Netsurion | EventTracker®

Device Name and Device Type extraction and assignment

EventTracker v9.3

Publication Date: September 3, 2020

Abstract

This document provides details about enhancements related to syslog receiver in terms of extracting the device id/name from the event descirption and assigning the device type.

Audience

This guide is intended for use by all the EventTracker users responsible for investigating and managing network security. This guide assumes that you have EventTracker access and understanding of the networking technology.

Table of Contents

1. Device ID/Name extraction

EventTracker supports regular expressions for extracting the device ID/Name from syslog device.

1.1 Device ID/Name extraction using single/multiple regular expressions per VCP

An enhancement is provided for extracting the device id/name from syslog device messages. It can extract multiple device ids or device names which are reporting to the same VCP by using single/multiple regular expressions.

1. Login to the EventTracker web console. Navigate to **Admin ->Manager**.
2. Click on **syslog/Virtual Collection Point** tab. You can view the gear icon for each VCP port.

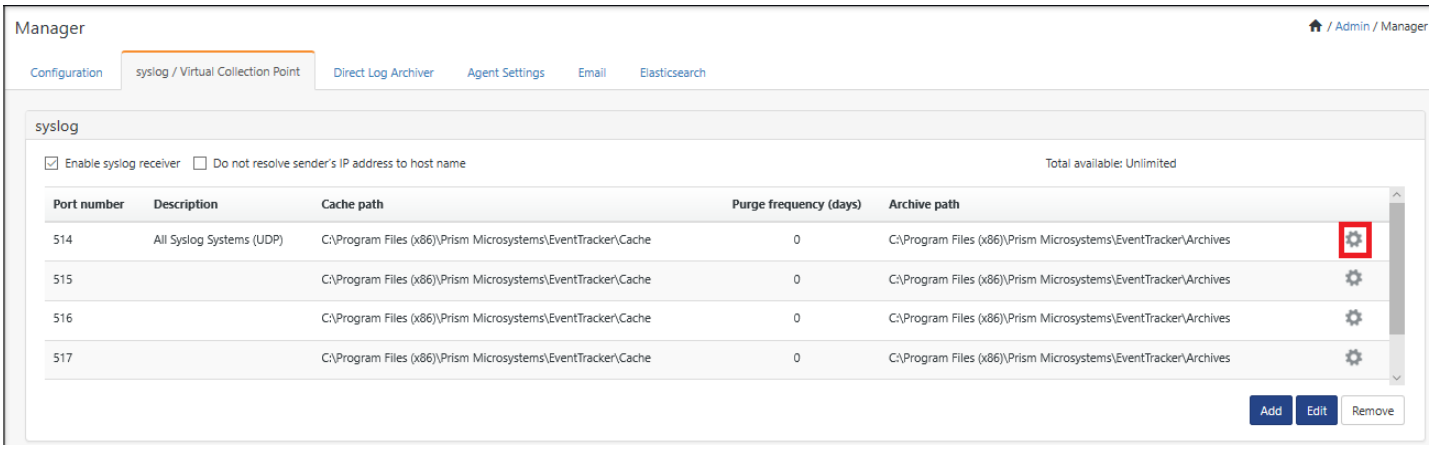

Figure 1

3. To extract device id/name, click the **gear** icon.
4. Click **Extract device id.** '**Extract device Id from syslog devices'** dialog box opens.

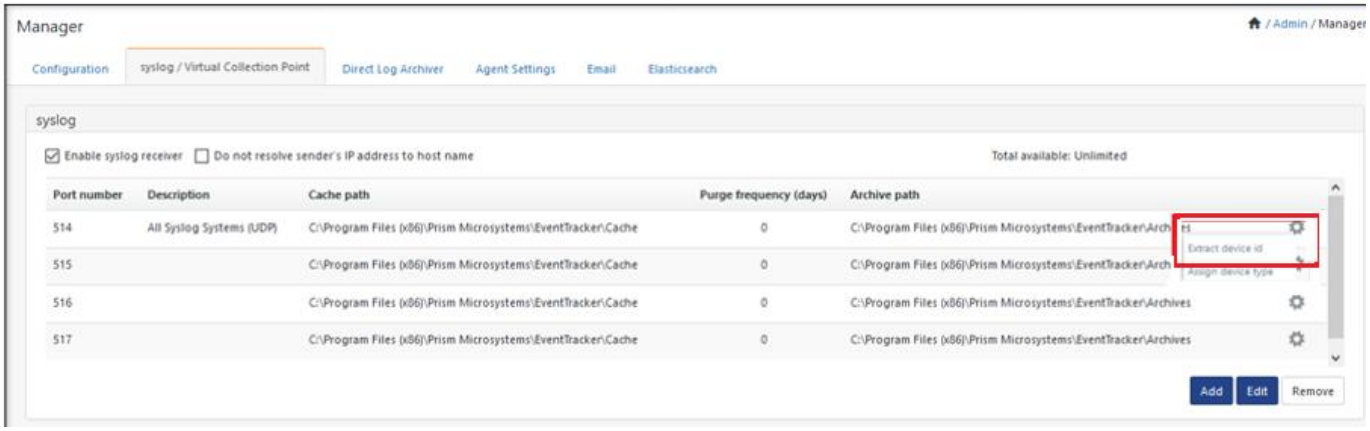

Figure 2

5. Provide the **Regular expression** and a **Token name** and check the **Active** option.

   Note: The token name must be same as Named Capture Group.

   Example 1: For this regular expression,

   .*devid=(?P<Computer>[\w\-]+).*

   The token name is “Computer”.

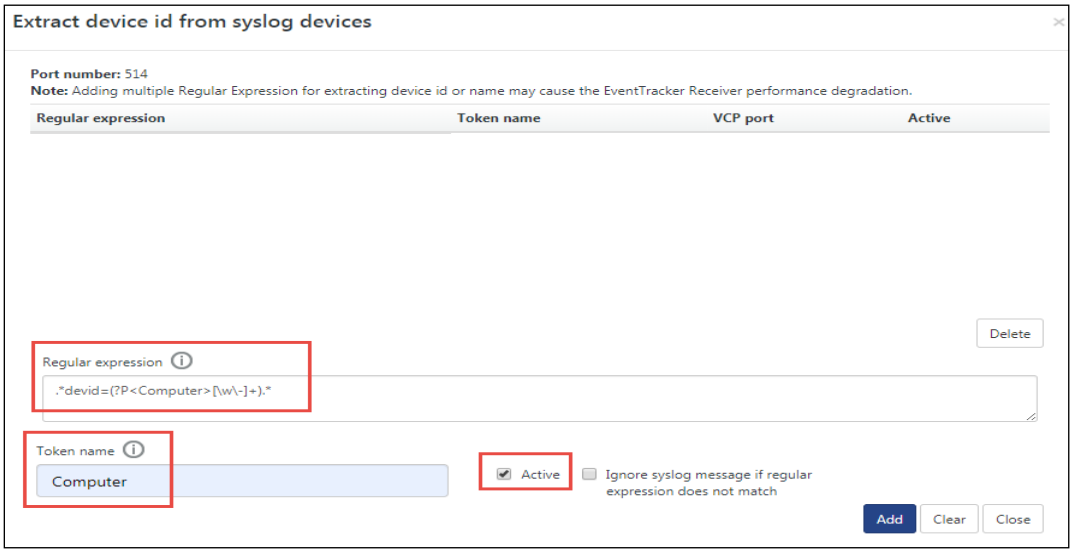

Figure 3

Example 2: For this regular expression,

.*dhost=(?P<computer>[^\s]+).*?cs\d+=(?P<MSPName>[\w\s]+)\scs\d+Label=MSPName.*?cs\d+=(?P<Tenant>.*?)cs\d+Label=TenantName.*

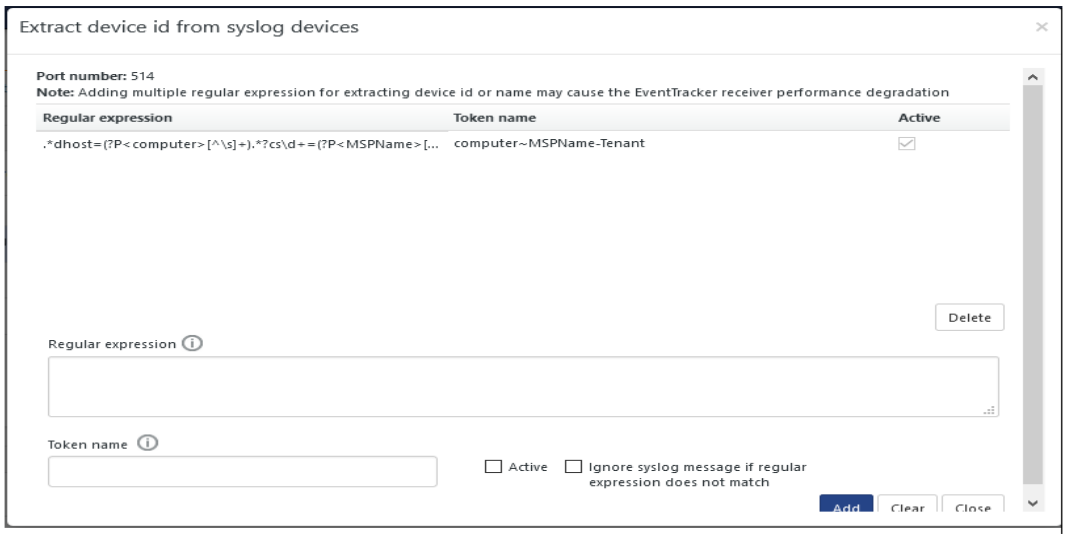

Figure 4

The token name is “computer~MSPName-Tenant.

Note: The computer name and group name should be separated by ~ (tilda) and multiple tokens in computer/group name should be separated by - (hyphen) characters.

Example: “Computer~MspName-TenantName"

6. Click **Add.** Regular expression and the token name are added as shown in below figure.

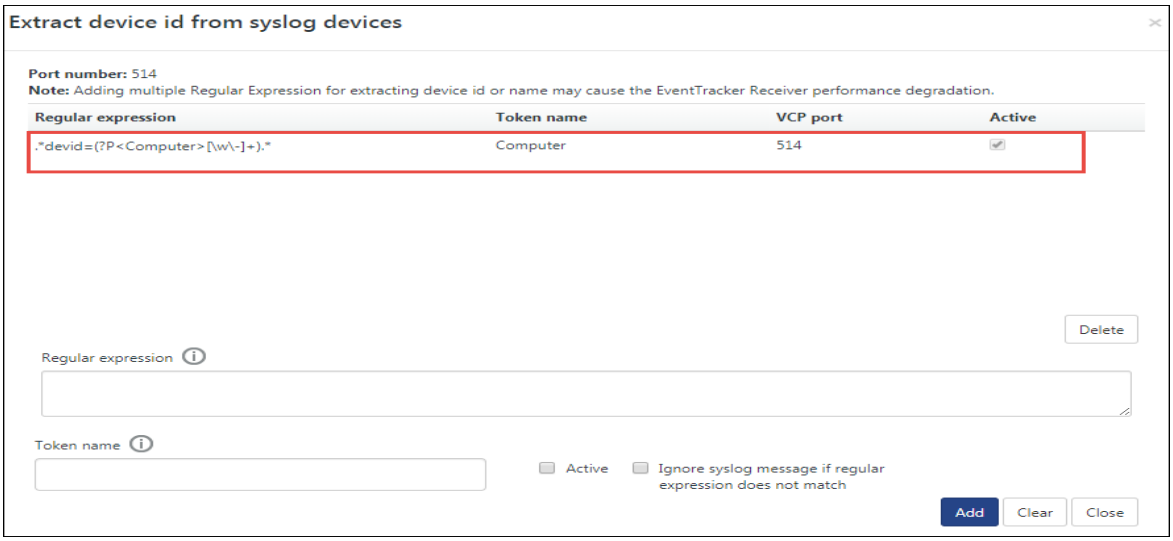

Figure 5

7. Click **Save** in the manager page.

1.2 Configuring multiple regular expressions

You can configure multiple regular expressions for a single/multiple VCP ports.

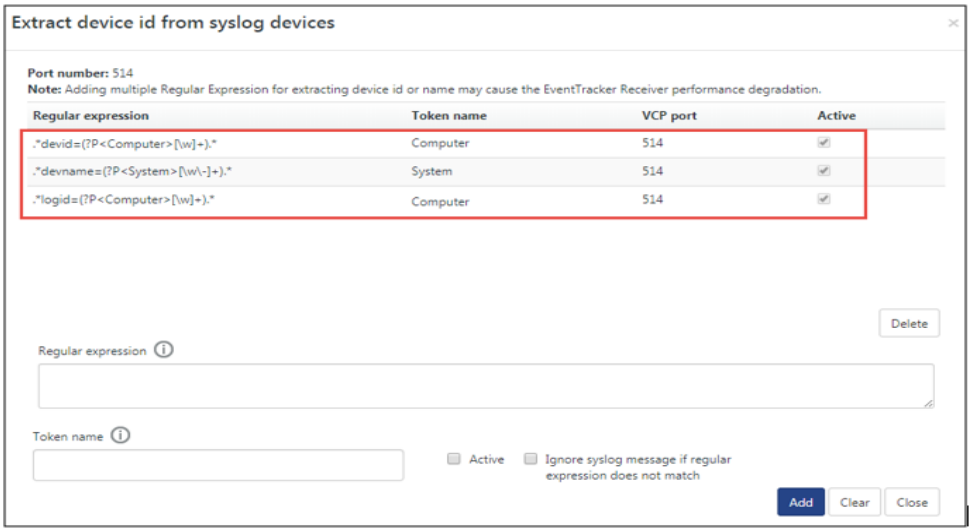

Figure 6

1.3 Ignoring syslog message if regular expression does not match

In case the device id could not be extracted from multiple regular expressions, you can select the checkbox "**Ignore syslog message if regular expression does not match**", which will ignore the events. You will not see the device id/name entry in the "System Manager' module.

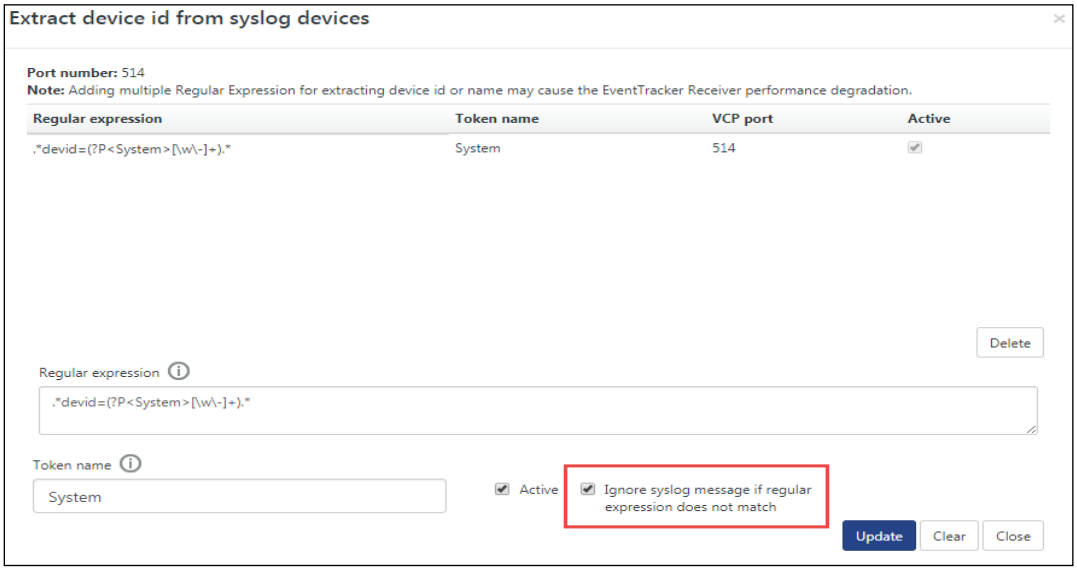

Figure 7

NOTE: Enabling "**Ignore syslog message if regular expression does not match"** will consider all the regular expressions configured for that given VCP port.

2. Device type extraction and assignment

The EventTracker application will extract the device type as per the regular expression provided and will assign it to the extracted system or reporting system.

2.1 Device type extraction/assignment using single/multiple regular expressions per VCP

An enhancement is provided for device type assignment to the extracted device names or reporting system. It can extract the device type as per the regular expression provided and will assign it to the extracted system or reporting system which are reporting to the VCP port.

1. Login to the EventTracker web console. Navigate to **Admin -> Manager**.
2. Click **syslog/Virtual Collection Point** tab. You can view the gear icon for each VCP port.

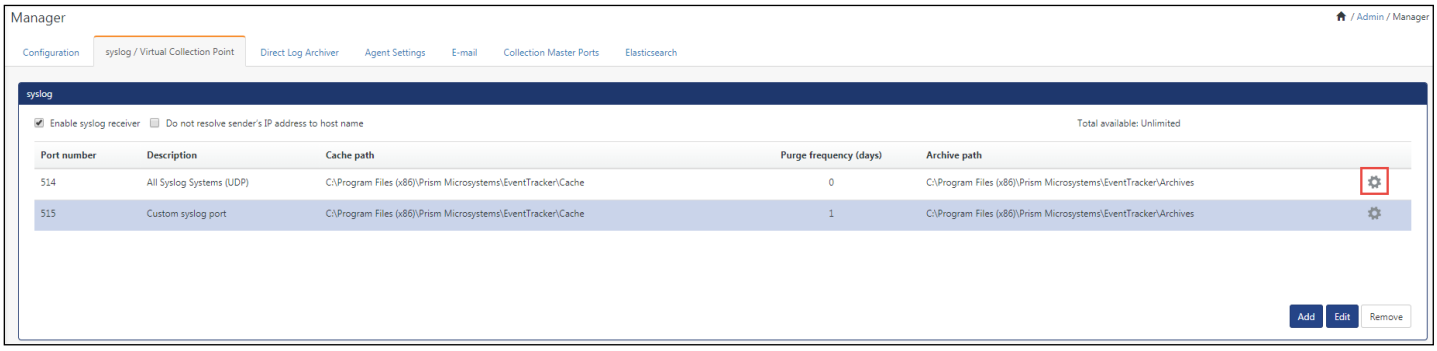

Figure 8

3. Click **Assign device type. 'Assign device type for syslog devices'** dialog box opens.

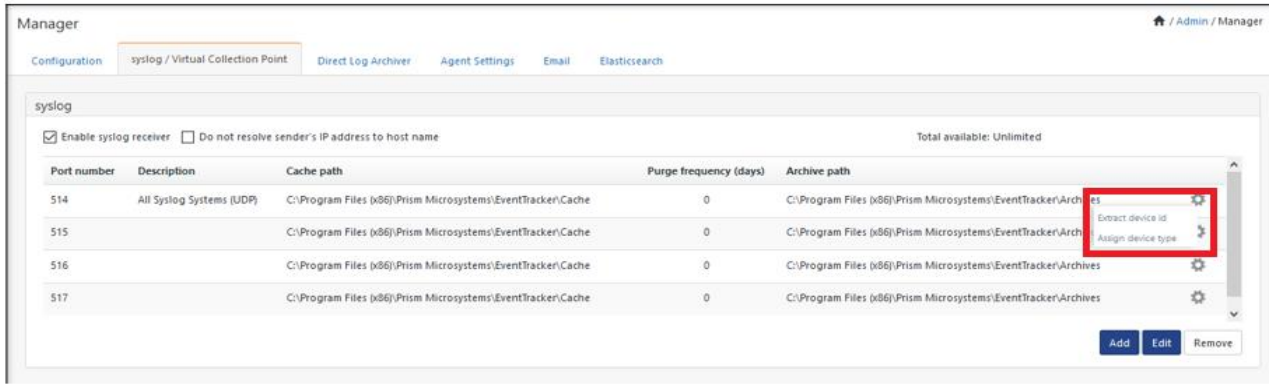

Figure 9

4. Provide the **regular expression** and select the **device type** from the drop-down box, check the **Active** option.

Example:.*dhost=(?P<computer>[^\s]+).*?cs\d+=(?P<MSPName>[\w\s]+)\scs\d+Label=MSPName.*?cs\d+=(?P<Tenant>.*?)cs\d+Label=TenantName.*

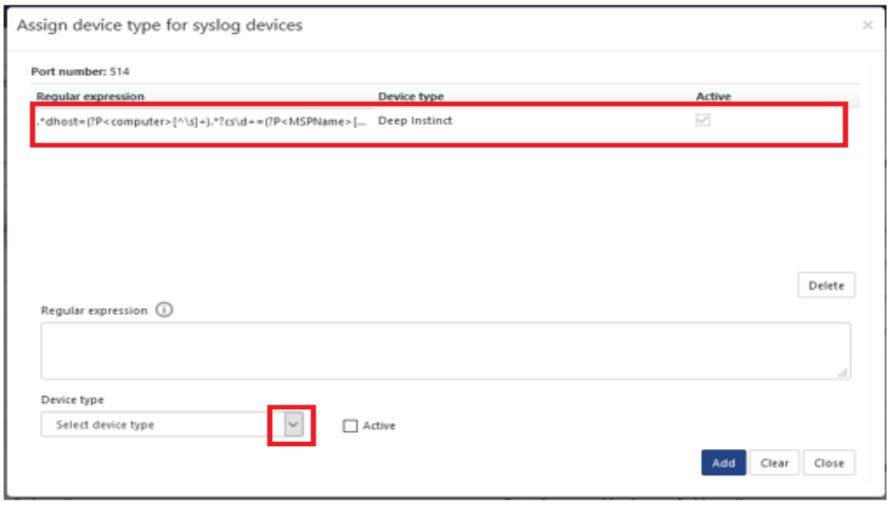

Figure 10

5. Click **Add.** Regular expression and the token name are added as shown in above figure.
6. Click **Save** in the manager page.

Once the device id and device types are extracted, they will be displayed in the system manager module.

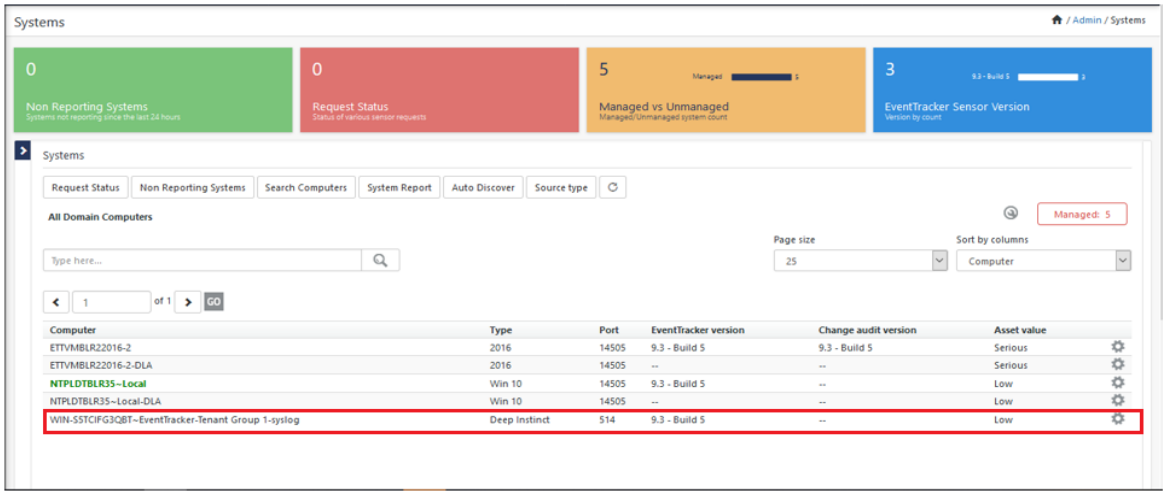

Figure 11