Netsurion™ | EventTracker

Enhancements in syslog Configuration, E-mail Incidents & syslog over TLS

Detailed Document

Publication Date: April 10, 2019

Abstract

This document provides enhancements related to syslog Configuration, E-mail Incidents and sylog over TLS in EventTracker v9.1.

Audience

EventTracker v9.1 user(s) who wish to configure syslog, use the E-mail Incident option and configure syslog over TLS in EventTracker v9.1.

Table of Contents

Support for Multiple Device Extraction

Allowing multiple Device ID/Name extraction using multiple regular expressions per VCP

An enhancement has been provided for extracting the device ID from syslog device while it is relaying. It will extract multiple device ids or device names that are reporting to the same Virtual Collection Point (VCP) by using multiple regular expressions.

- Login to the EventTracker web console. Navigate to **Admin** and then Manager.
- Click on **syslog/Virtual Collection Point** tab.
- Here, you can view the gear icon for each VCP port.

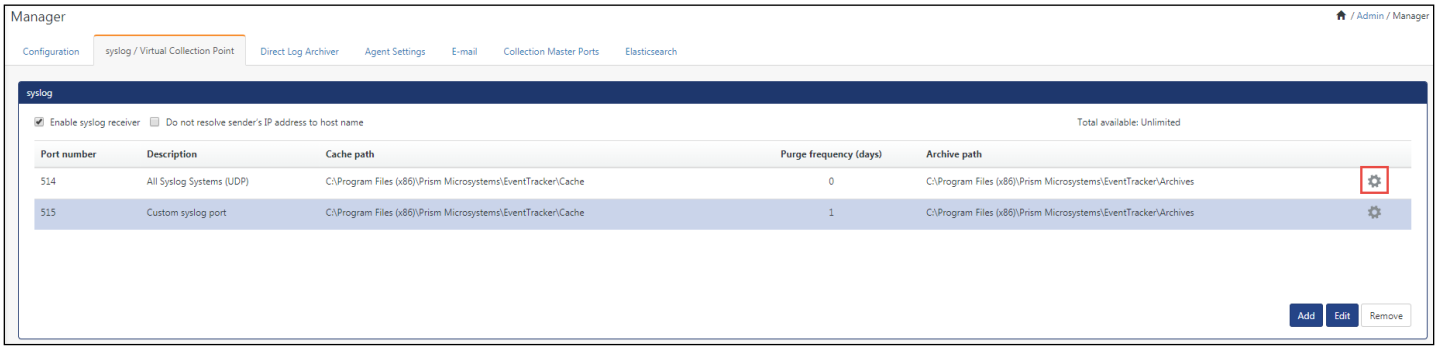


Figure 1

- To extract device id/name, provide the regular expression by clicking the gear icon.
- Provide the regular expression and a token name and check the Active option.

Please note that the token name must be same as Named Capture Group.

For example: For this regular expression,

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

The token name is “Computer”.

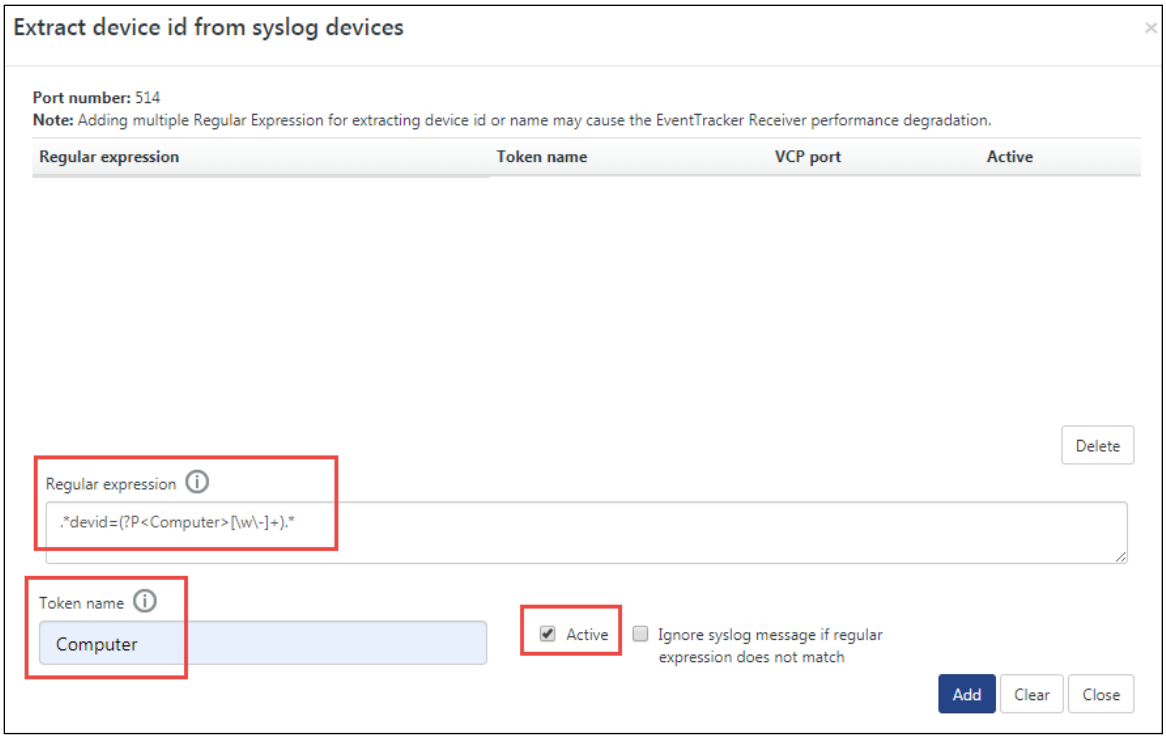


Figure 2

Once you click Add, it gets added. Click the Close button and Save it in Manager Configuration page.

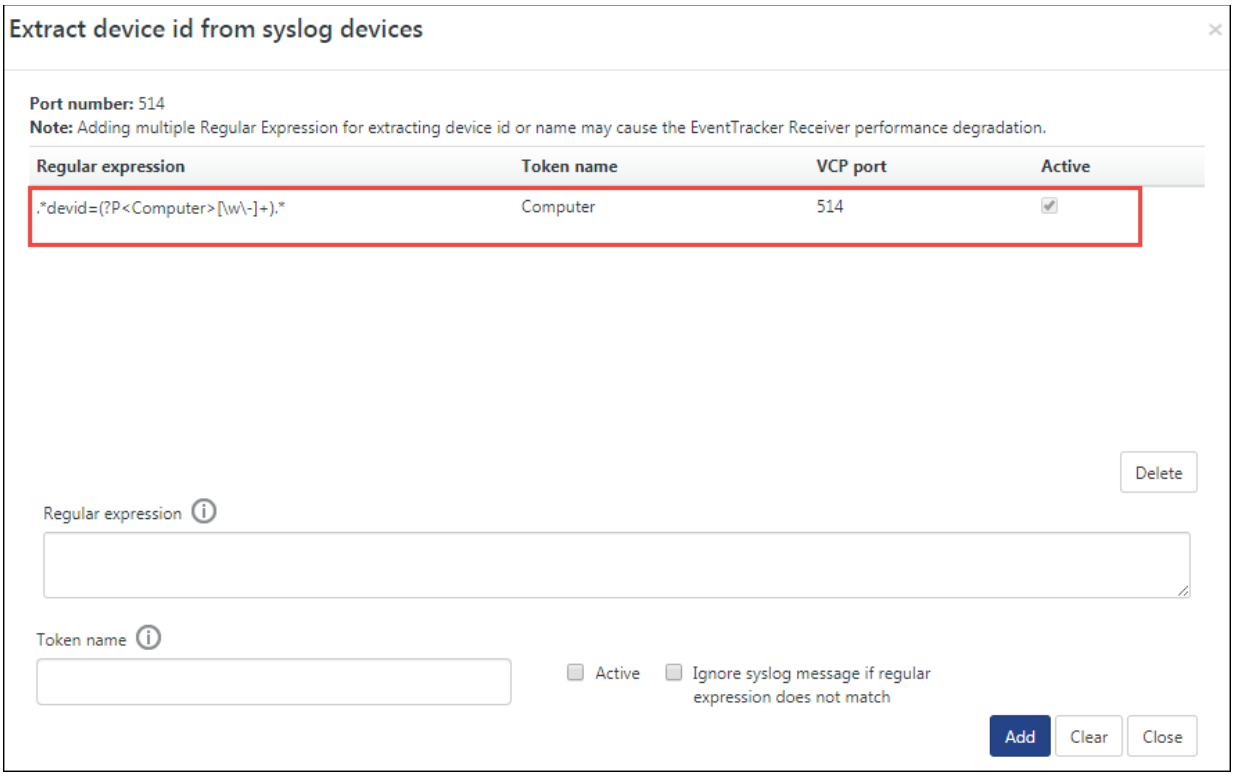


Figure 3

Once the syslog device starts forwarding the data, the respective device id/name will be extracted based on the provided regular expression.

In a similar way, you can configure multiple regular expressions for a single/multiple VCP ports.

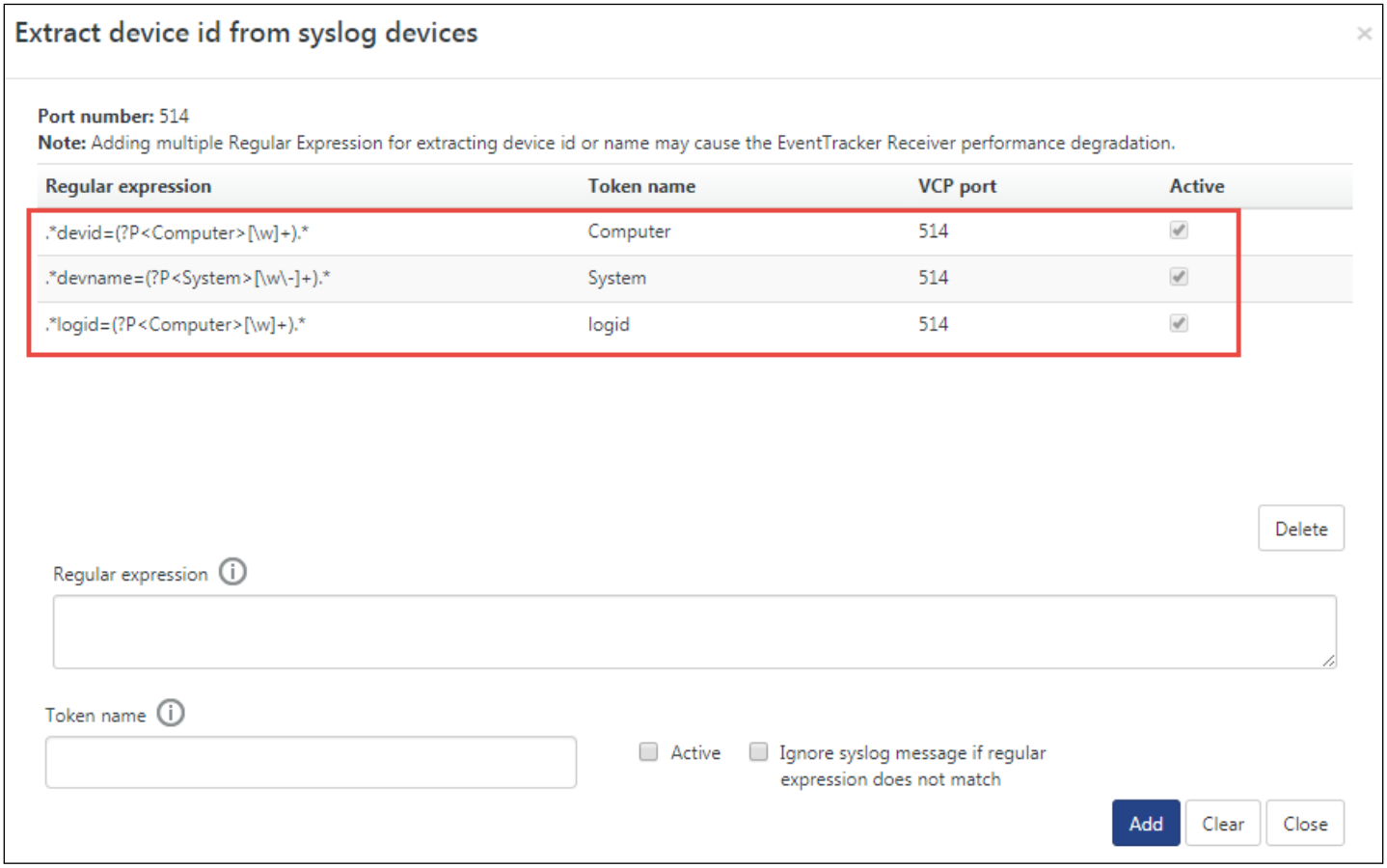


Figure 4

Once the device id is extracted, you can see it in the following format.

For example**: FG1K5D3I1480221-syslog**

Ignore syslog Message if Regular Expression does not match

1. **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 also not see the device id/name entry in the "System' module.

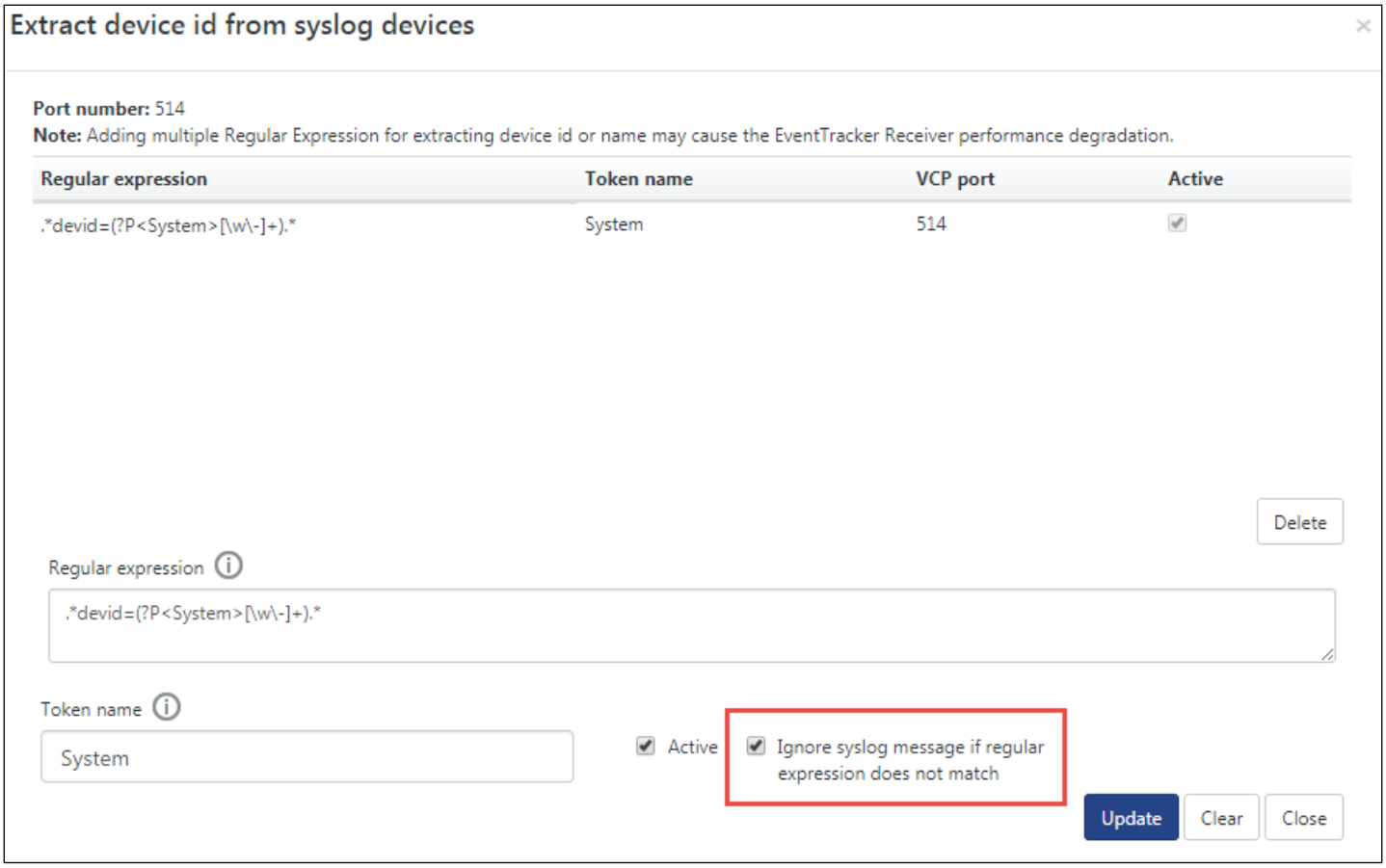


Figure 5

NOTE: Please note that if you enable "**Ignore syslog message if regular expression does not match",** it will consider for all the regular Expression configured for that particular VCP port.

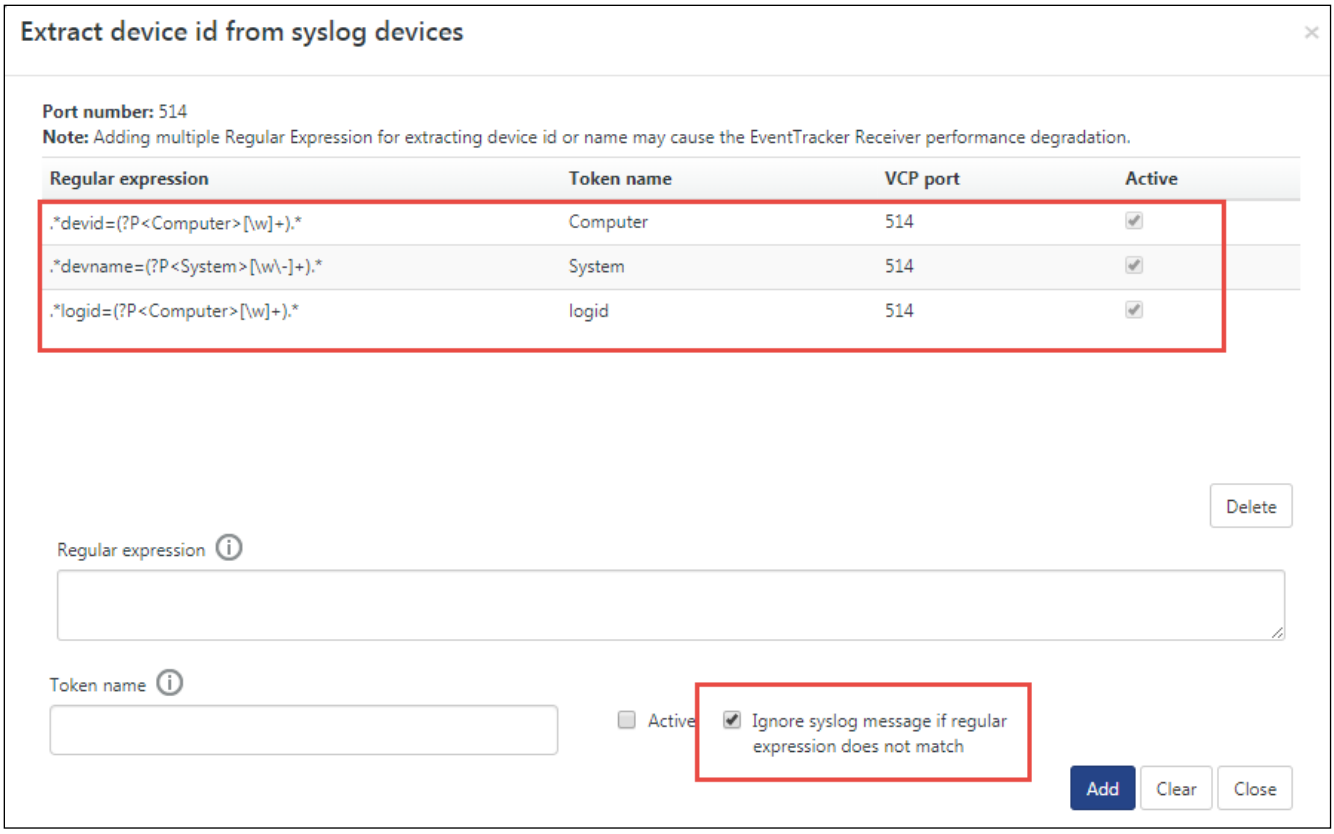


Figure 6

Not to Resolve the Sender's IP Address to Hostname

1. If the regular expression fails to extract the device id, then if you do not wish to resolve the sender's IP address to host name, enable the option "**Do not resolve sender's IP address to host name**". By disabling the same option, the IP address will get resolved to host name. You will see the IP Address or Hostname entry in the "System' module depending upon enabling or disabling this option.

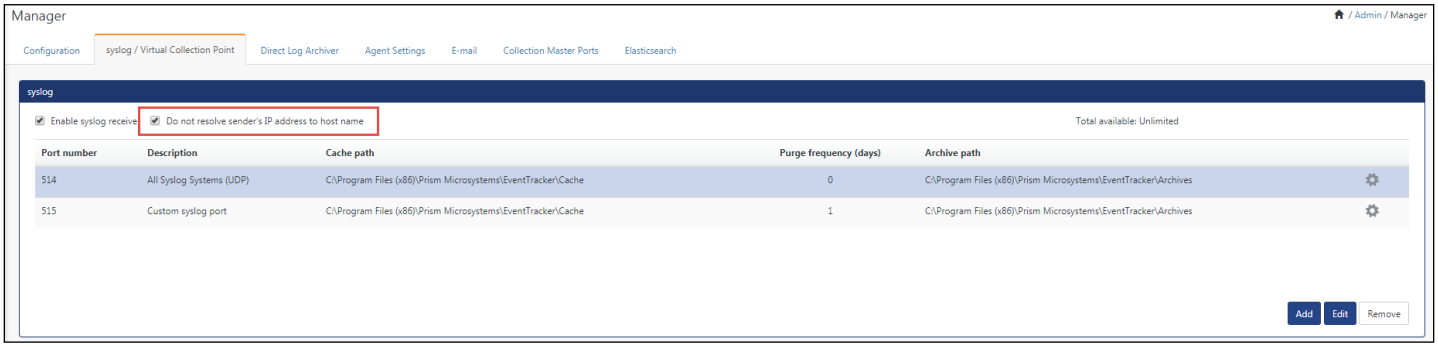


Figure 7

2. Even at the VCP level, you can resolve the Sender's IP Address to hostname. To do this, select the syslog port and click Edit. By default, it will be "**Use Global**" option under Resolve Hostname.

- When you select the "**Use Global**" option, it will consider the globally enabled or disabled "**Do not resolve sender's IP address to host name**" option.

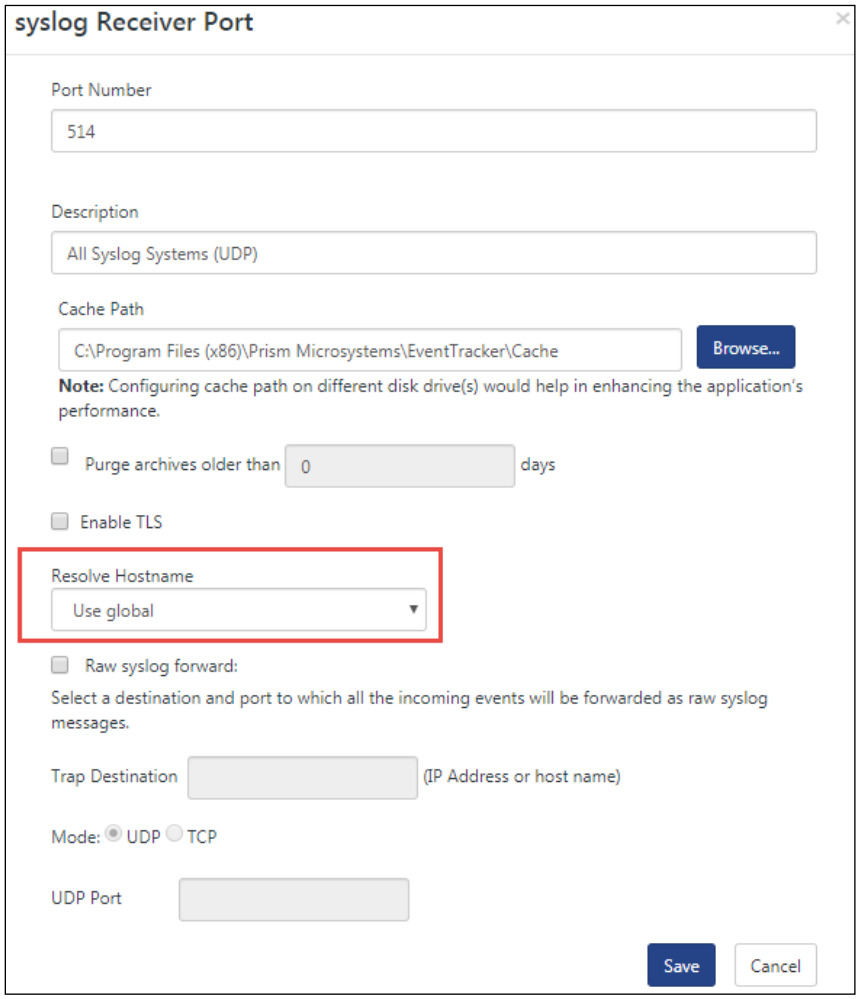


Figure 8

- If you select "**Resolve IP to Hostname**", it will consider resolving the sender IP to Hostname.

NOTE: If the "**Resolve IP to Hostname",** is selected at the VCP level and globally you have also selected "**Do not resolve sender's IP address to host name**", it will consider the option selected at the VCP level.

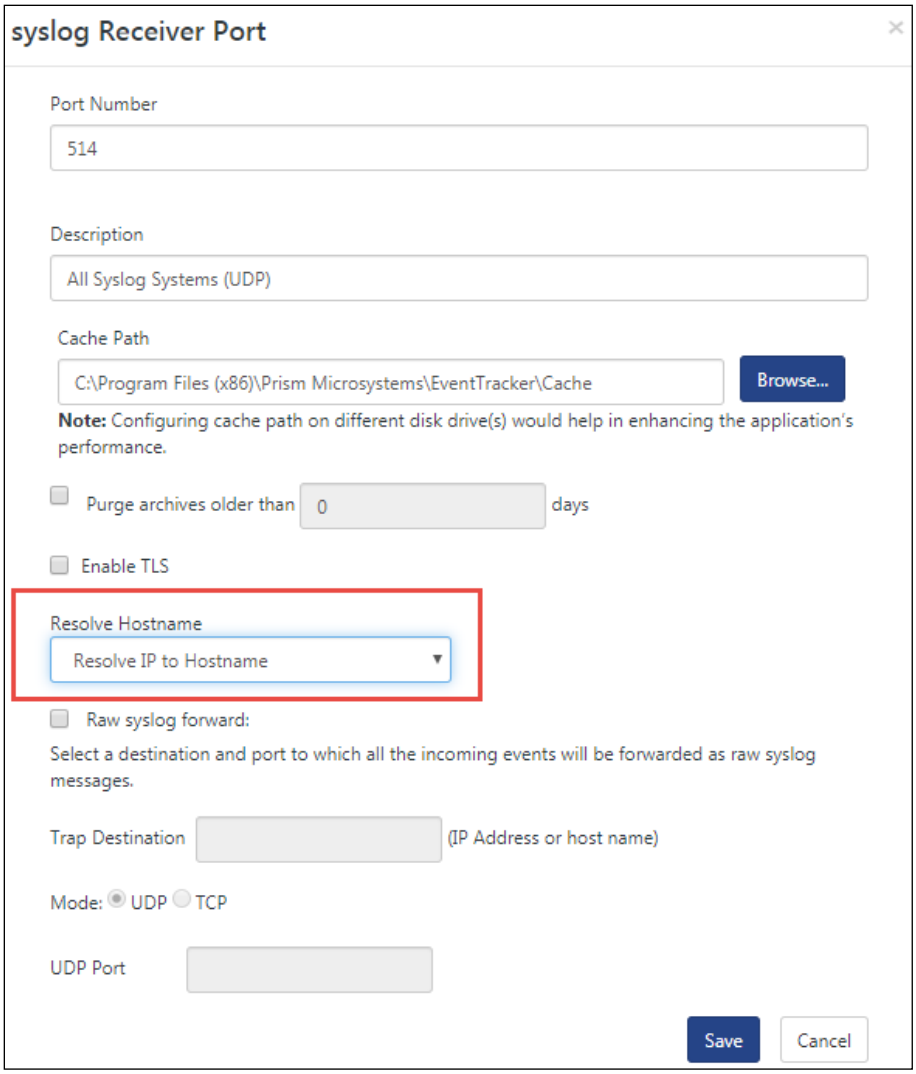


Figure 9

- If you select "**Do not Resolve IP to Hostname**", it will not resolve the sender IP to Hostname. It will remain as an IP address only.

  NOTE: If the "**Do not Resolve IP to Hostname",** is selected at the VCP level and globally you have also selected "**Do not resolve sender's IP address to host name**", it will consider the option selected at the VCP level.

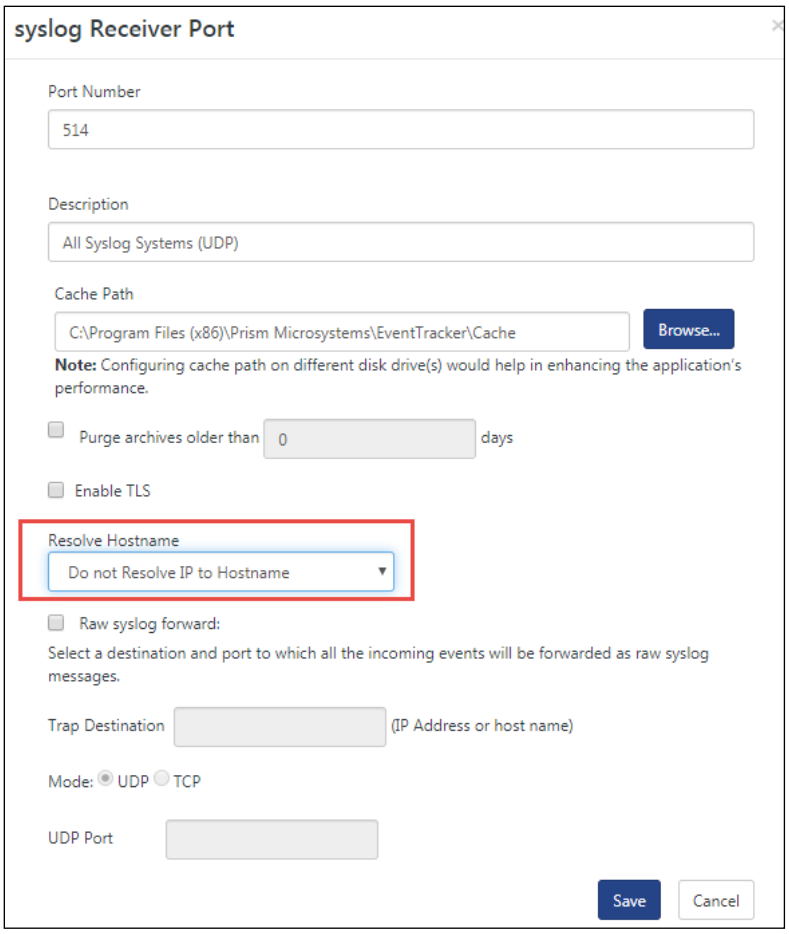


Figure 10

You will see the IP Address or Hostname entry in the "System' module depending upon enabling or disabling the option.

E-mail Incident

In this update, enhancement has been provided in the E-mail Incident option under Incident module.

In the e-mail Incident option, the email-ids of those users will be displayed who are having permission to that particular system/group.

From the Incidents Dashboard, click the Email Incident option.

Figure 11

The E-mail Incident window will get displayed.

Clicking the Add icon will display the e-mail ids of the users who have permission to this system/group.

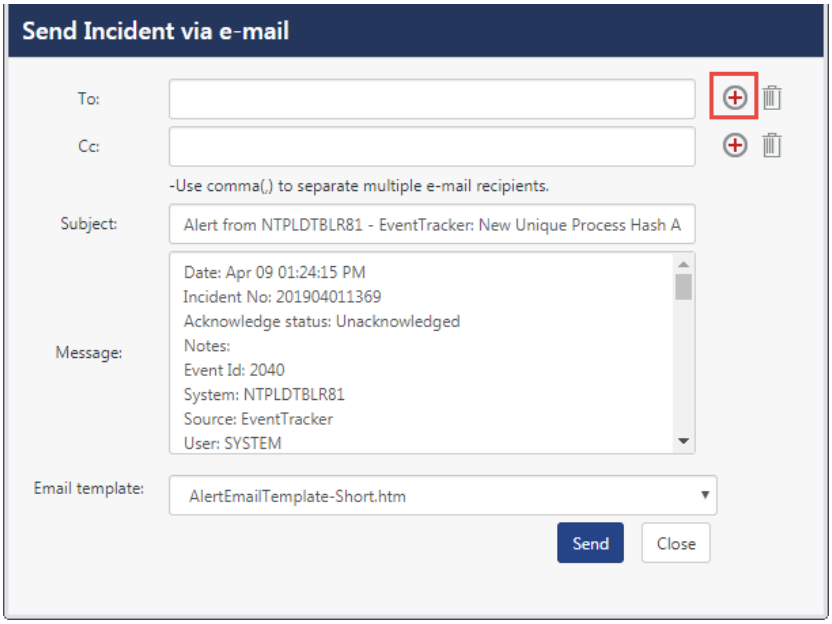


Figure 12

Select the email ids and click OK.

Figure 13

You can also select an E-mail Template from the dropdown options.

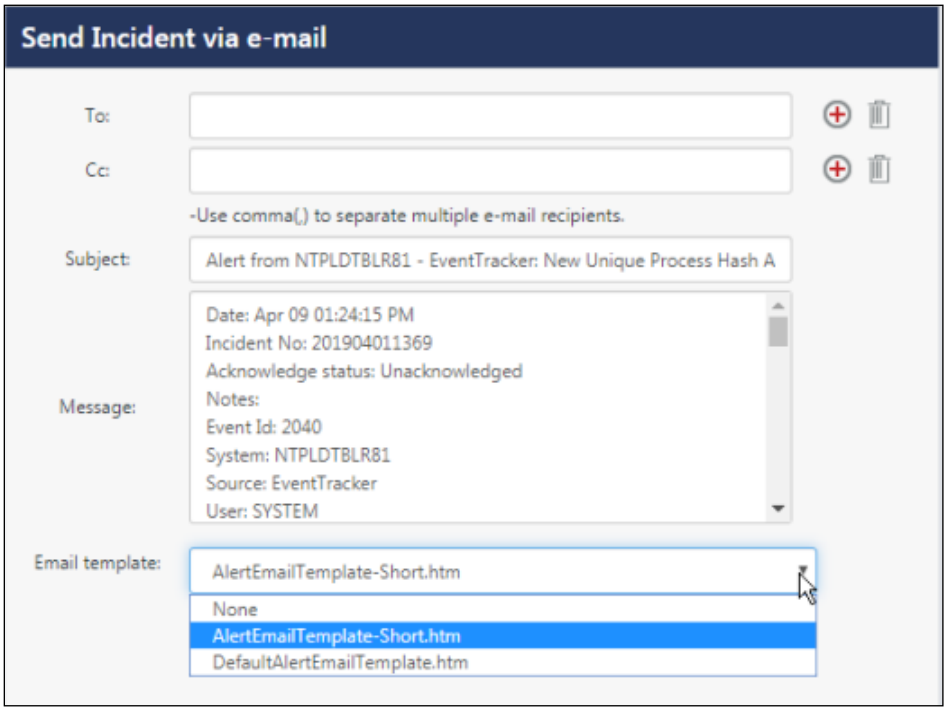


Figure 14

NOTE: For Collection Point site, only the email-ids of those users will be displayed, who has permission to the Collection Point site/group.

Configure syslog over TLS

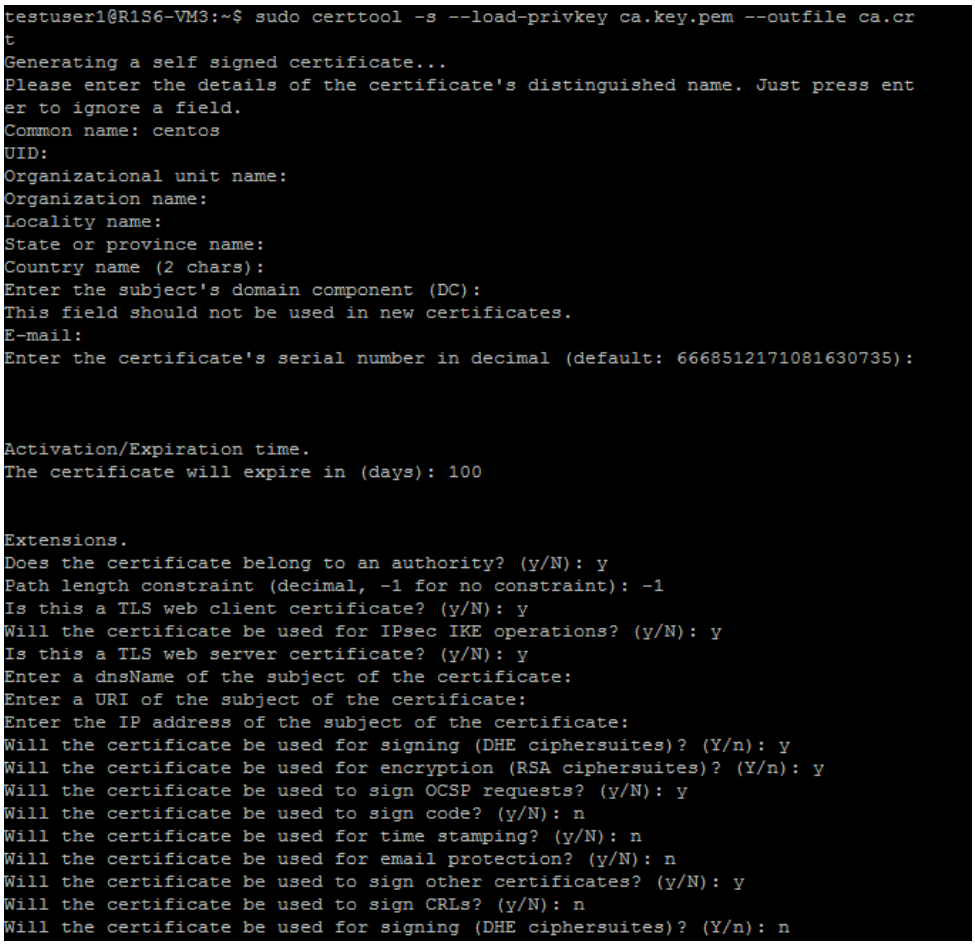
Pre-requisites

- Ensure to install the GnuTLS-utils for using the Certtool.

*****IMPORTANT: TLS will only support for TCP mode.**

How to create a Client certificate?

- Login to the Client Machine (CentOS or UBUNTU).
- Enter the below command:
  certtool -p --outfile ca.key.pem
- Enter the credentials to generate RSA private key.
- Next, enter the below command:
  certtool -s --load-privkey ca.key.pem --outfile ca.crt
- Next, enter the Common name, the certificate expiry date and the below fields as shown in the figure:



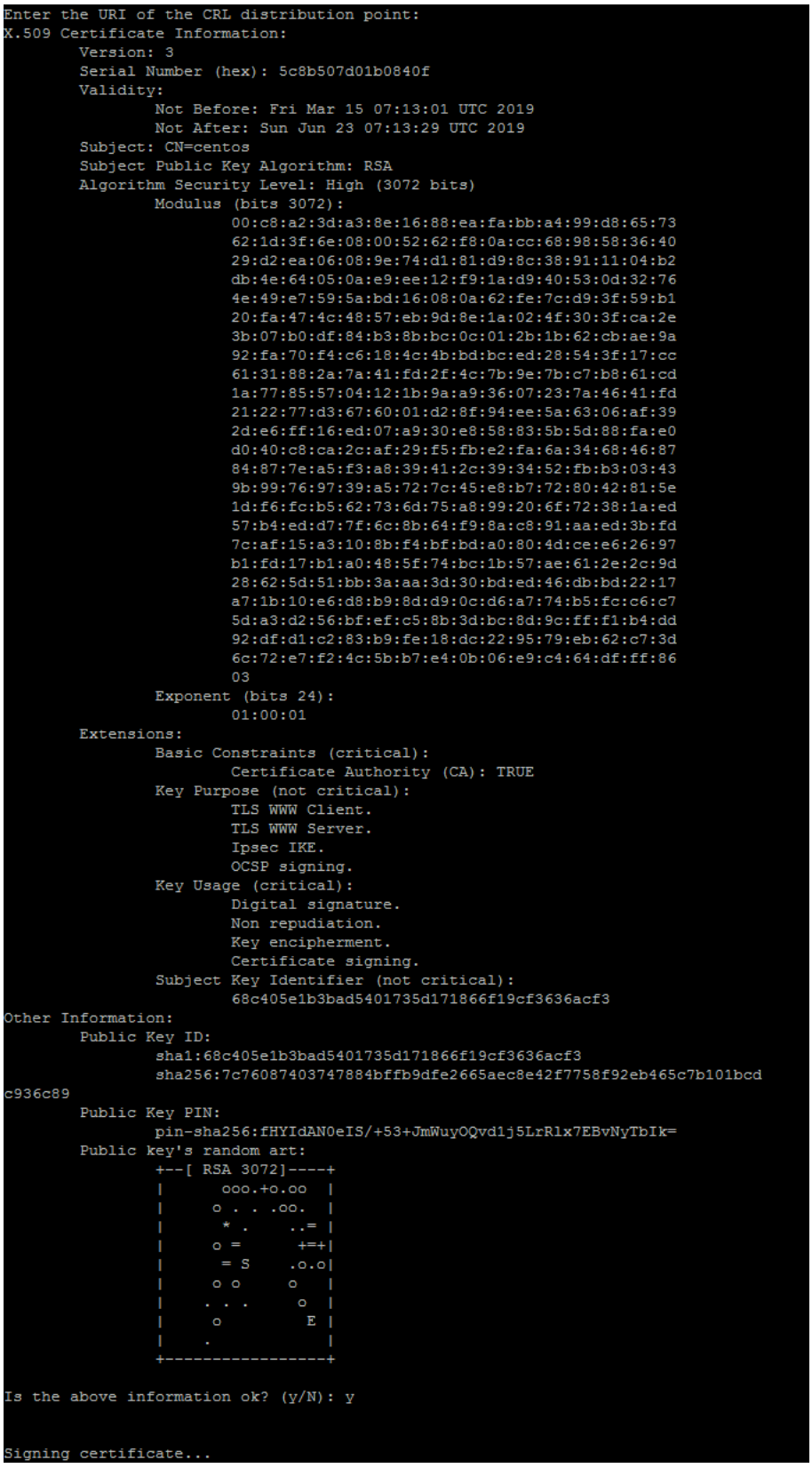

Enter the URI of the CRL distribution point:
X.509 Certificate Information:
Version: 3
Serial Number (hex): 5c8b507d01b0840f
Validity:
Not Before: Fri Mar 15 07:13:01 UTC 2019
Not After: Sun Jun 23 07:13:29 UTC 2019
Subject: CN=centos
Subject Public Key Algorithm: RSA
Algorithm Security Level: High (3072 bits)
Modulus (bits 3072):
00:c8:a2:3d:a3:8e:16:88:ea:fa:bb:a4:99:d8:65:73
62:1d:3f:6e:08:00:52:62:f8:0a:cc:68:98:58:36:40
29:d2:ea:06:08:9e:74:d1:81:d9:8c:38:91:11:04:b2
db:4e:64:05:0a:e9:ee:12:f9:1a:d9:40:53:0d:32:76
4e:49:e7:59:5a:bd:16:08:0a:62:fe:7c:d9:3f:59:b1
20:fa:47:4c:48:57:eb:9d:8e:1a:02:4f:30:3f:ca:2e
3b:07:b0:df:84:b3:8b:bc:0c:01:2b:1b:62:cb:ae:9a
92:fa:70:f4:c6:18:4c:4b:bd:bc:ed:28:54:3f:17:cc
61:31:88:2a:7a:41:fd:2f:4c:7b:9e:7b:c7:b8:61:cd
1a:77:85:57:04:12:1b:9a:a9:36:07:23:7a:46:41:fd
21:22:77:d3:67:60:01:d2:8f:94:ee:5a:63:06:af:39
2d:e6:ff:16:ed:07:a9:30:e8:58:83:5b:5d:88:fa:e0
d0:40:c8:ca:2c:af:29:f5:fb:e2:fa:6a:34:68:46:87
84:87:7e:a5:f3:a8:39:41:2c:39:34:52:fb:b3:03:43
9b:99:76:97:39:a5:72:7c:45:e8:b7:72:80:42:81:5e
1d:f6:fc:b5:62:73:6d:75:a8:99:20:6f:72:38:1a:ed
57:b4:ed:d7:7f:6c:8b:64:f9:8a:c8:91:aa:ed:3b:fd
7c:af:15:a3:10:8b:f4:bf:bd:a0:80:4d:ce:e6:26:97
b1:fd:17:b1:a0:48:5f:74:bc:1b:57:ae:61:2e:2c:9d
28:62:5d:51:bb:3a:aa:3d:30:bd:ed:46:db:bd:22:17
a7:1b:10:e6:d8:b9:8d:d9:0c:d6:a7:74:b5:fc:c6:c7
5d:a3:d2:56:bf:ef:c5:8b:3d:bc:8d:9c:ff:f1:b4:dd
92:df:d1:c2:83:b9:fe:18:dc:22:95:79:eb:62:c7:3d
6c:72:e7:f2:4c:5b:b7:e4:0b:06:e9:c4:64:df:ff:86
03
Exponent (bits 24):
01:00:01
Extensions:
Basic Constraints (critical):
Certificate Authority (CA): TRUE
Key Purpose (not critical):
TLS WWW Client.
TLS WWW Server.
Ipsec IKE.
OCSP signing.
Key Usage (critical):
Digital signature.
Non repudiation.
Key encipherment.
Certificate signing.
Subject Key Identifier (not critical):
68c405e1b3bad5401735d171866f19cf3636acf3
Other Information:
Public Key ID:
sha1:68c405e1b3bad5401735d171866f19cf3636acf3
sha256:7c76087403747884bffb9dfe2665aec8e42f7758f92eb465c7b101bcd
c936c89
Public Key PIN:
pin-sha256:fHYIdAN0eIS/+53+JmWuyOQvd1j5LrRlx7EBvNyTbIk=
Public key's random art:
+--[RSA 3072]----+
| ooo.+o.oo |
| o . . .oo. |
| * . ..= |
| o = +=+|
| = S .o.o|
| o o o |
| . . . o |
| o E |
| . |
+-----------------+
Is the above information ok? (y/N): y
Signing certificate...

Figure 15

It will generate a client certificate with the name **ca.crt**

To verify, whether it got generated or not, please enter the below command:

ls

How to generate a Server Certificate?

- Enter the below command with your machine name. (Machine name is not mandatory)
  In our example, we have taken machine name as “ntpldtblr300”. To generate the RSA private key:

certtool -p --outfile ntpldtblr300.key.pem

- To convert pem file to crt file, enter the below command:

certtool -c --load-privkey ntpldtblr300.key.pem --load-ca-privkey ca.key.pem --load-ca-certificate ca.crt --outfile ntpldtblr300.crt

- Next, enter the Common name, the certificate expiry date and the below fields as shown in the figure:
- **Please mention the server IP Address in the highlighted field.**

```
testuser1@R1S6-VM3:~$ sudo certtool -p --outfile ntpldtblr300.key.pem
Generating a 3072 bit RSA private key...
testuser1@R1S6-VM3:~$  sudo certtool -c --load-privkey ntpldtblr300.key.pem --load-ca-privkey ca.key.pem --load-ca-certificate ca.crt --outfile ntpldtblr300.crt
Generating a signed certificate...
Please enter the details of the certificate's distinguished name. Just press enter to ignore a field.
Common name: ntpldtblr300
UID:
Organizational unit name:
Organization name:
Locality name:
State or province name:
Country name (2 chars):
Enter the subject's domain component (DC):
This field should not be used in new certificates.
E-mail:
Enter the certificate's serial number in decimal (default: 6668516418939275721):


Activation/Expiration time.
The certificate will expire in (days): 100

Expiration time: Sun Jun 23 12:59:32 2019
CA expiration time: Sun Jun 23 12:43:29 2019
Warning: The time set exceeds the CA's expiration time
Is it ok to proceed? (y/N): y


Extensions.
Does the certificate belong to an authority? (y/N): y
Path length constraint (decimal, -1 for no constraint): -1
Is this a TLS web client certificate? (y/N): y
Will the certificate be used for IPsec IKE operations? (y/N): y
Is this a TLS web server certificate? (y/N): y
Enter a dnsName of the subject of the certificate:
Enter a URI of the subject of the certificate:
Enter the IP address of the subject of the certificate: 172.28.100.43
Will the certificate be used for signing (DHE ciphersuites)? (Y/n): y
Will the certificate be used for encryption (RSA ciphersuites)? (Y/n): y
Will the certificate be used to sign OCSP requests? (y/N): y
Will the certificate be used to sign code? (y/N): n
Will the certificate be used for time stamping? (y/N): n
Will the certificate be used for email protection? (y/N): n
Will the certificate be used to sign other certificates? (y/N): y
Will the certificate be used to sign CRLs? (y/N): n
Will the certificate be used for signing (DHE ciphersuites)? (Y/n): y
```

Figure 16

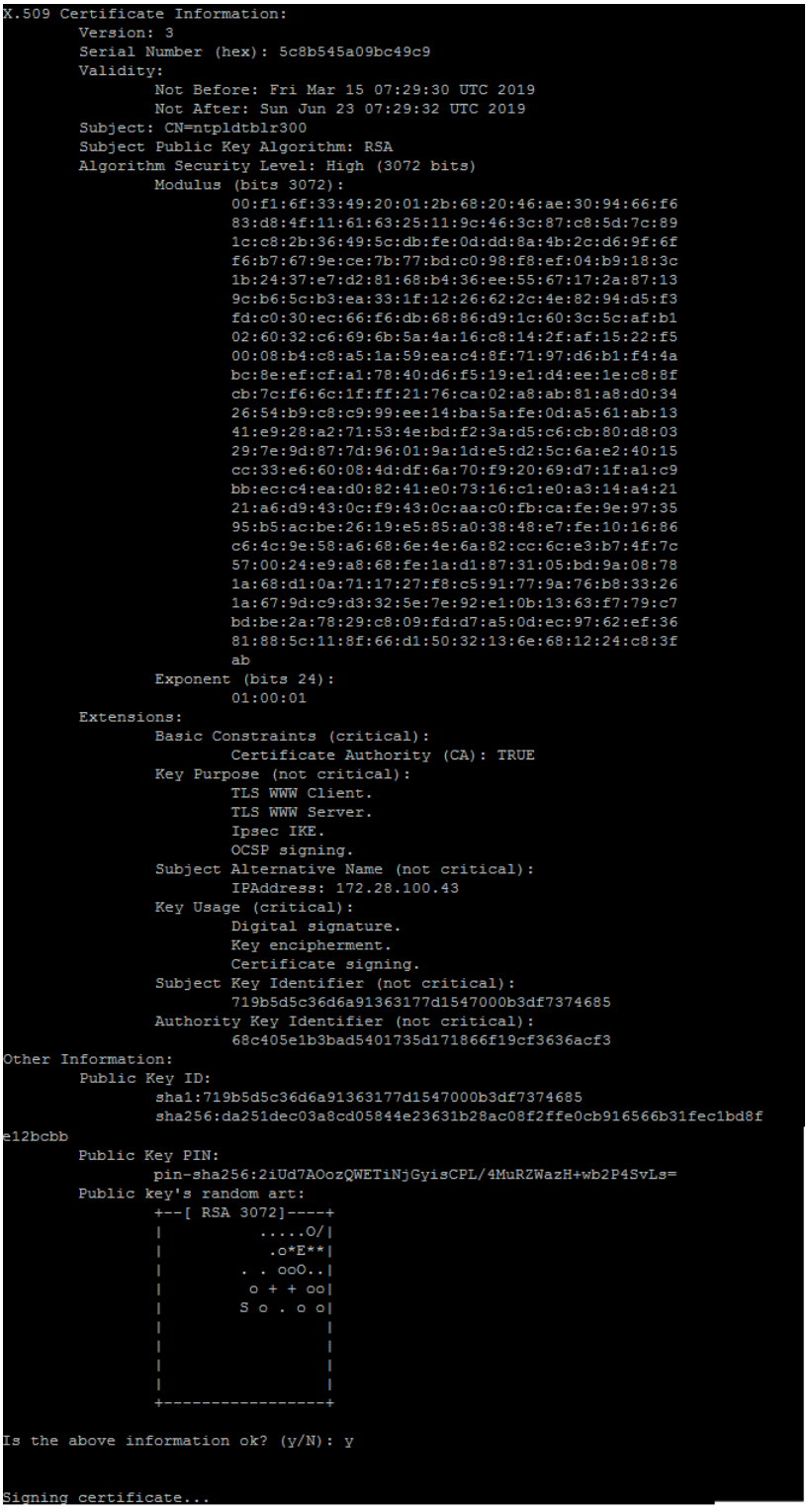


Figure 17

- Now, to convert crt file to pfx file, Enter the below command:

openssl pkcs12 -export -out ntpldtblr300.pfx -inkey ntpldtblr300.key.pem -in ntpldtblr300.crt

- Enter the Export password to use the server certificate.
- To verify, whether the certificate got generated or not, please enter the below command:

ls

```
testuser1@R1S6-VM3:~$  sudo openssl pkcs12 -export -out ntpldtblr300.pfx -inkey ntpldtblr300.key.pem -in ntpldtblr300.crt
[sudo] password for testuser1:
Enter Export Password:
Verifying - Enter Export Password:
testuser1@R1S6-VM3:~$ ls
ca.crt  ca.key.pem  ntpldtblr300.crt  ntpldtblr300.key.pem  ntpldtblr300.pfx
```

Figure 18

NOTE: Please export the certificate file (.pfx file) in the Server machine. If the user is not able to export the certificate file, give Read and Write permission to export the file as shown below:

chmod a+rw ntpldtblr300.pfx

How to Configure TLS in the Server Machine?

1. Login to the EventTracker web and then navigate to Admin and then Manager Configuration.
2. Go to syslog/Virtual Collection Point tab.
3. In the syslog pane, click Add.
4. In syslog Receiver port window, enter the Port number and then Enable TLS.
5. Provide the common name of the server certificate and then browse the path for the pfx certificate file.
6. Give the password, which was provided while exporting the certificate.

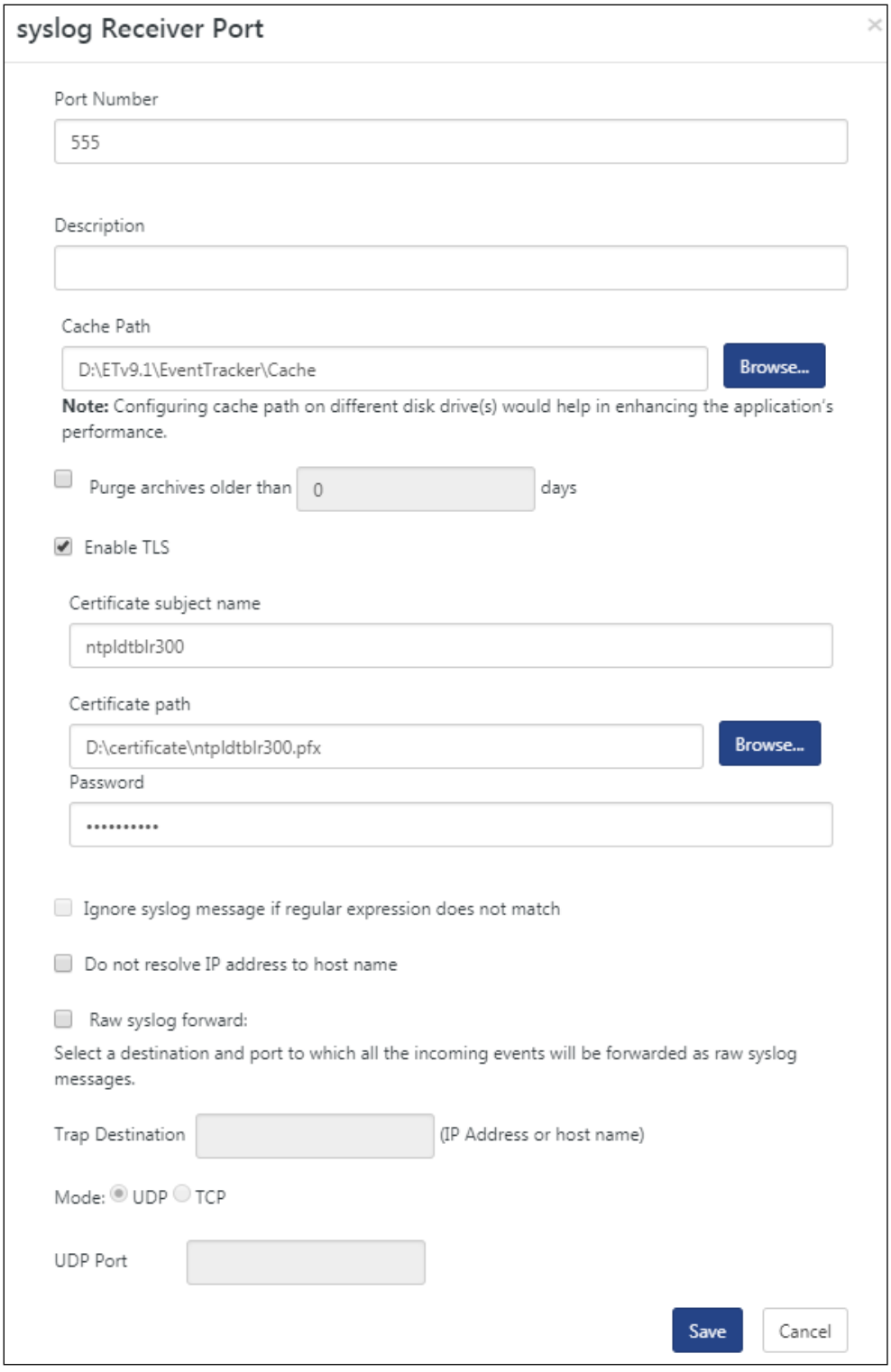


Figure 19

7. Click on **Save**.

Rsyslog Configuration to forward data from Client to server using certificate

- Login to the CentOS or UBUNTU client machine.
- Install rsyslog-gnutls
- Type the below command to configure rsyslog

vi /etc/rsyslog.conf

- Enter the password and the rsyslog configuration will display.
- Enter the below commands to enable the TLS.

```
$DefaultNetstreamDriverCAFile /etc/rsyslog.d/keys/ca.crt
#$DefaultNetstreamDriverCertFile /etc/rsyslog.d/keys/ca.d/79.crt
#$DefaultNetstreamDriverCertFile /etc/rsyslog.d/keys/ca.d/9227.crt
$DefaultNetstreamDriver gtls # use gtls netstream driver
$ActionSendStreamDriverMode 1 # require TLS for the connection
$ActionSendStreamDriverAuthMode anon # server is NOT authenticated
#$ActionSendStreamDriverAuthMode x509/certvalid
#$ActionSendStreamDriverAuthMode x509/name
```

Figure 20

- Please enable the following commands to communicate through TLS.

$DefaultNetstreamDriverCAFile /etc/rsyslog.d/keys/ca.crt

$DefaultNetstreamDriver gtls # use gtls netstream driver

$ActionSendStreamDriverMode 1 # require TLS for the connection

$ActionSendStreamDriverAuthMode anon # server is NOT authenticated

- Now, provide the IP address of the server and the port number to forward the data from client to server. An example is shown below:

```
*.* @@remote-host:514

start forwarding rule 1
$ActionQueueType LinkedList # use asynchronous processing
$ActionQueueFileName srvrfwd1 # set file name, also enables disk mode
$ActionResumeRetryCount -1 # infinite retries on insert failure
$ActionQueueSaveOnShutdown on # save in-memory data if rsyslog shuts down
*.* @@172.28.100.43:529
# end forwarding rule 1

start forwarding rule 2
$ActionQueueType LinkedList # use asynchronous processing
$ActionQueueFileName srvrfwd1 # set file name, also enables disk mode
$ActionResumeRetryCount -1 # infinite retries on insert failure
$ActionQueueSaveOnShutdown on # save in-memory data if rsyslog shuts down
*.* @@172.28.9.145:520
# end forwarding rule 1
```

Figure 21

Syslog-ng configuration to forward data from Client to server using certificate

- Login to the CentOs or UBUNTU client machine.
- Type the below command to configure syslog-ng

vi /etc/syslog-ng/syslog-ng.conf

- Now enter the password and the syslog-ng configuration will display.
- To forward data client to server, provide the IP address and the port number.
- For enabling TLS, enter the command shown below:

tls(peer_verify(optional-untrusted) ca_dir("/etc/rsyslog.d/keys/ca.crt")));

```
destination d_net {
tcp("172.28.100.52" port(514)
tls(peer_verify(optional-untrusted) ca_dir("/etc/rsyslog.d/keys/ca.crt")));
};
```

Figure 22

- To map the source configuration with destination, provide the below command:

log { source(s_src); destination(d_net);};