NAICE

Version: 0.8-11421
Date of publication: 20.06.2025

Table of Contents

Home Page

Description

The NAICE system home page serves as a dashboard containing a set of widgets. The widgets display key system performance indicators, providing summary information about its current state over the last 24 hours. Automatic data refresh is implemented for all widgets with a 2-minute interval.

Dashboard features:

- Widget set configuration is saved individually for each administrator;
- All changes to widget arrangement and composition apply only to the current administrator;
- The system automatically saves settings between work sessions.

Main page elements:

- `Control Panel` - located at the top of the interface, contains main dashboard controls;
- `Widget Set` - configurable workspace containing informational widgets with key system metrics.

Viewing the dashboard panel

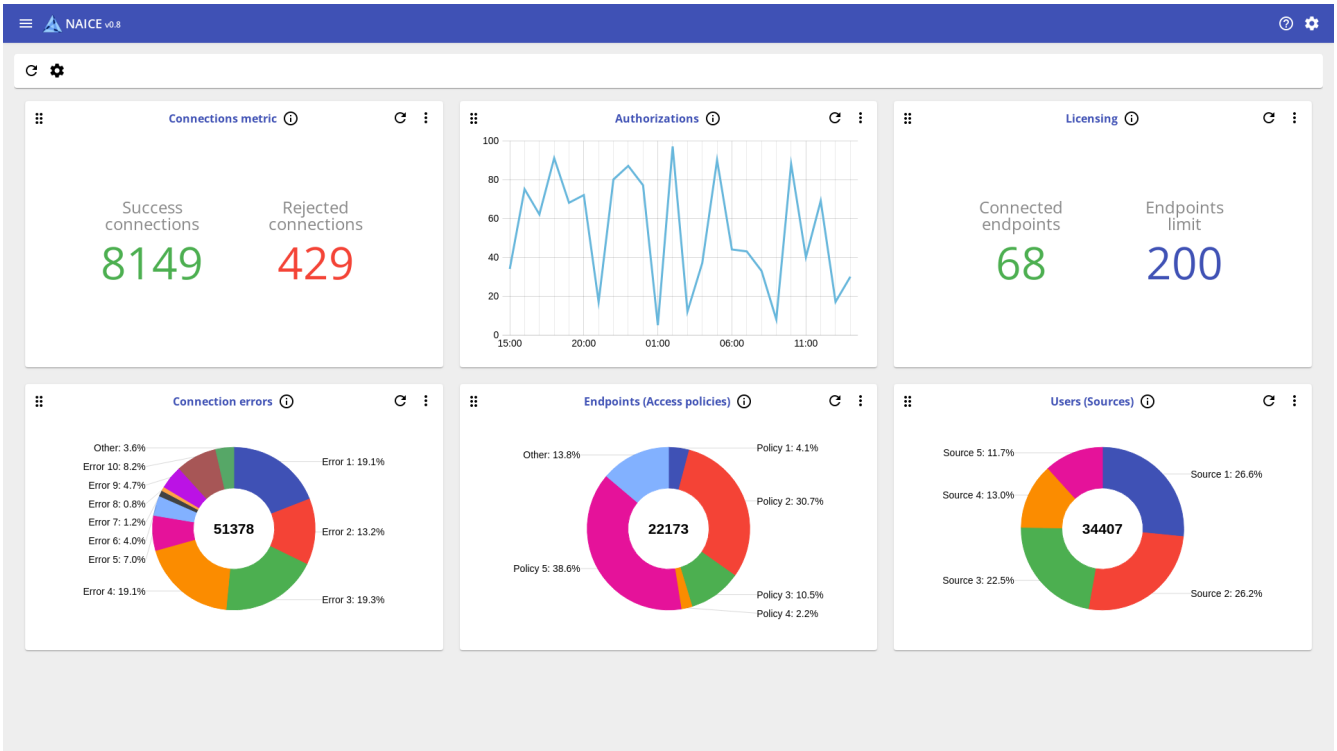

Figure 1. Dashboard control panel and displayed widgets

Dashboard control elements:

-  - Refresh data for all widgets displayed on the dashboard.
-  - Open the dashboard panel settings window.

Each widget consists of the following control elements:

- - Used to change widget order.
- "Authorizations" - Widget name. Serves as a hyperlink to the parent page.
- - Brief information about the widget.
- - Refresh data for this specific widget.
- - Action panel for the widget (e.g., delete).
- Data visualization area in the specified display format.

Configuring dashboard widgets

To select widgets for display on the dashboard, click , which will open the **Dashboard panel settings** window:

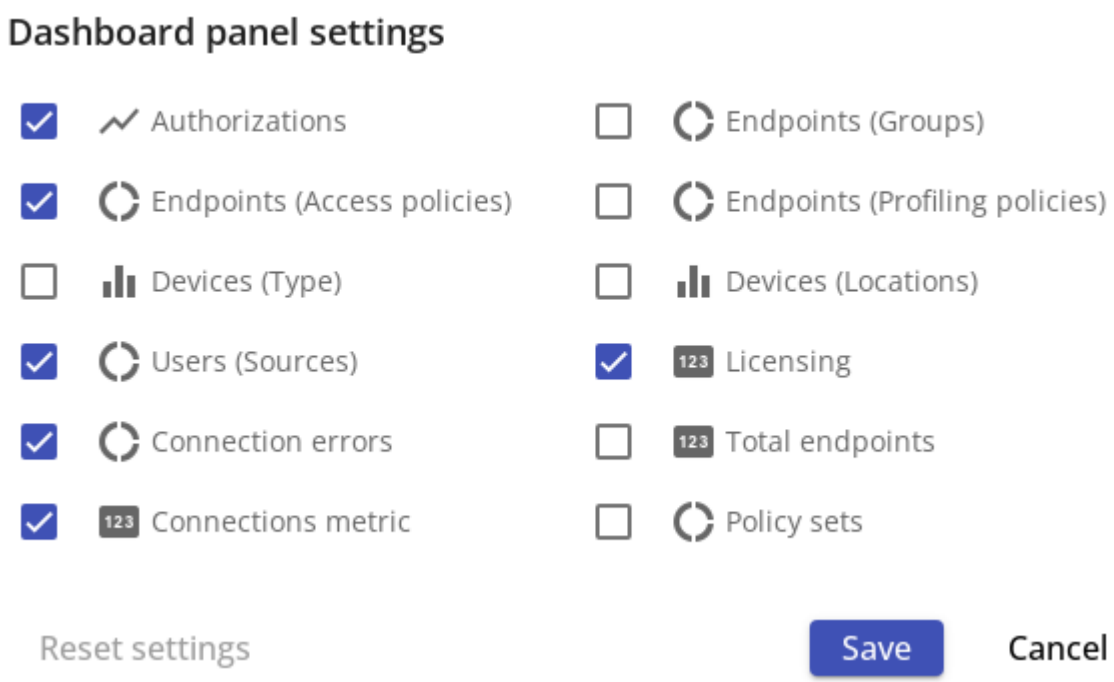

Figure 2. Dashboard panel settings window

The **Dashboard panel settings** window contains the following controls:

- - Checkbox to select items for further action (add or remove).
- - Widget data display type. Four display types are supported - graph, histogram, pie chart, and metric.
- `"Authorizations"` - Widget name.
- `Reset Settings` - Return to the default widget set.

To add or remove a widget from the dashboard, select it using the checkbox and click the **Save** button. Widgets with checked checkboxes will be displayed on the dashboard.

List of available widgets

Widget	Data display type	Brief description
Authorizations	Graph	Count of authorizations per hour for the last 24 hours
Licensing	Two-number metric	Current count of connected endpoints and maximum allowed per license
Connection metrics	Two-number metric	Count of connected and rejected connections for the last 24 hours
Total Endpoints metric	Single-number metric	Total count of learned endpoints
Devices (Type)	Histogram	Count of network devices through which the client was connected, by network device type
Devices (Locations)	Histogram	Count of network devices through which the client was connected, by location of network devices
Endpoints (Groups)	Pie chart	Count of endpoints studied that were authorized in the last 24 hours, by group
Endpoints (Profiling policies)	Pie chart	Count of endpoints studied that were authorized in the last 24 hours, by profiling policy
Endpoints (Access policies)	Pie chart	Count of endpoints studied that have been authorized in the last 24 hours, by policy set
Policy Sets	Pie chart	Current count of policy set hit
Connection errors	Pie chart	Client connection errors for the last 24 hours
Users (Sources)	Pie chart	Count of unique users, by source of identification, who were authorized in the last 24 hours

Each widget has a specific data display type. The display type cannot be changed.

Standard widget set

The **standard widget set** is displayed by default when you first log in to NAICE.

The **Standard Widget Set** is a preset dashboard configuration with widgets that is displayed on the home page when you first log in to NAICE system. This set contains the most popular widgets to quickly understand the current state of the system.

The standard set of widgets can be reset using the “Reset Settings” button in the Dashboard panel settings window.

The standard set includes the following widgets:

Connection metrics;

- Authorizations;
- Licensing;
- Connection errors;
- Endpoints (Access policies);
- Users (Sources).

Widgets with display type — Graph 📈

`Functionality:`

- Graph navigation via click for detailed data examination.
- Zoom and time range selection using scroll functionality.
- Hovering over a graph point displays device count with a tooltip showing time and date.
- Default view restoration via button in the widget's top-right corner.

Widget "Authorizations"

Displays data about authorization attempts (both Connected and rejected) in the system per hour for the last 24 hours, based on User sessions data.

Data is visualized as a time graph where:

- Vertical axis (Y) shows authorization attempt quantity;
- Horizontal axis (X) represents hourly timeline.

Enables quick monitoring of user activity and peak period identification.

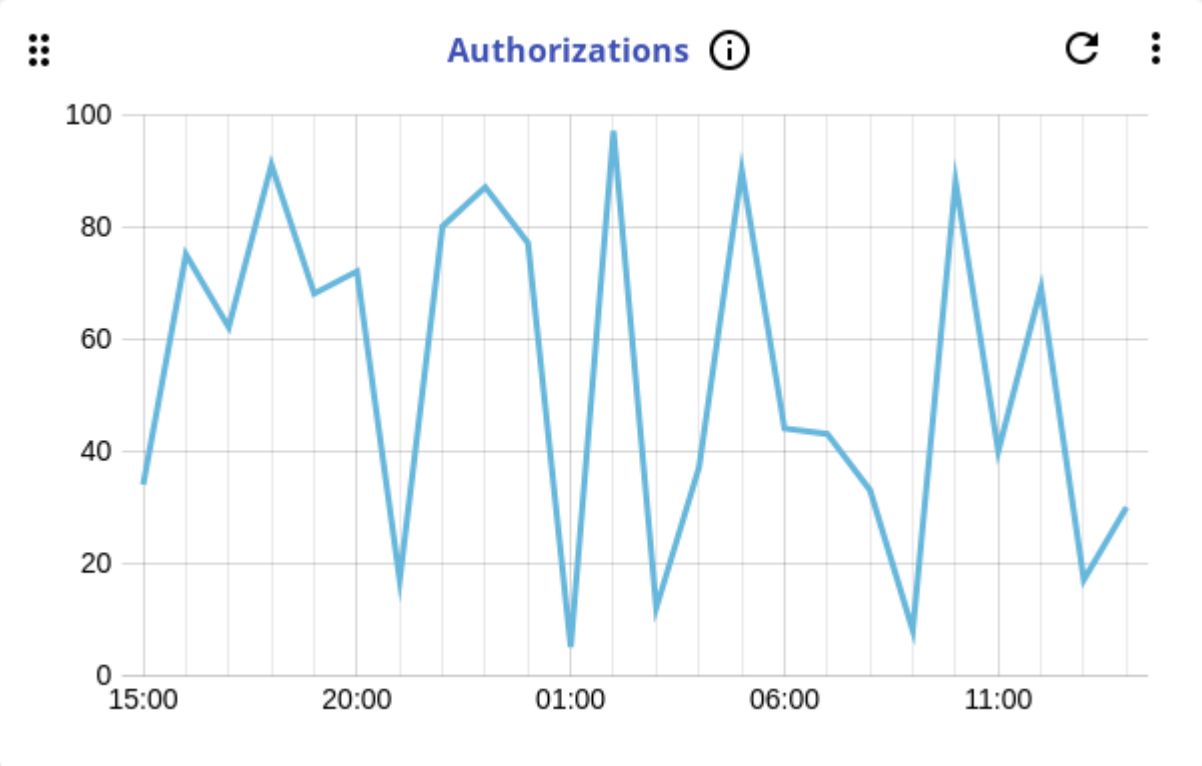

Figure 3. Widget "Authorizations"

Widgets with display type — Metric 123

`Functionality:`

- Compact display of key numerical indicators.
- Support for multiple simultaneous metrics.
- Numerical presentation for quick data comprehension.

Widget "Licensing"

Displays summary licensing information:

- `Connected Endpoints` - Current count of connected authorized unique endpoints for last 24 hours;
- `Endpoint Limit` - Maximum allowed count of endpoints according to the license.

Helps track endpoint limit proximity.

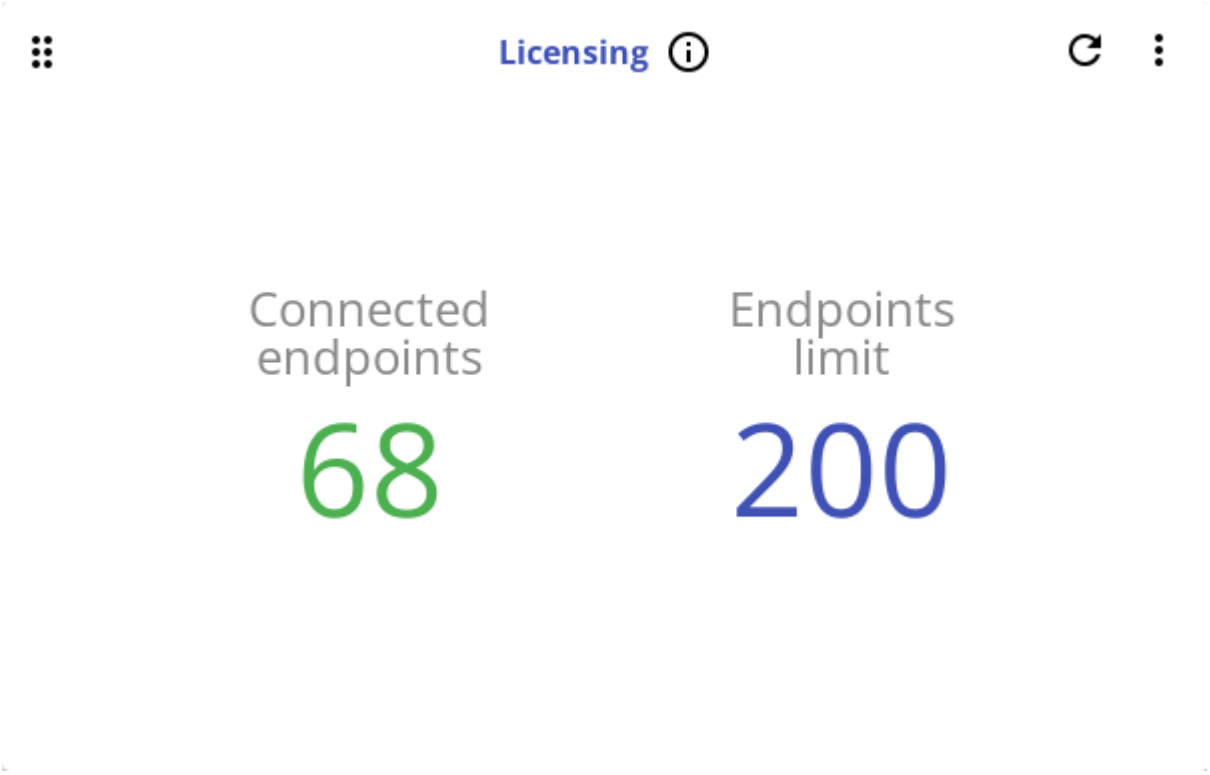

Figure 4. Widget "Licensing"

Widget "Connection metrics"

Displays connected and rejected connection counts for the last 24 hours based on User sessions data.

Shows session status ratio (connected vs rejected attempts) for daily tracking.

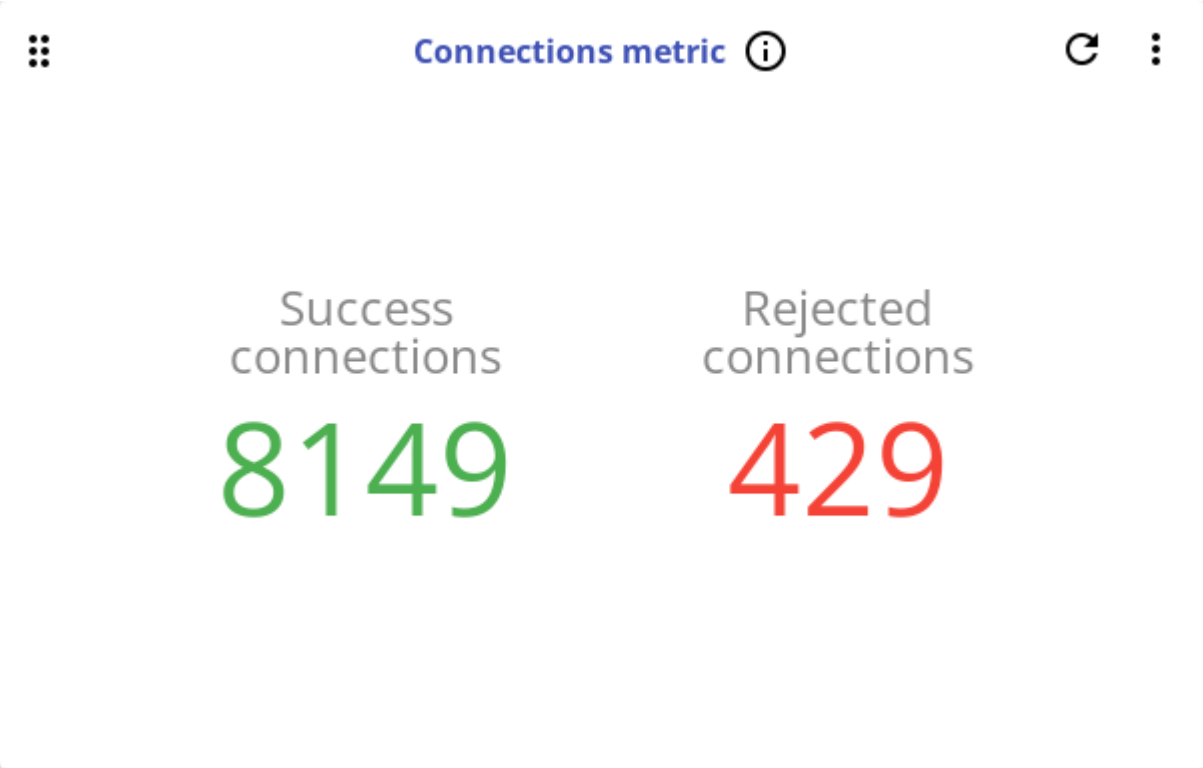

Figure 5. Widget "Connection metrics"

Widget "Total endpoints"

Displays the total count of known endpoints in the NAICE system based on data from the Endpoints table.

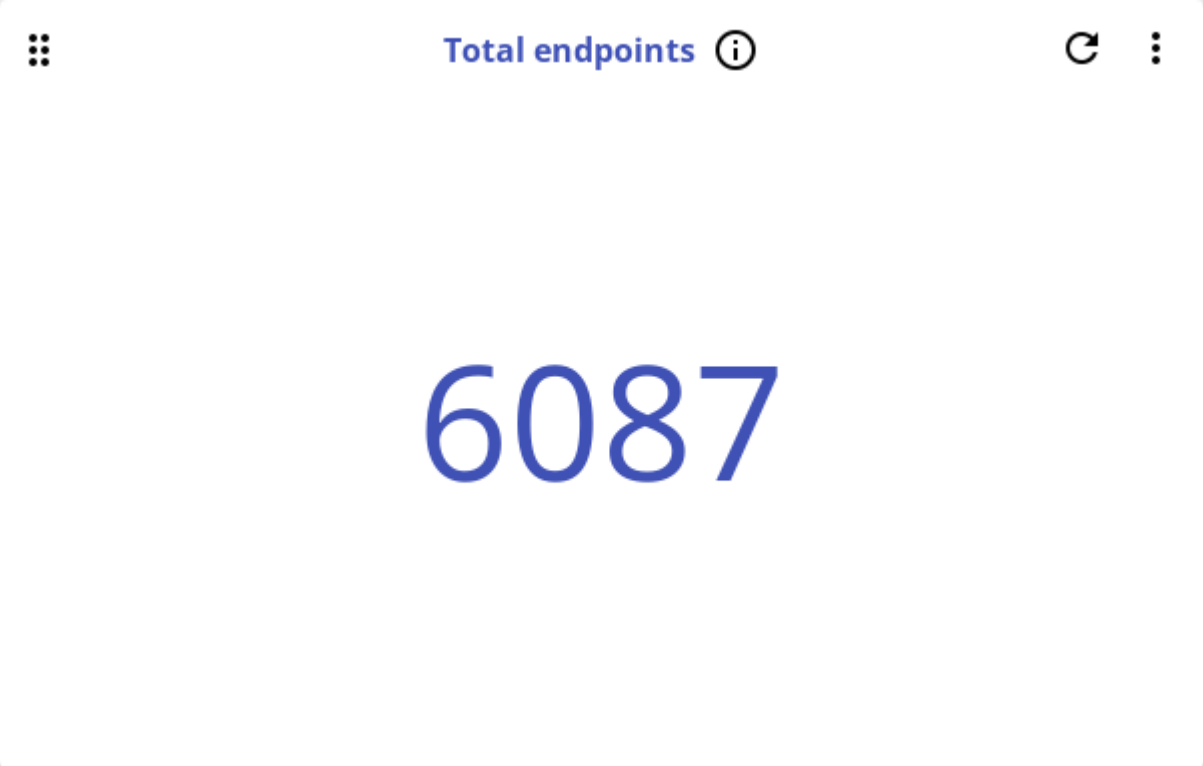

Figure 6. Widget "Total endpoints"

Widgets with display type — Histogram

`Functionality:`

- Each data segment includes a left-aligned name corresponding to the last nested group element.

- Value appears to the right of the data segment.
- Hover tooltip shows detailed information in the format: "Full nesting from last child to parent group: count".
- Limited to 10 data segments.
- Additional "Other" segment aggregates non-top-10 data.

Widget "Devices (Type)"

Displays the count of network devices by type through which client connections occurred.

Device groups for classification come from Device Groups.

Tracks device type usage trends.

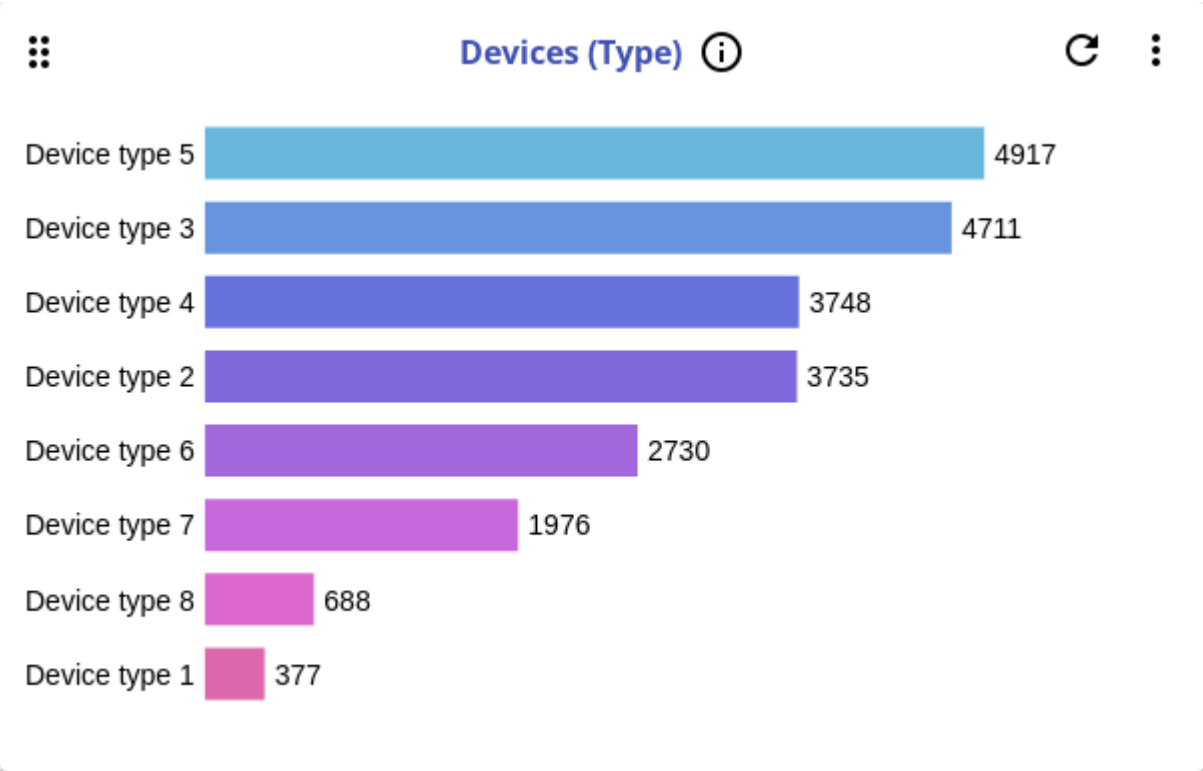

Figure 7. Widget "Devices (Type)"

Widget "Devices (Locations)"

Displays the count of network device by location through which client connections occurred.

Device groups for classification come from Device Groups.

Tracks device location usage trends.

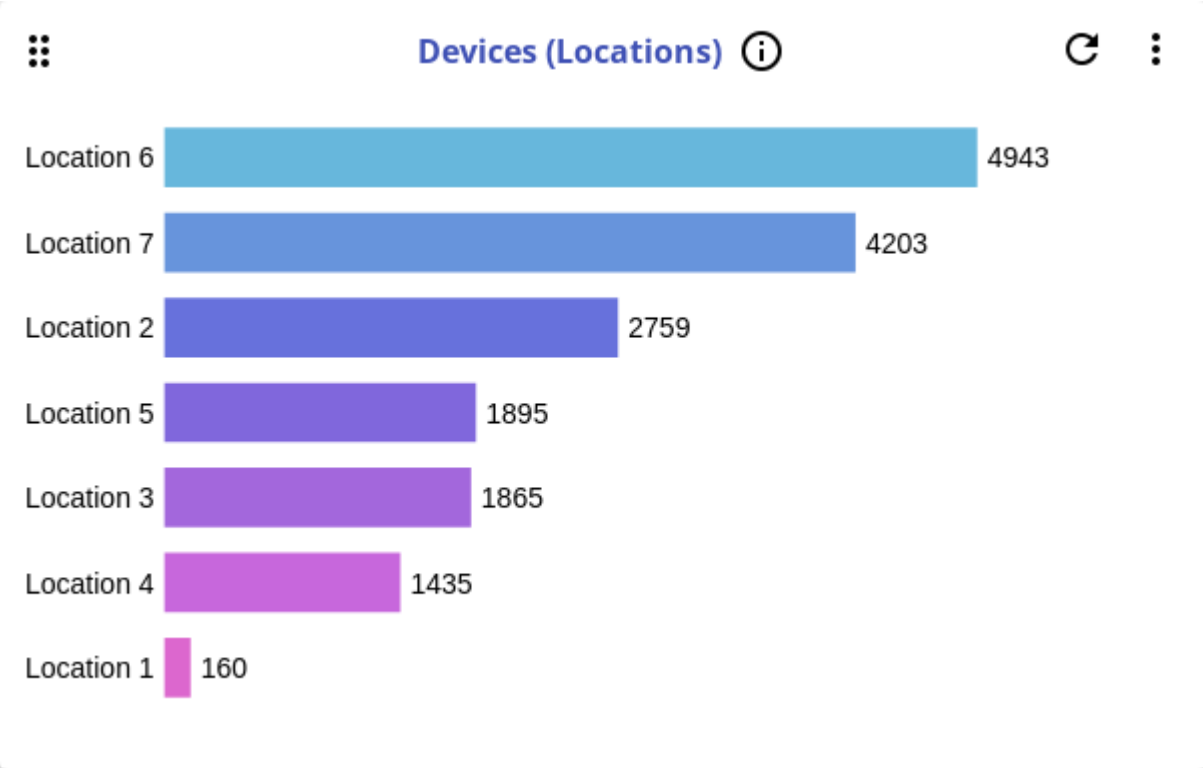

Figure 8. Widget "Devices (Locations)"

Widgets with display type — Pie chart

`Functionality:`

- Each segment is labeled in "Name: %" format.
- Hover tooltip shows "Name: % - count" details.
- Limited to 10 data segments.
- Additional "Other" segment aggregates non-top-10 data.

Widget "Endpoints (Groups)"

Displays the count of **learned** endpoints that underwent authorization in the last 24 hours, grouped by Endpoint Groups from profiling.

Data sourced from Endpoints and User sessions.

Uses the last group upon reconnection.

- Randomly generated MAC addresses are not counted.
- An endpoints is considered known if it is present in Endpoints table.
- *In automatic mode*, new endpoints added via RADIUS requests appear only after reconnection when system adds them to **Endpoints**.

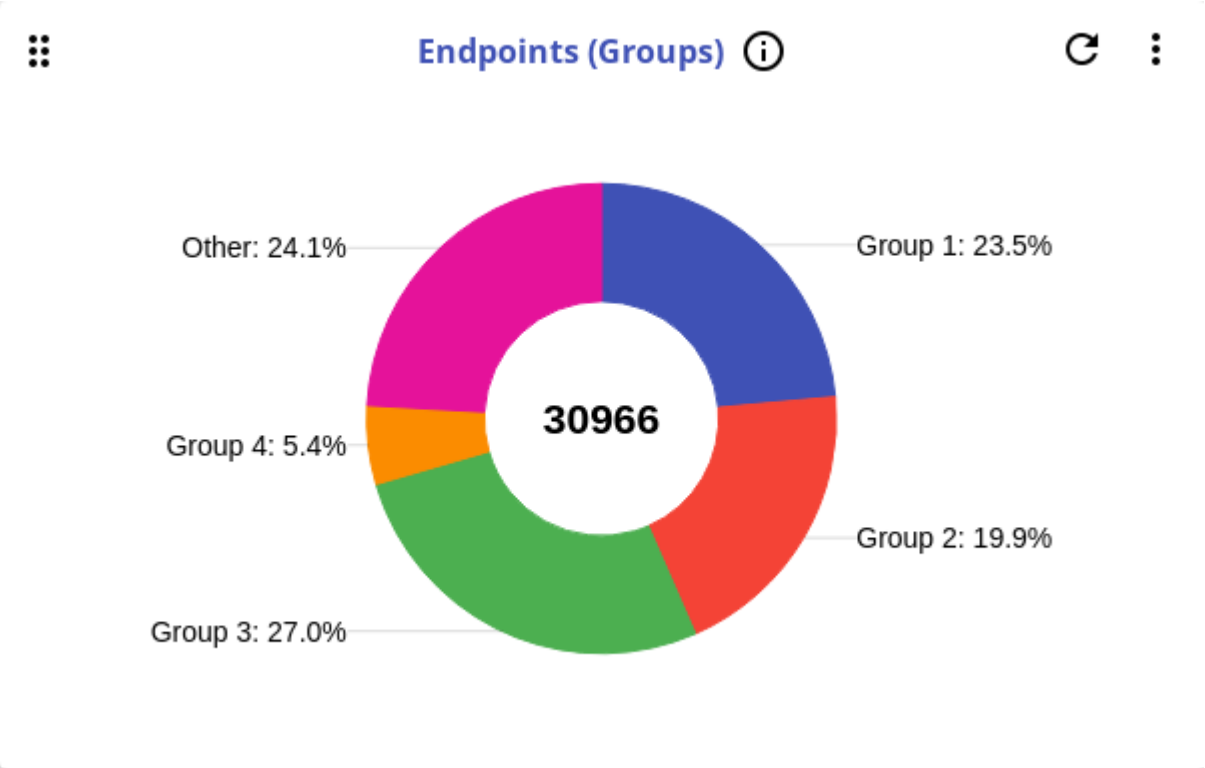

Figure 9. Widget "Endpoints (Groups)"

Widget "Endpoints (Profiling policies)"

Displays the count of **learned** endpoints that underwent authorization in the last 24 hours, grouped by Profiling policies from profiling.

Data sourced from Endpoints and User sessions.

The widget allows you to analyze the effectiveness of profiling policies and evaluate the distribution of endpoints to the profiling policies assigned to them.

Uses the last group upon reconnection.

- Randomly generated MAC addresses are not counted.
- An endpoints is considered known if it is present in Endpoints table.
- *In automatic mode*, new endpoints added via RADIUS requests appear only after reconnection when system adds them to **Endpoints**.

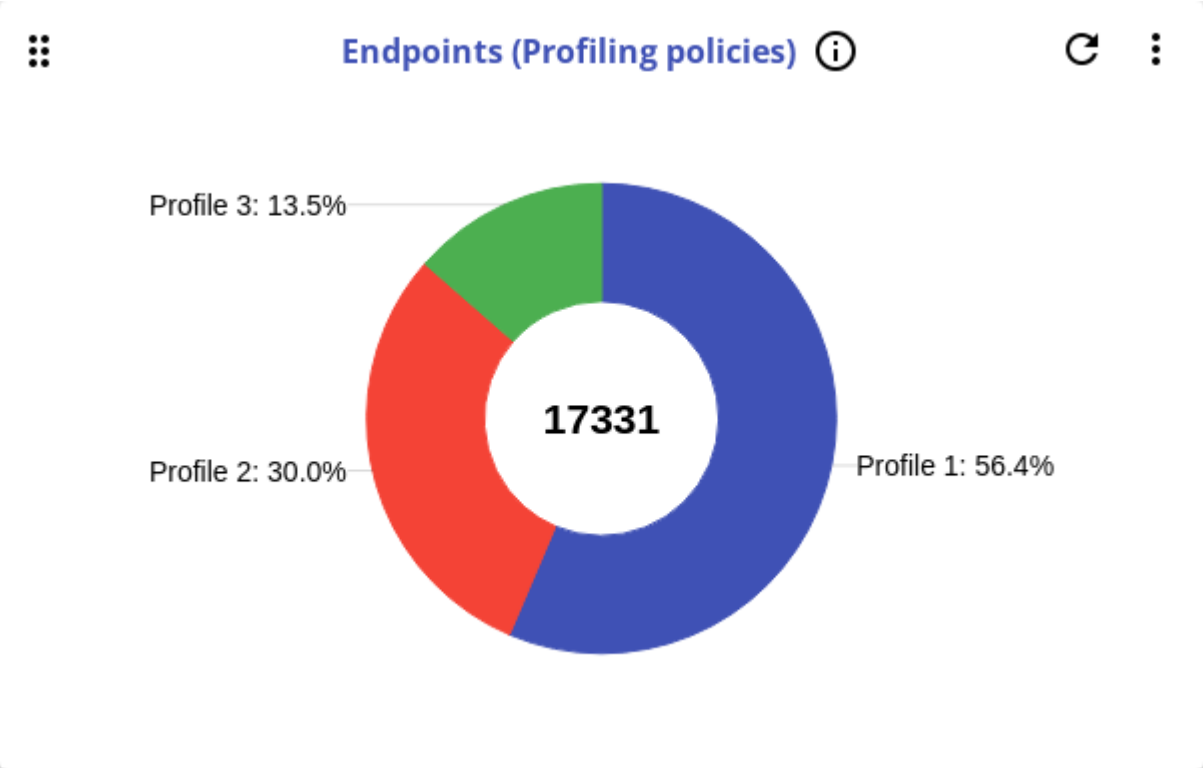

Figure 10. Widget "Endpoints (Profiling policies)"

Widget "Endpoints (Access policies)"

Displays the count of **learned** endpoints that underwent authorization in the last 24 hours, grouped by policy sets.

Data sourced from Endpoints and User sessions.

The widget allows you to evaluate the distribution of endpoints across access policies.

Uses the last group upon reconnection.

- Randomly generated MAC addresses are not counted.
- An endpoints is considered known if it is present in Endpoints table.
- *In automatic mode*, new endpoints added via RADIUS requests appear only after reconnection when system adds them to **Endpoints**.

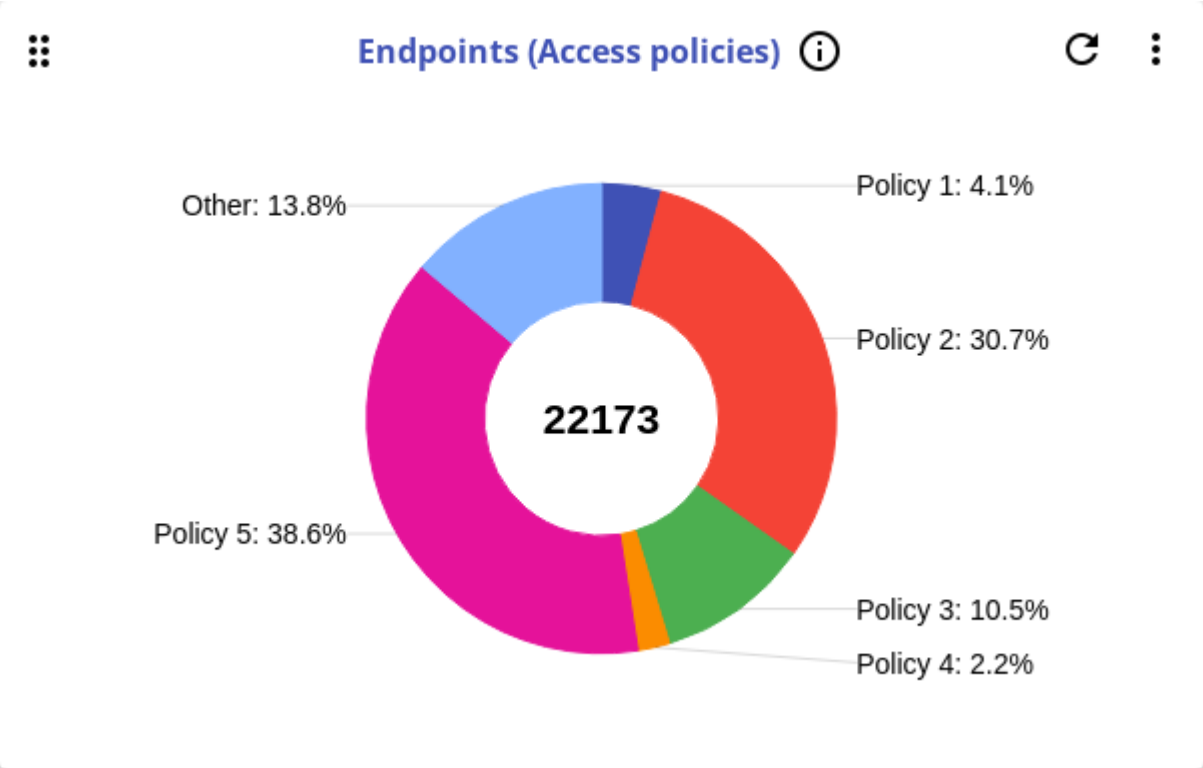

Figure 11. Widget "Endpoints (Access policies)"

Widget "Users (Sources)"

Displays unique user count by identification sources that underwent authorization in the last 24 hours.

Possible sources of identification:

- Internal DB - users from the system's internal database;
- Endpoints - devices when authorizing by MAC-address (MAB);
- External authentication systems (LDAP/Active Directory) configured in External identity sources.

The widget allows you to track the distribution of users authenticated through different identity sources.

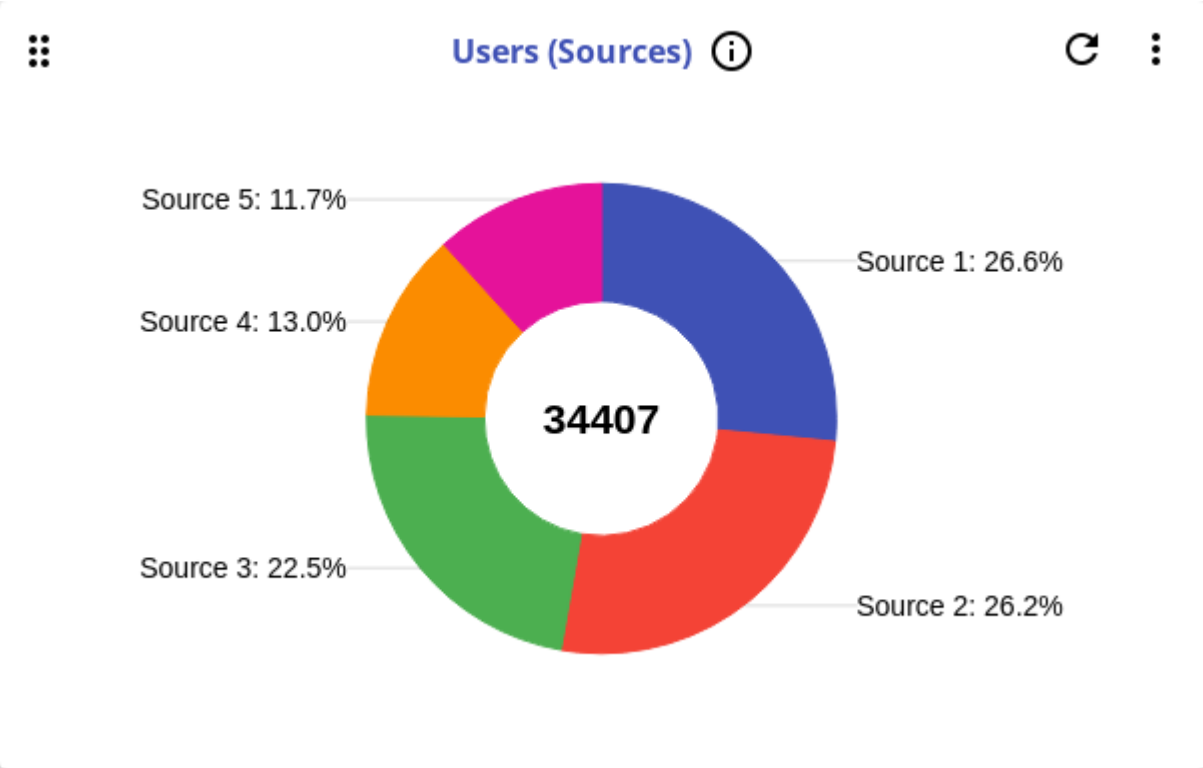

Figure 12. Widget "Users (Sources)"

Widget "Policy sets"

Displays the current count of policy set hit.

Policies with zero triggers are excluded.

Hits count data comes from the Policy Sets list.

The widget allows you to track the frequency of application of different sets of policies to analyze the effectiveness of access conditions.

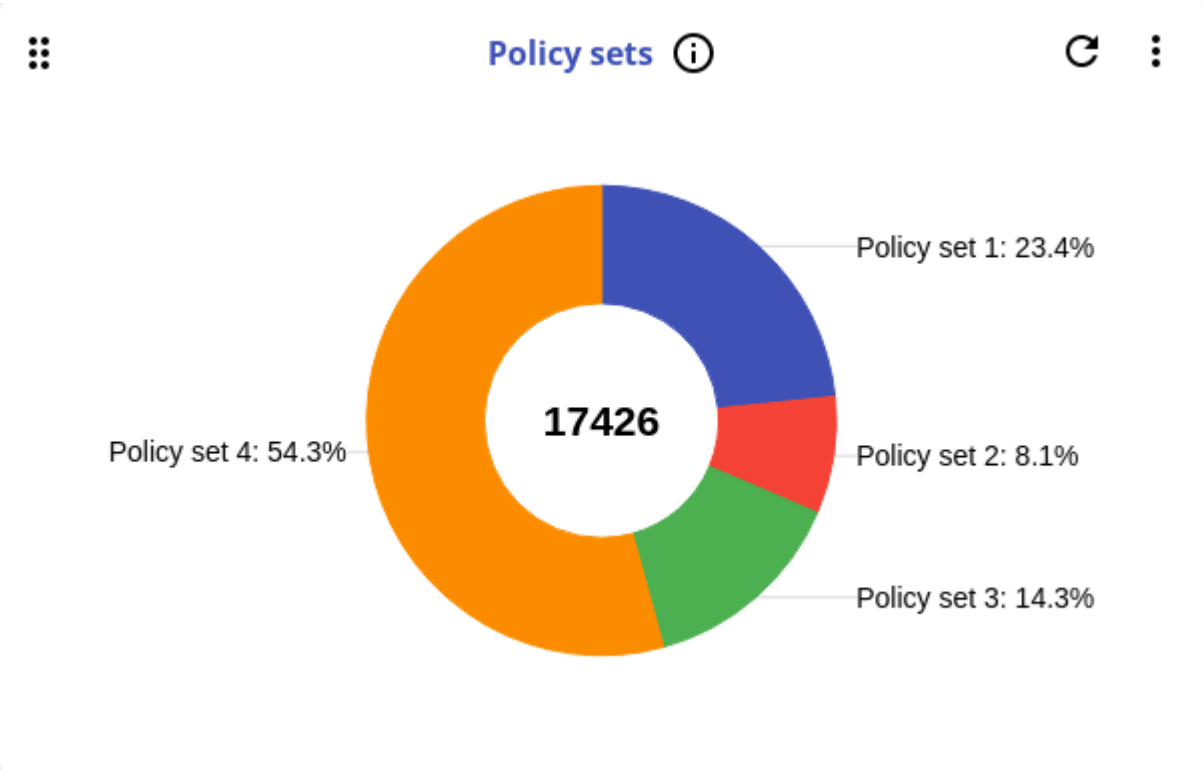

Figure 13. Widget "Policy sets"

Widget "Connection errors"

Displays client connection errors for the last 24 hours.

Connections rejected by access policies are not included.

Error data comes from User sessions.

The widget will allow you to identify and classify errors when connecting customers, excluding cases of deliberate blocking.

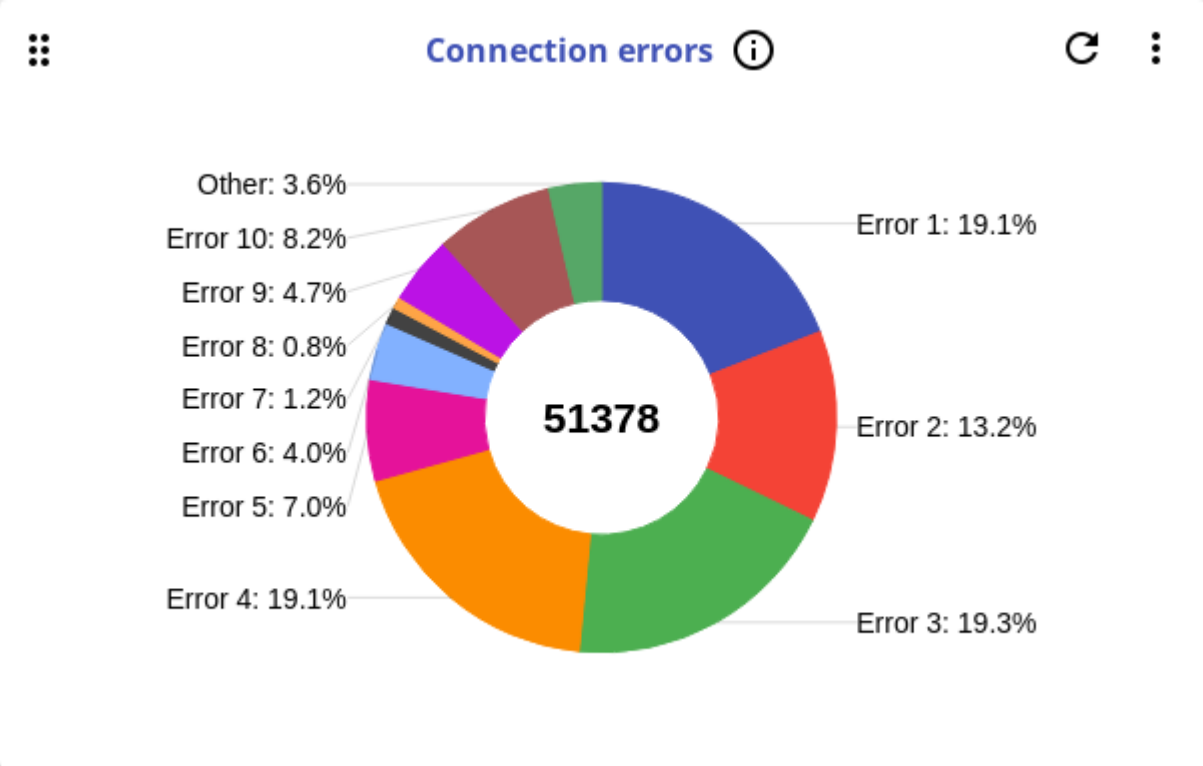

Figure 14. Widget "Connection errors"

Administration

Administrators

The Administrators section was created to manage the credentials of NAICE administrators.

View administrator accounts

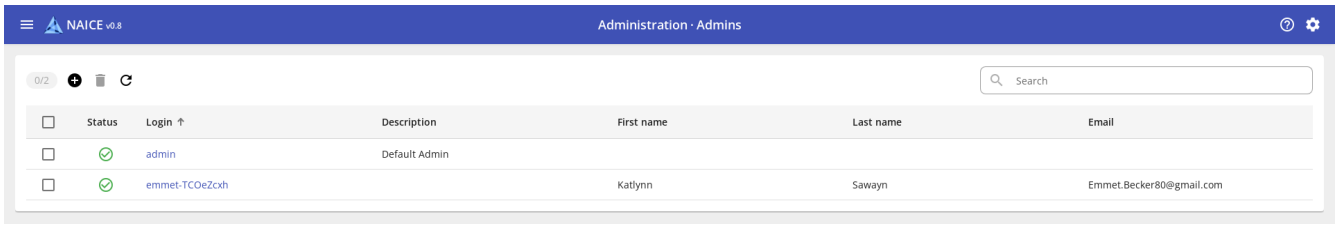

Figure 15. Table with a list of administrators on the view page

This page contains a table with a list of all system administrators.

The table contains the following information about system administrators:

- `Status` - controls permission to log in to the system: a disabled administrator will not be able to log in;
- `Login` - administrator login (must be unique);
- `Description` - arbitrary description;
- `Name` - administrator name;
- `Last name` - surname of the administrator;
- `Email` - administrator's email address.

Sorting in forward and reverse order across all columns of the table is allowed. By default, sorting is performed in direct (alphabetical) order by the "Login" column.

Controls:

- `Search` - Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.
- - Refresh table data.
- `0/1` - Counter of elements selected by the checkbox / total number of elements.
- - Add a new element.
- - Delete selected elements (inactive until at least one element is selected).
- - Change the current sort order.
- - Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).

Adding an administrator account

To add an administrator account, click on the action bar located above the table.

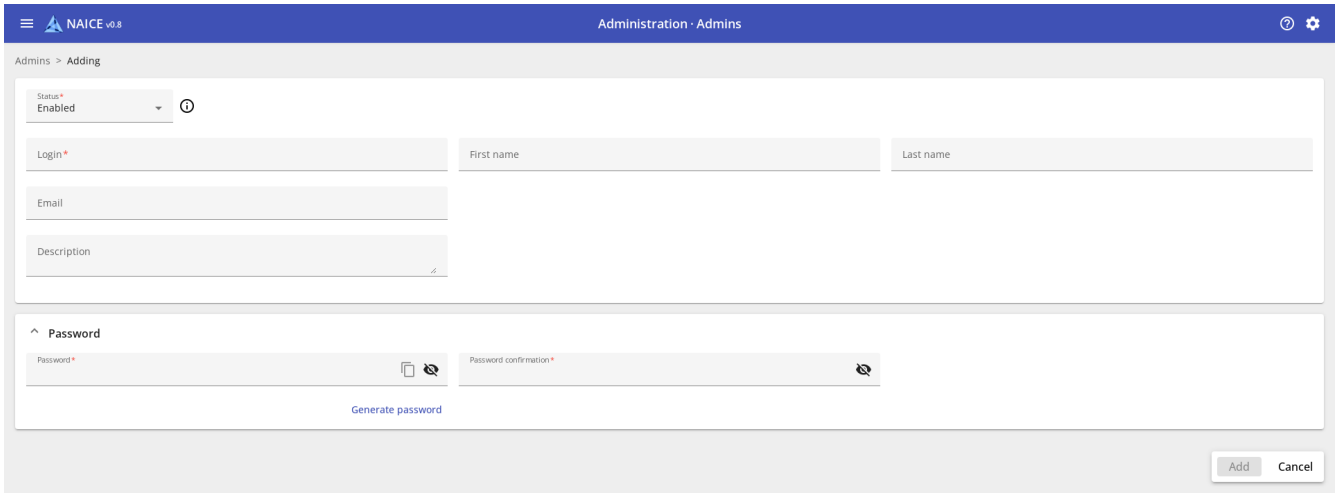

Figure 16. Add administrator page

The add administrator form includes the following fields:

- `Status` * - enable or disable the ability to log in to the system for this account;
- `Login` * (maximum length - 100 characters);
- `Name` (maximum length - 100 characters);
- `Last name` (maximum length - 100 characters);
- `Email` (maximum length - 100 characters);
- `Description` (maximum length - 250 characters);
- `Password` (maximum length - 100 characters);
- `Password confirmation` (maximum length - 100 characters).

* - fields that are required.

The password for logging into the administrator account can be generated by clicking on the **"Generate Password"** button, or you can enter it manually. The generated password is placed in the “Password” and “Password Confirmation” fields; it can be copied by clicking on .

After entering the required data, click the **"Add"** button.

Editing the administrator account

To edit an administrator account, on the list page, click on its login:

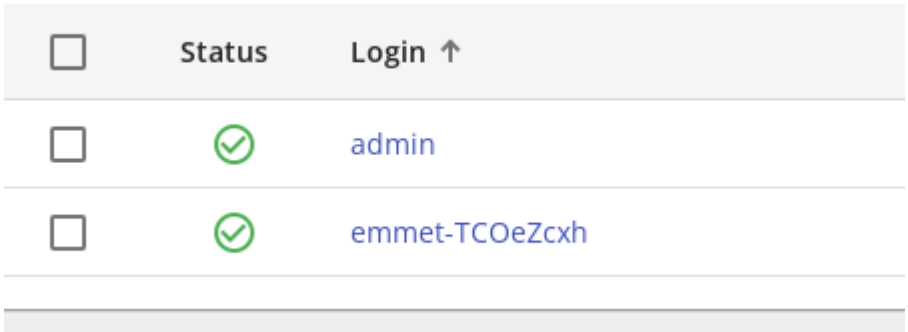

Figure 17. Hyperlink to admin edit page

This will open the admin edit page, similar to the add page:

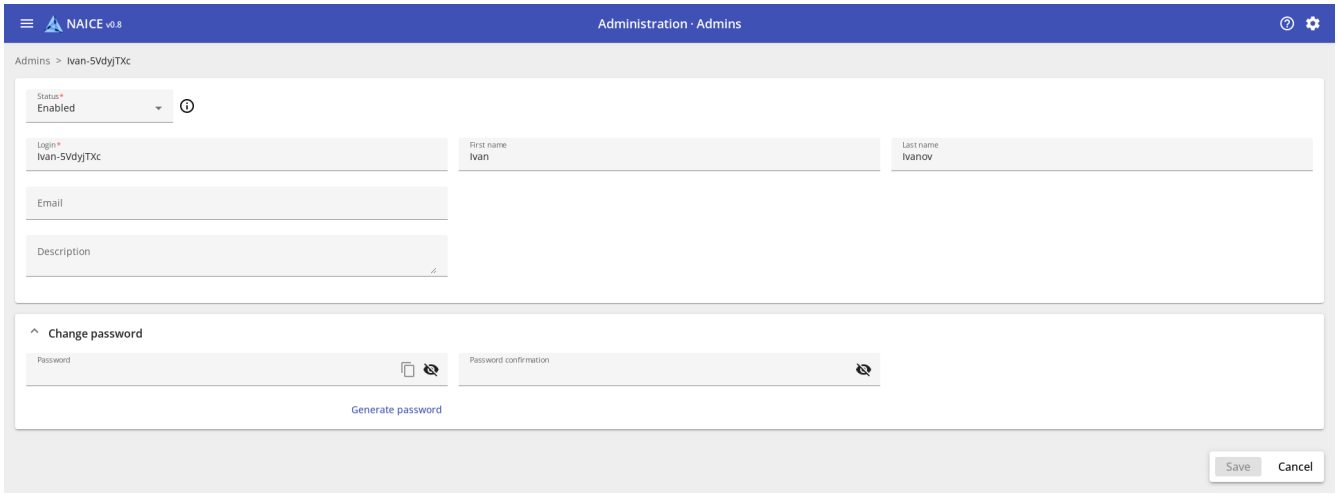

Figure 18. Admin Edit Page

After editing, click on the **"Save"** button. The button remains inactive until at least one field is changed.

Removing the Administrators account

To delete an administrator account in the window with a list of administrators, select the checkbox to the left of the accounts that you want to delete and click the button at the top left.

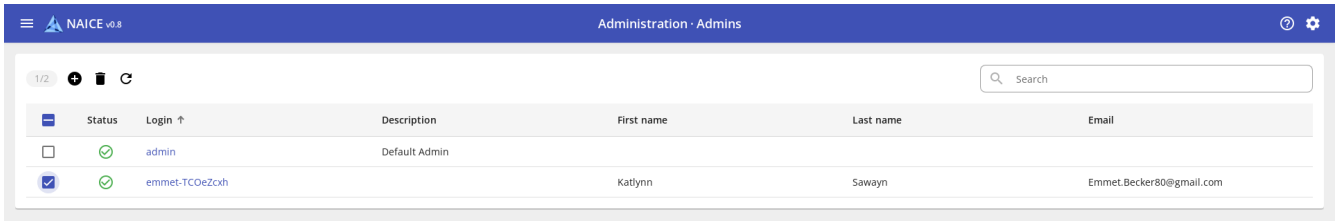

Figure 19. Selecting administrators in the table to delete

Deletion requires confirmation of the action, for which a modal dialog will open. After explicit confirmation, the selected items will be deleted.

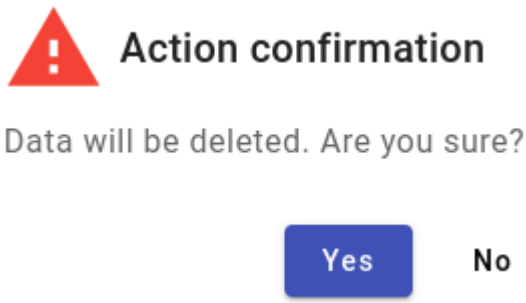

Figure 20. Modal dialog for confirmation

You cannot delete an account that is currently logged in.

Setting up the current administrator account

The current administrator's account settings are available on any page by clicking on in the upper right corner of the window in the **"Account Settings"** submenu.

On this page, you can view the credentials of the current administrator (with whose account you are logged in), as well as change the interface language. The following languages are supported: Russian, English.

The time zone setting affects the displayed time of the endpoint's last activity when monitoring connections.

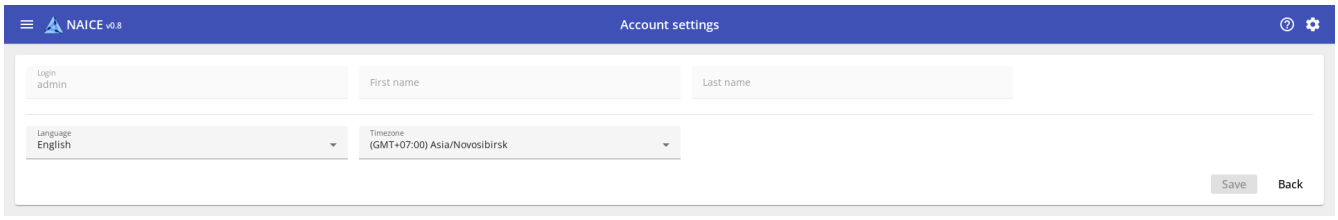

Figure 21. Setting up the current administrator account

The **"Save"** button saves the changes made to the account, the **"Return"** button returns to the page from which you went to Account Settings.

Change current administrator (logout)

To log out of the system on any page, you must click on ⚙ in the upper right corner of the window and select the submenu **"Logout"**.

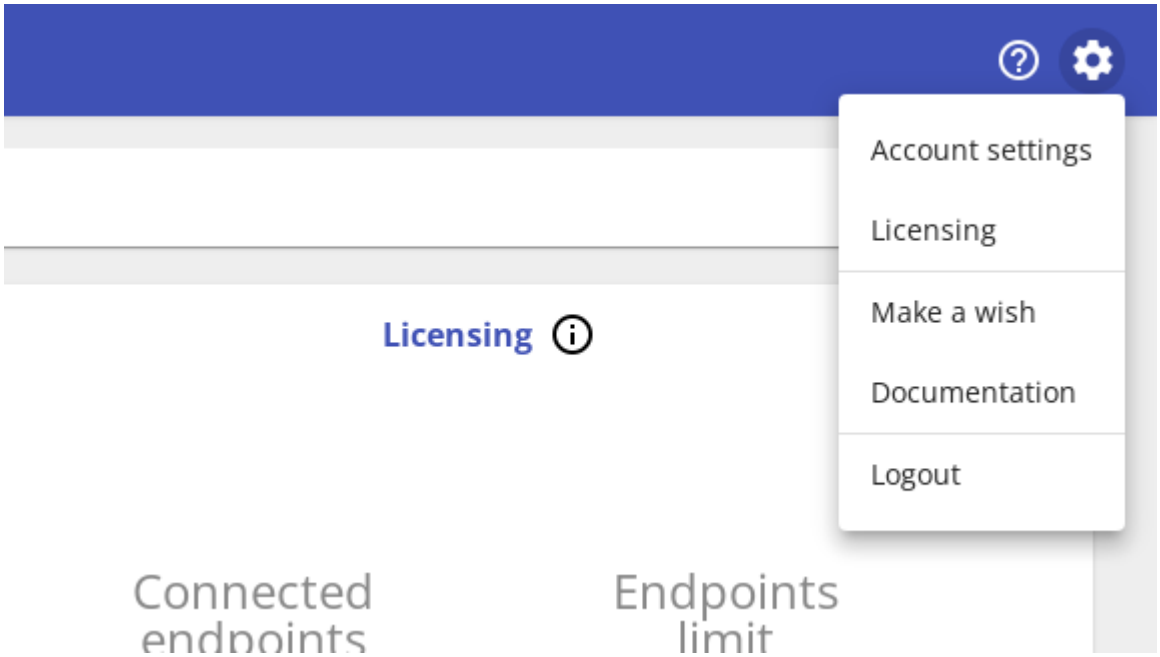

Figure 22. Menu item Logout

Next, you need to confirm logging out of the system by clicking on the **"Log Out"** button.

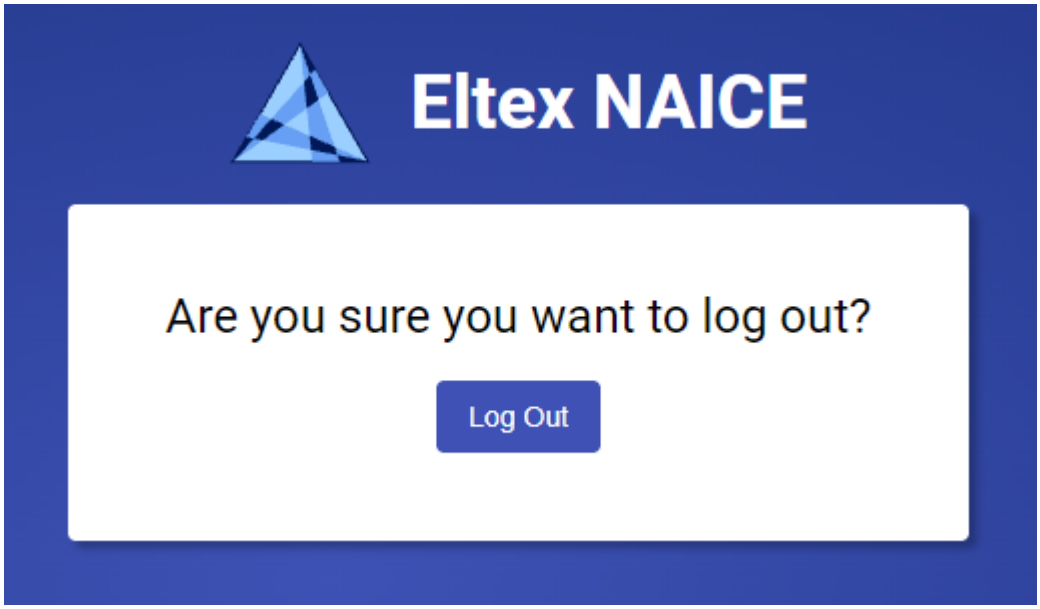

Figure 23. Logout confirmation page

After which you will be redirected to the authorization page.

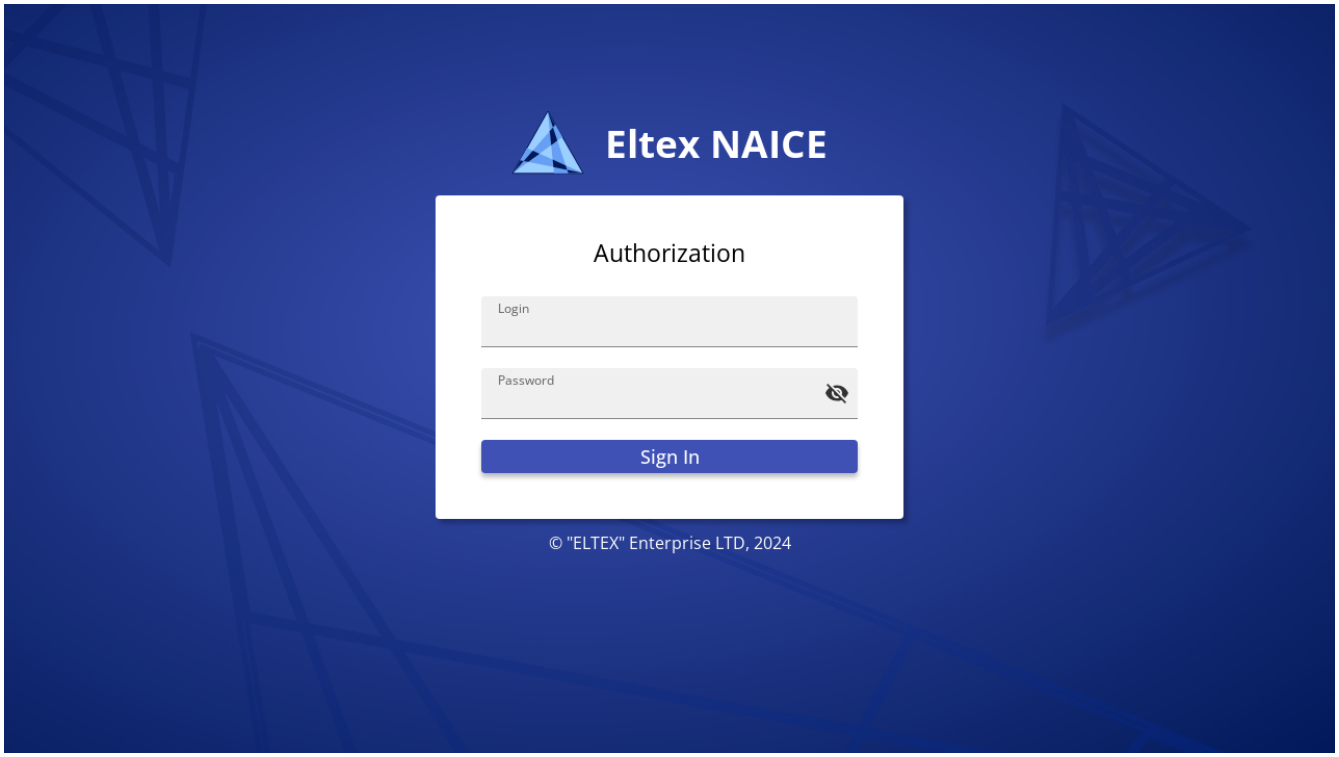

Figure 24. System login page

Network resources

Network device (authenticator, NAS - Network Attached Storage) - a station device that connects client devices to the network and implements their authentication using the 802.1x protocol, MAB or portal authorization.

Network devices are managed in the *"Administration"* → *"Network resources"* menu.

Contains sections:

- Devices - section for settings for interaction with network devices;

Device groups - section for setting group characteristics that can be used when configuring network devices;

- Device profiles - profiles that describe the features of interaction between network devices via the RADIUS protocol.

Devices

Description

Network device (authenticator, NAS - Network Attached Storage) - a station device that connects client devices to the network and implements their authentication using the 802.1x protocol, MAB or other types of connections.

The "Devices" section is responsible for viewing, adding, deleting, editing network devices in the NAICE system.

If the device has not been added to the system, then the request for authorization via the RADIUS protocol from it will not be processed!

It is important to understand that creating a new device is impossible without the created device profile.

View a list of network devices

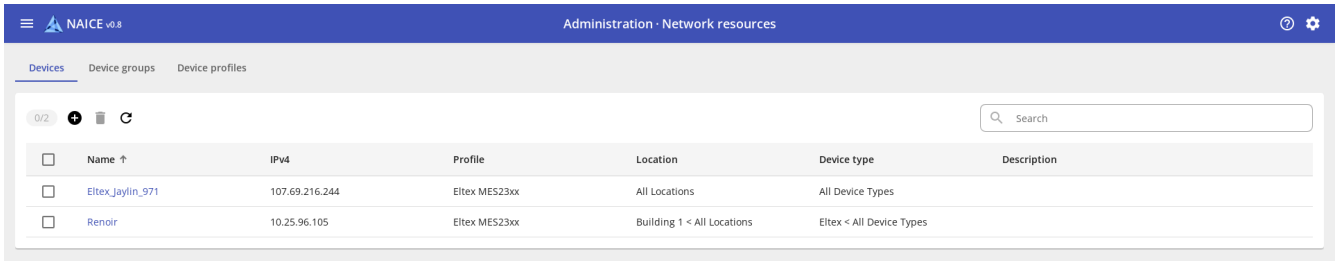

Figure 25. Table with a list of network devices on the viewing page

This page contains a table listing all network devices added to the system.

The table contains columns:

- `Name` – name of the network device.
- `IPv4` – IP address intended for interaction with the device (IPv4).
- `Profile` – assigned device profile.
- `Location` – a group that defines the location of the device.
- `Device type` – a group that defines the device type.
- `Description` – arbitrary description of the device.

It is possible to sort in direct and reverse order by the columns “Name”, “IPv4”, “Profile”. By default, sorting is performed in direct alphabetical order by the "Name" column.

Controls:

- `Search` - Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.

- - Refresh table data.
- `0/1` - Counter of elements selected by the checkbox / total number of elements.
- - Add a new element.
- - Delete selected elements (inactive until at least one element is selected).
- - Change the current sort order.
- - Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).

At the moment, IPv4 is the only sign by which the system determines which device it is working with.
Only a complete IP match is available, which means the addresses of all devices must be added to the system explicitly.

Adding a network device

To add a network device, click .

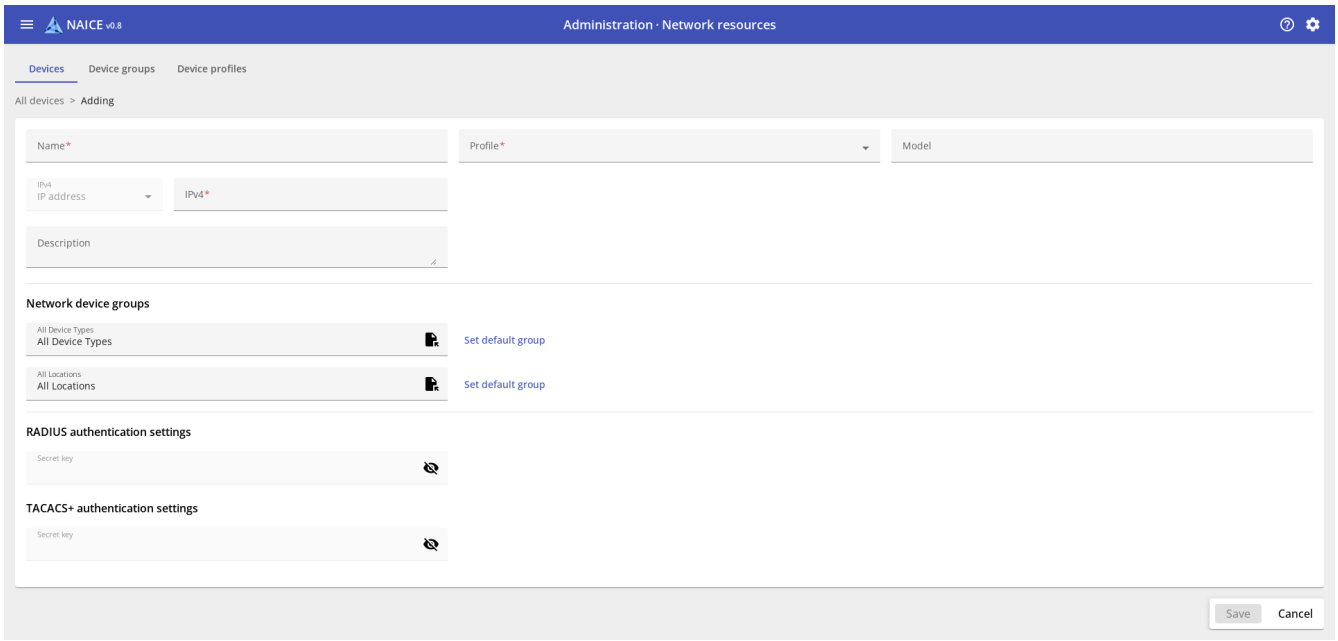

Figure 26. Add network device page

In the form that opens, you can fill in the following parameters:

- `Name` * – the name of the network device, must be unique within the list of network devices. Maximum length is 200 characters.
- `Profile` * – select a network device profile.
- `Model` – model of the network device. Maximum length is 100 characters.
- `IPv4` * – IP address of the network device. Recorded as four numbers from 0 to 255, separated by dots.
- `Description` – arbitrary description. Maximum length is 200 characters.

Network device groups – select groups of network device type and location. If you do not make a choice, default groups (i.e. root) will be assigned.

When you create a new root group, as described in section Device groups, they will appear automatically in the *Network device groups* list.

RADIUS authentication settings contains: - Secret key * for interaction with a network device using the RADIUS protocol. Length from 8 to 200 characters.

TACACS+ authentication settings contains: - Secret key * for interaction with a network device using the TACACS+ protocol. Length from 8 to 200 characters.

Parameters marked with an asterisk * are required.

After entering the required data, click the **"Save"** button.

Editing a network device

To edit a network device, on the list page, click its name.

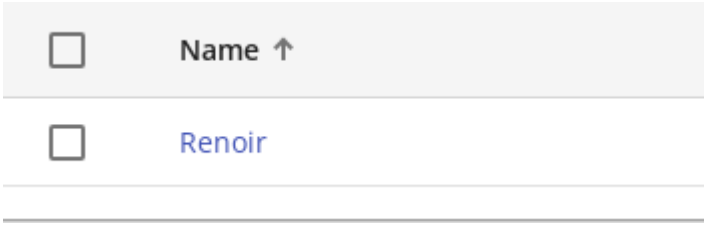

Figure 27. Hyperlink to the device editing page

After this, an editing window similar to the adding page will open.

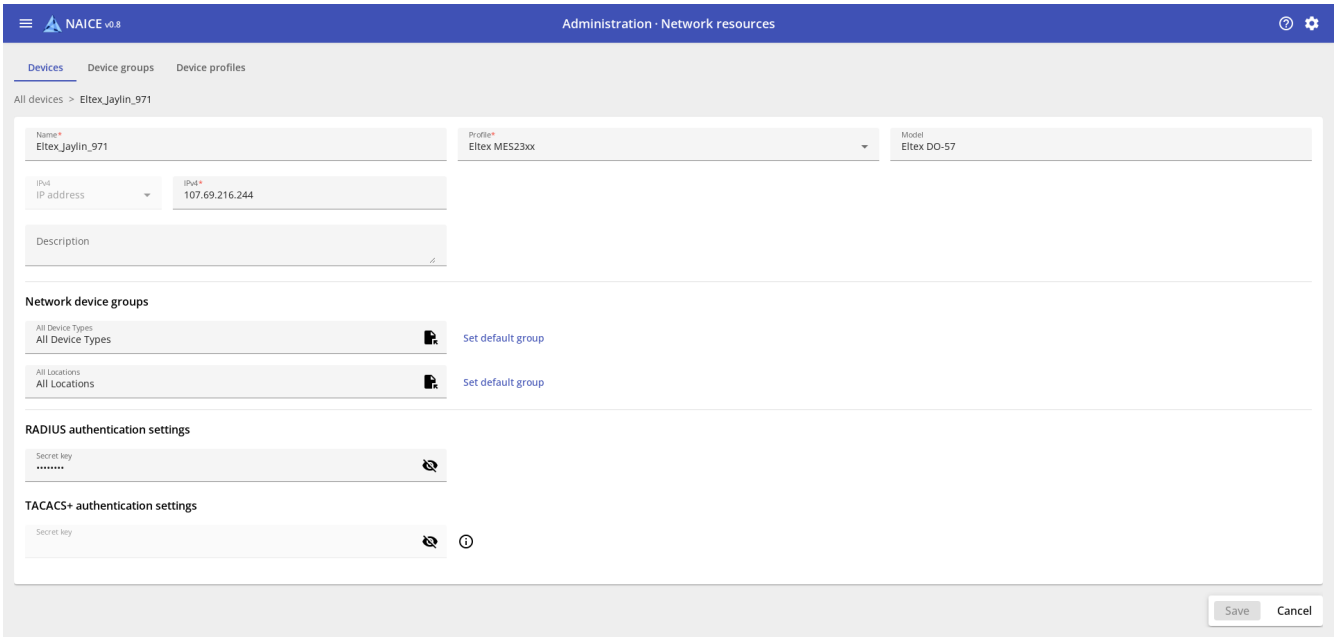

Figure 28. Device editing page

The RADIUS server included in NAICE caches network devices when they are added to the system. If there is an error when specifying a secret key and subsequent editing to the correct key, this data in the cache will not be updated. In this case, restart the naice-radius docker container to re-read the new data from the database.

After editing, click the "Save" button. The button remains inactive until at least one field is changed.

Removing a network device

To delete, in the list window, select the checkbox to the left of the name of the network devices that you want to delete, and click the button at the top left.

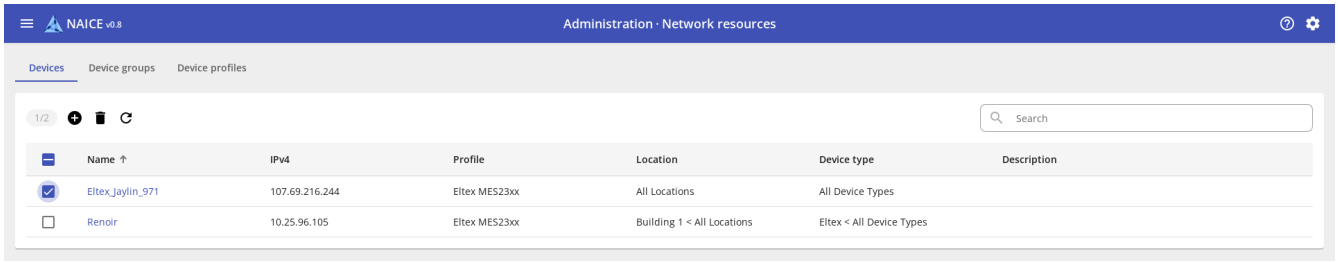

Figure 29. Selecting a device in the table to delete

Deletion requires confirmation of the action, for which a modal dialog will open. After explicit confirmation, the selected items will be deleted.

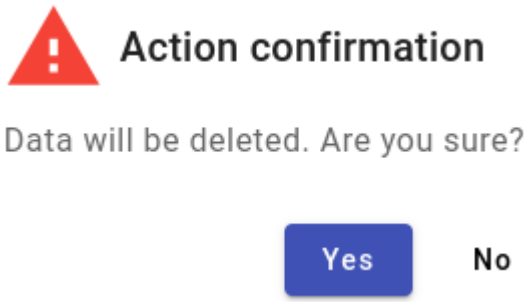

Figure 30. Modal dialog for confirmation

Device groups

Description

Device groups are intended for aggregation network devices according to various characteristics, with the further ability to define different authorization scenarios for different groups in policy sets.

View groups

This page contains a table listing all groups.

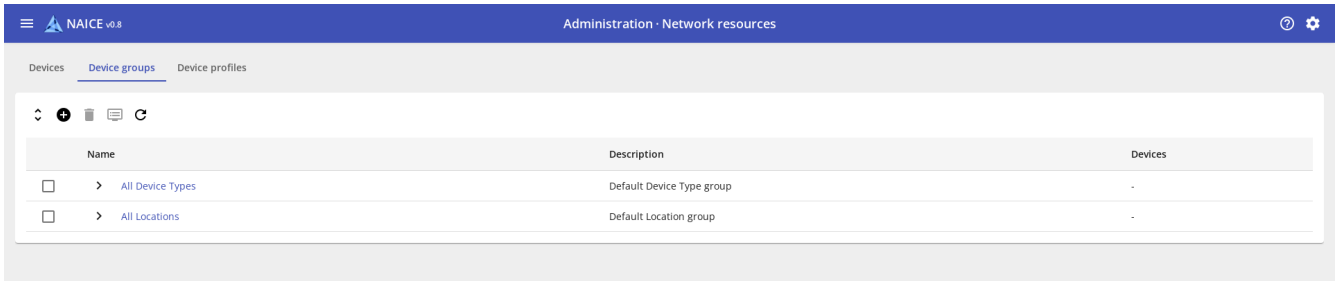

Figure 31. Group list view page

By default, there are two root groups:

- **All Device Types** to form groups based on the type of network devices
- **All Locations** to form groups based on the location of network devices.

These groups are system and cannot be deleted or changed.

If necessary, you can add new root groups. Thus, the administrator can create any hierarchy of devices, grouping them according to any characteristics, where the *attribute* is included in the Name of the root group, and the *attribute values* are included in the Names of child groups.

The table contains columns:

- `Name` - name of the group
- `Description` - arbitrary description of the group
- `Devices` - the number of devices in the group (for root groups the number of devices is not displayed)

Sorting is not provided.

Controls:

- - expand all groups.
- - refresh table data.
- - show devices of the group and its subgroups (inactive until the group is selected).
- - add a group.
- - delete a group (inactive until a group is selected).
- - expand the list of group subgroups.
- - collapse the list of group subgroups.
- - checkbox for selecting a group (you can select only one group).

Add a group

Adding a root group

To add a root group, click at the top left of the group list when no group is selected.

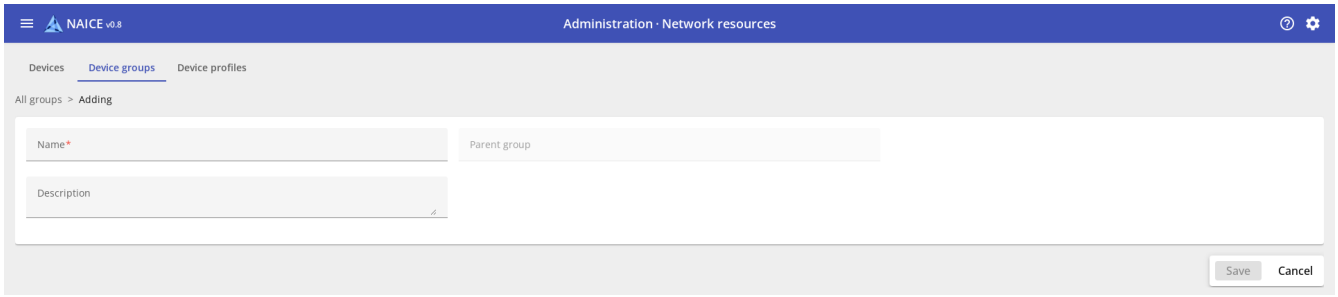

Figure 32. Page of add group

In the window that opens, you can fill in:

- `Name` * - name of the group. Maximum length is 100 characters.
- `Description` - description. Maximum length is 200 characters.
-

`Parent group` - filled in automatically, the value is taken from the group for which the subgroup is being created. When creating a root group, the field will be empty.

Parameters marked with an asterisk * are required.

After entering the required data, click the **"Save"** button.

Add a subgroup to an existing group

To add a group to an existing group, select it using the checkbox to the left of its name and click ⊕.

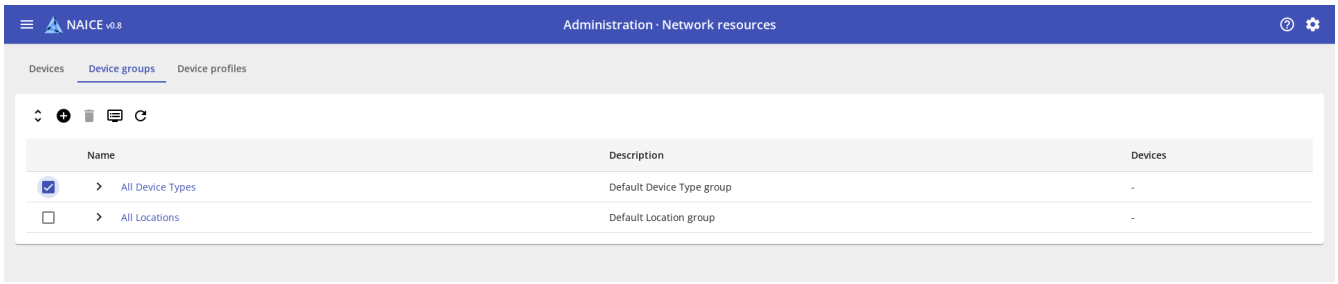

Figure 33. Page with selecting a root group to add a child group

When you add a subgroup, the "Parent group" field displays the name and ID of the parent group. This field cannot be changed.

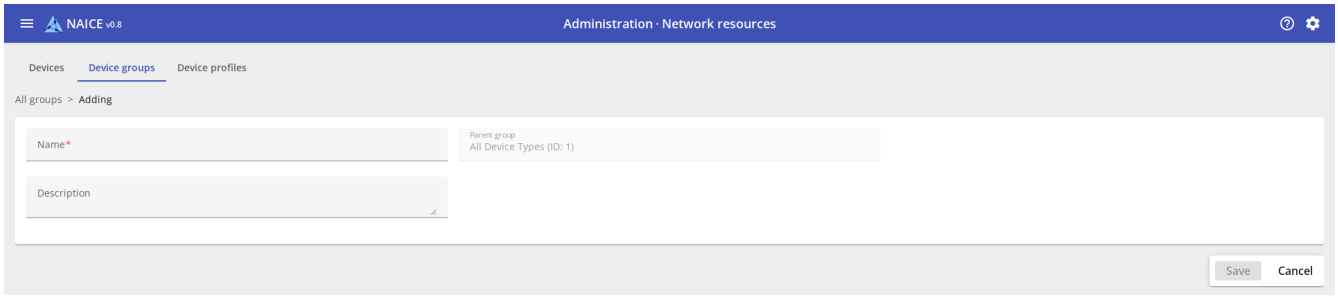

Figure 34. Page of added subgroup

Group editing

To edit a group, click on its name.

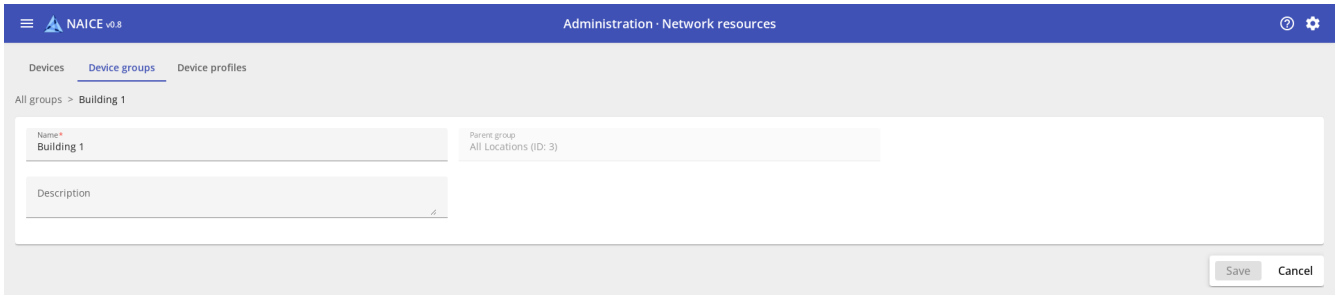

Figure 35. Group edit page

After editing, click on the **"Save"** button. The button remains inactive until at least one field is changed.

You cannot change the Parent Group. There is no procedure for moving a subgroup to another parent group. To change it, you need to delete the group and create it as a subgroup of another group.

Delete a group

To delete in the list window, select the checkbox to the left of the name and click the button at the top left.

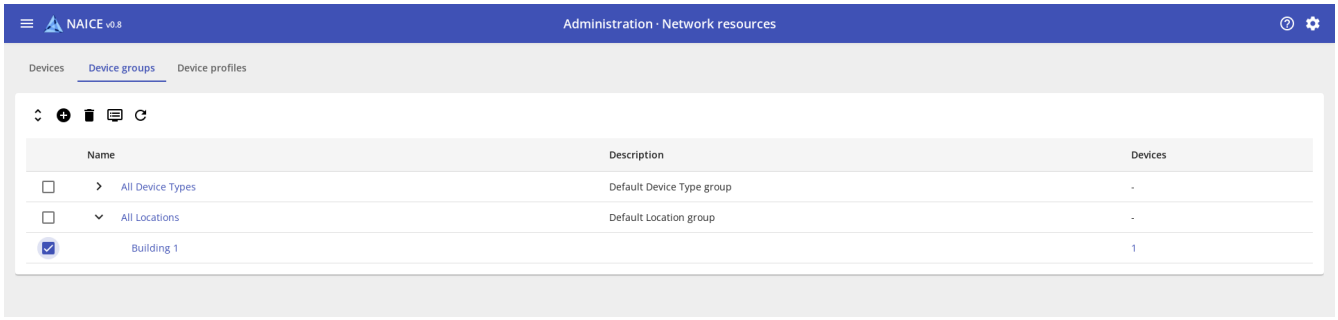

Figure 36. Page with a selected group for deletion

Deletion requires confirmation of the action, for which a modal dialog will open. After explicit confirmation, the selected items will be deleted.

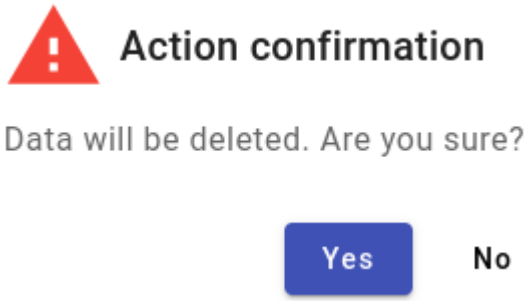

Figure 37. Modal dialog for confirmation

Restrictions:

- you cannot select and delete multiple groups;
- you cannot delete the "All Device Types" and "All Locations" system groups;
- you cannot delete a group containing subgroups;
- you cannot delete a group that is assigned to a network device.

View devices in a group

There are two ways to view devices in a group:

- viewing devices in a group and its subgroups by selecting a group and clicking on ;
- viewing devices of only this group by clicking on the counter opposite the group in the "Devices" column.

In both cases, a sidebar will open on the right side of the screen with a table of devices in the group.

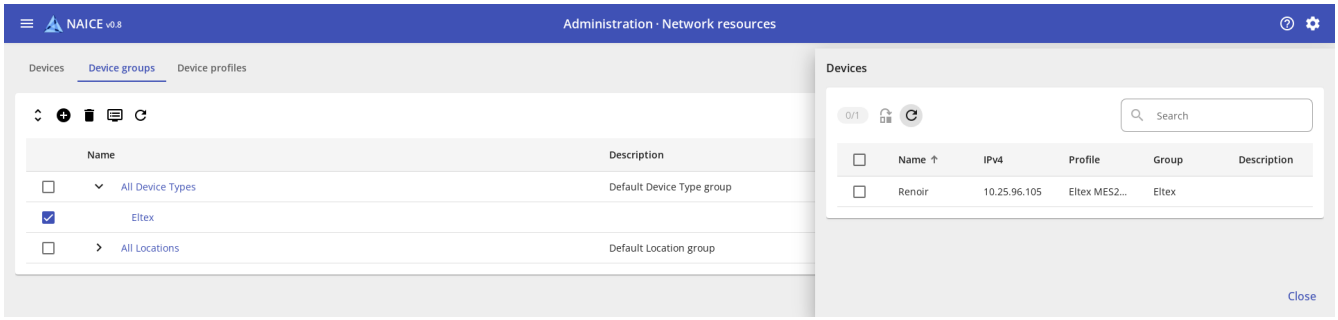

Figure 38. Panel for viewing devices in a group

The table contains columns:

- `Name` - device name;
- `IPv4` - IPv4 address of the device;
- `Profile` - device profile;
- `Group` - a subgroup of the device within this root group. Does not appear if the panel is open when clicking on the device counter.
- `Description` - arbitrary description of the device.

Sorting by "Name" and "IPv4" is available.

Controls:

- `Search` performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.
- refresh table data.
- checkbox, which is responsible for selecting network devices to perform further actions.
- `0/1` counter of elements selected by checkbox / total number of elements.
- move the devices selected by the checkbox to another group.
- change the current sort order.

Move a device to another group

After clicking on the device move button , a window will open with the selection of a group to move *within the same root group*.

Figure 39. Panel for moving devices to a group

The group is selected from the list that opens by clicking on .

Device profiles

Description

Device profiles are intended to summarize the settings of similar network devices. As a rule, devices from the same manufacturer and/or family have similar settings.

The main settings in device profiles are:

- *conditions for detecting the flow type* - upon receipt of which RADIUS attributes the user's connection will be determined, for example, as wired MAB or wireless 802.1x. Based on the connection type, you can configure access policies. For example, one VLAN can be assigned to a user connecting wired, and another VLAN for the same user connecting wirelessly.
- *process MAB* - the ability to authorize clients connected to this device via MAB and configure the features of this connection.
- *permissions* - configure the capability and RADIUS attributes for issuing VLANs and/or ACLs for clients connected to this device.

View a list of device profiles

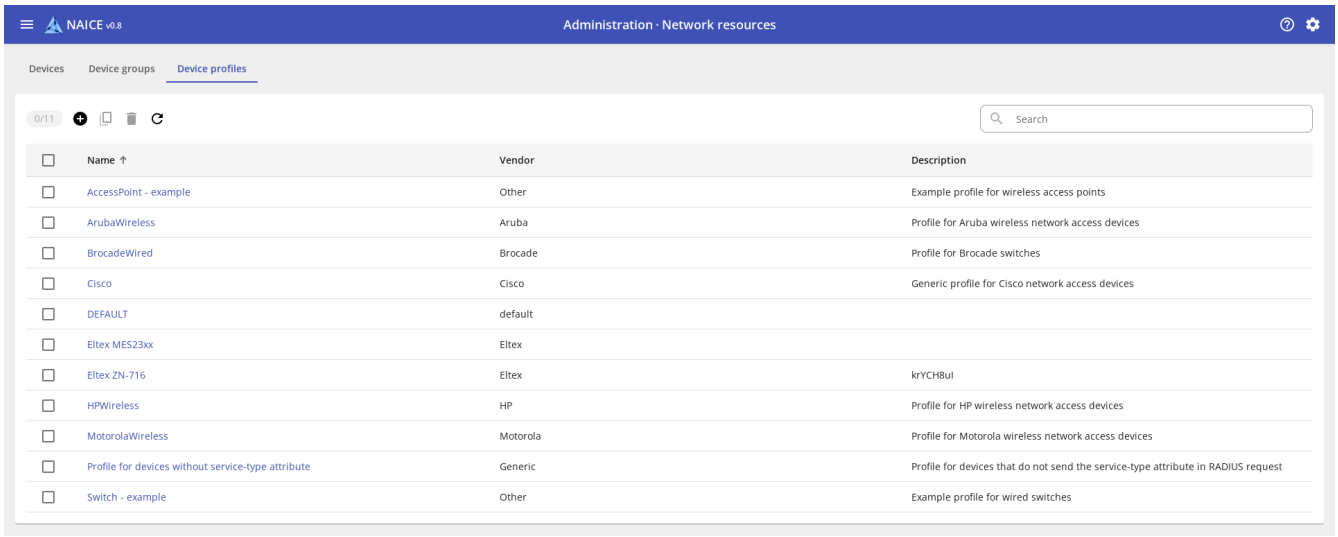

Figure 40. Table with a list of network device profiles

This page contains a table with a list of device profiles.

The table contains columns:

- `Name` - name of the profile;
- `Vendor` - the name of the device vendor;
- `Description` - arbitrary description of the profile.

Sorting by the columns `Name`, `Vendor` is available.

Controls:

-

`Search` - Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.

- - Refresh table data.
- `0/1` - Counter of elements selected by the checkbox / total number of elements.
- - Add a new element.
- - Delete selected elements (inactive until at least one element is selected).
- - Change the current sort order.
- - Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).

Adding a device profile

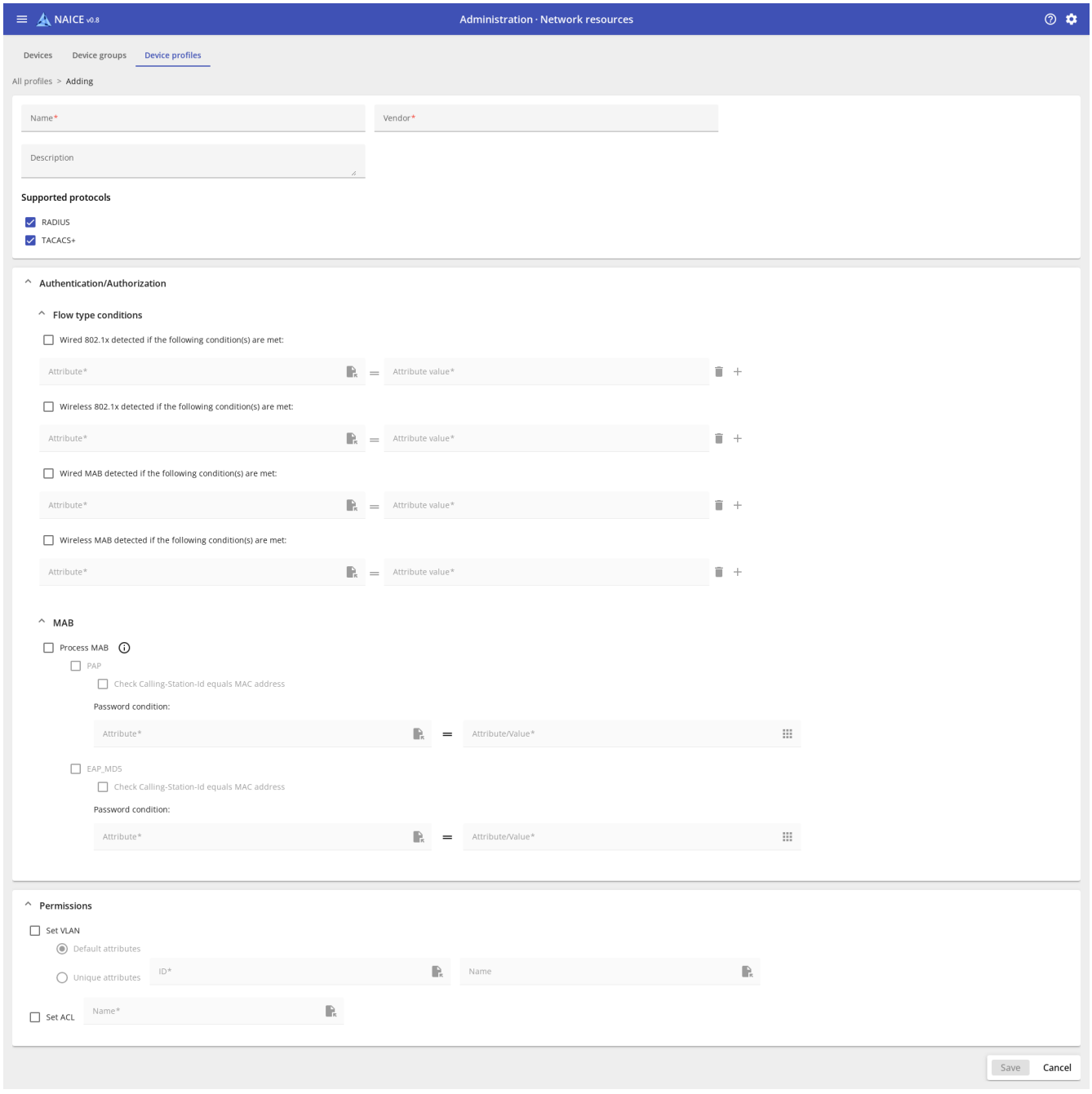

Figure 41. Page for adding a device network profile

To add a device profile, click ⊕.

In the window that opens, you must fill in the following parameters:

- `Name` * - name of the device profile. Maximum length is 100 characters.
- `Vendor` * - name of the network device vendor. Maximum length is 100 characters.
- `Description` : arbitrary description. Maximum length is 200 characters.
- `Supported protocols` - the protocol that is used to interact with the network device (is enabled by default).

Authentication/Authorization - a setting block responsible for determining the flow type of endpoint.

- `Wired 802.1x / Wireless 802.1x / Wired MAB / Wireless MAB detected if the following condition(s) are met` - enable the setting for detecting one of the connection types.
- `Attribute` - RADIUS attribute used in the condition.
- = means that the condition will be satisfied if the attribute is equal to the specified value. By clicking on the icon, you can change the condition to inequality.
- `Attribute value` - the value of the RADIUS attribute used in the condition.
- 🗑 delete the condition.
- ⊕ add a condition.

This block is responsible for determining the connection type. If several RADIUS attributes are used in a condition, they are combined with a logical “AND”. If the connection type is not enabled or has not been defined, the user continues authorization, his connection type is considered undefined.

You can configure access policies based on the connection type. For example, one VLAN can be assigned to a user connecting wired, and another VLAN for the same user connecting wireless.

MAB - setting block responsible for resolving and configuring MAB authorization features.

- `Process MAB` - enable MAB authorization permission on the device.
- `PAP / EAP_MD5` - enable MAB authorization permission for the specified protocols.
- `Check Calling-Station-Id equals MAC address' - allow authorization only for those devices in whose request the RADIUS attribute Calling-Station-Id matches the MAC address in the user name.
- `Password condition` - the condition under which the password will be considered correct. By default, the condition is set to equal the password to the user login.

Permissions - a setting block that determines the possibility of simplified issuance of additional attributes to the user after authorization.

- `Set VLAN` - enable the possibility of simplified issuance of VLANs in RADIUS attributes.

`Default attributes` - use standard IETF RADIUS attributes for issuing VLANs.

- `Unique attributes` - use vendor-specific RADIUS attributes to issue VLANs.
  - `ID` is a vendor-specific RADIUS attribute for issuing a VLAN in the format of a number from 1-4094.
  - `Name` is a vendor-specific RADIUS attribute for issuing a VLAN in string format.

- `Set ACL` - enable the ability to simplify the issuance of the name of a static ACL in RADIUS attributes.
  - `Name` is a vendor-specific RADIUS attribute for issuing the ACL name in string format.

Parameters marked with an asterisk * are required.

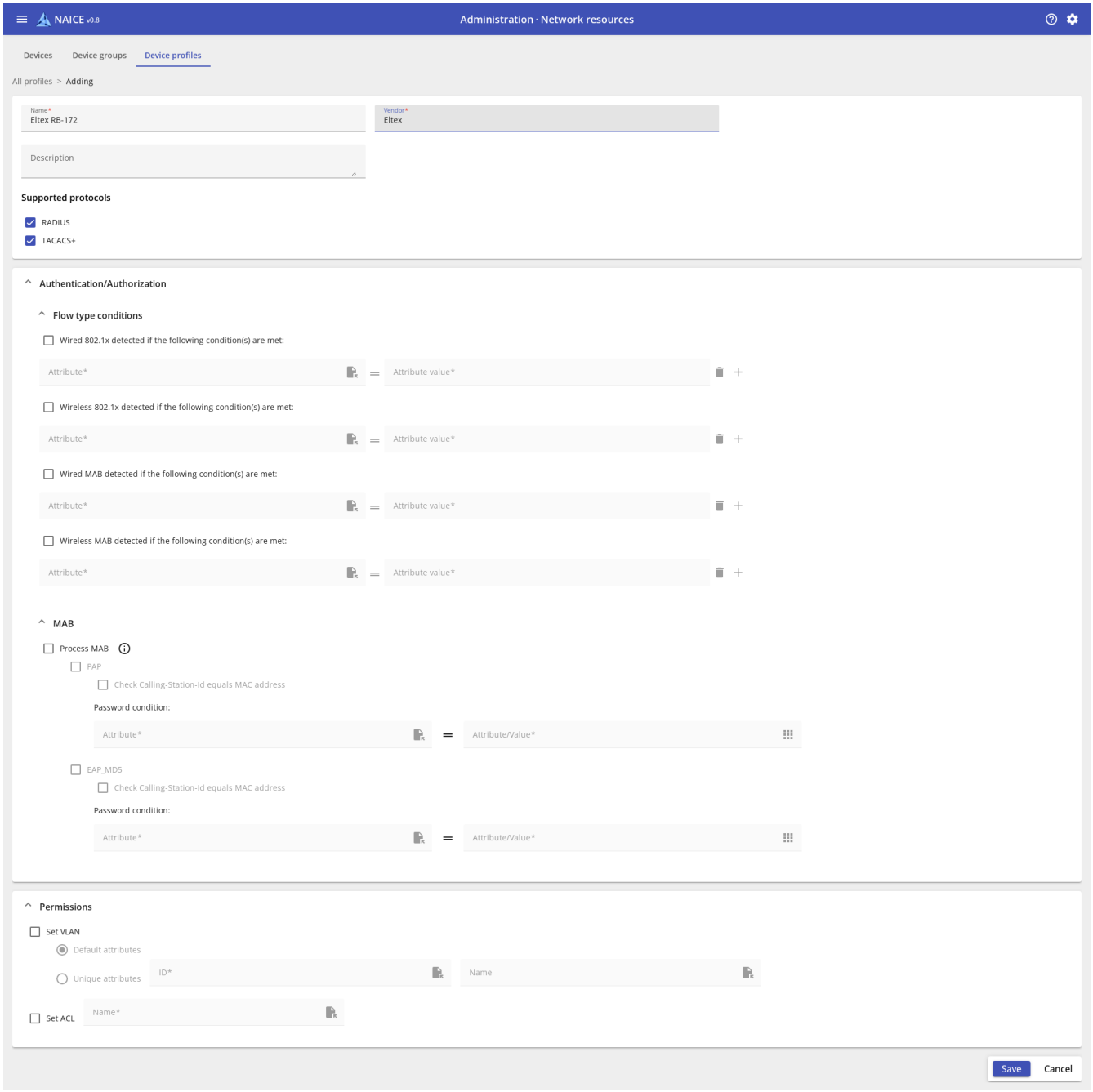

Figure 42. Page with filling device profile parameters

After entering the required data, click the **"Save"** button.

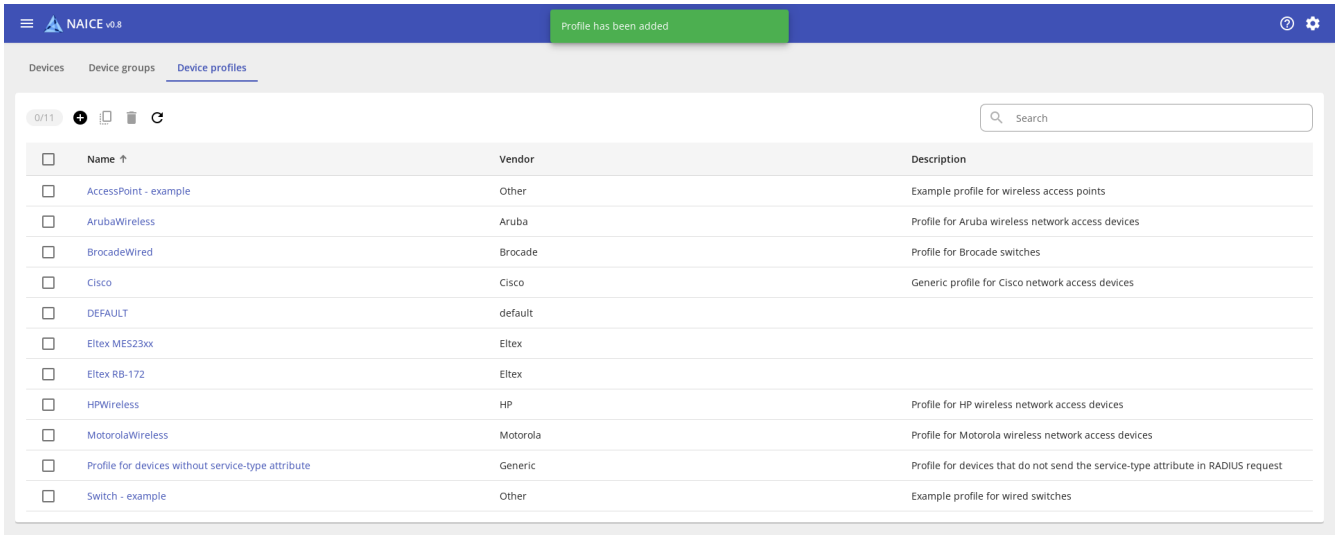

Figure 43. Network device profile creation success page

Editing a device profile

To edit a device profile, you need to click on its name on the list page, after which the editing window will open.

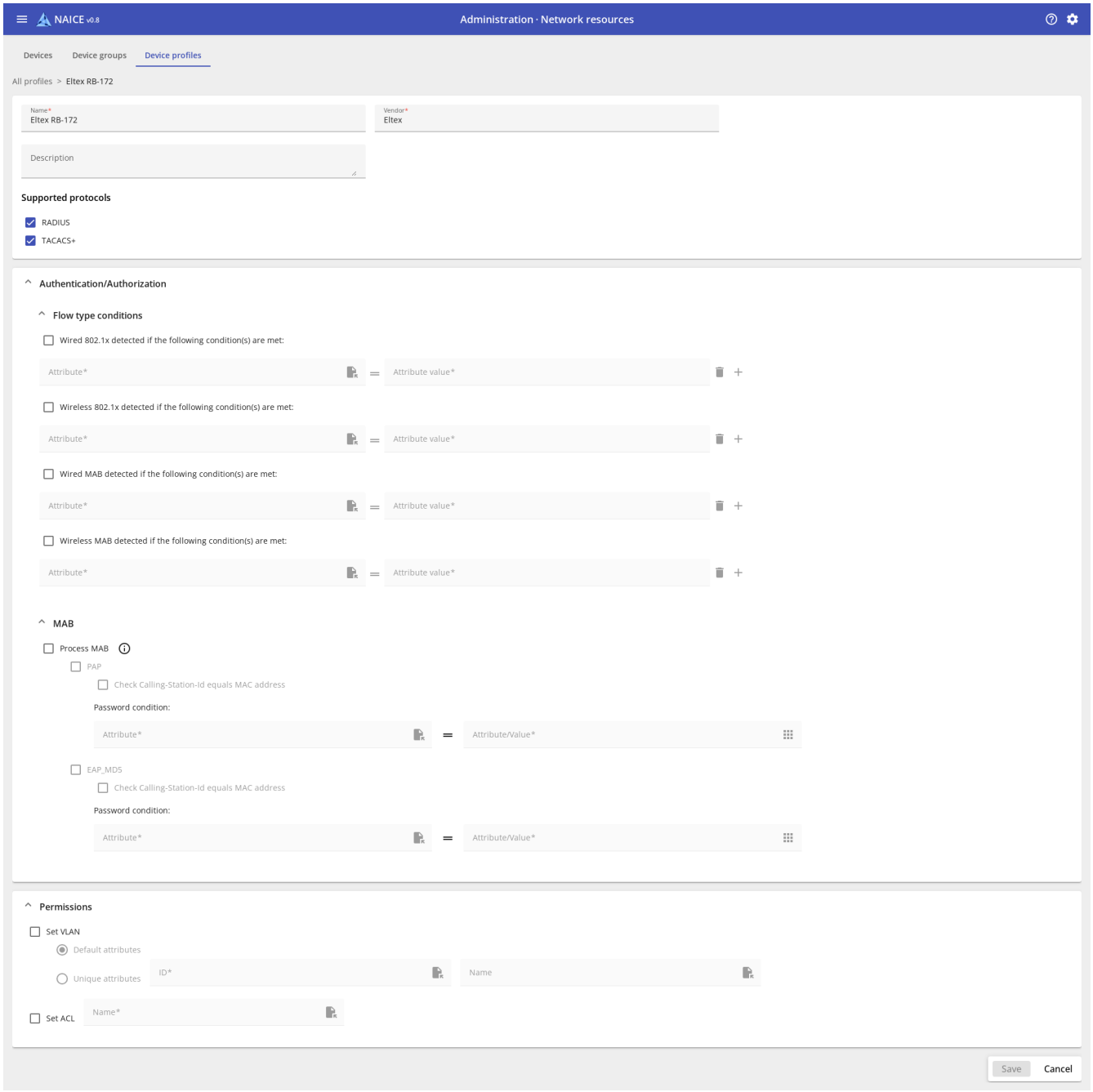

Figure 44. Network device profile editing page

After editing, click on the **"Save"** button. The button remains inactive until at least one field is changed.

Deleting a device profile

To delete a profile, select it with the checkbox and click the button at the top left.

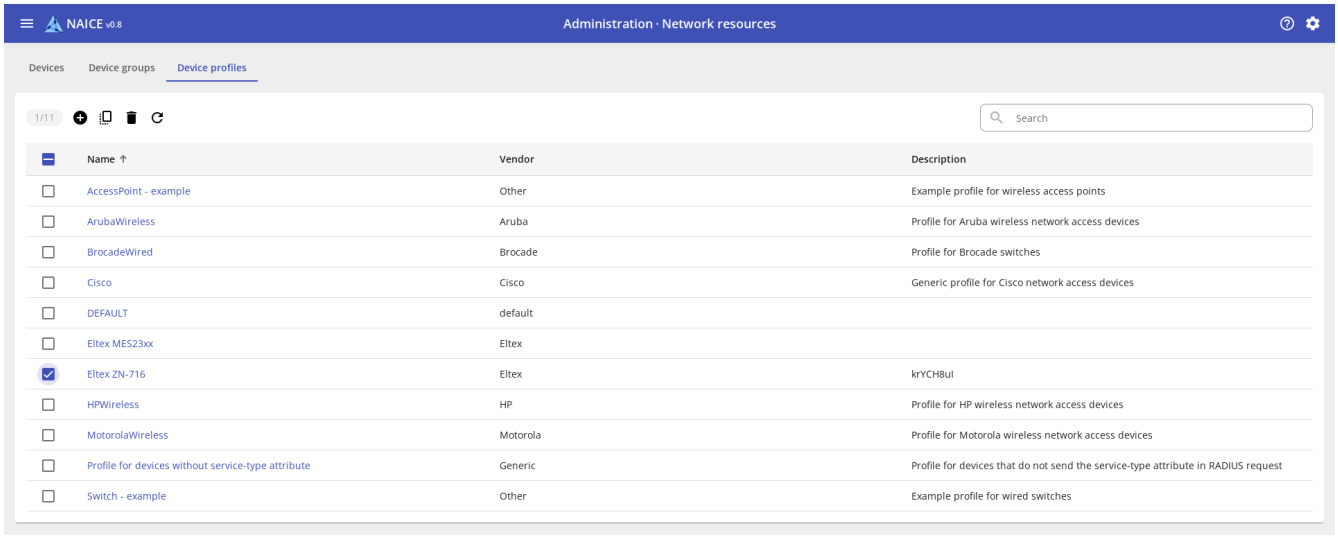

Figure 45. Page with the device profile selected for deletion

Deletion requires confirmation of the action, for which a modal dialog will open. After explicit confirmation, the selected items will be deleted.

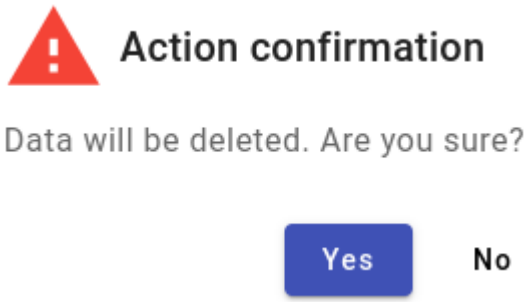

Figure 46. Modal dialog for confirmation

After deleting, you will be on the page for viewing the list of device profiles.

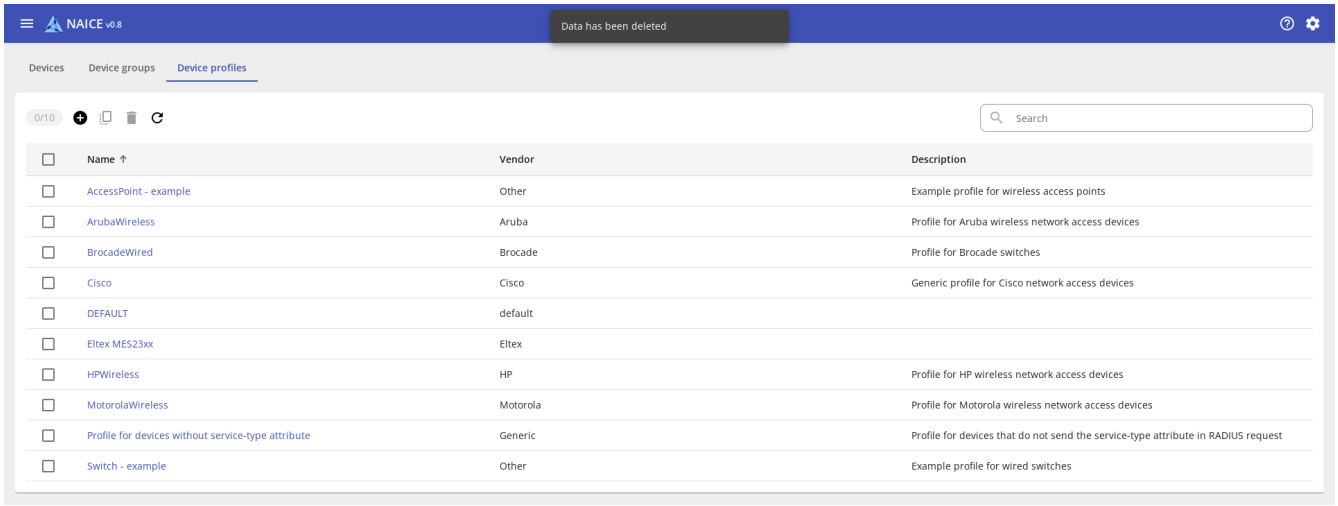

Figure 47. Page for viewing the list of device profiles after deletion

Restrictions:

- you cannot delete a profile that is already assigned to a device.
- you cannot delete a profile that is used in any authorization profile.

Identity management

Users (supplicants) are managed in the "Administration" → "Identity Management" menu.

The identity source used for user authentication can be an internal list of clients (their configuration is discussed in Network access users) and a connection to an external identity source such as Active Directory or LDAP.

Work with endpoints is also carried out here.

The menu contains sections:

- Network access users - section for managing the credentials of users with whom authorization on devices is performed.
- Network user groups - settings section that allows you to create entities for grouping users.
- Endpoints - section for working with a list of devices that connect to the network infrastructure.
- Endpoints groups - section for working with groups of endpoints.
- External identity sources - section for managing external identity sources.
- Identity sequences - a settings section that allows you to create lists of sources of user credentials.

Network access users

Description

The "Network Users" section is designed to manage the credentials of users with whom authorization on devices is performed.

View network users

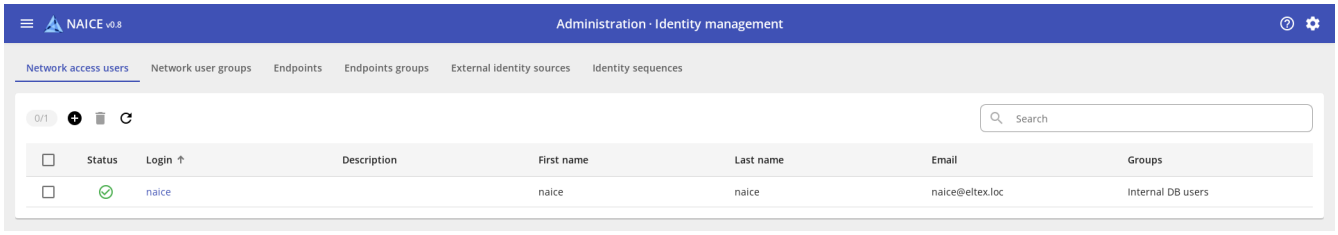

Figure 48. A table with a list of network users on the viewing page

This page contains a table listing user credentials.

The table contains columns:

- `Status` - user status (disabled or enabled);
- `Login` - user login (must be unique);
- `Description` - arbitrary description of the user;
- `First name` - user name;
- `Last name` - user surname;
- `Email` - user's email address;

`Groups` - groups in which the user is a member.

It is possible to sort in direct and reverse order by the columns “Status”, “Login”, “Description”, “First Name”, “Last Name”, “Email” (that is, by all columns except the “Groups” column). By default, sorting is performed in direct (alphabetical) order by the "Login" field.

Controls:

- `Search` - Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.
- - Refresh table data.
- `0/1` - Counter of elements selected by the checkbox / total number of elements.
- - Add a new element.
- - Delete selected elements (inactive until at least one element is selected).
- - Change the current sort order.
- - Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).

Adding a user

To add a user, click on the left side of the field above the table.

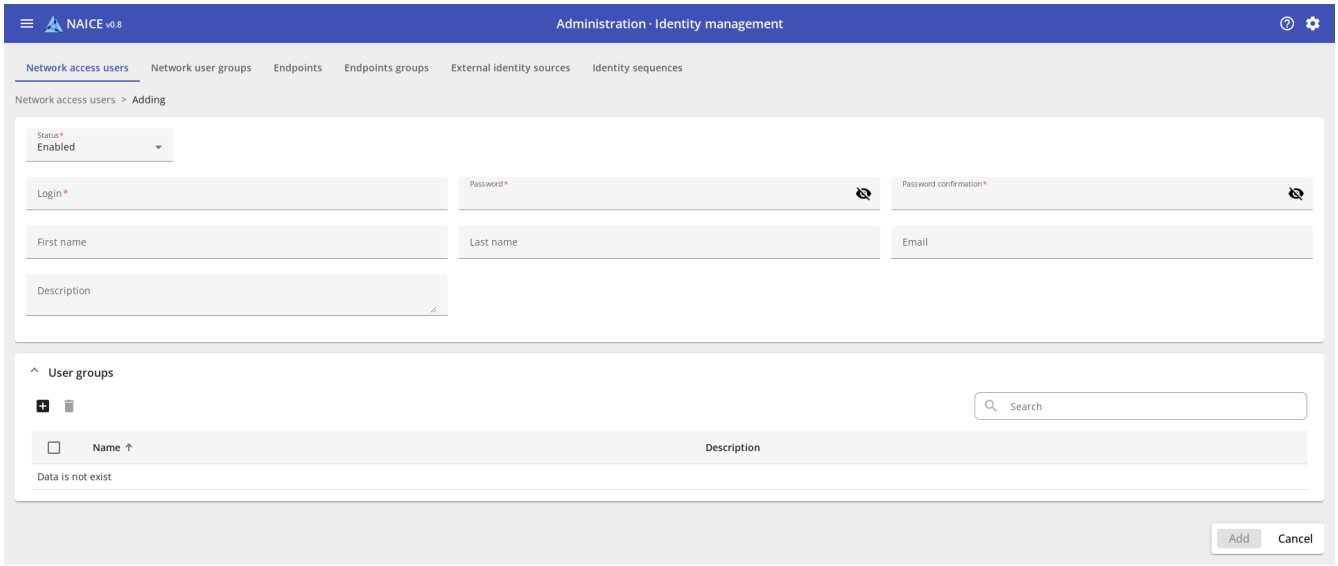

Figure 49. The page for adding a user

The page that opens presents the following parameters:

- `Status` * - user status, can take the values “enabled” or “disabled”. Authentication using disabled credentials is prohibited.
- `Login` * - user login. The maximum login length is 200 characters.
- `Password` * - user password. The minimum password length is 8 characters, the maximum is 200 characters. By clicking on you can enable the display of the entered password; by default, the entered text is hidden.

- `Password confirmation` * - user password confirmation field, must match the value from `Password`. By clicking on you can enable the display of the entered password; by default, the entered text is hidden.
- `First name` - user's name. Maximum length is 200 characters.
- `Last name` - user's last name. Maximum length is 200 characters.
- `Email` - user's email address. Must follow a specific format (eg naice@eltex.loc) and not exceed 200 characters.
- `Description` - a custom description of the user. Maximum length is 1000 characters.

Parameters marked with an asterisk * are required.

Also on this page there is a table **User groups**, which this user belongs to.

Controls:

- `Search` - case-insensitive filtering for all columns: only records that satisfy the filtering condition are displayed.
- - delete the user from the groups selected by the checkbox (inactive until at least one group is selected).
- - change the current sort order.
- - a checkbox that is responsible for selecting groups to perform further actions (for example, removing a user from a group).
- - add the user to groups.

By clicking , the **Adding user to groups** window appears, in which you need to select the groups where you want to add users.

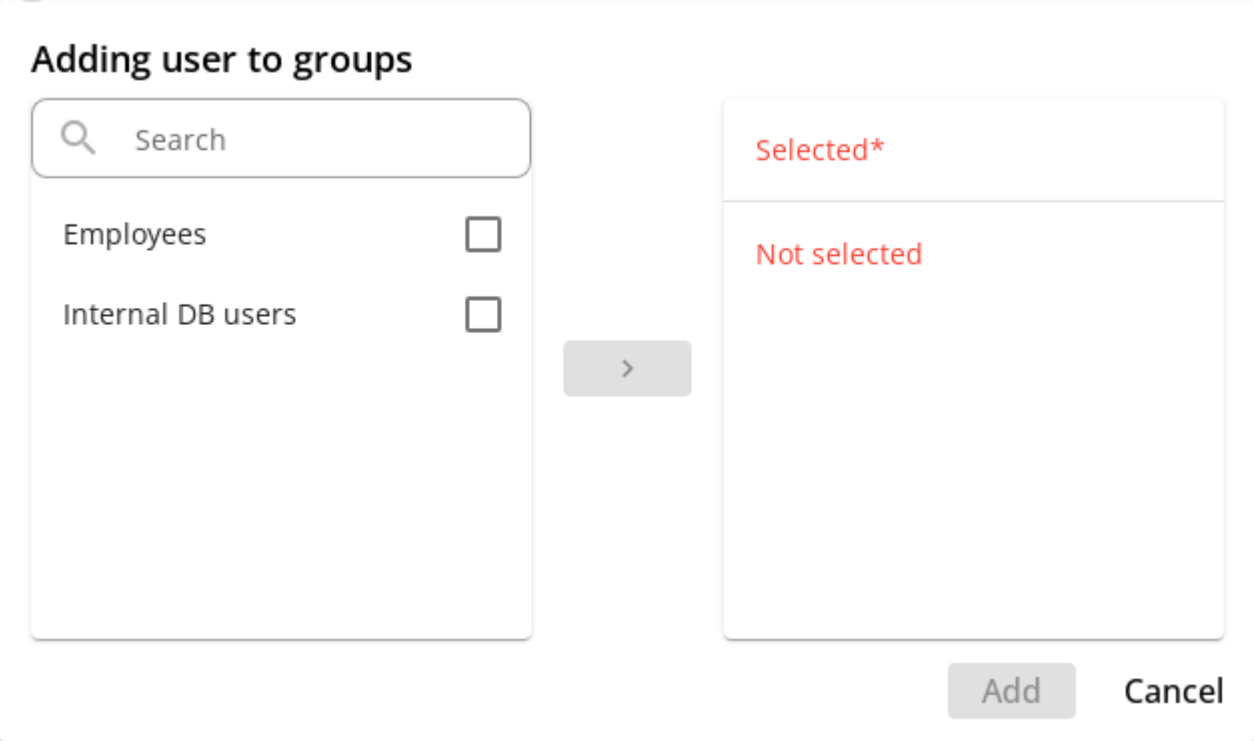

Figure 50. The page for adding a user to groups

Controls:

- `Search` - case-insensitive search among user groups: only groups that satisfy the filtering condition are displayed.
- ☐ - a checkbox that is responsible for selecting groups to assign to the user (displayed only for available groups).
- › - assign selected groups to the user.
- 🗑 - delete a group from the list of those selected for assignment (displayed only for selected groups).
- `Add` - apply changes (active only if there are changes).
- `Cancel` - cancel changes.

To add a user to the user list, do not forget to click `Add`. To reset the changes and return to the viewing page, click on `Cancel`.

User editing

To edit a previously added user, on the user view page, click on the user login in the table.

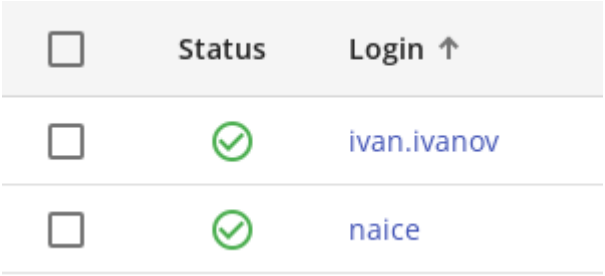

Figure 51. Hyperlink to the user's edit page

The editing page will open.

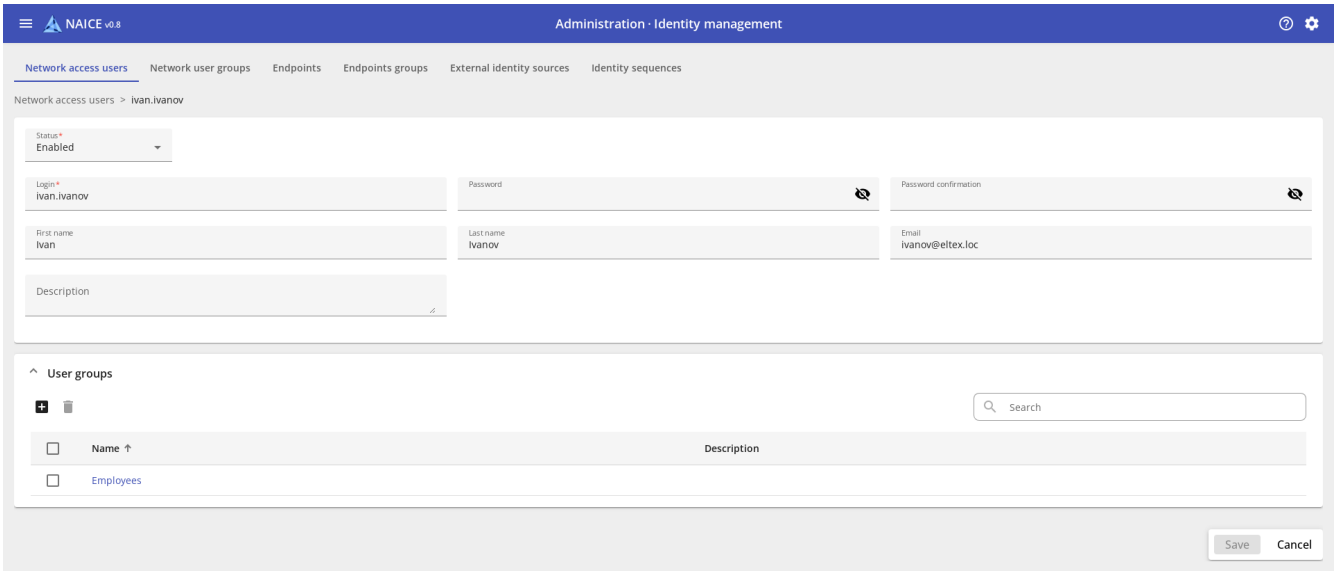

Figure 52. The user's edit page

The old user password is not displayed on the edit page!
If you do not want to change the user password, then leave the "Password" and "Confirm Password" fields empty.

After editing, click on `Save`. The button will be inactive until at least one field is changed.

Deleting a user

To delete users, on the viewing page, using the checkbox ☐, select the required users and in the upper left corner above the table click on 🗑.

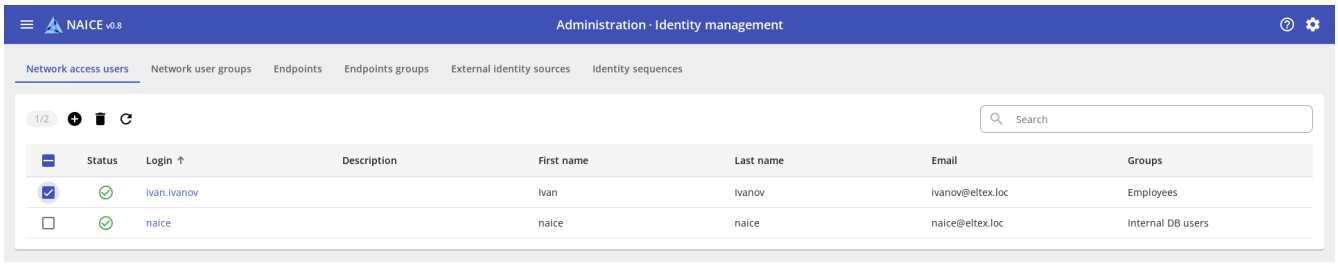

Figure 53. Selecting users in the table to delete

Deletion requires confirmation of the action, for which a modal dialog will open.
After explicit confirmation, the selected items will be deleted.

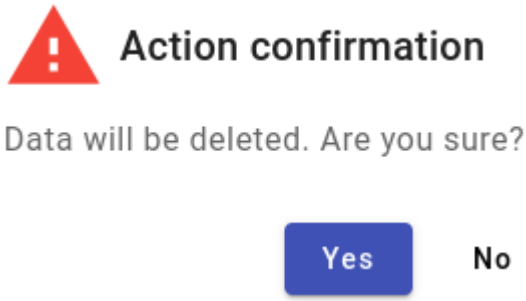

Figure 54. Modal dialog for confirmation

Network user groups

Description

It is possible to combine network users into *groups* and then use the sign of user membership in a group when setting up policy sets.

The "Network user groups" section is responsible for creating, editing, deleting and viewing these groups.

View network user groups

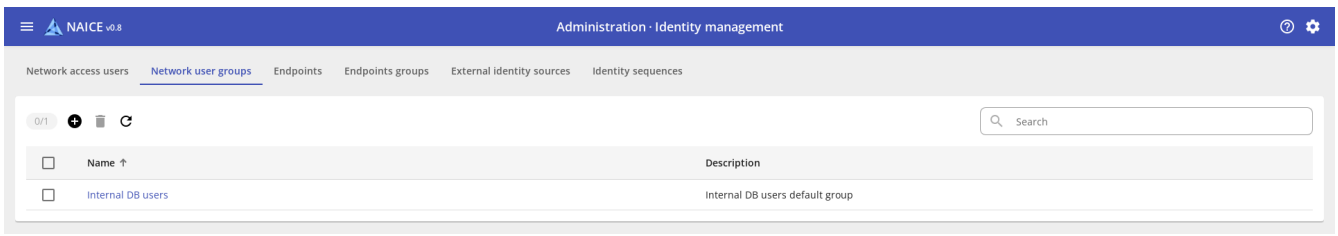

Figure 55. A table with a list of network user groups on the viewing page

This page contains a table listing all network user groups.

The table contains columns:

- `Name` - the name of the group.
- `Description` - arbitrary description of the group.

You can sort in forward and reverse order across all columns. By default, sorting is performed in direct (alphabetical) order by the `Name` field.

Controls:

- `Search` - Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.
- - Refresh table data.
- `0/1` - Counter of elements selected by the checkbox / total number of elements.
- - Add a new element.
- - Delete selected elements (inactive until at least one element is selected).
- - Change the current sort order.
- - Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).

Adding a user group

To add a user group, click on the left side of the field above the table, the **Add** page will open:

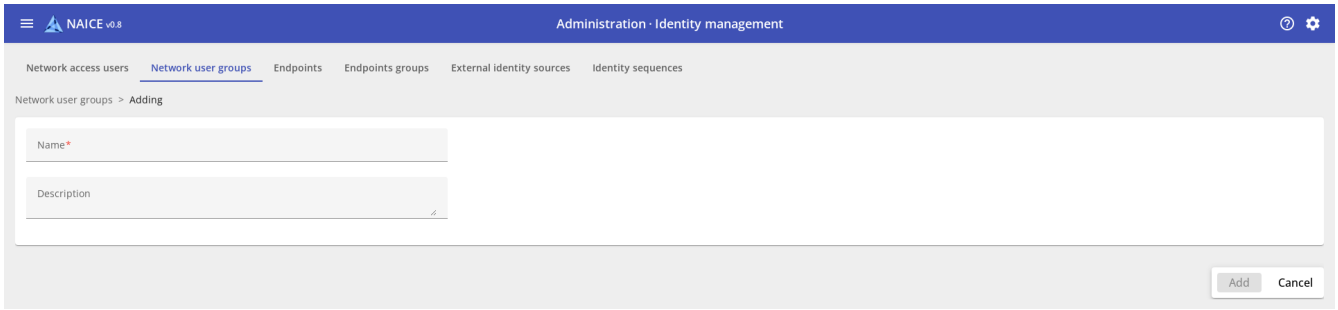

Figure 56. The page for adding a user group

The following parameters are available for filling:

- `Name` * - the name of the group. Maximum length is 200 characters.
- `Description` - arbitrary description of the group. Maximum length is 200 characters.

Parameters marked with an asterisk * are required.

> Adding a user to a group is available on the edit page of a previously added group.
> At the stage of creating a group, you cannot add users to it.

To add a group to the list of user groups, do not forget to click `Add`. To reset the changes and exit to the viewing page, click on `Cancel`.

Editing a user group

To edit a previously added group, on the user groups viewing page, click on the group name in the table.

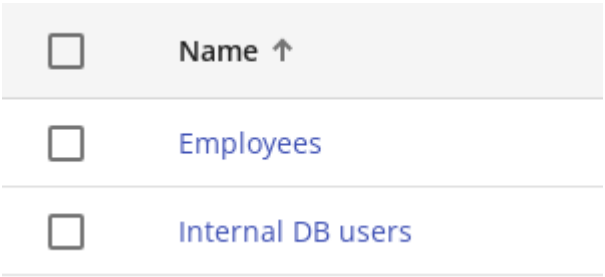

Figure 57. Hyperlink to the user group editing page

An edit page will open with the option to add users to the group.

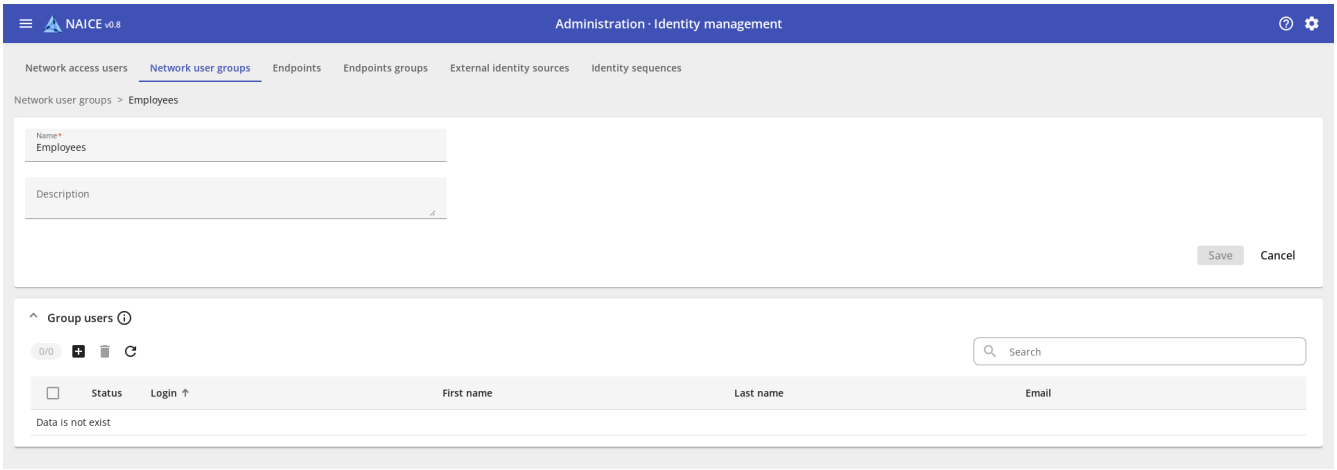

Figure 58. The user group edit page

Control elements in the **Group Users** table:

- `Search` - case-insensitive filtering for all columns: only records that satisfy the filtering condition are displayed.
- 🗑 - delete users selected by the checkbox from the group (inactive until at least one user is selected).
- ↑ - change the current sort order.
- ☐ - a checkbox that is responsible for selecting users to perform further actions (for example, removing a user from a group).
- `0/1` - counter of elements selected by the checkbox / total number of elements.
- ⊞ - add users to the group.

By clicking ⊞, the **Adding users to group** window appears, in which you must select users to add to the group.

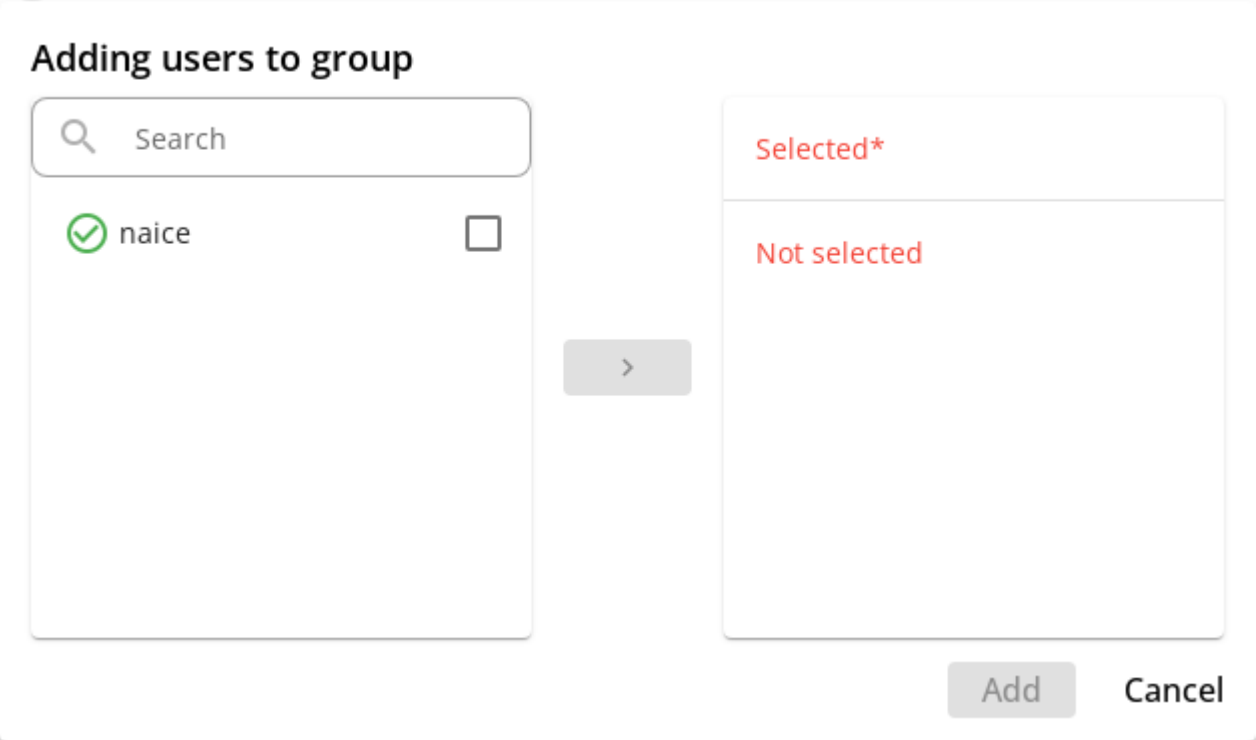

Figure 59. The window for adding users to a group

Controls:

- `Search` - case-insensitive search among users: only users that meet the filtering condition are displayed.
- ☐ - a checkbox that is responsible for selecting a user to add (displayed only in the left column).
- › - move users selected by the checkbox from the available ones to the selected list.
- 🗑 - delete a user from the selected list (displayed only in the right column).
- `Add` - apply changes (active only if there are changes).
- `Cancel` - cancel changes.

> ⚠ If, when editing a group, only users are changed (the name and description of the group remain the same), then the `Save` button will remain inactive, since changes in the list of group users are saved automatically.
> Just exit the editing mode using the `Cancel` button.

Delete a user group

To delete groups, on the viewing page, using the checkbox ☐, select the required groups and in the upper left corner above the table click on 🗑.

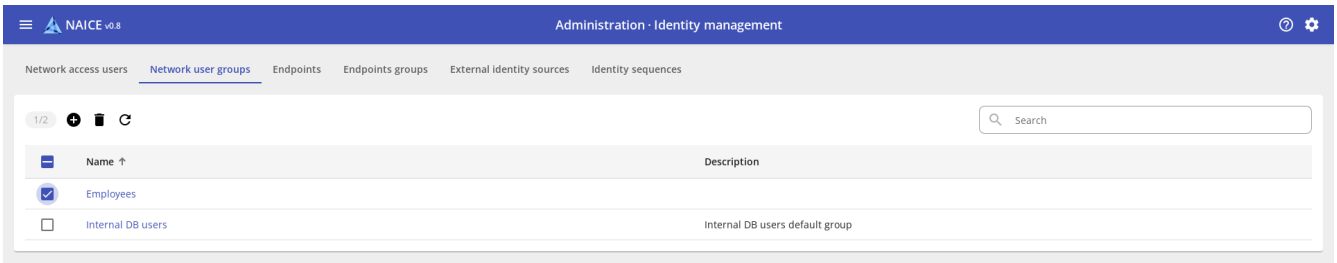

Figure 60. Selecting user groups in the table to delete

Deletion requires confirmation of the action, for which a modal dialog will open.
After explicit confirmation, the selected items will be deleted.

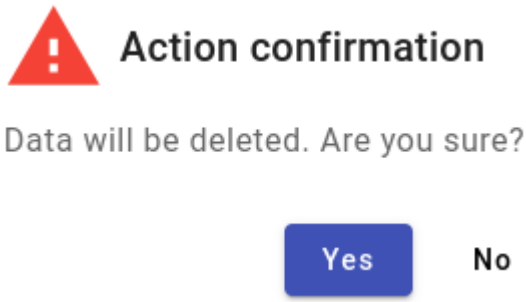

Figure 61. Modal dialog for confirmation

Restrictions:

- you cannot delete a group that users belong to. In this case, you must first remove all users from the group, then delete the empty group.
- you cannot delete a group that is used in any logical condition.

Endpoints

Description

Endpoints are networking devices such as computers, mobile phones, IoT devices, and others that establish communication across the network through authenticator (like switch or access point) using 802.1x authentication or MAB.

The NAICE system allows you to track endpoints in the network, group them by certain characteristics automatically or manually, and allow or deny access to the network based on the parameters obtained during profiling and policies.

Filling the endpoint table

The endpoint table is filled in automatically and manually mode.

- *in manual mode*: adding endpoints is performed by the system administrator in the same way as adding other entities.
- *in automatic mode*: endpoints are added when RADIUS requests are received from authenticators during client connections.

To determine the MAC address of the endpoint to be added, the value of the "Calling-Station-Id" attribute of the RADIUS request is used.

Randomized MAC addresses will not be added as endpoints in automatic mode. Add endpoints with this type of MAC manually.

View endpoints

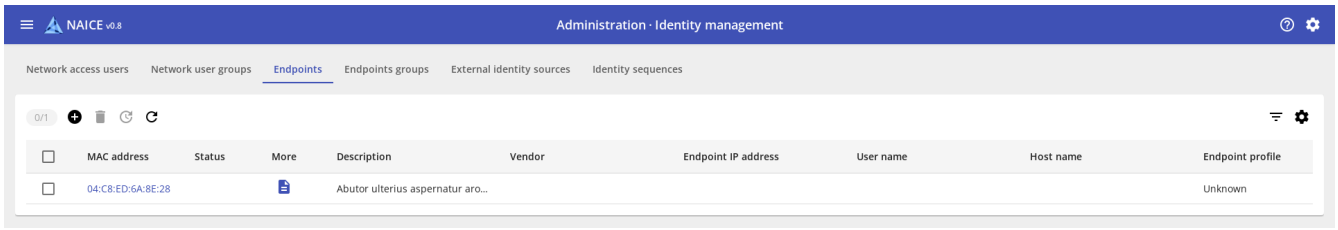

Figure 62. View endpoints list

This page contains a table with a list of all manually or automatically added endpoints.

The table contains the following columns by default:

- `MAC address` - MAC address of the endpoint in the format "XX:XX:XX:XX:XX:XX".
- `Status` - current endpoint connection status. The status is displayed after the first endpoint authentication attempt and can have the following values:
  - Connected - the device has successfully passed authentication and authorization and has gained access to the network;
  - Rejected - the device has not passed authentication and has not gained access to the network;
  - Disconnected - the device is disconnected from the network.
- `More` - go to the page with detailed information about the endpoint attributes and its latest authentication events.
- `Description` - arbitrary description.
- `Vendor` - the vendor of the endpoint device, determined by the first three octets of the MAC address (MAC OUI).
- `Endpoint IP address` - IP address of the endpoint, information about which was obtained during profiling. Profiling settings are required to obtain data.
- `User name` - username with which the endpoint was last authenticated.
- `Host name` - hostname of the endpoint, information about which was obtained during profiling. Profiling settings are required to obtain data.
- `Endpoint profile` - result of endpoint profiling.

Additionally, by clicking ⚙, you can customize the display of the following columns:

- `Authentication failure reason` - the cause of the error during client connection.
- `Authentication policy` - the name of the authentication policy rule that was applied within this session;
- `Authorization policy` - the name of the authorization policy rule that was applied within this session;
- `Authentication Protocol` - the protocol by which authentication was performed (for example, PAP).
- `Flow Type` - the connection type that was determined based on the network device profile settings.
- `Endpoint Type` - the logical profile to which the device belongs as a result of profiling.

`Last activity time`

- `Endpoint group` - the group to which the endpoint was automatically or manually added.
- `NAS name` - the name of the authenticator device.

You can sort in ascending or descending order by the columns `MAC address`, `Status`, `Description`, `Vendor`, `Endpoint IP address`, `User name`, `Endpoint profile`, `Last activity time` (by default), `Endpoint group`.

The page contain the following controls:

- - Refresh table data.
- 0/1 - Counter of elements selected by checkbox / total number of elements.
- - Add a new element.
- - Open the data filtering settings window for the table.
- - Customize the display of table columns.
- - Start updating profile of selected endpoints (inactive until at least one element is selected).
- - Delete selected elements (inactive until at least one element is selected).
- - Change the current sort order.
- - Checkbox that is responsible for selecting elements for further actions (for example, deletion).

Data filtering in the table is configured in the following window:

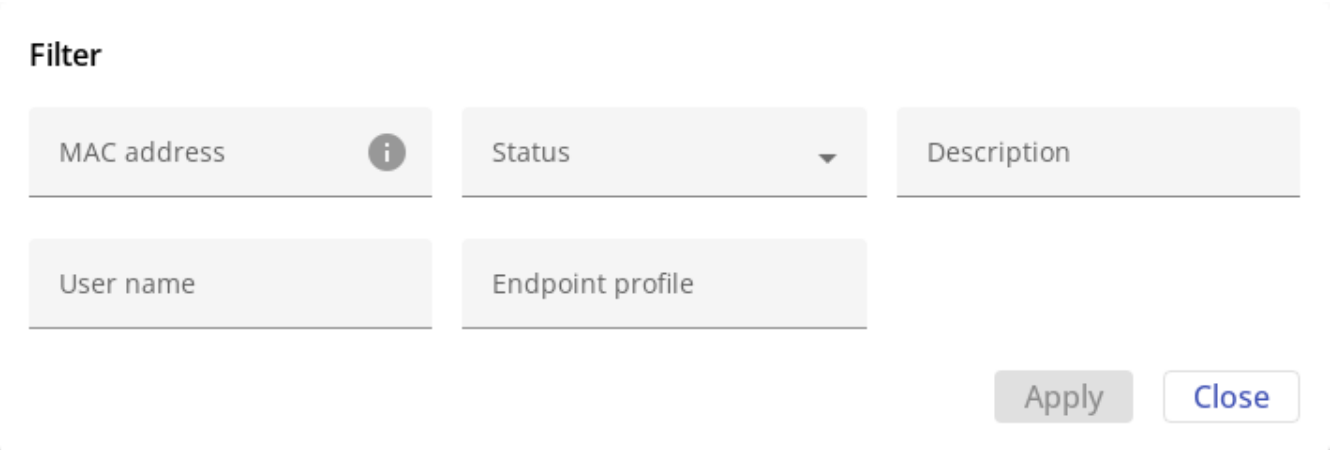

Figure 63. Configuring data filtering in the table

Filtering is available for the parameters `Endpoint profile`, `MAC address`, `Status`, `Description` and `User name`.

In the table settings you can change the set of the displayed columns.

The button selects or deselects all columns for display.

The button is reset displayed columns to their default state.

Adding an endpoint

Endpoints are automatically added to the system during authentication. An endpoint can be added manually. To add an endpoint, click ⊕ on the left side of the field above the table.

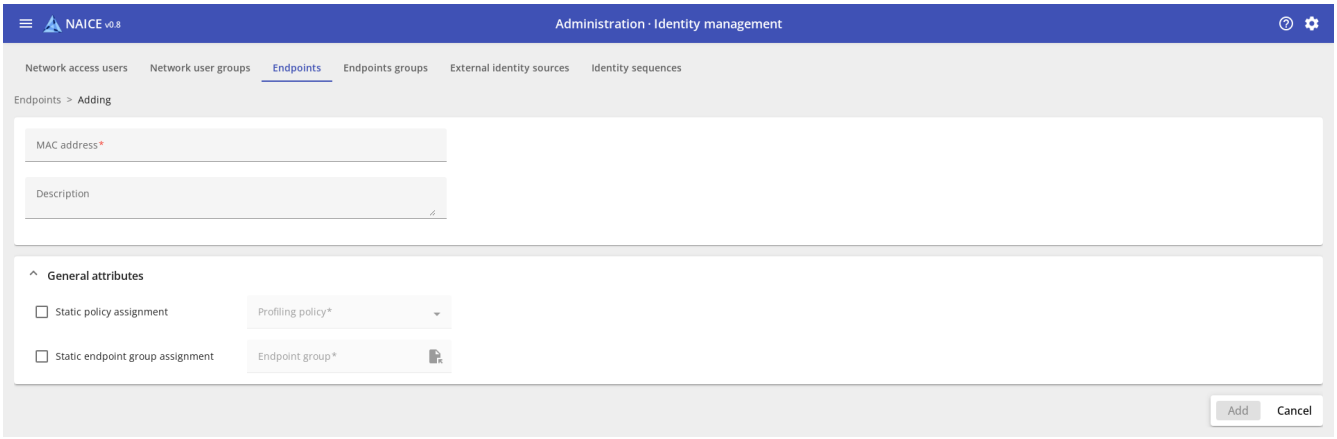

Figure 64. Adding an endpoint

The following parameters are presented on the page that opens:

- `MAC address` * - MAC address of the endpoint.
- `Description` - an arbitrary description up to 200 characters long.
- `Static policy assignment` - assign profiling policy to this endpoint manually. This value will not be overwritten by profiling.
- `Static endpoint group assignment` - assign group to this endpoint manually. This value will not be overwritten by profiling.

Parameters marked with * are required.

To add an endpoint to the list of endpoints, do not forget to click **Add**. To discard changes and return to the viewing page, click **Cancel**.

Editing an endpoint

To edit a previously added endpoint, on the view page, click on the endpoint's MAC address in the table.

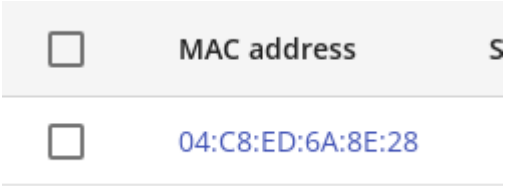

Figure 65. Hyperlink to the endpoint editing page

An editing page similar to the adding page will open.

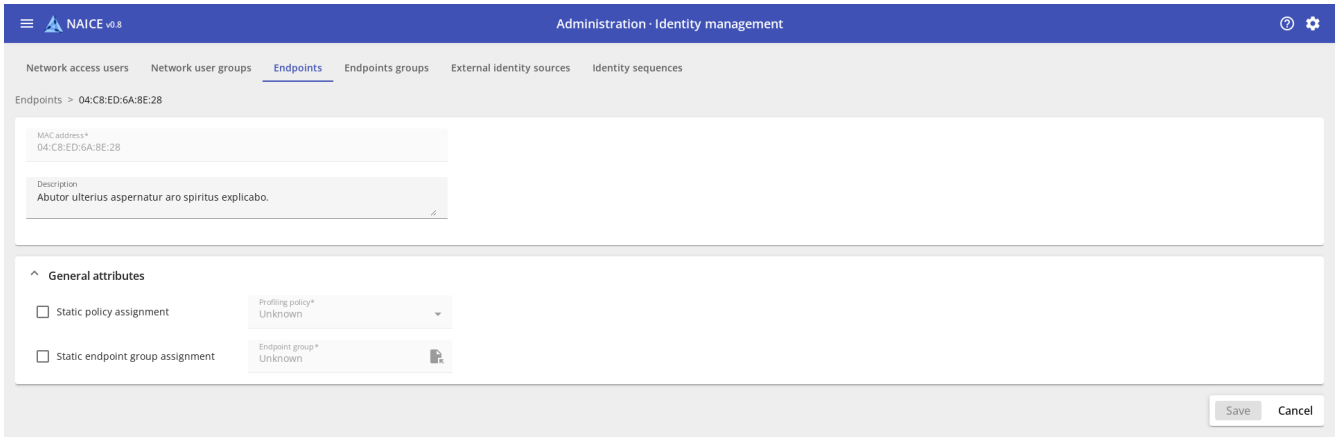

Figure 66. Editing an endpoint

Editing the endpoint's MAC address is not allowed.
If you need to edit the address, delete and create the endpoint again.

After editing, click **Save**. The button will remain inactive until at least one field is changed.

Viewing detailed information about an endpoint

To view detailed information about an endpoint, click on  in the `More` column in the table. A new tab with the required page will be opened.

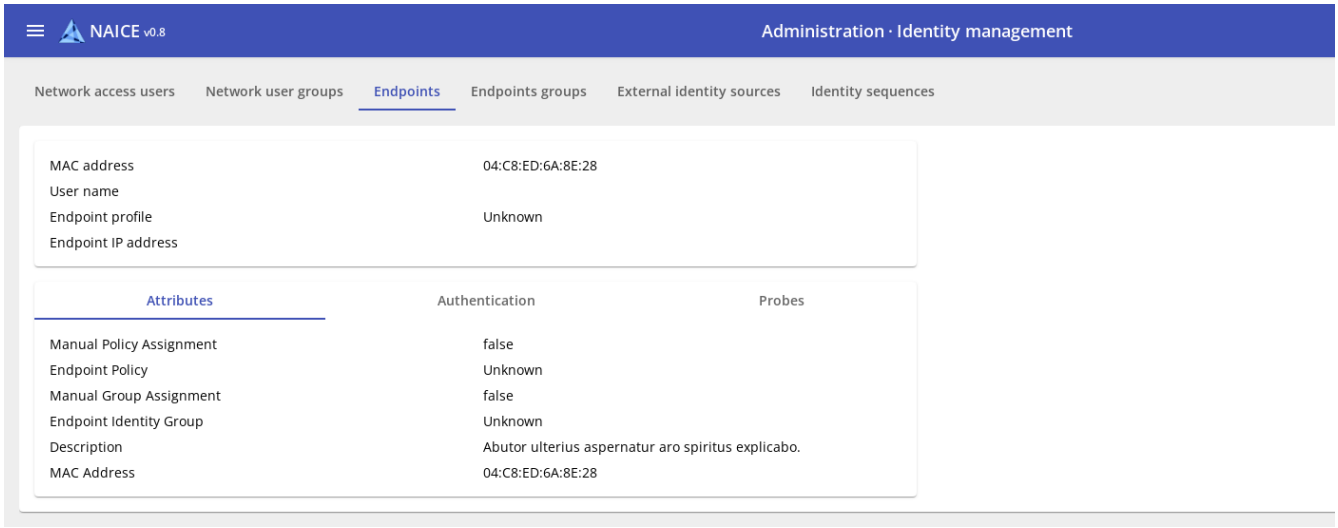

Figure 67. Viewing detailed information about an endpoint

The information on the page is divided into 4 blocks:

- Brief and most important information about the endpoint;
- **Attributes** - endpoint attributes that were obtained as a result of profiling or set by the administrator;
- **Authentication** - information about the last authentication of the endpoint:
  - `Overview` - brief information about the results of the last endpoint connection, displayed only if there were connection attempts;
  - `Authentication details` - detailed information that can be useful for debugging;
  - `Other attributes` - the contents of the packet received by NAICE from the RADIUS server;
  -

`Result` - a list of attributes that added in the client's response as a result of authorization (for example, attributes for issuing VLAN or ACL). If issuing additional attributes is not configured in the authorization profile, the list will be empty.

- **Probes** - data that can be used in profiling conditions.

Before the end of profiling and before the first authentication, the page may be almost empty. In this case, return to the page later.

Deleting an endpoint

The endpoint table is populated automatically during normal operation of NAICE then endpoints attempt to connect. If an endpoint has been deleted, it will be re-discovering the next time try to connect. Auto-discovering of endpoints can't be disabled.

To delete endpoints, on the viewing page, using the checkbox ☐, select the required endpoints and in the upper left corner above the table click on 🗑.

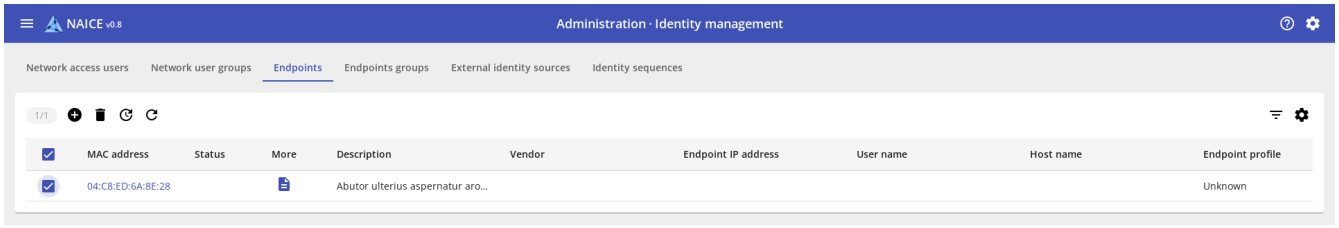

Figure 68. Selecting endpoints in the table to delete

Deletion requires confirmation of the action, for which a modal dialog will open.
After explicit confirmation, the selected items will be deleted.

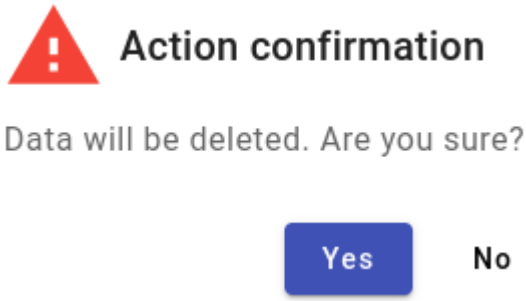

Figure 69. Modal dialog for confirmation

Endpoints groups

Description

Endpoints groups - is a collection of "Endpoints" grouped together based on logical criteria.

The NAICE system allows you to monitor endpoints in the network, group them manually or automatically, based on the parameters obtained during the profiling process.

Viewing all groups

When you navigate to the "Endpoint Groups" tab, a panel for viewing all groups will open.

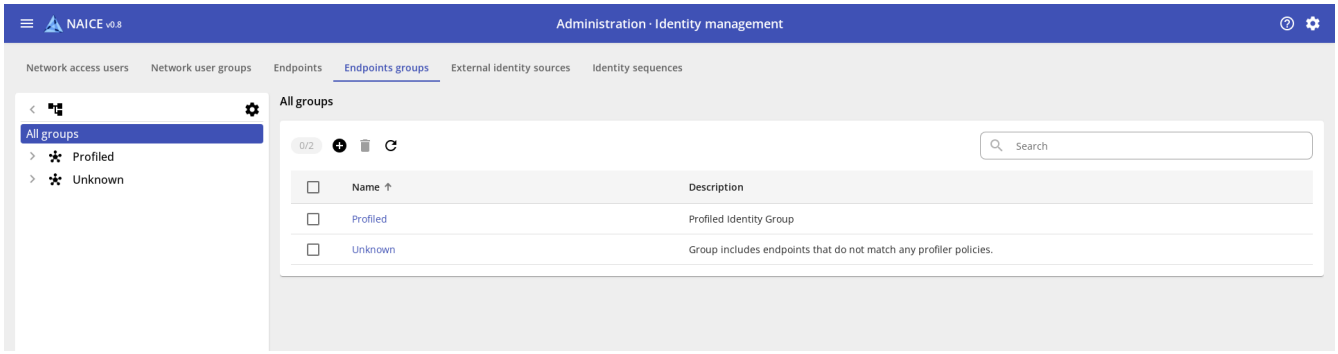

Figure 70. Viewing a list of endpoint groups

The table contains the following columns:

- `Name` - Group Name
- `Description` - Full description of the group

Controls:

- `Search` - Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.
- - Refresh table data.
- `0/1` - Counter of elements selected by the checkbox / total number of elements.
- - Add a new element.
- - Delete selected elements (inactive until at least one element is selected).
- - Change the current sort order.
- - Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).

A quick view panel in the form of a tree or list is located on the left side.

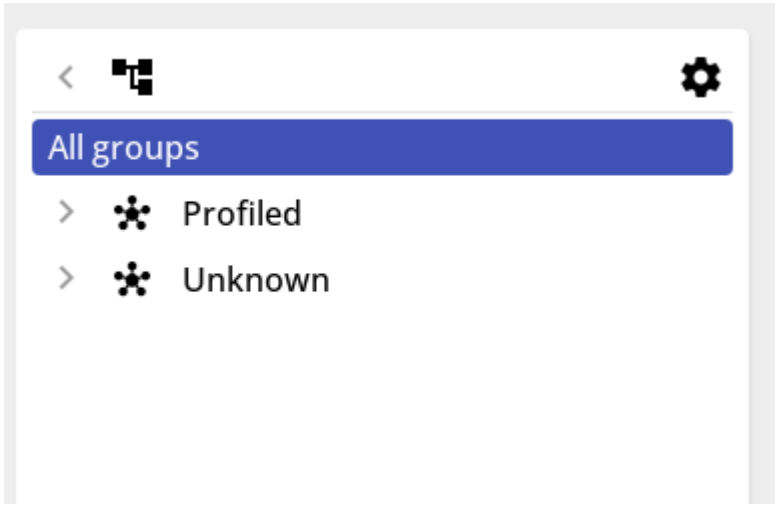

Figure 71. Menu for navigating the endpoint group tree

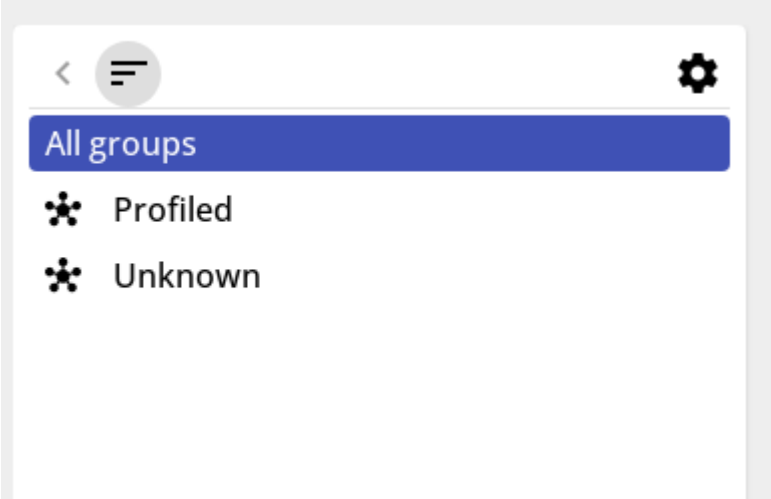

Figure 72. Menu for navigating in "list view mode"

The panel contains:

- `All Groups` - open the table for viewing and administering all groups
- ⚙ - Selection of available actions (depending on the selected item in the tree):
  - `Add root group`
  - `Add child group`
  - `Delete group`
- ⊞ - tree view mode enabled
- ☰ - list view mode enabled
- ‹ - move to the next level (active only in list mode).
- › - In "tree view mode", it is displayed to the left of the name of groups that have child elements if the list is closed. In "list view mode", it is displayed to the right of the name of groups that have child elements.

Group creation:

To add a group, please click the "Add Group" button. ⊕ On the left side of the field above the table, the 'Add Group' page will open.

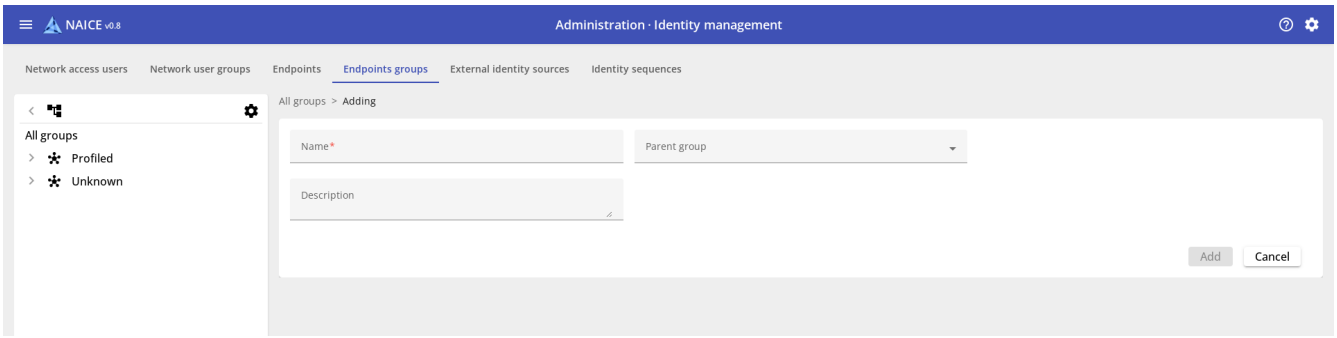

Figure 73. Endpoint group add form

The following parameters are available for filling in:

`Name` * - the name of the group. Maximum length - 100 characters.

- `Parent Group` - selecting the parent group from the list. This available for editing only at the time of group creation using the button ⊕.
- `Description` - a custom description of the group. Maximum length - 200 characters.

Parameters marked with a red asterisk * are required.

You can also create a group through the tree view panel by selecting the parent group and then clicking on `Add Child Group`.

Assigning a parent group cannot be changed later on.

Group editing

When you open a group record from the tree or table view, the group view/edit page will open.

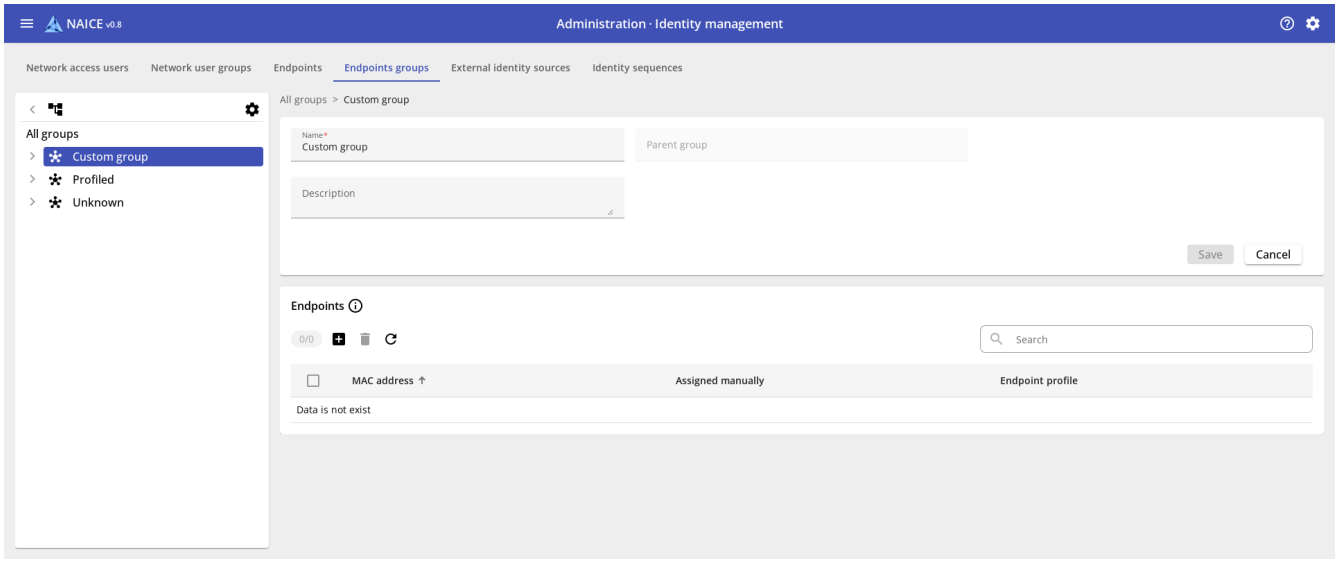

Figure 74. Endpoint group editing form

For editing, the following inputs are available:

- `Name` * - the name of the group. Maximum length - 100 characters.
- `Description` - a custom description of the group. Maximum length - 200 characters.

By clicking on `Save`, the changes you made to the group record will be updated in the system.

Assigning Endpoints to a Group

When you open a group record from the tree or table view, the group view page will open

At the bottom of the page, there will be a table displaying the assigned endpoints of the group.

The table contains the following columns:

- `MAC address` - The MAC address of endpoint.
- `Assigned manually` - Whether it was added to the group manually.

`Endpoint profile` - The profile assigned to this endpoint.

Controls:

- `Search` - Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.
- - Refresh table data.
- `0/1` - Counter of elements selected by the checkbox / total number of elements.
- - Add a new element.
- - Delete selected elements (inactive until at least one element is selected).
- - Change the current sort order.
- - Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).

When an endpoint is removed from a group, it is automatically assigned the **"Unknown"** group.

To add an endpoint to the group, click on . A window will open in which you need to select endpoints to add to the group using the checkboxes and move them to the “Selected” list using the button .

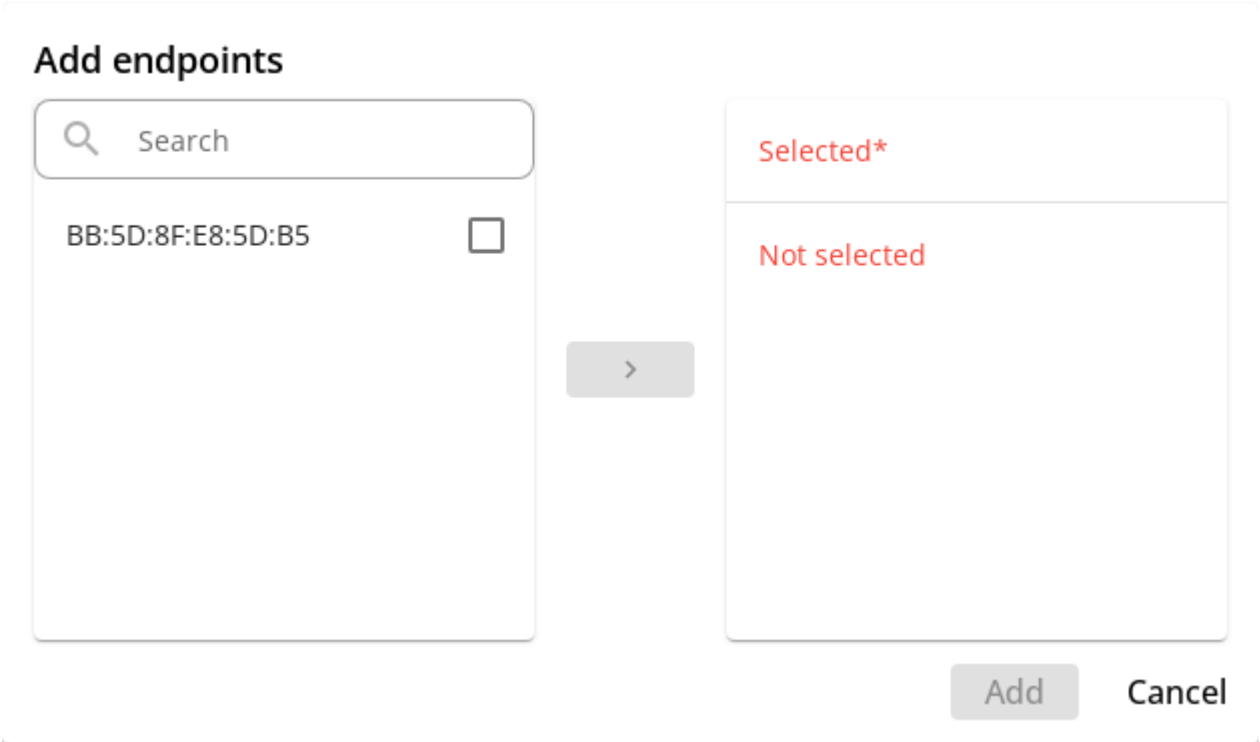

Figure 75. Modal dialog for adding endpoints

After adding all the required endpoints, click **Add**. The button will remain inactive until at least one endpoint is selected.

All changes in the **Endpoints** table are applied automatically and do not require pressing the **Save** button, the actions of which in this case apply only to the upper half of the panel.

Deleting a group

To delete groups, you need to go to the viewing page and use the checkbox. ☐, select the required groups and in the upper left corner above the table, click on 🗑 .

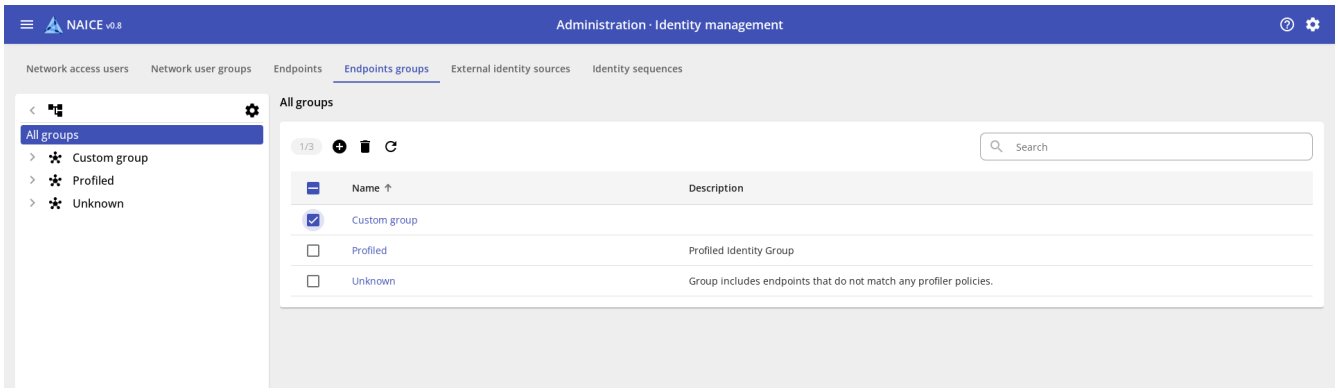

Figure 76. Select groups to delete

Deletion requires confirmation of the action, for which a modal dialog will open. After explicit confirmation, the selected items will be deleted.

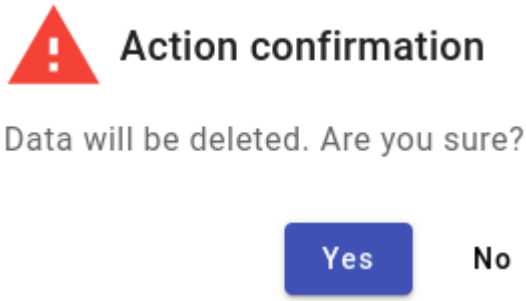

Figure 77. Modal dialog for confirmation

Restrictions:

- you cannot delete a group that has a child group;
- you cannot delete a group that contains endpoints;
- you cannot delete the Profiled and Unknown system groups.

External identity sources

Description

As a data source used for user authentication, in addition to internal user database, external sources of client data identification such as MS Active Directory or LDAP can be used.

In this section, you configure connections to external sources and add user groups and/or attributes that can later be used when setting up policy sets.

View external identity sources

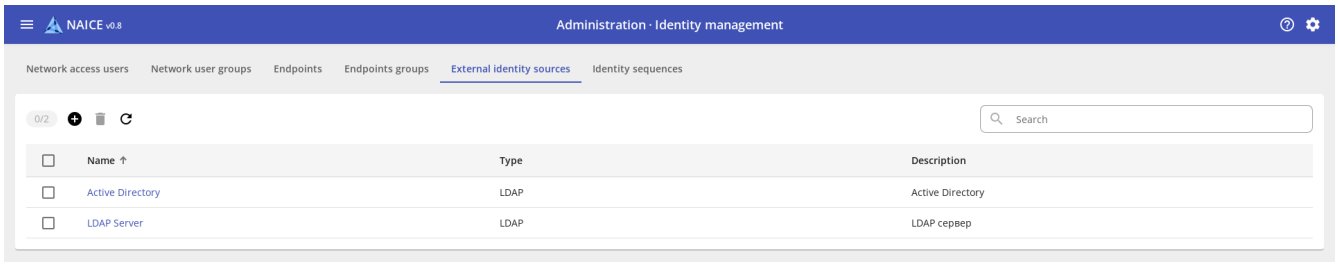

Figure 78. View external identity sources

This page contains a table with a list of external identification sources.

The table contains columns:

- `Name` - name of the source.
- `Type` - source type.
- `Description` - arbitrary description of the source.

It is possible to sort in direct and reverse order by the columns `Name`, `Description`. By default, sorting is performed in direct (alphabetical) order by the `Name` field.

Controls:

- `Search` - Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.
- - Refresh table data.
- `0/1` - Counter of elements selected by the checkbox / total number of elements.
- - Add a new element.
- - Delete selected elements (inactive until at least one element is selected).
- - Change the current sort order.
- - Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).

> Interaction with identification sources such as "MicroSoft Active Directory" and "LDAP" is supported.
> Each identity source has specific setup conditions and restrictions.

Setting up interaction with each type of identification source is discussed separately below.

Adding an Active Directory type identity source

Requirements

When integrating with a source of the MS Active Directory type, the following requirements must be met:

- The DNS server that are using by the Eltex-NAICE host must provide:

resolution of the full domain name (for example: EXAMPLE.ORG) in which Eltex-NAICE are operating;

  - resolution of the full name of the AD controllers (for example: SRV1.EXAMPLE.ORG) servicing the domain;
  - return a response to the DNS SRV query with a list of controllers servicing the domain.

- The minimum version of the Active Directory controller: Windows Server 2008 R2.
- The use of the NTLM protocol by the Active Directory controller on which user authorization is performed must be allowed.
- In the MS AD domain with which integration is performed, it is necessary to add computer and user accounts for interaction with Eltex-NAICE.
- The user and computer accounts must have a password.

You can set the password using the command in the PowerShell shell, which is part of Active Directory, launched with administrator rights:

```
Set-ADAccountPassword -Identity Computer-Name$ -Reset
```

enter the password twice in the terminal window.

If you need to specify the password explicitly in the command:

```
Set-ADAccountPassword -Identity Computer-name$ -Reset -NewPassword (ConvertTo-SecureString
-AsPlainText "password" -Force)
```

The computer name must be specified without the domain part, ending in "$". WARNING: The password must meet the requirements configured in MS AD.

The user account must have the following rights:

- Perform a search in Active Directory
- Get information about all users and groups in the domain

Rights to write information to Active Directory are not required.

Also, in the user settings, you must disable the "require password change on first connection" option (enabled by default)

Eltex-NAICE accesses Active Directory using the following ports:

Protocol	Port	Purpose	Note
UDP	53	DNS	The server responsible for resolving domain names can be separate from the Active Directory server
TCP/UDP	389	LDAP	
TCP/UDP	3268	LDAP GC	Can be used instead of port 389 if there is no forest of trees
TCP/UDP	49152-65535	RPC Dynamic Port Range	

Adding an identity source

To add an identification source, click ⊕ on the right side of the field above the table, the following page will open.

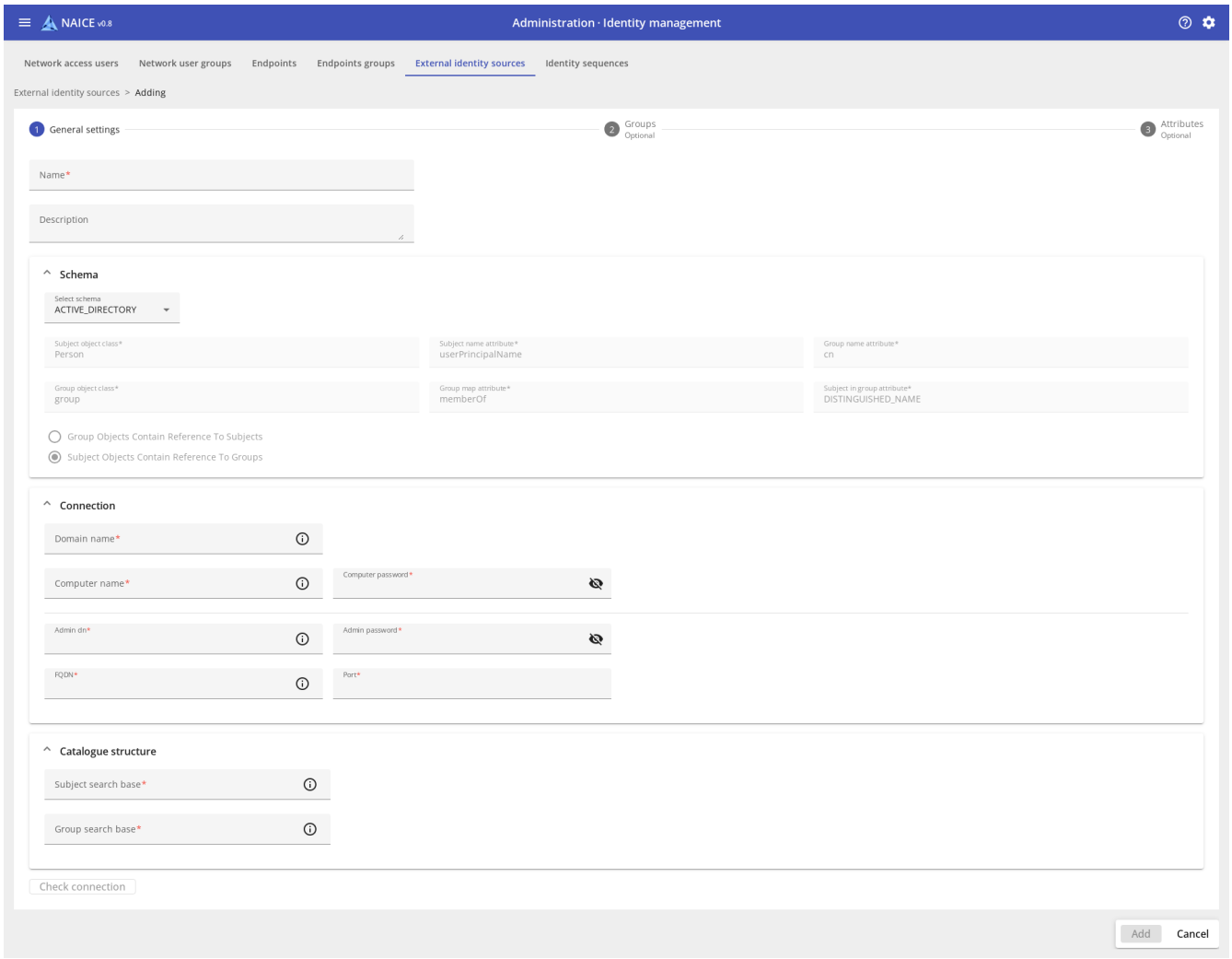

Figure 79. Window for adding identification source

This form provides the following parameters:

- Block **General settings**:
  - `Name` * - name of the identification source. The maximum field length is 64 characters.

- `Description` - description. The maximum field length is 200 characters.

- Block **Schema**:
  - `Select schema` * - scheme of the identification source attributes. "ACTIVE_DIRECTORY" is selected by default, for this scheme the attribute values are preset and cannot be changed.

- Block **Connection**:
  - `Domain name` * - name of the Active Directory domain in which users will be authorized. It is necessary to specify only the short name of the domain in which users will be authorized. The field is available only for the "ACTIVE_DIRECTORY" scheme. The maximum field length is 63 characters.
  - `Computer name` * - name of the administrative computer for interaction with Active Directory. It is necessary to specify only the name, without the domain part. The field is only available for the "ACTIVE_DIRECTORY" scheme. The maximum field length is 63 characters.
  - `Computer password` * - password of the administrative computer for interaction with Active Directory. Not displayed by default, to view it you need to click . The field is only available for the "ACTIVE_DIRECTORY" scheme. The maximum field length is 200 characters.
  - `Admin dn` * - administrative user data for interaction with Active Directory. The user name must be specified in the UPN format: <user>@<domain> or in the pre-Windows 2000 format: <DOMAIN NAME>\<user>. The maximum field length is 200 characters.
  - `Admin password` * - password of the administrative user. Not displayed by default, to view it you need to click . The maximum field length is 200 characters.
  - `FQDN` * - the full domain name or the full name of the Active Directory domain controller preferred for requests. The maximum field length is 255 characters. If a domain controller is specified as the preferred one for performing requests, requests to it will be performed while it is available. If it is unavailable, requests will be performed to the next server from the list of servers for the domain, obtained from the DNS query of the SRV type.
  - `Port` * - the port for connecting to the domain controller(s) (usually TCP:389 is used).

- **Directory Structure** block:
  - `Subject search base` * - context for searching for attributes of directory service records. The maximum field length is 200 characters.
  - `Group search base` * - context for searching for directory service groups. The maximum field length is 200 characters.

Both fields are in the format of a comma-separated attribute=value list, such as "dc=example,dc=org". If you want to limit the search to a specific department (ou), you must specify it, such as "ou=naice,dc=example,dc=org". If there are several nested departments, you must specify them all, starting with the one furthest from the root of the domain, such as "ou=test,ou=naice,dc=example,dc=org" - this will correspond to the structure:

```
(dc)org
       \-(dc)example
                    \-(ou)naice
                              \-(ou)test
```

More information about the format of the data entered in this field can be found by hovering over ⓘ or in the tooltip below. - `Check connection` - check the correctness of the settings and connection to the Active Directory server.

Parameters marked with an asterisk * are required.

Valid characters when entering Subject search base and Group search base parameters:

- space,
- double quotes (""),
- equal sign (=),
- comma (,),
- hyphen (-),
- latin letters (a-z)(A-Z),
- russian letters (а-я)(А-Я),
- numbers (0-9).

Entering other elements is prohibited.

When saving, the system automatically removes spaces near the equal sign (=) and comma (,), the value with a space is taken in double quotes. The attribute value entered to the left of the equal sign (=) is converted to lower case.

Example:

Entered value	Saved value
ou=naice test, dc = example ,dc = org	ou="naice test",dc=example,dc=org
ou="naice test",dc = example,dc=org	ou="naice test",dc=example,dc=org

After filling in all the necessary data, the **Add** and **Check connection** button will become active.

The **Add** button becomes active if all parameters are added and does not depend on the success of the connection check with the server.

If the connection with the server is successfully checked, a message similar to the following will appear:

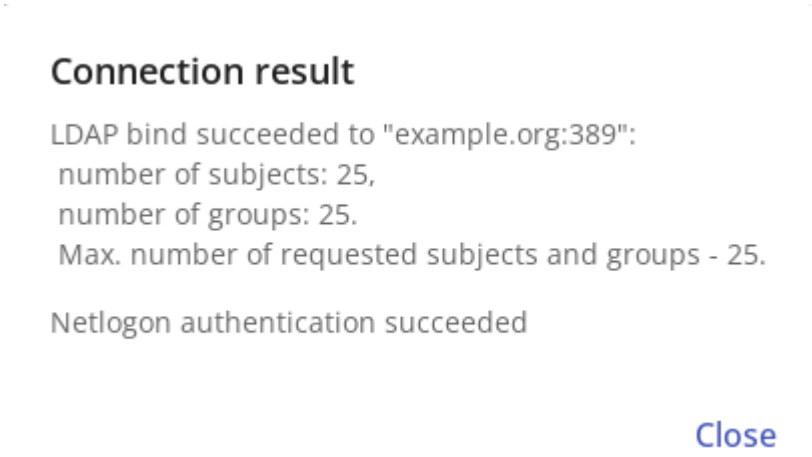

Figure 80. LDAP binding successful

A message like "Netlogon authentication succeeded" confirms that users can be authorized.

When checking a connection, no more than 25 items and groups are requested, so as not to cause unnecessary load on the server, so if the number “25” is shown more than real users or groups, this does not indicate a problem.

Adding user groups

Adding groups is not required to enable authentication through an external identity source. Groups can be used in user authorization policies.

After adding an identification source, the **Add** button will change to **Next**. You can also make the transition by clicking on the inscription **(2) Groups**, the page will open:

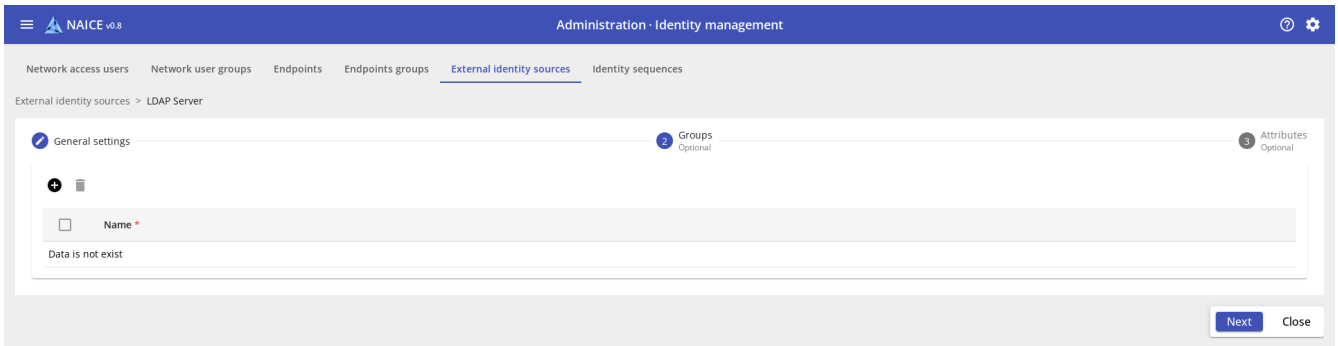

Figure 81. Empty group table

The table contains columns:

- `Name` * - group name

Controls:

-  - add a group.
-  - delete groups selected by the checkbox (inactive until at least one group is selected).
-  - edit a group (not displayed until at least one group has been added).

- save the group after editing (not displayed until editing of the group has started).

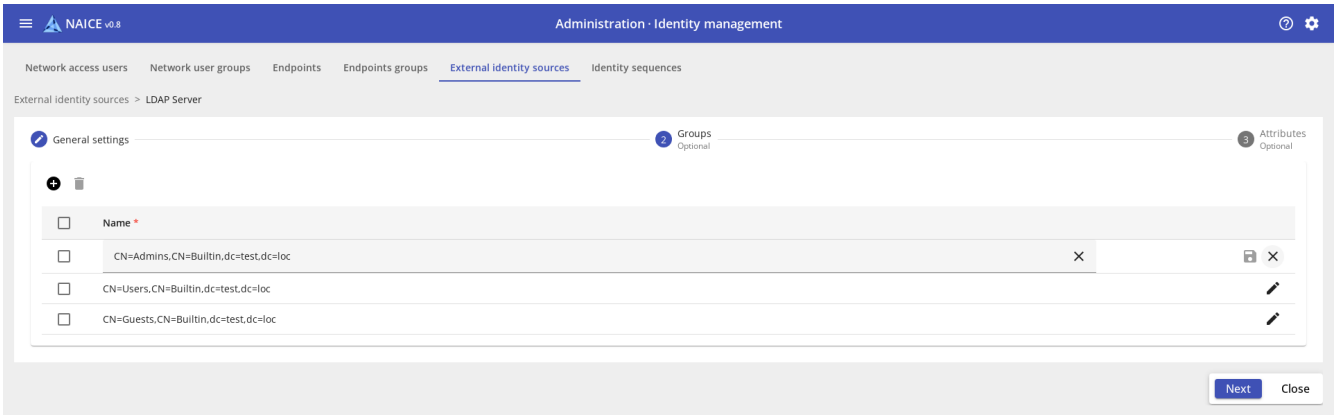

Figure 82. Group table in edit mode

After clicking on the button ⊕ a menu will open:

- `Add new group` - create a custom new group.
- `Select groups from directory` - add groups from the identification source.

Add new group

Figure 83. Add new group

In the line that appears, you need to specify a custom group name. After filling in the group name, the save button will become active. You need to click it to add a group.

Select groups from directory service

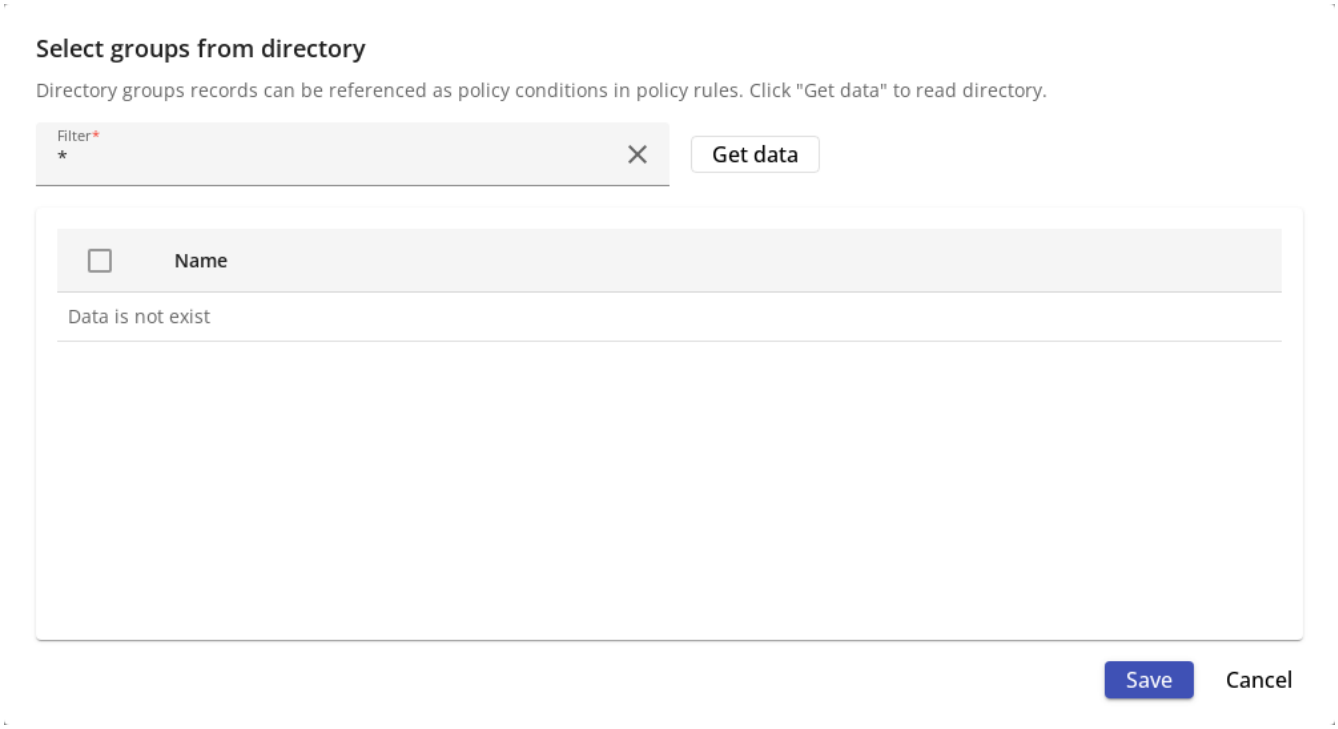

Figure 84. Group selection window

This window presents the following parameters:

- `Filter` * - filter for searching groups, default "*", you can enter the name of the group.
- `Get data` - get data taking into account the filter

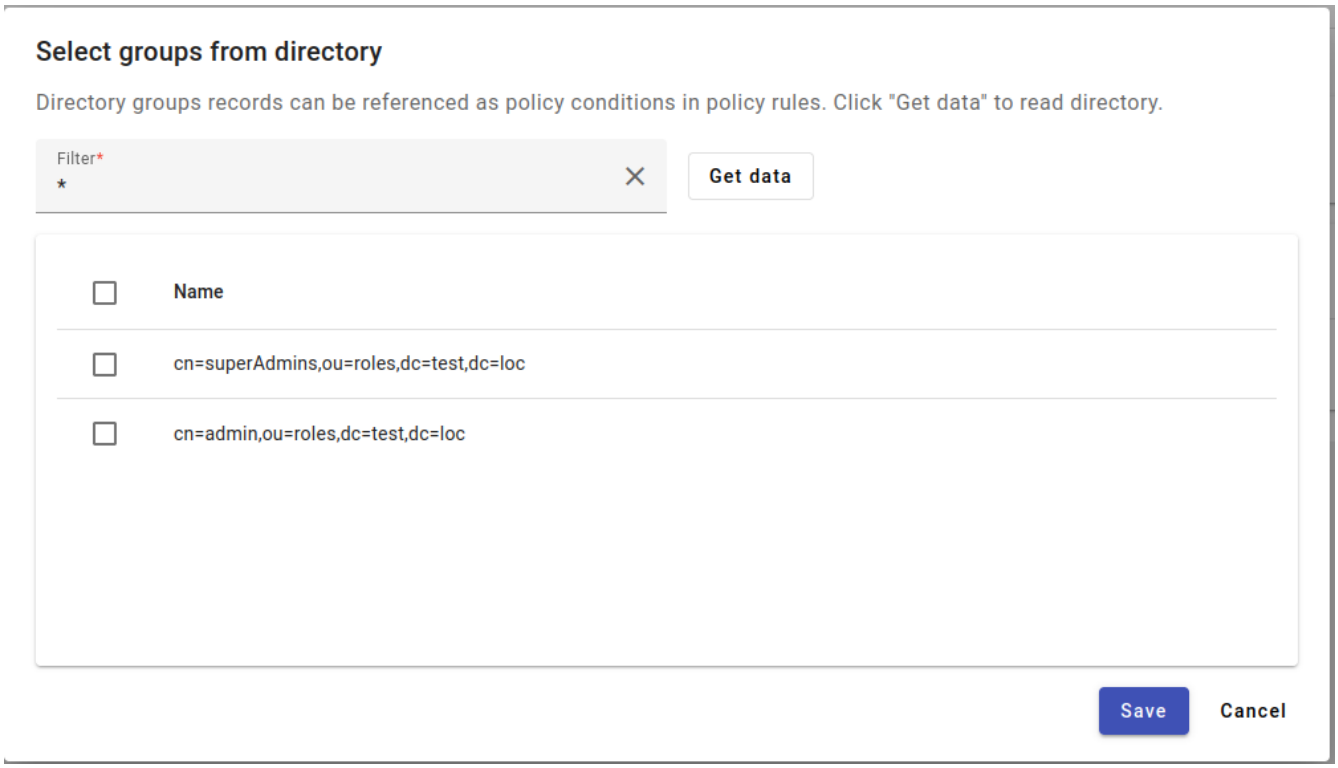

Figure 85. Group selection window after receiving data

You need to select the required groups using the ☐ checkbox on the left and click the **Save** button.

Previously saved groups that were not reselected in the search list will be deleted when resaving other selected groups!

Adding attributes

To be able to authenticate via an external identity source, adding attributes is optional. Attributes can be used in policies and user authorization profiles.

After adding groups, you can click the "Next" button at the bottom right of the screen. You can also make the transition by clicking on the inscription **(3) Attributes**, the page will open:

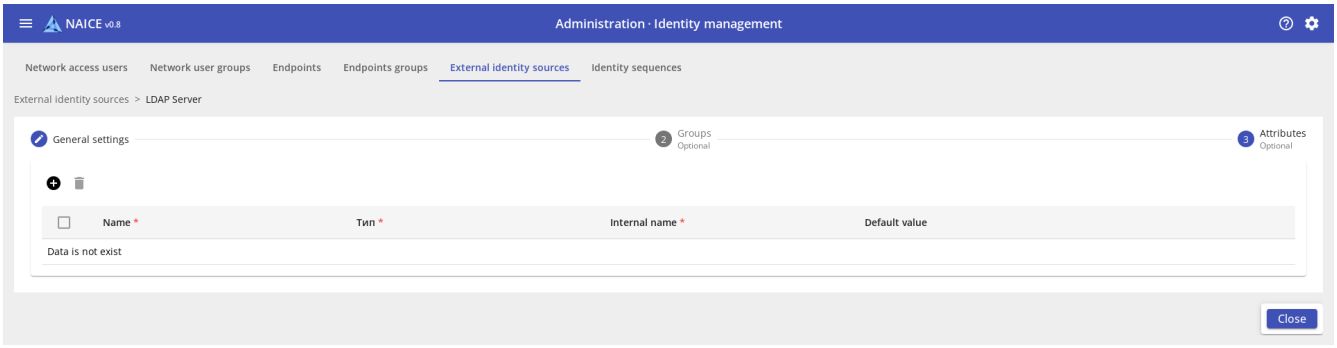

Figure 86. Adding attributes

The table contains columns:

- `Name` * - the name of the attribute that will be displayed in the LDAP dictionary and used when setting up logical conditions and authorization profiles. You can specify an arbitrary one for ease of use.
- `Type` * - attribute type, possible values:
  - `INTEGER` - numeric,
  - `IP_4_ADDR` - IPv4 address,
  - `STRING` - string.
- `Internal name` * - the name of the attribute in the Active Directory schema.
- `Default value` - the attribute value that will be used if it is not obtained from Active Directory.

Controls:

- - add attributes.
- - delete the attributes selected by the checkbox (inactive until at least one attribute is selected).
- - edit attributes (not displayed until at least one is added).
- - save the attribute after editing (not displayed until editing has started).

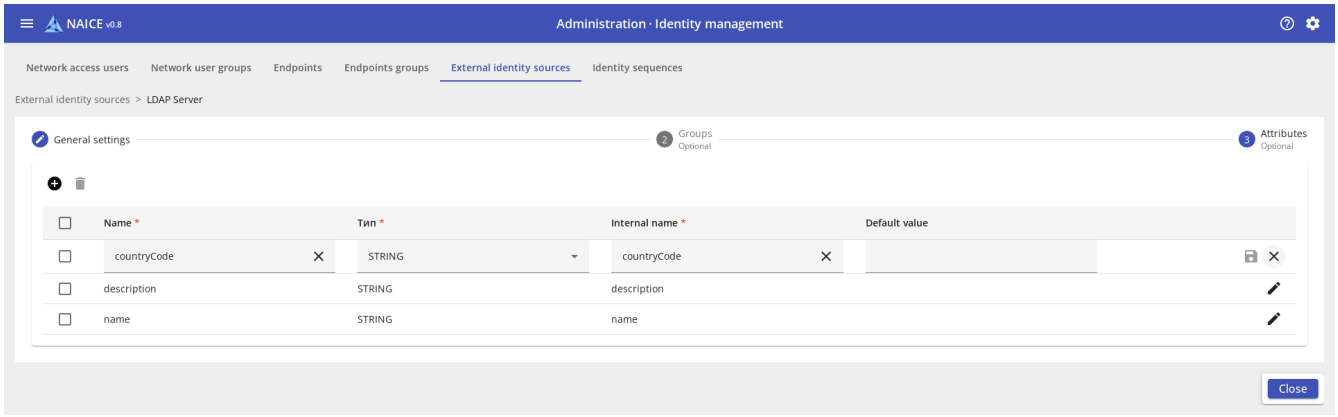

Figure 87. Attribute table in edit mode

After clicking on the button ⊕ a menu will open:

- `Add new attribute` - create an arbitrary new attribute.
- `Select attribute from directory` - add an attribute from the identification source.

Add new attribute

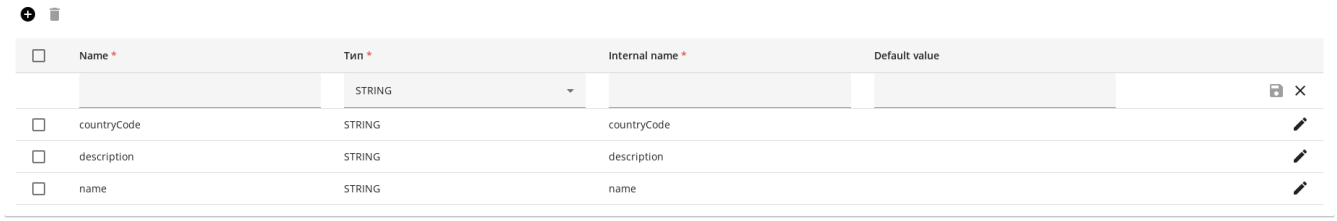

Figure 88. Add new attribute

The line that appears to add an attribute contains the following parameters:

- `Name` * - arbitrary attribute name that will be displayed in the dictionary.
- `Type` * - attribute type. Possible values:
  - `INTEGER` - numeric,
  - `IP_4_ADDR` - IPv4 address,
  - `STRING` - string (default).
- `Internal name` * - attribute name from the identification source.
- `Default value` - the attribute value that will be used if it is not obtained from Active Directory..

Parameters marked with an asterisk * are required.

After filling in the required parameters, the save button will become active. You need to click it to add an attribute.

Select attribute from directory service

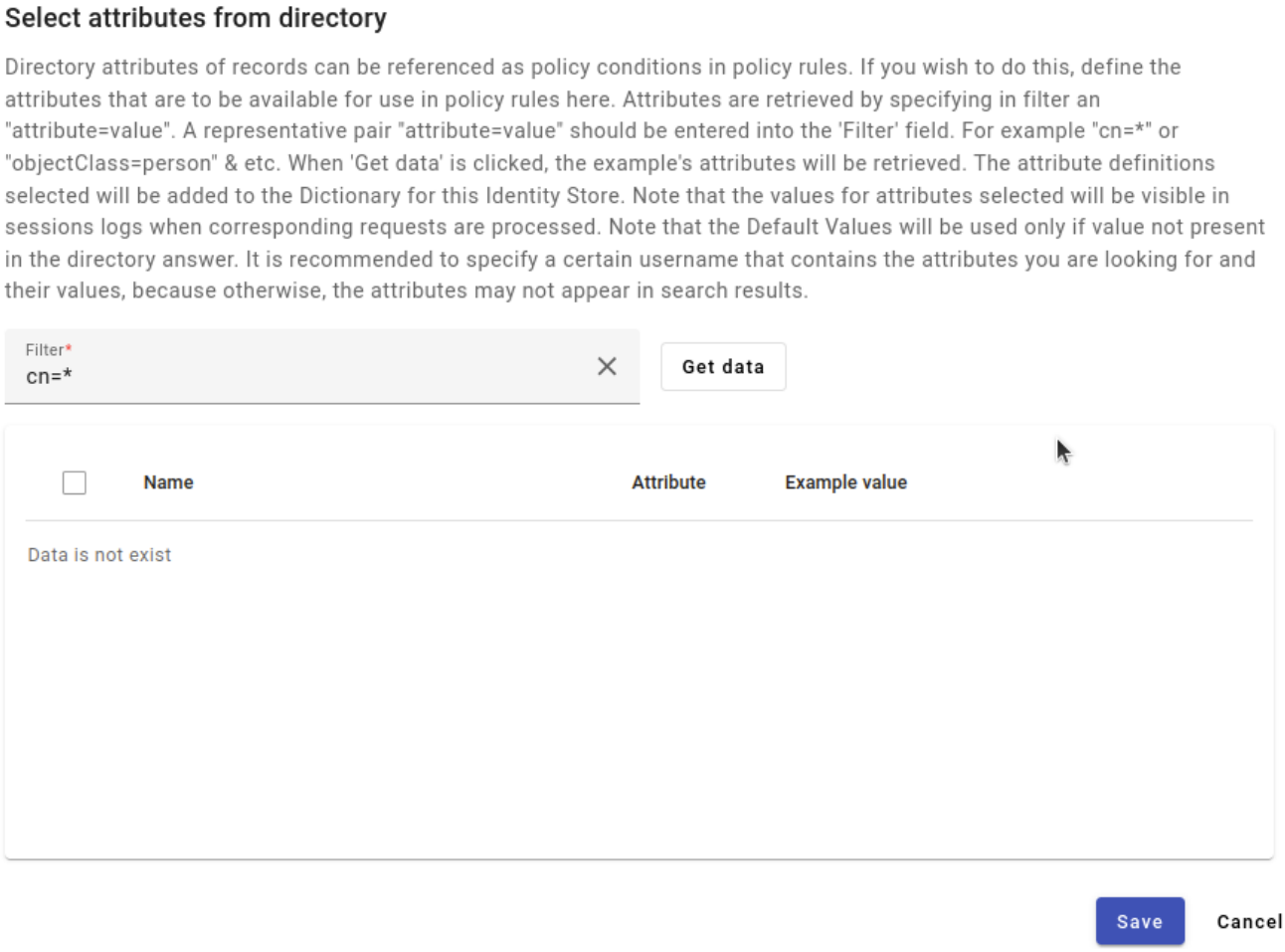

Figure 89. Selecting attributes from a directory service

This window presents the following parameters:

- `Filter` * - filter for searching attributes, default `cn=*`. You can use the expression `<Attribute>=<value>` as a filter; if the value is not important, you must specify `*`. If an attribute has multiple values, only the first one found is displayed.
- `Get data` - get data taking into account the filter.

In general, additional user attributes are added after they have been given values, and cannot be subtracted before that.

To select attributes from an Active Directory type source, it is recommended to use the `userPrincipalName` or `sAMAccountName` attribute, specifying a specific account that contains the entities being imported. For example:

```
userPrincipalName=ivan.ivanov@example.org

sAMAccountName=ivan.ivanov
```

To select attributes from an LDAP type source, it is recommended to use the attribute that is specified in the `Subject name attribute` schema setting.

After receiving attribute data:

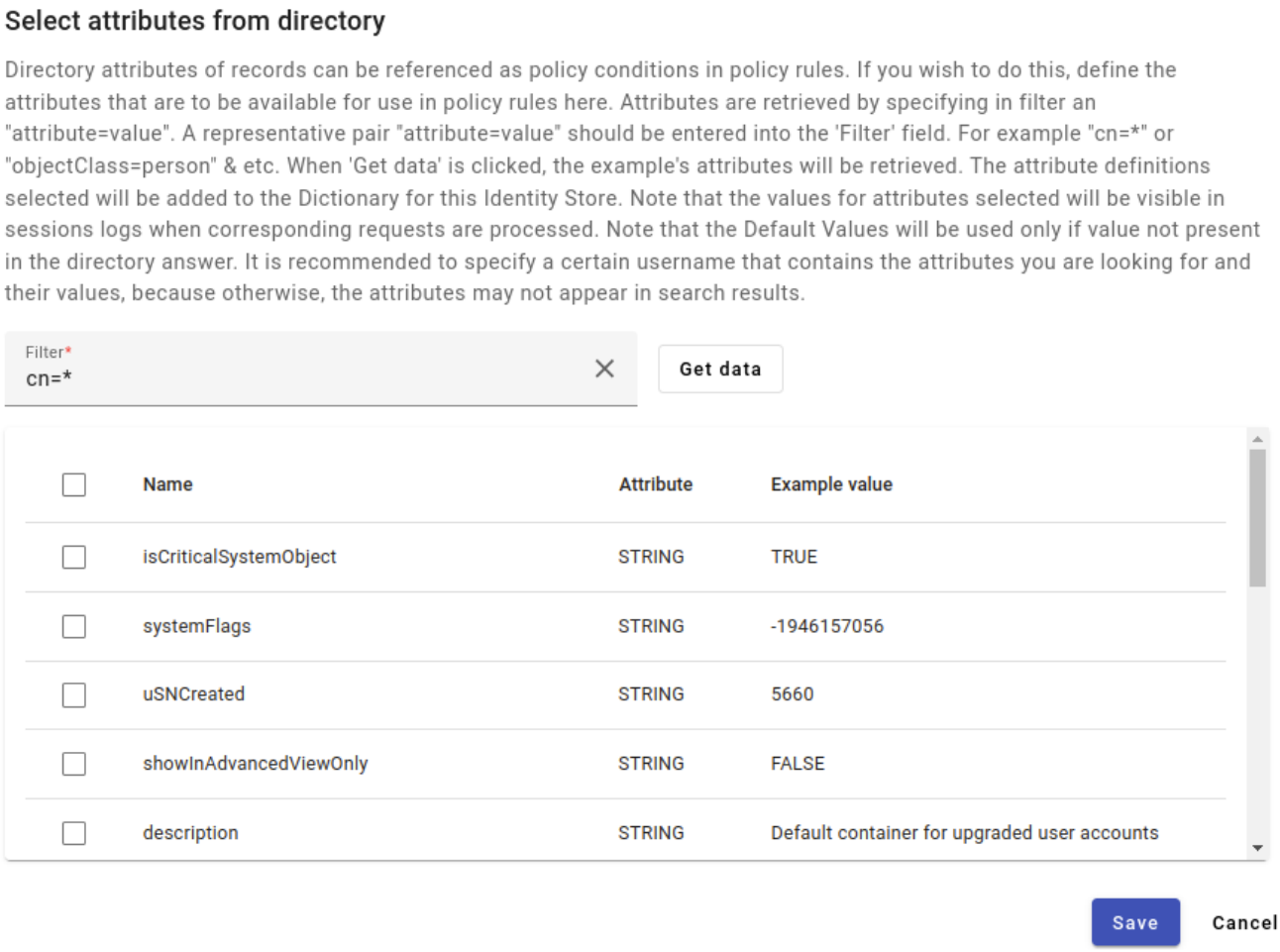

Figure 90. Attribute selection window after receiving data

You need to select the required attributes using the checkbox on the left and click the **Save** button.

Previously saved attributes that were not reselected in the search list will be deleted when resaving other selected attributes!

Adding a Custom identity source

This type of identification source is intended for integration with an LDAP server, which can have an arbitrary scheme.

Adding an identity source

To add an identification source, click on the right side of the field above the table, the following page will open, where you will need to select the `CUSTOM` scheme:

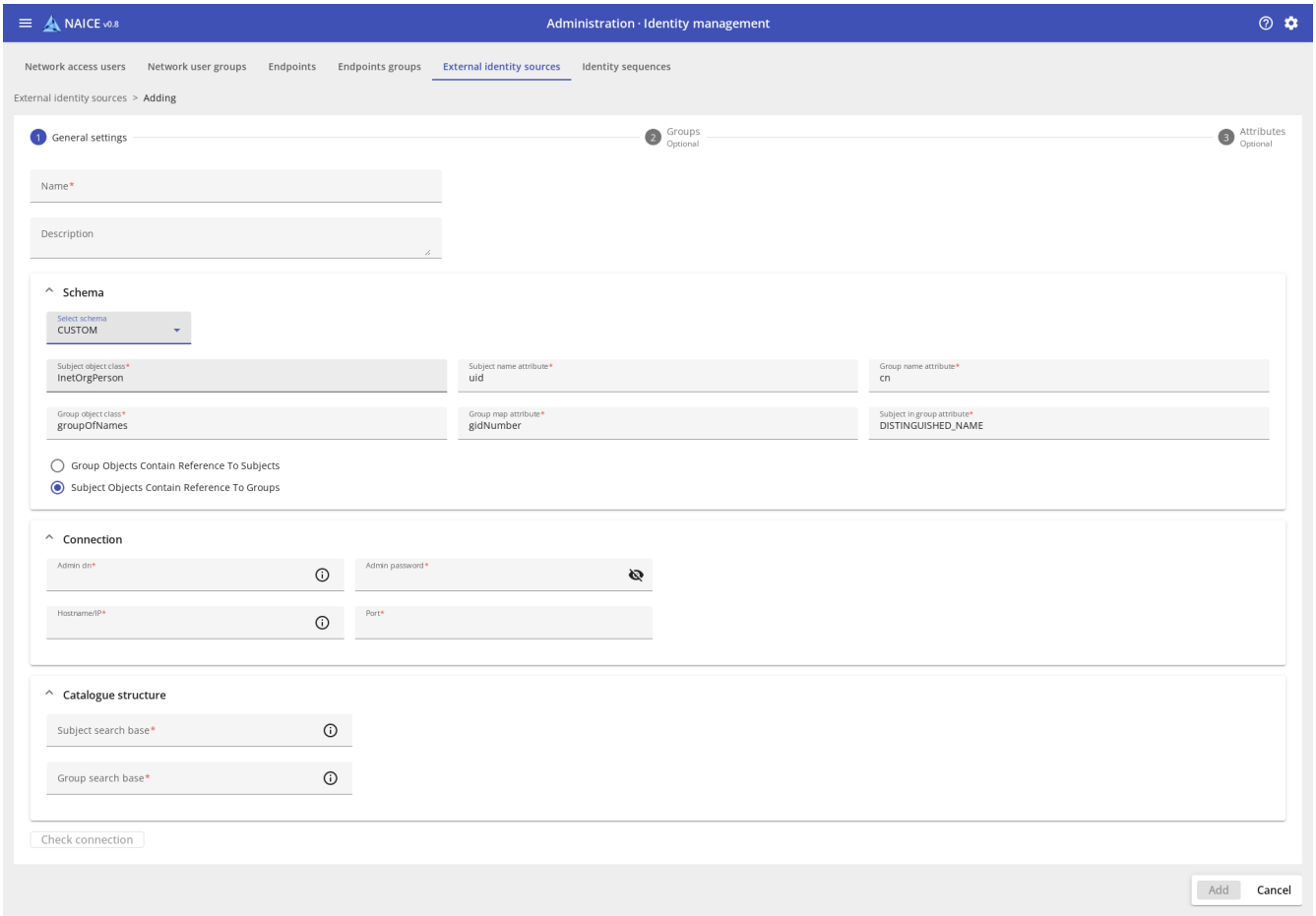

Figure 91. Window for adding identification source

This form provides the following parameters:

- Block **Basic settings**:
  - `Name` * - name of the identification source.
  - `Description` - description.
- Block **Scheme**:
  - `Select scheme` * - identification source attribute scheme. By default, `ACTIVE_DIRECTORY` is selected; you need to change it to `CUSTOM` to make the selection of schema attribute values available.
  - `Subject object class` * - attribute defining the user class.
  - `Subject name attribute` * - an attribute that defines the user name that he will use as a login on the client device.
  - `Group name attribute` * - attribute defining the user group name.
  - `Group object class` * - attribute defining the group class.
  - `Group map attribute` * - attribute that determines membership in a group.
  - `Subject in group attribute` - an attribute whose value is used in the value of the "Group map attribute" attribute when checking whether a user belongs to a group.
  - `Groups contain users` * - select if the user's group membership attribute is in the group attributes.
  - `Users contain groups` * - select if the user's group membership attribute is in the user attributes.

Block **Connection**:

- `Admin dn` * - administrative user data for interaction with LDAP (in the format "cn=admin,dc=example,dc=org").
- `Admin password` * - administrative user password. Not displayed by default, to view you need to click  .
- `Hostname/IP` * - IP address or domain name of the LDAP server.
- `Port` * - connection port (usually 389 is used).

- Block **Catalogue structure**:
  - `Subject search base` * - context for searching attributes in directory service.
  - `Group search base` * - context for searching groups in directory service.

Both fields have a comma-separated enumeration format attribute=value, for example dc=test,dc=loc or ou=naice test,dc=test,dc=loc.

Parameters marked with an asterisk * are required.

The maximum length of the `Name` field is 64 characters. Other fields have 200 characters.

Valid characters when entering Subject search base and Group search base parameters:

- space,
- double quotes (""),
- equal sign (=),
- comma (,),
- hyphen (-),
- latin letters (a-z)(A-Z),
- russian letters (а-я)(А-Я),
- numbers (0-9).

Entering other elements is prohibited.

When saving, the system automatically removes spaces near the equal sign (=) and comma (,), the value with a space is taken in double quotes. The attribute value entered to the left of the equal sign (=) is converted to lower case.

Example:

Entered value	Saved value
ou=naice test, dc = test ,dc = loc	ou="naice test",dc=test,dc=loc
ou="naice test",dc = test,dc=loc	ou="naice test",dc=test,dc=loc

After filling in all the necessary data, the **Add** and **Check connection** button will become active.

The **Add** button becomes active if all parameters are added and does not depend on the success of the connection check with the server.

If the connection to the server is successfully checked, a message like this will appear:

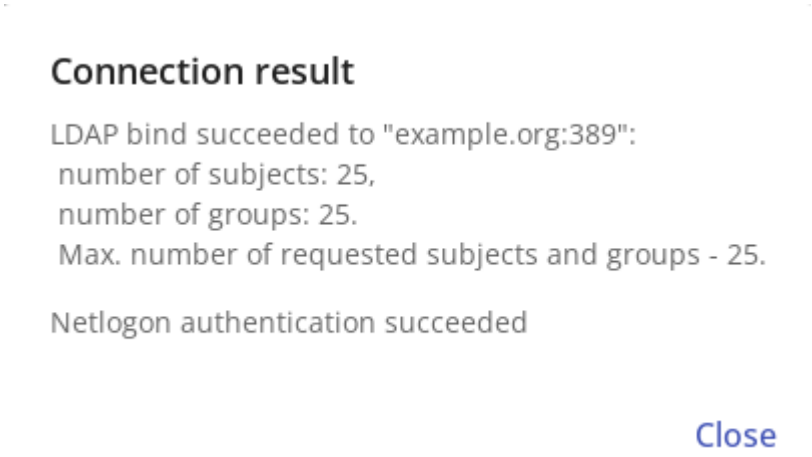

Figure 92. LDAP binding successful

When checking a connection, no more than 5 items and groups are requested, so as not to cause unnecessary load on the server, so if the number “5” is shown more than real users or groups, this does not indicate a problem.

Adding user groups

Adding groups is optional to enable authentication through an external identity source. Groups can be used in user authorization policies.

After adding an identification source, the **Add** button will change to "Next". You can also make the transition by clicking on the inscription **(2) Groups**, the page will open:

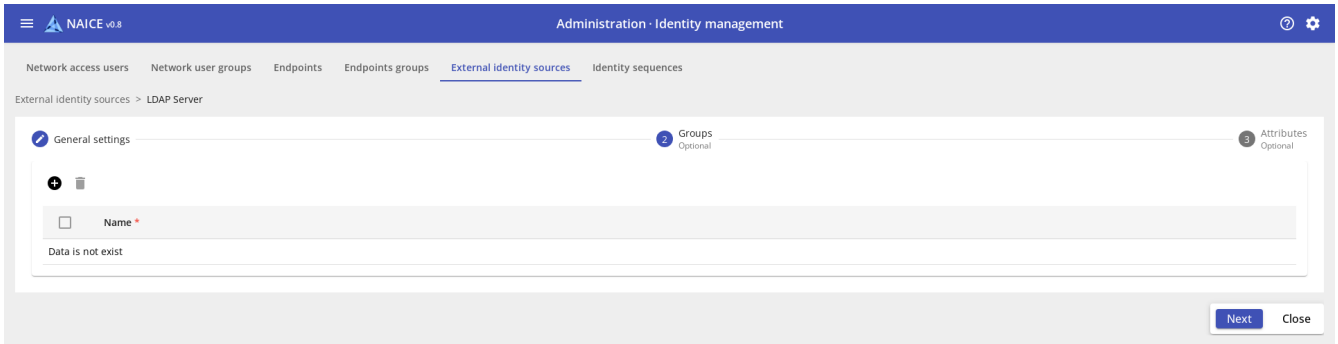

Figure 93. Empty group table

Controls:

-  - add a group.
-  - delete groups selected by the checkbox (inactive until at least one group is selected).

After clicking on the button  a menu will open:

`Add new group` - create a custom new group.

- `Select groups from directory service` - add groups from the identification source.

Add new group

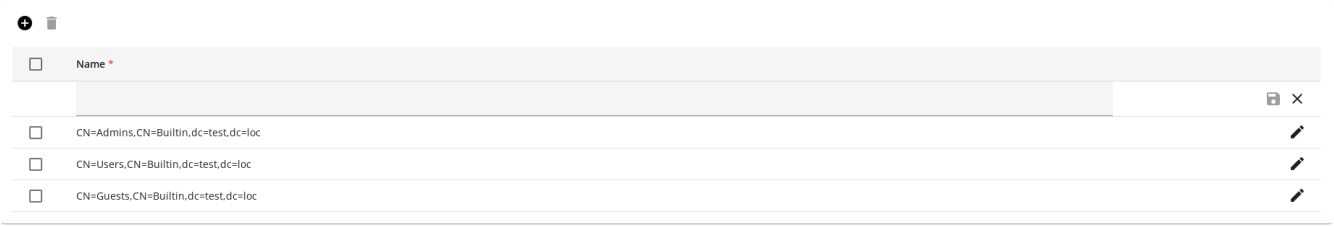

Figure 94. Add new group

In the line that appears, you need to specify a custom group name. After filling in the group name, the save button will become active. You need to click it to add a group.

Select groups from directory service

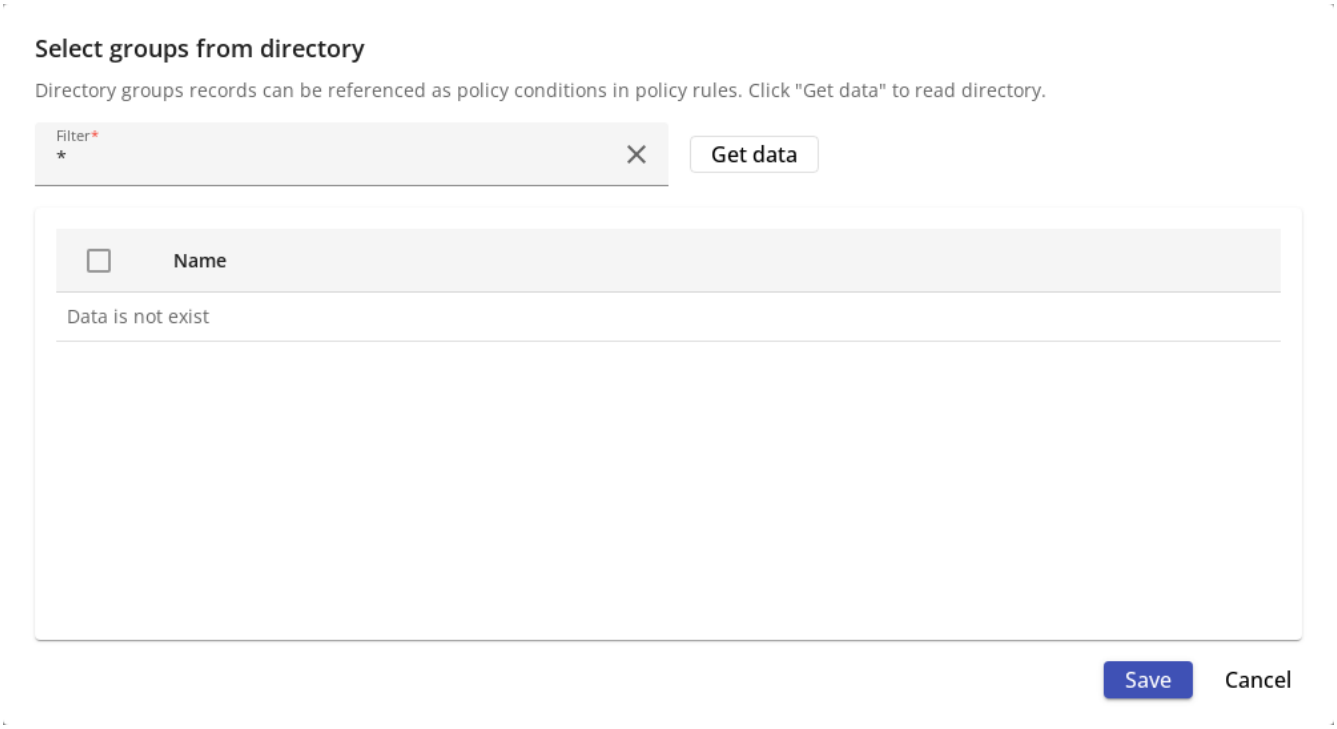

Figure 95. Group selection window

This window presents the following parameters:

- `Filter` * - filter for searching groups, by default *, you can enter the name of the group.
- `Get data` - get data taking into account the filter.

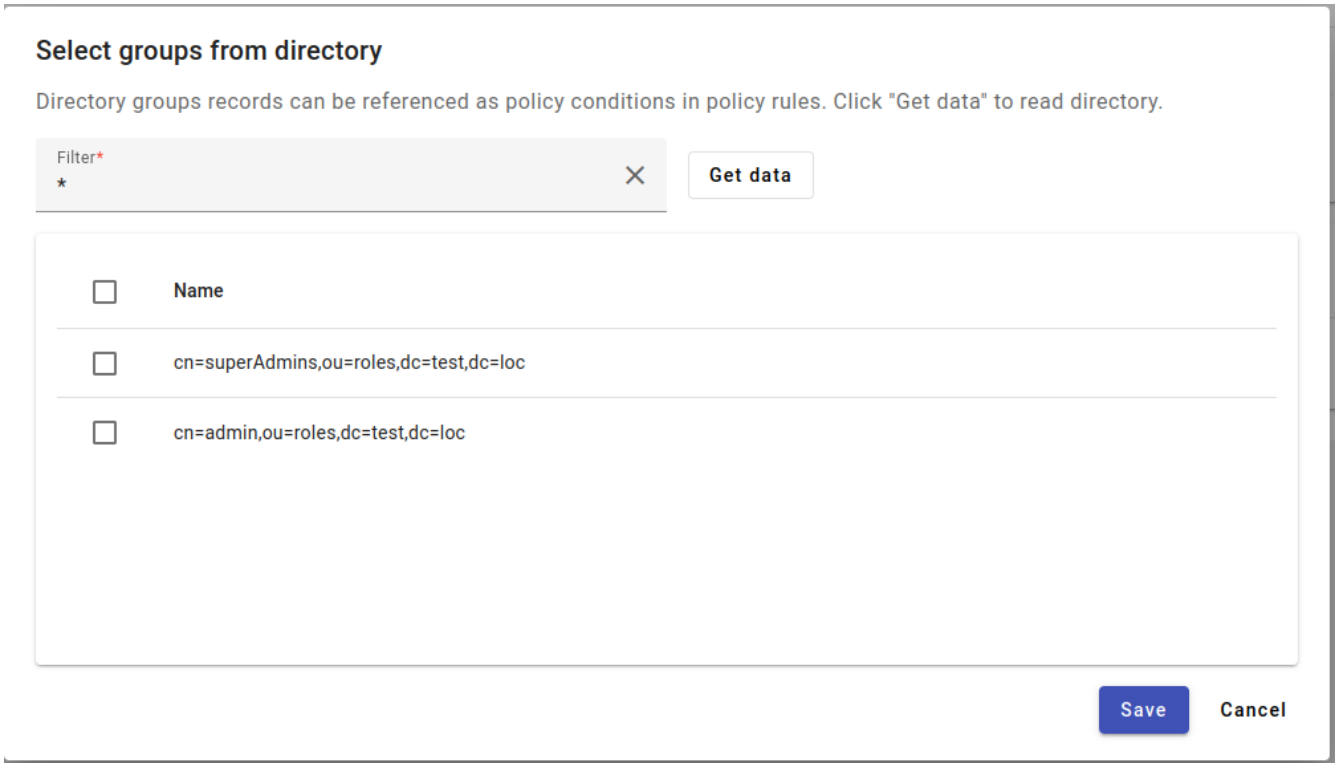

Figure 96. Group selection window after receiving data

You need to select the required groups using the ☐ checkbox on the left and click the **Save** button.

Previously saved groups that were not reselected in the search list will be deleted when resaving other selected groups!

Adding attributes

To be able to authenticate via an external identity source, adding attributes is optional. Attributes can be used in policies and user authorization profiles.

After adding groups, you can click the **Next** button at the bottom right of the screen. You can also make the transition by clicking on the inscription **(3) Attributes**, the page will open:

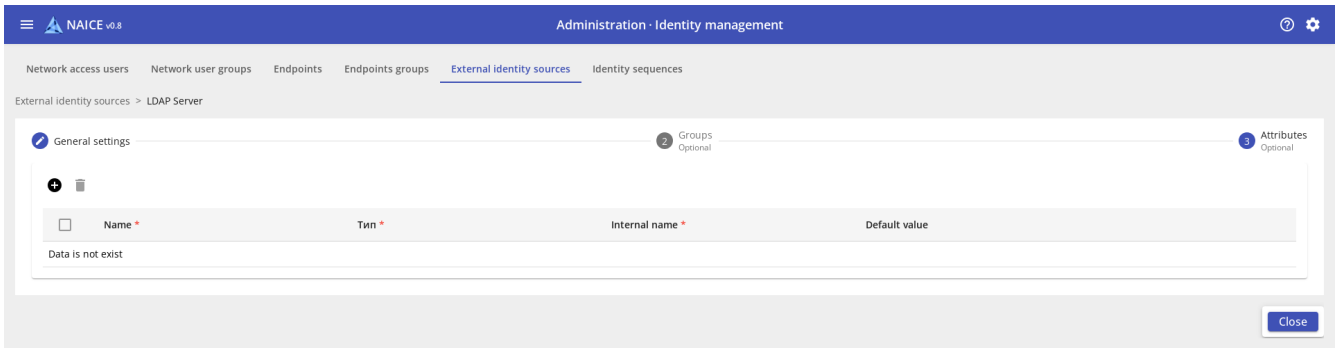

Figure 97. Adding attributes

Controls:

- ⊕ - add attributes.
- 🗑 - delete the attributes selected by the checkbox (inactive until at least one attribute is selected).

After clicking on the button ⊕ a menu will open:

- `Add new attribute` - create an arbitrary new attribute.
- `Select attribute from directory service` - add an attribute from the identification source.

Add new attribute

Figure 98. Add new attribute

The line that appears to add an attribute contains the following parameters:

- `Name` * - arbitrary attribute name that will be displayed in the dictionary.
- `Type` * - attribute type. Possible values:
  - `INTEGER` - numeric,
  - `IP_4_ADDR` - IPv4 address,
  - `STRING` - string (default).
- `Internal name` * - attribute name from the identification source.
- `Default value` - the attribute value that will be used if it is not obtained from Active Directory..

Parameters marked with an asterisk * are required.

After filling in the required parameters, the save button will become active. You need to click it to add an attribute.

Select attribute from directory service

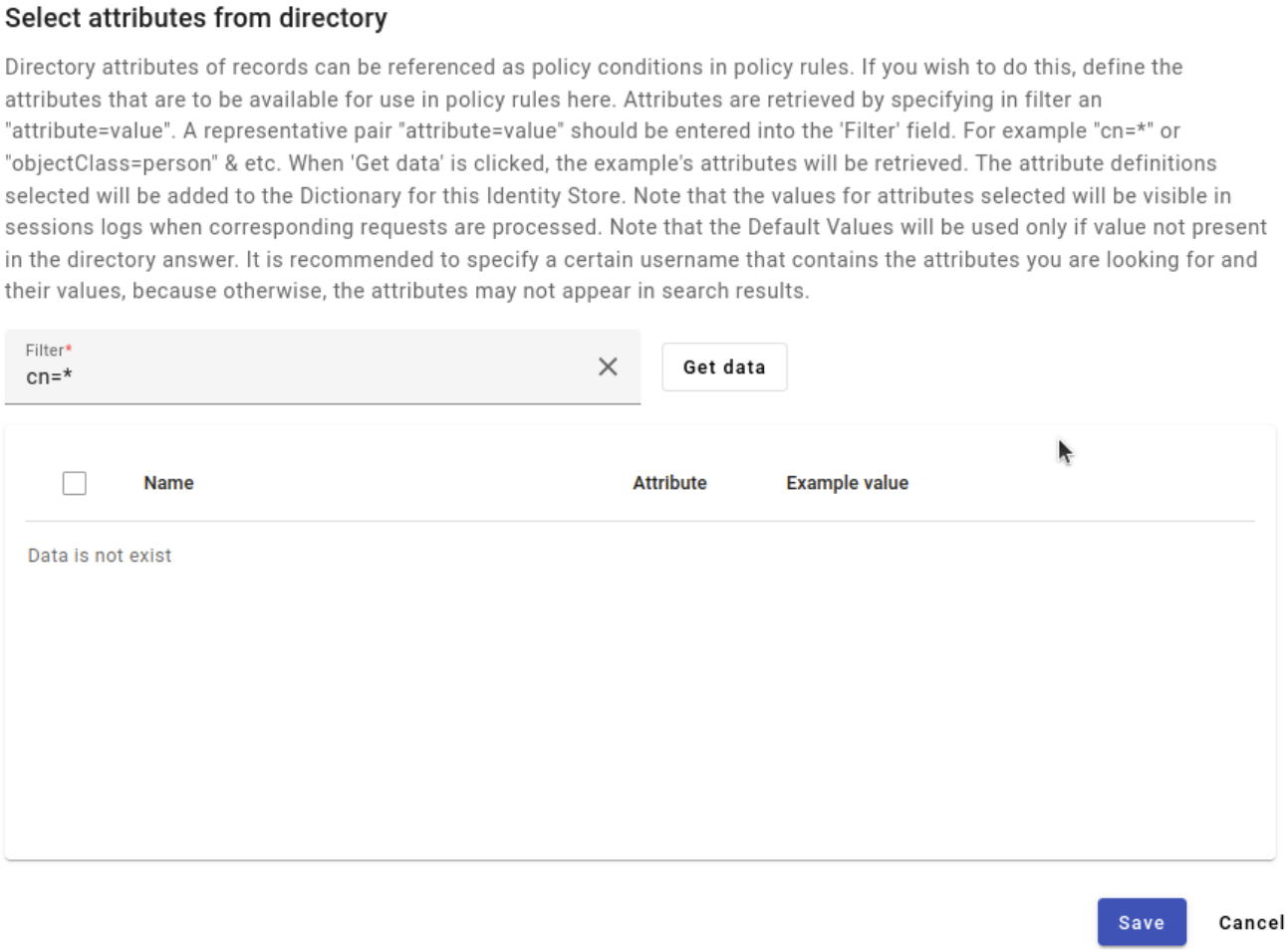

Figure 99. Selecting attributes from a directory service

This window presents the following parameters:

- `Filter` * - filter for searching attributes, default `cn=*`. You can use the expression `<Attribute>=<value>` as a filter; if the value is not important, you must specify `*`. If an attribute has multiple values, only the first one found is displayed. When performing an LDAP search, you can typically specify `uid=*` or `givenName=*`.
- `Get data` - get data taking into account the filter.

After receiving attribute data:

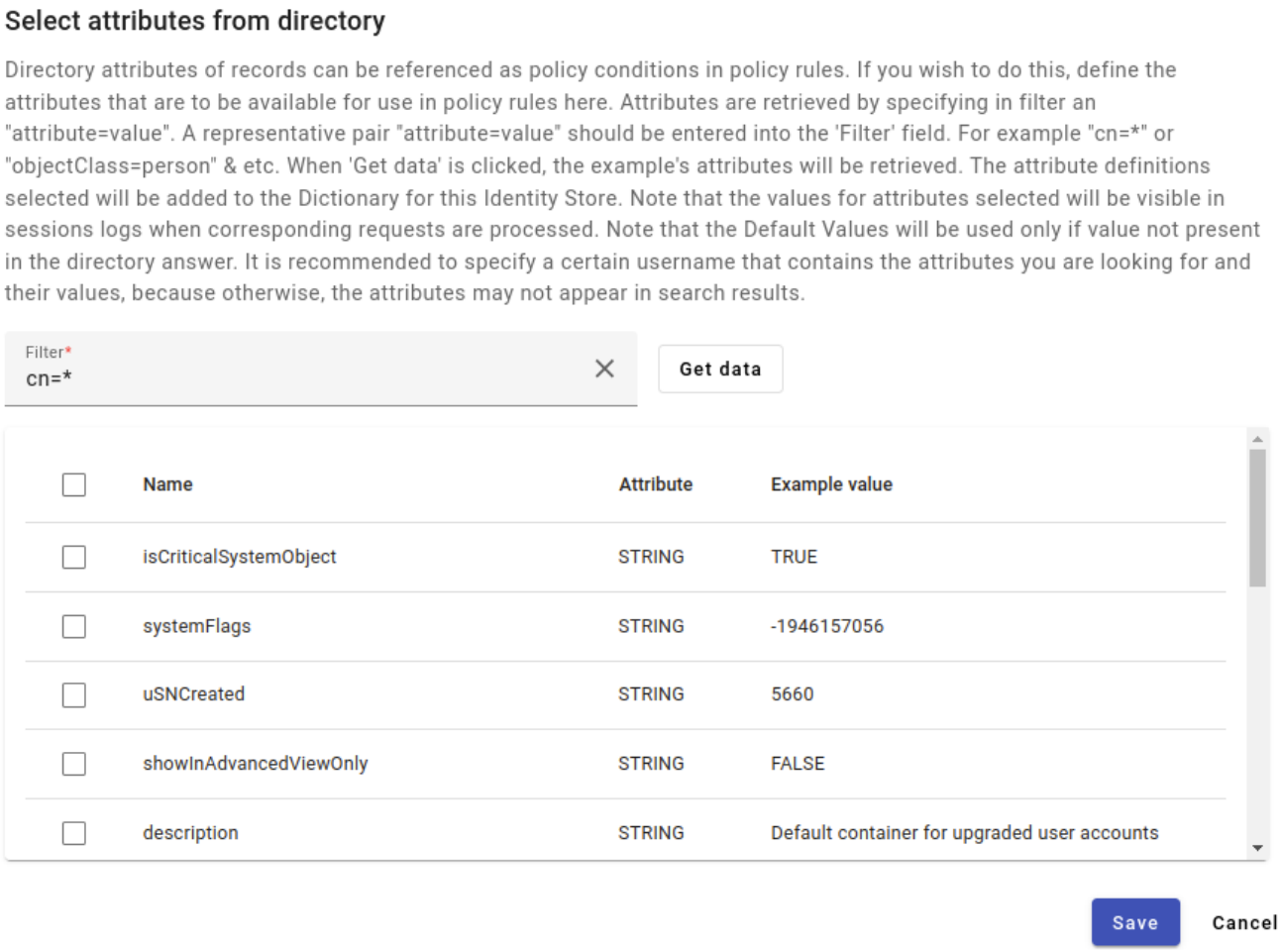

Figure 100. Attribute selection window after receiving data

You need to select the required attributes using the checkbox on the left and click the **Save** button.

Previously saved attributes that were not reselected in the search list will be deleted when resaving other selected attributes!

Implementation restrictions

There are the following limitations to implementing interaction with LDAP:

- The user's password must be stored in ClearText.
- Only Latin characters, numbers, and punctuation marks are allowed in usernames and passwords.

Editing Identity Source

To edit a previously added identification source, on the viewing page, click on the name of the source in the table.

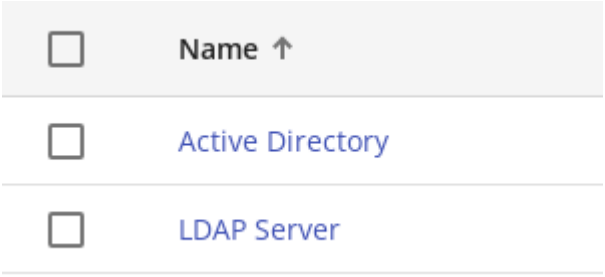

Figure 101. Column name

The editing page will open:

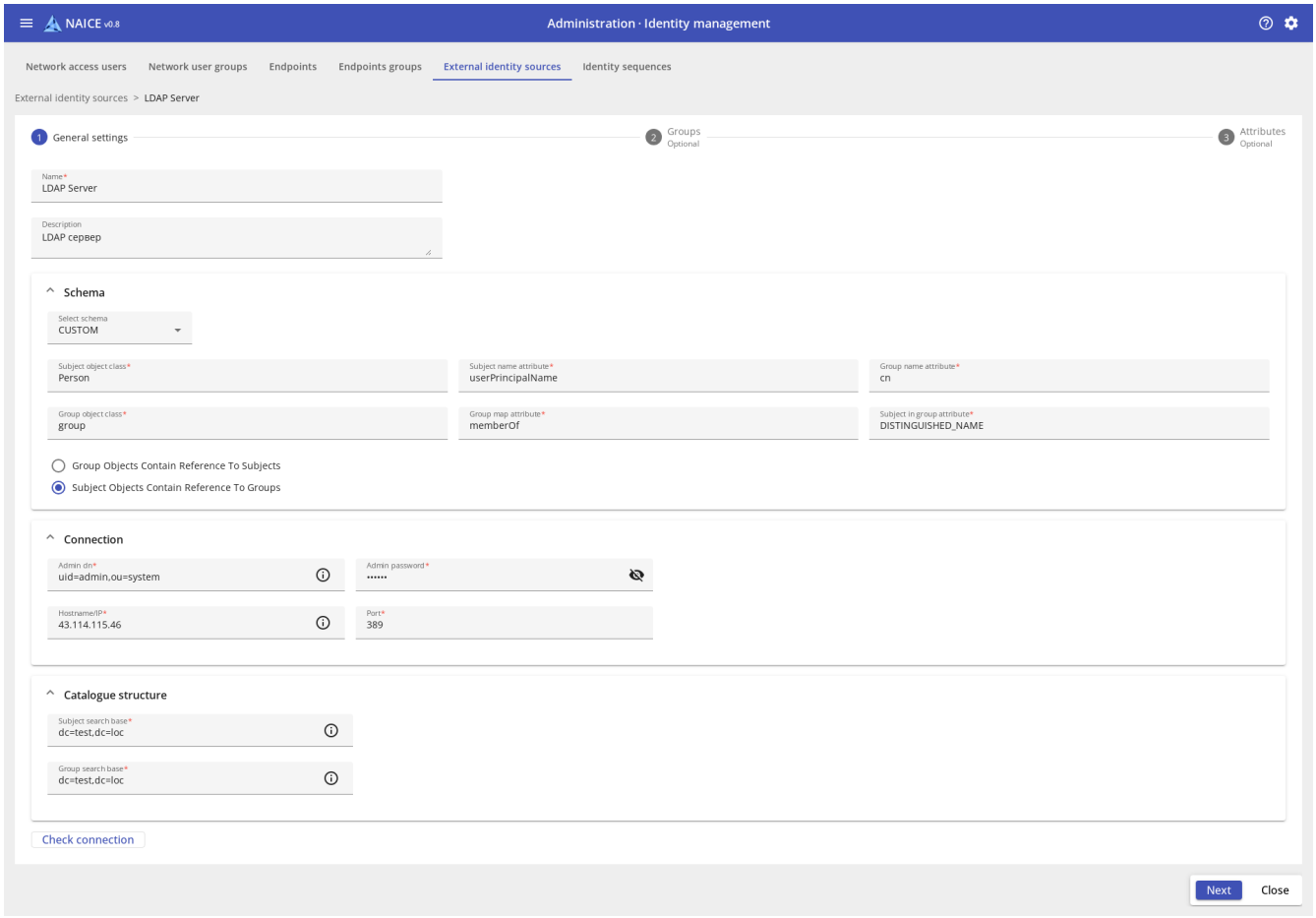

Figure 102. Source editing page

After editing, click on the **Save** button. The button will be inactive until at least one field is changed.

Removing an identity source

To delete one or more identification sources, you need to select the required sources on the viewing page using the checkbox ☐ and click on 🗑 in the upper right corner above the table.

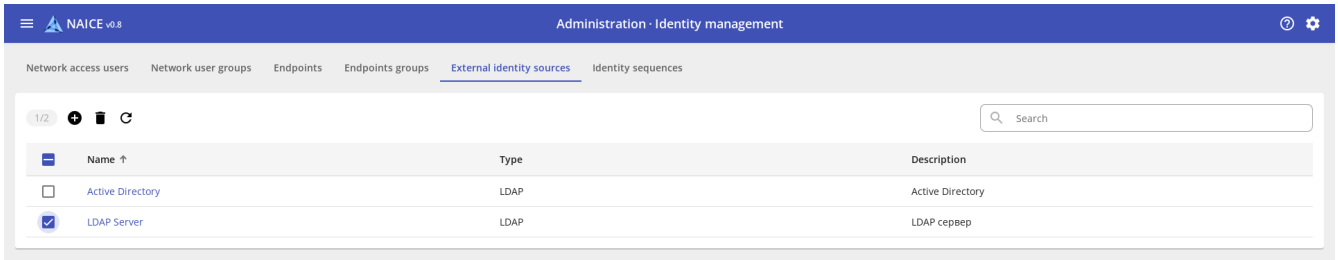

Figure 103. Selecting sources to delete

Deletion requires confirmation of the action, for which a modal dialog will open. After explicit confirmation, the selected items will be deleted.

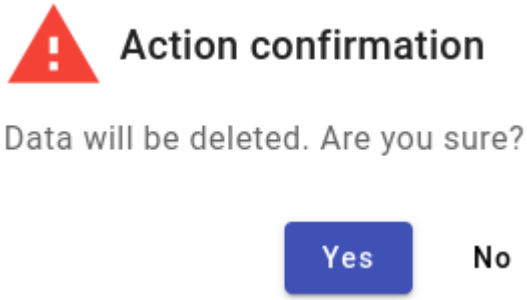

Figure 104. Modal dialog for confirmation

Identity sequences

Description

Identity sequences (identity source chains) are used in authentication policies when configuring policy sets. They determine which sources and in what order to look for users during authentication. Supported user sources include internal user database and external identity sources, such as MS AD and OpenLDAP.

View identity sequences

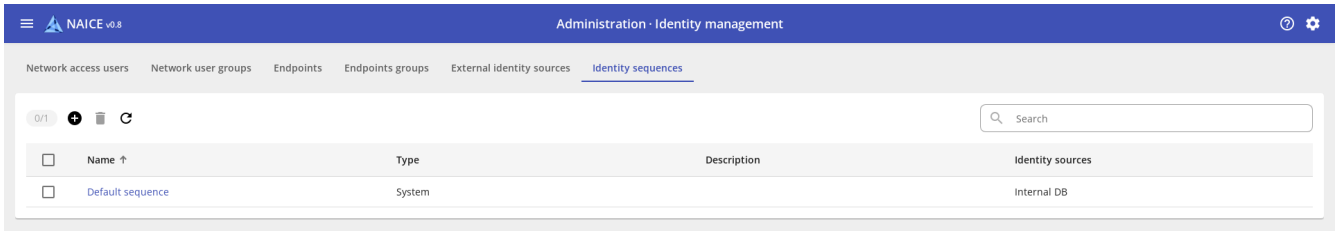

Figure 105. View identification sequences

This page contains a table listing all identity sources.

The table contains columns:

- `Name` - the name of the sequence.
- `Type` - type of the identification chain. The possible value is "Created by admin" or "System".
- `Description` - arbitrary description of the sequence.
- `Identity sources` - a list of user credential sources that are configured in this sequence.

It is possible to sort in forward and reverse order by the columns `Name` and `Description`. By default, sorting is performed in direct (alphabetical) order by the `Name` field.

Controls:

- `Search` - Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.
- - Refresh table data.
- `0/1` - Counter of elements selected by the checkbox / total number of elements.
- - Add a new element.
- - Delete selected elements (inactive until at least one element is selected).

↑ - Change the current sort order.

- ☐ - Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).

Identity sequences "[Default sequence]" are system, so you can't rename or remove them

Adding an identity sequence

To add an identity sequence ⊕ on the left side of the field above the table of the view page, the following page will open:

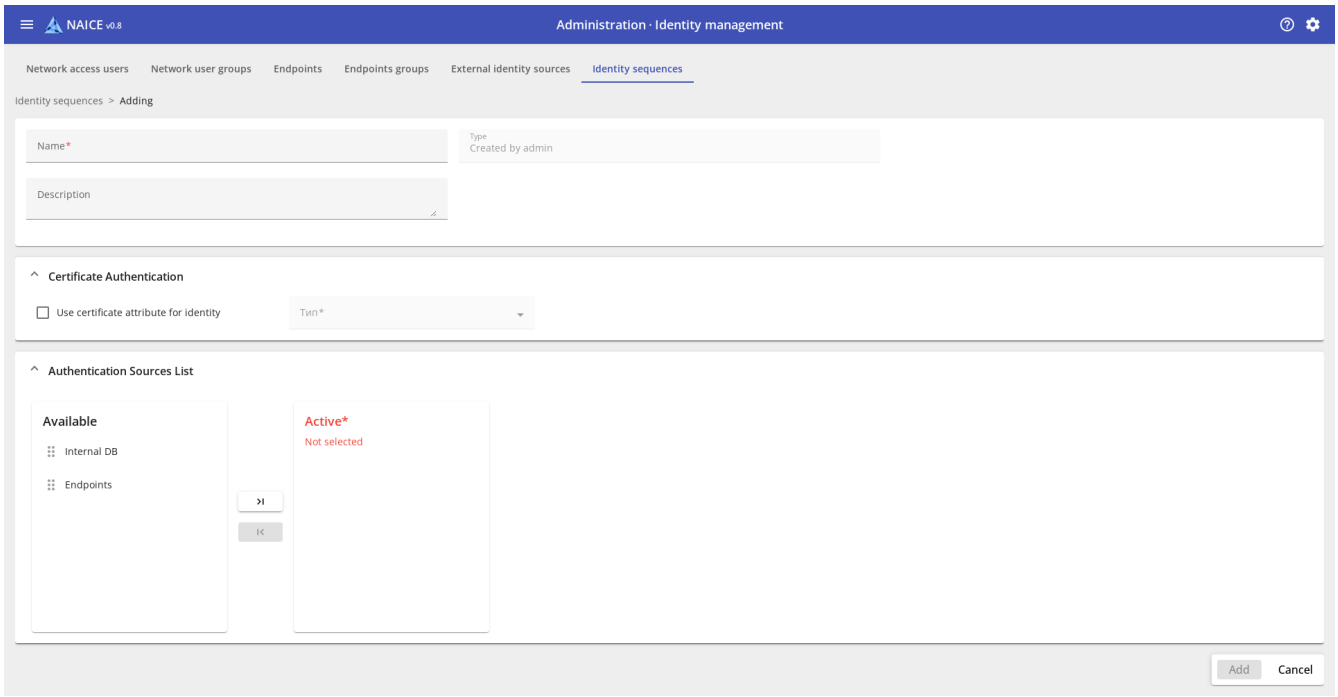

Figure 106. Add sequence page

The following parameters are available for filling:

- `Name` * - name of the sequence. Maximum length is 100 characters.
- `Type` - type of the identification chain. All manually created identification chains are set to "Created by an administrator" and cannot be changed.
- `Description` - arbitrary description of the sequence. Maximum length is 200 characters.

Parameters marked with an asterisk * are required.

Certificate Authentication

This setting can only be used when authenticating a user using the EAP-TLS protocol.

In this section, the validation of a selected certificate field against an identification source attribute is configured. The chosen attribute value from the user's certificate is compared with the attribute specified in the "Subject Name Attribute" field within the external identification source.When using an internal

identification source (Internal DB), the comparison is made with the value specified in the user's "Login" field.

`Use certificate attribute for identity` - enables the option to select an attribute to be used as the username for authentication. If this setting is disabled, the User-Name attribute from the RADIUS authentication request will be used instead.

After enabling the setting, the `Attribute` field will become available.

- `Attribute` - a field in the certificate containing data for user identification.

The field can take the following values:

- `Subject - Common Name`
- `Subject - Serial Number`
- `Subject`
- `Subject Alternative Name - Email`
- `Subject Alternative Name - DNS`
- `Subject Alternative Name - UPN`

Authentication Sources List

In this section, you select the authentication sources to be used.

- `Available` - list of all sources available for selection.
- `Active` - list of sources that will be applied for authentication.

To select a user credential source, grab it by the image field ⠿ and drag it from the "Available" column on the left to the "Active" column on the right.

Controls:

- ⏭ - select all available authentication sources.
- ⏮ - delete all selected authentication sources.

A search for a user by login is performed in all available sources specified in Active. The search is performed from top to bottom in the list. The search ends as soon as a matching user login is found in the source.

Editing the identity sequence

To edit, click on the name of the identification sequence in the table.

Figure 107. Column Title

The editing page will open.

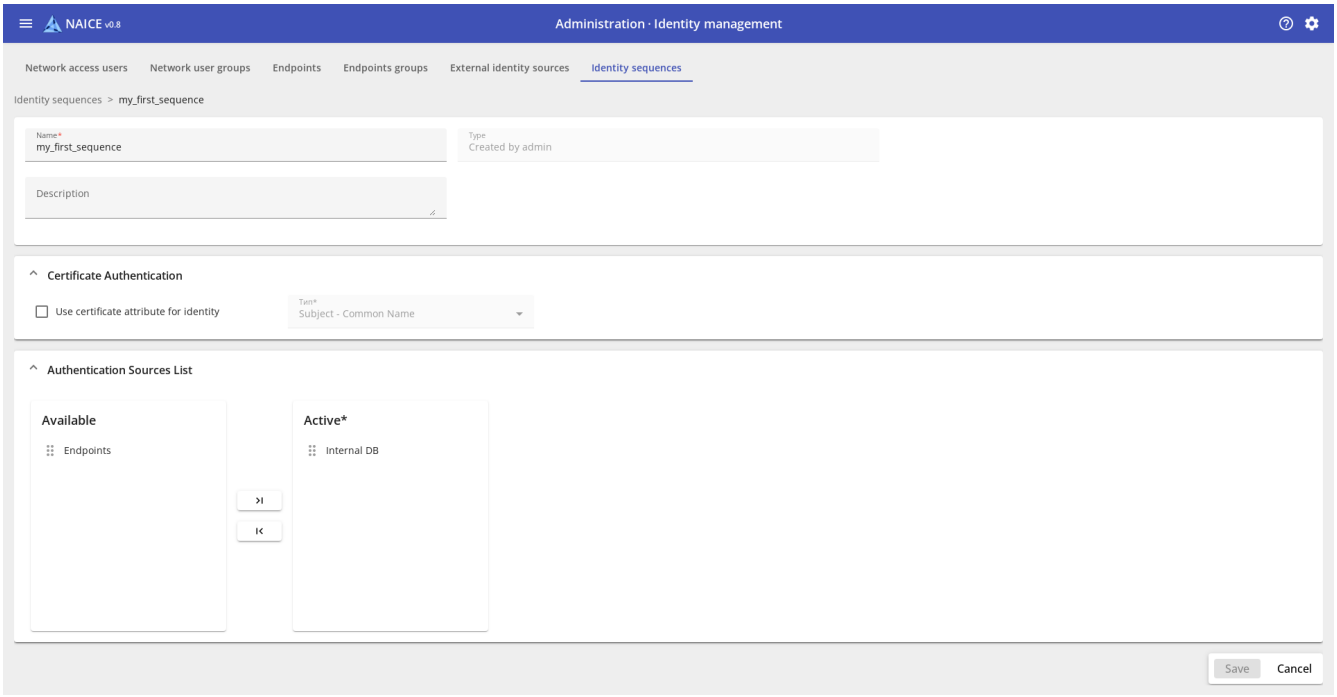

Figure 108. sequence editing panel

After editing, click **Save**. The button will be inactive until at least one change is made.

Deleting an identity sequence

To delete one or more identification sequences, you need to select them through the checkbox ☐ and in the upper left corner above the table click on 🗑 .

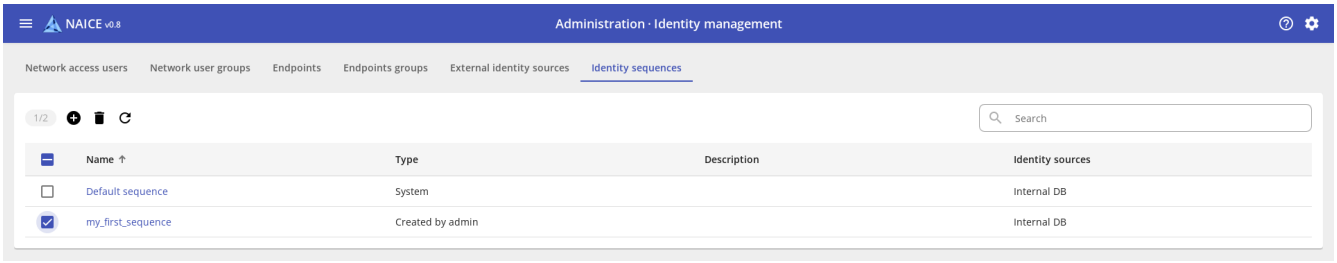

Figure 109. Selecting sequences to delete

Deletion requires confirmation of the action, for which a modal dialog will open. After explicit confirmation, the selected items will be deleted.

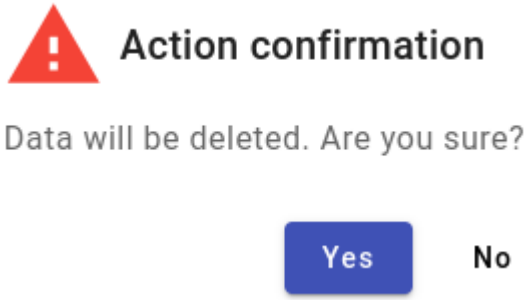

Figure 110. Modal dialog for confirmation

You will not be able to delete a sequence that is used in the authentication policies of any policy set.
To delete a sequence, you must first remove it from the authentication policy, and then delete the sequence itself.

Network devices control

This section contains information about functionality that is available as part of the separate NAICE-TACACS license option. To purchase this functionality, please contact your manager or email eltex@eltex-co.ru.

The Network Device Control section contains entities for configuring access to network devices using the TACACS+ protocol.

TACACS+ is an evolution of the TACACS (Terminal Access Controller Access Control System) protocol and is designed for centralized authentication and authorization of network device administrators. The protocol allows for the authorization of each command executed on a network device, as well as sending records of executed commands (accounting). NAICE can be a TACACS+ authorization server.

This section includes the following pages:

- Conditions – managing conditions used in network device policies to determine whether a current connection matches one of the policies;
- TACACS Command sets – managing command sets that define allowed and restricted commands for administrators to execute on devices.
- TACACS Profiles – managing TACACS profiles, which define privilege levels and other additional attributes for authorized users.
- Network devices policies – managing network device policies, which are the core element of access control and define the logic for processing and responding to TACACS authentication and authorization requests.

Policy elements

Conditions

Description

Logical conditions are the main element of authentication and authorization policies, which are responsible for generating criteria that allow determining whether a user can pass authentication and what actions should be applied to him when authorizing.

The algebra of logic is the basis for creating and processing a logical condition. The result of the condition is "True" or "False". The result may be inverted. The condition can be simple or complex. In a simple condition, only one attribute acts as a verification criterion. In a complex condition, you can use several different attributes, combining them with the "AND"/"OR" logical operations.

This section is similar to Access policy - Elements - Conditions, but only attributes that can be used in :policy-sets/index.html are available for creating conditions.

View a list of logical conditions

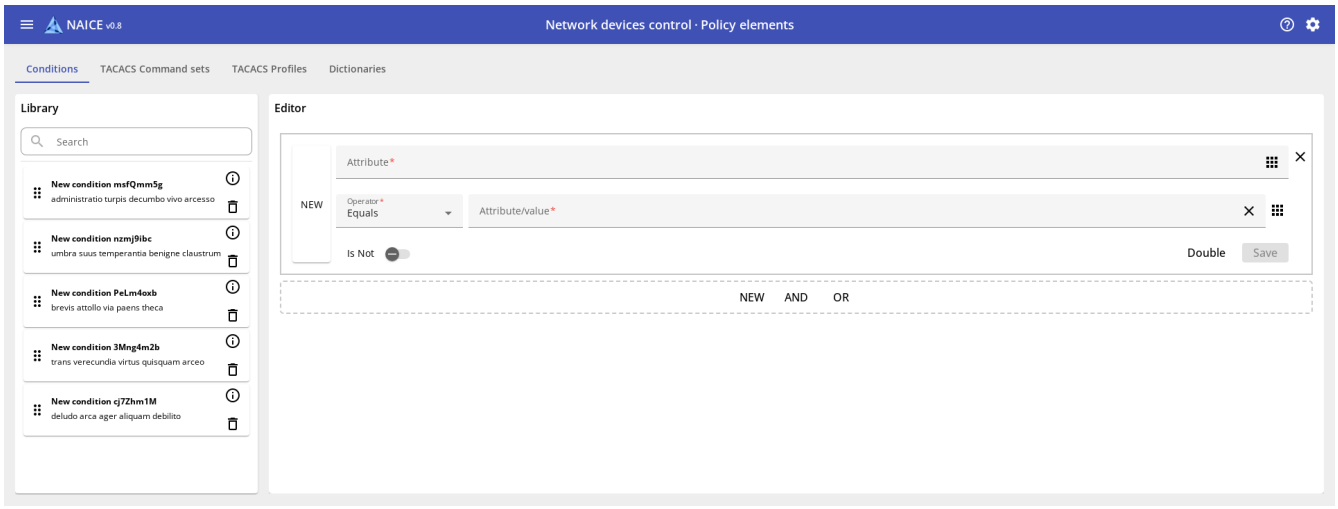

Figure 111. Library of logical conditions

On the left is a **Library** of logical conditions.

On the right is the logical condition **Editor**:

- `Attribute` * - attribute of a logical condition.
- `Operator` * - the selected logical condition operator. Can take values (depending on the attribute value type):
  - "More or equal" / "Less or equal"
  - "More than" / "Less than"
  - "Equals" / "Not equal"
  - "Equal to NULL" / "Not equal to NULL"
  - "Starts with" / "Doesn't start with"
  - "Ends with" / "Does not end with"
  - "Contains" / "Does not contain"
  - "Match" (*full* string match, case sensitive)
- `Attribute/value` * - attribute/value that is used to match the logical condition attribute in accordance with the selected operator. For an attribute that assumes predefined values, the value is selected from the list.
- `Is Not` - choice of inverting the result of the condition (by default the condition is "Complied", when the setting is enabled, the condition will be considered "Not Complied")
- `NEW` - adding a new logical condition to the existing hierarchy at the same level as the current one.
- `AND` - adding a new logical condition as a "child" for an existing one with the logical operator "AND".
- `OR` - adding a new logical condition as a "child" for an existing one with the logical operator "OR".

* - required fields.

Controls:

- `"Search"` - Performs case-insensitive filtering based on the library of logical conditions.
- - Preview the contents of the logical condition.
- - Deleting a logical condition.
- - Open the dictionary to add an element.
- - Remove an element from the editor. Action depends on location:
  - clicking to the right of the "Attribute" field will clear the corresponding field;
  - clicking to the right of the Attribute/Value field will clear the corresponding field;
  - clicking to the right of a logical condition will remove that condition.
- `"Save"` - Save the corresponding logical condition.

Attribute selection menu

To select an attribute to be used in the condition, click - the attribute selection menu will open.

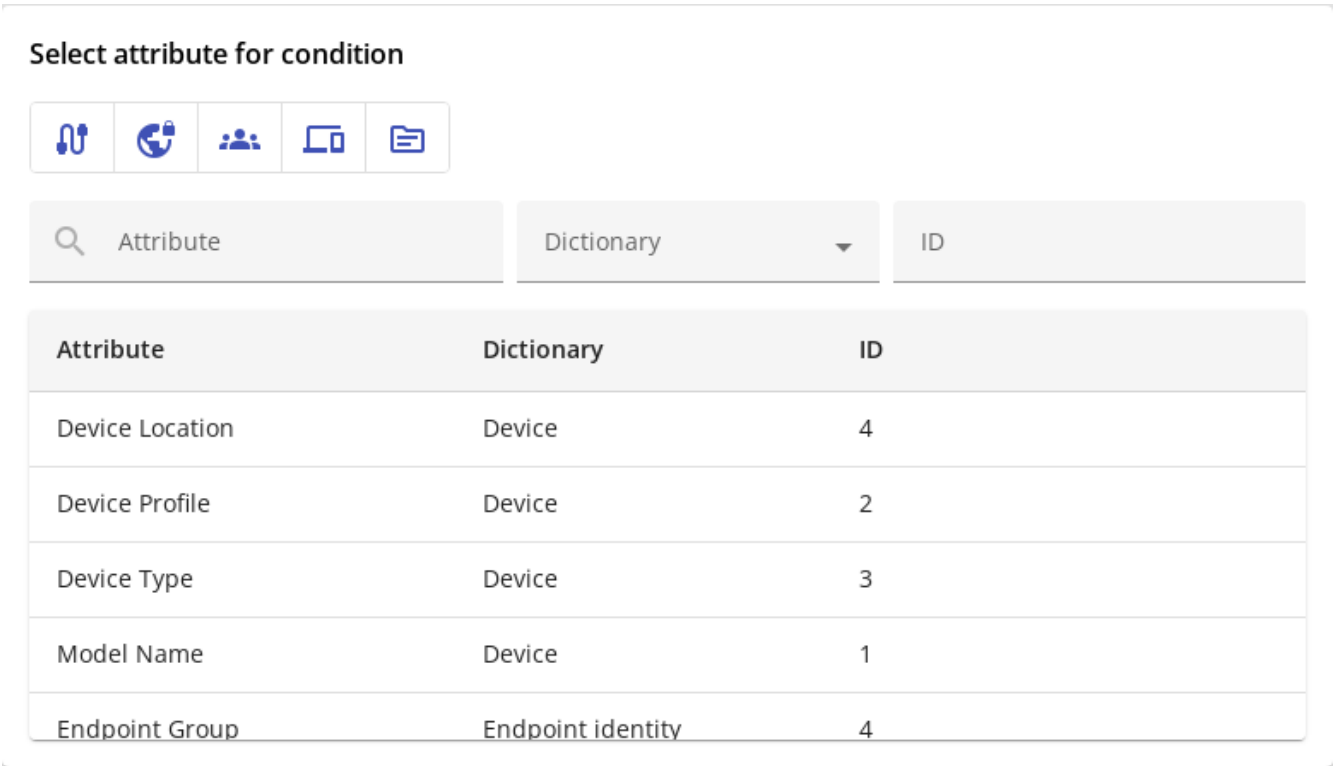

Figure 112. Attribute selection menu

At the top there is a list that allows you to filter by dictionary type. Only one type can be selected.

Types of dictionaries:

- `DEVICE` - device attributes.
- `IDENTITY` - users and endpoints attributes.
- `LDAP` - attributes of external identity sources.

- `NETWORK_ACCESS` - contains the IP-address of the device that the administrator uses to connect.
- `TACACS_PLUS` - TACACS+ attributes dictionary.

Below are attribute filtering columns.

- "Attribute" - case-insensitive filtering by attribute name.
- "Dictionary" - menu for selecting a dictionary. A dictionary type must be selected to use it.
- "ID" - filtering by attribute number.

Creating logical conditions

Creating a simple logical condition

You can create logical conditions at **Editor**.

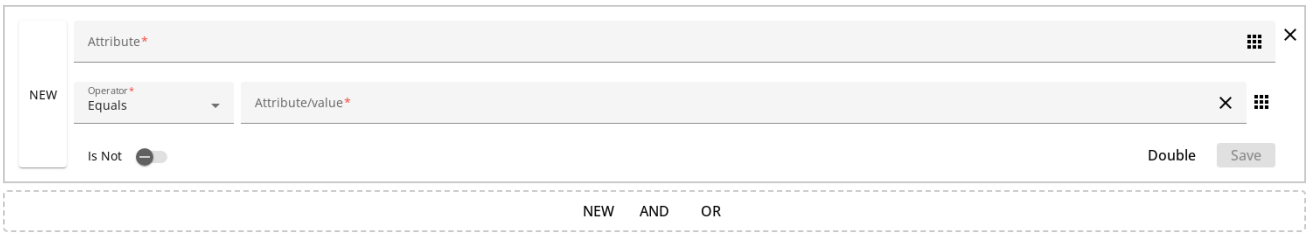

Figure 113. Initial state of Editor

After clicking on in the right side of the “Attribute” field, the dictionary will open.

To find the required attribute, you can use filtering by attribute name. Or select the type of dictionary and select the required dictionary by scrolling the drop-down list to determine the required attribute.

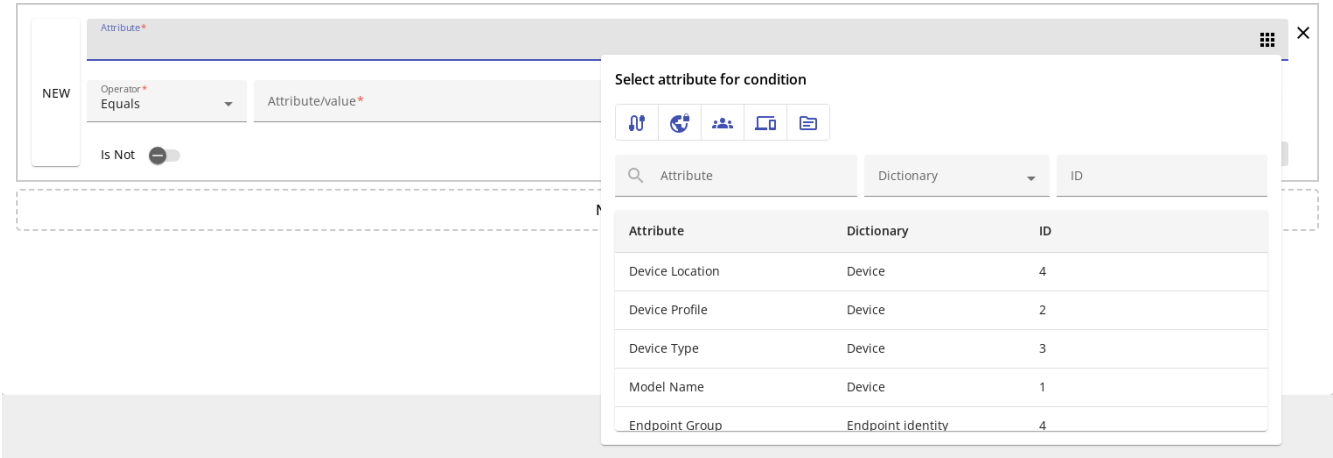

Figure 114. Attribute selection

After selecting an attribute, click on it, and it will be placed in the “Attribute” field.

Select the operator (by default, “Equal” is substituted). The operator selection list depends on the type of data that can be used in the value of the selected attribute.

Attribute data type	Supported operators
String	Matches, Ends with, Does not end with, Starts with, Does not begin with, Contains, Does not contain, Equal to, Not equal to, Equal to NULL, Not equal to NULL
Number	Greater than or equal to, Greater than, Less than or equal to, Less than, Equal to, Not equal to, Equal to NULL, Not equal to NULL
IPv4 address	Equal to, Not equal to, Equal to NULL, Not equal to NULL
MAC address	Equal to, Not equal to, Equal to NULL, Not equal to NULL, Starts with, Does not start with, Ends with, Does not end with, Contains, Does not contain,
Name	Equal to, Not equal to, Equal to NULL, Not equal to NULL
Byte sequence	Equal to NULL, Not equal to NULL

Select an attribute in the Attribute/value field or enter its value.

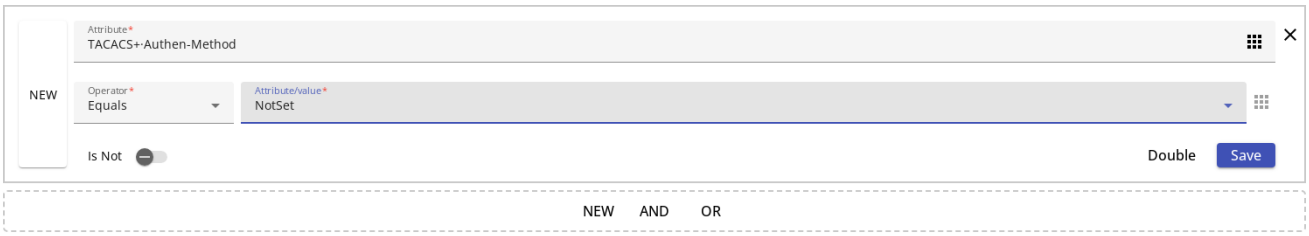

Figure 115. A condition in which all parameters are filled in

Then click the “Save” button. You can replace an existing condition in the library or save a new one.

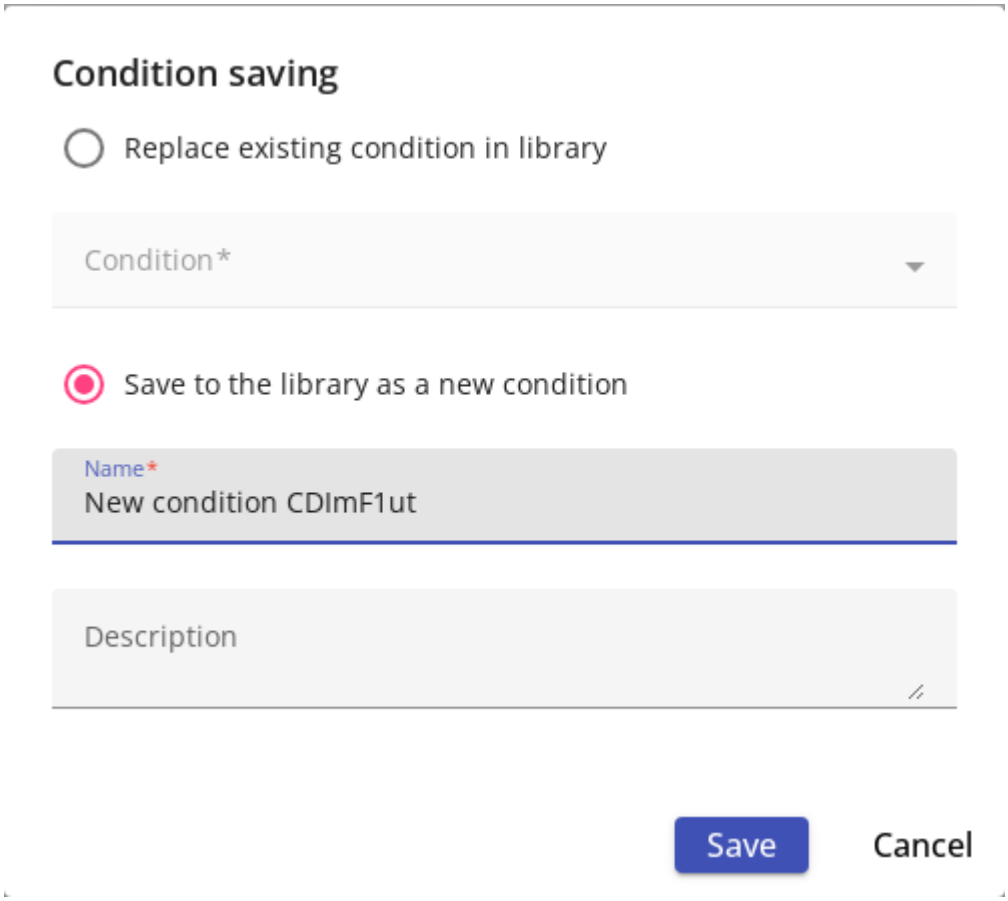

Figure 116. Condition saving modal dialog

By default, the action assumes saving the new condition:

- "Name" * - name of the condition. Maximum length is 100 characters.
- "Description" - arbitrary description. Maximum length is 200 characters.

* - required fields.

Then click the “Save” button.

Save and replace an existing condition in the library. To do this, select "Replace an existing condition in the library" and select a condition from the drop-down list. If necessary, you can filter by name by entering the appropriate text in the field in front of the list.

Then click the “Save” button.

The "Save" button is always active to be able to save an existing condition under a different name.

Creating a complex logical condition

To create a complex logical condition, use the panel under the logical condition.

Figure 117. Panel to create an additional logical condition

- "New" - add a logical condition at the same level as the existing one.

"AND" - add a child condition with logical "AND".

- "OR" - add a child condition with a logical "OR".

When you click "New", an additional rule will appear in the editor on the same level as the existing one, combined with a logical "AND".

Figure 118. Condition consisting of two conditions combined by a logical "AND"

- Logical "AND" combining rules can be changed to "OR".
- It is possible to save each condition separately using the “Save” button in its window or all together using the “Save” button at the bottom.
- To delete a condition, click on ✕ at the top right in the condition window.
- To completely clear all conditions in the editor, click ✕ at the top right of the editor, located behind the windows of individual conditions.

When you press "AND"/"OR", a new window will appear in which a new menu will be available, then you can add conditions at a new level or create child conditions. There is no restriction on the nesting of conditions.

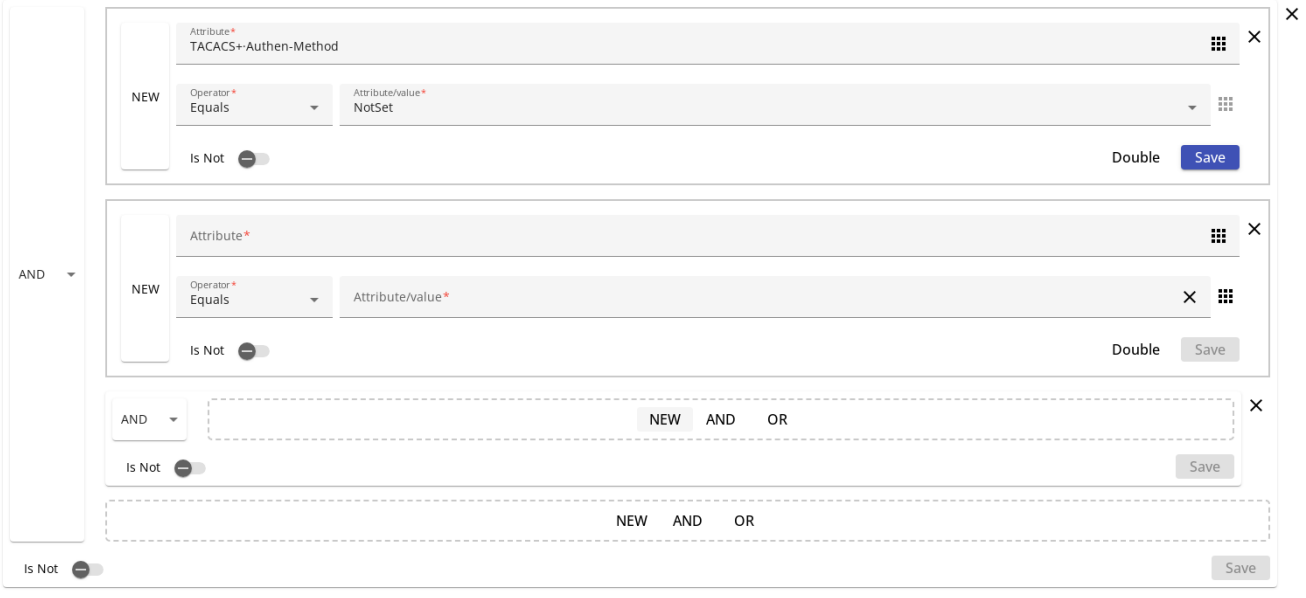

Figure 119. Condition containing nested rules

To save all conditions, click the "Save" button in the lower right corner.

Editing a logical condition

To edit a logical condition, you need to grab it with the cursor in the library and move it to the editor field.

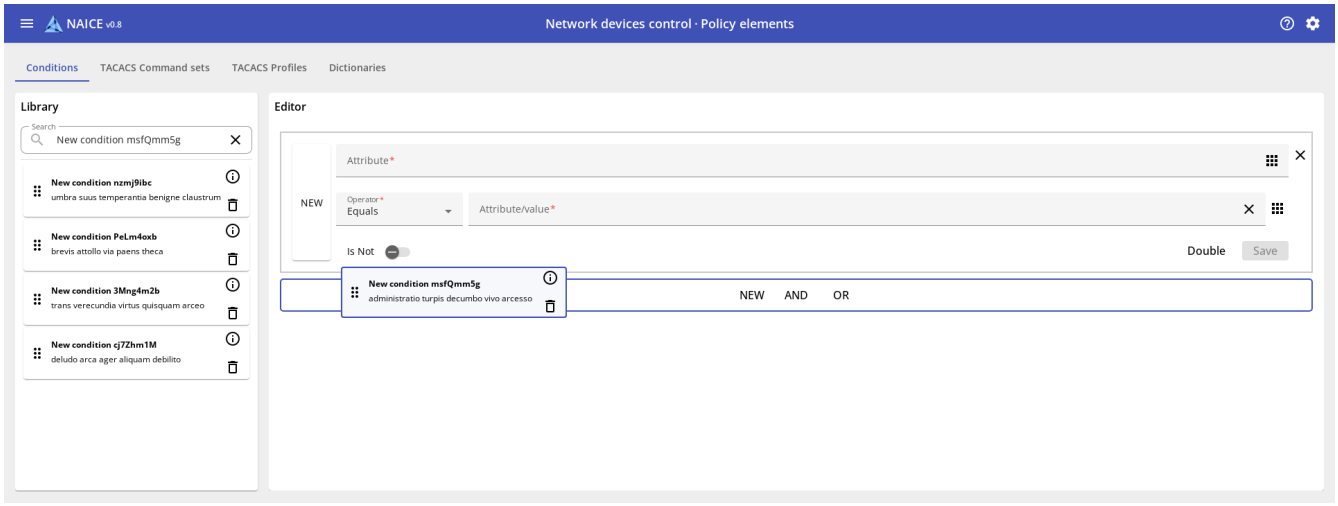

Figure 120. Selecting a logical condition

Figure 121. Editing a logical condition

To edit the condition, click the "Edit" button. After editing, click the "Save" button. Since the condition was previously saved in the library, by default it will be proposed to save it with the same name. If necessary, you can select another condition to be overwritten or select "Save to library as new condition." Click the "Save" button.

Also, during editing, you can drag conditions from the library into the child condition editor field.

Delete a logical condition

To delete a logical condition you need to find it in the library and click the button at the right of the condition name.

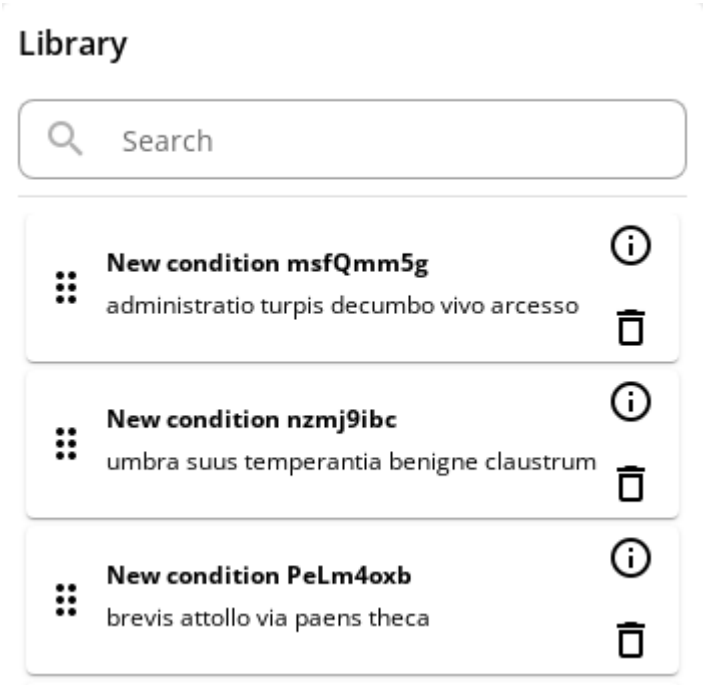

Figure 122. Selecting a condition to delete

Deletion requires confirmation of the action, for which a modal dialog will open. After explicit confirmation, the selected items will be deleted.

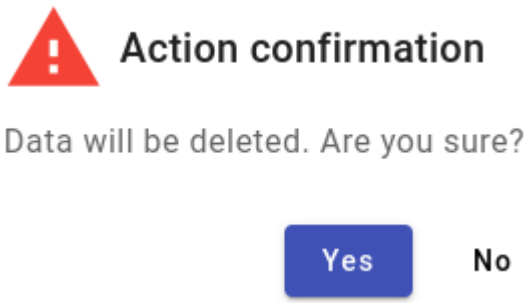

Figure 123. Modal dialog for confirmation

Restrictions:

- some system logical conditions cannot be deleted;
- you cannot delete logical conditions that are used in other complex logical conditions;
- You cannot delete logical conditions that are used in any set of policies.

TACACS Command sets

Description

TACACS command sets are used to define a list of commands that are allowed or denied to be executed on a device when using command authorization on a TACACS server. These command sets are further used in Network Device Policies when configuring the authorization policy.

Viewing TACACS Command Sets

This page contains a table listing all TACACS command sets.

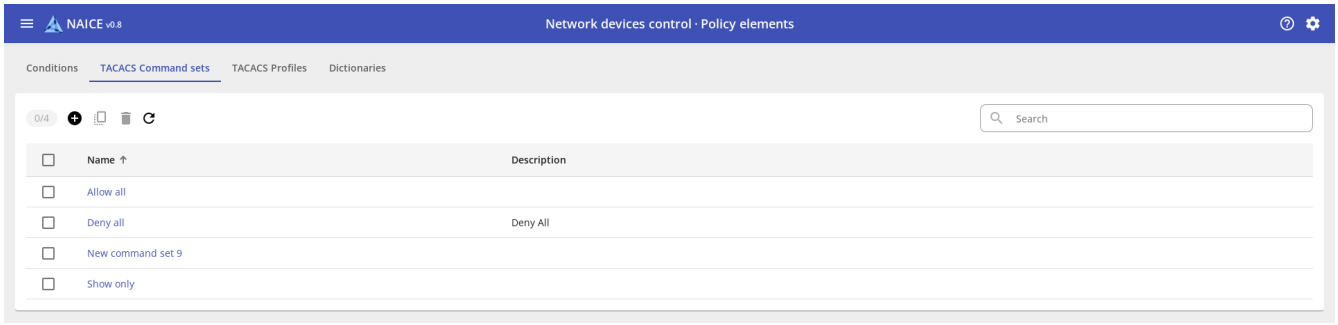

Figure 124. Table with a list of TACACS command sets on the view page

The table contains columns:

- `Name` - the name of the command set.
- `Description` - arbitrary description.

Sorting is possible only by the field `Name` in the forward and reverse order. By default, sorting is performed in the forward (alphabetical) order.

Controls:

- `Search` - Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.
- - Refresh table data.
- `0/1` - Counter of elements selected by the checkbox / total number of elements.
- - Add a new element.
- - Delete selected elements (inactive until at least one element is selected).
- - Change the current sort order.
- - Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).
- - Duplicate the command set selected by the checkbox.

Adding a new command set

To add a command set, click on the top left above the table.

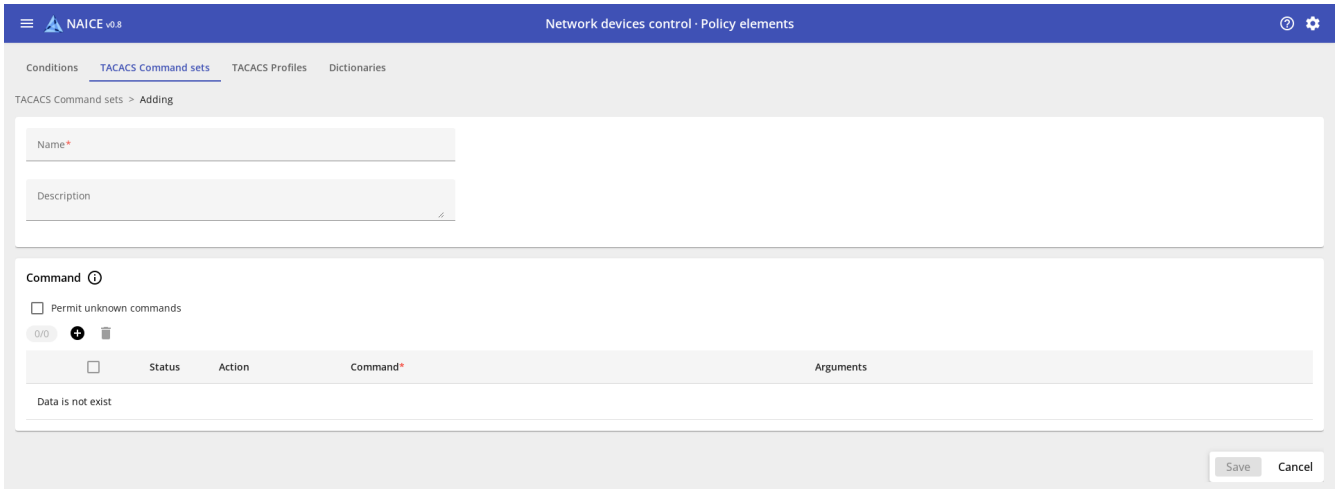

Figure 125. Form for adding a command set

The page that opens presents the following parameters:

- `Name` * - the name of the profiling condition. The maximum length is 100 characters.
- `Description` - arbitrary description of the profiling condition. Maximum length - 200 symbols.

Parameters marked with * are mandatory.

Command - a settings block for defining the commands allowed and denied for authorization. For the comfort configuration the commands are defined in the table, which contains the following columns:

- ⠿ - contains buttons, by dragging which you can change the order of rows in the table.

> ⚠ The command order is important because the matching of the authorization command with the commands in the table is going on **top-down to the first match**.

- ☐ - contains checkboxes to select items for further actions (e.g. delete 🗑).
- `Status` - can take the values ✓ (Enabled) or ⊗ (Disabled). Disabled commands do not participate iin the process of checking the authorized command. Disabling a command instead of deleting can be useful for debugging.
- `Action` - what action to perform when the comparing commands: allow or deny authorization of the command.
- `Command` * - the command for which authorization needs to be allowed or denied. Regular expressions can be used when specifying a command, see [Use of regular expressions in command sets].
- `Arguments` - allowed or denied arguments for the specified command. If no arguments are specified, then any arguments for the command fall under the `Action` specified in the rule. Regular expressions may be used when specifying arguments, see [Use of Regular Expressions in Command Sets].

Only commands containing **exactly** those attributes specified in the attribute row are allowed/denied. If a command attribute is followed by another attribute that is not specified in the command set, then such a command is considered to be unmatched and will be processed accordingly.

*Example. The authorized command is `show running-config interface GigabitEthernet0/1`.

The command set is:

Action	Command	Arguments
Allowed	show	running-config

In this case, the command being authorized **does not match** the specified rules and authorization will be **denied** according to the default behavior.

To allow any arguments after the specified arguments, you can use the `.*` regular expression (any character is expected any time) or any other suitable expression:

Action	Command	Arguments
Allowed	show	running-config .*

By default, any commands that are not listed are disallowed. This behavior can be changed with the setting ☐ `Permit unknown commands`.

To add a new command to the table, the ⊕ button is used. The command will be added to the top of the table (i.e. the new command will be the highest-priority if its order is not changed using ⠿).

To save the created command set, you should click **Save**, or cancel the creation with **Cancel**.

Editing a command set

To edit a TACACS Command Set, click on its name on the list page.

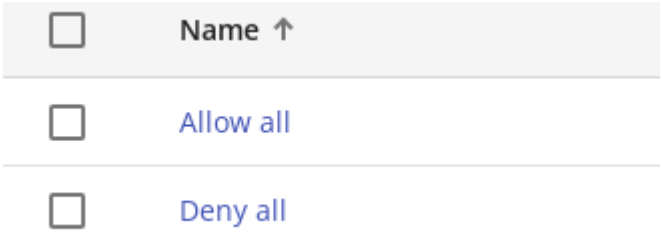

Figure 126. Hyperlink to the command set editing page

This will open the edit page.

The command set editing form is similar to the creation form, except for a few handy features that allow you to edit the command set table without leaving the page via the save button:

- ↻ - reset changes
-

`Apply` - save changes in the command table without leaving the editing page. Can be useful for debugging.

After editing, click on the **Save** button. The button stays disabled until at least one field has been changed.

Using regular expressions in command sets

When specifying a command or its arguments in a command set, regular expressions can be used. This allows you to specify a "pattern" that can be matched by multiple commands with just one line.

Example 1. Using regular expressions when specifying a command

Task: RADIUS server settings must be allowed to be configured on the device, with 2 commands possible on the device - `radius` to configure the server on the device and `radius-server` to configure an external server. Both commands must be allowed to the administrator.

Possible solutions:
To avoid specifying both commands in full form, you can use the regular expression: `radius.*`.
The symbol `.` here means any character, and `\*` means its repetition in the expression any number of times (including 0 times).

You can also make a stricter regular expression: `radius-?\w*`.
The `-?` construction means that a hyphen can occur 0 or 1 times, and `\w*` means 0 or more occurrences of any letter.

Example 2. Using regular expressions when specifying command arguments

Task: Restrict the `show` command to only allow output of information about configured RADIUS and TACACS servers.

Possible solutions:
The simplest and most linear solution is to specify two commands with appropriate arguments:

Command	Arguments
show	radius-servers
show	tacacs

But a shorter solution is to specify the arguments with `|` (or):

Command	Arguments
show	(radius-servers)|(tacacs)

Short list of frequently used metacharacters

- characters:
  - `.` - any character
  - `\d` - any digit
  - `\w` - any letter in any case
  - `\s' is a space character
  - `\` - any special character escape.
- grouping:
  - `[abc]` - one of the characters listed in brackets (or a, or b, or c)
  - `[a-z]` - one of the characters listed in the range
  - `(abc)` - combining characters in the specified order into one group
- quantifiers:
  - `a? ` - 0 or 1 occurrence of a character
  - `a*` - 0 or more occurrences of a character
  - `a+` - 1 or more occurrences of a character
  - `a{n}` - occurrence of the symbol n times
  - `a{n,}` - occurrence of the character n or more times
  - `a{n,m}` - occurrence of a symbol from n to m times
- logical operations:
  - `^a` - negation
  - `a|b` - one of two specified characters (OR)
- useful combinations:
  - `.*` - any character any number of times
  - `\w+` - any word
  - `(word1)|(word2)` - one of the specified words.

Deleting command sets

To delete command sets on the view page, select the checkbox to the left of the sets you want to delete and click at the top left.

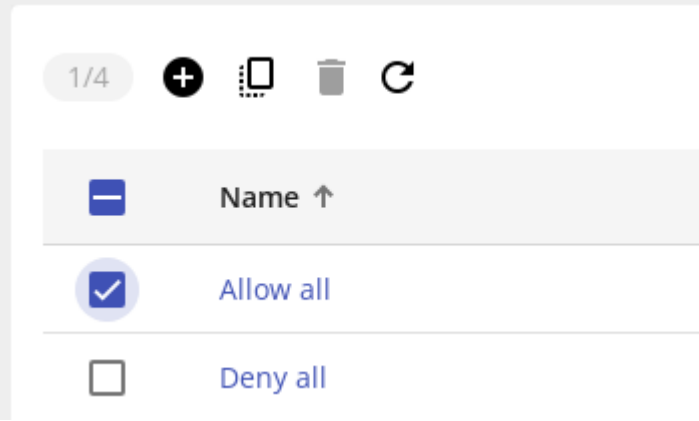

Figure 127. Select the set of commands in the table to delete

Deletion requires confirmation of the action, for which a modal dialog will open. After explicit confirmation, the selected items will be deleted.

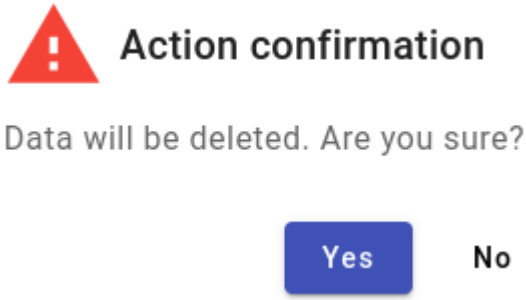

Figure 128. Modal dialog for confirmation

Restrictions:

- you cannot delete command sets that are used in any network device policy.
- you cannot delete system command sets `Allow all`, `Deny all`, and `Show only`.

TACACS Profiles

Description

TACACS profiles are designed to consolidate granular network device access privilege level configurations into distinct entities assigned to network administrators who have successfully authenticated and been authorized via the TACACS protocol.

The main settings in device profiles are:

- Privilege levels assigned within the profile (default level and maximum level).
- User attributes.

View TACACS profiles table

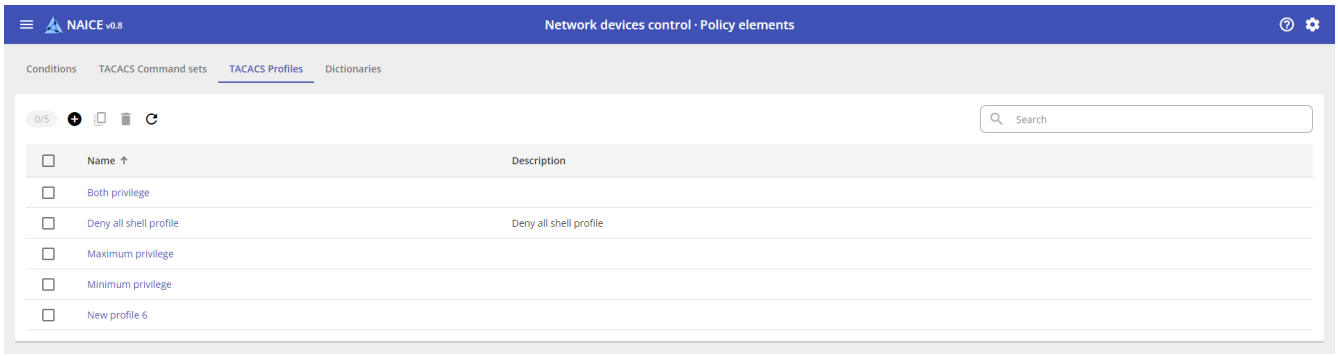

Figure 129. TACACS profile summary table

This page contains a table listing TACACS profiles.

The table contains the following columns:

- `Name` - Profile name;
- `Description` - Profile description.

The table can be sorted by the `Name` column.

Elements of control:

- 0/1 - Counter showing selected (checked) profiles and total profile count.
- - Add TACACS profile.
- - Duplicate TACACS profile.
- - Delete selected (checked) TACACS profile.
- - Refresh profiles table.

Add TACACS profile

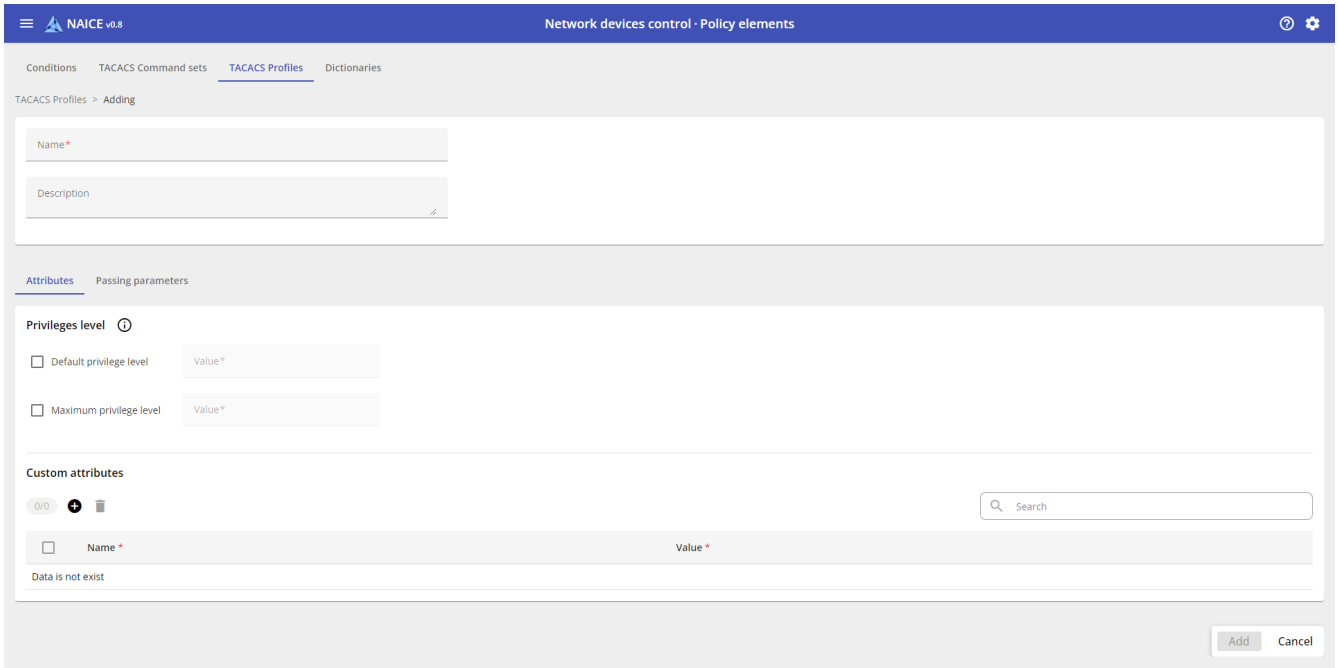

Figure 130. TACACS Profile Add Page

To add a TACACS profile, click ⊕.

fill in the following parameters in new window:

Parameters marked with * are required.

`Name` * - Profile name. `Description` - Description of the profile in any form (Will be displayed in the list of profiles). `Default privilege level` - The privilege level available to the authorized administrator immediately after authorization. `Maximum privilege level` - The privilege level that can be increased by an authorized administrator (the user can enable this level using authorized commands, for example during the configuration of a network device).

If the `Default Privilege Level' and `Maximum Privilege Level' options are unchecked, the authorized administrator account will be assigned the only available default privilege level of '1'.

`User attributes` or otherwise **Attribute-Value pairs** - attributes that define the parameters of authorization, accounts and sessions within the TACACS protocol.

Use the following controls to add and remove custom attributes:

- 0/1 - Counter of selected (checked) attributes adnd total number of attributes.
- ⊕ - Add attribute.
- 🗑 - Delete the selected (checked) attribute.

When adding an attribute, fields marked with * are required.

After completing the profile setup, click `Add` to add the created profile.

TACACS profiles available by default.

After enabling the TACACS functionality, several pre-installed basic TACACS profiles are already available to the system administrator:

- `Both privilege` - Authorized accounts that fall under this profile will be assigned a default privilege level of "1" and will be able to be elevated to a maximum privilege level of "15".
- `Deny all shell profile` - Authorized accounts that fall under this profile will be denied authorization.
- `Maximum privilege` - Authorized accounts that fall under this profile will be assigned the default privilege level of "15".
- `Minimum privilege` - Authorized accounts that fall under this profile will be assigned the privilege level by default, “1”.

Network devices policies

Description

Network device policies define the actions to be performed when processing authentication and authorization requests from network device administrators via the TACACS protocol.

Processing Order

1. Processing in the Network Device Policy Table:
   - The authorization request is checked for compliance with the logical conditions used in the authorization policy..
   - The verification is performed sequentially from top to bottom. Disabled policies are not evaluated and are skipped. For policies with the status "Condition Check", the policy hit counter is incremented, but no request processing is performed—the search for a matching policy continues further.
   - Once a matching policy is found, further policy evaluation stops, and processing continues within that policy set.
   - If no policy with a matching condition is found, the request will be processed according to the default policy `Default`. This policy is always last in the sequence, cannot be deleted, and its condition cannot be edited. By default, this policy set uses the **DenyAccess** authorization profile, which will reject connections to the network device. This behavior can be modified by adding or editing authentication and authorization policies in the default `Default` policy.
2. Processing Within the Matched Policy:
   - For requests from successfully authenticated users, the system verifies compliance with authorization policy conditions.
   - After the authorization policy is determined, the following actions are performed based on the request type:
     - Privilege level authorization request post-authentication: The system retrieves the "Default Privilege Level" value from the TACACS authorization profile assigned to the policy. If no value is specified, privilege level 1 is automatically assigned.
     - Privilege escalation request: The system retrieves the "Maximum Privilege Level" value from the TACACS authorization profile assigned to the policy and compares it with the requested privilege level - If the requested level ≤ the configured maximum: escalation is granted, If the requested level > the configured maximum: escalation is denied, If no maximum level is specified in the assigned profile: the privilege escalation request is automatically denied.
     - The system verifies whether the command is permitted in the TACACS command set assigned to the authorization policy. Command execution is allowed if included in the permitted set, otherwise denied.

When the default "Deny all shell profile" authorization profile is selected in the policy settings - All authentication and authorization requests matching this profile will be rejected. This applies even to successfully authenticated users.

View Policy Sets

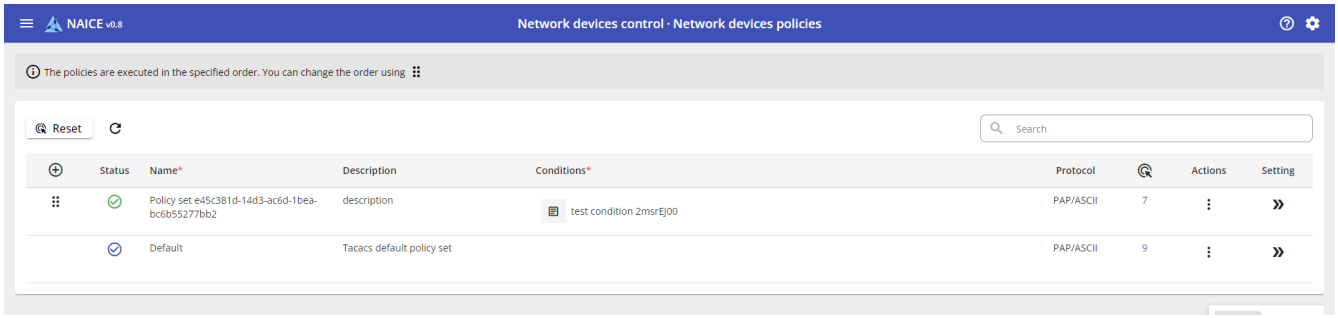

Figure 131. View all Policies.

Table Column Descriptions:

- `Status` – Policy status.
- `Name` * – Policy name.
- `Description` – Arbitrary description.
- `Conditions` * – Logical conditions used. If a library condition is applied, its name is displayed. If a non-library condition is used, its structure is shown.
- `Protocol` * – Always `PAP/ASCII`.
- – Number of authorization attempts matching the specified Conditions.
- `Actions` – Actions for adding/removing a set of policies.
- `Settings` – Navigate to view and edit the policy.

Elements of Control:

- `Search` – a registered search by name (search results will be highlighted yellow).
- – refresh data.
- **Delete** – delete counters for failed attempts on all policies (attempt counts).
- – add policy of network devices (policy will be added first in the list).
- – counter for successful logins under specified conditions.
- – actions:
  - `Add Top` – add policy *before* selected one.
  - `Add Bottom` – add policy *after* selected one.
  - `Delete` – remove selected policy.
  - » – go to `control` of selected policy.
- `Save` – save changes.
- `Cancel` – cancel changes.

All policies are evaluated in their displayed order: top to bottom. For this reason, all policies remain visible on the page at all times. Search terms entered in the Search field highlight matching policies in yellow without removing any policies from the list.

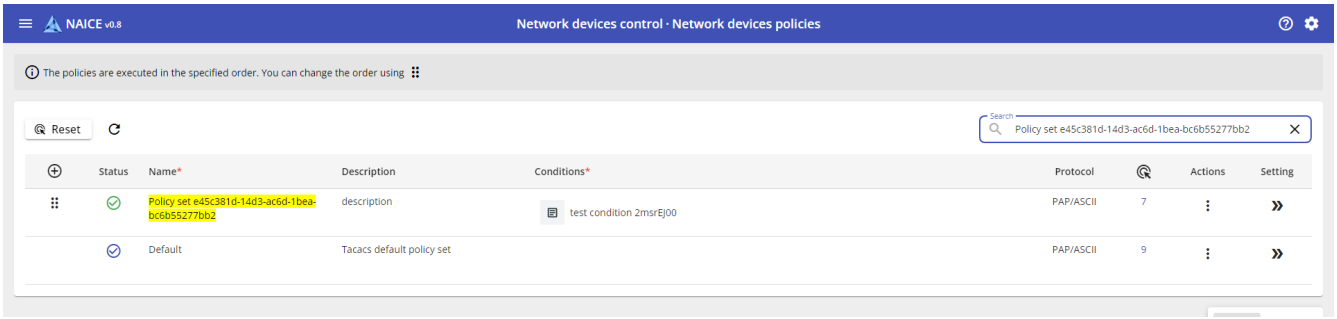

Figure 132. Search Policies.

To change the order, drag a policy by the ⠿ in the ⊕ column.

After reordering policies, remember to click the `Save` button; otherwise, the changes will not take effect.

To view the list of [authentication and authorization policies], click » in the View column to the right of the selected policy set.

Editing Policies

To add a policy in the policy list window, click the ⊕ button in the top-left corner—the new policy will be added at the top of the list.

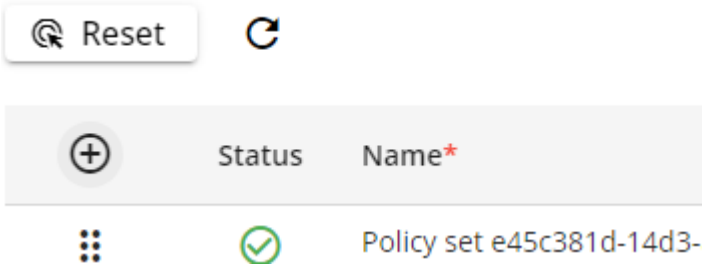

Figure 133. Add Policy icon.

If you need to insert a policy in a specific location, click the ⋮ button to the right of the selected policy and choose Add Above or Add Below from the dropdown menu.

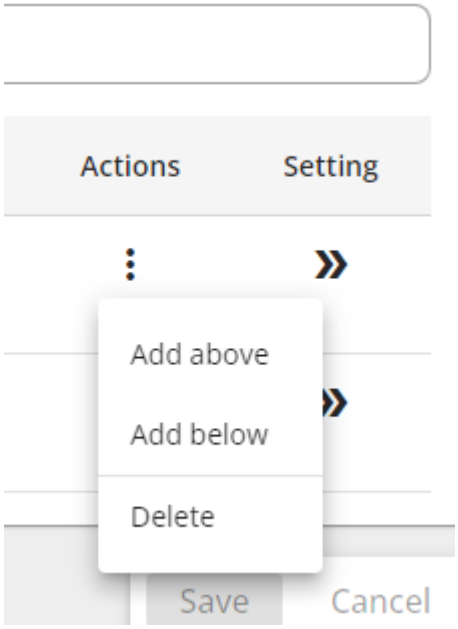

Figure 134. Dropdown Action Menu.

Status Information:

Enabled – Allows processing requests; Disabled – Excludes from processing, does not check the Condition, and does not handle requests; Monitor – Allows checking the Condition (and increments the trigger counter) but does not process requests; Default – Used only for the default policy (Default).

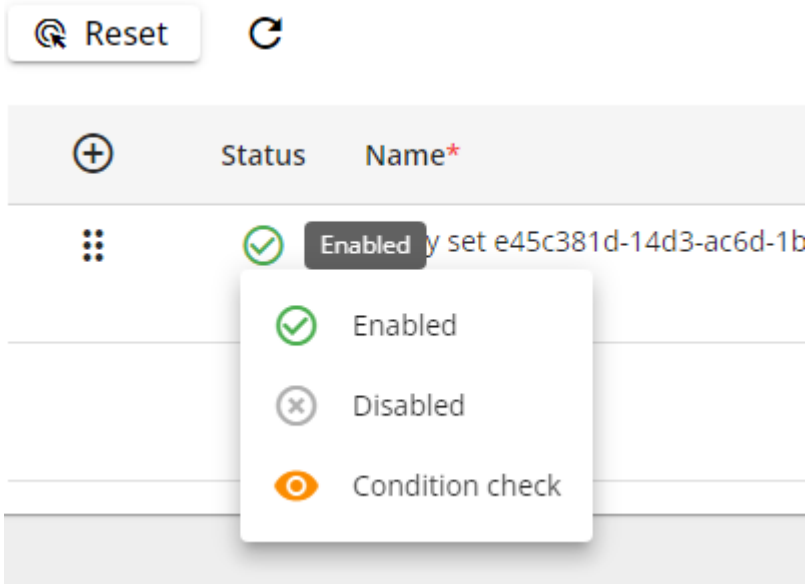

Figure 135. Policy status change.

In a newly created policy, enter a readable name in the `Name` field or leave the auto-generated name unchanged.

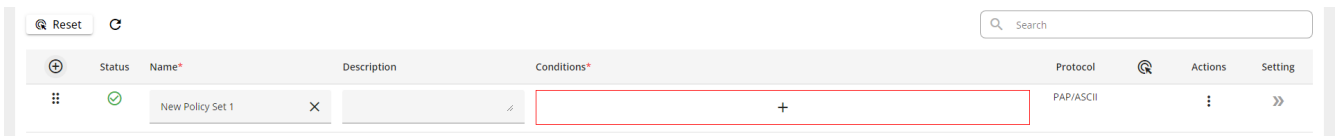

Figure 136. New Policy entry display. Required fields.

To edit a condition, click + , and the Condition Editor will open.

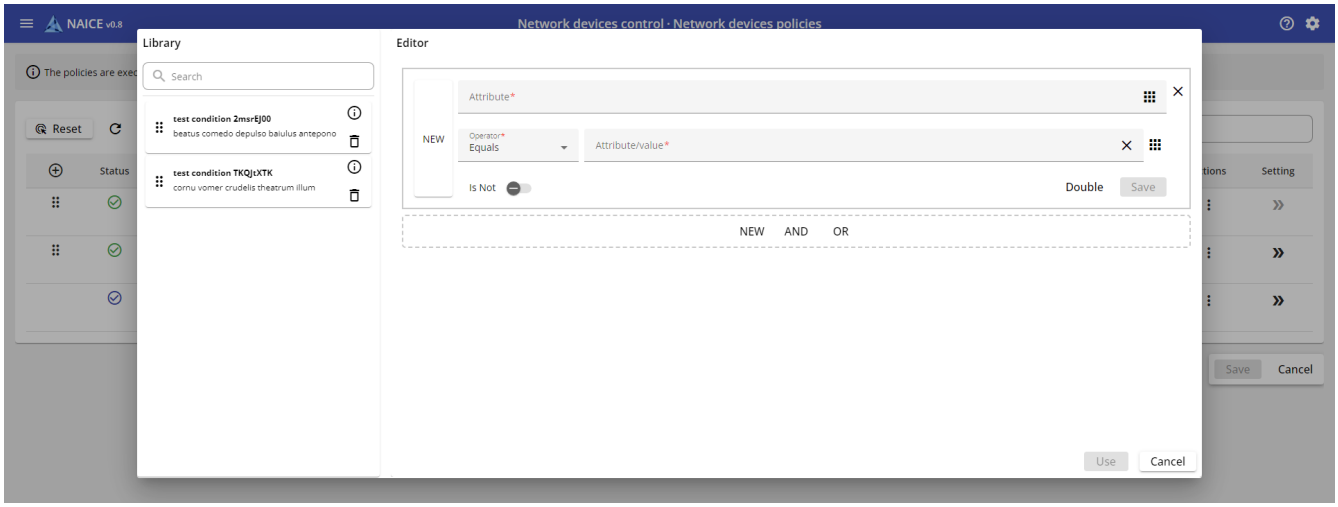

Figure 137. Condition Editor.

Editing conditions follows the same method described in [Conditions].

When configuring a policy condition, there are restrictions on the types of dictionaries that can be used. The following dictionaries are allowed: `NETWORK_ACCESS`, `TACACS_PLUS`, `DEVICE`.

When editing conditions directly in the policy, you can use the configured condition without saving it to the Library. To do this, after setting up the condition (without saving it), click the `Use` button.

Clicking the **Save** button will apply all changes.

After creating a new policy, you must configure its authentication and authorization policies. Otherwise, all connection attempts matching this policy's logical conditions will be rejected according to the default Default policy rules!

Policy deletion

Policy set deletion is available in the `Actions` menu. Only one policy set can be deleted at a time.

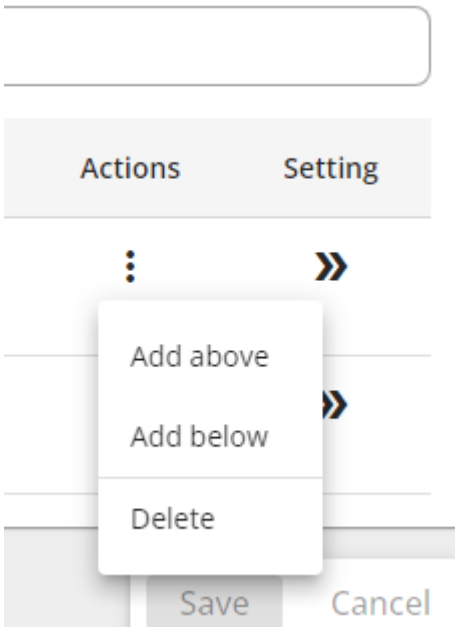

Figure 138. Policy deletion dropdown menu.

Policy hit count

The counters in the column show how many attempts were processed using this policy. Value changes indicate that the Condition is triggering.

Network devices policy configuration

Viewing the list of authentication and authorization policies in the selected network device control policy se

To view the list of TACACS authentication and authorization policies: In the `View` column, click the » icon next to the selected [policy set]. The detailed page for editing authentication and authorization policy rules will open.

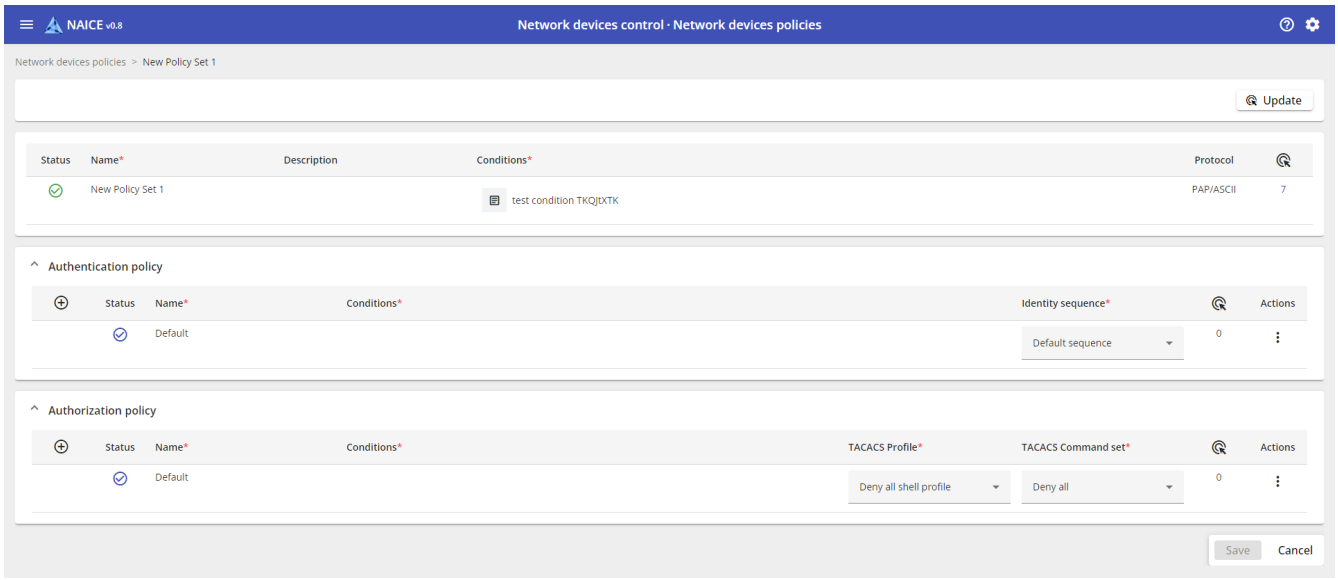

Figure 139. Policy set view & Edit page

> The final authentication and authorization policy rules named `Default` cannot be renamed or have their trigger conditions modified. They will always appear last in the list, no other rules can be placed below them. These rules define the default behavior when no other policies match.

The policy set view form is organized into sections:

- Policy Set Management Section - Displays the contents of the selected policy set in a format consistent with the page: Policy sets
- Authentication Policy - Manages user authentication processes.
- Authorization Policy - Controls User authorization for privilege level and profile access and lists of permitted commands.

Control Elements:

- Refresh - Requests current policy trigger counts
- `Status` - Enable/disable/monitor the corresponding policy
- `Name` * - Policy name (required field)

`Description` - Custom description (optional)

- `Conditions` * - Logical conditions. Displays the library condition name (if used). Shows condition structure (for non-library conditions).
- `Protocol` * - Always PAP/ASCII
- `Identification Chain` * - Selected [identity source chain]
- `TACACS Profile` * - Available [authorization profiles] selection
- `TACACS Command Set` * - Available [command sets] selection
- ⋮ - Actions menu:
  - `Add Above` - Insert policy *before* selected one
  - `Add Below` - Insert policy *after* selected one
  - `Delete` - Remove selected policy
- - Authorization attempts matching the Conditions. Click the counter to Reset it.
- `Save` - Apply changes
- `Cancel` - Discard changes

Parameters marked with an asterisk * are mandatory.

To change the order of Authentication and Authorization Policies, drag a policy using the ⠿ handle in the ⊕ column (visible on hover) - similar to the functionality described in Policy sets.

Editing Authentication and Authorization policies within network device control policies

To edit policies, click » next to the selected policy set.

You must configure at least one authentication policy and one authorization policy for successful client connections using this TACACS policy. Alternatively, reconfigure the default **Deny** rule `Default`.

The default Default policy can be modified to change its behavior. However, for security best practices: Configure custom rules for your specific needs, and keep the default policy behavior as **Deny**.

Authentication policy

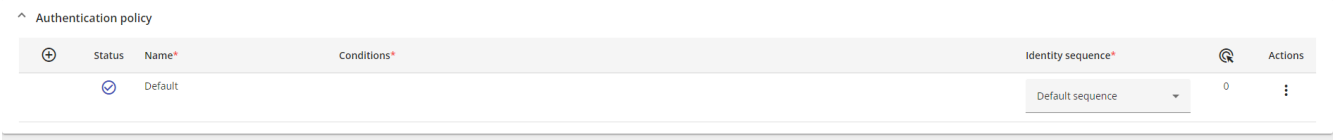

Figure 140. Authentication policy panel.

To configure an authentication policy in the Authentication Policy section: click the ⊕ button, and new rule will be created.

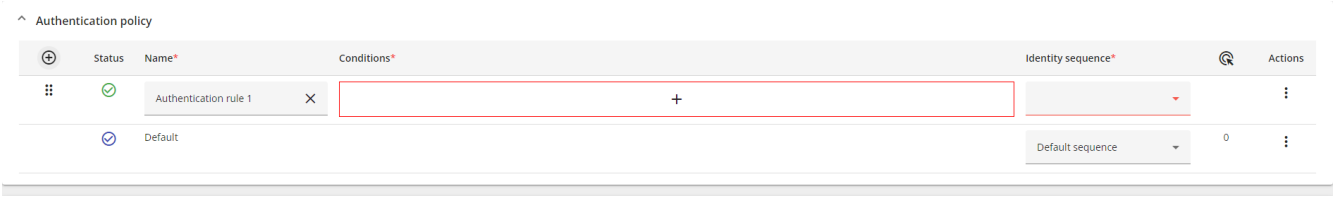

Figure 141. New authentication policy.

Input the policy name in the `Name` field.

Editing the conditions is performed the same way that described in [Conditions].

When configuring a policy condition, there are restrictions on the types of dictionaries that can be used. Only the following dictionaries are allowed: NETWORK_ACCESS, TACACS_PLUS, DEVICE.

When editing conditions in a policy, you can apply the configured condition without saving it to the Library. Just click `Use` after setup instead of saving.

Use the ⋮ button to the right of the policy to add a new rule above or below, or to delete the current one.

In the dropdown menu Identification Chain, select the required [chain].

Click the Save button to save your changes.

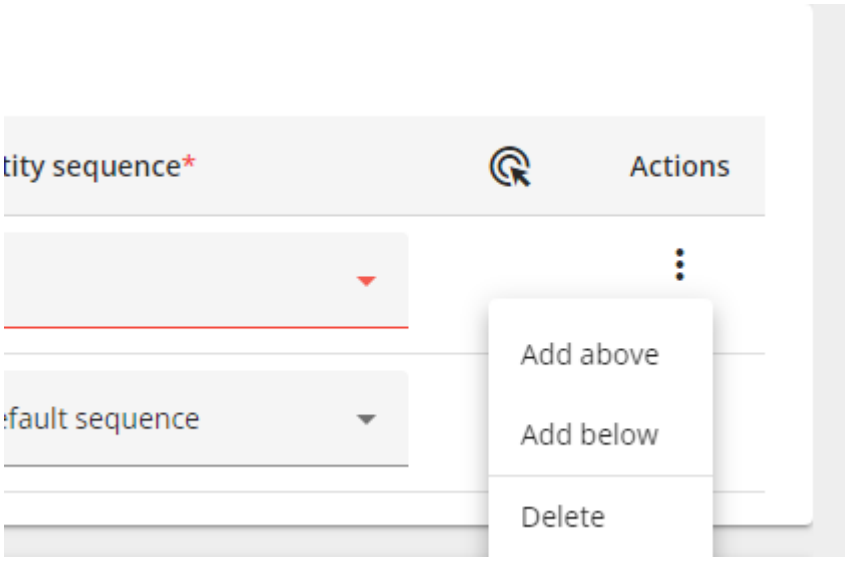

Figure 142. Authentication policy. Dropdown menu - Actions.

You can also change the policy status, similar to how statuses work in policy sets.

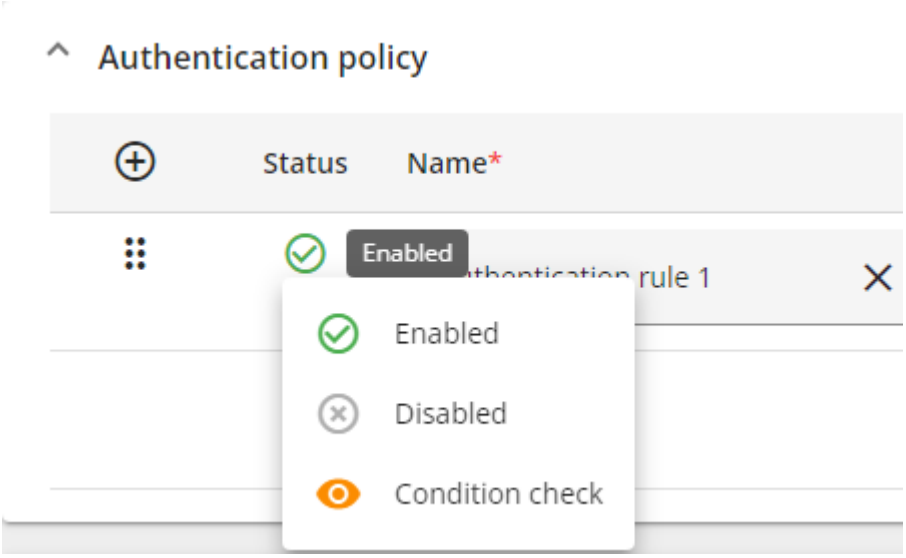

Figure 143. Authentication policy. Status Modification.

Authorization policy

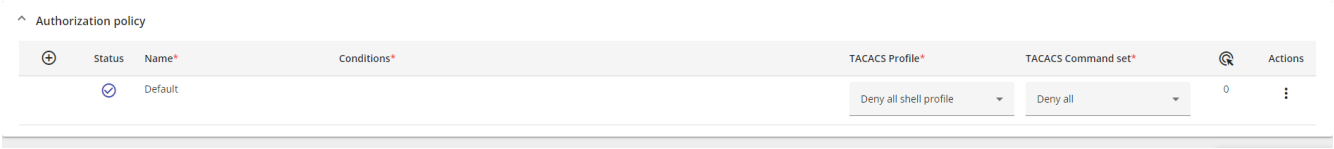

Figure 144. Authorization policies panel.

To configure an authorization policy rule, click ⊕ in the Authorization Policies section. A new rule will appear.

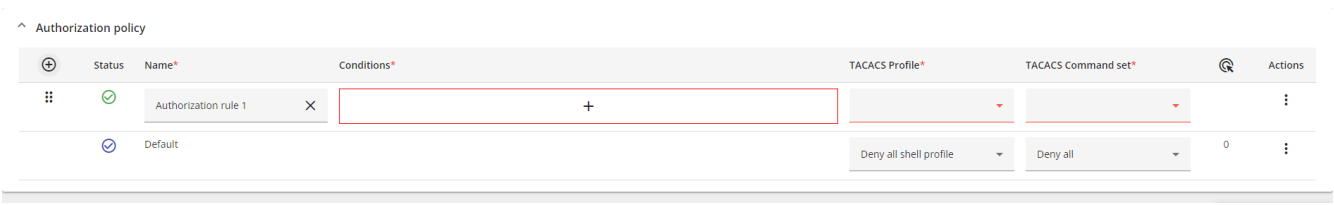

Figure 145. New Authorization policy.

In the `Name` field, enter the policy rule name.

To edit the condition, click + - the condition editor will open.

Conditions are edited in the same way as described in Conditions.

When configuring an authorization policy, you can use the following dictionaries: `LDAP`, `NETWORK_ACCESS`, `TACACS_PLUS`, `IDENTITY`, `DEVICE`.

When editing conditions directly within a policy, you can use the configured condition without saving it to the Library. To do this, set up the condition and click `Use` without saving it first.

In the **TACACS Profile** dropdown menu, select the required [TACACS profile].

In the **TACACS Command Set** dropdown menu, select the required [TACACS command set].

Using the ⚙ button to the right of a policy, you can: Add a new rule above the current one, add a new rule below the current one, delete the current rule

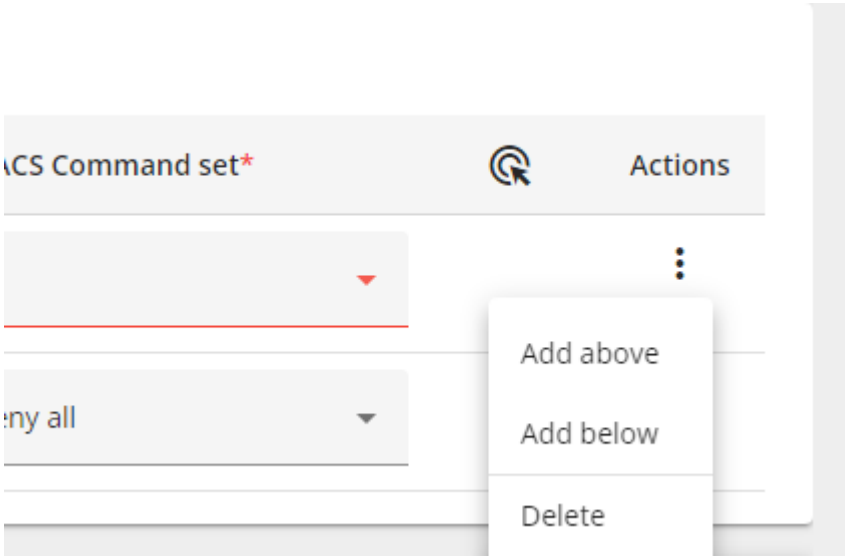

Figure 146. Authorization Policy. Dropdown menu - Actions.

Policy status can also be modified using the same status controls available in policy sets.

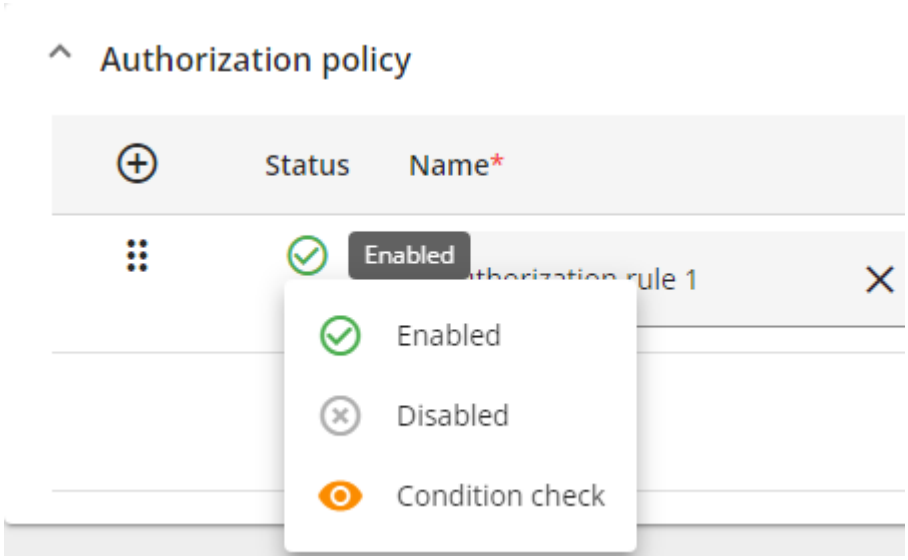

Figure 147. Authorization policy. Status Modification.

The `Save` button will only become available after: Adding at least one fully configured authentication policy and adding at least one fully configured authorization policy.

Click the `Save` button.

Policy rule Editing

Policy editing is performed by mouse-clicking the target setting field.

Then click the `Save` button.

Policy rule deletion.

The deletion is done by clicking on the "Settings" button: en:ROOT:icons/more_vert.png[100, 25] and selecting action **Delete**.

Deletion requires confirmation of the action, for which a modal dialog will open.
After explicit confirmation, the selected items will be deleted.

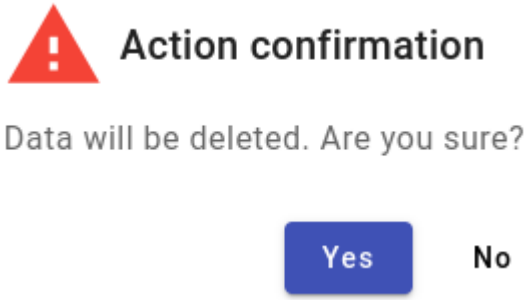

Figure 148. Modal dialog for confirmation

Access policy

Elements

Allowed Protocols

Description

Authentication protocol management allows you to allow or deny the use of specific protocols or authorization methods when authenticating a endpoint. It is possible to configure multiple lists of allowed protocols, which allows you to flexibly configure the allowed protocols in policy sets for each user scenario.

The following protocols are currently supported: PAP, MS-CHAPv2, EAP-PEAP, EAP-TLS.

You can configure to enable or disable MAB authorization.

View a list of allowed protocols

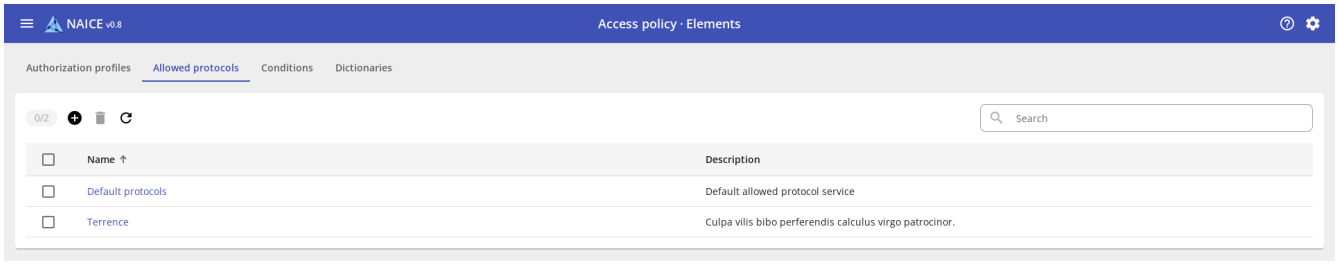

Figure 149. A table with a list of allowed protocol services on the viewing page

On the bottom is a list table that contains the following columns:

- `Service name` - the name of allowed protocols services.
- `Description` - arbitrary description.

You can sort in forward and reverse order by any column. By default, sorting is performed in direct (alphabetical) order by the "Service Name" column.

Controls:

- `Search` - Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.
- - Refresh table data.
- `0/1` - Counter of elements selected by the checkbox / total number of elements.
- - Add a new element.
- - Delete selected elements (inactive until at least one element is selected).
- - Change the current sort order.
- - Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).

Adding allowed protocols service

To add a allowed protocols service, click ⊕, and a window will open

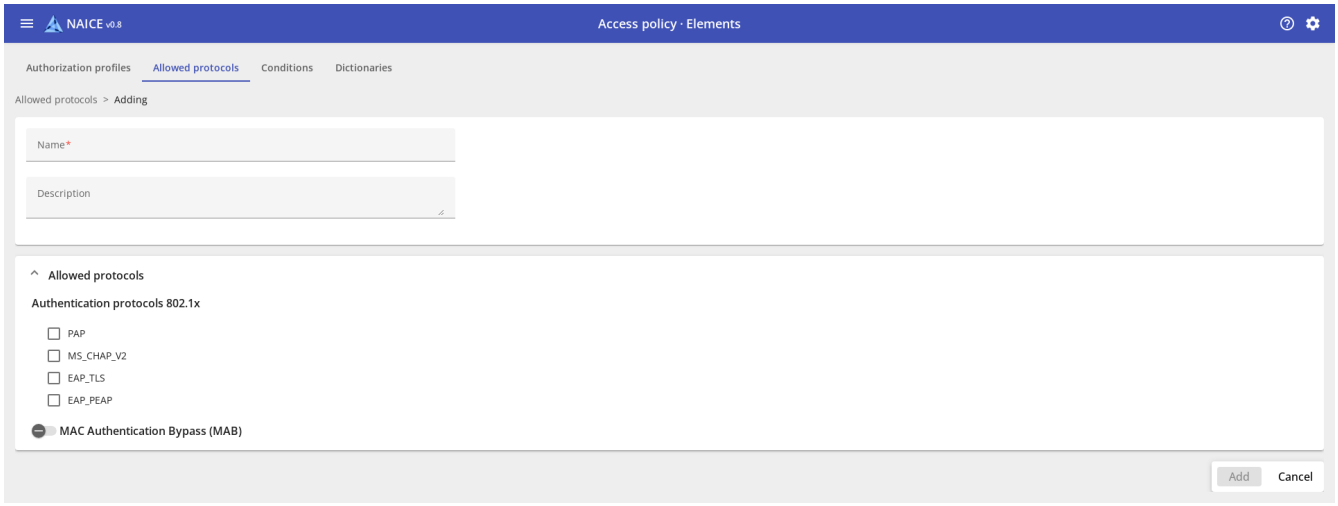

Figure 150. Window for adding a list of allowed protocols

- `Service name` `*` - name, must be unique. Maximum length is 100 characters.
- `Description` - arbitrary description. Maximum length is 200 characters.
- `Available protocols` - select available authentication protocols. By default, all protocols are disabled.
  - `PAP` - select the PAP protocol (password authentication protocol), which provides for sending the login and password to the authentication server in clear text.
  - `MS_CHAP_V2` - select the MS-CHAPv2 protocol (Microsoft challenge handshake authentication protocol version 2).
  - `EAP_TLS` - select the EAP-TLS protocol (Extensible Authentication Protocol Transport Layer Security)
  - `EAP_PEAP` - select the EAP-PEAP (Protected Extensible Authentication Protocol), which encapsulates EAP (Extensible Authentication Protocol) inside the TLS tunnel (Transport Layer Security).
  - `MAC Authentication Bypass (MAB)` - allow authentication of endpoint by MAC address.

`*` - required fields.

After entering the required data and selecting the available protocols, click the **"Add"** button.

Editing the allowed protocols service

To edit the allowed protocols service, on the page with the list, click on its name.

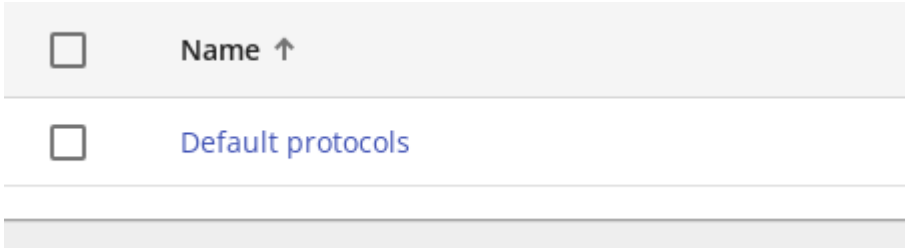

Figure 151. Hyperlink to the page for editing the list of allowed protocols

After this, the editing window will open.

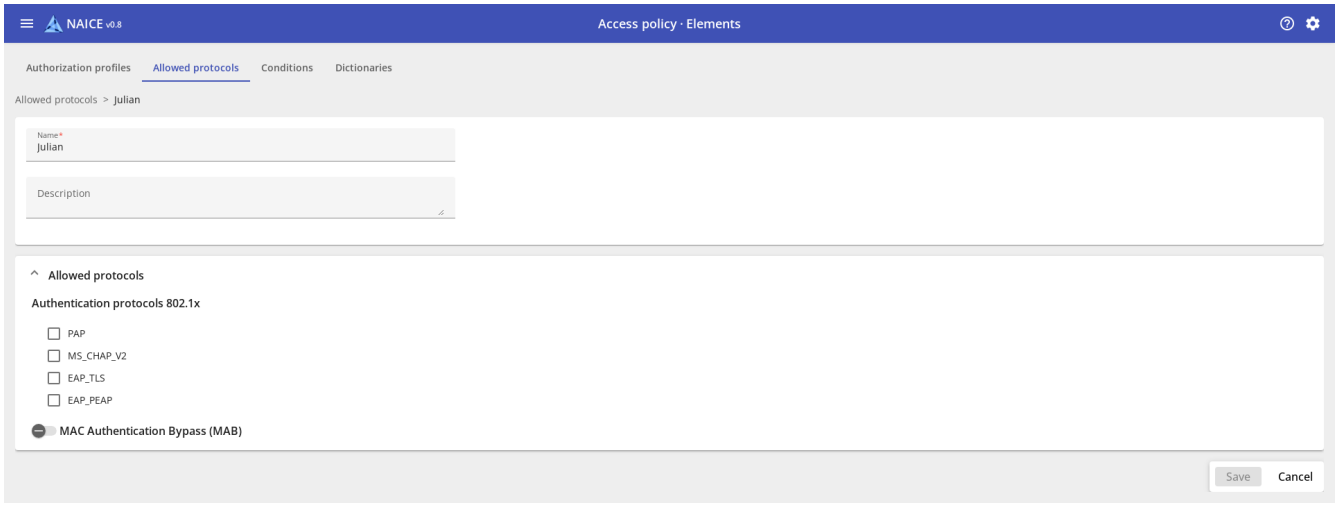

Figure 152. The window for editing the list of allowed protocols

After editing, click on the **"Save"** button. The button remains inactive until at least one field is changed.

Removing the allowed protocols service

To delete, in the list window, select the checkbox to the left of the allowed protocols services that you want to delete, and click the button at the top left.

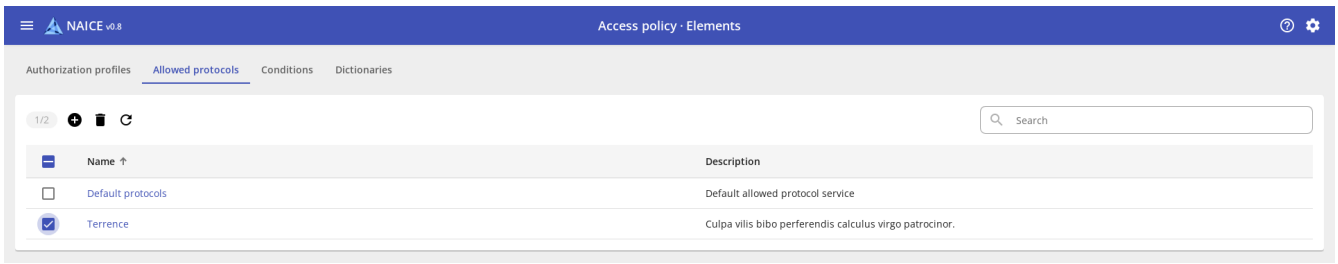

Figure 153. Selecting allowed protocol services in the table to delete

Deletion requires confirmation of the action, for which a modal dialog will open. After explicit confirmation, the selected items will be deleted.

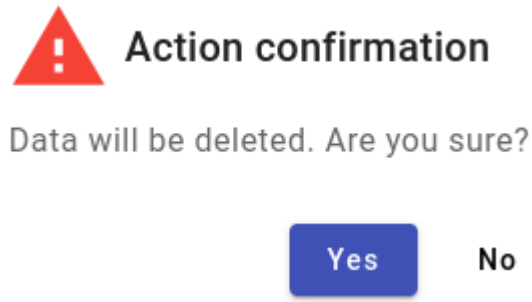

Figure 154. Modal dialog for confirmation

Restrictions:

- you cannot delete the Allowed Protocols service that is used in any policy sets.

Authorization profiles

Description

Authorization profiles allow you to define actions that need to be performed after a user is authenticated. Both access permission (ACCESS-ACCEPT) and access denial (ACCESS_REJECT) are available.

It is supported to add the following attributes to the ACCESS-ACCEPT response after client authentication:

- Dynamically assigned client VLAN, using standard IETF attributes (Tunnel-Medium-Type: IEEE-802, Tunnel-Type: VLAN, Tunnel-Private-Group-Id: <VLAN ID>) or attributes configured in the device profile.
- The name of the ACL that needs to be assigned to the client (an ACL with this name must be configured on the network equipment).
- Another RADIUS attributes via Advanced Attribute Settings

Viewing a list of available authorization profiles

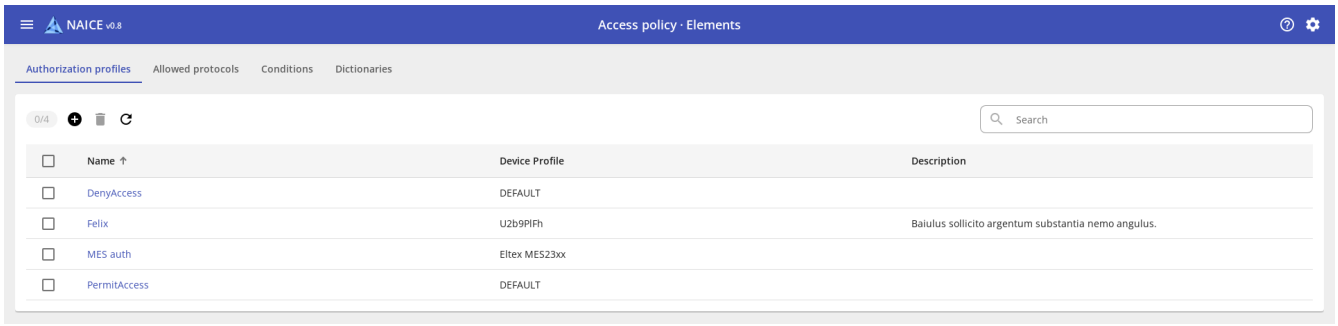

Figure 155. A table with a list of authorization profiles on the viewing page

On the bottom is a list table that contains the following columns:

- `Name` - name of the authorization profile.
- `Network device profile` - selected network device profile.
- `Description` - arbitrary description.

You can sort in forward and reverse order by any column. By default, sorting is performed in direct (alphabetical) order by the "Name" column.

Controls:

- `Search` - Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.
- - Refresh table data.
- `0/1` - Counter of elements selected by the checkbox / total number of elements.
- - Add a new element.
- - Delete selected elements (inactive until at least one element is selected).
- - Change the current sort order.
- - Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).

Adding an authorization profile

To add an authorization profile, click ⊕, the window for adding an authorization profile will open.

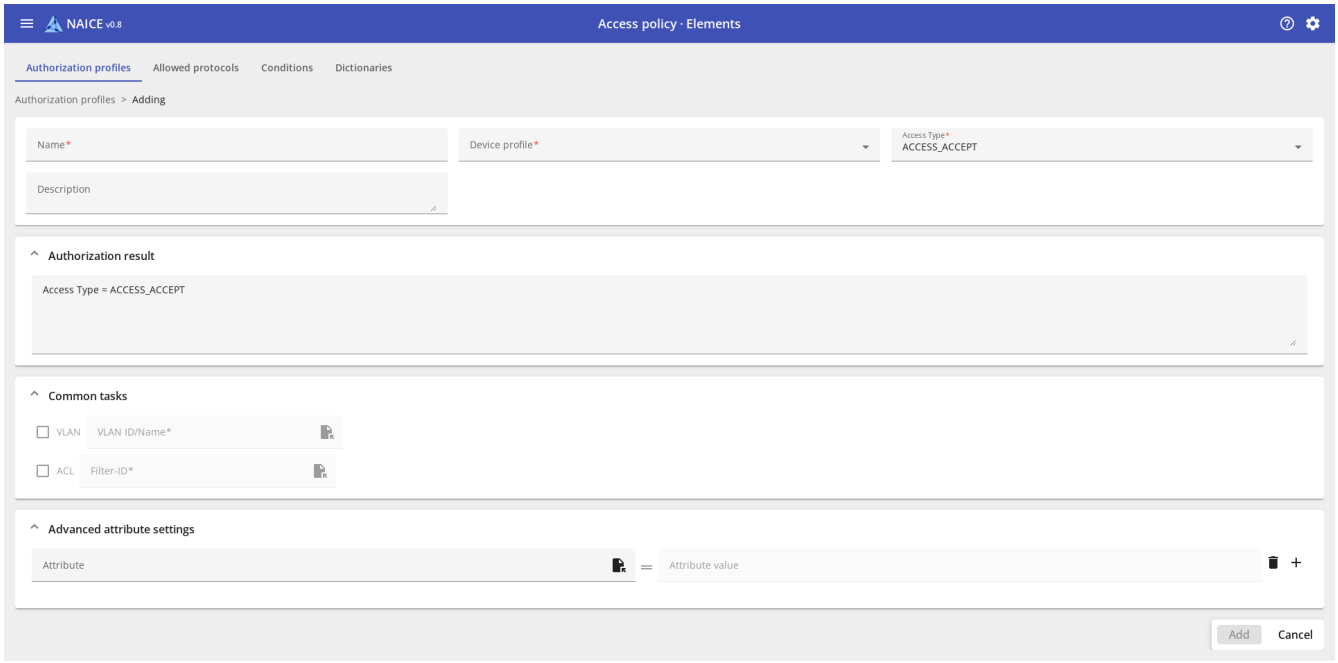

Figure 156. The window for adding an authorization profile

- `Name` * - name, must be unique. Maximum length is 100 characters.
- `Profile` * - network device profile. In the network device profile, you configure permission to issue a client VLAN and ACL, as well as which RADIUS attributes to use for this.
- `Access type` * - the access type for which the authorization profile will be applied. A drop-down list of two elements: `ACCESS_ACCEPT` (by default) and `ACCESS_REJECT`.
- `Description` - arbitrary description. Maximum length is 200 characters.
- `Authorization result` - visualization of attributes in the resulting RADIUS packet based on the settings of "Access type", "General tasks" and "Advanced attribute settings".
- `Common tasks` - enable and configure common scenarios during user authorization. Scenarios combine one or more attributes. By default, all scripts are disabled.
  - `VLAN` - enable dynamic assignment of VLAN to the user.
    - `VLAN ID/Name` - VLAN number or name, issued in the "Tunnel-Private-Group-Id" attribute or other attribute configured in the device profile.
  - `ACL` - enable issuance of the access list name to the user.
    - `Filter-ID` - the name of the access list assigned to the user. Must be configured with the appropriate name on the network equipment to which the user connects.
- `Advanced attribute settings` - manual configuration of the issuance of RADIUS attributes. It is recommended only if a script from the `Common tasks` list is not available for a certain authorization result.

* - required fields.

To assign a dynamic VLAN and ACL to a user during authorization, these actions must be enabled in the network device profile that is used in the authorization profile. Otherwise, their configuration will not be available.

After entering the required data and selecting the available protocols, click the "Add" button.

Editing an authorization profile

To edit the authorization profile, you need to click on its name on the list page.

Figure 157. Hyperlink to the authorization profile editing page

After that, the editing window will open.

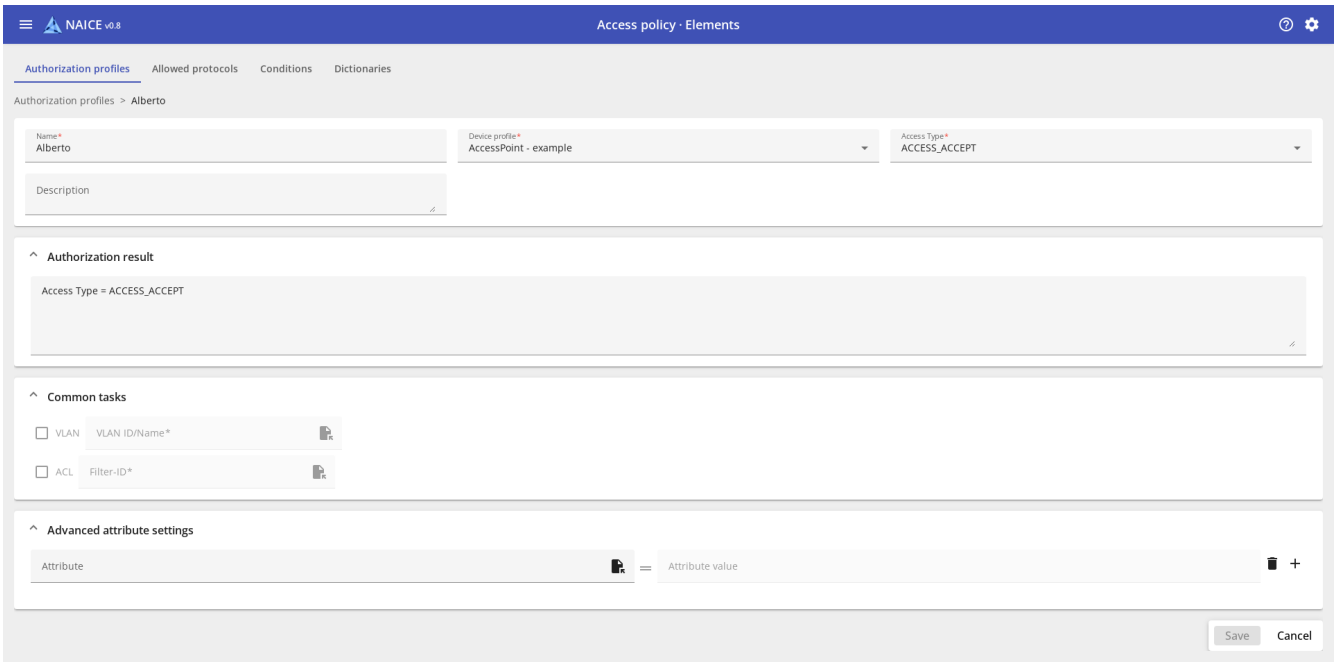

Figure 158. Authorization profile editing window

After editing, click on the **“Save"** button. The button remains inactive until at least one field is changed.

Deleting an authorization profile

To delete, in the list window, select the checkbox to the left of the authorization profiles that you want to delete, and click the button at the top left.

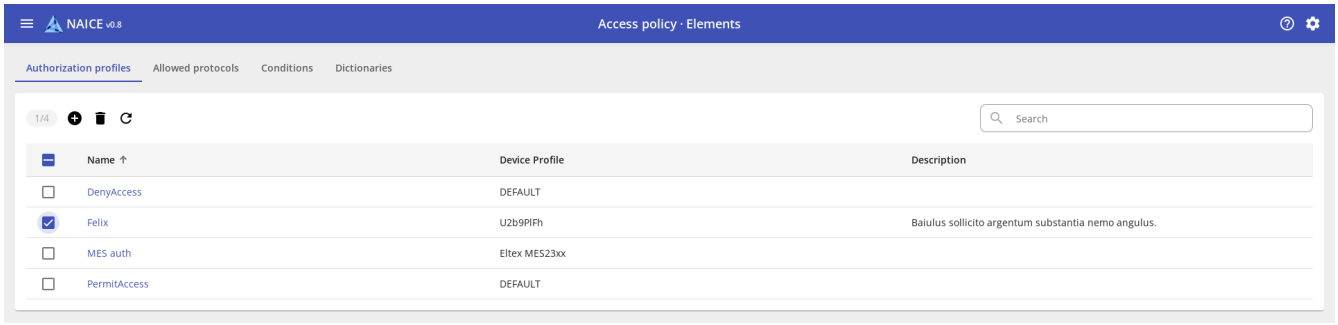

Figure 159. Selecting the authorization profile in the table to delete

Deletion requires confirmation of the action, for which a modal dialog will open. After explicit confirmation, the selected items will be deleted.

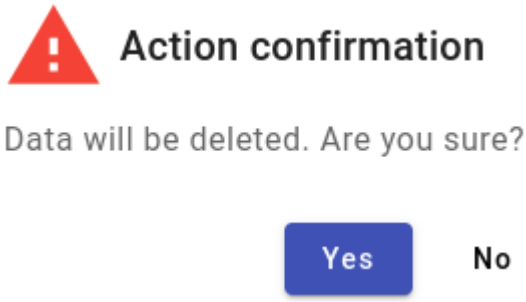

Figure 160. Modal dialog for confirmation

Restrictions:

- You cannot delete an authorization profile that is used in any authorization policy.

Conditions

Description

Logical conditions are the main element of authentication and authorization policies, which are responsible for generating criteria that allow determining whether a user can pass authentication and what actions should be applied to him when authorizing.

The algebra of logic is the basis for creating and processing a logical condition. The result of the condition is "True" or "False". The result may be inverted. The condition can be simple or complex. In a simple condition, only one attribute acts as a verification criterion. In a complex condition, you can use several different attributes, combining them with the "AND"/"OR" logical operations.

View a list of logical conditions

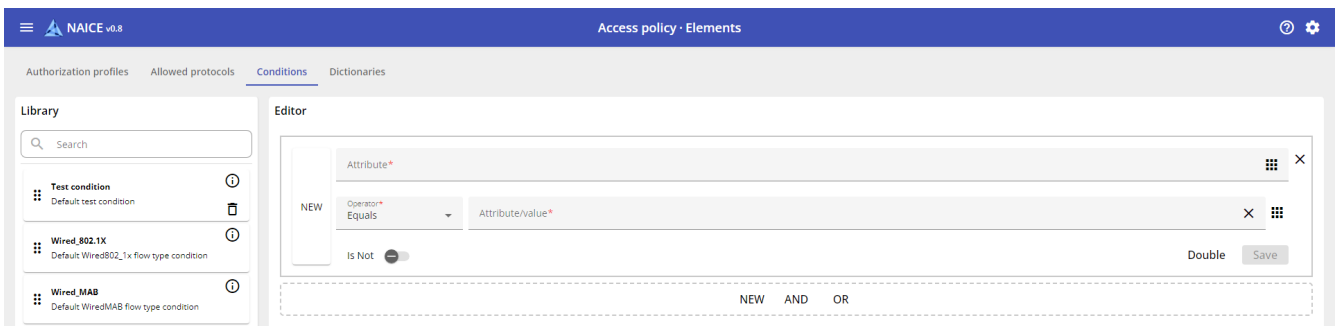

Figure 161. Library of logical conditions

On the left is a **Library** of logical conditions.

On the right is the logical condition **Editor**:

- `Attribute` * - attribute of a logical condition.
- `Operator` * - the selected logical condition operator. Can take values (depending on the attribute value type):
  - "More or equal" / "Less or equal"
  - "More than" / "Less than"
  - "Equals" / "Not equal"
  - "Equal to NULL" / "Not equal to NULL"
  - "Starts with" / "Doesn’t start with"
  - "Ends with" / "Does not end with"
  - "Contains" / "Does not contain"
  - "Match" (*full* string match, case sensitive)
- `Attribute/value` * - attribute/value that is used to match the logical condition attribute in accordance with the selected operator. For an attribute that assumes predefined values, the value is selected from the list.
- `Is Not` - choice of inverting the result of the condition (by default the condition is "Complied", when the setting is enabled, the condition will be considered "Not Complied")
- `NEW` - adding a new logical condition to the existing hierarchy at the same level as the current one.
- `AND` - adding a new logical condition as a "child" for an existing one with the logical operator "AND".
- `OR` - adding a new logical condition as a "child" for an existing one with the logical operator "OR".

* - required fields.

Controls:

- `"Search"` - Performs case-insensitive filtering based on the library of logical conditions.
-  - Preview the contents of the logical condition.
-  - Deleting a logical condition.
-  - Open the dictionary to add an element.
-  - Remove an element from the editor. Action depends on location:
  - clicking to the right of the "Attribute" field will clear the corresponding field;
  - clicking to the right of the Attribute/Value field will clear the corresponding field;
  - clicking to the right of a logical condition will remove that condition.
- `"Save"` - Save the corresponding logical condition.

Attribute selection menu

To select an attribute to be used in the condition, click - the attribute selection menu will open.

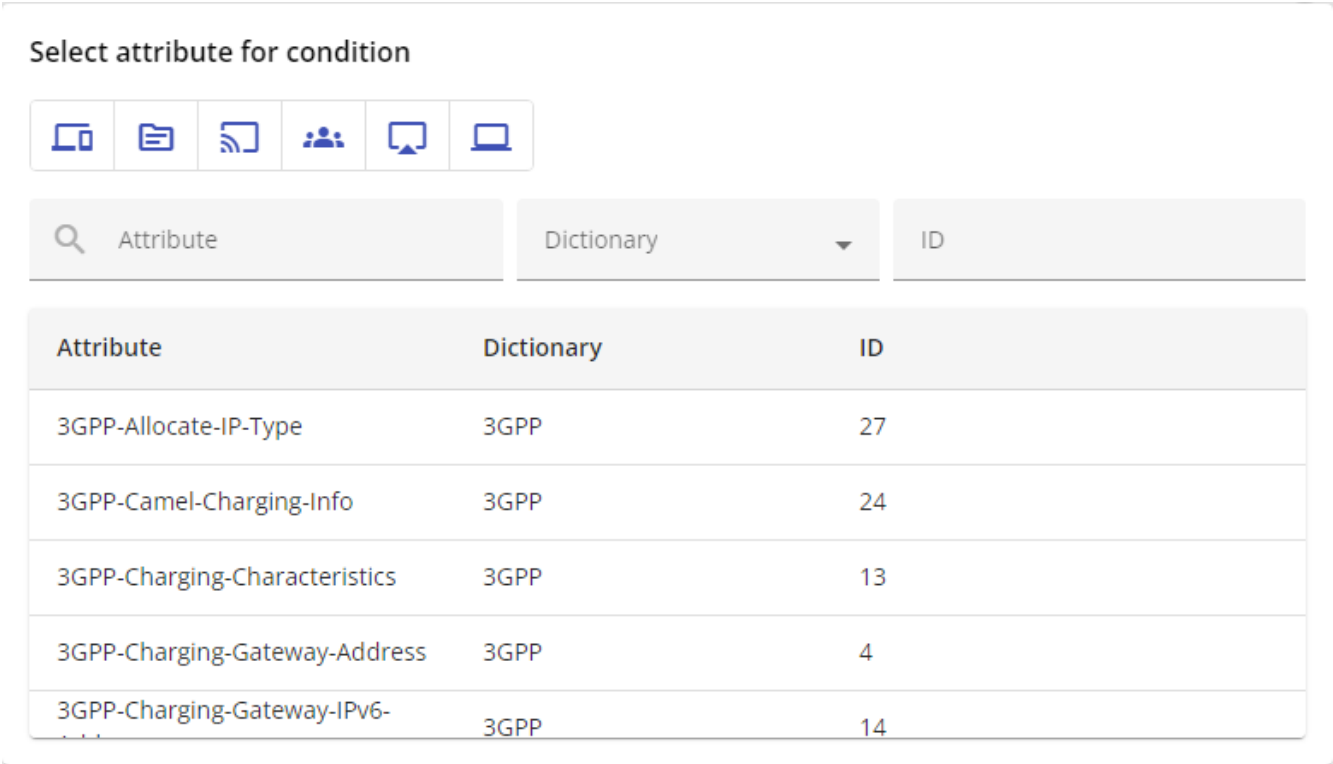

Figure 162. Attribute selection menu

At the top there is a list that allows you to filter by dictionary type. Only one type can be selected.

Types of dictionaries:

- `RADIUS` - dictionaries of RADIUS attributes, including vendor-specific.
- `NORMALISED_RADIUS` - system radius attributes calculated by the system.
- `INTERNAL_RADIUS` - service dictionary with system attributes is usually not used.
- `DEVICE` - device attributes.
- `IDENTITY` - users and endpoints attributes.
- `LDAP` - attributes of external identity sources.

Below are attribute filtering columns.

- "Attribute" - case-insensitive filtering by attribute name.
- "Dictionary" - menu for selecting a dictionary. A dictionary type must be selected to use it.
- "ID" - filtering by attribute number.

Creating logical conditions

Creating a simple logical condition

You can create logical conditions at **Editor**.

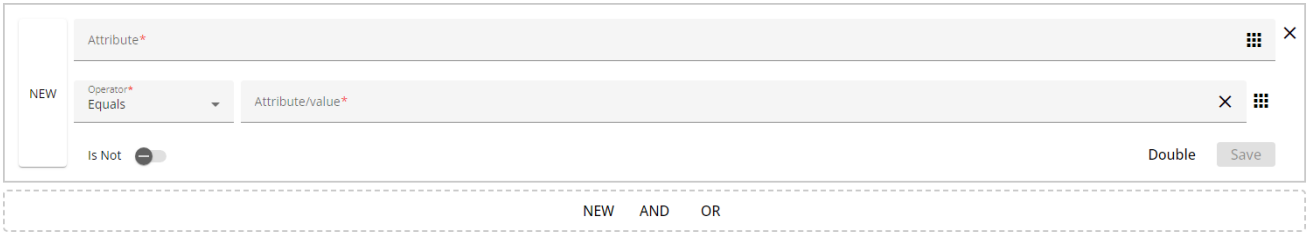

Figure 163. Initial state of Editor

After clicking on ⠿ in the right side of the “Attribute” field, the dictionary will open.

To find the required attribute, you can use filtering by attribute name. Or select the type of dictionary and select the required dictionary by scrolling the drop-down list to determine the required attribute.

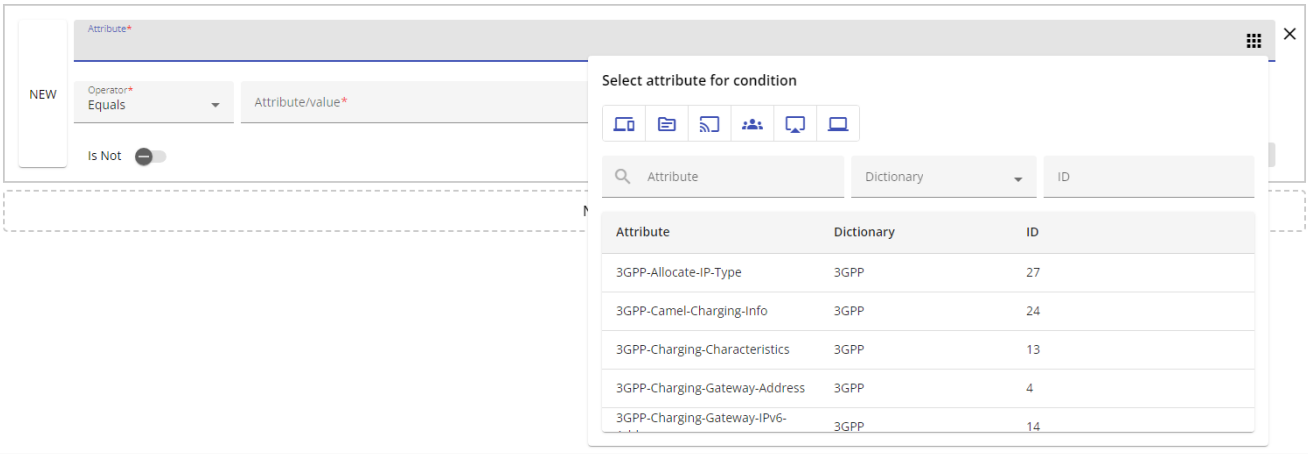

Figure 164. Attribute selection

After selecting an attribute, click on it, and it will be placed in the “Attribute” field.

Select the operator (by default, “Equal” is substituted). The operator selection list depends on the type of data that can be used in the value of the selected attribute.

Attribute data type	Supported operators
String	Matches, Ends with, Does not end with, Starts with, Does not begin with, Contains, Does not contain, Equal to, Not equal to, Equal to NULL, Not equal to NULL
Number	Greater than or equal to, Greater than, Less than or equal to, Less than, Equal to, Not equal to, Equal to NULL, Not equal to NULL
IPv4 address	Equal to, Not equal to, Equal to NULL, Not equal to NULL
MAC address	Equal to, Not equal to, Equal to NULL, Not equal to NULL, Starts with, Does not start with, Ends with, Does not end with, Contains, Does not contain,
Name	Equal to, Not equal to, Equal to NULL, Not equal to NULL
Byte sequence	Equal to NULL, Not equal to NULL

Select an attribute in the Attribute/value field or enter its value.

Figure 165. A condition in which all parameters are filled in

Then click the “Save” button. You can replace an existing condition in the library or save a new one.

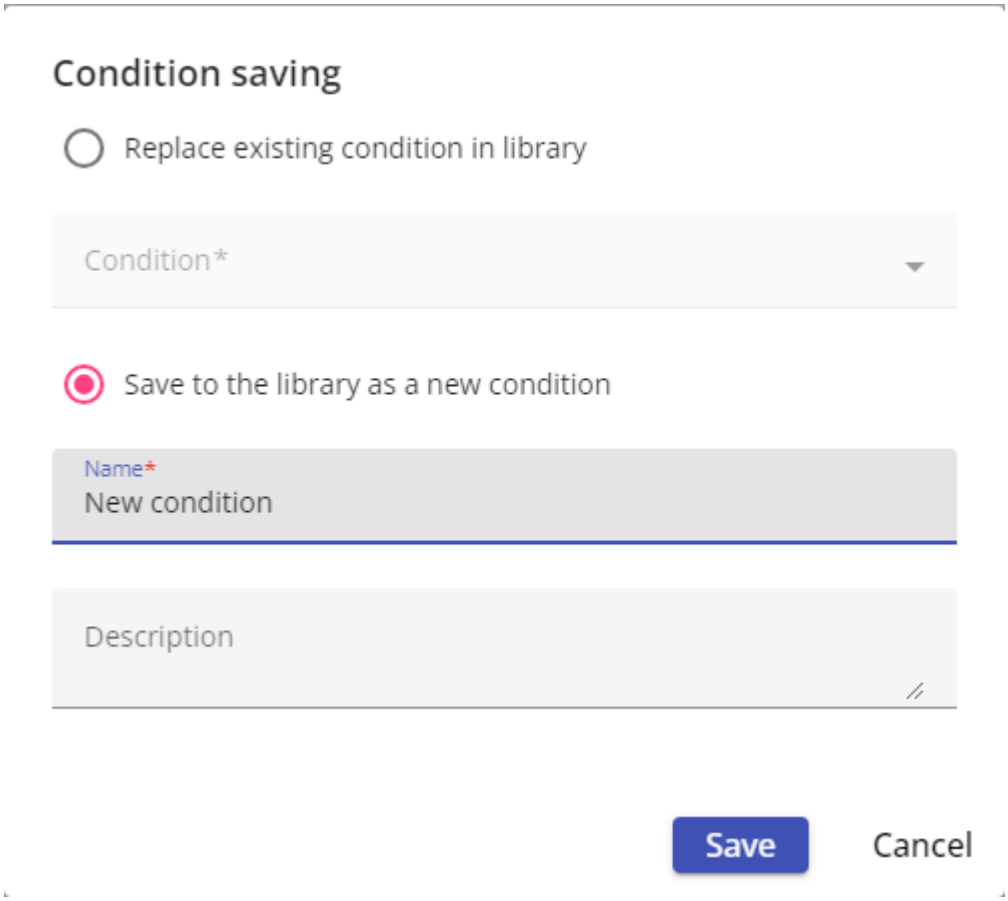

Figure 166. Condition saving modal dialog

By default, the action assumes saving the new condition:

- "Name" * - name of the condition. Maximum length is 100 characters.
- "Description" - arbitrary description. Maximum length is 200 characters.

* - required fields.

Then click the “Save” button.

Save and replace an existing condition in the library. To do this, select "Replace an existing condition in the library" and select a condition from the drop-down list. If necessary, you can filter by name by entering the appropriate text in the field in front of the list.

Then click the “Save” button.

The "Save" button is always active to be able to save an existing condition under a different name.

Creating a complex logical condition

To create a complex logical condition, use the panel under the logical condition.

Figure 167. Panel to create an additional logical condition

- "New" - add a logical condition at the same level as the existing one.

"AND" - add a child condition with logical "AND".

- "OR" - add a child condition with a logical "OR".

When you click "New", an additional rule will appear in the editor on the same level as the existing one, combined with a logical "AND".

Figure 168. Condition consisting of two conditions combined by a logical "AND"

- Logical "AND" combining rules can be changed to "OR".
- It is possible to save each condition separately using the “Save” button in its window or all together using the “Save” button at the bottom.
- To delete a condition, click on ✕ at the top right in the condition window.
- To completely clear all conditions in the editor, click ✕ at the top right of the editor, located behind the windows of individual conditions.

When you press "AND"/"OR", a new window will appear in which a new menu will be available, then you can add conditions at a new level or create child conditions. There is no restriction on the nesting of conditions.

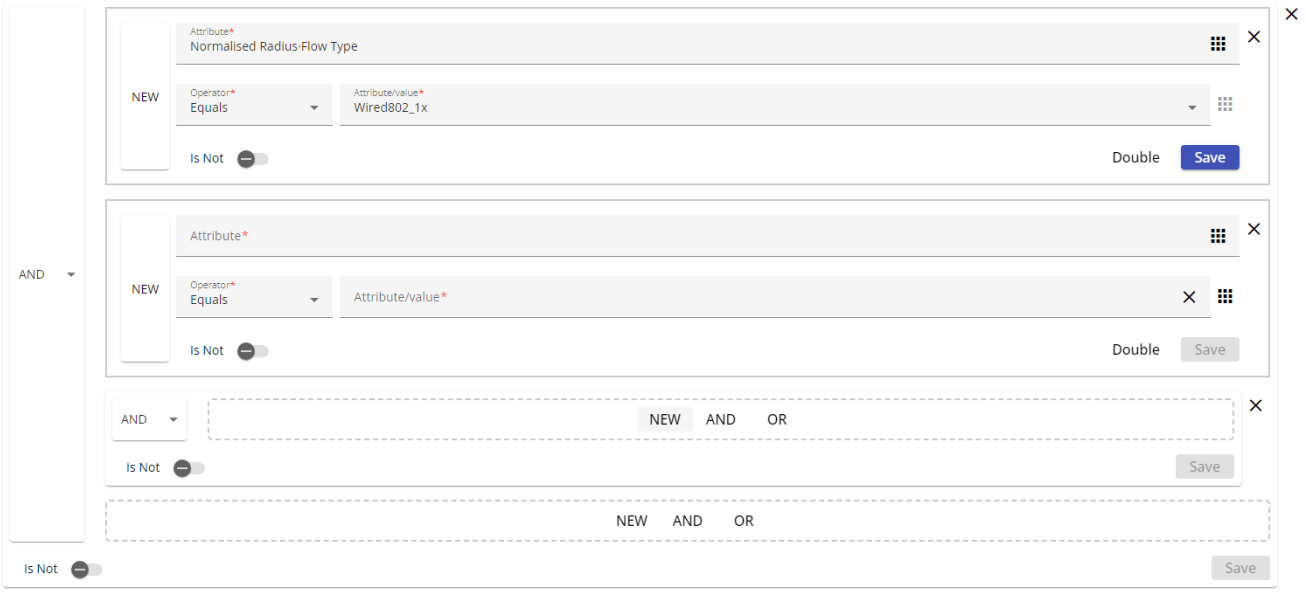

Figure 169. Condition containing nested rules

To save all conditions, click the "Save" button in the lower right corner.

Editing a logical condition

To edit a logical condition, you need to grab it with the cursor in the library and move it to the editor field.

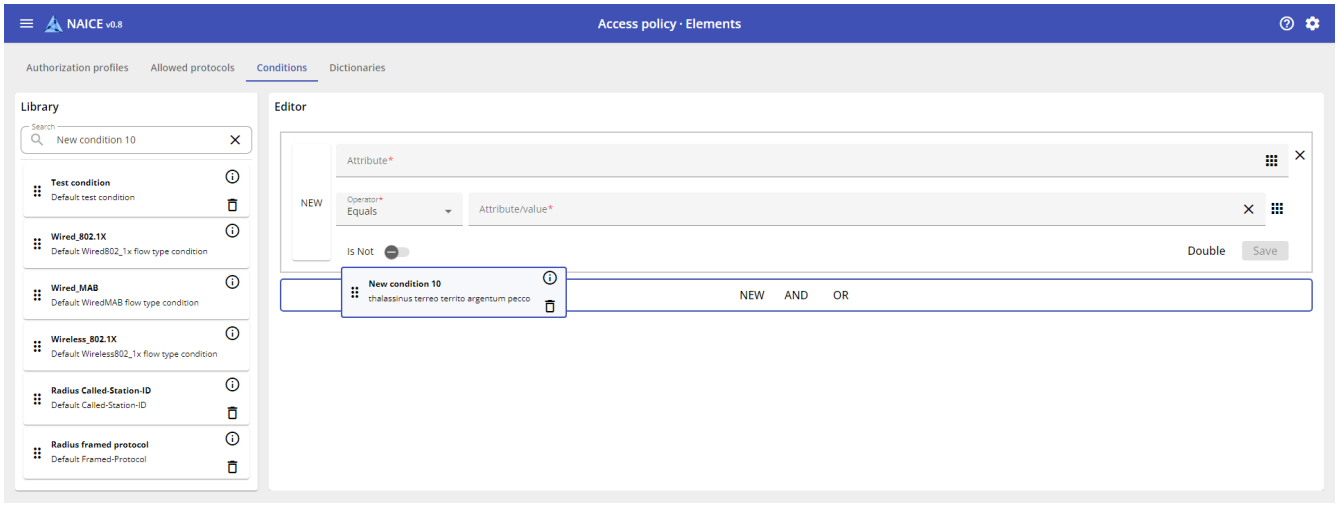

Figure 170. Selecting a logical condition

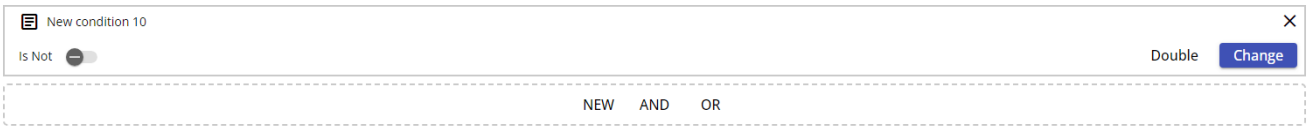

Figure 171. Editing a logical condition

To edit the condition, click the "Edit" button. After editing, click the "Save" button. Since the condition was previously saved in the library, by default it will be proposed to save it with the same name. If necessary, you can select another condition to be overwritten or select "Save to library as new condition." Click the "Save" button.

Also, during editing, you can drag conditions from the library into the child condition editor field.

Delete a logical condition

To delete a logical condition you need to find it in the library and click the button  at the right of the condition name.

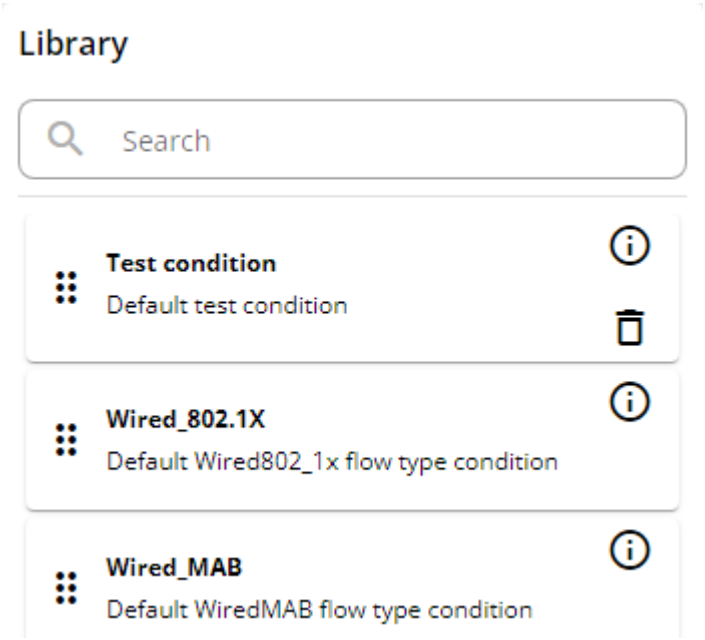

Figure 172. Selecting a condition to delete

Deletion requires confirmation of the action, for which a modal dialog will open. After explicit confirmation, the selected items will be deleted.

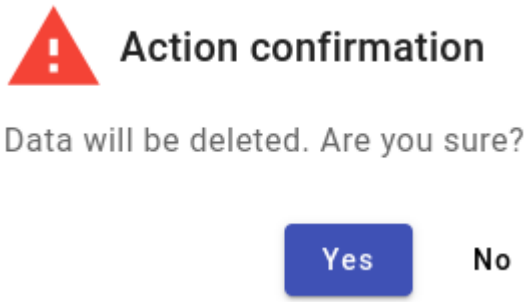

Figure 173. Modal dialog for confirmation

Restrictions:

- some system logical conditions cannot be deleted;
- you cannot delete logical conditions that are used in other complex logical conditions;
- You cannot delete logical conditions that are used in any set of policies.

Dictionaries

Description

The basic element when setting up logical condition are attributes grouped into dictionaries. In addition to basic and vendor-specific RADIUS attributes, NAICE allows the use of Non-RADIUS attributes, such as network device parameters (DEVICE dictionary) or user parameters (IDENTITY dictionary).

Dictionaries and attributes are available for viewing on a separate page. Adding new dictionaries or editing existing ones is not available.

If the dictionary you need is not added to the system, contact us using the "Make a wish" button, accessible from the navigation menu or the menu in the upper right part of the window.

View dictionaries

On the left side (with the heading "Dictionaries") there is a list of available dictionaries, on the right side - the contents of the selected dictionary (by default - the contents of the RADIUS dictionary):

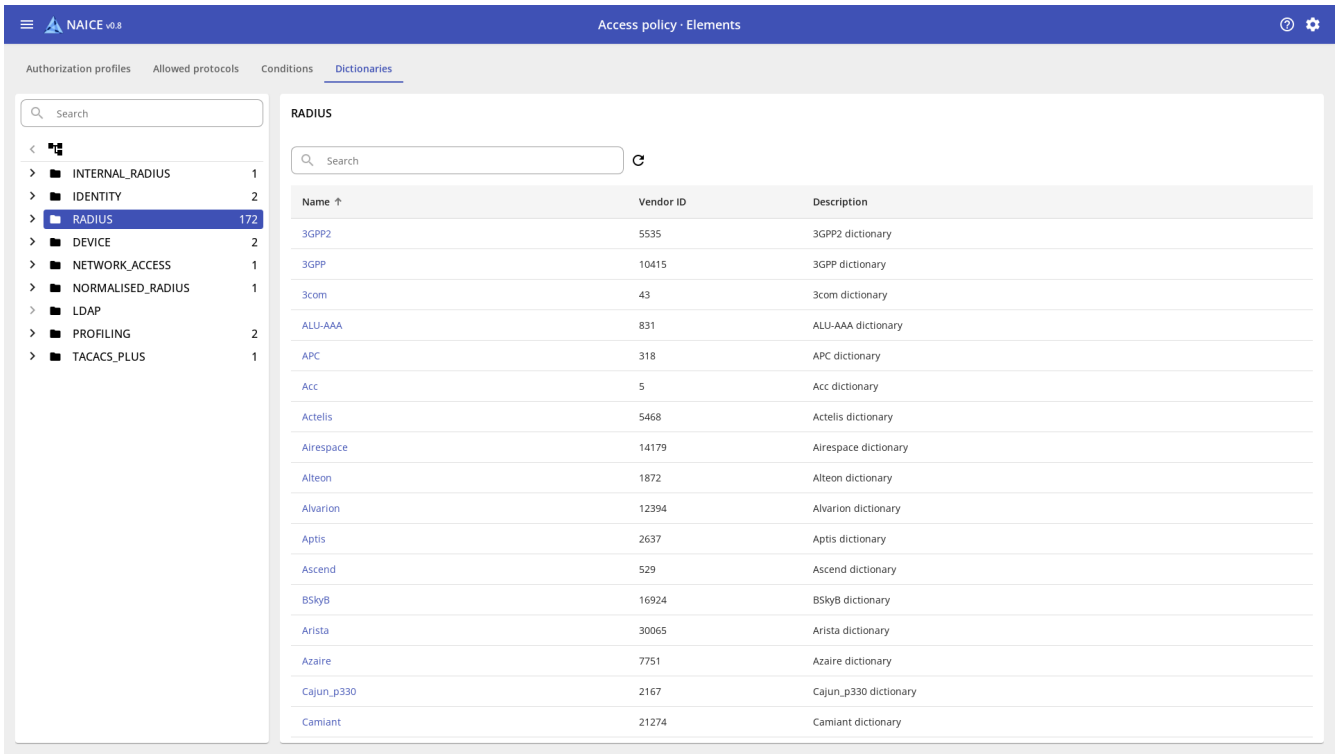

Figure 174. View dictionaries

Controls:

- › - Expand the list of nested dictionaries.
- `"Dictionaries. Search"` - Filtering by dictionary name.
- `"RADIUS. Search"` - Filtering by nested dictionaries and attributes.
- ↻ - Update the data
- ⊞ ☰ - Switch the display option for the dictionary navigation menu.

View nested dictionaries and attributes

To view information about an attribute, click on the attribute name in the attribute list:

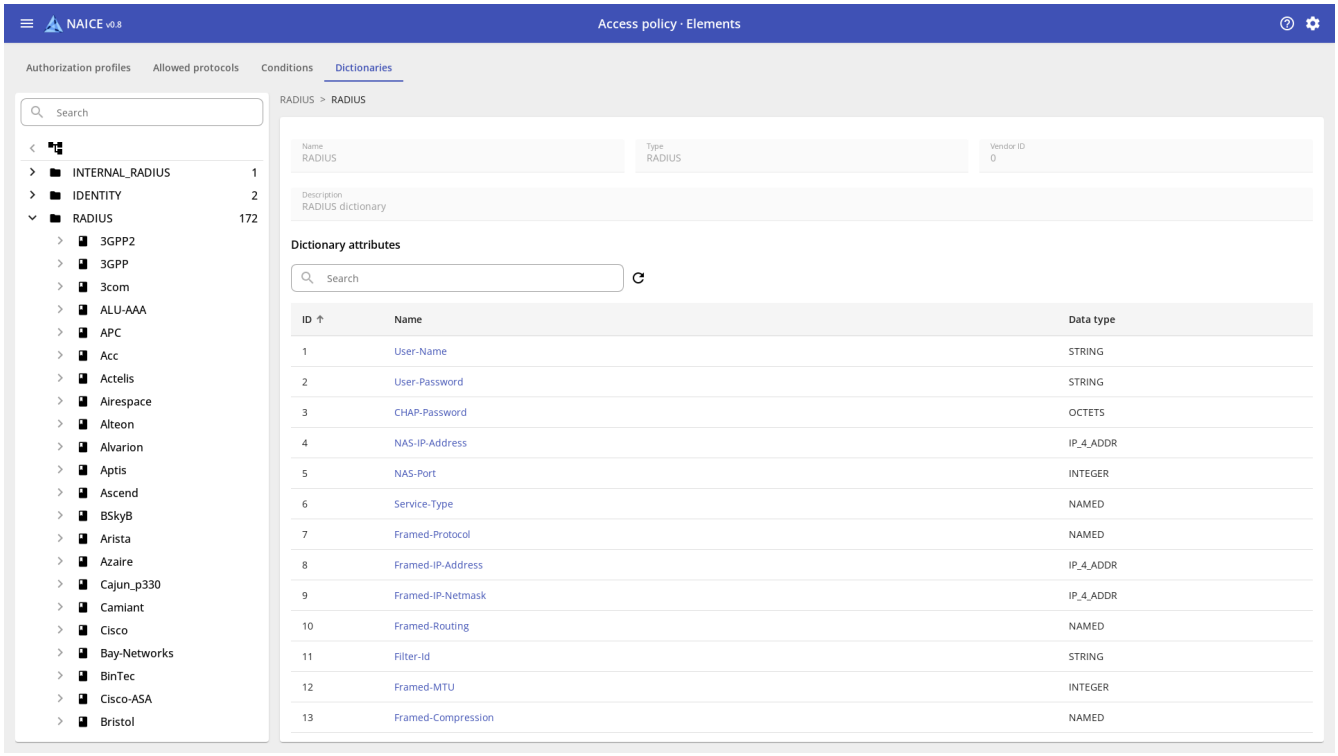

Figure 175. View attributes

To view information about an attribute, click its name:

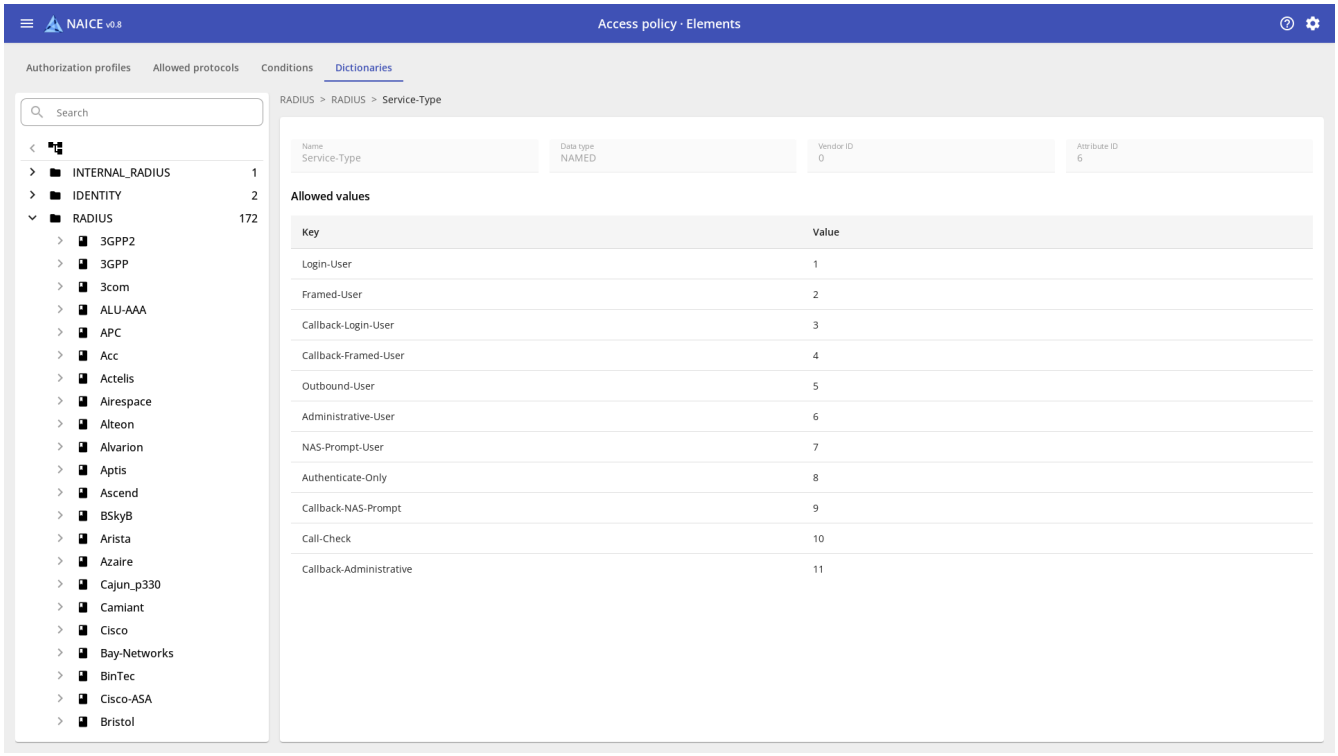

Figure 176. View information about an attribute

For attributes that have a finite list of valid values, this page will list a list of those values.

Policy sets

Description

Authentication and authorization policies define the actions that must be taken when receiving requests for user authentication from network devices via the RADIUS protocol and the actions when authorizing users.

Request processing order

The order of processing authentication/authorization requests from users transmitted by network devices is as follows:

1. Initial check of network device data:
    - Incoming RADIUS requests are analyzed for the presence of a `NAS-IP-Address` attribute - if missing, the packet is dropped and no response is returned.
    - The received `NAS-IP-Address` searched among records about ref:administration:network-resources/devices.adoc[network devices] - if missing, the packet is discarded and no response is returned.
    - The correctness of the secret in the RADIUS request is checked - if the secret is incorrect, `ACCESS-REJECT` is returned.
2. Processing in the policy table.
    - The RADIUS packet is checked for compliance with the logical conditions used in the policies.
    - The check is performed sequentially from top to bottom. Disabled policies are not included in the scan.
    - When a suitable policy is found, further search stops and checking continues within the framework of this policy.
    - If a policy with a suitable condition is not found, a response will be sent to the network device within the Default policy. By default, in this set of policies, the **DenyAccess** authorization profile is configured in the authorization policy, according to which ACCESS_REJECT will be sent to the network device. This behavior can be changed by editing the policies in Default.
3. Processing within the framework of the found policy:
    - The authentication protocol used is checked and compared with those available in the selected list of protocols. If no matches are found, an `ACCESS-REJECT` will be sent to the network device.
    - Authentication policies check from top to bottom until a matching condition is found. If no policy is found with a matching condition, an `ACCESS-REJECT` will be sent to the network device.
    - A search is performed for the user in the selected list of identity sequences.
    - Authorization policies check from top to bottom until a matching condition is found. If no policy is found with a matching condition, an `ACCESS-REJECT` will be sent to the network device using the Default rule. The default behavior can be overridden.
    - After defining the authorization policy, the user's password is checked. If it does not match, an `ACCESS-REJECT` will be sent to the network device.
    - After successful verification of the user's login/password, the attributes expected from the used authorization profile will be added to the response and the response will be sent to the network device. Both `ACCESS-ACCEPT` and `ACCESS-REJECT` responses can be configured in the authorization profile.

View a list of policy sets

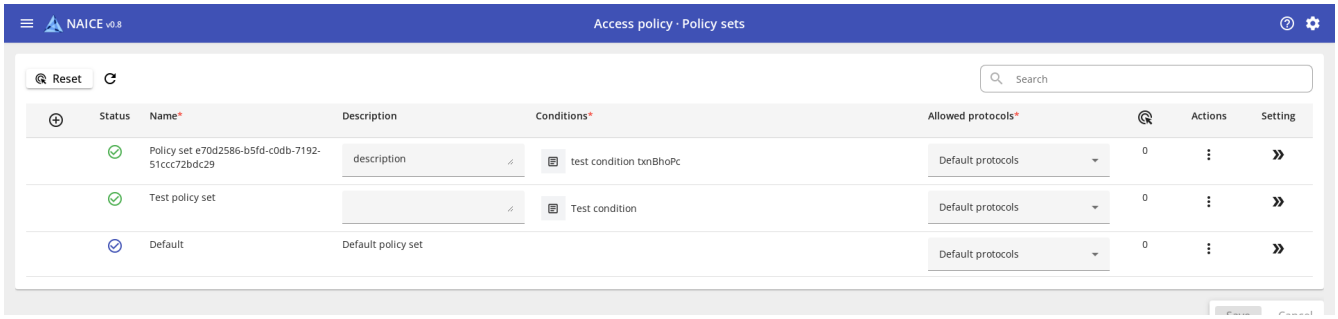

Figure 177. View all policy sets.

The table displays sets of policies in accordance with which authentication/authorization requests are processed.

> The last policy named `Default` cannot be deleted, nor can its name or condition be changed.
> It will always be the last one in the list, below which other policies cannot be placed.

Description of table columns:

- `Status` - status of the policy set (enabled / disabled / default).
- `Name` * - the name of the set of policies.
- `Description` - arbitrary description.
- `Conditions` * - used logical conditions. If a library condition is used, its name is displayed. If a non-library condition is used, its structure is displayed.
- `Allowed protocols` * - selected list of allowed protocols.
- - count of authorization attempts that fall under the specified Conditions.
- `Actions` - actions to add/remove a set of policies.
- `Setting` - switch to viewing and editing authentication/authorization policies of the selected set of policies.

Parameters marked with an asterisk * are required.

Controls:

- `Search` - case insensitive search by the name of a set of policies (found matches will be highlighted in yellow).
- - refresh data.
- **Reset** - reset the counters of RADIUS packets that were processed under this policy set for all policy sets.
- - add a policy (the policy will be added first in the list).
- - displays a counter of RADIUS packets that were processed according to this set of policies. By clicking on the counter value, the **Reset** button opens to reset the packet counters one at a time for

the selected set of policies.

- ⋮ - actions:
  - `Add on top` - add a set of policies *Before* the selected one;
  - `Add below` - add a set of policies *After* the selected one;
  - `Delete` - delete the selected set of policies.
- » - go to managing the authentication/authorization policies of the current set of policies.
- `Save` - save changes.
- `Cancel` - cancel changes.

All sets of policies are checked in order, as shown on the screen - from top to bottom. Therefore, ALL sets of policies are displayed on the page at once, and `Search` does not hide entries from the list, but only highlights them in yellow.

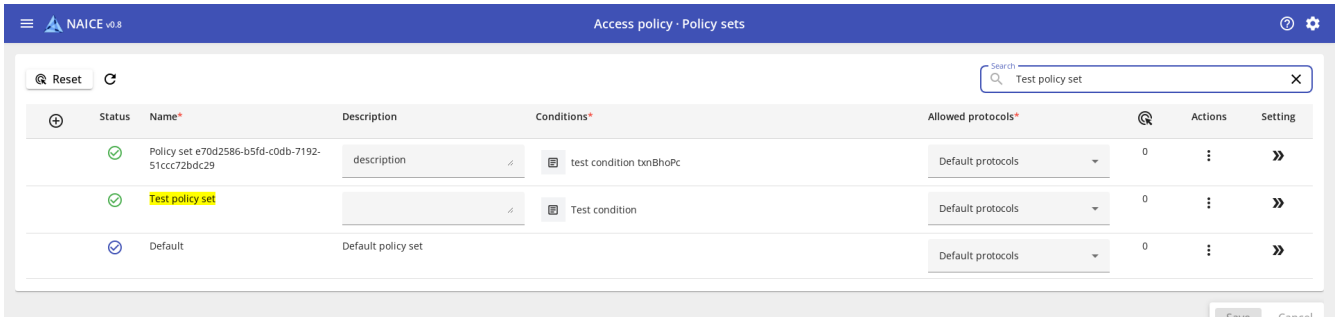

Figure 178. Search for policy set

To change the order, drag the policy by the ⠿ in the ⊕ column (becomes visible when you hover over this area).

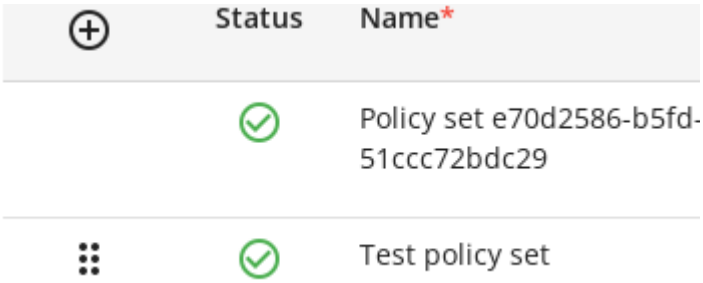

Figure 179. Change policy set order. Drag and drop action

After changing the order of policies, do not forget to click the `Save` button, otherwise the changes will not take effect.

To view the list of authentication and authorization policies, in the `Setting` column, click » to the right of the selected set of policies.

Editing a set of policies

To add a set of policies in the list of policy sets window, you can click the ⊕ button at the top left - the new set will be added first in the list.

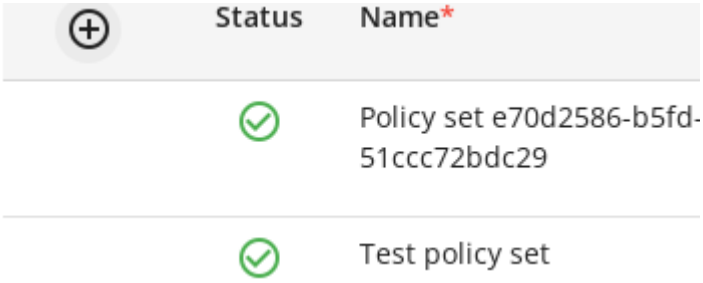

Figure 180. Display new policy. Add action.

If you need to add a set of policies to an arbitrary location, you must click on the button ⋮ to the right of the selected set of policies and select `Add on top` or `Add on bottom` in the drop-down menu.

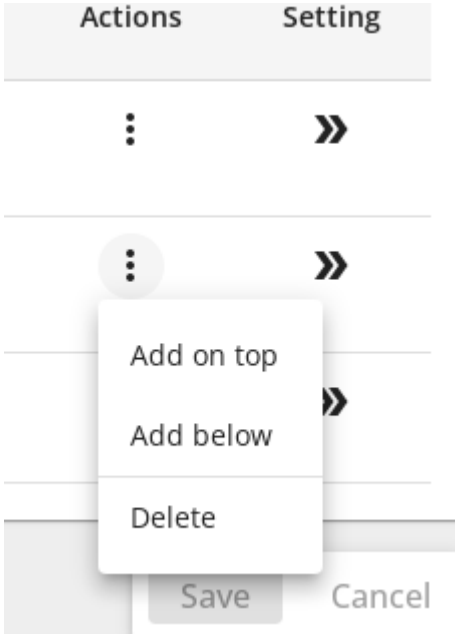

Figure 181. Display policy. Drop-down menus with actions.

Information on `Status`:

- `Enabled` - allows processing requests;
- `Disabled` - exclude from processing, don't check the Condition, don't process requests;
- `Monitor` - it is allowed to check the Condition (and increment the policy hits), process requests - no;
- `Default` - used only for the default policy.

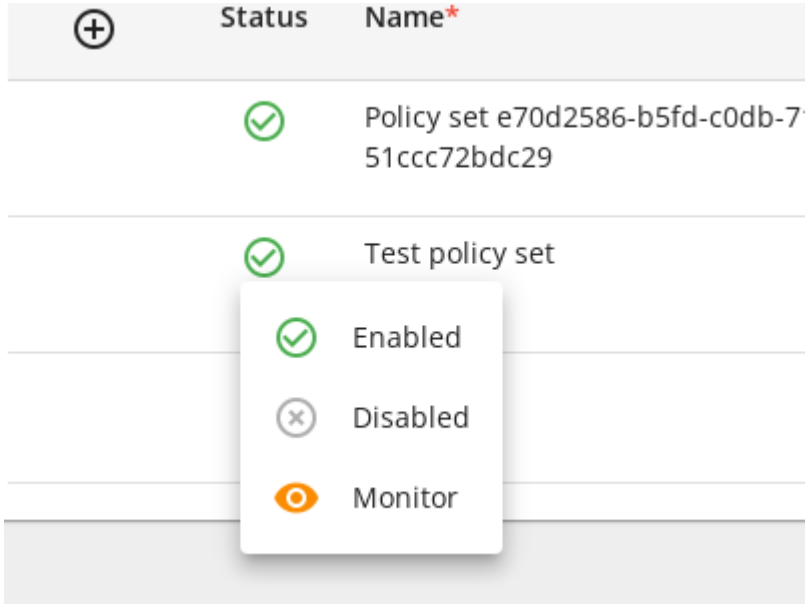

Figure 182. Change policy status.

In the newly created policy set, in the `Name` field, enter the name of the policy set or leave the automatically generated name unchanged.

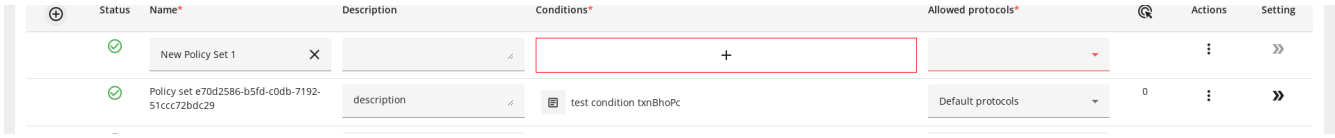

Figure 183. Displaying the new policy entry. Elements are required.

To edit a condition, click + and the condition editor will open.

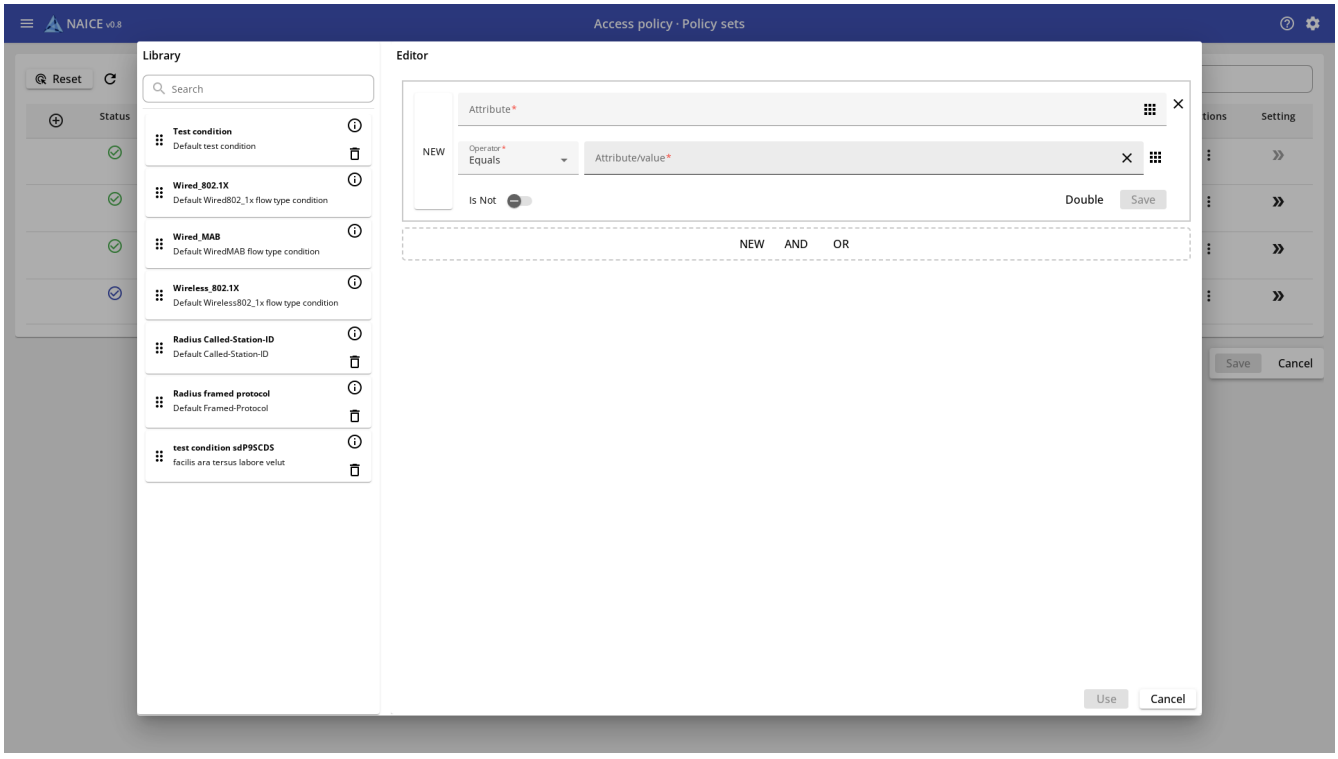

Figure 184. Conditions editor.

Editing conditions is done in the same way as described in conditions.

When setting up a policy, there is a limitation on the types of dictionaries used. You can use dictionaries: `DEVICE`, `RADIUS`, `NORMALISED_RADIUS`, `INTERNAL_RADIUS`. This is due to what information about the client connection can be obtained by the time the policy set is checked, and what information has not yet been obtained.

When editing conditions directly in the policy, the ability to use the configured condition without saving it in the **Library** is added. To do this, after setting, without saving the condition, click the `Use` button.

After that, in the `Available protocols` column, select the required list.

By clicking the **Save** button the files will be saved.

After creating a new policy, you must configure authentication and authorization policies for it; without this, all attempts to connect users that fall under the logical condition of this policy will be rejected!
To configure, go to Authentication and authorization policies.

Deleting a policy set

To delete policy set click on the ⚙ button and select the **Delete** action.

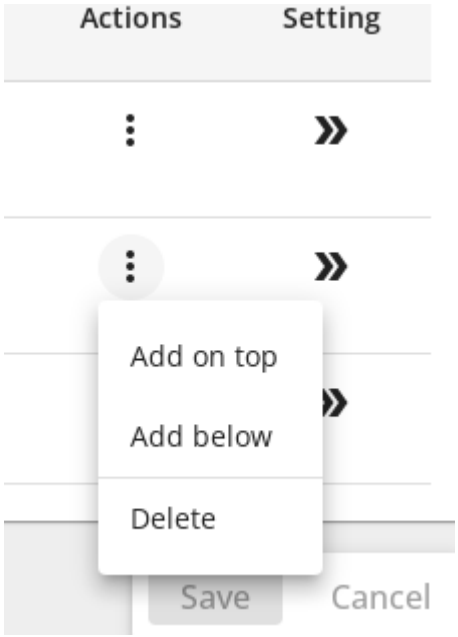

Figure 185. Drop-down menu for deletion of policy set

Deletion requires confirmation of the action, for which a modal dialog will open.
After explicit confirmation, the selected items will be deleted.

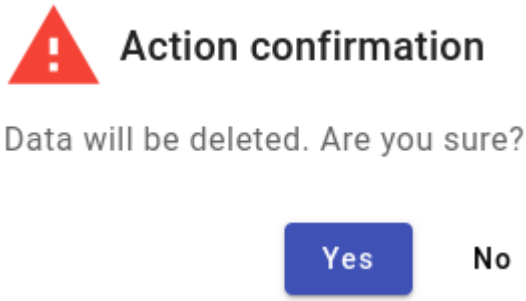

Figure 186. Modal dialog for confirmation

Policy hits count

The counters in the column show how many requests were processed using this policy. Changes in values indicate that the `Condition` is triggered; zero values, on the contrary, indicate that the received RADIUS requests do not correspond to the monitored condition.

Using the status `Monitor`, and observing the trigger counters, you can first select and debug the condition, and only then enable the policy to work, switching it to the status `Enabled`.

Authentication and authorization policies

View a list of authentication and authorization policies for the selected policy set

To view the list of authentication and authorization policies, in the `View` column, click » to the right of the selected policy set.

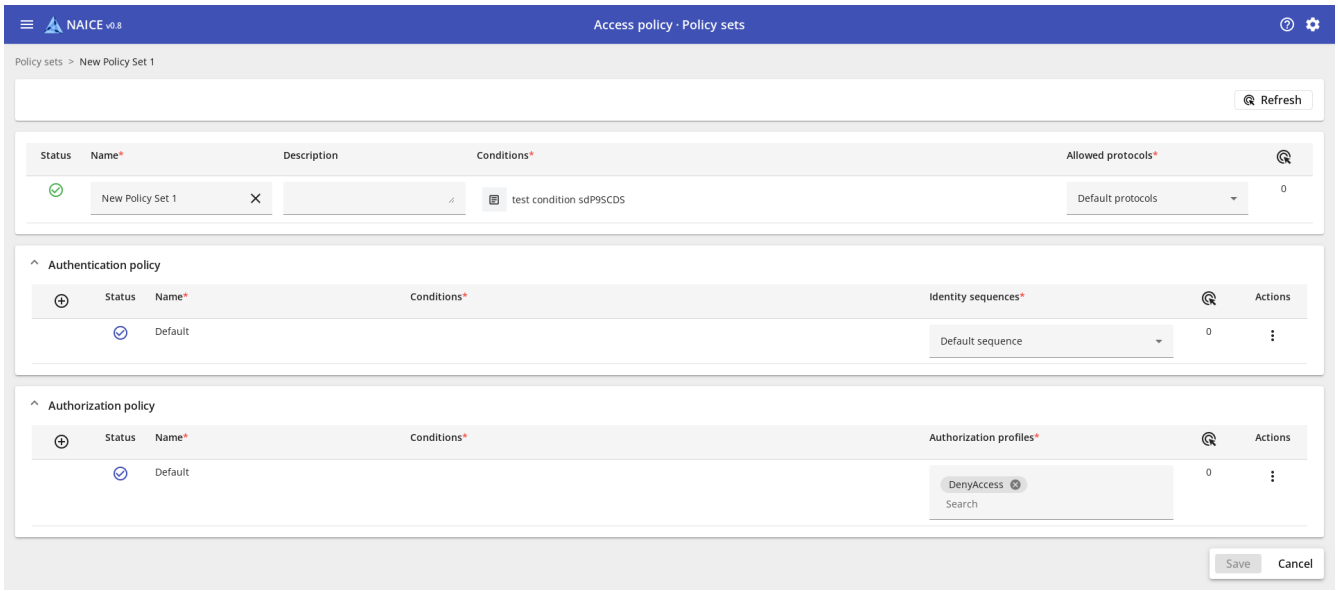

Figure 187. Policy et view and edition page.

The latest authentication and authorization policy rules named `Default` cannot be renamed or their trigger condition changed.
They will always be last in the list; other rules cannot be placed lower.
They will always "match" if none of the policies above are suitable.

The form for viewing a separate set of policies is divided into blocks:

- A block responsible for managing a set of policies, which displays the contents of the selected set of policies in a format similar to that used in Policy sets.
- **Authentication policy** - manages user authentication.
- **Authorization policy** - user authorization management.

Controls:

`Refresh` - request the current number of policies hits from the set.

- `Status` - enable, disable or monitor the policy.
- `Name` * - name of the policy.
- `Description` - arbitrary description.
- `Conditions` * - used logical conditions. If a library condition is used, its name is displayed. If a non-library condition is used, its structure is displayed.
- `Allowed protocols` * - selected list of allowed protocols.
- `Identity sequences` * - selected identity sequence.
- `Authorization profiles` * - selection of available authorization profiles.
- - the count of authorization attempts that fall under the specified Conditions. By clicking on the number of operations the counter can be **Reset**.
- `Save` - save changes.
- `Cancel` - cancel changes.

Parameters marked with an asterisk * are required.

To change the order of the Authentication and Authorization Policies, drag the policy by the element in the column (becomes visible when you hover over this area) similar to the Policy sets section.

Editing authentication and authorization policies

To edit, click to the right of the selected set of policies.

You must configure at least one authentication policy and one authorization policy for a client to successfully connect using this set of policies, otherwise the default deny rule will be applied.

The `Default` policy can be edited to set a different behavior, but for security it is recommended to configure your own rules with a narrower scope and leave the default behavior as deny.

Authentication Policy

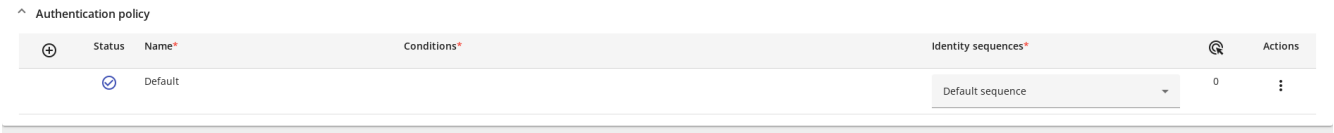

Figure 188. "Authentication" policies panel.

To configure the authentication policy in the **Authentication Policy** block, you must click the button . A new rule will appear.

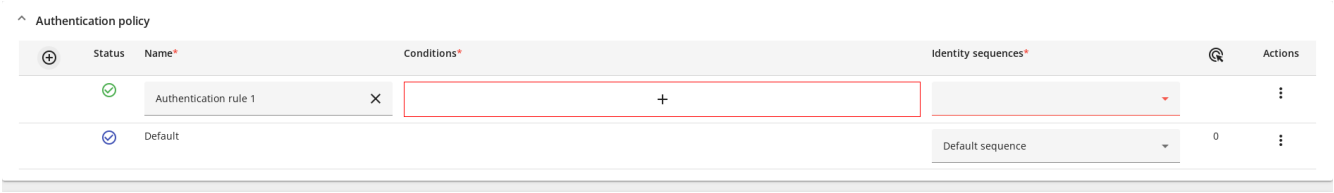

Figure 189. New "Authentication" policy.

In the `Name` field, enter the name of the policy.

To edit a condition, click + - the condition editor will open.

Editing conditions is performed in the same way as described in Conditions.

When setting up an authentication policy, there is a limitation on the types of dictionaries used. You can use dictionaries: `DEVICE`, `RADIUS`, `NORMALISED_RADIUS`, `INTERNAL_RADIUS`.

When editing conditions directly in the policy, the ability to use the configured condition without saving it in the library is added. To do this, after setting, without saving the condition, click the `Use` button.

In the `Identity sequences` drop-down menu, select the identity sequence.

Using the ⋮ button to the right of the policy, you can add a new one above or below, or delete the current one.

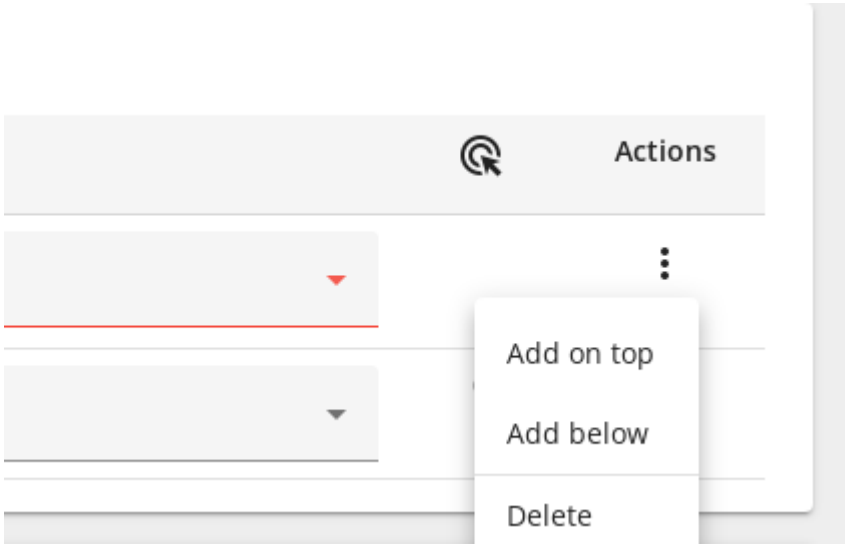

Figure 190. Authentication Policy. Dropdown Menus. Actions.

We can also change the policy status.

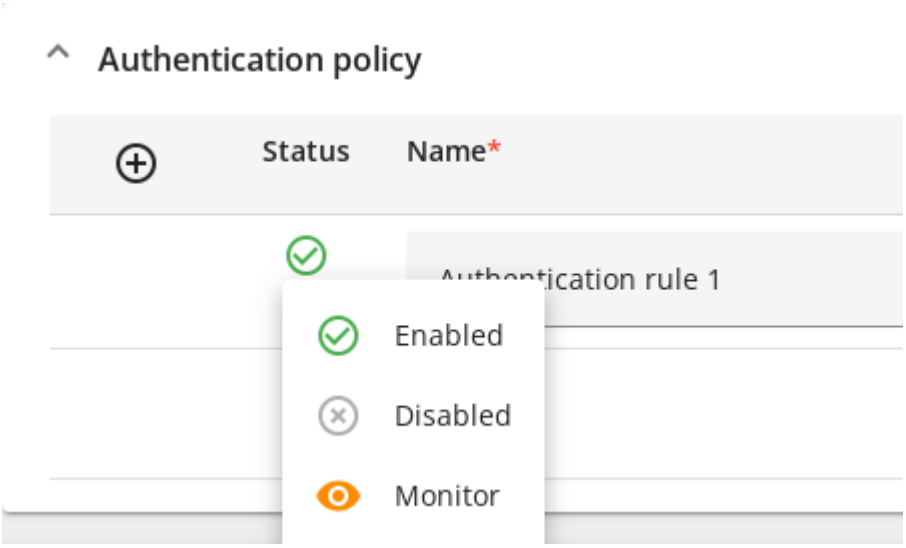

Figure 191. Authentication Policy. Change policy status.

Authorization Policy

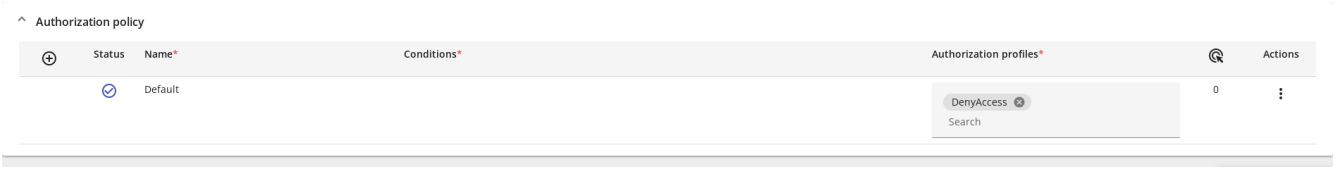

Figure 192. Policy panel "Authorizations".

To configure an authorization policy rule in the **Authorization Policies** block, click ⊕. A new rule will appear.

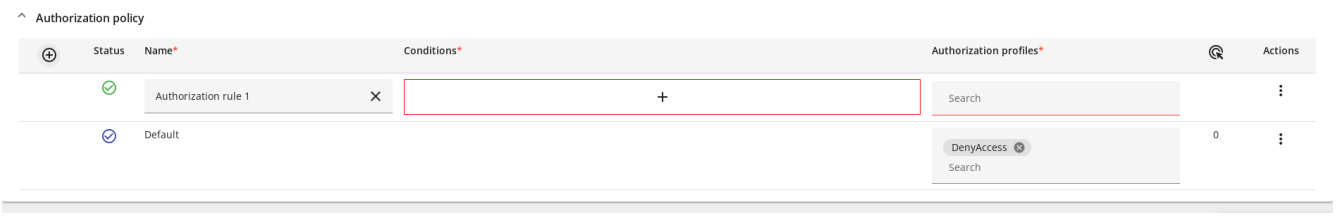

Figure 193. New "Authorization" policy.

In the `Name` field, enter the name of the policy.

To edit a condition, click + - the condition editor will open.

Editing conditions is performed in the same way as described in Conditions.

When setting up an authorization policy, you can use all types of dictionaries without restrictions.

When editing conditions directly in the policy, the ability to use the configured condition without saving it in the library is added. To do this, after setting, without saving the condition, click the `Use` button.

Select the required profile in the **Authorization profiles** drop-down menu. If necessary, you can add several profiles; their non-conflicting settings will be summed up.

Several Authorization Profiles can be linked to one Authorization Policy.
However, only those that match the current Device Profile will be considered when processing the request.

Using the ⋮ button to the right of the policy, you can add a new one above or below, or delete the current one.

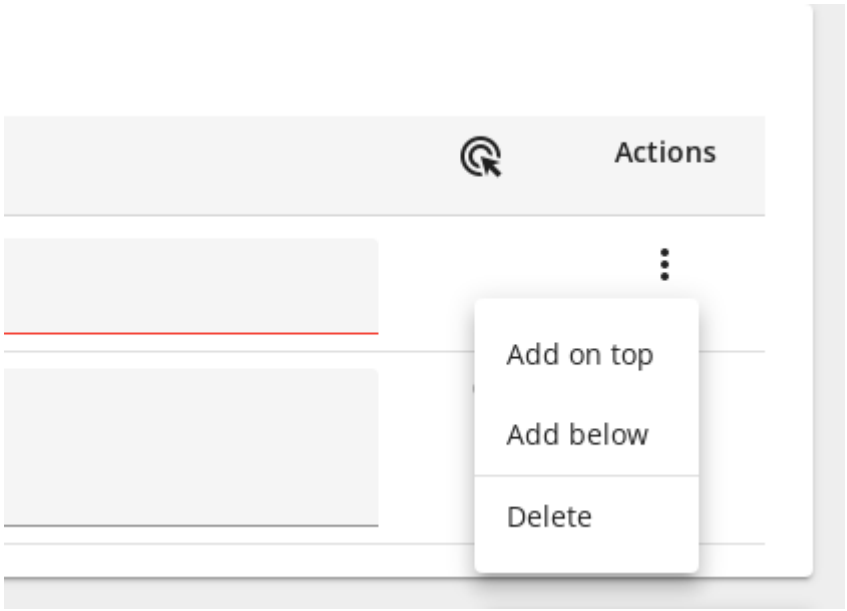

Figure 194. Authorization Policy. Dropdown Menus. Actions.

You can also change the status of a policy in a similar way to the statuses in policy sets.

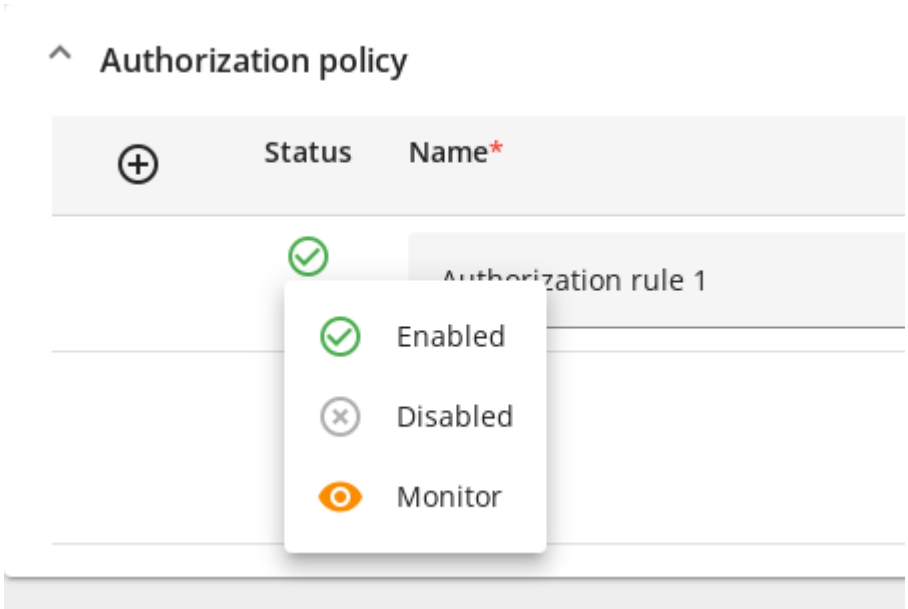

Figure 195. Authorization Policy. Change policy status.

The `Save` button will become available only after adding at least one fully configured authentication policy and authorization policy.

Click the `Save` button.

Editing policies

Policies are edited by clicking on the corresponding setting field.

After this, you need to click the `Save` button.

Deleting policies

To delete policy click on the ⋮ button and select the **Delete** action.

Deletion requires confirmation of the action, for which a modal dialog will open.
After explicit confirmation, the selected items will be deleted.

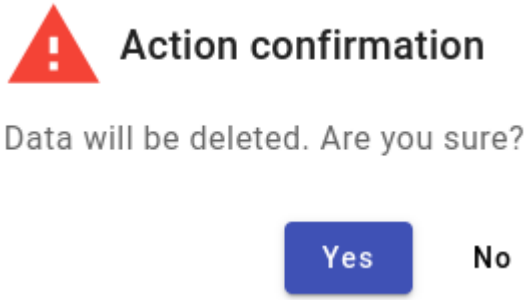

Figure 196. Modal dialog for confirmation

Profiling

Profiling is the process of dynamically detecting and classifying endpoints based on attributes obtained from various sources (probes). During profiling, collected attributes are matched to pre-created or user-defined conditions, which are then matched to profiles to assign them to an endpoint.

Contains sections:

- Profiling conditions - conditions defining how the collected attributes should be interpreted to classify the endpoint;
- Profiling policies - a set of rules that are used to automatically classify and control access to endpoints based on profiling results;
- Logical profiles - - combining certain profiling policies into a logical group for more convenient use in policy sets.

Profiling conditions

Description

Logical _profiling conditions _are the main elements used in profiling policies. They determine whether endpoint matches a certain attribute, based on which its type, model, manufacturer, operating system, and other attributes can be inferred.

The algebra of logic underlies the creation and processing of logical profiling conditions. The result of the condition is "True" or "False". Each profiling condition can contain only one attribute.

View a list of profiling conditions

This page contains a table listing all profiling conditions.

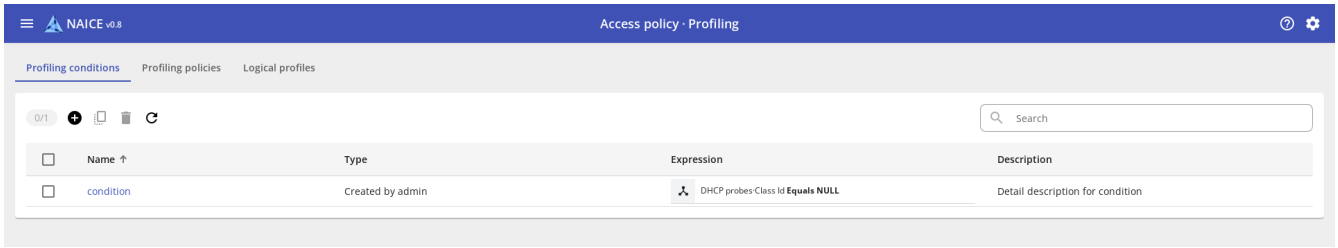

Figure 197. Profiling conditions table

The table contains columns:

- `Name` - name of profiling condition.
- `Type` - profiling condition type. Can be "System" or "Created by admin". System conditions are preset and cannot be deleted or changed.
- `Expression` - logical condition describing the criterion by which profiling will be performed.
- `Description` - arbitrary description of the profiling condition.

Sorting is only possible for the "Name" field in forward and reverse order. By default, sorting is performed in direct (alphabetical) order.

Controls:

- `Search` - Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.
- - Refresh table data.
- `0/1` - Counter of elements selected by the checkbox / total number of elements.
- - Add a new element.
- - Delete selected elements (inactive until at least one element is selected).
- - Change the current sort order.
- - Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).
- - Checkbox that is responsible for copying the selected element. Becomes active if only one item in the list is selected.

Adding a Profiling Condition

To add a profiling condition, click in the upper left part of the field above the table.

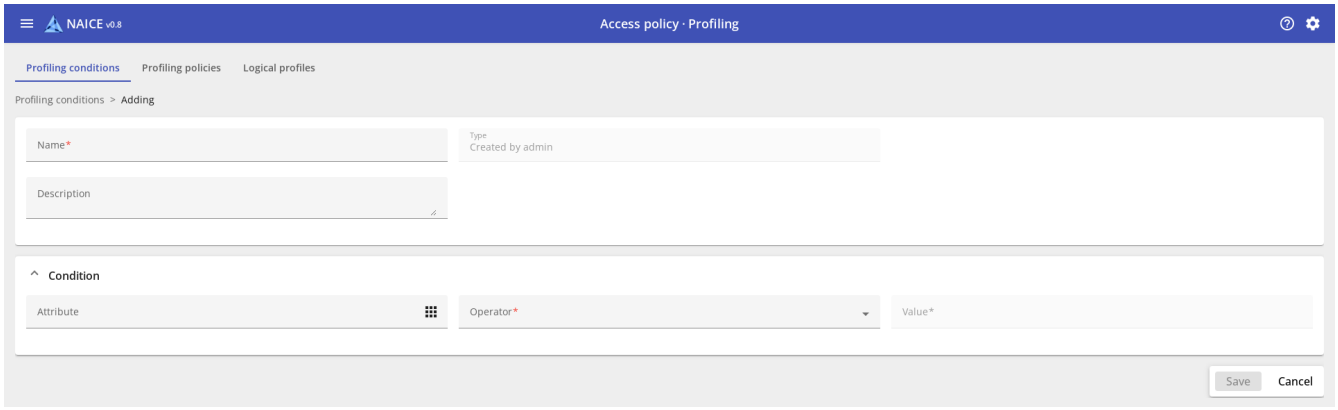

Figure 198. Profiling condition addition page

The page that opens contains the following parameters:

- `Name` * - Name of the profiling condition. Maximum login length is 100 characters.
- `Type` - Profiling condition type. Cannot be set and is always set to "Created by admin".
- `Description` - arbitrary description of the profiling condition. Maximum length - 200 characters.

Condition - block responsible for setting the profiling condition.

- `Attribute` * - at the click of a button a dictionary for adding an attribute will open in the left field.
- `Operator` * - selected logical condition operator. Can take values (depending on the attribute value type):
  - "Contains" / "Not contains"
  - "Ends with" / "Not ends with"
  - "Starts with" / "Not starts with"
  - "Equals" / "Not equals"
  - "Equals NULL" / "Not equals NULL"
  - "Matches" (*full* string match, case sensitive)
- `Value` * - value that is used to match the logical condition attribute in accordance with the selected operator. For an attribute that assumes predefined values, the value is selected from the list

Parametres marked with * is required.

Attribute selection menu

To select the attribute that will be used in the condition, click - the attribute selection menu will open.

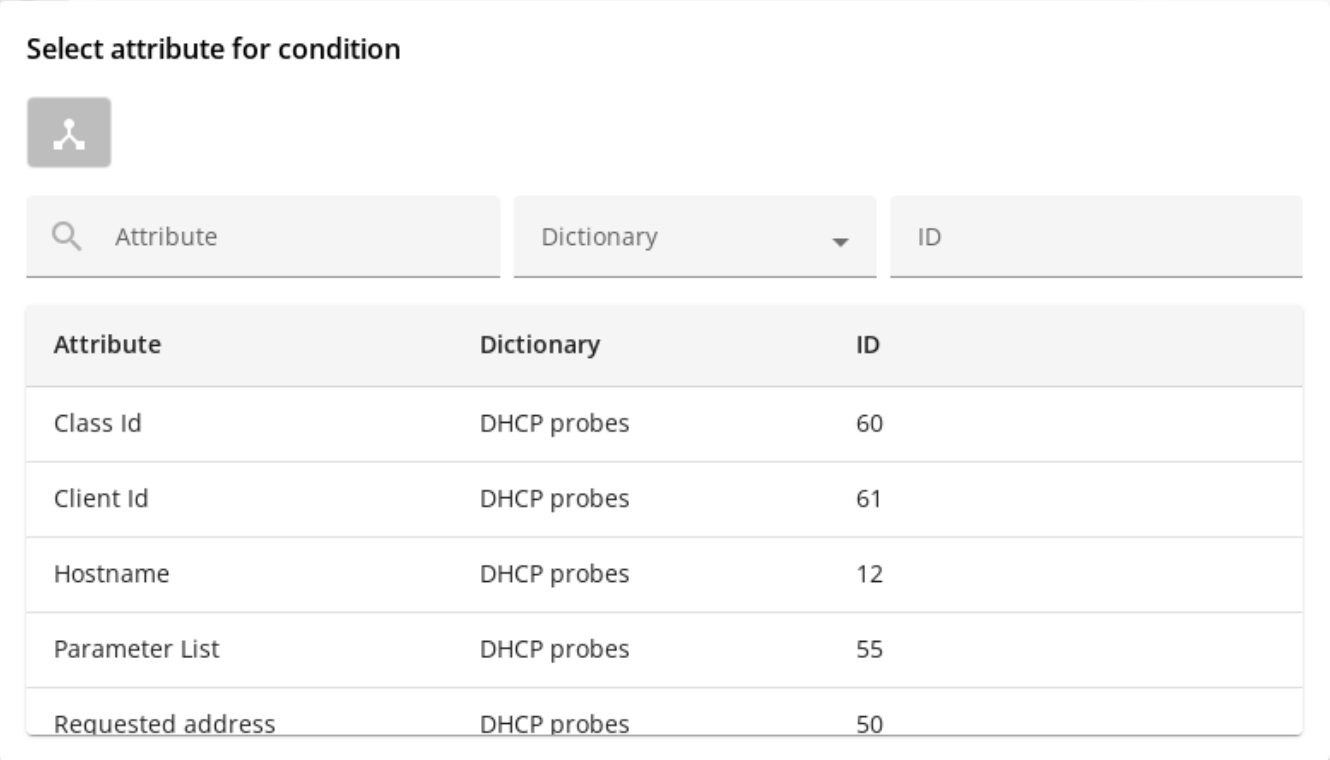

Figure 199. Attribute selection menu

Only attributes of dictionaries of the "PROFILING" type are available for selection. This type of dictionary is indicated by an icon .

At the top there is a list that allows you to filter attributes:

- `Attribute` - attribute name.
- `Dictionary` - the name of the dictionary, made in the form of a drop-down list. The "DHCP probes" and "MAC" dictionaries are available for selection. Also, available for selecting "Not selected" if you want to refuse filtering.
- `ID` - attribute ID (numeric value).

Editing a profiling condition

To edit a profiling condition, click on its name on the list page.

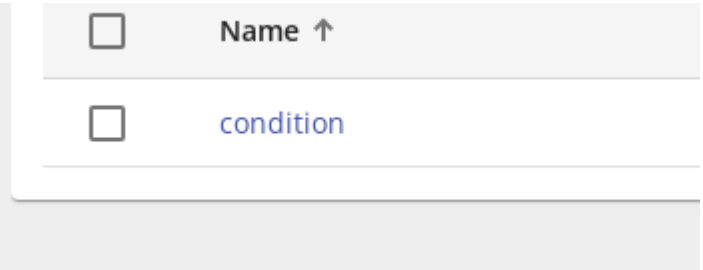

Figure 200. Hyperlink to profiling condition edition page

After this, the editing page will open.

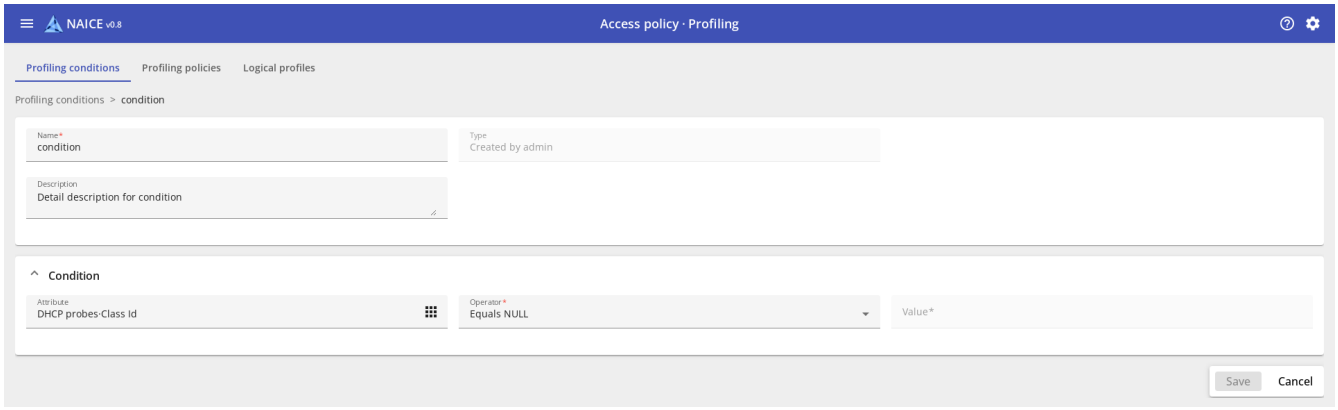

Figure 201. Profiling condition edition page

After editing, click on the "Save" button. The button remains inactive until at least one field is changed.

Copy profiling condition

A new profiling condition can be created based on an existing one.

To do this, select one of the existing conditions using the checkbox and click on . In the window for adding a condition that opens, all fields are filled with values from the selected condition. By default, "_copy" is added to the value in the `Name` field. You can choose any other name that is not already used in the system.

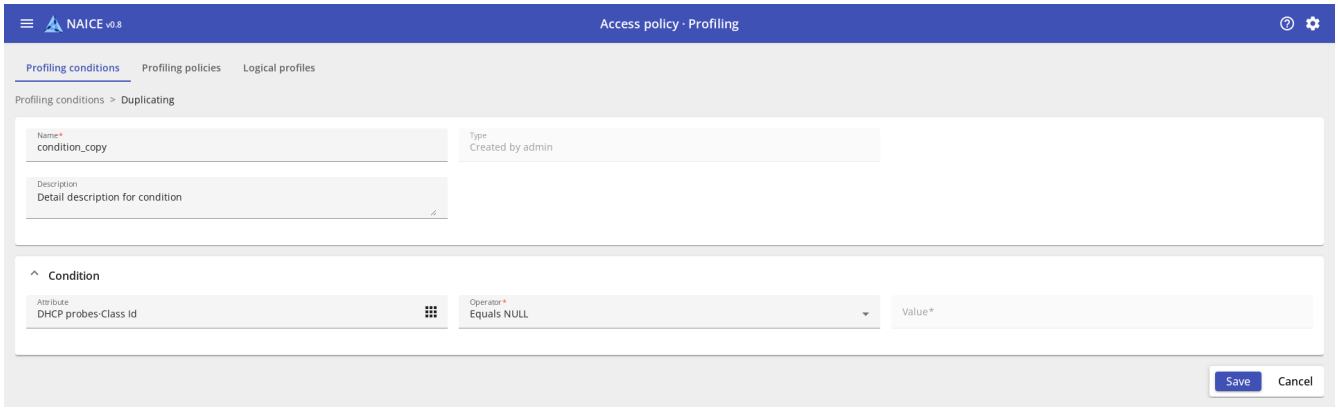

Figure 202. Profiling condition copy page

Once copied, the condition has no relation with the original condition. These conditions exist and work independently of each other. This is just filling out the fields at the time of adding.

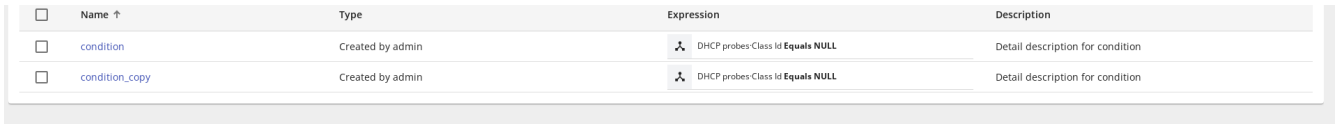

Figure 203. Profiling conditions table after condition copied

Deleting Profiling Conditions

To delete, in the list window, select the checkbox to the left of the name of the profiling conditions that you want to delete and click the button top left.

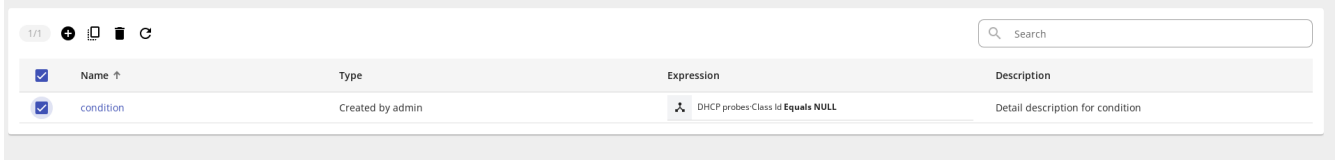

Figure 204. Selecting conditions for deletion

Deletion requires confirmation of the action, for which a modal dialog will open. After explicit confirmation, the selected items will be deleted.

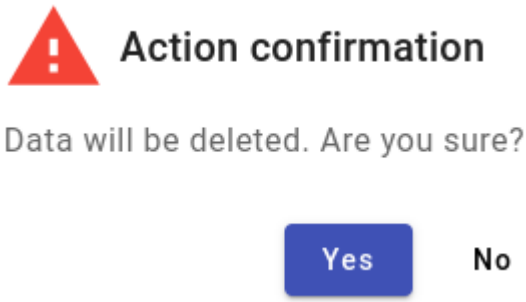

Figure 205. Modal dialog for confirmation

Restrictions:

You cannot delete a profiling condition that is already assigned to a profiling policy.

Profiling policies

Description

Profiling policies are designed to dynamically classify new and existing endpoints connected to the network. For classification, profiling conditions are used, based on which a profiling policy is defined and assigned to an endpoint. It can be used in authorization policy conditions to grant access in accordance with a specific policy. Also, based on the profiling policy, an endpoint is placed in a selected group of endpoints.

For example, based on profiling conditions, you can define an endpoint as a device of a certain type and manufacturer (for example, an Eltex IP phone), and configure an authorization policy to issue specific VLANs and ACLs to these devices.

The process of defining and assigning a profiling policy to an endpoint according to the conditions defined for it in the policy is called "Endpoint Profiling".

For endpoints that have a manually assigned “Profiling Policy” or “Endpoint Group” these values cannot be changed based on the results of profiling.

View profiling policies

This page allows you to view and manage profiling policies. Profiling policies have a hierarchical structure, which is necessary for grouping endpoints.

The left part of the window contains a tree of profiling policies, in which you can select a policy to view or edit.

The right part of the window displays a form for creating/editing a profiling policy. If the `All policies` item is selected in the tree, a table with a list of all profiling policies is displayed in the right part of the window.

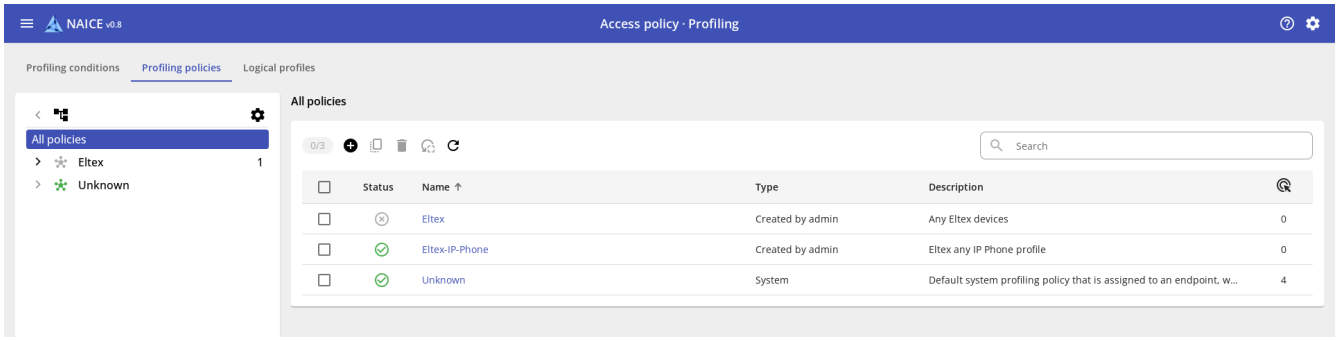

Figure 206. View profiling policies.

View a tree or list of profiling policies

The profiling policy tree is located on the left side and displays a list of profiling policies in the form of a tree structure or as a list of child profiling policies of the selected node - the display method can be switched, the default display is in the form of a tree structure.

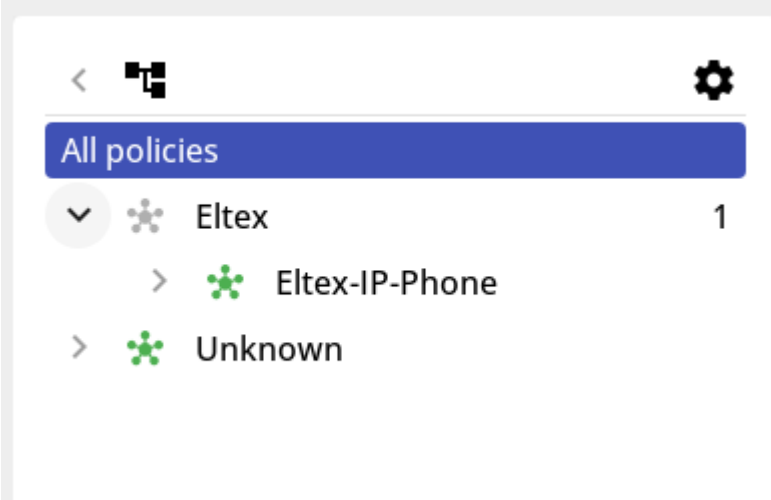

Figure 207. Tree of profiling policies.

Contains the following control elements:

- - display mode in the form of a tree structure of profiling policies (to switch the mode to the opposite, click on the icon).
- - display mode in the form of a list of child profiling policies (to switch the mode to the opposite, click on the icon).
- - adding/duplicating/deleting a policy. The selection of available actions depends on the selected item in the policy tree.
- - moving to a higher level from the current policy (active only in the list of child policies mode, when you are in a child policy).
- - in tree structure mode, displayed to the left of the profiling policy name if the list is closed. Inactive if there are no child elements. In list mode, displayed to the right of the profiling policy name that has child elements.
- - in tree structure mode it is displayed to the left of the name of policies that have child elements, if list is expanded.
- - element for designating a profiling policy.

`All policies` - title of the list of policies. When you select this element, a “flat” list of all profiling policies will be displayed on the right side of the window. Selected by default when you go to the profiling policies page.

`Unknown` is a system profiling policy that is used to profile endpoints that are not covered by other profiling policies. Cannot be edited. You also cannot create child policies for it.

View a list of profiling policies

A list of all profiling policies is displayed on the right side of the page in the form of a table if the "All policies" item is selected in the profiling policies tree.

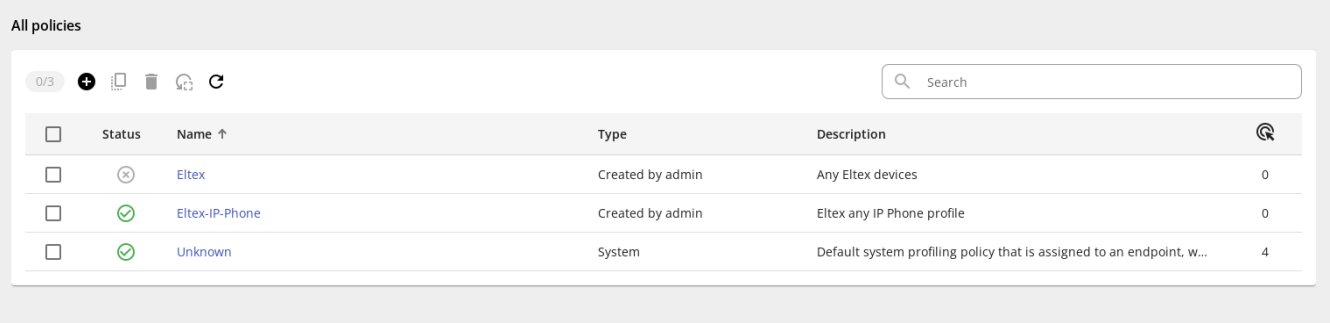

Figure 208. Table listing all profiling policies.

The table contains columns:

- `Status` - current status of the profiling policy: displays the icon whether it is on or off.
- `Name` - name of the profiling policy.
- `Type` - type of profiling policy. The possible value is "Created by admin" or "System".
- `Description` - description of the profiling policy.
- - the count of checks for endpoint compliance with the profiling policy.

Sorting is possible only for the “Status” and “Name” fields in forward and reverse order. By default, sorting is performed in direct (alphabetical) order by the "Name" field.

Controls:

- `Search` - Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.
- - Refresh table data.
- `0/1` - Counter of elements selected by the checkbox / total number of elements.
- - Add a new element.
- - Delete selected elements (inactive until at least one element is selected).
- - Change the current sort order.
- - Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).
-

- Checkbox that is responsible for copying the selected element. Becomes active if only one item in the list is selected.

- - Reset the counter of hits in the profiling policy. Becomes active if at least one item in the list is selected and the count of hits under the policy is greater than 0.

> The order of profiling policies is extremely important!
> The profiling policies are accessed to check if the endpoint matches the profiling policy from the top to the bottom of the list.

Adding a profiling policy

There are two ways to add a profiling policy:

- via the profiling policy tree: click the icon above the tree and select "Add root policy" if the "All policies" item is selected, or "Add child policy" if a profiling policy is selected.

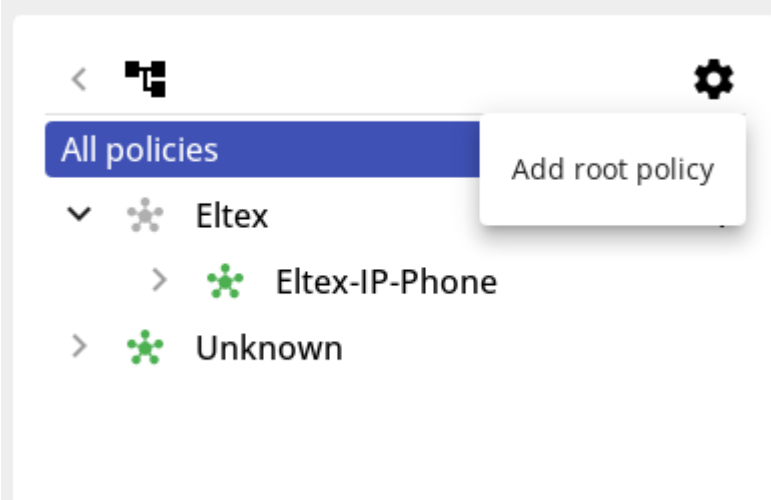

Figure 209. Adding a profiling policy. Actions.

- via the profiling policy table: click the icon in the upper left part of the field above the table.

> If you select a policy using the checkbox and then click the create icon, it will become the parent of the new policy.

> For the system profiling policy "Unknown", adding child policies is prohibited.

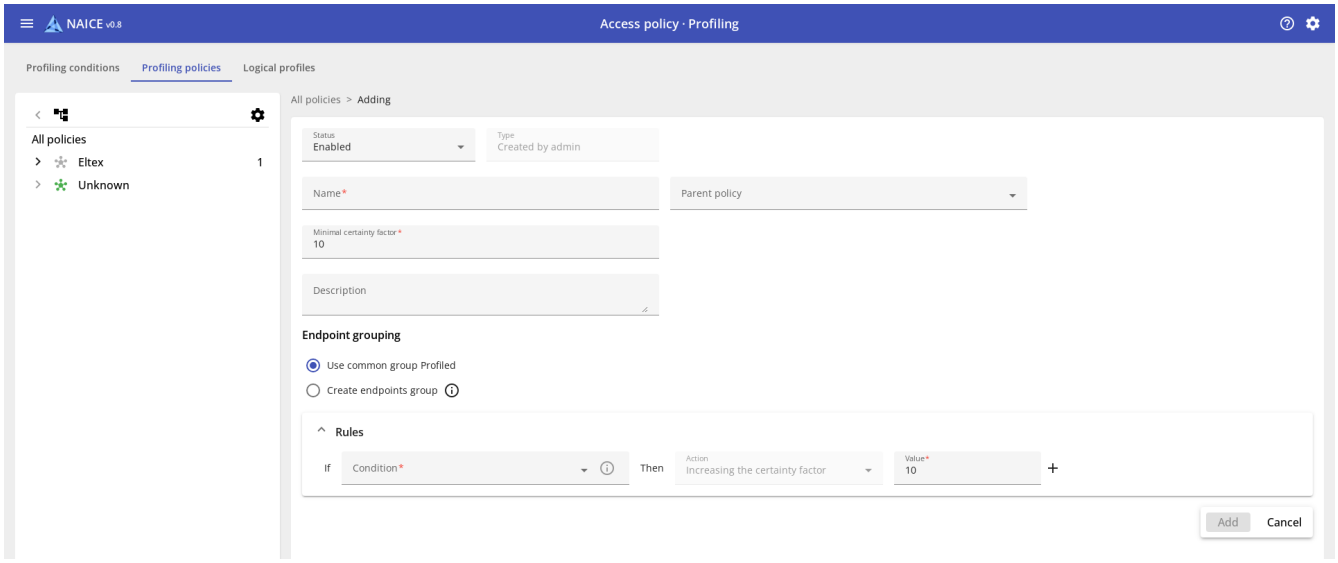

Figure 210. Adding a profiling policy.

As a result, the policy editing section will open on the right side of the page, containing the following parameters:

- `Status` - status of profiling policies. Can take the values "Enabled" and "Disabled". The default value is "Enabled".
- `Type` - type of profiling policy. All manually created profiling policies are set to "Created by an administrator" and cannot be changed.
- `Name` * - name of the profiling policy. Maximum length is 100 characters.
- `Parent policy` - parental profiling policy. You can select a parent profiling policy from the drop-down list or select nothing to create a root profiling policy. When creating a profiling policy from the policy tree by selecting "Add child policy", the profiling policy selected in the tree will be automatically substituted, which can be changed if necessary.
- `Minimal certainty factor` * - the minimum number of points that must be achieved in the rules for a policy to be considered suitable. Cannot be greater than the sum of the values of all trust levels configured in the Rules section. Can take values from 1 to 65535.
- `Description` - arbitrary description of the profiling policy condition. Maximum length is 200 characters.
- **Endpoint grouping** - section that defines the principle of grouping endpoints.
  The following values can be selected:
  - `Use common group Profiled` - this choice is available and displayed only for the root profiling policy. Endpoints classified as belonging to this profiling policy will be placed in the "Profiled" system endpoint group.
  - `Use parent policy endpoint group` - this choice is available and displayed only for child profiling policies. Endpoints classified as belonging to this profiling policy will be placed in the group specified in the parent policy. If no groups are specified for parent policies, the endpoints will be placed in the "Profiled" group.
  - `Create endpoints group` - automatically create a group of endpoints using the name of the profiling policy. Endpoints classified as belonging to a given profiling policy will be placed in this group.
-

Rules - section of the rules responsible for setting up the classification of endpoints using profiling conditions. Contains parameters:

- `Condition` * - menu for selecting profiling conditions.
- `Value` * - the value of points that will be assigned to the endpoint if the profiling condition matches.
- + - the icon is located to the right of the profiling condition. Clicking this icon below will add a new profiling condition.

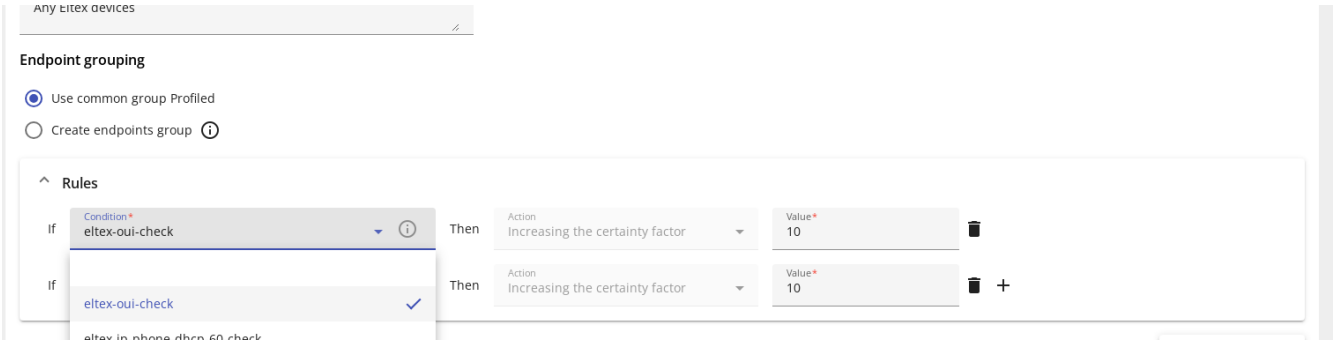

Figure 211. Adding rules to a profiling policy

Parameters marked with an asterisk * are required.

A profiling policy must contain at least one rule.

Multiple rules can be added for one profiling policy.

Adding the same rule several times is meaningless and therefore prohibited.

To add a policy, click the `Add` button. The button will become active after all required fields of the profiling policy are filled in.

Principle of checking endpoint compliance with profiling policy

When profiling an endpoint, the following actions are performed:

- For the first profiling condition specified in the profiling policy rules, a check is performed on the endpoint compliance with the specified condition:
  - If the endpoint complies with the profiling condition, the value corresponding to the rule is added to the current certainty factor;
  - If the endpoint does not comply with the condition, the certainty factor remains unchanged.
- The action is repeated for each rule in the policy.
- When the endpoint has been checked for compliance with all the rules of the policy, the total certainty factor is compared with the minimal certainty factor of the policy:
  - If the total certainty factor is equal to or greater than the minimal certainty factor, the endpoint complies with the profiling policy;

If the total certainty factor is less than the minimal, the endpoint does not comply with the profiling policy.

- Since the policies are nested, the tree is traversed in depth:
  - We search for the first matching root policy.
  - If the root policy has child policies, we traverse them for a match.
  - We return the "deepest" policy from the tree.
  - As soon as one of the policies of the current level matches, the traversal of this level stops, the search continues only among the child policies.

Editing a profiling policy

Editing the profiling policy is possible in two ways:

- Select a profiling policy in the policy tree on the left and click on it - an editing form will open on the right side.
- In the list of all policies in the “Name” column, click on the name of the policy - you will be taken to the form for editing this policy.

After a profiling policy is added, the `Policy hits count` field and the `Reset count` control are added inside its detail information.

- `Policy hits count` - the count of checks for endpoint compliance with the profiling policy.
-  - reset the counter of profiling policy hits. Becomes active if the count of hits under the policy is greater than 0.

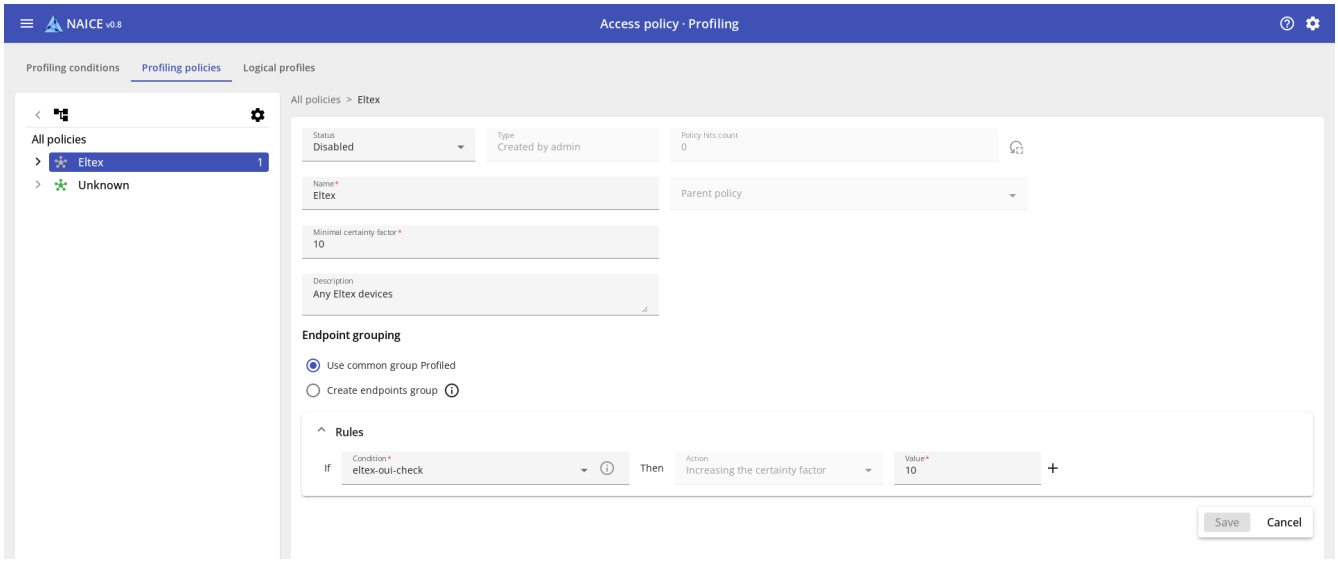

Figure 212. Editing a profiling policy.

After editing, click on the "Save" button. The button remains inactive until at least one field is changed.

Copying profiling policies

A new profiling policy can be created based on an existing one. This can be done in two ways:

-

In the policy tree, select one of the existing profiling policies and click the icon . In the list of available actions, select menu "Duplicate policy".

- In the list of all policies, select one of the existing profiling policies and click the icon .

> The action is not available if more than one policy or "Unknown" is selected.

In the added policies tab that opens, all fields will be filled with values from the selected policy. By default, "_copy" is added to the value in the `Name` field. You can choose any other name that is not already used in the system.

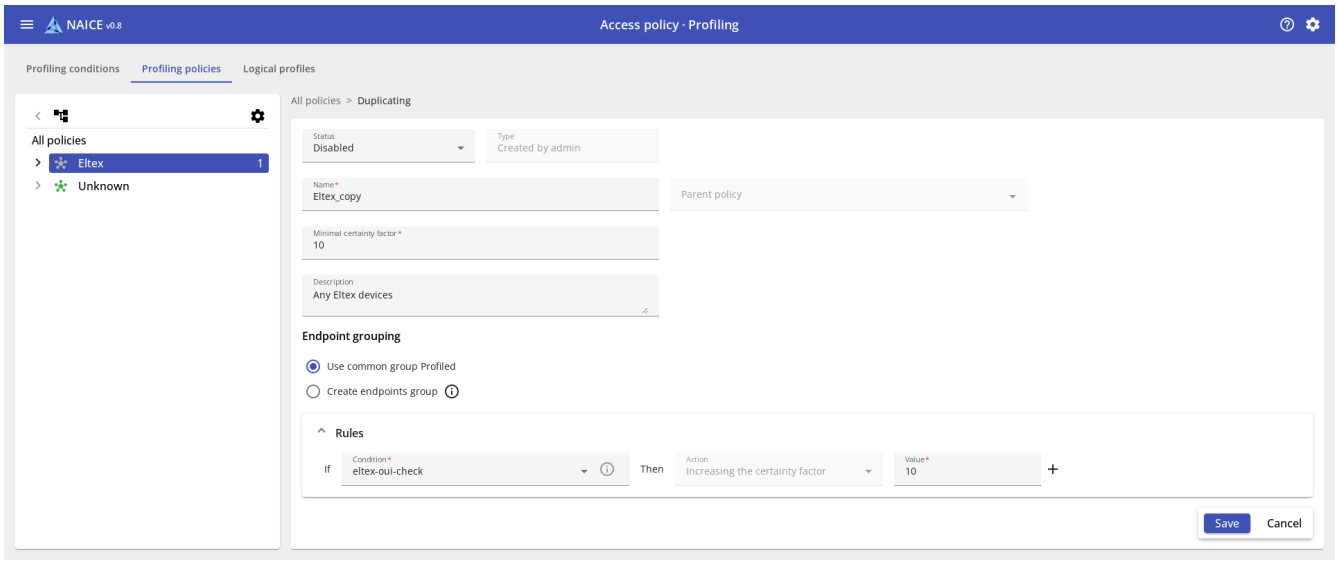

Figure 213. Copying profiling policy.

Once copied, the profiling policy has no connection with the original one. These profiling policies exist and work independently of each other - the original one is used to fill in the fields of the new one at the time of adding.

Removing profiling policies

Deleting profiling policies is possible in the policy tree on the left and in the list of all policies on the right.

- To delete profiling policies in the tree, you need to select the policy and click on the icon . In the list of available actions, select "Delete policy". In the policy tree, you can delete only one profiling policy.
- To delete in the window with a list of all policies, select the checkbox to the left of the name of the profiling policies that you want to delete, and click the button at the top left. You can select multiple profiling policies for deletion.

> Deletion requires confirmation of the action, for which a modal dialog will open.
> After explicit confirmation, the selected items will be deleted.

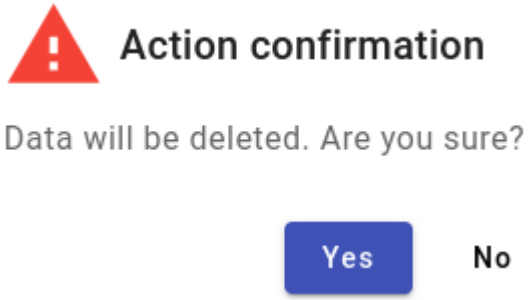

Figure 214. Modal dialog for confirmation

Restrictions:

- You cannot delete a profiling policy that is used in any logical profile.
- You cannot delete a profiling policy that is used in any logical condition or authorization policy condition.
- The system profiling policy "Unknown" cannot be deleted.

Logical profiles

Description

Logical profiles combine core profiling policy into a form that can be used as the basis for authorization policy, allowing for a simpler structure and fewer rules in view. For example, the logical profile "Printers" may contain profiling policies "HP Printers", "Xerox Printers" and "Canon Printers". A single profiling policy can consist of several different logical profiles.

Viewing Logical Profiles

This page contains a table listing all logical profiles.

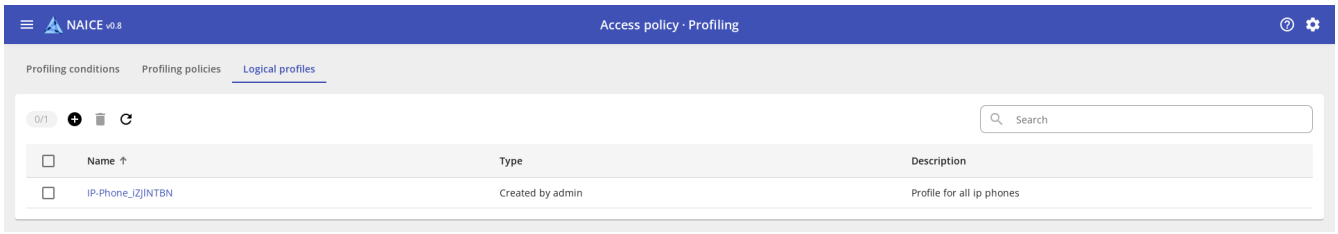

Figure 215. Logical profiles table

The table contains columns:

- `Name` - name of the logical profile.
- `Type` - type of logical profile. Can be "System" or "Created by admin". System conditions are preset and cannot be deleted or changed.
- `Description` - arbitrary description of the logical profile.

Sorting is only possible for the "Name" field in forward and reverse order. By default, sorting is performed in direct (alphabetical) order.

Controls:

-

`Search` - Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.

- - Refresh table data.
- `0/1` - Counter of elements selected by the checkbox / total number of elements.
- - Add a new element.
- - Delete selected elements (inactive until at least one element is selected).
- - Change the current sort order.
- - Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).

Adding a logical profile

To add a logical profile, click in the upper left part of the field above the table.

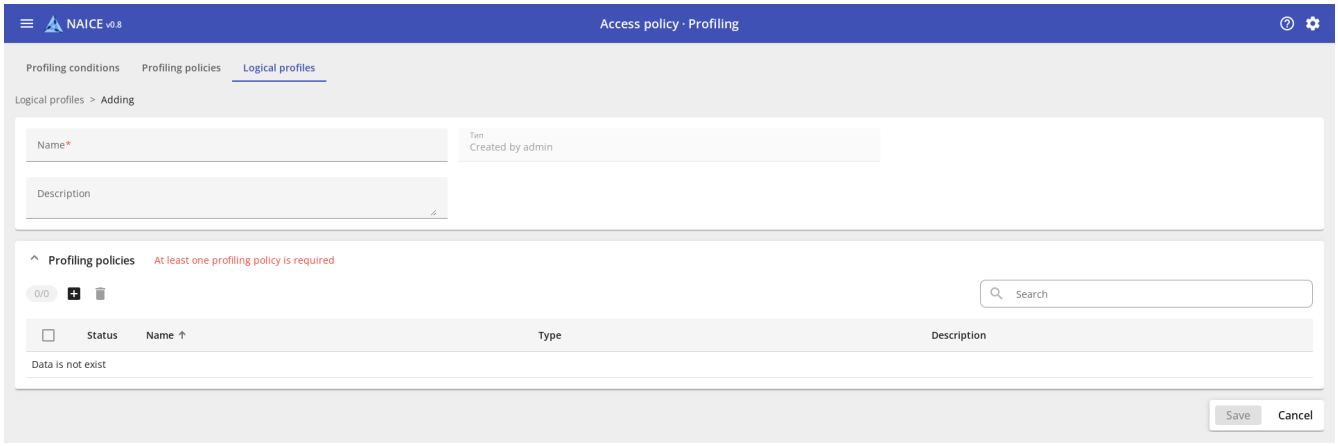

Figure 216. Logical profile addition page

The page that opens presents the following parameters:

- `Name` * - Name of the profiling condition. The maximum login length is 100 characters.
- `Type` - Type of profiling condition. Cannot be set and is always set to "Created by Admin".
- `Description` - arbitrary description of the profiling condition. Maximum length is 200 characters.

Profiling Policies - block responsible for adding/removing profiling policies. For ease of configuration, a list of assigned profiling policies is displayed below in tabular form. The table contains columns:

- `Search` - Performs case-insensitive filtering using the `Name` and `Description` columns: only records that satisfy the filtering condition are displayed.
- 0/1 - Counter of elements selected by the checkbox / total number of elements.
- - Add a new element.
- - Delete selected elements (inactive until at least one element is selected).
- - Change the current sort order.

☐ - Checkbox, which is responsible for selecting elements to perform further actions (for example, deleting).

Parameters marked with an asterisk * are required.

After adding the required policies, the logical profile can be saved.

A logical profile must contain at least one profiling policy. The "Save" button will be inactive while the list of profiling policies is empty or other required parameters are not filled in.

Add profiling policies to a logical profile

To add profiling policies to a logical profile, click on the icon ⊞ at the top left above the table in the **Profiling Policies** section.

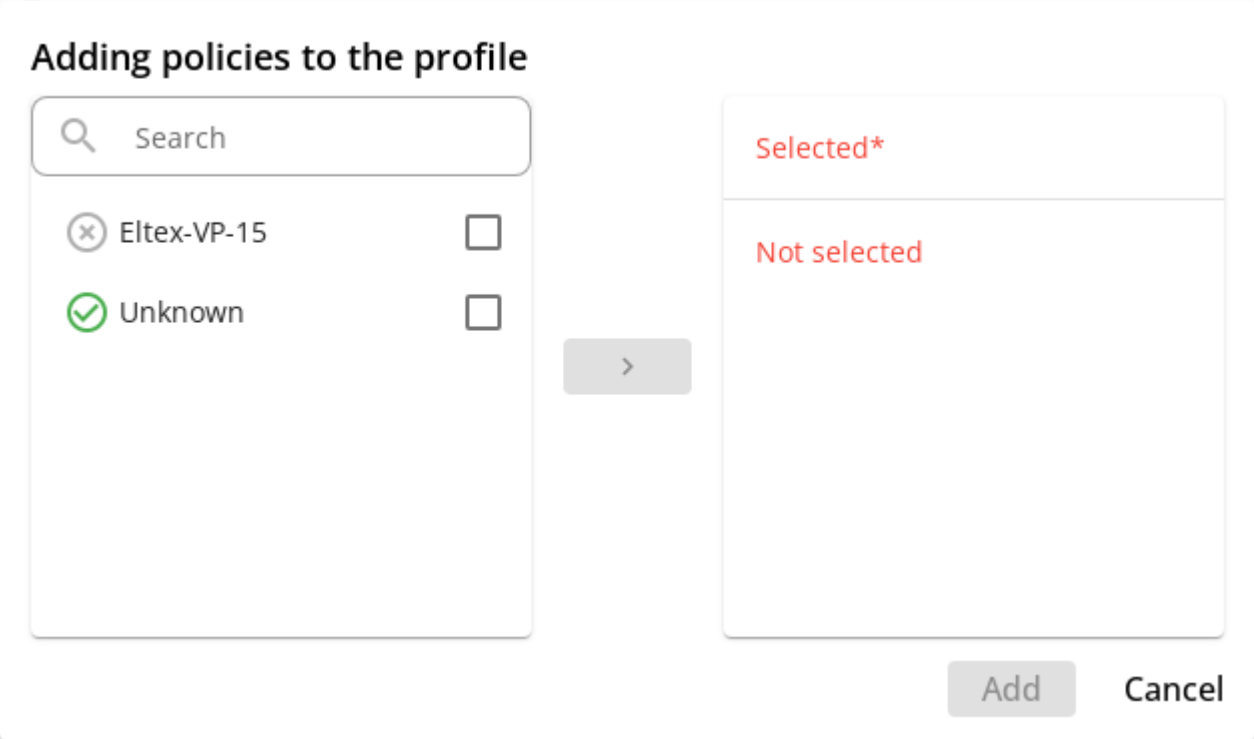

Figure 217. Modal dialog for adding profiling policies

In the left part of the modal window that opens, select the checkbox ☐ for the profiling policies that need to be added to the profile. To search for the desired policy, you can enter its name in the `Search` line.

After selecting the desired policies, click the icon › . Profiling policies marked with a checkbox will move to the right side of the modal window. If necessary, the profiling policy on the right side of the modal window can be deleted by clicking on the icon 🗑 to the right of the name. Once all the desired policies are selected, click the `Add` button to apply the changes.

Added profiling policies will begin to be displayed in the table in the **Profiling Policies** section. The order of the policies does not matter. They are all checked independently of each other.

The `Unknown` system profiling policy cannot be used in a logical profile.

Editing a logical profile

To edit a logical profile, click on its name on the list page.

After this, the editing window will open.

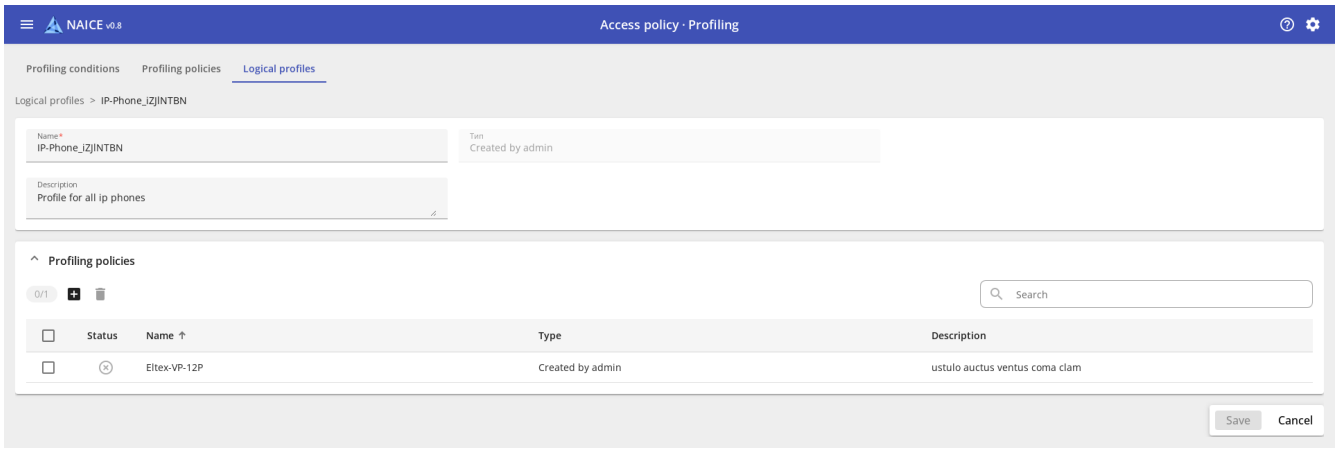

Figure 218. Logical profile edition page

After editing, click on the "Save" button. The button remains inactive until at least one field is changed or the profiling policy set is changed.

Deleting a logical profile

To delete, in the list window, select the checkbox to the left of the name of the logical profiles that you want to delete, and click the button  at the top left.

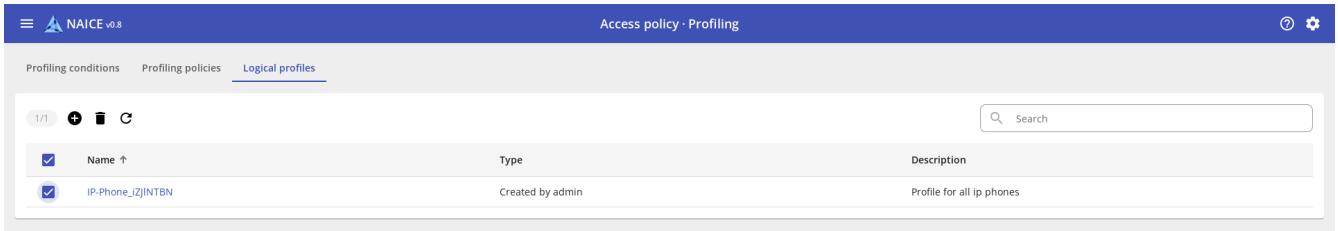

Figure 219. Selecting profiles for deletion

Deletion requires confirmation of the action, for which a modal dialog will open.
After explicit confirmation, the selected items will be deleted.

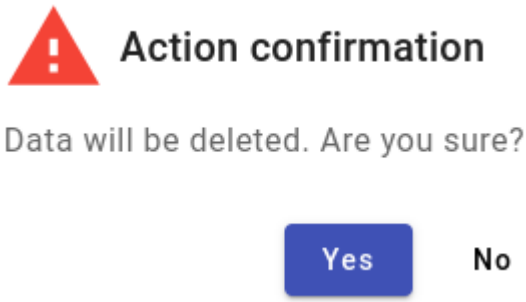

Figure 220. Modal dialog for confirmation

Restrictions:

- You cannot delete a logical profile that is used in any authorization policy.

Monitoring

RADIUS

User sessions

Description

Monitoring user sessions allows you to view user connections over a certain period of time, filter to find the necessary records, and analyze detailed information about a specific session.

View the list of user sessions

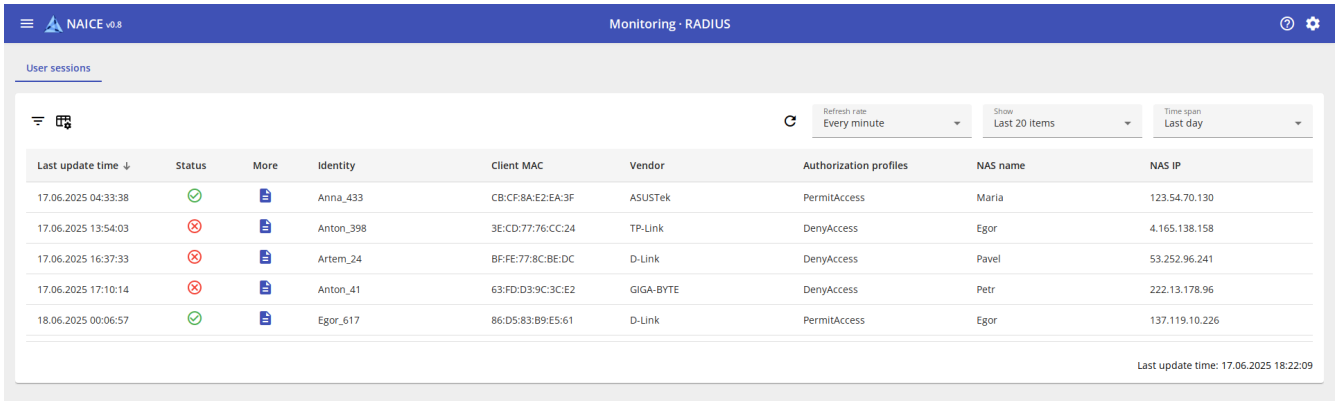

Figure 221. Table with a list of user sessions

The default table contains columns:

- `Last update time` - the time when the last RADIUS packet was received during this session.
- `Status` - the status of the session, can take values:
  - ⚠ - CREATED - the session was created, but for some reason the authorization was not completed;
  - ✓ - ACCEPTED - authorization was successful;
  - ✗ - REJECTED - authorization failed;
  - ⧗ - EXPIRED - the session was terminated after a certain time.
- `More` - a link to open the detailed session page, which contains detailed information about the session.
- `Identity` - the username of the user who was logged in.
- `Client MAC` - the identifier of the authorized client, which is specified in the RADIUS attribute Calling-Station-Id.
- `Vendor` - the name of the organization that produced the device that was authorized.
- `Authorization profiles` - a list of authorization profiles that were applied based on the results of the client's authorization.
- `NAS name` - the name of NAS devices in the system.
- `NAS IP` - IP address of the NAS device, obtained from the RADIUS attribute NAS-IP-Address.

`Acct Session ID` - the session ID from the Acct-Session-Id RADIUS attribute.

Additional columns are also available, configurable in ⚙ in the table header:

- `Authentication Policy` is the name of the authentication policy rule that was applied during this session;
- `Authorization Policy` is the name of the authorization policy rule that was applied during this session;
- `Failure reason` - the reason for the connection error.
- `Flow type` - the type of connection that was determined based on the settings of the network device profile.
- `Authentication protocol` - the protocol used for authorization (for example, PAP).

⚠ The user login when authorizing in Active Directory is always displayed in UPN format (for example, username@example.org)!

Controls:

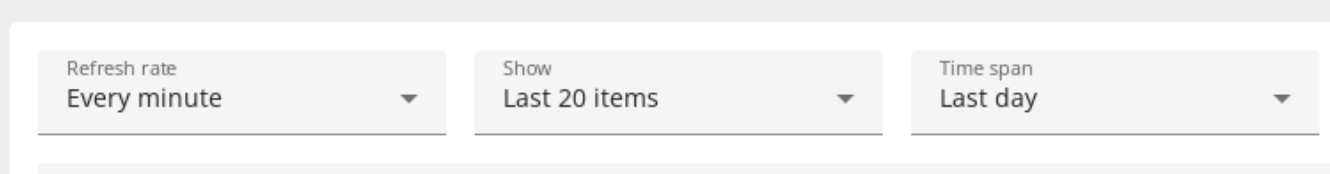

Figure 222. User activity display settings

- `Refresh rate` - setting the frequency of automatic re-reading of user sessions.
- `Show` - setting the number of records to display in the table.
- `Time span` - selection of the time period in which user session activity occurred for display.
- ↻ - update the table data manually.
- ⚌ - open the filtering settings window.
- ⚙ - open the settings window for the displayed columns of the table.

Filtering is configured in the following window:

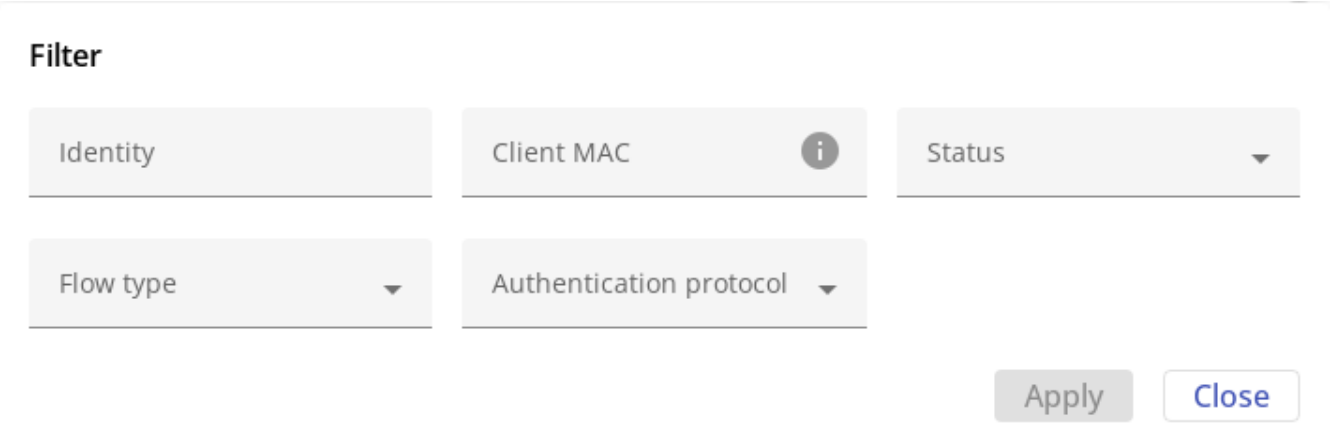

Figure 223. Window for filtering records

Filtering of records is available by the parameters "Client MAC", "Identity", "Status", "Flow type" and "Authentication protocol".

In the client MAC address input field, only hex digits can be entered. Octet separators (colons) are entered automatically.

A partial byte representation search is available.

To search for a part of the MAC address, it is necessary that all the searchable bytes of the address are the same. they were indicated in full.
for example: it is possible to search for "AA:BB:CC"; when searching for "A:BB:C" - no.

The "**Reset all**" button is designed to reset the configured search parameters.

In the table settings  you can change the set of the displayed columns.

The  button selects or deselects all columns for display.

The  button is reset displayed columns to their default state.

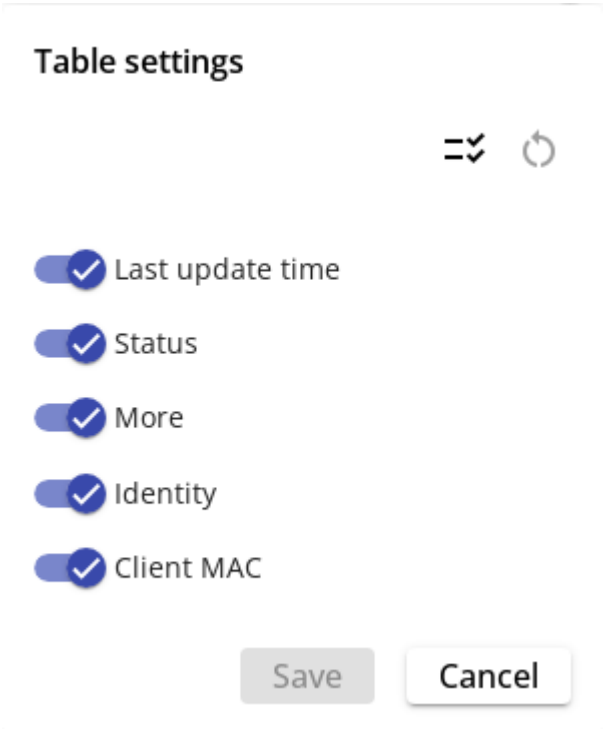

Figure 224. The window for configuring the displayed columns in the table

View detailed session information

To view detailed information about a session from a table with all sessions, click on  in the “Details” column for the selected session.

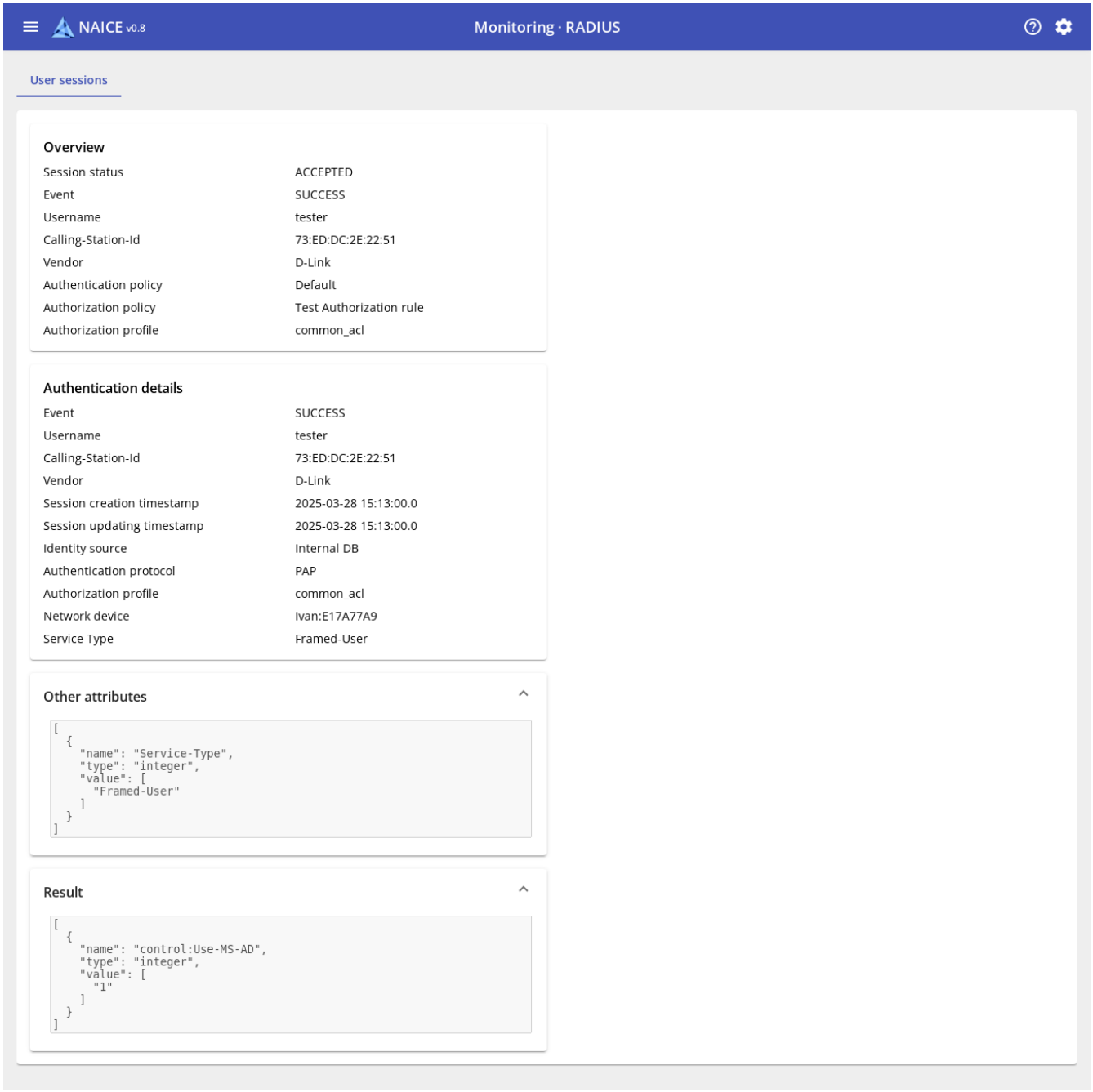

Figure 225. Detailed information about the session

The information on the page is divided into 4 blocks:

- `Overview` - brief and most important information about the session;
- `Authentication details` - detailed information that can be useful for debugging;
- `Other attributes` - the contents of the package received by NAICE from the RADIUS server;
- `Result` is a list of attributes that were used to enrich the response to the client as a result of authorization (for example, attributes for issuing VLANs or ACLs). If the authorization profile is not configured to issue additional attributes, the list will be empty.

TACACS

Connections journal

Description

Monitoring connections journal allows you to view administrator connections over a certain period of time, filter to find the necessary records, and analyze detailed information about a specific session.

View the list of TACACS+ connections

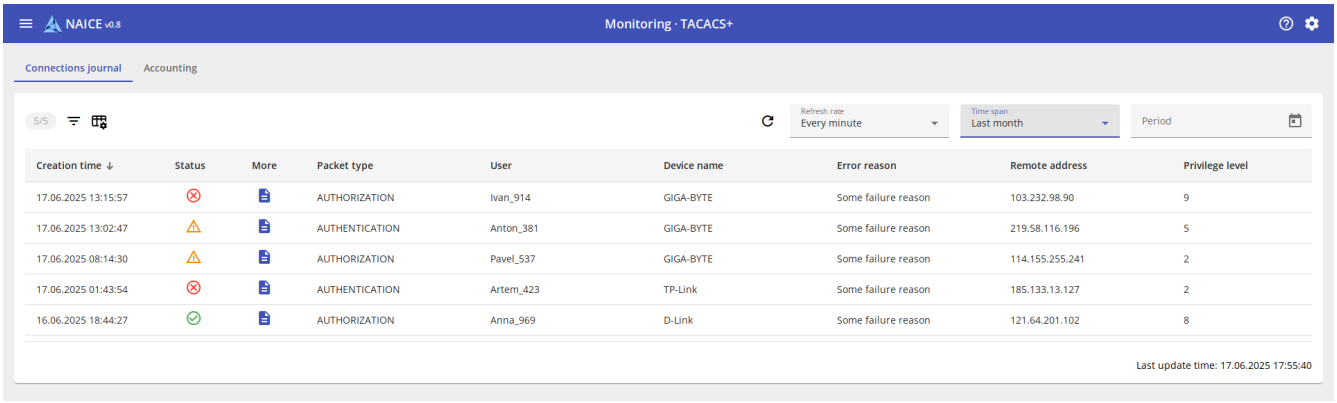

Figure 226. Table with a list of connections TACACS+

The default table contains columns:

- `Creation time` - the time when a connection attempt was made within this session.
- `Status` - the status of the session, can take values:
  - - PASS - authorization was successful;
  - - FAIL - authorization failed;
  - - EXPIRED - the session was terminated after a certain time.
- `More` - a link to open the detailed session page, which contains detailed information about the session.
- `Packet type` - takes the values "AUTHENTICATION" or "AUTHORIZATION", depending on what the request was for in the session.
- `User` - the identifier of administrator.
- `Device Name` - the name of the network device on which authorization took place.
- `Error reason` - description of the error that caused unsuccessful authentication or authorization.
- `Remote address` - the IP address of the device from which the administrator made the connection.
- `Privilege level` - values of the privilege level assigned to the administrator.
- `Command` - the name of the command on the network device for which the authorization request was made.
- `Session ID` - TACACS session identifier.

Additional columns are also available, configurable in in the table header:

- `Device IP` - the address of the device to which the connection was made.
-

`Authentication Policy` is the name of the authentication policy rule that was applied during this session;

- `Authorization Policy` is the name of the authorization policy rule that was applied during this session;
- `Port` - the name of the protocol used to connect to the device.
- `Device type` - the device type that was determined based on the device settings.
- `Device location` - the location of the device, which is determined from the device settings.
- `TACACS profile` - The name of the TACACS profile assigned to the administrator as a result of authorization.
- `Command set` - the name of the set of commands assigned to the administrator as a result of authorization.

Controls:

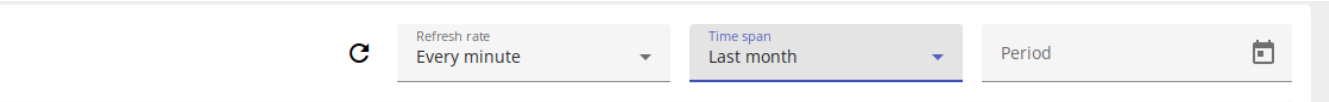

Figure 227. User activity display settings

- `Refresh rate` - setting the frequency of automatic re-reading of user sessions.
- `Show` - setting the number of records to display in the table.
- `Time span` - selection of the time period in which user session activity occurred for display.
- - update the table data manually.
- - open the filtering settings window.
- - open the settings window for the displayed columns of the table.

After scrolling the first 25 elements, the "Refresh rate" parameter switches to the "Disabled" state.
To return, you must either manually specify the update time or click the update button .

Filtering is configured in the following window:

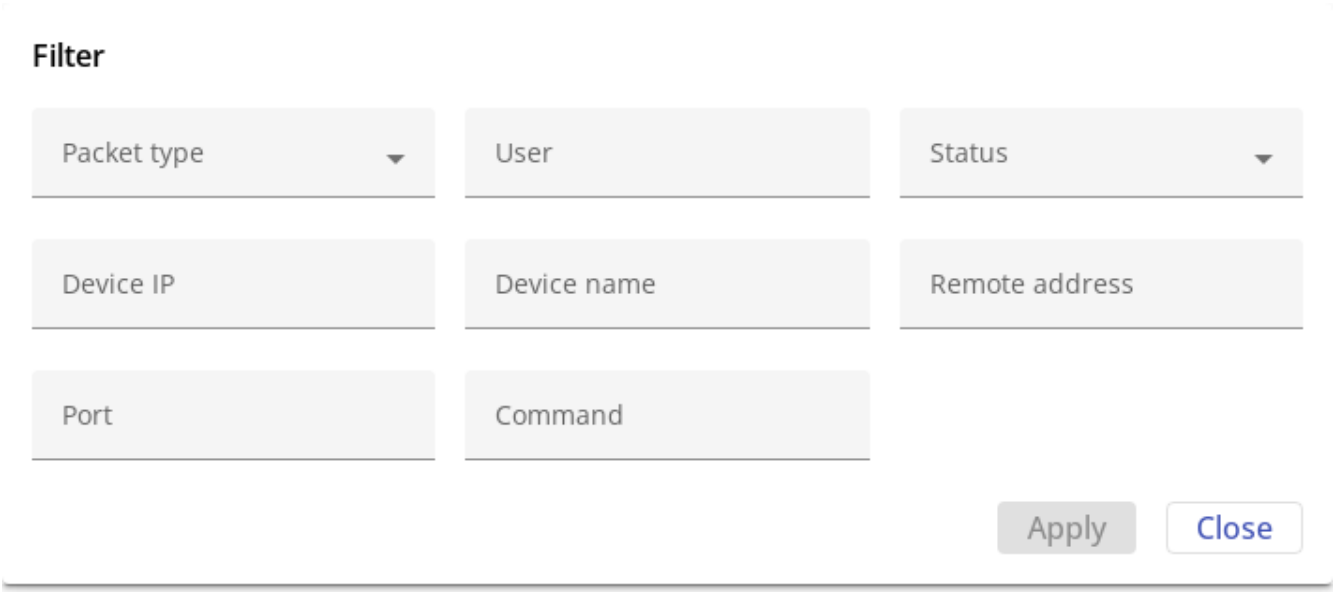

Figure 228. Window for filtering records

Filtering of records is available by the parameters "Packet type", "User", "Status", "Device IP", "Device name", "Remote address", "Port", "Command".

The "**Reset all**" button is designed to reset the configured search parameters.

In the table settings you can change the set of the displayed columns.

The button selects or deselects all columns for display.

The button is reset displayed columns to their default state.

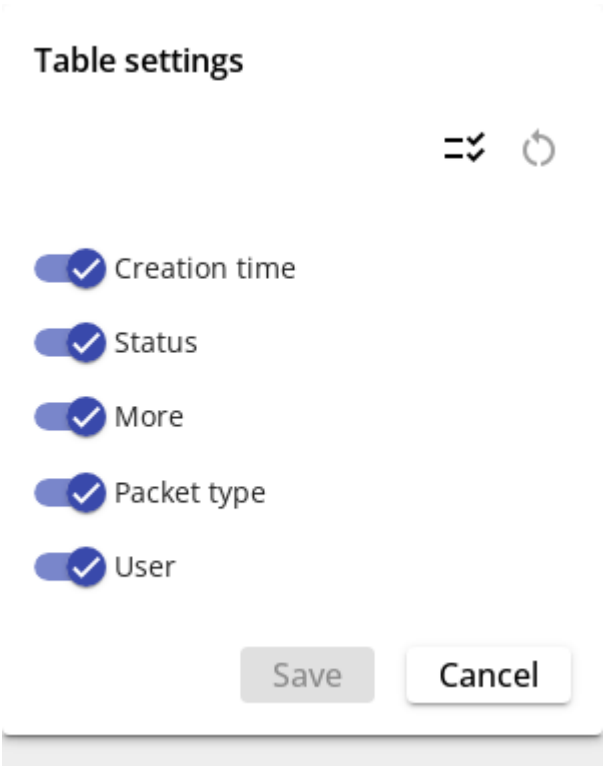

Figure 229. The window for configuring the displayed columns in the table

View detailed session information

To view detailed information about a session from a table with all sessions, click on in the “Details” column for the selected session.

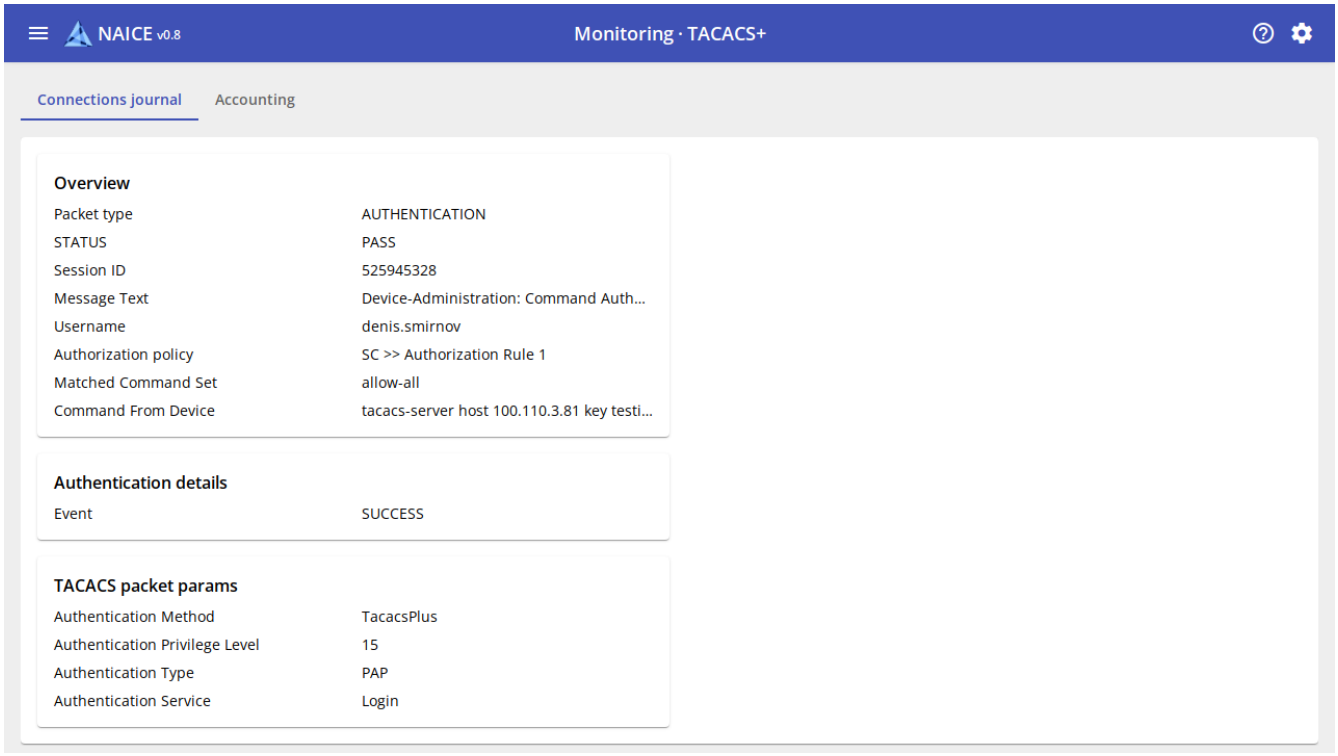

Figure 230. Detailed information about the session

The information on the page is divided into 4 blocks:

- `Overview` - brief and most important information about the session;
- `Authentication details` - detailed information about the authentication that can be useful for debugging;
- `Authorization details` - detailed information about the authorization that can be useful for debugging;
- `TACACS packet params` - other attributes received by NAICE from the TACACS server.

Displaying of blocks "Authentication details" and "Authorization details" depends on the packet type.

Accounting

Description

The TACACS+ account allows you to view information about the actions of network device administrators using the TACACS+ protocol for a specified period of time and filter to find the necessary records.

View the TACACS+ command accounting list

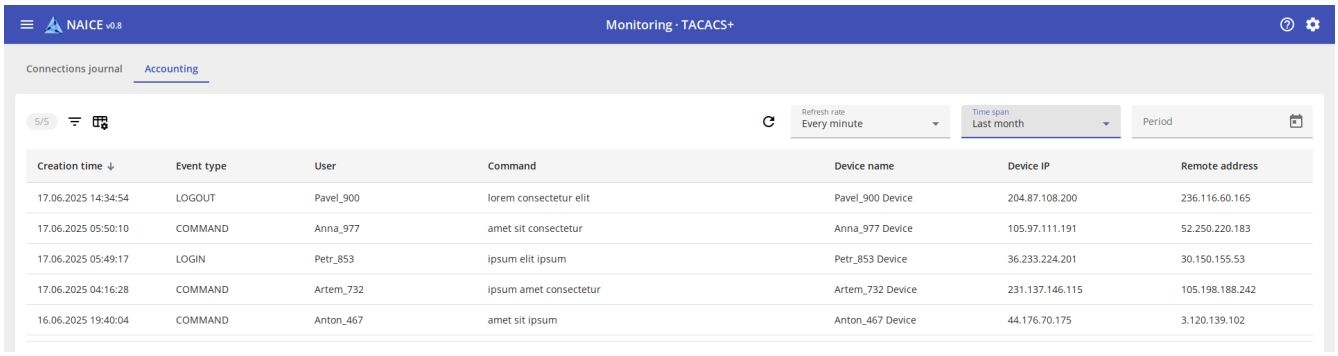

Figure 231. Table with TACACS+ command accounting list

The default table contains columns:

- `Creation time` - the time when a connection attempt was made.
- `Event type` - Depending on the event, it can take the following values: LOGIN - for login events, COMMAND - for command events, EXIT - for exit events.
- `User` - the identifier of administrator.
- `Command` - the name of the command on the network device that the administrator executed.
- `Device Name` - the name of the network device on which authorization took place.
- `Device IP` - the address of the device to which the connection was made.
- `Remote address` - the IP address of the device from which the administrator made the connection.
- `Session ID` - TACACS session identifier.

Additional columns are also available, configurable in in the table header:

- `Privelege level` - values of the privilege level assigned to the administrator.
- `Port` - the name of the protocol used to connect to the device.
- `Authentication method` - the user authentication method by which the command was recorded.
- `Authentication service` - the name of the authentication service through which the command was recorded.
- `Authentication protocol` - the name of the authentication protocol by which the command was recorded.
- `Request arguments` - arguments of the request by which the command was taken into account.

Controls:

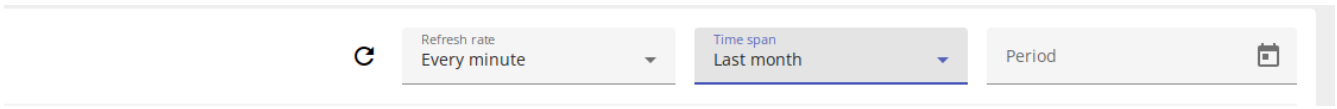

Figure 232. User activity display settings

- `Refresh rate` - setting the frequency of automatic re-reading of accounting events.

`Show` - setting the number of records to display in the table.

- `Time span` - selection of the strict time period in which user session activity occurred for display.
- `Period` - select an arbitrary time interval in which activity occurred by sessions for display.
- - update the table data manually.
- - open the filtering settings window.
- - open the settings window for the displayed columns of the table.

After scrolling the first 25 elements, the "Refresh rate" parameter switches to the "Disabled" state.
To return, you must either manually specify the update time or click the update button .

Filtering is configured in the following window:

Figure 233. Window for filtering records

Filtering of records is available by the parameters "User", "Device IP", "Device name", "Remote address", "Port", "Command".

The "**Reset all**" button is designed to reset the configured search parameters.

In the table settings you can change the set of the displayed columns.

The button selects or deselects all columns for display.

The button is reset displayed columns to their default state.

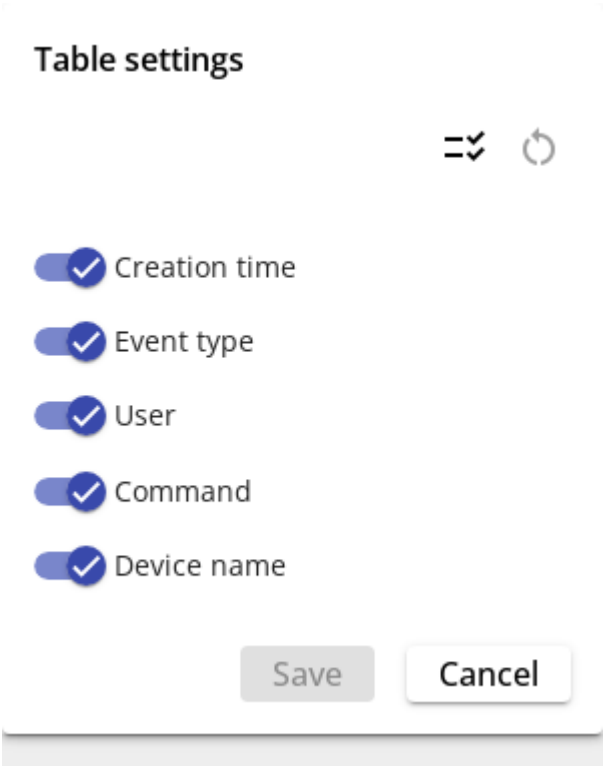

Figure 234. The window for configuring the displayed columns in the table

System

System events

Description

The system event log displays information about licensing events. Allows to select the period and level of event logging. It also allows to filter events.

Viewing system events

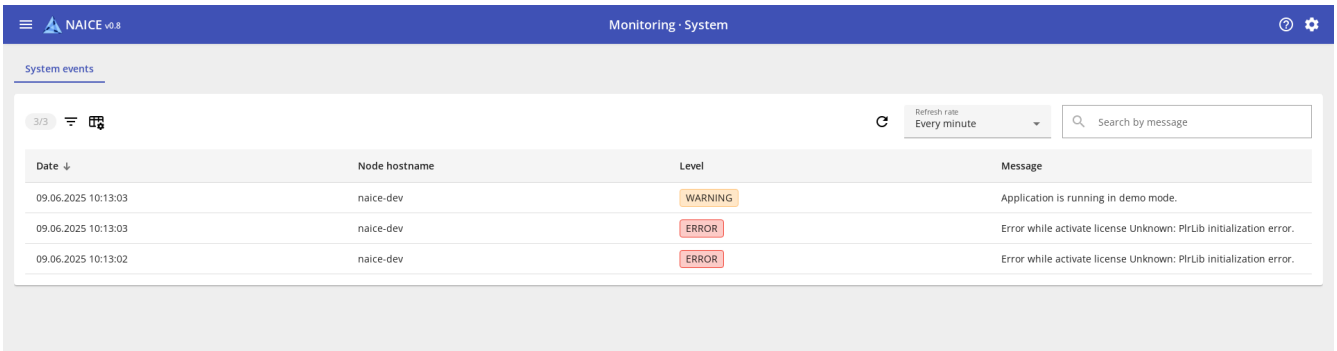

Figure 235. Table with a list of system events

The table contains columns:

- `Date` - date and time of the event.
- `Node hostname` - name of the node that generated the event.
- `Level` - event logging level.
- `Message` - Event information.

Additional columns are also available, configurable in the table header:

- `Group` - the group of the event. Possible values:
  - `Licensing` - events occurred as a result of the licensing system operation.
  - `CMS` - this type of event will be supported in the future.
  - `Portal` - this type of event will be supported in the future.
- `Key` - result of performing actions reflected in the event.
- `Administrator` - who caused this event. The administrator login is displayed if the action was performed by the system administrator or the system user `system` if the event was caused by the system.

The `Date` and `Message` columns cannot be disabled.

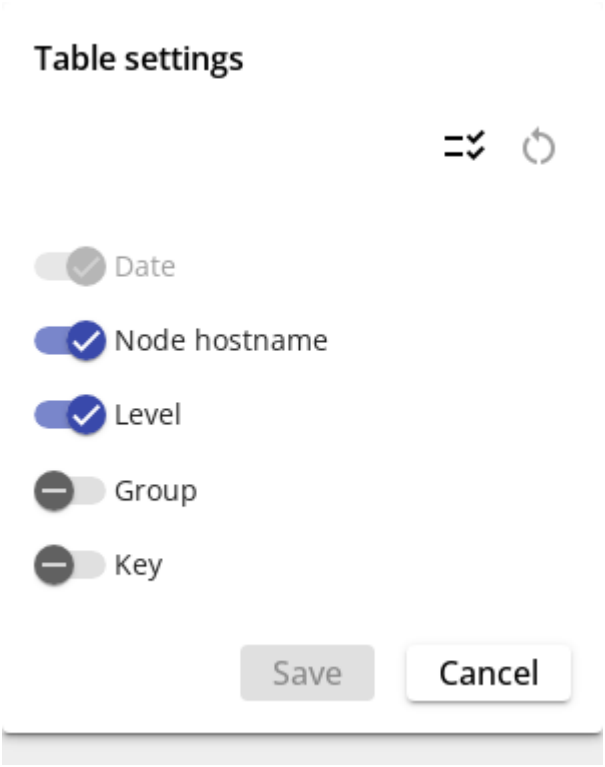

Figure 236. Configure system event table columns to display

Control elements:

- `0/1` - Counter of displayed / total number of events.
-  - Open the filter settings window.
-  - Open the window for customizing the displayed table columns.
-  - Change the current sorting order. Sorting is available only by the `Date` column.
-  - Refresh the table data manually.
- `Refresh frequency` - setting the frequency of automatic rereading of system events.

When you scroll through the first 25 table items, the “Refresh Rate” parameter goes to the “Disabled” state.
To return, you must either manually specify the refresh time or refresh the browser page.

- `Search by message` - case-independent search in the `Message` column.

Figure 237. Search by message

To reset the search expression, you must click ✕ on the right side of the search form.
The button is not displayed until a value is entered.

Filter is configured in the following window:

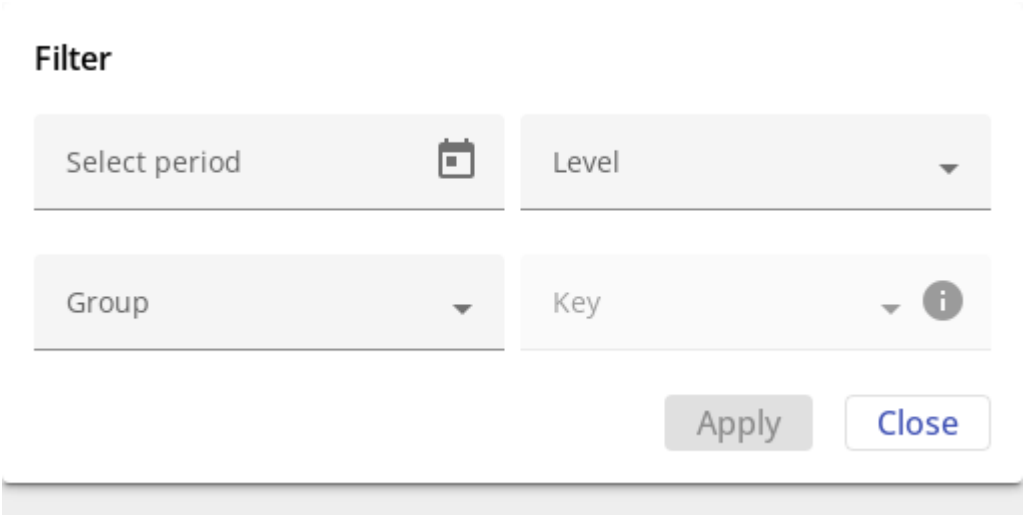

Figure 238. filter customization window

Filtering of records is available by parameters:

- `Select period` - allows to select the time period up to date.
- `Level` - allows to select the level of displayed events:
  - `INFO` - display events of `INFO`, `WARNING`, `ERROR` levels.
  - `DEBUG` - display events of all levels.
  - `WARNING` - display events of `WARNING`, `ERROR` level.
  - `ERROR` - display events of `ERROR` level.
- `Group` - selection of the displayed group of events. In the current version only events of the `Licensing` group are saved.
- `Key` - selection of the event type from a certain group. In the current version it is possible to select the event type only for the `Licensing` group. If the group is not selected, the key selection is not available.

To reset all filters use the `Reset all` button in the upper right corner of the filter parameters selection window. The button becomes visible only if at least one filter is selected.

System Events List

The contents of the "Message" field for events is displayed according to the language specified in the `URSUS_DEFAULT_EVENT_LOG_LOCALE` environment variable.

Events – Licensing

Event Key	Description	Level	Message	Source
`License activation`	License activation – successful communication with ELM or local PLR validation	INFO	The license `<productId>` successfully activated.	Gulo
`Upload file license`	License file upload	INFO	The `<fileType>` for `<productId>` on `<hostname>` successfully uploaded.	User / UI
`Demo mode`	Product running in demo mode	WARNING	Application is running in demo mode.	Gulo
`License applied`	License successfully applied (on services like Ovis, Aquila)	DEBUG	The license `<productId>` applied at `<service>`. Features: `<params>`.	Ovis / Aquila
`Functionality is limited`	Functionality is limited (for various reasons)	WARNING	The functionality is limited.	Ovis / Aquila
`License removed`	License removed	INFO	The license `<productId>` has been deleted.	User / UI

Event Key	Description	Level	Message	Source
`License activation error`	License activation error	ERROR	Error while activate license `<productId>`: `<error>`.	Gulo
`License upgrade status`	License upgraded to status (e.g., init - ready, manually - backup)	DEBUG	The license with `<productId>` has been upgraded to the status `<status>`.	Gulo
`License activation file create`	Activation file created (after call to EPG service)	INFO	Activation file successfully created with `<productId>`.	Gulo
`License activation file error`	Activation file creation failed (error contacting EPG service)	ERROR	Activation file creation error for `<productId>`: `<error>`.	Gulo
`License Pk file already exists`	PK file already exists	ERROR	PK file for `<hostname>` already exists.	Ursus
`Upload file license error`	License file upload error	ERROR	Failed to upload `<fileType>` for `<productId>` on `<hostname>`.	Gulo
`License activation cmd`	License activation cmd	INFO	Activates license `<productId>`.	Gavia
`License activation file create cmd`	License activation file create cmd	INFO	Creates an activation file for license `<productId>`.	Gavia

Licensing

Description

The NAICE network access control system is distributed under a commercial license. This means that in order to access the functionality, you must purchase and activate a license.

Licensing can be carried out according to one of the following schemes:

- Using the **Eltex License Manager** license server (hereinafter referred to as **ELM**), which performs the function of licensing software and hardware products of the Eltex company. It assumes a periodic request to the license server. You can use:
  - the Eltex license server (hereinafter referred to as Online ELM), available at https://elm.eltex-co.ru:8099;
  - an ELM server installed in the customer's infrastructure (hereinafter referred to as Offline ELM).

  In both cases, the address of the ELM server is specified during the installation of NAICE and it should be available at the time of license activation. The ability to work with a WEB server using an HTTP proxy server (using login/password authentication or without authentication) is supported.
- File licensing (hereinafter referred to as **PLR**, permanent license request) is licensing with reference to the physical parameters of the host on which NAICE is installed. When changing the host parameters, re-activation is required.

After installation, NICE is in **demo mode** with limited functionality. The limitations of the demo mode are specified by link:index.html#*demonstration* mode[next].

When you purchase access to a product with a certain licensing type, a **product key file** is generated, unique for each NAICE instance. To unlock the NAICE functionality corresponding to this license, the file must be downloaded and activated on the *licensing* page.

License types and licensed functionality

The current version implements the only licensing type **BASIC**. At this type, access to the main service is provided - RADIUS authorization endpoints. The licensed parameter is **the number of successfully authorized unique end devices per day**. This number is agreed upon at the license acquisition stage and depends on the number of client devices on the network.

An example of calculating the number of end devices in a network

Organization A has 1,000 employees, each of whom has a laptop for work. Employees of company "A" do not connect from personal devices. The company also has 10 cameras, 5 printers and 2 TVs connected to the network. All these devices must be authorized in the NAC system.

Calculation of the number of unique endpoints in the network: 1000 * 1 (number of devices of 1 employee) + 10 (cameras) + 5 (printers) + 2 (televisions) = 1,017 pcs. – unique devices in the company.

It is recommended to purchase licenses for more endpoints than are designed for unique devices.

If necessary, the number of endpoints in the license can be increased. To do this, contact your manager or send a request to our email address. eltex@eltex-co.ru .

An additional module **NAICE-TACACS** is also available for purchase, activating the TACACS server as part of NAICE. Modules are additionally purchased for the basic license of any type.

Licenses of any types can be issued for a period of 1, 3 or 5 years.

If you have any questions about obtaining a license, please contact us by email eltex@eltex-co.ru .

Demo mode

After installation, NAICE is in demo mode. In this mode, all functionality corresponding to the maximum license type and with all additional modules is available, but with the following restrictions:

- the maximum number of devices added to the system is 15;
- the maximum number of successfully authorized unique endpoints per day is 15.

The demo mode is unlimited in time, but it is only available **until the first successful activation of the license**. After activating the license, the demo mode will be disabled without the possibility of recovery.

The corresponding warning in the upper right part of the page indicates that the system is in demo mode.

Figure 239. Warning about demo mode

Clicking on the warning will take you to the *licensing* page, which contains the current parameters and limits of the demo mode, as well as controls for downloading and administering licenses.

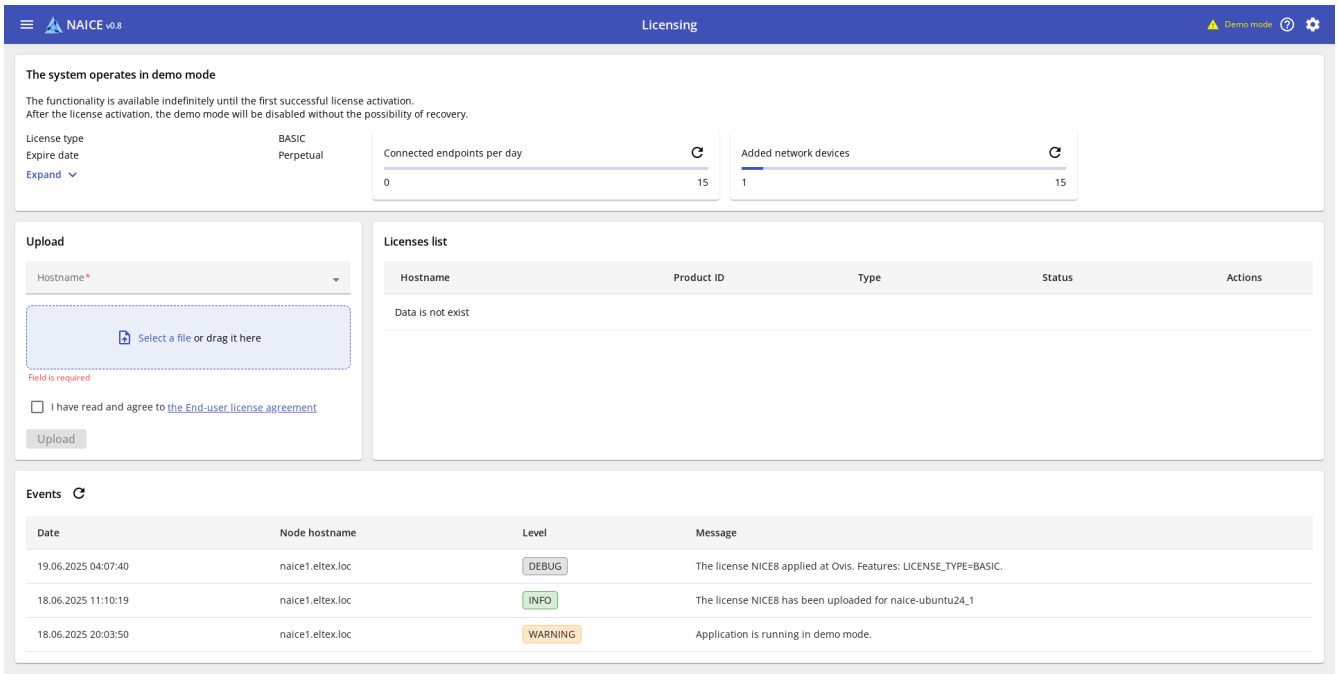

Figure 240. The Licensing in demo mode page

Actions to activate the license

The license is activated on the *licensing* page, the image of which is shown above.

In addition to the current parameters of the demo mode or license, the page contains the following controls:

- the "Upload" block - elements for loading licensed files;
- the "Licenses List" block - management of loaded licenses;
- the "Events" block - system events related to licensing.

Uploading the product key

To activate the license, you must have the *product key file* received from your manager when purchasing the system. The product key file contains the *Product ID*, which is the serial number that identifies one copy of the software, and the *Product Key* that identifies the license owner.

The format of the product key file name is *NICENNNNNNN.txt * for an ELM license (for example - NICE1111111.txt) and *FNICENNNNNNN.txt * for a PLR license (for example - FNICE1111111.txt).

A valid product key file cannot be empty or have a size of more than 1 MB.

Product ID can only be linked to one host. Attempts to load the *Product ID*, which is already present in the table, are prohibited by the system. The restriction is not lifted even if the *Product ID* is in the `Backup` state. All uploaded *Product ID* must be from the same license (have the same *License Key*). Attempts to download *Product ID* from different *License key* are prohibited by the system.

The load of the product key is performed in the "Upload" block in several steps:

1. **Hostname** to load the license from the list by its hostname. With a standard installation, the hostname matches the name of the host on which NAICE is deployed.
2. **Select a file** by dragging it into the load field or selecting it through the Explorer when clicking on "*Select file*". If necessary, before clicking on the `Upload` button, the file can be replaced by clicking on  on the right side of the upload field.
3. Review and confirm **agreement with** **User Agreement**.
4. Click on the `Upload' button.

Figure 241. Uploading a product key file

When using NAICE in a cluster, you need to upload your product key for each NAICE host.

After downloading the product key file, the license will be added to the license table in the "Licenses List" block.

License activation

The activation mechanisms for ELM and PLR licenses differ significantly.

ELM

The ELM license is activated automatically by connecting to an Online or Offline ELM server. Upon successful activation, the license acquires the status of **Active** in the list of licenses, and the functionality becomes available according to the license parameters. The parameters of the active license are displayed in the upper "License Information" block.

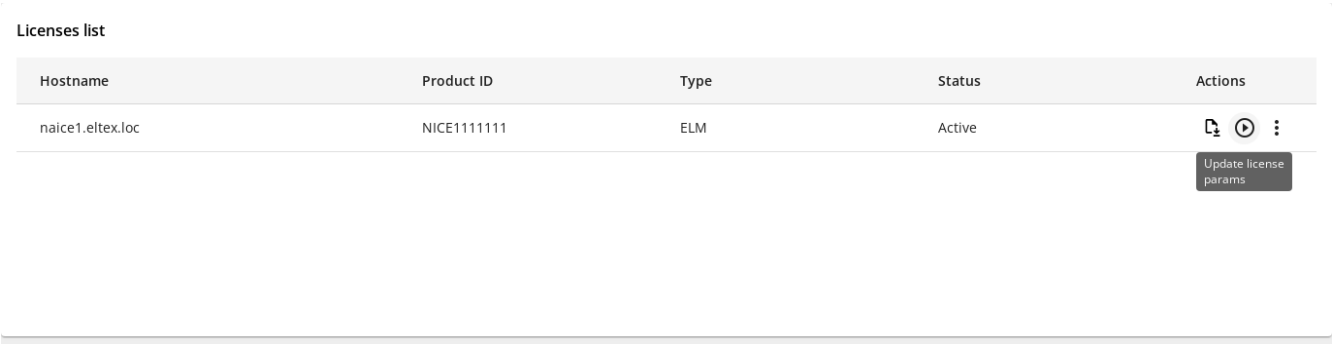

Figure 242. Activation of the ELM license

PLR

The PLR mode is activated by downloading the product key, which is supplied as a file. This file is being released based on a request from Eltex company.

After downloading the PLR license product key, it will appear in the "Licenses list" table with the **Init** status. This status means that the license has been initialized and the *license activation file* has been generated. The

file, among other things, contains a cast of the host machine's environment parameters, to which the license is attached.

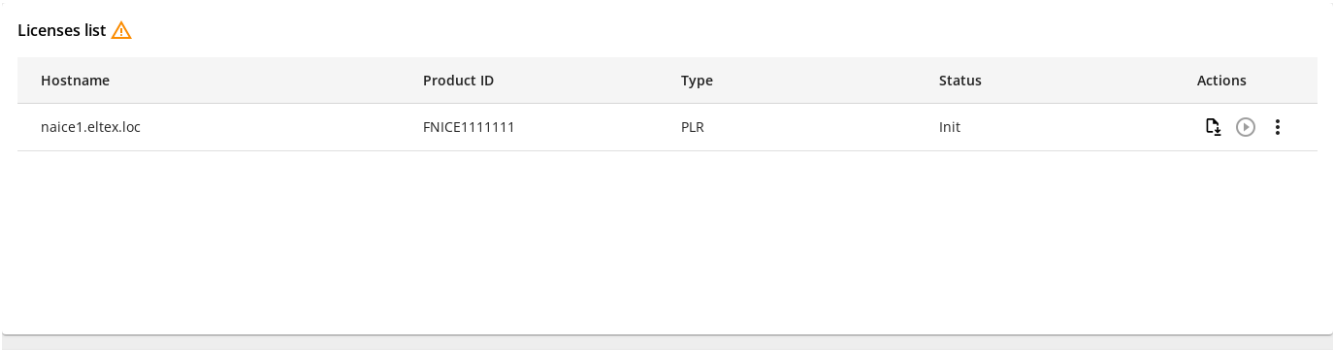

Figure 243. PLR license after downloading the product key

The license activation file must be downloaded and sent to Eltex company to release the license file, which is the final file containing the parameters of the purchased license with their activation linked only in a specific environment. For this:

1. Click on in the "List of licenses" table in the Actions column and select `Download activation file`.

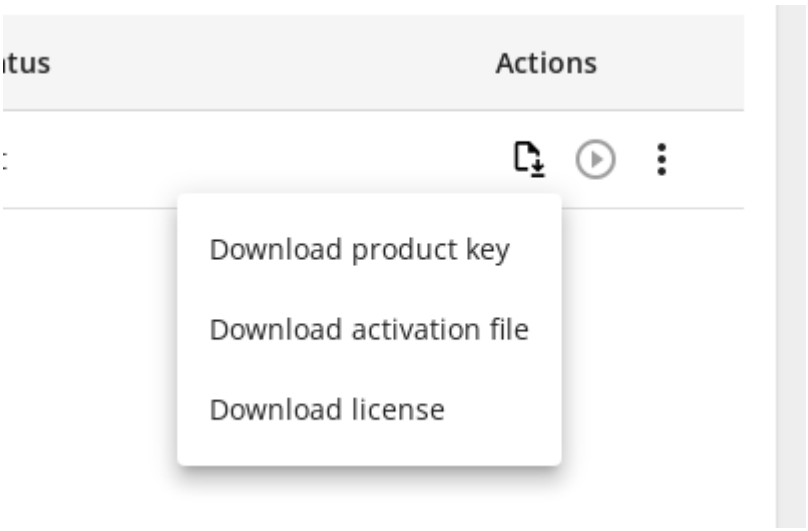

Figure 244. Download menu for licensed files

Activation file name format **request-<YYYY-MM-DD>-<Product ID>-<NAICE Version>.txt**, for example - *request-2025-06-17-FNICE1111111-0.8.0.txt *.

The activation file must be sent to the Eltex company. This will allow you to issue a file license corresponding to the provided activation file.

Get the license file from the Eltex company.

The license file must be uploaded to the system in the same way as Uploading the product key. Upon successful download and verification of the file, an attempt will be made to automatically activate the license. If there are no errors, the license acquires the status of **Active** in the list of licenses, and the functionality becomes available according to the license parameters. The parameters of the active license are displayed in the upper "About License" block.

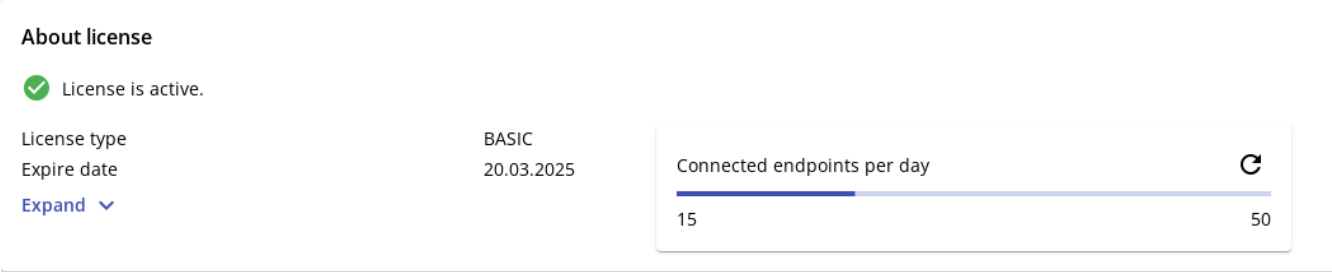

Figure 245. Information about the active license

License activation errors

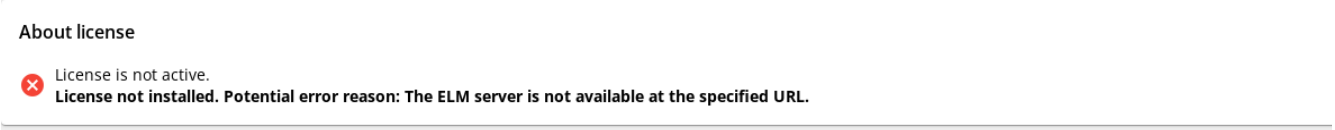

Figure 246. Error when activating the license

If license activation errors occur, the error that occurred during the activation process will be displayed on the page under the license status. The error message is also displayed in its original form in Events. In this case, the license itself acquires the status of **Invalid**.

Usually errors during license activation are related to: - When interacting with the ELM server: problems with access to the server (incorrect ELM address in the NAICE configuration, lack of network connectivity) or with errors in the license itself (the license has not expired or expired). - When using PLR licensing: changing the environment settings after creating the license activation file or with errors in the license itself.

To activate the license, you must first fix the initial error, and then click on ▶ next to the desired license in the "Licenses list" table in the "Actions" column.

In case of problems with the automatic activation of the license, it remains in the **Ready** status. In this case, you must manually activate the license by clicking on ▶ next to the desired license in the "Licenses list" table in the Actions column.

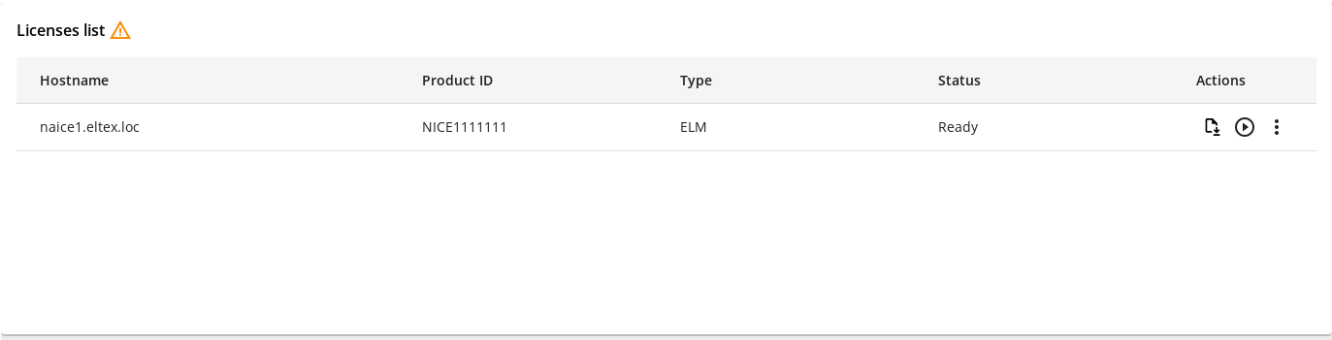

Figure 247. The license has the Ready status

License management and monitoring

After successful activation of the licenses, their status can continue to be monitored on the *Licensing* page. To access the page from any section of NAICE, select ⚙ in the upper-right corner, and select "Licensing" in the menu that opens.

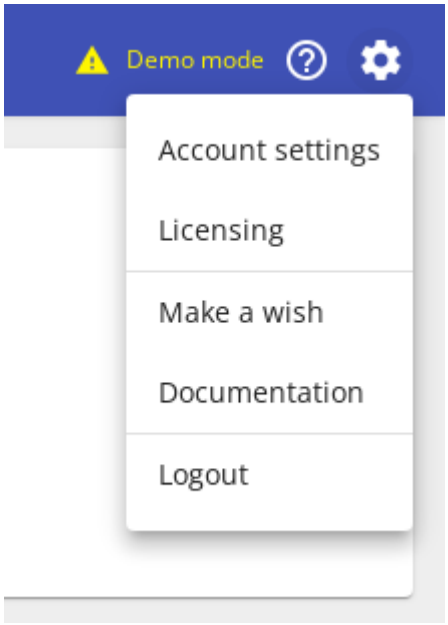

Figure 248. System Settings menu

Information about the active license

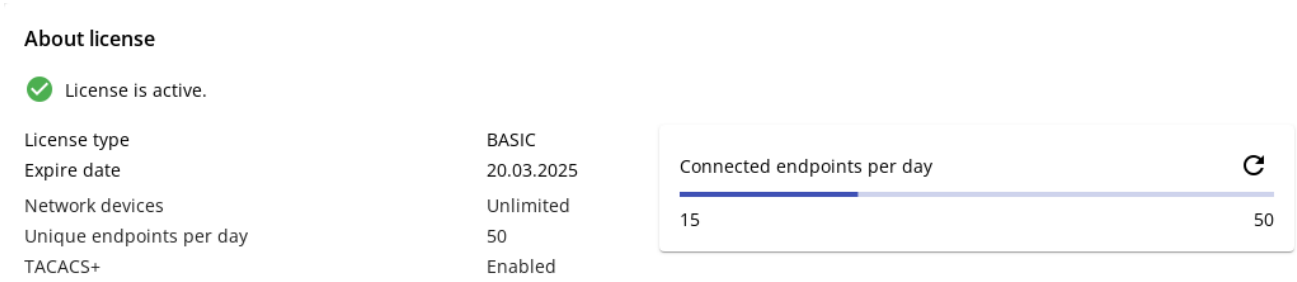

Figure 249. License information

The page contains the following elements:

- `License is active' - current license status.
- License parameters:
  - `License type` defines the NAICE functionality available for configuration and use, see License types and licensed functionality
  - `Expire date` is the date on which the current fixed-term license expires.

    Upon expiration of the license, the licensed NAICE functionality will be blocked, **including authorization of end devices**. Renew the license in advance when you see link:index.html#_revention_to reach the limits[warnings] to avoid such situations.

  - `Network devices' - the limit on the number of network devices added to the system.
  - `Unique endpoints per day' - the limit on the number of connected endpoints per day stipulated by the license.

    When the limit on the number of connected endpoints per day is reached, end devices will not be authorized beyond this limit. Devices that were previously authorized in the last 24 hours will be successfully reauthorized.

- `TACACS+` - the presence or absence of the additional NAICE-TACACS module in the license.

- A counter for the current number of connected endpoints per day. It is automatically updated every 5 minutes.
- - manual counter update.

Features of counting the number of connected devices per day

- The connected endpoint counter increases only when a unique endpoint is connected, i.e. an endpoint that has not been successfully authorized by NAICE in the last 24 hours.
- To determine the uniqueness of the endpoint, it is necessary that the RADIUS attribute `Calling-Station-Id` containing the MAC address of the endpoint device is passed in the RADIUS request.
- The device is considered active exactly 24 hours after the last connection. Upon repeated successful authorization on these days, the 24-hour countdown is updated.

  Example.

  The endpoint was authorized on June 10 at 13:31:10. The endpoint will "free up space" in the licensed limit on June 11 at 13:31:11.

  If the end device was successfully re-authorized on June 10 at 20:20:10, the time will be shifted to June 11 at 20:20:11.

Management of downloaded licenses

All licenses that are uploaded to NAICE are displayed in the "Licenses list" table.

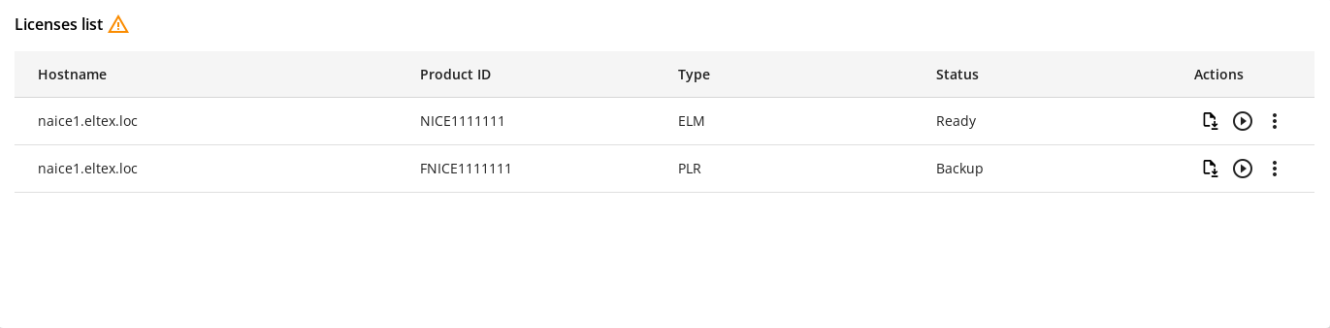

Figure 250. License list

The table contains columns:

- `Hostname` - which host is this license downloaded for;
- `Product ID` is a unique identifier of the software in the licensing system;
- `Type` - license type: regular (ELM) or file-based (PLR);
- `Status` - current license status, which can take one of the following values:
  - **Init** _ (for PLR only)_ - the product key is loaded, the environment parameters are collected, the license activation file is generated;
  -

Ready - the license is ready for activation, there is a product key and a PLR license file in case of file licensing.;

- **Active** - the license has been activated, its parameters have been applied on the specified host;
- **Invalid** - the product key (or file license) was not activated.
- **Mismatched** *(for PLR only)* - received an event about a mismatch of environment parameters;
- **Expired** - the license has expired;
- **Backup** is an inactive license that is currently disabled from licensing; it can be activated if necessary.

The system allows you to leave any number of *Product ID* in the `Backup` state in the database. In case of switching between ELM-PLR types, it is not necessary to delete records of the unused *Product ID*. They can be stored in the database for quick recovery of work "according to a different scheme".

- `Actions' - available actions with a license, including:

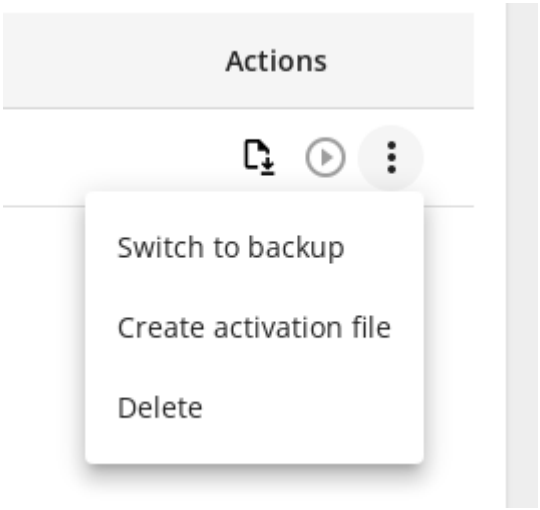

Figure 251. License actions

-  - download of licensed files of various types;
-  - activating an inactive license / updating the parameters of an active license;
- - additional actions:
  - `Switch to backup` - set the license status to **Backup**;
  - `Create activation file` *(for PLR only)* - manual request for problems with automatic generation of the activation file, as well as for Reactivation of the PLR license;
  - `Delete` - delete the license from the downloaded list, as well as all related license files.

In order to provide the service continuously, the transfer to the **Backup** status and the deletion of active licenses (licenses with the **Active** status) does not occur instantly. The license that was deleted or transferred to **Backup** will be reset to the "Unlicensed" state only if you restart the NAICE services. Until then, you should activate another license, otherwise the licensed functionality will be disabled.

Events

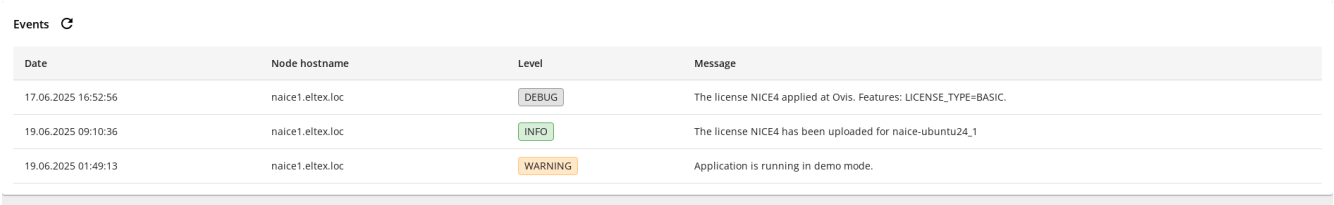

Figure 252. Licensing system events

The Events block is an analog of the System events

The table contains the following columns:

- `Date' - the time when the event was recorded in the database; the time is displayed based on the time zone specified in the account settings;
- `Node hostname` - the name of the host associated with the event;
- `Level' - the importance of the event, can take one of the following values:
  - `INFO` - information events, usually about the success of completed actions;
  - `WARNING` - events that are worth paying attention to;
  - `ERROR` - important events with license errors;
  - `DEBUG' - debugging events.
- `Message' - the content of the event.

Filtering and changing the sorting order are not available. The frequency of auto-updating of the event list is once every 5 minutes. A manual update of the event list is available by clicking

When scrolling through the first 25 elements of the table, auto-updating of the list of events is disabled.
To enable it, you must manually update by clicking .

Warnings

Warnings about reaching limits

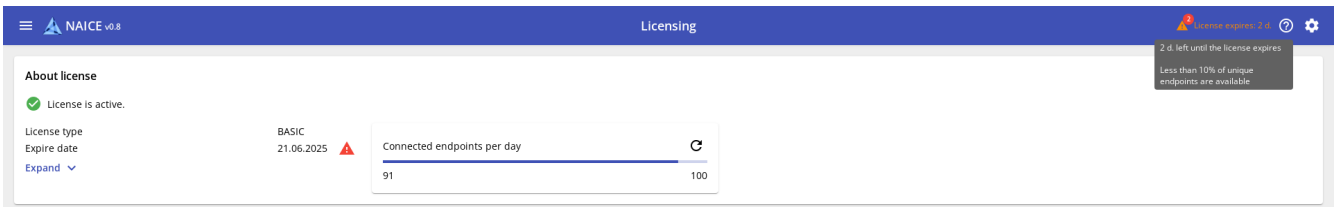

Figure 253. Warnings about reaching limits

When approaching the license or demo mode limit in terms of the number of enabled endpoints, or when approaching the license expiration date, warnings about approaching or reaching the limits will be displayed in the upper-right part of any NAICE page. Clicking on the warning takes you to the *licensing* page.

A warning about the endpoint limit starts to be displayed when the counter reaches a value of 90% of the licensed limit.

A warning about the approaching expiration date of the license starts to be displayed 90 days before that date.

In addition to being displayed at the top of the pages, these warnings are displayed on the Licensing page opposite the corresponding parameter in the form of ⚠.

Unavailability of the ELM server

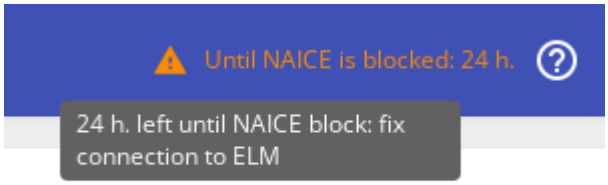

Figure 254. Warning about the unavailability of ELM

NAICE must periodically update the parameters of the current ELM license on the ELM server. If NAICE could not receive the parameters during the next update, the countdown to NAICE lock starts from that time. The countdown is displayed in the upper right part of the page, similar to the warnings about reaching the limits.

If access to ELM is not restored within **72 hours**, the licensed NAICE functionality will be blocked and the license will be reset. After resetting the license, you will need to reactivate it.

To check the availability of the ELM server, you can use the following command:

```
$ curl -k https://<ELM IP address>:<ELM port>/elm/Hello
```

If the ELM server is available, the output of the command will look like:

```
{"server-info":
{"version":"1.4","build":"10","root":true,"serverType":"elm","daemonMode":"server","serverMode":"r
type":"elm","protocol-supported":2,"protocol-actual":4},"status":2,"result":"OK"}
```

Unavailability of the EPG service

The continuous operation of the epg-service container is necessary for the smooth operation of the file license. In case of disconnection or loss of connection with this container, the license will be reset after 12 hours. The epg-service container is included in NAICE by default and works together with other containers.

Changing environment settings

If the total time spent working with the license on the current server configuration is less than 30 days, then if the server environment settings are changed, the license will be forcibly reset after 14 days.

If the total time spent working with the license on the current server configuration is more than 30 days, then if the server environment settings are changed, the license will be forcibly reset after 30 days.

Licensing Scenarios

License transfer to another host

It is possible to edit the hostname of the downloaded license. This may be required when using a NAICE cluster, when license files have been mistakenly uploaded to another host.

To edit the hostname of the downloaded license, you need to set the license to the **Backup** status, and then hover the cursor over the hostname value of the selected license. The icon will appear to the right of the hostname value.

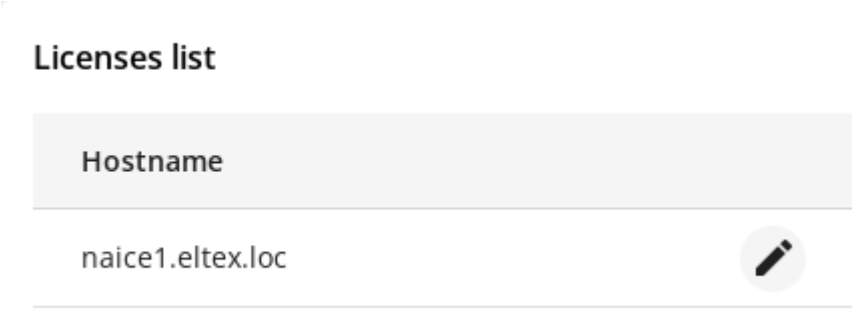

Figure 255. Editing the hostname

After clicking on the icon, a new host for the license will be selected. Save your choice.

If necessary, activate the new license by clicking on in the Action column.

Changing the license composition

If you need to change the composition of the license - to increase the number of endpoints, to enable the TACACS+ functionality - you need to contact the Eltex company.

Online connection to the ELM server

If you use an online connection to the public licensing server of Eltex, after making changes to the license, the update will occur automatically, within 1 hour.

If you need to perform a compulsory license update:

1. Switch the current license to to the **Backup** status.
2. Reactivate the license

Connecting to Offline ELM

If you use an Offline ELM server, you will need to obtain a new bundle license file with a modified license composition from Eltex and install it in Offline ELM.

After downloading the new license bundle, the update will happen automatically, within 1 hour. The forced updating of the license parameters is performed in the same way as for an online connection.

PLR license

If you use a PLR license, you will need to obtain a new license file from Eltex company with a modified license structure.

After you receive the new license file, you must download it in the same way as Uploading the product key.

Full license replacement

If it is necessary to replace one license with another, the general algorithm of actions is as follows:

1. Transfer the current license to the status **Backup**.
2. Load the product key of the new license according to the Uploading the product key.
3. Activate the new license according to License activation.
4. If desired, delete the previous license.

Reactivation of the PLR license

License reactivation is the reactivation of a file license when changing the environment settings to which the license is linked.

Reactivation may be required in the following cases:

- Cloning a virtual machine image.
- Change the configuration of disks, RAM and processor.
- Reinstallation of the system running the software.

It is allowed to increase the RAM and the number of processor cores without the need for reactivation.

The reactivation procedure is similar to the procedure for License activation, except that the product key has already been uploaded. The following steps must be performed:

1. Re-generate the license activation file for the changed environment by selecting the corresponding additional action in the "License List" table for the required license.

Transfer the new activation file to the Eltex company.

If one of the collected environment parameters is changed, after sending the activation file, the generated license will no longer match the host machine. In this case, you will need to download a new activation file and attach it to the application. It is better not to allow this.

Get a new license file.

The license file must be uploaded to the system in the same way as Uploading the product key.

Renewal of the PLR license

Due to the specifics of the implementation of file licensing, periodic regular renewal of the PLR license is required.

The renewal procedure is similar to the procedure of Reactivation of the PLR license.

End user license agreement

This End User License Agreement (this "Agreement") contains information about the legal relationship between the users of this software and the copyright holder – ELTEX Ltd. (ELTEX).

1. This Agreement is a contract entered into between an individual or legal entity agreeing to these terms and ELTEX Ltd. (ELTEX), which governs the end user's use of the software, embedded programs, software interfaces, user interfaces, and any other type of instructions or code provided by ELTEX that accompany or refer to this Agreement, along with any related documentation (hereinafter — the "Software").
2. By installing, running, or otherwise using the Software, the user (i) confirms that they have read and understand this Agreement, (ii) agrees to comply with this Agreement, and (iii) confirms that they have the legal rights to enter into this agreement on behalf of both an individual and a legal entity.
3. This Agreement comes into effect on the earlier of the following dates: upon installation, launch, or otherwise use of the Software, and terminates upon termination in accordance with this clause (hereinafter – the "Term").
4. This Agreement automatically terminates without notice from ELTEX if the user breaches any provision or condition of this Agreement.
5. Upon termination of this Agreement, the user shall immediately cease using the Software and delete (i) the Software, (ii) any other application provided to the user on behalf of ELTEX for interaction with the Software, and (iii) any object obtained as a result of using the Software.
6. The user may terminate this Agreement by ceasing all use of the Software and deleting the Software from their devices.
7. Subject to the user's compliance with the terms of this Agreement, ELTEX grants the user a limited, revocable, non-exclusive, non-sublicensable license to use the Software during the Term solely for the user's internal purposes (not for further transfer of rights to the Software to third parties, not for sale), and for Software supplied with ELTEX equipment, solely for the purpose of supporting ELTEX equipment.
8. Ownership rights, including intellectual property rights, regarding the Software belong to ELTEX.
9. The user is not entitled to modify, distribute, publicly display, publicly perform, or create derivative works of the Software.
10. The user is not entitled to disassemble, reverse translate, decompile, attempt to discover or obtain the source code of the Software, or allow others to do so.
11. The user is not entitled to: rent, sell, lease, loan, sublicense, provide commercial hosting services using the Software, or in any other way permit third parties to use the Software.
12. The user is not entitled to: alter, circumvent, deactivate, impair, or block any software or hardware protection mechanism that ELTEX uses to protect the Software.
13. The user acknowledges that if the Software requires access to non-ELTEX owned hardware or software to perform a task or provide a function, and the user refuses such permission, the corresponding function or feature will not be available or perform properly.
14.

Certain functions of the Software may require access to specific software and/or hardware. Where permission is required, the user hereby grants ELTEX permission during the Term to access all software embedded in ELTEX equipment, if necessary for the Software to perform these functions.

15. Nothing in this Agreement grants the user any rights to new versions of the Software. If ELTEX, at its sole discretion, introduces updates, fixes, or corrective inserts into the Software made available during the Term, without providing replacement terms, this Agreement shall apply to such updates, fixes, and corrective inserts.
16. Provided that the functionalities and features of the Software remain substantially the same thereafter, ELTEX may automatically update the Software without the user's consent.
17. The user acknowledges and agrees that ELTEX may, in accordance with the law, collect anonymized personal data related to the user's use of the Software, including data generated by the Software, and/or data generated by any device on which the software is installed that interacts with the Software.
18. The user acknowledges and agrees that ELTEX may, in accordance with the law, create records of aggregated data using anonymized personal data.
19. The user acknowledges and agrees that ELTEX may, in accordance with the law, use records of aggregated data to improve the Software, develop new software or services, understand industry trends, create and publish technical documentation, reports or databases summarizing the foregoing, for research purposes and to assist in resolving and/or preventing actual or potential illegal activities and, in general, for any lawful purpose related to ELTEX's commercial activities, and also retain anonymized personal data upon deletion of the Software.
20. Written consent to ELTEX's offer to replace the software usage agreement and, accordingly, approval of such replacement may be given by clicking a button presented in the replacement agreement, or by using the Software after the replacement agreement is presented.
21. Third-party resources that may be linked to or accessible through the Software are not considered part of the Software, and ELTEX may, at its discretion, disable the integration of a third-party resource or the compatibility of the Software with a third-party resource.
22. The Software is provided "as is" and "as available." To the maximum extent permitted by law, ELTEX disclaims all warranties, express, implied, or statutory, including, but not limited to, implied warranties of merchantability, satisfactory quality or fitness for a particular purpose, reliability or availability, accuracy, absence of viruses, non-infringement of third-party rights or other rights. ELTEX does not warrant that this software will operate and remain available without interruption or errors. Advice or information obtained by the user from ELTEX or its partners, in writing or orally, in no way affects this disclaimer of warranties regarding the software and does not create additional warranties.
23. Certain third-party resources may be included in or accessible through the software. ELTEX makes no representations about any third-party resource. As ELTEX has limited or no control over such resources, the user acknowledges and agrees that ELTEX is not responsible for such resources. In particular, the user understands and agrees that the user uses the third-party resource at their own risk and assumes all risks associated with unsatisfactory quality, performance, accuracy, or labor costs. The user agrees that ELTEX is not directly or indirectly liable for any damages and losses, including any damage or loss of data resulting from or alleged to result from, or in connection with the use of or reliance on, a third-party resource available in or through such software. The user understands and agrees that the use of any third-party resource is subject to the terms, license agreement, privacy policy, or other similar agreements, and that any information or personal data knowingly or unknowingly provided by the user

to the providers of such resources will be subject to the third party's privacy policy, if any. ELTEX is not responsible for disclosure of information and any other actions of the third party. In particular, ELTEX makes no guarantees regarding the third party's receipt of user data and the third party's use of the user's personal information.

24. In no event shall ELTEX be liable to the user or any third party for damages incurred in connection with the use of or access to any component of the software or the inability to use or access any component of the software, including, but not limited to, damages arising from errors, omissions, interruptions, defects, delays in operation or transmission, computer viruses, and any other direct, indirect, actual, incidental, punitive, or consequential damages, even if ELTEX has been advised of the possibility thereof. Notwithstanding the foregoing, ELTEX's aggregate liability for all losses, damages, causes of action, including under contract, tort, or other liability, arising out of the use of the software or in connection with any provisions of this agreement, shall not exceed the fair market value of that component of the software.
25. The foregoing limitations, exclusions, and disclaimers of liability in this agreement apply to the maximum extent permitted by applicable law, even if the applied remedy fails its essential purpose.
26. In the event of a breach by the user of any provision of this Agreement, ELTEX shall be entitled to recover monetary compensation for the damages incurred from the user.
27. This Agreement is governed by the laws of the Russian Federation.