Incidents

Successfully pass the free certification exam at IW Academy and become an Infinet Certified Engineer.

To the certification exam

- Incidents review
- Incident processing
- Incidents notifications

An **InfiMONITOR NEXT** user can obtain a list of all the incidents for the wireless devices and the links in his visibility area by going at the "**Incidents**" section.

The section includes two key areas:

- **Incidents list** - all incidents for the devices and the links in the user's visibility area are displayed here.
- **Incident profile side view** - if this area is open, an incident profile with detailed information will be displayed without hiding the list of incidents. If the area is hidden, then the selected incident profile will be opened, but the list of incidents will be hidden.

For easy operation with the incidents list a filter is available at the top of the page. Besides the standard filter by incident occurrence period, additional filters allows to sort incidents by the following parameters:

- assignee;
- status;
- severity;
- rule;
- object.

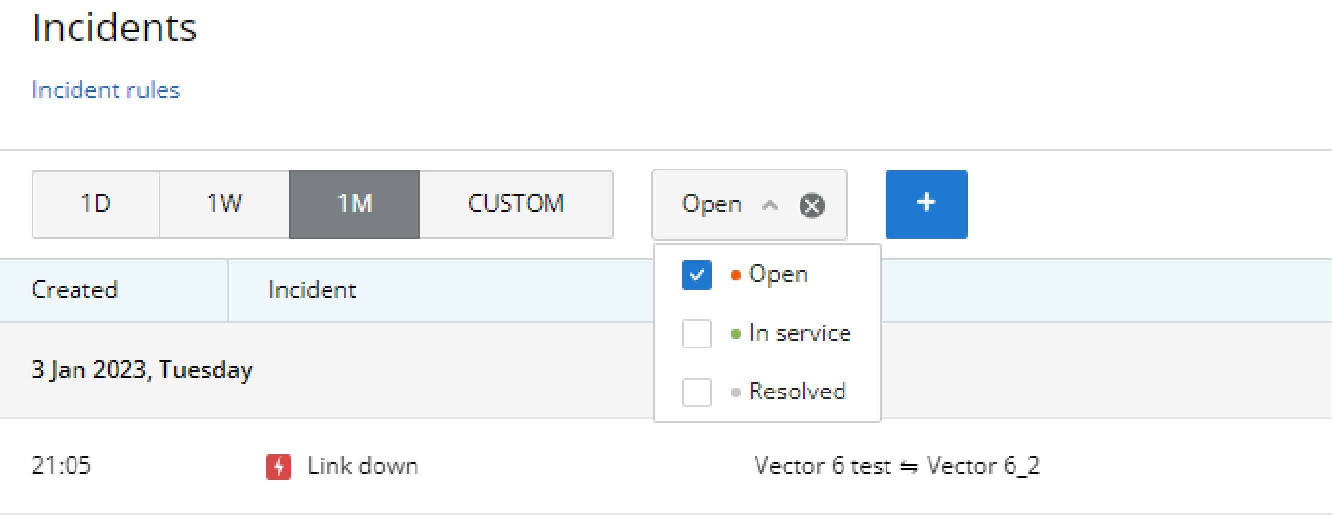


Figure - incidents list

Incidents review

The incidents list is presented in a table having the following columns:

- **Created** - the date and time when incident was created.
- **Incident** - it displays the title and severity of the rule according to which the incident was created.
- **Object** - the device for which the incident was created.
- **Status** - current incident's status. The possible statuses are described in the Incident management article.
- **Assignee** - user who was assigned for resolving this incident.
- **Updated** - the date and time when the rule conditions were met last time.

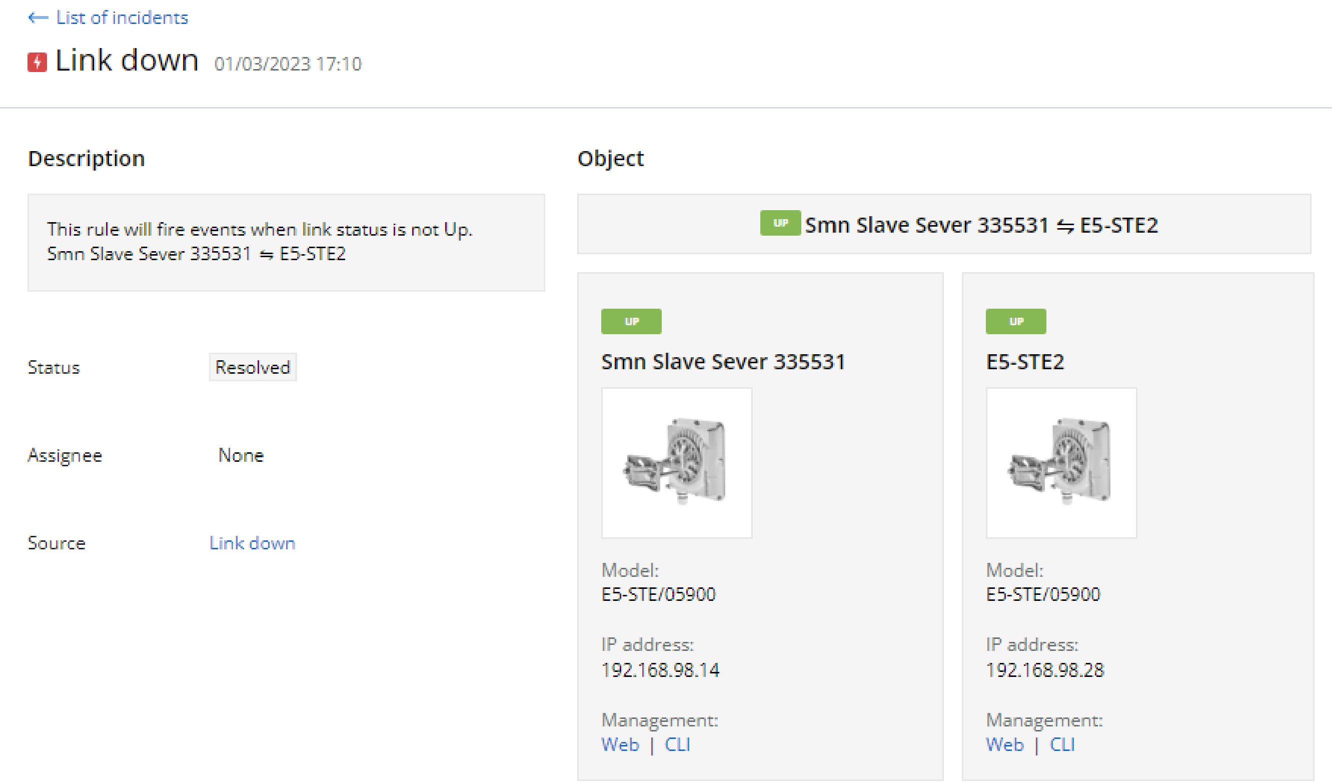
By default, all incidents are sorted by date, therefore the new incidents will be displayed first.

> ⚠ **Note**
>
> In order to display an incident time correctly, it is necessary to set date and time on the virtual machine where **InfiMONITOR NEXT** is installed. Time settings can not be made in the monitoring system.

Incident profile

A profile contains the following detailed information:

- **Description** - the device or link for which the incident was generated will be displayed here. Also there is a description from the appropriate rule.
- **Status** - current incident status.
- **Assignee** - user responsible for handling the incident.
- **Source** - rule title.
- **Scheme**:
  - Device incident - additional information about the device, including its status, model and IP address.
  - Link incident - additional information about the devices connected to the link for which the incident is generated.
  - There is possibility to switch to the web interface of each device or to manage it via the command line.
- **Comments** - comments added by engineers to this incident.



← List of incidents

Link down 01/03/2023 17:10

Description

This rule will fire events when link status is not Up.
Smn Slave Sever 335531 ⇋ E5-STE2

Status	Resolved
Assignee	None
Source	Link down

Object

UP Smn Slave Sever 335531 ⇋ E5-STE2

UP
Smn Slave Sever 335531

Model:
E5-STE/05900

IP address:
192.168.98.14

Management:
Web | CLI

UP
E5-STE2

Model:
E5-STE/05900

IP address:
192.168.98.28

Management:
Web | CLI

Figure - incident profile

Incident processing

Incident processing - one of the incident's lifecycle stages (see Incident management). An incident is processed when a responsible person is assigned to it:

- Superadmin and Admin users can assign incidents to other users in the visibility area corresponding to the device for which the incident was generated. The Superadmin user can not become an assignee.
- A user can assign an incident to himself, thereby making himself responsible for eliminating the cause.

To accept an incident, the user must click on the "**Take on**" button in the incident profile. This will lead to the following changes:

- The incident's status will change to "**In service**".
- The incident will be assigned to the user, which will be reflected in the "**Assignee**" field.

Incident will be resolved automatically after eliminating the cause. In this case the rule conditions won't be met and incident will be closed with status "**Resolved**".

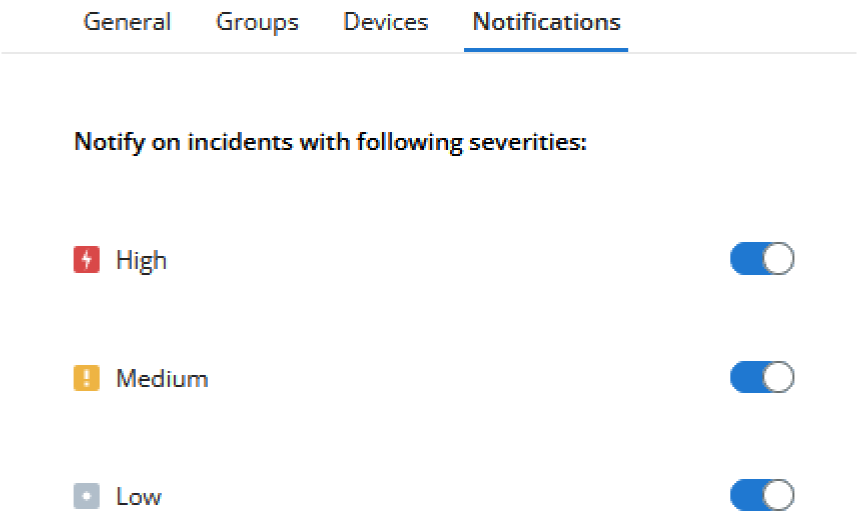
Engineers can leave comments in the incident profile that will be visible to other engineers, whose visibility area includes the particular device.

Incidents notifications

The monitoring system users can receive notifications about incidents. To activate notifications, configure the connection to the email server (see System configuration).

InfiMONITOR NEXT sends notifications containing incidents related to the devices and wireless links in the user's visibility area. Notifications are sent every 30 seconds and include all changes, accumulated during this time period.

Notification settings are available in "Notifications" section of user profile.



General | Groups | Devices | **Notifications**

Notify on incidents with following severities:

- High ☑
- Medium ☑
- Low ☑

Figure - Notifications settings

Here the user can select the incident severity levels for the notifications he wants to receive.

The "**Group**" option activates joining of several incidents with the same severity level into one notification. In this case each notification will include incidents with the same severity only.