

Enhancement in Agent syslog collector to resolve sender IP Address

EventTracker Enterprise

Enhancement in Agent syslog collector to resolve sender IP Address.

Update: ET82U16-031/ET82UA16-031

Abstract: This update will help the user to change the FQDN related configurations.

Who should read this document?

Customers who use v 8.2 Build 14.

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

This document is for informational purposes only. Prism Microsystems 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 Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems 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 Prism Microsystems, 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.

© 2016 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Process to be followed after applying the Update.....	3
To Report System Name as FQDN.....	5
To Assign suffix or string to a System Name,.....	6
To assign system name as FQDN and add string to it,.....	9

Process to be followed after applying the Update

- Open the **EventTracker Control Panel**.
- Double-click **EventTracker Agent Configuration**.

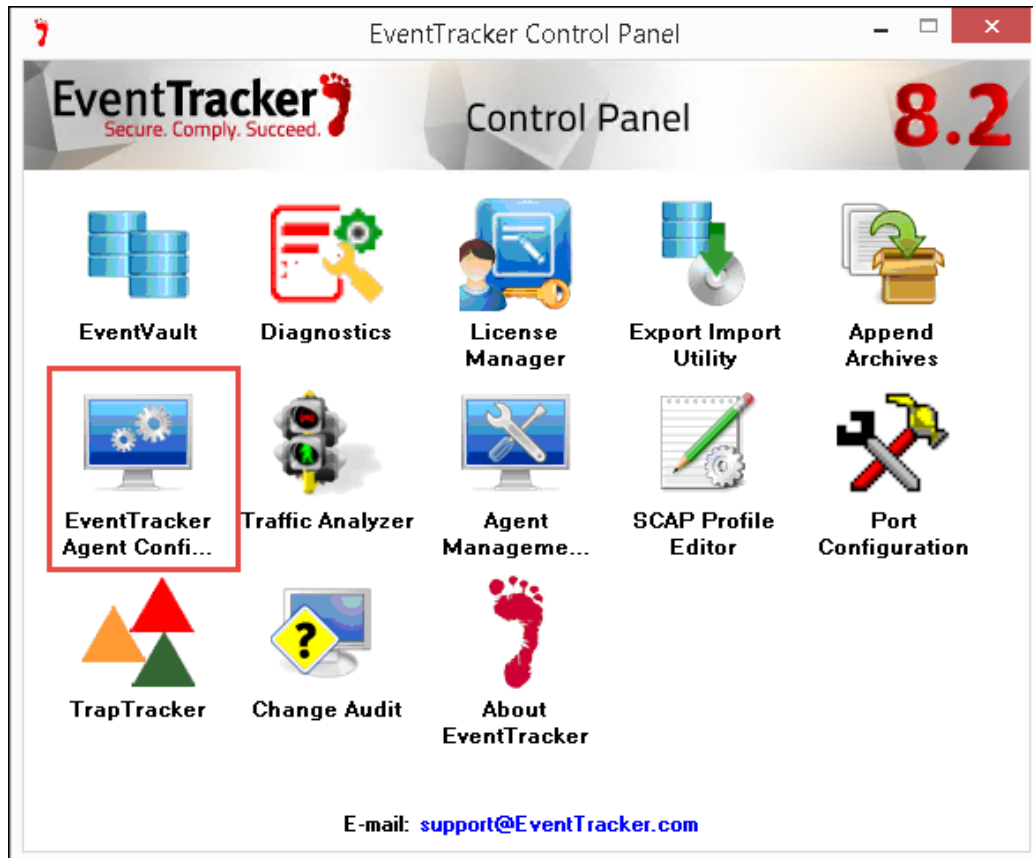


Figure 1

EventTracker Agent Configuration window displays.

Enhancement in Agent syslog collector to resolve sender IP Address.

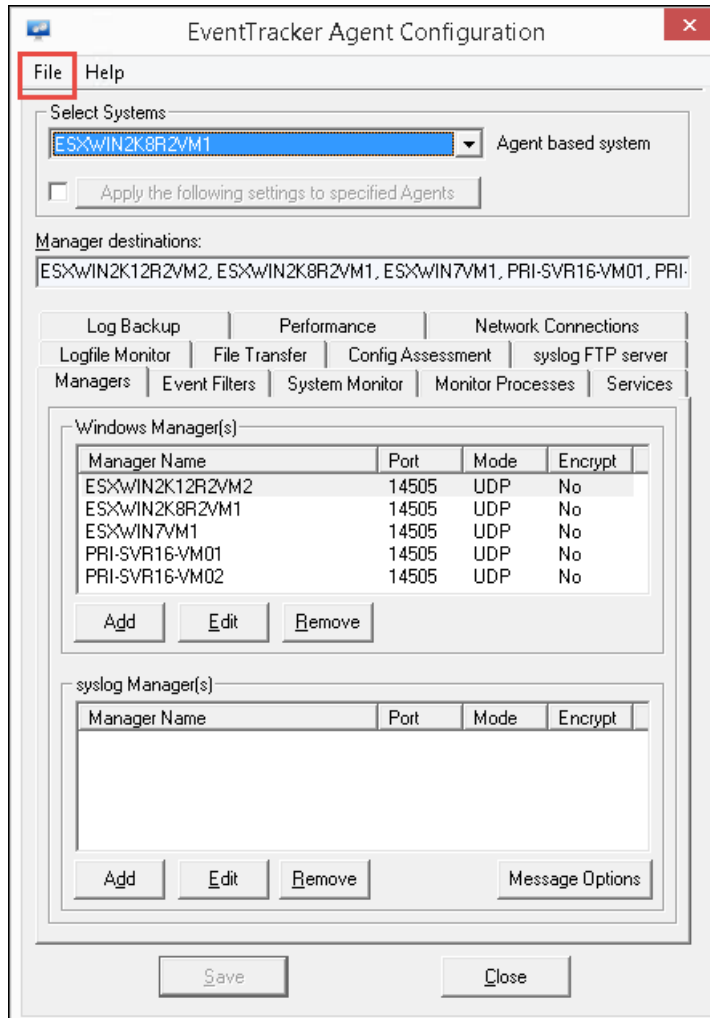


Figure 2

- Click the **File** option and select **Systems** from the dropdown list.

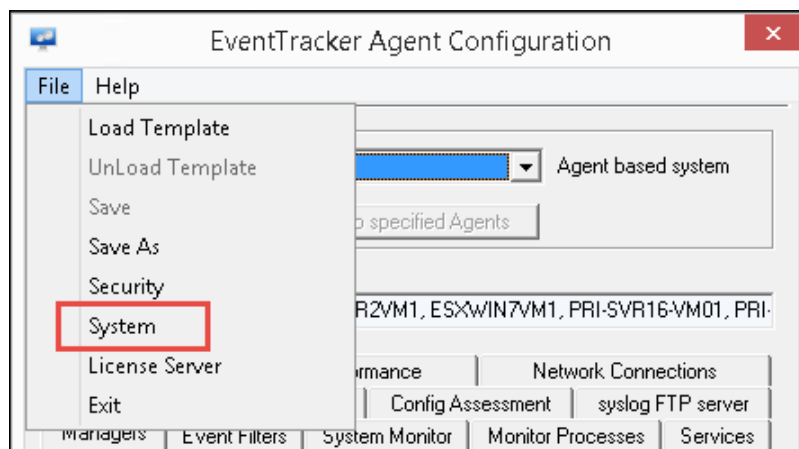


Figure 3

Enhancement in Agent syslog collector to resolve sender IP Address.

The System window gets displayed.

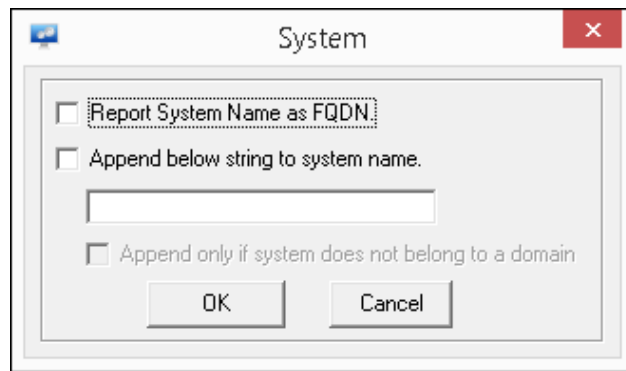


Figure 4

To Report System Name as FQDN

- Check the 'Report System Name as FQDN'.

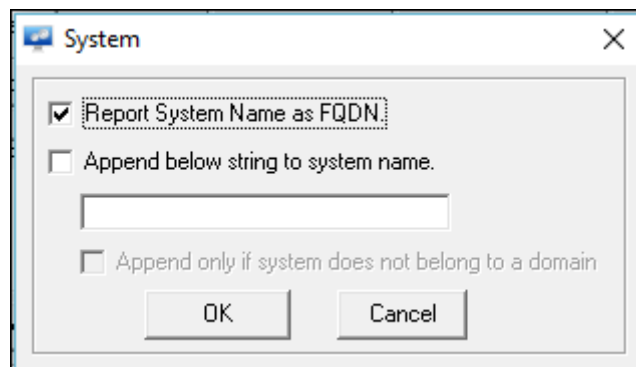


Figure 5

- Click **OK** and **Save** the configuration changes.

NOTE:

- The reporting manager will display the NetBIOS system name along with the FQDN name, when the FQDN is enabled.
- The user should select the NetBIOS system name if he/she wants to perform a search/report for older period.

To view the system name as FQDN, login to **EventTracker web-> Admin->Systems**.

Enhancement in Agent syslog collector to resolve sender IP Address.

COMPUTER	TYPE	PORT	EVENTTRACKER VERSION	CHANGE AUDIT VERSION	ASSET VALUE	
ESXWIN2K12R2VM2	2016	14505	8.2 - Build 14	--	High	⚙️
ESXWIN2K8R2VM1	2012 R2	14505	8.2 - Build 14	8.2 - Build 14	High	⚙️
ESXWIN2K8R2VM1-DLA	2012 R2	14505	--	--	Serious	⚙️
ESXWIN2K8R2VM1.Toons.local	2012 R2	14505	8.2 - Build 14	--	High	⚙️
ESXWIN7VM1	Win 8.1	14505	8.2 - Build 14	--	Low	⚙️
PRI-SVR16-VM01	2016	14505	8.2 - Build 14	--	High	⚙️
PRI-SVR16-VM02	2016	14505	8.1 - Build 9	--	High	⚙️

Figure 6

Syslog System with FQDN enabled:

COMPUTER	TYPE	PORT	EVENTTRACKER VERSION	CHANGE AUDIT VERSION	ASSET VALUE	
pnpl-2-test.Toons.local-syslog	Syslog	514	Managed	-NA-	Low	⚙️
R153VM1.Toons.local-syslog	pnpl-2-test.Toons.local-syslog		8.2 - Build 14	--	High	⚙️
R153VM1.Toons.local-syslog	2008 R2	14540	--	--	High	⚙️

Figure 7

To Assign suffix or string to a System Name,

- Check the 'Append below string to system name' option.
- Add the suffix, for example: 'EventTracker'.

NOTE: The Allowed Special Characters are: ".", "_", "-" and <%Mac%> for system MAC address.

Enhancement in Agent syslog collector to resolve sender IP Address.

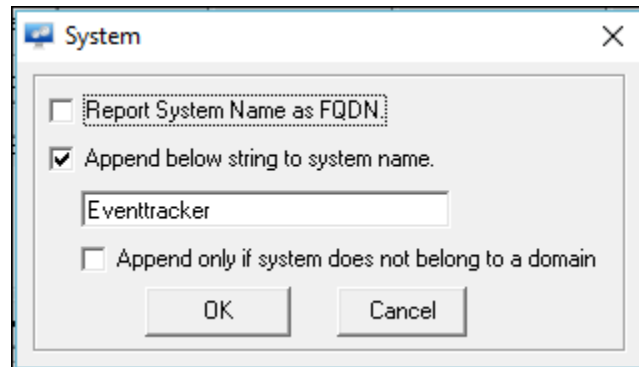
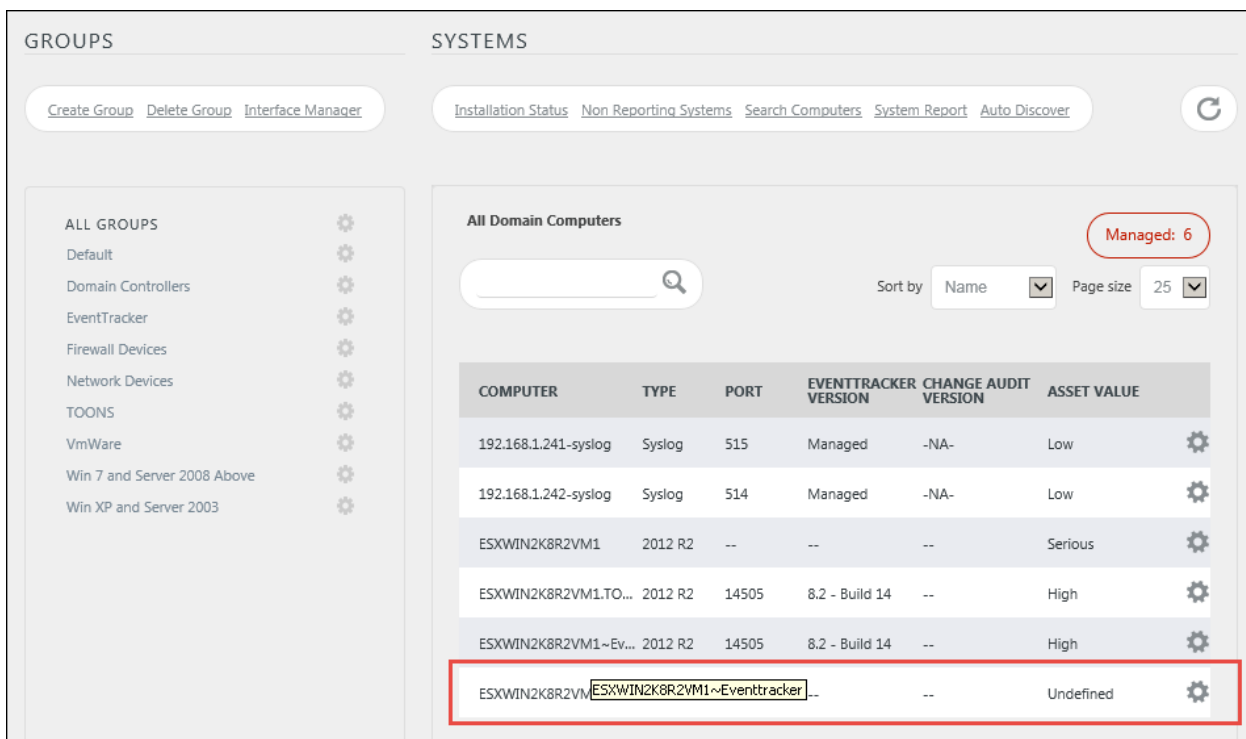


Figure 8

- Click **OK** and **Save** the configuration changes.

To view the System name with suffix '**EventTracker**', login to **EventTracker web-> Admin->Systems**.



GROUPS SYSTEMS

Create Group Delete Group Interface Manager Installation Status Non Reporting Systems Search Computers System Report Auto Discover

ALL GROUPS Default Domain Controllers EventTracker Firewall Devices Network Devices TOONS VmWare Win 7 and Server 2008 Above Win XP and Server 2003

All Domain Computers Managed: 6

Sort by Name Page size 25

COMPUTER	TYPE	PORT	EVENTTRACKER VERSION	CHANGE AUDIT VERSION	ASSET VALUE
192.168.1.241-syslog	Syslog	515	Managed	-NA-	Low
192.168.1.242-syslog	Syslog	514	Managed	-NA-	Low
ESXWIN2K8R2VM1	2012 R2	--	--	--	Serious
ESXWIN2K8R2VM1.TO...	2012 R2	14505	8.2 - Build 14	--	High
ESXWIN2K8R2VM1~Ev...	2012 R2	14505	8.2 - Build 14	--	High
ESXWIN2K8R2VM1~Eventtracker	--	--	--	--	Undefined

Figure 9

Enhancement in Agent syslog collector to resolve sender IP Address.

Syslog System with String enabled:

Name	OS	IP	Version	Build	Severity	Actions
ESXWIN7VM1-DLA	Unknown	14505	--	--	Undefined	⚙️ ^
PRI-SVR16-VM01	2016	14505	8.1 - Build 9	--	High	⚙️
PRI-SVR16-VM01-DLA	Unknown	14505	--	--	Undefined	⚙️
PRI-SVR16-VM02	2016	14505	8.2 - Build 14	--	Serious	⚙️
PRI-SVR16-VM02-DLA	2016	14505	--	--	Serious	⚙️
PRI-SVR16-VM02.To...	2016	14505	8.2 - Build 14	--	High	⚙️
PRI-SVR16-VM02~E...	2016	14505	8.2 - Build 14	--	High	⚙️
PRI-SVR16-VM02~E...	2016	14505	--	--	High	⚙️
WIN-I660NFU9LNA	Unknown	14505	8.2 - Build 14	--	Undefined	⚙️

Figure 10

For MAC Systems with string enabled:

- Enter the string '<%MAC%>' as shown below. Click **OK** and **Save** the changes.

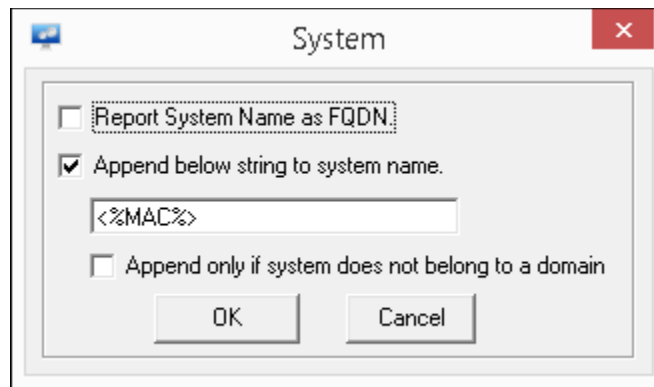
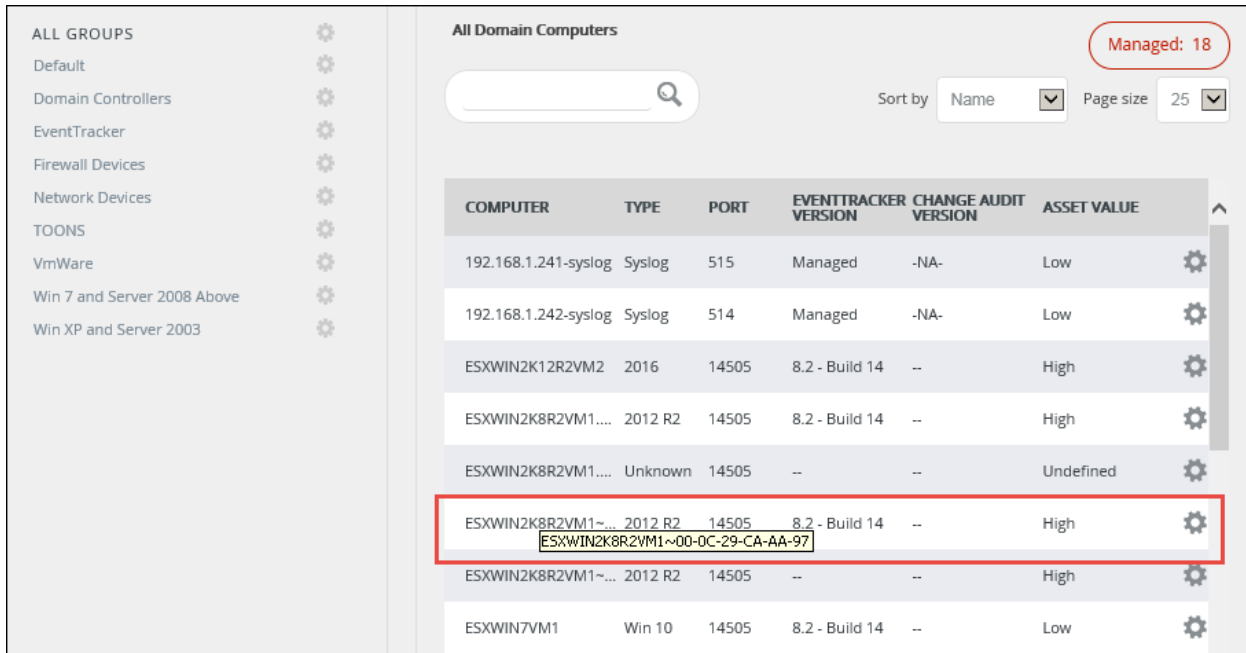


Figure 11

- View the changes in System Manager.

Enhancement in Agent syslog collector to resolve sender IP Address.



COMPUTER	TYPE	PORT	EVENTTRACKER VERSION	CHANGE AUDIT VERSION	ASSET VALUE
192.168.1.241-syslog	Syslog	515	Managed	-NA-	Low
192.168.1.242-syslog	Syslog	514	Managed	-NA-	Low
ESXWIN2K12R2VM2	2016	14505	8.2 - Build 14	--	High
ESXWIN2K8R2VM1...	2012 R2	14505	8.2 - Build 14	--	High
ESXWIN2K8R2VM1...	Unknown	14505	--	--	Undefined
ESXWIN2K8R2VM1~... ESXWIN2K8R2VM1~00-0C-29-CA-AA-97	2012 R2	14505	8.2 - Build 14	--	High
ESXWIN2K8R2VM1~...	2012 R2	14505	--	--	High
ESXWIN7VM1	Win 10	14505	8.2 - Build 14	--	Low

Figure 12

To assign system name as FQDN and add string to it,

- Check both the options 'Report System Name as FQDN' and 'Append below string to system name'.
- Add the string name.

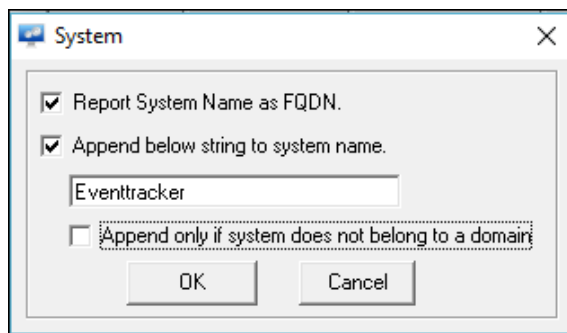


Figure 13

- Click **OK** and **Save** the configuration changes.

To view the changes in System Manager, login to **EventTracker web**-> **Admin**->**Systems**.

The system name appears with the FQDN '**Toons.local**' and Suffix '**Eventtracker**'.

Enhancement in Agent syslog collector to resolve sender IP Address.

The screenshot shows the 'SYSTEMS' section of the EventTracker interface. On the left, there is a 'GROUPS' sidebar with various categories like 'ALL GROUPS', 'Default', 'Domain Controllers', etc. The main area displays 'All Domain Computers' with a search bar and sorting options. A table lists system details:

COMPUTER	TYPE	PORT	EVENTTRACKER VERSION	CHANGE AUDIT VERSION	ASSET VALUE
192.168.1.241-syslog	Syslog	515	Managed	-NA-	Low
192.168.1.242-syslog	Syslog	514	Managed	-NA-	Low
ESXWIN2K8R2VM1	2012 R2	--	--	--	Serious
ESXWIN2K8R2VM1.To...	2012 R2	14505	8.2 - Build 14	--	High
ESXWIN2K8R2VM1.To...	2012 R2	14505	8.2 - Build 14	--	High
ESXWIN2K8R2VM1.Toons.local~Eventtracker				--	Undefined
ESXWIN2K8R2VM1~Ev...	2012 R2	14505	8.2 - Build 14	--	High
ESXWIN2K8R2VM1~Ev...	Unknown	14505	--	--	Undefined

Figure 14

For Syslog System with FQDN and String enabled, it will appear as below:

The screenshot shows the 'SYSTEMS' section of the EventTracker interface. On the left, there is a 'GROUPS' sidebar. The main area displays 'All Domain Computers' with a search bar and sorting options. A table lists system details:

COMPUTER	TYPE	PORT	EVENTTRACKER VERSION	CHANGE AUDIT VERSION	ASSET VALUE
192.168.1.241-syslog	Syslog	515	Managed	-NA-	Low
192.168.1.242-syslog	Syslog	514	Managed	-NA-	Low
PRI-SVR16-VM02.Toons.local~Eventtracker-syslog			- Build 14	--	High
PRI-SVR16-VM02	2016	14505	8.2 - Build 14	--	Serious
PRI-SVR16-VM02-DLA	2016	14505	--	--	Serious
PRI-SVR16-VM02.To...	2016	14505	8.2 - Build 14	--	High
WIN-I660NFU9LNA	Unknown	14505	8.2 - Build 14	--	Undefined
WIN-SR0JQLUQUU	Unknown	14505	8.2 - Build 14	--	Undefined
ESXWIN7VM1-DLA	Unknown	14505	--	--	Undefined

Figure 15

Enhancement in Agent syslog collector to resolve sender IP Address.

If the user wants to assign or add string to a system belonging to an unknown domain or work group,

- Check the option '**Append only if system does not belong to a domain**'.
- Click **OK** and **Save** the changes.

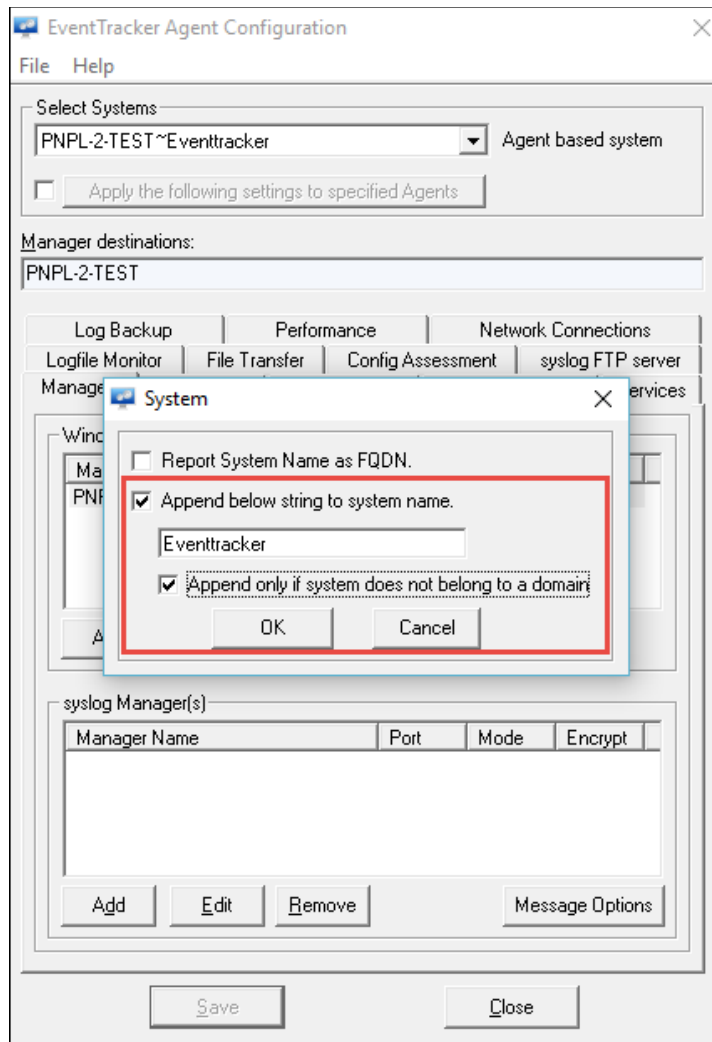


Figure 16

The system can be viewed in the System Manager with the mentioned suffix '**EventTracker**'.

Enhancement in Agent syslog collector to resolve sender IP Address.

The screenshot displays the 'Default - Default Group' management interface. On the left, a sidebar lists various system groups like 'Domain Controllers', 'EventTracker', and 'Network Devices'. The main area shows a table of managed assets. The table is filtered to show 2 managed items. The second item, 'PNPL-2-TEST~Eventtr...', is highlighted with a red border. A tooltip below it displays the full name 'PNPL-2-TEST~Eventtracker'.

COMPUTER	TYPE	PORT	EVENTTRACKER VERSION	CHANGE AUDIT VERSION	ASSET VALUE
EXCHTEST	Unknown	14505	8.2 - Build 14	--	Undefined
PNPL-2-TEST~Eventtr...	Unknown	14505	8.2 - Build 14	--	Undefined

Figure 17