# Prewikka - Bug #204

## Not seeing all alerts in Prewikka

02/21/2007 12:09 AM -

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | Yoann VANDOORSELAERE | **% Done:** | 0% |
| **Category:** | | **Estimated time:** | 0.00 hour |
| **Target version:** | 0.9.10 | | |
| **Resolution:** | fixed | | |

**Description**

After upgrading to Prewikka 0.9.9 some of the alert grouping is not correct.
In 0.9.8 when grouping by classification.text in alert_listing the same classification alert on multiple sensors would list all of the sensors the event was detected on. In 0.9.9 Only 1 sensor is shown.
Also when there are two events with similar properties e.g. user authentication failed for the same user. the front end show 2x alerts, but when entering that event the alert_listing only shows the details for 1 of the events.

### History

#### #1 - 02/21/2007 01:29 PM - Yoann VANDOORSELAERE

*- Status changed from New to Assigned*

I am able to reproduce the first part of your report: only one of two analyzer of the same name but **different node** will show up.

The second part I am not able to reproduce, could you please provide me more details about this specific issue, and the exact settings you are using to reproduce it?

#### #2 - 02/21/2007 09:41 PM -

Two alerts with the same classification.text but different assessment.impact.severity or assesment.impact.completion.
On the frontend it groups these alerts as similar but on entering the alert the filtering of assesment.impact.completion and assessment.impact.severity removes some of the results.
Hope that helps

#### #3 - 03/07/2007 12:55 AM - Yoann VANDOORSELAERE

*- Status changed from Assigned to Closed*

*- Resolution set to fixed*

(In r8831) Correct handling of empty value for hash key generation. Fix #204.

#### #4 - 04/29/2009 12:21 PM - Yoann VANDOORSELAERE

*- Project changed from PRELUDE SIEM to Prewikka*

*- Category deleted (5)*

*- Target version deleted (0.9.10)*