	47.722" shost="dsk-s4bkex1" uid="095a73d4-a9d7-955a-e0a4-5ac10b2d5aed" domainTreePath=" /Desktops/Desktops Windows 10/ "
	message="Web Traffic Scanning Alert Infection: Trojan.Script.745076 Object name: http://www.google.dk/url?sa=t&rct=j&q=&esrc=s&source=web&cd
	=1&ved=2ahUKEwililiM_7nbAhVHh6YKHQtvDOYQFjAAegQIARAv&url=httpATrojan.Script.745076FTrojan.Script.745076Fgmai.comTrojan.Script.745076F&
	usg=AOvVaw3dxE3SBiHsK78gNuS2x8Wx 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	1.3.6.1.4.1.2213.12.2147483647.2 07	Contoso2-pc	rootMember Servers/Contoso2-pc	BehavesLike:BAT.Delet e	williams	e6c01642-ae95-9a22-1bf4- 075797350b2f	The file was quarantined	Malicious code found in file E:ljcp\start\start.bat. Infection: BehavesLike:BAT.Delete Action: The file was quarantined.	E:\jcp\start\start.bat.
FSECURE	1.3.6.1.4.1.2213.12.2147483647.2 07	Contoso-pc	root/Laptops/Laptops Windows 10/Contoso-pc	JS:Trojan.Cryxos.1623	sam	c3006ccc-2f9d-11b2-a85c- fd261fba95af	The file was quarantined	C:\Users\hnb\AppData\Local\Packa	kyb3d8bbwe\AC\#!001\MicrosoftEd

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: Quaranti	ned [alertMeta@0 oid="1.3.6.1.4.1.2213.12.2	147483647.207" shost="
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: Quaranti	ined [alertMeta@0 oid="1.3.6.1.4.1.2213.12.2	147483647.207" shost="
	'uid="c3006ccc-2f9d-11b2-a85c-fd261fba95af" domainTreePath="	/Laptops/Laptops Windows 10/	" message="Malicious code fo
	und in file C:\Users\hnb\AppData\Local\Packages\Microsoft.MicrosoftE	dge_8wekyb3d8bbwe\AC\#!001\MicrosoftE	dge\Cache\BOCIZVGC\index2.htm. In
	fection: 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.



	Compute							-			
ogTime 7/05/2018 02:22:41 PM	r FSECURE	Host Name Contoso-pc		Object ID 1.3.6.1.4.1.2213.12.2147483647.	Action none	Domain Tree Path root/Member	Threat Name Gen:Application.Bundle	Threat Family	Threat Type riskware		Message Spyware detected: Type: riskwa
			1bf4-075797350b2f	290		Servers/Contoso-pc				p.exe	Family: Name: Gen:Application.Bundler.InstallIG
											Object: E:\bcl\FinalMediaPlayer2011Setu
											xe Action: none.
7/05/2018 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.AH		riskware	E:\kelu\Downloads\Setup_FileVi ewPro_2016.exe	Spyware detected: Type: riskwa Family: Name:
											Application.Bundler.AHN Object: E:\kelu\Downloads\Setup_File\Vie
											Pro_2016.exe Action: none.
						Figure 9					
						Figure 9					
ample los	a ¢.					Figure 9					
ample lo	gs:					Figure 9					
ample log	-		Jul 03 13:38:53	580f-secure02 May 6 08:48	3:31 fsec	-	: [alertMeta@0 oid=	="1.3.6.1.4.1.2	2213.12.2147	7483647.290" shost="	" uid="ебс01642
	-		Jul 03 13:38:53	580f-secure02 May 6 08:48	3:31 fsec	-	:[alertMeta@0 oid=	="1.3.6.1.4.1.2	2213.12.2147	7483647.290" shost="	" uid="e6c01642
	-		Jul 03 13:38:53 +- none	580f-secure02 May 6 08:48	3:31 fsec	-	: [alertMeta@0 oid=	="1.3.6.1.4.1.2	2213.12.2147	7483647.290" shost="	" uid="e6c01642
Jul 09 05:30:18	-			580f-secure02 May 6 08:48	3:31 fsec	-	:[alertMeta@0 oid=	="1.3.6.1.4.1.2	2213.12.2147	7483647.290" shost="	" uid="e6c01642
Jul 09 05:30:18	PM		+- none +- Fsecure	580f-secure02 May 6 08:48 580f-secure02 May 6 08:48		ure Spyware Alert	-				" uid="e6c01642 ' uid="e6c01642-
Jul 09 05:30:18 action event_computer	PM		+- none +- Fsecure Jul 03 13:38:53		B:31 fsec	:ure Spyware Alert cure Spyware Alert	-	="1.3.6.1.4.1.;	2213.12.214		' uid="e6c01642-
Jul 09 05:30:18 action event_computer	PM		 +- none +- Fsecure Jul 03 13:38:53 ae95-9a22-1bf 	580f-secure02 May 6 08:44	B:31 fsec TreePath	:ure Spyware Alert cure Spyware Alert :="/Merr	t [alertMeta@0 oid: nber Servers/	="1.3.6.1.4.1.; " message=	2213.12.214	7483647.290" shost="	' uid="e6c01642-
Jul 09 05:30:18 action event_computer	PM		 +- none +- Fsecure Jul 03 13:38:53 ae95-9a22-1bf 	- 580f-secure02 May 6 08:44 4-075797350b2f" domainT	B:31 fsec TreePath	:ure Spyware Alert cure Spyware Alert :="/Merr	t [alertMeta@0 oid: nber Servers/	="1.3.6.1.4.1.; " message=	2213.12.214	7483647.290" shost="	' uid="e6c01642-
Jul 09 05:30:18 action event_computer event_description	PM		 +- none +- Fsecure Jul 03 13:38:53 ae95-9a22-1bf pplication.Bur 	580f-secure02 May 6 08:44 4-075797350b2f" domainT Idler.InstallIQ Object: E:\bo	B:31 fsec TreePath	:ure Spyware Alert cure Spyware Alert :="/Merr	t [alertMeta@0 oid: nber Servers/	="1.3.6.1.4.1.; " message=	2213.12.214	7483647.290" shost="	'uid="e6c01642-

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**.



EventTracker Con	trol Panel			_	\times
	annen	- John	Ev	entTracker	9
EventVault	Diagnostics	License Manager	Export Import Utility	Append Archives	
00		X	\mathbf{X}		
EventTracker Agent Confi	Traffic Analyzer	Agent Manageme	Port Configuration	TrapTracke	r
?	- 문급 -				
Change Audit	About EventTracker				
	E-mail: s	support@EventTra	cker.com		
		Figure 11			

3. Click the **Import** tab.

Alerts

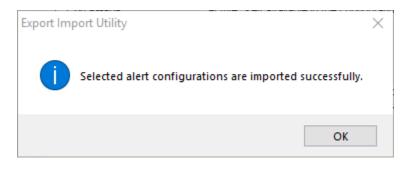
1. Click Alert option, and then click the browse

port Import		
. Provide the path and file na 2. Click the Import button.	ame of the Alerts file. Use the '' but	ton to browse and locate the import file.
Options	Location	
Category	Import E-mail settings	
03,	Set Active	
 Filters 	Only if notifications set	This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on
Alerts	 By default 	"Active" key available in the configuration section.
Systems and Groups	Watchlist Configuration	
Systems and Groups	Import Watchlist configurat	ion
🔘 Token Value		for alerts which have Advanced watchlist configured.
O D		the user should make sure the watchlist groups are available
Reports	off the console where the aler	s are imported.
Behavior Correlation		
	Source :	
	D:\product\fsecurity\kp\Ale	erts_F-Secure Client Secure.isalt

button.



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





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

Categories

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

New York Import Utility	_		\times
Export Import			
 Provide the path and file name of the Categories file. Use the '' button to browse and locate the import file. Click the Import button. 			
Options Location Category Filters Alerts Systems and Groups Source :			
Impo	ort	Close	;

Figure 14

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



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

EventTracker displays a success message.

Export Im	port Utility	\times
1	Selected category details are imported successfully.	
	ОК	
	Figure 15	

4. 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 file named KO_F-Secure Client Security .etko.

I	Import				×
	KO_F-Secure Client Security.etko	🗁 Browse	Upload		

Close	
-------	--

Figure 16

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



×

Import

Select file 🗁 Browse					
1	Object name	Applies to	Group name		
1	F-Secure Client Security Application Blocked	F-Secure Client Security 12.x and above	F-Secure Client Security		
/	F-Secure Client Security Spyware Detected	F-Secure Client Security 12.x and above	F-Secure Client Security		
•	F-Secure Client Security Virus Detected	F-Secure Client Security 12.x and above	F-Secure Client Security		
*	F-Secure Client Security Web Traffic Scanning	F-Secure Client Security 12.x and above	F-Secure Client Security		

Import Close

Figure 17

4. Knowledge objects are now imported successfully.

localhost:8080 says	
File imported successfully.	
	ОК



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 Token_F-Secure Client.ettd.



Template name	Separator	Template description	Added date	Added by	Group Name
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 appli cation by system control heuristics. Application path: \?\c:\users\ksr\downloads\isl light client 84241228 (1).exe File hash: c7d8a707a 3dcc9f9e5bc505481486a54e945d468"]	Jul 05 02:52:47 PM		F-Secure Client Security
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="1.3.6.1.4.1.2213.12.21 47483647.290" shost=""""""""""""""""""""""""""""""""""""	Jul 05 03:39:30 PM		F-Secure Client Security
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="1.3.6.1.4.1.2213.12.2147483647.20 2" shost="contoso-pc" uid="contoso-pc" domainTreePath="Root/contoso-pc" suser="contoso-PC\contoso" message="Malicious co de found in file C:\Users\contoso\AppData\Loca\\Temp\537d898a-9fcf-4236-9625-1973ce5d31e5.tmp. Infection: EICAR_Test_File Act ion: The file was deleted. "]	Jul 05 04:23:15 PM		F-Secure Client Security
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/co ntoso" 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 \mathbb{T} Import option.

Flex Reports

On the EventTracker Control Panel,

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

Options	late, first import template and proceed with exportimport utility.	
) Filters		
Alerts	Legacy (*.issch) New (*.etcrx)	
Systems and Groups	Source :	
	*issch	
) Token Value		
Reports		
Behavior Correlation		
-		
) benavior correlation		



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

Reports Import				\times
Note : If report(s) contains template, first import template and proc	eed with report import process.			
Select file D:\product\fsecurity\kp\Reports_F-Secure Client S	ecurity.etcrx		Select file	e
Available reports			7	
Title	Frequency Show all	- Q Q		
	Title		Sites	Groups
EDIT F-Secure Client Security - Application blocked			NTPLDTBLR47	
EDIT F-Secure Client Security - Spyware detected			NTPLDTBLR47	Default
EDIT F-Secure Client Security - Virus detected			NTPLDTBLR47	Default
EDIT F-Secure Client Security - Web Traffic Scanning			NTPLDTBLR47	Default
<				>
Note: Set run time option is not applicable for Defined Reports a	and Hourly Reports			
Set run time for report(s) from	at interval of minutes	Set 🚺		
Replace to	Replace	Assign systems		
		Note: Make sure tha	at Site(s), Group(s) and System(s) selection	s are valid.

Figure 21

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

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

Figure 22



Dashlets

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

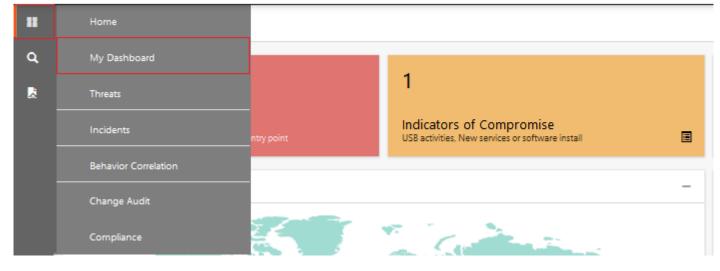


Figure 23

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

Import						
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.						
Dashboard_F-Security Client Security.e	twd		🗁 Browse	Upload		
				Close		
	Figure 2	4				



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

Available widgets



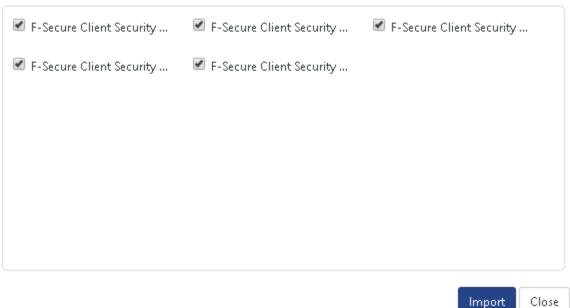


Figure 25

6. Click 'customize' (a) to locate and choose created dashlet.



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.

·							Search by	Al	f-secure Q
							concir by	Alert name 🔻	f-secure 🔍 🦉
	14				134	System User	23	134	Critical 10 High Low 14 Madium 15 Serious 27
available					System/Use Count for syst	r Defined Alei em and user defi	ts ned alerts		Threat Level lerts by threat level
Activate Now Click 'Activate No	w' after making all changes	5							Total: 4 Page Size 25
Alert Name ∧		Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
ent Security - Application blocked		•							F-Secure Client Security 12.x and above
ent Security - Spyware detected		•							F-Secure Client Security 12.x and above
ent Security - Virus detected		•							F-Secure Client Security 12.x and above
ent Security: Malware blocked		•							F-Secure Client Security 12.x and above
		Activate Now Click 'Activate Now' after making all changes Alert Name Alert Security - Application blocked ent Security - Spyware detected ent Security - Virus detected	available Total number of active alerts Activate Now Click 'Activate Now' after making all changes Alert Name A Threat ent Security - Application blocked ent Security - Spyware detected ent Security - Virus detected	Activate Now Click 'Activate Now' after making all changes Alert Name Alert Name Alert Security - Application blocked Activate Security - Spyware detected Alert Security - Virus Alert Securit	Activate Now Click 'Activate Now' after making all changes Alert Name Alert Name Alert Security - Application blocked ent Security - Spyware detected ent Security - Virus detected Diamon Security - Virus	Activate Now Click 'Activate Now' after making all changes Forward as SIMM Alert Name ^ Threat Active E-mail Forward as SIMM ent Security - Application blocked Image:	Activate Now Click 'Activate Now' after making all changes Forward as SNMP Forward as SNMP Alert Name ^ Threat Active E-mail Forward as SNMP Syslog ent Security - Application blocked Image: Comparison of the security - Spyware detected <	Activate Now Click 'Activate Now' after making all changes Forward as Syslog Forward as Syslog Remedial Action at Console Alert Name ^ Threat Active E-mail Forward as Syslog Remedial Action at Console ent Security - Application blocked Image: Comparison of the comparison of th	Activate Now Click 'Activate Now' after making all changes Count for system and user defined alerts Count of all changes Alert Name A Threat Active E-mail Forward as System Remedial Action at Agent ent Security - Application blocked Image: Active alerts Image: Active alerts

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 Tree Search	Total category groups: 20 Total categories: 405	
All Categories	Last 10 modified categories	
🗐 *All error events 🗐 *All information events	Name	Modified date
- 🗐 *All warning events	F-Secure Client Security - Virus Detected	Jul 09 05:27:16 PM
Security: All security events	F-Secure Client Security - Spyware Detected	Jul 09 05:26:51 PM
🗈 🔁 Aruba AirWaive	F-Secure Client Security - Application Blocked	Jul 09 05:26:36 PM
🖶 🔁 Aruba OS	F-Secure Client Security Web Traffic Scanning	Jul 06 12:27:49 PM
🖶 🔁 Bitdefender GravityZone	MS RRAS: Request Discard	Jun 26 06:56:44 PM
Bluecoat Content Analysis	MS RRAS: Authentication Failure	Jun 26 06:55:56 PM
Change Audit	MS RRAS: Accounting Type	Jun 26 06:55:42 PM
Cisco ASA Firewall	MS RRAS: Access Reject	Jun 26 06:55:27 PM
+ 🔁 EventTracker	MS RRAS: Access Accept	Jun 26 06:55:14 PM
🖶 🔁 F-Secure Client Security	MS RRAS: Accept-Request	Jun 26 06:55:00 PM
F-Secure Client Security - Applicati		
F-Secure Client Security - Spyware		

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							📌 / Admi	n / Knowle	dge O)bject
Search objects	Q	Q Activate N	Now				Obje	cts 🕂 🗍	i 1	; \$
Groups 🕀 🧭 🗓		st name F-Secure Client Se esto F-Secure Client Secu	ecurity Application Blocked rity 12.x and above					٢		¢
F-Secure Client Security -Secure Client Securit Ø 🏥 -Secure Client Securit Ø 前	Rules	Title	1	Event source	Event id	Event type				
-Secure Client Securit 🧭 🏢	+	F-Secure Client Security /	Log type	syslog*	Eventia	Event type		<i>i</i>	<u>ش</u>	Ð.
-Secure Client Securit 🧭 🏢	_			ath\=.*?message\=\"(Application\s+ A	ction\s+by\s+malware\s+)was∖s+blocked		00		#7
Forti-test		Message Exception:								
Fortigate Firewall		Expressions								
IIS Web Server		Expression type	Expression 1			Expression 2	For mat string			
		Regular Expression	(? <key>\w+)\=\"(?<value>.*?)\</value></key>						١	
Linux OS		Regular Expression	(?<=File\s +hash\:).*?(?=\"\])				1:File Hash			
Linux Test		Regular Expression	(?<=Application\s+path\: Malw	vare\s+path\:).*?(?=File\s+hash\:)			1:Application Path		2	



Token Templates

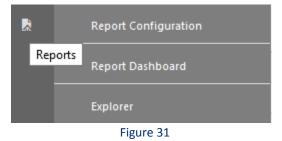
- 1. In the EventTracker Enterprise web interface, click the Admin drop-down, and then click Parsing rules.
- 2. On **Template** tab, click on the **Cisco IWAN** group folder to view the imported Token Values.

Parsing Rules									🔒 / Adı	min / Parsing Rules
Parsing Rule Template										
Groups		+	Group : F-Secure Client Security	Search	Q					CİŢ
Default		^								
Apache Web Server	Ē	1	Template Name	Template Description	Added By	Added Date	Active	\checkmark		
Aruba AirWave	Ē	۲	F-Secure Client Security- Application blocked			Jul 05 02:52:47 PM	\checkmark		0	
ArubaOS	Ē	1	F-Secure Client Security-			Jul 05 03:39:30 PM	Active 🗹			
Bitdefender GravityZ	Ē	1	Spyware Detected						0	
Bluecoat Content Ana	Ē	1	F-Secure Client Security-Virus detected			Jul 05 04:23:15 PM	\checkmark	\checkmark	Ø	
Cisco AMP	Ē	1	F-Secure Client Security-Web			Jul 05 04:58:20 PM			Ø	
Cisco ASA	Ē	1	Traffic Scanning						0	
Ev F-Secure Client Security	Ī	1	L	_						
F-Secure Client Secu	Ē	1								

Figure 30

Flex Reports

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



- 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.

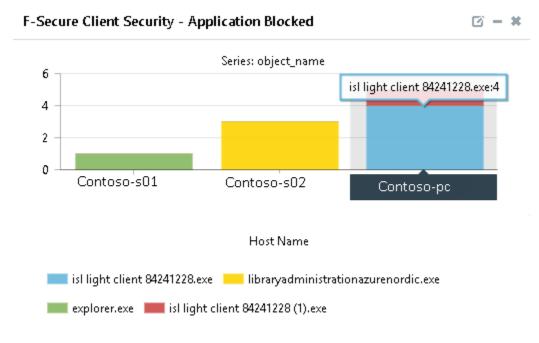


○ Scheduled ○ Queued Defined					Search	ର୍ ବ୍	I				
Report Groups		\oplus		Reports con	figuration: F-Secure Client Security						
Bitdefender GravityZ	Ü	0	^	🕂 🗓 é	2					Total	: 4
Bluecoat Content Ana	Ē	Ø			Title		Created on	Modified on			
Cisco AMP	Ē	1		- 🄅	F-Secure Client Security - Web Traffic Scanning		Jul 05 05:02:13 PM	Jul 05 05:02:13 PM	(j	5	F
Cisco ASA F-Secure Client Security		Ø			F-Secure Client Security - Virus detected		Jul 05 04:25:28 PM	Jul 06 12:34:47 PM	(i)	5	4
F-Secure Client Secu				D 🔅	F-Secure Client Security - Spyware detected		Jul 05 03:49:41 PM	Jul 06 12:35:50 PM	(i)	5	4
Linux OS	Ē	I Contraction of the second se			F-Secure Client Security - Application blocked		Jul 05 12:59:22 PM	Jul 06 12:43:54 PM	()	5	Ŧ
Alicrosoft Windows RR	Ē	1									
Gffice 365	Ē	0									



Dashlets

Title: F-Secure Client - Application Blocked







Title: F-Secure Client Security – Spyware Detected

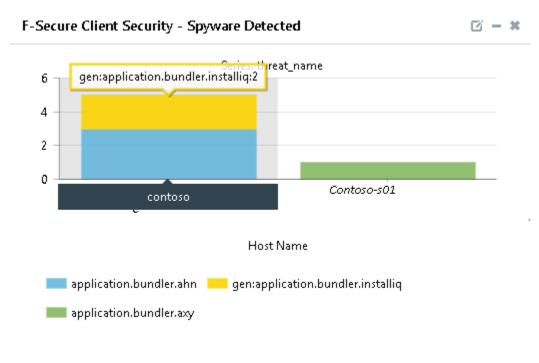
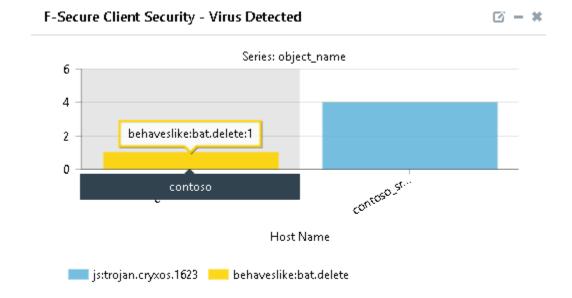


Figure 34

Title: F-Secure Client Security -Virus Detected





Title: F-Secure Client Security - Virus Detected Action

