

Integrate Juniper JunOS

EventTracker V9.x or above

Publication Date: June 4, 2019

Abstract

This guide provides instructions to configure Juniper JunOS to send the syslog to EventTracker. Once syslog is being configured to send to EventTracker, alerts and reports can be configured into EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x and later, Juniper JunOS 11.4 and later.

Audience

Administrators who are responsible for monitoring Juniper JunOS which are running 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
Juniper JunOS	3
Prerequisites Verifying Software Version on Juniper device	3 3
Configuring Juniper JunOS to send syslog Messages from Juniper device Using J-Web to EventTracker	4
Juniper JunOS Knowledge Pack Alerts	5 5
Flex Reports	5
Dashboards	7
Importing Juniper JunOS knowledge pack into EventTracker Alerts	9 9
Template(s)1	.1
Flex Reports	.3
Knowledge Objects1	.5
Dashboards1	.6
Verifying Juniper JunOS knowledge pack in EventTracker	.9 .9
Template(s)1	.9
Flex Reports	0
Alerts	2 1



Juniper JunOS

Juniper JunOS is a free BSD-based operating system used in Juniper networks hardware routers. It is an operating system that is used in Juniper's routing, switching and security devices. EventTracker supports Juniper JunOS, it forwards the syslog messages to EventTracker. EventTracker generates the alert and report for critical events.

Prerequisites

- EventTracker v9.x should be installed.
- Juniper JunOS 11.4 and later should be installed.
- To enable logging in some features advanced licenses are required.

Verifying Software Version on Juniper device

- 1. Using CLI:
 - a. Login as root.
 - Enter the following command.
 root> show version
- 2. Using J-Web:
 - a. Login JunOS device using J-Web.
 - b. Enter valid username and password when prompted.
 - c. J-Web Dashboard appears, your Software Version is listed in the System Identification section below Hostname.



Figure 1



Configuring Juniper JunOS to send syslog Messages from Juniper device Using J-Web to EventTracker

Configuring Syslog logging:

Syslog is a standard for forwarding log messages in an IP network. Syslog captures the log information provided by the network devices.

- 1. Log in to the Juniper device.
- 2. Click **Configure > CLI Tools > Point** and click CLI in the Juniper device.
- 3. Expand System and click Syslog.
- 4. In the Syslog page, click Add New Entry placed next to 'Host'.
- 5. Enter the source IP address of the EventTracker.
- 6. Click **Apply** to save the configuration.

	Dashboard	Configure	Monitor		Maintain		Troub	leshoot	
D Interfaces	Configur	ation	System						
D Authentication	(Expand)	all (Hide all)	Syslog						
P NAT	E nan	t-authentication	OK Cancel	Re	fresh C	ommit	Disca	rd.	
Security	E logi	n vices	Author E						
D IPSec VPN	E lice	leg nse	Source address	es Edit	Delete	1			
Wireless LAN	E ntp	taces	Time format	les.					
Switching	E snmp	2			-				
P Routing	E secur	rity	Console (None c	onfigure	d) Add ney	w entry	8		
Class of Service	· acces	cations	File Add new ent	CX X					
System Properties	🗷 ylans	and the second se	File name		Match	Neste	ed Configura	ation Actions	
			messages					Edit Dei	ete
D Services			interactive-com	mands				Edit De	lete
CLI Tools									
CLI Viewer			Host Add new ent	TX					
OlEdar			Host name	Match	Facility ov	erride	Log prefix	Source address	Actions
CLI LUND	-		192.168.170.20						Edit Delete
Point and Olide CLI									

Figure 2

Netsurion... EventTracker

Juniper JunOS Knowledge Pack

Find the specified knowledge pack in the following sequences-

- Alerts
- Flex Reports
- Dashboard

Alerts

- 1. Juniper JunOS: Authentication failed This alert is generated when authentication fails in JunOS.
- 2. Juniper JunOS: Link flap This alert is generated when link flaps.
- 3. Juniper JunOS: Login failure This alert is generated when logon fails.

Flex Reports

• Juniper JunOS Login Activities by User - This report provides information related to login and logon activities by a user.

LogTime	Computer	User Name	Source	Logon type
05/28/2019 05:02:51 PM	JUN	test5	192.168.3.1	
05/28/2019 05:02:51 PM	JUN	root8	43.229.53.79	SSHD
05/28/2019 05:02:56 PM	JUN	root8	43.229.53.79	SSHD
05/28/2019 05:02:56 PM	JUN	test5	192.168.3.1	
05/28/2019 05:02:58 PM	JUN	test5	192.168.3.1	
05/28/2019 05:02:58 PM	JUN	root8	43.229.53.79	SSHD
05/28/2019 05:02:59 PM	JUN	root8	43.229.53.79	SSHD
05/28/2019 05:02:59 PM	JUN	test5	192.168.3.1	
05/28/2019 05:03:00 PM	JUN	root8	43.229.53.79	SSHD
05/28/2019 05:03:00 PM	JUN	test5	192.168.3.1	
05/28/2019 05:03:10 PM	JUN	test5	192.168.3.1	
05/28/2019 05:03:10 PM	JUN	root8	43.229.53.79	SSHD
05/28/2019 05:04:47 PM	JUN	root8	43.229.53.79	SSHD
05/28/2019 05:04:47 PM	JUN	test5	192.168.3.1	
05/28/2019 05:04:50 PM	JUN	test5	192.168.3.1	
05/28/2019 05:04:50 PM	JUN	root8	43.229.53.79	SSHD

Figure 3

Sample Log:

sshd[2952]: Accepted password for root from 192.168.1.2 port 1430 ssh2 <<< Successful login login: Login attempt for user abc from host 192.168.1.2



• Juniper JunOS Web Filter details- This report provides information related to web-filter activities (URL Filter status).

LogTime	Computer	Source Address	Source Port	Destination Address	Destination Port	Destination URL	URL Status
05/29/2019 02:50:13 PM	JUN	10.252.2.03	50227	74.125.239.155	80	ad.doubleclick.net	BLOCKED
05/29/2019 02:50:13 PM	JUN	10.252.2.02	50222	77.67.126.10	80	a2.espncdn.com	PERMITTED
05/29/2019 02:50:13 PM	JUN	10.252.2.04	50222	77.67.126.11	80	a2.espncdn.com	PERMITTED
05/29/2019 02:50:13 PM	JUN	10.252.2.05	50227	74.125.239.150	80	ad.doubleclick.net	BLOCKED
05/29/2019 02:50:13 PM	JUN	10.252.2.06	50222	77.67.126.12	80	a2.espncdn.com	PERMITTED
05/29/2019 02:50:13 PM	JUN	10.252.2.07	50227	74.125.239.145	80	ad.doubleclick.net	BLOCKED
05/29/2019 02:50:13 PM	JUN	10.252.2.09	50227	74.125.239.140	80	ad.doubleclick.net	BLOCKED
05/29/2019 02:50:13 PM	JUN	10.252.2.10	50222	77.67.126.15	80	a2.espncdn.com	PERMITTED
05/29/2019 02:50:13 PM	JUN	10.252.2.11	50227	74.125.239.166	80	ad.doubleclick.net	BLOCKED
05/29/2019 02:50:13 PM	JUN	10.252.2.12	50222	77.67.126.19	80	a2.espncdn.com	PERMITTED
05/29/2019 02:50:13 PM	JUN	10.252.2.08	50222	77.67.126.13	80	a2.espncdn.com	PERMITTED
05/29/2019 02:50:13 PM	JUN	10.252.2.01	50227	74.125.239.160	80	ad.doubleclick.net	BLOCKED
05/29/2019 02:50:24 PM	JUN	10.252.2.02	50222	77.67.126.10	80	a2.espncdn.com	PERMITTED
05/29/2019 02:50:24 PM	JUN	10.252.2.01	50227	74.125.239.160	80	ad.doubleclick.net	BLOCKED
05/29/2019 02:50:25 PM	JUN	10.252.2.12	50222	77.67.126.19	80	a2.espncdn.com	PERMITTED
05/29/2019 02:50:25 PM	JUN	10.252.2.03	50227	74.125.239.155	80	ad.doubleclick.net	BLOCKED

Figure 4

Sample Log:

Oct 25 16:08:54 rng-aa RT_UTM: WEBFILTER_URL_BLOCKED: WebFilter: ACTION="URL Blocked" 10.252.2.01(50227)->74.125.239.160(80) CATEGORY="Enhanced_Advertisements" REASON="BY_PRE_DEFINED" PROFILE="junos-wf-enhanced-default" URL=ad.doubleclick.net OBJ=/adj/espn.us.com.espn/espnfrontpage;pgtyp=espnfrontpage;sp=espn;ref=other;mnr=f;pos=incontent;swid=20 b69aac-7584-4e46-b1a6-880a71f319ab;dcopt=ist;sz=300x600,300x250,1x1;tile=3;ord=3800646760 USERNAME=Test1 ROLES=N/A)

• Juniper JunOS Attack Detection Details- This report provides information related to JunOS Screen attack details activities.

LogTime	Computer	Source Address	Source Port	Address	ion Port	Protocol Type	Attack Type
05/29/2019 02:50:13 PM	JUN	10.252.2.03	50227	74.125.239.155	80	SESSION_LIMIT	UDP flood
05/29/2019 02:50:13 PM	JUN	10.252.2.02	50222	77.67.126.11	80	SESSION_LIMIT	TCP syn Flood
05/29/2019 02:50:13 PM	JUN	10.252.2.04	50222	74.125.239.150	80	SESSION_LIMIT	UDP flood
05/29/2019 02:50:13 PM	JUN	10.252.2.05	50227	74.125.239.145	80	SESSION_LIMIT	TCP syn Flood
05/29/2019 02:50:13 PM	JUN	10.252.2.06	50222	74.125.239.140	80	SESSION_LIMIT	ICMP Flood
05/29/2019 02:50:13 PM	JUN	10.252.2.07	50227	74.125.239.166	80	SESSION_LIMIT	TCP syn Flood
05/29/2019 02:50:13 PM	JUN	10.252.2.09	50227	77.67.126.12	80	SESSION_LIMIT	ICMP Flood
05/29/2019 02:50:14 PM	JUN	10.252.2.10	50222	77.67.126.15	80	SESSION_LIMIT	Dst IP session limit
05/29/2019 02:50:14 PM	JUN	10.252.2.11	50227	77.67.126.13	80	SESSION_LIMIT	ICMP Flood
05/29/2019 02:50:14 PM	JUN	10.252.2.12	50222	74.125.239.150	80	SESSION_LIMIT	UDP flood
05/29/2019 02:50:14 PM	JUN	10.252.2.08	50222	77.67.126.19	80	SESSION_LIMIT	ICMP Flood
05/29/2019 02:50:14 PM	JUN	10.252.2.01	50227	74.125.239.160	80	SESSION_LIMIT	TCP syn Flood
05/29/2019 02:50:25 PM	JUN	10.252.2.02	50222	77.67.126.10	80	SESSION_LIMIT	ICMP Flood
05/29/2019 02:50:25 PM	JUN	10.252.2.01	50227	74.125.239.155	80	SESSION_LIMIT	TCP syn Flood
05/29/2019 02:50:25 PM	JUN	10.252.2.12	50222	77.67.126.11	80	SESSION_LIMIT	UDP flood
05/29/2019 02:50:25 PM	JUN	10.252.2.03	50227	77.67.126.12	80	SESSION_LIMIT	Dst IP session limit
05/29/2019 02:50:25 PM	JUN	10.252.2.04	50222	74.125.239.145	80	SESSION_LIMIT	UDP flood
05/29/2019 02:50:25 PM	JUN	10.252.2.05	50227	77.67.126.13	80	SESSION_LIMIT	Dst IP session limit
05/29/2019 02:50:25 PM	JUN	10.252.2.07	50227	74.125.239.140	80	SESSION_LIMIT	Dst IP session limit

Figure 5

Sample Log:

Apr 20 16:21:03 SRX-2 RT_IDS: RT_SCREEN_SESSION_LIMIT: Dst IP session limit! destination: 206.25.34.12, action: drop

Dashboards

• Juniper JunOS Login Activities by User:

Juniper JunOS Login Activities by User	C - ×
log_info: login	
svc_junos-space abc	



- Juniper JunOS Events Commands:



• Juniper JunOS Login Failure by Users:



Figure 8



• Juniper JunOS Web-filter Status:



Figure 9

Importing Juniper JunOS knowledge pack into EventTracker

Find the specified knowledge pack in the following sequences-

- Alerts
- Template(s)
- Flex Reports
- Knowledge Objects
- Dashlets

Alerts

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





- 3. Click the Import tab.
- 4. Select the Alert option.
- 5. Click on **Browse** button and select the **file path**.
- 6. Click on Import.



Lange Strate Strategy Export Import Utility		_	×
Export Import			
 Provide the path and file nar Click the Import button. 	ne of the Alerts file. Use the '' butt	on to browse and locate the import file.	
Options	Location		
Category	Import E-mail settings		
⊖ Filters	Set Active Only if notifications set By default	This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.	
Alerts			
O Systems and Groups	Watchlist Configuration		
O Takan Valua	Import Watchlist configurati	on	
	This setting is applicable only f	or alerts which have Advanced watchlist configured.	
◯ Reports	on the console where the alert	s are imported.	
O Machine learning			
	Source :		
	D:\KP_ITEMS\Junos OS\C	onfiguration \Alert_Junos OS.isalt	
		Import	Close

Figure 11

7. Alerts are now imported successfully.



Figure 12

Template(s)

- 1. Login to EventTracker console.
- 2. Click on the Admin option in the EventTracker page and select Parsing Rules.



≡	Event Tracker 🕀						🐥 🛛 Admin 🗸	Tools 🗕 (
	Parsing Rules				Active Watch Lists	Event Filters	😥 Parsing Rules	📌 / Ad
Q	D. J. D. L. Trunchete				Alerts	Eventvault	Report Settings	
	Parsing Rule Template				Behavior Correlation Rules	FAQ Tile Configuration	Systems	
2	Groups		⊕ Ⅲ	Group : All	🗞 Behavior Correlation Settings	Group Management	QQ Users	
	Default		-		Casebook Configuration	Q IP Lookup Configuration	D Weights	
	ABC	Ē	1	Template Name	ele Category	· 🔆 Knowledge Objects	Windows Agent Config	Active
	Brocade Switch		1	ES Big ID ITM SSL Error	Diagnostics	Manager		
	Cerberus SFTP Server	Ē	0	is orgin envisorenti	failure			2



3. Select **Templet** and click on the **import \$** icon.

	Parsing Rules							† / A	dmin /	Parsing Rules
۹	Parsing Rule Template									
	Groups	+	Group : All	Search	Q					
	Kaspersky Security C] 🧭 📩							С	主王
	Kaspersky Security C	j 🏈	Template Name	Template Description	Group Name	Added By	Added Date	Active		<u>^</u>
	Microsoft cloud app	j 🧭	F5 Big IP LTM SSL Error	F5 Big IP LTM SSL TLS Handshake	F5 BIG IP LTM	adarsh.p	Apr 08 01:31:10 PM	v		1
	OKTA SSO	j 🎯		failure				_	_	
	OpenDNS	ī 🧭	Brocade ICX Switch: SNMP	Brocade ICX Switch: SNMP Status	Brocade Switch	adarsh.p	Mar 12 12:15:35 PM			Ø

Figure 14

4. Browse Juniper JunOS templet files.



Figure 15

- 5. Select all Juniper JunOS template names.
- 6. Click on the **Import** button.

Import

	Template name	Separator	Template description
8	Juniper JUNOS VPN Session Details	\n	Sep 9 06:57:34 kmd[1393]: KMD_VPN_UP_ALARM_USER: VPN test_vpn fro m 10.10.10.3 is up. Local-ip: 10.10.10.8, gateway name: ike-gw, vpn name: vpn1, tunnel-id: 131073, local tunnel-if: st0.0, remote tunnel-ip: Not-Avail able, Local IKE-ID: 10.10.10, Remote IKE-ID: 10.10.10.2, XAUTH usernam e: Robert, VR id: 0, Traffic-selector: , Traffic-selector local ID: ipv4_subnet(a ny:0,[0.7]=192.168.10/24), Traffic-selector remote ID: ipv4_subnet(any:0, [0.7]=192.168.3.0/24) Sep 7 09:08:44 kmd[1334]: KMD_VPN_PV_PHASE1:1 KE Phase-1 Failure: No proposal chosen [spi=(null), src_ip=10.10.10.2, dst_ ip=10.10.10.1]
8	Juniper JUNOS Webfilter Details	\n	Oct 25 16:08:54 rng-aa RT_UTM: WEBFILTER_URL_BLOCKED: WebFilter: AC TION="URL Blocked" 10.252.2.11(50227)->74.125.239.155(80) CATEGORY ="Enhanced_Advertisements" REASON="BY_PRE_DEFINED" PROFILE="jun os-wf-enhanced-default" URL=ad.doubleclick.net OBJ=/adj/espn.us.com. espn/espnfrontpage.pgtyp=espnfrontpage.sp=espn:ref=other:mnr=f;pos =incontent;swid=20b69aac-7584-4e46-b1a6-880a71f319ab;dcopt=ist;sz =300x600,300x250,1x1;tile=3;ord=3800646760 USERNAME=William ROL ES=N/A Oct 25 16:08:54 rng-aa RT_UTM: WEBFILTER_URL_PERMITTED: W ebFilter: ACTION="URL Permitted" 10.252.2.111(50222)->77.67.126.10(80) CATEGORY="N/A" REASON="BY_OTHER" PROFILE="junos-wf-enhanced- default" URL=a2.espncdn.com OBJ=/prod/assets/header_sprite_fp:v4.png USERNAME=Joe ROLES=N/A
•	Juniper JUNOS SSH logon success	\t	Sep 23 20:17:01 EX3300-node0 sshd[10797]: Accepted password for Mack from 172.31.4.3 port 1284 ssh2

Figure 16

7. Template(s) imported successfully.



Figure 17

Flex Reports

On EventTracker Control Panel,

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

ort Utility			_	
t				
ne path and file nan Import button port(s) contains temp	ne of Schedule Report file. Use the '.	' button to browse and locate d with exportimport utility.	the import file.	
	Location			
у				
	 Legacy (*.issch) 	New (*.etcrx)		
s and Groups	Source : *.issch			
Value				
or Correlation				
			Import	Close
	ort Utility	s and Groups Value Torrelation Value	er path and file name of Schedule Report file. Use the '' button to browse and locate moot button of the sport import utility. Location y s and Groups value a or Correlation	er Utility —



2. Locate the file named **Reports_Juniper JunOS.etcrx** and select all the checkbox.

Frequency Show all Q Q Image: State Gravins Swidens Frequency Image: State Ortosojunosex/200 contosojunosex Undefined Image: State Default contosojunosex/200 contosojunosex Undefined Image: State NTPLDTBLR40 Default contosojunosex/200 contosojunosex/2	vailable	eports			00001110	
Thie Sites Grouns Systems Frequency EDIT JUNOS-Console logon success NTPLDTBLR40 Default contoso_junos ex 2200, contoso_junos Undefined EDIT JUNOS-Dynamic ARP inspection failure NTPLDTBLR40 Default contoso_junos ex 2200, contoso_junos Undefined EDIT JUNOS-Row session details NTPLDTBLR40 Default contoso_junos ex 2200, contoso_junos Undefined EDIT JUNOS-Row session details NTPLDTBLR40 Default contoso_junos ex 2200, contoso_junos Undefined EDIT JUNOS-Untrusted DHCP server detect NTPLDTBLR40 Default contoso_junos ex 2200, contoso_junos Undefined EDIT JUNOS-User authentication failure NTPLDTBLR40 Default contoso_junos ex 2200, contoso_junos Undefined EDIT JUNOS-User authentication success NTPLDTBLR40 Default contoso_junos ex 2200, contoso_junos Undefined EDIT JUNOS-User authentication success NTPLDTBLR40 Default contoso_junos ex 2200, contoso_junos Undefined EDIT JUNOS-VPN session detals	itle		Frequency Show all	- ପ୍ ଷ୍		
✓ EDIT JUNOS-Console logon success NTPLDTBLR40 Default contosojunos ex 2200, contosojunos Undefined ✓ EDIT JUNOS-Dynamic ARP inspection failure NTPLDTBLR40 Default contosojunos ex 2200, contosojunos Undefined ✓ EDIT JUNOS-Row session detais NTPLDTBLR40 Default.TOONS Baracuda-VPN-1, Baracuda-VPN-2, D Undefined ✓ EDIT JUNOS-Screen attack detais NTPLDTBLR40 Default.TOONS Baracuda-VPN-1, Baracuda-VPN-2, D Undefined ✓ EDIT JUNOS-Untrusted DHCP server detect NTPLDTBLR40 Default contosojunos ex 2200, contosojunos Undefined ✓ EDIT JUNOS-Untrusted DHCP server detect NTPLDTBLR40 Default contosojunos ex 2200, contosojunos Undefined ✓ EDIT JUNOS-User authentication success NTPLDTBLR40 Default contosojunos ex 2200, contosojunos Undefined ✓ EDIT JUNOS-User authentication success NTPLDTBLR40 Default contosojunos ex 2200, contosojunos Undefined ✓ EDIT JUNOS-VPN session detais NTPLDTBLR40 Default.TOONS Baracuda-VPN-1, B		Title	Sites	Gmuns	Systems	Frequenc
Image: Septimer of the server of the serv		I JUNOS-Console logon success	NTPLDTBLR40	Default	contoso-junos-ex-2200,contoso-junos	Undefined
Image: September 1 JUNOS-Row session details NTPLDTBLR40 Default:TOONS Baracuda-VPN-1,Baracuda-VPN-2,D Uhdefined Image: September 2 JUNOS-Screen attack details NTPLDTBLR40 Default:TOONS Baracuda-VPN-1,Baracuda-VPN-2,D Uhdefined Image: September 2 JUNOS-Untrusted DHCP server detect NTPLDTBLR40 Default cortosoj.unos ex: 2200, cortosoj.unos Uhdefined Image: September 2 JUNOS-User authentication failure NTPLDTBLR40 Default cortosoj.unos ex: 2200, cortosoj.unos Uhdefined Image: September 2 JUNOS-User authentication failure NTPLDTBLR40 Default cortosoj.unos ex: 2200, cortosoj.unos Uhdefined Image: September 2 JUNOS-User authentication success NTPLDTBLR40 Default cortosoj.unos ex: 2200, cortosoj.unos Uhdefined Image: September 2 JUNOS-VPN session details NTPLDTBLR40 Default:TOONS Baracuda-VPN-1,Baracuda-VPN-2,D Uhdefined Image: September 2 JUNOS-Webfilter details NTPLDTBLR40 Default:TOONS Baracuda-VPN-1,Baracuda-VPN-2,D Uhdefined Image: September 2 JUNOS-Webfilter details NTPLDTBLR40 Default:TOONS Baracuda-VPN-1,Baracuda-VPN-2,D <td< td=""><td></td><td>IT JUNOS-Dynamic ARP inspection failure</td><td>NTPLDTBLR40</td><td>Default</td><td>contoso-junos-ex-2200,contoso-junos</td><td>Undefined</td></td<>		IT JUNOS-Dynamic ARP inspection failure	NTPLDTBLR40	Default	contoso-junos-ex-2200,contoso-junos	Undefined
Image: Septement at a contrast details NTPLDTBLR40 Default:TOONS Baracuda-VPN-1,Baracuda-VPN-2,D Undefined Image: Septement at a contrast details NTPLDTBLR40 Default contrast details Undefined Image: Septement at a contrast details NTPLDTBLR40 Default contrast details Undefined Image: Septement at a contrast details NTPLDTBLR40 Default contrast details Undefined Image: Septement at a contrast details NTPLDTBLR40 Default contrast details Undefined Image: Septement at a contrast details NTPLDTBLR40 Default contrast details Undefined Image: Septement at a contrast details NTPLDTBLR40 Default contrast details Undefined Image: Septement at a contrast details NTPLDTBLR40 Default contrast details Undefined Image: Septement at a contrast details NTPLDTBLR40 Default:TOONS Baracuda-VPN-1,Baracuda-VPN-2,D Undefined Image: Septement at a contrast details NTPLDTBLR40 Default:TOONS Baracuda-VPN-1,Baracuda-VPN-2,D Undefined Image: Septement at a contrast details NTPLDTBLR40 Default:TOONS Baracuda-VPN-1,Baracuda-VPN-2,		IT JUNOS-Flow session details	NTPLDTBLR40	Default:TOONS	Barracuda-VPN-1,Barracuda-VPN-2,D	Undefined
Image: September 2 EDIT JUNOS-Untrusted DHCP server detect NTPLDTBLR40 Default cortosojunos ex: 2200, cortosojunos Undefined Image: September 2 JUNOS-User authentication failure NTPLDTBLR40 Default cortosojunos ex: 2200, cortosojunos Undefined Image: September 2 JUNOS-User authentication success NTPLDTBLR40 Default cortosojunos ex: 2200, cortosojunos Undefined Image: September 2 JUNOS-User authentication success NTPLDTBLR40 Default cortosojunos ex: 2200, cortosojunos Undefined Image: September 2 JUNOS-User authentication success NTPLDTBLR40 Default cortosojunos ex: 2200, cortosojunos Undefined Image: September 2 JUNOS-Verviser 8 NTPLDTBLR40 Default: TOONS Baracuda-VPN-1, Baracuda-VPN-2, D Undefined Image: September 2 JUNOS-Webfilter details NTPLDTBLR40 Default: TOONS Baracuda-VPN-1, Baracuda-VPN-2, D Undefined		IT JUNOS-Screen attack details	NTPLDTBLR40	Default:TOONS	Barracuda-VPN-1,Barracuda-VPN-2,D	Undefined
Image: September 2000 S-User authentication failure NTPLDTBLR40 Default contosojunos ex: 2200, contosojunos Uhdefined Image: September 2000 S-User authentication success NTPLDTBLR40 Default contosojunos ex: 2200, contosojunos Uhdefined Image: September 2000 S-User authentication success NTPLDTBLR40 Default contosojunos ex: 2200, contosojunos Uhdefined Image: September 2000 S-User authentication success NTPLDTBLR40 Default contosojunos ex: 2200, contosojunos Uhdefined Image: September 2000 S-User authentication success NTPLDTBLR40 Default contosojunos ex: 2200, contosojunos Uhdefined Image: September 2000 S-User authentication success NTPLDTBLR40 Default:TOONS Baracuda-VPN-1, Baracuda-VPN-2, D Uhdefined Image: September 2000 S-User authentication success NTPLDTBLR40 Default:TOONS Baracuda-VPN-1, Baracuda-VPN-2, D Uhdefined Image: September 2000 S-User 2000		IT JUNOS-Untrusted DHCP server detect	NTPLDTBLR40	Default	contoso-junos-ex-2200,contoso-junos	Undefined
Image: September 2000 S-User authentication success NTPLDTBLR40 Default contosojunos-ex-2200,contosojunos Uhdefined Image: September 2000 S-User logon failure NTPLDTBLR40 Default contosojunos-ex-2200,contosojunos Uhdefined Image: September 2000 S-User logon failure NTPLDTBLR40 Default contosojunos-ex-2200,contosojunos Uhdefined Image: September 2000 S-User logon failure NTPLDTBLR40 Default:TOONS Baracuda-VPN-1,Baracuda-VPN-2,D Uhdefined Image: September 2000 S-Webfilter details NTPLDTBLR40 Default:TOONS Baracuda-VPN-1,Baracuda-VPN-2,D Uhdefined		JUNOS-User authentication failure	NTPLDTBLR40	Default	contoso-junos-ex-2200,contoso-junos	Undefined
EDIT JUNOS-User logon failure NTPLDTBLR40 Default contoso-junos-ex-2200, contoso-junos Undefined EDIT JUNOS-VPN session details NTPLDTBLR40 Default:TOONS Barracuda-VPN-1, Barracuda-VPN-2, D Undefined EDIT JUNOS-Webfilter details NTPLDTBLR40 Default:TOONS Barracuda-VPN-1, Barracuda-VPN-2, D Undefined		IT JUNOS-User authentication success	NTPLDTBLR40	Default	contoso-junos-ex-2200,contoso-junos	Undefined
EDIT JUNOS-VPN session details NTPLDTBLR40 Default:TOONS Barracuda-VPN-1,Barracuda-VPN-2,D Undefined EDIT JUNOS-Webfilter details NTPLDTBLR40 Default:TOONS Barracuda-VPN-1,Barracuda-VPN-2,D Undefined		IT JUNOS-User logon failure	NTPLDTBLR40	Default	contoso-junos-ex-2200,contoso-junos	Undefined
EDIT JUNOS-Webfilter details NTPLDTBLR40 Default:TOONS Barracuda-VPN-1,Barracuda-VPN-2,D Undefined		JUNOS-VPN session details	NTPLDTBLR40	Default:TOONS	Barracuda-VPN-1,Barracuda-VPN-2,D	Undefined
		T UNIVE Weldling details	NTPLDTBLR40	Default:TOONS	Barracuda-VPN-1,Barracuda-VPN-2,D	Undefined
		11 JONOS-Webliker decails				

Figure 19



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





Knowledge Objects

- 1. Login to EventTracker console
- 2. Click on Knowledge objects under the Admin option in the EventTracker page.

Knowledge Objects		🕈 / Admin / Knowledge Objects
Search objects Q Q	Activate Now	Objects 🕀 Ţ 🏦 🌣



3. Locate the file named KO_ Juniper JunOS.etko

Import	
KO_Juniper JunOS.etko	🗁 Browse



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



Import			×	
Select file	11		🗁 Browse Upload	
	Object name	Applies to	Group name	
	Juniper JunOS	Juniper JunOS	Juniper JunOS	
			Import Close	

Figure 23

5. Knowledge objects are now imported successfully.





Dashboards

1. Open EventTracker in the browser and log in.



-	Home		
۹	My Dashboard		
R	Threats		1
	Incidents	ntry point	Indicators of Compromise US8 activities, New services or software install
	Behavior Correlation		
	Change Audit		-
	Compliance		Contraction

Figure 25

- 2. Navigate to **My Dashboard**.
- 3. Click on the **Import configuration** \mathbb{T} icon on the top right corner.
- 4. In the popup window browse the file named **Dashboard_Juniper JunOS.etwd.**

Import		
Note: If dashlet configured using persisted report, first import the report and proceed with import	ing dashlet.	
Dashboards_Juniper JunOS.etwd	🗁 Browse	Upload

Figure 26

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



Import		
Note: If dashlet configured using persisted report, first import the report and proceed with importing da	ishlet.	
	🗁 Browse	Upload
Available widgets		
Select All		
🖉 Juniper JunOS Event Comma 🗹 Juniper JunOS Login Activ 🗹 Juniper JunOS Login Faile		
	Import	Close

Figure 27

- 6. Click 'customize' <a>[6] locate and choose created Dashlets.
- 7. Click **Add** to add Dashlets to the dashboard.

Customize dashlets				×
juniper				Q
 Juniper JunOS Event Commands 	✓ Juniper JunOS Login Activities b	✓ Juniper JunOS Login Failed by U		
			Add Delete	Close

Figure 28

Netsurion... EventTracker

Verifying Juniper JunOS knowledge pack in EventTracker

Knowledge Object

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

≡	Event Tracker #								
	Knowledge Objects								
Q 	Search objects Q Q Activate Now								
	Groups 💮 🖄	Object name Juniper JunOS							
	Extremesummitx440	Applies to Juniper JunOS							
	F5 BIG IP LTM	Rules							
	Juniper JunOS	Title							
	Juniper JunOS	🗄 Juniper JunOS							
		Message Signature:							
	Kaspersky Security Center	Kaspersky Security Center \b(AAA AAMW ACCT ACTIONS ACX FAILED AGENTD AGNETD ALARMD AMD ANALYTICS ANALYZER							
	Microsoft IIS Web Server	Message Exception:							
		Figure 29							

Template(s)

1. In the EventTracker web interface, click the Admin drop-down, and then click Parsing Rules.

≡	Event Tracker ⊕							🐥 🛛 Admin 🗸	Tools 👻 🦸
	Parsing Rules					Active Watch Lists	Event Filters	🧭 Parsing Rules	† / Ac
Q	Denvice Dula Tamalata					Alerts	Ventvault	Report Settings	
	Parsing Rule Template			B Behavior Correlation Rules FAQ Tile Con		Systems			
<u>~</u>	Groups		+		Group : All	🗞 Behavior Correlation Settings	Group Management	Q Users	
	Default					Casebook Configuration	Q IP Lookup Configuration	T Weights	
	ABC		1	L	Template Name	📲 Category	· Knowledge Objects	Windows Agent Config	Active
	Brocade Switch		Ø	L	E5 Big IP ITM SSL Error	Diagnostics	Manager		
	Cerberus SFTP Server	Ē	Ø		To big in child obe circle	failure			



Netsurion... EventTracker

- 2. Select Templet and find the Juniper JunOS Group.
- 3. Click on Juniper JunOS Group to see the All Template(s).

	Parsing Rules					
۹	Parsing Rule Template					
	Groups		(+)	Group : Juniper JunOS	Search	Q
	Juniper JunOS	Ē	0			
	Juniper JUNOS	Ī	1	Template Name	Template Description	Added By
	Kaspersky Endpoint S		1	SSH logon success	SSH logon success	ETAdmin
	Kaspersky Security C		1			
	Kaspersky Security C		0			
	Microsoft cloud app		0			
				Figure 31		

Flex Reports

In the EventTracker web interface,

1. Click the **Reports** icon, and then select the **Report Configuration**.

≡	Event Tracker #
	Home
٩	
R	Report Configuration
	Report Dashboard
	Explorer
	Апаскег



- 2. In Reports Configuration pane, select a Defined option.
- 3. Click on the Juniper JunOS group folder to view the imported Juniper JunOS.



Report Configuration										
Scheduled OQueued	Defined					(Search			
Report Groups Reports configuration: Juniper JUNOS										
All Inreat Report		۷	<u></u>) 🗓 🙆	2					
Brocade Switch		Ø			Title		Created on			
Cerberus SFTP Server		1		~~	IIINOS User authentication success		May 23 07:01:14 PM			
Dell FORCE 10 Switch	Ē	1		472 M	Jonos-oser admentication success		May 25 07.01.14 PM			
EventTracker	Ī	Ø		£\$3	JUNOS-User authentication failure		May 23 07:01:14 PM			
Extremesummitx440	<u></u>			€3	JUNOS-User logon failure		May 23 07:01:14 PM			
F5 Big IP LTM	Ē	0		₹ € 3	JUNOS-Dynamic ARP inspection failure		May 23 07:01:14 PM			
🔁 Juniper JUNOS	Ī	1		£\$5	JUNOS-Untrusted DHCP server detection		May 23 07:01:14 PM			
kespersky	Ē	1		£\$5	JUNOS-Webfilter details		May 23 07:01:14 PM			
Microsoft IIS	Ī	Ø		2	JUNOS-Flow session details		May 23 07:01:14 PM			
Nuskin Cloud App Sec		Ø		2.5	JUNOS-Screen attack details		May 23 07:01:14 PM			
OKTA SSO		Ø		£3	JUNOS-VPN session details		May 23 07:01:14 PM			
OpenDNS	Ē	Ø		233	JUNOS-Console logon success		May 23 07:01:13 PM			
Pa Decewordstate	THE A	CAR				-				

Figure 33

Alerts

1. In the EventTracker web interface, click the Admin icon, and then select Alerts.

≡	Event Tracker #				🔎 Admin 🗸	Tools +	
-	Home		Active Watch Lists	Event Filters	🧭 Parsing Rules		
Q			Alerts	Sector Eventvault	Report Settings		
	0	2	Behavior Correlation Rules	FAQ Tile Configuration	Systems		
Å			🗞 Behavior Correlation Settings	Group Management	Q Users		
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry	USB activities, Ne	Casebook Configuration	🔍 IP Lookup Configuration	🕀 Weights	ing Systen orting since th	
		_	● Category	·☆ Knowledge Objects	Windows Agent Config		
	A		-				
			Figure 34				

2. In the Alert search bar, we can search the alert name and view the imported Juniper JunOS.



≡	Event Tracker #						
==	Alerts						
۹	Show All						
	190 26						
	Available Alerts Total number of alerts available Total number of active Alerts	Active Alerts Total number of active alerts					
	Activate Now Click 'Activate Now' after making all	changes					
	Alert Name A		Threat	Active	E-mai		
	🗹 🛱 JUNOS: Authentication failed		•				
	🗹 🚱 JUNOS: Link flap		•				
	🗹 ြိုးပို JUNOS: Login failure		•				

Figure 35

