Rsyslog and Winsyslog

Rsyslog and Winsyslog are two almost identical agents (similar GUI). They are marketed by the same company. There are a few differences depending on the licence. You can see the comparison ici and ici.

Rsyslog and Winsyslog are configured in the same way.

note: Rsyslog and Winsyslog are proprietary and licensed.

Installation

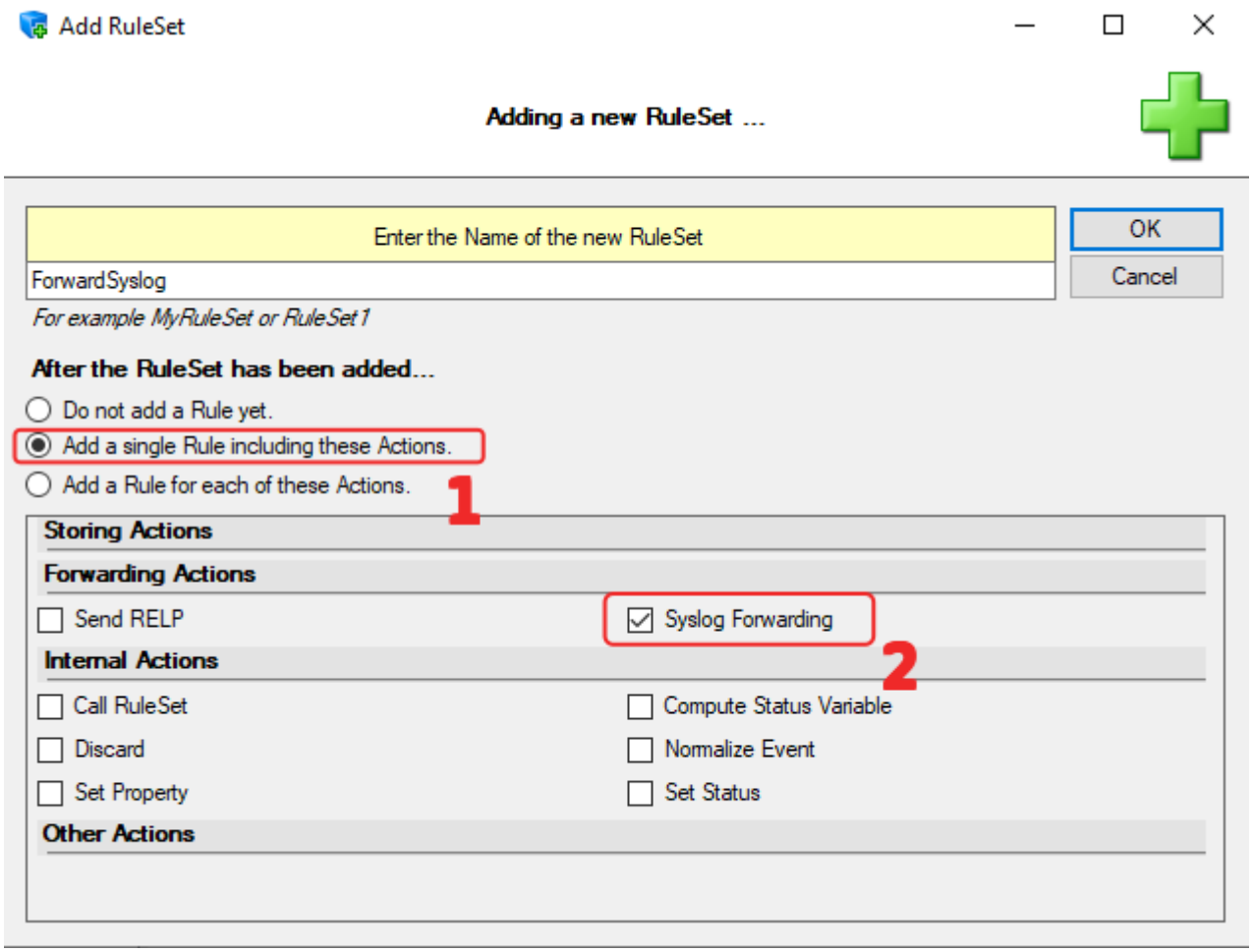
File **.exe** which you can download ici (rsyslog) and/or ici (winsyslog).

Create a rule

The first step is to create a rule. A default rule already exists. You can delete it.

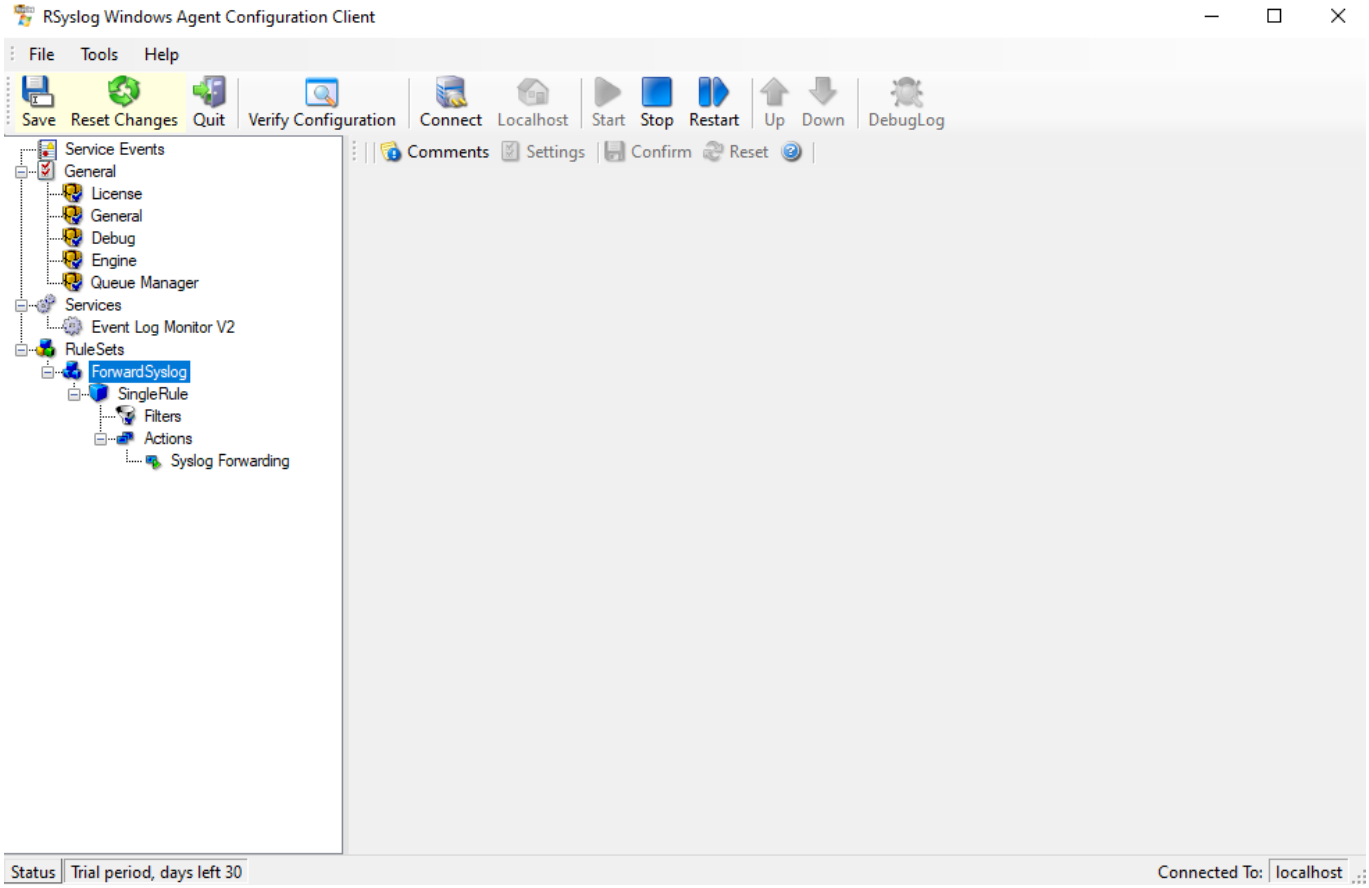
To add a rule, right-click on **RuleSets** > **Add RuleSet**

Name your rule and tick only “. **Add a single Rule including these Actions**and ” **Syslog Forwading** “

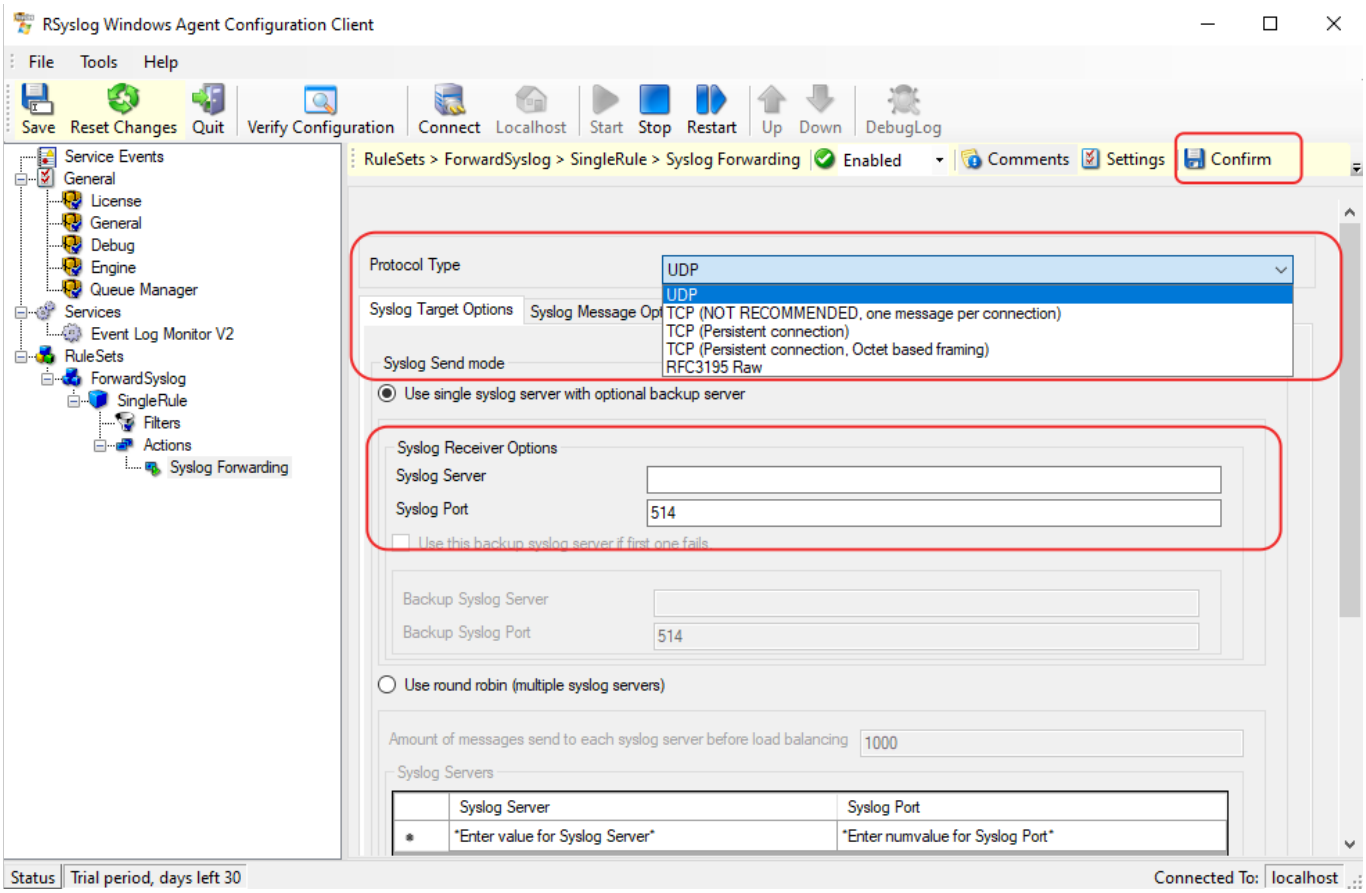


note: this rule simply forwards logs without any particular filter

The rule appears in the left side menu.



Expand the tree to find the rule action and click on it.

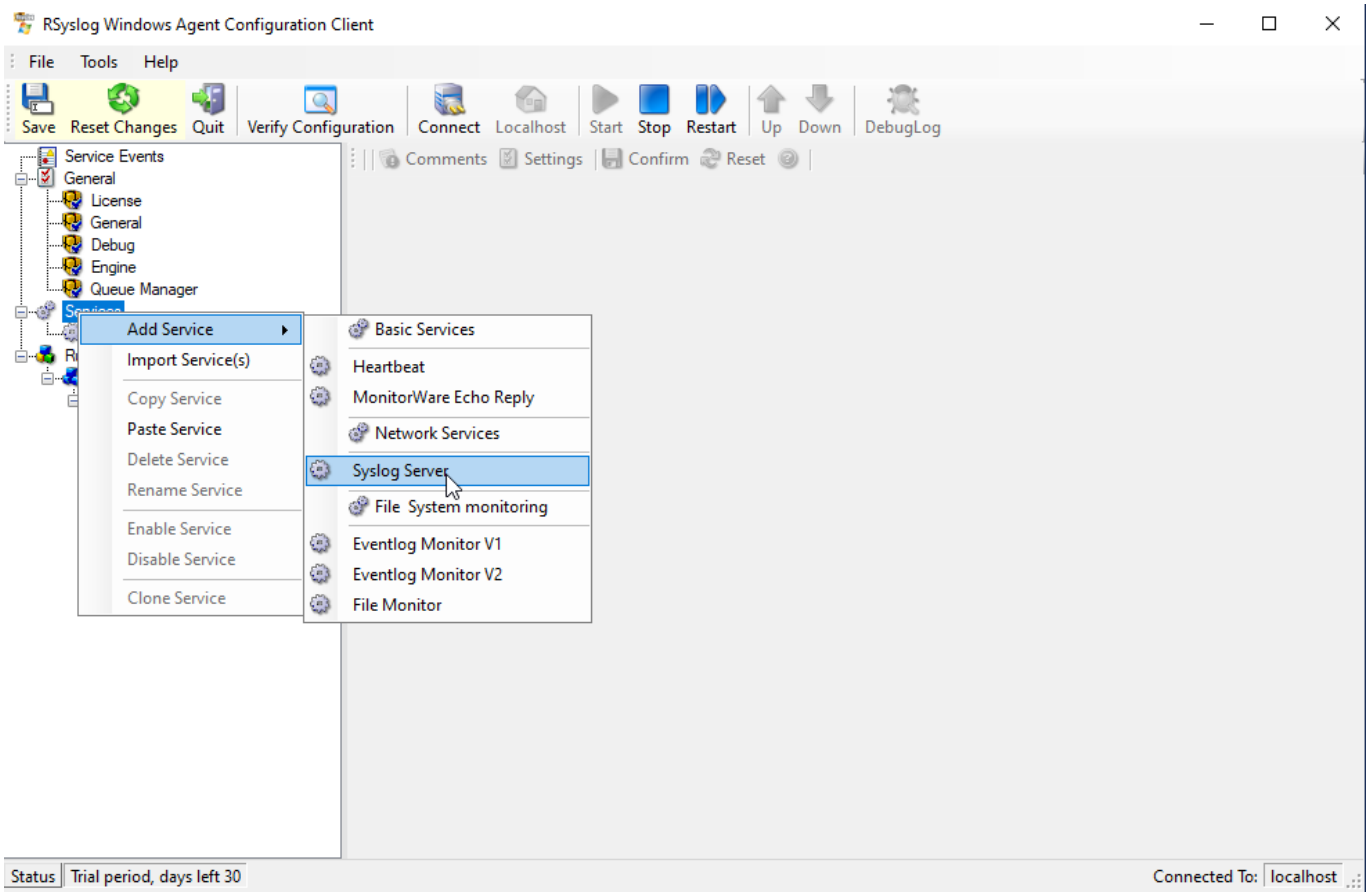


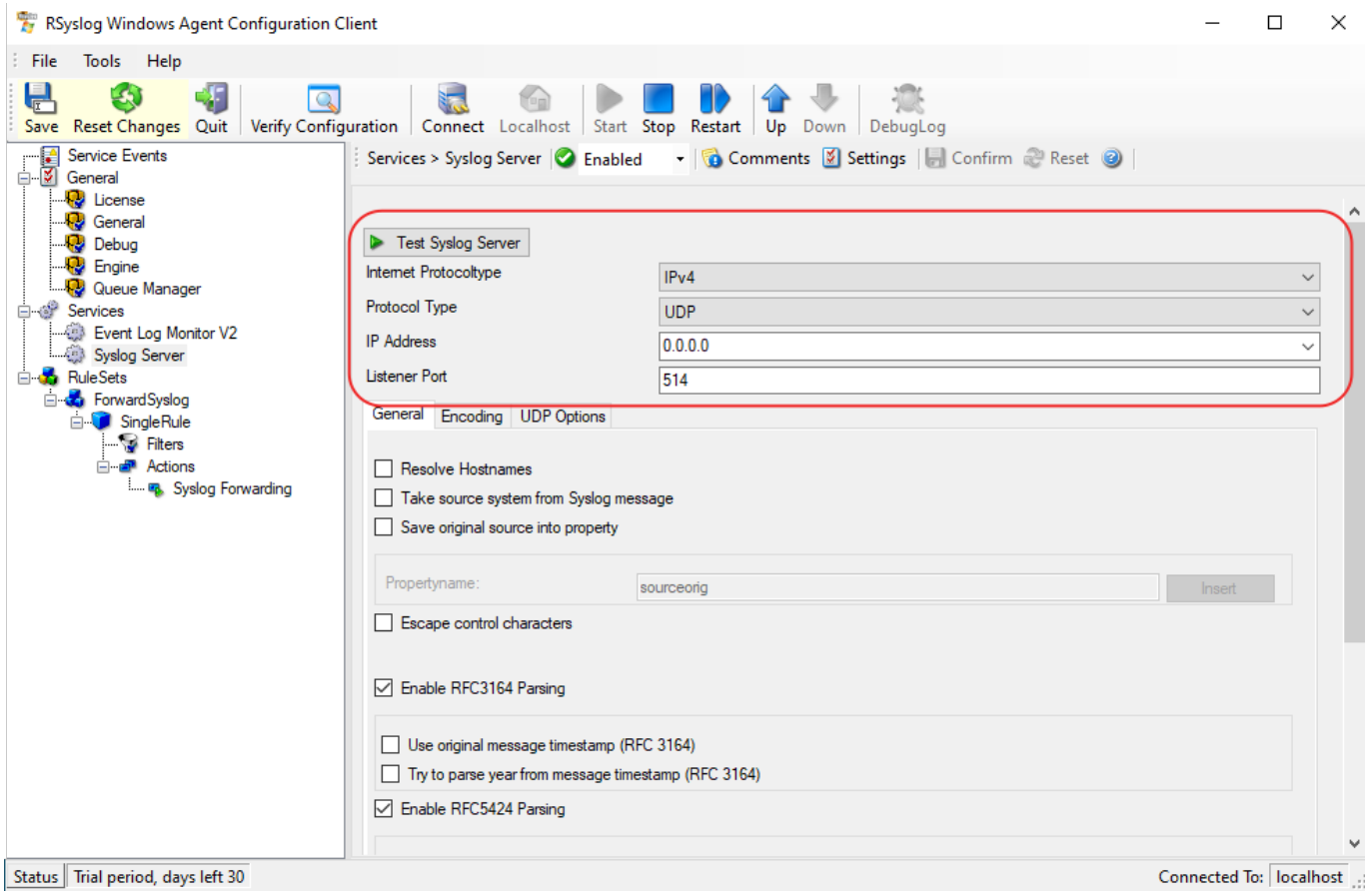
Choose **UDP** or **TCP** according to your preference, enter the**IP address** address of the Syslog server and the port.

To finish, click on **Confirm** “in the top right-hand corner.

Defining a Syslog server

Right-click on **Services** > **Add Service** > **Syslog Server**



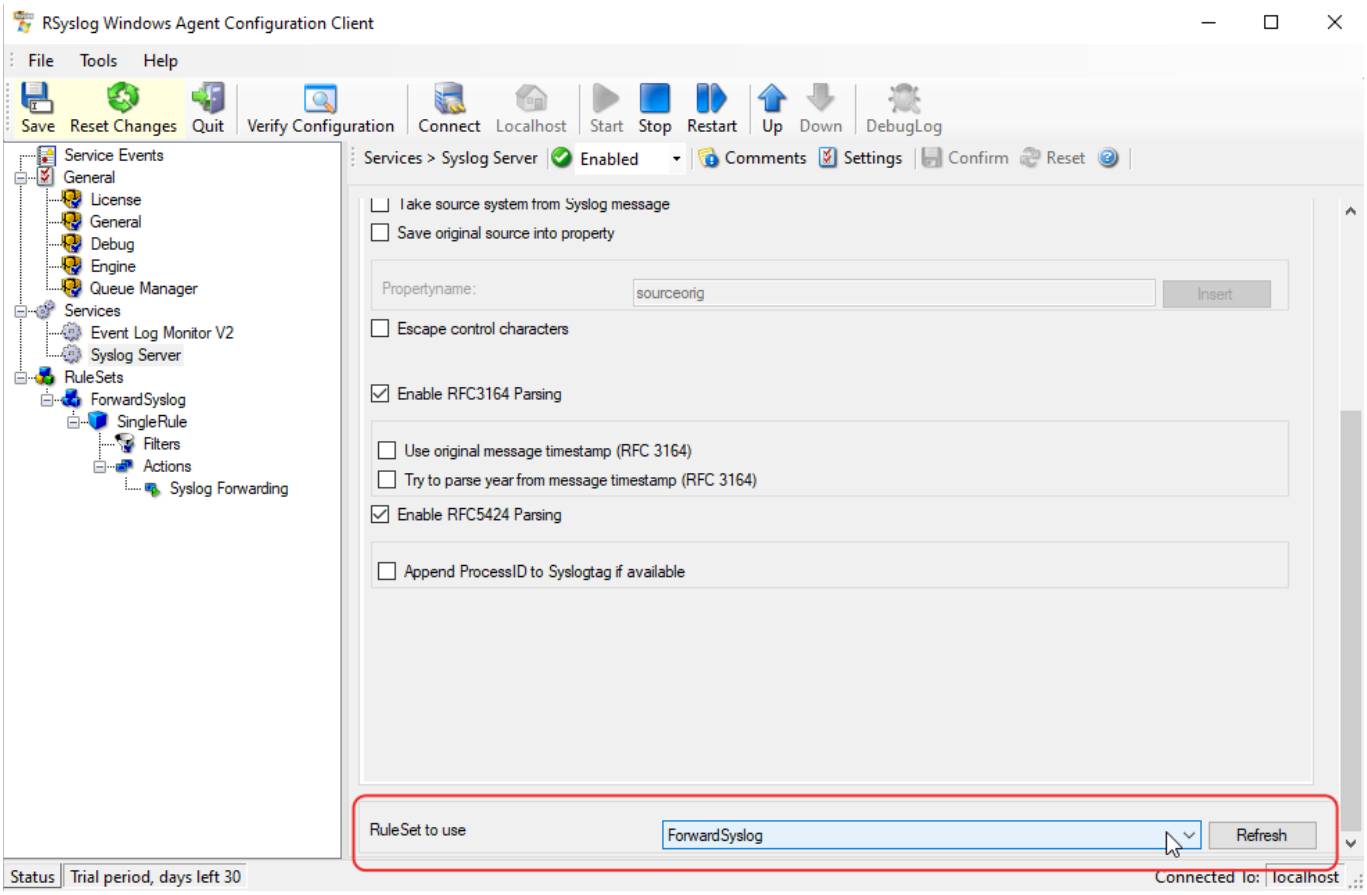


Configure the server to be reached by entering :

- IPv4 or IPv6
- Protocol

- IP address
- Listening port

Then, at the bottom, select the rule you created earlier.



Configure the Syslog agent

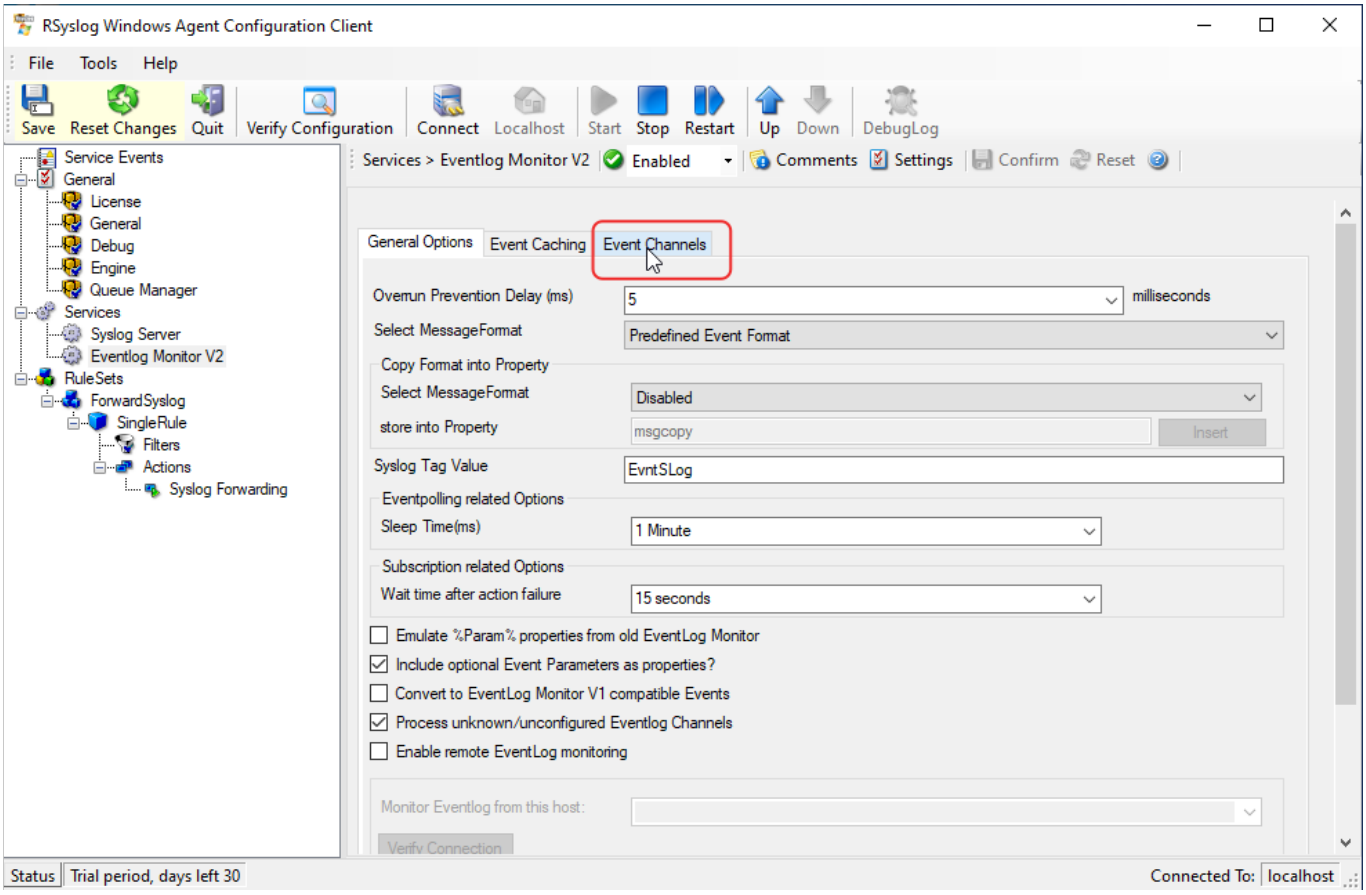
Right-click on **Services** > **Add Service** > **EventLog V1 or V2 Monitor**

Depending on OS version :

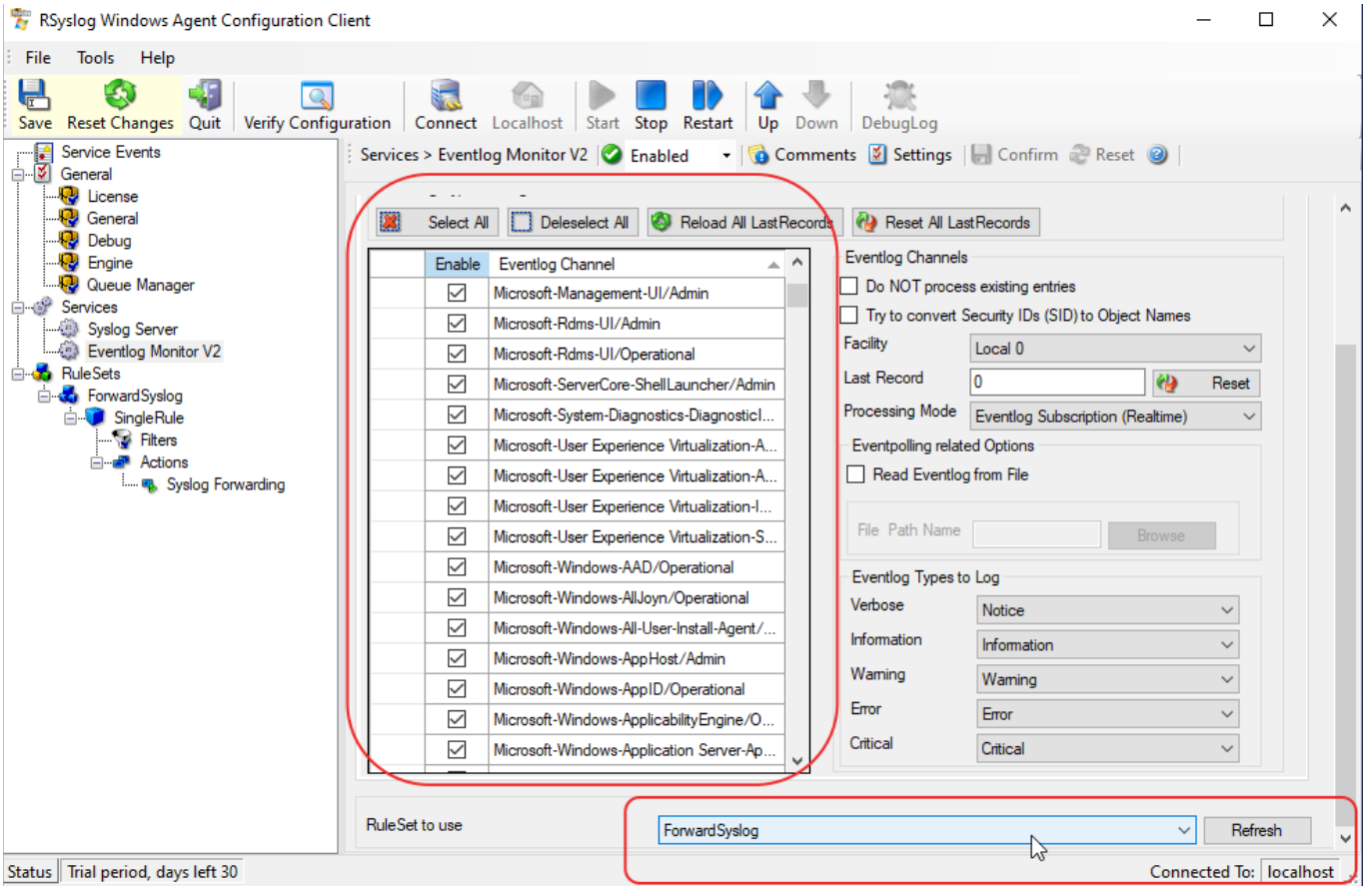
- EventLog V1 monitor: 2000, XP, 2003
- EventLog V2 Monitor: Vista, 2008, 7, 10

note: for server versions, refer to the kernel (e.g. microsoft server 2019 = windows 10) Services > Add Service > Eventlog Monitor V1/2

Click on the " **Event Channels** "



From here you can select the eventslog to be forwarded. Don't forget to select the right rule at the bottom of the window (if there are several) and save before exiting.



Start the service

Click on start to start the service. Once the service has been configured and started, you can close the program.