# Network Olympus Documentation

Search this documentation


## Network Olympus: Monitoring

# Techpaper



## List of terms

Dashboard: web interface or workspace of Network Olympus which opens after a successful login. Contains the header, the current panel, widgets and the status bar.

Panel: space that contains widgets. Each panel stores information about the location of its widgets.

Widget: key element of the dashboard. Each widget type performs a particular function.

## Minimum system requirements for the server

| | |
|---|---|
| CPU | 4 CPU Cores |
| RAM | 8 GB |
| Disk Space | At least 300 MB. The amount of space required for installation + additional space for a growing database.<br>Monitoring of a single device will produce about 300 MB of data per year. |
| Network | TCP/IP |
| OS | Windows 7 / Server 2008 or newer |

## Network Olympus Web Interface

Web Interface supports the following HTML5-enabled browsers:

- Google Chrome
- Safari
- Mozilla Firefox
- Microsoft Edge

## Requirements for remote devices

| Sensor category or type | Requirements |
|---|---|
| NetBase | Appropriate protocol support and deployed TCP port availability |
| WinBase and System | Windows NT4, 2000, XP Pro, Vista, 7, 8, 8.1, 10, Server 2000/2003/2008/2012(incl R2)/2016; administrator rights; ipc$, admin$ resources |
| Registry key | "Remote registry" service |
| WinBase (apart from Registry key) | RPC protocol, open TCP port 135, "Windows management Instrumentation" (WMI) service |
| FileSystem | NetBIOS and SMB protocols, open TCP ports 445 and 139 |

# FAQ



## Q: How do I get started?

A: After installing Network Olympus, you can start from the Network tree dashboard or go to the Scanner. A few demo devices have already been added to the tree automatically. They are placed in groups Local Network and Remote (Demo). If you need to just add a few devices, create a group in the network tree and add devices using the context menu. If you want to scan the local network and add all the discovered devices to the tree, go to the Scanner panel and scan the domain or IP range using the Scanner status widget.

To check specific parameters or device uptime, you need to add sensors. Sensors can be added using the network tree context menu or from the Scenario builder dashboard. From here, you can also add notifications and actions that can be performed depending on the monitoring results.

The other dashboards will help you keep an eye on sensors and executed actions and track their stats. The most comprehensive information on all elements and their status is available in the Activity log.

## Q: I already own one or more of Softinventive Lab's products. May I count on a discount when purchasing Network Olympus?

A: Of course. We're grateful for your confidence in our products and ready to provide a discount for Network Olympus.
For detailed information, see this page.

## Q: Can I use the database that I already have?

A: Yes, it's enough to select your database during the Network Olympus installation.
At the moment, the app supports only PostgreSQL.
More information is available here.

## Q: How can I find which port numbers are used for WinBase & FileSystem checks, so I can configure the firewall?

A: WinBase sensors use the RPC protocol. Make sure that TCP port 135 is open. When using Windows Firewall, it's enough to enable a special exception entitled "Windows Management Instrumentation (WMI-In)".

FileSystem sensors use the SMB and NetBIOS protocols. They can be allowed by enabling the File and Printer Sharing exception in the Windows Firewall or TCP ports 445 and 139 in other firewalls.

# Free/trial version limitations

Network Olympus is distributed as shareware.

## Trial version

The evaluation version has 1 limitation: the program only works in this mode for 60 days after its first launch on a computer.

The number of devices and sensors is unlimited.

To view the trial period end date and other license information, click on the application version on the left side of the Status bar. This will open the license information panel (About Network Olympus).

Upon reaching the end of the trial period, the Free mode will be activated.

## Free version

The free version is not limited by time, but has 1 limitation: you can monitor up to 10 devices.

# Discounts for TNI, TNM and TSD users

Most users of commercial Softinventive Lab products are eligible for a discount on any Network Olympus license.

To request a discount, please contact us at sales@softinventive.com

- Each Total Network Monitor 2 user is eligible for a 50% discount on any Network Olympus license.
- Each user of a Total Network Inventory or Total Software Deployment license with the number of nodes higher than 25 is eligible for a 30% discount for a Network Olympus license with the corresponding (or lesser) number of devices.

  Please refer to the following table to find out which license you can get a discount for:

| TNI STD/PRO or TSD | Network Olympus |
|---|---|
| 25 nodes | 25 devices |
| 50 nodes | 50 devices |
| 100 nodes | 100 devices |
| 150 nodes | 200 devices |
| 250 nodes | 300 devices |
| 350 nodes | 500 devices |
| 500 nodes | 500 devices |
| 750 nodes | 1000 devices |
| 1000 nodes | 1000 devices |
| 1500 nodes | 1500 devices |
| 2000 nodes | 2000 devices |
| Unlimited | Unlimited |

  For example, owners of the TNI Standard 150 nodes license are eligible for a 30% discount for Network Olympus for 200 devices, as well as for 100 devices.

  However, the discount will not be lost if a higher license is needed. It will be calculated as 30% from the license corresponding to the one they own. For the above example, that means that any license higher than 200 devices will be discounted 30% * [price for 200 devices].

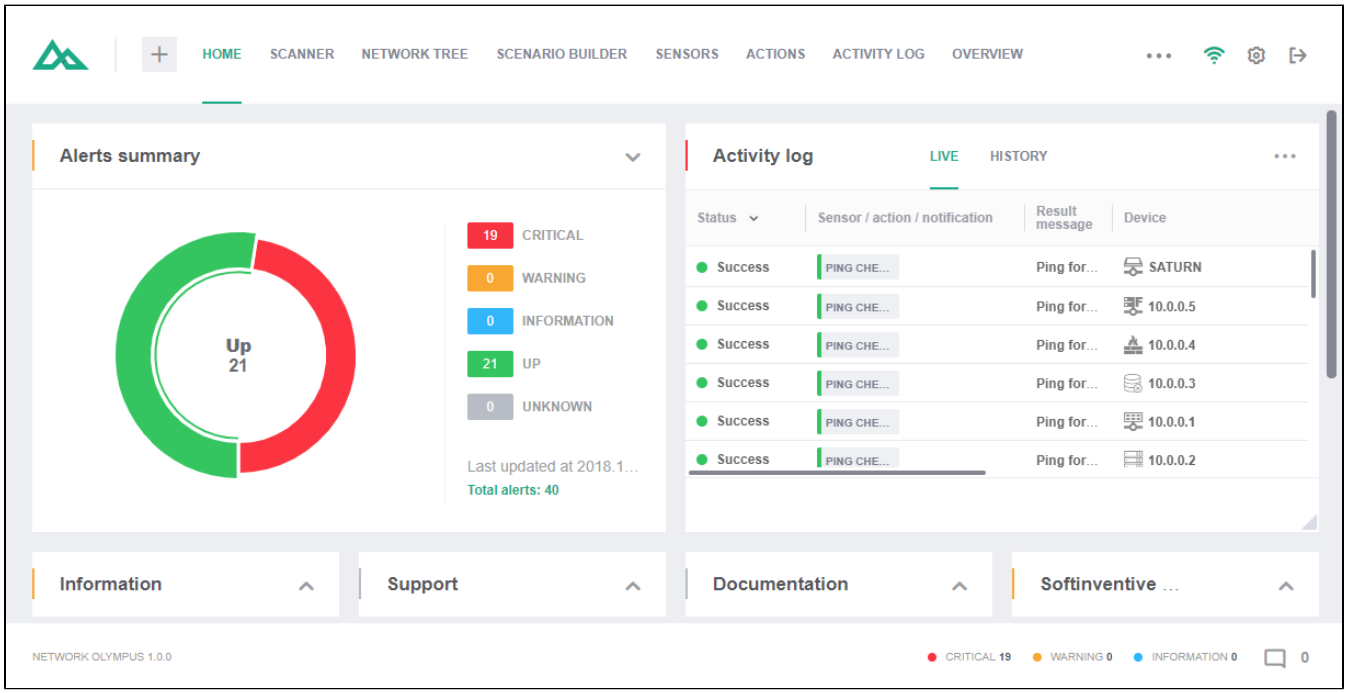
# Workspace



When you run the Web application, you must first log in.

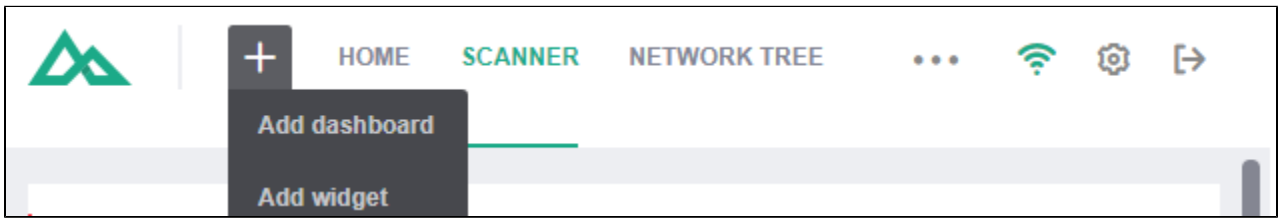
More information about logging in can be found in the Authentication section.

The user interface is loaded immediately after a successful login.




## Page header

The header contains the dashboard management panel.




From here, you can switch between various dashboards, as well as create new dashboards and widgets.

On the right side of the header is the indicator of connection status with the Network Olympus web server.
You can also access program settings here.

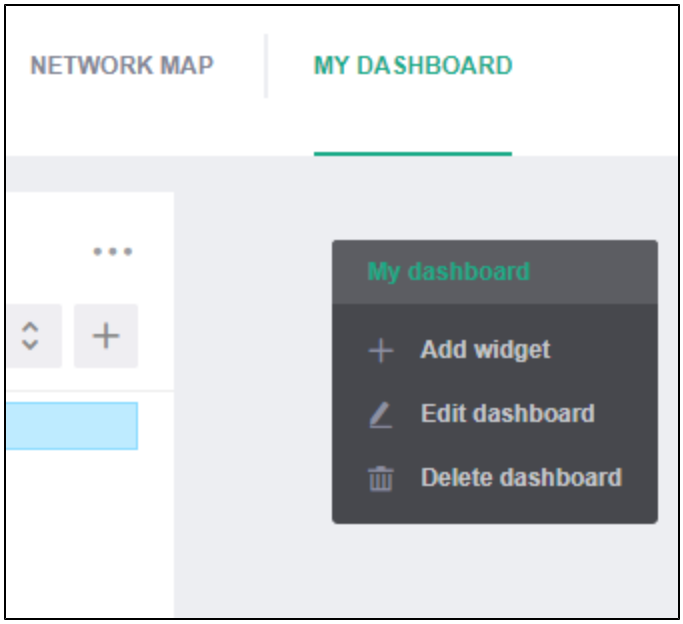
## Dashboards and widgets

A dashboard is a separate space that contains widgets. Each dashboard stores information about the location of the widgets.

A widget is a key element of the interface. It displays specific information or allows you to perform certain actions.

Widgets can be moved similarly to the way you move windows. Widget positions are automatically aligned in the grid.

Use the + button in the header to add an empty dashboard or to add one of the widgets to the current dashboard.
Widgets can also be added using the context menu in the empty space of a dashboard.




Any widget can be minimized and expanded from a menu in its top right corner. You can open its settings from here too.

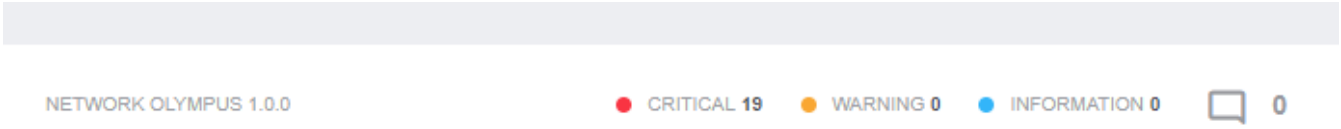
> Most widgets contain clickable information. You can view details or edit objects such as sensors and devices.

## Status bar

At the bottom of the page is the status bar.

The application version is displayed on its left side.
You can open the license information panel by clicking on the version.

To the right, information about the sensor statuses is displayed, sorted by their severity.
This area is also used to display system messages to the user.
A sidebar containing the previously shown system messages can be opened from here.



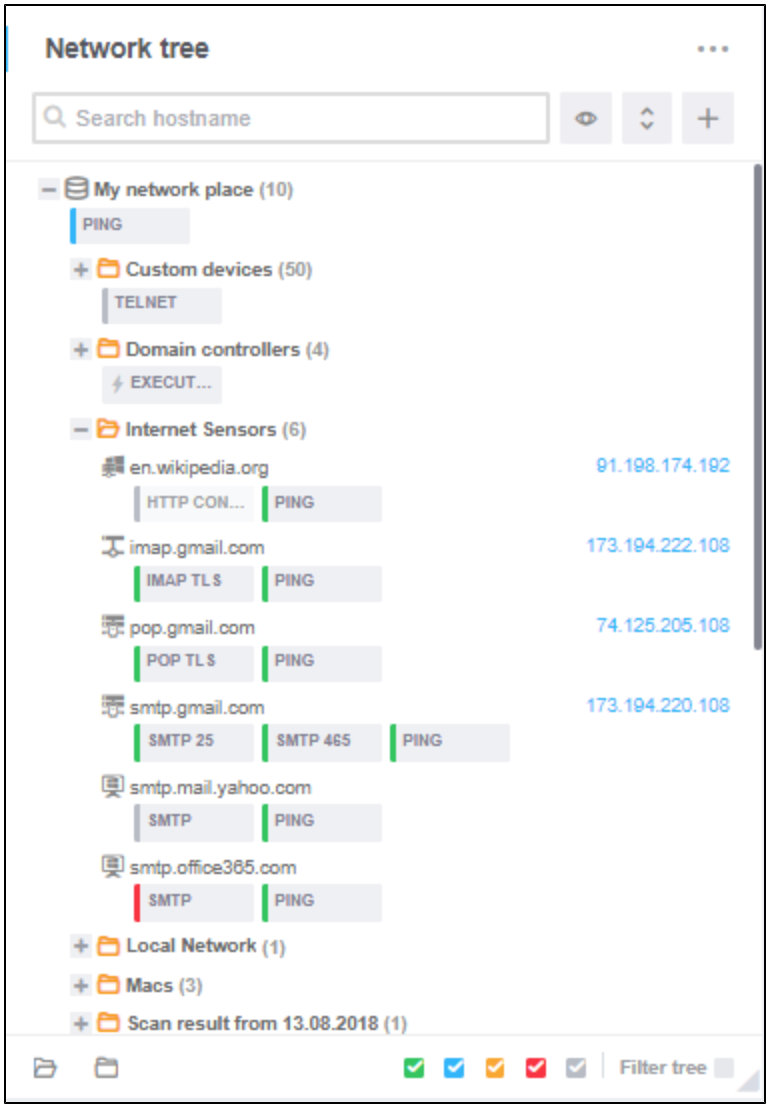
# Network tree



The Network tree is the main management widget. Here, the hierarchy of monitoring objects is displayed.

Groups and devices serve as nodes in the tree.

Sensors and actions assigned to each node are displayed below it.




## Devices

Devices correspond to actual network devices that can be monitored.

Each device has a number of attributes, or parameters: address, network name, OS, etc.

The easiest way to fill the tree with devices is to scan the network.

You can also add devices manually using the Network tree context menu or the + button at the top of the widget.

## Groups

Groups allow to build a hierarchical structure that will lead to a more effective monitoring scenario.
They can include both devices and other groups.

The system provides an ability to import the existing Active Directory structure. More information can be found in the Adding scan tasks section.

Related topics:

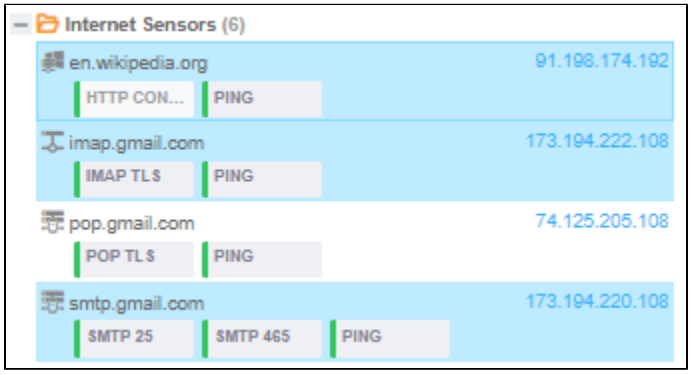
- Selecting a node
- Information display settings
- Searching in the Network tree

## Selecting a node

You can select one or multiple nodes when you need to delete or move them to a different group.

Use left click to select a node. To select multiple nodes, press and hold Ctrl.

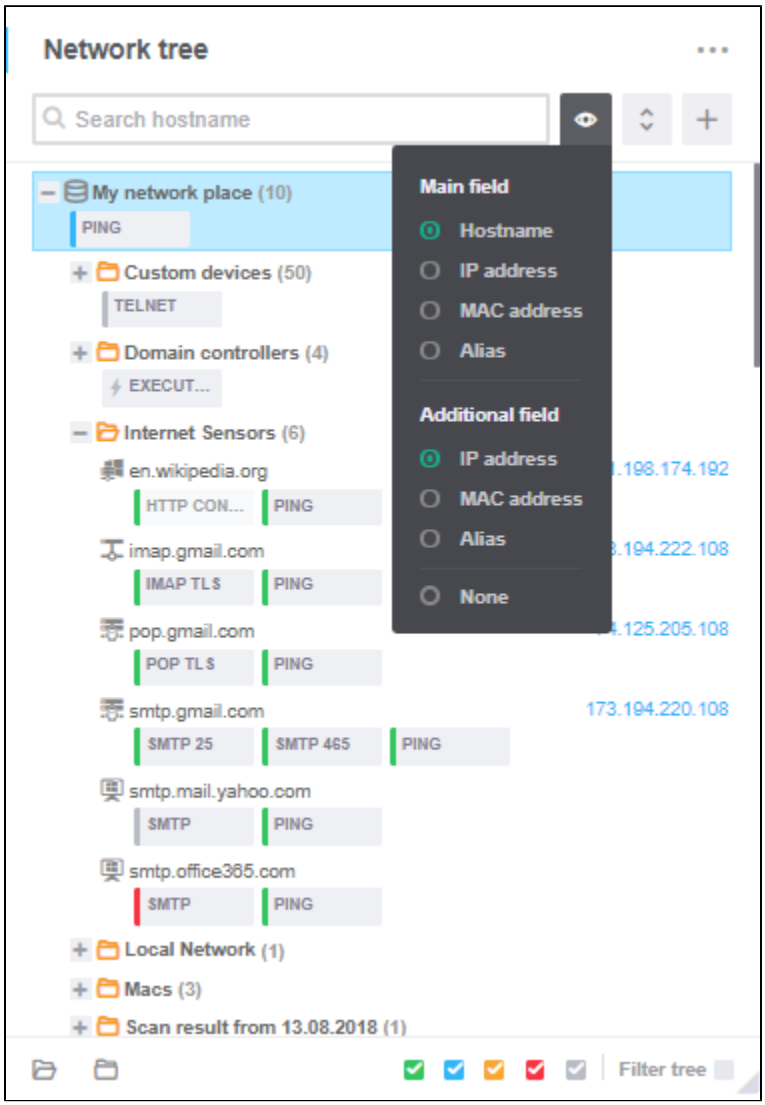
The selected nodes will be highlighted with the blue background:



# Information display settings

The displayed name for each device in the Network tree can be chosen in the Visualization mode menu on the Network tree toolbar.

By default, hostnames are displayed in the main field and IP addresses in the additional field:




Only values displayed in the main field are used when searching in the network tree.

## Main field

The value displayed in the main field serves as the device name. One of the four main device properties can be displayed as the device name: network name, IP address, MAC address, alias.

> If the Alias is set as the device name, you can rename devices from their properties.

## Additional field

An additional value can be displayed in the Network tree for every device. One of the following can be selected: IP address, MAC address, alias.

## Sorting the nodes

To the right of the Visualization mode, select the sorting criteria: nodes can be sorted either by the displayed device names or by the additional field values, with an option to reverse the sorting order.

## Filtering the sensors

The displayed sensors can be filtered by their current status and severity using the checkboxes in the bottom right part of the widget.

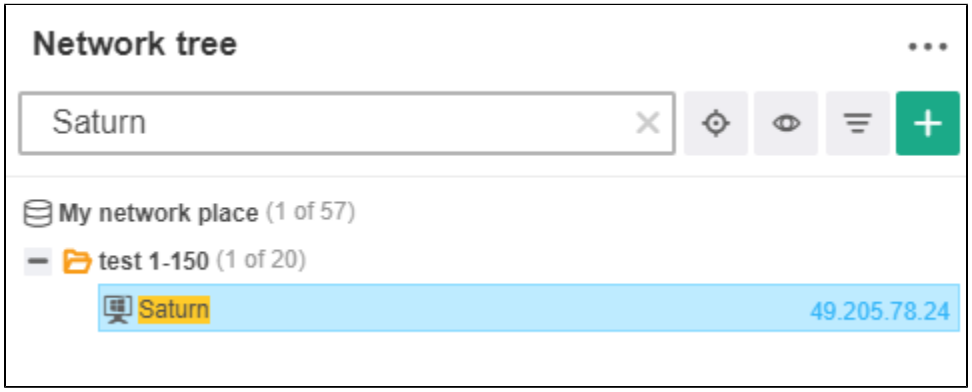
Here on the left, you can collapse and expand the group nodes.

## Searching in the Network tree

Use the Search field to quickly find nodes in the Network tree.

After pressing Enter, the contents of the tree will be filtered.

Devices can be searched only by their main field values (see Information display settings).



# Network scanning

Scanning is the process of retrieving information about devices in the network and about its logical or physical organization.

Network scanning is performed from the Scanner status widget.

When the system starts, the scanner automatically creates scan tasks for the network elements detected while analysing the environment.

These can be the available IP ranges for installed network adapters, an Active Directory domain, or a workgroup (if the computer where Network Olympus is installed is a member of them).

Related topics:

- Adding scan tasks
- Scan process and scan results

# Adding scan tasks



To initiate a scan, use the Scanner status widget.

The scan results are displayed in the Scanner log widget.

## Scanner status

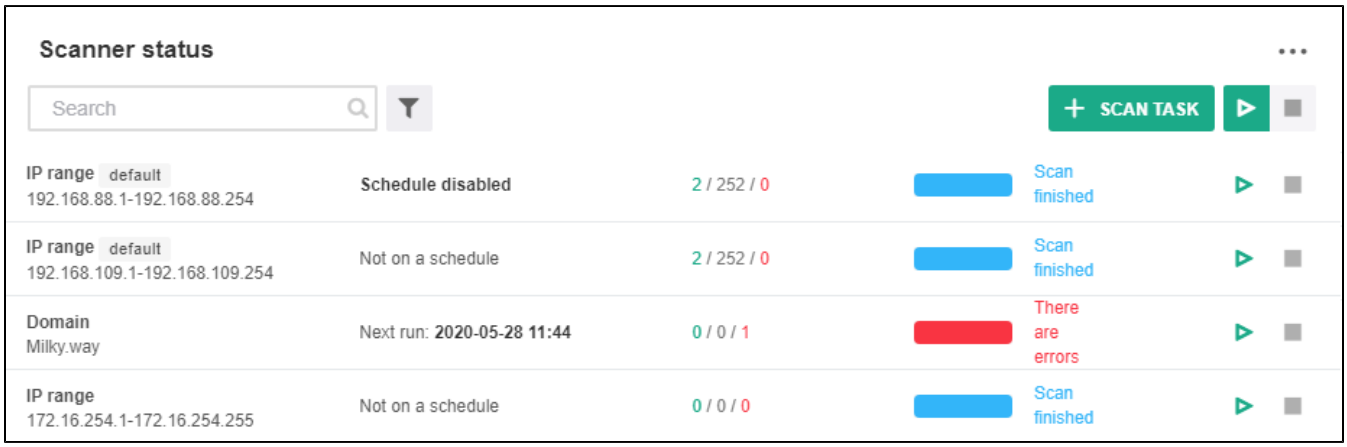
Scanner status allows to quickly run scan tasks set up by you or automatically by the scanner at system startup.

Quick scan options are available in the widget's main area.

Quick scan doesn't require any additional configuration.

You can start one of the suggested scan tasks or all of them at the same time.

Clicking Scan task allows to add more tasks.




The widget displays the following information about each task in 4 columns:

- summary (type, scan target and the default tag if the task is created automatically) – click to edit the task;
- time of next run – click to add or edit the schedule;
- number of successfully and unsuccessfully scanned devices – the totals for all tasks are displayed in the bottom panel;
- current task status – click to view information about the last scan.

The search field and filters can be used to find scan tasks.
Filtering criteria include the origin of the task (default or custom) and the target type (IP range, domain or workgroup).

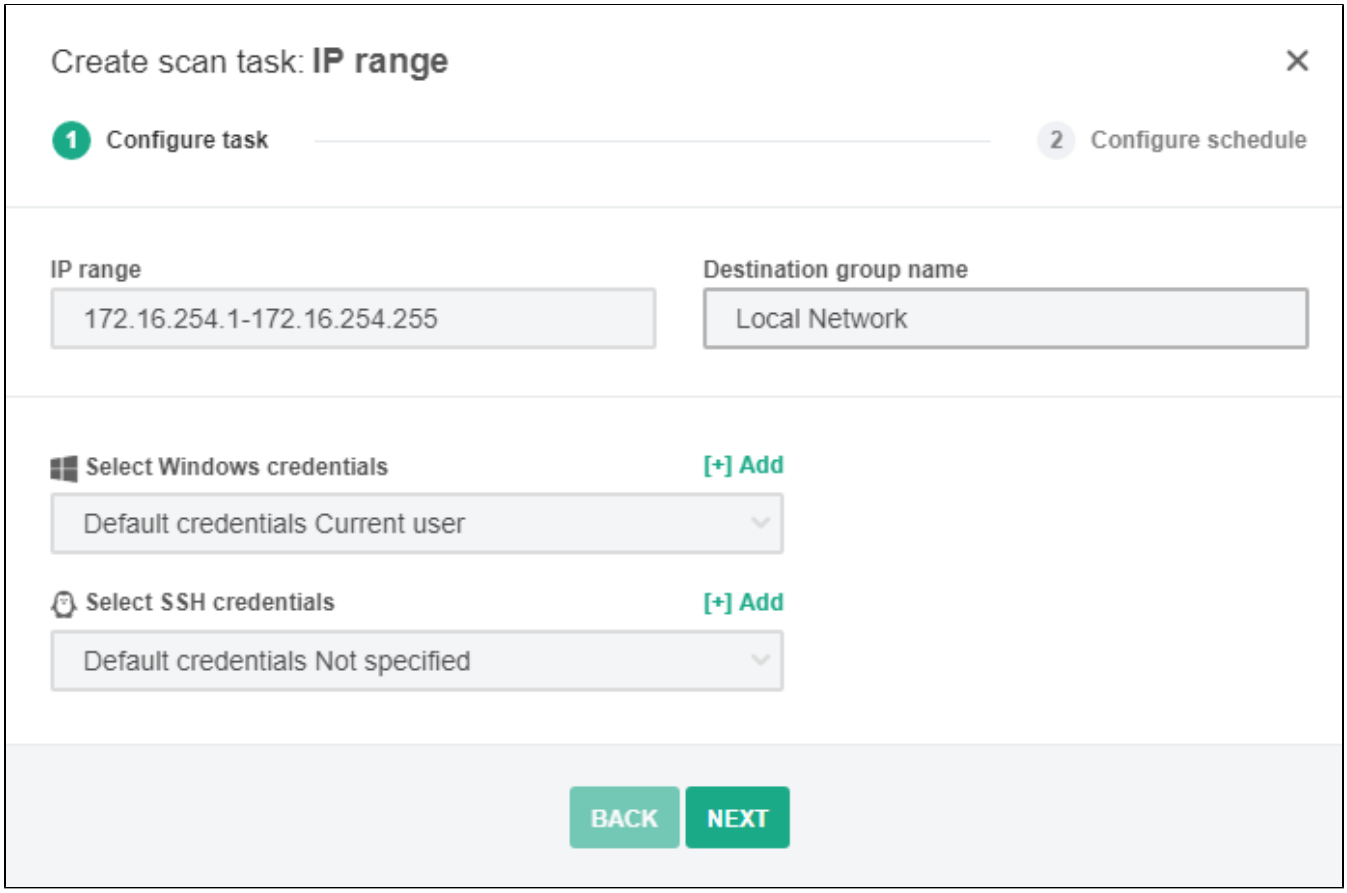
## Adding custom tasks

You can create custom scan tasks:

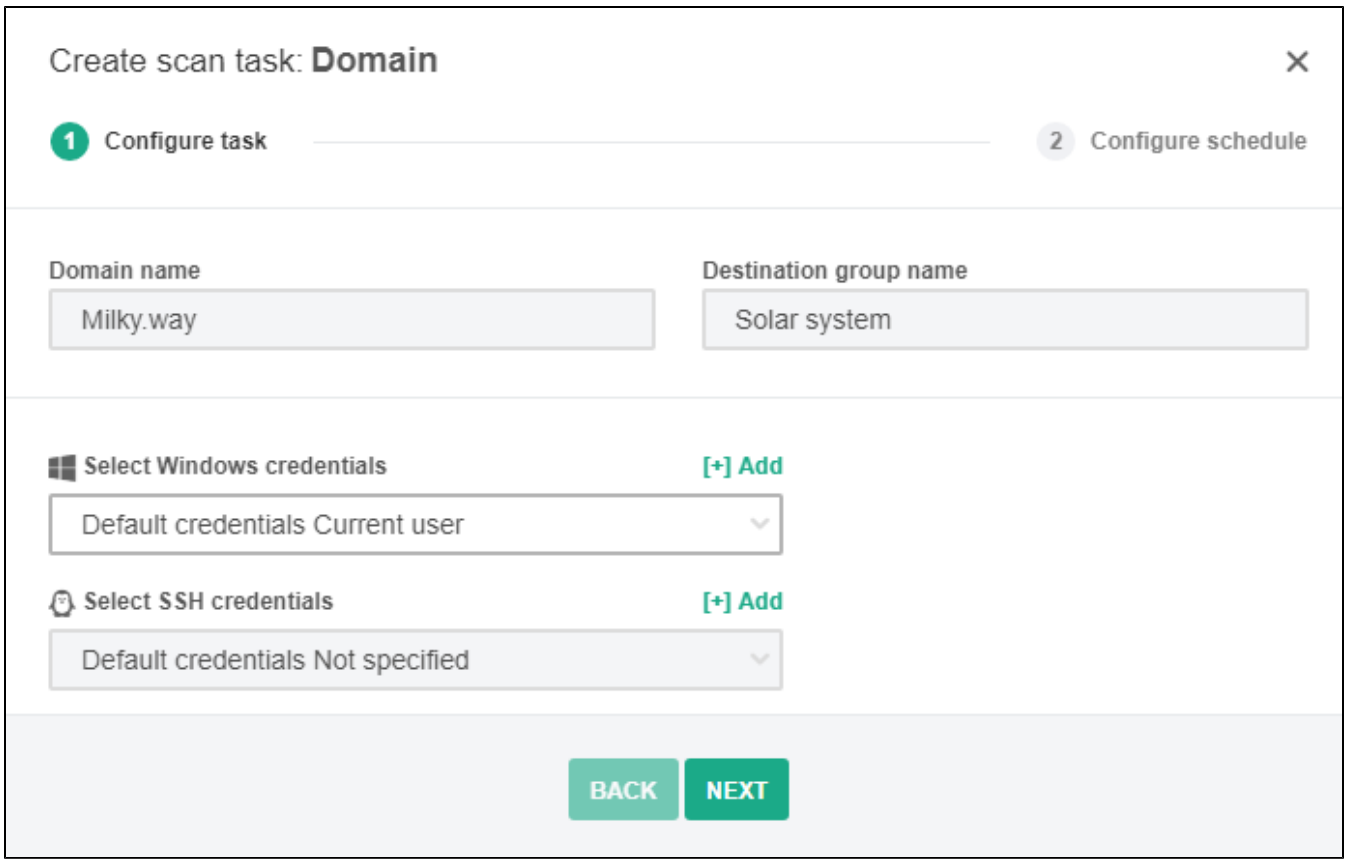
- for IP ranges;
- for workgroups;
- for Active Directory domains.

For this, click Scan task.

For any task, you must specify the name of the network tree group where the scan results will be placed.

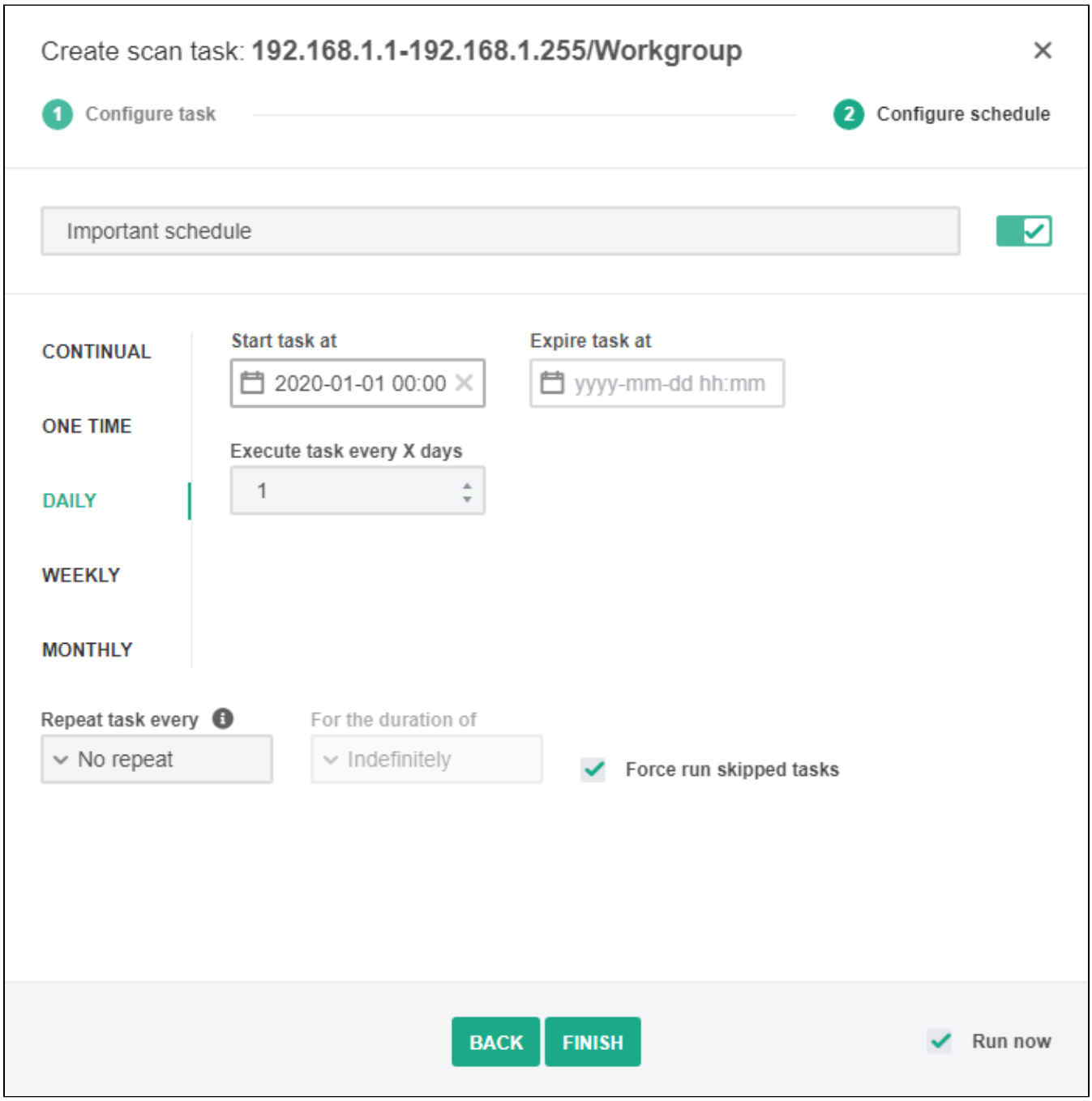



For domain tasks, authentication may be required.




You can also configure periodic scanning.

The way the scan scheduler works is described in detail in the corresponding section.



# Scan process and scan results



## Scan process

Initially, Network Olympus pings each discovered target device. When a device is resolved, the scanner checks if a matching object already exists in the network tree and either updates the existing object or creates a new device. The resulting action concerning each discovered device is written into the scanner log.

Devices can be distinguished from one another by one of the three criteria (you can choose which criterium should be used in the program settings):

- by MAC address (the default setting);
- by IP address;
- by hostname.

If a matching object already exists, its properties are updated.

You can monitor and control the scanning process in the Scanner status and Scanner log widgets.

## Scanner log

All scan events are stored in the system and are viewable in the Scanner log widget.

The following information about scan events is available:

- event status;
- nature of the event and what device is involved;
- scan task where the event was generated (click it to view the details);
- event timestamp.

The Scanner log widget can work in two modes:

- Live
- History

### Filtering events

Scanner log allows to filter events by various criteria corresponding to the displayed columns with information.

To activate the filters, change the filter status indicator (ON/OFF) in the widget's header.

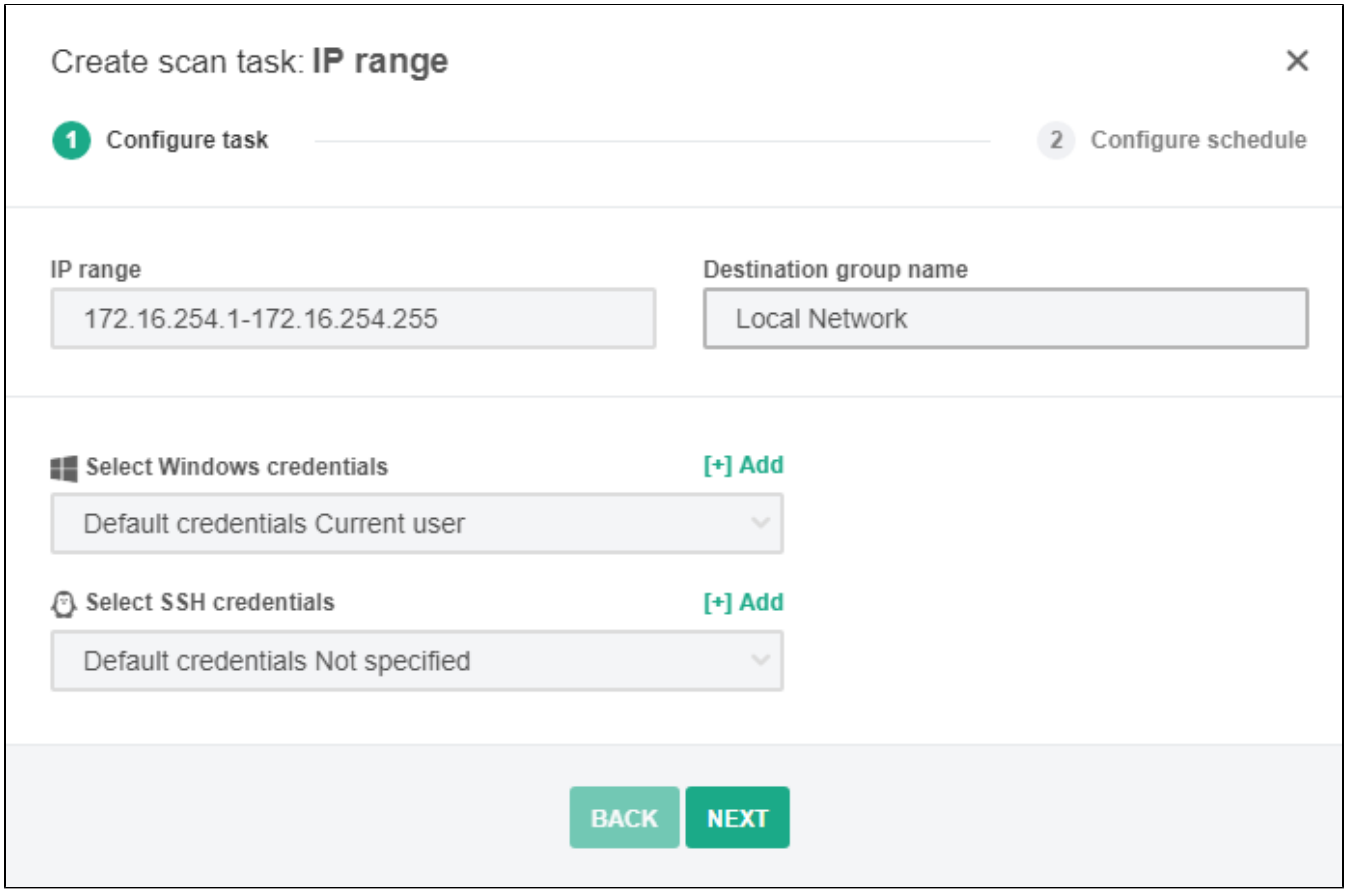
A panel will appear containing all filter types. You can combine different filters for more accurate results.

> The Event time filter can only be activated in the History mode.

## Scan results

New devices are placed into a separate group in the network tree. The existing structure of the network tree will remain unchanged.

You can specify the name of the destination group when manually setting up a scan task.



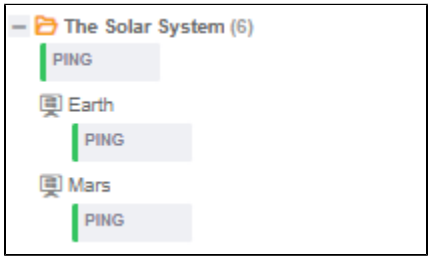

If no new devices are found, then the group is not created.

# Monitoring

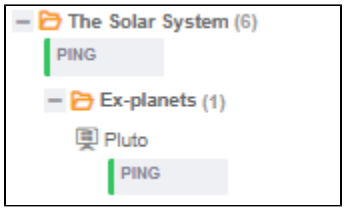
The main goal of the application is network monitoring. It involves multiple checks of various types for devices on the network and a response according to the results of these checks.

For this purpose, the user creates sensors. Sensors track certain aspects of the device operation. Each sensor collects and analyzes information about the device, then evaluates the current state based on the user settings and, if necessary, notifies about possible issues.


Each sensor can monitor one node in the network tree. Thus, a sensor can be assigned to a device or a group.
If the sensor is assigned to a group, it will monitor and be displayed for each device in that group. This can be useful when a particular monitoring scenario is viable for multiple devices.
Therefore, to start monitoring a new device, it's enough to place it in a group to which the necessary sensors are already assigned.




If a group contains subgroups, then its sensors will also apply to all devices in the subgroups.




## Sensors can be started in three ways

- Manually:
  A manual start of a sensor initiates an immediate, single check.
  You can start a sensor once from its context menu in various widgets, for example: in the Network tree, in the Sensor list, etc.
- On schedule:
  In this case the Scheduler is used. It can be enabled when creating or editing a sensor, on the Configuration step.
- Based on the result of another sensor:
  Logic chains can be formed into a monitoring scenario to detect issues more effectively.
  With their help, various actions can be performed and notifications sent out depending on sensor results, and additional sensors can be run as well.

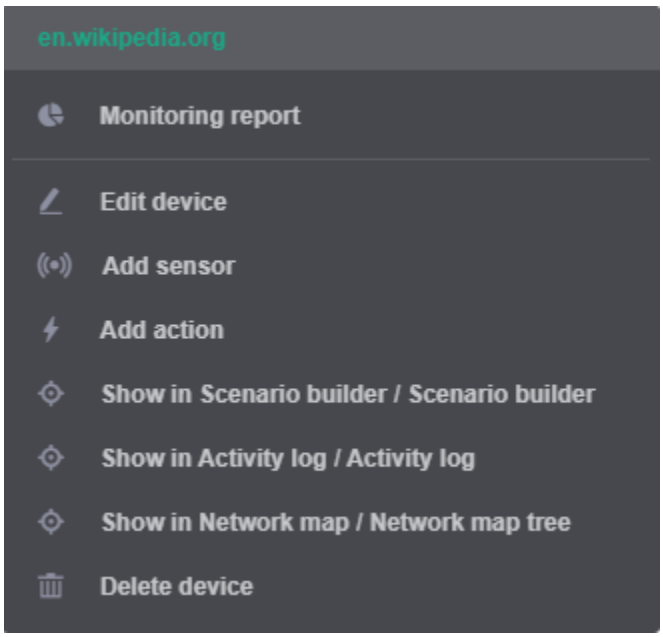
> Any sensor can be disabled. In such a case, it can't be run until reenabled from its context menu or editor.

Related topics:

- Creating sensors
- Setting up actions and notifications
- Monitoring results
- List of sensors, actions & notifications

## Creating sensors

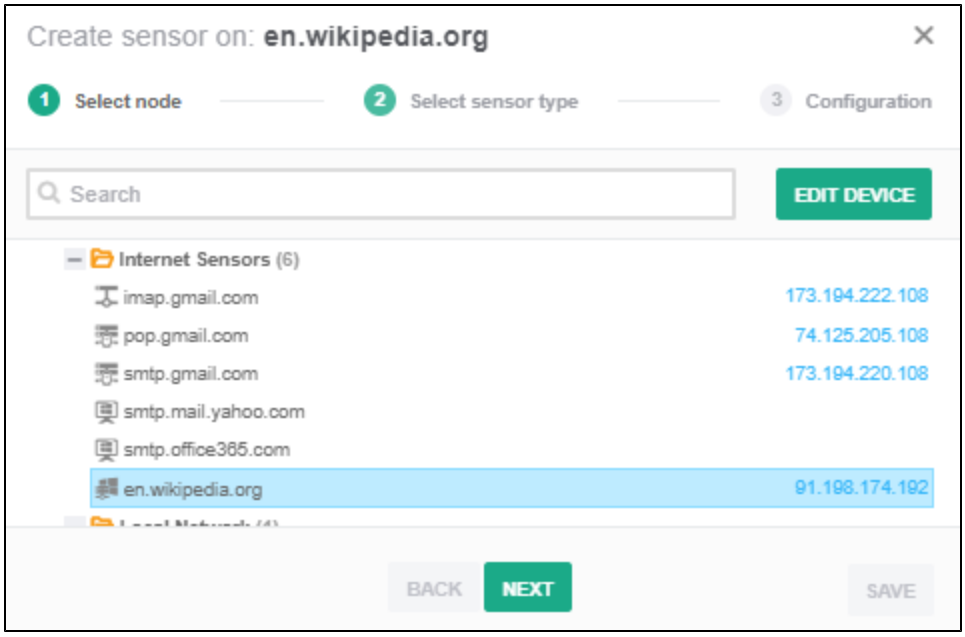
To create a new sensor, use the context menu of the device or group in the Network tree.



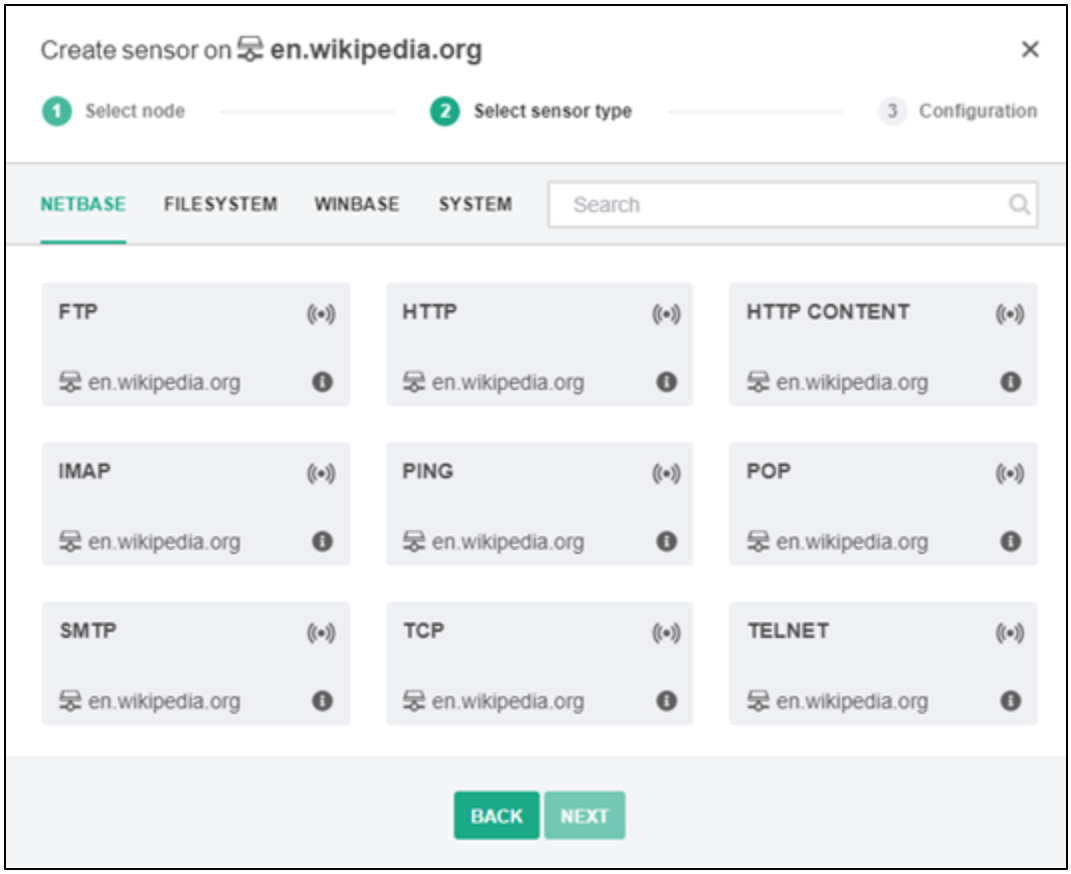

You can also create sensors when building monitoring scenarios.

A special wizard is used for sensor configuration.

The first step involves the selection of a network node for monitoring.
If the node is already selected, this step will be automatically skipped, but you can return to it if you need to select a different node.




On the second page, select the sensor type.
Use the four tabs to browse between sets of sensor types grouped by modules.

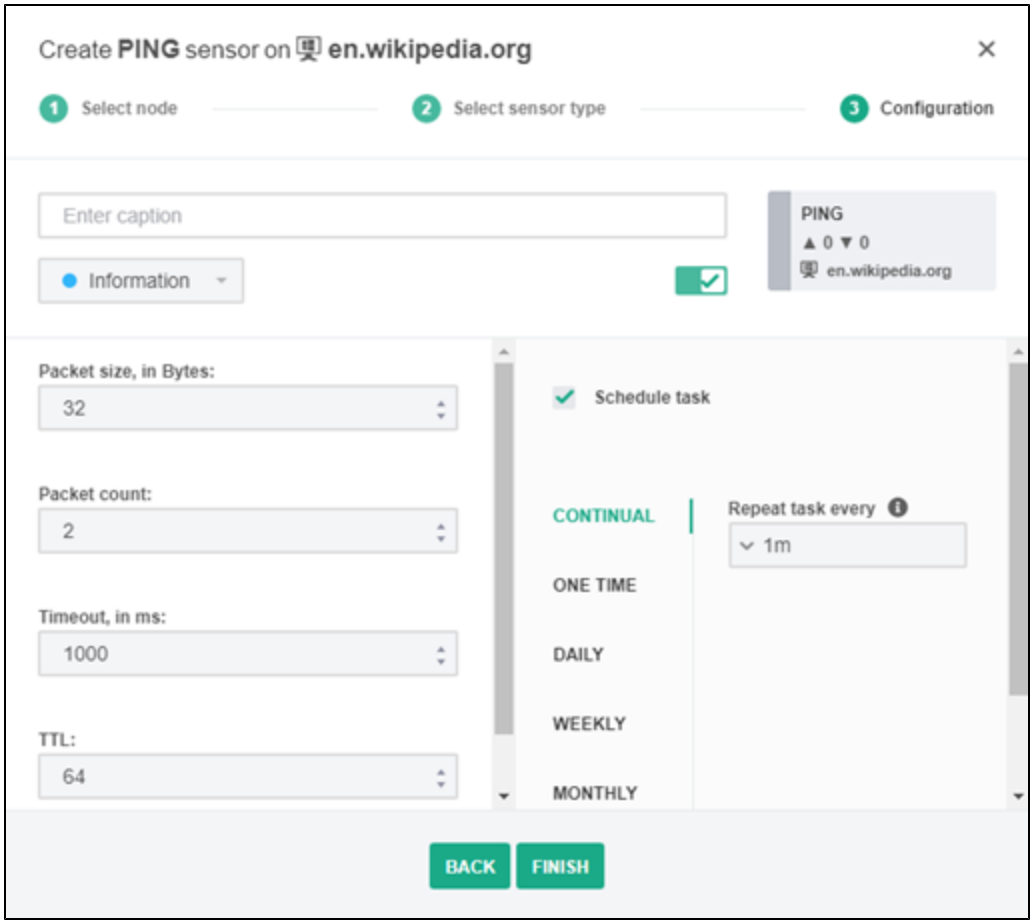



> Some sensors may request login information for authentication on the remote device.
>
> If the corresponding logins are not found, the wizard will prompt you to add a new login.
>
> For more information about how it works, see the Authentication section.

On the final step, you will be asked to set the parameters of the selected sensor, including its severity level.

You can also configure the periodic execution of the sensor using the Task scheduler here.

By default, the sensor is configured to run every minute starting from the moment the configuration is complete.




To view the complete list of existing sensors and information about them and to manage them, use the Sensor list widget located on the Sensors panel.

# Setting up actions and notifications



Actions are used to automatically correct problems and influence certain aspects of a local or remote system.

For example, you can restart an incorrectly functioning service, modify the registry by running a script, shut down the computer, and so on.

Actions are triggered by the results of sensors or other actions, as regulated by the monitoring scenario.

Like sensors, actions can also be started manually or on a schedule.

> Any action can be disabled. In such a case, it can't be run until reenabled from its context menu or editor.

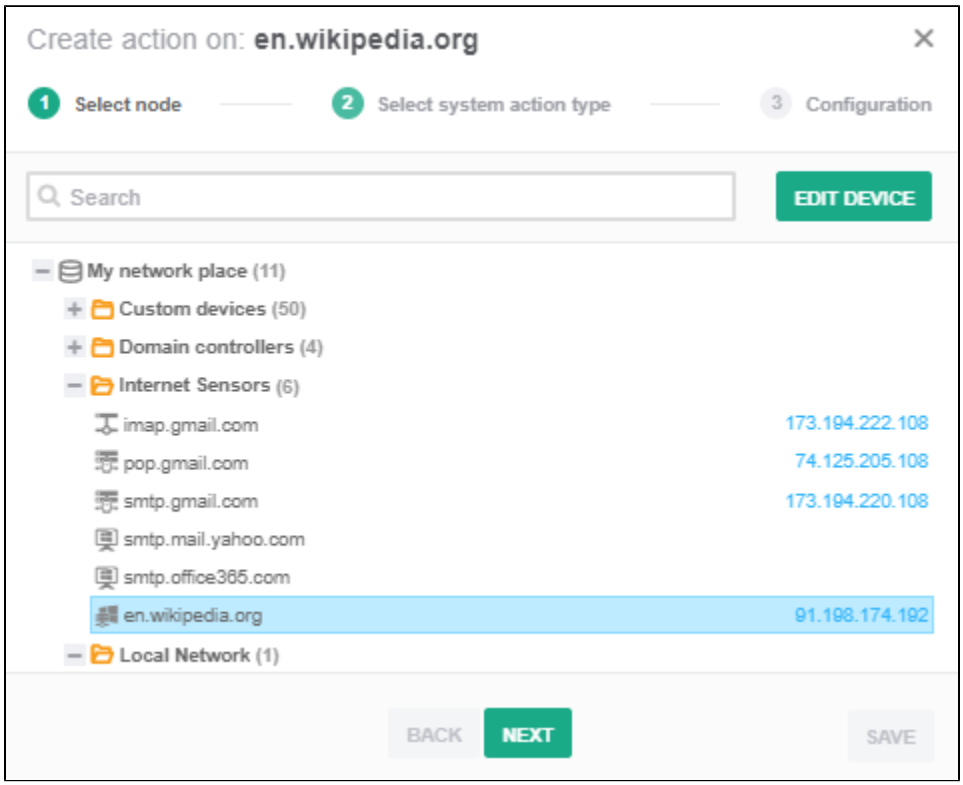
## Creating actions

To create an action and assign it to a sensor (or another action), use the Scenario builder.

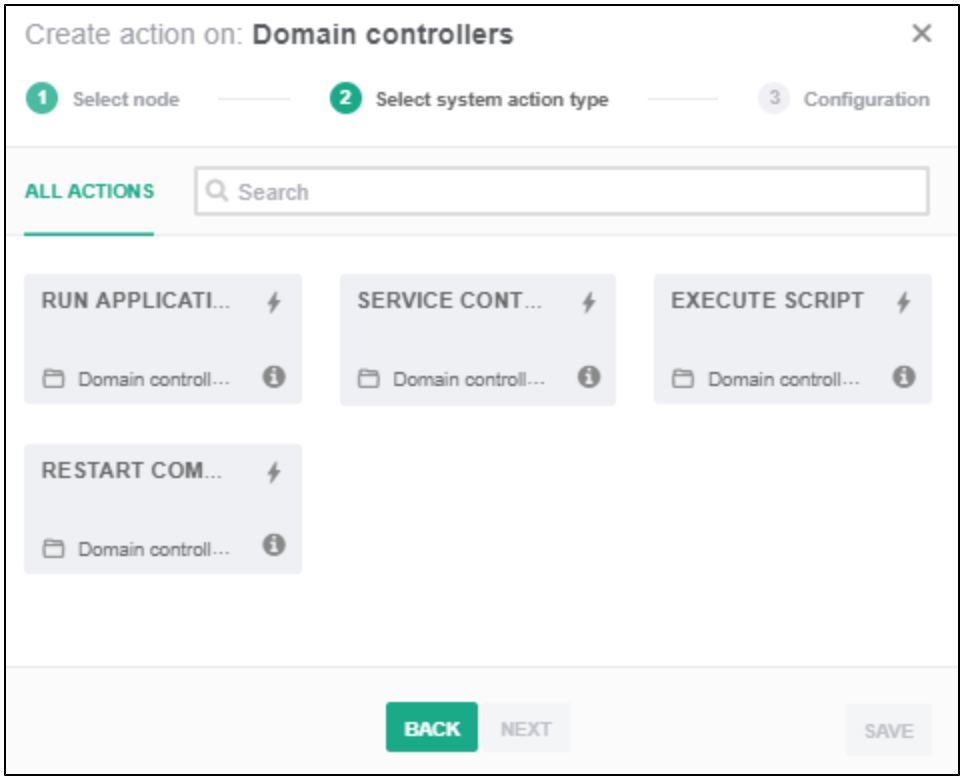
Actions can also be created and assigned to a specific device or group in the same way as sensors.
This can be done from the context menu of a device or group in the Network tree.

Whichever method is used, the action configuration wizard will appear.

The first step involves the selection of a network node where the action will be performed.
If the node is already selected, this step will be automatically skipped, but you can return to it if you need to select a different node.



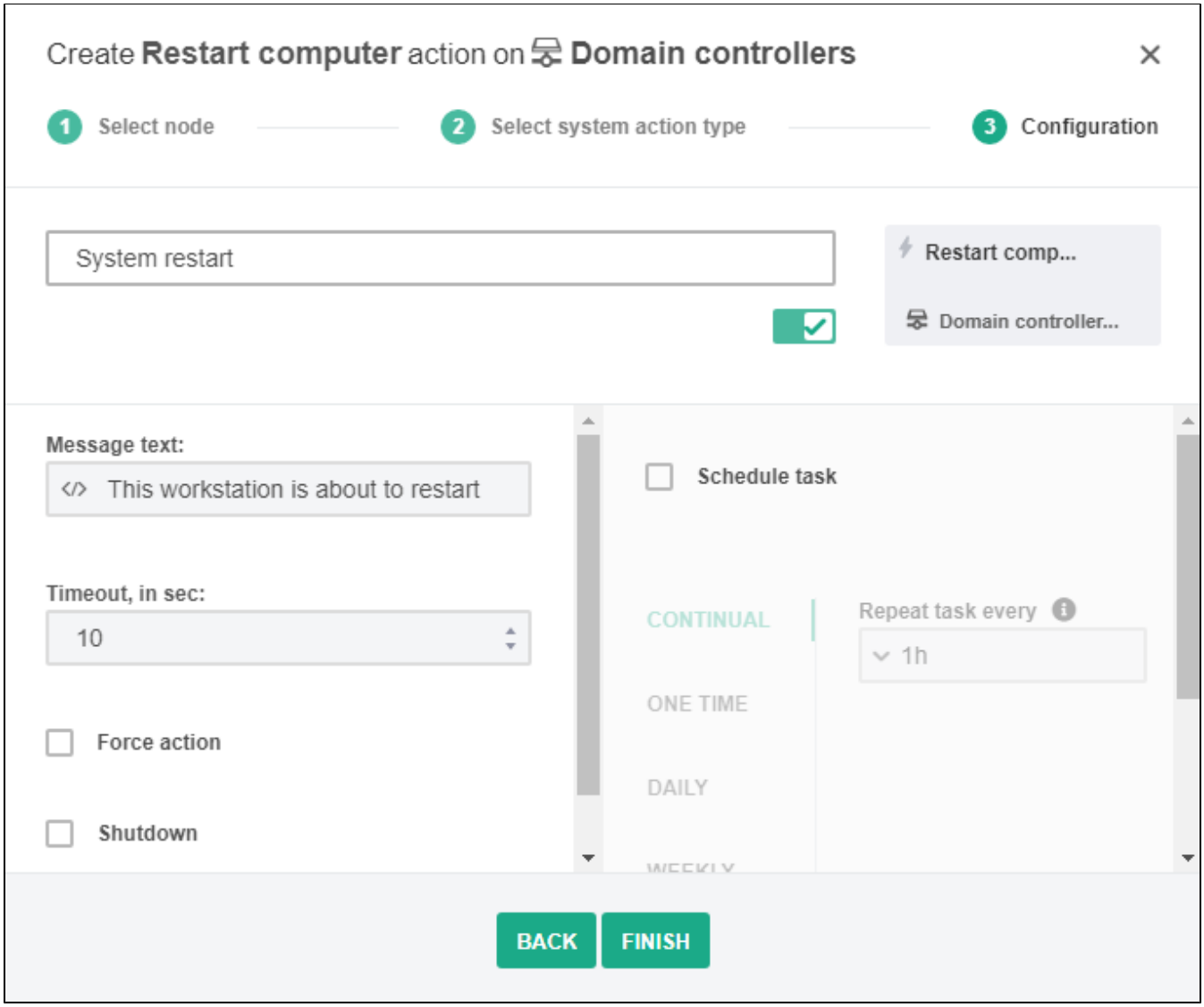

On the second step, select the action type.




> Some actions may request login information for authentication on the remote device.
> If the corresponding logins are not found, the wizard will prompt you to add a new login.
> For more information about how it works, see the Authentication section.

On the final step, you will be asked to set the parameters of the selected action.

You can also configure the periodic execution of the action using the Task scheduler here.




To view the complete list of existing actions and information about them and to manage them, use the Action list widget located on the Actions dashboard.

## Assigning notifications

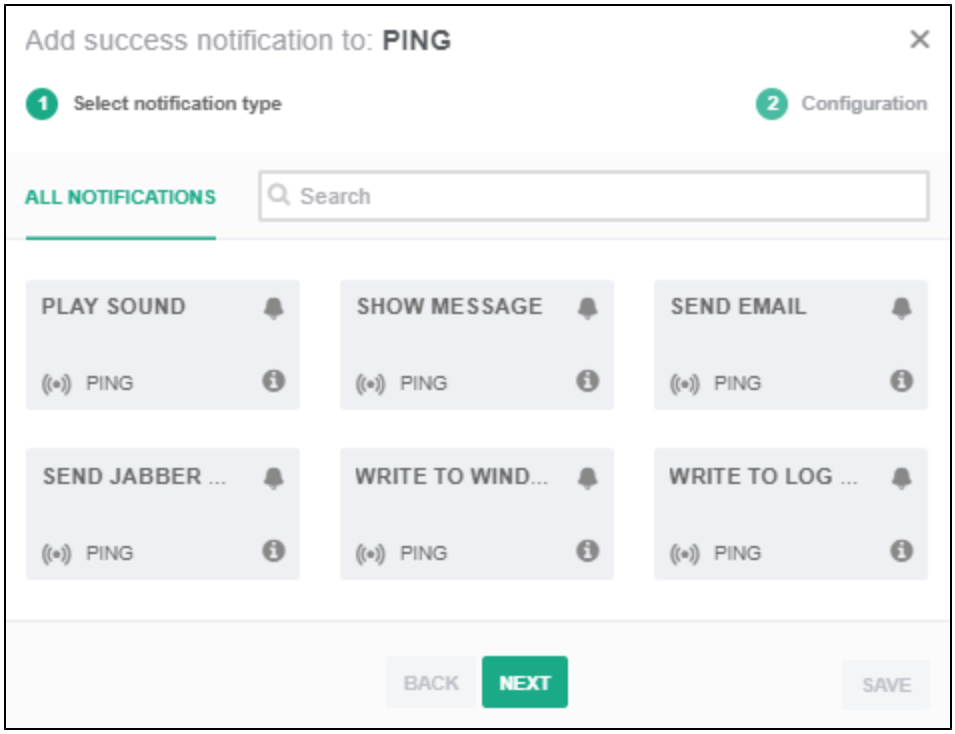
To instantly notify the appropriate personnel about sensor and action results, notifications are used.

Sensors and actions can be assigned any number of notifications that are executed after the checks or action operations are over, depending on the event status (Up/Down or Done/Failed).

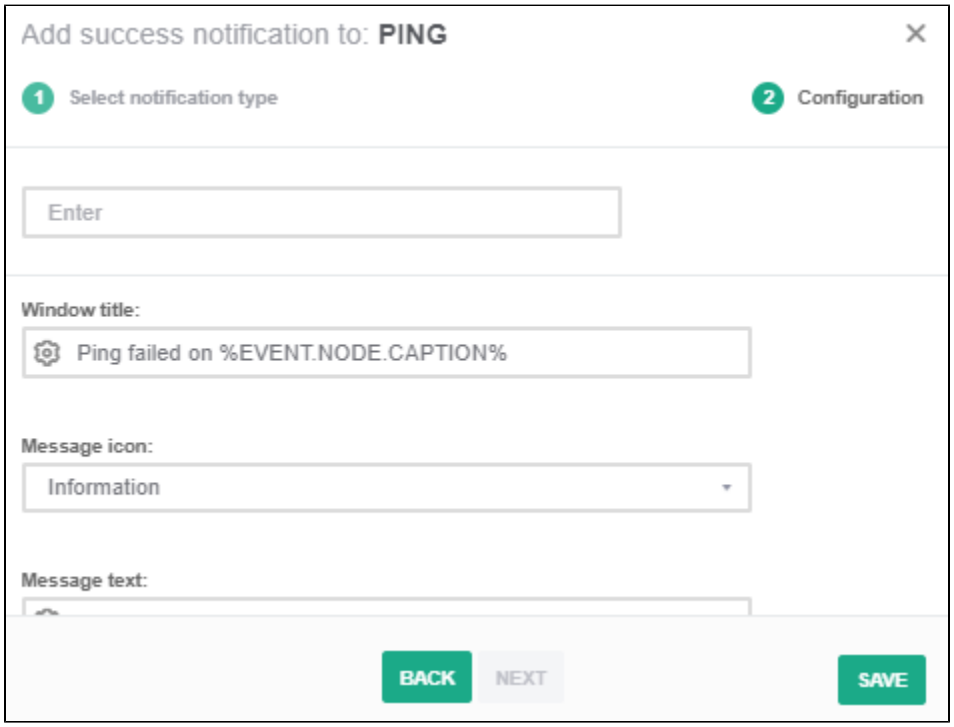
If a sensor or action is assigned to a group that contains multiple devices, then notifications will be sent for each of the devices based on the status of each event.

To assign a notification about the Up or Down (Done/Failed) status, use the context menu of the corresponding sensor or action.

On the first step, select the notification type.




Set the parameters for the selected type of notification on the second step.




To view the list of assigned notifications and change their parameters, edit the corresponding sensor or action and go to step 3 (Linked notifications). You can also add new notifications from here.

# Monitoring results



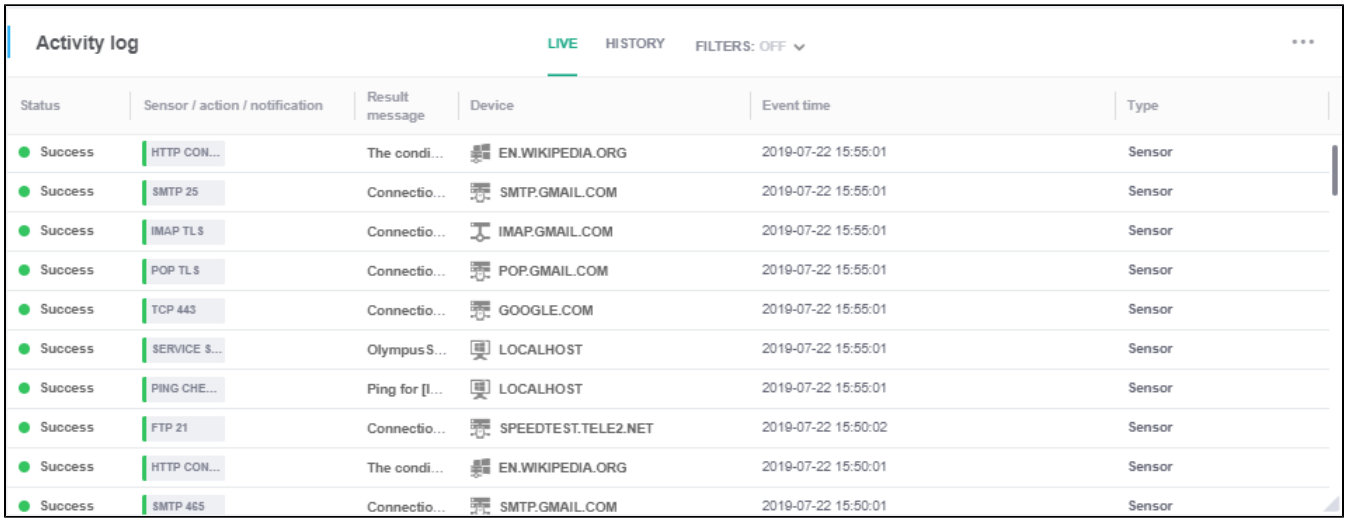
When a sensor or action is executed on a particular device, an event is produced. It contains information about the results of a single execution.

The event status determines the further monitoring scenario:

- UP or Done means that the sensor or action was executed successfully and the current state of the aspect checked by the sensor matches the set parameters.
- DOWN (Critical/Warning/Information) or Failed means that an error occurred during the execution of the sensor or action, or that the current state of the aspect checked by the sensor doesn't match the set parameters.

## Activity log

All events are stored in the system and are viewable on the Activity log dashboard where the corresponding widget is opened.




The following information about sensors and actions is available:

- event status (click it to view the details);
- date and time of execution;
- hostname and other properties of the corresponding devices;
- additional information about their operation or the cause of the error.

The Activity log widget can work in two modes:

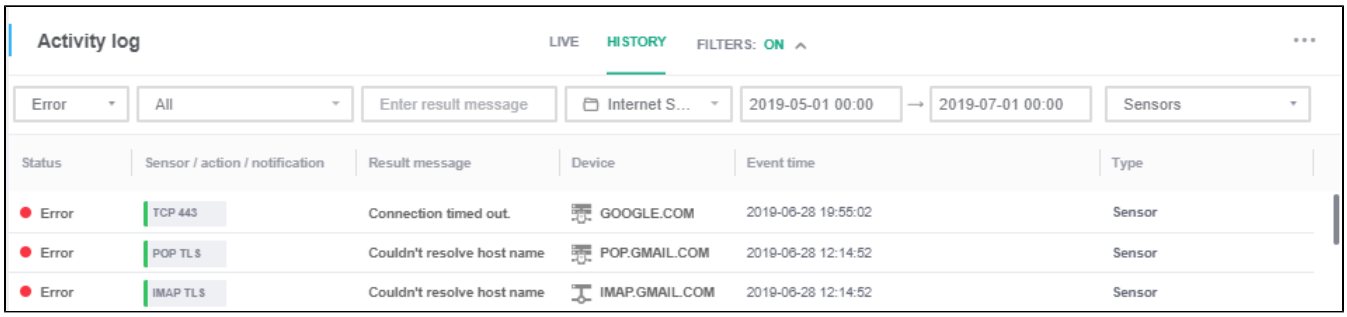
- Live
- History

### Filtering events

Activity log allows to filter events by various criteria corresponding to the displayed columns with information.

To activate the filters, change the filter status indicator (ON/OFF) in the widget's header.

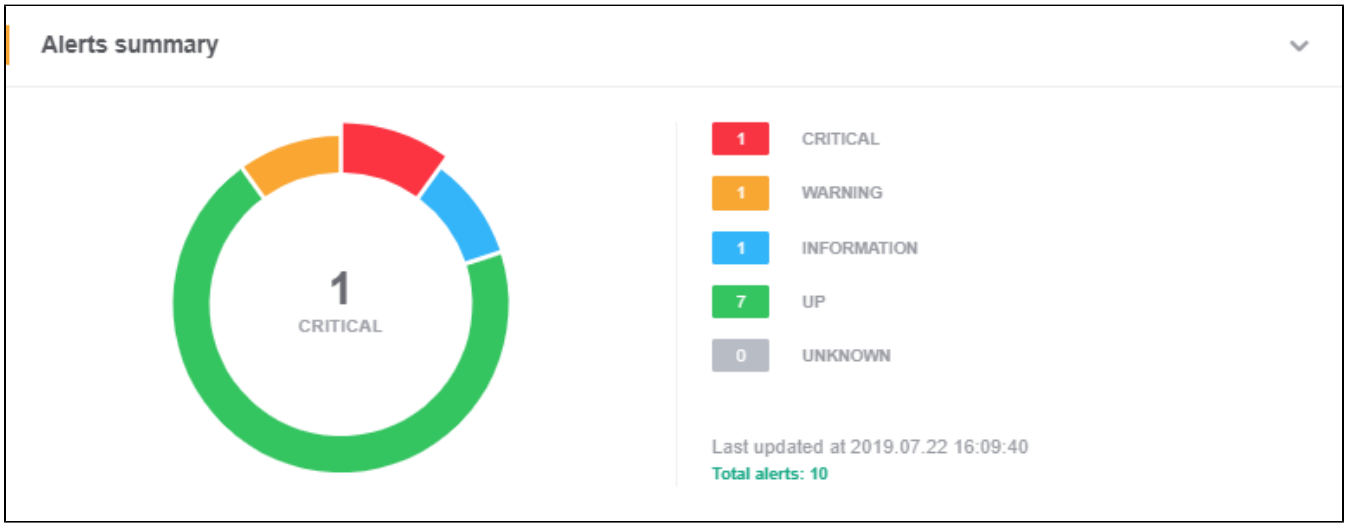
A panel will appear containing all filter types. You can combine different filters for more accurate results.



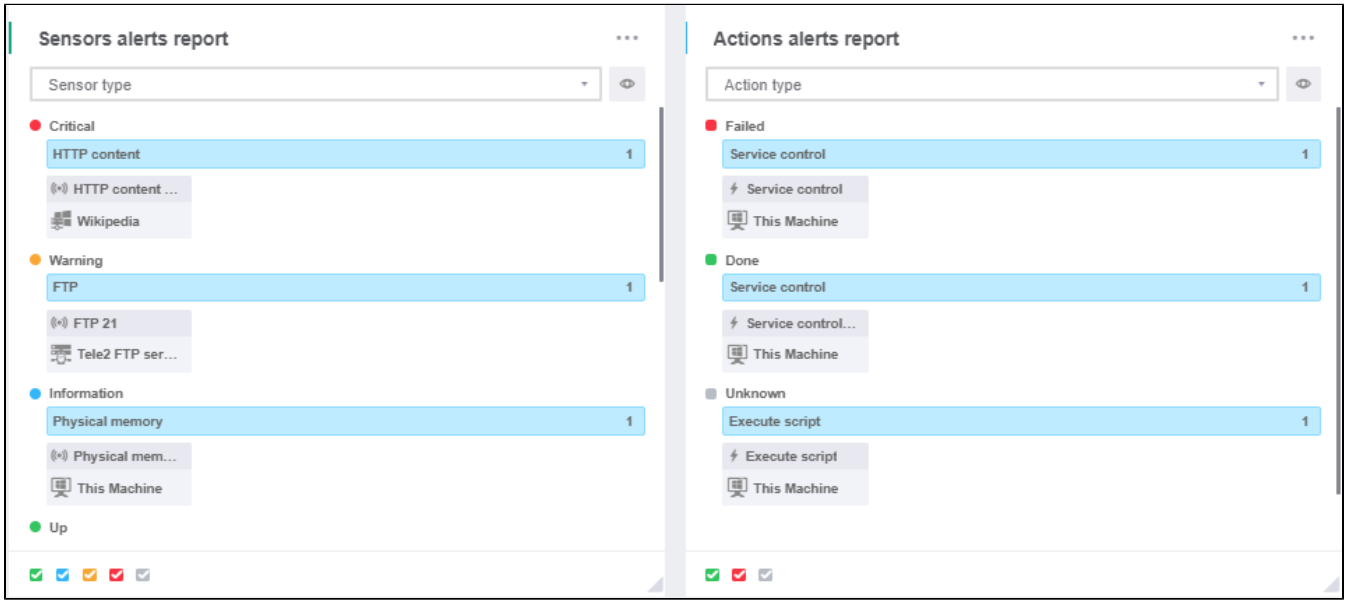
The Event time filter can only be activated in the History mode.

## Alerts summary and reports

On the Home dashboard, you can find a summary chart that shows what proportion of sensors currently has the Up status and the distribution of sensors with the Down status by severity.




The Overview dashboard includes the Sensors alerts report and Actions alerts report. These widgets allow you to generate reports showing information about the operation of existing sensors and actions, respectively.




Information in the reports is grouped by the current event status (and sensor severity), and it can be filtered using checkboxes on the bottom control panel.

On the top panel, you can also choose from the drop-down menu by what parameter sensors and actions will be further grouped.

In the Visualization mode menu, you can choose what information is displayed about the devices to which sensors and actions are assigned. You can select one of the four main device properties: hostname, IP address, MAC address or alias.

# List of sensors, actions & notifications

Please note that the Registry key sensor uses Registry service on remote computers. The sensor will not work if this service is stopped.



## Sensors

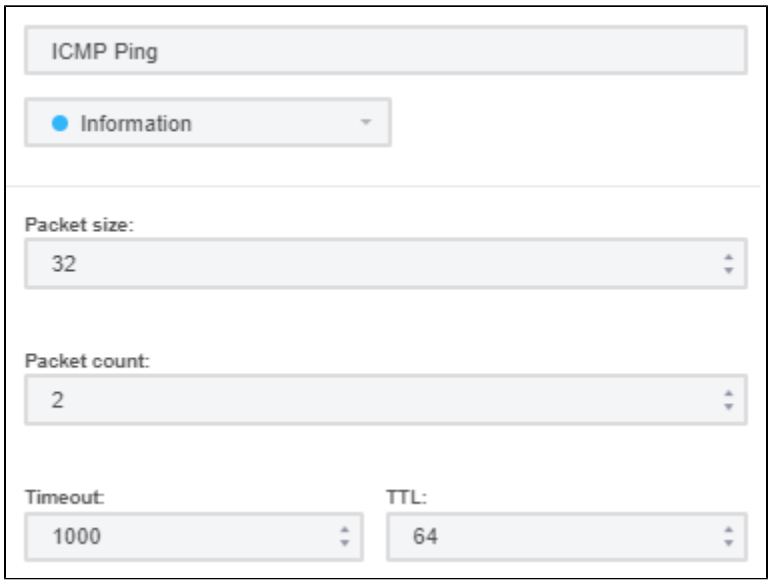
Network Olympus currently offers 23 types of sensors split into 4 categories.

### Netbase

Network sensors that allow to monitor the uptime and availability of remote hosts and local servers and workstations.

#### Ping

Allows to check if there's such a host on the network using the ICMP ping scanning method.




You can:

- set the scanning packet size (in bytes) in the Packet size field;
- specify the number of sent packets in the Packet count field;
- set how long (in ms) the sensor will wait for the reply in the Timeout field;
- set the limit of network hops for the packets in the TTL (Time To Live) field.

If at least one packet is delivered, the ping will be deemed successful, and the Result will show the round-trip time and the number of delivered packets.

#### TCP

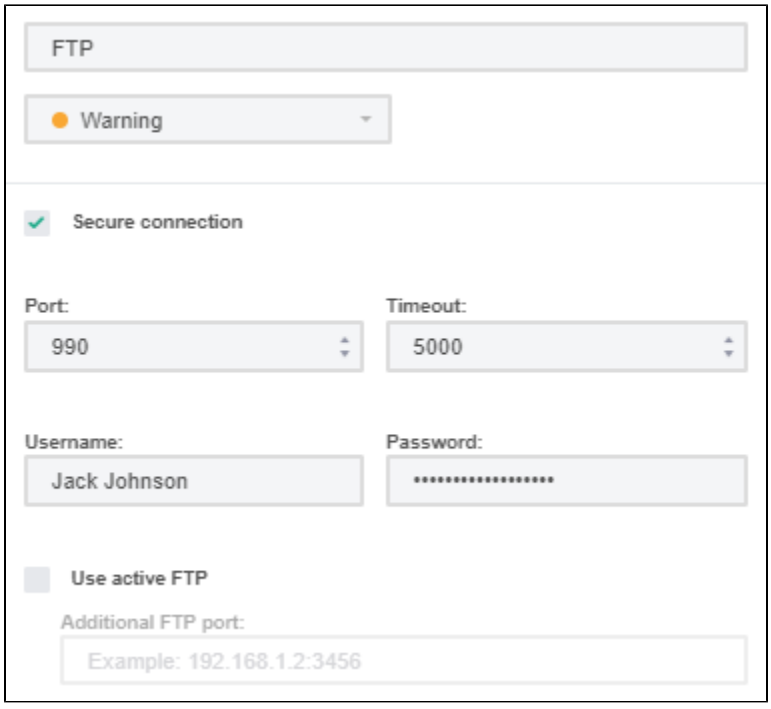
Allows to check if the specified TCP port is available.


Enter the TCP port to be checked.
Set how long (in ms) the sensor will wait for the reply in the Timeout field.

If the remote port is open, the check will be successful.

FTP

Allows to check the FTP server.



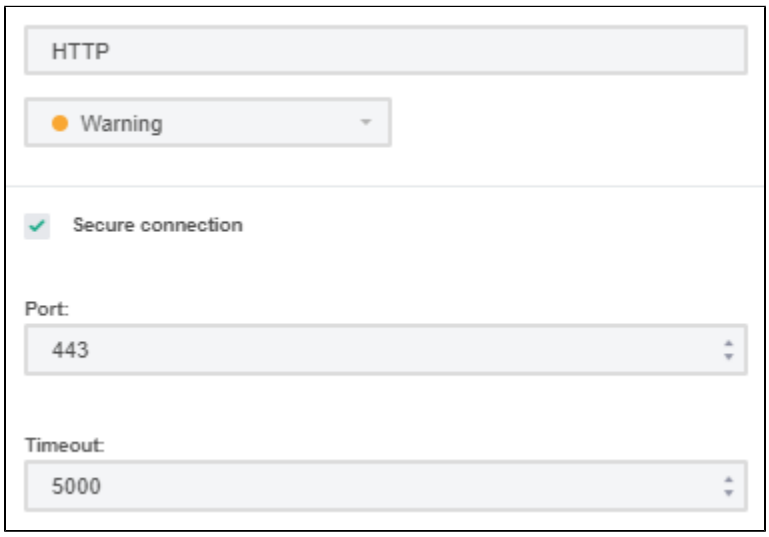

You can:

- use FTPS by enabling Secure connection;
- enter the port to be checked;
- set how long (in ms) the sensor will wait for the reply in the Timeout field;
- enter the Username and Password to be used during the authorization on the FTP-server;
- change the FTP transfer mode from Passive to Active by checking Use active FTP;
- for active FTP, specify a local Additional port that should receive the reply in the address:port format. IPv6 addresses are not supported at the moment.
  Examples:
  192.168.1.2:0 - auto-picks a free port;
  192.168.1.2:32000-33000 - selects a random port from a range;
  curl.se:32123 - using a hostname instead of IP.

If the reply is received, the check will be successful.

HTTP

Allows to check server connectivity using the HTTP protocol, by sending a HEAD request.



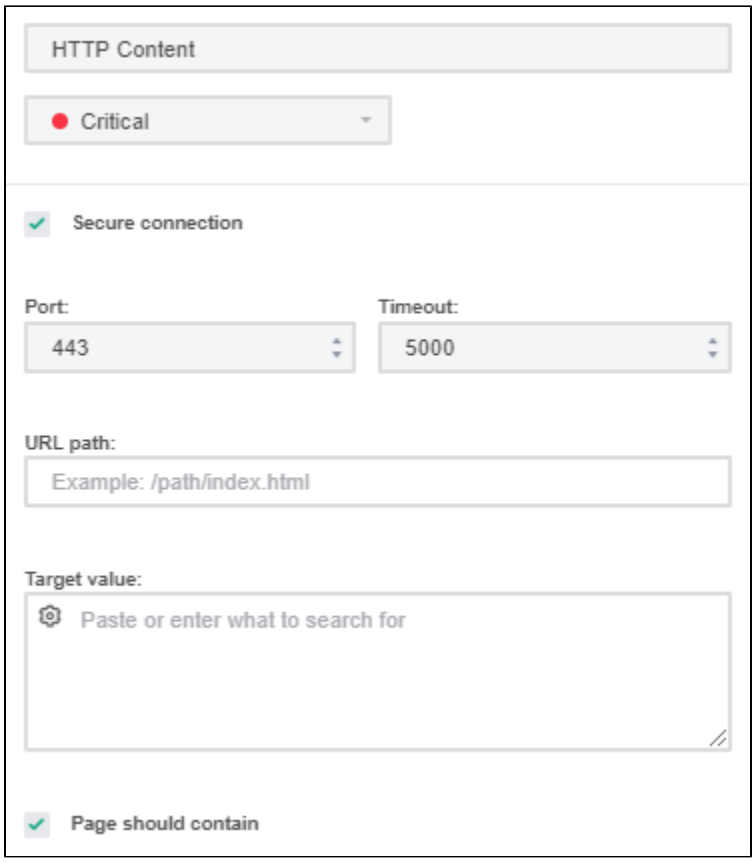

You can:

- use HTTPS by enabling Secure connection;
- enter the port to connect to;
- set how long (in ms) the sensor will wait for the reply in the **Timeout** field.

If there's a positive reply from the server, the check will be successful.

### HTTP Content

Checks if the remote HTML page contains (or is missing) the specified value by sending a GET request.




Enter the address of the HTML page to be checked into the URL path field in the following format:

```
/path/index.html
```

Enter the line you want to check into the Target value field.

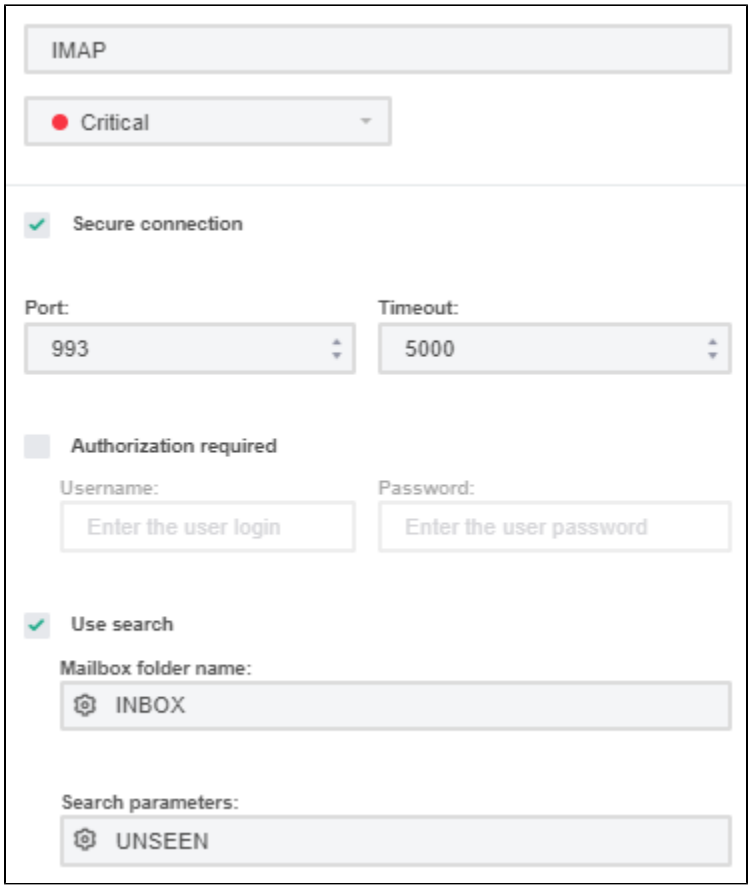
You can also:

- use HTTPS by enabling Secure connection;
- enter the port to connect to;
- set how long (in ms) the sensor will wait for the reply in the Timeout field;
- check instead if the page is missing the line by unticking the box.

If the page content meets the specified condition, the check will be successful.

### IMAP

Allows to check server connectivity using the IMAP protocol, and shows the number of messages that match the criteria.



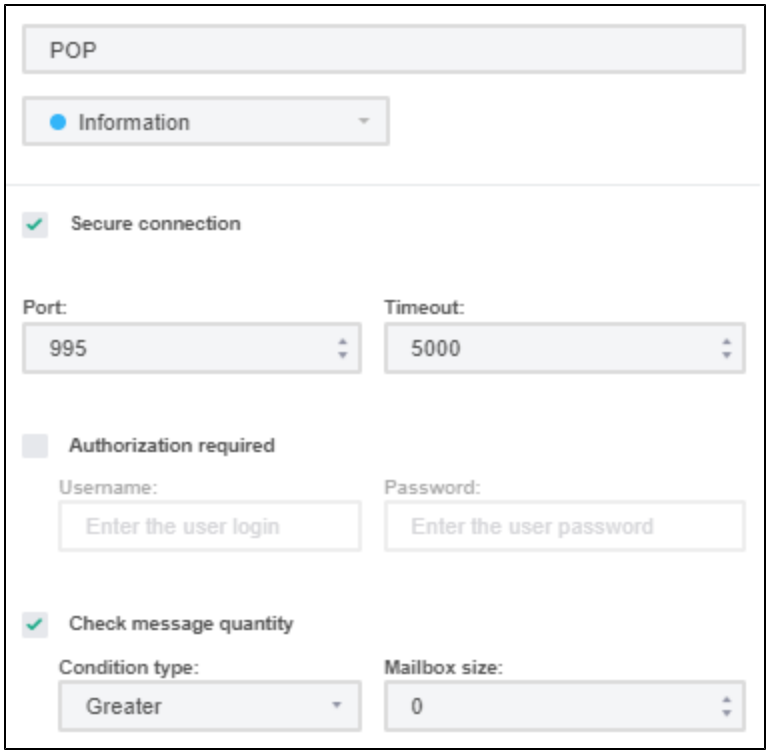

You can:

- use IMAPS by enabling Secure connection;
- enter the port to connect to;
- set how long (in ms) the sensor will wait for the reply in the Timeout field;
- enable the authorization on the IMAP server if required, and enter the Username and Password;
- enable Using search and specify the Mailbox folder name and one or multiple Search parameters, such as ALL, RECENT, NEW...
  A few more complex examples:
  DELETED NOT FROM Smith NOT SINCE 1-Feb-2019
  OR SUBJECT Olympus SUBJECT TNI
  The full list of search criteria is available here.

If the connection is successful and at least one mailbox message meets the specified criteria, the check will be successful.
The message number will be displayed in the Result field.

### POP

Allows to check server connectivity using the POP protocol, and it can also check the total number of messages.



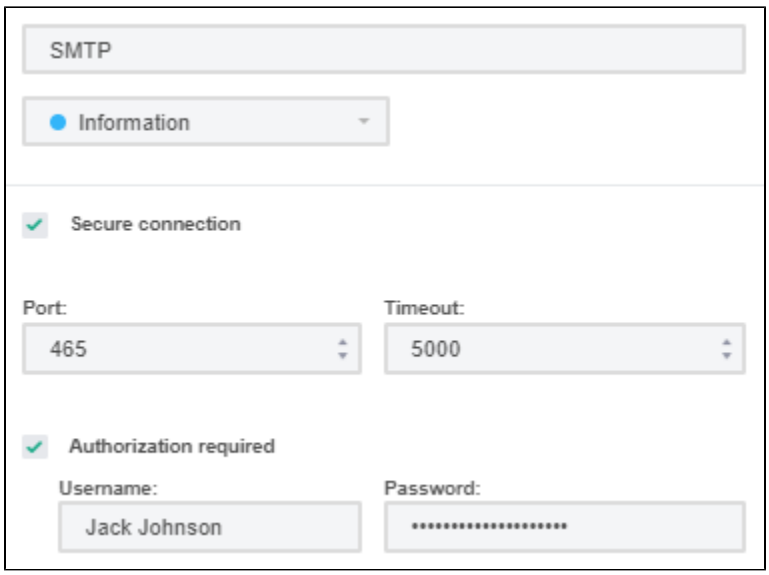

You can:

- use POP3S by enabling Secure connection;
- enter the port to connect to;
- set how long (in ms) the sensor will wait for the reply in the Timeout field;
- enable the authorization on the POP server if required, and enter the Username and Password;
- enable Checking the message quantity in the mailbox against the expected condition.

If the connection is successful and the number of messages meets the specified condition, the check will be successful. The message quantity will be displayed in the Event details.

SMTP

Allows to check server connectivity using the SMTP protocol.




You can:

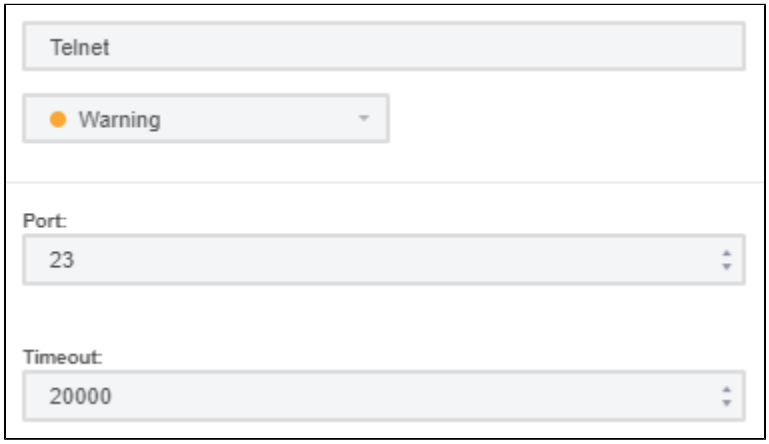
- use SMTPS by enabling Secure connection;
- enter the port to connect to;
- set how long (in ms) the sensor will wait for the reply in the Timeout field;

- enable the authorization on the SMTP server if required, and enter the Username and Password.

If there's a positive reply from the server, the check will be successful.

### Telnet

Allows to check server connectivity using the Telnet protocol.




Enter the Telnet port to be checked.
Set how long (in ms) the sensor will wait for the reply in the Timeout field.

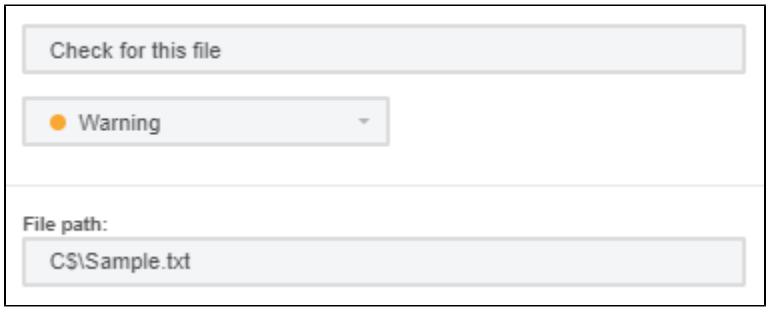
If the server responds, the check will be successful.

## Filesystem

File system sensors that allow to monitor files, folders and drive space on network computers.

### File existence

Allows to check if a particular file exists via the specified path.




Enter the path to the file into the File path field in the NetBIOS format, using the dollar sign instead of the colon: D$\directory\file.txt or \directory\file.txt for network shares.

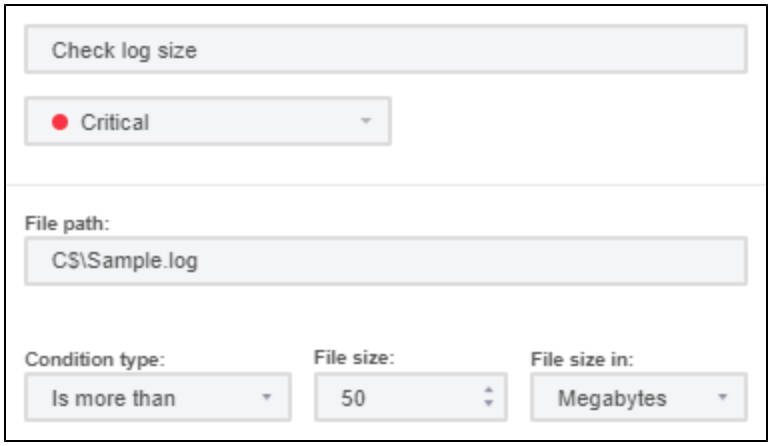
You can use the following wildcard characters in the file name (but not in the rest of the path) to create file masks and look for different possible files:

- * - an asterisk will represent any amount of characters (zero as well);
- ? - a question mark will be interpreted as any single character.

If at least one file exists that matches the path, the check will be successful.

### File size

Allows to check the size of a particular file.




Enter the path to the file into the File path field in the NetBIOS format, using the dollar sign instead of the colon: D$\directory\file.txt or \dire ctory\file.txt for network shares.

You can use the following wildcard characters in the file name (but not in the rest of the path) to create a file mask and check the combined size of multiple files:

- * - an asterisk will represent any amount of characters (zero as well);
- ? - a question mark will be interpreted as any single character.

Select a rule for the sensor from the Condition type drop-down list:

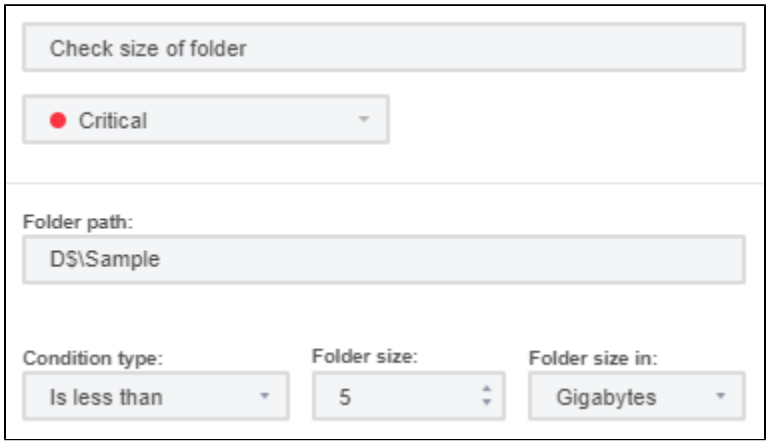
- Is more than: the size of the file(s) must be larger than the specified value for the check to be successful;
- Is less than: the size of the file(s) must be smaller than the specified value for the check to be successful.

Then specify the target File size value and select its units from the drop-down list.

If at least one file exists that matches the path, and the condition is satisfied, the check will be successful.

### Folder size

Allows to check the size of a particular folder.




Enter the path to the folder into the Folder path field in the NetBIOS format, using the dollar sign instead of the colon: D$\directory or \direct ory\files\ for network shares.

You can use the following wildcard characters in the folder name (but not in the rest of the path) to create a folder mask and check the combined size of multiple folders:

- * - an asterisk will represent any amount of characters (zero as well);
- ? - a question mark will be interpreted as any single character.

Select a rule for the sensor from the Condition type drop-down list:

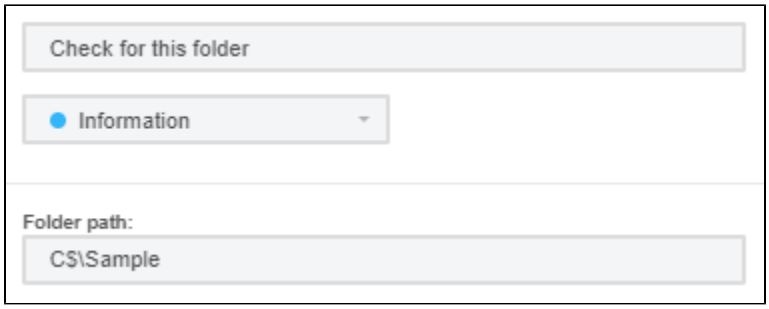
- Is more than: the size of the folder(s) must be larger than the specified value for the check to be successful;
- Is less than: the size of the folder(s) must be smaller than the specified value for the check to be successful.

Then specify the target Folder size value and select its units from the drop-down list.

If at least one folder exists that matches the path, and the condition is satisfied, the check will be successful.

### Folder existence

Allows to check if a particular folder exists via the specified path.




Enter the path to the folder into the Folder path field in the NetBIOS format, using the dollar sign instead of the colon: D$\directory\ or \directory\files for network shares.

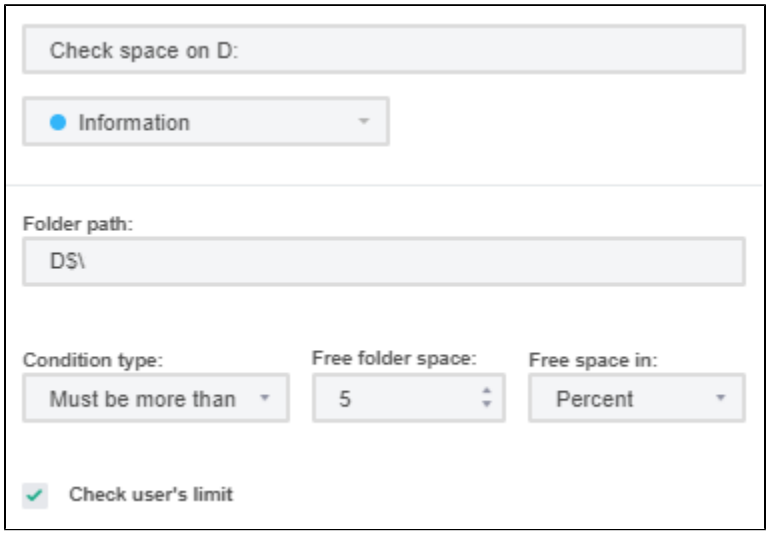
You can use the following wildcard characters in the file name (but not in the rest of the path) to create folder masks and look for different possible files:

- * - an asterisk will represent any amount of characters (zero as well);
- ? - a question mark will be interpreted as any single character.

If at least one folder exists that matches the path, the check will be successful.

### Folder free space

Allows to check the available space on a local or network drive.




Enter the path to the folder or drive into the Folder path field in the NetBIOS format, using the dollar sign instead of the colon: C$\ or \directory\files for network shares.

If you need to make sure that free available space is lower, not higher, than a certain value or percentage, change the Condition type to Must be less than.

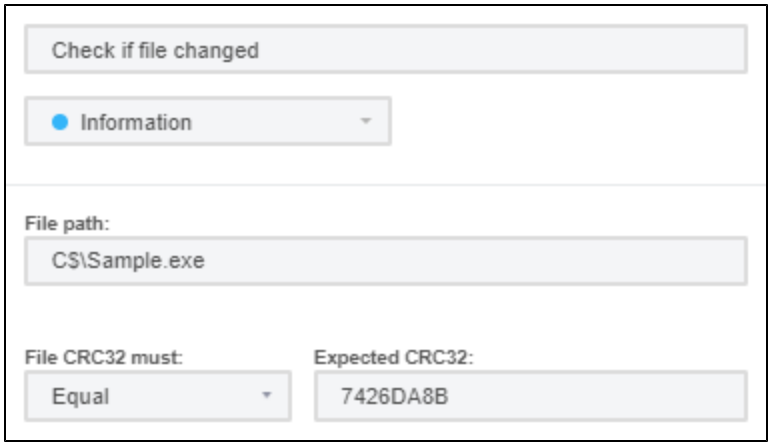
Then specify the target Free folder space value (storage units or percents) and select its units from the drop-down list.

Check user`s limit controls whether the sensor checks the space available to all users or to the user whose credentials are selected for the device.

If the folder or drive is found and the condition is satisfied, the check will be successful.

### File CRC32

Allows to check for changes in the file's CRC32.




Enter the path to the file into the File path field in the NetBIOS format, using a dollar sign instead of a colon: D$\directory\file.txt or \director y\file.txt for network shares.

You can choose between two rules for the condition:

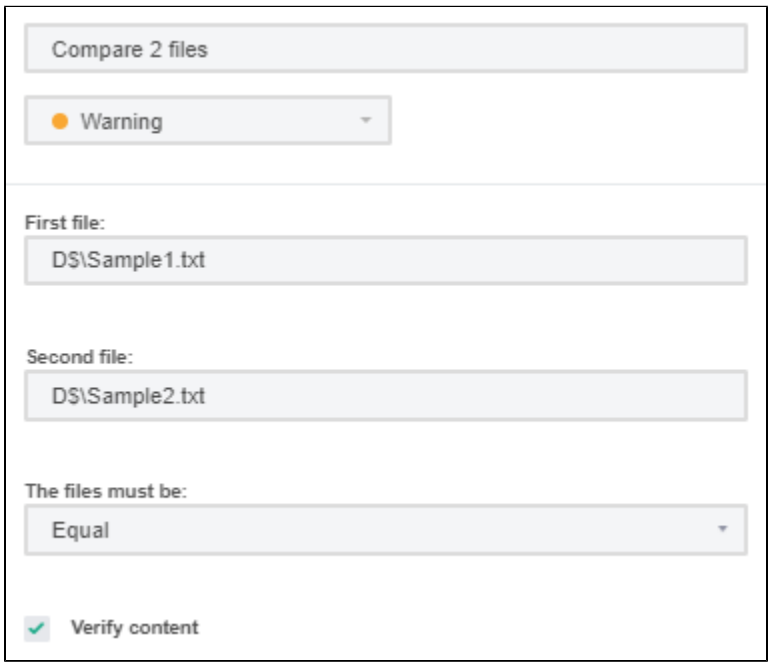
- Equal: the sensor will check if the file has the specified checksum;
- Not equal: the sensor will verify that the file has a different checksum.

Specify what CRC32 checksum to check for in the other field.

If the condition is satisfied, the check will be successful.

### File compare

Allows to compare two files by size and optionally by content as well.




Enter the paths to the files into the First file and Second file fields in the following format: C$\[your path here]

You can also:

- Enter the path in the normal format (with the colon) to point to a local file: C:\[your path here]
- Choose if the files must be Equal or Not equal;
- Tick the Verify content box if you want to also compare the content of the two files.
  If the box is unchecked, the sensor will check Date modified and File size.
  If the checkbox is set, the sensor will still check File size in addition to content. Date modified is not checked in this case.

If the condition is satisfied, the check will be successful.

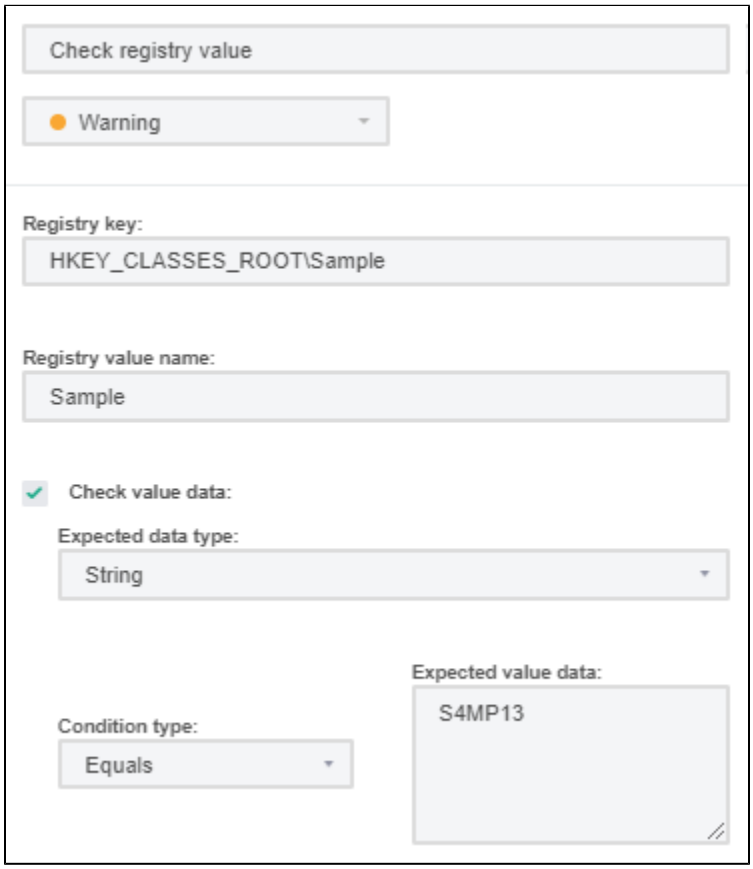
> Relative paths to network shares are not allowed for this sensor.

## Winbase

Windows sensors that allow to track various system parameters.

### Registry key

Allows to check the existence of the specified Windows registry key or parameter, or to check its value.




Set the path to the Registry key that you want to check (example: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run). If no other fields are specified, then the program will only check the key.
To check whether a certain parameter is present in the registry, enter its name in the next field: Registry value name.

If Check value data is enabled, the sensor will also check the parameter's value.
Select the Expected data type from the drop-down list: String, Expendable string, Multistring, Binary, DWORD, QWORD.

Specify the target parameter value in the Expected value data field. To enter binary data use hexadecimal notation 0x (e.g. 0xABC123).

Select a rule for the sensor from the Condition type drop-down list:

- Equals: the registry value is exactly equal to the specified value (default rule);
- Does not equal: the registry value is not exactly equal to the specified value;
- Contains: the parameter value contains all of the specified value;
  If searching in a multi-string value, a single matching string will satisfy this condition.
- Does not contain: the parameter value doesn't contain the specified value;
- Is greater than and Is less than: compares the size of the value (for DWORD and QWORD).

If the condition is met, the check will be successful.
If the sensor checked value data, then the actual value and type will be displayed in the Event details.

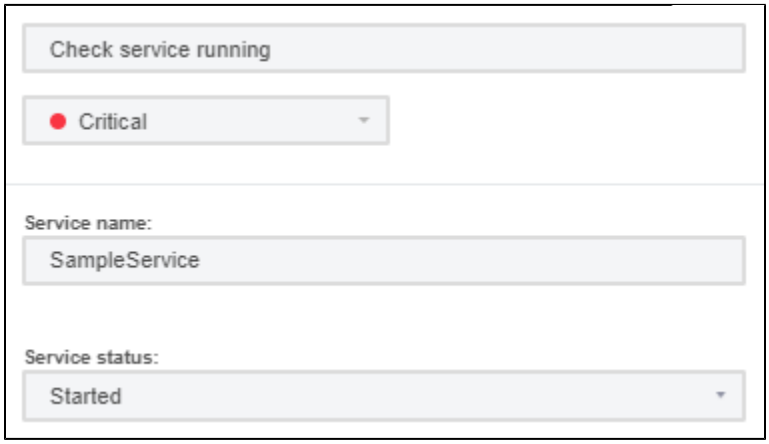
> The Registry key sensor uses the Remote Registry service on remote computers. The sensor will not operate if this service is stopped.

## System

System sensors that allow to track various system performance and other system parameters.

### Service status

Allows to check the status of a particular system service.



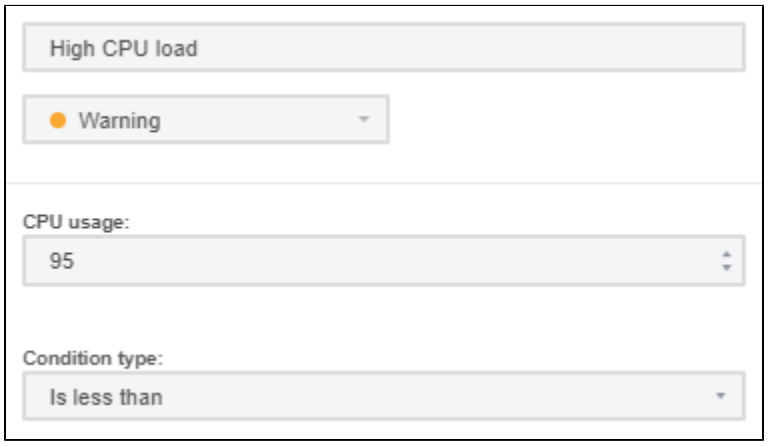

Enter the Service name that you want to check.

Select the expected state (Started, Stopped, or Paused) from the Service status drop-down list.

If the actual state is matched, the check will be successful.
In any case, the state of the specified service at the time of the check will be available in the Event details.

### CPU usage

Allows to check the CPU load.




Enter the target CPU usage percentage.
By default, the sensor will check that the remote computer is staying below this value.

You can select from the drop-down list if the sensor should instead check if the CPU load is greater, exactly equal or not equal.

If the query is made successfully and the current CPU usage meets the specified condition, the check will be successful.
The load value at the time of the check will be displayed in the Event details.

### Physical memory

Allows to check the availability of physical memory.


Enter the target Used physical memory, in %.

Select from the drop-down list if the sensor should check if the Physical memory is less, greater, exactly equal or not equal to this value.

If the query is made successfully and the current physical memory usage meets the specified condition, the check will be successful. The used memory percentage at the time of the check will be displayed in the Event details.

### Virtual memory

Allows to check the availability of virtual memory (physical memory + page file).

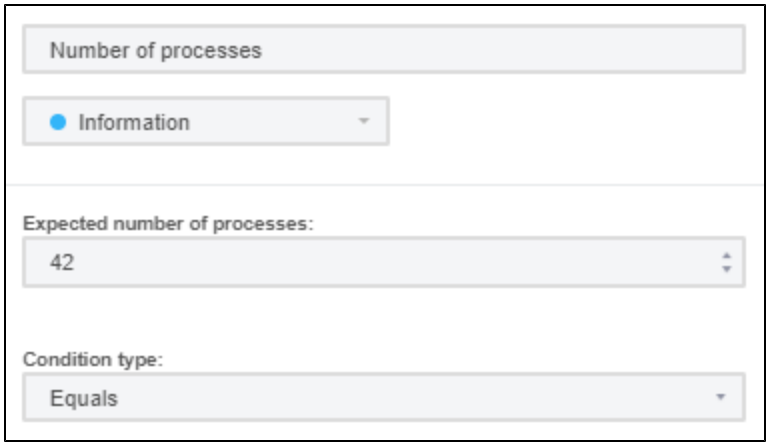

Enter the target Used virtual memory, in %.

Select from the drop-down list if the sensor should check if the Virtual memory is less, greater, exactly equal or not equal to the value.

If the query is made successfully and the current virtual memory usage meets the specified condition, the check will be successful. How much memory was used at the time of the check will be displayed in the Event details.

### Process count

Allows to check the number of running processes.



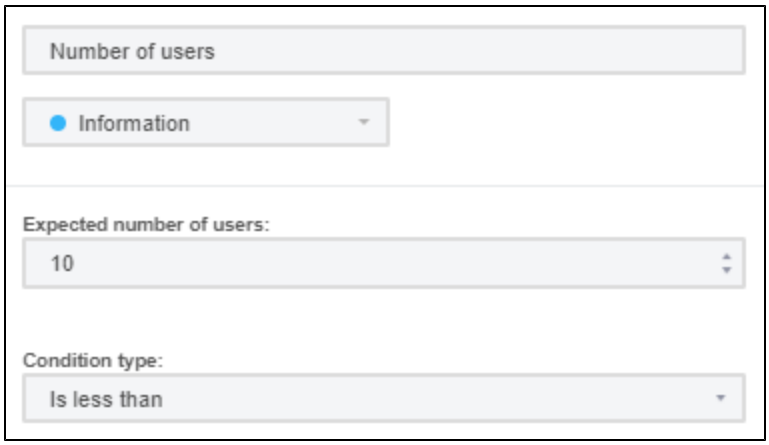

Enter the Expected number of processes.

Select from the drop-down list if the sensor should check if the number of processes is less, greater, exactly equal or not equal to the value.

If the query is made successfully and the current process count meets the specified condition, the check will be successful.
How many processes were running at the time of the check will be displayed in the Event details.

### User count

Allows to check the number of users.




Enter the Expected number of users.

Select from the drop-down list if the sensor should check if the number of users is less, greater, exactly equal or not equal to the value.

If the query is made successfully and the current user count meets the specified condition, the check will be successful.
Event details will show how many users were found at the time of the check.

## Actions

Network Olympus currently offers 5 types of actions that can respond to arising issues and automatically address them.

### Run application

Runs the specified third-party program on the local computer.

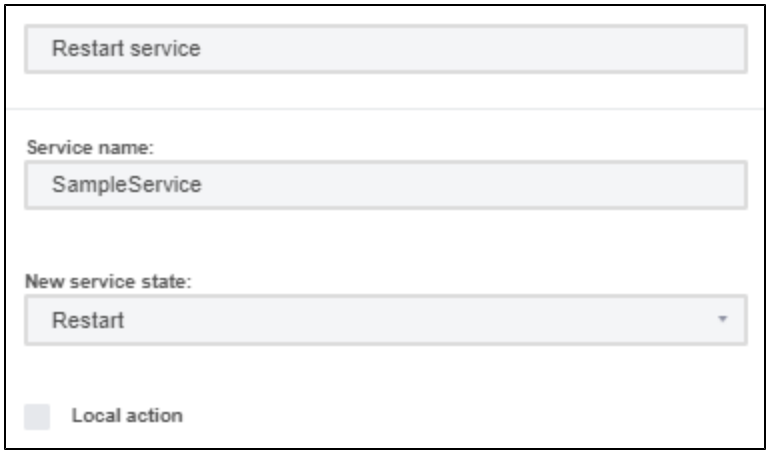

Enter the Absolute path to local application that will be run when the action is triggered. This must be a local path.

You can also:

- Specify the command line Parameters to run the application with, if needed;
- Specify the path to the application's Working directory.

### Service control

Changes the state of the specified service (for example, restarts it) on the local or remote computer.




Enter the Service name for which you want to change the status.

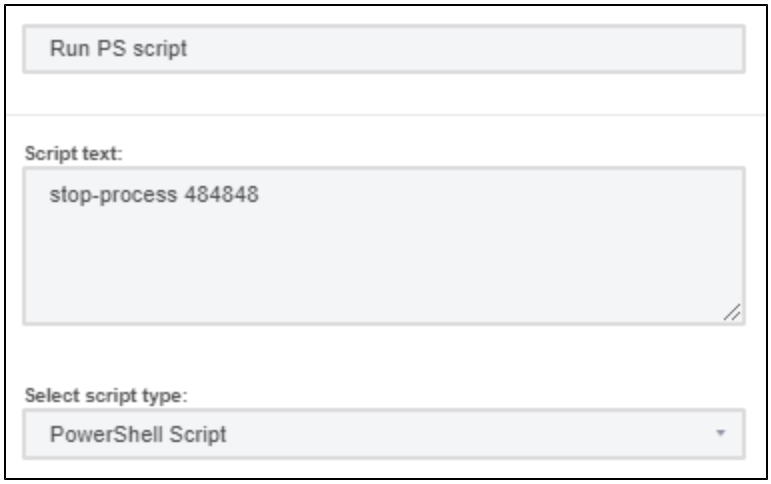
Choose the action for the service (Start, Pause, Continue, Restart, Stop) from the New service state drop-down list.

By default, this action controls the service on the remote computer. To control a local service, check the Local action box.

Event details will contain additional information, such as the previous service state.

### Execute script

Locally executes a script in Visual Basic, JavaScript or PowerShell, or in Windows command line.




Enter the code in the Script code field.

Select the interpretator which will execute the script from the Select script type drop-down list. You can choose from Visual Basic, JavaScript, Windows Command Line (.bat or .cmd) or go with the default PowerShell Script.

Event details may contain output data from the script interpretator or the error message.

### Restart computer

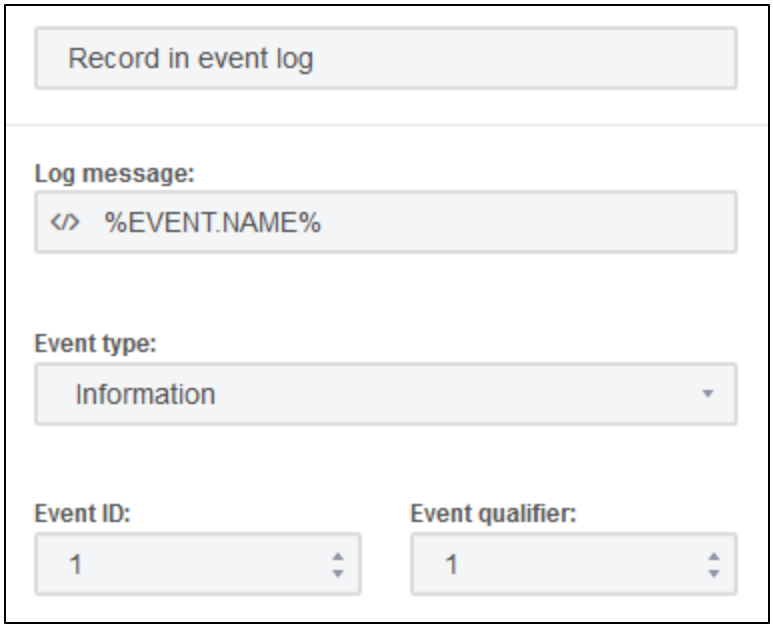
Reboots (or switches off) the remote computer. A timeout can be set that allows the system to correctly close all running applications and save all data.


You can:

- Enter the Message text that will alert the remote user before the reboot or shutdown.
- Specify the time (in ms) before the computer is rebooted or switched off in the Timeout field.
- Tick the Force action box to shut down the computer without waiting for applications to exit correctly.
- Perform a Shutdown instead of a restart by ticking the checkbox.

### Write to Windows Event Log

Creates an Event Log entry in the Windows application log on a remote computer.




Enter the text of the Log message. You can use macros.

Select the Event type (Success, Error, Information, Warning, Audit success or Audit failure) from the drop-down list.

Event ID can be any number from 1 to 65535.

Event qualifier can be any number from 1 to 65535.

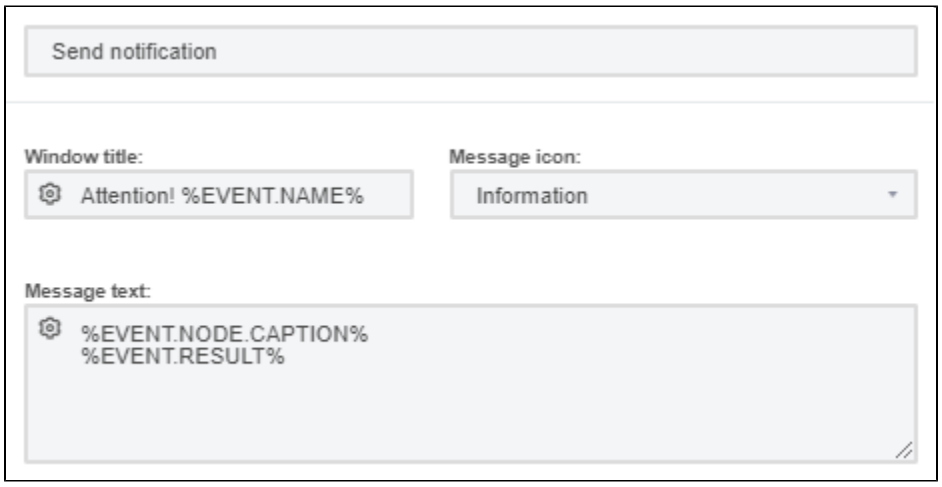
> If the event log has reached its limit, no logging shall be made. In this case, clear the Application log.

## Notifications

Network Olympus currently offers 5 types of notifications.

### Show message

Displays a text message on the local computer.




Enter the message title into the Window title field.

Select the Message icon from 3 available types (Error, Questrion, Information) in the drop-down list. Select None so no icon is displayed.

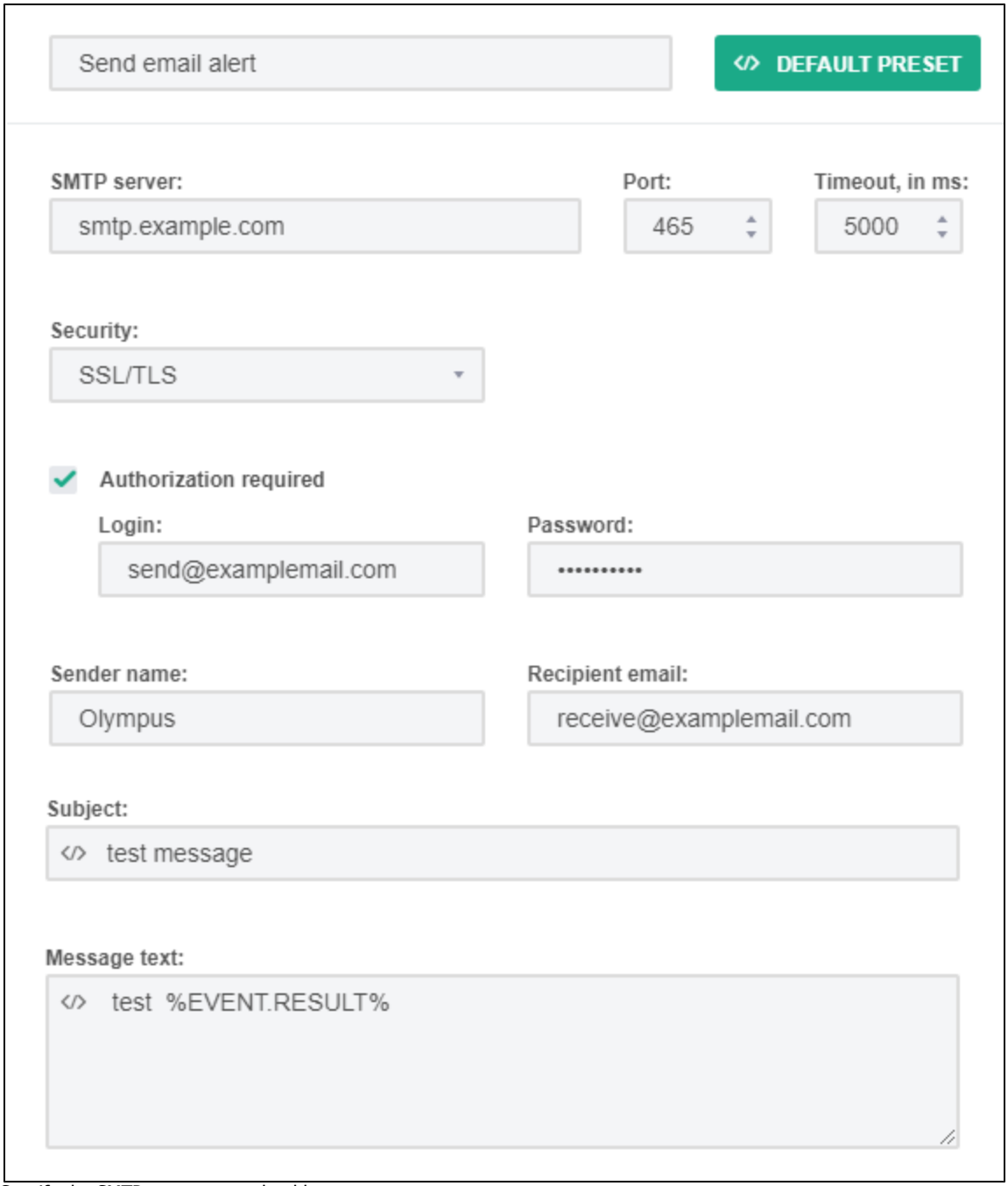
Enter the Message text.

You can use macros both in the title and the text.

Example result:


## Send email

Sends an e-mail message to the specified address.




Specify the SMTP server network address.

Change the Security level (SSL/TLS, STARTTLS or none), Port number and Timeout if needed.

Enable the authorization on the SMTP server if required, and enter the Username and Password.

Enter the Sender name (arbitrary text or an email address) and the Recipient email address in the sender@example.com format.

Specify the message title in the Subject field.

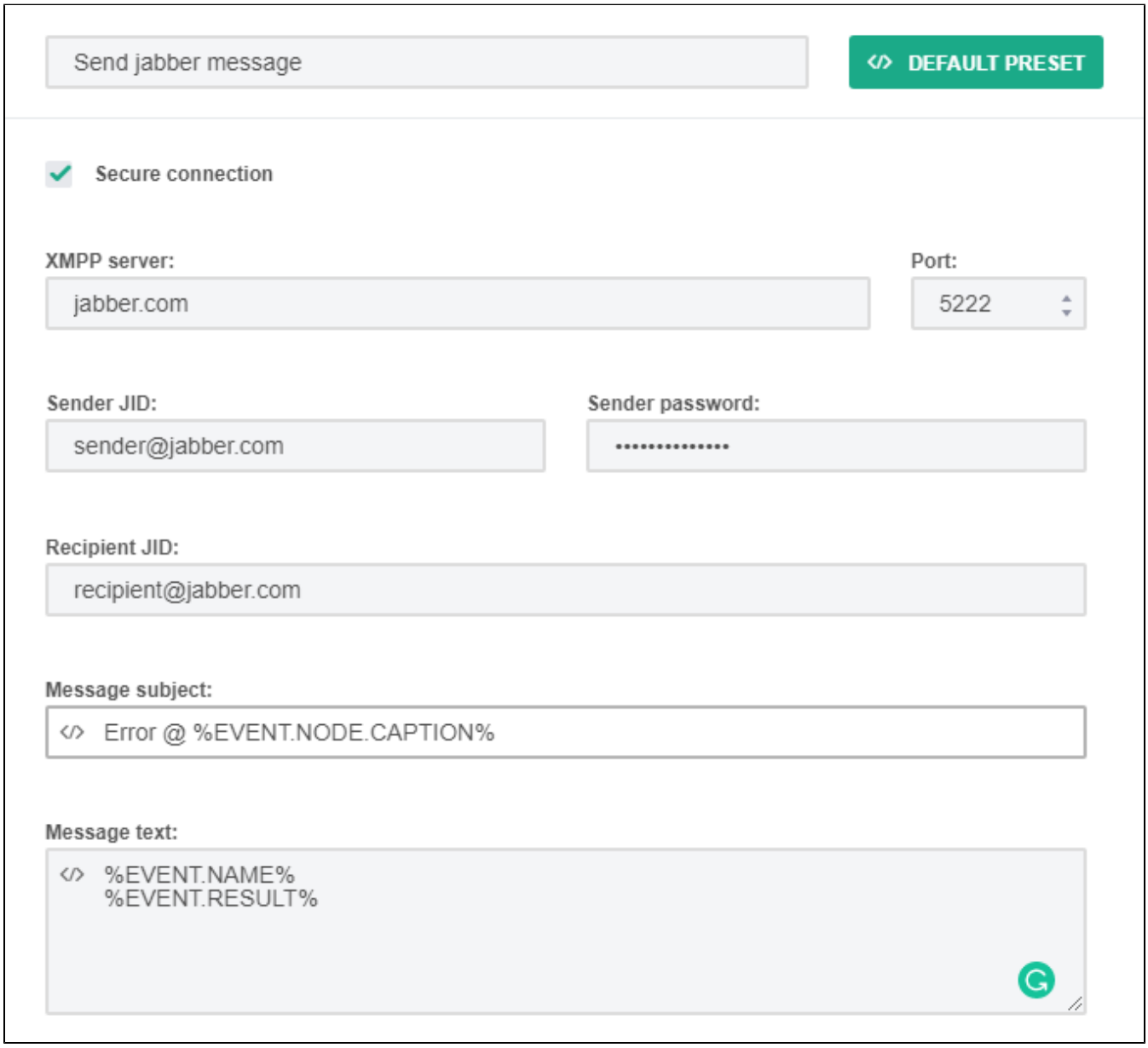
Finally, enter the Message text itself.

You can also use macros both in the title and the text.

> Attention!
> If notifications are not sent and the Login denied message is generated in the log, you may additionally need to open access for third-party applications in the mail server settings.
>
> For example, to open access in **Gmail**, go to **Manage your Google Account** and open the **Security** tab. Enable the option **Less secure app access**.

## Send jabber message

Sends a message to the specified Jabber account.




Specify the remote XMPP server's IP address or FQDN.
Change the Port if needed (port 5222 is used by default).

Specify the user identifier, as well as the name of the server he's registered with, into the Sender JID field. The JID and the server name should be separated by the @-sign. For example, sender@jabber.com means that the message will be sent on behalf of sender through server jabber.com.
Then enter the Sender password.

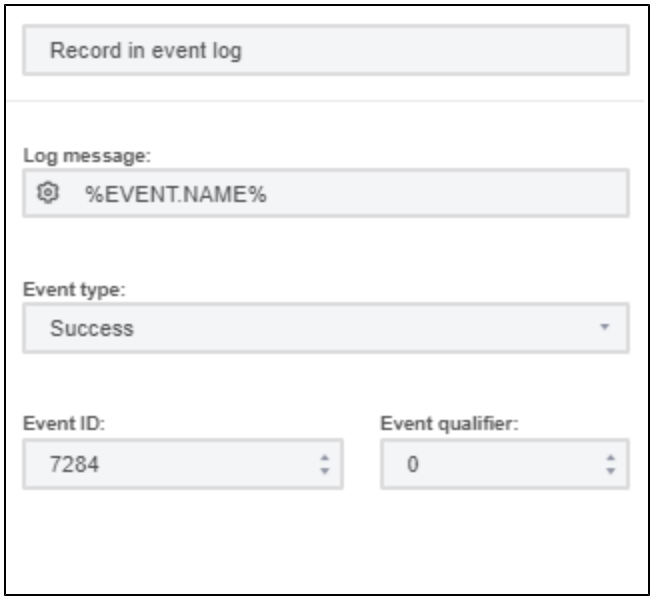
Similarly, specify the Jabber identifier of the user you want to send a message to, and its server, in the Recipient JID field.

Specify the message title in the Message subject field.

Finally, enter the Message text itself.

## Write to Windows Event Log

Creates an Event Log entry in the Windows application log.




Enter the text of the Log message. You can use macros.

Select the Event type (Success, Error, Information, Warning, Audit success or Audit failure) from the drop-down list.

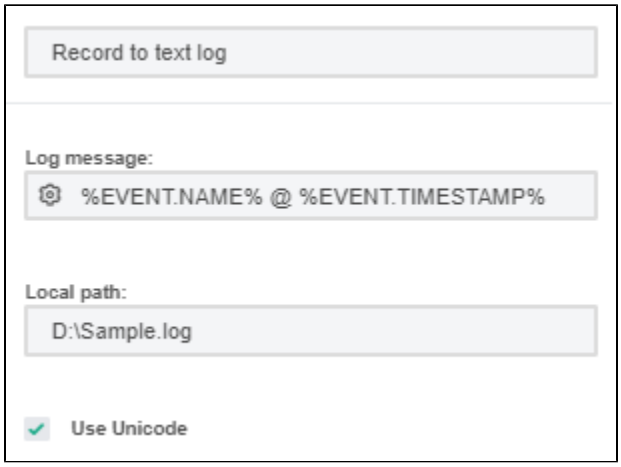
Event ID can be any number from 1 to 65535.

Event qualifier can be any number from 1 to 65535.

> If the event log has reached its limit, no logging shall be made. In this case, clear the Application log.

### Write to log file

Writes an entry at the end of the selected log file.




Enter the text of the logged entry into the Log message field. You can use macros here.

Specify the Local path to the file where the record should be made.

You can also disable the Unicode code table if you need to make the entry in ASCII, by unticking Use Unicode.

# Scenario builder



The main goal of a monitoring system is to detect and notify about problems and, where possible, automatically solve them.

In Network Olympus, the scenario building engine provides the ability to generate various types of actions and notifications based on the results of sensors and actions.

The status of the result (event status) determines which scenario branch is followed.

If one of the parameters is beyond the acceptable range or an error occurs during execution, then a Down event will be generated and the subsequent scenario elements along the red branch are performed. If everything is fine, then the green branch is performed.

## Monitoring scenarios

A scenario is a sequence of sensors, actions, and notifications that form a logic execution chain.

This feature allows you to create flexible monitoring plans, more accurately identify issues and malfunctions and automate the process of their elimination.

To create a scenario, use the Scenario builder, located on the dashboard of the same name.


The displayed scenario depends on which device, group, sensor or action is selected in the dropdown field at the top of the widget.

On the first step when creating each individual scenario, only a sensor can be added. To do this, click the button under Create a new scenario .
On the subsequent steps other scenario elements (sensors, actions and notifications) can be added to each branch. When you choose to add a new element, this element's wizard will open.
For more information about this, visit the Monitoring section.

Previously added sensors and actions can be edited using their context menus.
From their editors, parameters of the notifications assigned to them can also be changed.

To change the scale in the Builder, use the mouse wheel or buttons +/– on the right side of the widget.
From here, you can also restore the default position and scale.

## Examples of scenarios

1. Check whether the devices in the group are online. If the device is online, then record this in the log file. If an error occurred while checking the device, send a Jabber notification to the system administrator and log the event.

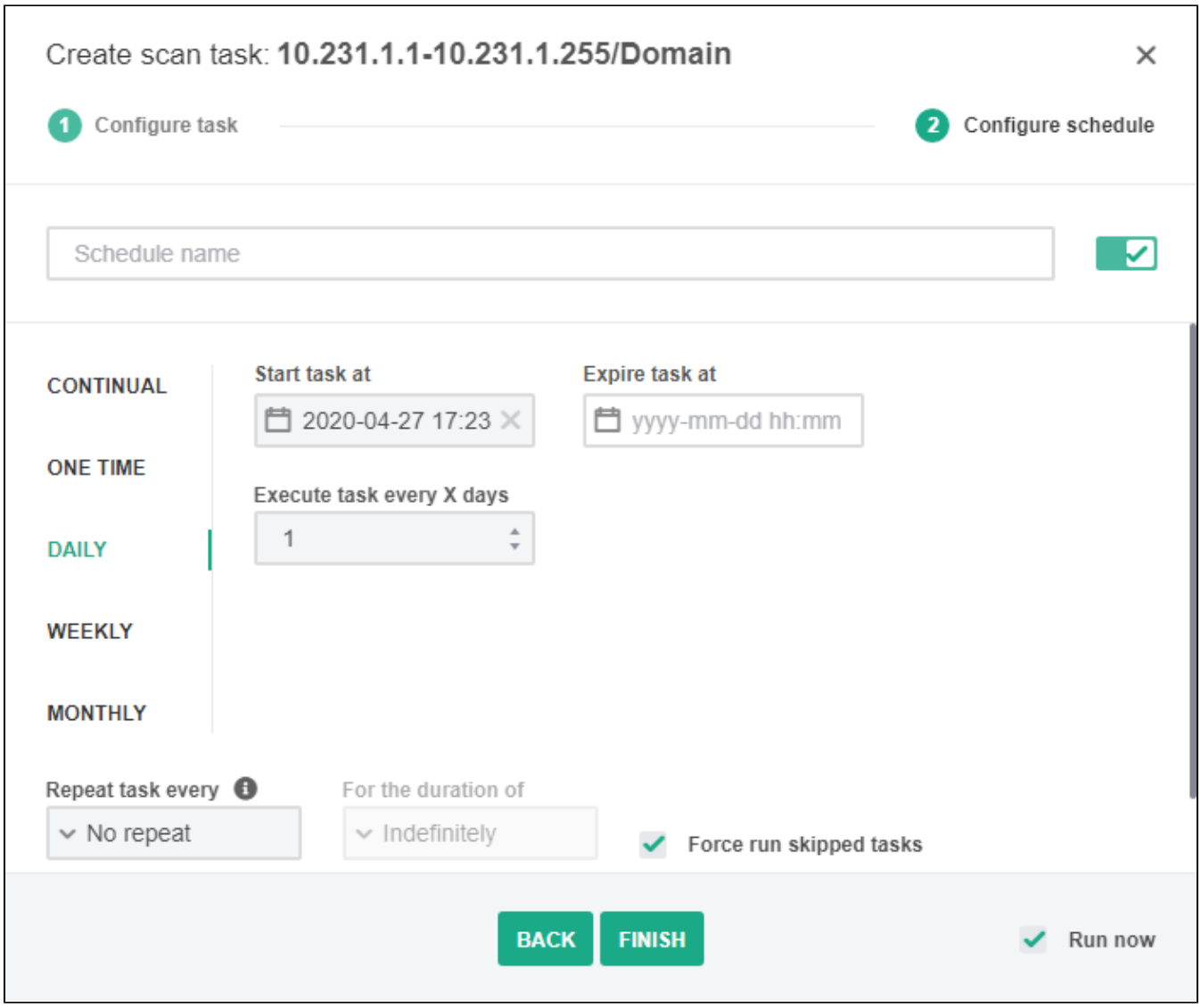
2. Check the value in the registry key on the remote server. If the value deviates from the norm, then execute a script that restores the required value.
3. Check the availability of the server. If the server is available, then check the availability of the company website. If for some reason one of the operations resulted in an error, restart the server and send an email to the system administrator.

# Scheduling tasks



Network Olympus provides the tools for setting up and adjusting schedules for most kinds of tasks.

This includes the launch of sensors and actions, network scans and updating of device information.




In the current version, the task scheduler can be used to perform the following operations:

1. Running sensors on a schedule.
   The scheduler parameters can be set during the sensor setup, on the Configuration step.
2. Running actions on a schedule.
   The scheduler parameters can be set during the action setup, on the Configuration step.
3. Running scans on a schedule.
   The scheduler parameters are set during the configuration of a scan task. You can create, update or delete a schedule in the Scanner status widget.

## Main task parameters

Tasks can be scheduled to run with various frequency:

| Frequency | Recurrence | Description | Parameters | Example |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| Continual | Yes | The task will be run every 60 seconds to 24 hours. You can select a preset interval from the drop-down menu or you can define it manually using the s,m,h annex (seconds, minutes, hours). | Execution interval | 35m |
| Once | No | The task will run at a selected time on a selected day. | Run date and time | January 22, 2020 at 3 PM |
| Daily | Yes | The task will run every few days. | Start date<br><br>Interval in days | since 4 PM on October 15, 2019<br><br>every third day |
| Weekly | Yes | The task will run on selected days of the week every few weeks. | Start date<br><br>Days of the week<br><br>Interval in weeks | since 7 PM on March 10, 2018<br><br>Monday and Friday<br><br>every week |
| Monthly on specific days | Yes | The task will run on selected days of the month.<br><br>The last day of the month can be selected. | Start date<br><br>Months<br><br>Days of the month | since 11:30 on April 16, 2019<br><br>in April and December<br><br>on the 16th and 19th |
| Monthly on specific weeks and days of the week | Yes | The task will run on selected days of selected weeks of selected months.<br><br>The last week of the month can be selected. | Start date<br><br>Months<br><br>Days of the week<br><br>Week numbers | since 8:50 on June 5, 2018<br><br>June, July and August<br><br>Monday and Friday<br><br>first and last week |

The following intervals are preset for the Continual scheduler mode:

- 1m for sensors
- 1h for actions
- 12h for scan tasks

You can change these values in Settings on the Monitoring tab.

## Additional task parameters

For all types of tasks, you can set the following parameters:

- Enable scheduled task:
  If the scheduled task is disabled, it won't be run by the scheduler until it's enabled.
- Force run skipped tasks:
  This setting is designed to run tasks that were skipped for some reason. In such a case, the task will be run once in the closest possible time.
  The date and time for the next run is then recalculated from this moment according to the schedule.

For recurring tasks, you can additionally set:

- Date and time of task finish:
  After the specified date and time is reached, the period in which the task is enabled comes to an end and no further tasks will be

run.
If the field is empty, the task will be run until it's disabled manually or deleted.

- Loop for the task (Repeat task every).
  Allows to repeat the task at regular intervals.
  In this way, tasks can also be run in the interim period between the runs triggered by the main parameters.
  The interval can be set either manually or from the drop-down menu, allowing to repeat the task every 60 seconds to 24 hours.
- Period for the interval (For the duration of).
  Allows to limit the period in which looped tasks will be performed.
  For example: repeat task every 1 hour for the duration of 8 hours.

# Network map



The Network map widget is located on the corresponding dashboard and allows you to create graphical representations of various network infrastructure and manage them by creating and editing map projects. The map can also be used to monitor the sensor states.

You can add objects of three types on the map:

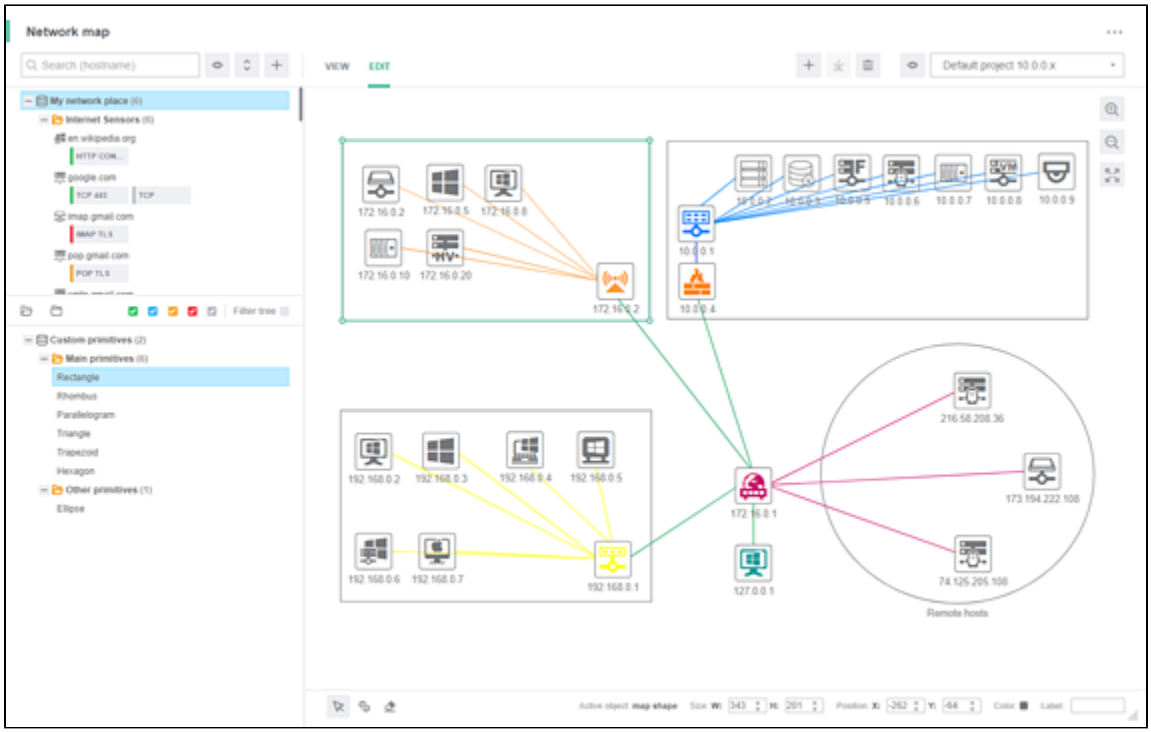
- Network map nodes (devices and groups from the network tree);
- Links that allow to create connections between individual devices and groups;
- Various pre-defined shapes.

This widget can work in two primary modes:

- Edit mode;
- View mode.

You can switch between the modes using the widget's main toolbar.

## Edit mode




When in this mode, the widget consists of three areas:

- Network tree (in the upper left);
- Shapes tree (in the lower left);
- Map edit area where graphical objects can be arranged to form a network map.
  Open the context menu in this area to manage the project.

Above the main area is the main toolbar where you can:

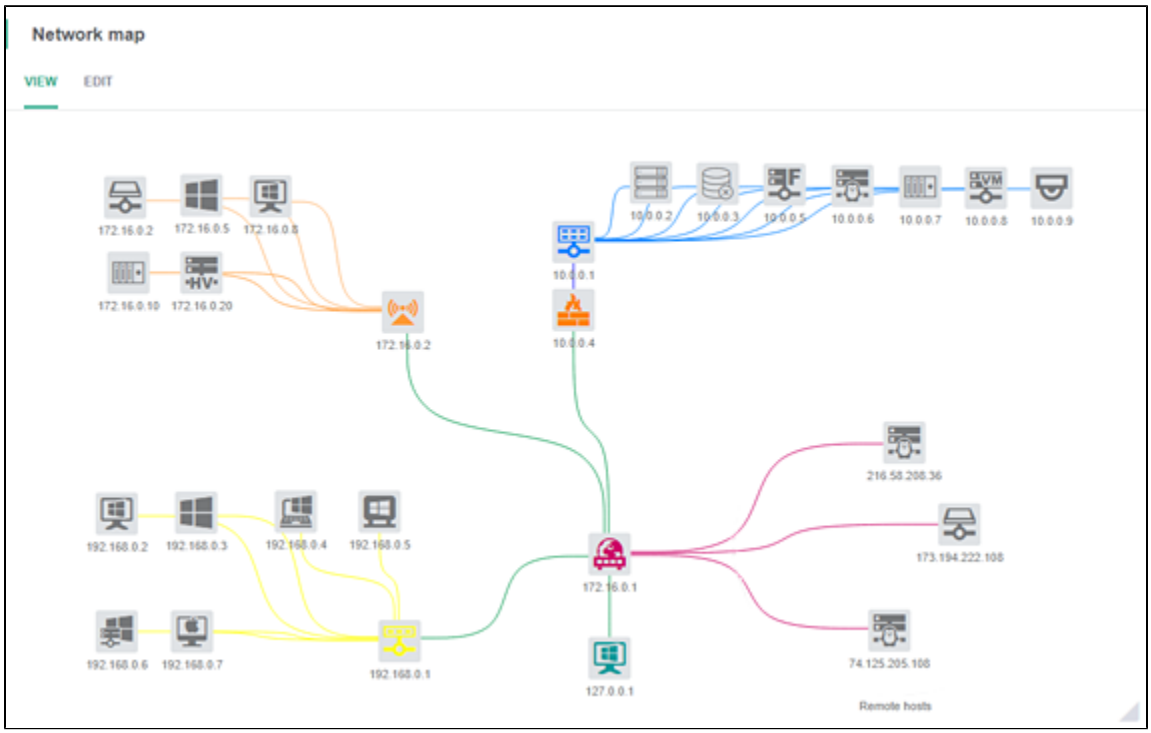
- switch between the modes;
- add, rename, save or delete a map project;
- change the visualization mode of map objects;
- switch between the existing projects.

To the right of the map you can find the buttons that allow to zoom the map.

The bottom part contains the toolbar for editing various graphical objects on the network map.

For more information, see Creating and editing the map.

## View mode




Above the main area is the main toolbar where you can:

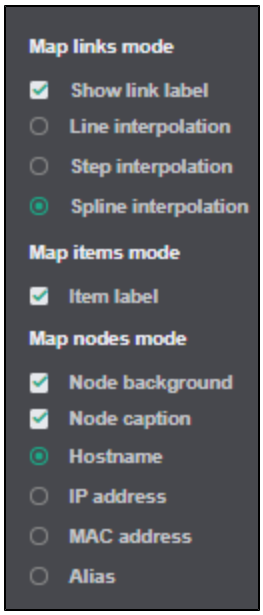
- switch between the modes;
- change the visualization mode of map objects;
- switch between the existing projects.

In the main area, the network map of the selected project is displayed.

To the right of the map you can find the buttons that allow to zoom the map.

## Configuring the display of map objects

To change the way that the graphical objects are displayed, use the Visualization mode menu located on the upper toolbar (regardless of the selected mode).




The following options are available for links:

- disable link captions (labels);
- select how links are displayed (line, step or spline interpolation).

The following options are available for devices, groups and shapes:

- disable the display of item labels (captions that can be assigned on the bottom toolbar);
- remove own background that node icons have by default;
- disable the display of node captions (network device properties selected below, and also group names);
- select which of the device properties will serve as the caption for map nodes when their display is turned on. You can select from the following properties: network names, IP addresses, MAC addresses, aliases.

## Navigating the map

The widget's main area is used to view or edit the network map.
Both modes allow to zoom and navigate the map.

To navigate the map, click and hold somewhere in the empty map space and drag it in the desired direction.

> When in the Edit mode, use Ctrl+click and hold somewhere on the map and drag it in the desired direction.
> Using Ctrl is not required if you click in empty space.
> Do not attempt to drag the map by Ctrl-clicking the nodes. This action is for creating connections.

To alter the zoom level, use the mouse wheel or buttons +/– on the right side of the map.

Between these two buttons is another button that restores the default view and zoom level.

Related topics:

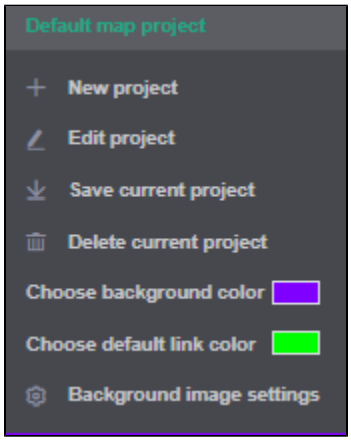
- Creating and editing the map

# Creating and editing the map



## Creating a project

To create a map project, switch to the Edit mode and use the corresponding toolbar button or context menu item.
A form will open. Specify a name for the project and click OK. The name can be changed at any time using the network map context menu.




From this context menu, you can also change the background color of the map (white by default) or upload any background image.
To choose the background color, click the menu item and select from the palette.
In the same way, you can choose the default link color.
To upload or remove the background image, go to Background image settings.

## Adding objects

When the project is created, you can start filling the network map with objects.

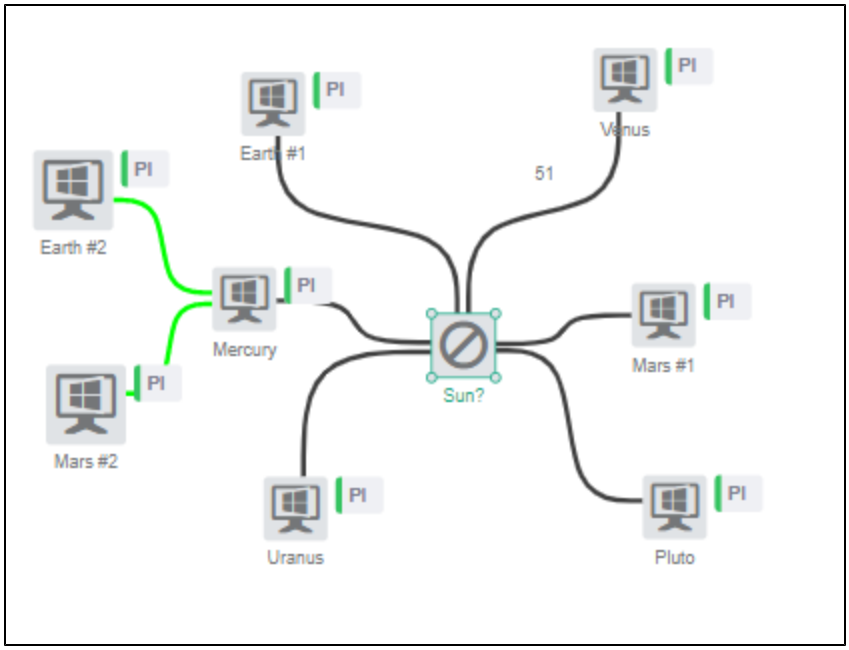
> Don't forget to save the project after making a series of changes. The map is saved automatically after such actions as switching to another project, to another dashboard, etc.
> To save changes while editing the map, save the map project from the toolbar or context menu.

### Map nodes

On the map, you can add an unlimited number of nodes which will correspond to devices and groups in the network tree. To do this, simply drag them from the network tree on the left side when in the Edit mode.

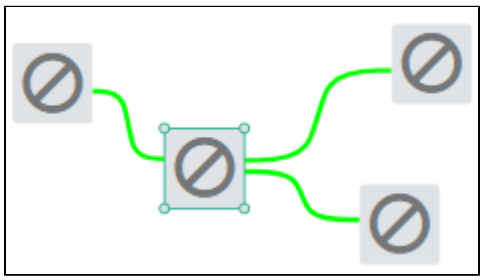
A single network tree node can be added to the map an unlimited number of times. To differentiate between such nodes, you can label them on the map.

Map nodes are displayed in the form of a square icon that shows the type of the corresponding node in the network tree.




To the right of the node icon, the device sensor icons will be displayed indicating their current state.

Deleting nodes from the network tree does not lead to the deletion of the corresponding nodes from the map. These map nodes will look like this:



### Links

Links allow to show the connections between nodes in your network infrastructure.

To establish a link between two devices, click Add link on the bottom toolbar and draw a line between the two map nodes.

> When adding connections, selecting objects becomes unavailable. When you've finished, we recommend that you reenable the default Select map object mode (to the left of Add link).

To draw links in the Select map object mode, hold Ctrl.

### Shapes

You can additionally fill the map with various preset geometric shapes by dragging them from the tree of shapes.

The following shapes are available right now: triangle, rectangle, parallelogram, trapezoid, rhombus, hexagon, ellipse, figure arrows, images.

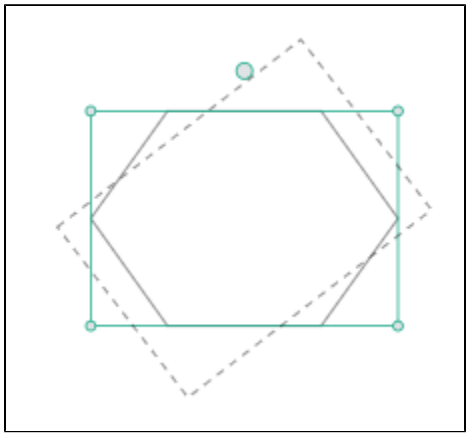
When adding an image, the program will ask you to choose the image file on your computer.

## Editing objects

After adding node objects and shapes on the map, you can use drag & drop and resizing handles to change their position and size.

To resize a shape or the icon of a node, grab and drag one of the corners of the object's frame. To display the frame, select the object using the left mouse button.

Shapes can be rotated using the rotation controller.



To select multiple objects, hold Shift and click on the objects or use rectangle selection.

> When selecting or moving objects, make sure that Selecting of map objects is enabled in the toolbar under the network map area.

> When editing nodes, the position and length of any links between them will change automatically.

If you need to fine-tune an object's dimensions and position, you can edit its coordinates, width and height on the bottom toolbar.

The bottom toolbar can also be used to change the following for each individual node and shape:

- select the color of the node's icon or shape's lines;
- add a label.

For each connection, you can:

- select the color;
- add a label.

### Deleting objects

There are three ways of deleting one or several network map objects:

- using Delete on your keyboard (the only way of deleting multiple selected objects at the same time);
- from the object's context menu;
- by enabling deletion of map objects on the bottom toolbar and then selecting an object with the mouse.

When attempting to delete objects, you will be prompted to confirm the action.

If you delete a map node, its connections will also be deleted.

## Managing projects

If you have more than one network map project, use the drop-down list on the project's toolbar to switch between them.

You can change the project name using the Edit project item in the network map context menu or using the toolbar button.

To delete a project:

- enable the Edit mode;
- select the project from the list;
- click Delete map project on the toolbar or in the context menu;
- confirm its deletion.

# Authentication



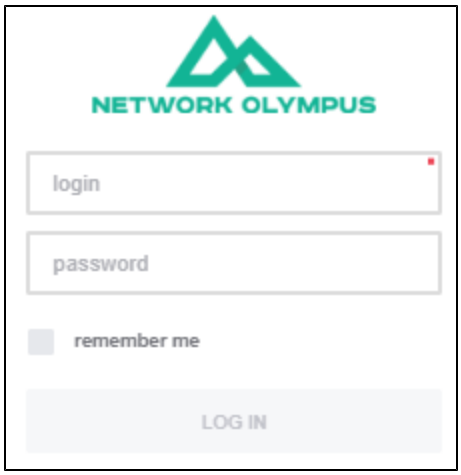
Authentication in Network Olympus is the process of verifying the identity of a user. It's performed by requesting a login and password.

On the dashboard, it may be required for:

- Logging into the Olympus system;
- Network scanning;
- Operation of sensors, actions and notifications.

## Logging in

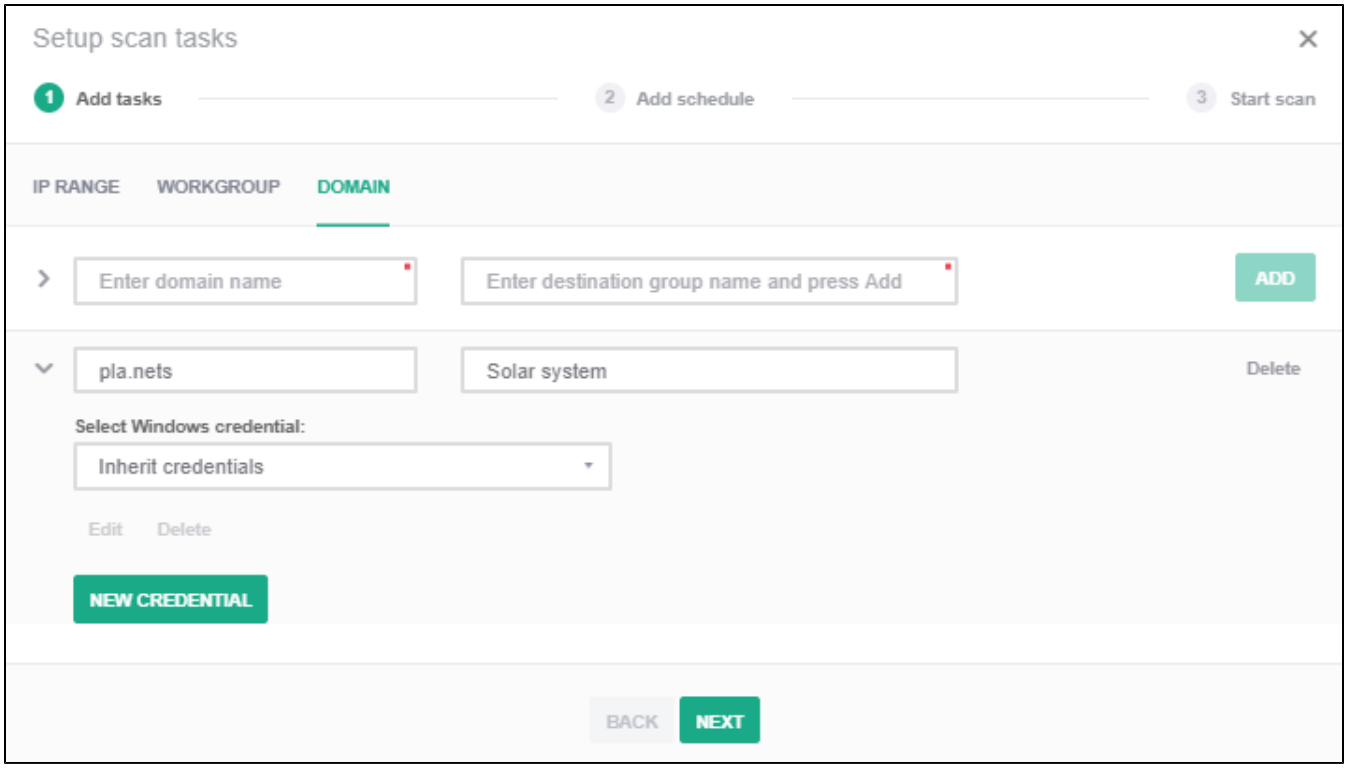
In order to log into the system, simply enter the login and password that were specified during the installation and press LOG IN or Enter on the keyboard.




If the checkbox is ticked, the system will remember the entered login and password, and you won't need to enter them again.

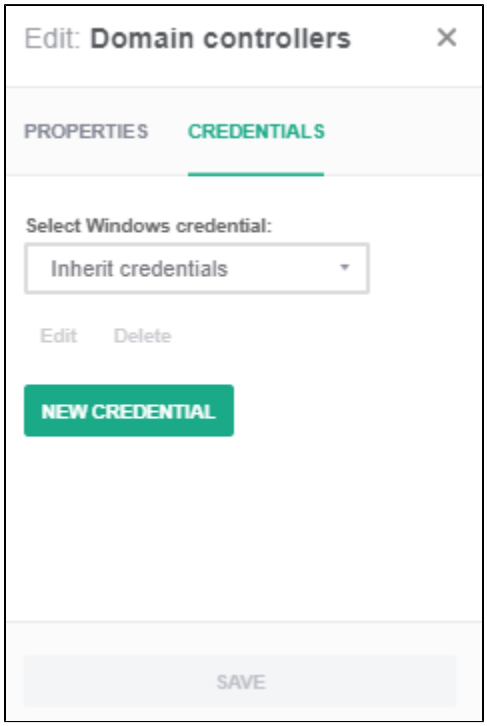
## Network scanning

When scanning the network, authentication may be required for Domain network groups.
Authentication data can be entered in the appropriate form by expanding the group options when adding a task in the Scanner wizard.




## Authentication for sensors, actions and notifications

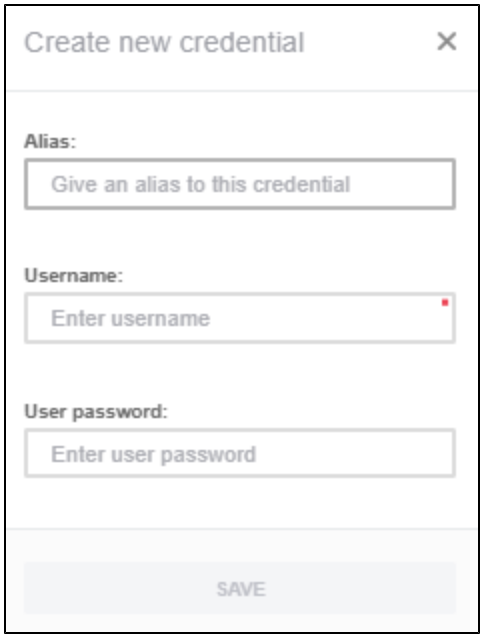
Authentication for any given sensor (action, notification) is made using the login of the device where this sensor (action, notification) is executed. You can assign a login to a device (or a group of devices) on the Credentials tab when editing or adding a new device (or group).




If the Inherit credentials option is selected, then the procedure of searching for logins towards the top of the network tree hierarchy will be used (i.e. the login of the parent group of devices will be taken). If the group has no logins assigned to it, then the higher group will be searched, and so on, up to the root node.

The default login option means using the login created by the system during the installation. Usually, it's a blank login and password.

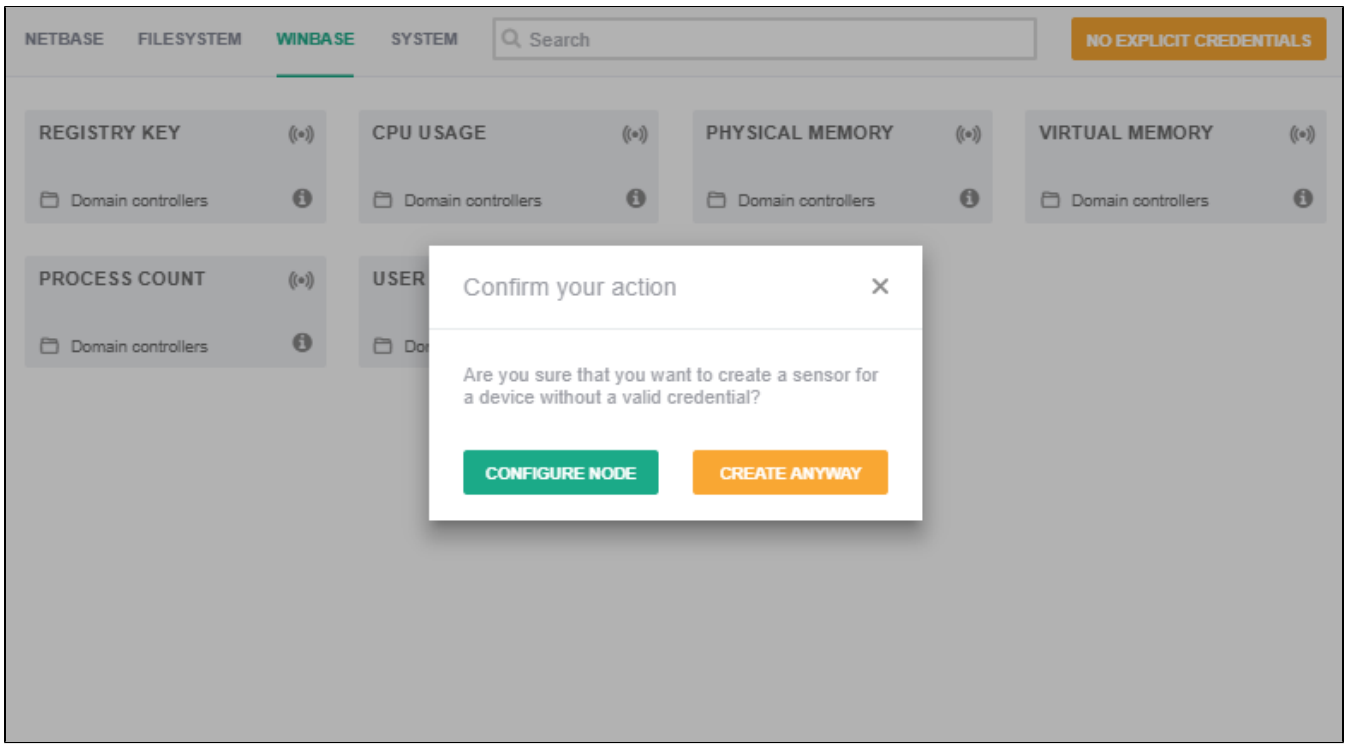
You can also create a new login by selecting New credential.




Specify a unique identifier for the login in the Alias field. This identifier will be displayed in the list of logins. Thus, you'll be able to select the same login for many sensors (actions, notifications).

Then enter the Username and User password and confirm the creation of the new login by clicking Save.

You can also assign a login when adding sensors (actions, notifications) to a device or a group by clicking the Node has no explicit credentials warning. This must be done for those sensors that may require authentication (for example, for the check for file existence).



# Database support

Network Olympus uses the PostgreSQL database to store information.

Database access can be provided during the installation of Network Olympus.

> To setup the connection to an external database, you must provide an account username and password.

## Working with PostgreSQL

Comes bundled with Network Olympus.

Suitable in most cases. Installation doesn't require any additional actions from the user.

The Network Olympus installer will prompt you to set the administrator account parameters for the installed database cluster. This data may be needed later if migrating to another DBMS becomes necessary.

The PostgreSQL server uses TCP port 5432. Before installing, make sure that this port is not taken by any other application.

Windows Firewall rules will be created automatically.

> Uninstalling Network Olympus will lead to the deletion of the Olympus database and uninstallation of PostgreSQL. In order to be able to preserve and then restore your database on a new installation, create a backup before uninstallation.

# Backup and restore

Network Olympus provides the ability to create backups of the database used by the application.
A backup can be used to restore the previous version of the database, for example due to loss of information in the live version.

In the current version of Network Olympus, database backups can only be done manually.

## Working with PostgreSQL

A backup must be performed on the computer where Network Olympus is installed.

Before creating a backup, it's important to stop the Network Olympus Core Service (OlympusCore).

Tools used for creating backup and restoring are located in the application folder: C:\Program Files (x86)\Network Olympus\Database\bin by default.

> Successful restoration from backup can only be guaranteed on the same application version as was used to make the backup.

To create a backup, use the following command:

pg_dump.exe -h localhost -p 5432 -d olympus -U root -w -c -f backup.sql

To restore from a backup:
psql.exe -h localhost -p 5432 -d olympus -U root -w -f backup.sql

where 5432 is the default port used by the database;
root is the database owner's default username;
backup.sql is a user-defined name of the file containing the backup.

The port can be set during the installation of the program.
If these values have been changed, you can look them up in the registry at HKEY_LOCAL_MACHINE\SOFTWARE\SoftinventiveLab\Olympus\Database

> Modification of this registry string may cause program malfunction.

# Remote management and mobile access

Browsers supported by Network Olympus can be used to access the application's interface from devices on the local network.

Enter the IP address of the server where Network Olympus is installed, as well as the port number that was specified during the installation, into the address bar.

For example: https://10.0.0.55:3000

## Access from a smartphone

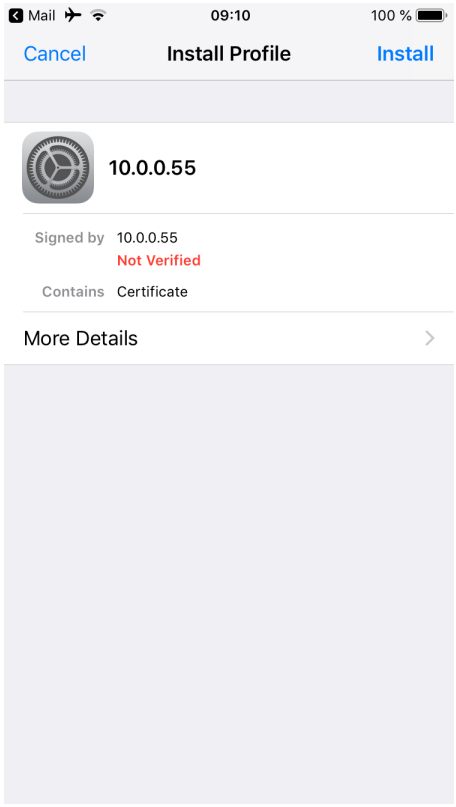
Android devices can access the Network Olympus interface without any issues.

Before connecting using an iOS device in secure mode (HTTPS), the following has to be taken into account. By default, a self-signed certificate is generated during the installation of Network Olympus. The OS recognizes this certificate as untrusted and blocks the connection.

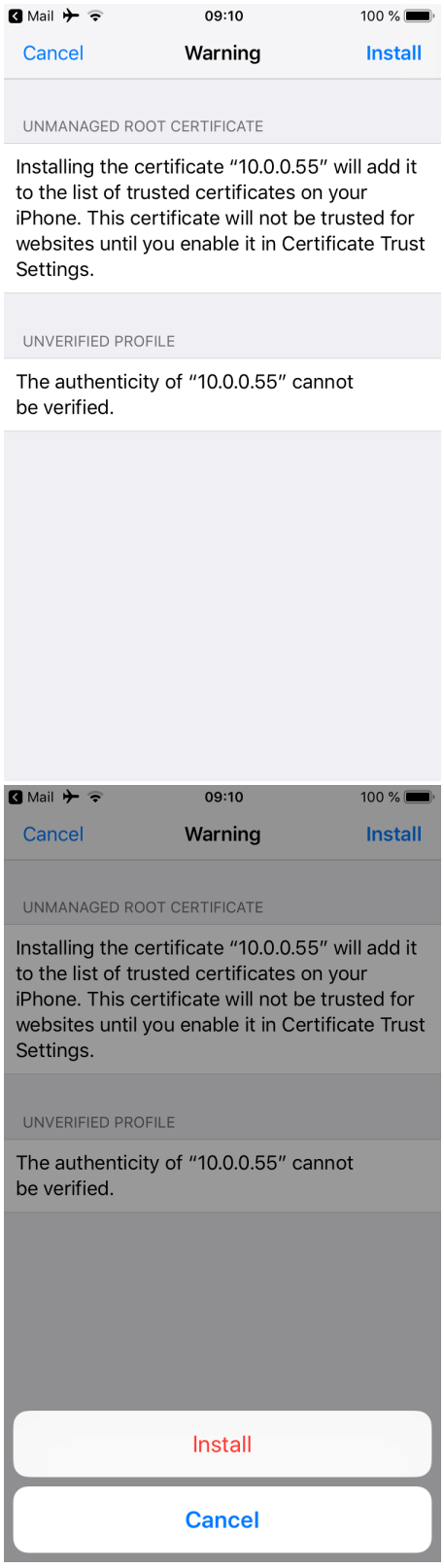
There are two ways of solving this issue:

- You can purchase your own web server certificate, or provide the one you already have.
  The application's installer allows you to select your own certificates.
  If the application is already installed with a self-signed certificate, then replace the certificate files in \Network Olympus\Bin\Certs\
- Install the default, self-signed certificate on the iOS device.
  The file is located in the following application subfolder: \Network Olympus\Bin\Certs\ca.cer
  It must be copied to the device and installed.
  - How to install the certificate

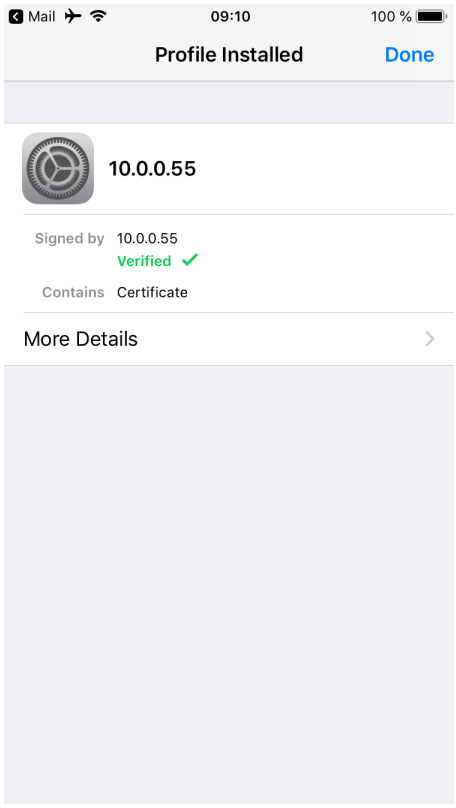
    Upload the certificate to the device.
    For example, send it by email.




Click Install and confirm again:



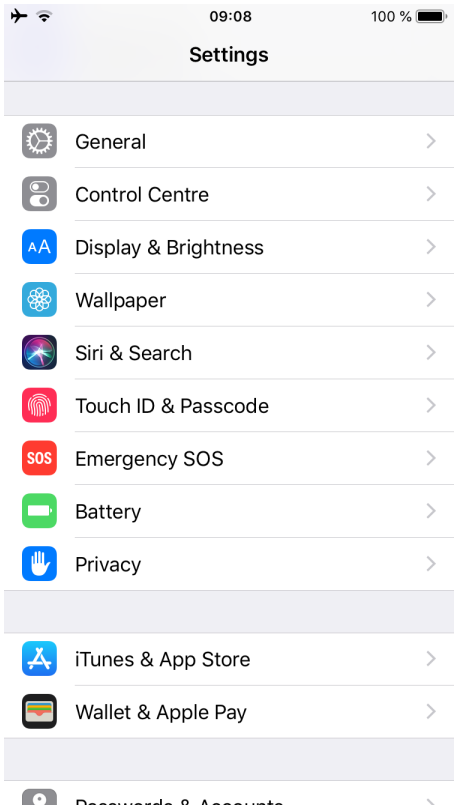

This results in a verified profile:

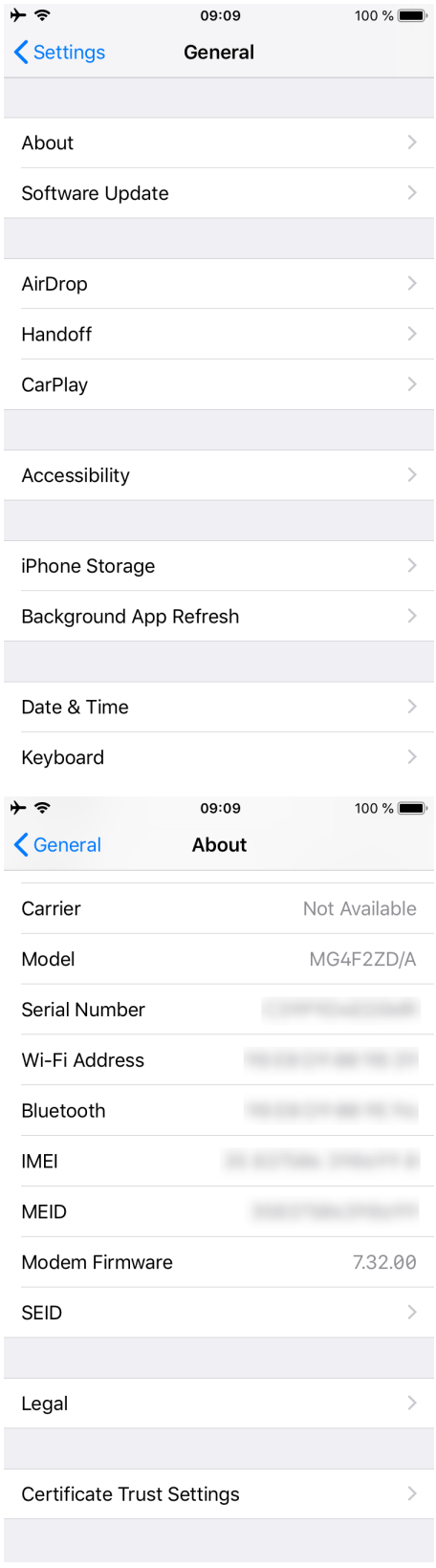



Now you need to make the certificate trusted.

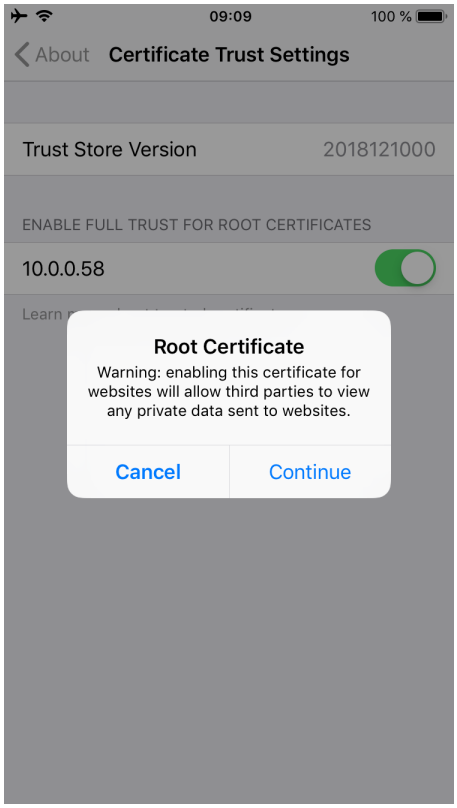
How to make the certificate trusted

Go to Settings → General → About → Certificate Trust Settings:






Enable the installed certificate by tapping it and confirm:


09:09
100 %
About
Certificate Trust Settings
Trust Store Version
2018121000
ENABLE FULL TRUST FOR ROOT CERTIFICATES
10.0.0.58
Root Certificate
Warning: enabling this certificate for websites will allow third parties to view any private data sent to websites.
Cancel
Continue