Receive and Forward syslog events through EventTracker Agent

EventTracker v8.2

Publication Date: Aug. 23, 2016

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Abstract

The purpose of this document is to help users to receive syslog messages from various network devices, encrypt them and then forward these syslog messages to EventTracker Manager.

Target Audience

This guide is helpful for users who receive and forward syslog messages through EventTracker agent.

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, Inc. must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, Inc. and Prism Microsystems, Inc. cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems, Inc. MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Prism Microsystems, Inc. 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, Inc. 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.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

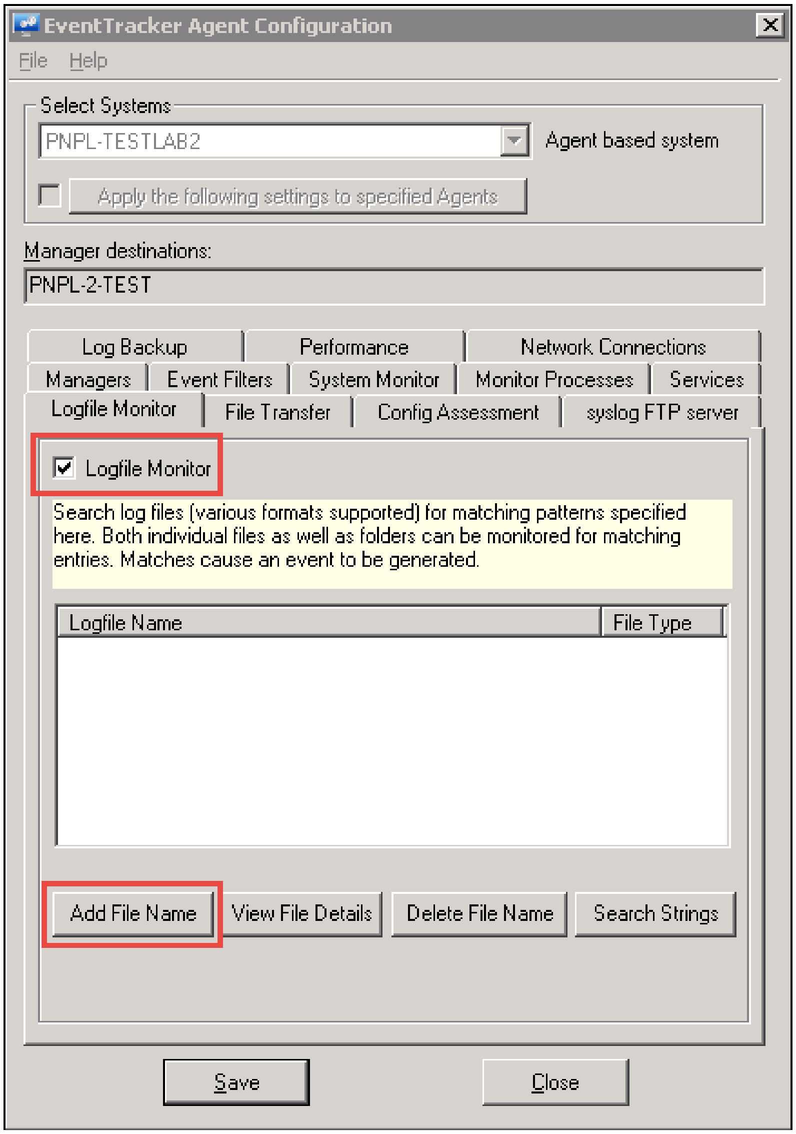
Table of Contents

Pre-requisite

- The user should have licensed **LogFile Monitor** feature.
- User should apply the Update: **ET82U16-018** and **ET82UA16-018.**

Process to be followed after applying the Update ET82U16-018 and ET82UA16-018

- Open the **EventTracker Control Panel**.
- Double-click on **EventTracker Agent Configuration**.
- Select **Logfile Monitor** tab and then check the **Logfile Monitor** option.



Select Systems: PNPL-TESTLAB2 — Agent based system

☐ Apply the following settings to specified Agents

Manager destinations: PNPL-2-TEST

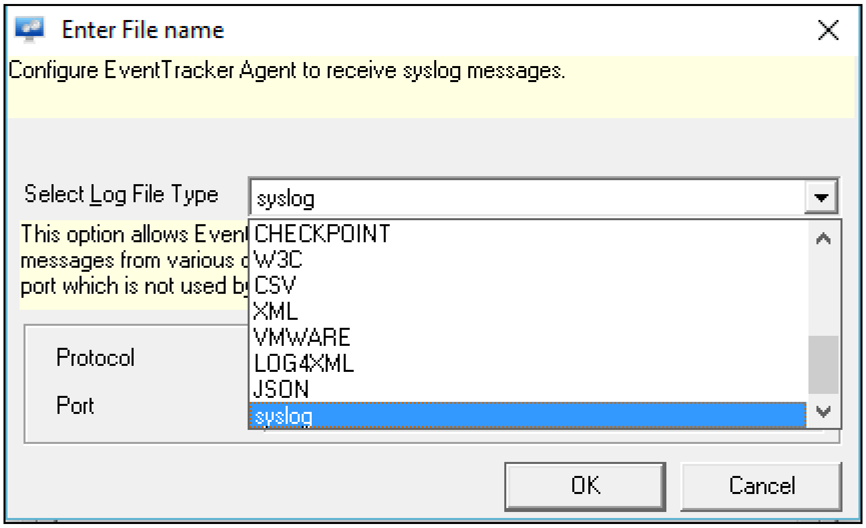
☑ Logfile Monitor

Search log files (various formats supported) for matching patterns specified here. Both individual files as well as folders can be monitored for matching entries. Matches cause an event to be generated.

Figure 1

- Select **Add File Name** option.
- Select Logfile type as '**syslog**".

This is shown in the figure below:



Enter File name

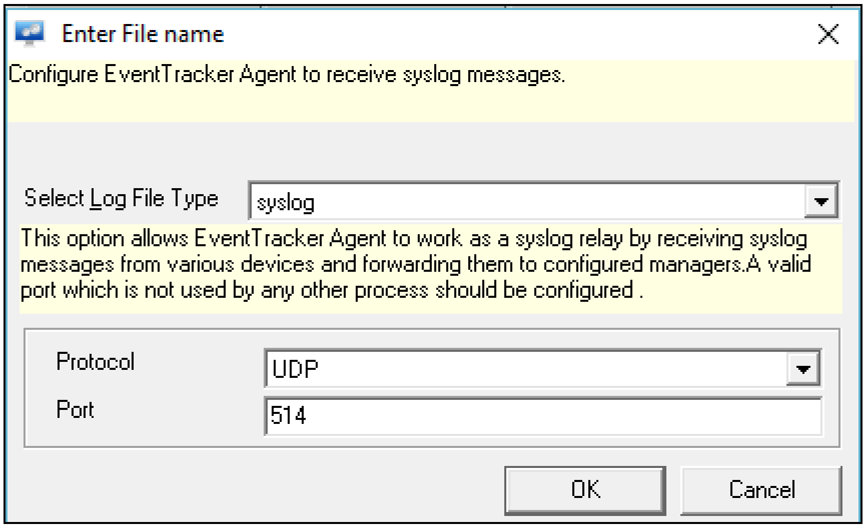
Configure EventTracker Agent to receive syslog messages.

Select Log File Type: syslog

This option allows Event
messages from various d
port which is not used b

Figure 2

- Select the **Protocol** from the dropdown list, i.e. **UDP/TCP.**
- Enter the valid **Port** number, which is not used by other processes and then click **OK**.



Enter File name

Configure EventTracker Agent to receive syslog messages.

Select Log File Type: syslog

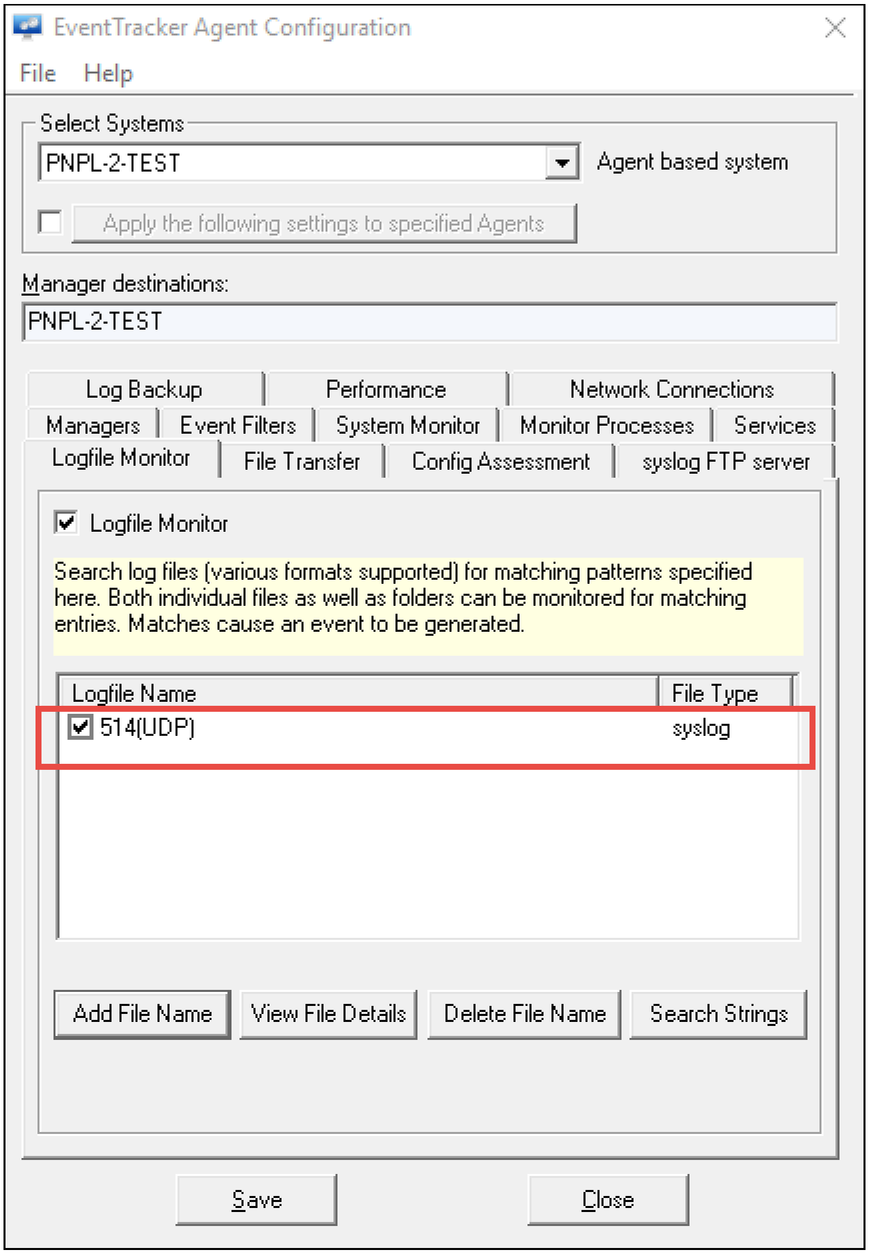
This option allows EventTracker Agent to work as a syslog relay by receiving syslog messages from various devices and forwarding them to configured managers.A valid port which is not used by any other process should be configured .

Protocol: UDP

Port: 514

Figure 3

- The port gets added in the **EventTracker Configuration** window.



Select Systems: PNPL-2-TEST

Manager destinations: PNPL-2-TEST

☑ Logfile Monitor

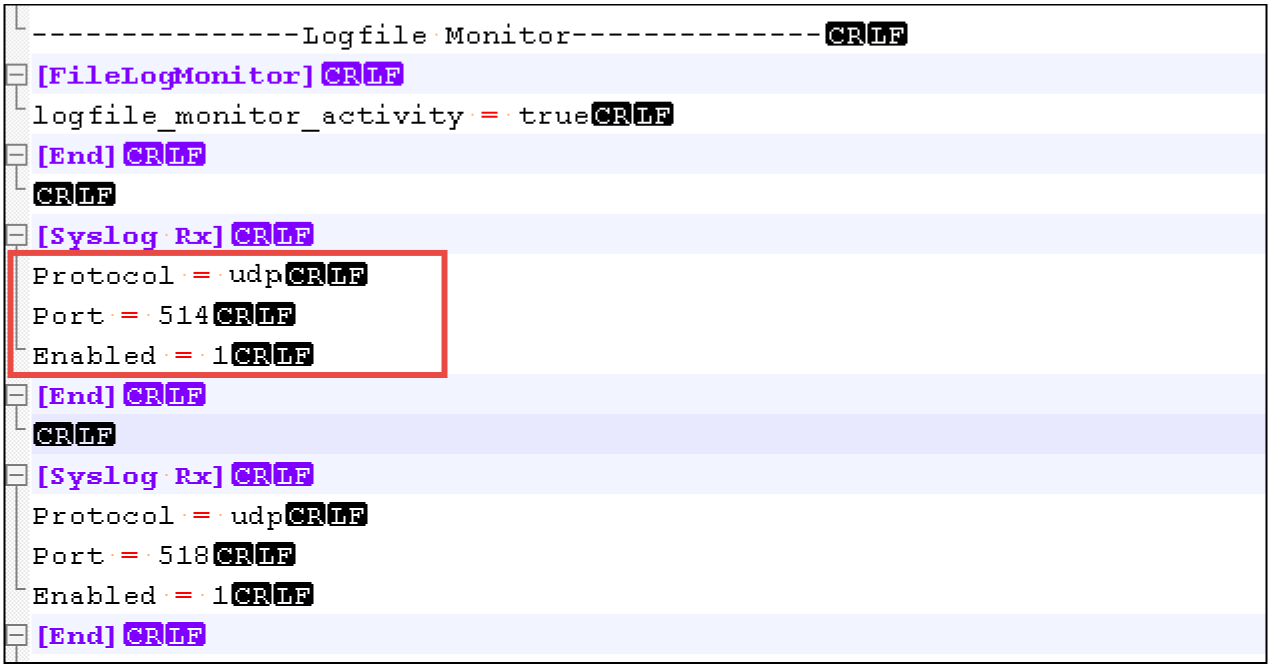
Search log files (various formats supported) for matching patterns specified here. Both individual files as well as folders can be monitored for matching entries. Matches cause an event to be generated.

Logfile Name	File Type
☑ 514(UDP)	syslog

Figure 4

- Click **Save** and then **Close** the window.

The **ETAconfig.ini** logfile detail includes '**Syslog_Rx"** which gets created under Logfile Monitor activity, with the added field names. This is shown below:



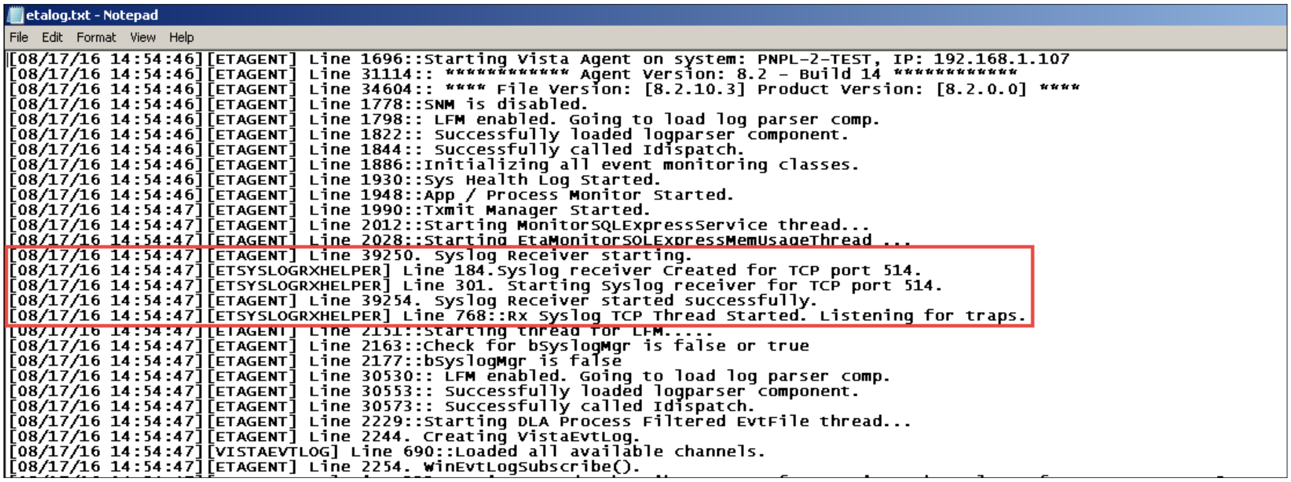
```
---------------Logfile Monitor--------------
[FileLogMonitor]
logfile_monitor_activity = true
[End]

[Syslog Rx]
Protocol = udp
Port = 514
Enabled = 1
[End]

[Syslog Rx]
Protocol = udp
Port = 518
Enabled = 1
[End]
```

Figure 5

EventTracker Agent will receive the syslog message on the configured port and will forward syslog message to the EventTracker Manager. The syslog message will be received on the port to which the agent is reporting.

To verify whether the configured port is listening and receiving the syslog messages in the Agent Machine

- Open the '**etalog.txt**" kept in the Install directory Agent folder.
- Verify whether the syslog receiver is getting created for the configured port, i.e. '**514**".

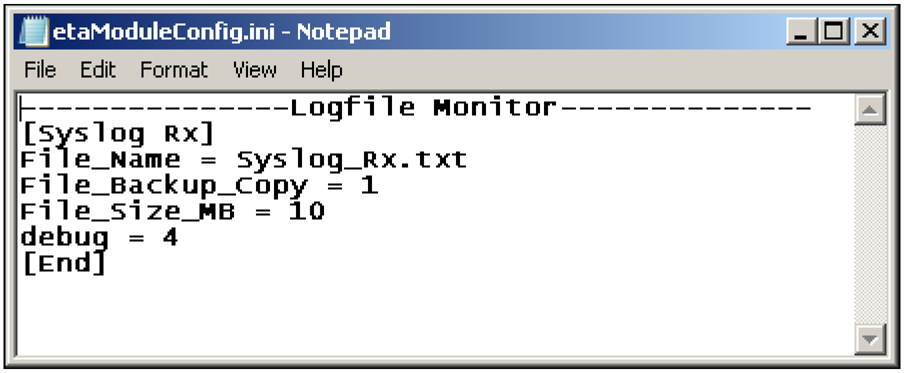


```
[08/17/16 14:54:46][ETAGENT] Line 1696::Starting Vista Agent on system: PNPL-2-TEST, IP: 192.168.1.107
[08/17/16 14:54:46][ETAGENT] Line 31114:: ************* Agent Version: 8.2 - Build 14 *************
[08/17/16 14:54:46][ETAGENT] Line 34604:: **** File Version: [8.2.10.3] Product Version: [8.2.0.0] ****
[08/17/16 14:54:46][ETAGENT] Line 1778::SNM is disabled.
[08/17/16 14:54:46][ETAGENT] Line 1798:: LFM enabled. Going to load log parser comp.
[08/17/16 14:54:46][ETAGENT] Line 1822:: Successfully loaded logparser component.
[08/17/16 14:54:46][ETAGENT] Line 1844:: Successfully called Idispatch.
[08/17/16 14:54:46][ETAGENT] Line 1886::Initializing all event monitoring classes.
[08/17/16 14:54:46][ETAGENT] Line 1930::Sys Health Log Started.
[08/17/16 14:54:46][ETAGENT] Line 1948::App / Process Monitor Started.
[08/17/16 14:54:47][ETAGENT] Line 1990::Txmit Manager Started.
[08/17/16 14:54:47][ETAGENT] Line 2012::Starting MonitorSQLExpressService thread...
[08/17/16 14:54:47][ETAGENT] Line 2028::Starting EtaMonitorSQLExpressMemUsageThread ...
[08/17/16 14:54:47][ETAGENT] Line 39250. Syslog Receiver starting.
[08/17/16 14:54:47][ETSYSLOGRXHELPER] Line 184.Syslog receiver Created for TCP port 514.
[08/17/16 14:54:47][ETSYSLOGRXHELPER] Line 301. Starting Syslog receiver for TCP port 514.
[08/17/16 14:54:47][ETAGENT] Line 39254. Syslog Receiver started successfully.
[08/17/16 14:54:47][ETSYSLOGRXHELPER] Line 768::Rx Syslog TCP Thread Started. Listening for traps.
[08/17/16 14:54:47][ETAGENT] Line 2151::Starting thread for LFM.....
[08/17/16 14:54:47][ETAGENT] Line 2163::Check for bSyslogMgr is false or true
[08/17/16 14:54:47][ETAGENT] Line 2177::bSyslogMgr is false
[08/17/16 14:54:47][ETAGENT] Line 30530:: LFM enabled. Going to load log parser comp.
[08/17/16 14:54:47][ETAGENT] Line 30553:: Successfully loaded logparser component.
[08/17/16 14:54:47][ETAGENT] Line 30573:: Successfully called Idispatch.
[08/17/16 14:54:47][ETAGENT] Line 2229::Starting DLA Process Filtered EvtFile thread...
[08/17/16 14:54:47][ETAGENT] Line 2244. Creating VistaEvtLog.
[08/17/16 14:54:47][VISTAEVTLOG] Line 690::Loaded all available channels.
[08/17/16 14:54:47][ETAGENT] Line 2254. WinEvtLogSubscribe().
```

Figure 6

For addition logging,

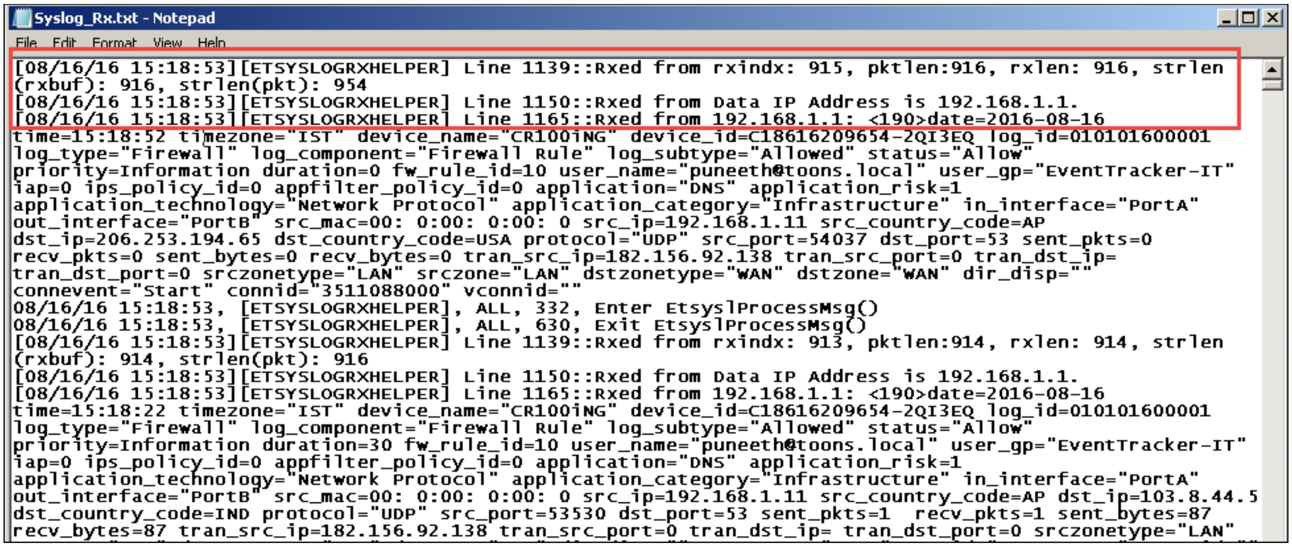
1. Create a file named ‘**etamoduleconfig.ini**” in the format shown below:



```
---------------Logfile Monitor---------------
[Syslog Rx]
File_Name = Syslog_Rx.txt
File_Backup_Copy = 1
File_Size_MB = 10
debug = 4
[End]
```

Figure 7

2. Copy the ‘**etamoduleconfig.ini**” file in the Install directory Agent folder and then restart the agent service.
3. The ‘**Syslog_Rx.txt**” log file gets created, which will have the details of the syslog messages received. Refer to the figure shown below:

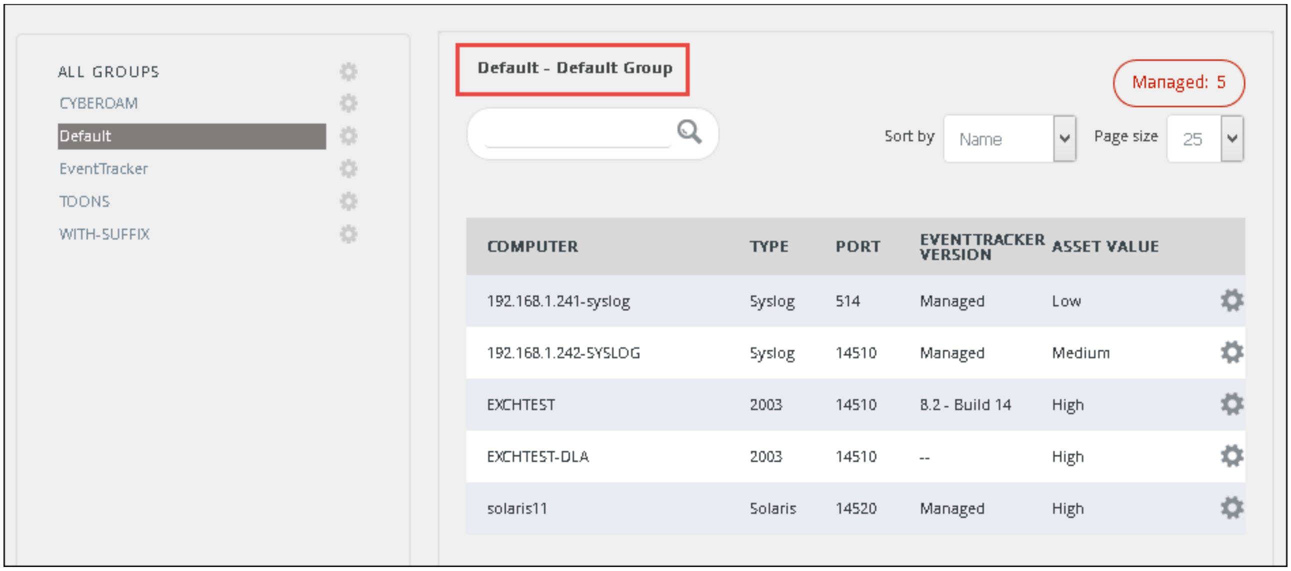


```
[08/16/16 15:18:53][ETSYSLOGRXHELPER] Line 1139::Rxed from rxindx: 915, pktlen:916, rxlen: 916, strlen
(rxbuf): 916, strlen(pkt): 954
[08/16/16 15:18:53][ETSYSLOGRXHELPER] Line 1150::Rxed from Data IP Address is 192.168.1.1.
[08/16/16 15:18:53][ETSYSLOGRXHELPER] Line 1165::Rxed from 192.168.1.1: <190>date=2016-08-16
time=15:18:52 timezone="IST" device_name="CR100iNG" device_id=C18616209654-2QI3EQ log_id=010101600001
log_type="Firewall" log_component="Firewall Rule" log_subtype="Allowed" status="Allow"
priority=Information duration=0 fw_rule_id=10 user_name="puneeth@toons.local" user_gp="EventTracker-IT"
iap=0 ips_policy_id=0 appfilter_policy_id=0 application="DNS" application_risk=1
application_technology="Network Protocol" application_category="Infrastructure" in_interface="PortA"
out_interface="PortB" src_mac=00: 0:00: 0:00: 0 src_ip=192.168.1.11 src_country_code=AP
dst_ip=206.253.194.65 dst_country_code=USA protocol="UDP" src_port=54037 dst_port=53 sent_pkts=0
recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip=182.156.92.138 tran_src_port=0 tran_dst_ip=
tran_dst_port=0 srczonetype="LAN" srczone="LAN" dstzonetype="WAN" dstzone="WAN" dir_disp=""
connevent="Start" connid="3511088000" vconnid=""
08/16/16 15:18:53, [ETSYSLOGRXHELPER], ALL, 332, Enter EtsyslProcessMsg()
08/16/16 15:18:53, [ETSYSLOGRXHELPER], ALL, 630, Exit EtsyslProcessMsg()
[08/16/16 15:18:53][ETSYSLOGRXHELPER] Line 1139::Rxed from rxindx: 913, pktlen:914, rxlen: 914, strlen
(rxbuf): 914, strlen(pkt): 916
[08/16/16 15:18:53][ETSYSLOGRXHELPER] Line 1150::Rxed from Data IP Address is 192.168.1.1.
[08/16/16 15:18:53][ETSYSLOGRXHELPER] Line 1165::Rxed from 192.168.1.1: <190>date=2016-08-16
time=15:18:22 timezone="IST" device_name="CR100iNG" device_id=C18616209654-2QI3EQ log_id=010101600001
log_type="Firewall" log_component="Firewall Rule" log_subtype="Allowed" status="Allow"
priority=Information duration=30 fw_rule_id=10 user_name="puneeth@toons.local" user_gp="EventTracker-IT"
iap=0 ips_policy_id=0 appfilter_policy_id=0 application="DNS" application_risk=1
application_technology="Network Protocol" application_category="Infrastructure" in_interface="PortA"
out_interface="PortB" src_mac=00: 0:00: 0:00: 0 src_ip=192.168.1.11 src_country_code=AP dst_ip=103.8.44.5
dst_country_code=IND protocol="UDP" src_port=53530 dst_port=53 sent_pkts=1  recv_pkts=1 sent_bytes=87
recv_bytes=87 tran_src_ip=182.156.92.138 tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczonetype="LAN"
```

Figure 8

To verify whether the syslog messages are being received in the EventTracker Manager Console

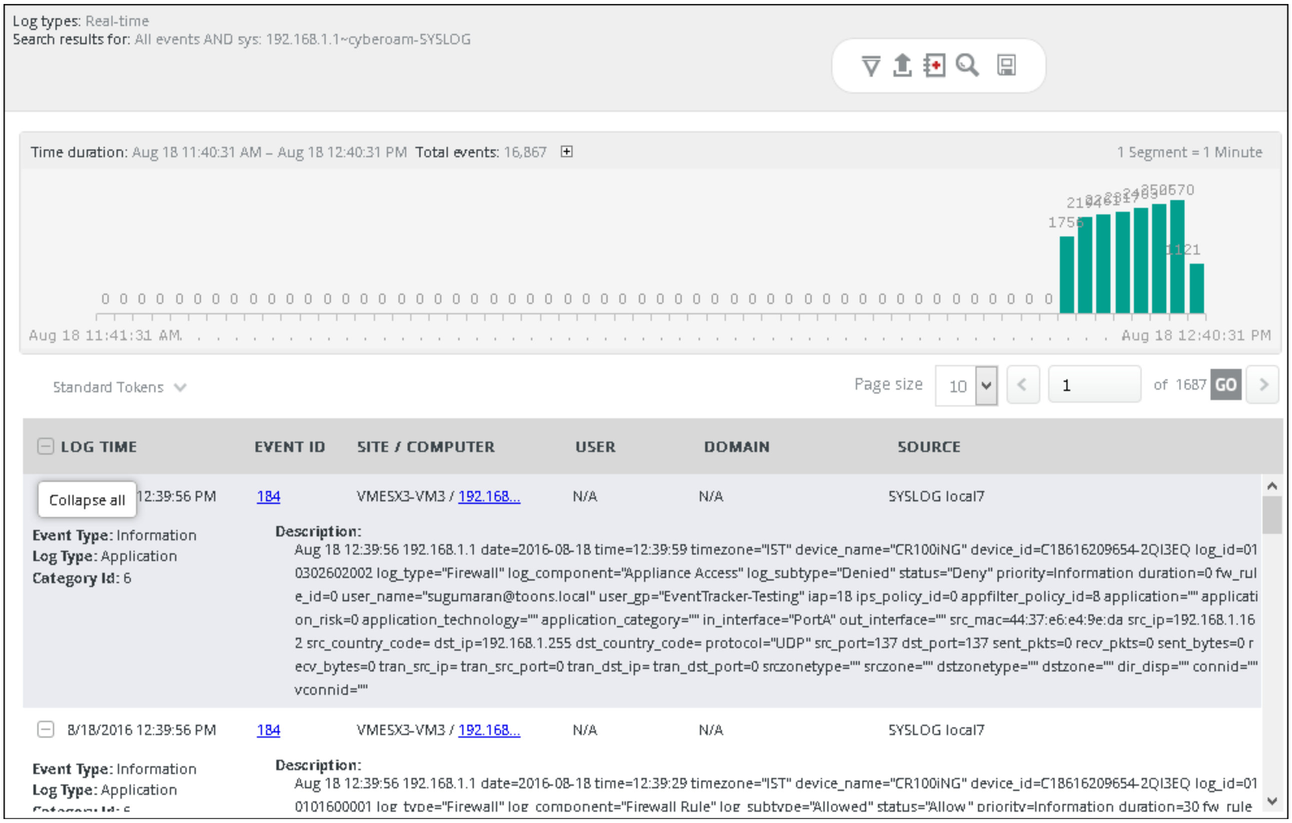
- Open **EventTracker web-> Admin-> System Manager**.
  The systems will be listed under the Default Group.



COMPUTER	TYPE	PORT	EVENTTRACKER VERSION	ASSET VALUE
192.168.1.241-syslog	Syslog	514	Managed	Low
192.168.1.242-SYSLOG	Syslog	14510	Managed	Medium
EXCHTEST	2003	14510	8.2 - Build 14	High
EXCHTEST-DLA	2003	14510	--	High
solaris11	Solaris	14520	Managed	High

Figure 9

- The user can also perform a log search and get the results as shown below:



Log types: Real-time
Search results for: All events AND sys: 192.168.1.1~cyberoam-SYSLOG

Time duration: Aug 18 11:40:31 AM – Aug 18 12:40:31 PM Total events: 16,867

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
12:39:56 PM	184	VMESX3-VM3 / 192.168...	N/A	N/A	SYSLOG local7

Event Type: Information
Log Type: Application
Category Id: 6

Description:

```
Aug 18 12:39:56 192.168.1.1 date=2016-08-18 time=12:39:59 timezone="IST" device_name="CR100iNG" device_id=C18616209654-2QI3EQ log_id=01
0302602002 log_type="Firewall" log_component="Appliance Access" log_subtype="Denied" status="Deny" priority=Information duration=0 fw_rul
e_id=0 user_name="sugumaran@toons.local" user_gp="EventTracker-Testing" iap=18 ips_policy_id=0 appfilter_policy_id=8 application="" applicati
on_risk=0 application_technology="" application_category="" in_interface="PortA" out_interface="" src_mac=44:37:e6:e4:9e:da src_ip=192.168.1.16
2 src_country_code= dst_ip=192.168.1.255 dst_country_code= protocol="UDP" src_port=137 dst_port=137 sent_pkts=0 recv_pkts=0 sent_bytes=0 r
ecv_bytes=0 tran_src_ip= tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczonetype="" srczone="" dstzonetype="" dstzone="" dir_disp="" connid=""
vconnid=""
```

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
8/18/2016 12:39:56 PM	184	VMESX3-VM3 / 192.168...	N/A	N/A	SYSLOG local7

Event Type: Information
Log Type: Application

Description:

```
Aug 18 12:39:56 192.168.1.1 date=2016-08-18 time=12:39:29 timezone="IST" device_name="CR100iNG" device_id=C18616209654-2QI3EQ log_id=01
0101600001 log_type="Firewall" log_component="Firewall Rule" log_subtype="Allowed" status="Allow" priority=Information duration=30 fw_rule
```

Figure 10