

# Incident management



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

[To the certification exam](#)

- Incidents
  - Severity
  - Life cycle
  - Visibility areas
- Rules
  - Structure
  - Device groups
  - Rule conditions
  - Rule creation

All incidents in **InfMONITOR NEXT** are generated according to the rules that describe the conditions under which the incidents should be created.

## Incidents

### Severity

The incident's severity helps network engineers to correctly prioritize the problems identified by the monitoring system in the wireless network. The higher the priority, the more important is the problem. **InfMONITOR NEXT** provides 3 levels of severity:

- **High** - maximum importance. Indicates critical issues leading to a failure in the wireless network.
- **Medium** - medium importance. Indicates problems that do not have a critical impact on the wireless network functioning, but require the network engineer's attention.
- **Low** - low importance. Information messages that require the network engineer's attention, but do not affect the functioning of the wireless network.

The priority is defined in the incident generation rule.

### Life cycle

An incident's life cycle includes several stages described in the table below.

Stage	Incident status	Description
<b>Fulfillment of the rule condition</b>		The incident condition specified in the rule is met, confirmation procedure is started. Incident is not created at this stage.
<b>Confirmation of the incident</b>		Fulfillment of the rule condition will be checked during the confirmation time. If condition is met for the entire time, an incident will be created. If the condition is not met at least once, an incident is marked as not confirmed and its lifecycle ends.
<b>Incident creation</b>	Open	Created incident may be assigned to a responsible person. In this case incident will be moved to the "Incident processing" stage. Otherwise the rule condition fulfillment will be checking periodically during the regular polling cycle. If the condition is not met at least once the incident will be moved to the "Confirmation of the incident resolving" stage.
<b>Incident processing</b>	In service	Responsible person performs actions to eliminate the incident reason. The rule condition fulfillment is checking periodically during the regular polling cycle. If the condition is not met at least once the incident will be moved to "Confirmation of the incident resolving" stage.
<b>Confirmation of resolving</b>	Open / In service	Fulfillment of the rule condition will be checked during the confirmation time. If condition is not met for the entire time, incident will be moved to the "Closure" stage. Otherwise incident will be moved back to the previous stage: "Incident creation" or "Incident processing" depending on whether a responsible person is assigned or not.

## Title

Closure	Resolved	This stage is final, the incident is resolved.
---------	----------	--

"**Resolved**" status is final and means that the incident was closed. If the incident conditions are met again, a new incident will be created.

## Visibility areas

The incident will be available to the monitoring system user only if the device is in the user's visibility area.

## Rules

### Structure

Each rule has the following structure:

- **Title** - an arbitrary rule name.
- **Severity** - the importance which will be assigned to the created incident.
- **Description** - an arbitrary description, which will allow faster understanding of the incident's nature.
- **Device groups** - device groups that are assigned to the rule and for which incidents will be created.
- **Incident conditions**:
  - **Trigger conditions** - one or more conditions, combined by logical operators.
  - **Confirmation time** - time period during which confirmation of incident is performed.

### Device groups

Each rule contains the list of device groups for which it will be applied. There are the following categories may be used to define the rule scope:

- **All device groups** - the rule will be applied to devices of all groups.
- **Specified groups** - the rule will be applied to devices of selected groups.
- **Excluding groups** - the rule will be applied to devices of all groups groups excluding selected ones.

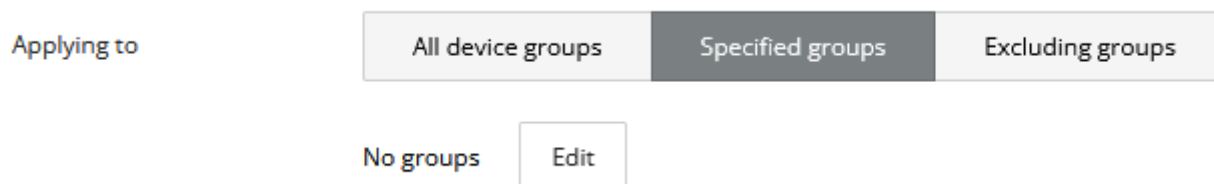


Figure - incident rule scope

### Rule conditions

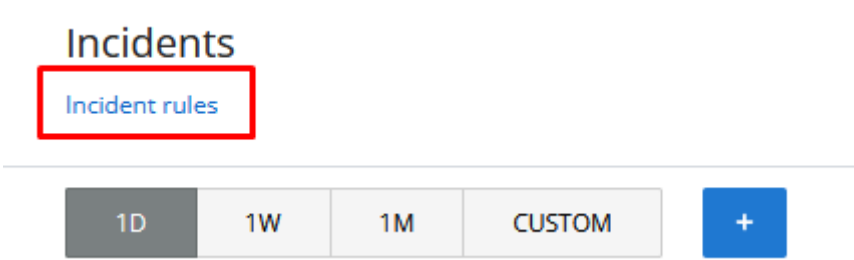
Each condition is described by the following parameters:

1. **Window function** - applied to a set of metric values, collected during the confirmation time. Example: window size is set to 20 minutes, during which 4 polling cycles were performed with the following set of results "23, 52, 31, 15". Window function "Max", applied to this set will give the value "52", "Min" - 15, "All" - "23, 52, 31, 15" etc.
2. **Metric** - the metric which will be used in the condition.
3. **Operator** - operator for comparing the threshold and current metric values.
4. **Value** - reference value which will be used to compare with actual value metric.

Confirmation time - time period during which confirmation of an incident is performed. At this period the polling frequency of the corresponding device is increased to one per minute.

### Rule creation

Incident rules are managed in the "**Incidents**" section - "**Incident rules**":



By default, there are two rules added to **InfimONITOR NEXT**:

- **Host down** - the incident will be created if the network host's status goes DOWN.
- **Link down** - the incident will be created if the wireless link's status goes DOWN.



Правило	Описание	Группы
 Host down	This rule will fire events when host changes status to oth...	Default Group Auto-Discovered Devices XG Evo
 Link down	This rule will fire events when link status is not Up.	Default Group Evo XG Auto-Discovered Devices

Figure - Incident rules by default

To create a new rule, click on the **"Add new rule"** button. Fill the form:

1. rule title;
2. incident severity;
3. description;
4. device groups.

The next step is to specify the conditions for the incident creation. The reference value set by the rule's conditions will be compared with the actual value obtained during the polling process of the wireless device.





For example, it is necessary to generate incidents when CPU load exceeds 75% during 5 minutes and memory usage is not less than 50%. For this, in the incident condition, we should set the following values:

- In case there are more than one condition you should set the **"Must complete"** parameter to **"All conditions"** value.
- The **"Max"** window function with window size of 15 minutes should be used for both conditions. It means that the maximum value will be used from all values collected during 15 minutes.
- Comparison operator should be used for **"CPU load"** and **">="** for **"Memory usage"**.
- Confirmation time is 5 minutes.

Incident condition

Must completeAll conditionsAny condition

Conditions

Window function	Metric	Operator	Value	Window size (minutes)	
Max	CPU load	>	75	15	 
Max	Memory usage	>=	50	15	 

+ Add new condition

Confirmation time (minutes)5

Figure - incident condition example

To complete the rule configuration, click on the **"Save"** button. The rule will be used starting with the next polling cycle of the wireless device.