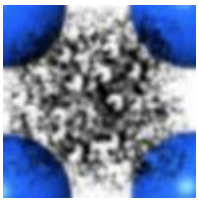


Ev2T
The Event to Trap Generat

Html Help File

About Ev2T from Network Computing Technologies, Inc.
Ev2T is a one-of-a-kind application that monitors the Event Log of NT based systems. For each entry recorded to event logs (Application, System, and Security) an SNMP trap is produced.
Ev2T is composed of two (2) applications: Ev2t.exe and Ev2tcfg.exe. Ev2t.exe is service application that performs the monitoring and SNMP trap generation. Ev2tcfg.exe is an MFC based application providing a convenient interface to the Ev2t.exe configuration.

The Ev2T Service

Ev2t.exe is a light-weight service based application. It used the Microsoft Eventlog API to monitor the event logs and it uses the registry to store configuration data. Otherwise, it is completely stand-alone.
Ev2t.exe is based on C++ object modeling using Rational Rose. Ev2t also employs full source code analysis using BoundsChecker and TrueCoverage from Compuware.
From the DOS prompt, the ev2t.exe program accepts one (1) argument. This can be either

- -i
- -v
- -u

The "-i" parameter installs the ev2t.exe as a service.
The "-v" parameter verifies whether ev2t.exe is installed as a service.
The "-u" parameter uninstalls the ev2t.exe service.
You should not need to execute ev2t.exe from the command line, however. Once installed, the Services Control Panel Applet is used to start and stop the service.

The Ev2T Configuration Application

There are three main, indepenent sections (tabs):

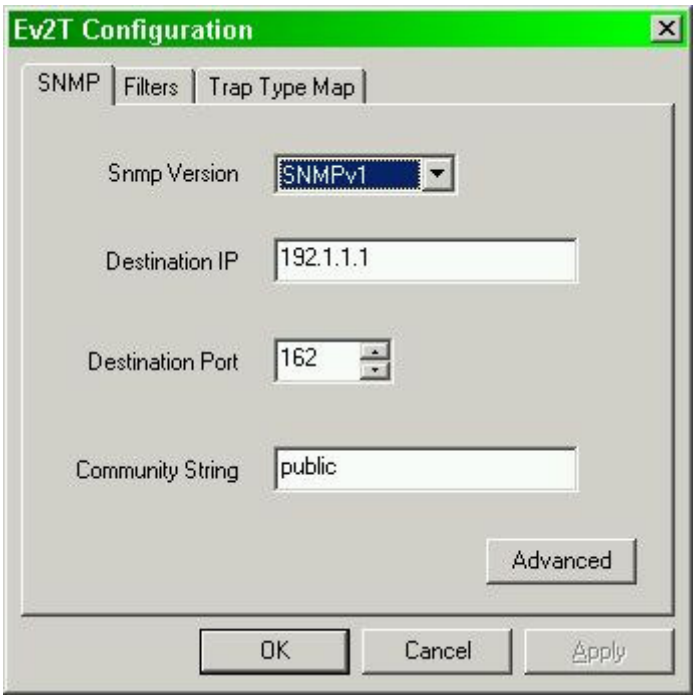
- SNMP Parameters
- Filters
- Event ID Mapping

SNMP Parameters

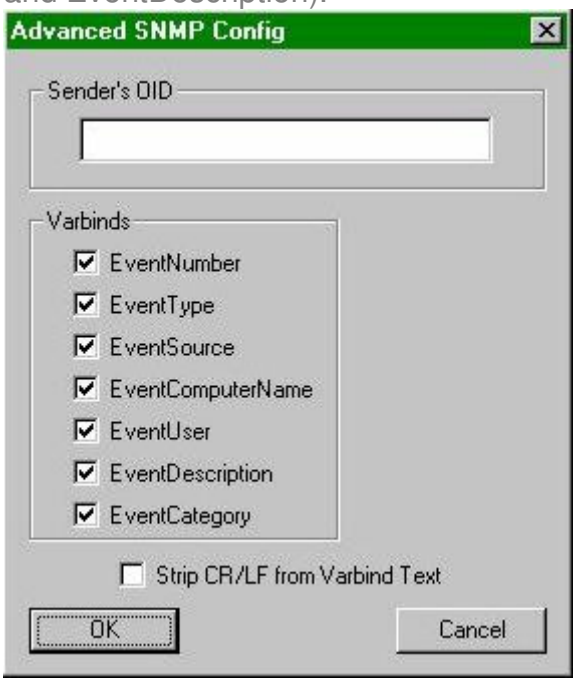
Hopefully these four parameters are self-explanitory.

- SNMP Version - tells Ev2t which format of the SNMP trap to send.
- Destination IP - tells Ev2t the destination host name or IP address for sending traps.
- Destination Port - tells Ev2t the destination port for sending traps
- Community - tells Ev2t which community string to use in the traps it sends.

- Advanced Settings - for specifying an alternate Sender's OID and controlling varbinds.



Clicking on the "Advanced" button will display the following dialog for configuring the Enterprise (Sender's) OID (default is as specified in the MIB), for controlling which varbinds to include in the trap (all are included by default), and an option to strip CR/LF in the string type varbinds (EventSource, EventComputerName, EventUser, and EventDescription).



Figur 1

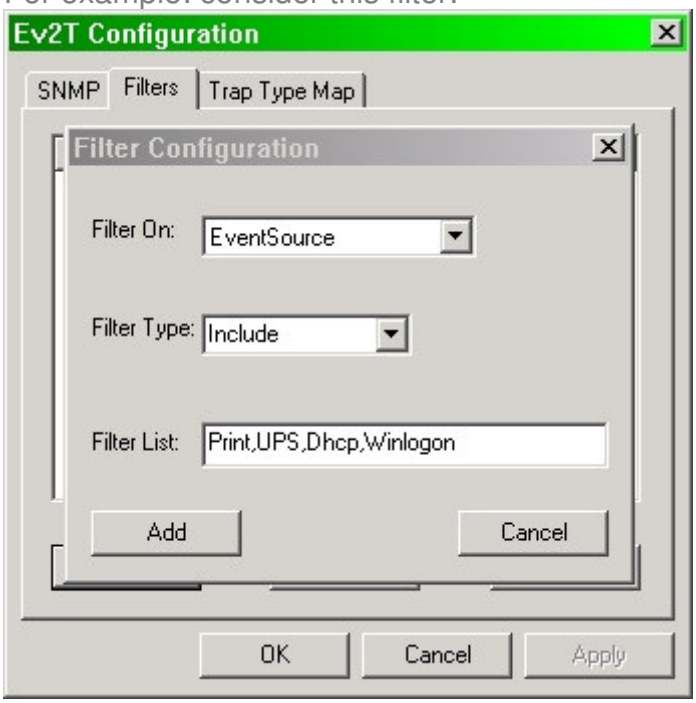
Filters

Ev2T will filter its SNMP trap output. This reduces the number of SNMP traps generated and allows you to see only those events in which you are truly interested.

Filters are managed on the Filters tab. Here you can add, delete, and modify filters. A filter is composed of the pieces of information:

- Filter On - You may filter based on any of the trap objects (EventComputerName, EventDescription, EventId, EventSource, EventType, EventUser, or EventCategory). Please refer to the mib file for a description of these data.
- Filter Type - There are two types of filters; include filters and exclude filters. An include filter is an "include only" filter. Therefore, all traps are excluded except those that match the associated filter list. An exclude filter is an "exclude only" filter. Therefore, all traps are included except those that match the associated filter list.
- Filter List - This field specifies the value or values of the "Filter On" field that must match for the filter to be active (included or excluded depending on filter type).

For example: consider this filter:

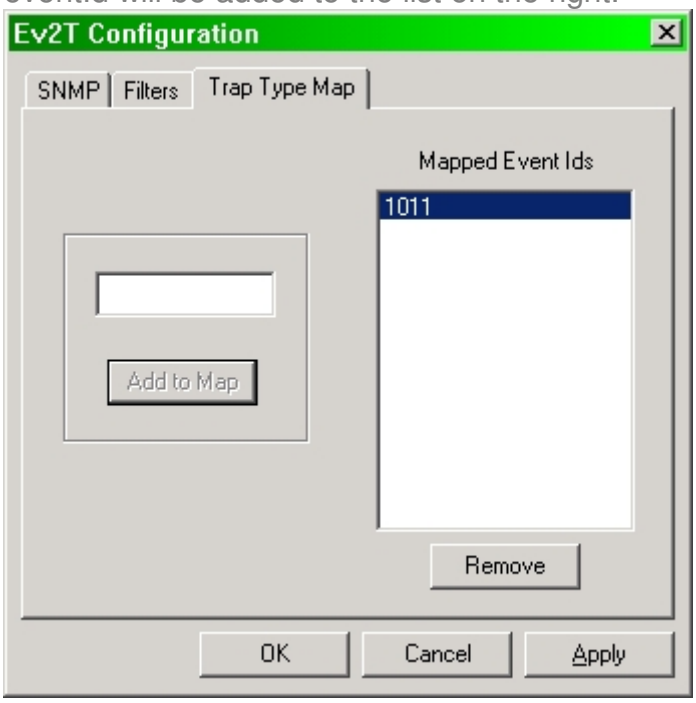


This filter says generate the trap only if the EventSource equals "Print", or "UPS", or "Dhcp", or "Winlogon". On the other hand, if this were an exclude filter (Filter Type: Exclude), then traps except those that have their EventSource equal to "Print", or "UPS", or "Dhcp", or "Winlogon" would be generated.
Technically, you would only need only six filters total; one for each of the trap objects in the MIB. However, you can have more if it make more sense. For example, you could have one filter on EventSource that includes "Print" and a second filter on EventSource that includes "Dhcp". There is no functional difference and very little impact on efficency.

Event ID Mapping

If you examine the MIB, you will see that Ev2t generates only one trap. Each trap can contain different variable bindings depending on the event that generated it.
However, some trap processing is easier when the trap "looks" different (either community string, sender's OID, generic type or specific type). To achieve this, Ev2t

provides mapping. Mapping replaces the specific trap type with the EventId from the event that caused the trap. Please note that the EventId variable is still present in the variable binding list.
To instruct Ev2t to map eventIds, just provide the specific Ids you want mapped on the "Trap Type Map" tab. First enter the eventId in the box just above the "Add to Map" button. You can find the eventId by using the event viewer that comes with the operating system. After entering the eventId, press the "Add to Map" button. The eventId will be added to the list on the right.



To removed mapped eventIds, select the eventId from the list on the right, and click "Remove".

Further Information

There is a geeky kind of diagram on Ev2T on our web site. To report defects in the program, please email ev2tbugs@ncomtech.com. General comments, questions, and criticism can be directed to support@ncomtech.com.
Happy Trapping!