# Prelude Correlator - Feature #375

## Prelude Correlator upper event limit

04/06/2010 07:40 PM - James Chapple

| | | | |
|---|---|---|---|
| **Status:** | Assigned | **Start date:** | 04/06/2010 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | Francois POIROTTE | **% Done:** | 0% |
| **Category:** | | **Estimated time:** | 0.00 hour |
| **Target version:** | | | |
| **Resolution:** | | | |

**Description**

When a corrleated event such as Eventscan or Eventstorm contains large numbers of events, the Prewikka GUI times out and is unable to display the event details. On several test systems available to me, the threshold seemed to be around 5K events. This was discovered during a Nessus scan of monitored systems, where Nessus is scanning every port. Iptables is logging every blocked port, potentially generating many thousands of events during the window.

The ability to specify an upper limit in the Correlator rules for a given correlated event would be useful to prevent excessive messages in a single event.

**Related issues:**

| | | |
|---|---|---|
| Related to Prewikka - Bug #495: Request-URI Too Large | **Closed** | **05/30/2012** |

### History

#### #1 - 05/05/2010 03:40 PM - Yoann VANDOORSELAERE

Hi James,

It would be interesting to have some information concerning the slow query generating this timeout. Could you please enable query logging using the following configuration directive:

```
log: /path/to/your_log_file
```

Under the [idmef_database] Prewikka configuration section, and try to provides us information concerning the slow query when the mentionned condition occur?

#### #2 - 05/31/2011 07:48 AM - Yoann VANDOORSELAERE

*- Project changed from PRELUDE SIEM to Prelude Correlator*

#### #3 - 02/08/2012 08:20 PM - Francois POIROTTE

*- Status changed from New to Assigned*

*- Assignee set to Francois POIROTTE*

Probl