

Integrate ForeScout CounterAct

EventTracker v9.0 and Above

Publication Date: July 4, 2019

Abstract

This guide provides instructions to configure ForeScout CounterAct to generate logs for critical events. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor the network access control.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x and later, and ForeScout CounterAct v8.0.

Audience

IT Admins, ForeScout CounterAct administrator, and EventTracker users who wish to forward logs to EventTracker and monitor events using EventTracker.

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
Configuring ForeScout CounterAct syslog Syslog plugin Configuration	3 3
Sending ForeScout event messages	3
Using actions to send endpoint messages	8
EventTracker Knowledge Pack (KP)	.0 .0
Reports1	0
Dashboards1	2
Importing Knowledge Pack into EventTracker	.5 16
Knowledge Objects1	17
Token Template1	.8
Flex Reports 2	20
Dashlets 2	22
Verifying Knowledge Pack in EventTracker 2 Alerts. 2	26 26
Knowledge Object	27
Token Template	27
Flex Reports	28
Dashlets	29



Overview

ForeScout CounterAct gives you network access control. It maintains the policies and network configuration and deploys them to the ForeScout CounterACT appliances.

ForeScout CounterAct can be integrated with EventTracker using syslog. With the help of ForeScout CounterAct KP items, we can monitor the network access control activities, malicious process and mail infection on applications and also trigger the alert whenever any malicious process is running, and mail infection is detected. EventTracker dashboard will help you to visualize the web activities on applications. It can even create a report that helps to collect user activities happening in the applications for a time interval. This will help you to review the different malicious and network activities. EventTracker CIM will help you to correlate from network access control activities, malicious process, and mail infection, etc.

Prerequisites

- EventTracker v9.x or above should be installed.
- ForeScout CounterAct v8.0 or latest version should be installed.
- ForeScout CounterAct core extension module Syslog plugin v3.5 should be installed.

Configuring ForeScout CounterAct syslog

Syslog plugin Configuration

This section describes how to configure the syslog plugin. There are two types of messages that you can send to syslog:

- Sending ForeScout event messages.
- Using actions to send endpoint messages.

Sending ForeScout event messages

Select an Appliance to Configure

This section describes how to configure the plugin to ensure that the CounterACT device can properly communicate with syslog servers.

Configuring the syslog plugin

1. In the Modules pane, select **Core Extensions >Syslog** and then select **Appliances**. The syslog - Appliances installed dialog box opens.



Syslog - Appliances Installed		—
V Devices	Show sub-folders	
C Enterprise Manager	Search Q	
Appliances	CounterACT Device 🔺 💁 Status Version	<u>R</u> ollback
	Enterprise Manager D Running 3.4.0	<u>S</u> tart
		St <u>o</u> p
		<u>C</u> onfigure
	1 items (1 selected)	Test
		Close



2. Select any appliance or the **Enterprise Manager** and select **Configure**. You cannot configure multiple CounterACT devices simultaneously. The Configuration dialog box opens. Need to configure send events to, syslog triggers, default action configuration for sending logs to the EventTracker.

Syslog@Enterprise Manager Plugin Configuration	×
Send Events To Syslog Triggers Default Action Configuration Receive From	
Send messages triggered by events to all of the following Syslog servers. Each message includes the Message Identity and the Priority (Facility and Severity) defined below.	
Server Ad Server Port Server Pr Use TLS Soft-fail OCSP Identity Facility Severity	Add
10.44.1.10 514 false false EM - 10.4 local4 info	<u>E</u> dit
	move
ОК	Cancel



3. When the configuration is complete, select ok.

Send Events To

The **Send Events To** tab lists the syslog servers to which the CounterACT device will send messages regarding the event types selected in the syslog triggers tab. For each syslog server, define:

- 1. In the Send Events Total, do one of the following:
 - To define a syslog server not in the table, select Add.

Syslog@Enterprise Ma	anager Plugin Configuration	8						
	Send Events To Syslog Triggers Default Action Configuration Receive From							
	Send messages triggered by events to all of the following Syslog servers. Each message includes the Message Identity and the Priority (Facility and Severity) defined below.							
	Server Ad Server Port Server Pr Use TLS Soft-fail O Identity Facility Severity	<u>A</u> dd						
S Add	1	Edit						
Server A	Address	<u>R</u> emove						
Server F	Port 0 0							
Server F	Protocol V							
Use T	TLS							
Soft-fa	all OCSP requests							
Identity								
Facility								
Severity	y							
	OK Cancel							
		OK Cancel						

Figure 3

• To modify the definition of an existing server, select it in the table and select Edit.

Syslog@Enterprise Ma	nager Plugin Co	onfiguration							
	Send Event	s To Sysi	og Triggers	Default A	ction Configuration	Receive	From		
	Send messages triggered by ever Each message includes the Mess			l of the follow intity and the	s. nd Severity) defined below.		w.	[
	Server Ad	Server Port	Server Pr	Use TLS	Soft-fail OCSP	Identity	Facility	Severity	Add
	10.44.1.10	514		false	talse	EM - 10.4	local4	info	<u>E</u> dit
									Remove
									OK Cancel





- 2. Specify the following information for the server:
 - Server Address: Provide EventTracker installed host IP address.
 - Server Port: Provide syslog (default 514) port.
 - Server Protocol: Syslog messaging can use TCP or UDP. Select the protocol to be used for communicating with this syslog server.
 - o **Identity**: Free-text field for identifying the syslog message.
 - **Facility**: (Optional) Syslog message facility that is transmitted as part of the message Priority field. If the facility value is not mentioned, it is set to **local5**.
 - Severity: Mention severity as Info.
- 3. Select OK. The updated server definition appears in the table.

Syslog Triggers

Configure the settings in the syslog triggers tab.

Syslog messages can be generated by Forescout platform policies when endpoints meet conditional criteria.

1. Select "Include timestamp and CounterACT device identifier in all messages".

Syslog@Enterprise Ma	anager Plugin Configura	ation				×
	Send Events To	Syslog Triggers	Default Action Cont	figuration	Receive From	
	General Settings Include only messages generated by the "Send Message to Syslog" action. Include timestamp and CounterACT device identifier in all messages					
	Select CounterACT	device identifier form	at.	Device Nan	ne 🗸	
	Select format type f	or system log events	and user operations:	Short ~		



2. Select options in the tab to define which event types trigger syslog messages. Follow below screenshot and click ok.



Syslog@Enterprise Ma	anager Plugin Configuration		— × —
	Send Events To Syslog Triggers Default Action Con	figuration Receive	e From
	General Settings		
	Include timestamp and CounterACT device identifier in all m	nessages	
	Select CounterACT device identifier format	Device Name \vee	
	Select format type for system log events and user operations:	Short ~	
	NAC Events		
	Include NAC policy logs		
	Include NAC policy match/unmatch events		
	Threat Protection		
	✓ Include bite events		
	✓ Include scan events		
	✓ Include lockdown events		
	✓ Include block events		
	✓ Include email worm events		
	System Logs and Events		
	Include system uptime events		
	✓ Include system log events		
	Include system status messages		
	✓ Include Packet Engine status messages		
	User Operations		
	Include user operations		
	Operating System Messages		
	Include operating system messages		
		ок	Cancel

Figure 6

Default Action Configuration

The Default Action Configuration tab allows you to define default values for the **Send Message** to syslog action parameters. These default values are applied to parameters that are not defined in policies. View Send Message to syslog action for details.



Syslog@Enterprise Mai	nager Plugin Configur	ation			x
	Send Events To	Syslog Triggers	Default Action Configuration	Receive From	
	Server Address				
	Server Port	614 Ç			
	Server Protocol	UDP 🗸			
	Message Identity	CounterACT			
	Facility	local4			
	Severity	info			



Specify the following values:

- 1. Server Address: Mention EventTracker installed host IP address.
- 2. Server Port: Mention syslog server(default 514) port.
- 3. **Server Protocol**: Syslog messaging can use TCP or UDP. Select the protocol to be used for communicating with this server.
- 4. Message Identity: Free-text field for identifying the syslog message.
- 5. **Facility**: (Optional) Syslog message facility that is transmitted as part of the message priority field. If the facility value is not mentioned, it is set to **local5**.
- 6. Severity: Mention severity as Info.

Using actions to send endpoint messages

Send Message to syslog

The Send Message to syslog action is used by the syslog plugin to send a message to the syslog server. This message overrides syslog plugin configuration options.

- 1. In the Policy Manager, select a policy and select Edit. The Policy Properties dialog box opens.
- 2. Next to the Main Rule section select Edit. The Policy Conditions dialog box opens.
- 3. Next to the Actions section select Add. The Action dialog box opens.
- 4. In the left pane expand the Audit folder.
- 5. Select Send Message to syslog.

Netsurion... EventTracker

Search Q	This action sends a mes	sage to a Syslog server. If you specify "Default",		
- 🗖 Actions	values will be taken from the Syslog plugin configuration.			
> 📥 AWS	Parameters Sched	fule		
✓ audit Audit	Message to Syslog			
Send Compliant CEF message				
Send Customized CEF message				
Send Message to Syslog	Message Identity	Click here to replace default value		
Send Not Compliant CEF message	Syslog Server Address	Click here to replace default value		
C ePO Add to Detected System	Carles Canad Dad	Oligie have to excluse default value		
> 🍰 Authenticate	Sysiog Server Port	Crick here to replace detault value		
> 🛃 Classify	Syslog Server Protocol	Click here to replace default value ~		
> 🛃 Manage	Syslog Facility	Click here to replace default value		
> 🐥 Notify	Syslog Severity	Click here to replace default value		
> 🕂 Remediate	Use TLS			
> 🖉 Restrict	Soft-fail OCSP reque	sts		
> 💿 VMware NSX	Tags :	Add Tags		
> 🛃 VMware vSphere				

Figure 8

- 6. Specify the following or use **Default** where applicable to apply the default configuration.
 - **Message to syslog**: Type a message to send to the syslog server when the policy is triggered.
 - **Message Identity**: Free-text field for identifying the syslog message.
 - Syslog Server Address: Provide EventTracker installed host IP address.
 - **Syslog Server Port**: Set syslog port number (default is 514).
 - **Syslog Server Protocol**: Syslog messaging can use TCP or UDP. Select the protocol to be used for communicating with this server.
 - **Syslog Facility:** (Optional) Syslog message facility that is transmitted as part of the message Priority field. If the facility value is not mentioned, it is set to **local**.
 - Syslog Priority: Mention severity as Info.
 - **Tags:** Mention tag as ForeScout CounterAct.

Netsurion... EventTracker

EventTracker Knowledge Pack (KP)

Once logs are received in EventTracker; alert, reports and dashboards can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker v9.x and later to support ForeScout CounterAct.

Alert

- ForeScout CounterAct: Blocked events This alert will trigger whenever the IP addresses and ports are blocked.
- ForeScout CounterAct: Mail infection detected This alert will trigger whenever an infection is found in the email attachments.

Reports

• ForeScout CounterAct – Blocked events – This report provides information related to the blocked events IP address, port details, firewall blocking status and reason.

LogTime	Log Type	Source IP Address	Port and Service	Destination IP Address	Firewall Blocking	Reason
06/06/2019 03:35:14 PM	Block Event	10.10.2.123	23/TCP	10.20.3.234	false	Port block
06/06/2019 03:35:14 PM	Block Event	10.10.2.123	23/TCP	10.20.3.234	false	Port block
06/06/2019 03:35:14 PM	Block Event	10.10.2.123	23/TCP	10.20.3.234	false	Port block
06/06/2019 03:35:14 PM	Block Event	10.10.2.123	23/TCP	10.20.3.234	false	Port block
06/06/2019 03:35:19 PM	Block Event	10.10.2.123	23/TCP	10.20.3.234	false	Port block
06/06/2019 03:35:19 PM	Block Event	10.10.2.123	23/TCP	10.20.3.234	false	Port block
06/06/2019 03:35:20 PM	Block Event	10.10.2.123	23/TCP	10.20.3.234	false	Port block
06/06/2019 03:35:20 PM	Block Event	10.10.2.123	23/TCP	10.20.3.234	false	Port block

Figure 9

• ForeScout CounterAct – Mail infection activities – This report provides information related to mail ids of sender and receiver, mail subject and IP address.

LogTime	Log Type	Source IP Address	Mail From	Mail To	Mail Subject
06/06/2019 03:35:14 PM	Mail Infection Attempt	10.10.1.123	sender@from.com	recipient@to.com	Check out this report
06/06/2019 03:35:14 PM	Mail Infection Attempt	10.10.1.123	sender@from.com	recipient@to.com	Check out this report
06/06/2019 03:35:14 PM	Mail Infection Attempt	10.10.1.123	sender@from.com	recipient@to.com	Check out this report
06/06/2019 03:35:14 PM	Mail Infection Attempt	10.10.1.123	sender@from.com	recipient@to.com	Check out this report
06/06/2019 03:35:19 PM	Mail Infection Attempt	10.10.1.123	sender@from.com	recipient@to.com	Check out this report
06/06/2019 03:35:19 PM	Mail Infection Attempt	10.10.1.123	sender@from.com	recipient@to.com	Check out this report
06/06/2019 03:35:20 PM	Mail Infection Attempt	10.10.1.123	sender@from.com	recipient@to.com	Check out this report

Figure 10



• ForeScout CounterAct – Network access control activities - This report provides information related to IP address, rule names, rule message, and reason.

LogTime	Log Type	Source IP Address	Rule Name	Category	Rule Match	Message	Reason
06/06/2019 07:25:56 PM	NAC Policy Log	192.0.2.1	Policy "AntiVirus Compliance" Not Compliant		AV Not Running:Mat ch	Host evaluation changed from "AV Not Installed:Match" to "AV Not Running:Match" due to condition	Property update: AntiVirus Installed: Added: AV Software.
06/06/2019 07:25:56 PM	NAC Policy Log	192.0.2.1	Policy "AntiVirus Compliance"	Not Compliant	AV Not Running:Mat ch	Host evaluation changed from "AV Not Installed:Match" to "AV Not Running:Match" due to condition	Property update: AntiVirus Installed: Added: AV Software.
06/06/2019 07:25:56 PM	NAC Policy Log	192.0.2.1	Policy "AntiVirus Compliance"	Not Compliant	AV Not Running:Mat ch	Host evaluation changed from "AV Not Installed:Match" to "AV Not Running:Match" due to condition	Property update: AntiVirus Installed: Added: AV Software.
06/06/2019 07:25:56 PM	NAC Policy Log	192.0.2.1	Policy "AntiVirus Compliance"	Not Compliant	AV Not Running:Mat ch	Host evaluation changed from "AV Not Installed:Match" to "AV Not Running:Match" due to condition	Property update: AntiVirus Installed: Added: AV Software.

Figure 11

• ForeScout CounterAct - Threat protection events- This report provides information related to IP addresses, port bite, scan event, and manual event.

LogTime	Log Type	Sorce IP Address	Destination IP Address	Client Port
06/18/2019 12:51:22 PM	Manual event	10.10.1.123		
06/18/2019 12:51:22 PM	Scan event	106.101.1.23		
06/18/2019 12:51:22 PM	Port bite	120.10.1.23	130.20.3.45	139
06/18/2019 12:51:25 PM	Manual event	10.10.1.123		
06/18/2019 12:51:25 PM	Scan event	106.101.1.23		
06/18/2019 12:51:25 PM	Port bite	120.10.1.23	130.20.3.45	139
06/18/2019 12:51:26 PM	Manual event	10.10.1.123		
06/18/2019 12:51:26 PM	Scan event	106.101.1.23		
06/18/2019 12:51:26 PM	Port bite	120.10.1.23	130.20.3.45	139
06/18/2019 12:51:28 PM	Port bite	120.10.1.23	130.20.3.45	139

Figure 12

• ForeScout CounterAct - User login and logout- This report provides information related to user login and logout.

LogTime	User Name	Source IP Address	Client IP Address	Reason	Log Status
06/18/2019 01:01:32 PM	admin	10.23.78.123	21.45.34.89	User admin changed Enterprise Manager Console	Logout succeeded
06/18/2019 01:01:34 PM	admin	10.23.78.123	21.45.34.89	User admin Enterprise Manager Console	Login succeeded
06/18/2019 01:01:36 PM	admin	10.23.78.123	21.45.34.89	User admin changed Enterprise Manager Console	Logout succeeded
06/18/2019 01:11:27 PM	admin	10.21.78.12	22.46.4.189	User admin changed Enterprise Manager Console	Logout succeeded
06/18/2019 01:11:29 PM	admin	10.23.78.123	21.45.34.89	User admin changed Enterprise Manager Console	Logout succeeded

Figure 13



• ForeScout CounterAct - User activities – This report provides information about admin changed network configuration, admin changed policy rules.

LogTime	Log Type	Message
06/18/2019 12:51:21 PM	User admin changed Configuration	Paused Network Integrity rules:1.1 Primary Classification
06/18/2019 12:51:21 PM	User admin changed Configuration	Change field lists definition toListsMaaS360 Software Installed -> Application Name: MaaS360 Unauthorized MobileApplicationsNetBIOS Domain: Corporate domain names, Corporate domain names_1VM ware Server Product ID: ESXi Server ListWindows Applications Installed -> Name: sqlserverWindows Services Running: Microsoft virtual services
06/18/2019 12:51:21 PM	User admin changed HPS Inspection Engine Configuration	Edited thefollowing Enterprise Manager: :Endpoint Remote Inspection method: Previous Value:wmi_only CurrentValue:wmi_with_fall_back
06/18/2019 12:51:21 PM	User admin changed Configuration	Policy: '1.1 PrimaryClassification'Sub-Rule changes:Sub-Rule Linux\UnixOld Condition:Network Function: Unix Server/Workstation, Linux Desktop/ServerNew Condition:Network Function: Unix Server/Workstation, Linux Desktop/Server OR OpenPorts: 22/TCP
06/18/2019 12:51:24 PM	User admin changed Configuration	Paused Network Integrity rules:1.1 Primary Classification

Figure 14

Dashboards

• ForeScout CounterAct NAC Activities – This dashboard shows information network access control activities like IP addresses, firewall action status, and reason.



Figure 15



• ForeScout CounterAct Blocked Events – This dashboard shows information about suspicious activities blocked by ForeScout CounterAct.



 ForeScout CounterAct Mail Infection Detected – This dashboard shows information about mail recipient addresses, IP addresses, and mail subject.



Figure 17



ForeScout CounterAct threat protection events – This dashboard shows information about the IP addresses, port bite, scan event, and manual event.





• ForeScout CouterAct user activities – This dashboard shows information about admin changes network configuration, admin modified policy rules.



Figure 19

Netsurion... EventTracker

 ForeScout CounterAct user login and logout – This dashboard shows information about user login and logout.



Figure 20

Importing Knowledge Pack into EventTracker

Find the specified knowledge pack in the following sequences-

- Alerts
- Knowledge Objects
- Token Template
- Flex Reports
- Dashlets
- 1. Launch the EventTracker Control Panel.
- 2. Double click **Export/Import Utility**, and then click the **Import** tab.

Netsurion... EventTracker



Figure 21

3. Import Tokens/Flex Reports as given below.

Alerts

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

1. Provide the path and file r 2. Click the Import button.	ame of the Alerts file. Use the '' button	to browse and locate the import file.
Uptions	Location	
Category		
Filters	Import E-mail settings	
Alerts	Set Active	
	Only if notifications set	This setting is applicable only for imports from Legacy (v6v) Alert files. For v7, the active status will be set
Systems and Groups	Du de Guilt	based on "Active" key available in the configuration
BSS Feeds	Sy derault	section.
0 1100 1 0003		
Reports	Source :	
	*.isalt	
Behavior Rules		
SCAP		
0.000		
🔘 Token Value		



- 2. Locate the Alerts_ForeScout CounterAct.isalt file, and then click the Open button.
- To import alerts, click the Import button.
 EventTracker displays a success message.





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

Knowledge Objects

- 1. Login into EventTracker and click **Knowledge objects** under the Admin option in the EventTracker page.
- 2. Locate the file named KO_ForeScout CounterAct.etko.

Import		×
KO_ForeScout CounterAct.etko 😂 Browse.	. Upload	
		Close



3. Now select all the checkbox and then click on \mathbb{T} the '**Import**' option.

Impo	rt			×
Se	lect file		🗁 Browse Upload	
\checkmark	Object name	Applies to	Group name	
\checkmark	ForeScout CounterAct blocked events	ForeScout CounterAct	ForeScout CounterAct	
\checkmark	ForeScout CounterAct mail infection detected	ForeScout CounterAct	ForeScout CounterAct	
\checkmark	ForeScout CounterAct NAC activities	ForeScout CounterAct	ForeScout CounterAct	
	ForeScout CounterAct threat protection events	ForeScout CounterAct	ForeScout CounterAct	
\checkmark	ForeScout CounterAct user activities	ForeScout CounterAct	ForeScout CounterAct	
\checkmark	ForeScout CounterAct user login and logout	ForeScout CounterAct	ForeScout CounterAct	

import close

Figure 25

4. Knowledge objects are now imported successfully. Please click **OK** and **Activate Now**.





Token Template

- 1. Login to the EventTracker.
- 2. Click on Admin >> Parsing Rules.

Netsurion... EventTracker

		🐥 Admin -	Tools 🗸
Active Watch Lists	Event Filters	💯 Parsing Rules	
Alerts	Eventvault	Report Settings	÷
m 🖲 Behavior Correlation Rules	FAQ Tile Configuration	Systems	
behavior Correlation Settings	Group Management	🗙 Users	
Casebook Configuration	Q IP Lookup Configuration	T Weights	
● Category	· C Knowledge Objects	Windows Agent Config	
Diagnostics	D Manager		

Figure 27

3. Click on **Template** and click **import configuration** Symbol.

Parsing Rules				Admin / Parsing Rules
Parsing Rule Template				
Groups 🕒 🎬	Group : All	Search	Q	C 1 T
Default				
Groups 🕀 🔡 Default	Group : All	Search	Q	C1

Figure 28

4. Locate the Template_ForeScout CounterAct.ettd file and click on import.

🧕 Token Template - Mozilla Firefox					- 🗆	×
(localhost:8080/EventTracker/Analysis/TokenTemplate	ImportExpor	t.aspx?Type=Import			⊠ ☆	≡
Import						
selected file is: Template_ForeScout CounterAct.ettd		🖀 Browse 😱				
☑ Template name	Separator	Template description	Added date	Added by	Group Name	
ForeScout CounterAct - Blocked events	\n	Block Event: Host: 10.10.2.123, Target: 10.20.3.234, Time 1469975529, Servic e: 23/TCP, Is Virtual Firewall blocking rule: false, Reason: Port block	Jan 01 12:00:00 PM	ETAdmin	ForeScout CounterA	Act
ForeScout CounterAct - Mail infection activities	\n	$\label{eq:mail_star} Mail Infection \ Attempt. \ Source: \ 10.10.1.123. \ Details: \ mail_from=sender@from.com, mail_to=recipient@to.com, mail_subject=Check \ out \ this \ report$	Jan 01 12:00:00 PM	ETAdmin	ForeScout CounterA	Act
ForeScout CounterAct - Network access control activities	\n	NAC Policy Log: Source: 192.0.2.1, Rule: Policy "AntiVirus Compliance", Match: "AV Not Running:Match", Category: Not Compliant, Details: Host evaluation changed from "AV Not Installed:Match" to "AV Not Running:M atch" due to condition. Reason: Property update: AntiVirus Installed: Add ed: AV Software.	Jan 01 12:00:00 PM	ETAdmin	ForeScout CounterA	Act
ForeScout CounterAct - Threat protection events	\n	Port bite. Source: 120.10.1.23. Destination: 130.20.3.45:139	Jan 01 12:00:00 PM	ETAdmin	ForeScout CounterA	Act
✓ ForeScout CounterAct - User activities	\n	User admin changed Configuration. Details: Policy: '1.1 PrimaryClassificati on'Sub-Rule changes:Sub-Rule Linux\UnixOld Condition:Network Functio n: Unix Server/Workstation, Linux Desktop/ServerNew Condition:Network Function: Unix Server/Workstation, Linux Desktop/Server OR OpenPorts: 2 2/TCP	Jan 01 12:00:00 PM	ETAdmin	ForeScout CounterA	Act
ForeScout CounterAct - User login and logout	\n	User admin changed Enterprise Manager Console. Details: Logout from 1 0.23.78.123 by host 21.45.34.89 : Logout succeeded	Jan 01 12:00:00 PM	ETAdmin	ForeScout CounterA	Act



5. Templates are imported now successfully.



Flex Reports

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



Detions	plate, first import template and procee Location	a with exportimport utility.	
) Filters			
) Alerts	O Legacy (*.issch)	New (*.etcrx)	
Systems and Groups	Source :		
RSS Feeds	IDect		
Reports			
Behavior Rules			
) SCAP			
) Token Value			



2. Locate the file named Flex_Reports_ForeScout CounterAct.etcrx and select all the checkbox.



🔁 Rep	orts Im	port					×
Nete :	f moot	*(a) appreciate template first impart template and ap	and with most impact process				
Note .	ii repor	tis contains template, inst import template and pro	ceed with report import process.				
Selec	t file	\\192.168.1./\Event Iracker KP\Security Intellig	ence Team\Pavan\ForeScout Cou	unterAct\Configuration\Hex_Reports	s_ForeScout CounterAct.etc Select file		
Availal	ble repo	rts	7		1		
Title			Frequency Show all	- Q Q			
		Title	Sites	Groups	Systems	Frequen	c y
	<u>EDIT</u>	ForeScout CounterAct - Blocked events		Default	Forescout Counteract	Undefined	
	<u>EDIT</u>	ForeScout CounterAct - Mail infection		Default	Forescout Counteract	Undefined	
	<u>EDIT</u>	ForeScout CounterAct - Network acce		Default	Forescout Counteract	Undefined	
	<u>EDIT</u>	ForeScout CounterAct - Threat protecti		Default	Forescout Counteract	Undefined	
	<u>EDIT</u>	ForeScout CounterAct - User activities		Default	Forescout Counteract	Undefined	
	<u>EDIT</u>	ForeScout CounterAct - User login and		Default	Forescout Counteract	Undefined	
<u>`</u>							_
Note Set	e: Set n run tii	un time option is not applicable for Defined Report me for report(s) from	s and Hourly Reports at interval of minu	tes Set			
nep	piace		Re	place Assign systems			0
				Note: Make sure tha	t Site(s), Group(s) and System(s) selections are	valid.	\otimes

Figure 32

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



Figure 33

Dashlets

In EventTracker 9.0, we have added a new feature that will help to import/export of dashlet. Following is the procedure to do that:

1. Login into EventTracker.

	Even	t Track	eræ				
1	Username						
	Password						
		Login					
log	8 s processed s	,333,946 ince install on	Dec 30, 2017				
	35,002 logs processed today						
Co	ntact Us	FAQ	Help				

Figure 34

2. Go to My Dashboard option.

Dashboard
Behavior Correlation
Compliance
My Dashboard
Home
Incidents
Threats
Q Search
Reports



3. Click on the **import** button and select **.etwd** File.

Figure 36



Figure 37

4. Click upload and select Dashboard which you want to import.

Netsurion EventTracker

🧕 Import dashlets - Mozilla Firefox	—		ב	\times
(localhost:8080/EventTracker/Flex/ImportWidget.aspx	•••	${igsidential}$	☆	≣
Import				^
Note: If dashlet configured using persisted report, first import the report and proceed w dashlet.	ith imp	portin	g	
Available widgets	wse	U	pload	
Select All				
🗹 ForeScout CounterAct NAC 🗹 ForeScout CounterAct bloc 🗹 ForeScout Co	unterA	lct ma	ail	
☑ ForeScout CounterAct thre ☑ ForeScout CounterAct user ☑ ForeScout Co	unterA	Act us	er	
	Impo	ort	Close	•

Figure 38

5. Click on the **Import** button. It will upload all selected dashboards.

Verifying Knowledge Pack in EventTracker

Alerts

- 1. Login to EventTracker.
- 2. Click the **Admin** menu, and then click **Alerts**.

≡	Event Tracker ⊕					🔎 🛛 Admin 🛨	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dasht
q		_	Alerts	Correlation	🔍 IP Lookup Configuration	🛱 Users	
	0	2	Behavior Correlation Rules	A Diagnostics	· Knowledge Objects	A Weights	
1			🗞 Behavior Correlation Settings	Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	P Eventvault	🧭 Parsing Rules		
			● Category	FAQ Configuration	Report Settings		
	Attacker			- News			



3. In the **Search** box, type **'ForeScout CounterAct'**, and then click the **Go** button. Alert Management page will display all the imported alerts.

Alerts								1 Admin / Alerts
Show All						Search by	Alert name 🗸	ForeScout Q Q
161 Available Alerts Total number of alerts available	60 Active Alerts Total number of active alerts			161 System/User Count for system	System User Defined Alert: m and user defin	53 5 s eed alerts	161 Alerts by Count of a	Critical Low Serios 10 12 22 Threat Level
Activate Now Click 'Activate N	ow' after making all changes							Total: 2 Page Size 25 V
Alert Name A	Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
다 않아 ForeScout CounterAct: Blocked events	•							ForeScout CounterAct v8.0
ForeScout CounterAct: Mail infection detected	ed 🔶							ForeScout CounterAct v8.0

Figure 40

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

EventTracker displays a message box.

Successfully saved configuration.
 ОК

Figure 41



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

NOTE: Specify appropriate systems in the alert configuration for better performance.

Knowledge Object

- 1. Login to EventTracker.
- 2. Click the Admin menu, and then click the Knowledge Object.
- In Knowledge Object Group Tree to view imported knowledge object, scroll down and click the ForeScout CounterAct group folder.
- 4. Knowledge Object is displayed in the pane.

Knowledge Objects	😭 / Admin / Knowledge Objects
ForeScout Q Q Activate Now	Objects 🕀 ፒ 🏦 🌣
Groups 🕀 🧭 🗓	±
E ForeScout CounterAct	
ForeScout CounterAct bl Ø II ForeScout CounterAct m Ø II	Select Object from the left panel.
	Figure 42

Token Template

- 1. Login to the EventTracker.
- 2. Click on Admin >> Parsing Rules.

			🐥 Admin -	Tools -
	Active Watch Lists	Event Filters	😥 Parsing Rules	
	Alerts	Sector Eventvault	Report Settings	÷
m	Behavior Correlation Rules	FAQ Tile Configuration	Systems	
	🗞 Behavior Correlation Settings	Group Management	QQ Users	
	Casebook Configuration	🔍 IP Lookup Configuration	🕀 Weights	
	● Category	· 🔆 Knowledge Objects	Windows Agent Config	
	Diagnostics	Manager		





3. Click on Template and search for ForeScout CounterAct.

					🛧 / Admin / Parsing Rules
Group : ForeScout CounterAct	ForeScout CounterAct	Q	Q		CİT
Template Name	Template Description	Added By	Added Date	Active	^
ForeScout CounterAct - Blocked events	ForeScout CounterAct - Blocked events	ETAdmin	6/12/2019 3:05:03 PM		0
ForeScout CounterAct - Mail infection activities	ForeScout CounterAct - Mail infection activities	ETAdmin	6/12/2019 3:05:03 PM		Ø
ForeScout CounterAct - Network access control activities	ForeScout CounterAct - Network access control activities	ETAdmin	6/12/2019 3:05:03 PM		Ø
ForeScout CounterAct - Threat protection events	ForeScout CounterAct - Threat protection events	ETAdmin	6/17/2019 7:21:34 PM		Ø
ForeScout CounterAct - User activities	ForeScout CounterAct - User activities	ETAdmin	6/18/2019 12:27:33 PM		0
ForeScout CounterAct - User login and logout	ForeScout CounterAct - User login and logout	ETAdmin	6/18/2019 11:56:17 AM		Ø

Figure 44

Flex Reports

- 1. Login to EventTracker.
- 2. Click the **Reports** menu, and then **Configuration**.
- 3. Select **Defined** in report type.
- In Report Groups Tree to view imported Scheduled Reports, scroll down and click the ForeScout CounterAct group folder.
- 5. Reports are displayed in the Reports configuration pane.

				† / F	Reports / Report Confi	guration /	Defined
			ForeScout		Q Q	Ē	1 🗹
Rep	orts con	figuration: ForeScout CounterAct					
÷	Û Ĝ	2				Total:	6
		Title	Created on	Modified on			
	€\$3	ForeScout CounterAct - User activities	Jun 18 12:31:34 PM	Jun 18 12:31:34 PM	()	8	+
	()	ForeScout CounterAct - User login and logout	Jun 18 12:09:28 PM	Jun 18 12:24:11 PM	()	5	+
	£3	ForeScout CounterAct - Threat protection events	Jun 17 08:06:42 PM	Jun 18 01:47:59 PM	()	5	+
		ForeScout CounterAct - Blocked events	Jun 12 03:06:00 PM	Jun 12 03:06:07 PM	(j)	5	+
	3	ForeScout CounterAct - Mail infection activities	Jun 12 03:06:00 PM	Jun 17 07:07:47 PM	<u>(</u>)	5	+
	1	ForeScout CounterAct - Network access control activities	Jun 06 07:20:41 PM	Jun 12 03:06:07 PM	(j)	5	+



Dashlets

- 1. Login to EventTracker.
- 2. Click the Dashboard menu, and then My Dashboard.
- 3. Then click on **Customize Dashlet** button (a) and search for **"ForeScout CounterAct"**

Available dashlets			×
ForeS			Q
ForeScout CounterAct Blocked	ForeScout CounterAct mail infe	ForeScout CounterAct NAC acti	ForeScout CounterAct threat pr
ForeScout CounterAct user acti	ForeScout CounterAct user logi		
			Export Close

Figure 46

