# EventTracker

Actionable Security Intelligence

# Virtual Collection Point Configuration Guide

Publication Date: May 10, 2017

#### Abstract

The purpose of this document is to help users understand Virtual Collection Points (VCP) architecture and its benefits.

It also provides detailed descriptions to

- Configure Virtual Collection Points for Windows.
- Configure Windows systems to forward events through different ports.
- Configure Virtual Collection Points for SYSLOGS.
- Configure NIX systems to forward SYSLOG messages to the EventTracker Manager through different ports (default port: 514 (UDP/TCP).
- Forward incoming events as raw SYSLOG messages

#### Audience

Users of EventTracker monitoring large numbers of Windows and NIX systems/devices are requested to go through this document. This document will help

- Users analyze their EventTracker deployment plan and recommend the best deployment solution suitable to individual company requirements.
- Configuring your EventTracker deployment to perform at an optimal level, besides giving you deployment ideas based on the EventTracker VCP architecture.
- Garner best usage of hardware resources and bandwidth.
- Provide best performance outputs from key EventTracker Manager modules, namely, data collection, analysis and reporting.



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.

© 2017 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	
Virtual Collection Point Why go for VCP?	
Implement VCP	
Virtual Collection Points Architecture	5
Virtual Collection Points for SYSLOGS Configure VCP for SYSLOGS	6 7
Forward Raw Syslog Messages	
Configure SYSLOG Daemon	9
Configure SYSLOG Port	9
Edit SYSLOG Configuration	
Verification	15
Virtual Collection Points for Windows Configure Virtual Collection Points for Windows	18 18
Configure EventTracker Agents to Forward Events on Different Ports	19
Verification	
Summary	



## **Virtual Collection Point**

VCP stands for Virtual Collection Point. VCP is an architectural enhancement available in the EventTracker Manager using which the EventTracker can simultaneously collect event logs on multiple ports. This increases the load capacity of the product significantly while providing performance improvement to all analysis and reporting modules.

### Why go for VCP?

The key benefits of using this architecture are

- Significantly faster analysis and reporting
- Best utilization of system resources and network bandwidth
- Increased load capacity

VCP is ideal for environments where many Windows and NIX systems / devices are monitored by EventTracker. Large setup is measured not only by the number of systems / devices being monitored but also the volume of events / syslogs forwarded by the monitored systems / devices.

By default, EventTracker Receiver works on

- Port 14505 (UDP/TCP) for Windows events
- Port 514 (UDP/TCP) for SYSLOGS

As a benchmark, it is recommended to opt for a VCP model deployment if EventTracker is receiving more than 250 events per second. The VCP model will balance the load and proportionately channel events / SYSLOGS coming into the EventTracker. VCP also eliminates additional hardware enhancements by optimally utilizing the single hardware/system. Last but not the least it creates significant performance improvements in the Analysis and Reporting modules of the product thereby directly saving on valuable end user time.

#### Implement VCP

- Identify the systems / devices that generate high volume of events / SYSLOGS baseline being 100/sec.
- Segregate those systems
- Group those systems into a manageable size
- Assign different port(s) to individual systems / devices in each group to communicate with the EventTracker Manager.

For example, consider EventTracker is monitoring 100 Windows systems. All those systems are critical and generate high volume of events that is above the baseline 500/sec. Assemble those systems into 10 groups with 10 system per group. Assign ports 14505 (default), 14515, 14525, 14535, 14545, 14555, 14565, 14575,



14585 and 14595 respectively to individual systems in each group to communicate with the EventTracker Receiver.

This way the load on Manager is balanced which ultimately enhances the performance. For detailed instructions go to appropriate sections.

## Virtual Collection Points Architecture

Virtual Collection Points (VCP) enable the existing receiver to behave like a collection master without having the physical Collection Points installed. The Existing Collection Point (CP-CM model) requires physically organized Collection Points reporting to a Collection Master. CP-CM model requires several hardware facilities and a large degree of deployment difficulty.

VCP provides the solution to break down the huge volume of input events using the existing set up with minimal configuration changes, thus helps to process the received data in a short time at the reporting end.





EventTracker behaves the same way with multiple instances of its core components. VCP should be configured in such a way that the single instance of EventTracker takes care of a group of systems.

Each EventTracker Receiver instance will receive events from their respective group of systems and maintain the respective cache.



## Virtual Collection Points for SYSLOGS

EventTracker Syslog Receiver can be configured to listen on 10 UDP/TCP ports for Unix/Linux/Solaris Syslogs.

ET Modules	Suggested Trap Ports
You ought to add ports to the Firewall exceptions list.	
EventTracker Syslog Receivers (Incoming)	Default: 514 (UDP/TCP) for Syslogs. You can add max 10 ports for Syslogs

PRISM			Welcome Nir	mal  💐   <u>New</u>	s   <u>Search</u>	Admin   Tools	Help
Alerts Security Operations Netflow	My EventTracker Comp	iance Windows Ana	alysis Log View	Change A	udit Config A	Assessment	
Create Group Delete Group Interface I	lanager		System To	ools		Auto discove	er 🖻
Groups Groups	Systems Search:	Go		Sort by:	Name 💌	Page Size: 25	
	ESXWIN2K864VM2	Windows Server 2008	-	Unmanaged	Unmanaged	High 🛃	
EXCHSUPP	ESXWIN2K864VM3	Windows Server 2008	-	Unmanaged	Unmanaged	High	
	K EXCHTEST	Windows 2003 - Server	-	Unmanaged	Unmanaged	High	
	鰔 GIJOE	Windows XP Pro	-	Unmanaged	Unmanaged	Low	
	🌉 ISA	Windows 2003 - Server	-	Unmanaged	Unmanaged	High	
	🔍 ISA-DLA	Windows 2003 - Server	14515	Agent	Unmanaged	Undefined	
	isAfirewall-DLA	Windows 2003 - Server	14515	Agent	Unmanaged	Undefined	
	JERRY	Windows XP Pro	-	Unmanaged	Unmanaged	Low	
	触 linux,toons,local-syslog	SysLog System	514	Managed	-NA-	Low	
	MICKEY	Windows Vista	-	Unmanaged	Unmanaged	Low	
	MINNIE	Windows XP Pro	-	Unmanaged	Unmanaged	Low	
	MOUGLI	Windows XP Pro	-	Unmanaged	Unmanaged	Low	
	A OBELIX	Windows XP Pro	-	Unmanaged	Unmanaged	Low	
	A OBELIX-II	Windows XP Pro	-	Unmanaged	Unmanaged	Low	
	123						
Freedow B							
Event Tracker 7	Server Time: 08/25 02:58:3	7 PM Response: 0.906 secs			© Copyright 199	99 - 2010 Prism Micros	ystems, Inc.



Details	X
System : linux.toons.lo	cal-syslog
IP Address:	192.168.1.4
Туре:	SysLog System
Port:	514
EventTracker Status:	Managed
Change Audit Status:	-NA-
Description:	-none-
	Ok Close



#### Configure VCP for SYSLOGS

- 1. Log on to EventTracker.
- 2. Click the Admin hyperlink at the upper-right corner.
- 3. Click Manager, click the Syslog / Virtual Collection Point tab.

ISM A							Welcome Nirma	al  💐   <u>News</u>	Search	Admin	Tools	<u>Help</u>
Alerts Security	Operations	Netflow N	My EventTracker	Compliance	Windows	Analysis	Log View	Change Au	dit Conf	ìg Assessm	nent	
Manager Configu	ration											
Configuration	Syslog / Virtual	Collection Point	Direct Log Arch	iver / Netflow Re	ceiver	Agent Settings	E-mail Co	nfiguration				
Syslog Enable SYSLOG	receiver											
Receiver port n	umber		Description		Sy	stem	Protocol	Syslo	g forward p	ort		
514		1	All Syslog Systems (UD	)P)								
										bha	Edit	Remove
Virtual Collection Poi	nts									Haa		Comore
Port number					Des	cription						
14505					All Sy	/stems						
										Add	Edit F	Remove
										[	Save C	ancel
Event Tracker 🦻			Server Time: 08/.	25 03:06:38 PM	Response: 3.250	secs			© Copyright	1999 - 201	0 Prism Micr	osystems, i

Figure 4

4. Click Add under Syslog.

EventTracker displays the Syslog Receiver Port window.

Syslog Receiver Port	X
Port Number :	
Description :	
🗆 Raw Syslog Forward :	
Select a destination and port to which all the incoming events will be forwarded as raw SYSLOG messages.	
Trap Destination :(IP Address or host name)	
Mode: © UDP C TCP	
TCP Port :	
Save	ncel

Figure 5



5. Type the UDP / TCP Port details in the **Port Number** and **Description** fields.

This pair should be unique. Before providing the port details, refer the man pages / documents to confirm that the ports are not used by any other daemons / processes. Move the mouse pointer over the Port Number field, EventTracker displays the well-known ports in a tooltip.

#### 6. Click Save.

EventTracker adds the newly configured ports.

PRISM								Welcome Nirma	al  💐   <u>News</u>	Search	Admin	Tools	Help
Alert	Security	Operations	Netflow	My EventTracker	Compliance	Window:	s Analysis	Log View	Change Audi	t Confi	g Assessmi	ent	
Man	aqer Confiqu	ration											
	onfiguration	Syslog / Virtua	al Collection Poi	int Direct Log Arc	hiver / Netflow Re	ceiver	Agent Settings	E-mail Co	nfiguration				
Sy	slog Enable SYSLOG	receiver											
F	eceiver port r	umber		Description		9	iystem	Protocol	Syslog	forward p	ort		
5	14			All Syslog Systems (U	DP)								
5	15			VCP									
Vir	tual Collection Po ort number	pints				De	scription				Add	Edit F	emove
1	4505					All	5ystems						
											Add	Edit F	lemove
												Save C	ancel
E	vent Tracker			Server Time: 08	/25 03:10:30 PM	Response: 0.2	% secs		C	) Copyright	1999 - 2010	Prism Micro	osystems, Inc.

Figure 6

- 7. Click Save.
- 8. Add the ports to the Firewall exceptions list.

EventTracker Manager listens on two ports 514/UDP, which is the default and 515/UDP, which is user defined.

Group and Configure the NIX systems to forward SYSLOGS through port 514 and 515. For example, if there are 10 NIX systems in your environment, configure 5 systems to forward SYSLOGS through 514/UDP and 5 systems through 515/UDP. This enhances the performance of EventTracker Receiver.

#### Forward Raw Syslog Messages

This option helps to forward received Syslog messages in raw format i.e. forwarded in the same format as it is received from the source to a specified destination.

1. Select the Raw Syslog Forward check box.



Syslog Receiver Port	Х
Port Number :	
Description :	
Raw Syslog Forward :	
Select a destination and port to which all the incoming events will be forwarded as raw SYSLOG messages.	
Trap Destination :(IP Address or host name)	
Mode: O UDP C TCP	
UDP Port	
Save Car	ncel
Save Car	ncel



- 2. Type the name or IP address of the destination in the Trap Destination field.
- 3. Select an appropriate **Mode** of transport.
- 4. Enter/select an appropriate port with respect to the mode chosen.
- 5. Click Save.

#### Configure SYSLOG Daemon

#### Configure SYSLOG Port

1. Log in as root.





2. Type **cd /etc** at the command prompt.



Figure 9

- 3. Press ENTER on your keyboard.
- 4. Type vi services.





- 5. Press ENTER on your keyboard.
- Press i on your keyboard to insert / edit the syslog port.
   For example: syslog 514/udp as syslog 515/udp.

🛃 root@mango:/etc				
pop3s	995/udp		# POP-3 over SSL	^
#				
# UNIX specific	services			
#				
exec	512/tcp			
biff	512/udp	comsat		
login	513/tcp			
who	513/udp	whod		
shell	514/tcp	cmd	# no passwords used	
syslog	51 <mark>4</mark> /udp			
printer	515/tcp	spooler	# line printer spooler	
printer	515/udp	spooler	# line printer spooler	
talk	517/udp			
ntalk	518/udp			
utime	519/tcp	unixtime		
utime	519/udp	unixtime		
efs	520/tcp			
router	520/udp	route routed	# RIP	
ripng	521/tcp			
ripng	521/udp			
timed	525/tcp	timeserver		
timed	525/udp	timeserver		
INSERT				~



- 7. Press **ESC** on your keyboard.
- 8. Type :wq on your keyboard to save the changes.

🛃 root@mango:/etc	:				$\mathbf{X}$
pop3s	995/udp		#	POP-3 over SSL	^
# # UNIX specific	services				
#					
exec	512/tcp				
biff	512/udp	comsat			
login	513/tcp				
who	513/udp	whod			
shell	514/tcp	cmd	#	no passwords used	
syslog	515/udp				
printer	515/tcp	spooler	#	line printer spooler	
printer	515/udp	spooler	#	line printer spooler	
talk	517/udp				_
ntalk	518/udp				=
utime	519/tcp	unixtime			
utime	519/udp	unixtime			
efs	520/tcp				
router	520/udp	route routed	#	RIP	
ripng	521/tcp				
ripng	521/udp				
timed	525/tcp	timeserver			
timed	525/udp	timeserver			
: MC					



9. Press ENTER on your keyboard.



Figure 13

10. Type ./init.d/syslog restart to restart the syslog daemon.



Figure 14

11. Press ENTER on your keyboard.





Figure 15

#### Edit SYSLOG Configuration

1. Type vi syslog.conf at the command prompt.



Figure 16



2. Press ENTER on your keyboard.

🖻 root@mango:/etc	
<pre> # Log anything (except mail) of level info or higher. # Don't log private authentication, cron, or vmkernel messages! *.info;mail.none;authpriv.none;cron.none;ftp.none /var/log/messages # Log ftp messages in ftp.log ftp.* -/var/log/ftp.log</pre>	
# Save boot messages also to boot.log local2.* /var/log/local2.1	og
auth.*;authpriv.* /var/log/auth.log *.* @192.168.1.44 *.* @192.168.1.24 *.* @192.168.1.113 *.* @192.168.1.115 ~ ~ ~ ~ ~ ~ ~	
"syslog.conf" 14L, 479C	~

Figure 17

- 3. Press I on your keyboard to insert.
- 4. Type \*.\* @IP address
- \*.\* @192.168.1.19
- Type "asterisk' followed by a "period' and an "asterisk'
- Press **TAB** on your keyboard.
- Type "at the rate" symbol followed by IP address of the EventTracker server.
- \*.\* signifies all Syslog messages will be forwarded to the destination computer.
- 5. Press ESC on your keyboard.
- 6. Type :wq to save the changes.
- 7. Press ENTER on your keyboard.
- 8. Type ./init.d/syslog restart to restart the syslog daemon.
- 9. Click ENTER on your keyboard.



#### Verification

Open the Task Manager to verify EventTracker Receiver spawned a new process EtReceiver-S-515.exe.

oplications	Processes Perform	ance Networking Users			
Image Nan	ne	User Name	CPU	Mem Usage	
wmiprvse.	exe	NETWORK SERVICE	00	4,032 K	
Collection	lasterConsole.exe	SYSTEM	00	6,960 K	
csrss.exe		SYSTEM	00	1,408 K	
EtReceiver	-S-514.exe	SYSTEM	00	10,600 K	
evtarmgr.e	exe	SYSTEM	00	9,180 K	
sqlservr.ex	æ	NETWORK SERVICE	00	153,396 K	
taskmgr.ex	e	nirmal	00	5,480 K	
evtmgr.ex	e	SYSTEM	00	8,108 K	
EtSchedule	er.exe	SYSTEM	00	8,420 K	
rdpclip.exe		nirmal	00	1,648 K	
explorer.e	xe	nirmal	02	9,696 K	
EtReceiver	-S-515.exe	SYSTEM	00	11,064 K	
inetinfo.ex	e	SYSTEM	00	3,336 K	
UserActivit	y.exe	SYSTEM	00	11,684 K	
wmiprvse.	exe	SYSTEM	00	816 K	
UltiDevCas	sinWebServer2a.ex	e SYSTEM	00	59,388 K	
svchost.e>	e	SYSTEM	00	2,324 K	
ccApp.exe		nirmal	00	608 K	
svchost.e>	e	SYSTEM	00	584 K	
svchost.e>	e	SYSTEM	00	1,556 K	
logon.scr		LOCAL SERVICE	00	240 K	-
🔽 Show pr	ocesses from all use	rs		<u>E</u> nd Pro	ocess

Figure 18

1. Open the System Manager to verify EventTracker Receiver receives SYSLOG messages at the configured port 515/UDP.



vers Jecuity Operations Weth	iow My Event tracker Compile	ance Windows Ana	iysis Log v	lew Change A	uait Config A	Assessment
Create Group Delete Group Interf	ace Manager		Syste	em Tools		Auto discover
roups Groups	Systems Search:	Go		Sort by:	Name 💌	Page Size: 25 💌
	ESXWIN2K864VM2	Windows Server 2008	2	Unmanaged	Unmanaged	High
EXCHSUPP	ESXWIN2K864VM3	Windows Server 2008	-	Unmanaged	Unmanaged	High
	K EXCHTEST	Windows 2003 - Server	ň.	Unmanaged	Unmanaged	High
	🙏 GIJOE	Windows XP Pro	-	Unmanaged	Unmanaged	Low
	🍂 ISA	Windows 2003 - Server	12	Unmanaged	Unmanaged	High
	🙏 ISA-DLA	Windows 2003 - Server	14515	Agent	Unmanaged	Undefined
	鷠 ISAfirewall-DLA	Windows 2003 - Server	14515	Agent	Unmanaged	Undefined
	🍂 JERRY	Windows XP Pro	-	Unmanaged	Unmanaged	Low
	属 linux.toons.local-syslog	SysLog System	515	Managed	-NA-	Low
	MICKEY	Windows Vista	-	Unmanaged	Unmanaged	Low
	鰔 MINNIE	Windows XP Pro	1	Unmanaged	Unmanaged	Low
	🙏 MOUGLI	Windows XP Pro	-	Unmanaged	Unmanaged	Low
	M OBELIX	Windows XP Pro	18	Unmanaged	Unmanaged	Low
	OBELIX-II	Windows XP Pro	-	Unmanaged	Unmanaged	Low
	123					

Figure 19

- 2. Click **Log View** on the EventTracker home page.
- 3. Select the Syslog system from the System(s) drop-down list.

PRISM						Welcome Nirma	al  💐   <u>News</u>	<u>Search</u>	Admin	Tools	Help
Alerts Security Operation	s Netflow	My EventTracker	Compliance	Windows	Analysis	Log View	Change Audit	: Confi	g Assessme	ent	
Log View System(s): Select system(s) System(s): Select system(s) Control Control Co	DC DC-DLA -DLA ;.local-syslog iERVER1-DLA -DLA	Category:	Select a category	All Alerts		] ¥ Go	Cancel New S	iearch		я <b>ц</b>	
Event Tracker 🦻		Server Time: 08/	25 03:33:34 PM 1	Response: 0.109 si	105		C	Copyright	1999 - 2010	Prism Micros	ystems, Inc.

Figure 20



4. Select the **Syslog** -> **\*All Syslog events** Category from the Category drop-down list.

PRISM								Welcome Nirr	nal  💐   <u>News</u>	Search	Admin	<u>Tools</u>	Help
Alerts	Security	Operations	Netflow	My EventTracker	Compliance	Windows	Analysis	Log View	Change Aud	it Config	g Assessme	ent	
Log Vi	ew (s): Iinux.too All Sy	ns.local-syslog stems		Category:	Select a categor McAfee Microsc Motoro Netscre Solaris	y > Sidewinder Fire > Sidewinder Fire > Stewinder Sire BSM all UTM ous Network Act Syslog events cal Facilities > log: Authorizatic	ewall ber V tivity		Cencel New	Search			
Eve	nt Tracker 7	5		Server Time: 08	1/25 03:34:17 PM	Response: 0.734 s	ecs		G	) Copyright :	1999 - 2010	Prism Micros	ystems, Inc.

Figure 21

5. Click **Go**.

PRISM							Welcome Nirmal) 🂐   <u>News</u>   <u>Search</u>   <u>Admin</u>   <u>Tools</u>   <u>Help</u>
Alerts Security	Opera	tions Netflow	My EventTra	cker   Compliance	Windows	s Analysis	Log View Change Audit Config Assessment
Log View System(s): linux.ti	oons:local-sy Systems	rslog	× Cat	egory: *All Syslog eve All Categor	ents ies 🗖 All Aler	ts	So Carcel New Search
Log Time	Event Id	l Computer	User	Domain Log Type	Event Type	Source	Description
8/25/2010 3:34:16 PM	0	LINUX.TOONS.LOCAL SYSLOG	N/A	N/A System	Information	SYSLOG kernel	Aug 25 15:34:16 linux.toons.local MARK
8/25/2010 3:33:16 PM	0	LINUX.TOONS.LOCAL SYSLOG	N/A	N/A System	Information	SYSLOG kernel	Aug 25 15:33:16 linux.toons.local MARK
8/25/2010 3:32:16 PM	0	LINUX.TOONS.LOCAL SYSLOG	N/A	N/A System	Information	SYSLOG kernel	Aug 25 15:32:16 linux.toons.local MARK
8/25/2010 3:31:16 PM	0	LINUX.TOONS.LOCAL SYSLOG	N/A	N/A System	Information	SYSLOG kernel	Aug 25 15:31:16 linux.toons.local MARK
8/25/2010 3:30:16 PM	0	LINUX.TOONS.LOCAL SYSLOG	N/A	N/A System	Information	SYSLOG kernel	Aug 25 15:30:16 linux.toons.local MARK
8/25/2010 3:29:16 PM	0	LINUX.TOONS.LOCAL SYSLOG	N/A	N/A System	Information	SYSLOG kernel	Aug 25 15:29:16 linux.toons.local MARK
8/25/2010 3:28:20 PM	0	LINUX.TOONS.LOCAL SYSLOG	N/A	N/A System	Information	SYSLOG kernel	Aug 25 15:28:20 linux.toons.local kernel: klogd 1.4.1, log source = /proc/kmsg started.
8/25/2010 3:28:16 PM	40	LINUX.TOON5.LOCAL SYSLOG	N/A	N/A System	Information	SYSLOG syslog	Aug 25 15:28:16 linux.toons.local syslogd 1.4.1: restart.
Event Tracker	7		Server	Time: 08/25 03:34:17 PM	Response: 0.73	14 secs	© Copyright 1999 - 2010 Prism Microsystems, Inc.

Figure 22



## **Virtual Collection Points for Windows**

EventTracker Receiver can be configured to listen on 10 ports for Windows.

ET Modules	Suggested Trap Ports					
You ought to add ports to the Firewall exceptions list.						
EventTracker Syslog Receivers (Incoming)	14505 default port.14515, 14525, 14535, 14545, 14555, 14565, 14575, 14585, 14595 (max 10 ports).					

### Configure Virtual Collection Points for Windows

- 1. Log on to EventTracker.
- 2. Click the **Admin** hyperlink at the upper-right corner.
- 3. Click Manager on the Control Panel.
- 4. Click the Syslog / Virtual Collection Point tab.
- Click Add under Virtual Collection Points.
   EventTracker displays the Receiver Port pop-up window.
- Type the port number and description in the **Port Number** and **Description** fields.
   Before typing the port numbers, refer the man pages / documents to confirm that the ports are not used by any other services / processes.

Receiver Port		X
Port Number :	14525	
Description :	Managed Comp: WEBDOC1	
		Save Cancel

Figure 23

7. Click Save.

EventTracker adds the newly configured ports.



SM 4								Welcome Nirm	al  💐   <u>News</u>	Search	Admin	Tools	<u>He</u>
erts	Security	Operations	Netflow	My EventTracker	Compliance	Windows	Analysis	Log View	Change Aud	it Confi	g Assessmi	ent	
anac	er Confiqu	ration											
Conf	iguration	Syslog / Virtua	l Collection Poi	nt Direct Log Arc	hiver / Netflow Re	eceiver	Agent Settings	E-mail C	onfiguration				
Syslo I E	g nable SYSLOG	receiver											
Rec	eiver port n	umber		Description		59	stem	Protocol	Syslog	forward p	ort		
514				All Syslog Systems (U	DP)								
515				VCP									
Virtua Po <u>r</u>	l Collection Po t number	ints		De	scription								
Virtua	l Collection Po	ints		De	cuintion								
145	)5			ALS	iystems								
145	25			Mar	aged Comp: WEB	BDOC1							
											Add	Edit F	lemove
												Sauce	ancol
E.c.											_	Dave C	ancer

Figure 24

- 8. Click **Save** on the Manager Configuration page.
- 9. Add the ports to the Firewall exceptions list.
  - EventTracker Manager listens on two ports 14505, which is the default and 14525, which is user defined.

## Configure EventTracker Agents to Forward Events on Different Ports

Group and Configure the Windows systems to forward events through port 14505 and 14525. For example, if there are 10 Windows systems in your environment, configure 5 systems to forward events through 14505 and 5 systems through 14515. This enhances the performance of EventTracker Receiver.

Open the etagentconfig.ini of the remote system.
 For example, etaconfig.ini.WEBDOC1 from the EventTracker installation folder...\Program Files\Prism Microsystems\EventTracker\AgentConfig



Ď etaconfig.ini.WEBDOC1 - Notepad	
File Edit Format View Help	
GeneralGeneral [Product] prod_name = prod_ver = prod_serial = debug = 0 [End]	4
<pre>[System] sys_name = WEBDOC1 sys_et_port = 14503 sys_evtlog = true sys_services = false sys_activity = true sys_type = 1 [End]</pre>	
[security] agent_version = 7.0 - Build 105 protect_ip = protect_flag = false ver_minor = 5 ver_major = 1 remedial_action = false [End]	
ManagersManagers [Manager] mgr_name = ESXWEBDOC mgr_port = 14505 mgr_report = traps commstr = public cache_path = encryption_req = false [End]	-1

#### Figure 25

It is clear from figure above, by default, remote agent communicates with the Manager through port 14505. When you change the port number through Agent Configuration window, EventTracker updates this field with the new value.

- 1. Double-click EventTracker Agent Configuration on the desktop Control Panel.
- 2. Select a managed system from the Select Systems drop-down list.



ventTracker Agent Cor	nfiguration		
Help			
elect Systems			
/EBDOC1		Agent based	l system
Apply the following set	tinas to specified Aa	ents	
hager destinations:			
XWEBDUC			
Services   Log Back	up Processe	s Network Con	nections
Loghie Monitor	File Fransfer	Config Asses	isment itor Apps
	illers   System		itor Apps
Jpto 5 managers can be co	onfigured.		
Manager Name	Port	Mode Encr	runt T
ESXWEBDOC	14505	UDP No	<u>984  </u>
A <u>d</u> d <u>E</u> dit	<u>R</u> emove		
Cours	1	Class	
Zave		<u><u>C</u>1056</u>	

Figure 26

Select the Manager Name and then click Edit.
 EventTracker displays the Edit Destination window.



🕎 Edit Des	tination	×
Destination	ESV/EPDOC	_
Destination:	Fervice	
Port:	14505	
Connect t	o Manager using	
High Perfo and is the	prmance Mode uses minimal network traffic (UDF best choice for most installations.	<sup>2</sup> )
⊙ <u>H</u> igh F	Performance Mode (UDP)	
⊂ <u>G</u> uara	nteed Delivery Mode (TCP)	
Encry	ypt: No	
Even	it <u>c</u> ache folder:	
<u>M</u> inin on St	num Amount of Free space to be left torage Device (%):	3
	OK Ca <u>n</u> cel	

Figure 27

4. Type the port number as 14525 in the **Port** field and then click **OK**. EventTracker updates the port number.



🕎 EventTracker Agent Configura	tion			×
<u>F</u> ile <u>H</u> elp				
Select Systems				
WEBDOC1		▼ Agent	based system	
Apply the following settings to	specified Ager	rts		
Manager destinations:				
ESXWEBDOC				-
Services   Log Backup   Logfile Monitor   File Managers   Event Filters	Processes Transfer System N	Netwo Config Monitor	rk Connections Assessment Monitor Apps	
Upto 5 managers can be configured	d.			
Manager Name	Port	Mode	Encrypt	
ESXWEBDOC	14525	UDP	No	
Add Edit Be	emove			
<u>S</u> ave		<u>C</u> lose		

Figure 28

5. Click <u>Save</u> and then click Close.

Open etaconfig.ini.WEBDOC1 from the location mentioned earlier to check if EventTracker has updated the mgr\_port with new port number.



📕 etaconfig.ini.WEBDOC1 - Notepad	
Eile Edit Format View Help	
GeneralGeneral [Product] prod_name = prod_ver = prod_serial = debug = 0 [End]	
<pre>[system] sys_name = WEBDOC1 sys_et_port = 14503 sys_evtlog = true sys_services = false sys_activity = true sys_type = 1 [End]</pre>	
<pre>[security] agent_version = 7.0 - Build 105 protect_ip = protect_flag = false ver_minor = 5 ver_major = 1 remedial_action = false [End]</pre>	
Managers [Manager] mgr_name = ESXWEBDOC mgr_port = <mark>14525</mark> mgr_report = traps commstr = Public cache_path = encryption_req = false [End]	
I	► //

Figure 29

#### Verification

• Open the Task Manager to verify EventTracker Receiver spawned a new process EtReceiver-W-14525.exe.



	Treiroiniand	e   Networking   Users				
Image Name		User Name	CPU	Mem Usage		
wmiprvse.exe		NETWORK SERVICE	00	4,116 K		
EtReceiver-W-14525.exe		SYSTEM	00	11,272 K		
EtScheduler.exe		SYSTEM	00	8,400 K		
evtProcessEcFile.exe		SYSTEM	02	6,512 K		
EtReceiver-S-514.exe		SYSTEM	02	10,348 K		
csrss.exe		SYSTEM	00	1,432 K		
evtmgr.exe		SYSTEM	00	8,128 K		
CollectionMasterConsole.exe		SYSTEM	00	6,960 K	_	
w3wp.exe		NETWORK SERVICE	00	81,040 K		
sqlservr.exe		NETWORK SERVICE	02	75,132 K		
rdpclip.exe		nirmal	00	3,152 K		
explorer.exe inetinfo.exe wmiprvse.exe EtReceiver-W-14505.exe UltiDevCassinWebServer2a.exe		nirmal	00	11,144 K		
		SYSTEM	00	3,344 K		
		SYSTEM	00	724 K		
		SYSTEM	00	11,316 K		
		SYSTEM	00	70,772 K		
svchost.exe		SYSTEM	00	2,336 K		
ccApp.exe		nirmal	00	532 K		
svchost.exe		SYSTEM	00	428 K		
svchost.exe		SYSTEM	00	1,560 K		
logon.scr		LOCAL SERVICE	00	240 K	-	
Show processes from all users				End Pro	End Process	

Figure 30

• Open the System Manager to verify EventTracker Receiver receives Windows events at the configured port 14525.



		mpliance mindows Analy	55 209 0000		Coning Abbo	Sincrit		
reate Group Delete Group Interfa	ace Manager		System Too	<u>lls</u>		Auto discover		
ups 	Systems Search: Go Sort by: Name Page Size: 25 V							
	123							
	Computer	Туре	EventTracker Port	EventTracker Status	Change Audit Status	Asset value		
	SUPPSERVER	Windows 2003 - Server	14 (A)	Unmanaged	Unmanaged	High		
	SYMSERVER	Windows 2003 - Server	1.50	Unmanaged	Unmanaged	High		
- SUPPORT	🙀 SYS5	Windows XP Pro	-	Unmanaged	Unmanaged	Low		
TOONS	🝂 SY58	Windows XP Pro	14	Unmanaged	Unmanaged	Low		
	🙏 ТОМ	Windows XP Pro	12	Unmanaged	Unmanaged	Low		
	M TOMCRUISE	Windows XP Pro		Unmanaged	Unmanaged	Low		
	WEBDOC1	Windows XP Pro	14525	Agent	Unmanaged	Low		
	WEBDOC1-DLA	Windows XP Pro	14505	Agent	Unmanaged	Low		
	WINHV2K8	Windows Server 2008	(27)	Unmanaged	Unmanaged	High		
	123							

Figure 31

#### Summary

Success of any application depends on performance optimization and load balancing, EventTracker is no exception.

Implementing Virtual Collection Points will give the following benefits

- Significantly faster analysis and reporting
- Best utilization of system resources and network bandwidth
- Increased load capacity
- Enhances the overall performance of EventTracker.

