

NAICE

Table of Contents

Main page	1
RADIUS widgets	6
TACACS+ widgets	19
SMS widgets	32
Monitoring	34
RADIUS	34
Connections journal	34
Active sessions	38
TACACS+	42
Connections journal	42
Accounting	46
System	49
System events	49
System Events List	52
Log Collectors	66
Users and devices	78
System users	78
Accounts	78
Roles	97
Network resources	112
Devices	112
Device groups	124
Device profiles	137
Identity management	146
Network access users	147
Network user groups	159
Endpoints	170
Endpoints groups	183
External identity sources	196
Identity sequences	221
Network access	227

Policy elements	227
Authorization profiles	227
Allowed Protocols	231
Dictionaries	235
Conditions	237
RADIUS Session Limits	247
RADIUS policies	249
Authentication and authorization policies	256
Profiling	262
Profiling conditions	262
Profiling policies	268
Logical profiles	277
Guest portals	283
Guest endpoints	283
Portal users	286
Portal builder	290
Device access	300
Policy elements	227
Conditions	300
TACACS+ Command sets	310
TACACS+ profiles	325
Network devices policies	329
TACACS+ policy configuration	334
Notification gateways	341
Notification gateways management	341
HTTP/HTTPS	345
SMTP	349
System settings	352

System	49
Common settings	352
Services	353
RADIUS	353
TACACS+	355
Event log	355
Licensing	356
Connection to ELM	356
Security and access	358
System Log In	358
Password policies	364
Lockout policy	366
Two-factor authentication	368
Interaction with Active Directory	369
Certificate store	373
Trusted Certificates	373
Server Certificates	380
Troubleshooting	380
Logs	380
Nodes	382
Licensing	383
End user license agreement	398
Account settings	401

Main 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 system user;
- All changes to widget arrangement and composition apply only to the current system user;
- 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

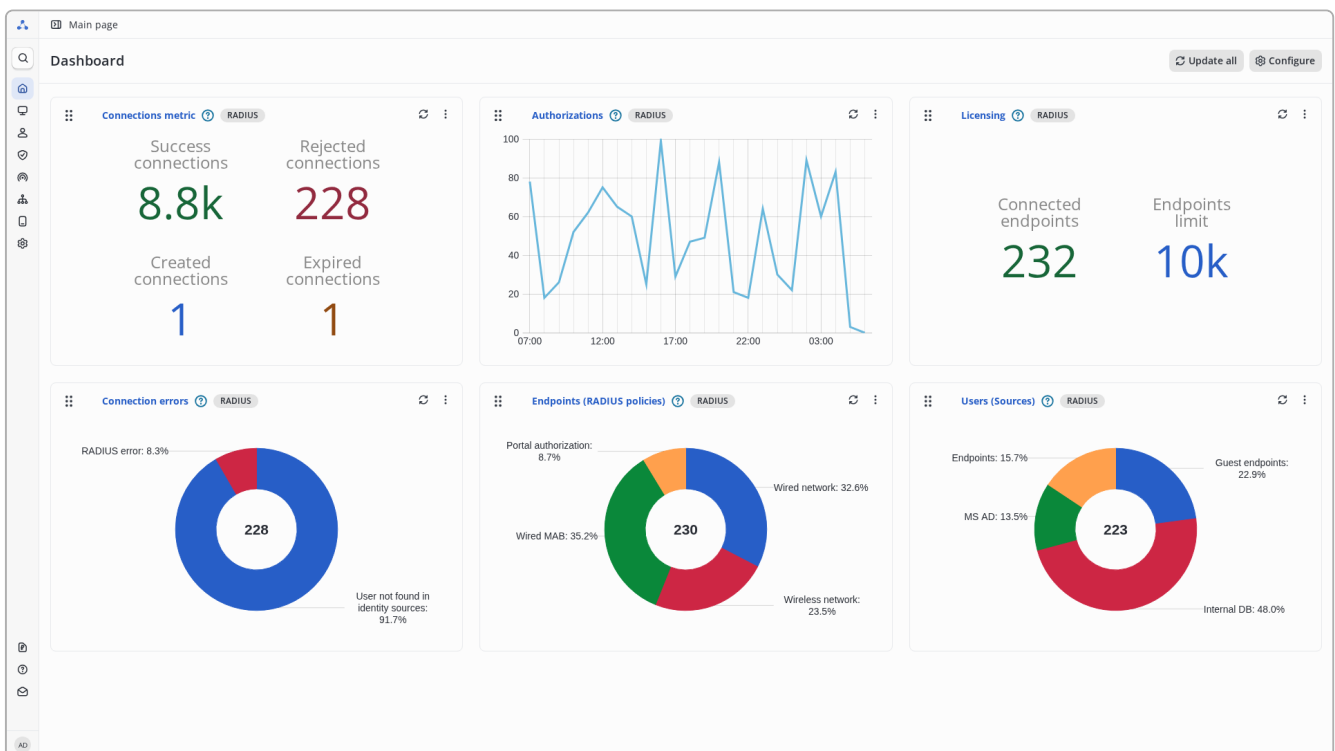






Figure 1. Dashboard control panel and displayed widgets


Dashboard control elements:

- **Update all** - Refresh data for all widgets displayed on the dashboard.
- **Configure** - 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.
- **RADIUS** - widget tag. Indicates which part of the functionality the widget belongs to.
-  - 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  **Configure**, which will open the **Dashboard panel settings** window:

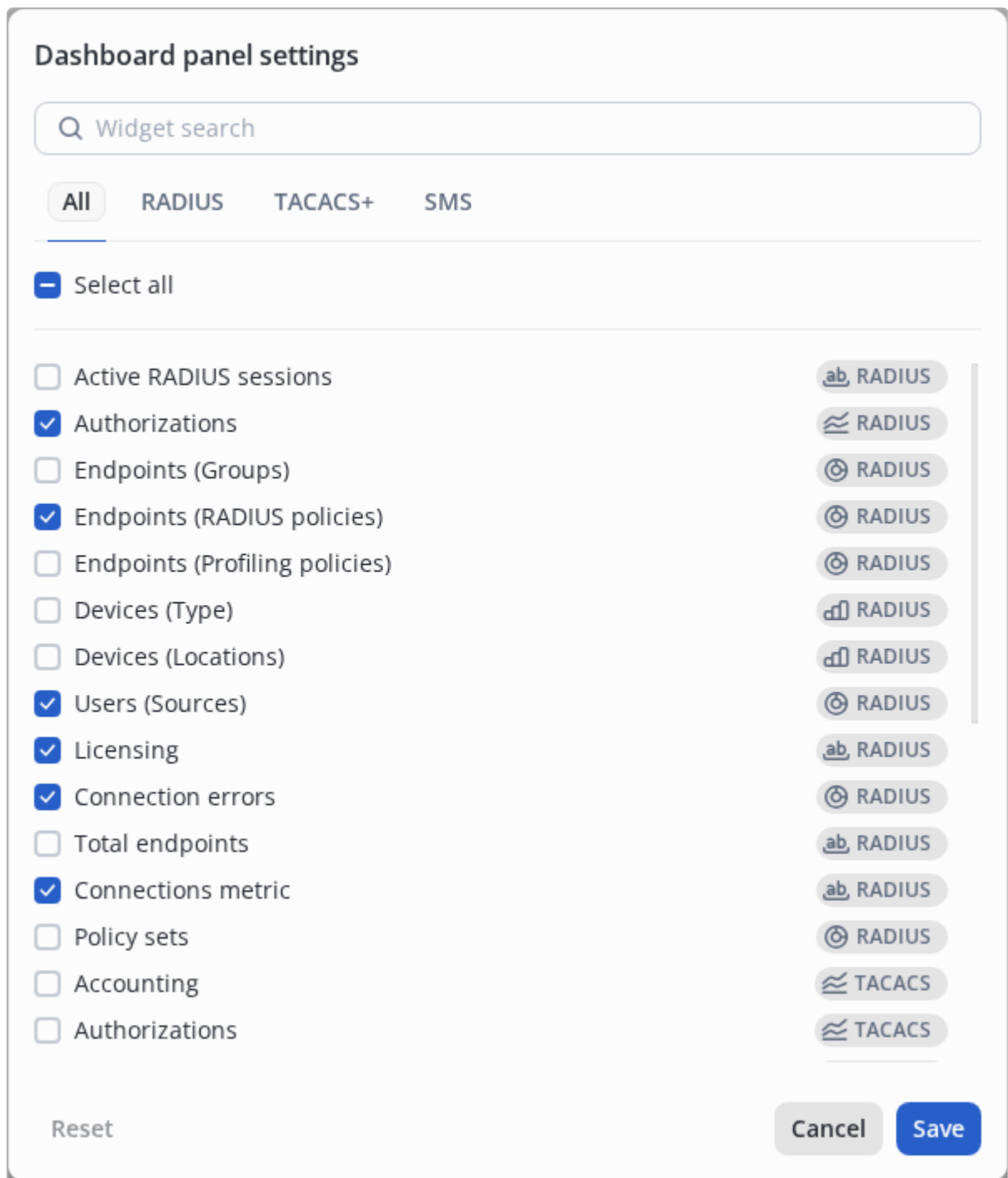




Figure 2. Dashboard panel settings window

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.
- RADIUS - Widget tag.
-  Widget Search - Widget search field.
- Reset - 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.

Widget search

For easier customization and selection of displayed widgets, they are grouped into sections, depending on what part of the functionality they relate to. Also, for greater convenience, a search for widgets by name has been implemented.

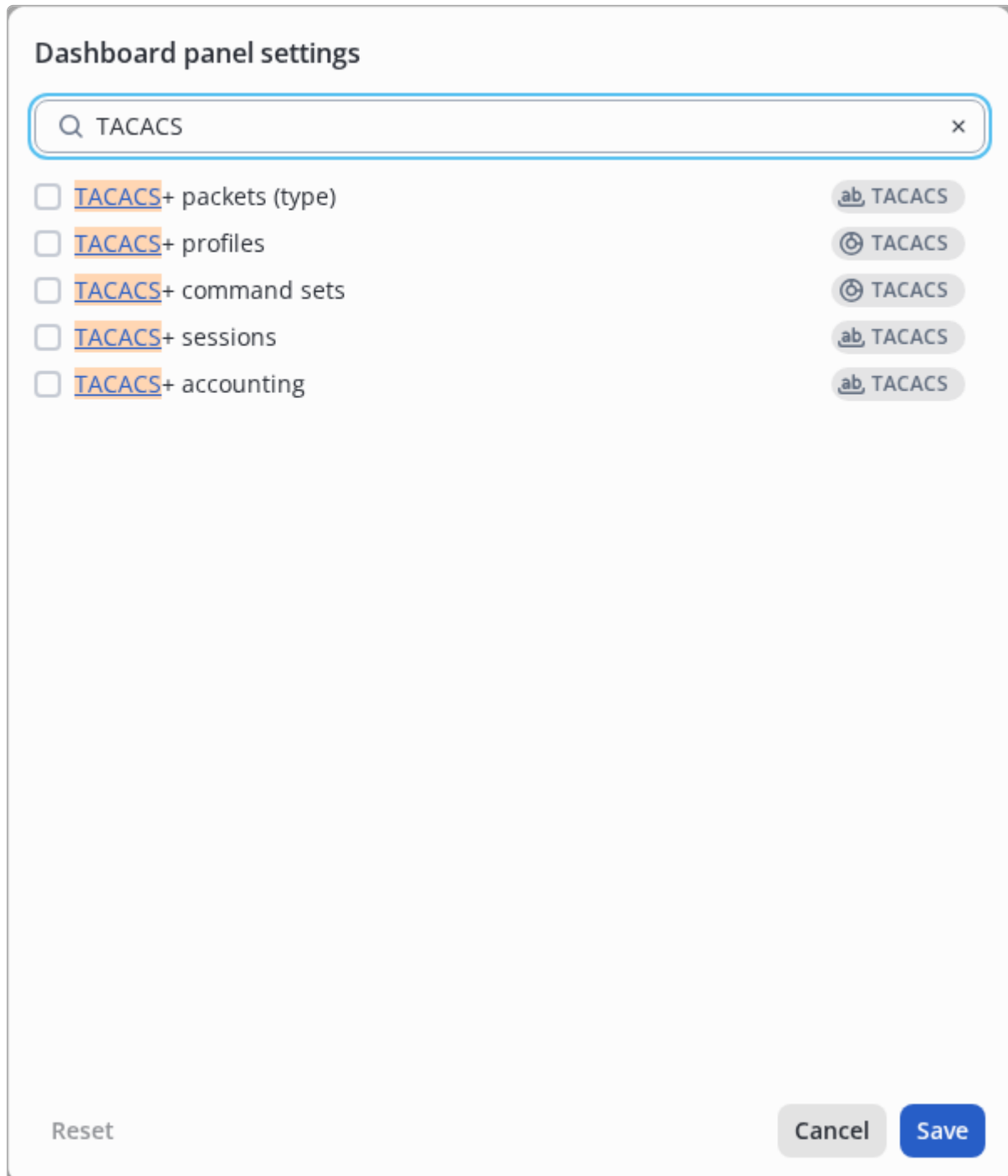


Figure 3. Widget search by name

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” button in the [Dashboard panel settings](#) window.

The standard set includes the following widgets:

- **RADIUS** Connection metrics;
- **RADIUS** Authorizations;
- **RADIUS** Licensing;
- **RADIUS** Connection errors;
- **RADIUS** Endpoints (Access policies);
- **RADIUS** Users (Sources);

Widget types

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.

Widgets with display type — Metric

Functionality:

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

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.

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.

RADIUS widgets

List of available widgets

Widget	Data display type	Brief description
Active RADIUS sessions	Metric	Count of active RADIUS sessions
Authorizations	Graph	Count of authorizations per hour for the last 24 hours
Licensing	Metric	Current count of connected endpoints and maximum allowed per license
Connection metrics	Metric	Count of connected, rejected, created, and expired connections for the last 24 hours
Total Endpoints metric	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 (RADIUS 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

Widget	Data display type	Brief description
RADIUS sessions	Metric	Total number of sessions for the entire data retention period. The retention period is displayed in days.



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



Widgets with the data display type "metric" or "pie chart" show large numbers in an short format (for example, 40k instead of 40123). The exact metric value is displayed in a tooltip when hovering over the value.

Widget "Active RADIUS sessions"

The widget displays the total number of active user sessions. All active sessions can be seen in the Monitoring section [Active sessions](#)

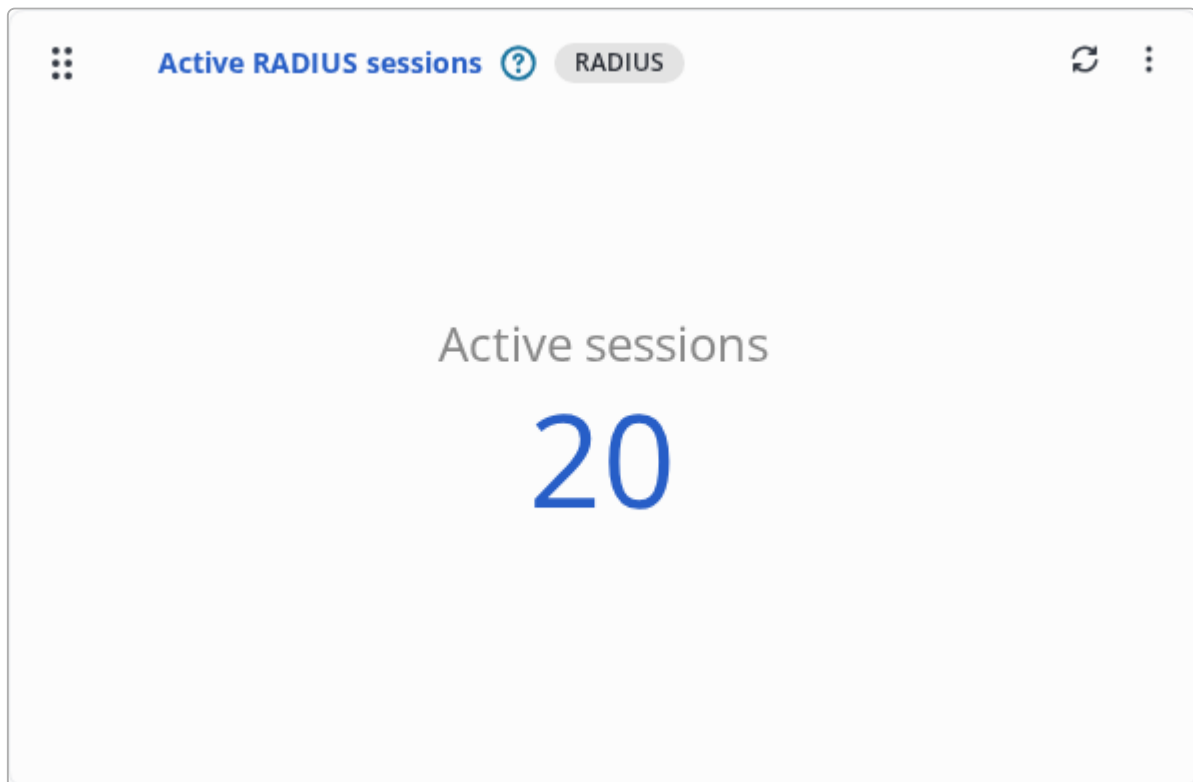


Figure 4. Widget "Active RADIUS sessions"

Widget "Authorizations"

Displays data about authorization attempts (both Connected and rejected) in the system per hour for the last 24 hours, based on [Connections journal](#) 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.

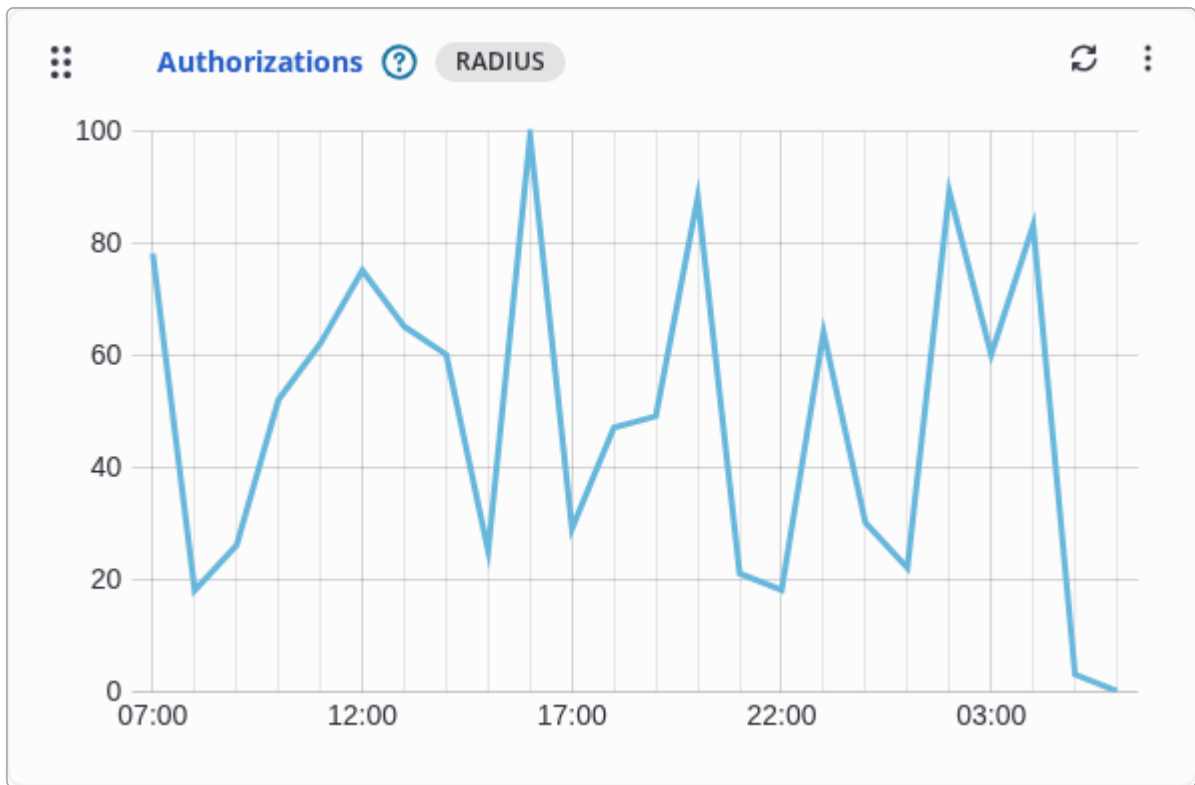


Figure 5. Widget "Authorizations"

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.

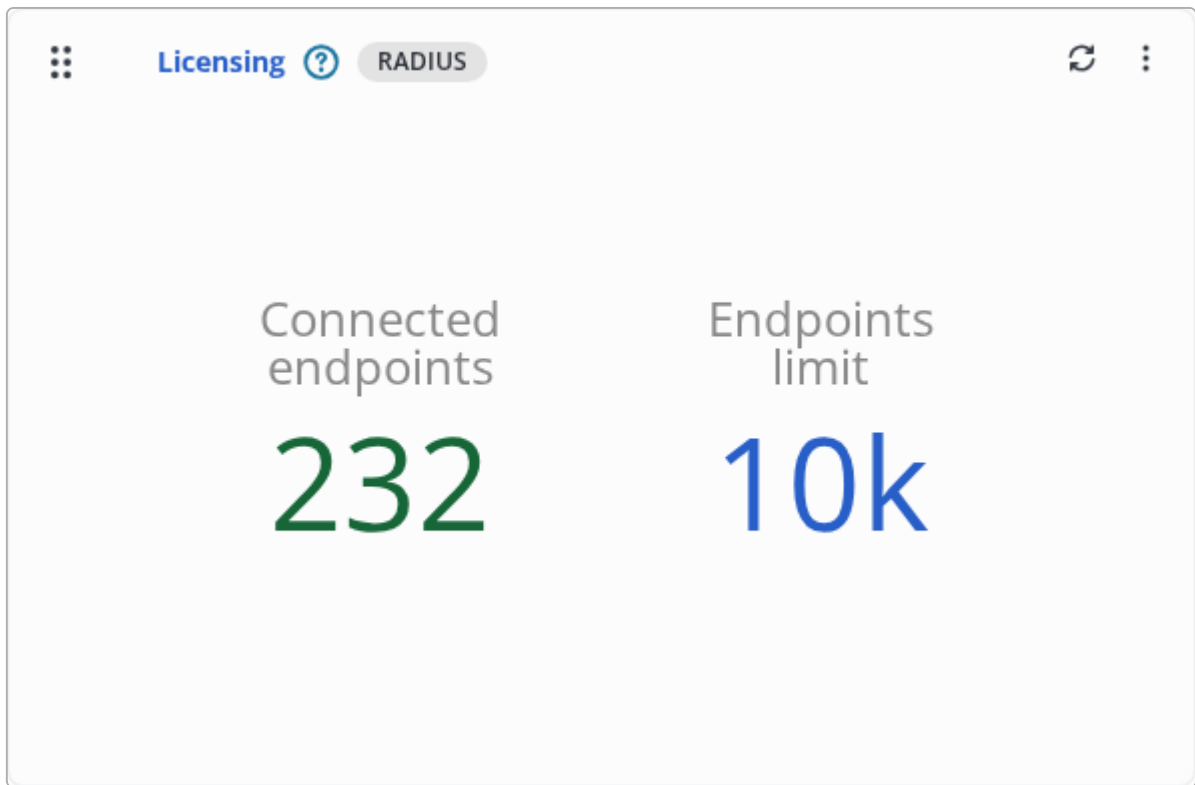


Figure 6. Widget "Licensing"

Widget "Connection metrics"

Displays connected and rejected connection counts for the last 24 hours based on [Connections journal](#) data.

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

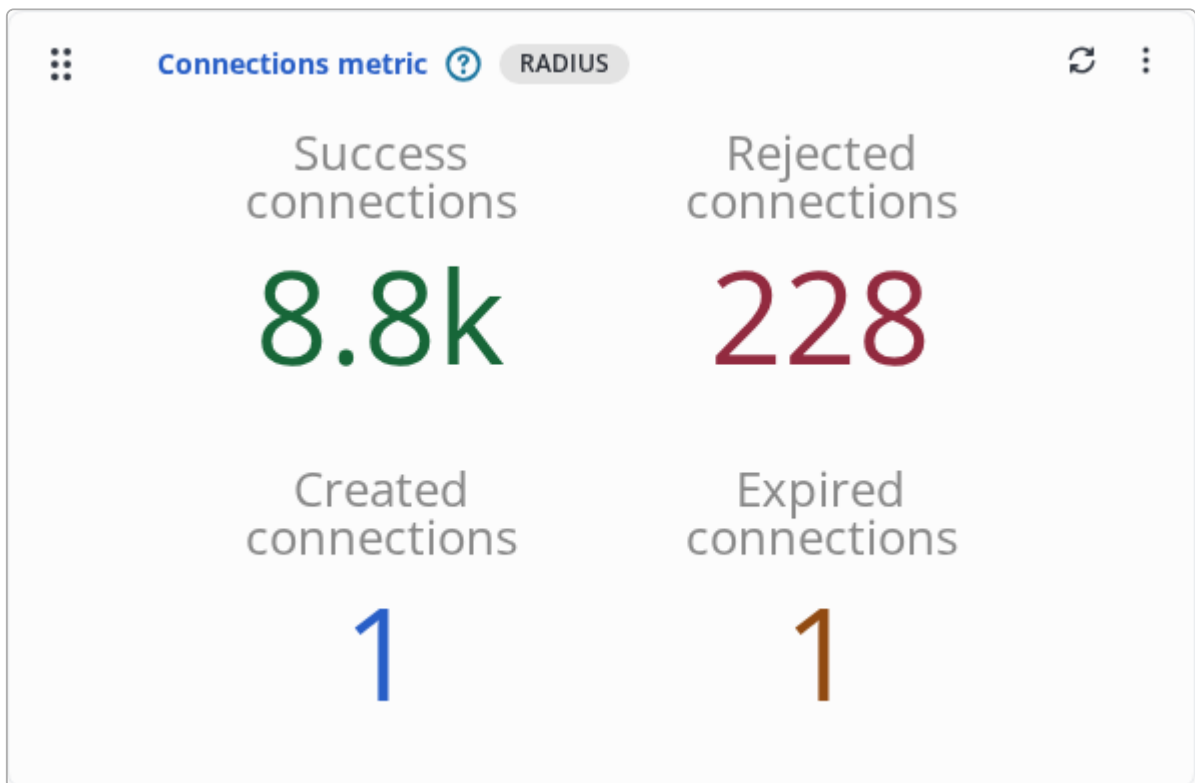


Figure 7. Widget "Connection metrics"

Widget "Total endpoints"

Displays the total count of known endpoints in the NAICE system based on data from the [Endpoints](#) table.

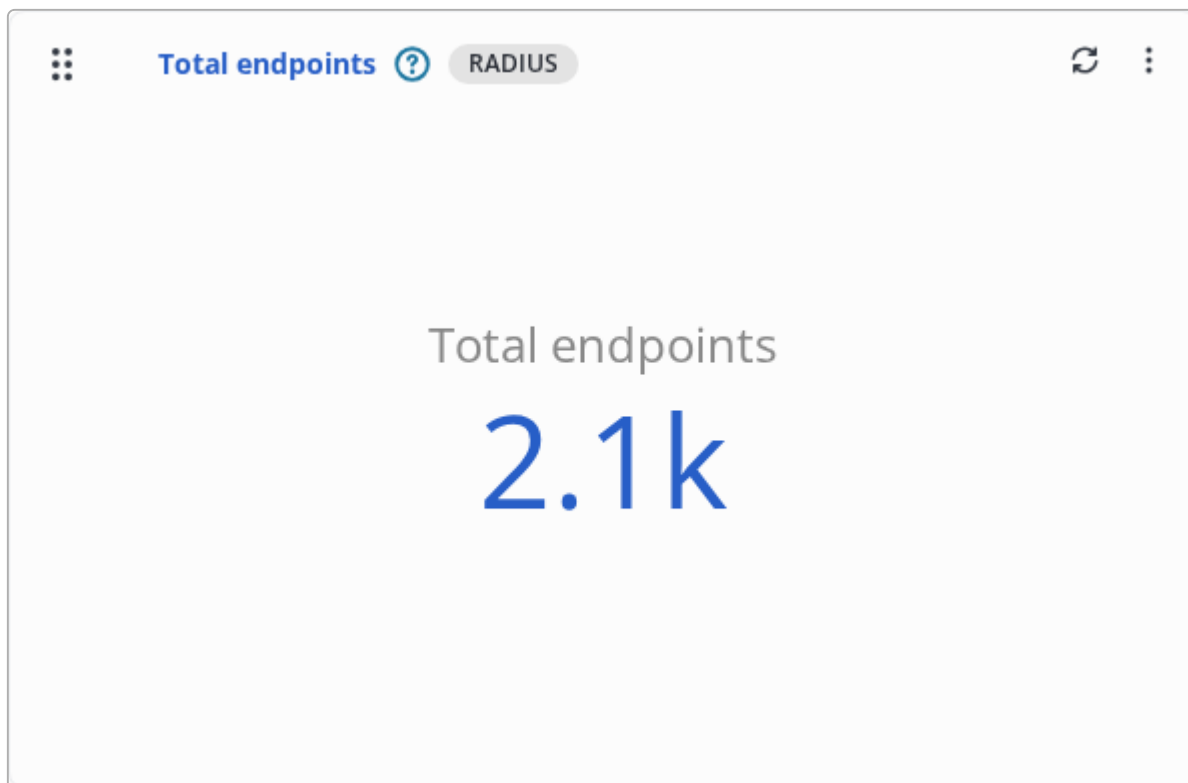


Figure 8. Widget "Total endpoints"

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.

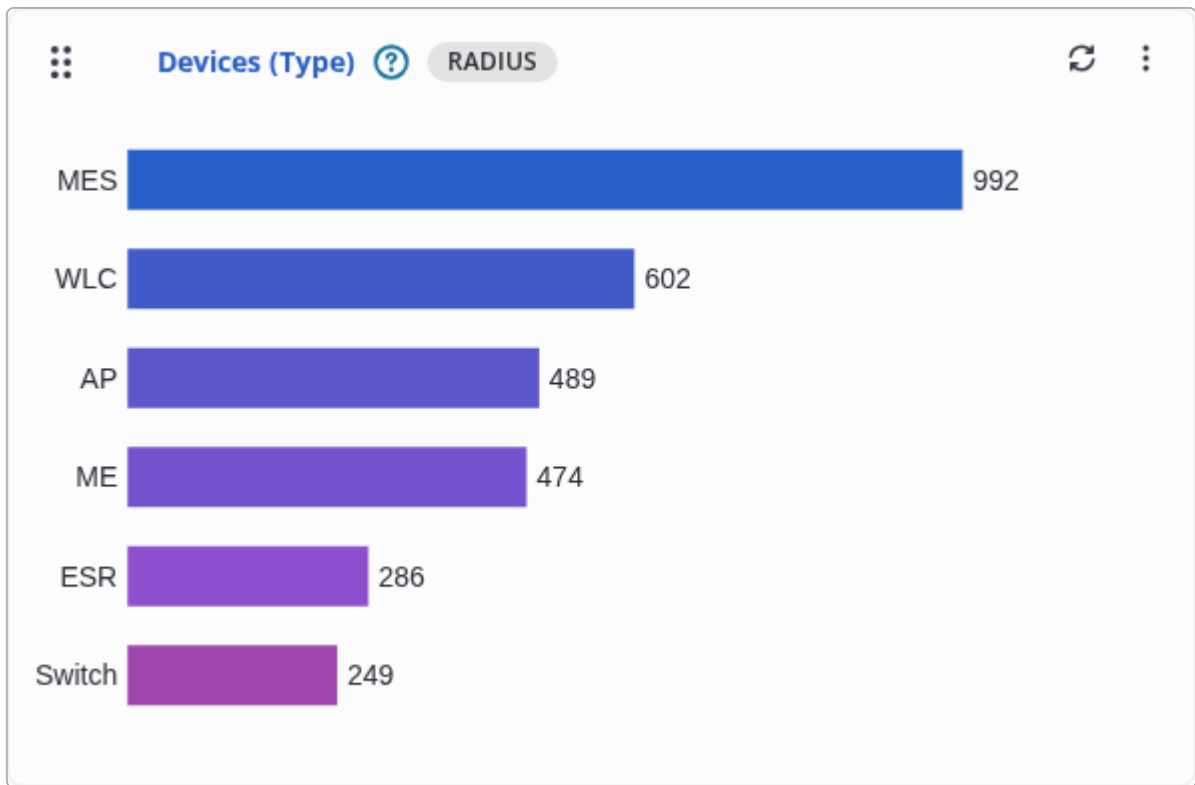


Figure 9. Widget "Devices (Type)"

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.

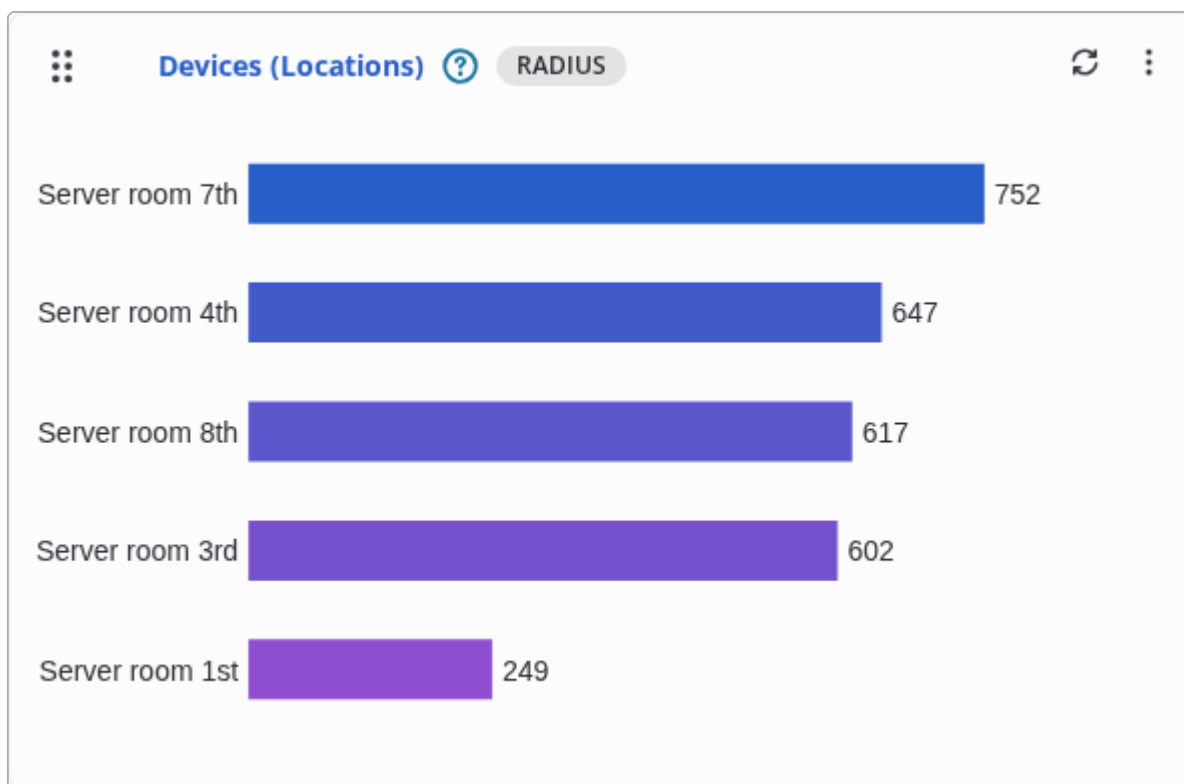


Figure 10. Widget "Devices (Locations)"

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 [Connections journal](#).

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**.

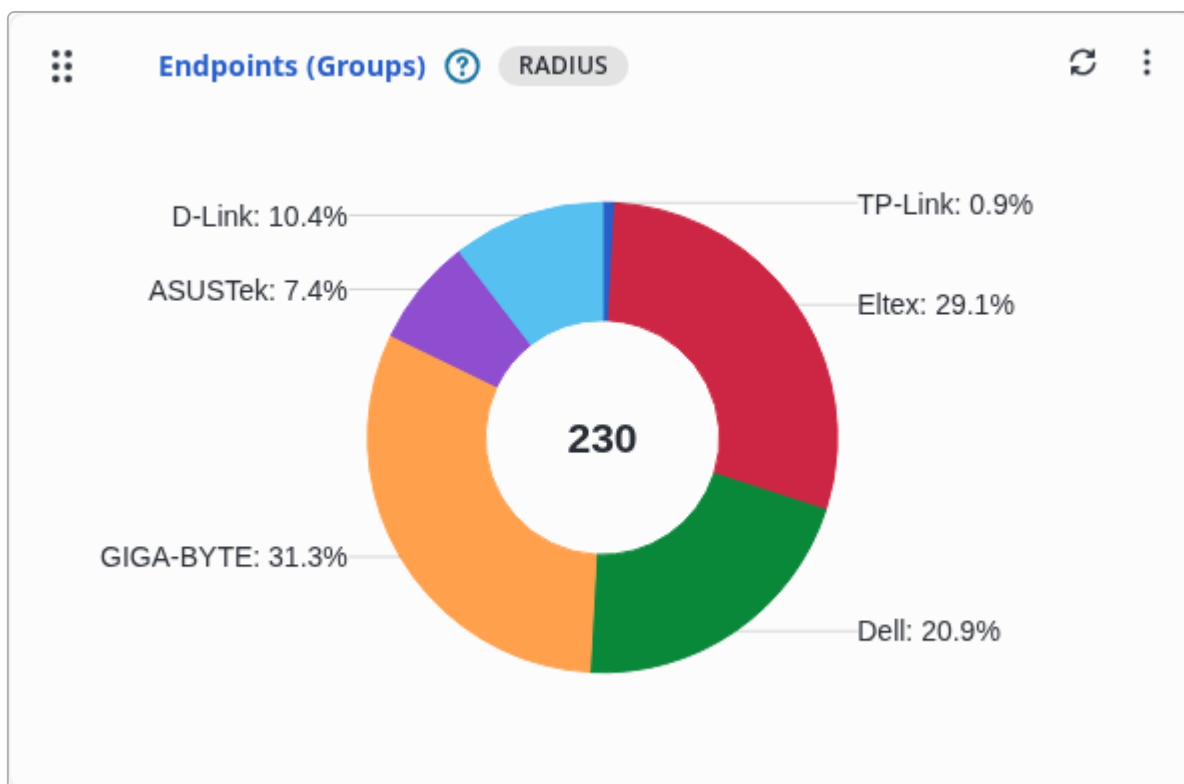


Figure 11. Widget "Endpoints (Groups)"

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 [Connections journal](#).

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**.

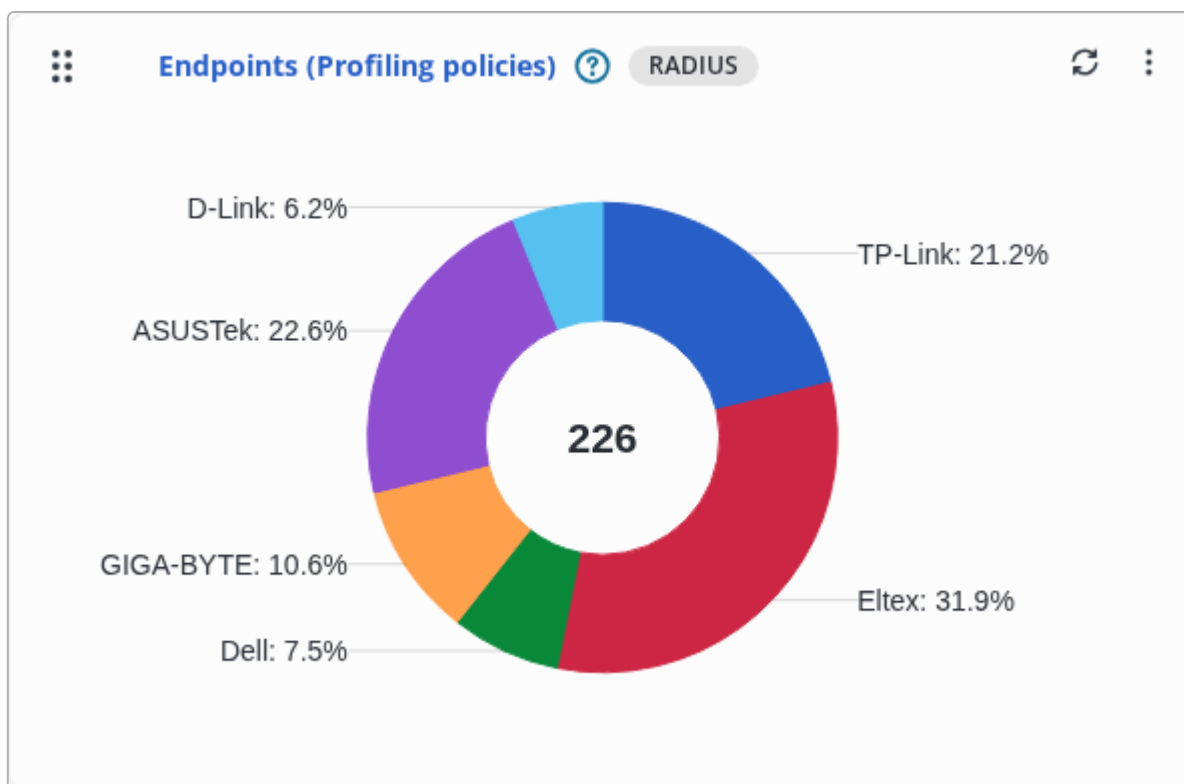


Figure 12. Widget "Endpoints (Profiling policies)"

Widget "Endpoints (RADIUS policies)"

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

Data sourced from [Endpoints](#) and [Connections journal](#).

The widget allows you to evaluate the distribution of endpoints across RADIUS 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**.

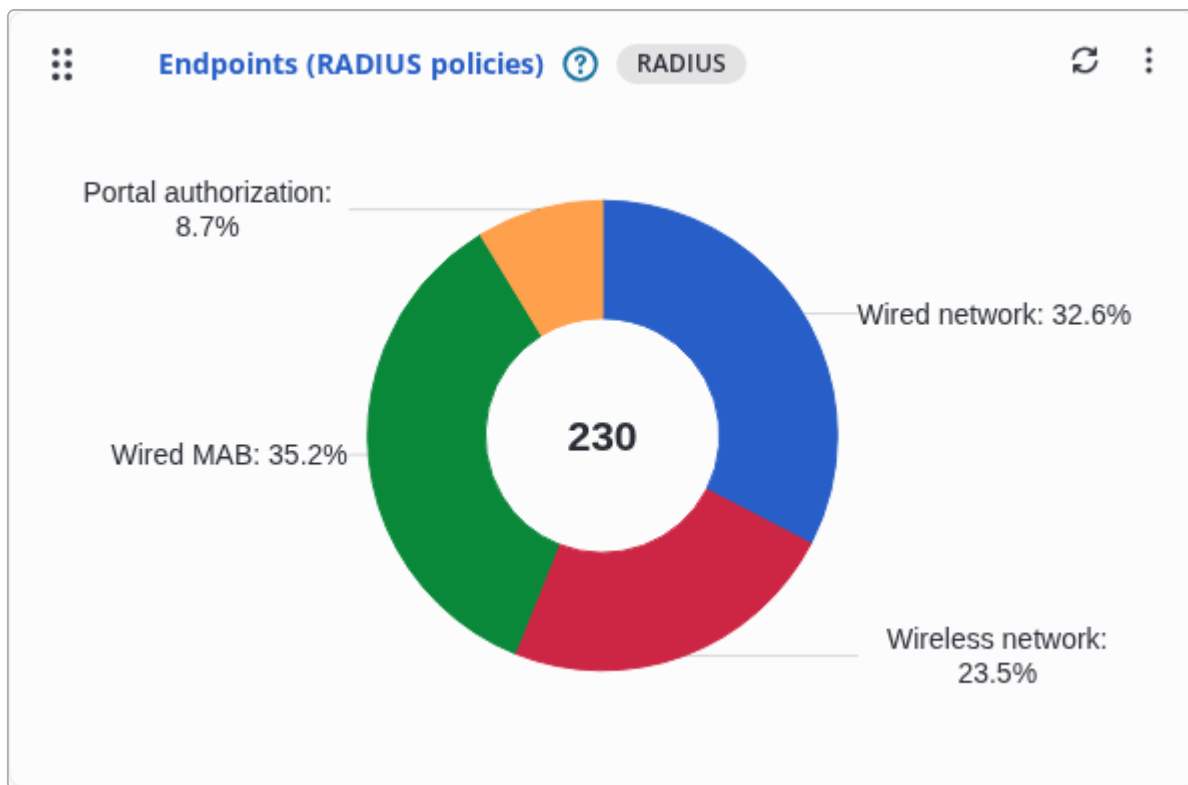


Figure 13. Widget "Endpoints (RADIUS policies)"

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.

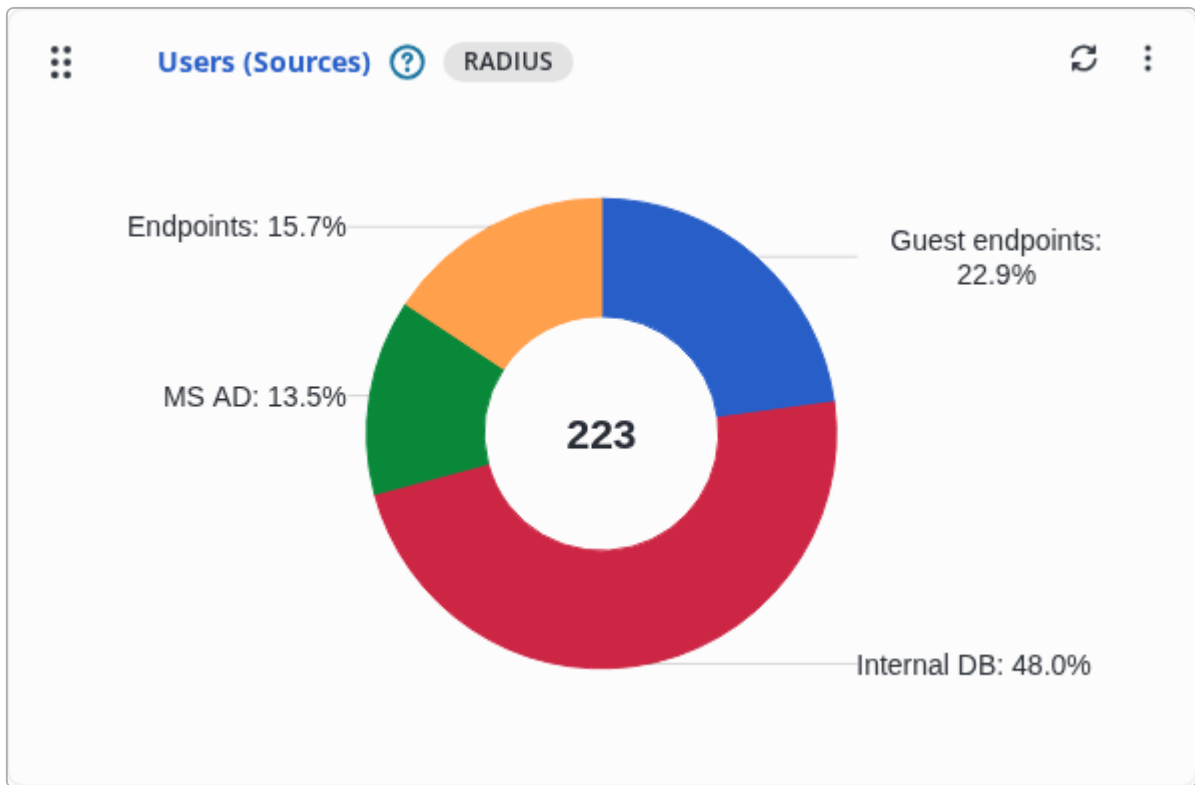


Figure 14. Widget "Users (Sources)"

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.

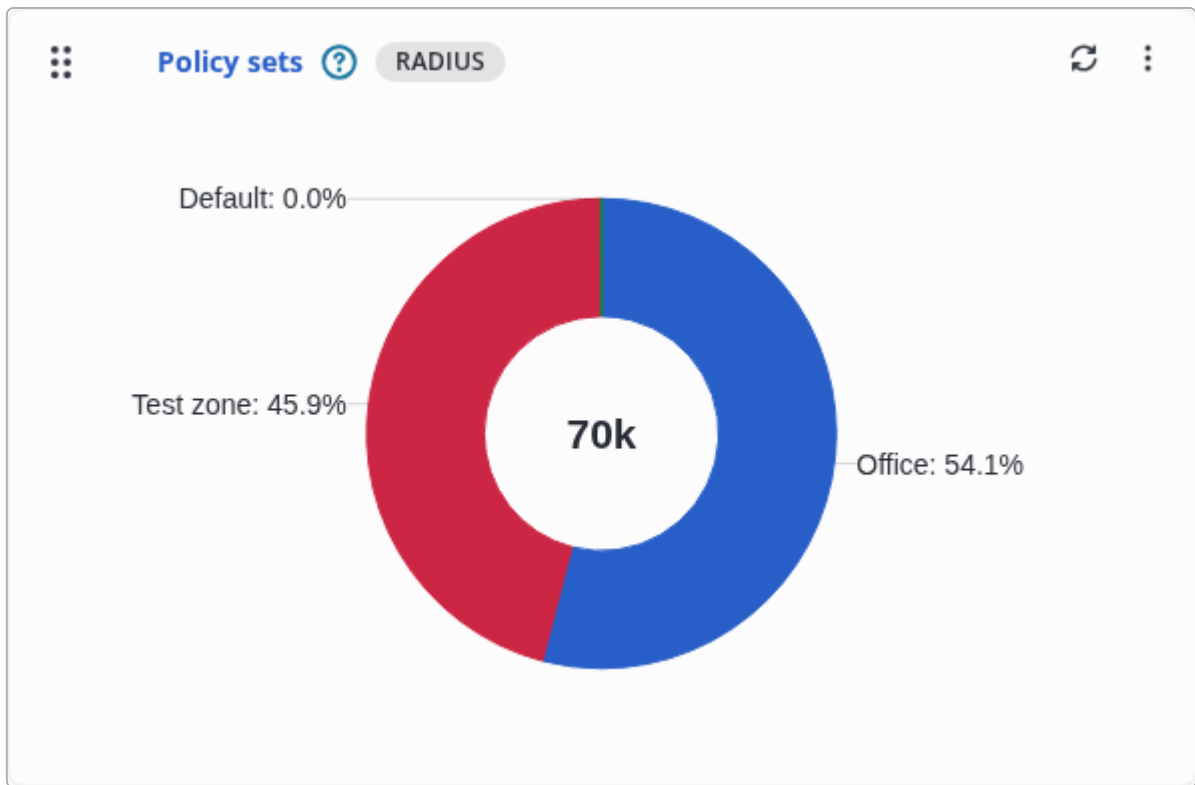


Figure 15. Widget "Policy sets"

Widget "Connection errors"

Displays client connection errors for the last 24 hours.

Connections rejected by RADIUS policies are not included.

Error data comes from [Connections journal](#).

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

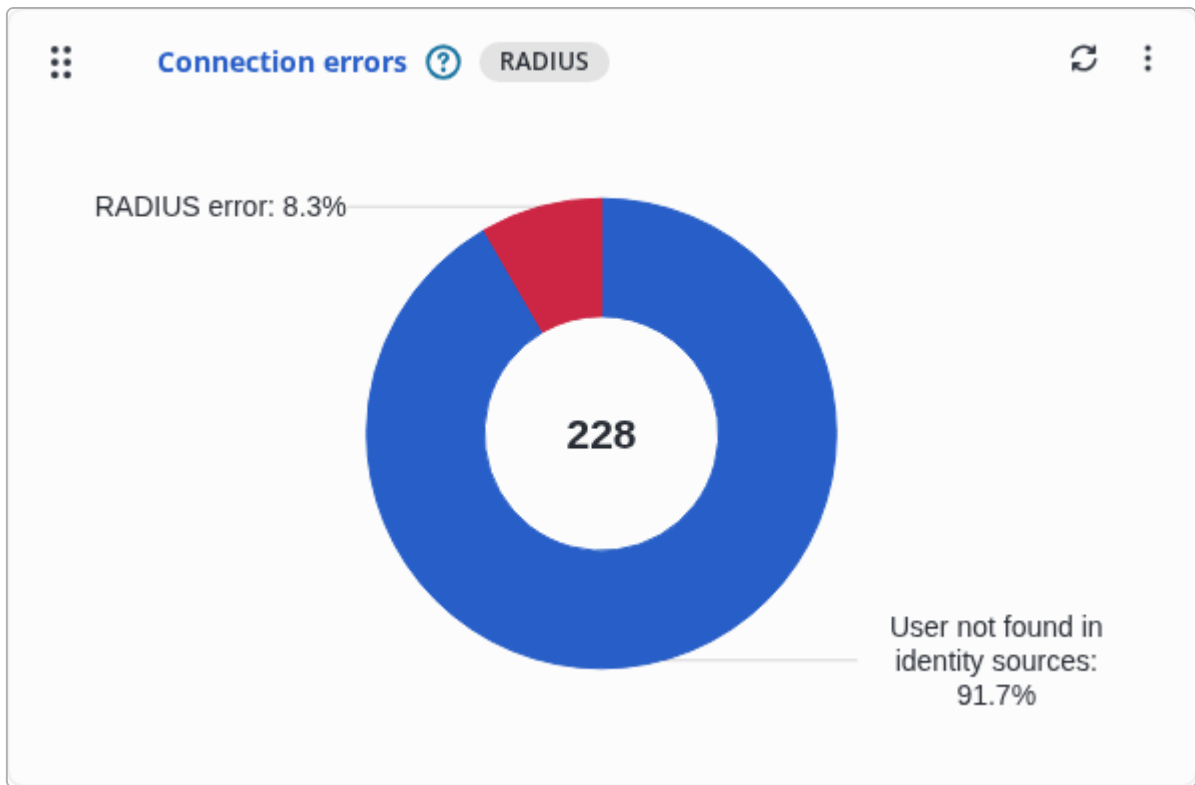


Figure 16. Widget "Connection errors"

Widget "RADIUS sessions"

The widget displays the total number of RADIUS sessions for the entire data retention period, without applying any filters during the count. The retention period is also displayed in the widget, the unit of display is days.

The list of sessions can be seen in the table [Connections journal](#).

The widget allows estimating the size of the corresponding table in the database, as well as the number of user connections over a period longer than a day.

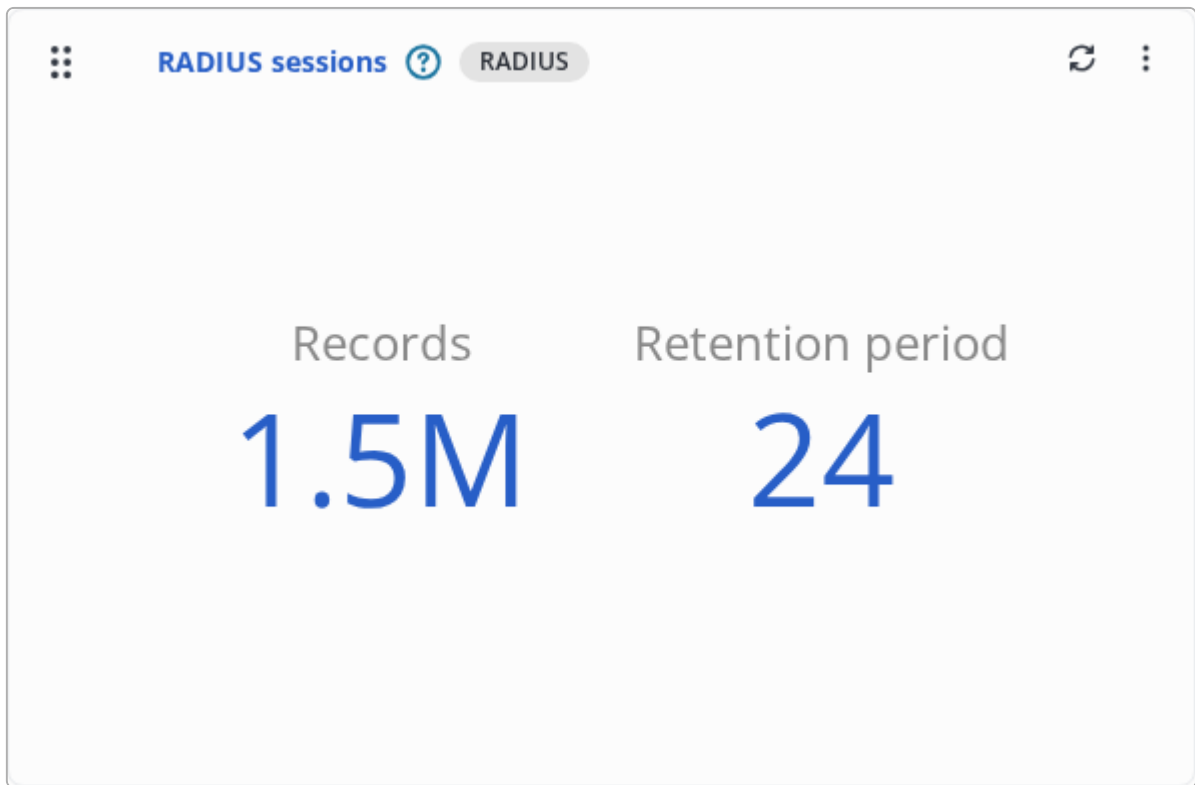


Figure 17. Widget "RADIUS sessions"

TACACS+ widgets



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

List of available widgets

Widget	Data display type	Brief description
Authorizations	Graph	Count of network administrator authorizations and authentications over the last 24 hours by hour.
Accounting	Graph	Count of accounting requests over the last 24 hours by hour.
Connection count	Metric	Count of successful and rejected connections by network administrators over the past 24 hours.
TACACS packets (type)	Metric	Count of TACACS+ packets by type received in the last 24 hours.
Devices (Type)	Histogram	Count of network devices through which the administrator connected, by network device type.
Devices (Locations)	Histogram	Count of network devices through which the administrator connected, by the location of the network devices.

Widget	Data display type	Brief description
TACACS profiles	Pie chart	Current number of TACACS+ profile hits.
TACACS Command sets	Pie chart	Current number of TACACS+ Command sets hits.
TACACS Policy Sets	Pie chart	Current number of TACACS+ policy sets hits.
Connection errors	Pie chart	Network administrator connection errors over the last 24 hours.
Users (Sources)	Pie chart	Count of unique network administrators, by source of identification, who were authorized in the last 24 hours
TACACS+ sessions	Metric	Total count of TACACS+ sessions for the entire data retention period. The retention period is displayed in days.
TACACS+ accounting	Metric	Total count of TACACS+ accounting records for the entire data retention period. The retention period is displayed in days.



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



Widgets with the data display type "metric" or "pie chart" show large numbers in an short format (for example, 40k instead of 40123). The exact metric value is displayed in a tooltip when hovering over the value.

Widget "Authorizations"

Displays data about authorization and authentication attempts (both Connected and rejected) in the system per hour for the last 24 hours, based on [Connections journal](#) data.

Data is visualized as a time graph where:

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

Enables quick monitoring of user activity and peak period identification.

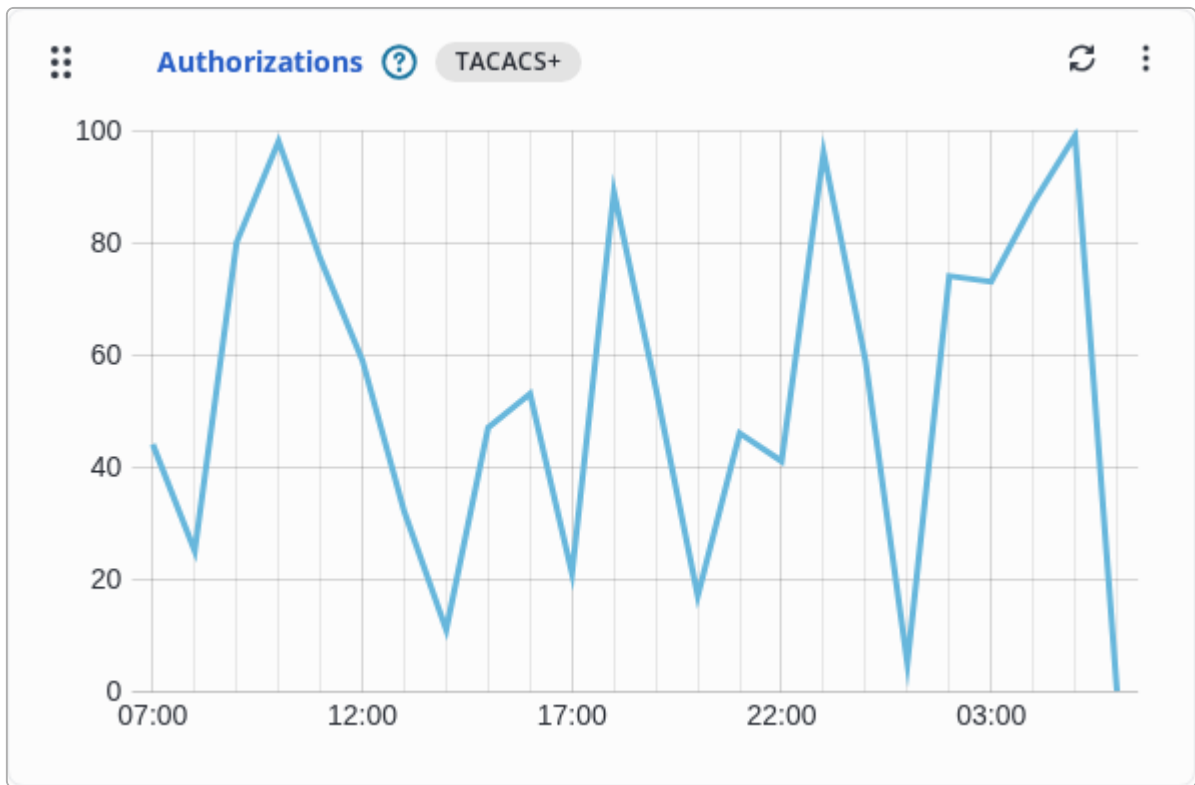


Figure 18. Widget "Authorizations"

Widget "Accounting"

Displays data on the number of accounting requests in the system per hour for the last 24 hours, based on [Connections journal](#).

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.

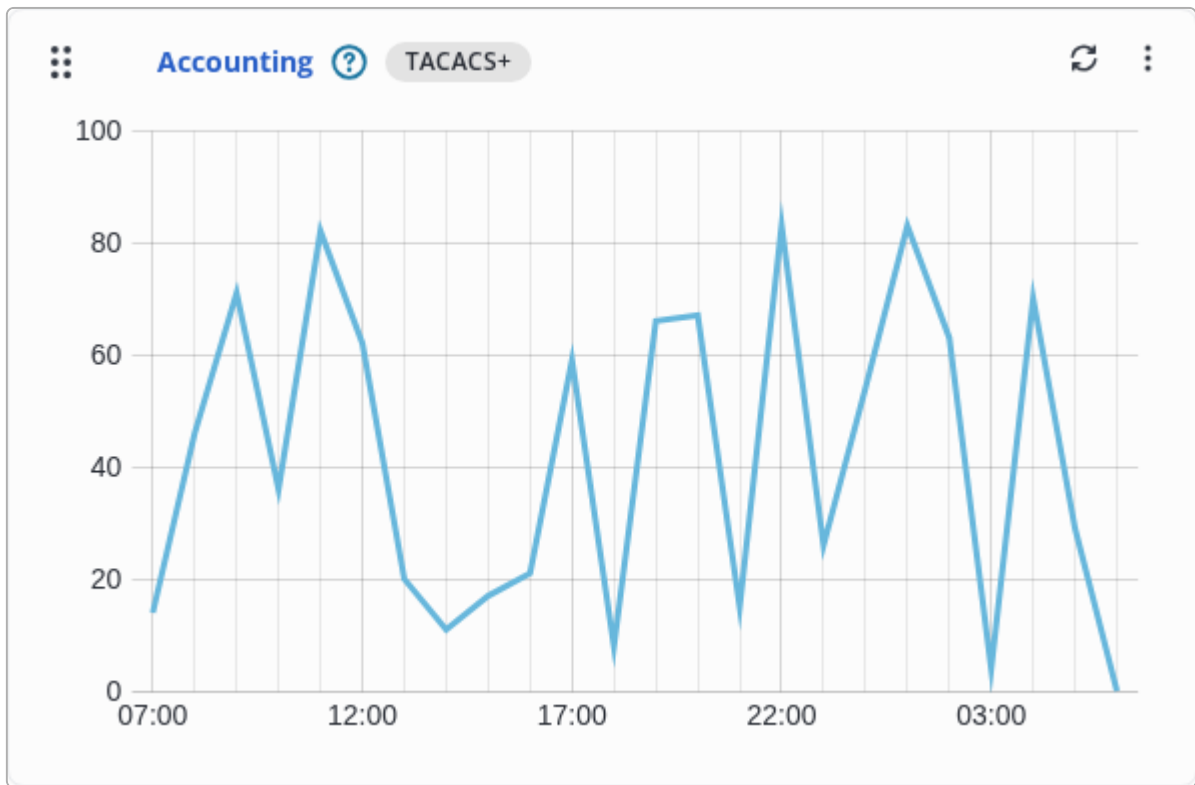


Figure 19. Widget "Accounting"

Widget "Connection count"

Displays connected and rejected connection counts for the last 24 hours based on [Connections journal](#) data.

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

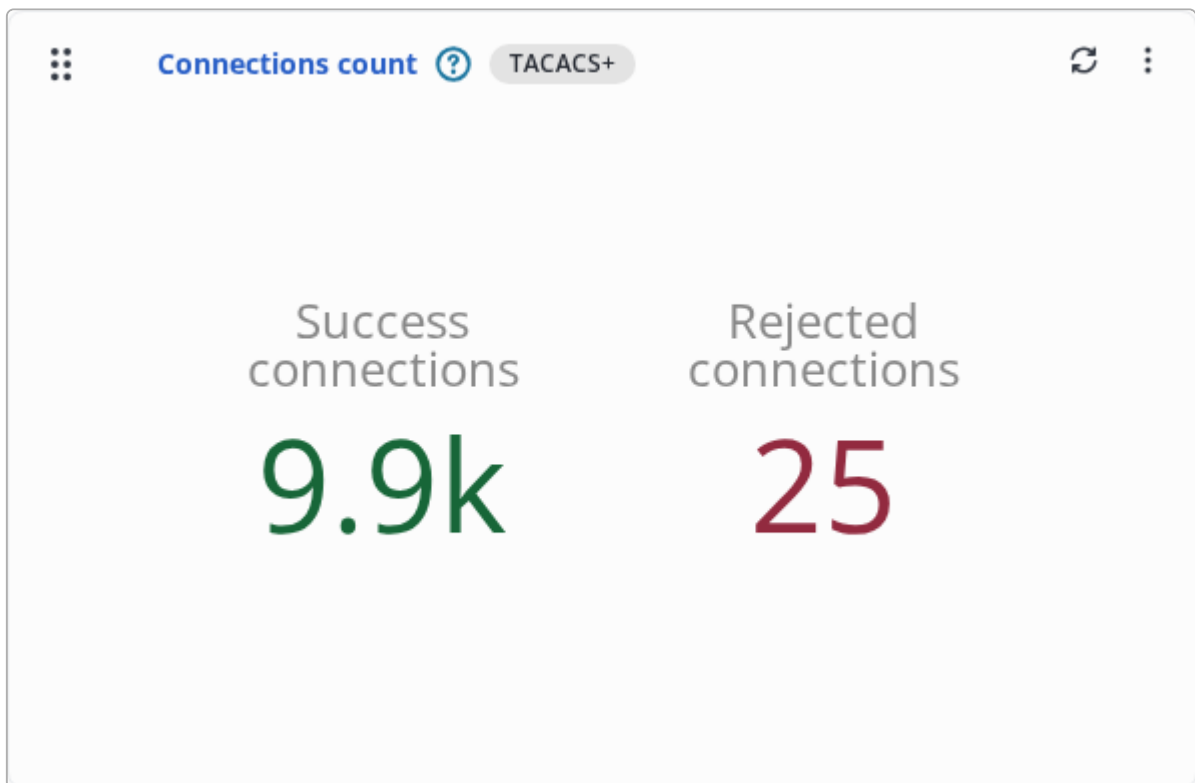


Figure 20. Widget "Connection count"

Widget "TACACS packets (type)"

The widget displays data on the number of received TACACS+ packets on network devices by packet type over the last 24 hours based on data from [Connections journal](#).

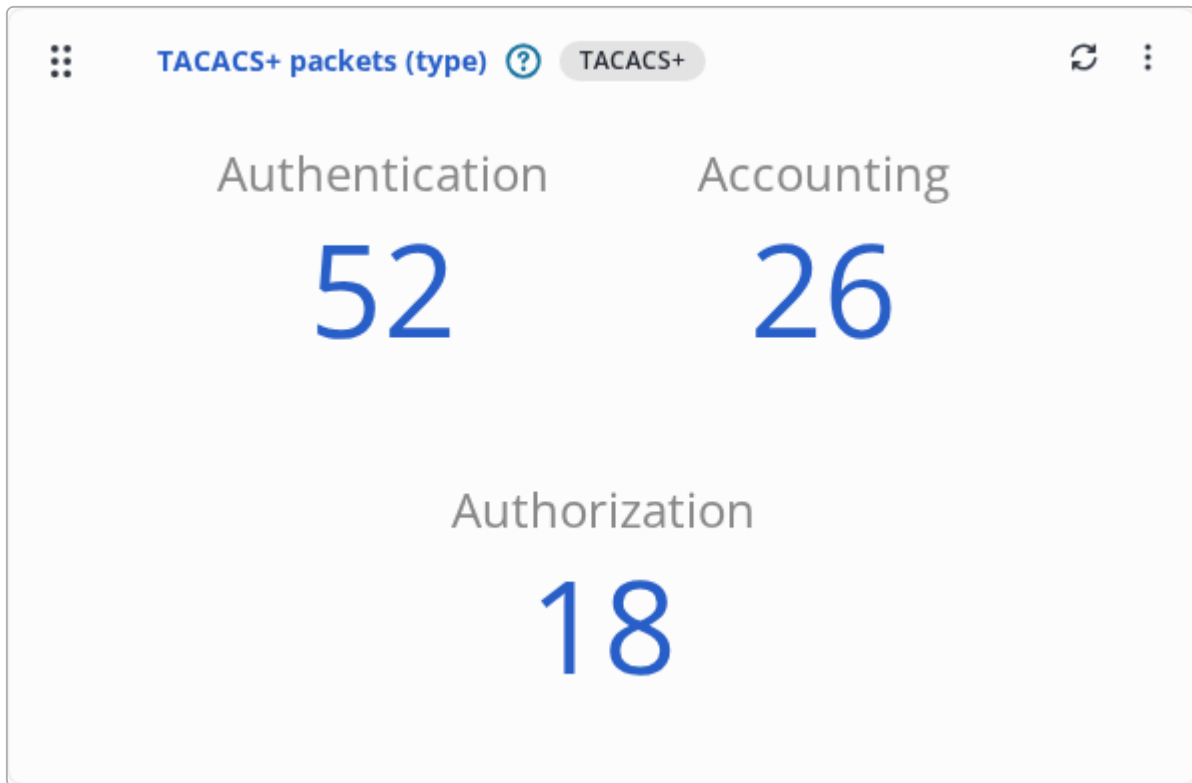


Figure 21. Widget "TACACS packets (type)"

Widget "Devices (Type)"

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

Device groups for classification come from [Device Groups](#).

Tracks device type usage trends.

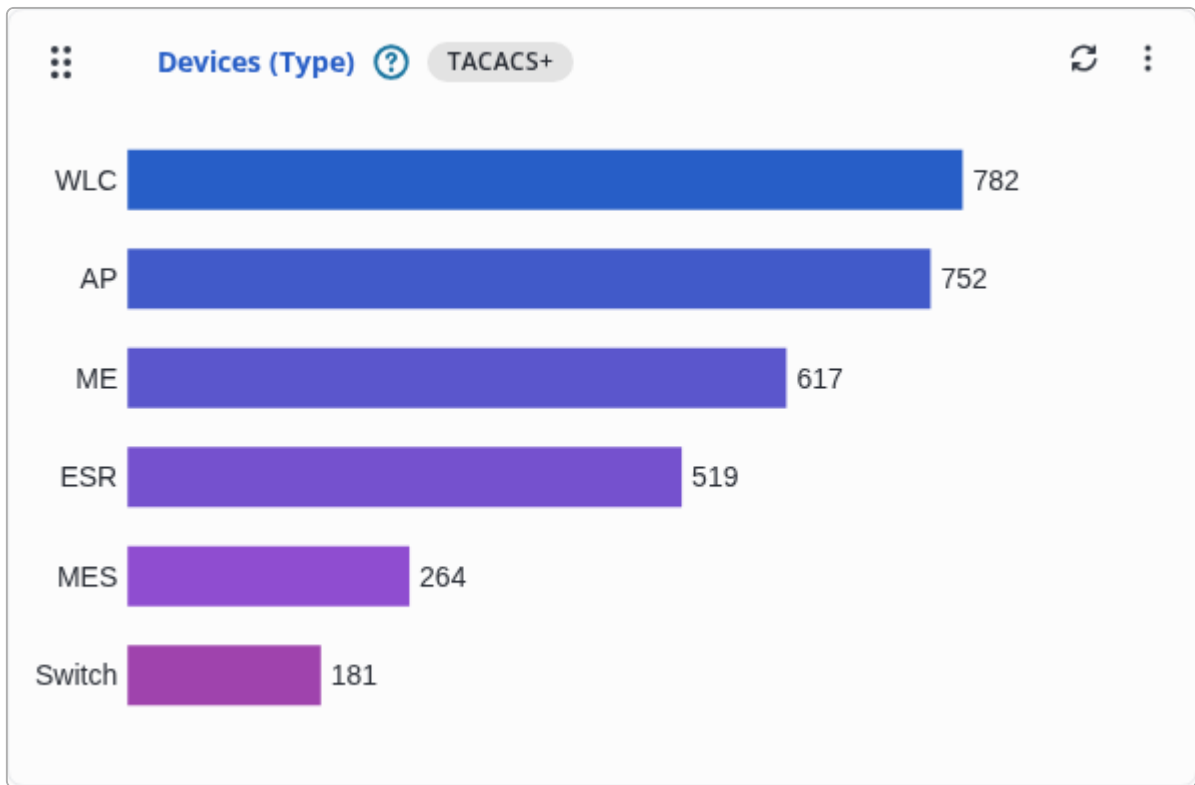


Figure 22. Widget "Devices (Type)"

Widget "Devices (Locations)"

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

Device groups for classification come from [Device Groups](#).

Tracks device location usage trends.

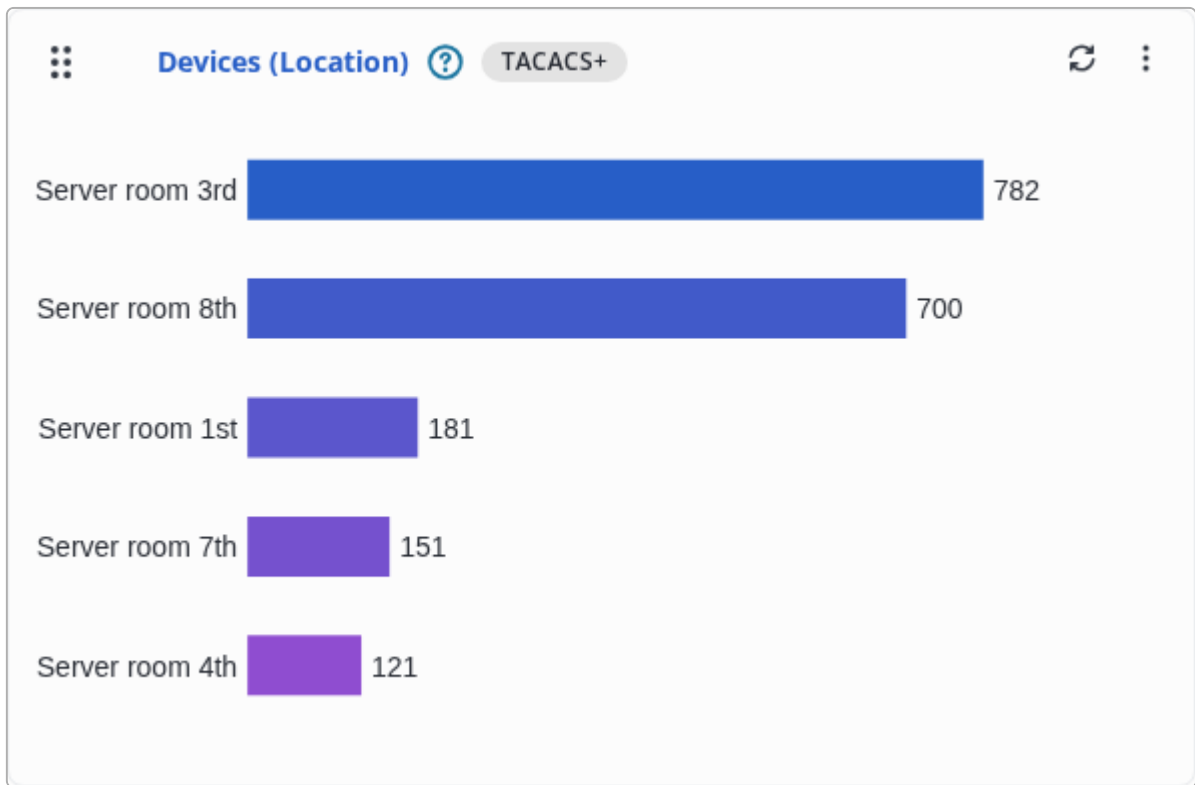


Figure 23. Widget "Devices (Locations)"

Widget "TACACS profiles"

The widget displays the current number of assigned TACACS+ profiles.

Profiles with zero hits are not displayed.

The data on the number of assigned profiles for the widget is taken from the list [TACACS Profiles](#).

The widget allows you to track the frequency of using different profiles to analyze the effectiveness of access conditions.

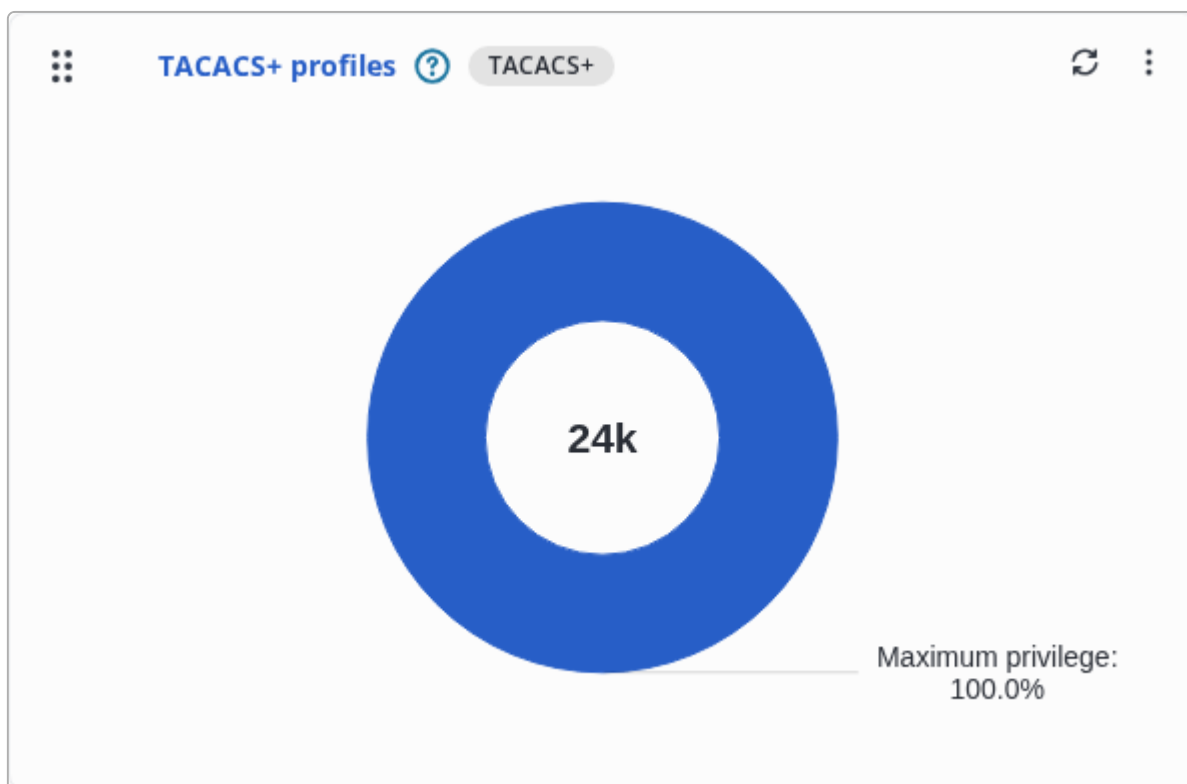


Figure 24. Widget "TACACS profiles"

Widget "TACACS Command sets"

The widget displays the current number of assigned TACACS+ Command sets.

Command sets with zero hits are not displayed.

The widget command set hit count data is taken from the [Command Sets](#) list.

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

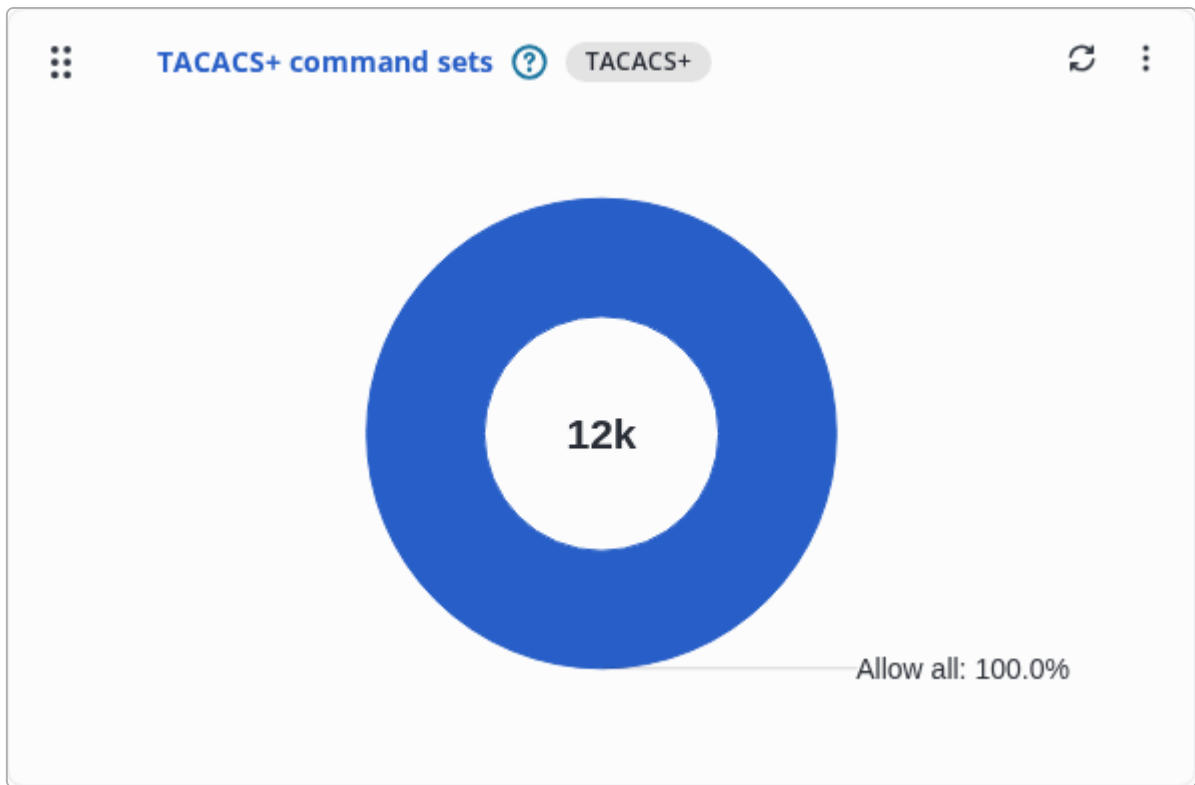


Figure 25. Widget "TACACS Command sets"

Widget "TACACS Policy Sets"

The widget displays the current number of TACACS+ policy sets being triggered.

Policies with zero triggers are not displayed.

The widget's policy set triggers are taken from the list [Policy Sets](#).

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

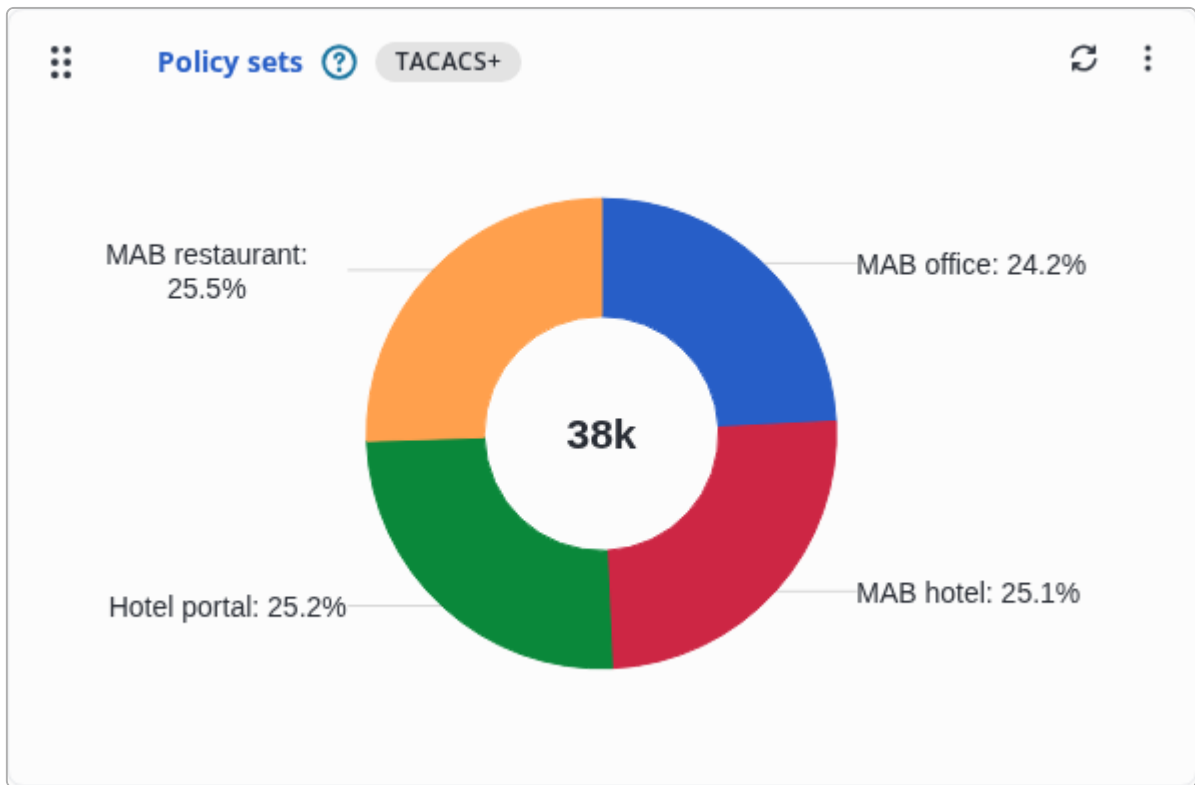


Figure 26. Widget "TACACS Policy Sets"

Widget "Connection errors"

Displays client connection errors for the last 24 hours.

Connections rejected by access policies are not included.

Error data comes from [Connections journal](#).

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

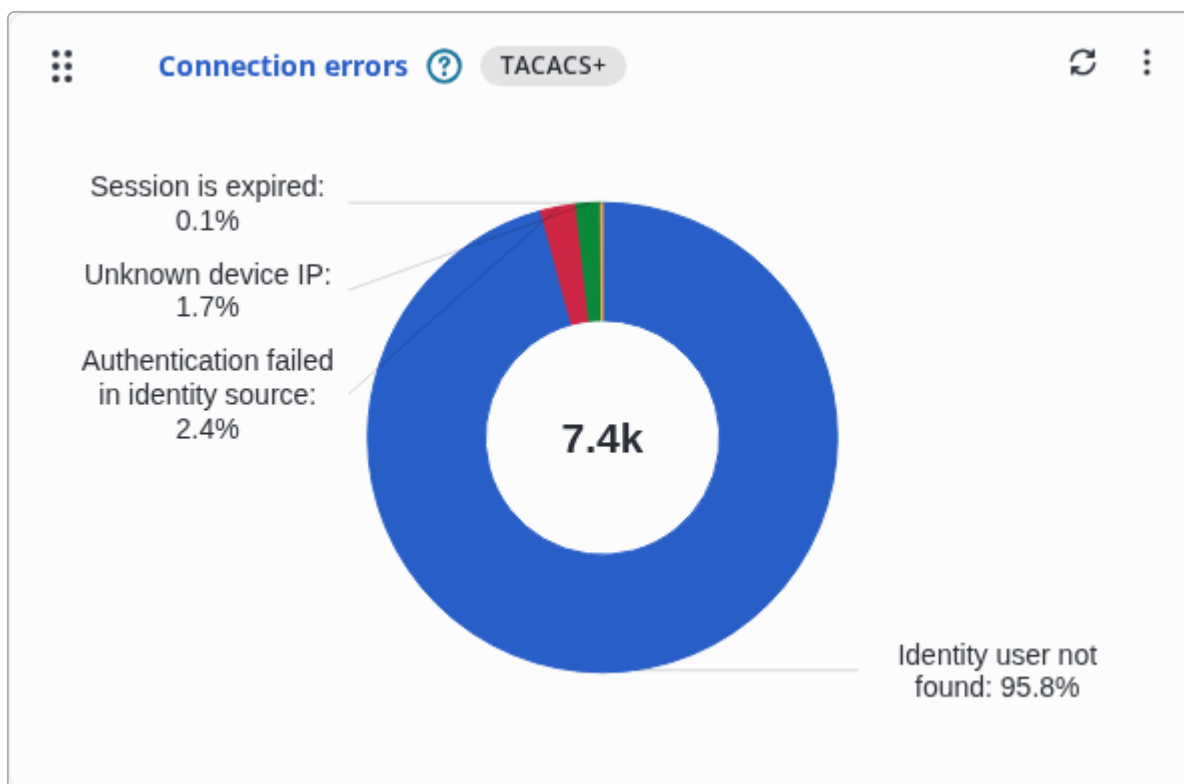


Figure 27. Widget "Connection errors"

Widget "Users (Sources)"

Displays unique system administrator 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;
- External authentication systems (LDAP/Active Directory) configured in [External identity sources](#).

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

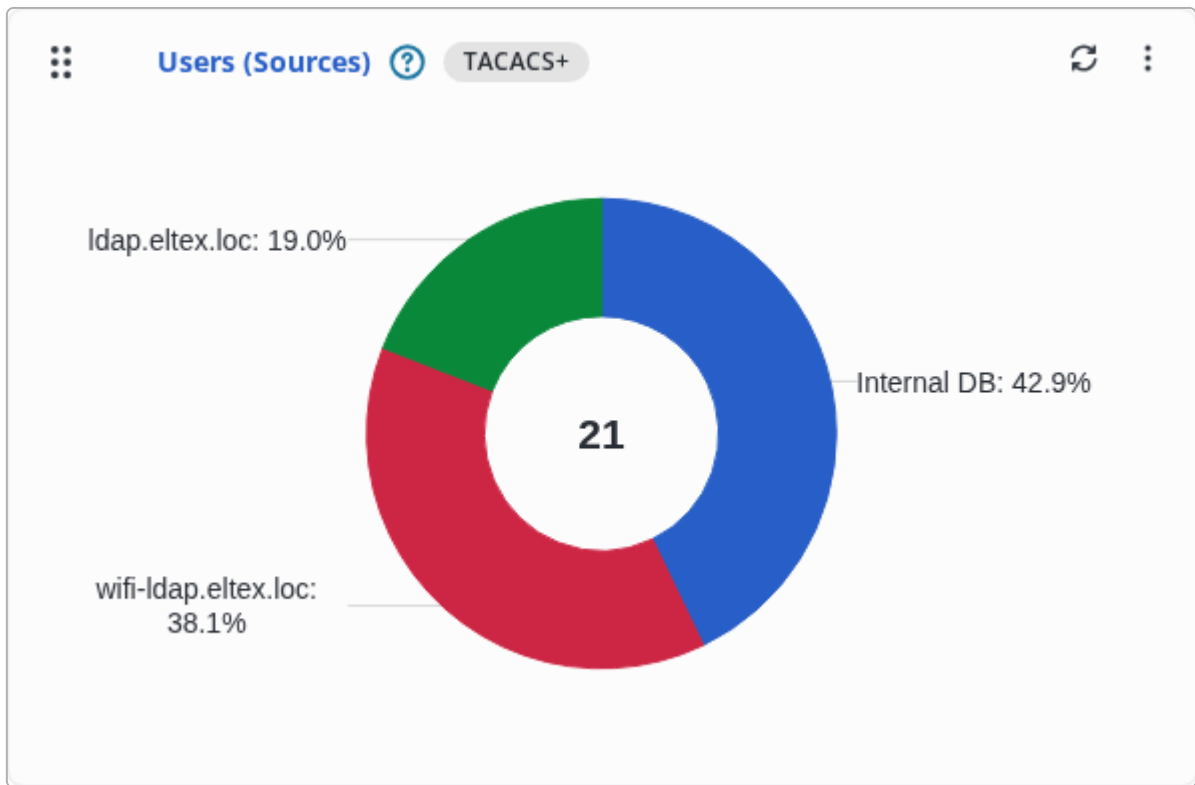


Figure 28. Widget "Users (Sources)"

Widget "TACACS+ sessions"

The widget displays the total number of TACACS+ sessions for the entire data retention period, without applying any filters during the count. The retention period is also displayed in the widget, the unit of display is days.

The list of sessions can be seen in the table [Connections journal](#).

The widget allows estimating the size of the corresponding table in the database, as well as the number of user connections over a period longer than a day.



Figure 29. Widget "TACACS+ sessions"

Widget "TACACS+ accounting"

The widget displays the total number of TACACS+ accounting records for the entire data retention period, without applying any filters during the count. The retention period is also displayed in the widget, the unit of display is days.

The list of accounting sessions can be seen in the table [Accounting](#).

The widget allows estimating the size of the corresponding table in the database, as well as the number of user connections over a period longer than a day.

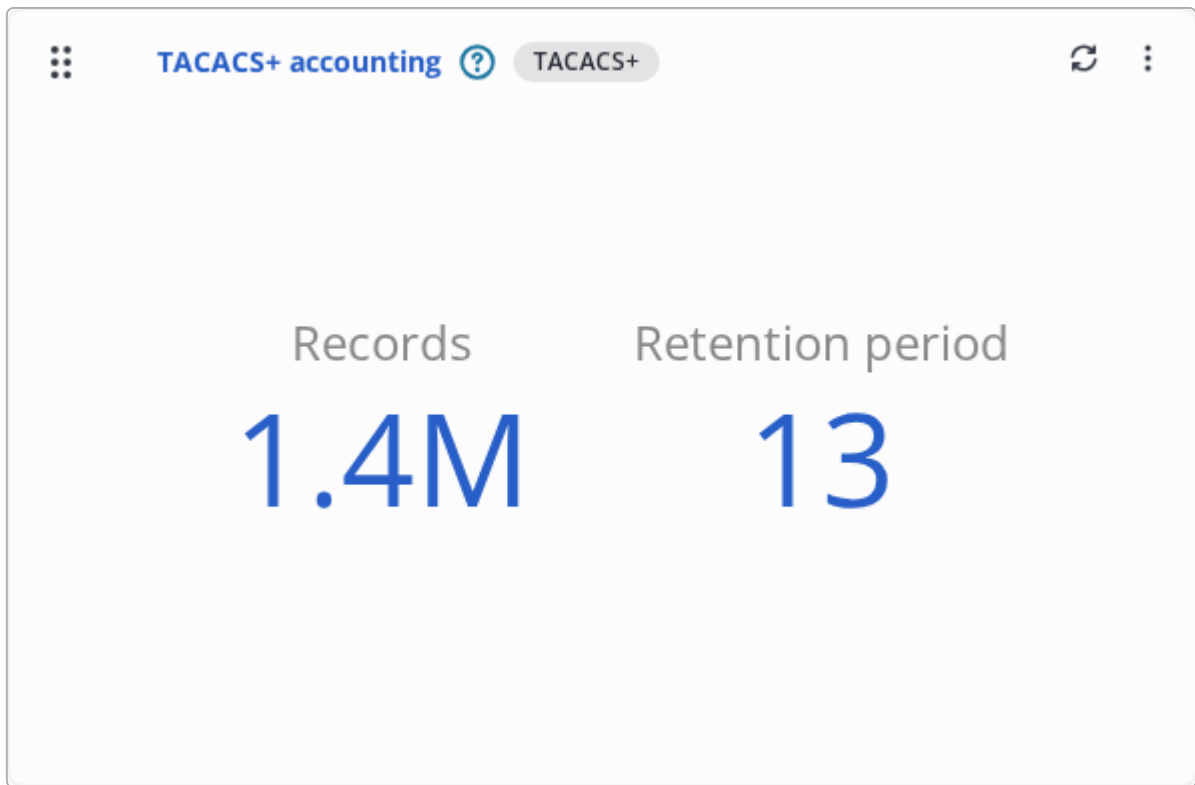


Figure 30. Widget "TACACS+ sessions"

SMS widgets



This section provides information about functionality available with the **ADVANCED** level license. To purchase this functionality, contact your manager or write to the e-mail address eltex@eltex-co.ru.

List of available widgets

Widget	Data display type	Brief description
SMS Sending Schedule	Graph	Count of SMS sendings over the last 24 hours by hour.
Total SMS Sent	Metric	Count of successful and failed SMS over the past 24 hours.

Widget "SMS Sending Schedule"

Displays data about SMS sendings in the system per hour for the last 24 hours.

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.

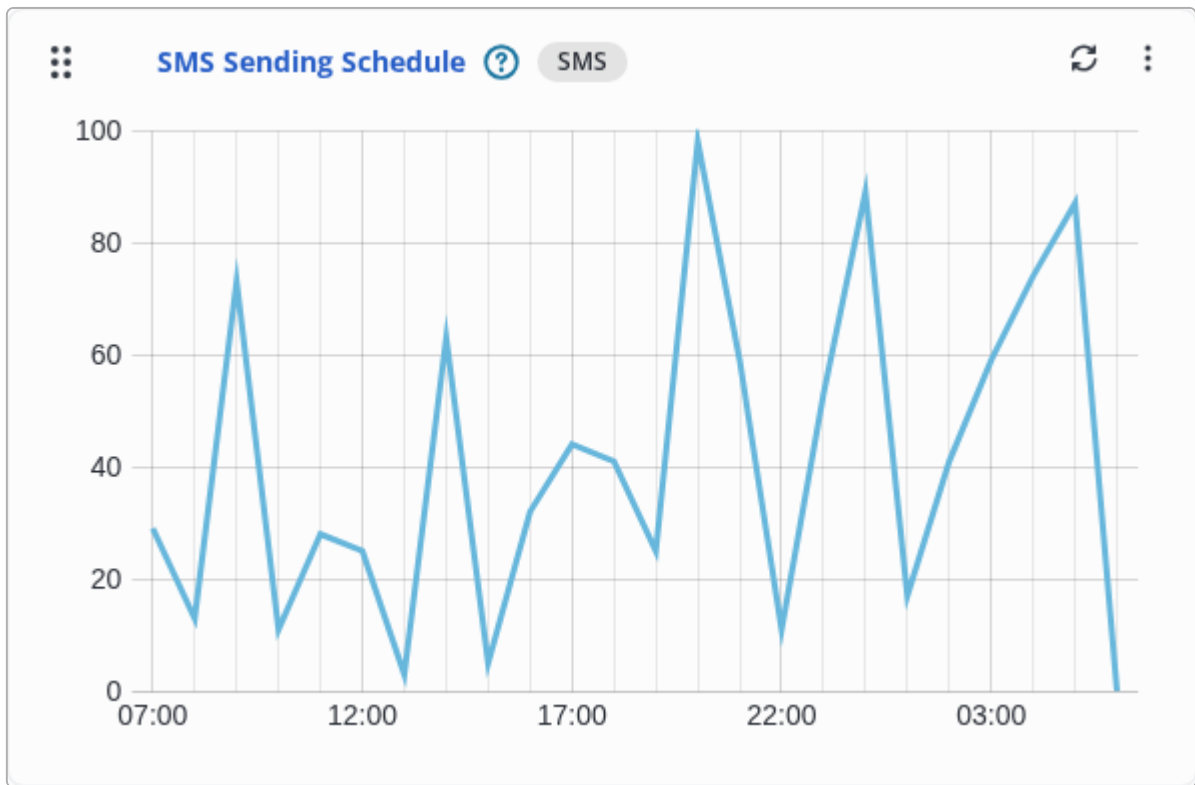


Figure 31. Widget "SMS Sending Schedule"

Widget "Total SMS Sent"

Displays successful and failed SMS counts for the last 24 hours.

Shows SMS status ratio for daily tracking.

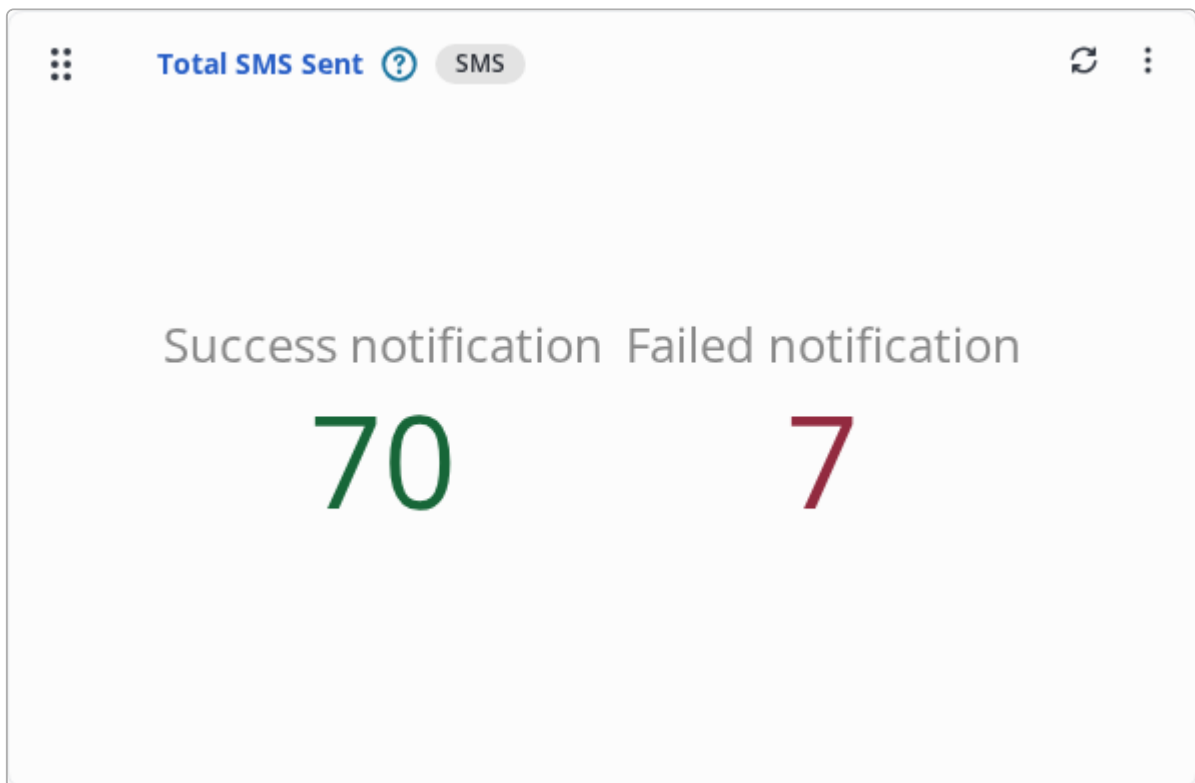


Figure 32. Widget "Total SMS Sent"

Monitoring

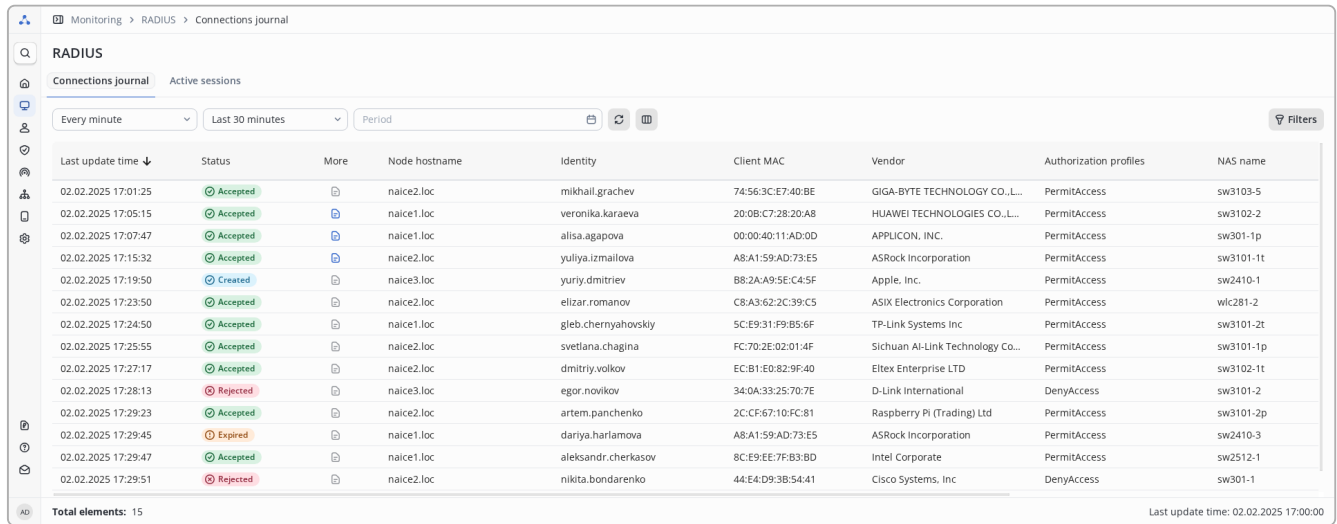
RADIUS

Connections journal

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





The screenshot shows the 'RADIUS Connections journal' interface. It features a search bar, a filter dropdown set to 'Every minute', and a 'Last 30 minutes' period selector. The table below lists 15 sessions with columns for 'Last update time', 'Status', 'More', 'Node hostname', 'Identity', 'Client MAC', 'Vendor', 'Authorization profiles', and 'NAS name'. The status column uses color-coded icons: green for 'Accepted', red for 'Rejected', and orange for 'Expired'. The 'More' column contains icons for session details or links.

Last update time ↓	Status	More	Node hostname	Identity	Client MAC	Vendor	Authorization profiles	NAS name
02.02.2025 17:01:25	Accepted		naice2.loc	mikhail.grachev	74:56:3C:E7:40:BE	GIGA-BYTE TECHNOLOGY CO.,L...	PermitAccess	sw3103-5
02.02.2025 17:05:15	Accepted		naice1.loc	veronika.karaeva	20:0B:C7:28:20:A8	HUAWEI TECHNOLOGIES CO.,L...	PermitAccess	sw3102-2
02.02.2025 17:07:47	Accepted		naice1.loc	alisa.agapova	00:00:40:11:AD:0D	APPLICON, INC.	PermitAccess	sw301-1p
02.02.2025 17:15:32	Accepted		naice2.loc	yuliya.izmailova	A8:A1:59:AD:73:E5	ASRock Incorporation	PermitAccess	sw3101-1t
02.02.2025 17:19:50	Created		naice3.loc	yuriy.dmitriev	B8:2A:A9:5E:C4:5F	Apple, Inc.	PermitAccess	sw2410-1
02.02.2025 17:23:50	Accepted		naice2.loc	elizar.romanov	C8:A3:62:2C:39:C5	ASIX Electronics Corporation	PermitAccess	wlc281-2
02.02.2025 17:24:50	Accepted		naice1.loc	gleb.chernyahovskiy	5C:E9:31:F9:B5:6F	TP-Link Systems Inc	PermitAccess	sw3101-2t
02.02.2025 17:25:55	Accepted		naice2.loc	svetlana.chagina	FC:70:2E:02:01:4F	Sichuan AI-Link Technology Co...	PermitAccess	sw3101-1p
02.02.2025 17:27:17	Accepted		naice2.loc	dmitriy.volkov	EC:B1:E0:82:9F:40	Eltex Enterprise LTD	PermitAccess	sw3102-1t
02.02.2025 17:28:13	Rejected		naice3.loc	egor.novikov	34:0A:33:25:70:7E	D-Link International	DenyAccess	sw3101-2
02.02.2025 17:29:23	Accepted		naice2.loc	artem.panchenko	2C:CF:67:10:FC:81	Raspberry Pi (Trading) Ltd	PermitAccess	sw3101-2p
02.02.2025 17:29:45	Expired		naice1.loc	dariya.harlamova	A8:A1:59:AD:73:E5	ASRock Incorporation	PermitAccess	sw2410-3
02.02.2025 17:29:47	Accepted		naice1.loc	aleksandr.cherkasov	8C:E9:EE:7F:B3:BD	Intel Corporate	PermitAccess	sw2512-1
02.02.2025 17:29:51	Rejected		naice2.loc	nikita.bondarenko	44:E4:D9:3B:54:41	Cisco Systems, Inc	DenyAccess	sw301-1

Figure 33. 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.:
 -  — a link is exist.
 -  — a link is not exist. This situation can occur when the **session storage duration** exceeds the storage duration of detailed session information (7 days).
- **Node hostname** — name of the node that generated the event. Useful for cluster installation.
- **Identity** — the username of the user who was logged in.



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

- **Client MAC** — the identifier of the authorized client, which is specified in the RADIUS attribute Calling-Station-Id (if the attribute is missing in the RADIUS request or does not contain a MAC, the field will be empty).
- **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).

Controls:



Figure 34. User activity display settings

- **Refresh rate** — setting the frequency of automatic re-reading of user sessions.






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



- **Time range** — selection of a predefined time period during which user session activity occurred for display, from a finite list of options. When the **Custom period** option is selected, the **Period** field configuration is required.
- **Period** — selection of a custom time period during which user session activity occurred for display.



Sessions are displayed from 00:00 of the start day until 23:59 of the end day for the selected period. The time accounts for the timezone specified in the [Account settings](#) section of the current administrator.

-  — update the table data manually.
-  — open the settings window for the displayed columns of the table.
-  **Filters** — open the filtering settings window.

Filtering is configured in the following window:

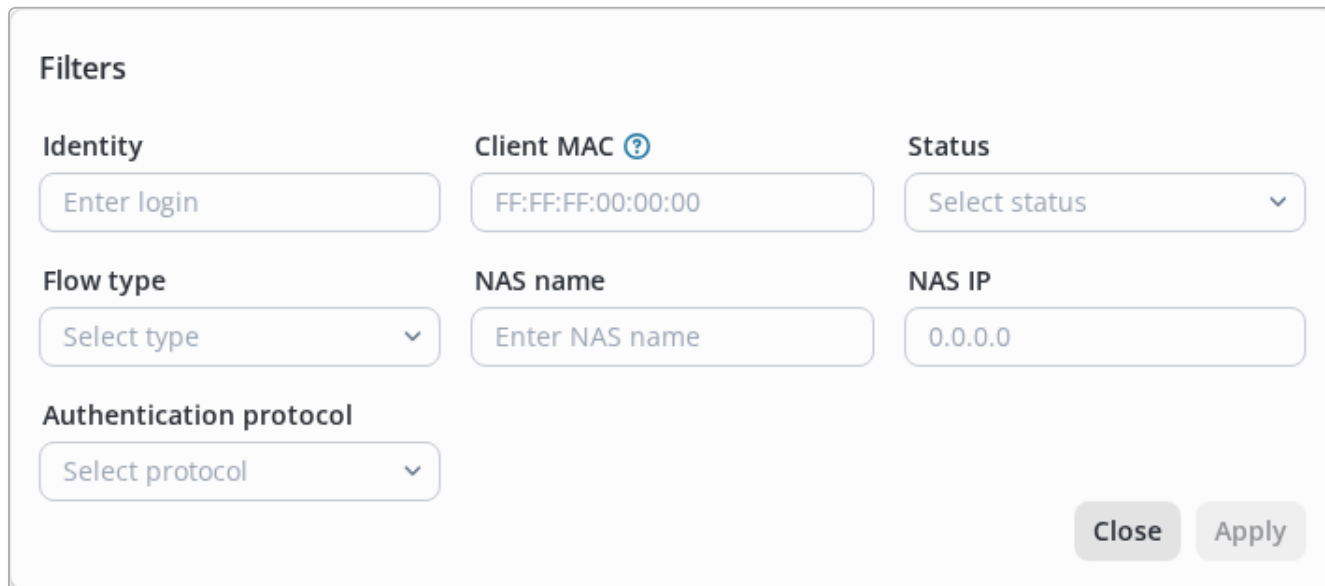


Figure 35. Window for filtering records

Filtering of records is available by the parameters "Identity", "Client MAC", "Status", "Flow type", "NAS name", "NAS IP" 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. It is displayed only if at least one of params are filled.

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

The **Reset all** button is reset displayed columns to their default state.

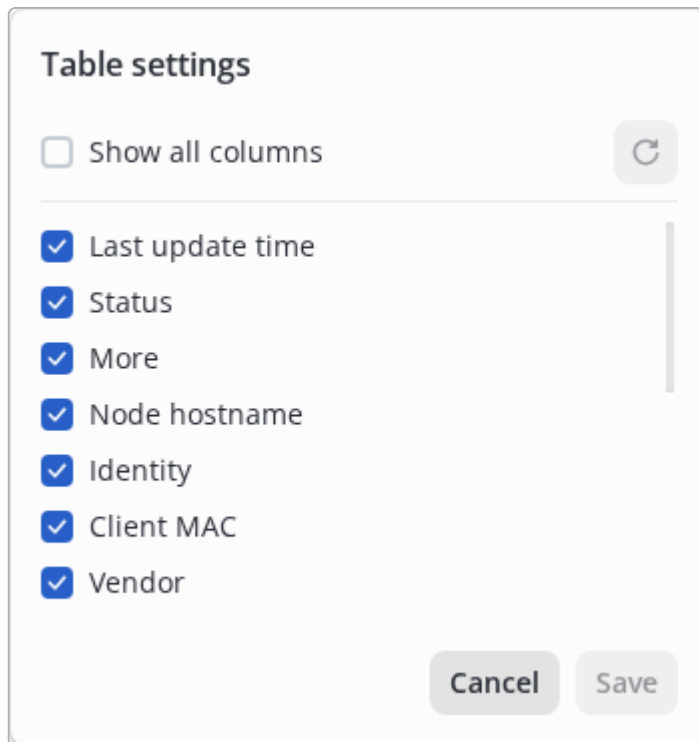



Figure 36. The window for configuring the displayed columns in the table

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.

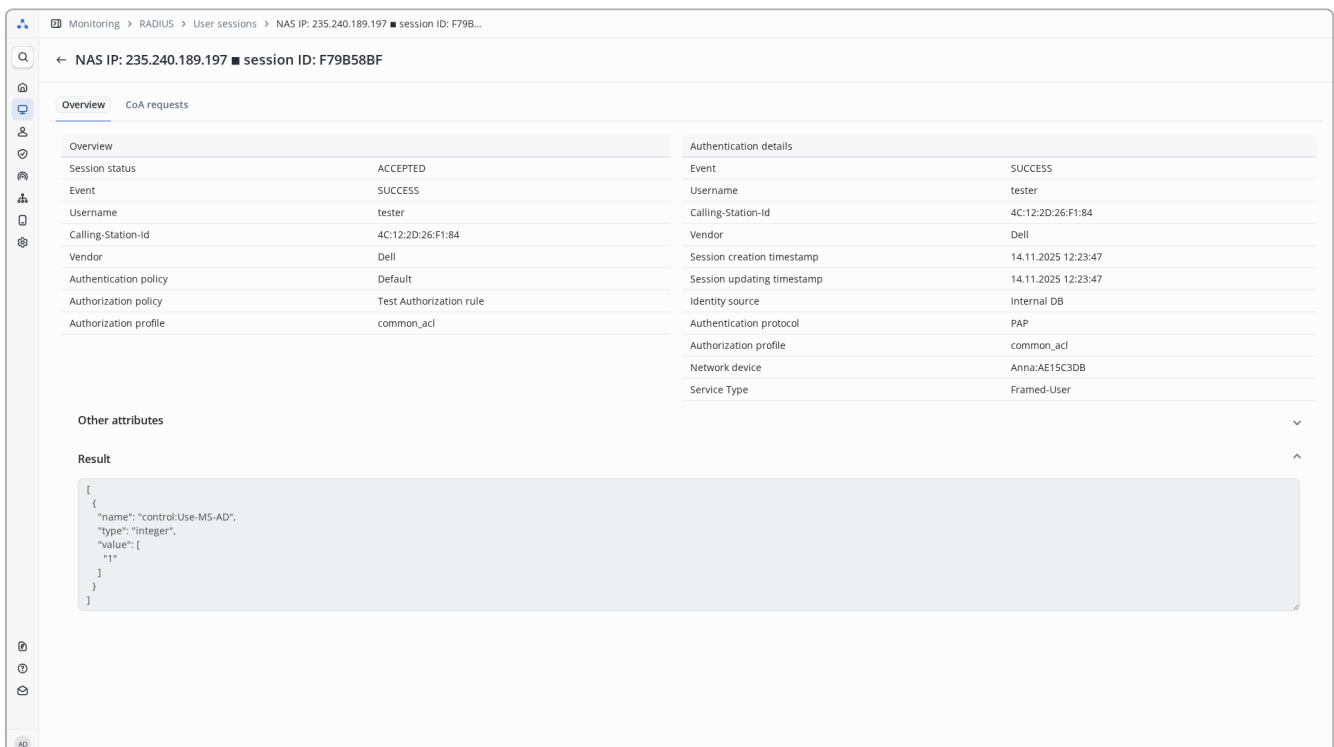


Figure 37. Detailed information about the session

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.

You can also view CoA requests associated with this session in a separate tab.

Time	CoA request type	Request status	RADIUS request type	Response status	RADIUS response type
14.11.2025 06:58:11	Re-auth	In progress	CoA-Request	Failed	No response
Request			Response		
Request fields			Attribute list		
Packet Identifier	0x24		lorem		amet
Length	118		amet		ipsum
Authenticator	dd131c2326cc018c028d6b5f7312843		ipsum		sit
Code	43		sit		elit
13.11.2025 22:39:30	Disconnect	Failed	No request	Failed	No response

Figure 38. CoA Requests List

Active sessions

Description

The *Active sessions* section is designed for monitoring user sessions that are in an active state in real time. The log allows you to view information about each session, filter records, and manually terminate hung sessions.

Viewing the List of Active Sessions

Last update time	Identity	Identity source	Client MAC	Node hostname	Creation date	NAS IP	Acct Session ID
02.02.2025 17:01:25	mikhail.grachev	mikhail.grachev	74:56:3C:E7:40:BE	naice2.loc	02.02.2025 17:01:25	172.16.0.210	ccc061bc-6440-3cda-4ec1-d...
02.02.2025 17:05:15	veronika.karaeva	veronika.karaeva	20:0B:C7:28:20:A8	naice1.loc	02.02.2025 17:05:15	172.16.0.211	9abd5e49-1dde-8a5c-a89e-8...
02.02.2025 17:07:47	alisa.agapova	alisa.agapova	00:00:40:11:AD:0D	naice1.loc	02.02.2025 17:07:47	172.16.0.219	Sacb0e42-73d1-e2b0-b61f-b...
02.02.2025 17:15:32	yuliya.izmailova	yuliya.izmailova	A8:A1:59:AD:73:E5	naice2.loc	02.02.2025 17:15:32	172.16.2.44	a21b1ee0-46fb-938c-0a26-2...
02.02.2025 17:19:50	yuriy.dmitriev	yuriy.dmitriev	B8:2A:A9:5E:C4:5F	naice3.loc	02.02.2025 17:19:50	172.16.0.38	c1db4306-5804-ccfd-28fe-fc...
02.02.2025 17:23:50	elizar.romanov	elizar.romanov	C8:A3:62:2C:39:C5	naice2.loc	02.02.2025 17:23:50	172.16.1.149	5538bc15-a11e-cec7-d5eb-6...
02.02.2025 17:24:50	gleb.chernyahovskiy	gleb.chernyahovskiy	5C:E9:31:F9:B5:6F	naice1.loc	02.02.2025 17:24:50	172.16.2.45	06d2ae88-21d9-8c2c-c8b8-b...
02.02.2025 17:25:55	svetlana.chagina	svetlana.chagina	FC:70:2E:02:01:4F	naice2.loc	02.02.2025 17:25:55	172.16.0.194	5667376d-87a2-a3c3-c7bf-4...
02.02.2025 17:27:17	dmitriy.volkov	dmitriy.volkov	EC:B1:E0:82:9F:40	naice2.loc	02.02.2025 17:27:17	172.16.2.47	a4274bf3-7882-cec8-78c7-df...
02.02.2025 17:28:13	egor.novikov	egor.novikov	34:0A:33:25:70:7E	naice3.loc	02.02.2025 17:28:13	172.16.0.193	a25bd1c1-b488-151d-022b-...
02.02.2025 17:29:23	artem.panchenko	artem.panchenko	2C:CF:67:10:FC:81	naice2.loc	02.02.2025 17:29:23	172.16.0.196	889ab8e7-545e-a92e-4251-5...
02.02.2025 17:29:45	dariya.harlamova	dariya.harlamova	A8:A1:59:AD:73:E5	naice1.loc	02.02.2025 17:29:45	172.16.1.150	bbec4c65-3bde-a771-385d-4...

Figure 39. Active RADIUS sessions table

The table contains the following columns:

Last update time - the time when the last RADIUS Accounting packet was received for this session.

- Identity - the username under which the connection was made.
- Identity source - the name of the authentication source to which the connected user belongs.
- Client MAC - the MAC address of the authorized device, specified in the RADIUS attribute Calling-Station-Id.
- Node hostname - the name of the NAICE node that processed the packet that created the session.
- Creation date - the date and time when the session was created.
- NAS IP - the IP address of the NAS device, obtained from the RADIUS attribute NAS-IP-Address.

Controls:



Figure 40. Active sessions display settings





- Refresh rate - setting the frequency of automatic re-reading of active session data.



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



- Time range - selection of a predefined time period for displaying sessions from the list of options. When the **Custom period** option is selected, the Period field configuration is required.
- Period - selection of a custom time period for displaying sessions.
-  - update the table data manually.
-  - open the displayed columns settings window.
-  - terminate selected sessions. The button is disabled if no active session is selected.
-  Filters - open the filtering settings window.

Filtering is configured in the following window:

Figure 41. Window for filtering records

Filtering of records is available by the parameters: "Identity", "Identity source", "Client MAC", and "NAS IP".

The **Close** button closes the filtering window without applying changes. The **Apply** button applies the configured filters to the table.

Partial matching search is available for text fields.



To search for a part of the MAC address, it is necessary that all searchable octets of the address are specified in full.
For example, searching for "AA:BB:CC" is possible, searching for "A:BB:C" - is not.

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

The **Reset all** button is reset displayed columns to their default state.

Figure 42. Window for configuring displayed columns in the table

Terminating an Active Session

To terminate an active session, use the checkbox to select the required session and click in the panel above the table.



The session is closed only in the NAICE system. The CoA request is not sent, and the actual network connection may remain active.

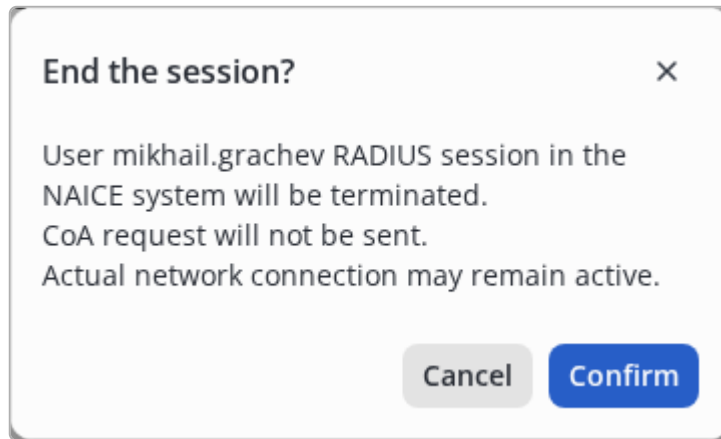


Figure 43. Confirmation of terminating a single session

When clicking the terminate button, a modal window appears with information that the user's RADIUS session will be terminated in the NAICE system and the CoA request will not be sent.

To mass-terminate sessions, use the checkboxes in the first column of the table:

Last update time	Identity	Identity source	Client MAC	Node hostname	Creation date	NAS IP	Acct Session ID	
<input checked="" type="checkbox"/>	02.02.2025 17:01:25	mikhail.grachev	mikhail.grachev	74:56:3C:E7:40:BE	naice2.loc	02.02.2025 17:01:25	172.16.0.210	ccc061bc-6440-3cda-4ec1-d...
<input type="checkbox"/>	02.02.2025 17:05:15	veronika.karaeva	veronika.karaeva	20:0B:C7:28:20:A8	naice1.loc	02.02.2025 17:05:15	172.16.0.211	9abd5e49-1dde-8a5c-a89e-8...
<input type="checkbox"/>	02.02.2025 17:07:47	alisa.agapova	alisa.agapova	00:00:40:11:AD:0D	naice1.loc	02.02.2025 17:07:47	172.16.0.219	5acb0e42-73d1-e2b0-b61f-b...
<input type="checkbox"/>	02.02.2025 17:15:32	yulyia.izmailova	yulyia.izmailova	A8:A1:59:AD:73:E5	naice2.loc	02.02.2025 17:15:32	172.16.2.44	a21b1ee0-46fb-938c-0a26-2...
<input type="checkbox"/>	02.02.2025 17:19:50	yuriy.dmitriev	yuriy.dmitriev	B8:2A:A9:5E:C4:5F	naice3.loc	02.02.2025 17:19:50	172.16.0.38	c1db4306-5804-ccfd-28fe-fc...
<input type="checkbox"/>	02.02.2025 17:23:50	elizar.romanov	elizar.romanov	C8:A3:62:2C:39:C5	naice2.loc	02.02.2025 17:23:50	172.16.1.149	5538bc15-a11e-cec7-d5eb-6...
<input type="checkbox"/>	02.02.2025 17:24:50	gleb.chernyahovskiy	gleb.chernyahovskiy	5C:E9:31:F9:B5:6F	naice1.loc	02.02.2025 17:24:50	172.16.2.45	06d2ae88-21d9-8c2c-c8b8-b...
<input type="checkbox"/>	02.02.2025 17:25:55	svetlana.chagina	svetlana.chagina	FC:70:2E:02:01:4F	naice2.loc	02.02.2025 17:25:55	172.16.0.194	5667376d-87a2-a3c3-c7bf-4...
<input type="checkbox"/>	02.02.2025 17:27:17	dmitriy.volkov	dmitriy.volkov	EC:B1:E0:82:9F:40	naice2.loc	02.02.2025 17:27:17	172.16.2.47	a4274bf3-7882-cec7-78c7-df...
<input type="checkbox"/>	02.02.2025 17:28:13	egor.novikov	egor.novikov	34:0A:33:25:70:7E	naice3.loc	02.02.2025 17:28:13	172.16.0.193	a25bd1c1-b488-151d-022b-...
<input type="checkbox"/>	02.02.2025 17:29:23	artem.panchenko	artem.panchenko	2C:CF:67:10:FC:81	naice2.loc	02.02.2025 17:29:23	172.16.0.196	889ab8e7-545e-a92e-4251-5...
<input type="checkbox"/>	02.02.2025 17:29:45	dariya.harlamova	dariya.harlamova	A8:A1:59:AD:73:E5	naice1.loc	02.02.2025 17:29:45	172.16.1.150	bbec465-3bde-a771-385d-4...

Figure 44. Session selection checkbox

After selecting one or more sessions, the button becomes active and allows to terminate all selected sessions:

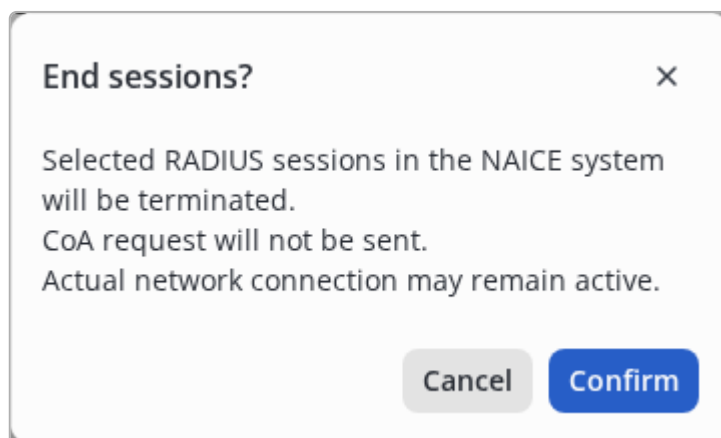


Figure 45. Confirmation of terminating multiple sessions

The terminate button action is similar to receiving a RADIUS Accounting Stop packet - the session is closed in the NAICE system and the quota is freed for the next user connection.



To use the session terminate button, privileges to edit the active session monitoring log are required.

How a Session Is Terminated

A session is considered active from the moment of successful user authentication and is displayed in the table until one of the following events occurs:

- Receiving a *RADIUS Accounting Stop* packet - the session is terminated automatically, the simultaneous connection quota is freed.
- Inactivity timeout - if no Accounting packets (Interim-Update) are received for the session within the specified period, the system automatically terminates the session. The lifetime is configured in the [RADIUS Session Limits](#) section.
- Manual termination by the administrator - the session is closed in the NAICE system, the simultaneous connection quota is freed. The CoA request is not sent.

After termination, the session is excluded from the active list and is no longer counted in the simultaneous session limit check. An event indicating the reason for session termination is recorded in the [event log](#).

TACACS+

Connections journal



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

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

Creation time	Status	More	Node hostname	Packet type	User	Device name	Error reason	Remote address	Privilege level	Command	Session ID
02.02.2025 10:00:00	Pass		naice1.loc	AUTHENTICATION	mikhail.grachev	sw3103-5		192.168.0.210	1		8981842260656128
02.02.2025 09:48:00	Pass		naice3.loc	AUTHORIZATION	veronika.karaeva	sw3102-2		192.168.0.211	1	enable	6488106203086848
02.02.2025 09:43:00	Pass		naice3.loc	AUTHORIZATION	alisa.agapova	sw301-1p		192.168.0.219	15	configure	839972996807936
02.02.2025 09:38:00	Pass		naice2.loc	AUTHORIZATION	yuliy.izmailova	sw3101-1t		192.168.2.44	7	show port-security	1030253162976
02.02.2025 09:38:00	Pass		naice1.loc	AUTHORIZATION	yuriy.dmitriev	sw2410-1		192.168.0.38	1	show version	1154042430488576
02.02.2025 09:28:00	Expired		naice1.loc	AUTHENTICATION	elizar.romanov	wlc281-2		192.168.1.149	1		2723169678917632
02.02.2025 09:27:00	Pass		naice3.loc	AUTHORIZATION	gleb.chernyahovskiy	sw3101-2t		192.168.2.45	15	switchport access vlan 16	8998556985720832
02.02.2025 09:25:00	Pass		naice2.loc	AUTHORIZATION	svetlana.chagina	sw3101-1p		192.168.0.194	7	show flow-control	1321859566010368
02.02.2025 09:21:00	Pass		naice2.loc	AUTHORIZATION	dmitriy.volkov	sw3102-1t		192.168.2.47	15	interface switchport trunk...	2126500451057664
02.02.2025 09:20:00	Fail		naice1.loc	AUTHORIZATION	egor.novikov	sw3101-2	Command not defined in...	192.168.0.193	1	show running-config	831712128925696
02.02.2025 09:20:00	Pass		naice1.loc	AUTHORIZATION	artem.panchenko	sw3101-2p		192.168.0.196	1	show spanning-tree	3572081620942848
02.02.2025 09:18:00	Pass		naice3.loc	AUTHENTICATION	dariya.harlamova	sw2410-3		192.168.1.150	15		1677682836242432
02.02.2025 09:14:00	Pass		naice3.loc	AUTHORIZATION	aleksandr.cherkasov	sw2512-1		192.168.0.46	1	show bootvar	3493989330190336
02.02.2025 09:12:00	Fail		naice2.loc	AUTHENTICATION	nikita.bondareno	sw301-1	Identity user not found	192.168.0.218	1		3112534305406976
02.02.2025 09:14:00	Pass		naice1.loc	AUTHORIZATION	denis.kastanaev	sw2410-2		192.168.1.148	15	interface GigabitEthernet...	602526305655680

Figure 46. 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:
 - **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.
- **Node hostname** — name of the node that generated the event. Useful for cluster installation.
- **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 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 47. 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 settings window for the displayed columns of the table.
-  Filters — open the filtering settings window.



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:

Filters

Packet type
Select type

User
Enter login

Status
Select status

Device IP
0.0.0.0

Device name
Enter name

Remote address
0.0.0.0

Port
Enter port

Command
Enter command

Close Apply

Figure 48. Window for filtering records

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



For device and remote user addresses, a partial match search is available for any octet/octets of the IP address.

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 **Reset all** button is reset displayed columns to their default state.

Table settings

Show all columns

Creation time

Status

More

Node hostname

Packet type


User

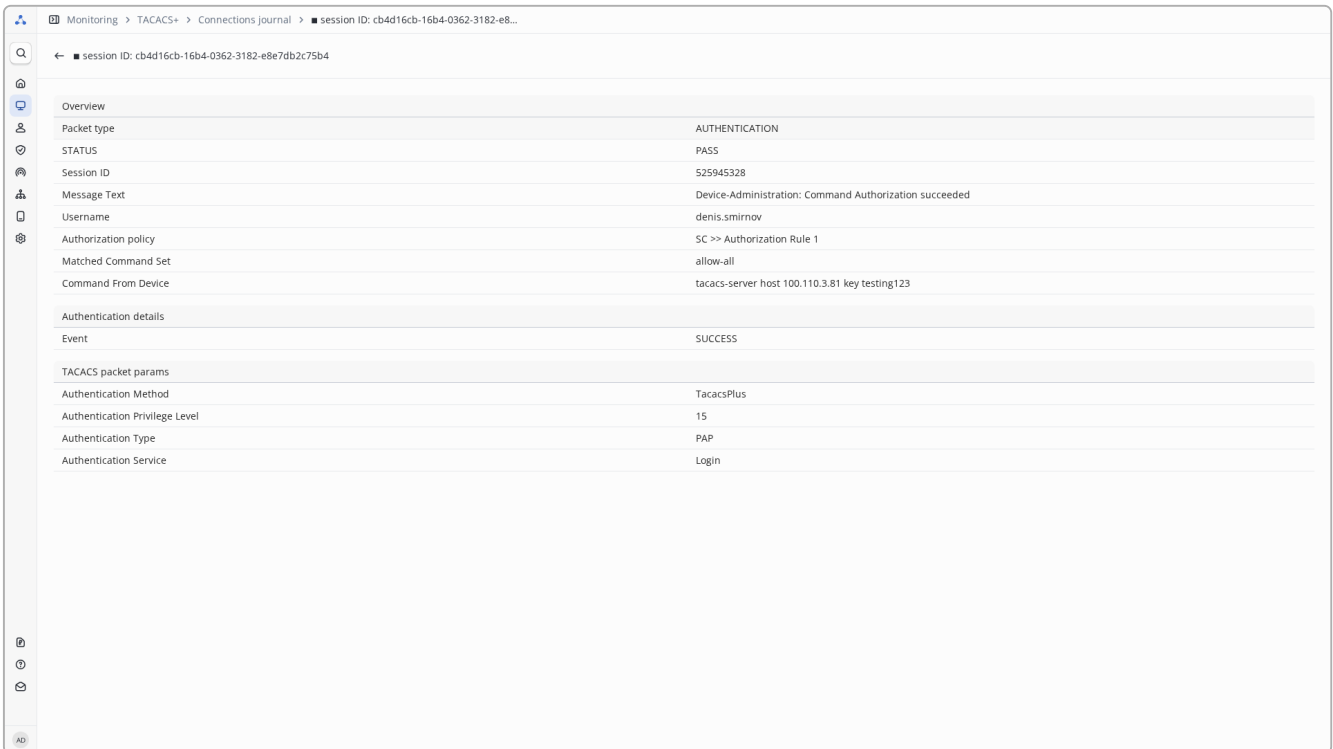
Device name

Cancel Save

Figure 49. 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.



Packet type	AUTHENTICATION
STATUS	PASS
Session ID	525945328
Message Text	Device-Administration: Command Authorization succeeded
Username	denis.smirnov
Authorization policy	SC >> Authorization Rule 1
Matched Command Set	allow-all
Command From Device	tacacs-server host 100.110.3.81 key testing123
Authentication details	
Event	SUCCESS
TACACS packet params	
Authentication Method	TacacsPlus
Authentication Privilege Level	15
Authentication Type	PAP
Authentication Service	Login

Figure 50. 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

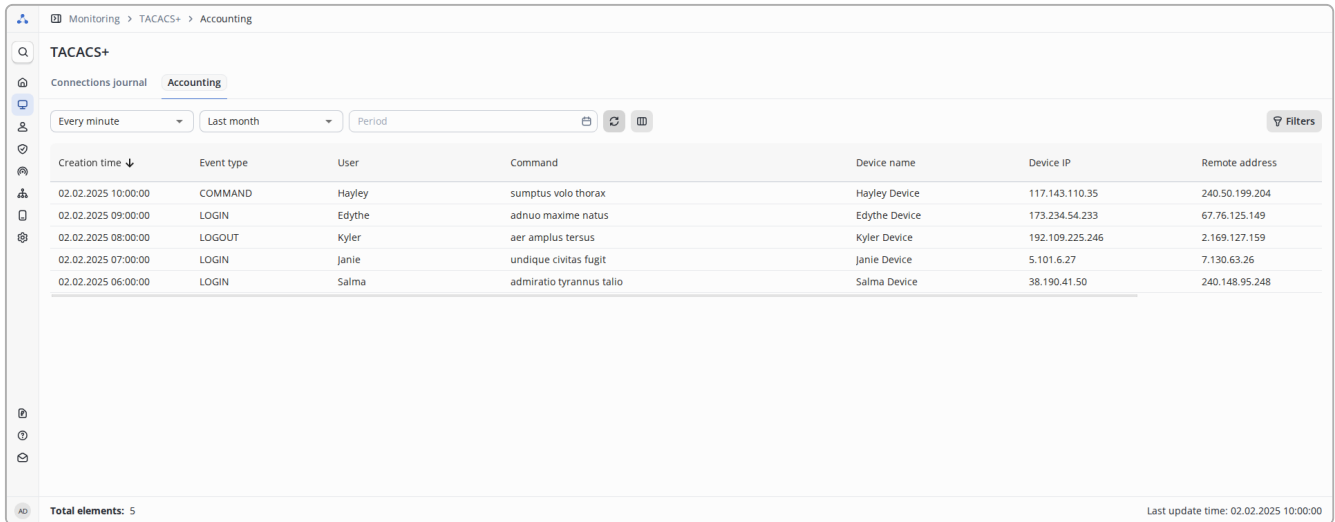


This section contains information about functionality that is available as part of the additional **NAICE-TACACS+** license option. To purchase this functionality, please contact your manager or email eltex@eltex-co.ru.

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




The screenshot shows a web interface for TACACS+ Accounting. The breadcrumb path is 'Monitoring > TACACS+ > Accounting'. The page title is 'TACACS+'. There are tabs for 'Connections Journal' and 'Accounting'. The 'Accounting' tab is active. Below the tabs, there are filters: 'Every minute' (refresh), 'Last month' (period), and 'Period' (calendar icon). A 'Filters' button is on the right. The table has columns: 'Creation time', 'Event type', 'User', 'Command', 'Device name', 'Device IP', and 'Remote address'. The table contains 5 rows of data. At the bottom, it says 'Total elements: 5' and 'Last update time: 02.02.2025 10:00:00'.

Creation time	Event type	User	Command	Device name	Device IP	Remote address
02.02.2025 10:00:00	COMMAND	Hayley	sumptus volo thorax	Hayley Device	117.143.110.35	240.50.199.204
02.02.2025 09:00:00	LOGIN	Edythe	adnuo maxime natus	Edythe Device	173.234.54.233	67.76.125.149
02.02.2025 08:00:00	LOGOUT	Kyler	aer amplius tersus	Kyler Device	192.109.225.246	2.169.127.159
02.02.2025 07:00:00	LOGIN	Janie	undique civitas fugit	Janie Device	5.101.6.27	7.130.63.26
02.02.2025 06:00:00	LOGIN	Salma	admiratio tyrannus talio	Salma Device	38.190.41.50	240.148.95.248

Figure 51. 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:

- **Privilege 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 52. 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 settings window for the displayed columns of the table.
- **Filters** - open the filtering settings window.



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:

Filters

User	Device IP	Device name
<input type="text" value="Enter login"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="Enter name"/>
Remote address	Port	Command
<input type="text" value="0.0.0.0"/>	<input type="text" value="Enter port"/>	<input type="text" value="Enter command"/>

Figure 53. Window for filtering records

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



For device and remote user addresses, a partial match search is available for any octet/octets of the IP address.

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 **Reset all** button is reset displayed columns to their default state.

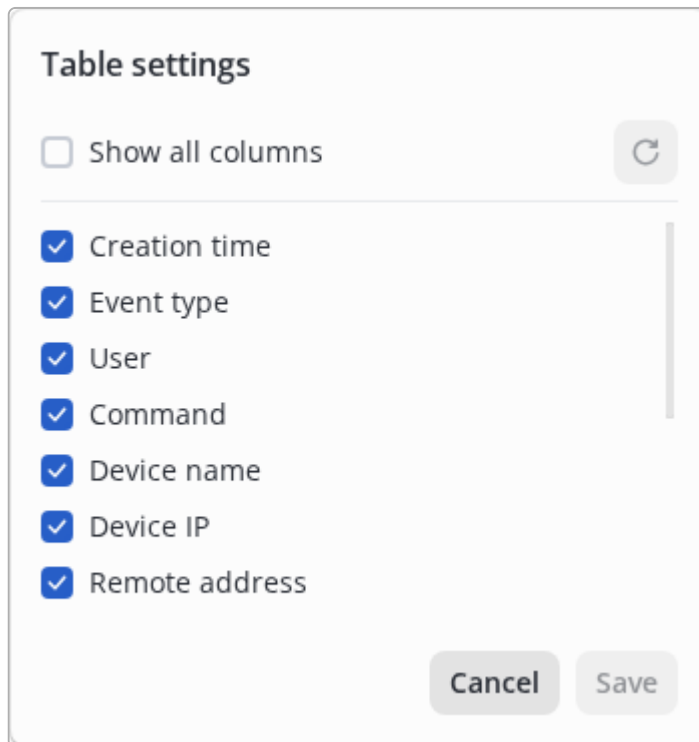


Figure 54. The window for configuring the displayed columns in the table

System

System events

Description

System Events displays information about events occurring in the system, such as license activation, user login/logout, creation and editing of various entities. The list of possible events can be found on the [:system/list-events.html](http://system/list-events.html) page.

For convenient event analysis, you can select the time period when events occurred, their severity level, the event group they belong to. Additionally, you can search for specific events by their message text.

Viewing system events

Date	Node hostname	Level	Message
02.02.2025 10:00:00	naice1.eltex.loc	ERROR	Event log - Language: en -- de.
02.02.2025 09:00:00	naice3.eltex.loc	DEBUG	Session retention period, days: 16 -- 9.
02.02.2025 08:00:00	naice3.eltex.loc	DEBUG	Password policies - Password must not match login: enabled -- disabled.
02.02.2025 07:00:00	naice3.eltex.loc	DEBUG	Password policies - Send notifications about user creation: enabled -- disabled.
02.02.2025 06:00:00	naice1.eltex.loc	DEBUG	Event log - Event retention period, days: 15 -- 17.
02.02.2025 05:00:00	naice2.eltex.loc	WARNING	Event log - Event retention period, days: 16 -- 16.
02.02.2025 04:00:00	naice3.eltex.loc	WARNING	Session retention period, days: 2 -- 22.
02.02.2025 03:00:00	naice2.eltex.loc	DEBUG	Session retention period, days: 11 -- 29.
02.02.2025 02:00:00	naice1.eltex.loc	DEBUG	Authentication and command accounting port: 62687 -- 38620.
02.02.2025 01:00:00	naice1.eltex.loc	INFO	Password policies - Password must contain uppercase letters: enabled -- disabled.
02.02.2025 00:00:00	naice1.eltex.loc	INFO	Password policies - Password must contain lowercase letters: enabled -- disabled.
01.02.2025 23:00:00	naice3.eltex.loc	INFO	Password policies - Password must contain uppercase letters: enabled -- disabled.
01.02.2025 22:00:00	naice1.eltex.loc	DEBUG	Password policies - Send notifications about user data modification: enabled -- disabled.
01.02.2025 21:00:00	naice3.eltex.loc	ERROR	Password policies - Password must not match login: enabled -- disabled.
01.02.2025 20:00:00	naice2.eltex.loc	INFO	Password policies - Email notification gateway: disabled -- SMTP Gateway.

Figure 55. Table with a list of system events

The table contains default columns:

- **Date** - date and time of the event.
- **Node hostname** - name of the node that generated the event. Useful for cluster installation.
- **Level** - event logging level.
- **Message** - text description of the event.

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

- **IP** - the address of the host that caused the event to be created.
- **Group** - the group of the event. The list of possible event groups can also be found on the page [:system/list-events.html](http://system/list-events.html).
- **Key** - result of performing actions reflected in the event.
- **Author** - caused this event the **system user** login. If the action was performed by the system displayed system.
- **Role** - the **role** of the user who caused the system event.



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





Table settings

Show all columns 

Date

Node hostname

IP

Level

Group

Key

Message




Cancel **Save**

Figure 56. Configure system event table columns to display

To reset all settings use the  button in the upper right corner of the selection window.

Control elements:

-  **Filters** - 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.

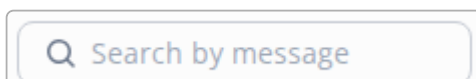


Figure 57. Search by message



To reset the search expression, you must click `x` 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:

Filters





<p>Select period</p> <input style="width: 90%;" type="text" value="Period"/> 	<p>Level</p> <input style="width: 90%;" type="text" value="Select level"/> 
<p>Group</p> <input style="width: 90%;" type="text" value="Select group"/> 	<p>Key ?</p> <input style="width: 90%;" type="text" value="Select key"/> 
<p>Author</p> <input style="width: 90%;" type="text" value="Enter login"/>	<p>Role</p> <input style="width: 90%;" type="text" value="Select role"/>
<p>IP</p> <input style="width: 90%;" type="text" value="0.0.0.0"/>	

Figure 58. filter customization window

Filtering of records is available by parameters:

- `Select period` - allows to select the time period up to date and time.
- `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.
- **Key** - selection of the event type from a certain group. If the group is not selected, the key selection is not available.
- **Author** - filter by the **user** who initiated the events.
- **Role** - **role** of the system user associated with the event.
- **IP Address** - filter by the host address from which the event was initiated. A partial match search is available for any octet/octets of the IP address.

System Events List



The contents of the "Message" field for events is displayed according to the language specified at the **System language** setting in section [Common settings](#)



Some functional described on this page are only available with an extended license. These features are marked with special labels in the form of colored icons next to the name.

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
License activation error	License activation error	ERROR	Error while activate license <productId> : <error> .	Gulo

Event Key	Description	Level	Message	Source
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
License drop reason	License drop occurred and the drop reason was provided	ERROR	License will be dropped. <dropReason>	Gulo
License limit for guest endpoints is reached	Guest endpoints limit exceeded in demo mode	WARNING	Demo mode limit of <limit> guest endpoints exceeded	Gulo

Event Key	Description	Level	Message	Source
License recipient init error	License initialization error in the recipient	ERROR	An error occurred in the service operation while applying the license	Gulo

Events – RADIUS Authentication

Event Name	Description	Level	Message	Source
RADIUS session created	New RADIUS session created	INFO	RADIUS session created.	Ovis
RADIUS authentication successful	RADIUS session successfully authenticated	INFO	RADIUS session authenticated.	Ovis
RADIUS session expired	RADIUS session expired	INFO	RADIUS session expired.	Ovis
RADIUS session rejected	RADIUS session rejected	WARNING	RADIUS session rejected.	Ovis
RADIUS session stopped manually	RADIUS session stopped by system user	INFO	RADIUS session for user <identityUserName> (mac <userMAC> , nasIp <userIp>) has been stopped by admin <adminLogin>	Gavia
RADIUS session stopped automatic	RADIUS active session stopped automatically	INFO	RADIUS session for user <identityUserName> (mac <userMAC> , nasIp <userIp>) has been stopped automatically	Ovis

Events – Update roles privileges

Event Name	Description	Level	Message	Source
User created	New system user created	INFO	System user with login <login> and role <role> created.	User / UI
User modified	System user data modified	INFO	System user with login <login> and role <role> modified.	User / UI
Users deleted	System users deleted	WARNING	System users with logins <logins> deleted.	User / UI
Current user modified	User modified their own account parameters	INFO	User with login <login> and role <role> modified their account parameters.	User / UI

Event Name	Description	Level	Message	Source
Role modified	RBAC role parameters modified	INFO	Role with name <role> edited.	User / UI
Roles deleted	RBAC roles deleted	INFO	Roles with names <roles> were deleted.	User / UI

Events – Update network resources

Event Name	Description	Level	Message	Source
Network device created	New network device created	INFO	Network device <deviceName> was created.	User / UI
Network device modified	Network device parameters modified	INFO	Network device <deviceName> was modified.	User / UI
Network devices deleted	Network devices deleted	INFO	Network devices <devicesNames> were deleted.	User / UI
Network group created	New network group created	INFO	Network group <groupName> was created.	User / UI
Network group modified	Network group parameters modified	INFO	Network group <groupName> was modified.	User / UI
Network groups deleted	Network groups deleted	INFO	Network groups <groupsNames> were deleted.	User / UI
Network profile created	New network profile created	INFO	Network profile <profileName> was created.	User / UI
Network profile modified	Network profile parameters modified	INFO	Network profile <profileName> was modified.	User / UI
Network profiles deleted	Network profiles deleted	INFO	Network profiles <profilesNames> were deleted.	User / UI

Events – Update identity management elements elements

Event Name	Description	Level	Message	Source
Network user created	New network user created	INFO	Network user <identityUserName> was created.	User / UI
Network user modified	Network user parameters modified	INFO	Network user <identityUserName> was modified.	User / UI

Event Name	Description	Level	Message	Source
Network user group created	New network user group created	INFO	Network user group <identityUsersGroupName> was created.	User / UI
Network user group modified	Network user group parameters modified	INFO	Network user group <identityUsersGroupName> was modified.	User / UI
Network user groups deleted	Network user groups deleted	INFO	Network user groups <identityUsersGroupsNames> were deleted.	User / UI

Events – Update identity source sequence

Event Name	Description	Level	Message	Source
Identity chain created	New identity chain created	INFO	Identity chain <identitySequenceName> was created.	User / UI
Identity chain modified	Identity chain parameters modified	INFO	Identity chain <identitySequenceName> was modified.	User / UI
Identity chains deleted	Identity chains deleted	INFO	Identity chains <identitySequencesNames> were deleted.	User / UI

Events – Update external identity sources

Event Name	Description	Level	Message	Source
External identity source created	New external identity source created	INFO	External identity source <externalSourceName> was created.	User / UI
External identity source modified	External identity source parameters modified	INFO	External identity source <externalSourceName> was modified.	User / UI
External identity sources deleted	External identity sources deleted	INFO	External identity sources <externalSourcesNames> were deleted.	User / UI
Domain computer's password has been successfully changed	Domain computer's password has been successfully changed	INFO	External source <externalSourceName> . Domain computer's <externalSourceComputerName> password has been auto-changed by system.	Ursus

Event Name	Description	Level	Message	Source
Failed to change domain computer's password	Failed to change domain computer's password	ERROR	Failed to auto-change password by system for domain computer <externalSourceComputerName> in external source <externalSourceName> .	Ursus

Events – Update RADIUS policies

Event Name	Description	Level	Message	Source
RADIUS policy sets created	New RADIUS policy sets created	INFO	Policy sets <radiusPolicySetName> created.	User / UI
RADIUS policy sets modified	RADIUS policy sets parameters modified	INFO	Policy sets <radiusPolicySetName> modified.	User / UI
RADIUS policy sets deleted	RADIUS policy sets deleted	INFO	Policy sets <radiusPolicySetName> deleted.	User / UI
RADIUS authorization profile created	New RADIUS authorization profile created	INFO	Authorization profile <radiusAuthProfileName> created.	User / UI
RADIUS authorization profile modified	RADIUS authorization profile parameters modified	INFO	Authorization profile <radiusAuthProfileName> modified.	User / UI
RADIUS authorization profiles deleted	RADIUS authorization profiles deleted	INFO	Authorization profiles <radiusAuthProfilesNames> deleted.	User / UI
RADIUS allowed protocols list created	New RADIUS allowed protocols list created	INFO	Allowed protocols list <radiusAllowedProtocolName> created.	User / UI
RADIUS allowed protocols list modified	RADIUS allowed protocols list parameters modified	INFO	Allowed protocols list <radiusAllowedProtocolName> modified.	User / UI
RADIUS allowed protocols lists deleted	RADIUS allowed protocols lists deleted	INFO	Allowed protocols list <radiusAllowedProtocolNames> deleted.	User / UI
RADIUS condition created	New condition for RADIUS policies created	INFO	Condition <radiusConditionName> created.	User / UI

Event Name	Description	Level	Message	Source
RADIUS condition modified	Condition for RADIUS policies parameters modified	INFO	Condition <radiusConditionName> modified.	User / UI
RADIUS conditions deleted	Conditions for RADIUS policies deleted	INFO	Conditions <radiusConditionNames> deleted.	User / UI

Events – Update profiling

Event Name	Description	Level	Message	Source
Profiling policy created	New profiling policy created	INFO	Profiling policy <policyName> was created.	User / UI
Profiling policy modified	Profiling policy parameters modified	INFO	Profiling policies <policyName> were modified.	User / UI
Profiling policies deleted	Profiling policies deleted	INFO	Profiling policies <policiesNames> were deleted.	User / UI
Profiling condition created	New profiling condition created	INFO	Profiling condition <conditionName> was created.	User / UI
Profiling condition modified	Profiling condition parameters modified	INFO	Profiling condition <conditionName> was modified.	User / UI
Profiling conditions deleted	Profiling conditions deleted	INFO	Profiling conditions <conditionsNames> were deleted.	User / UI
Logical profile created	New logical profile created	INFO	Logical profile <logicalProfileName> was created.	User / UI
Logical profile modified	Logical profile parameters modified	INFO	Logical profile <logicalProfileName> was modified.	User / UI
Logical profiles deleted	Logical profiles deleted	INFO	Logical profiles <logicalProfilesNames> were deleted.	User / UI

Events – Update system configuration

Event Name	Description	Level	Message	Source
Log collector created	New log collector created	INFO	Log collector <logCollectorName> was created.	User / UI

Event Name	Description	Level	Message	Source
Log collector modified	Log collector parameters modified	INFO	Log collector <logCollectorName> was modified.	User / UI
Log collectors deleted	Log collectors deleted	INFO	Log collectors <logCollectorsNames> were deleted.	User / UI
User sent test event to log collector	User sent test event to log collector.	INFO	User sent test event to log collector.	User / UI

Events – User Sessions

Event Name	Description	Level	Message	Source
Creating user session	The user is logged in into the system	INFO	User <login> sign in to system with role <roleName>' from ip <userIp> through the source <sourceName> .	User / UI
Destroying user session	The user has logged out of the system	INFO	User <login> is authenticated via <sourceName> logout from system from ip <userIp> .	User / UI
Terminating user session	The user's session was terminated by the system.	INFO	User session <login> is authenticated via <sourceName> from ip <userIp> is terminated.	User / UI
Expired user session	The user session has been expired.	INFO	User session <login> is authenticated via <sourceName> from ip <userIp> is expired.	User / UI
Failed user session: wrong username	Attempted authentication with an invalid login.	WARNING	User failed authentication with login <login> through <externalSourceName> source from ip <userIp> , wrong login.	User / UI
Failed user session: wrong password	Attempted authentication with an incorrect password.	WARNING	User failed authentication with login <login> through <externalSourceName> source from ip <userIp> , wrong password.	User / UI
Failed user session: system user disabled	Attempting to authenticate with a deactivated user.	WARNING	User failed authentication with login <login> through <externalSourceName> source from ip <userIp> , disabled account.	User / UI

Event Name	Description	Level	Message	Source
Failed user session: empty username	Attempted authentication with empty login.	ERROR	Authentication attempt through <externalSourceName> source without login from ip <userIp> .	User / UI
Failed user session: empty password	Attempted authentication with empty password.	WARNING	User failed authentication with login <login> through <externalSourceName> source from ip <userIp> , empty password.	User / UI
Failed user session: role not found	Attempted authentication with an inappropriate role.	WARNING	User failed authentication with login <login> through <externalSourceName> source from ip <userIp> , role not found.	User / UI
Failed user session: external source is unavailable	Attempted authentication with an unavailable external source.	WARNING	User failed authentication with login <login> through <externalSourceName> source from ip <userIp> , external source is unavailable.	User / UI
Failed user session: other errors	Other errors that occur during authentication.	ERROR	User failed authentication with login <login> through <externalSourceName> source from ip <userIp> , error: <error> .	User / UI

Events – Update endpoints

Event Name	Description	Level	Message	Source
Endpoint created	New endpoint created	INFO	Endpoint <endpointName> was created.	User / UI
Endpoints modified	Endpoints parameters modified	INFO	Endpoints <endpointsNames> were modified.	User / UI

Event Name	Description	Level	Message	Source
Endpoints deleted	Endpoints deleted	INFO	Endpoints <endpointsNames> were deleted.	User / UI
Endpoint group created	New endpoint group created	INFO	Endpoint group <endpointsGroupName> was created.	User / UI
Endpoint group modified	Endpoint group parameters modified	INFO	Endpoint group <endpointsGroupName> was modified.	User / UI
Endpoint groups deleted	Endpoint groups deleted	INFO	Endpoint groups <endpointsGroupsNames> were deleted.	User / UI

Events — Update service configuration

Event Name	Description	Level	Message	Source
Request to change services configuration	Changing services configuration	DEBUG	A request was made to change the configuration of services:: <ul style="list-style-type: none"> <serviceName> <serviceName> . 	Phoca
Applying service configuration	Service configuration applied	DEBUG	Configuration applied for service <serviceName>.	<serviceName>

Events — Update container configuration

Event Name	Description	Level	Message	Source
Request to change containers configuration	Changing containers configuration	DEBUG	A request was made to change the configuration of containers: <ul style="list-style-type: none"> <containerName> <containerName> . 	Phoca
Applying containers configuration	Containers configuration applied	DEBUG	Configuration applied for container <containerName>.	<containerName>

Events — Update system configuration

Event Name	Description	Level	Message	Source
------------	-------------	-------	---------	--------

Event Name	Description	Level	Message	Source
Creating trust certificate	A trusted certificate has been created.	INFO	Trust certificate '<certName>' has been created.	User / UI
Editing trust certificate	The trusted certificate has been edited.	INFO	Trust certificate '<certName>' has been edited.	User / UI
Deleting trust certificate	The trusted certificate has been deleted.	INFO	Trust certificate '<certName>' has been deleted.	User / UI
Editing trust certificate status	The trusted certificate has been changed.	WARNING	Status of trust certificate '<certName>' has been changed to <status>.	User / UI
Trust certificate expiring soon	The trusted certificate will expire soon.	WARNING	Trust certificate <certName> will expire on <expirationDate> (in <daysLeft> days)	Phoca
Trust certificate expired	The trusted certificate has expired.	ERROR	Trust certificate <certName> expired on <expirationDate>	Phoca

ADVANCED Events – Guest Portal

Event Name	Description	Level	Message	Source
Authentication service unavailable	Portal service is unavailable.	ERROR	Authentication service <service> is unavailable.	Castor
Portal send SMS error	An error occurred while sending SMS during portal authorization.	ERROR	Error sending SMS to phone number <target> on portal <portalName>: <error>.	Castor

ADVANCED Events – SMS Notifications

Event Name	Description	Level	Message	Source
Demo SMS Received	SMS received from demo gateway.	INFO	Demo SMS received: <smsMessage>.	Bubo
Error sending email notification	Notification error while sending email	ERROR	Error while sending email to <email>: <error>	Bubo

ADVANCED Events – TACACS+ Authentication

Event Name	Description	Level	Message	Source
TACACS+ access authentication started	User started access authentication via TACACS+	INFO	User <user> started authentication via <tacacsProtocol> .	Aquila
TACACS+ access authentication successful	User successfully passed access authentication via TACACS+	INFO	User <user> passed authentication via <tacacsProtocol> .	Aquila
TACACS+ access authentication error	User failed access authentication via TACACS+	INFO	User <user> failed authentication via <tacacsProtocol> .	Aquila
TACACS+ enable authentication started	User started authentication for privilege level change	INFO	User <user> started privilege level change to <privilegeLevel> via <tacacsProtocol> .	Aquila
TACACS+ enable authentication successful	User successfully changed privilege level	INFO	User <user> successfully changed privilege level to <privilegeLevel> via <tacacsProtocol> .	Aquila
TACACS+ enable authentication error	User failed to change privilege level	INFO	User <user> failed privilege level change to <privilegeLevel> via <tacacsProtocol> .	Aquila

ADVANCED Events – TACACS+ Authorization

Event Name	Description	Level	Message	Source
TACACS+ access authorization successful	User successfully passed access authorization	INFO	User <user> passed authorization via TACACS+.	Aquila
TACACS+ access authorization error	User failed access authorization	INFO	User <user> failed authorization via TACACS+.	Aquila
TACACS+ command authorization successful	User authorized to execute command	INFO	User <user> authorized to execute command <tacacsCommand> .	Aquila

Event Name	Description	Level	Message	Source
TACACS+ command authorization error	User not authorized to execute command	INFO	User <user> failed authorization to execute command <tacacsCommand> .	Aquila

ADVANCED Events – TACACS+ Activity Accounting

Event Name	Description	Level	Message	Source
TACACS+ login	User logged into system	INFO	User <user> logged in.	Aquila
TACACS+ logout	User logged out of system	INFO	User <user> logged out.	Aquila
TACACS+ command execution	User executed command	INFO	User <user> executed commands <tacacsCommand> .	Aquila
Unknown TACACS+ accounting event	Unknown accounting event	INFO	Unknown accounting event for user <user>.	Aquila

ADVANCED Events – Update portal components

Event Name	Description	Level	Message	Source
Portal created	New portal created	INFO	Portal <portalName> was created.	User / UI
Portal modified	Portal parameters modified	INFO	Portal <portalName> was modified.	User / UI
Portal deleted	Portal deleted	INFO	Portal <portalName> was deleted.	User / UI

ADVANCED Events – Update TACACS+ policy

Event Name	Description	Level	Message	Source
TACACS+ policy set created	New TACACS+ policy set created	INFO	TACACS+ policy set <tacacsPolicySetName> was created.	User / UI
TACACS+ policy sets modified	TACACS+ policy sets parameters modified	INFO	TACACS+ policy sets <tacacsPolicySetsNames> were modified.	User / UI
TACACS+ policy sets deleted	TACACS+ policy sets deleted	INFO	TACACS+ policy sets <tacacsPolicySetsNames> were deleted.	User / UI
TACACS+ profile created	New TACACS+ profile created	INFO	TACACS+ profile <tacacsProfileName> was created.	User / UI

Event Name	Description	Level	Message	Source
TACACS+ profile modified	TACACS+ profile parameters modified	INFO	TACACS+ profile <tacacsProfileName> was modified.	User / UI
TACACS+ profiles deleted	TACACS+ profiles deleted	INFO	TACACS+ profiles <tacacsProfilesNames> were deleted.	User / UI
TACACS+ command set created	New TACACS+ command set created	INFO	TACACS+ command set <tacacsCommandName> was created.	User / UI
TACACS+ command set modified	TACACS+ command set parameters modified	INFO	TACACS+ command set <tacacsCommandName> was modified.	User / UI
TACACS+ command sets deleted	TACACS+ command sets deleted	INFO	TACACS+ command sets <tacacsCommandsNames> were deleted.	User / UI
TACACS+ condition created	New condition for TACACS+ policies created	INFO	TACACS+ condition <tacacsConditionName> was created.	User / UI
TACACS+ condition modified	Condition for TACACS+ policies parameters modified	INFO	TACACS+ condition <tacacsConditionName> was modified.	User / UI
TACACS+ conditions deleted	Conditions for TACACS+ policies deleted	INFO	TACACS+ conditions <tacacsConditionsName> were deleted.	User / UI

ADVANCED Events – Update notification gateways

Event Name	Description	Level	Message	Source
Notification gateway created	New notification gateway created	INFO	Notification gateway <notificationGateway> was created.	User / UI
Notification gateway modified	Notification gateway parameters modified	INFO	Notification gateway <notificationGateway> was modified.	User / UI

Event Name	Description	Level	Message	Source
Notification gateways deleted	Notification gateways deleted	INFO	Notification gateways <notificationGateways> were deleted.	User / UI

ADVANCED Events – Update guest users configuration

Event Name	Description	Level	Message	Source
Portal user created	New portal user created	INFO	Portal user <portalUserName> was created.	User / UI
Portal user modified	Portal user parameters modified	INFO	Portal user <portalUserName> was modified.	User / UI
Portal users deleted	Portal users deleted	INFO	Portal users <portalUsersNames> were deleted.	User / UI

Log Collectors

Description

Log Collectors allow configuring the collection and forwarding of system events by event groups to external centralized logging and monitoring systems — for example, SIEM systems or log collectors. This provides centralized event collection, analysis, and storage, simplifying diagnostics, auditing, and security control.

On the **Log Collectors** page, system users can view, add, edit, and delete log collector configurations for different event groups. Events are sent using UDP or TCP to the IP address and port specified in the collector configuration.

Viewing Log Collectors

Name	Server IP address	Port	Event groups
LocalCollector			RADIUS accounting, Licensing, TACACS+ authentication +3
SIEM 1	192.168.223.15	514	RADIUS authentication, TACACS+ activity accounting, Update portal components +3
SIEM 2	192.168.12.68	514	Update network resources, Update identity source sequence, TACACS+ activity accoun... +5

Figure 59. Table with a list of log collectors

The table contains the following columns:

- **Name** – Unique name of the log collector.
 - - This entity is system and cannot be deleted or edited.

Table column settings are configured using the additional menu available via the button: 

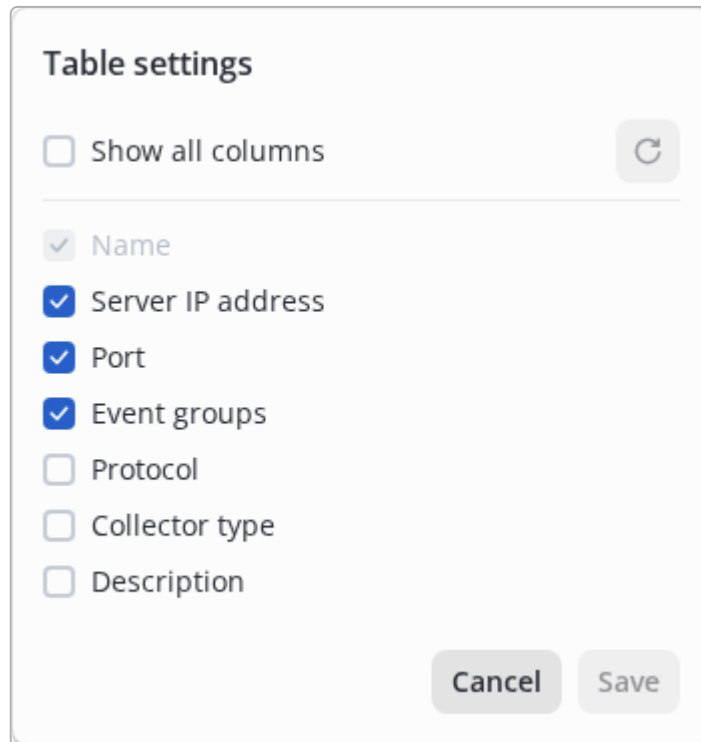



Table settings

Show all columns 

Name

Server IP address

Port

Event groups

Protocol

Collector type

Description






Cancel **Save**

Figure 60. Table column settings

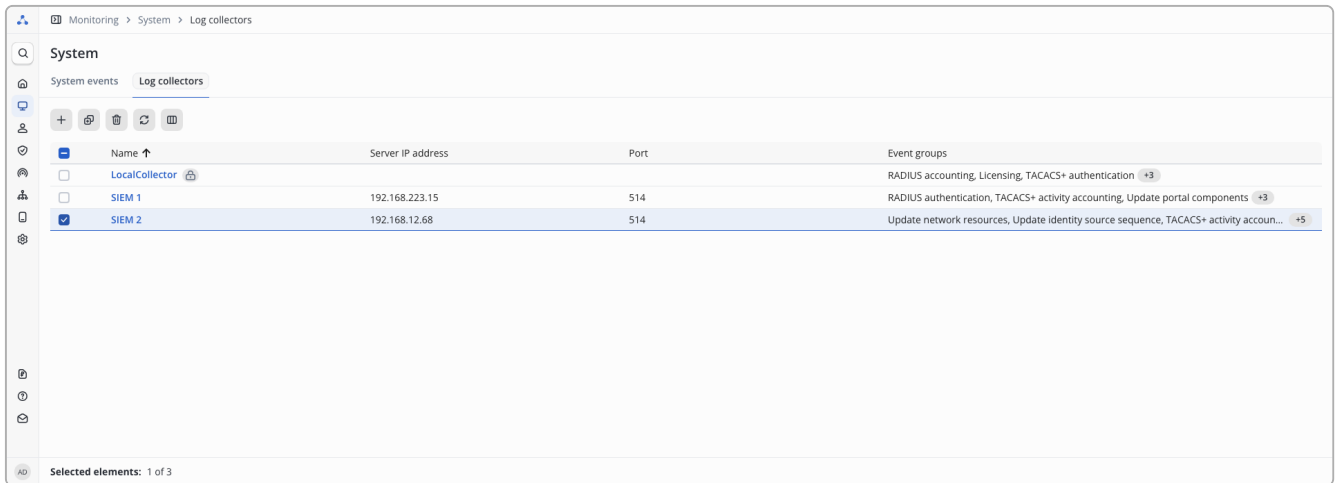
Full list of available table columns:

- **Name** – Unique name of the log collector.
- **Server IP address** – IP address of the server receiving events.
- **Port** – Network port used for event delivery.
- **Event groups** – List of event groups whose events are sent by this collector. A shortened list is displayed (for example, “Update network resources, Update external identity sources... +20”); hovering over the field shows the full list.
- **Protocol** – Data transfer protocol (UDP or TCP).
- **Collector type** – Type of the log collector. All collectors created by a system user have type **Custom**.
- **Description** – Optional description of the log collector.

The page includes the following controls:

-  – Add a new log collector.
-  – Duplicate the selected log collector (available only when exactly one item is selected).
-  – Delete selected log collectors (inactive until at least one item is selected).
-  – Refresh table data.
-  – Change sorting order (available for columns “Name”, “Protocol”, “Collector type”).
- – Checkbox used to select log collectors for further actions.

At the bottom of the page, the total number of log collectors and the number of selected items are displayed.



The screenshot shows a table with the following columns: Name, Server IP address, Port, and Event groups. The table contains three rows: LocalCollector, SIEM 1, and SIEM 2. SIEM 2 is selected, and the bottom status bar indicates 'Selected elements: 1 of 3'.

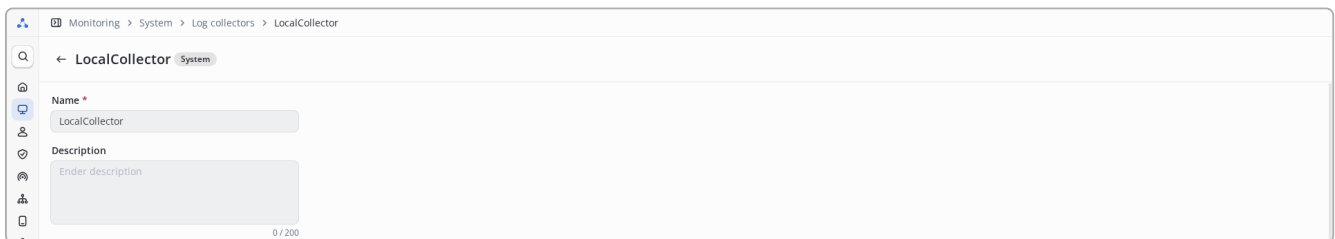
Name	Server IP address	Port	Event groups
LocalCollector			RADIUS accounting, Licensing, TACACS+ authentication +3
SIEM 1	192.168.223.15	514	RADIUS authentication, TACACS+ activity accounting, Update portal components +3
SIEM 2	192.168.12.68	514	Update network resources, Update identity source sequence, TACACS+ activity accoun... +5

Figure 61. Log collector counter

System Log Collector

By default, the table contains a predefined system log collector `LocalCollector` with collector type `System` collector.

This log collector is used to collect internal NAICE system events and store them in the local database:



The screenshot shows the configuration page for the LocalCollector. It includes a 'Name' field with the value 'LocalCollector' and a 'Description' field with the placeholder text 'Enter description'. The 'Name' field is marked as required with an asterisk.

Figure 62. System log collector "LocalCollector"

The `LocalCollector` already includes mandatory event groups that are stored in the local database and displayed in the system event log. These groups are shown as locked and cannot be edited. Other groups may be enabled or disabled if required:

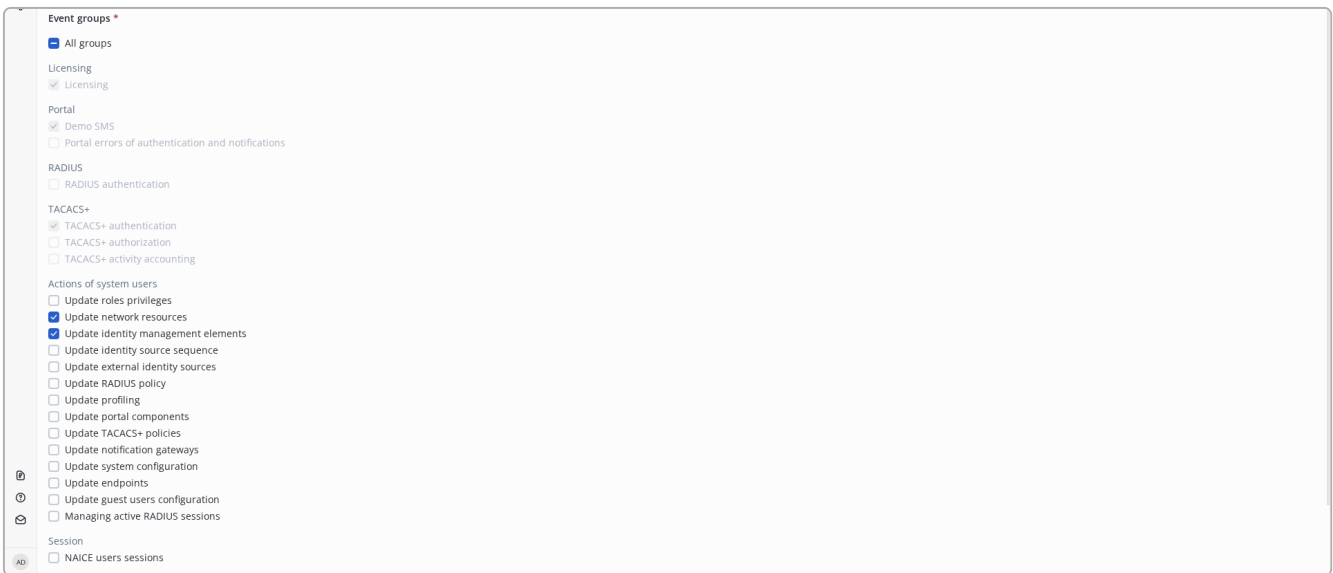


Figure 63. Event groups of the "LocalCollector"

Disabling editable event groups in the system collector results in those events not being stored in the local database and therefore not being displayed in the system event log.



Restrictions for the system log collector:

- The system log collector cannot be deleted.
- The Name and Description fields are not editable for the system log collector.
- Some event groups are mandatory and selected by default; they cannot be modified.
- New log collectors with type System collector cannot be created. All administrator-created collectors are automatically assigned type Custom.

Adding a Log Collector

To add a new log collector, click the button: 

In the opened form, fill in the following fields:

Figure 64. Adding a new log collector (basic settings)

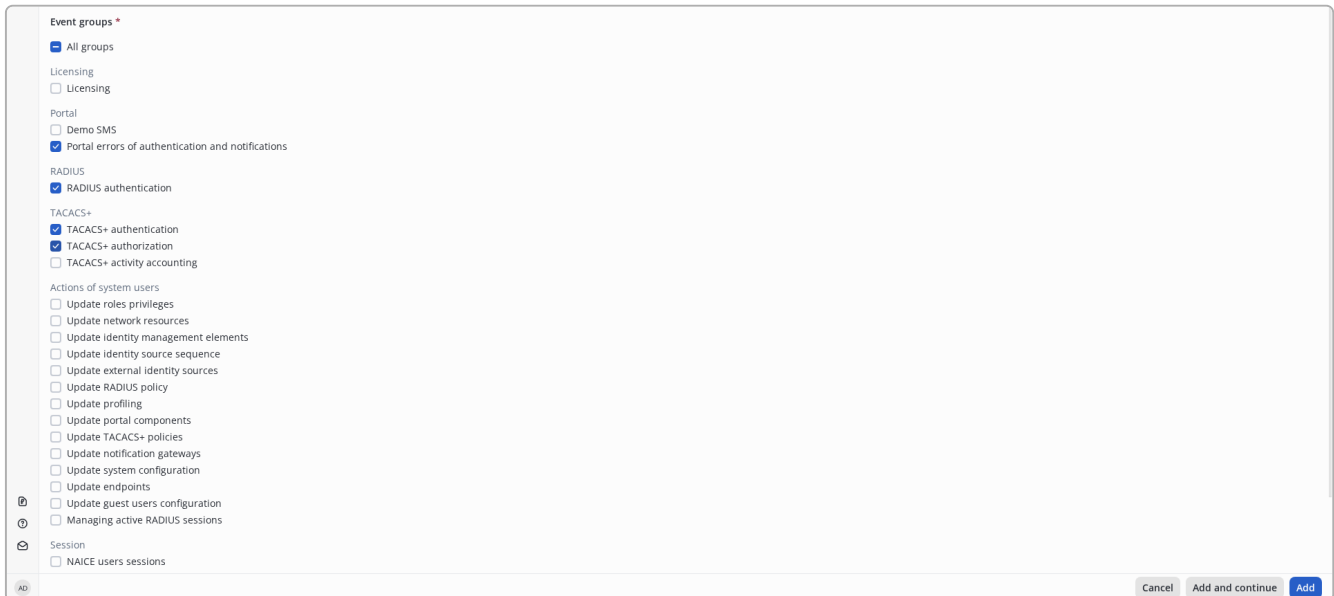
- Name * – Unique name of the log collector.

Server IP address * – IP address of the external system receiving events.

- Port * – Network port on which the external system listens for events.
- Data transfer protocol * – Event transfer protocol. Available options: TCP and UDP.
- Description – Optional text description.

Fields marked with * are mandatory.

In the Event groups section, select the required groups:



The screenshot shows a dialog box titled "Event groups *". It contains a list of event groups with checkboxes. The "All groups" checkbox is selected. Other selected groups include "RADIUS authentication", "TACACS+ authentication", "TACACS+ authorization", and "TACACS+ activity accounting". The dialog also has "Cancel", "Add and continue", and "Add" buttons at the bottom right.

Figure 65. Adding a new log collector (event group selection)

Event group descriptions:

- All groups – Select all available event groups.
- Licensing – Events related to licensing.
- Portal – Events related to Demo SMS messages and portal authentication or notification errors.
- RADIUS – Events related to RADIUS authentication.
- TACACS+ – Events related to TACACS+ authentication, authorization, and activity accounting.
- Actions of system users – Events related to updates of NAICE configuration entities (role privileges, network resources, identity sources, policy sets, etc.).
- Session – Events related to NAICE user sessions.

For adding an event route, the system provides two submit buttons that differ in their subsequent behavior:

- "Add and continue" — after clicking, the form does not close, and the "Send test event" button becomes available.
- "Add" — after clicking, the user is redirected to the event route list page.

Sending Test Events

The operation of a custom log collector can be verified by sending a test event to the external system. To do this, click the **"Send test event"** button.



The **"Send test event"** button is disabled until at least one event group is selected and the log collector is saved.



The result of sending a test event depends on the selected protocol. When using UDP, confirmation from the external system is not possible due to protocol limitations. When using TCP, delivery confirmation is available and displayed in the result window.

Possible results:

- **Test event successfully sent. Check the SIEM system** – Test event sent using UDP.
- **Test event successfully sent** – Test event sent using TCP.
- **Test event send timeout** – No response received from the external system when establishing the TCP connection.
- **SIEM system unavailable** – TCP connection could not be established (connection refused or failed).

Examples of test event result dialogs:

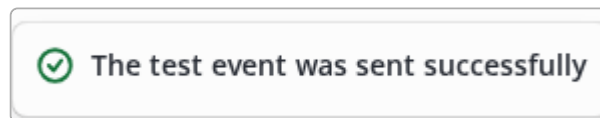


Figure 66. Non-redundant setup, test event sent successfully, TCP protocol

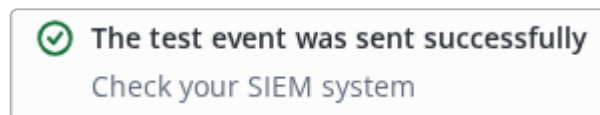


Figure 67. Non-redundant setup, test event sent, UDP protocol

When using a redundant deployment, test events are sent from both NAICE hosts, and two services are shown in the confirmation window.

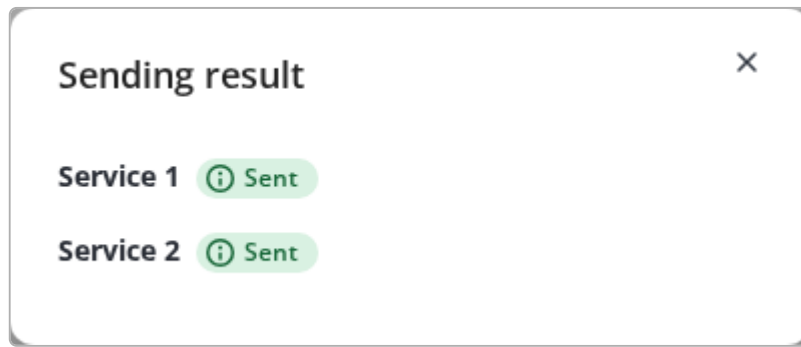


Figure 68. Redundant setup, test event sent successfully from both hosts, TCP protocol

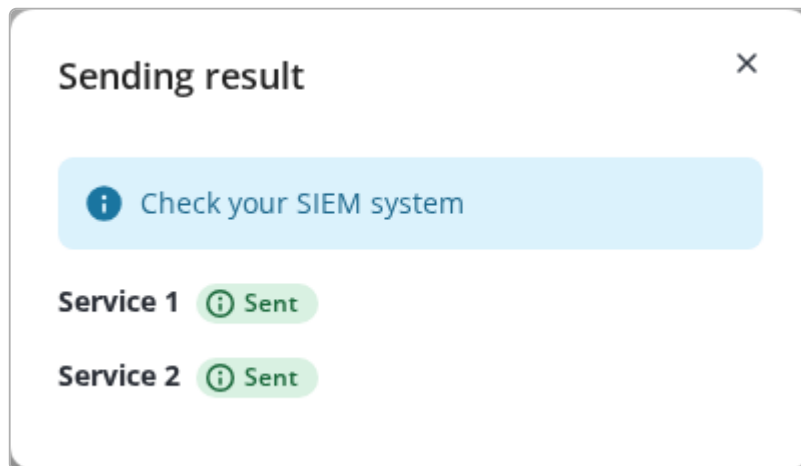


Figure 69. Redundant setup, test event sent from both hosts, UDP protocol

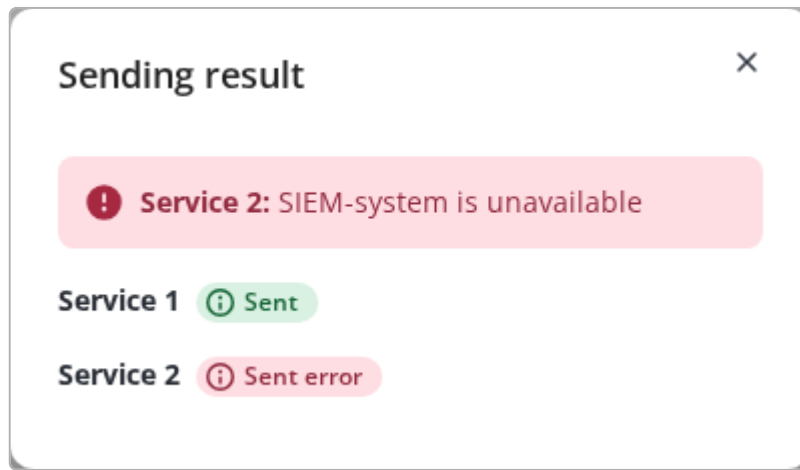


Figure 70. Redundant setup, test event failed on one host, TCP protocol

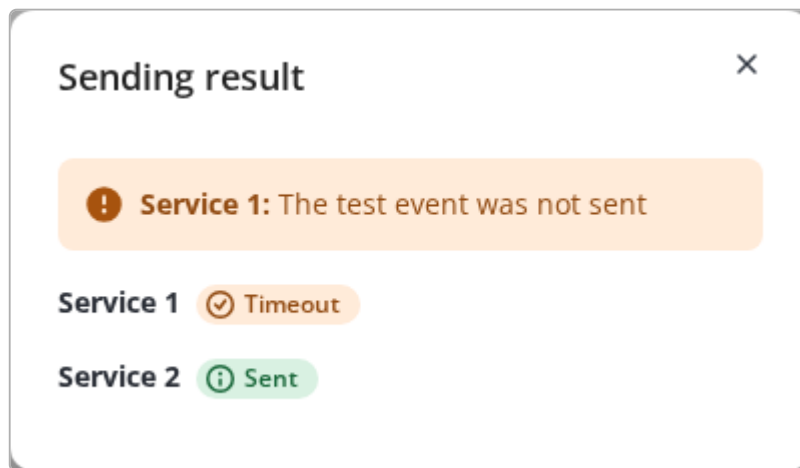


Figure 71. Redundant setup, test event timeout on one host, TCP protocol

Editing a Log Collector

To edit a log collector, on the `Log Collectors` page select the required collector and click its name in the `Name` column.

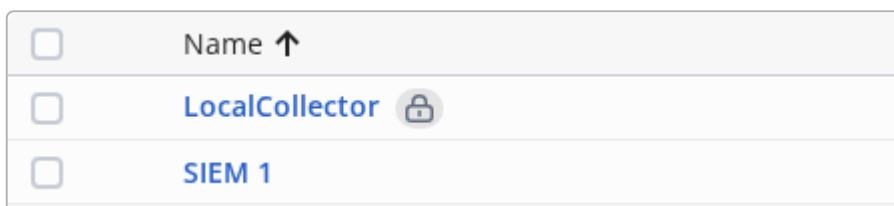


Figure 72. Link to the log collector editing page

The edit form is identical to the add log collector form.



When changes are made to the form, the **"Send test event"** button becomes unavailable. The button is reactivated only after the changes are saved.

Figure 73. Editing log collector fields

Figure 74. Editing log collector event groups

For saving an event route, the system provides two save buttons that differ in their subsequent behavior:

- **"Save and continue"** — after clicking, the form does not close, and the **"Send test event"** button becomes available again.
- **"Save"** — after clicking, the user is redirected to the event route list page.

Duplicating a Log Collector

To duplicate a log collector, select it using the checkbox on the left side of the table:

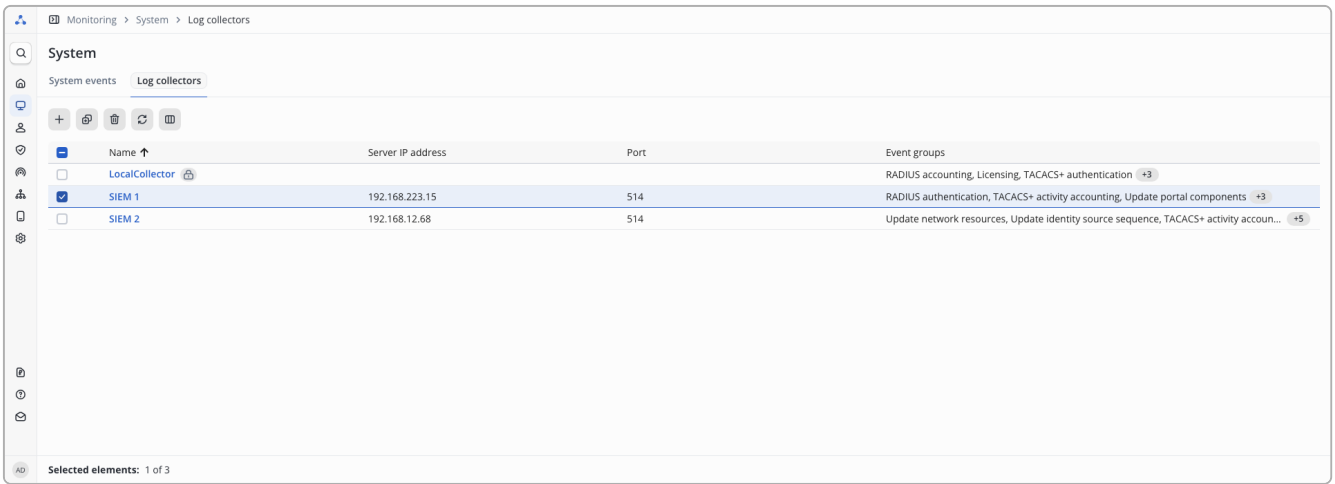


Figure 75. Selecting a log collector for duplication

Then click the button  above the table.

A form will open, similar to the addition form, with all fields filled with values from the selected reference. 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.

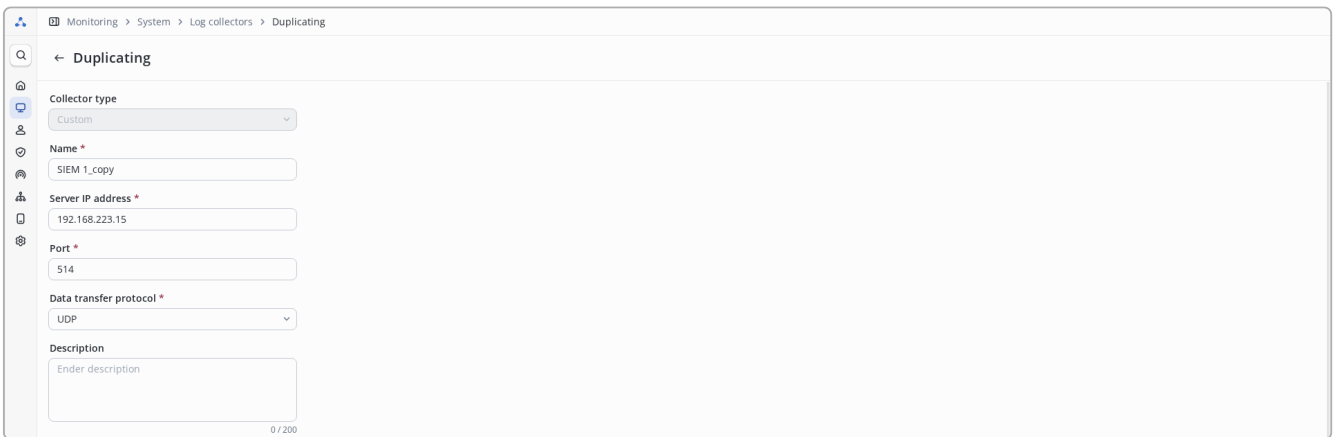


Figure 76. Duplicated log collector settings

If necessary, modify event groups:

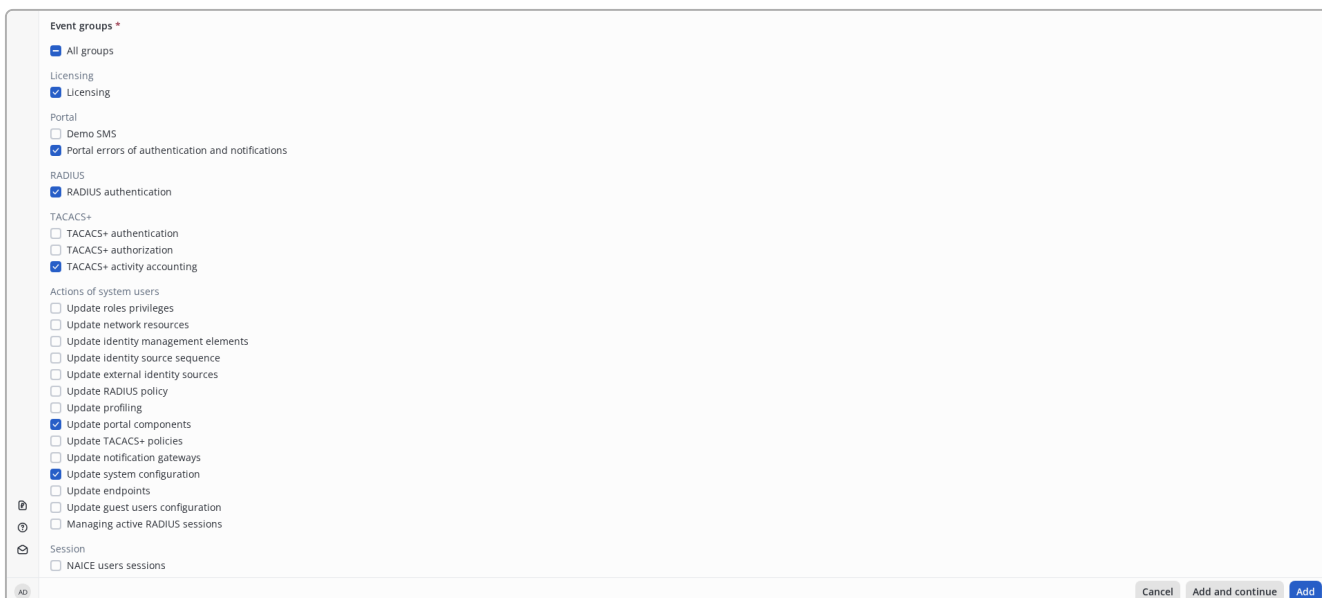


Figure 77. Event groups in the duplicated log collector

For adding an event route, the system provides two submit buttons that differ in their subsequent behavior:

- **"Add and continue"** — after clicking, the form does not close, and the **"Send test event"** button becomes available.
- **"Add"** — after clicking, the user is redirected to the event route list page.

Deleting a Log Collector

To delete one or more log collectors, select them using the checkboxes:

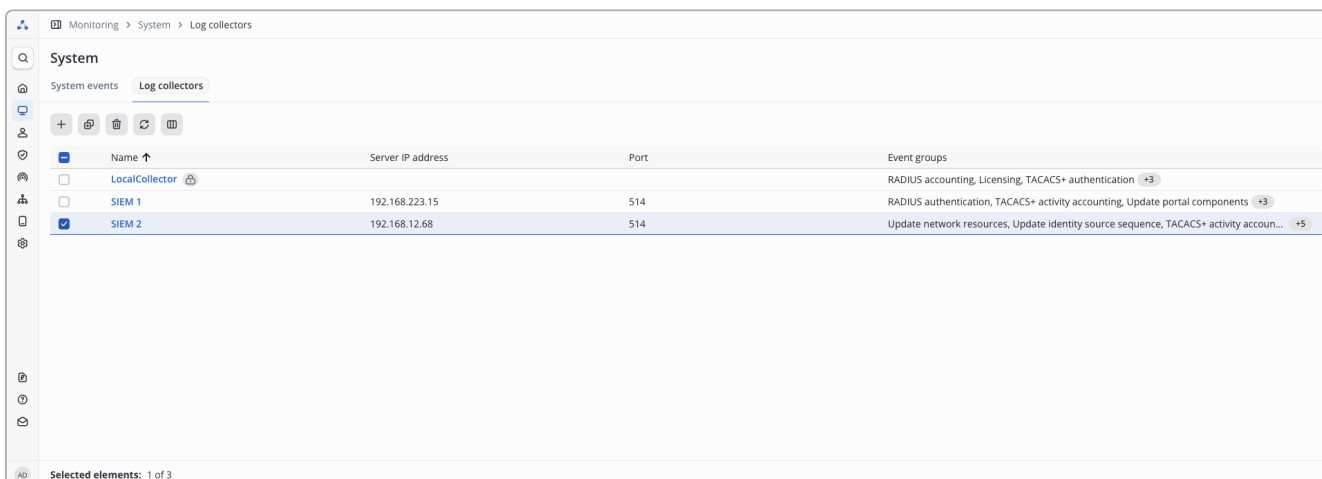


Figure 78. Selecting log collectors for deletion

Then click the button  above the table.

After deletion, events will no longer be sent to the server specified in the log collector. The action can be confirmed or canceled in the confirmation dialog:



Deleting items requires confirmation in the modal window.
The selected items will be deleted only after explicit confirmation of the operation.

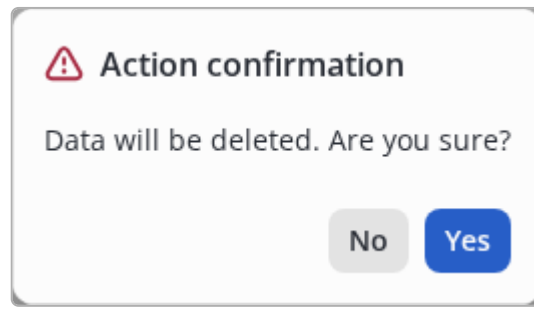


Figure 79. Modal dialog for confirmation

Users and devices

System users

Accounts

Description

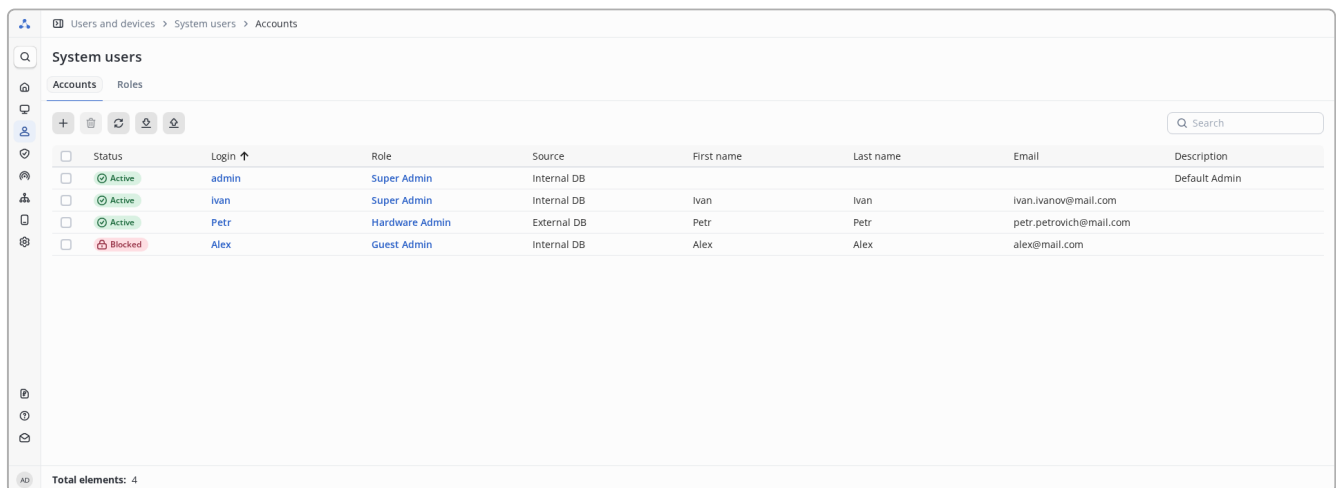
This section is intended for managing the credentials of users of the NAICE system.

System user accounts are divided into two types:

- **Local** — created directly in the NAICE system (`Internal DB` source);
- **External** — created automatically upon first successful authentication through an [external identity source](#).

[Account settings](#) of the current system user are available on any page by clicking on **AD** in the lower left corner of the window in the menu.

View all system user accounts



The screenshot shows a web interface for managing system users. The breadcrumb path is 'Users and devices > System users > Accounts'. The page title is 'System users'. There are tabs for 'Accounts' and 'Roles'. A search bar is present. The table below lists four system user accounts with columns for Status, Login, Role, Source, First name, Last name, Email, and Description.

	Status	Login ↑	Role	Source	First name	Last name	Email	Description
<input type="checkbox"/>	Active	admin	Super Admin	Internal DB				Default Admin
<input type="checkbox"/>	Active	Ivan	Super Admin	Internal DB	Ivan	Ivan	ivan.ivanov@mail.com	
<input type="checkbox"/>	Active	Petr	Hardware Admin	External DB	Petr	Petr	petr.petrovich@mail.com	
<input type="checkbox"/>	Blocked	Alex	Guest Admin	Internal DB	Alex	Alex	alex@mail.com	

Total elements: 4

Figure 80. A table with a list of system user accounts on the viewing page

This page displays a table containing a list of all local and external system user accounts.

The table contains the following information about system users:

- **Status** — account state that determines authentication capability:
 - **Active** — the user can sign in to the system;
 - **Disabled** — the user cannot sign in to the system. An account disabling period and disabling reason can be specified;
 - **Blocked** — the user is temporarily blocked, for example, after exceeding the limit of unsuccessful sign-in attempts;
- **Login** — system user login (must be unique and contain no spaces);
- **Role** — [the role](#) of the system user. It is a hyperlink to the page for viewing/editing this role;

Source — indicates the origin of the account: **Internal DB** (created in the NAICE system) or the name of the **external source** (created automatically upon successful authentication through an external source);








- **First name** — system user first name;
- **Last name** — surname of the system user;
- **Email** — system user's email address;
- **Description** — arbitrary description.

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.



Hovering the mouse cursor over the account status in the table displays a tooltip with detailed information: the status validity period (start and end date and time) and the reason for its application.

Controls:

-  — Add a new element.
-  — Delete selected elements (inactive until at least one element is selected).
-  — Refresh table data.
-  — Allows you to download data from a csv file.
-  — Allows you to upload data to a csv file.
- — Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).
-  — Change the current sort order.
-  **Search** — Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.

External system user accounts

External accounts (their local copies) are created automatically in the system upon the user's first successful login through an external identity source.

To view an external system user account, click on the login on the list page. This will open the viewing page for the external system user account:

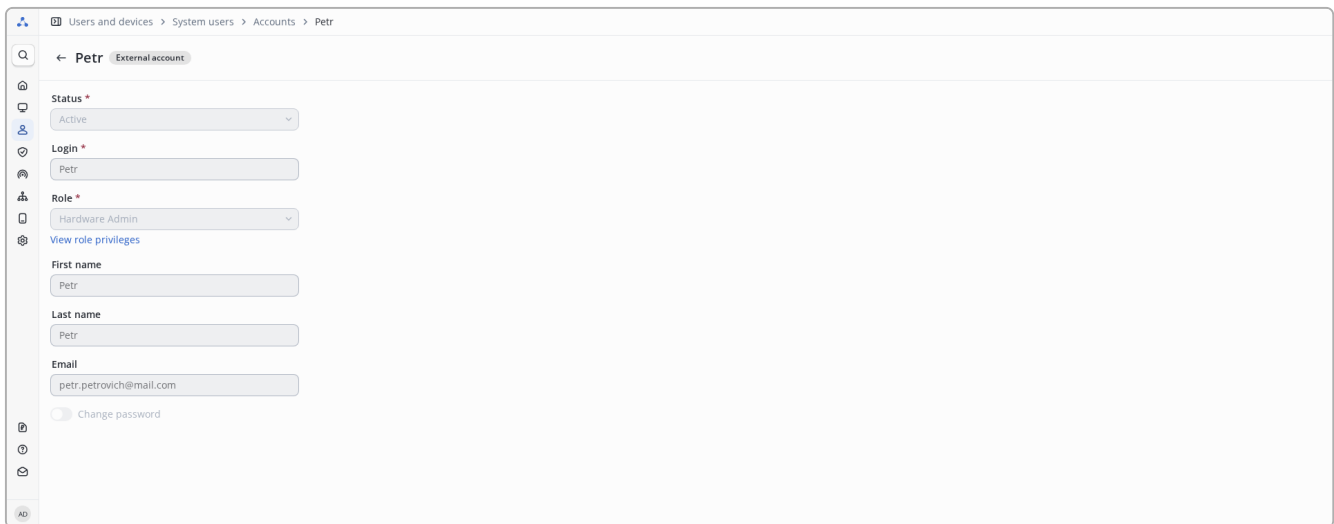





Figure 81. External system user account viewing form

The external account viewing form contains the following fields:

- **Status** — account state that determines authentication capability. For external accounts, the **Active** and **Disabled** statuses are inherited from the external identity source and cannot be changed in NAICE;
 - Exception: if the account has the **Blocked** status, the administrator can manually unblock it by changing the status to **Active**.
- **Login** — user identifier in the external system (must not exceed 100 characters):
 - For accounts from **Active Directory**, the login is always displayed in **UPN (User Principal Name)** format with the domain specified;
 - For accounts from **OpenLDAP**, the login corresponds to the attribute value specified in the **Subject name attribute** field when configuring the external source;
- **Role** — **role** of the external system user, automatically assigned based on the mapping of the user's groups to the groups specified in the NAICE external role settings. The role determines the level of access to the system functionality;
- **First name**, **Last name**, **Email** — user personal data. Populated with values from the corresponding attributes configured in the "**System user information mapping**" block when setting up the external source.

The button "**View role privileges**" opens a window with a table of privileges for the selected role:

- Names of privileges;
- Statuses of issued rights:
 -  — the user has access,
 -  — access is not provided,
 -  — the user does not have access.



Editing external accounts is prohibited. All changes must be made directly in the external identity source.

Exception: unblocking an account if it was blocked by the lockout policy.

With each subsequent login to the system, external account synchronization is performed:



- **attribute updates** (Status, First name, Last name, Email) in accordance with the current data from the external source;
- **role recalculation** based on the current group membership of the user in the external source.

Adding a system user account

To add a system user account, click **+** on the action bar located above the table.


Privilege	Reading	Creation	Editing	Deletion
RADIUS policies	✓	✓	✓	✓
RADIUS monitoring	✓	✓	✓	✓
Endpoints	✓	✓	✓	✓
Network resources	✓	✓	✓	✓
TACACS+ policies	✓	✓	✓	✓
TACACS+ monitoring	✓	—	—	—
Profiling	✓	✓	✓	✓
Roles and accounts	✓	✓	✓	✓
Guest access	✓	✓	✓	✓
Guest users	✓	✓	✓	✓
Enterprise users	✓	✓	✓	✓
System settings	✓	✓	✓	✓
External sources	✓	✓	✓	✓
Notification services	✓	✓	✓	✓

Figure 82. Add system user account page

The add system user form includes the following fields:

- **Status *** — defines the current state of the account. Allows you to allow or deny the user access to the system. The default value is **Active**;
- **Login *** (maximum length — 100 characters);
- **Role *** — select **roles** for the system user. The role determines the level of access to the system functionality;
- **First name** (maximum length — 100 characters);

Last name (maximum length — 100 characters);

- Email (maximum length — 200 characters);
- Description (maximum length — 200 characters);
- Password * (maximum length — 72 characters). By clicking on  you can enable the display of the entered password; by default, the text is hidden. The password must match the current [password policy](#).

* — fields that are required.



You cannot assign a role with higher rights than the current user.

After upgrading the license level, additional privilege settings may be required. Roles that require additional configuration are marked with a warning:

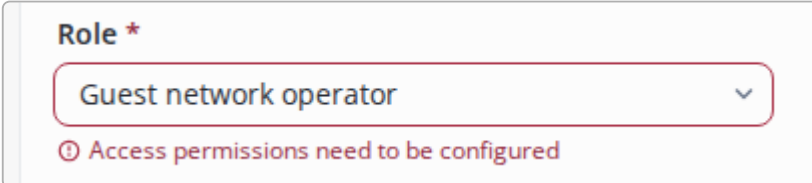






Figure 83. Warning "Access permissions need to be configured"

The button "[View role privileges](#)" opens a window with a table of privileges for the selected role:

- Names of privileges;
- Statuses of issued rights:
 -  — the user has access,
 -  — access is not provided,
 -  — the user does not have access.

In the window, using the **Role** drop-down list, you can view the access rights assigned to other roles. When you click the "**Apply**" button, the role will be re-selected in the account addition form.

The password for the system user can be generated by clicking on the "**Generate Password**" button, or you can enter it manually. The generated password is placed in the "New password" field; it can be copied by clicking on .

To create an account, click the "**Add**" button.

Editing the system user account

To edit a system user account, on the list page, click on its login:

<input type="checkbox"/>	Status	Login ↑
<input type="checkbox"/>	✔ Active	admin
<input type="checkbox"/>	✔ Active	ivan
<input type="checkbox"/>	✔ Active	Petr
<input type="checkbox"/>	🔒 Blocked	Alex

Figure 84. Hyperlink to system user account edit page

This will open the system user account edit page, similar to the add page:

The screenshot shows the 'System user edit form' for user 'ivan'. The breadcrumb navigation is 'Users and devices > System users > Accounts > ivan'. The form fields include:

- Status:** Active (dropdown menu)
- set the shutdown period
- Login:** ivan (text input)
- Role:** Super Admin (dropdown menu)
- [View role privileges](#)
- First name:** ivan (text input)
- Last name:** ivan (text input)
- Email:** ivan.ivanov@mail.com (text input)
- Description:** Enter description (text area, 0/200 characters)
- Change password (toggle)

Figure 85. System user edit form

To change the system user password, you need to enable the **"Change password"** toggle, then enter the desired password in the appropriate fields.



After saving changes **for login, password, and/or role**, the session will be interrupted and re-authentication will be required.



WARNING: Editing your own account is prohibited. To change your account data, go to the [Account settings](#) section.

After making the changes, you need to click on the **"Save"** button. The button is hidden until at least one field is changed.

The **"Cancel"** button resets the changes made to their original state.

Managing account status

The **Status** field defines the state of the system user account.

The following values are available:

Status	Description
Active	The user can sign in to the system.
Disabled	The user cannot sign in to the system. When this status is selected, a disabling period and disabling reason can be specified.
Blocked	The user is temporarily blocked. This status is assigned automatically when the lockout policy is triggered and cannot be set manually.



To enable users to receive email notifications about changes to their account status (blocking, disabling, unblocking), notification delivery must be configured in the **System Settings** → **Security and access** → «[Password policy](#)» section.

Scheduled account disabling

For an active account, a disabling period can be specified in advance.

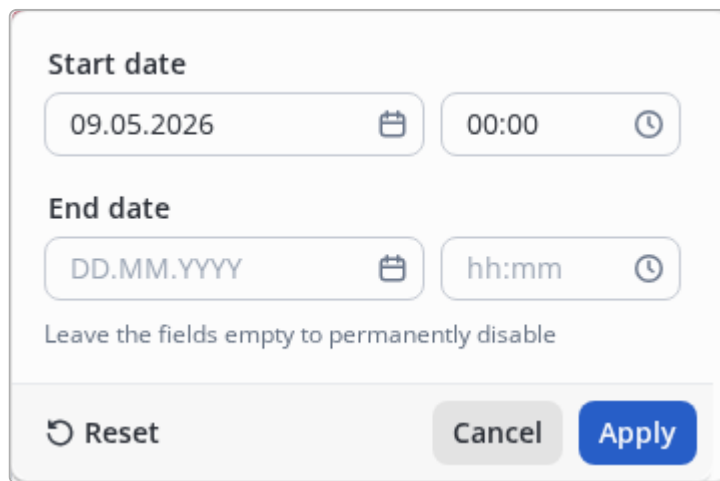
To set a disabling period, select the "**Specify disabling period**" checkbox.

The screenshot shows a form for editing an account. It includes a 'Status' dropdown menu currently set to 'Active'. Below it is a checked checkbox labeled 'set the shutdown period'. Underneath is a 'Disable period' field with a calendar icon, showing the date and time '09.05.2026 00:00 - indefinitely'. At the bottom is a text area for 'Disable account reason' with the placeholder text 'Enter reason' and a character count '0 / 200'.

Figure 86. Account edit form with scheduled disabling

When scheduled disabling is activated, the following fields become available:

- **Account disabling period** — the interval during which the account will be unavailable.
 - **Start date and time** — from this moment the account will be disabled;
 - **End date and time** — after this moment access will be restored.
- **Disabling reason** — an explanation of why the account is being disabled.



The image shows a dialog box for selecting a disabling period. It has two sections: 'Start date' and 'End date'. The 'Start date' section has a date field with '09.05.2026' and a calendar icon, and a time field with '00:00' and a clock icon. The 'End date' section has a date field with the placeholder 'DD.MM.YYYY' and a calendar icon, and a time field with the placeholder 'hh:mm' and a clock icon. Below these fields is the text 'Leave the fields empty to permanently disable'. At the bottom are three buttons: 'Reset' (with a circular arrow icon), 'Cancel', and 'Apply' (in blue).

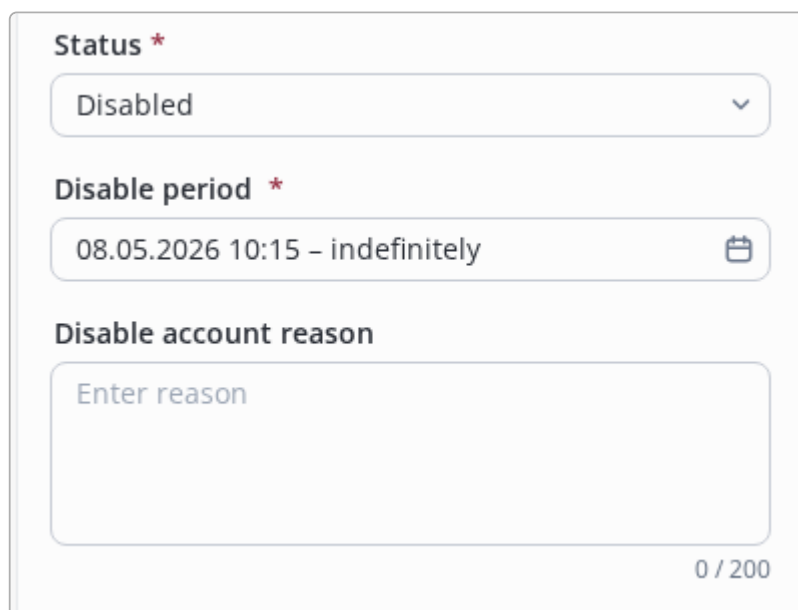
Figure 87. Account disabling period selection window



- The **start** date and time are required and must be later than the current moment.
- If the **end** date and time are not specified, the account will be disabled indefinitely.

Disabling an account

To prevent the user from signing in, change the `Status` field value to `Disabled`.



The image shows a form for disabling a local account. It has three main sections: 'Status *' with a dropdown menu showing 'Disabled'; 'Disable period *' with a date and time field showing '08.05.2026 10:15 - indefinitely' and a calendar icon; and 'Disable account reason' with a text input field containing the placeholder 'Enter reason'. At the bottom right of the text field is a character count '0 / 200'.

Figure 88. Disabling a local account

When an account is disabled, additional fields become available:

- `Account disabling period` — the interval during which the account will be unavailable. The start field is automatically filled with the current time (the moment the changes are saved);
- `Disabling reason` — an explanation of why the account is being disabled.

If the **end** date and time are not specified, the account will be disabled indefinitely.

Blocked account



Figure 89. Blocked account in the table

An account can be automatically blocked by the system when the [lockout policy](#) is triggered — for example, after exceeding the allowed number of unsuccessful sign-in attempts.

The `Blocked` status is assigned automatically and **cannot be set manually** through the edit form. The block can be removed in one of the following ways:

- automatically — after the lockout time specified in the policy expires;
- manually — the administrator can unblock the account by changing the status to `Active`.

Local account

For a local account, the edit form displays lockout details:

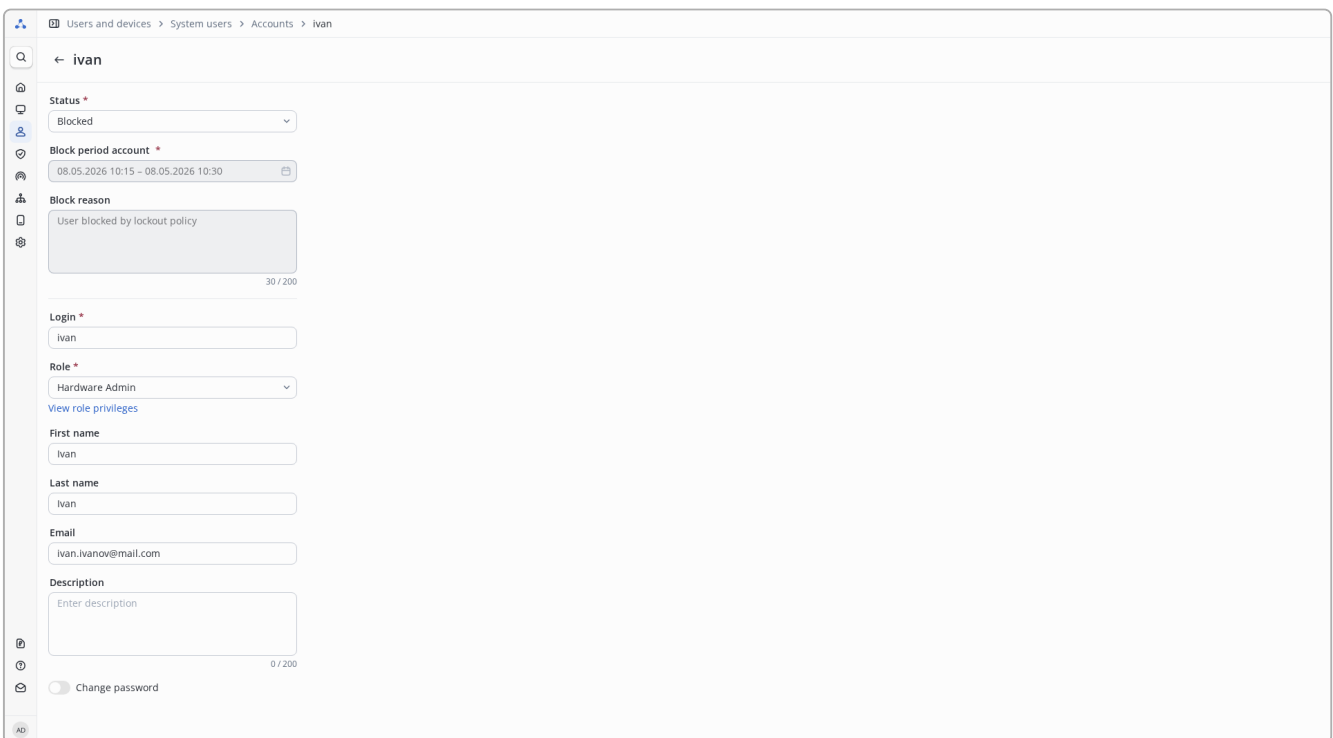


Figure 90. Blocked local account edit form

The following fields are available:

- `Account lockout period` — the time interval during which the account remains blocked;
- `Lockout reason` — the reason why the account was blocked (generated automatically by the system).

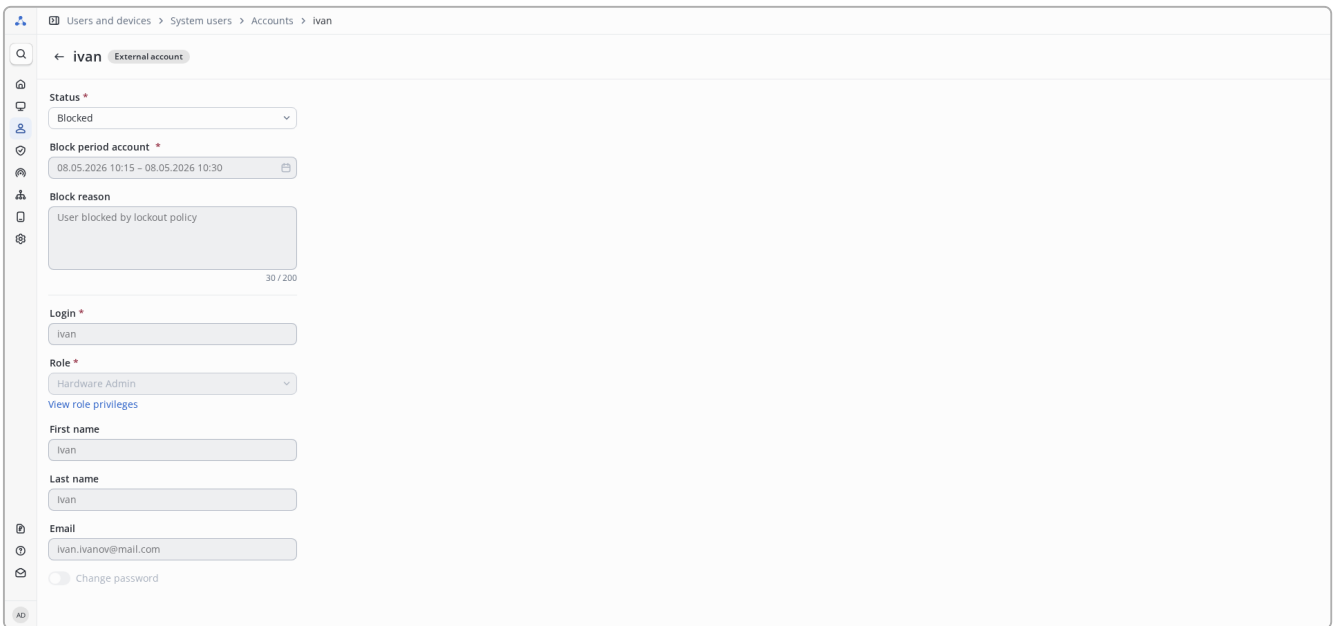
The administrator can change the state of a blocked account:

- to **unblock** the account, change the `Status` field value to `Active`;
- to **disable** the account (for example, to temporarily deny access), change the `Status` field value to `Disabled`.

After changing the status, save the changes by clicking the "Save" button.

External account

For an external account, lockout details are displayed in the viewing form:



The screenshot shows a web interface for managing system users. The breadcrumb trail is 'Users and devices > System users > Accounts > ivan'. The user 'ivan' is identified as an 'External account'. The form displays the following fields:

- Status ***: A dropdown menu set to 'Blocked'.
- Block period account ***: A date range field showing '08.05.2026 10:15 - 08.05.2026 10:30' with a calendar icon.
- Block reason**: A text area containing 'User blocked by lockout policy' with a character count of '30 / 200'.
- Login ***: A text field containing 'ivan'.
- Role ***: A dropdown menu set to 'Hardware Admin' with a link to 'View role privileges'.
- First name**: A text field containing 'ivan'.
- Last name**: A text field containing 'ivan'.
- Email**: A text field containing 'ivan.ivanov@mail.com'.
- Change password**: A toggle switch that is currently turned off.


Figure 91. Blocked external account viewing form

The following fields are available for a blocked external account:

- **Account lockout period** — the time interval during which the account remains blocked;
- **Lockout reason** — the reason why the account was blocked (generated automatically by the system).

The administrator can change the state of a blocked external account by changing the **Status** field value to **Active**.

Removing the system user account

To delete a system user account, in the table, select the checkbox to the left of the account to be deleted and click  on the action bar located above the table.



If the selected system user (both local and external) had a session open, it will terminate immediately.

Status	Login	Role	Source	First name	Last name	Email	Description
<input type="checkbox"/>	admin	Super Admin	Internal DB				Default Admin
<input checked="" type="checkbox"/>	Ivan	Super Admin	Internal DB	Ivan	Ivan	ivan.ivanov@mail.com	
<input checked="" type="checkbox"/>	Petr	Hardware Admin	External DB	Petr	Petr	petr.petrovich@mail.com	
<input type="checkbox"/>	Alex	Guest Admin	Internal DB	Alex	Alex	alex@mail.com	

Figure 92. Selecting system user accounts in the table for deletion



Deleting items requires confirmation in the modal window. The selected items will be deleted only after explicit confirmation of the operation.

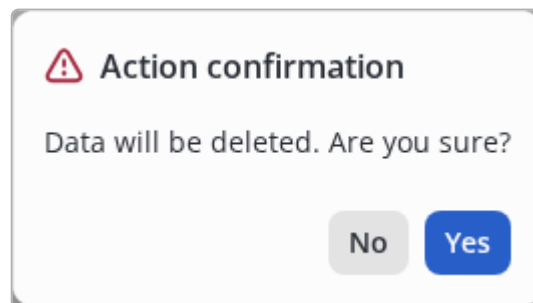


Figure 93. Modal dialog for confirmation



You cannot delete an account that is currently logged in.

Import

NAICE supports importing data from CSV files.

Preliminary preparation before Import

1. Create or verify the existence of necessary related entities (e.g., device profile).
2. Review the CSV file requirements:
 - Encoding must be UTF-8;
 - Delimiters:
 - Field delimiter: comma (,)
 - String/text delimiter: double quotation mark (")
 - Headers and values must be enclosed in double quotation marks (")
 - Maximum file size is 2MB.
3. Check the file content for extraneous quotation marks before importing;
4. Check that the values containing the double quotation mark (") or the slash (/) are correctly escaped.

- Values containing a double quotation mark (") are escaped using \"
- Values containing the slash (/) are escaped using \/

Correct spelling of values (with escaping using \") using the example of the contents of the file for importing the TACACS Command set

"name:Required"	"description"	"permit_unmatched(true/false)"	"commands(Grant/command/arguments/enabled;...)"
"command_set"	"\"Test command set\""	"false"	"PERMIT/\"show/vlan 1 2 \"/true"


Incorrect spelling of values (without escaping) using the example of the contents of the file for importing the TACACS Command set

"name:Required"	"description"	"permit_unmatched(true/false)"	"commands(Grant/command/arguments/enabled;...)"
"command_set"	"Test command set"	"false"	"PERMIT/show/vlan 1 2 /true"



Failure to escape these characters will lead to incorrect data recognition.

Import procedure


To import data from a CSV file, click on  in the action panel located above the table. This will open the import window:

Import

When importing, duplicate data will not be overwritten or edited - the system will skip it. If you want to change old data, delete it from the system manually before importing.

Carefully review the [Documentation](#) to ensure the import completes without errors.

Select a file*
Max file size 2MB

 Upload or drag it here

Field is required

Data source *

NAICE ▾

Ignore exist data ⓘ

Stop import on first error

Cancel
Import

Figure 94. Window Import

Data import proceeds through several steps:

1. Select the required CSV file by dragging it into the upload area or by selecting it through the file explorer by clicking the **"Upload"**;



To apply changes, you must re-upload an updated CSV file.

2. Select the data source (if not predefined);
3. Configure import flags (if needed):

Ignore exist data

- On: Duplicate records trigger warnings.
- Off: Duplicates are treated as errors.

Stop import on first error

- On: Import halts at the first error. Only records that were successfully processed before it occurred will be imported.
-

Off: Erroneous lines are skipped, and the import continues to the end. Only valid records will be imported.

4. To start the import, click the "**Import**".



When importing, duplicate data will not be overwritten or edited - the system will skip it. If you want to change old data, delete it from the system manually before importing.

Viewing the Import report

An import report window opens immediately after file processing.

If all records in the file were processed correctly, you will see the following window:

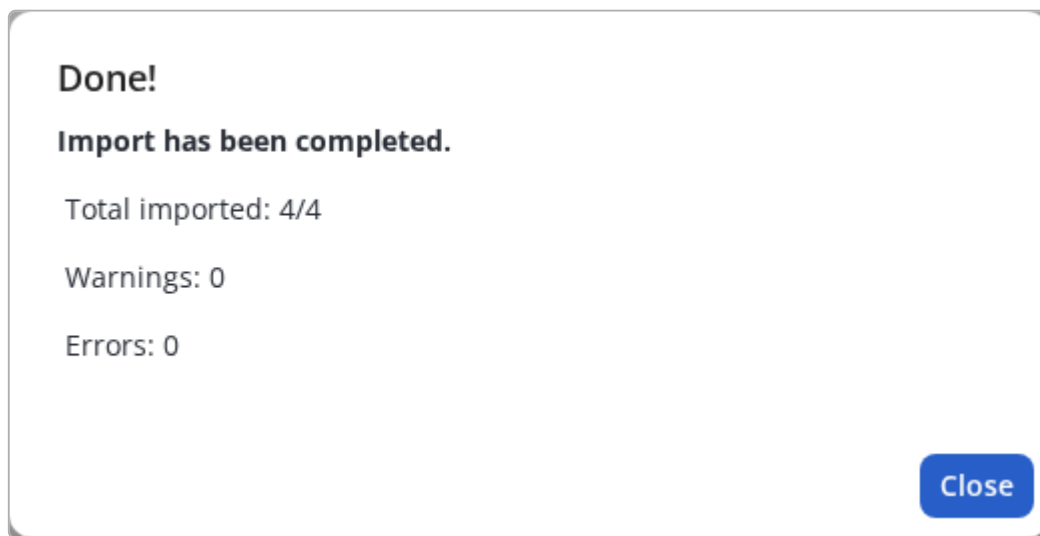


Figure 95. Window Import report (all entries were processed correctly)

The summary block contains:

- **Total Imported** - Counter of records imported (vs. total rows processed);
- **Warnings** - Number of warnings that occurred;
- **Errors** - Number of errors that occurred.

If not all records were processed correctly, you will see the following window:

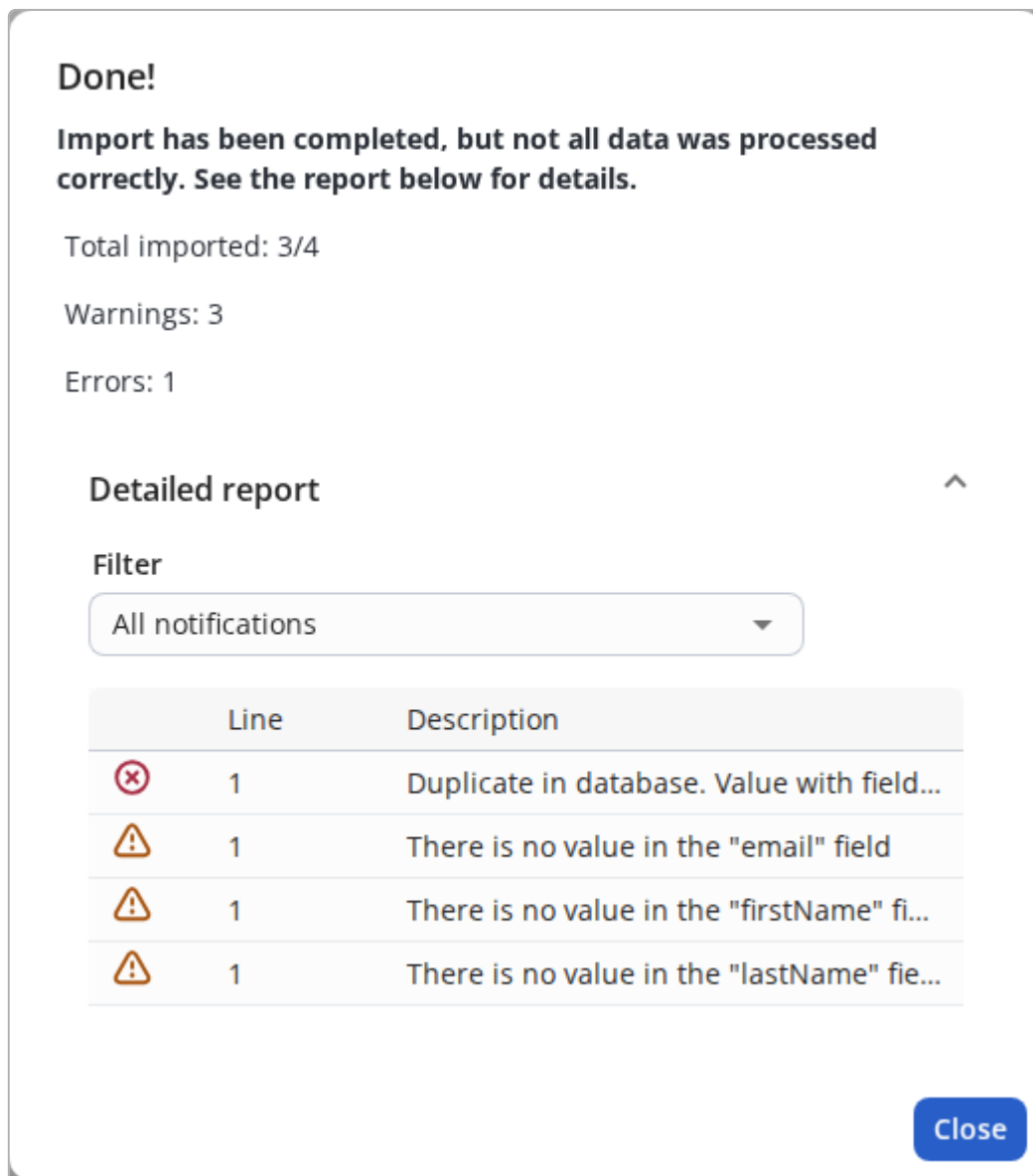


Figure 96. Window Import report (entries processed with errors/warnings)

Detailed report contains the following information:

- **Filter** - Dropdown list allowing you to select which notifications to display (All notifications , Only errors , or Only warnings)

The notification table contains columns:

- **Line** - The line number in the CSV file where an error or warning was detected;
- **Description** - Detailed text explanation of the error or warning.



Hover your cursor over a row in the Description column to view the full error/warning message in a tooltip.

Import particularities for system user accounts



Only NAICE is supported as a data source for importing system user accounts.



Import of external accounts is not supported.

The table below lists the fields, their requirements, descriptions, and requirements:

Field	Description	Requirements
login:Required	System user login	Required Maximum length - 100 characters Must be unique Spaces are not allowed
role:Required	System user role	Required The role must exist in the system
password:Required	System users password. Can be imported in either hashed or plain text format	Required Maximum length - 72 characters Must match the current password policy Symbols № and ` are not allowed
isEncrypted:Required	Password hashing flag. Indicates the format in which the password is transmitted	Required Possible values: - true — the transmitted password is hashed - false — the password is transmitted in plain text and will be hashed during import
status:Required	User status	Required Possible values: - ENABLED — user is enabled - DISABLED — user is disabled - BLOCKED — user is blocked
disableStartTime	Time from which the user is disabled	Time in YYYY-MM-DDTHH:MM:SSZ format Used if a disabling period is set for the user
disableEndTime	Time until which the user is disabled	Time in YYYY-MM-DDTHH:MM:SSZ format If no value is specified, the user will be disabled indefinitely
disableReason	User disabling reason	Maximum length - 200 characters
firstName	System user first name	Maximum length - 100 characters
lastName	Surname of the System user	Maximum length - 100 characters

Field	Description	Requirements
email	Email address	Maximum length - 200 characters Format: admin123@gmail.com Invalid characters: <ul style="list-style-type: none"> • cyrillic letters (а-я)(А-Я) • space • double quotes " • numero sign № • semicolon ; • colon : • comma , • parentheses () • square brackets [] • greater-than/less-than signs < > • backslash \
description	Arbitrary description	Maximum length - 200 characters
totpSeed	TOTP secret	TOTP secret encrypted with AES-256-GCM
activatedEmailOtp	Email OTP	Possible values: <ul style="list-style-type: none"> - true — method enabled - false — method disabled
backupCodes	Backup codes	Backup codes hashed with Bcrypt (no more than 10 codes)



When importing accounts with configured 2FA, the encryption master key (AES-256-GCM) for TOTP secrets must match on the source and target instances. Otherwise, TOTP will not work.

Example of a correctly formatted file:

"login: Required"	"role: Required"	"password: Required"	"is Encrypted: Required"	"status: Required"	"first Name"	"last Name"	"email"	"description"	"disableStart Time"	"disableEndTime"	"disableReason"	"totpSeed"	"activateEmailOtp"	"backupCodes"
"administrator"	"Super Admin"	"password"	"false"	"ENABLED"	"Иван"	"Иванов"	"ivanov@te.st.ru"	"Default"	"2020-05-26T11:22:07Z"	"2020-05-26T13:00:00Z"	"Много наболю дал"	"/M JRA E4p 6F ..."	"true"	"\$2a\$10\$gVjsW..."



Values containing double quotation marks (") or slashes (/) must be escaped using \". Failure to escape these characters will result in incorrect data recognition.



All imported records receive the source `Internal DB` (NAICE system internal database).

Export

NAICE supports exporting data in CSV format. Values and headings are framed by `double quotes`, the field separator is `comma (,)`.

Export procedure

Two export modes are available:

- `Export all` - Exports all records from the current section. System entities are not included during export.
- `Export selected` - Exports only checked records.

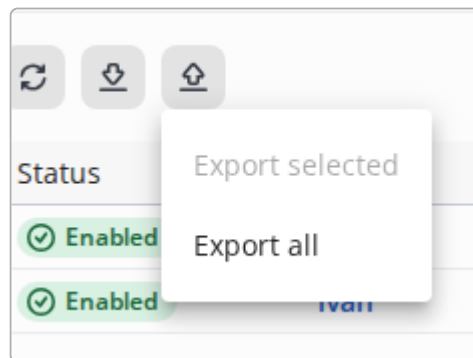



Figure 97. Window export menu



Values containing double quotation marks (") or slashes (/) will be escaped using \".

Export all

On the action panel above the table, click  and select the **"Export all"** mode. In the window that opens, confirm the action by clicking the **"Export"**:

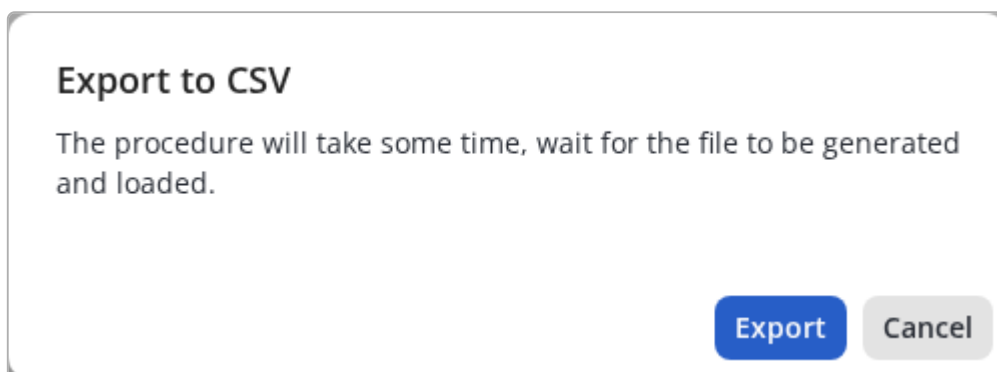



Figure 98. Export all

After clicking the **"Export"**, a file containing all records from the current section will be downloaded to your device.

Export selected

On the action panel above the table, click  and select the **"Export selected"** mode. In the window that opens, confirm the action by clicking the **"Export"**:

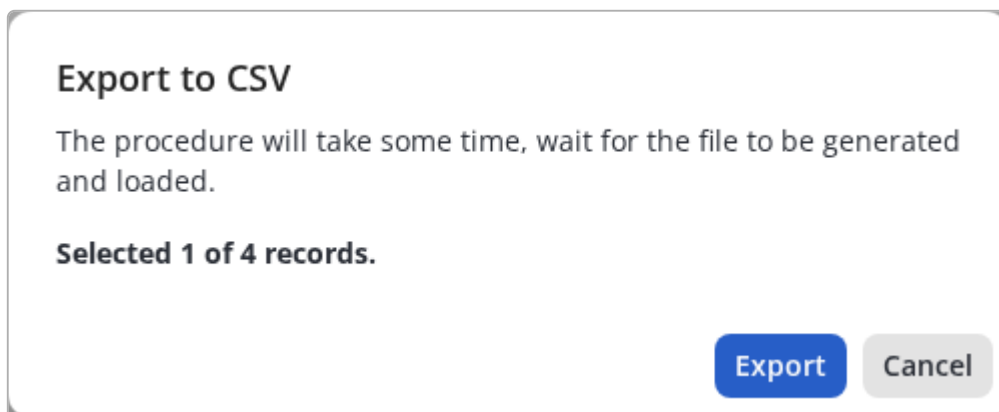


Figure 99. Export selected

After clicking the **"Export"**, a file containing only the checked records will be downloaded to your device.



When **opening** CSV files, **always** use a **comma (,)** as the field delimiter. **Double quotation marks (")** or **empty values** may be used as string/text delimiters.

When **saving** CSV files, **always** use a **comma (,)** as the field delimiter, with an **empty value** as the string/text delimiter.



If a double quotation mark (") was used as the line delimiter when opening the file, values containing double quotation marks (") or slashes (/), escaped as "\", may receive an extra quotation mark (") upon saving. Please check the file in a text editor and remove any extra quotation marks if they appear.

Template

If there are no records in the table (or only system entities are present), selecting the **"Export all"** mode will generate a CSV file containing only the column headers. This file can be used as a **template** for preparing data prior to import.

Export particularities for system user accounts

When exporting, consider the following features:

- **Passwords** are exported from the database in a hashed format (Bcrypt algorithm). Recovery of original passwords is not possible.
- **External accounts** are also included in the exported CSV file.



For correct import of external accounts into the target system, you must:

1. Pre-create the **external identity source** (AD, LDAP) in NAICE that corresponds to the exported records.
2. Configure **external roles** for group mapping.

If the external source or roles are missing, importing external accounts will be impossible.

The structure of the CSV file for system user accounts is described in the section "[Import particularities for system user accounts](#)".

Roles

Description

The "Roles" section is designed for managing access rights for NAICE system users.

NAICE provides two types of roles:

- **Internal roles** — assigned manually to local accounts.
- **External roles** — assigned automatically to external accounts based on user membership in groups within an external identity source.

Access levels

The system supports five access levels for each privilege:

Level	Description
0 (Disabled)	Access to functionality is absent. Associated sections are not displayed in the interface.
1 (Reading)	Viewing data and sections related to the privilege.
2 (Creation)	Creating new entities in addition to viewing.
3 (Editing)	Modifying existing entities in addition to viewing and creating.
4 (Deletion)	Full access, including entity deletion.

Each subsequent access level includes the capabilities of the previous one.



Some privileges (such as those related to monitoring) have a maximum access level of **1** (read-only).

Predefined roles



Deleting and editing preset roles is prohibited.

The system includes the following preset roles for typical usage scenarios:

- **Super Admin** — full access to all functionality.
- **Network Admin** — network access management.
- **Hardware Admin** — network device management.
- **System Admin** — system administrator.
- **Guest Admin** — guest network management.
- **Guest Operator** — guest network operator.
- **Monitor** — monitoring and data viewing.

Privilege levels for preset roles

Privilege	Super Admin	Network Admin	Hardware Admin	System Admin	Guest Admin	Guest Operator	Monitor
RADIUS policy	4	4	0	4	1	0	1
RADIUS monitoring	4	4	0	4	4	1	1
Endpoints	4	4	0	4	0	0	1
Network resources	4	4	4	4	1	0	1
TACACS+ policy	4	0	4	4	0	0	1
TACACS+ monitoring	1	0	1	1	0	0	1
Profiling	4	4	0	4	1	0	1
Roles and accounts	4	0	0	1	0	0	0
Guest access	4	1	0	4	4	1	1
Guest users	4	4	0	4	4	4	0
Enterprise users	4	4	4	4	0	0	0
System settings	4	0	0	4	0	0	0
External sources	4	1	1	4	0	0	1
Notification services	4	1	0	4	1	1	1

Privileges and system sections

This section provides a complete list of NAICE system privileges and their corresponding interface sections.

Sections not requiring privileges

The following sections are available to all authorized system users regardless of assigned roles:

Sections Not Requiring Privileges

Account settings — management of own credentials.

- **Documentation** — built-in help information.
- **Dashboard** — widget availability on the main page depends on assigned privileges.
- **System events** — availability of event groups is determined by user privileges.

Sections Managed by Privileges



Legend in the table:

- **— (dash)** in the **Access Restrictions** column means that [standard access level rules](#) apply for this privilege.

If text is specified in the column, there are additional conditions described in the cell.

Privilege	Section	Access Restrictions	License Level
RADIUS policy	Network access → Policy elements: → Authorization profiles → Allowed protocols → Conditions → Dictionaries → RADIUS session limits	RADIUS session limits: • Levels 1-3: only <i>Read</i> rights + • <i>Management</i> becomes available from level 4	BASIC
	Network access: → RADIUS policies	• Levels 1-3: only <i>Read</i> rights • <i>Full management, reset count</i> becomes available from level 4	BASIC
	Users and devices → Identity management: → Identity sequences	—	BASIC
RADIUS monitoring	Monitoring → RADIUS: → Connections journal → Active sessions	Active sessions: • Levels 1-3: only <i>Read</i> rights + • <i>End the session</i> becomes available from level 4	BASIC
Endpoints	Users and devices → Identity management: → Endpoints → Endpoint groups	Endpoint groups: • <i>Create/Delete</i> endpoint groups becomes available from level 2 • <i>Add/Remove</i> endpoints to/from groups becomes available from level 3	BASIC
Network resources	Users and devices → Network resources: → Devices → Device groups → Device profiles	—	BASIC

Privilege	Section	Access Restrictions	License Level
TACACS+ policy	Device access → Policy elements: → Conditions → TACACS+ Command sets → TACACS+ Profiles → Dictionaries	—	TACACS+ Module
	Device access: → TACACS+ policies	<ul style="list-style-type: none"> • Levels 1-3: only <i>Read</i> rights • <i>Full management</i>, reset count becomes available from level 4 	TACACS+ Module
	Users and devices → Identity management: → Identity sequences	—	BASIC
TACACS+ monitoring	Monitoring → TACACS+: → Connections journal → Accounting	—	TACACS+ Module
Profiling	Policies → Profiling: → Profiling conditions → Profiling policies → Logical profiles	Profiling policies: <ul style="list-style-type: none"> • Reset count becomes available from level 4 	BASIC
	Policies → Elements: → Dictionaries	—	BASIC
Roles and accounts	Users and devices → System users: → Accounts → Roles	—	BASIC
Guest access	Guest portals → Portal management: → Portal Builder	—	ADVANCED
	Users and devices → Identity management: → Identity sequences	—	BASIC
Guest users	Guest portals → Portal management: → Guest endpoints → Portal users	—	ADVANCED
Enterprise Users	Users and devices → Identity management: → Network users → Network user groups	Network user groups: <ul style="list-style-type: none"> • <i>Create/Delete</i> user groups becomes available from level 2 • <i>Add/Remove</i> users to/from groups becomes available from level 3 	BASIC

Privilege	Section	Access Restrictions	License Level
System settings	Monitoring → System: → Log collectors	<ul style="list-style-type: none"> • Send test event becomes available from level 2 	BASIC
	System settings	<ul style="list-style-type: none"> • Levels 1-3: only <i>Read</i> rights • Level 4: <i>Full management</i> 	BASIC
	Licensing	<ul style="list-style-type: none"> • Levels 0-3: only <i>Read</i> rights • Level 4: <i>Full management</i> 	—
External sources	Users and devices → Identity management: → External identification sources	<ul style="list-style-type: none"> • Check connection available from level 1 • <i>Adding</i> groups and attributes becomes available from level 2 • <i>Deleting</i> groups and attributes becomes available from level 3 	BASIC
Notification services	Notification gateways: → Notification gateways management	<ul style="list-style-type: none"> • Send test SMS/email becomes available from level 2 	BASIC

Dependencies between privileges

For correct system operation, some privileges require the presence of other privileges. When assigning such privileges, the system **automatically activates the necessary related privileges at the read level**.

Privilege	Requires (at least read level)
RADIUS policy	Network resources, Profiling, Guest access
TACACS+ policy	Network resources
Endpoints	Profiling
Roles and accounts	External sources
Guest users	Guest access
Guest access	Notification services
System Settings	External sources, Notification services

Viewing the roles list

Status	Role ↑	Type	Description
Not available	AD_Operators ⚠	External	
Available	Guest Admin	Internal	System role for guest network administrator
Available	Guest Operator	Internal	System role for guest network operator
Available	Hardware Admin	Internal	System role for hardware access administrator
Available	Monitor	Internal	System role for monitoring only with read-only privileges
Available	Network Admin	Internal	System role for network access administrator
Available	read	Internal	
Available	Super Admin	Internal	System role with privileges for all pages and actions
Available	System Admin	Internal	System role for system administrator

Figure 100. Table with list of roles

The page displays a table with all roles. The table contains the following columns:

- **Role** — role name.
 - — this entity is system and cannot be deleted or edited.
 - — warning: indicates an incorrect role configuration.
- **Type** — role type: **internal** (manually assigned) or **external** (automatically assigned based on groups from an external source).
- **Status** — role availability for assignment:
 - **Available** — role can be assigned to users;
 - **Not available** — external role with incorrect settings (for example, when switching from one external source to another or when disabling external authentication). Users cannot obtain this role until the configuration is fixed.
- **Description** — arbitrary description of the role.

Controls:

- — Add a new element.
- — Duplicate chosen element. Becomes active if only one element in the list is selected.
- — Delete selected elements (inactive until at least one element is selected).
- — Refresh table data.
- — Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).
- — Change the current sort order.

Adding a role

To add a new role, click on the action panel above the table.

Adding an internal role

Users and devices > System users > Roles > Adding

← Adding

Role *
Enter name

Description
Enter description
0 / 200

Role type
 internal
 external

Privileges *
Before setting up privileges, carefully read the list of sections included in the privileges

Privilege	<input type="checkbox"/> Reading	<input type="checkbox"/> Creation	<input type="checkbox"/> Editing	<input type="checkbox"/> Deletion
RADIUS policies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
RADIUS monitoring	<input type="checkbox"/>	—	—	—
Endpoints	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Network resources	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TACACS+ policies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TACACS+ monitoring	<input type="checkbox"/>	—	—	—
Profiling	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Roles and accounts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Guest access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Guest users	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Enterprise users	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System settings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
External sources	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Notification services	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Cancel Add

Figure 101. Internal role addition form

The form contains the following fields:

- **Role *** — role name.
- **Description** — arbitrary description (maximum length - 200 characters).
- **Role type *** — select "**internal**" value.
- **Privileges *** — access rights configuration table. You must select a level for at least one privilege.

* — required fields.



You cannot create a role with higher privileges than the current user.

To add a role, click the "**Add**" button.

Adding an external role

The screenshot shows a web interface for adding a role. The breadcrumb trail is 'Users and devices > System users > Roles > Adding'. The form has a search bar and a back arrow. The main form fields are:

- Role ***: A text input field with the placeholder 'Enter name'.
- Description**: A text area with the placeholder 'Enter description' and a character count '0 / 200'.
- Role type**: Radio buttons for 'internal' and 'external' (selected).
- Access source**: A dropdown menu showing 'MS AD'.
- To assign a role need**: Radio buttons for 'be in all specified groups (AND)' (selected) and 'be in at least one of groups (OR)'.
- Directory service groups ***: A search input field with a plus sign.
- Privileges ***: A table with columns for 'Privilege', 'Reading', 'Creation', 'Editing', and 'Deletion'. The table lists various system components like RADIUS policies, Network resources, etc.

At the bottom right, there are 'Cancel' and 'Add' buttons.

Figure 102. External role addition form

The form contains the following fields:

- **Role *** — role name.
- **Description** — arbitrary description (maximum length - 200 characters).
- **Role type *** — select "**external**" value.
- **Access source** — external identity source whose groups are used for mapping.



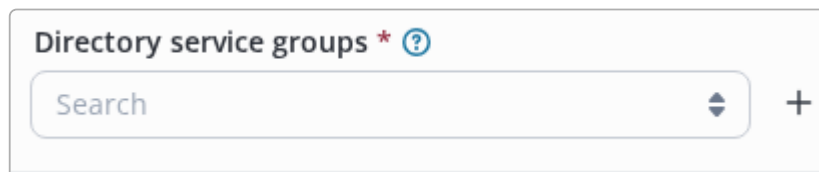
The field is filled automatically based on the configuration in the [System Log In](#) section and does not require manual selection. The source specified in the "Authentication source" field when the "Use external identity source as the main authentication source" option is enabled is used as the value.

- **To assign a role need** — selecting a condition when checking whether users belong to groups from the directory service.
 - **be in all specified groups** (logical «AND») — the role is assigned only to users who are members of **all** selected groups simultaneously. This is the default value.
 - **be in at least one of groups** (logical «OR») — the role is assigned to users who are members of **at least one** of the selected groups. This option becomes available only when two or more groups are specified.

Rules for group and logic compatibility:

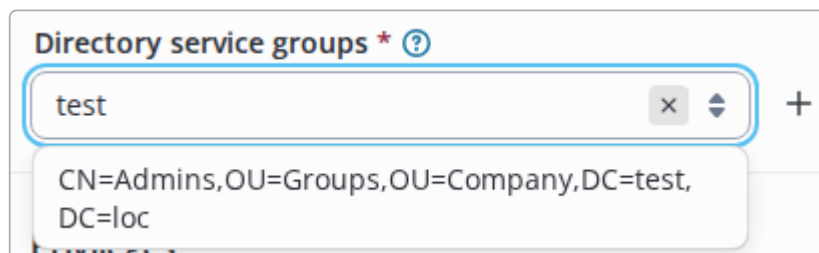
- Creating two or more roles with the same set of groups and the *same* logic is prohibited.
- Groups already used in any role with the «OR» logic cannot be reused in another role with the «OR» logic.
- Creating roles with the same set of groups but *different* logic («AND» and «OR») is allowed, **except when the set consists of a single group**:
 - A group that is the **only** group in a role with the «AND» logic cannot be used in a role with the «OR» logic.
 - A group already used **in any role with the «OR» logic** cannot be used as the **only** group in a role with the «AND» logic.

- **Directory service groups *** — groups that were added when setting up the corresponding external source (the “Groups” tab) are available for selection.



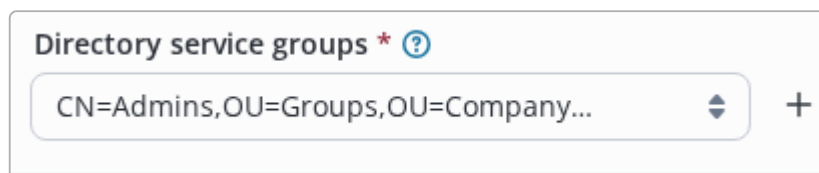
A screenshot of a user interface element titled "Directory service groups * ?". Below the title is a search input field with the placeholder text "Search". To the right of the search field is a small downward-pointing arrow icon and a plus sign icon.

To see a list of groups from an external source, it is needed to click on the "Search" field and select the desired value in the drop-down list.



A screenshot of the same "Directory service groups * ?" search field. The search input now contains the text "test". A dropdown menu is open below the search field, displaying a list of group names. The first visible group name is "CN=Admins,OU=Groups,OU=Company,DC=test,DC=loc". There is a small 'x' icon to the right of the search input and a plus sign icon to the right of the dropdown menu.

It is possible to filter groups selecting from an external source. Filtering is register-independent, displays all groups that have fallen under the filter.



A screenshot of the "Directory service groups * ?" search field. The search input now contains the text "CN=Admins,OU=Groups,OU=Company...". There is a small downward-pointing arrow icon to the right of the search input and a plus sign icon to the right of the search field.

It is necessary to add at least one group.

- **Privileges *** — access rights configuration table. You must select a level for at least one privilege.



* — required fields.



You cannot create a role with higher privileges than the current user.

To create a role, click the "Add" button.

Conditions for obtaining an external role

- The role must have status  **Available**. Roles with status  **Not available** are not assigned.
- The external source associated with the role must be **available** and correctly configured.
 - The user must satisfy the condition defined in the role settings:
 - with the «AND» logic — be a member of **all** groups listed in the role settings;
 - with the «OR» logic — be a member of **at least one** of the specified groups.



Role assignment is checked and recalculated **with each user login** based on the current group composition.

Role Selection in Case of Multiple Matches

If a user meets the conditions of several external roles, the assignment is performed according to the following algorithm:

1. AND priority over OR

Roles with AND logic are considered first. If at least one matching AND role is found, roles with OR logic are not considered.

2. Selection among AND roles

From all matching AND roles, the one that requires the largest number of groups is selected. If several roles have the same number of groups, priority is given to the role created earlier (with the smaller identifier).

3. Selection among OR roles

If there are no matching AND roles, the system checks matching OR roles. If several OR roles match, priority is given to the role created earlier (with the smaller identifier).

Editing a role

To edit a role, click on the role name in the table on the list page.

<input type="checkbox"/>	Status	Role ↑
<input type="checkbox"/>	⊗ Not available	AD_Operators ⚠
<input type="checkbox"/>	✓ Available	Guest Admin 🔒
<input type="checkbox"/>	✓ Available	Guest Operator 🔒
<input type="checkbox"/>	✓ Available	Hardware Admin 🔒
<input type="checkbox"/>	✓ Available	Monitor 🔒
<input type="checkbox"/>	✓ Available	Network Admin 🔒
<input type="checkbox"/>	✓ Available	read
<input type="checkbox"/>	✓ Available	Super Admin 🔒
<input type="checkbox"/>	✓ Available	System Admin 🔒

Figure 103. Hyperlink to role editing page

This will open the role editing page, similar to the addition page.



Changing the role type is prohibited if the role is assigned to at least one system user.

Editing an internal role

Users and devices > System users > Roles > Radius policy

← Radius policy

⚠ When changing the privileges of a role, the sessions of users with this role will be interrupted - re-authorization will be required

Role *

Radius policy

Description

Role type

internal
 external

Privileges *

Before setting up privileges, carefully read the list of sections included in the privileges

Privilege	Reading	Creation	Editing	Deletion
RADIUS policies ⚠	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
RADIUS monitoring	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Endpoints	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Network resources ⓘ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TACACS+ policies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TACACS+ monitoring	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Profiling ⓘ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Roles and accounts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Guest access ⓘ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Guest users	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Enterprise users	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System settings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
External sources	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Notification services ⓘ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Cancel Save

Figure 104. Internal role editing form



After saving changes to **role privileges**, all active sessions of users with this role will be terminated — re-authentication will be required.

After editing, click the "Save" button. The button becomes active when changes are present.

The "Cancel" button resets the changes made to their original state.

Editing an external role

Users and devices > System users > Roles > AD_Operators

← AD_Operators

When changing the privileges of a role, the sessions of users with this role will be interrupted - re-authentication will be required

Role *

AD_Operators

Description

Enter description

0 / 200

Role type

Internal

external

Access source

MS AD

To assign a role need

be in all specified groups (AND)

be in at least one of groups (OR)

Directory service groups *

CN=Admins,OU=Groups,OU=Company... +

Privileges *

Before setting up privileges, carefully read the list of sections included in the privileges

Privilege	<input checked="" type="checkbox"/> Reading	<input checked="" type="checkbox"/> Creation	<input checked="" type="checkbox"/> Editing	<input type="checkbox"/> Deletion
RADIUS policies	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
RADIUS monitoring	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Endpoints	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Network resources	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TACACS+ policies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TACACS+ monitoring	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Profiling	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Roles and accounts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Guest access	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Guest users	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Enterprise users	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System settings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
External sources	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Notification services	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Cancel Save

Figure 105. External role editing form



After saving changes to **role privileges** or **external source group composition**, all active sessions of users with this role will be immediately terminated — re-authentication will be required.

After editing, click the "Save" button. The button becomes active when changes are present.

The "Cancel" button resets the changes made to their original state.

Deleting roles

To delete, select the checkbox to the left of the roles to be deleted and click on the action panel above the table.



You cannot delete a role that is assigned to a system user.

Status	Role	Type	Description
Not available	AD_Operators	External	
Available	Guest Admin	Internal	System role for guest network administrator
Available	Guest Operator	Internal	System role for guest network operator
Available	Hardware Admin	Internal	System role for hardware access administrator
Available	Monitor	Internal	System role for monitoring only with read-only privileges
Available	Network Admin	Internal	System role for network access administrator
Available	read	Internal	
Available	Super Admin	Internal	System role with privileges for all pages and actions
Available	System Admin	Internal	System role for system administrator

Figure 106. Selecting roles in table for deletion



Deleting items requires confirmation in the modal window. The selected items will be deleted only after explicit confirmation of the operation.

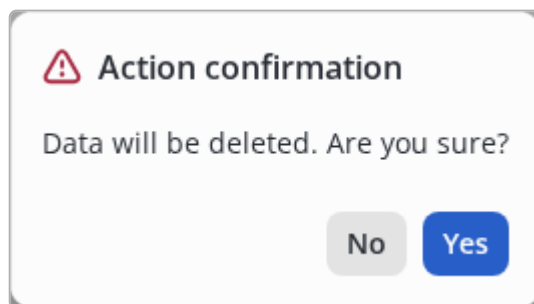


Figure 107. Modal dialog for confirmation

Specifics when changing an external source

When changing the system login configuration ([System Log In](#) section), all external roles associated with the **old source** automatically change to status **Not available**.



Figure 108. Warning about source change

Changing the primary authentication source

When switching from one external source to another (for example, from MS Active Directory to OpenLDAP), the unavailable external role form looks as follows:

Figure 109. Unavailable external role editing form (Source Change)

- The **Authentication source** is automatically populated with the **current source** (the current main source from the login settings).
- Previously selected groups are highlighted as outdated.



Duplicating a role allows you to quickly create its copy with the current source. Groups from the old source are not transferred.

Disabling the use of an external source

When disabling the use of an external source (unchecking the "Use external identity source as the main authentication source" checkbox), the unavailable external role form looks as follows:

Users and devices > System users > Roles > AD_Operators

← AD_Operators

External login disabled - this role can no longer be granted

Role *

AD_Operators

Description

Enter description

0 / 200

Role type ⚠

internal

external

Access source

MS AD

To assign a role need

be in all specified groups (AND)

be in at least one of groups (OR)

Directory service groups * ⓘ

CN=Admins,OU=Groups,OU=Company...

Privileges *

Before setting up privileges, carefully read the list of sections included in the privileges

Privilege	Reading	Creation	Editing	Deletion
RADIUS policies	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
RADIUS monitoring	<input type="checkbox"/>	—	—	—
Endpoints	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Network resources ⓘ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TACACS+ policies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TACACS+ monitoring	<input type="checkbox"/>	—	—	—
Profiling ⓘ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Roles and accounts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Guest access ⓘ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Guest users	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Cancel Save

Figure 110. Unavailable external role editing form (External login disabled)

- In the **Role type** block, the "external" option is disabled — only the "internal" type can be selected.
- Blocks related to external authentication (**Authentication source** and **Groups from directory service**) are not available for editing.



Duplicating an unavailable external role requires changing the role type to "internal".

Specifics When Changing License Level

License Upgrade

After upgrading the license level, additional configuration of privileges may be required. Roles that require additional configuration are marked with a warning:

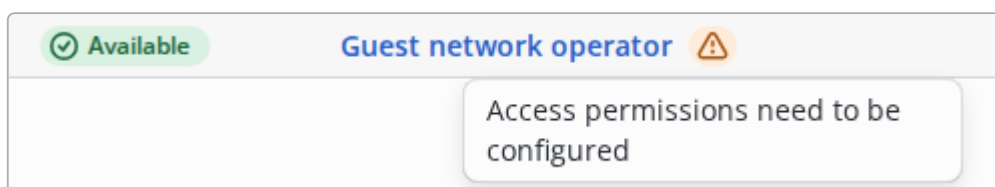


Figure 111. Warning about need for role reconfiguration

Users with such roles will see a system notification in the interface:


 Role need to be configured

Figure 112. Notification in navigation menu "Role Configuration Required"

License Downgrade

When editing a role that has privileges not included in the current license, the rights to these privileges will be reset after confirmation of saving:

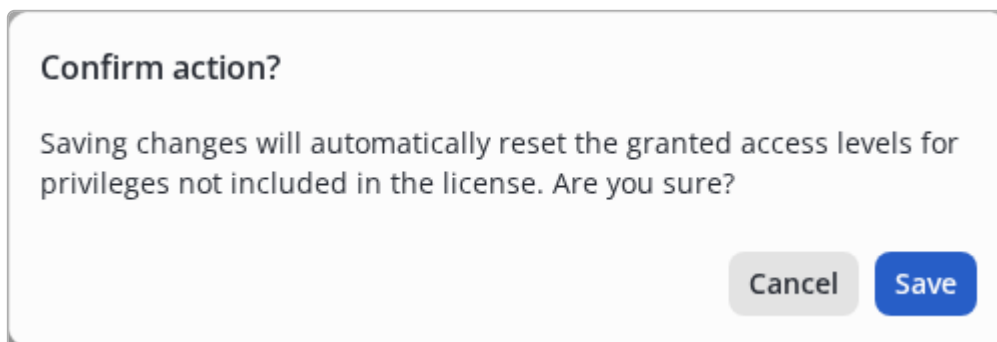


Figure 113. Confirmation of saving changes

Network resources

Network device (authenticator, NAS - Network Access Server) - 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 "Users and devices" → "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 and TACACS+ protocols.

Devices

Description

Network device (authenticator, NAS - Network Access Server) - 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

Name	IPv4	Profile	Protocols	Location	Device type	Description
Renoir	10.25.96.105	Eltex MES	RADIUS TACACS+	Building 1 < All Locations	Eltex < All Device Types	
Samsung_Catharine_430	63.238.75.65	Eltex MES	RADIUS TACACS+	Building 1 < All Locations	Eltex < All Device Types	


Figure 114. 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. It is a hyperlink to the page for viewing/editing the settings of this device profile.
- **Protocols** — shows the configuration status of the RADIUS and TACACS protocols.
 - **Gray** status - the protocol is disabled in the selected profile;
 - **Red** status - the protocol is enabled in the selected profile, but the secret is not specified in the device settings.;
 - **Green** status - the protocol is enabled in the selected profile, the secret is specified in the device settings.
- **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.








When you hover over the line with the profile you are interested in, a hint appears  when you click on it, you can view the settings for this profile.

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:

-  — Add a new element.
-  — Delete selected elements (inactive until at least one element is selected).

-  — Refresh table data.
-  — Allows you to download data from a csv file.
-  — Allows you to upload data to a csv file.
- — Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).
-  — Change the current sort order.
-  Search — Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.



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 .

The screenshot shows a web interface for adding a network device. The breadcrumb trail is 'Users and devices > Network resources > Devices > Adding'. The form has a left sidebar with navigation icons. The main form area contains the following sections:

- Name ***: Text input field with placeholder 'Enter name'.
- Profile ***: Dropdown menu with 'Select profile'.
- Model**: Text input field with placeholder 'Enter model'.
- Address type**: Dropdown menu with 'IPv4 address' selected.
- Value ***: Text input field with '0.0.0.0'.
- Description**: Text area with placeholder 'Enter description text' and a character count '0 / 200'.
- Network device groups**:
 - All Device Types ***: Dropdown menu with 'All Device Types'.
 - All Locations ***: Dropdown menu with 'All Locations'.
- RADIUS authentication settings**:
 - Secret key**: Text input field with placeholder 'Enter text'.
- TACACS+ authentication settings**:
 - Secret key**: Text input field with placeholder 'Enter text'.

At the bottom right, there are 'Cancel' and 'Add' buttons.

Figure 115. 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. It is a required field if the RADIUS protocol is enabled in the selected profile. Length from 1 to 200 characters.

TACACS+ TACACS+ authentication settings contains:

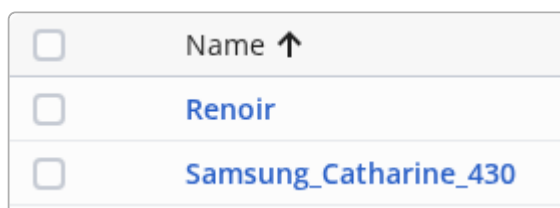
- Secret key for interaction with a network device using the TACACS+ protocol. Length from 0 to 64 characters.

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.



<input type="checkbox"/>	Name ↑
<input type="checkbox"/>	Renoir
<input type="checkbox"/>	Samsung_Catharine_430

Figure 116. Hyperlink to the device editing page

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

Figure 117. 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 is hidden until at least one change is made.

The **"Cancel"** button resets the changes made to their original state.

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.

Name	IPv4	Profile	Protocols	Location	Device type	Description
<input checked="" type="checkbox"/> Renoir	10.25.96.105	Eltex MES	RADIUS TACACS+	Building 1 < All Locations	Eltex < All Device Types	
<input type="checkbox"/> Samsung_Catharine_430	63.238.75.65	Eltex MES	RADIUS TACACS+	Building 1 < All Locations	Eltex < All Device Types	

Figure 118. Selecting a device in the table to delete



Deleting items requires confirmation in the modal window.
The selected items will be deleted only after explicit confirmation of the operation.

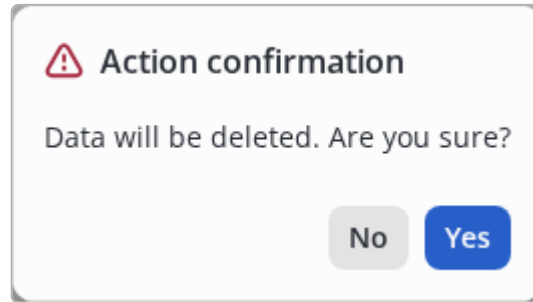


Figure 119. Modal dialog for confirmation

Import

NAICE supports importing data from CSV files.

Preliminary preparation before Import

1. Create or verify the existence of necessary related entities (e.g., device profile).
2. Review the CSV file requirements:
 - Encoding must be UTF-8;
 - Delimiters:
 - Field delimiter: comma (,)
 - String/text delimiter: double quotation mark (")
 - Headers and values must be enclosed in double quotation marks (")
 - Maximum file size is 2MB.
3. Check the file content for extraneous quotation marks before importing;
4. Check that the values containing the double quotation mark (") or the slash (/) are correctly escaped.
 - Values containing a double quotation mark (") are escaped using \"
 - Values containing the slash (/) are escaped using \"

Correct spelling of values (with escaping using `\`) using the example of the contents of the file for importing the TACACS Command set

"name:Required"	"description"	"permit_unmatched(true/false)"	"commands(Grant/command/arguments/enabled;...)"
"command_set"	"Test command set"	"false"	"PERMIT/\\"show/vlan 1 2 \"/true"


Incorrect spelling of values (without escaping) using the example of the contents of the file for importing the TACACS Command set

"name:Required"	"description"	"permit_unmatched(true/false)"	"commands(Grant/command/arguments/enabled;...)"
"command_set"	"Test command set"	"false"	"PERMIT/show/vlan 1 2 /true"



Failure to escape these characters will lead to incorrect data recognition.

Import procedure


To import data from a CSV file, click on  in the action panel located above the table. This will open the import window:

Import

When importing, duplicate data will not be overwritten or edited - the system will skip it. If you want to change old data, delete it from the system manually before importing.

Carefully review the [Documentation](#) to ensure the import completes without errors.

Select a file*
Max file size 2MB

 **Upload** or drag it here

Field is required

Data source *

NAICE

Ignore exist data (i)
 Stop import on first error
 Automatically create missing records (i)

Cancel
Import

Figure 120. Window Import

Data import proceeds through several steps:

1. Select the required CSV file by dragging it into the upload area or by selecting it through the file explorer by clicking the "**Upload**";



To apply changes, you must re-upload an updated CSV file.

2. Select the data source (if not predefined);
3. Configure import flags (if needed):

Ignore exist data

- On: Duplicate records trigger warnings.
- Off: Duplicates are treated as errors.

Stop import on first error

- On: Import halts at the first error. Only records that were successfully processed before it occurred will be imported.

- Off: Erroneous lines are skipped, and the import continues to the end. Only valid records will be imported.

Stop import on first error

- On: When importing, missing records will be filled in automatically. The list of auto-completed entries can be found by hovering over the tooltip to the right of the switch.
- Off: All required fields must be filled in manually.

4. To start the import, click the "**Import**".



When importing, duplicate data will not be overwritten or edited - the system will skip it. If you want to change old data, delete it from the system manually before importing.

Viewing the Import report

An import report window opens immediately after file processing.

If all records in the file were processed correctly, you will see the following window:

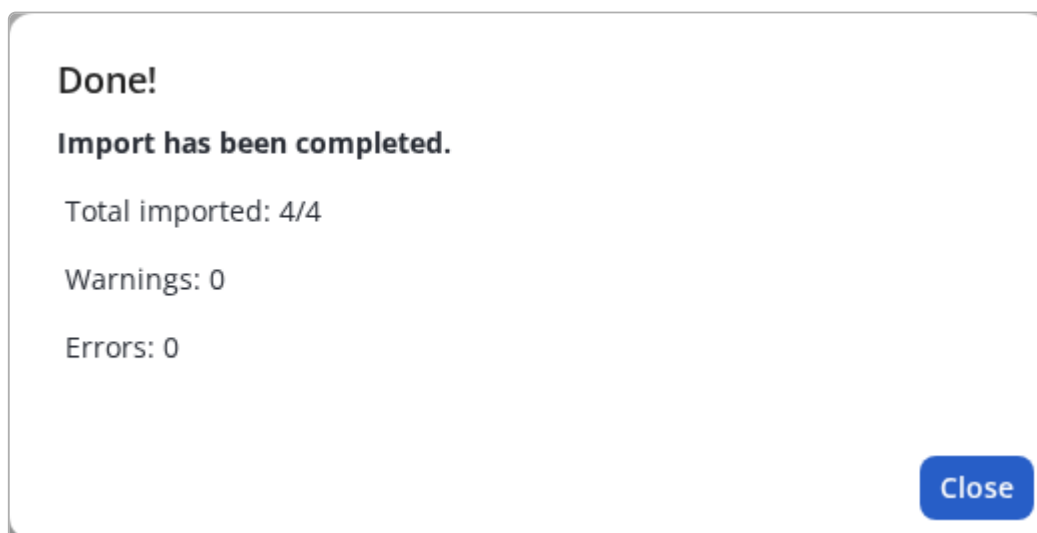


Figure 121. Window Import report (all entries were processed correctly)

The summary block contains:

- **Total Imported** - Counter of records imported (vs. total rows processed);
- **Warnings** - Number of warnings that occurred;
- **Errors** - Number of errors that occurred.

If not all records were processed correctly, you will see the following window:

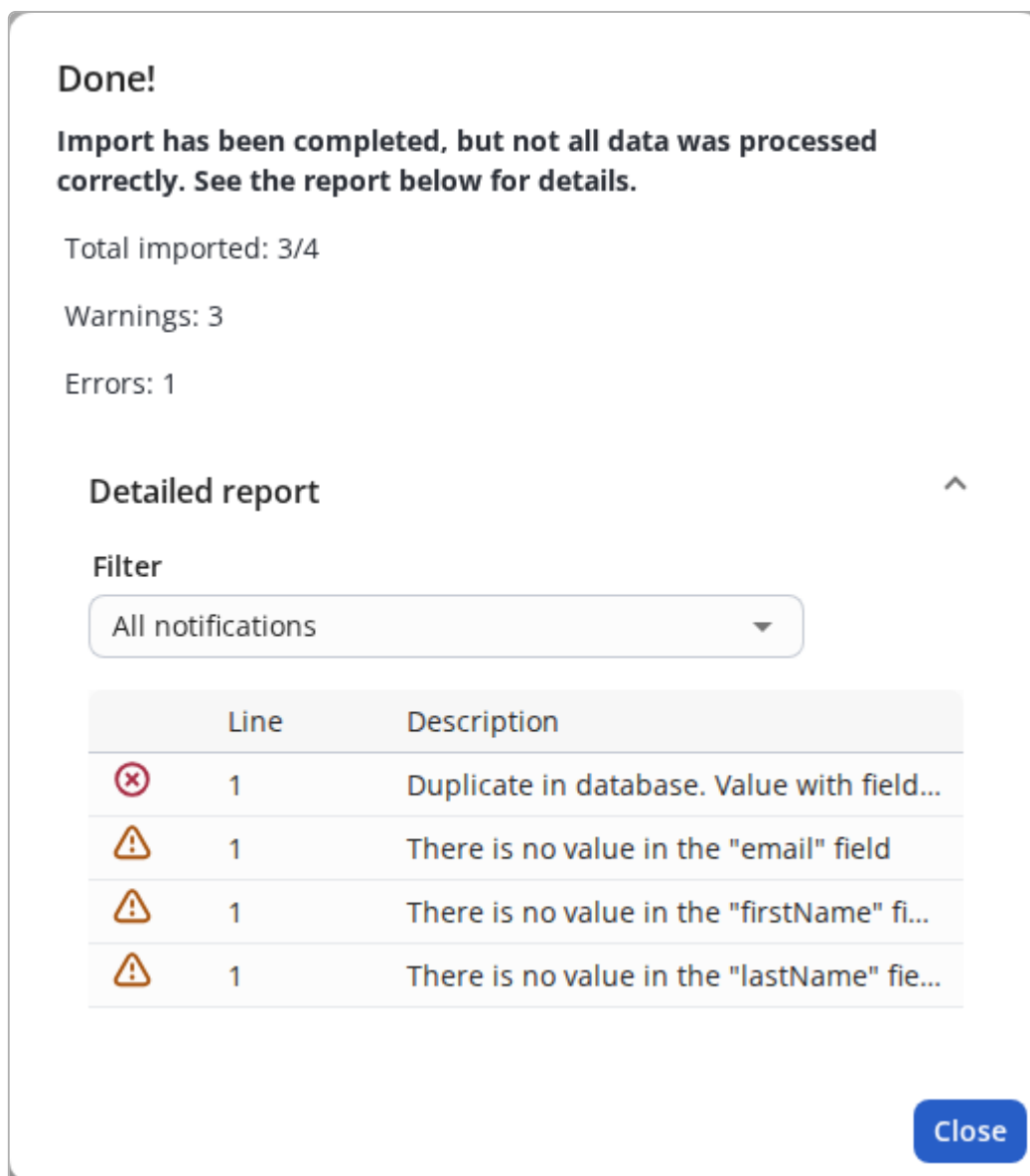


Figure 122. Window Import report (entries processed with errors/warnings)

Detailed report contains the following information:

- **Filter** - Dropdown list allowing you to select which notifications to display (All notifications , Only errors , or Only warnings)

The notification table contains columns:

- **Line** - The line number in the CSV file where an error or warning was detected;
- **Description** - Detailed text explanation of the error or warning.



Hover your cursor over a row in the Description column to view the full error/warning message in a tooltip.

Import particularities for Devices



For Network devices imports, only the **NAICE** data source is supported.

The table below lists the fields, their requirements, descriptions, and requirements:

Field	Description	Requirements
name:Required	Name of the network device	Required Must be unique Maximum length - 100 characters
description	Free-form description of the device	Maximum length - 200 characters
ip_address:Required	IP address of the device (IPv4)	Required Must be unique Format: four numbers 0-255 , separated by dots
model_name	Model of the network device	Maximum length - 100 characters
network_device_profile:Required	Network device profile	Required Profile must exist in the system
network_device_groups	Groups to which the device will belong (full path specified)	Groups must exist in the system Format: group#subgroup Path separator: ;
radius_secret	RADIUS secret key	Required when RADIUS is enabled in the profile Length: 1-200 characters Spaces are not allowed
tacacs_secret	TACACS+ secret key	Maximum length - 64 characters Spaces are not allowed



If no groups are specified for the device in `network_device_groups` or groups are not found, root groups will be assigned to it.

Example of correctly formatted file content

"name:Required"	"description"	"ip_address:Required"	"model_name"	"network_device_profile:Required"	"network_device_groups"	"radius_secret"	"tacacs_secret"
"MES"	""	"10.25.96.105"	"MES2324P"	"Eltex MES"	"All Locations#Building 1;All Device Types#Eltex"	"secret123"	"secret123"

Instructions for obtaining a CSV template file are described later in the "**Export**" section.

Export

NAICE supports exporting data in CSV format. Values and headings are framed by double quotes, the field separator is comma (,).

Export procedure

Two export modes are available:

- **Export all** - Exports all records from the current section. System entities are not included during export.
- **Export selected** - Exports only checked records.

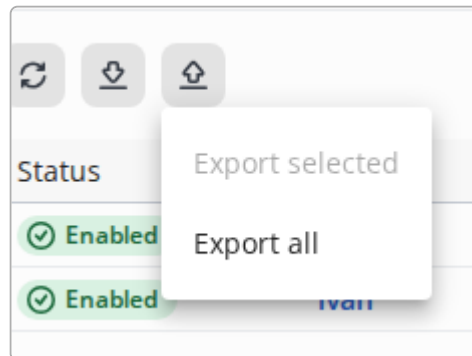



Figure 123. Window export menu



Values containing double quotation marks (") or slashes (/) will be escaped using \".

Export all

On the action panel above the table, click  and select the "**Export all**" mode. In the window that opens, confirm the action by clicking the "**Export**":

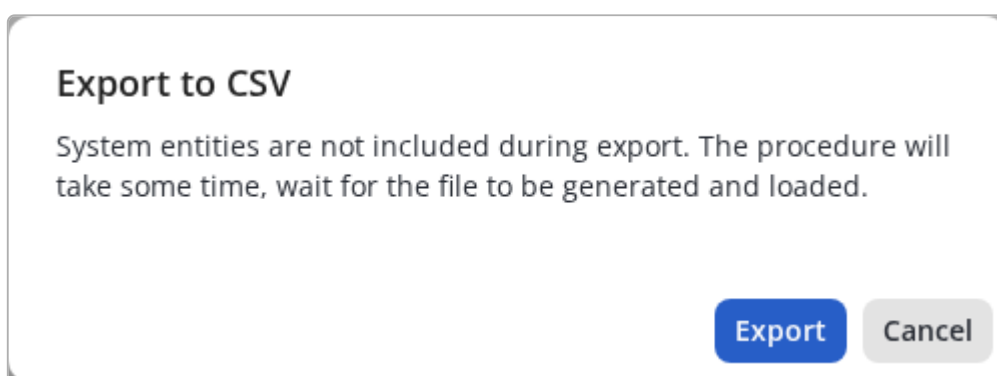



Figure 124. Export all

After clicking the "**Export**", a file containing all records from the current section will be downloaded to your device.

Export selected

On the action panel above the table, click  and select the "**Export selected**" mode. In the window that opens, confirm the action by clicking the "**Export**":

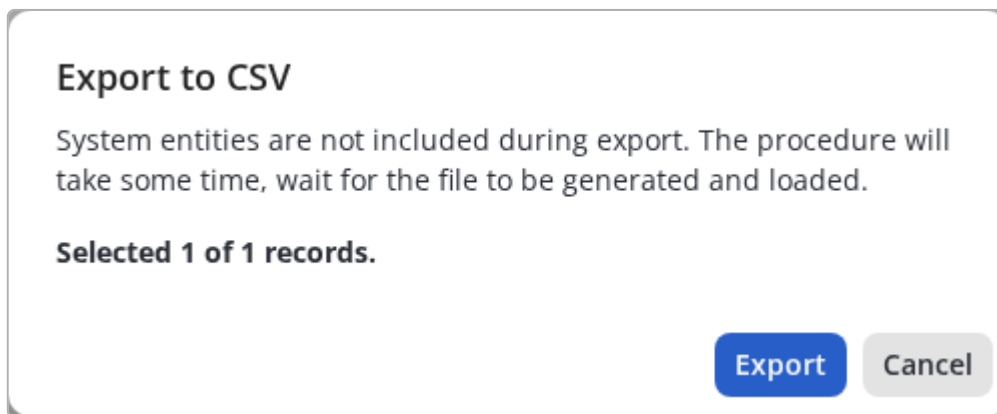


Figure 125. Export selected

After clicking the "**Export**", a file containing only the checked records will be downloaded to your device.



When **opening** CSV files, always use a **comma (,)** as the field delimiter. **Double quotation marks (")** or **empty values** may be used as string/text delimiters.

When **saving** CSV files, always use a **comma (,)** as the field delimiter, with an **empty value** as the string/text delimiter.



If a double quotation mark (") was used as the line delimiter when opening the file, values containing double quotation marks (") or slashes (/), escaped as "\", may receive an extra quotation mark (") upon saving. Please check the file in a text editor and remove any extra quotation marks if they appear.

Template

If there are no records in the table (or only system entities are present), selecting the "**Export all**" mode will generate a CSV file containing only the column headers. This file can be used as a **template** for preparing data prior to import.

Export particularities for Devices



The full path to the subgroup that includes the device will be specified using the separator - #. Each individual path to a group will be separated using - ; .

The structure of the CSV file for network devices is described in the section "[Import particularities for Devices](#)".

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 [RADIUS policies](#) or [Network devices policies](#).

View groups

This page contains a table listing all groups.

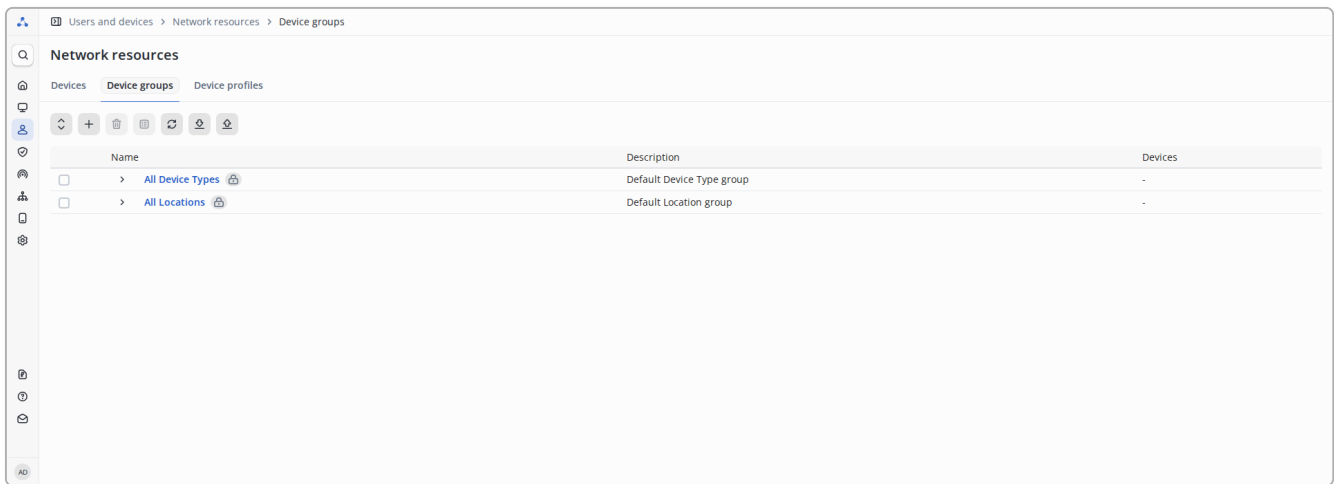


Figure 126. Group list view page

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 system user 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
 - — This entity is system and cannot be deleted or edited.
- **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.
- — Add a new element.
- — Delete selected elements (inactive until at least one element is selected).
- — Show devices of the group and its subgroups (inactive until the group is selected).
- — Refresh table data.
- — Allows you to download data from a csv file.
- — Allows you to upload data to a csv file.
- — 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.

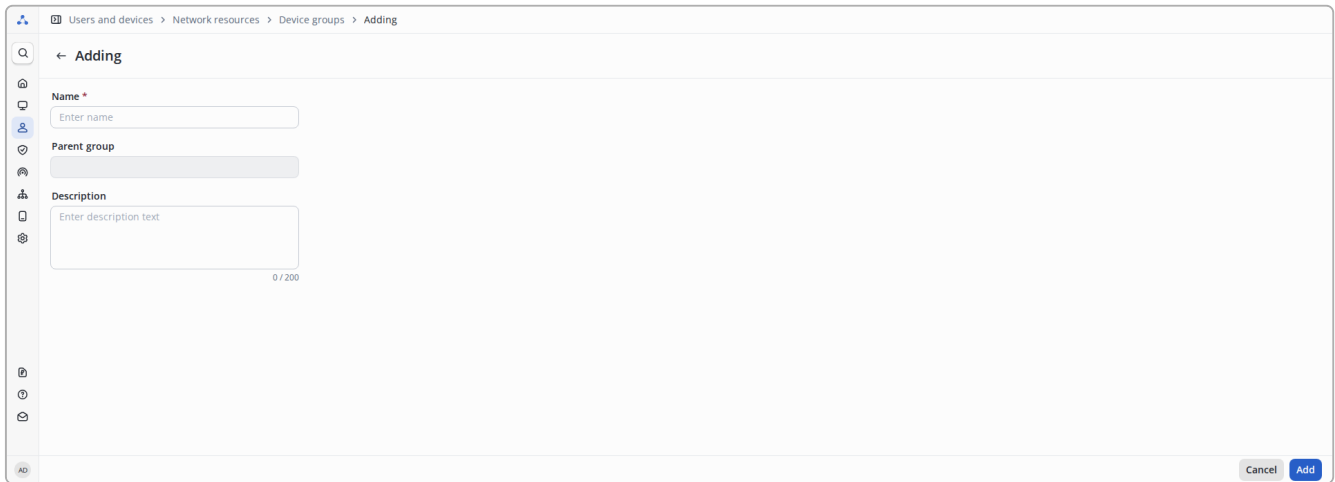


Figure 127. Page of add group

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 .

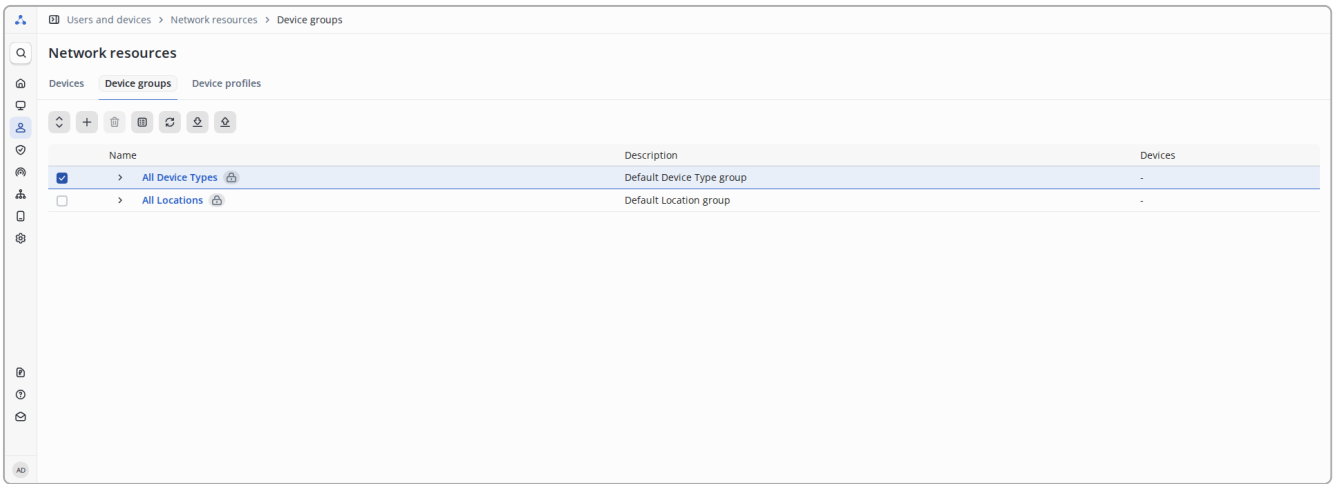


Figure 128. Page with selecting a root group to add a child group

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

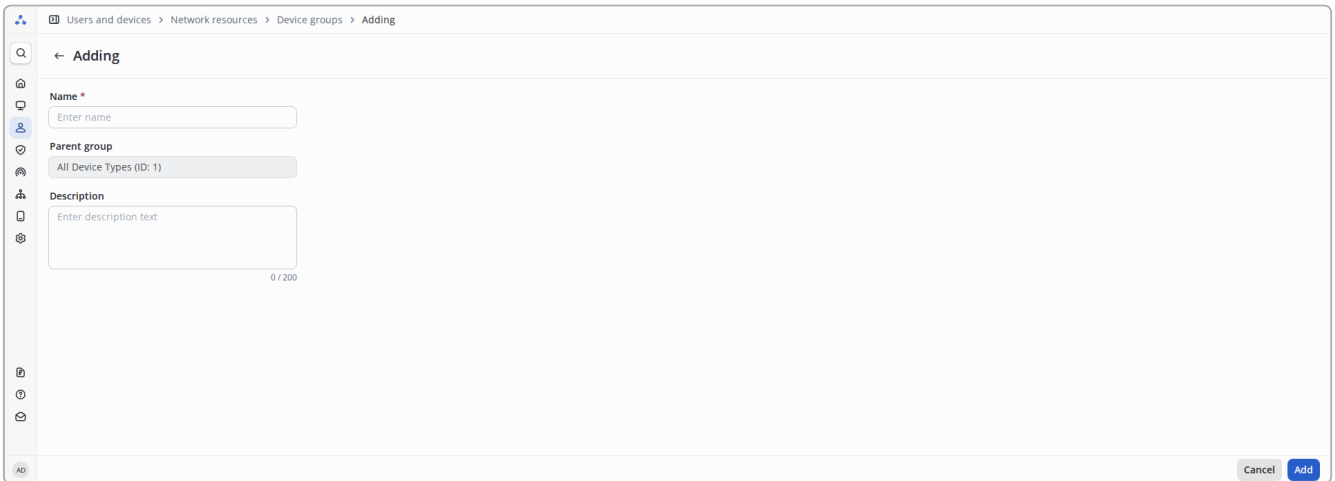


Figure 129. Page of added subgroup

Group editing

To edit a group, click on its name.

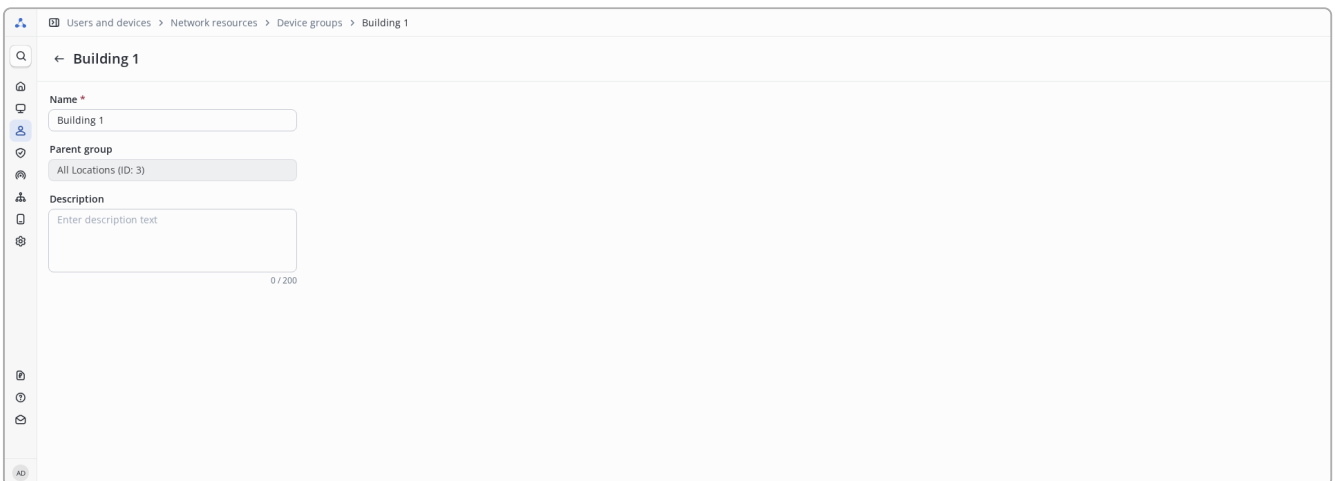


Figure 130. Group edit page


After editing, click the **"Save"** button. The button is hidden until at least one change is made.

The **"Cancel"** button resets the changes made to their original state.



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.

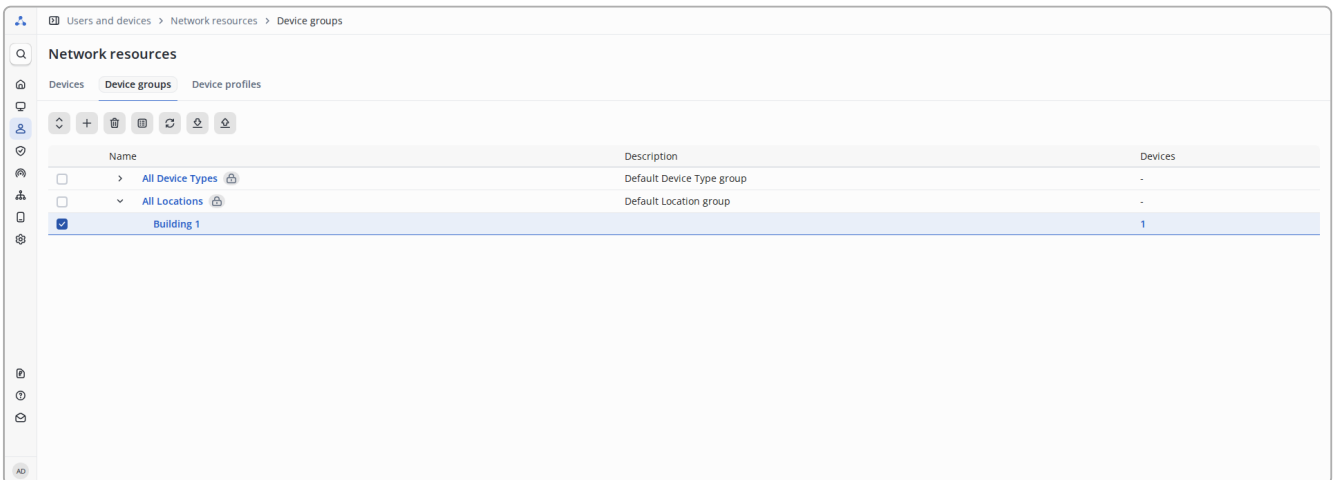


Figure 131. Page with a selected group for deletion



Deleting items requires confirmation in the modal window. The selected items will be deleted only after explicit confirmation of the operation.

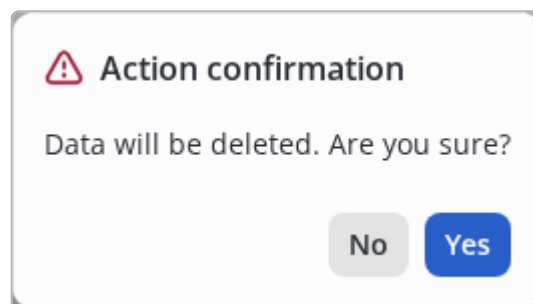


Figure 132. Modal dialog for confirmation


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.

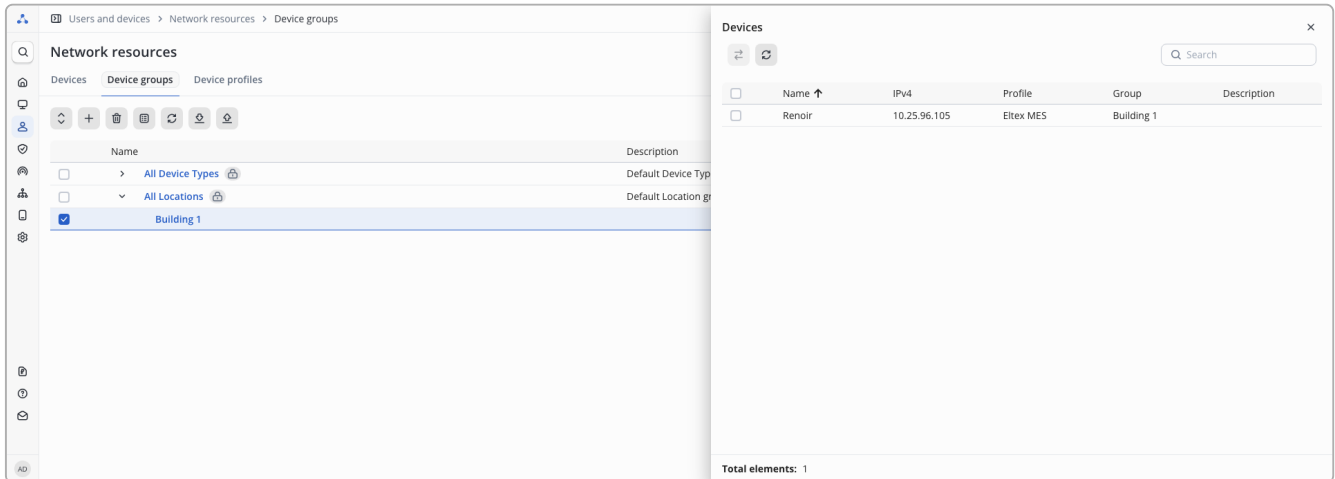






Figure 133. Panel for viewing devices in a group

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. By default, sorting is performed in direct (alphabetical) order by the "Name" field.

Controls:

-  — move the devices selected by the checkbox to another group (inactive until at least one element is selected).
-  — refresh table data.
- **Search**  — performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.
- — checkbox, which is responsible for selecting network devices to perform further actions.
-  — change the current sort order.

Move a device to another group

To move devices to another group, in the device list window, mark the devices that need to be moved with a checkbox on the left. After clicking on the device move button , a window will open with the selection of a group to move *within the same root group*.

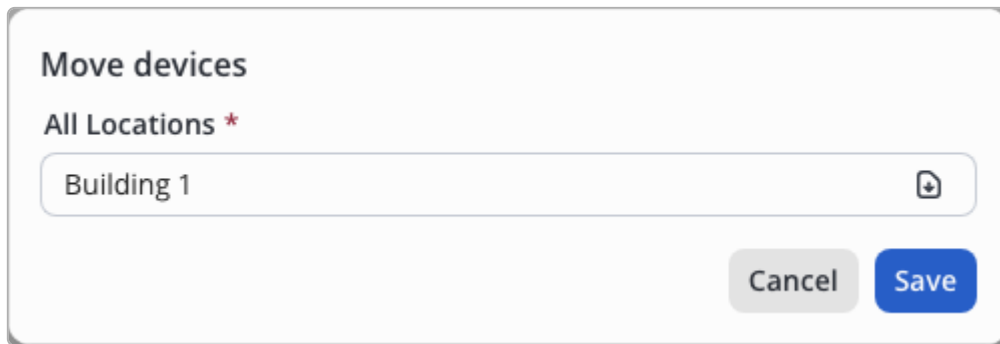


Figure 134. Panel for moving devices to a group

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

Import

NAICE supports importing data from CSV files.

Preliminary preparation before Import

1. Create or verify the existence of necessary related entities (e.g., device profile).
2. Review the CSV file requirements:
 - Encoding must be UTF-8;
 - Delimiters:
 - Field delimiter: comma (,)
 - String/text delimiter: double quotation mark (")
 - Headers and values must be enclosed in double quotation marks (")
 - Maximum file size is 2MB.
3. Check the file content for extraneous quotation marks before importing;
4. Check that the values containing the double quotation mark (") or the slash (/) are correctly escaped.
 - Values containing a double quotation mark (") are escaped using \"
 - Values containing the slash (/) are escaped using \"

Correct spelling of values (with escaping using `\`) using the example of the contents of the file for importing the TACACS Command set

"name:Required"	"description"	"permit_unmatched(true/false)"	"commands(Grant/command/arguments/enabled;...)"
"command_set"	"\\"Test command set\\""	"false"	"PERMIT/\\"show/vlan 1 2 \"/true"


Incorrect spelling of values (without escaping) using the example of the contents of the file for importing the TACACS Command set

"name:Required"	"description"	"permit_unmatched(true/false)"	"commands(Grant/command/arguments/enabled;...)"
"command_set"	"Test command set"	"false"	"PERMIT/show/vlan 1 2 /true"



Failure to escape these characters will lead to incorrect data recognition.

Import procedure


To import data from a CSV file, click on  in the action panel located above the table. This will open the import window:

Import

When importing, duplicate data will not be overwritten or edited - the system will skip it. If you want to change old data, delete it from the system manually before importing.

Carefully review the [Documentation](#) to ensure the import completes without errors.

Select a file*
Max file size 2MB

 Upload or drag it here

Field is required

Data source *

NAICE
▼

Ignore exist data (i)

Stop import on first error

Cancel
Import

Figure 135. Window Import

Data import proceeds through several steps:

1. Select the required CSV file by dragging it into the upload area or by selecting it through the file explorer by clicking the **"Upload"**;



To apply changes, you must re-upload an updated CSV file.

2. Select the data source (if not predefined);
3. Configure import flags (if needed):

Ignore exist data

- On: Duplicate records trigger warnings.
- Off: Duplicates are treated as errors.

Stop import on first error

- On: Import halts at the first error. Only records that were successfully processed before it occurred will be imported.
-

Off: Erroneous lines are skipped, and the import continues to the end. Only valid records will be imported.

4. To start the import, click the "**Import**".



When importing, duplicate data will not be overwritten or edited - the system will skip it. If you want to change old data, delete it from the system manually before importing.

Viewing the Import report

An import report window opens immediately after file processing.

If all records in the file were processed correctly, you will see the following window:

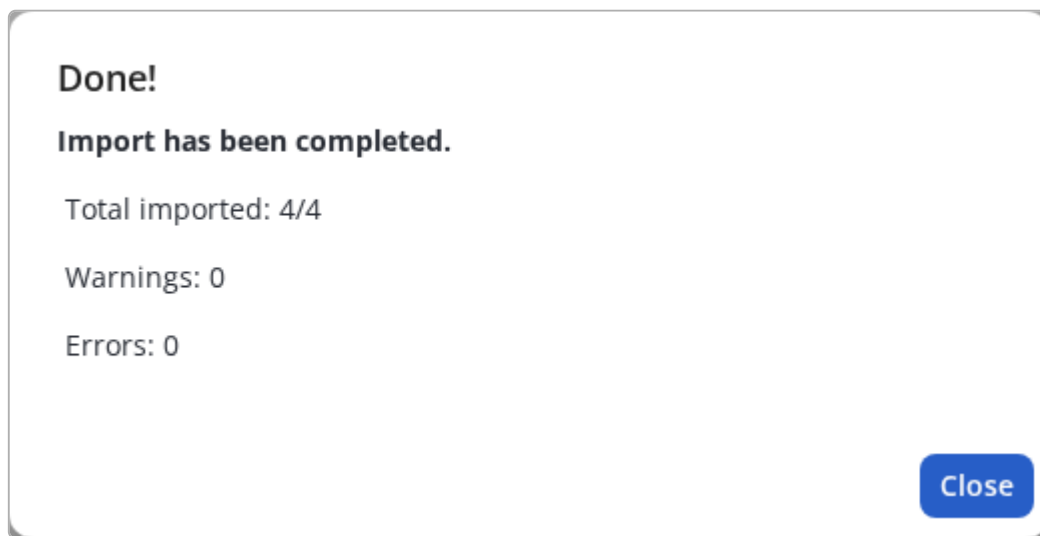


Figure 136. Window Import report (all entries were processed correctly)

The summary block contains:

- **Total Imported** - Counter of records imported (vs. total rows processed);
- **Warnings** - Number of warnings that occurred;
- **Errors** - Number of errors that occurred.

If not all records were processed correctly, you will see the following window:

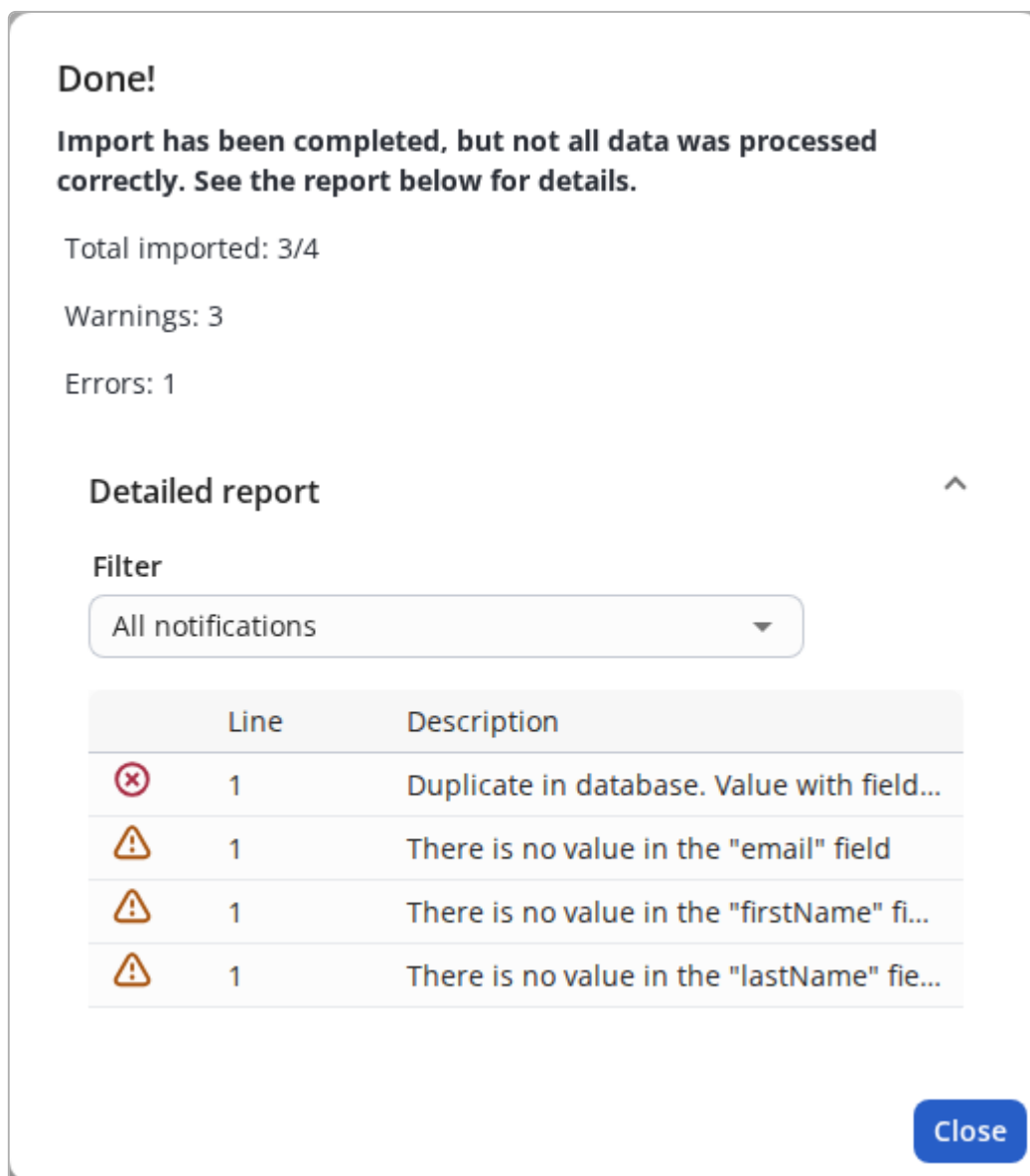


Figure 137. Window Import report (entries processed with errors/warnings)

Detailed report contains the following information:

- **Filter** - Dropdown list allowing you to select which notifications to display (All notifications , Only errors , or Only warnings)

The notification table contains columns:

- **Line** - The line number in the CSV file where an error or warning was detected;
- **Description** - Detailed text explanation of the error or warning.



Hover your cursor over a row in the Description column to view the full error/warning message in a tooltip.

Import particularities for Device groups



For Device groups imports, only the NAICE data source is supported.

The table below lists the fields, their requirements, descriptions, and requirements:

Field	Description	Requirements
name:Required	Name of the group (full path must be specified)	Required Format: group#subgroup
description	Free-form description of the group	Maximum length - 200 characters



If there is no intermediate root/child group in the system, it will be created automatically.

Example of correctly formatted file content:

"name:Required"	"description"
"All Device Types#Switch"	""

Instructions for obtaining a CSV template file are described later in the "**Export**" section.

Export

NAICE supports exporting data in CSV format. Values and headings are framed by double quotes, the field separator is comma (,).

Export procedure

Two export modes are available:

- **Export all** - Exports all records from the current section. System entities are not included during export.
- **Export selected** - Exports only checked records.

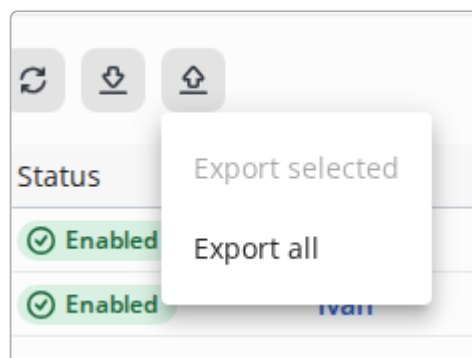



Figure 138. Window export menu



Values containing double quotation marks (") or slashes (/) will be escaped using \".

Export all

On the action panel above the table, click  and select the "**Export all**" mode. In the window that opens, confirm the action by clicking the "**Export**":

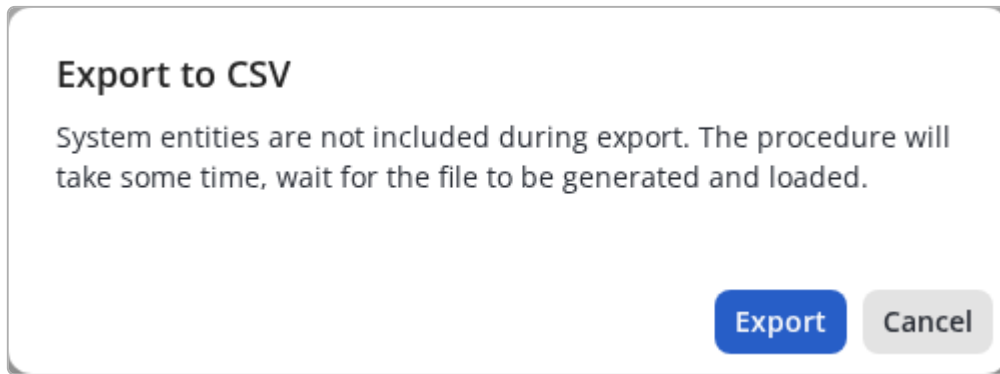



Figure 139. Export all

After clicking the "**Export**", a file containing all records from the current section will be downloaded to your device.

Export selected

On the action panel above the table, click  and select the "**Export selected**" mode. In the window that opens, confirm the action by clicking the "**Export**":

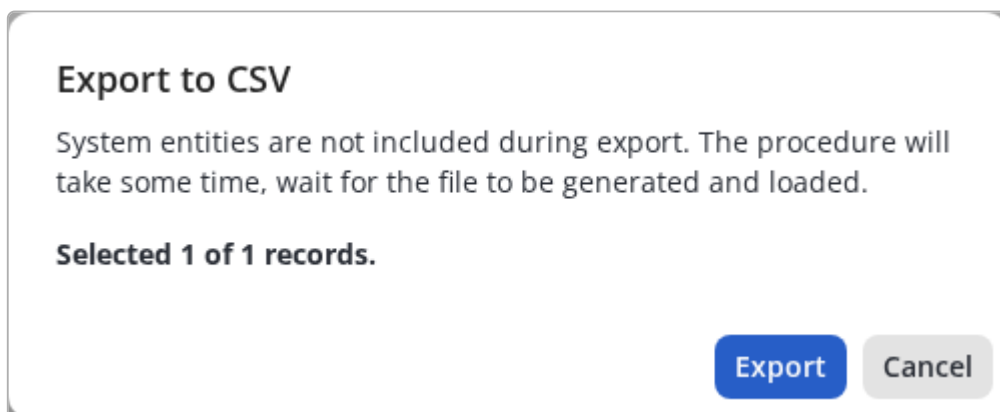


Figure 140. Export selected

After clicking the "**Export**", a file containing only the checked records will be downloaded to your device.



When **opening** CSV files, **always** use a **comma (,)** as the field delimiter. **Double quotation marks (")** or **empty values** may be used as string/text delimiters.

When **saving** CSV files, **always** use a **comma (,)** as the field delimiter, with an **empty value** as the string/text delimiter.



If a double quotation mark (") was used as the line delimiter when opening the file, values containing double quotation marks (") or slashes (/), escaped as \", may receive an extra quotation mark (") upon saving. Please check the file in a text editor and remove any extra quotation marks if they appear.

Template

If there are no records in the table (or only system entities are present), selecting the "**Export all**" mode will generate a CSV file containing only the column headers. This file can be used as a **template** for preparing data prior to import.

Export particularities for Device Groups



The name of the group will be specified in the format of the full path using the separator - # .

The structure of the CSV file for device groups is described in the section "[Import particularities for Device groups](#)".

Device profiles



Some functional described on this page are only available with an extended license. These features are marked with special labels in the form of colored icons next to the name.

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.
- *RADIUS CoA settings* - relevant if the device supports RADIUS CoA.
- **ADVANCED** *web redirection settings*.

View a list of device profiles

<input type="checkbox"/>	Name ↑	Protocols	Vendor	Description
<input type="checkbox"/>	AccessPoint - example	RADIUS TACACS+	Other	Example profile for wireless access points
<input type="checkbox"/>	ArubaWireless	RADIUS TACACS+	Aruba	Profile for Aruba wireless network access devices
<input type="checkbox"/>	BrocadeWired	RADIUS TACACS+	Brocade	Profile for Brocade switches

Figure 141. 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;
- **Protocols** — shows the configuration status of the RADIUS and TACACS protocols.
 - **Gray** status - the protocol is disabled in the profile.
 - **Green** status - the protocol is enabled in the profile.
- **Vendor** - the name of the device vendor;
- **Description** - arbitrary description of the profile.



When you hover over the line with the profile you are interested in, a hint appears ⓘ when you click on it, you can view the settings for this profile.

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

Controls:

- **+** — Add a new element.
- **📄** — Duplicate chosen element. Becomes active if only one element in the list is selected.
- **🗑️** — Delete selected elements (inactive until at least one element is selected).
- **🔄** — Refresh table data.
- — Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).
- **↑** — Change the current sort order.
- **🔍 Search** — Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.

Adding a device profile

Page for adding a device network profile

To add a device profile, click **+**.

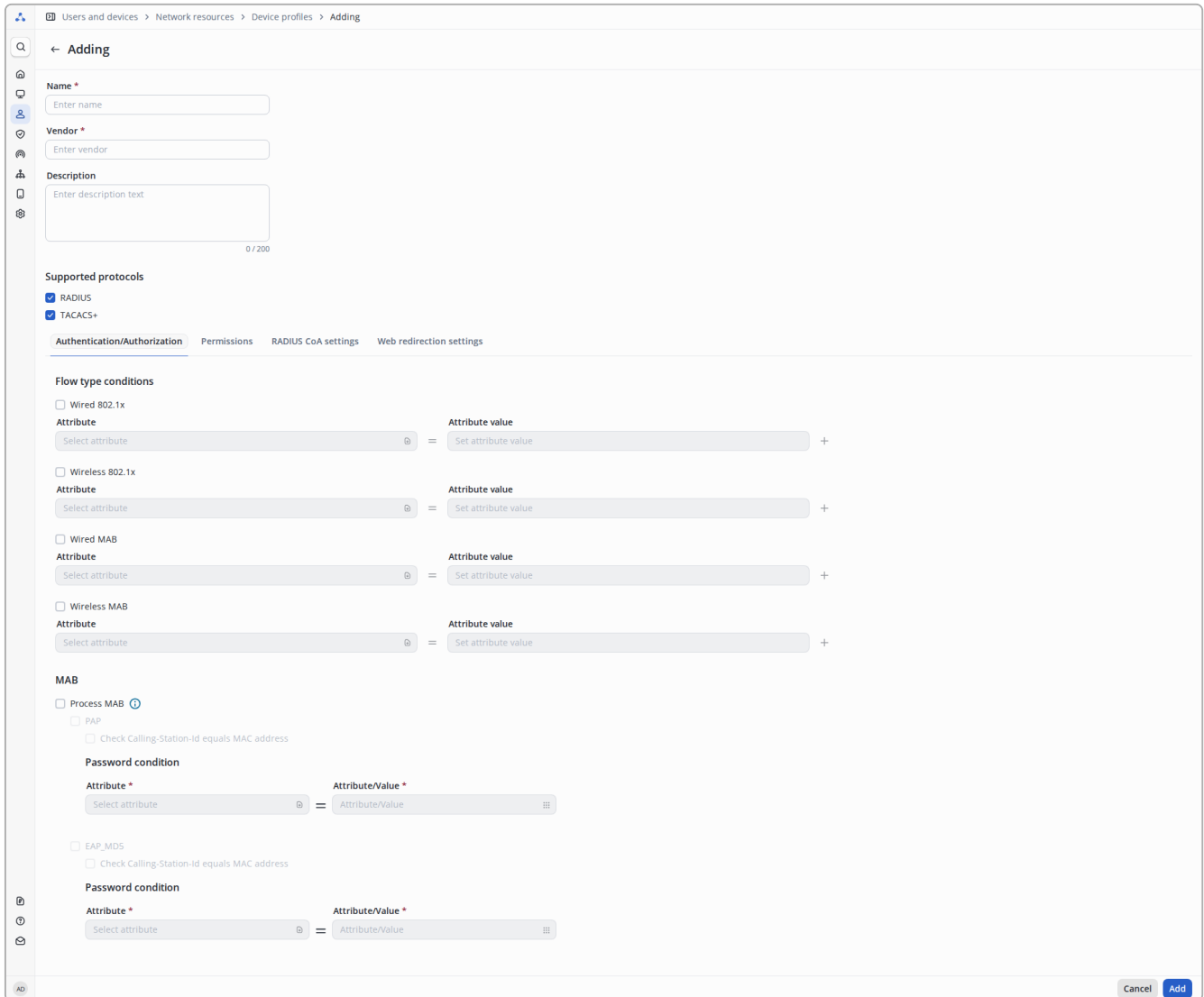


Figure 142. Page with filling device profile parameters. The Authentication/Authorization tab

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 protocols used to communicate with the network device. RADIUS and TACACS+ are 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.



ADVANCED Portal authorization requires **Wireless MAB** flow type detection to be enabled!

- **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.



When enabling the detection of any connection type, the attributes will be set to default values. You can edit them or leave them unchanged.



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.



ADVANCED Portal authorization requires MAB to be enabled and configured!

- **Process MAB** - enable MAB authorization permission on the device.
- **PAP / EAP_MD5** - enable MAB authorization permission for the specified protocols.
- **Check Calling-Station-Id and MAC address match** - Enables authorization only for devices whose RADIUS request's Calling-Station-Id attribute matches the MAC address in the username. Requires the specified attribute to be present in the device's RADIUS request.
- **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.

The screenshot shows a web interface for adding a device profile. The breadcrumb trail is 'Users and devices > Network resources > Device profiles > Adding'. The page title is '← Adding'. There are three input fields: 'Name *' (placeholder: Enter name), 'Vendor *' (placeholder: Enter vendor), and 'Description' (placeholder: Enter description text, with a 0/200 character count). Below these is the 'Supported protocols' section, where 'RADIUS' and 'TACACS+' are both checked. The 'Permissions' tab is active, showing 'Set VLAN' and 'Set ACL' as unchecked options. A 'Name *' dropdown menu is present with the placeholder 'Select attribute'. At the bottom right, there are 'Cancel' and 'Add' buttons.

Figure 143. Page with filling device profile parameters. The Permissions tab

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.

The screenshot shows a web interface for adding a device profile. The breadcrumb trail is 'Users and devices > Network resources > Device profiles > Adding'. The page title is '← Adding'. There are three input fields: 'Name *' (placeholder: Enter name), 'Vendor *' (placeholder: Enter vendor), and 'Description' (placeholder: Enter description text, with a 0/200 character count). Under 'Supported protocols', 'RADIUS' and 'TACACS+' are checked. Below this are four tabs: 'Authentication/Authorization', 'Permissions', 'RADIUS CoA settings' (selected), and 'Web redirection settings'. In the 'RADIUS CoA settings' tab, there is a checkbox 'Device supports RADIUS CoA'. Below it are three input fields: 'RADIUS CoA port *' (placeholder: Enter port), 'Timeout Interval, sec *' (placeholder: Enter interval), and 'Retry Count *' (placeholder: Enter count). There is also a checkbox 'Sending of attribute Message-Authenticator' with a help icon. The 'Reauthentication' section has a table with two columns: 'Attribute' and 'Attribute value'. The 'Attribute' column has a dropdown menu with 'Select attribute' and a search icon. The 'Attribute value' column has an input field with 'Set attribute value' and a plus sign. At the bottom right, there are 'Cancel' and 'Add' buttons.

Figure 144. Page with filling device profile parameters. The RADIUS CoA settings tab

RADIUS CoA settings - a settings block that allows you to configure RADIUS CoA for dynamic management of user sessions via the RADIUS server.

- **Device supports RADIUS CoA** - enables the RADIUS CoA setting.
 - **RADIUS CoA port *** - The port for sending RADIUS CoA. This must match the port configured on the network device (the manufacturer-set value can be 1700 or 3799). If CoA is enabled, the default value in NAICE will be 1700.
 - **Timeout Interval, sec *** - The number of seconds during which a response is expected after sending the CoA.
 - **Retry Count *** - count of attempts to send a request if there is no response.
- **Sending of attribute Message-Authenticator** - The option adds an attribute for checking the authenticity and integrity of CoA and Disconnect packets.



The attribute value is formed based on the RADIUS secret key specified in the device settings. The packet recipient checks this value using the secret key known to it. If the values do not match, the packet is discarded, preventing the processing of forged packets.

- **Reauthentication** is the settings block responsible for re-verifying user credentials without disconnecting the connection.
 - **Attribute** - RADIUS attribute used in the condition.
 - **Attribute value** - the value of the RADIUS attribute used in the condition.

Figure 145. Page with filling device profile parameters. The Web redirection settings tab

ADVANCED **Web redirection settings** - a settings block responsible for automatically redirecting users to the web portal.



For portal authorization to work, you must enable WirelessMAB connection type detection!

- **Set redirection** - enables configuration of web portal redirect link parameters.
 - **URL** - parameters for passing the Guest Portal authorization page redirect link in the RADIUS packet.
 - **Attribute *** - RADIUS attribute used in the condition.
 - **Attribute value *** - RADIUS attribute value used in the condition.
 - **ACL** - parameters for passing the ACL in the RADIUS packet that will be assigned when redirecting to the portal.
 - **Attribute *** - RADIUS attribute used in the condition.
 - **Attribute value *** - RADIUS attribute value used in the condition

Parameters marked with an asterisk * are required.

Users and devices > Network resources > Device profiles > Adding

← Adding

Name *
Huawei EY-886

Vendor *
Huawei

Description
Enter description text
0 / 200

Supported protocols
 RADIUS
 TACACS+

Authentication/Authorization | Permissions | RADIUS CoA settings | Web redirection settings

Flow type conditions

Wired 802.1x
Attribute: Select attribute = Set attribute value +

Wireless 802.1x
Attribute: Select attribute = Set attribute value +

Wired MAB
Attribute: Select attribute = Set attribute value +

Wireless MAB
Attribute: Select attribute = Set attribute value +

Cancel Add

Figure 146. Page with filling device profile parameters

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

Users and devices > Network resources > Device profiles

Network resources

Devices | Device groups | Device profiles

+ @ 🗑️ ↻ 🔍 Search

<input type="checkbox"/>	Name ↑	Protocols	Vendor	Description
<input type="checkbox"/>	AccessPoint - example	RADIUS TACACS+	Other	Example profile for wireless access points
<input type="checkbox"/>	ArubaWireless	RADIUS TACACS+	Aruba	Profile for Aruba wireless network access devices
<input type="checkbox"/>	BrocadeWired	RADIUS TACACS+	Brocade	Profile for Brocade switches
<input type="checkbox"/>	Huawei EY-886	RADIUS TACACS+	Huawei	

Profile has been added

Total elements: 4

Figure 147. 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.

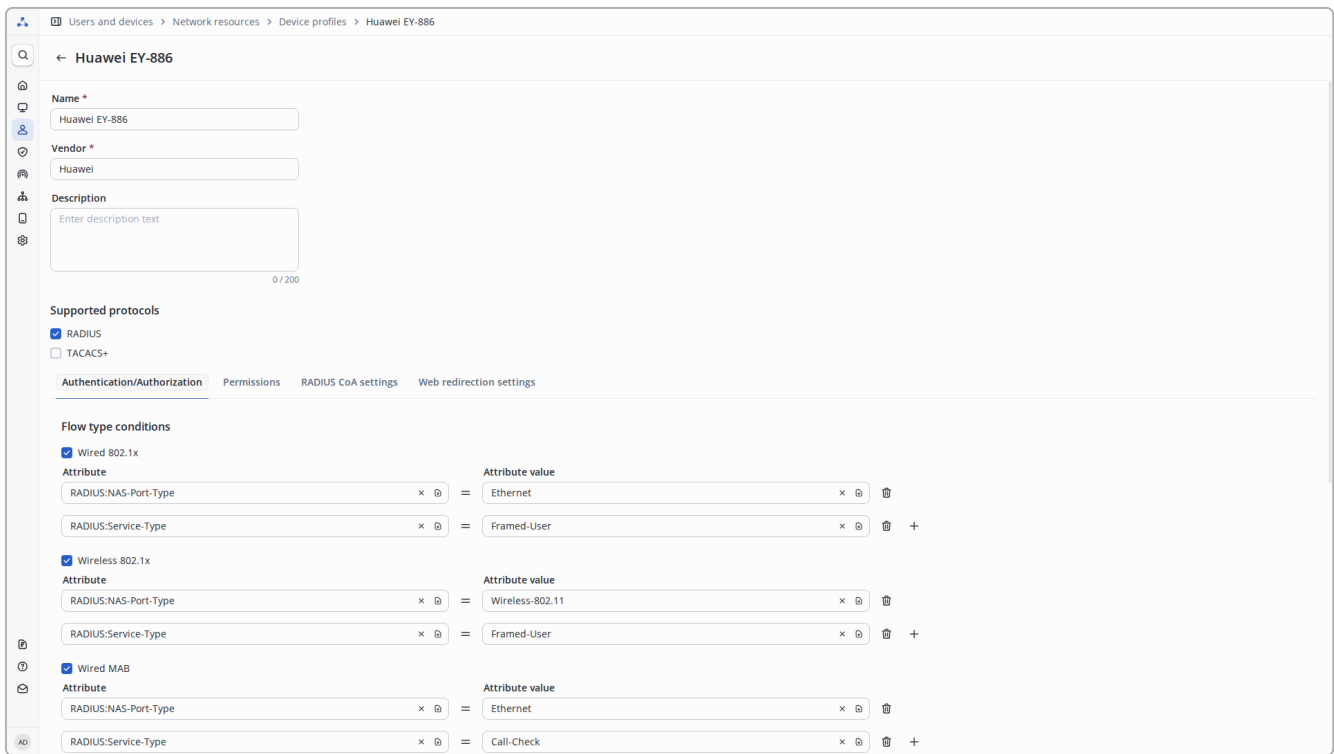


Figure 148. Network device profile editing page

After editing, click the "Save" button. The button is hidden until at least one change is made.

The "Cancel" button resets the changes made to their original state.

Deleting a device profile

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

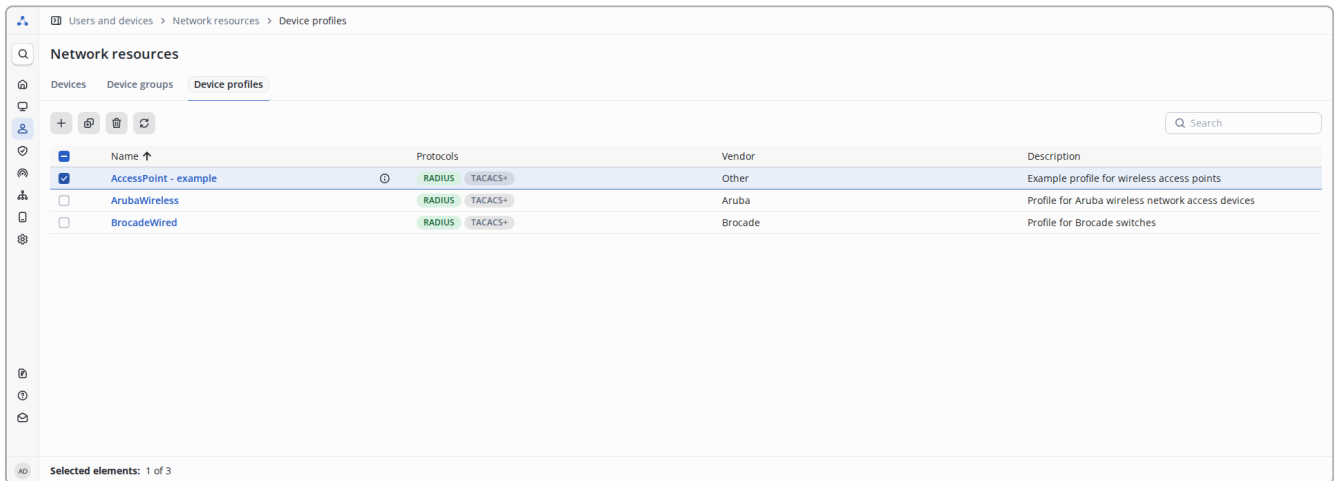


Figure 149. Page with the device profile selected for deletion



Deleting items requires confirmation in the modal window. The selected items will be deleted only after explicit confirmation of the operation.

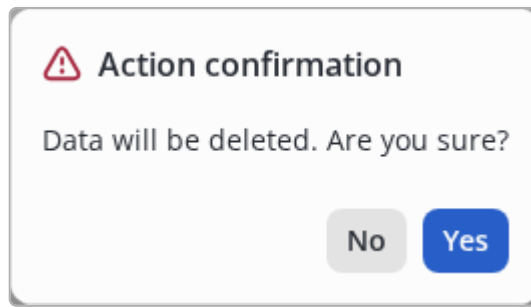


Figure 150. Modal dialog for confirmation

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

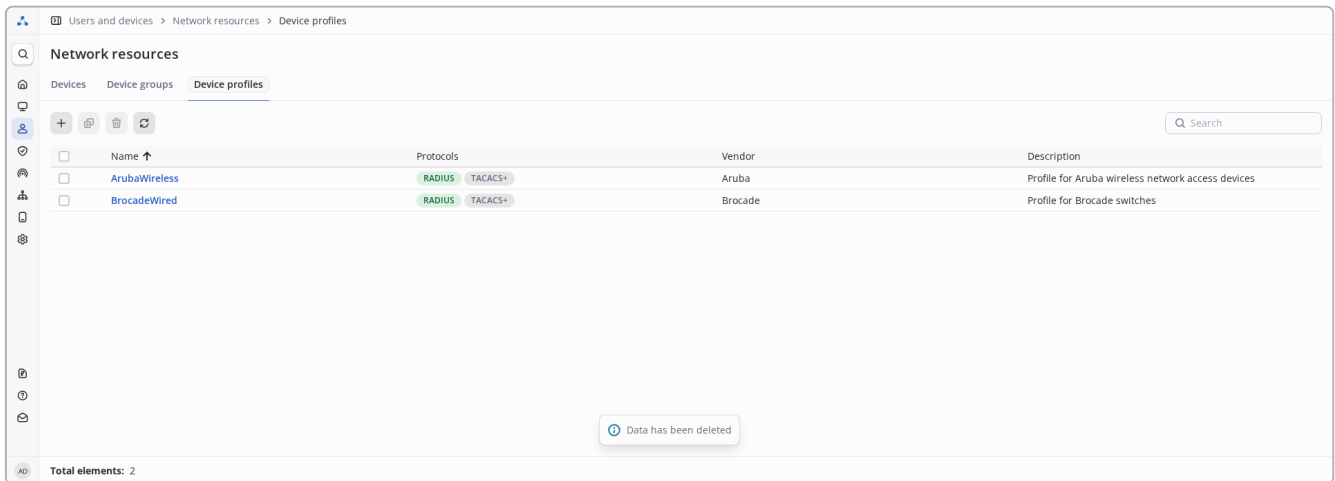


Figure 151. Page for viewing the list of device profiles after deletion



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 (suplicants) are managed in the "Users and devices" → "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.

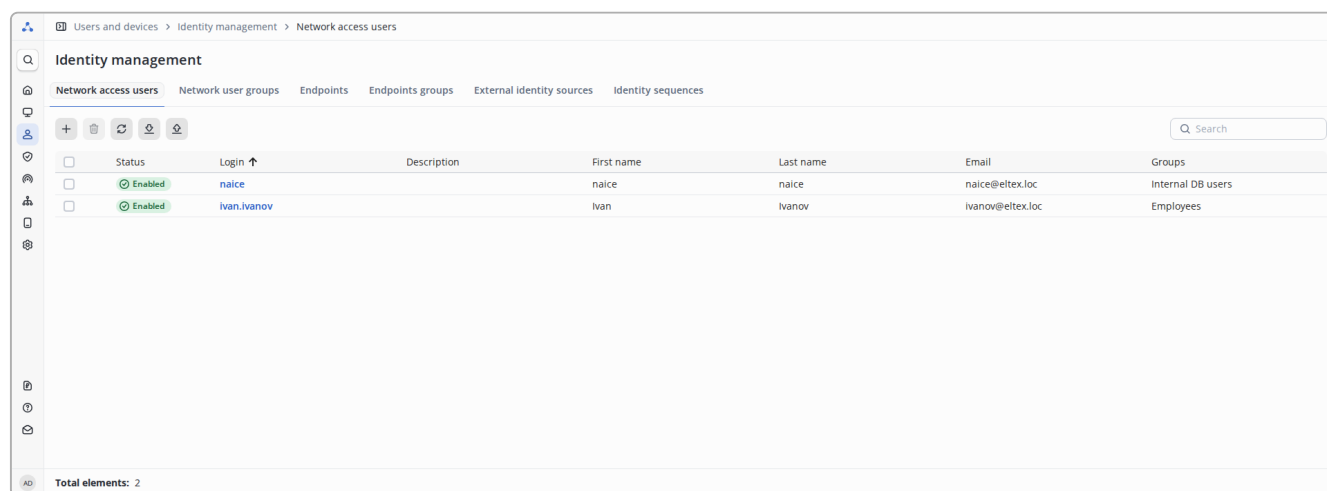
- [Identity sequences](#) - a settings section that allows you to create lists of sources of user credentials.

Network access users

Description

The *Network Users* section is designed for managing local user credentials used for authentication on devices. Such users are grouped into the *Internal DB* source.

View network users



Status	Login ↑	Description	First name	Last name	Email	Groups
Enabled	naice		naice	naice	naice@eltex.loc	Internal DB users
Enabled	ivan.ivanov		Ivan	Ivanov	ivanov@eltex.loc	Employees

Figure 152. 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.

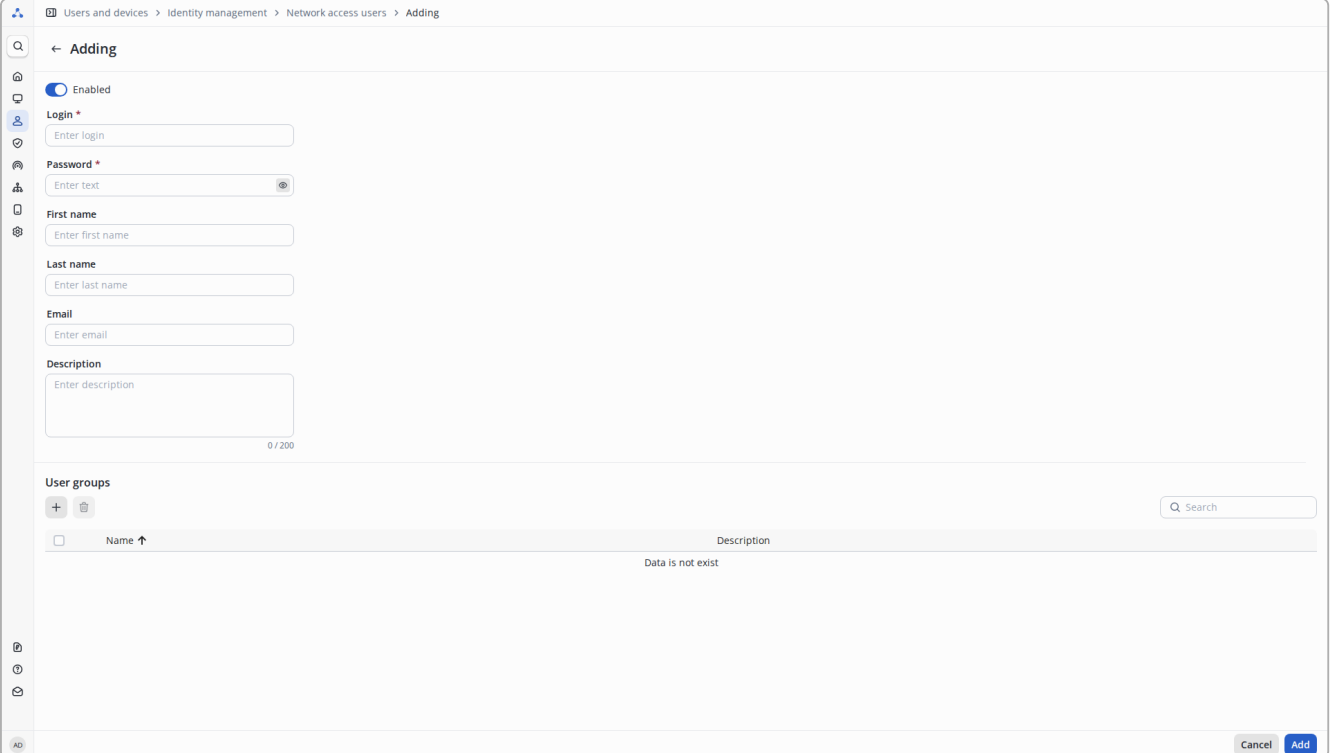
Controls:

- **+** — Add a new element.
- **🗑️** — Delete selected elements (inactive until at least one element is selected).
- **🔄** — Refresh table data.

-  — Allows you to download data from a csv file.
-  — Allows you to upload data to a csv file.
- — Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).
-  — Change the current sort order.
-  Search — Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.

Adding a user




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



The screenshot shows a web interface for adding a user. The breadcrumb trail is "Users and devices > Identity management > Network access users > Adding". The page title is "Adding". There is a search bar at the top left. The main form includes a toggle for "Enabled" (currently on), and input fields for "Login *", "Password *", "First name", "Last name", "Email", and "Description". The "Password" field has a visibility toggle (currently hidden) and a copy icon. Below the form is a "User groups" section with a search bar and a table with columns "Name" and "Description". The table is empty with the message "Data is not exist". At the bottom right, there are "Cancel" and "Add" buttons.

Figure 153. The page for adding a user

The page that opens presents the following parameters:

-  - user status switch, can take the values “enabled” or “disabled”. Authentication using disabled credentials is prohibited.
- **Login *** - user login. The maximum login length is 100 characters.
- **Password *** - user password. The minimum password length is 8 characters, the maximum is 100 characters. By clicking on  you can enable the display of the entered password, by default, the entered text is hidden. Password can be copied by clicking on .
- **First name** - user’s name. Maximum length is 100 characters.
- **Last name** - user’s last name. Maximum length is 100 characters.
-

Email - user's email address. Must follow a specific format (eg naice@eltex.loc) and not exceed 100 characters.

- Description - a custom description of the user. Maximum length is 200 characters.

Parameters marked with an asterisk * are required.

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

Controls:

- - add the user to groups.
- - delete the user from the groups selected by the checkbox (inactive until at least one group is selected).
- Search - case-insensitive filtering for all columns: only records that satisfy the filtering condition are displayed.
- - 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).

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

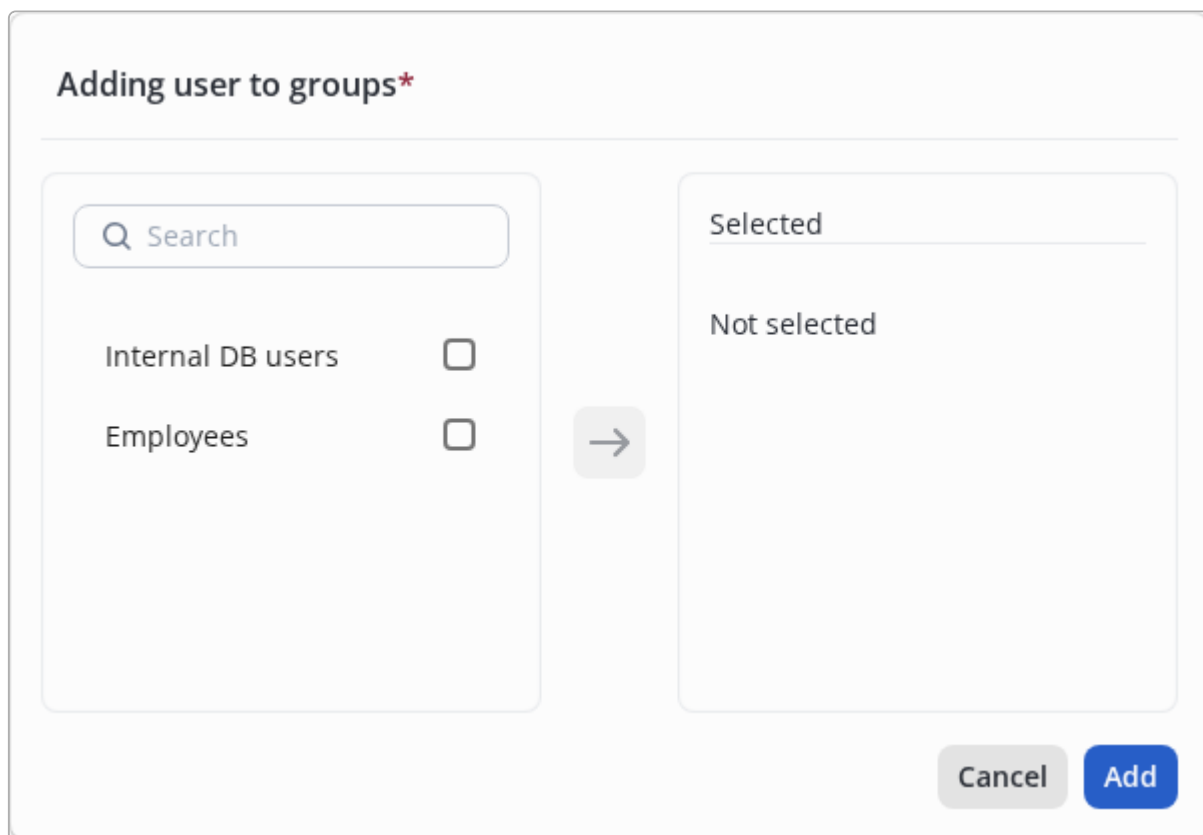


Figure 154. The page for adding a user to groups

Controls:

Q 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.

<input type="checkbox"/>	Status	Login ↑
<input type="checkbox"/>	✔ Enabled	naice
<input type="checkbox"/>	✔ Enabled	ivan.ivanov

Figure 155. Hyperlink to the user's edit page

The editing page will open.

The screenshot shows the user edit page for 'ivan.ivanov'. The page is titled 'Users and devices > Identity management > Network access users > ivan.ivanov'. The user's status is 'Enabled'. The 'Login' field is 'ivan.ivanov'. There are fields for 'First name' (Ivan), 'Last name' (Ivanov), 'Email' (ivanov@eltex.loc), and 'Description' (0 / 200). Below the user details is a 'User groups' section with a search bar and a table showing the user is assigned to the 'Employees' group.


Figure 156. The user's edit page



The old user password is not displayed on the edit page!
To change password, toggle *Change password* and enter new password in the appearing field.

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 .

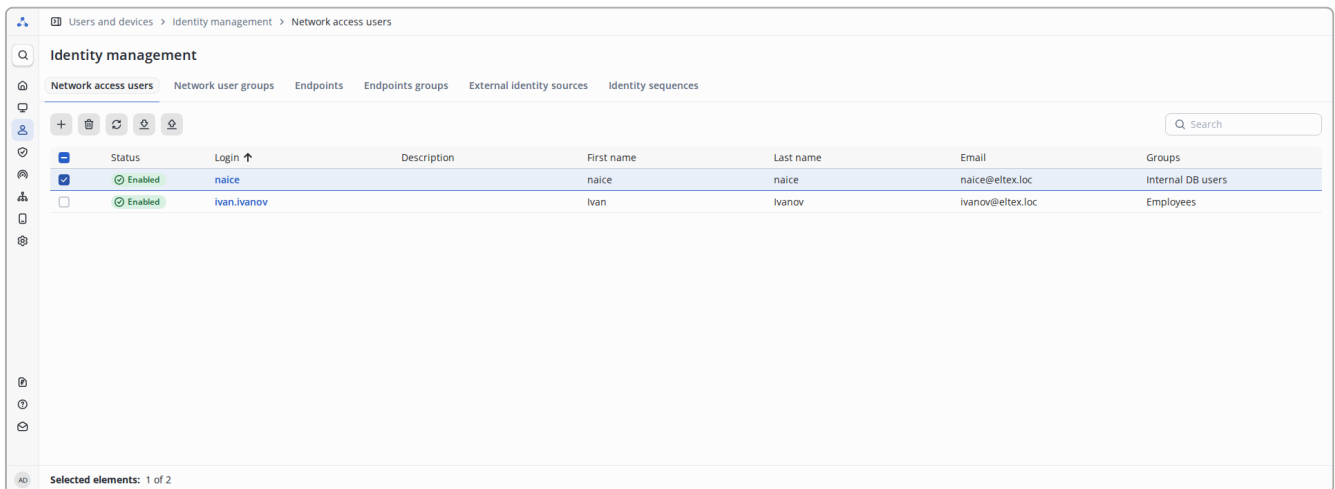


Figure 157. Selecting users in the table to delete



Deleting items requires confirmation in the modal window.
The selected items will be deleted only after explicit confirmation of the operation.

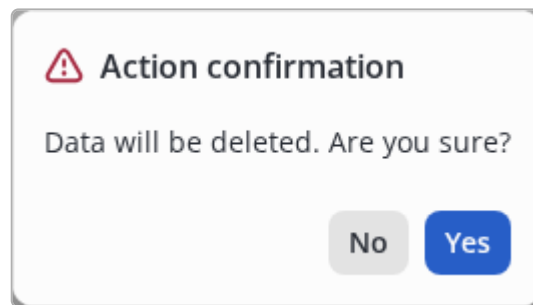


Figure 158. Modal dialog for confirmation

Import

NAICE supports importing data from CSV files.

Preliminary preparation before Import

1. Create or verify the existence of necessary related entities (e.g., device profile).
2. Review the CSV file requirements:
 - Encoding must be UTF-8;
 - Delimiters:

Field delimiter: comma (,)

- String/text delimiter: double quotation mark (")

- Headers and values must be enclosed in double quotation marks (")
- Maximum file size is 2MB.

3. Check the file content for extraneous quotation marks before importing;

4. Check that the values containing the double quotation mark (") or the slash (/) are correctly escaped.

- Values containing a double quotation mark (") are escaped using \
- Values containing the slash (/) are escaped using \

Correct spelling of values (with escaping using \") using the example of the contents of the file for importing the TACACS Command set

"name:Required"	"description"	"permit_unmatch ed(true/false)"	"commands(Grant/command/argume nts/enabled;...)"
"command_set"	"Test command set"	"false"	"PERMIT/\\"show/vlan 1 2 \"/true"


Incorrect spelling of values (without escaping) using the example of the contents of the file for importing the TACACS Command set

"name:Required"	"description"	"permit_unmatch ed(true/false)"	"commands(Grant/command/argume nts/enabled;...)"
"command_set"	"Test command set"	"false"	"PERMIT/show/vlan 1 2 /true"



Failure to escape these characters will lead to incorrect data recognition.

Import procedure


To import data from a CSV file, click on  in the action panel located above the table. This will open the import window:

Import

When importing, duplicate data will not be overwritten or edited - the system will skip it. If you want to change old data, delete it from the system manually before importing.

Carefully review the [Documentation](#) to ensure the import completes without errors.

Select a file*
Max file size 2MB

 Upload or drag it here

Field is required

Data source *

NAICE ▾

- Ignore exist data ⓘ
- Stop import on first error
- Automatically create missing records ⓘ

Cancel
Import

Figure 159. Window Import

Data import proceeds through several steps:

1. Select the required CSV file by dragging it into the upload area or by selecting it through the file explorer by clicking the **"Upload"**;



To apply changes, you must re-upload an updated CSV file.

2. Select the data source (if not predefined);
3. Configure import flags (if needed):

Ignore exist data

- On: Duplicate records trigger warnings.
- Off: Duplicates are treated as errors.

Stop import on first error

- On: Import halts at the first error. Only records that were successfully processed before it occurred will be imported.

- Off: Erroneous lines are skipped, and the import continues to the end. Only valid records will be imported.

Stop import on first error

- On: When importing, missing records will be filled in automatically. The list of auto-completed entries can be found by hovering over the tooltip to the right of the switch.
- Off: All required fields must be filled in manually.

4. To start the import, click the "**Import**".



When importing, duplicate data will not be overwritten or edited - the system will skip it. If you want to change old data, delete it from the system manually before importing.

Viewing the Import report

An import report window opens immediately after file processing.

If all records in the file were processed correctly, you will see the following window:

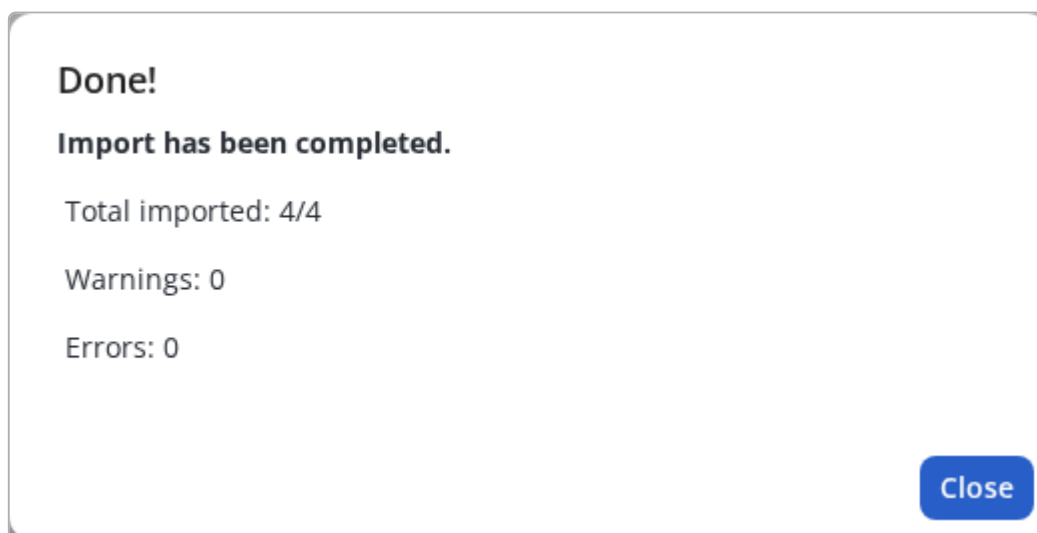


Figure 160. Window Import report (all entries were processed correctly)

The summary block contains:

- **Total Imported** - Counter of records imported (vs. total rows processed);
- **Warnings** - Number of warnings that occurred;
- **Errors** - Number of errors that occurred.

If not all records were processed correctly, you will see the following window:

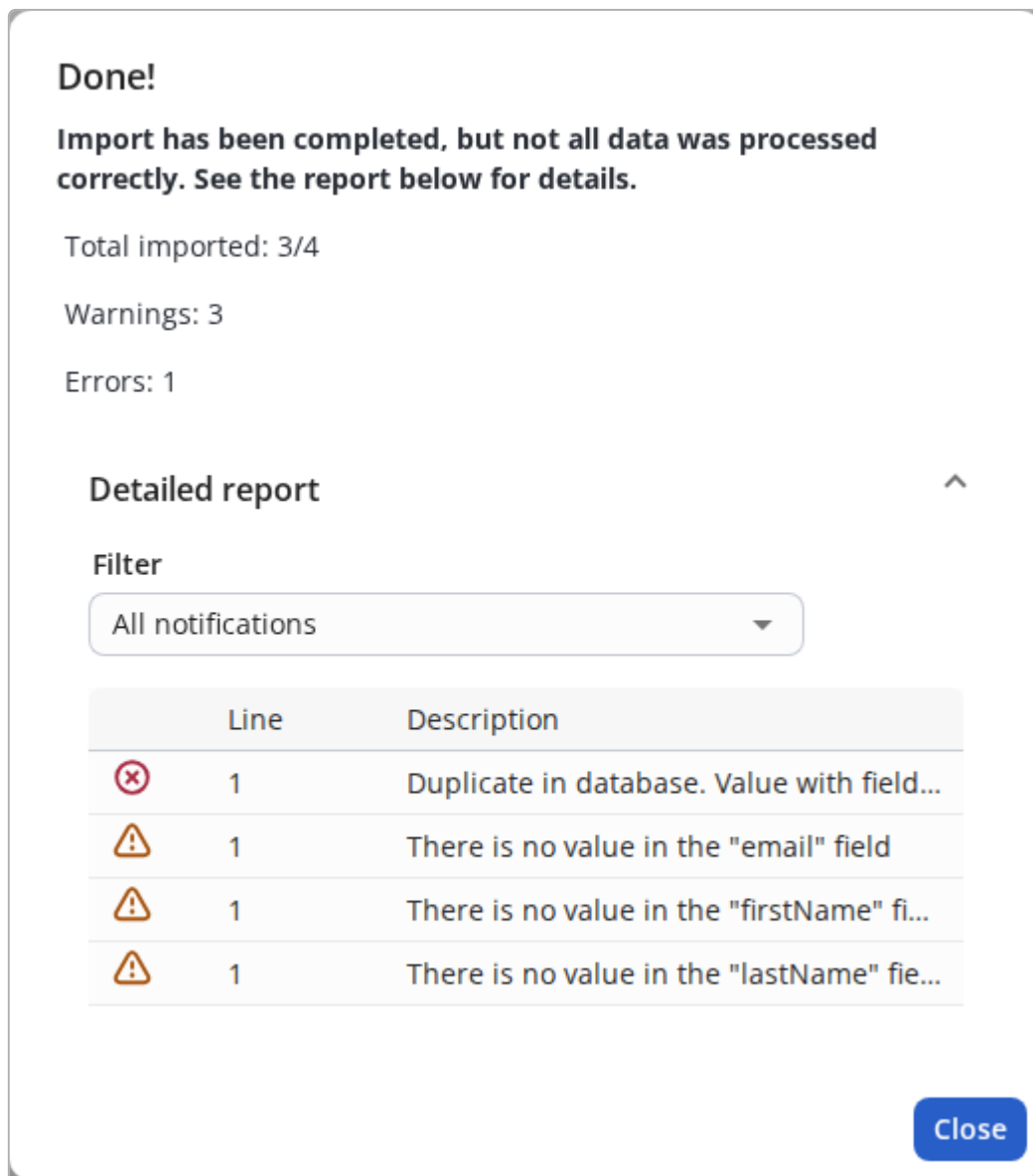


Figure 161. Window Import report (entries processed with errors/warnings)

Detailed report contains the following information:

- **Filter** - Dropdown list allowing you to select which notifications to display (All notifications , Only errors , or Only warnings)

The notification table contains columns:

- **Line** - The line number in the CSV file where an error or warning was detected;
- **Description** - Detailed text explanation of the error or warning.



Hover your cursor over a row in the Description column to view the full error/warning message in a tooltip.

Import particularities for Users



For Network user imports, only the NAICE data source is supported.

The table below lists the fields, their requirements, descriptions, and requirements:

Field	Description	Requirements
login:Required	User login	Required Maximum length - 100 characters Must be unique Spaces are not allowed
password:Required	User password. Can be imported either in hashed or plain text format	Required Length: 8-100 characters Spaces are not allowed The symbol № cannot be used
isEncrypted:Required	Password hashing flag. Indicates the format in which the password is transmitted	Required Possible values: <ul style="list-style-type: none"> • true - the transmitted password is hashed • false - the password is transmitted in plain text and will be hashed during import
enabled:Required	Authorization capability	Required Possible values: <ul style="list-style-type: none"> • true - status "Enabled" • false - status "Disabled"
firstName	User name	Maximum length - 100 characters
lastName	User surname	Maximum length - 100 characters
email	User's email address	Maximum length - 200 characters Format: admin123@gmail.com Invalid characters: <ul style="list-style-type: none"> • cyrillic letters (а-я)(А-Я) • space • double quotes " • numero sign № • semicolon ; • colon : • comma , • parentheses () • square brackets [] • greater-than/less-than signs < > • backslash \
description	Free-form description	Maximum length - 200 characters
groups	Network user groups	Groups must exist in the system Separator between groups: ;

Example of correctly formatted file content:

"login:Required"	"password:Required"	"isEncrypted:Required"	"enabled:Required"	"firstName"	"lastName"	"email"	"description"	"groups"
"user_1"	"password"	"false"	"true"	"Ivan"	"Ivanov"	"ivan@t est.ru"	""	"Internal DB;Users"

Instructions for obtaining a CSV template file are described later in the "**Export**" section.

Export

NAICE supports exporting data in CSV format. Values and headings are framed by double quotes, the field separator is comma (,).

Export procedure

Two export modes are available:

- **Export all** - Exports all records from the current section. System entities are not included during export.
- **Export selected** - Exports only checked records.

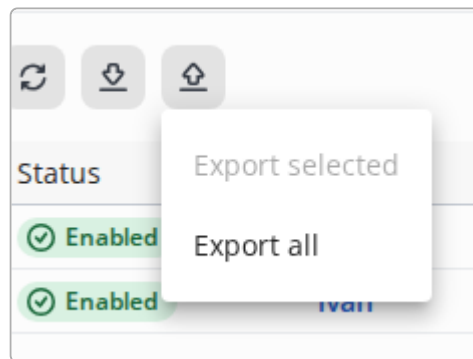



Figure 162. Window export menu



Values containing double quotation marks (") or slashes (/) will be escaped using \".

Export all

On the action panel above the table, click  and select the "**Export all**" mode. In the window that opens, confirm the action by clicking the "**Export**":

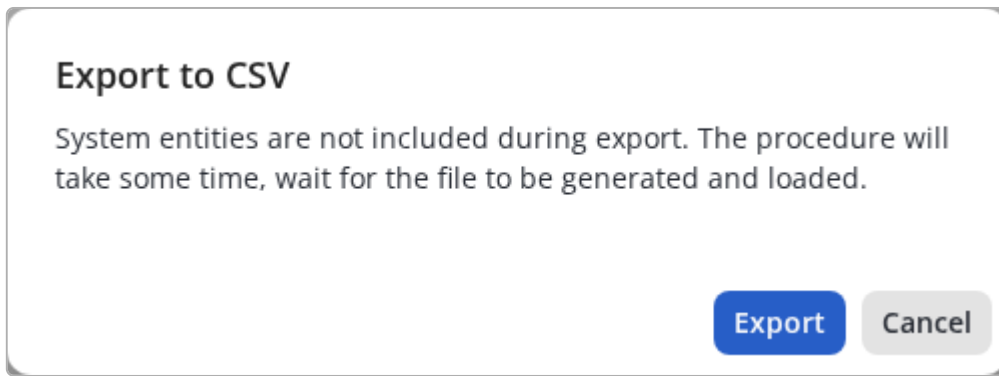



Figure 163. Export all

After clicking the "**Export**", a file containing all records from the current section will be downloaded to your device.

Export selected

On the action panel above the table, click  and select the "**Export selected**" mode. In the window that opens, confirm the action by clicking the "**Export**":

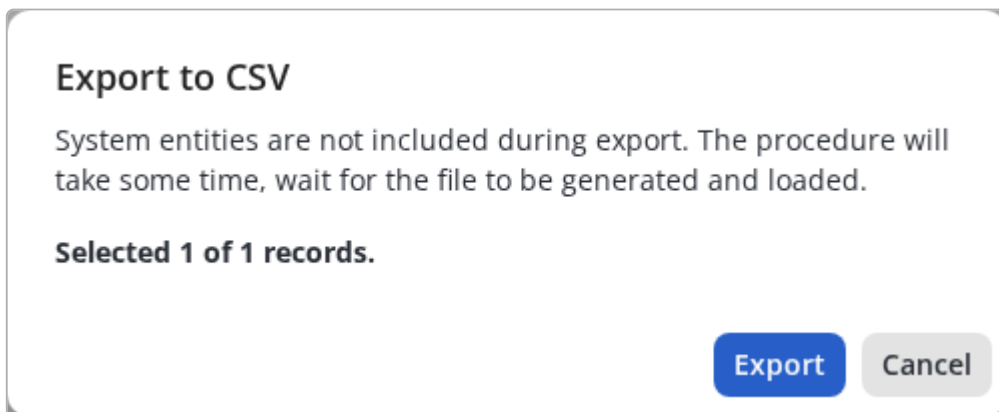


Figure 164. Export selected

After clicking the "**Export**", a file containing only the checked records will be downloaded to your device.



When **opening** CSV files, always use a **comma (,)** as the field delimiter. **Double quotation marks (")** or **empty values** may be used as string/text delimiters.

When **saving** CSV files, always use a **comma (,)** as the field delimiter, with an **empty value** as the string/text delimiter.



If a double quotation mark (") was used as the line delimiter when opening the file, values containing double quotation marks (") or slashes (/), escaped as \", may receive an extra quotation mark (") upon saving. Please check the file in a text editor and remove any extra quotation marks if they appear.

Template

If there are no records in the table (or only system entities are present), selecting the "**Export all**" mode will generate a CSV file containing only the column headers. This file can be used as a **template** for preparing data prior to import.

Export particularities for Users



User passwords will be exported from the database in a hashed format using ntHash.

The structure of the CSV file for users is described in the section "[Import particularities for Users](#)".

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 [RADIUS policies](#) or [Network devices policies](#).

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

View network user groups

The screenshot shows the 'Identity management' interface with the 'Network user groups' tab selected. The table lists the following groups:

Name ↑	Description
Internal DB users	Internal DB users default group
Employees	

Figure 165. 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:

- - Add a new element.
- - Delete selected elements (inactive until at least one element is selected).
- - Refresh table data.
- - Allows you to download data from a csv file.
- - Allows you to upload data to a csv file.

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

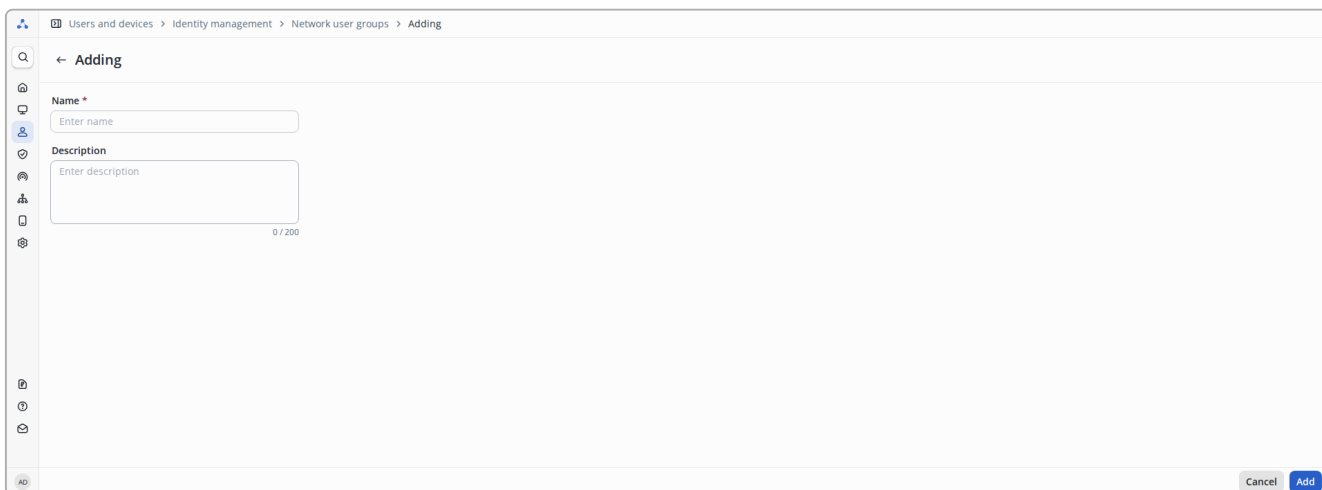


Figure 166. The page for adding a user group

The following parameters are available for filling:

- **Name *** - the name of the group. Maximum length is 100 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.

<input type="checkbox"/>	Name ↑
<input type="checkbox"/>	Internal DB users
<input type="checkbox"/>	Employees

Figure 167. Hyperlink to the user group editing page

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

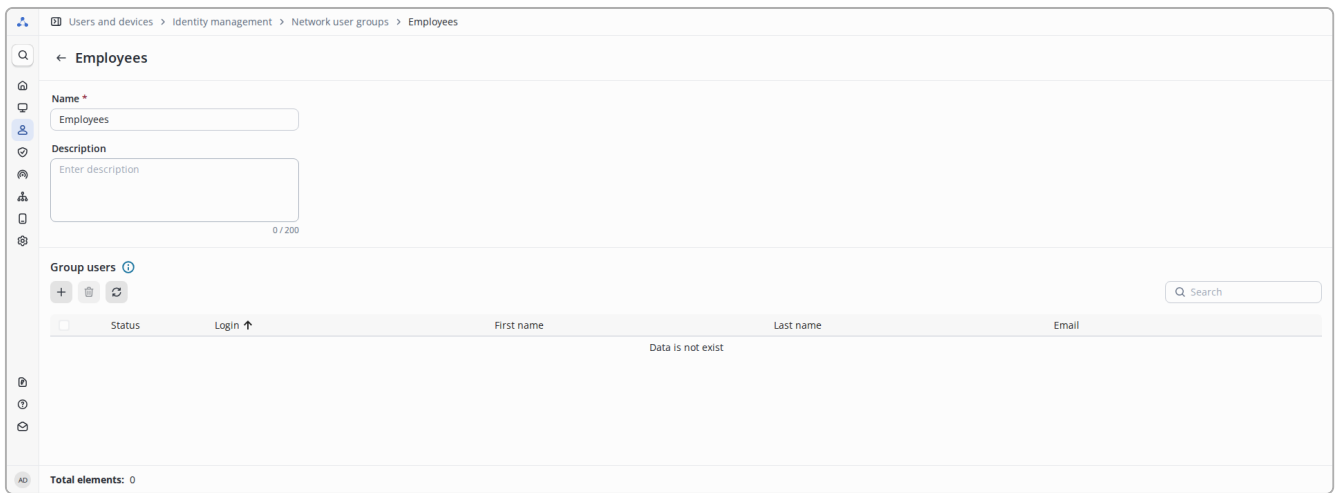


Figure 168. The user group edit page

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).
- **+** - 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.

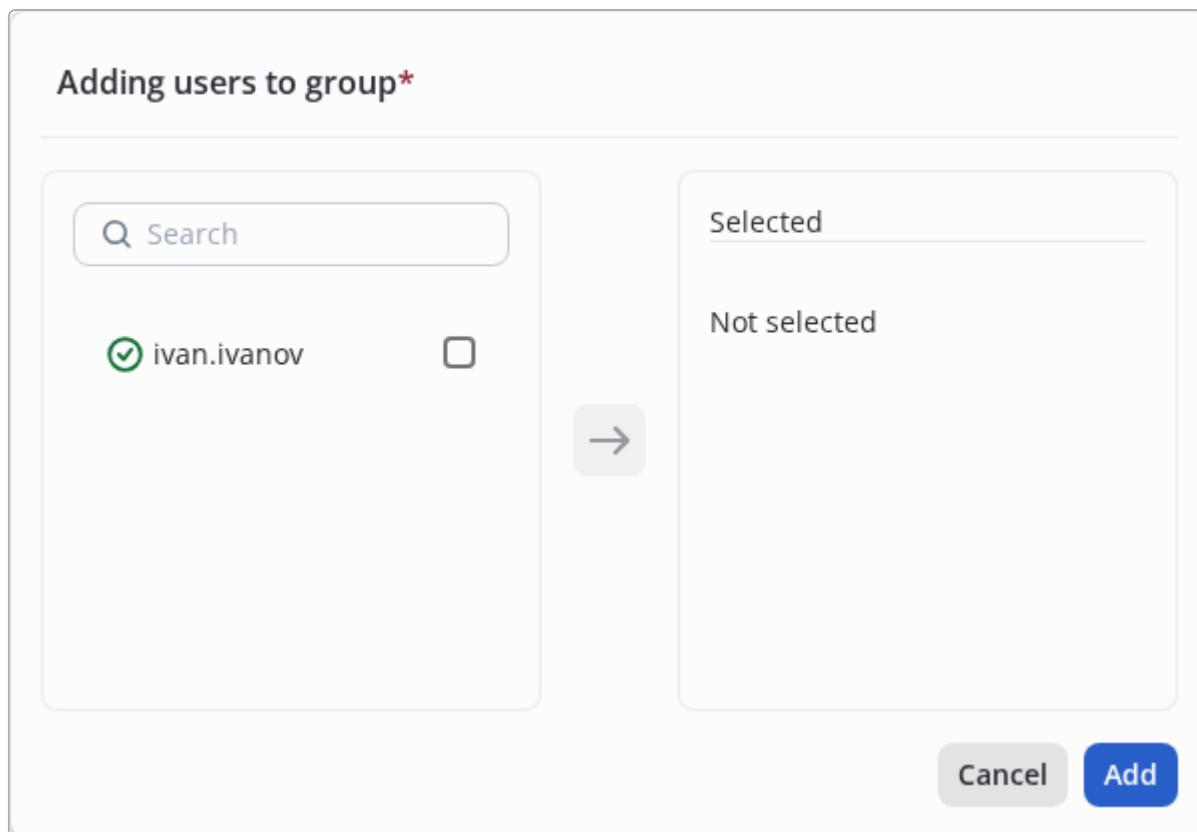



Figure 169. The window for adding users to a group


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 .

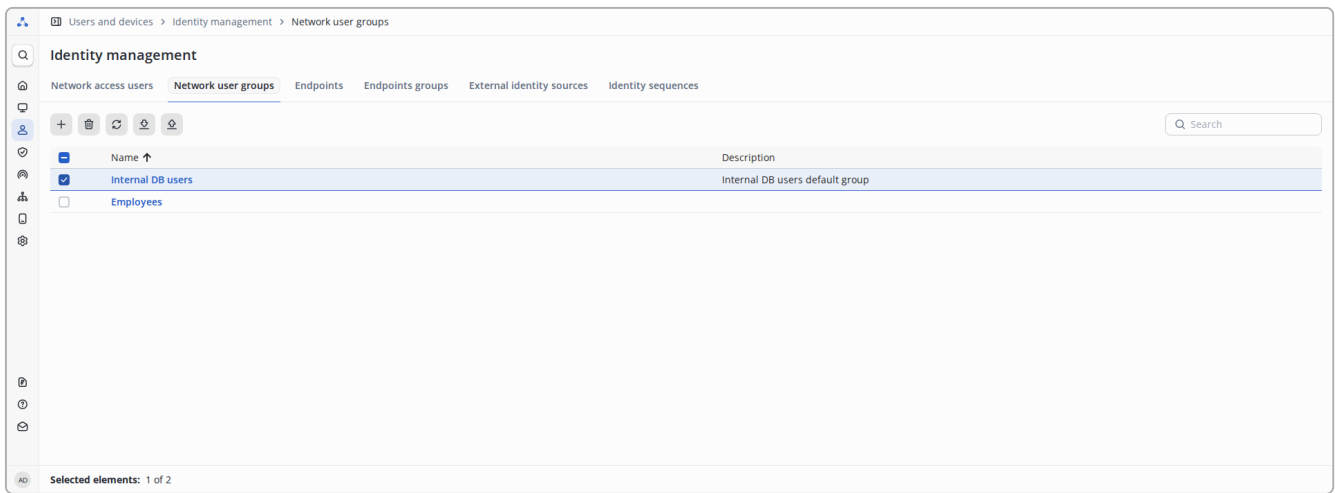


Figure 170. Selecting user groups in the table to delete



Deleting items requires confirmation in the modal window. The selected items will be deleted only after explicit confirmation of the operation.

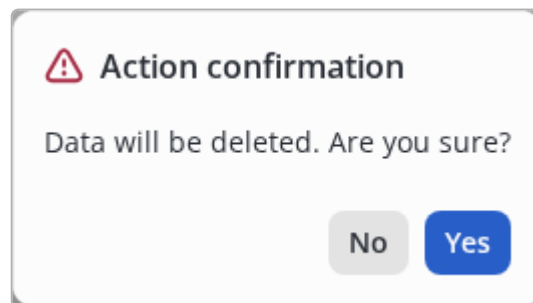


Figure 171. Modal dialog for confirmation



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.

Import

NAICE supports importing data from CSV files.

Preliminary preparation before Import

1. Create or verify the existence of necessary related entities (e.g., device profile).
2. Review the CSV file requirements:
 - Encoding must be UTF-8;
 - Delimiters:
 - Field delimiter: comma (,)
 - String/text delimiter: double quotation mark (")
 - Headers and values must be enclosed in double quotation marks (")

Maximum file size is 2MB.

3. Check the file content for extraneous quotation marks before importing;
4. Check that the values containing the double quotation mark (") or the slash (/) are correctly escaped.
 - Values containing a double quotation mark (") are escaped using \"
 - Values containing the slash (/) are escaped using \/

Correct spelling of values (with escaping using \") using the example of the contents of the file for importing the TACACS Command set

"name:Required"	"description"	"permit_unmatched(true/false)"	"commands(Grant/command/arguments/enabled;...)"
"command_set"	"\"Test command set\""	"false"	"PERMIT/\"show/vlan 1 2 \"/true"


Incorrect spelling of values (without escaping) using the example of the contents of the file for importing the TACACS Command set

"name:Required"	"description"	"permit_unmatched(true/false)"	"commands(Grant/command/arguments/enabled;...)"
"command_set"	"Test command set"	"false"	"PERMIT/show/vlan 1 2 /true"



Failure to escape these characters will lead to incorrect data recognition.

Import procedure

To import data from a CSV file, click on  in the action panel located above the table. This will open the import window:

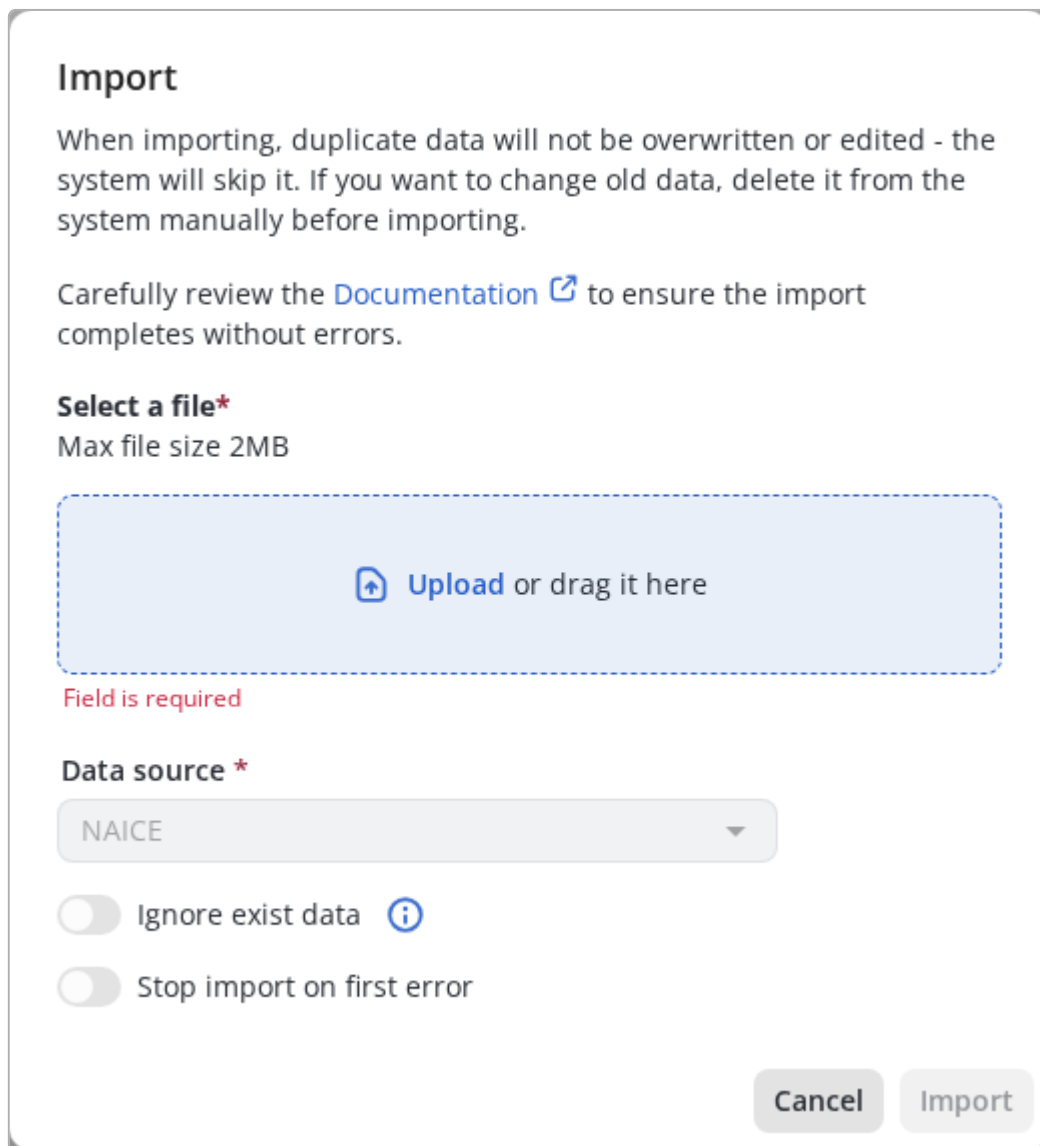


Figure 172. Window Import

Data import proceeds through several steps:

1. Select the required CSV file by dragging it into the upload area or by selecting it through the file explorer by clicking the "**Upload**";



To apply changes, you must re-upload an updated CSV file.

2. Select the data source (if not predefined);
3. Configure import flags (if needed):

Ignore exist data

- On: Duplicate records trigger warnings.
- Off: Duplicates are treated as errors.

Stop import on first error

- On: Import halts at the first error. Only records that were successfully processed before it occurred will be imported.
-

Off: Erroneous lines are skipped, and the import continues to the end. Only valid records will be imported.

4. To start the import, click the "**Import**".



When importing, duplicate data will not be overwritten or edited - the system will skip it. If you want to change old data, delete it from the system manually before importing.

Viewing the Import report

An import report window opens immediately after file processing.

If all records in the file were processed correctly, you will see the following window:

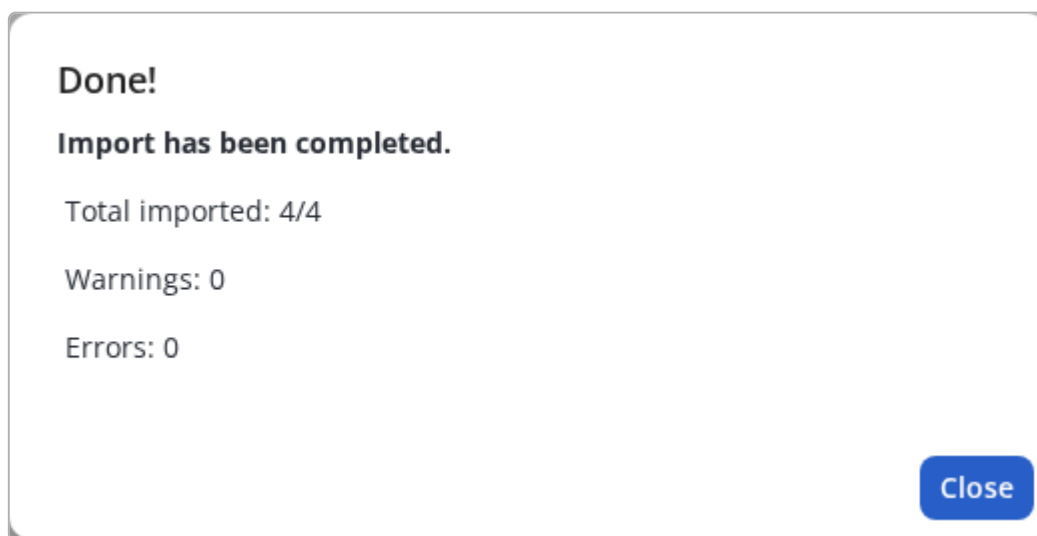


Figure 173. Window Import report (all entries were processed correctly)

The summary block contains:

- **Total Imported** - Counter of records imported (vs. total rows processed);
- **Warnings** - Number of warnings that occurred;
- **Errors** - Number of errors that occurred.

If not all records were processed correctly, you will see the following window:

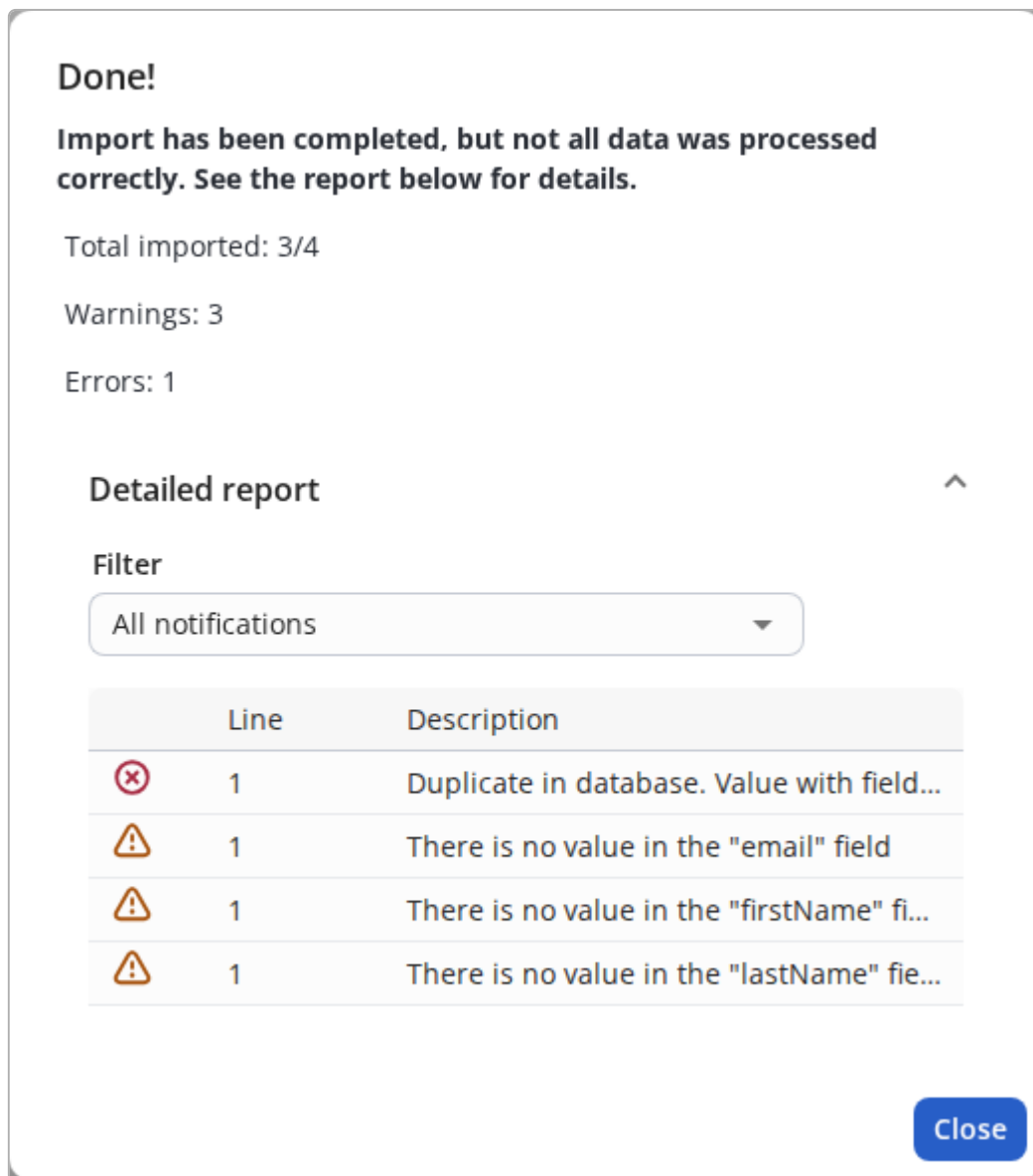


Figure 174. Window Import report (entries processed with errors/warnings)

Detailed report contains the following information:

- **Filter** - Dropdown list allowing you to select which notifications to display (All notifications , Only errors , or Only warnings)

The notification table contains columns:

- **Line** - The line number in the CSV file where an error or warning was detected;
- **Description** - Detailed text explanation of the error or warning.



Hover your cursor over a row in the Description column to view the full error/warning message in a tooltip.

Import particularities for Network user groups



For Network user groups imports, only the NAICE data source is supported.

The table below lists the fields, their requirements, descriptions, and requirements:

Field	Description	Requirements
name:Required	Name of the group	Required Maximum length - 100 characters
description	Free-form description of the group	Maximum length - 200 characters

Example of correctly formatted file content:

"name:Required"	"description"
"Internal DB users"	"Internal DB users"

Instructions for obtaining a CSV template file are described later in the "**Export**" section.

Export

NAICE supports exporting data in CSV format. Values and headings are framed by double quotes, the field separator is comma (,).

Export procedure

Two export modes are available:

- **Export all** - Exports all records from the current section. System entities are not included during export.
- **Export selected** - Exports only checked records.

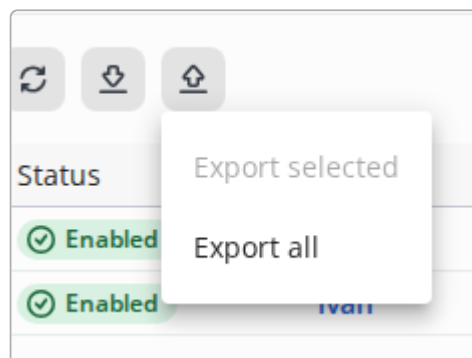



Figure 175. Window export menu



Values containing double quotation marks (") or slashes (/) will be escaped using \".

Export all

On the action panel above the table, click  and select the "**Export all**" mode. In the window that opens, confirm the action by clicking the "**Export**":

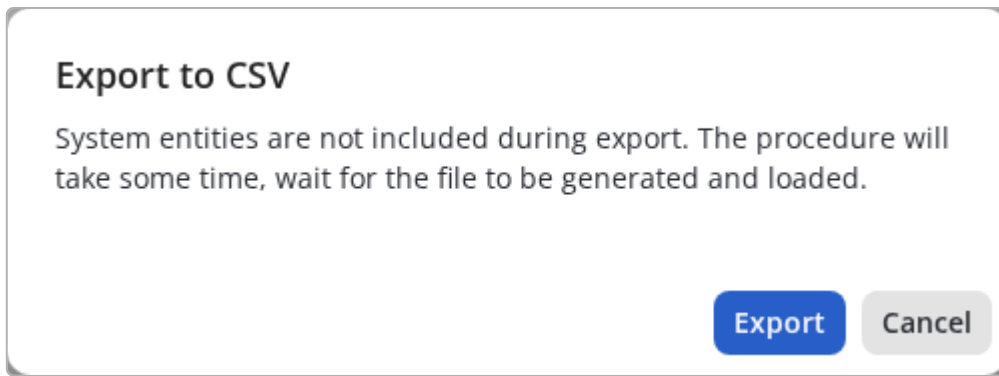



Figure 176. Export all

After clicking the "**Export**", a file containing all records from the current section will be downloaded to your device.

Export selected

On the action panel above the table, click  and select the "**Export selected**" mode. In the window that opens, confirm the action by clicking the "**Export**":

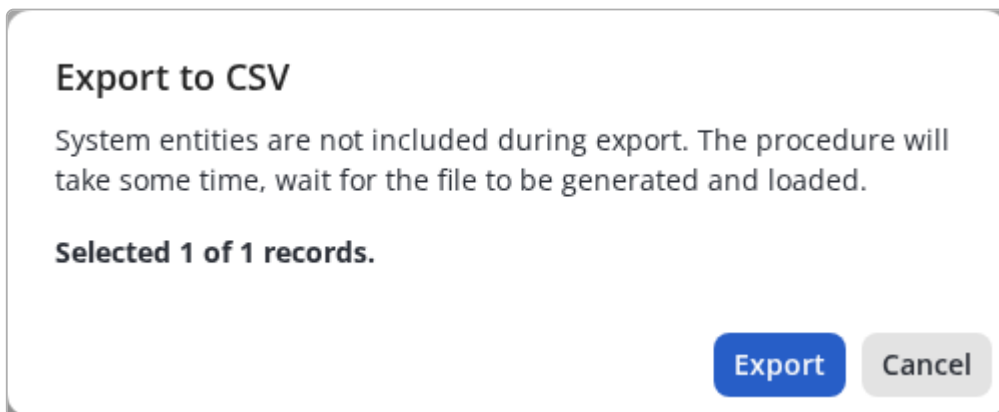


Figure 177. Export selected

After clicking the "**Export**", a file containing only the checked records will be downloaded to your device.



When **opening** CSV files, **always** use a **comma (,)** as the field delimiter. **Double quotation marks (")** or **empty values** may be used as string/text delimiters.

When **saving** CSV files, **always** use a **comma (,)** as the field delimiter, with an **empty value** as the string/text delimiter.



If a double quotation mark (") was used as the line delimiter when opening the file, values containing double quotation marks (") or slashes (/), escaped as \", may receive an extra quotation mark (") upon saving. Please check the file in a text editor and remove any extra quotation marks if they appear.

Template

If there are no records in the table (or only system entities are present), selecting the "**Export all**" mode will generate a CSV file containing only the column headers. This file can be used as a **template** for preparing data prior to import.

Export particularities for User Groups

The structure of the CSV file for user groups is described in the section "[Import particularities for Network user groups](#)".

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 [RADIUS 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 user 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. If the attribute is missing in the RADIUS request or if it does not contain a MAC address, the endpoint will not be displayed in the table, but will be taken into account in the license limit.



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




View endpoints

MAC address	Status	Description	Vendor	Endpoint IP address	User name	Host name
74:56:3C:E7:3D:9C	Connected	Discovered Endpoint	GIGA-BYTE TECHNOLOGY CO.,L...	192.168.118.179	74563ce73d9c	PC-16489
B8:2A:A9:5E:C4:5F	Rejected	Discovered Endpoint	Apple, Inc.	192.168.130.58	b82aa95ec45f	
44:E4:D9:3B:54:1A	Rejected	Discovered Endpoint	Cisco Systems, Inc.	192.168.87.192	44e4d93b541a	
A8:F9:4B:26:C0:16	Connected	Discovered Endpoint	Eltex Enterprise Ltd.	192.168.30.198	a8f94b26c016	NV-501-Wac-revA
7C:C2:C6:4B:0D:C9	Connected	Discovered Endpoint	TP-Link Systems Inc	192.168.50.25	7cc2c64b0dc9	LAPTOP-JFLJ6IBE
40:86:CB:44:C1:8A	Rejected	Discovered Endpoint	D-Link Corporation	192.168.240.155	4086cb44c18a	
A4:3B:0E:00:8C:39	Connected	Discovered Endpoint	Huawei Device Co., Ltd.	192.168.23.150	a43b0e008c39	MNA-LX9
50:EB:F6:DB:65:FA	Connected	Computer	ASUSTEK COMPUTER INC.	192.168.151.144	50ebf6db65fa	PC-16488
14:58:D0:C5:2A:36	Connected	Discovered Endpoint	Hewlett Packard	192.168.126.51	1458d0c52a36	user-HP-ProBook-450-G2
CC:9D:A2:C7:C6:50	Connected	Discovered Endpoint	Eltex Enterprise Ltd.	192.168.179.242	cc9da2c7c650	WEP-3ax
68:13:E2:09:7A:77	Connected	Discovered Endpoint	Eltex Enterprise LTD	192.168.113.111	6813e2097a77	VP-12P
74:56:3C:26:B4:5F	Connected	Discovered Endpoint	GIGA-BYTE TECHNOLOGY CO.,L...	192.168.106.231	74563c26b45f	DESKTOP-NUBAQB5
00:ED:4C:68:30:FF	Connected	Discovered Endpoint	REALTEK SEMICONDUCTOR CO...	192.168.96.151	00e4c6830ff	azurecloud-o-pc
A4:BA:DB:D4:CD:EF	Connected	Discovered Endpoint	Dell Inc.	192.168.35.90	a4badbd4cddef	vostro
E8:F7:91:DF:B2:36	Connected	Discovered Endpoint	Xiaomi Communications Co Ltd	192.168.50.137	e8f791dfb236	Redmi11N

Figure 178. 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:

-  - Add a new element.
-  - Delete selected elements (inactive until at least one element is selected).
-  - Start updating profile of selected endpoints (inactive until at least one element is selected).
-  - Refresh table data.
-  - Allows you to download data from a csv file.
-  - Allows you to upload data to a csv file.
-  - Customize the display of table columns.
- - Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).
-  - Change the current sort order.
-  **Filters** - Open the data filtering settings window for the table.

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

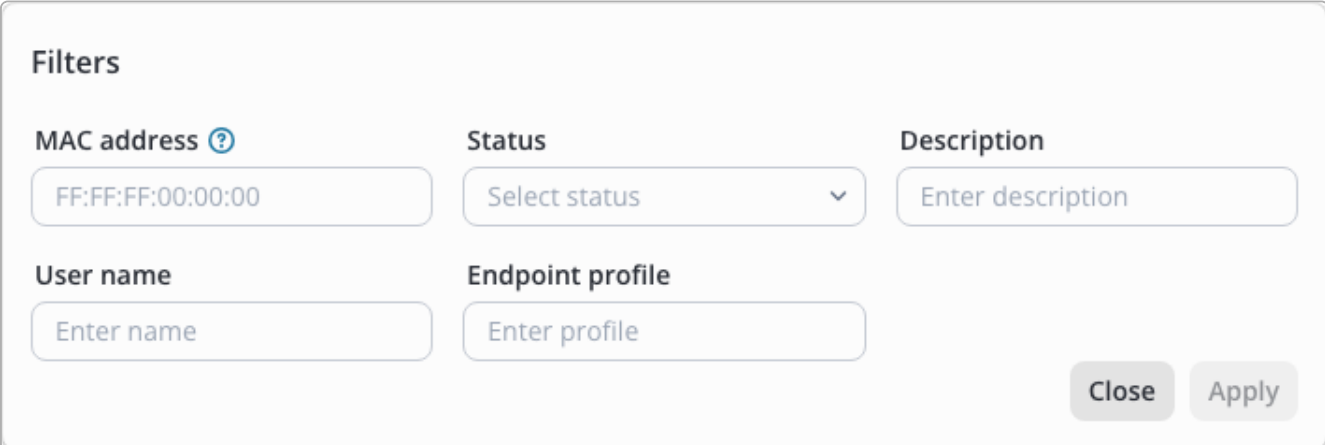



Figure 179. Configuring data filtering in the table

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 **Reset all** 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.

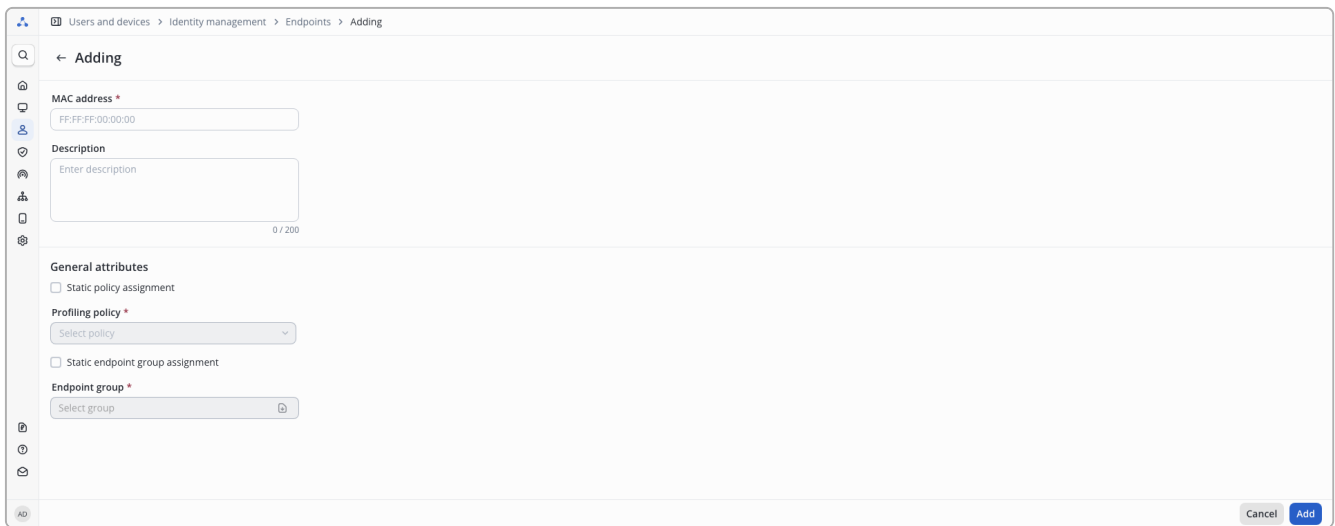


Figure 180. Adding an endpoint

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.

<input type="checkbox"/>	MAC address	Status
<input type="checkbox"/>	74:56:3C:E7:3D:9C	✔ Connected
<input type="checkbox"/>	B8:2A:A9:5E:C4:5F	✘ Rejected
<input type="checkbox"/>	44:E4:D9:3B:54:1A	✘ Rejected
<input type="checkbox"/>	A8:F9:4B:26:C0:16	✔ Connected
<input type="checkbox"/>	7C:C2:C6:4B:0D:C9	✔ Connected
<input type="checkbox"/>	40:86:CB:44:C1:8A	✘ Rejected
<input type="checkbox"/>	A4:3B:0E:00:8C:39	✔ Connected
<input type="checkbox"/>	50:EB:F6:DB:65:FA	✔ Connected
<input type="checkbox"/>	14:58:D0:C5:2A:36	✔ Connected
<input type="checkbox"/>	CC:9D:A2:C7:C6:50	✔ Connected
<input type="checkbox"/>	68:13:E2:09:7A:77	✔ Connected
<input type="checkbox"/>	74:56:3C:26:B4:5F	✔ Connected
<input type="checkbox"/>	00:E0:4C:68:30:FF	✔ Connected
<input type="checkbox"/>	A4:BA:DB:D4:CD:EF	✔ Connected
<input type="checkbox"/>	E8:F7:91:DF:B2:36	✔ Connected

Figure 181. Hyperlink to the endpoint editing page

An editing page similar to the adding page will open.

Figure 182. 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.

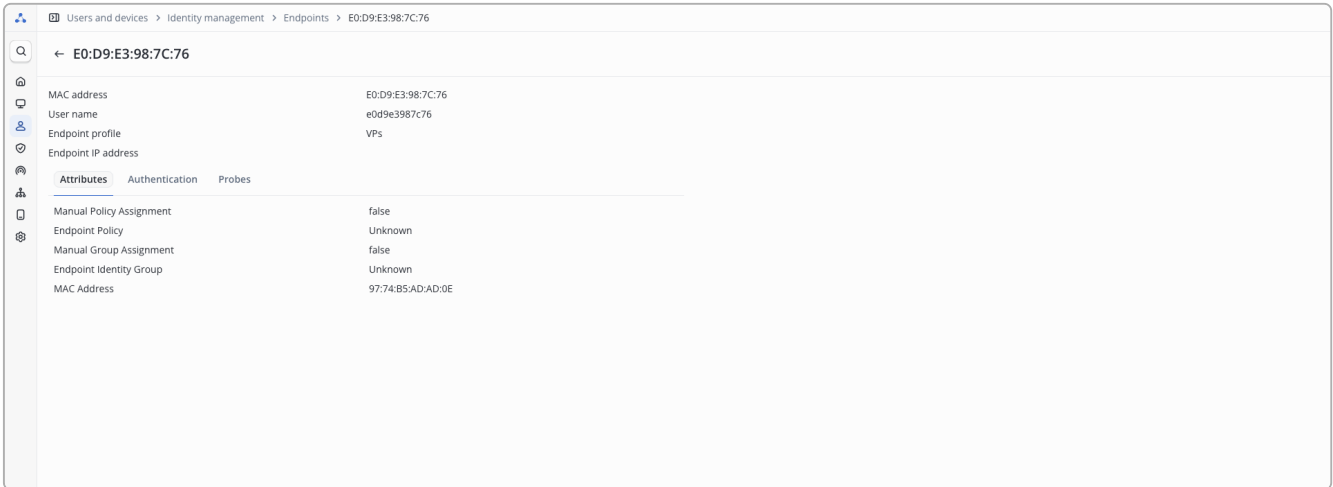


Figure 183. Viewing detailed information about an endpoint

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 system user;
- **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 .

Users and devices > Identity management > Endpoints

Identity management

Network access users Network user groups **Endpoints** Endpoints groups External identity sources Identity sequences

Filters

	MAC address	Status	More	Description	Vendor	Endpoint IP address	User name	Host name
<input checked="" type="checkbox"/>	74:56:3C:E7:3D:9C	Connected		Discovered Endpoint	GIGA-BYTE TECHNOLOGY CO.,L...	192.168.118.179	74563ce73d9c	PC-16489
<input type="checkbox"/>	B8:2A:A9:5E:C4:5F	Rejected		Discovered Endpoint	Apple, Inc.	192.168.130.58	b82aa95ec45f	
<input type="checkbox"/>	44:E4:D9:3B:54:1A	Rejected		Discovered Endpoint	Cisco Systems, Inc	192.168.87.192	44e4d93b541a	
<input type="checkbox"/>	A8:F9:4B:26:C0:16	Connected		Discovered Endpoint	Eltex Enterprise Ltd.	192.168.30.198	a8f94b26c016	NV-501-Wac-revA
<input type="checkbox"/>	7C:C2:C6:4B:0D:C9	Connected		Discovered Endpoint	TP-Link Systems Inc	192.168.50.25	7cc2c64b0dc9	LAPTOP-JFLI6IBE
<input type="checkbox"/>	40:86:CB:44:C1:8A	Rejected		Discovered Endpoint	D-Link Corporation	192.168.240.155	4086cb44c18a	
<input type="checkbox"/>	A4:3B:0E:00:8C:39	Connected		Discovered Endpoint	Huawei Device Co., Ltd.	192.168.23.150	a43b0e008c39	MNA-LX9
<input type="checkbox"/>	50:EB:F6:DB:65:FA	Connected		Computer	ASUSTek COMPUTER INC.	192.168.151.144	50ebf6db65fa	PC-16488
<input type="checkbox"/>	14:58:D0:C5:2A:36	Connected		Discovered Endpoint	Hewlett Packard	192.168.126.51	1458d0c52a36	user-HP-ProBook-450-G2
<input type="checkbox"/>	CC:9D:A2:C7:C6:50	Connected		Discovered Endpoint	Eltex Enterprise Ltd.	192.168.179.242	cc9da2c7c650	WEP-3ax
<input type="checkbox"/>	68:13:E2:09:7A:77	Connected		Discovered Endpoint	Eltex Enterprise LTD	192.168.113.111	6813e2097a77	VP-12P
<input type="checkbox"/>	74:56:3C:26:B4:5F	Connected		Discovered Endpoint	GIGA-BYTE TECHNOLOGY CO.,L...	192.168.106.231	74563c26b45f	DESKTOP-NU8AQB5
<input type="checkbox"/>	00:ED:4C:68:30:FF	Connected		Discovered Endpoint	REALTEK SEMICONDUCTOR CO...	192.168.96.151	00e04c6830ff	azurecloud-o-pc

Selected elements: 1 of 15

Figure 184. Selecting endpoints in the table to delete



Deleting items requires confirmation in the modal window. The selected items will be deleted only after explicit confirmation of the operation.

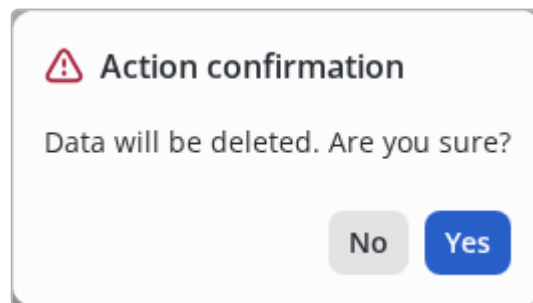


Figure 185. Modal dialog for confirmation

Import

NAICE supports importing data from CSV files.

Preliminary preparation before Import

1. Create or verify the existence of necessary related entities (e.g., device profile).
2. Review the CSV file requirements:
 - Encoding must be UTF-8;
 - Delimiters:
 - Field delimiter: comma (,)
 - String/text delimiter: double quotation mark (")
 - Headers and values must be enclosed in double quotation marks (")
 - Maximum file size is 2MB.
3. Check the file content for extraneous quotation marks before importing;
4. Check that the values containing the double quotation mark (") or the slash (/) are correctly escaped.
 - Values containing a double quotation mark (") are escaped using \

Values containing the slash (/) are escaped using \"

Correct spelling of values (with escaping using \") using the example of the contents of the file for importing the TACACS Command set

"name:Required"	"description"	"permit_unmatched(true/false)"	"commands(Grant/command/arguments/enabled;...)"
"command_set"	"Test command set"	"false"	"PERMIT/\"show/vlan 1 2 \"/true"


Incorrect spelling of values (without escaping) using the example of the contents of the file for importing the TACACS Command set

"name:Required"	"description"	"permit_unmatched(true/false)"	"commands(Grant/command/arguments/enabled;...)"
"command_set"	"Test command set"	"false"	"PERMIT/show/vlan 1 2 /true"



Failure to escape these characters will lead to incorrect data recognition.

Import procedure


To import data from a CSV file, click on  in the action panel located above the table. This will open the import window:

Import

When importing, duplicate data will not be overwritten or edited - the system will skip it. If you want to change old data, delete it from the system manually before importing.

Carefully review the [Documentation](#) to ensure the import completes without errors.

Select a file*
Max file size 2MB

 Upload or drag it here

Field is required

Data source *

NAICE ▾

- Ignore exist data ⓘ
- Stop import on first error
- Automatically create missing records ⓘ

Cancel
Import

Figure 186. Window Import

Data import proceeds through several steps:

1. Select the required CSV file by dragging it into the upload area or by selecting it through the file explorer by clicking the **"Upload"**;



To apply changes, you must re-upload an updated CSV file.

2. Select the data source (if not predefined);
3. Configure import flags (if needed):

Ignore exist data

- On: Duplicate records trigger warnings.
- Off: Duplicates are treated as errors.

Stop import on first error

- On: Import halts at the first error. Only records that were successfully processed before it occurred will be imported.

- Off: Erroneous lines are skipped, and the import continues to the end. Only valid records will be imported.

Stop import on first error

- On: When importing, missing records will be filled in automatically. The list of auto-completed entries can be found by hovering over the tooltip to the right of the switch.
- Off: All required fields must be filled in manually.

4. To start the import, click the "**Import**".



When importing, duplicate data will not be overwritten or edited - the system will skip it. If you want to change old data, delete it from the system manually before importing.

Viewing the Import report

An import report window opens immediately after file processing.

If all records in the file were processed correctly, you will see the following window:

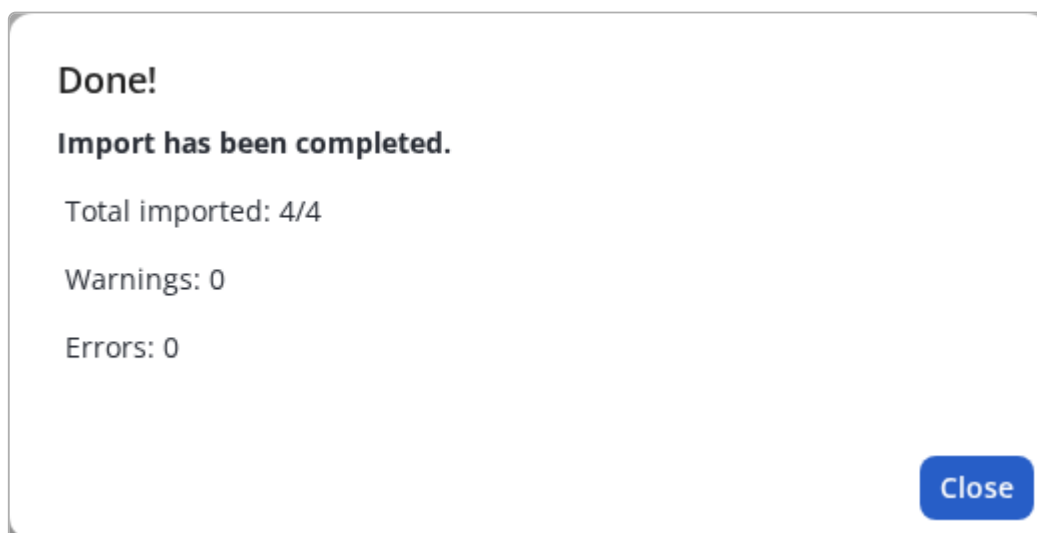


Figure 187. Window Import report (all entries were processed correctly)

The summary block contains:

- **Total Imported** - Counter of records imported (vs. total rows processed);
- **Warnings** - Number of warnings that occurred;
- **Errors** - Number of errors that occurred.

If not all records were processed correctly, you will see the following window:

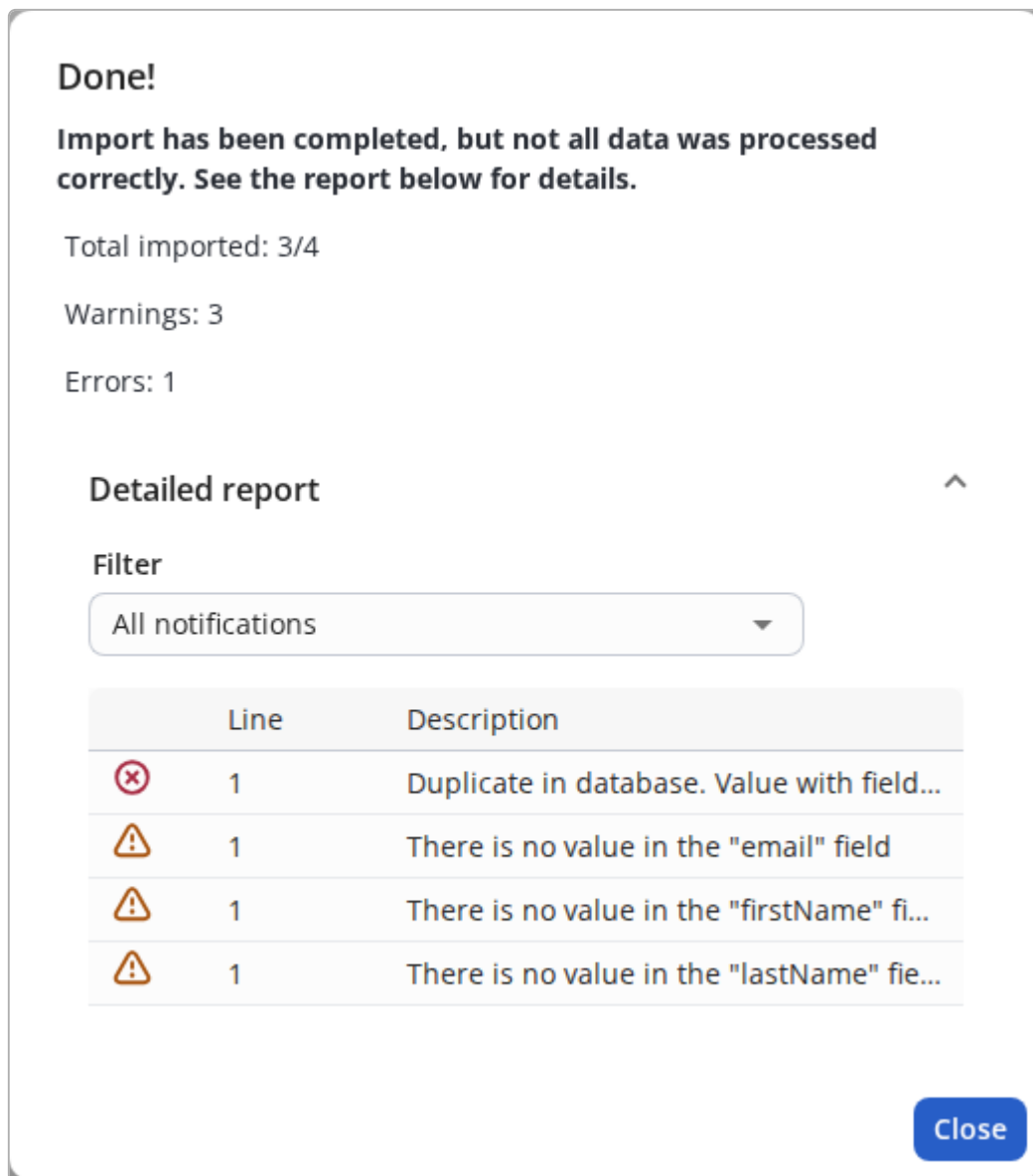


Figure 188. Window Import report (entries processed with errors/warnings)

Detailed report contains the following information:

- **Filter** - Dropdown list allowing you to select which notifications to display (All notifications , Only errors , or Only warnings)

The notification table contains columns:

- **Line** - The line number in the CSV file where an error or warning was detected;
- **Description** - Detailed text explanation of the error or warning.



Hover your cursor over a row in the Description column to view the full error/warning message in a tooltip.

Import particularities for Endpoints



For Endpoints imports, only the NAICE data source is supported.

The table below lists the fields, their requirements, descriptions, and requirements:

Field	Description	Requirements
mac_address:Required	MAC address of the endpoint	Required The following MAC address formats are valid: - XX:XX:XX:XX:XX:XX - XX-XX-XX-XX-XX-XX - XXXX.XXXX.XXXX - XXXXXXXXXXXX
vendor	Manufacturer of the end device	This field is ignored during import
description	Free-form description	Maximum length - 200 characters
profiler_policy	Profiling policy to be assigned to the endpoint (full path required)	Must exist in the NAICE system Format: parent_policy#policy
endpoint_group	Group to be assigned to the endpoint (full path required)	Must exist in the NAICE system Format: group#subgroup
hostname	Hostname of the endpoint	Maximum length - 100 characters
username	Username	Maximum length - 100 characters
current_ip_addresses	IP address of the endpoint	Format: four numbers 0-255, separated by dots

Logic for processing the fields profiler_policy and endpoint_group :



- If the value is found in the system — the policy/group is considered **manually assigned** and will not be overwritten as a result of future **profiling**.
- If the value is absent/not found — it is automatically assigned the value **Unknown**, which may be overwritten as a result of future **profiling**.

Example of correctly formatted file content:

"mac_address:Required"	"vendor"	"description"	"profiler_policy"	"endpoint_group"	"hostname"	"username"	"current_ip_addresses"
"85:BF:DA:B7:87:66"	""	""	"test#test_policy"	"test_group"	"test"	"tester"	"10.25.95.105"

Instructions for obtaining a CSV template file are described later in the "**Export**" section.

Export

NAICE supports exporting data in CSV format. Values and headings are framed by double quotes, the field separator is comma (,).

Export procedure

Two export modes are available:

- **Export all** - Exports all records from the current section. System entities are not included during export.
- **Export selected** - Exports only checked records.

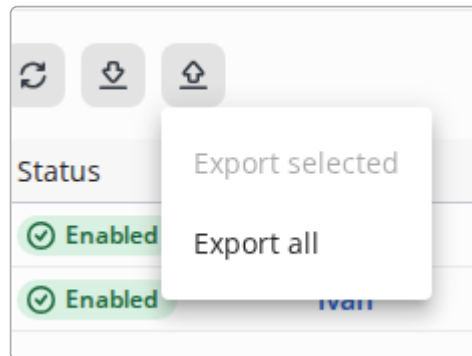



Figure 189. Window export menu



Values containing double quotation marks (") or slashes (/) will be escaped using \".

Export all

On the action panel above the table, click  and select the "**Export all**" mode. In the window that opens, confirm the action by clicking the "**Export**":

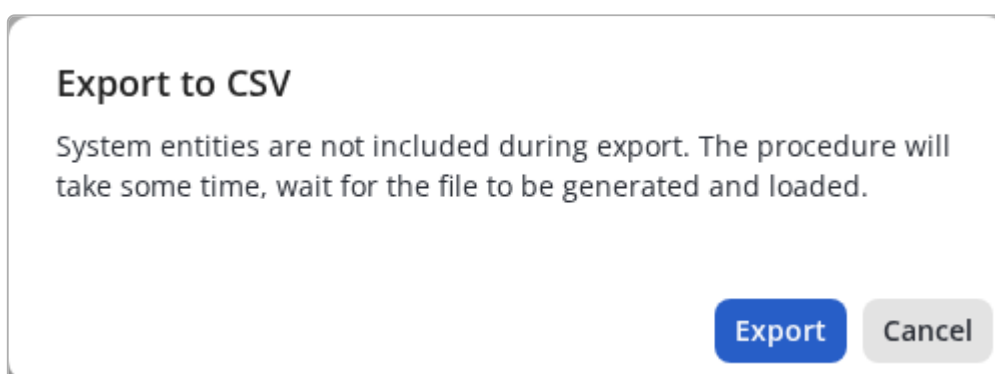



Figure 190. Export all

After clicking the "**Export**", a file containing all records from the current section will be downloaded to your device.

Export selected

On the action panel above the table, click  and select the "**Export selected**" mode. In the window that opens, confirm the action by clicking the "**Export**":

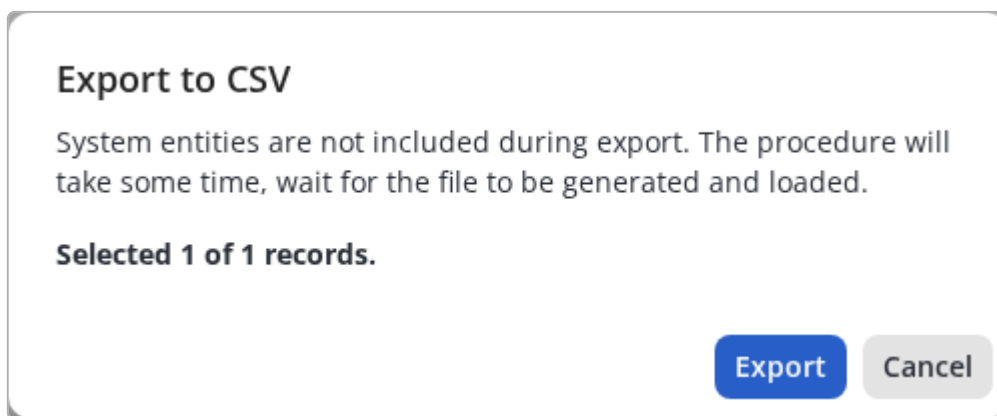


Figure 191. Export selected

After clicking the **"Export"**, a file containing only the checked records will be downloaded to your device.



When **opening** CSV files, **always** use a **comma (,)** as the field delimiter. **Double quotation marks (")** or **empty values** may be used as string/text delimiters.

When **saving** CSV files, **always** use a **comma (,)** as the field delimiter, with an **empty value** as the string/text delimiter.



If a double quotation mark (") was used as the line delimiter when opening the file, values containing double quotation marks (") or slashes (/), escaped as \", may receive an extra quotation mark (") upon saving. Please check the file in a text editor and remove any extra quotation marks if they appear.

Template

If there are no records in the table (or only system entities are present), selecting the **"Export all"** mode will generate a CSV file containing only the column headers. This file can be used as a **template** for preparing data prior to import.

Export particularities for Endpoints



The exported file will include the vendor field — the manufacturer of the end device, determined by the first three octets of the MAC address (MAC OUI).



The policy/group for endpoints will be recorded in the format of its full path using the separator - #.

The structure of the CSV file for endpoints is described in the section ["Import particularities for Endpoints"](#).

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.

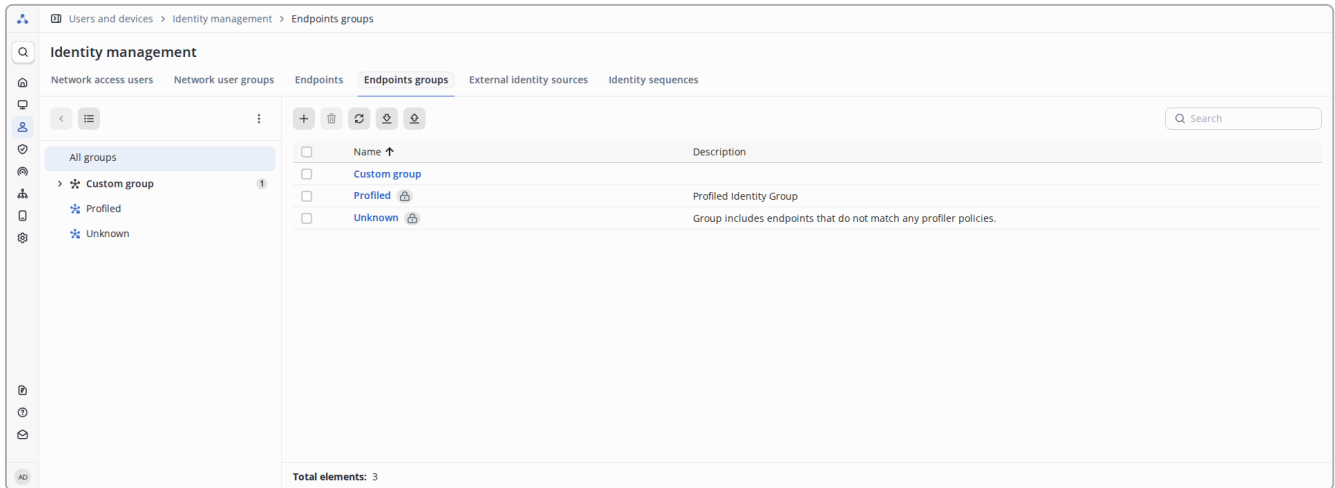


Figure 192. Viewing a list of endpoint groups

The table contains the following columns:

- **Name** - Group Name
 - - This entity is system and cannot be deleted or edited.
- **Description** - Full description of the group

Controls:

- — Add a new element.
- — Delete selected elements (inactive until at least one element is selected).
- — Refresh table data.
- — Allows you to download data from a csv file.
- — Allows you to upload data to a csv file.
- — Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).
- — Change the current sort order.
- **Search** — Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.

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

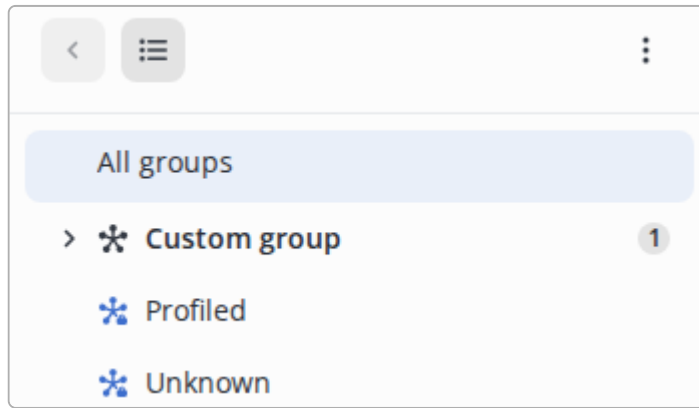


Figure 193. Menu for navigating the endpoint group tree

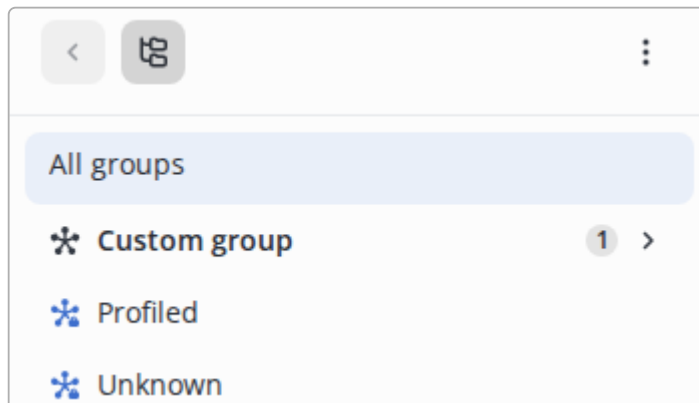







Figure 194. Menu for navigating in "list view mode"

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 195. 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 196. 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:

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



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  .

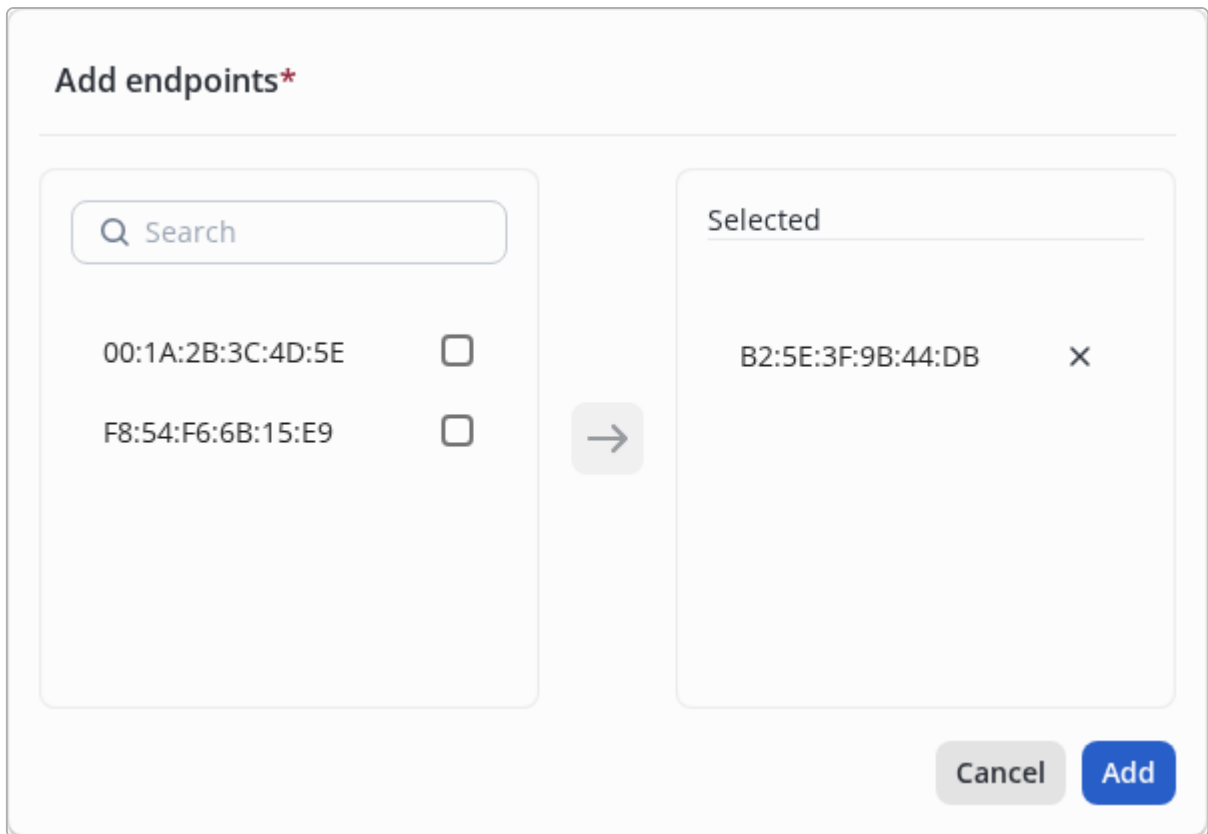



Figure 197. Modal dialog for adding endpoints

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 .

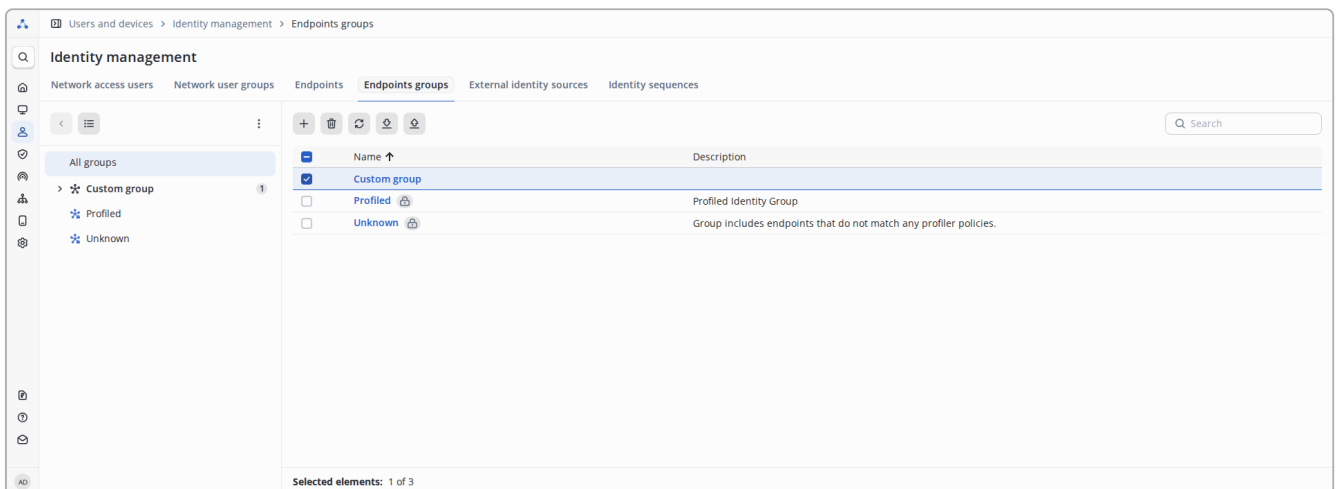


Figure 198. Select groups to delete



Deleting items requires confirmation in the modal window.
The selected items will be deleted only after explicit confirmation of the operation.

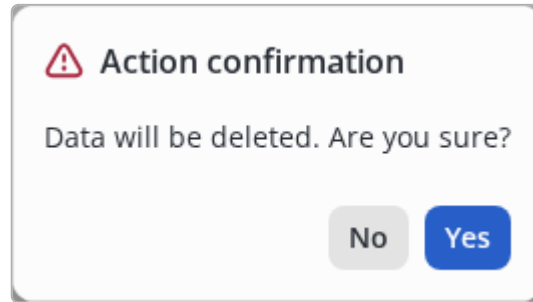


Figure 199. Modal dialog for confirmation



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.

Import

NAICE supports importing data from CSV files.

Preliminary preparation before Import

1. Create or verify the existence of necessary related entities (e.g., device profile).
2. Review the CSV file requirements:
 - Encoding must be UTF-8;
 - Delimiters:
 - Field delimiter: comma (,)
 - String/text delimiter: double quotation mark (")
 - Headers and values must be enclosed in double quotation marks (")
 - Maximum file size is 2MB.
3. Check the file content for extraneous quotation marks before importing;
4. Check that the values containing the double quotation mark (") or the slash (/) are correctly escaped.
 - Values containing a double quotation mark (") are escaped using \
 - Values containing the slash (/) are escaped using \

Correct spelling of values (with escaping using `\`) using the example of the contents of the file for importing the TACACS Command set

"name:Required"	"description"	"permit_unmatched(true/false)"	"commands(Grant/command/arguments/enabled;...)"
"command_set"	"\"Test command set\""	"false"	"PERMIT/\"show/vlan 1 2 \"/true"


Incorrect spelling of values (without escaping) using the example of the contents of the file for importing the TACACS Command set

"name:Required"	"description"	"permit_unmatched(true/false)"	"commands(Grant/command/arguments/enabled;...)"
"command_set"	"Test command set"	"false"	"PERMIT/show/vlan 1 2 /true"



Failure to escape these characters will lead to incorrect data recognition.

Import procedure

To import data from a CSV file, click on  in the action panel located above the table. This will open the import window:

Import

When importing, duplicate data will not be overwritten or edited - the system will skip it. If you want to change old data, delete it from the system manually before importing.

Carefully review the [Documentation](#) to ensure the import completes without errors.

Select a file*
Max file size 2MB

Upload or drag it here

Field is required

Data source *
NAICE

Ignore exist data ⓘ

Stop import on first error

Cancel Import

Figure 200. Window Import

Data import proceeds through several steps:

1. Select the required CSV file by dragging it into the upload area or by selecting it through the file explorer by clicking the **"Upload"**;



To apply changes, you must re-upload an updated CSV file.

2. Select the data source (if not predefined);
3. Configure import flags (if needed):

Ignore exist data

- On: Duplicate records trigger warnings.
- Off: Duplicates are treated as errors.

Stop import on first error

- On: Import halts at the first error. Only records that were successfully processed before it occurred will be imported.
-

Off: Erroneous lines are skipped, and the import continues to the end. Only valid records will be imported.

4. To start the import, click the "**Import**".



When importing, duplicate data will not be overwritten or edited - the system will skip it. If you want to change old data, delete it from the system manually before importing.

Viewing the Import report

An import report window opens immediately after file processing.

If all records in the file were processed correctly, you will see the following window:

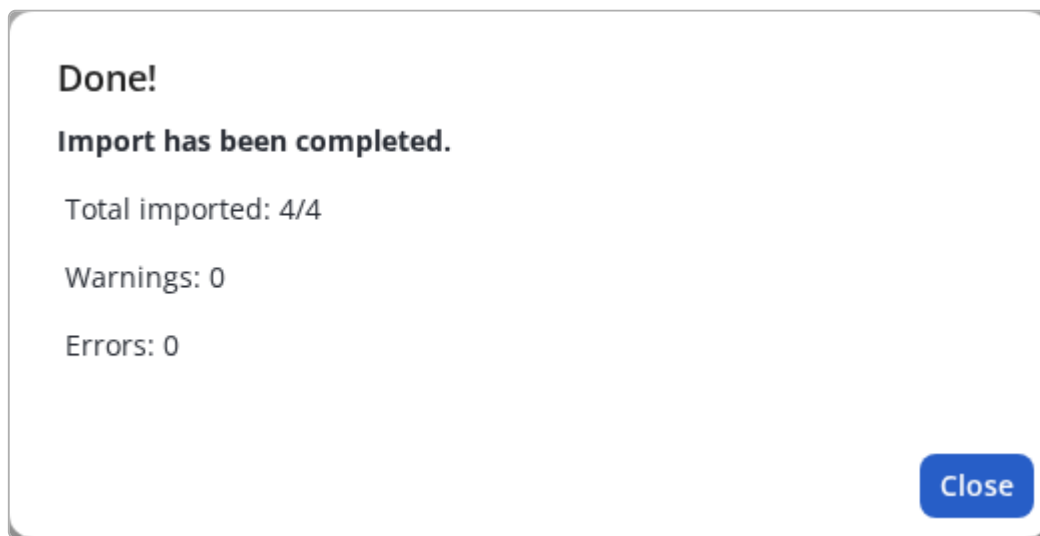


Figure 201. Window Import report (all entries were processed correctly)

The summary block contains:

- **Total Imported** - Counter of records imported (vs. total rows processed);
- **Warnings** - Number of warnings that occurred;
- **Errors** - Number of errors that occurred.

If not all records were processed correctly, you will see the following window:

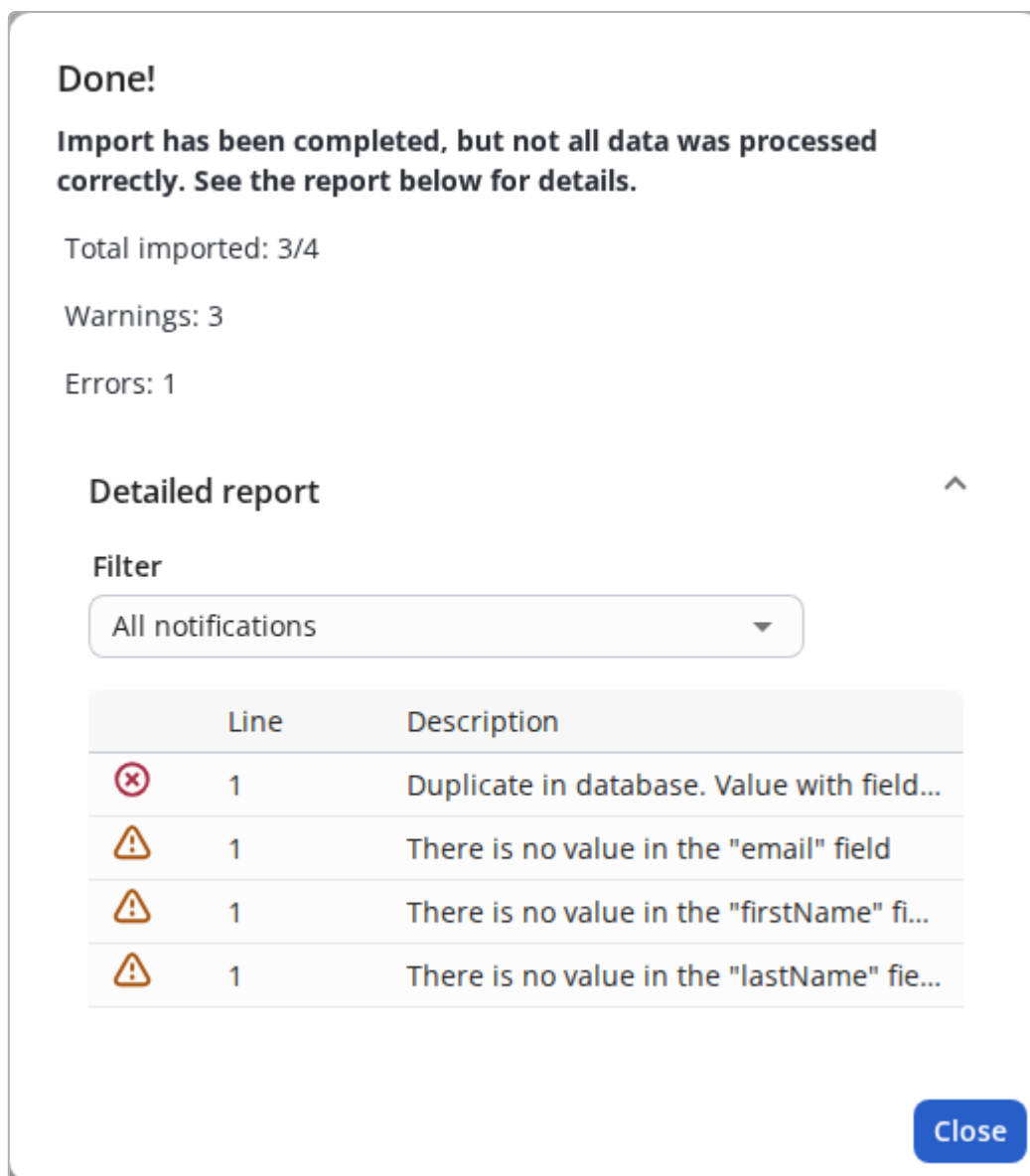


Figure 202. Window Import report (entries processed with errors/warnings)

Detailed report contains the following information:

- **Filter** - Dropdown list allowing you to select which notifications to display (All notifications , Only errors , or Only warnings)

The notification table contains columns:

- **Line** - The line number in the CSV file where an error or warning was detected;
- **Description** - Detailed text explanation of the error or warning.



Hover your cursor over a row in the Description column to view the full error/warning message in a tooltip.

Import particularities for Endpoint groups



For Endpoint groups imports, only the NAICE data source is supported.

The table below lists the fields, their requirements, descriptions, and requirements:

Field	Description	Requirements
name:Required	The name of the group in the format of its full path	Required Format: group#subgroup
description	Free-form description of the group	Maximum length - 200 characters



If there is no intermediate root/child group in the system, it will be created automatically.

Example of correctly formatted file content:

"name:Required"	"description"
"test#test_1"	""

Instructions for obtaining a CSV template file are described later in the "**Export**" section.

Export

NAICE supports exporting data in CSV format. Values and headings are framed by double quotes, the field separator is comma (,).

Export procedure

Two export modes are available:

- **Export all** - Exports all records from the current section. System entities are not included during export.
- **Export selected** - Exports only checked records.

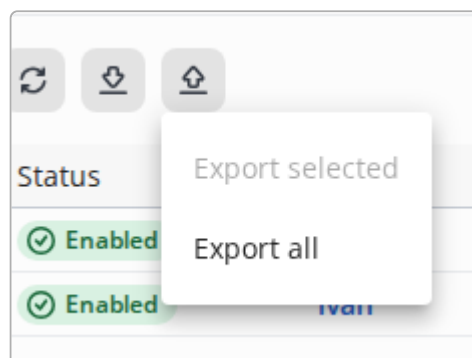



Figure 203. Window export menu



Values containing double quotation marks (") or slashes (/) will be escaped using \".

Export all

On the action panel above the table, click  and select the "**Export all**" mode. In the window that opens, confirm the action by clicking the "**Export**":

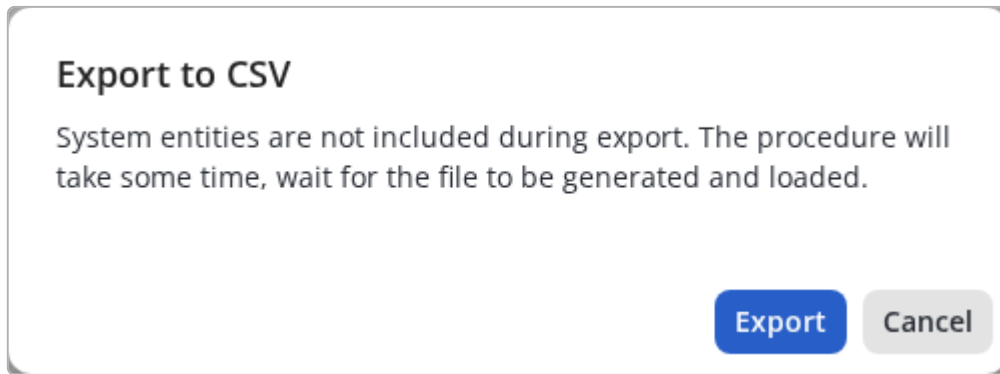



Figure 204. Export all

After clicking the "**Export**", a file containing all records from the current section will be downloaded to your device.

Export selected

On the action panel above the table, click  and select the "**Export selected**" mode. In the window that opens, confirm the action by clicking the "**Export**":

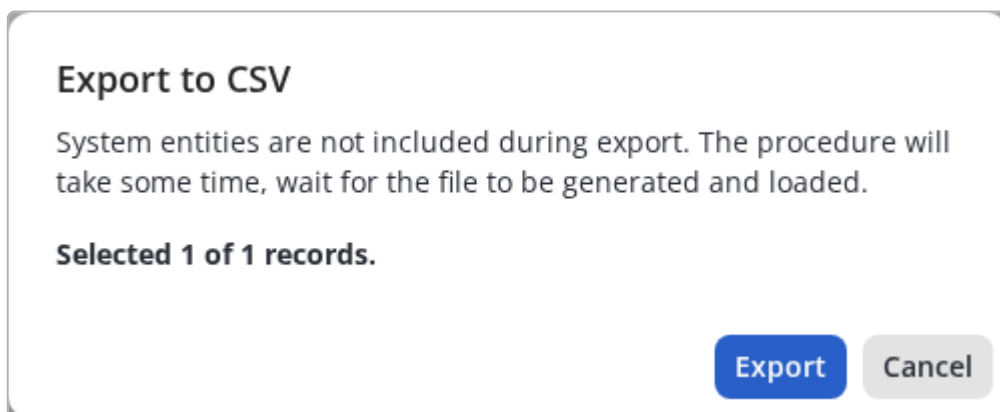


Figure 205. Export selected

After clicking the "**Export**", a file containing only the checked records will be downloaded to your device.



When **opening** CSV files, **always** use a **comma (,)** as the field delimiter. **Double quotation marks (")** or **empty values** may be used as string/text delimiters.

When **saving** CSV files, **always** use a **comma (,)** as the field delimiter, with an **empty value** as the string/text delimiter.



If a double quotation mark (") was used as the line delimiter when opening the file, values containing double quotation marks (") or slashes (/), escaped as \", may receive an extra quotation mark (") upon saving. Please check the file in a text editor and remove any extra quotation marks if they appear.

Template

If there are no records in the table (or only system entities are present), selecting the "**Export all**" mode will generate a CSV file containing only the column headers. This file can be used as a **template** for preparing data prior to import.

Export particularities for Endpoint Groups



The name of the endpoint group will be recorded in the format of its full path using the separator - #.

The structure of the CSV file for device groups is described in the section "[Import particularities for Endpoint groups](#)".

External identity sources

Description

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

External identity sources can be used in NAICE:

- **For system user (administrator) authentication** - an external identity source can be configured **as the primary authentication source on the [System Log In page](#)**. System users will be able to log in to the NAICE web interface using their enterprise accounts, and their data (name, surname, email) will be automatically pulled from directory attributes.
- **For network user authentication** - an external source is used when configuring [access policies](#). Users authenticate on network equipment through an external directory, and their attributes and groups can be used in conditions and authorization profiles.

In this section, you configure connections to external sources and add user groups and/or attributes that can later be used when configuring [RADIUS policies](#), [Network devices policies](#), and when configuring [external roles](#).

View external identity sources

Name ↑	Type	Description
LDAP	LDAP	OpenLDAP
MS AD	LDAP	MS Active Directory

Figure 206. 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:

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



Interaction with identification sources such as "Microsoft Active Directory" and "OpenLDAP" 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 NAICE.

- The user and computer accounts must have a password.



If redundant installation is used, a separate computer account must be added for each NAICE node for proper interaction with Active Directory. The service user account will be the same for all NAICE nodes.

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
```



- After the command is run, enter the password twice in the terminal.

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	Appointment	Note
UDP	53	DNS	The server responsible for resolving domain names can be separate from the Active Directory server
TCP/UDP	389	LDAP	No encryption of transmitted data, searching within the specified local domain
TCP/UDP	636	LDAPS	Used for secure connection with encryption of transmitted data, searched within the specified local domain

TCP/UDP	3268	LDAP GC	No encryption of transmitted data, searched the entire Active Directory domain forest
TCP/UDP	3269	LDAPS GC	Used for secure connection with encryption of transmitted data, searched the entire Active Directory domain forest
TCP/UDP	49152-65535	RPC Dynamic Port Range	Used to verify user password during authentication in Active Directory, encryption of transmitted data is used

Implementation limitations

There are the following limitations to implementing Active Directory interoperability:

- Users, their attributes, and groups can only be searched within a single Active Directory global catalog.
- Within the local domain specified in the settings, the username on the client device can be entered in the following formats:
 - <login>, without specifying a domain (when accessing Active Directory, the domain will be added automatically).
 - UPN: <login>@<FQDN domain> or pre-Windows 2000 format: <DOMAIN NAME >\<login>.
- If the user belongs to a different Active Directory global catalog domain (than specified in the local domain settings), the username must be specified on the client device in UPN format: <user>@<FQDN domain>.
- If the username has a prefix other than Active Directory domain, only UPN format must be used: <login>@<domain prefix>.
- Only Latin characters, numbers, punctuation are allowed in usernames and passwords.
- It is allowed to use user groups that contain a user not directly, but through the inclusion of another group containing a user.
- A user group that is specified in Active Directory as **Primary Group** cannot be used because it is not returned in the list of user groups when searching for them in Active Directory.

Adding an identity source

To add an identification source, click  on the action bar above the table:


Figure 207. 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 63 characters.
 - **Description** - description. The maximum field length is 200 characters.
 - **Enable LDAPS** - Enables the use of a secure connection to the directory service via the LDAPS (LDAP over TLS) protocol, which ensures encryption of transmitted data and verification of the server certificate. Certificates of the service must be uploaded to the [trusted certificates](#) store. When this option is enabled, the additional option **Trust unknown sources** becomes available.
 - **Trust unknown sources** - Available only when **Enable LDAPS** is activated. Allows connection to the directory service via the LDAPS protocol using an **untrusted** or **unknown** certificate.

Figure 208. Enabling the "Enable LDAPS" option

- 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.
 - **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.

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),
- cyrillic letters (a-я)(A-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

- Block **Computer accounts** - available only for the "ACTIVE_DIRECTORY" scheme. This block configures computer accounts for interaction with Active Directory individually for each NAICE node. Computer names in the list must not be duplicated.
 - **Hostname** - dropdown list with available NAICE nodes. Select the node for which the computer account is being configured.
 - **Computer name** - the computer name that NAICE will use to connect to Active Directory. Allowed characters: Latin letters, numbers, hyphen. Maximum length: 63 characters. The name must be unique within the list.
 - **Password** - computer account password. Not displayed by default, to view it you need to click . The maximum field length is 200 characters.

To add an entry, fill in the **Hostname**, **Computer name**, **Password** fields and click the **Add** button. The entry will appear in the **List of accounts** table.

The **List of accounts** table contains the following columns:

- **Hostname** - NAICE node name.
- **Computer** - computer account name.

Actions - account action menu, which opens by clicking on  :

- **Edit** - opens the account editing dialog. The hostname, computer name, and password of the computer account can be changed.
- **Delete** - removes the account from the list.



For the "ACTIVE_DIRECTORY" scheme, at least one computer account must be added.

- **Check connection** - check the correctness of the settings and connection to the Active Directory server.

Parameters marked with an asterisk * are required.

- Block **Matching information about system users** - configuration for mapping attributes from the external source to NAICE system user account fields:
 - **First name attribute** - attribute whose value will be inserted into the **Name** field of the external account.
 - **Last name attribute** - attribute whose value will be inserted into the **Last name** field.
 - **Email attribute** - attribute whose value will be inserted into the **Email** field.



For the "ACTIVE_DIRECTORY" schema, the attribute fields are populated automatically:

- Name attribute - givenName attribute.
- Last name attribute - sn attribute.
- Email attribute - mail attribute.



If attributes in the directory for a user are not populated, the corresponding account fields will remain empty.

If attributes are specified in the settings but are missing for a specific user in the directory, when checking the connection with the server, even if the connection to the server is successful, an error like this will be returned: Unable to find the "mail" field for the users.

After filling in all the necessary data, the "**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:

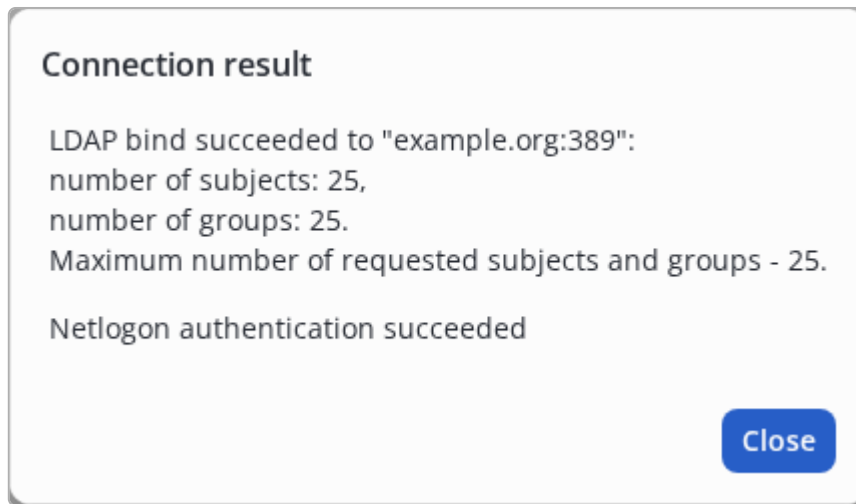


Figure 209. LDAP binding successful



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



For network user authentication through an external identity source, adding groups is not required.

Groups can be used in user authorization policies.



To use an external source for system user (administrator) authentication on the [System Log In](#) page, **adding groups is mandatory**.

Without groups, it is impossible to configure external roles. In the absence of external roles, system login is impossible - an error "You have no privileges" will be returned.

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:

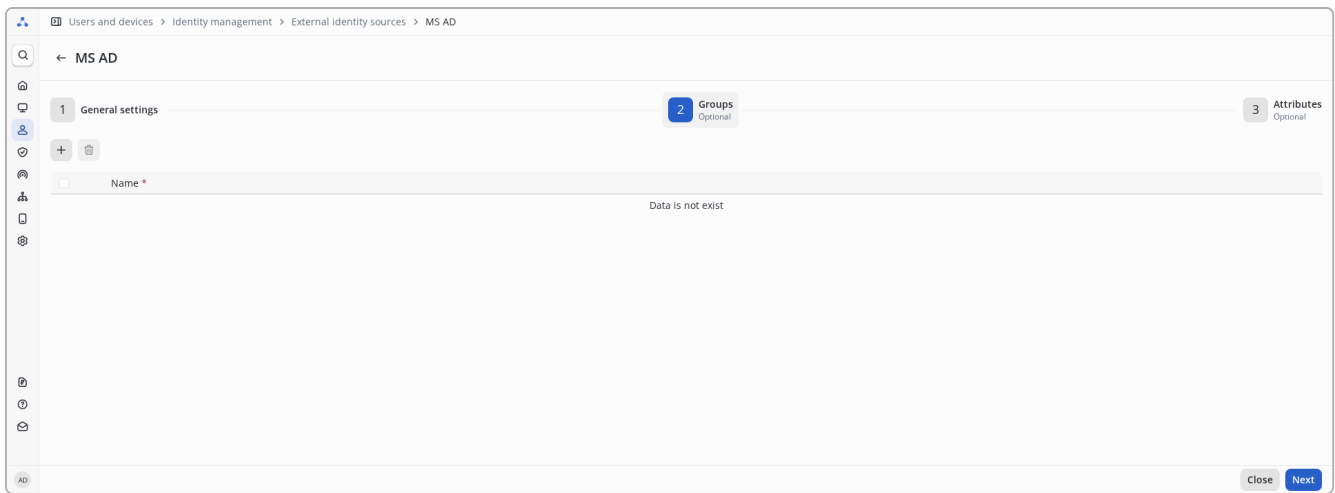


Figure 210. Empty group table

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).

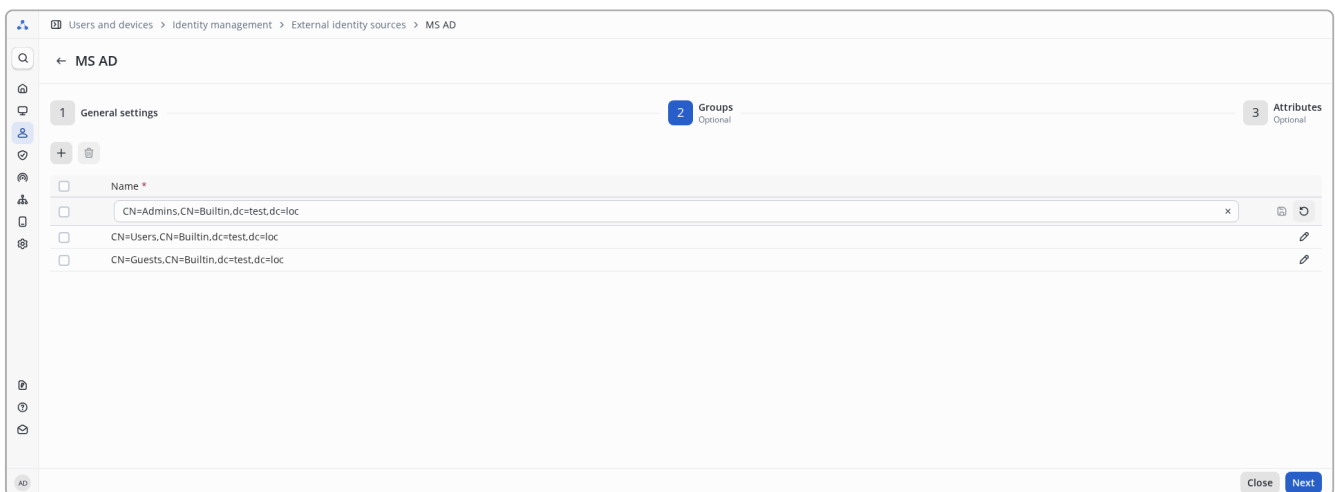


Figure 211. Group table in edit mode

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

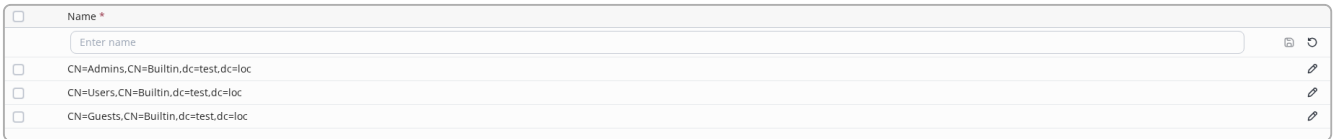


Figure 212. Add new group

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

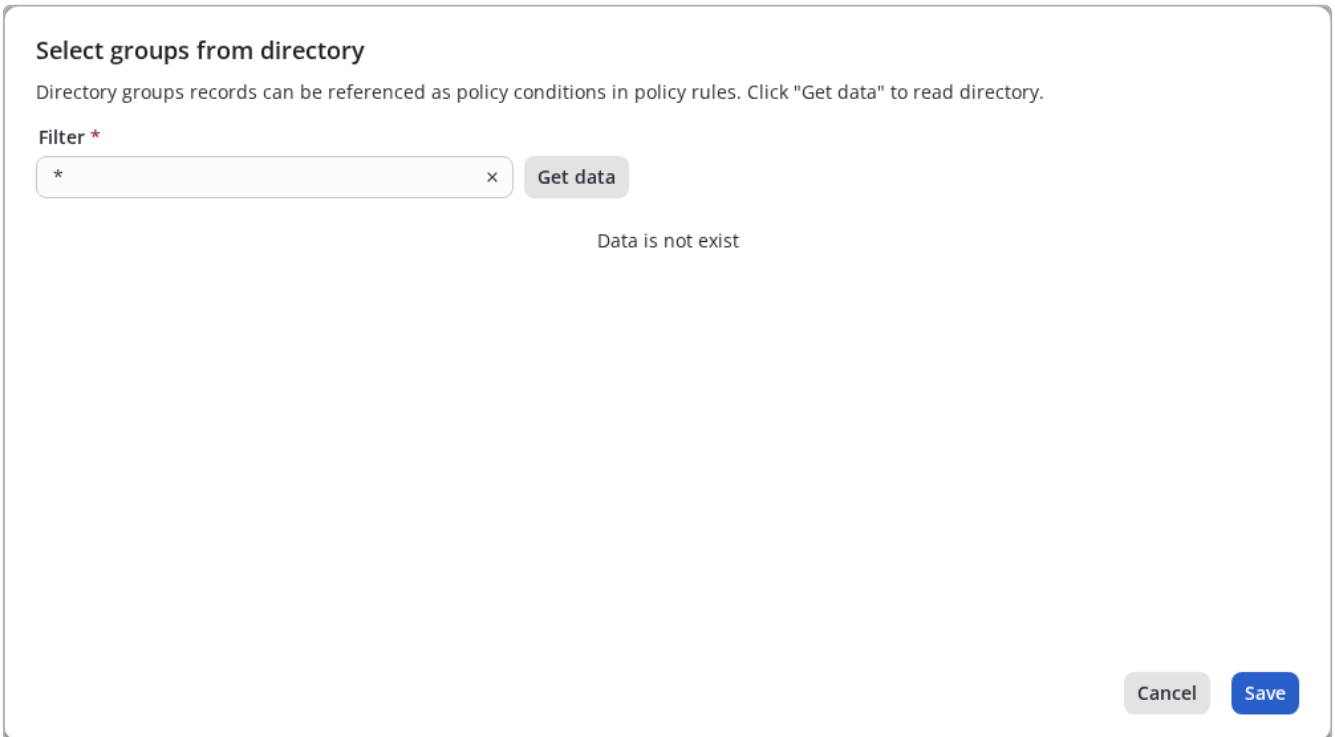


Figure 213. Group selection window

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

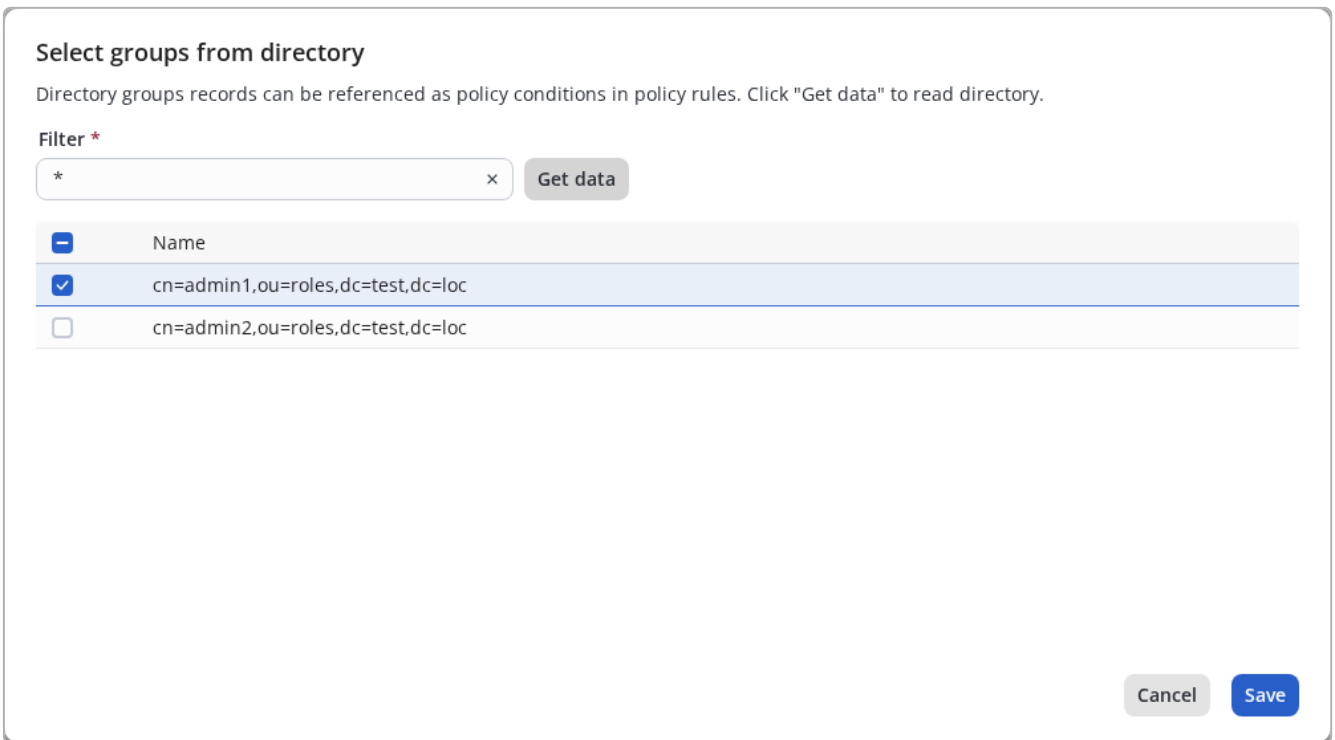


Figure 214. Group selection window after receiving data

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:

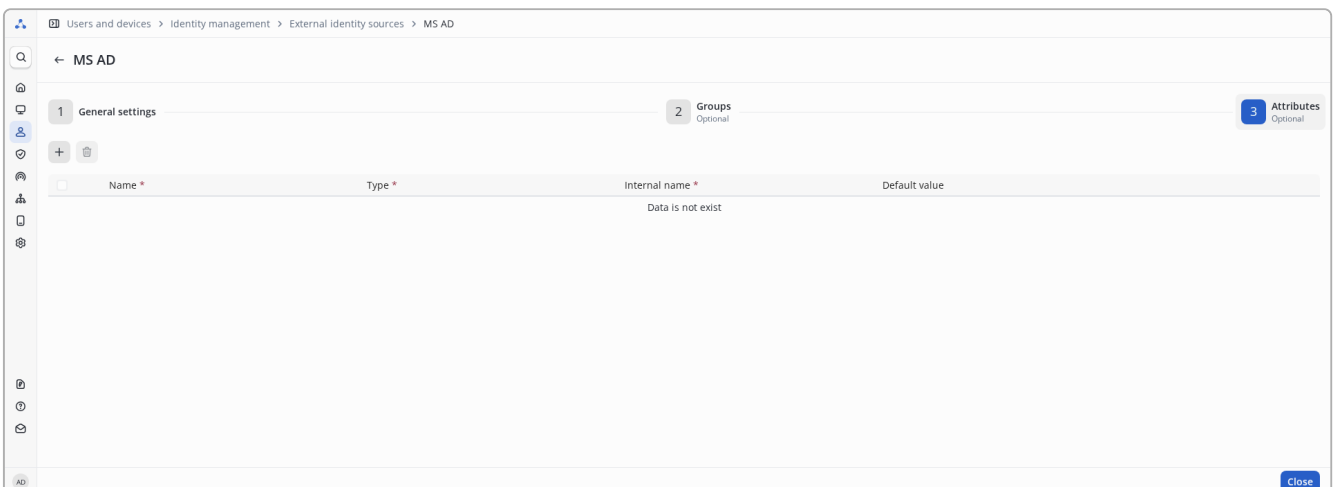






Figure 215. Adding attributes

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).

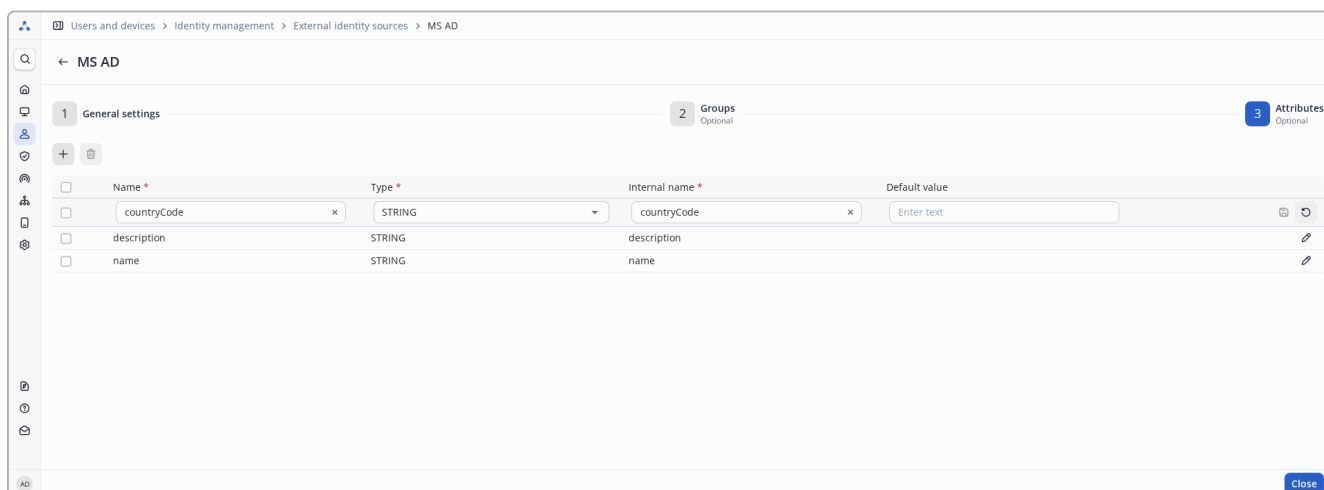


Figure 216. Attribute table in edit mode

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

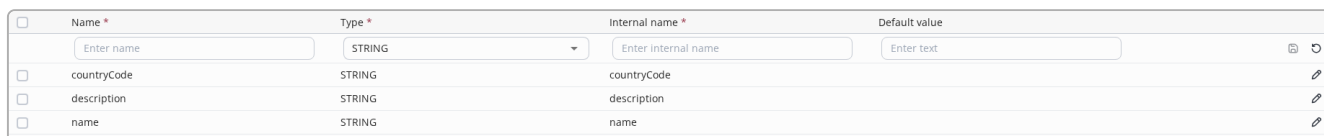


Figure 217. Add new attribute

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

Select attributes from directory

Directory attributes of records can be referenced as policy conditions in policy rules. If you wish to do this, define the attributes that are to be available for use in policy rules here. Attributes are retrieved by specifying in filter an "attribute=value". A representative pair "attribute=value" should be entered into the 'Filter' field. For example "cn=*" or "objectClass=person" & etc. When 'Get data' is clicked, the example's attributes will be retrieved. The attribute definitions selected will be added to the Dictionary for this Identity Store. Note that the values for attributes selected will be visible in sessions logs when corresponding requests are processed. Note that the Default Values will be used only if value not present in the directory answer. It is recommended to specify a certain username that contains the attributes you are looking for and their values, because otherwise, the attributes may not appear in search results.

Filter *

Data is not exist

Figure 218. 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:

Select attributes from directory

Directory attributes of records can be referenced as policy conditions in policy rules. If you wish to do this, define the attributes that are to be available for use in policy rules here. Attributes are retrieved by specifying in filter an "attribute=value". A representative pair "attribute=value" should be entered into the 'Filter' field. For example "cn=*" or "objectClass=person" & etc. When 'Get data' is clicked, the example's attributes will be retrieved. The attribute definitions selected will be added to the Dictionary for this Identity Store. Note that the values for attributes selected will be visible in sessions logs when corresponding requests are processed. Note that the Default Values will be used only if value not present in the directory answer. It is recommended to specify a certain username that contains the attributes you are looking for and their values, because otherwise, the attributes may not appear in search results.

Filter * Get data

<input checked="" type="checkbox"/> Name	Type	Example value
<input checked="" type="checkbox"/> isCriticalSystemObject	STRING	TRUE
<input checked="" type="checkbox"/> uSNCreated	INTEGER	56123

Cancel
Save

Figure 219. 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.

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.

Adding an identity source


To add an identification source, click on the action bar above the table, after which the following page will open, where you will need to select the `CUSTOM` scheme:

The screenshot shows a web-based configuration interface for adding an external identity source. The interface is organized into a multi-step process, with the first step, 'General settings', currently active. The form contains several sections: a top section for basic identification (Name, Description, Enable LDAPs), a middle section for schema and connection details (Schema dropdown set to 'CUSTOM', Admin dn, Admin password, Hostname/IP, Port, Subject search base, Group search base), and a bottom section for user system matching (radio buttons for reference types, and fields for First name, Last name, and Email attributes). A 'Check connection' button is located at the bottom left, and 'Cancel' and 'Add' buttons are at the bottom right.

Figure 220. Window for adding identification source

This form provides the following parameters:

- Block **Basic settings**:
 - `Name *` - name of the identification source.
 - `Description` - description.
- Block **Schema**:
 - `Select schema *` - 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:
 - When **Groups contain users** is selected - this is a group attribute that contains references to its members.
 - When **Users contain groups** is selected - this is a user attribute that contains references to groups they belong to.
- Subject in group attribute * - specifies the format (attribute) in which users or groups are listed in the Group map attribute .
- 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 (the default port is 389 for an unsecured connection or 636 for a secure connection).
- Block **Catalogue structure**:
 - Subject search base * - context for searching users (subjects) 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, the Hostname/IP field is 255 characters, and other fields are 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),
- cyrillic letters (a-я)(A-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

- Block **Matching information about system users** - configuration for mapping attributes from the external source to NAICE system user account fields:
 - **First name attribute** - attribute whose value will be inserted into the **Name** field of the external account.
 - **Last name attribute** - attribute whose value will be inserted into the **Last name** field.
 - **Email attribute** - attribute whose value will be inserted into the **Email** field.



Fields are **optional**. If attributes are not specified or are not populated in the directory for a user, the corresponding account fields will remain empty.

If attributes are specified in the settings, but they are missing from the directory for the found users, a warning similar to the following will be returned when checking the connection to the server: **Unable to find the "mail" field for the users.**

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

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

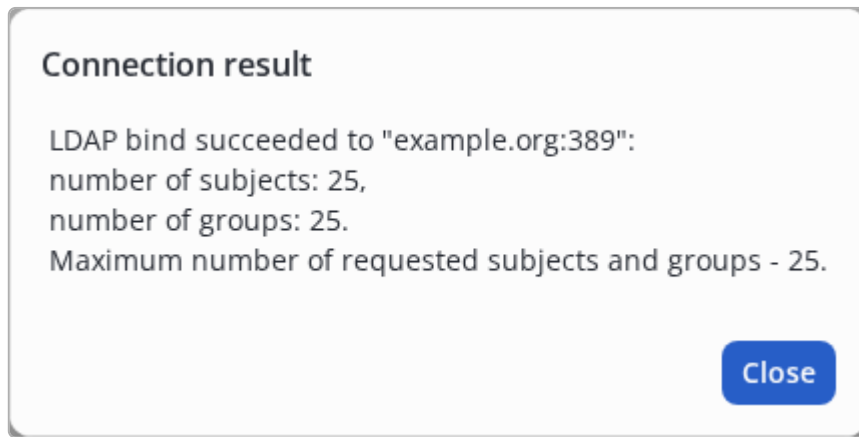


Figure 221. LDAP binding successful



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



For network user authentication through an external identity source, adding groups is not required.

Groups can be used in user authorization policies.



When using an external source for system user (administrator) authentication on the [System Log In](#) page, **adding groups is mandatory**.

Without groups, it is impossible to configure external roles. In the absence of external roles, system login is impossible - an error "You have no privileges" will be returned.

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:

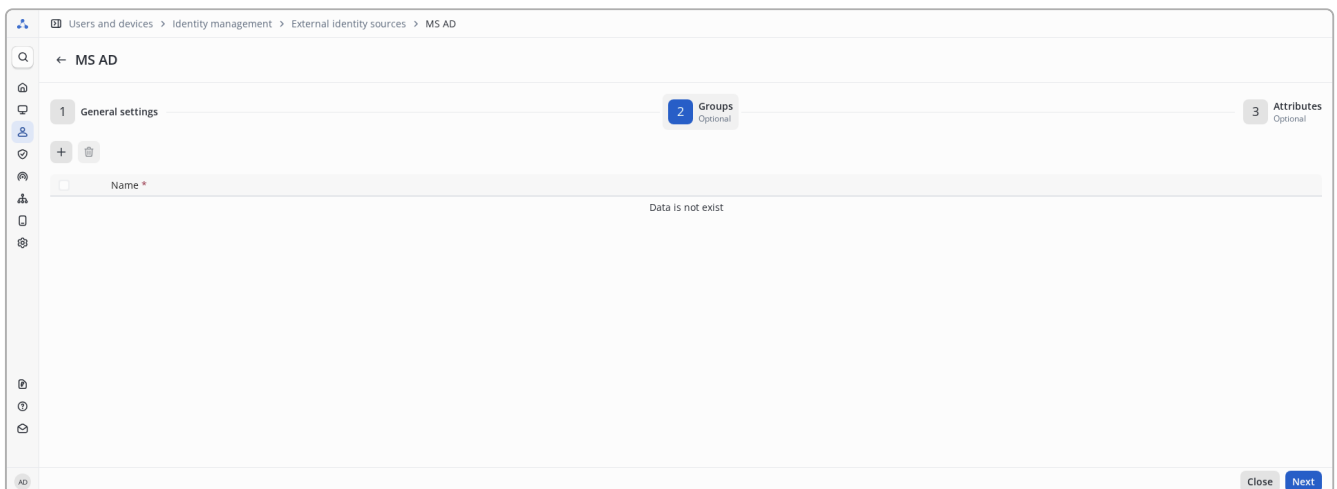


Figure 222. Empty group table

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

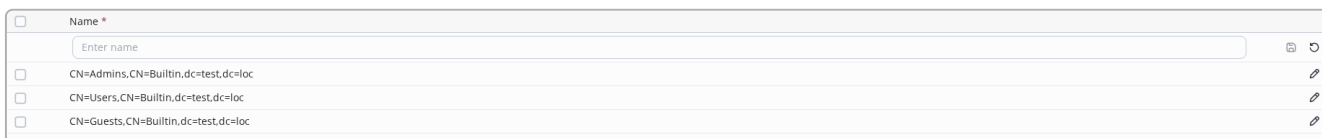


Figure 223. Add new group

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



Group search is performed using the DN (Distinguished Name) attribute to differentiate groups with the same name in different branches of the directory service tree. If the schema uses a different attribute for the **Group name attribute**, the group search query may be executed incorrectly. In such a case, adding a new group should be performed manually.

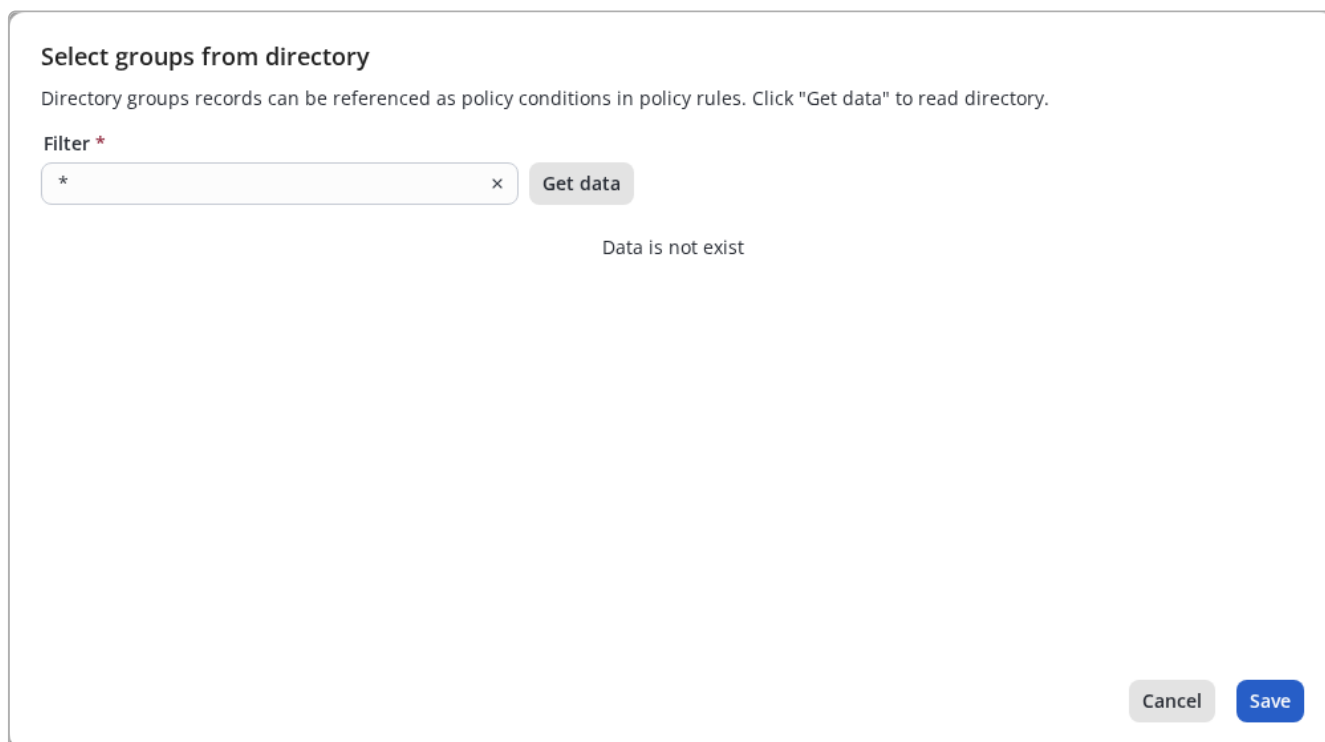


Figure 224. Group selection window

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.

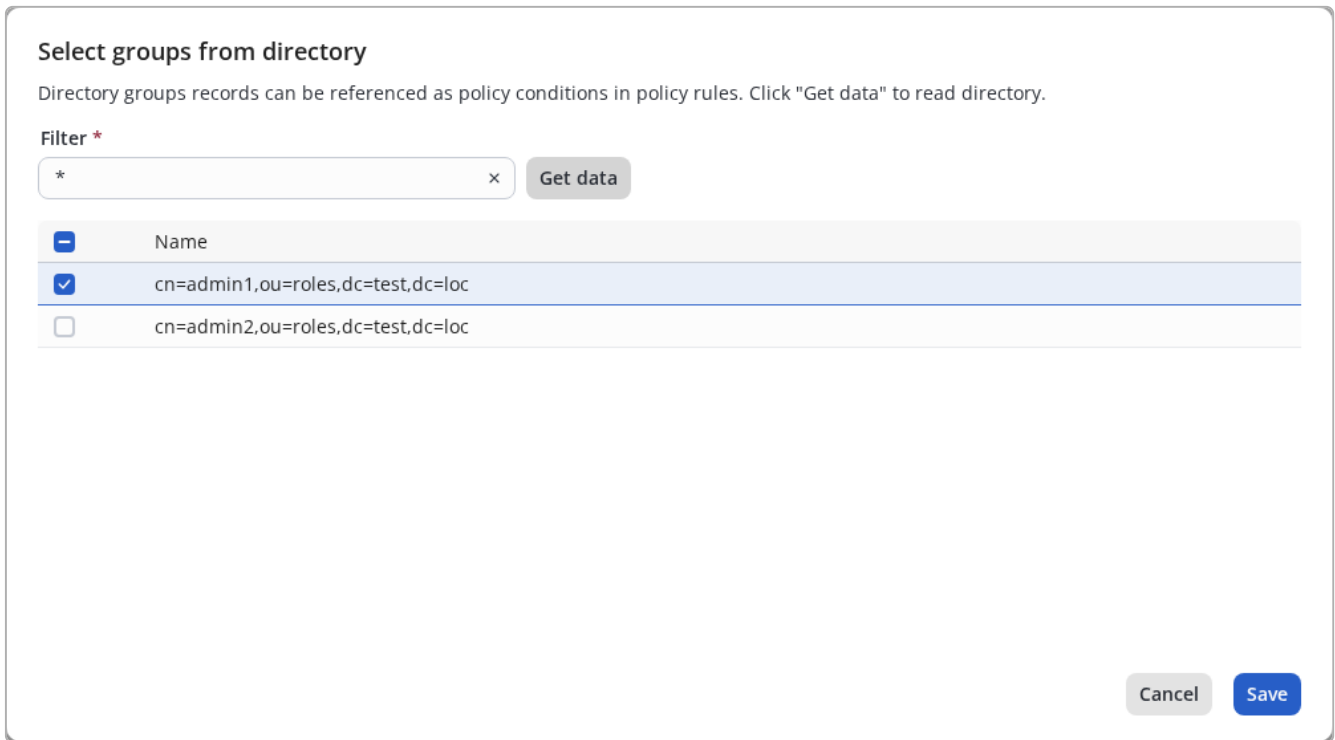


Figure 225. Group selection window after receiving data

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:

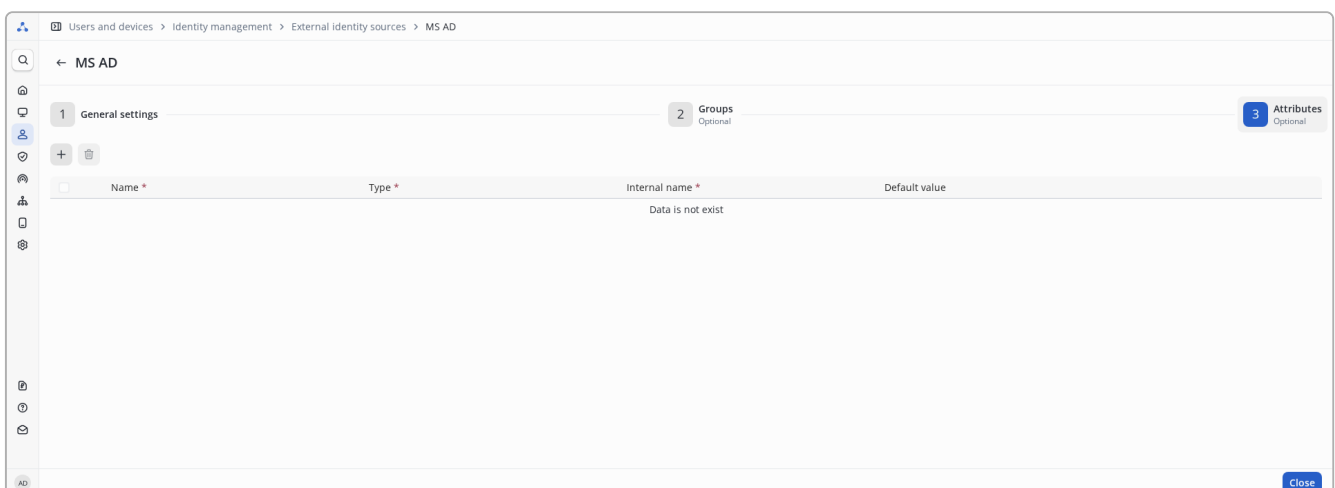




Figure 226. Adding attributes

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






<input type="checkbox"/>	Name *	Type *	Internal name *	Default value	
<input type="checkbox"/>	<input type="text" value="Enter name"/>	STRING	<input type="text" value="Enter internal name"/>	<input type="text" value="Enter text"/>	 
<input type="checkbox"/>	countryCode	STRING	countryCode		
<input type="checkbox"/>	description	STRING	description		
<input type="checkbox"/>	name	STRING	name		

Figure 227. 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

Select attributes from directory

Directory attributes of records can be referenced as policy conditions in policy rules. If you wish to do this, define the attributes that are to be available for use in policy rules here. Attributes are retrieved by specifying in filter an "attribute=value". A representative pair "attribute=value" should be entered into the 'Filter' field. For example "cn=*" or "objectClass=person" & etc. When 'Get data' is clicked, the example's attributes will be retrieved. The attribute definitions selected will be added to the Dictionary for this Identity Store. Note that the values for attributes selected will be visible in sessions logs when corresponding requests are processed. Note that the Default Values will be used only if value not present in the directory answer. It is recommended to specify a certain username that contains the attributes you are looking for and their values, because otherwise, the attributes may not appear in search results.

Filter *

Data is not exist

Figure 228. 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:

Select attributes from directory

Directory attributes of records can be referenced as policy conditions in policy rules. If you wish to do this, define the attributes that are to be available for use in policy rules here. Attributes are retrieved by specifying in filter an "attribute=value". A representative pair "attribute=value" should be entered into the 'Filter' field. For example "cn=*" or "objectClass=person" & etc. When 'Get data' is clicked, the example's attributes will be retrieved. The attribute definitions selected will be added to the Dictionary for this Identity Store. Note that the values for attributes selected will be visible in sessions logs when corresponding requests are processed. Note that the Default Values will be used only if value not present in the directory answer. It is recommended to specify a certain username that contains the attributes you are looking for and their values, because otherwise, the attributes may not appear in search results.

Filter *

<input checked="" type="checkbox"/>	Name	Type	Example value
<input checked="" type="checkbox"/>	isCriticalSystemObject	STRING	TRUE
<input checked="" type="checkbox"/>	uSNCreated	INTEGER	56123

Figure 229. 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!

Editing Identity Source

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

<input type="checkbox"/>	Name ↑
<input type="checkbox"/>	LDAP
<input type="checkbox"/>	MS AD

Figure 230. Hyperlink to external identity source edit page

The editing page will open, similar to the add page:

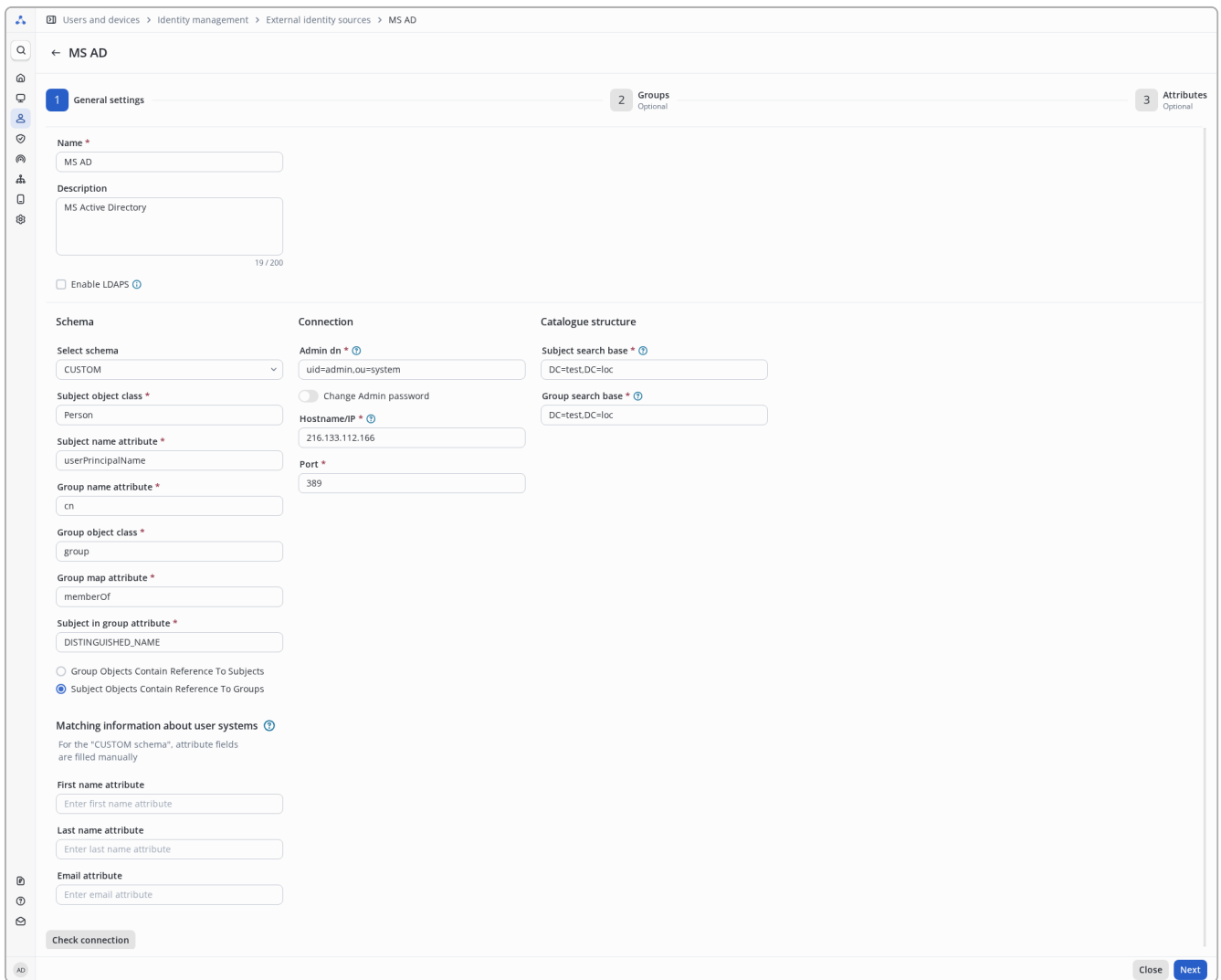



Figure 231. Identity source editing page

To change the Admin password, activate the toggle "Change Admin password", and then enter the desired password in the appropriate field. To change the computer account password, click **Edit** in the **Actions** column of the **List of accounts** table, activate the **Change password** toggle, and enter the new password.

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

The "Cancel" button resets the changes made to their original state.

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  on the action bar above the table.

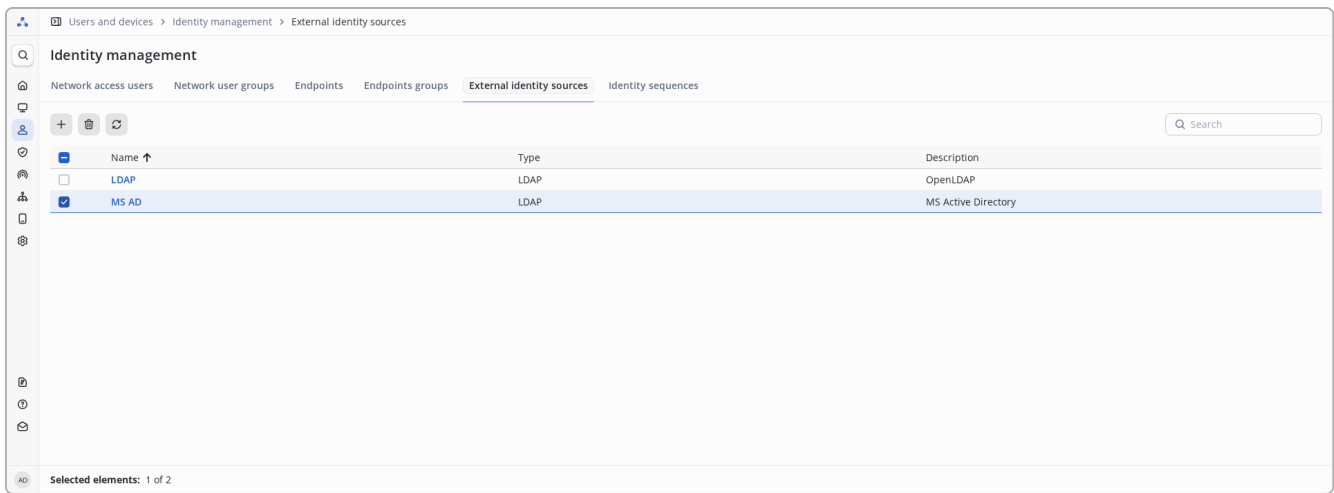


Figure 232. Selecting sources to delete



When deleting an external source, all external user accounts obtained from this source will also be deleted.

Deleting an external source requires confirmation:

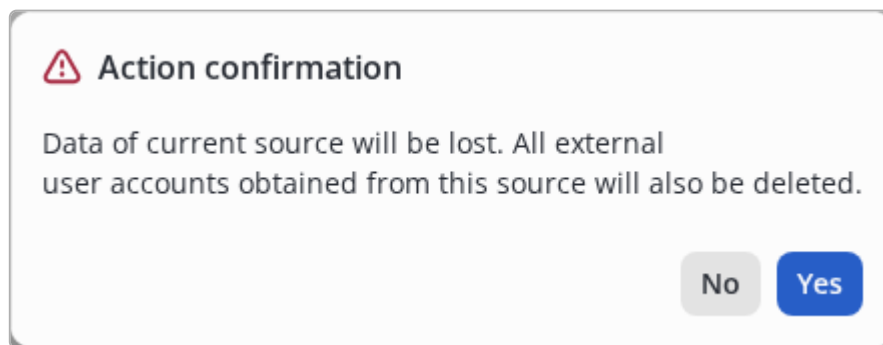


Figure 233. External source deletion confirmation

Identity sequences



Some functional described on this page are only available with an extended license. These features are marked with special labels in the form of colored icons next to the name.

Description

Identity sequences (identity source chains) are used in authentication policies when configuring [RADIUS policies](#) and [Network devices policies](#). They define in which sources and in what order to search for users during authentication.

Supported identity sources include [the internal user database](#) and [external identity sources](#), such as MS AD and OpenLDAP.

ADVANCED

For portal authorization, [Portal](#) and [Guest endpoint](#) sources are additionally used as identity sources.

View identity sequences

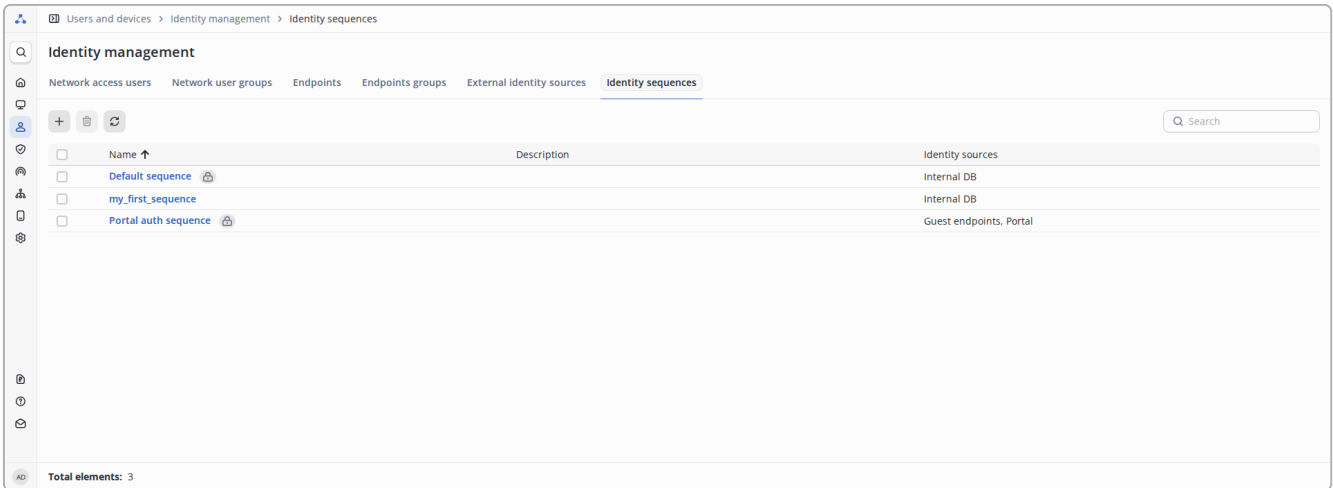



Figure 234. View identification sequences






This page contains a table listing all identity sources.

The table contains columns:

- **Name** - the name of the sequence.
 -  - This entity is system and cannot be deleted or edited.
- **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:

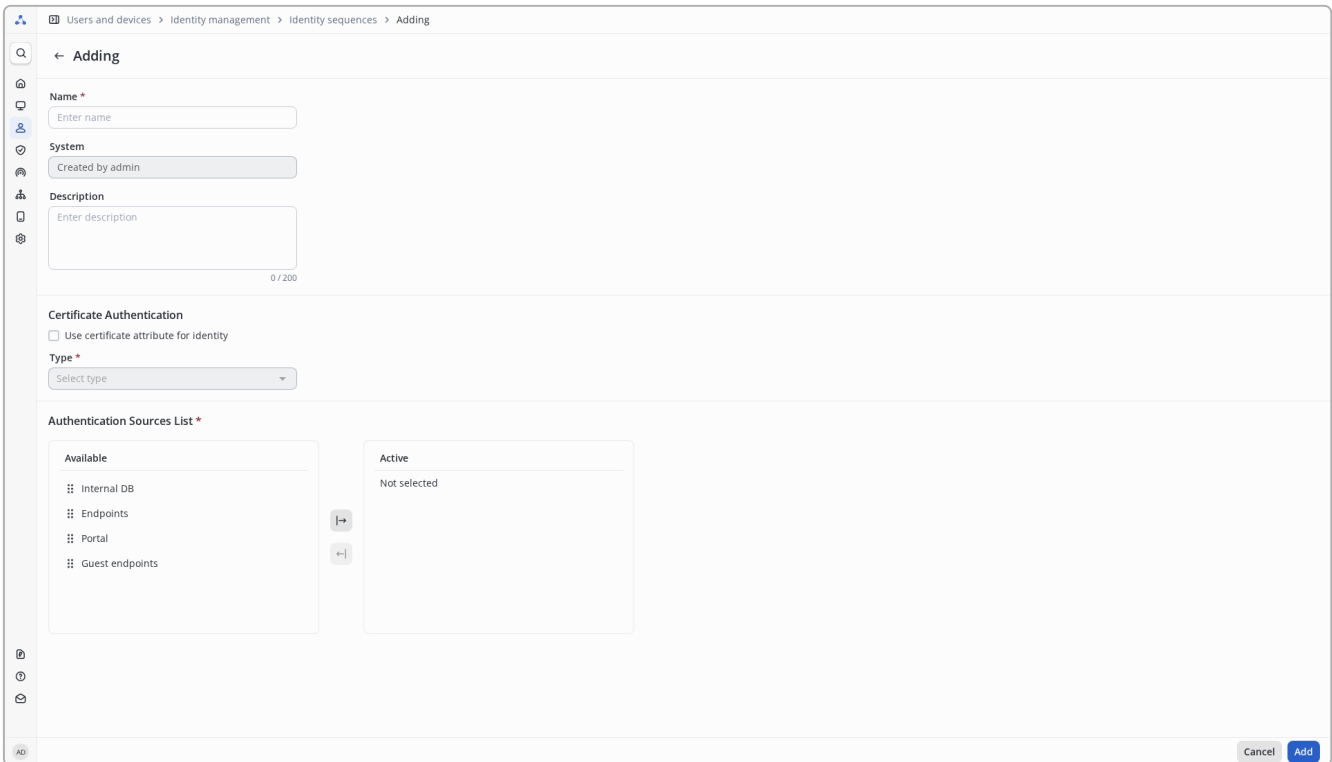
-  — Add a new element.
-  — Delete selected elements (inactive until at least one element is selected).
-  — Refresh table data.
- — Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).
-  — Change the current sort order.
-  **Search** — Performs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



Identity sequences "[Default sequence, Portal auth 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:



The screenshot shows the 'Adding' page for an identity sequence. The breadcrumb trail is 'Users and devices > Identity management > Identity sequences > Adding'. The page has a search bar and a back arrow. The main form includes:

- Name ***: A text input field with the placeholder 'Enter name'.
- System**: A dropdown menu with 'Created by admin' selected.
- Description**: A text area with the placeholder 'Enter description' and a character count '0 / 200'.
- Certificate Authentication**: A checkbox 'Use certificate attribute for identity' (unchecked) and a dropdown menu 'Type *' with 'Select type' selected.
- Authentication Sources List ***: Two columns, 'Available' and 'Active'. The 'Available' column contains 'Internal DB', 'Endpoints', 'Portal', and 'Guest endpoints'. The 'Active' column contains 'Not selected'. There are '+' and '-' buttons between the columns.

At the bottom right, there are 'Cancel' and 'Add' buttons.

Figure 235. 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.





Some sources may not be available depending on your current license type.

- `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.



<input type="checkbox"/>	Name ↑
<input type="checkbox"/>	Default sequence 
<input type="checkbox"/>	my_first_sequence
<input type="checkbox"/>	Portal auth sequence 

Figure 236. Column Title


The editing page will open.

The screenshot shows the editing interface for an identity sequence named 'my_first_sequence'. The breadcrumb navigation is 'Users and devices > Identity management > Identity sequences > my_first_sequence'. The page title is '← my_first_sequence'. The form includes fields for 'Name *' (containing 'my_first_sequence'), 'System' (containing 'Created by admin'), and 'Description' (with a '0 / 200' character count). Below these is the 'Certificate Authentication' section with a checkbox 'Use certificate attribute for identity' and a 'Type *' dropdown menu. The 'Authentication Sources List *' section is divided into 'Available' and 'Active' columns. The 'Available' column contains 'Endpoints', 'Portal', and 'Guest endpoints'. The 'Active' column contains 'Internal DB'. There are bidirectional arrows between the columns and a plus-minus button below them. A sidebar on the left contains navigation icons, and the bottom status bar shows 'AD'.

Figure 237. 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 .

The screenshot shows the 'Identity management' interface with the 'Identity sequences' tab selected. The breadcrumb navigation is 'Users and devices > Identity management > Identity sequences'. The page title is 'Identity management'. The navigation menu includes 'Network access users', 'Network user groups', 'Endpoints', 'Endpoints groups', 'External identity sources', and 'Identity sequences'. A search bar is present in the top right. The table below has columns for 'Name', 'Description', and 'Identity sources'. The 'my_first_sequence' row is selected, indicated by a checked checkbox and a blue background. The status bar at the bottom shows 'Selected elements: 1 of 3'.

Name	Description	Identity sources
<input type="checkbox"/> Default sequence		Internal DB
<input checked="" type="checkbox"/> my_first_sequence		Internal DB
<input type="checkbox"/> Portal auth sequence		Guest endpoints, Portal

Figure 238. Selecting sequences to delete



Deleting items requires confirmation in the modal window. The selected items will be deleted only after explicit confirmation of the operation.

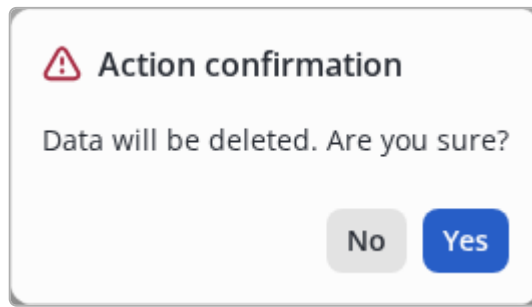


Figure 239. Modal dialog for confirmation



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 access

Policy elements

Authorization profiles



Some functional described on this page are only available with an extended license. These features are marked with special labels in the form of colored icons next to the name.

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).
- Web redirection URL and pre-auth ACL.
- Another RADIUS attributes via Advanced Attribute Settings

Viewing a list of available authorization profiles

The screenshot shows a web interface for managing network access policy elements. The breadcrumb path is "Network access > Policy elements > Authorization profiles". The page title is "Policy elements". There are tabs for "Authorization profiles", "Allowed protocols", "Conditions", and "Dictionaries". The "Authorization profiles" tab is active. Below the tabs are icons for adding, deleting, and refreshing. A search bar is present. The main content is a table with the following data:

<input type="checkbox"/>	Name ↑	Device Profile	Description
<input type="checkbox"/>	DenyAccess	DEFAULT	
<input type="checkbox"/>	MES auth	Eltex MES	
<input type="checkbox"/>	PermitAccess	DEFAULT	
<input type="checkbox"/>	Portal web redirect profile	Eltex WLC	

Total elements: 4







Figure 240. 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.

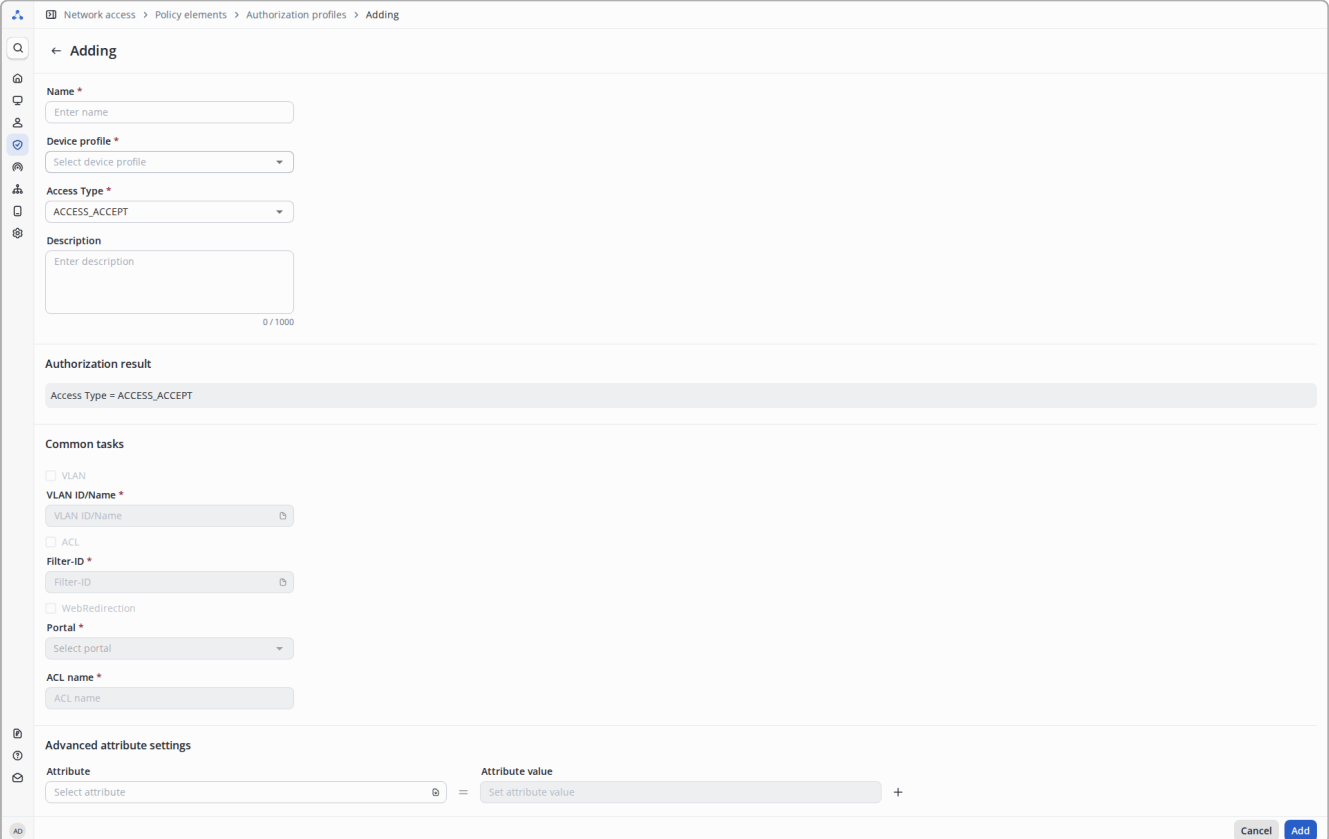
You can sort in forward and reverse order by any column. By default, sorting is performed in direct (alphabetical) order by the "Name" column.

Controls:

-  — Add a new element.
-  — Duplicate chosen element. Becomes active if only one element in the list is selected.
-  — Delete selected elements (inactive until at least one element is selected).
-  — Refresh table data.
- — Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).
-  — Change the current sort order.
-  Search — Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.

Adding an authorization profile

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



The screenshot shows a web interface for adding an authorization profile. The breadcrumb path is "Network access > Policy elements > Authorization profiles > Adding". The form includes the following sections:

- Name ***: A text input field with a placeholder "Enter name".
- Device profile ***: A dropdown menu with a placeholder "Select device profile".
- Access Type ***: A dropdown menu with the value "ACCESS_ACCEPT".
- Description**: A text area with a placeholder "Enter description" and a character count "0 / 1000".
- Authorization result**: A section showing "Access Type = ACCESS_ACCEPT".
- Common tasks**: A section with several options:
 - VLAN: Includes a "VLAN ID/Name *" field with a placeholder "VLAN ID/Name".
 - ACL: Includes a "Filter-ID *" field with a placeholder "Filter-ID".
 - WebRedirection
 - Portal ***: A dropdown menu with a placeholder "Select portal".
 - ACL name ***: A text input field with a placeholder "ACL name".
- Advanced attribute settings**: A section with an "Attribute" dropdown (placeholder "Select attribute") and an "Attribute value" input field (placeholder "Set attribute value").

At the bottom right, there are "Cancel" and "Add" buttons.

Figure 241. 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, configure in [device profile](#). 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** WebRedirection - enable redirect for the specified portal.
 - Portal - a [portal](#) to which the user will be redirected when connected to the network.
 - ACL name - name of the ACL that will be assigned when redirecting to the portal. ACL must be pre-configured on the network device.
- 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.

<input type="checkbox"/>	Name ↑
<input type="checkbox"/>	DenyAccess
<input type="checkbox"/>	MES auth
<input type="checkbox"/>	PermitAccess
<input type="checkbox"/>	Portal web redirect profile

Figure 242. Hyperlink to the authorization profile editing page

After that, the editing window will open.

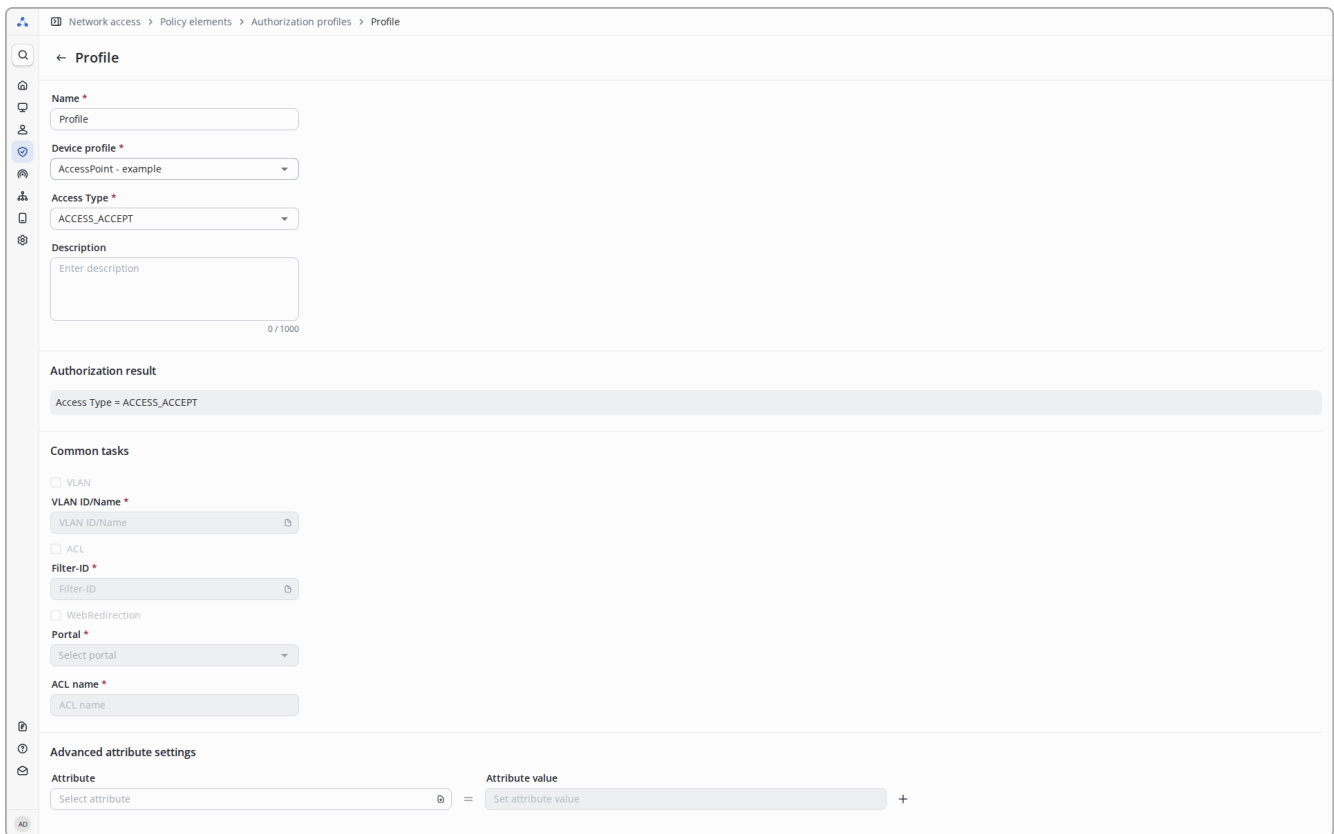



Figure 243. Authorization profile editing window

After editing, click the **"Save"** button. The button is hidden until at least one change is made.


The **"Cancel"** button resets the changes made to their original state.

Duplicating an authorization profile

A new profile can be created based on an existing one. To do this, select the profile to be copied using the checkbox, and then click the button .

A form will open, similar to the addition form, with all fields filled with values from the selected reference. 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.

Deleting

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.

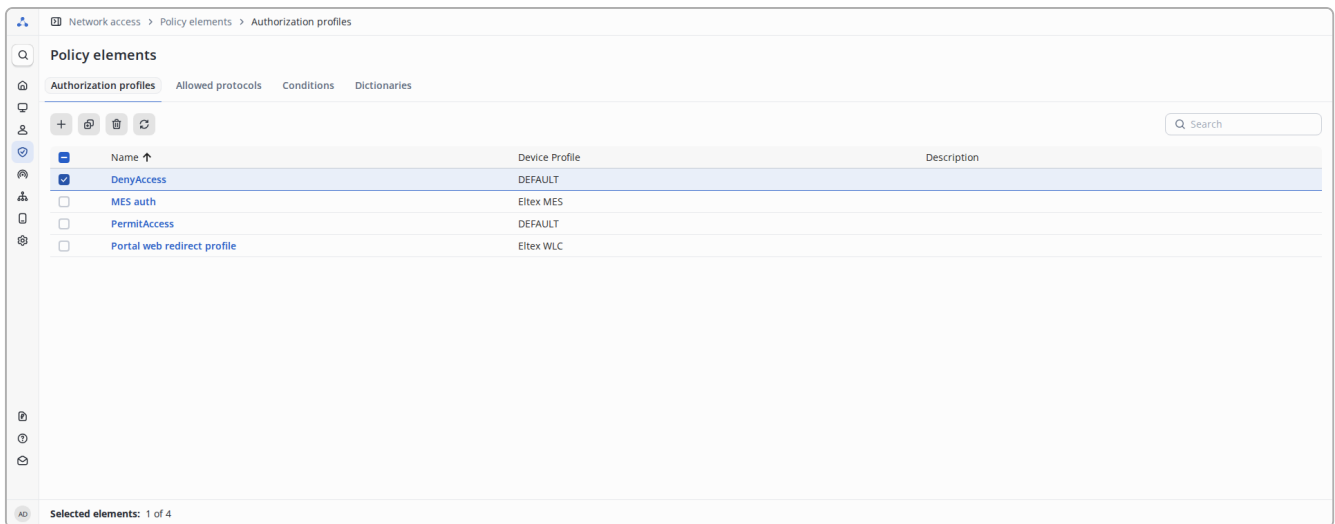


Figure 244. Selecting the authorization profile in the table to delete



Deleting items requires confirmation in the modal window. The selected items will be deleted only after explicit confirmation of the operation.

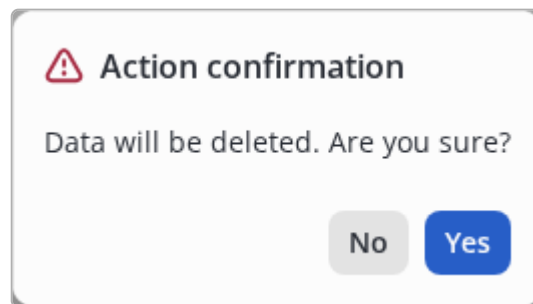


Figure 245. Modal dialog for confirmation



Restrictions:

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

Allowed Protocols

Description

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

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

You can configure to enable or disable MAB authorization.

View a list of allowed protocols

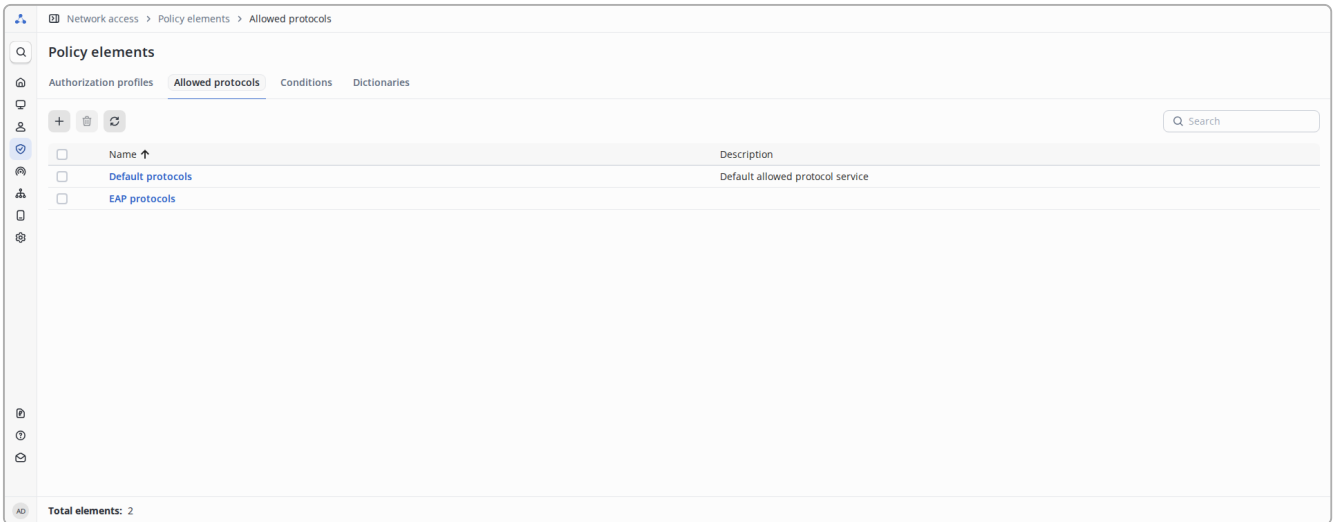


Figure 246. A table with a list of allowed protocol services on the viewing page

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

- **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 "Name" column.

Controls:

- **+** — Add a new element.
- **🗑️** — Delete selected elements (inactive until at least one element is selected).
- **🔄** — Refresh table data.
- — Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).
- **↑** — Change the current sort order.
- **🔍 Search** — Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.

Adding allowed protocols service

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

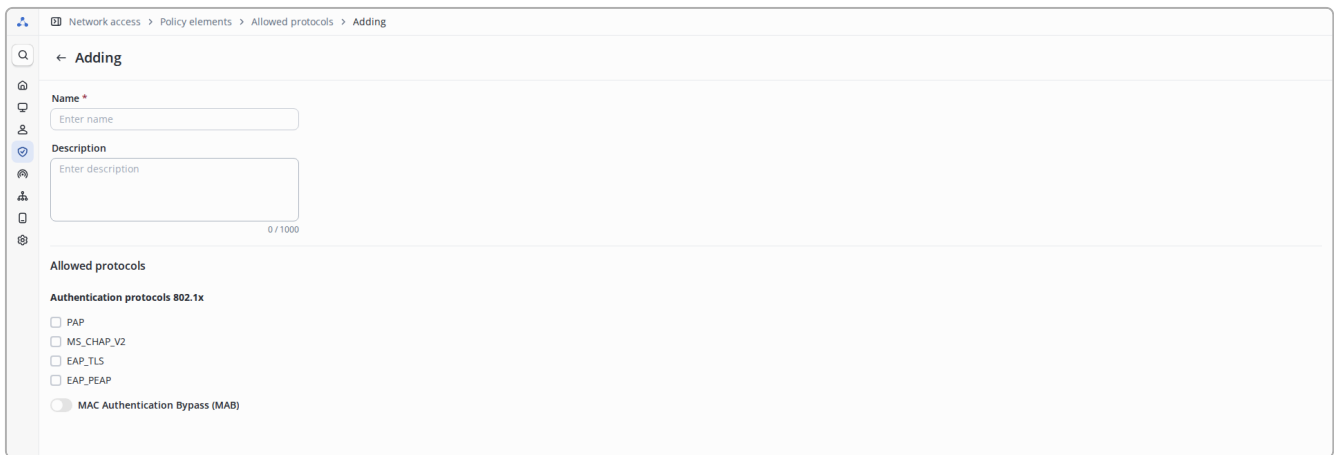


Figure 247. Window for adding a list of allowed protocols

- **Service name *** - name, must be unique. Maximum length is 100 characters.
- **Description** - arbitrary description. Maximum length is 1000 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).
 - **EAP_TTLS** - select the EAP-TTLS (Tunneled TLS) - a more flexible analogue of PEAP, which can carry not only modern EAP methods, but also old password verification protocols (such a PAP).
 - **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.

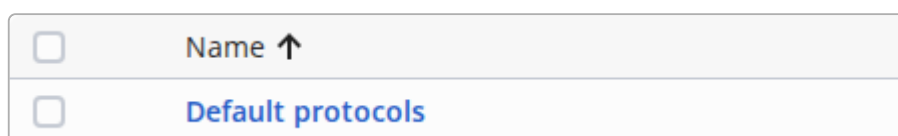


Figure 248. Hyperlink to the page for editing the list of allowed protocols

After this, the editing window will open.

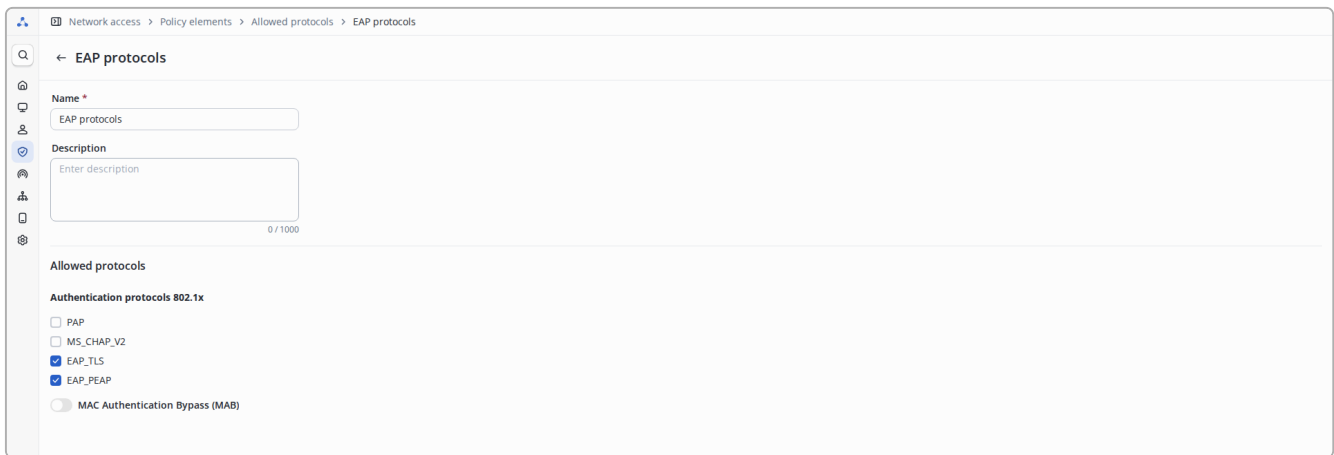



Figure 249. The window for editing the list of allowed protocols

After editing, click the **"Save"** button. The button is hidden until at least one change is made.

The **"Cancel"** button resets the changes made to their original state.

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.

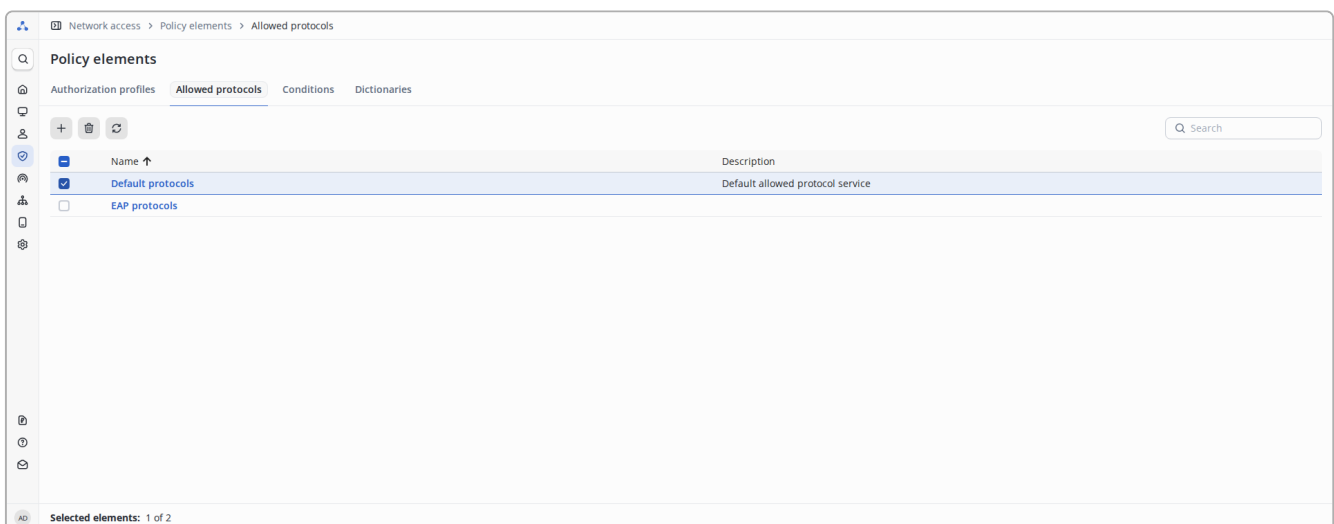


Figure 250. Selecting allowed protocol services in the table to delete



Deleting items requires confirmation in the modal window. The selected items will be deleted only after explicit confirmation of the operation.

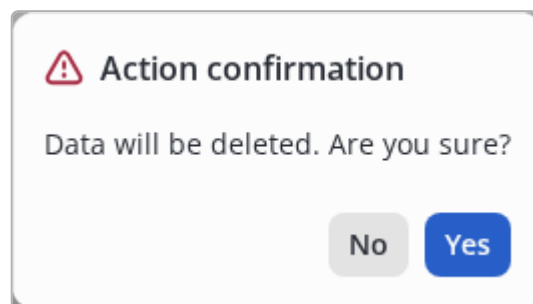


Figure 251. Modal dialog for confirmation



Restrictions:

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


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).

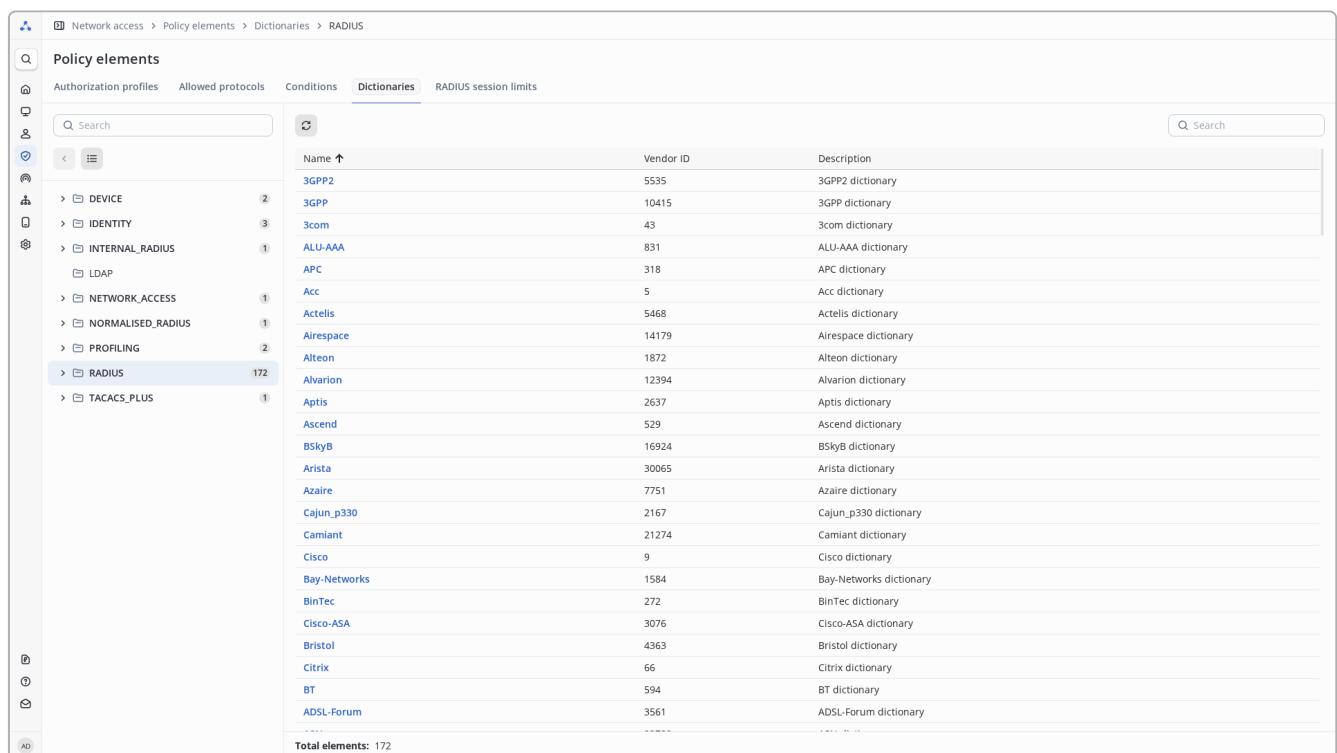
Dictionaries and attributes are available for viewing on a separate page. Adding new dictionaries or editing existing ones is not available.



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  in the lower left part of the navigation menu.

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):




Name ↑	Vendor ID	Description
3GPP2	5535	3GPP2 dictionary
3GPP	10415	3GPP dictionary
3com	43	3com dictionary
ALU-AAA	831	ALU-AAA dictionary
APC	318	APC dictionary
Acc	5	Acc dictionary
Actelis	5468	Actelis dictionary
Airespace	14179	Airespace dictionary
Alteon	1872	Alteon dictionary
Alvarion	12394	Alvarion dictionary
Aptis	2637	Aptis dictionary
Ascend	529	Ascend dictionary
BSkyB	16924	BSkyB dictionary
Arista	30065	Arista dictionary
Azair	7751	Azair dictionary
Cajun_p330	2167	Cajun_p330 dictionary
Camiant	21274	Camiant dictionary
Cisco	9	Cisco dictionary
Bay-Networks	1584	Bay-Networks dictionary
BinTec	272	BinTec dictionary
Cisco-ASA	3076	Cisco-ASA dictionary
Bristol	4363	Bristol dictionary
Citrix	66	Citrix dictionary
BT	594	BT dictionary
ADSL-Forum	3561	ADSL-Forum dictionary

Figure 252. View dictionaries

Controls:

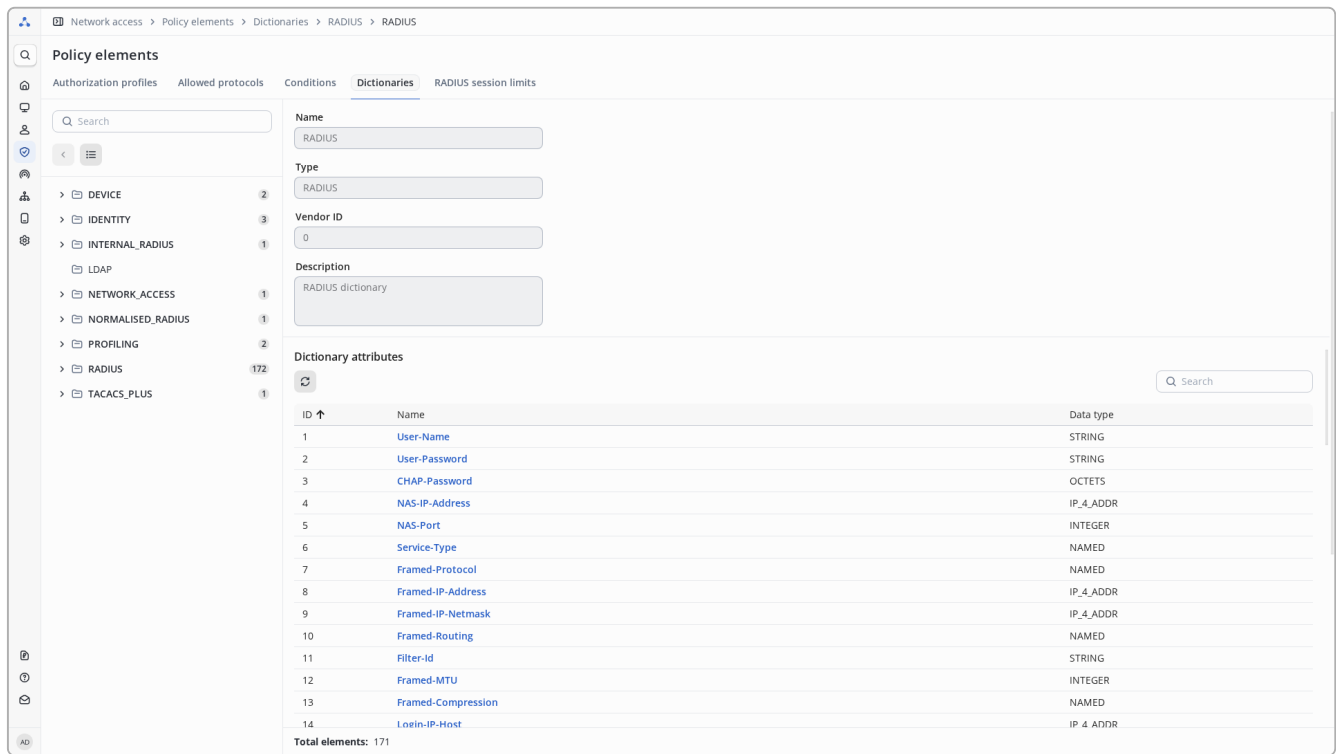
-  - Expand the list of nested dictionaries.
- "Dictionaries. Search" - Filtering by dictionary name.
- "RADIUS. Search" - Filtering by nested dictionaries and attributes.

 - 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:



The screenshot shows the 'Policy elements' interface for 'RADIUS' dictionaries. The left sidebar lists various policy elements, with 'RADIUS' having 172 elements. The main content area shows the 'RADIUS' dictionary configuration, including fields for Name, Type, Vendor ID, and Description. Below this is a table of 'Dictionary attributes' with columns for ID, Name, and Data type.

ID	Name	Data type
1	User-Name	STRING
2	User-Password	STRING
3	CHAP-Password	OCTETS
4	NAS-IP-Address	IP_4_ADDR
5	NAS-Port	INTEGER
6	Service-Type	NAMED
7	Framed-Protocol	NAMED
8	Framed-IP-Address	IP_4_ADDR
9	Framed-IP-Netmask	IP_4_ADDR
10	Framed-Routing	NAMED
11	Filter-Id	STRING
12	Framed-MTU	INTEGER
13	Framed-Compression	NAMED
14	Login-IP-Host	IP_4_ADDR

Total elements: 171

Figure 253. View attributes

To view information about an attribute, click its name:

RADIUS ×

Name

Data type

Vendor ID

Attribute ID

Allowed values

Key	Value
Login-User	1
Framed-User	2
Callback-Login-User	3
Callback-Framed-User	4
Outbound-User	5
Administrative-User	6
NAS-Prompt-User	7
Authenticate-Only	8
Callback-NAS-Prompt	9
Call-Check	10
Callback-Administrative	11

Total elements: 11

Figure 254. View information about an attribute

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

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

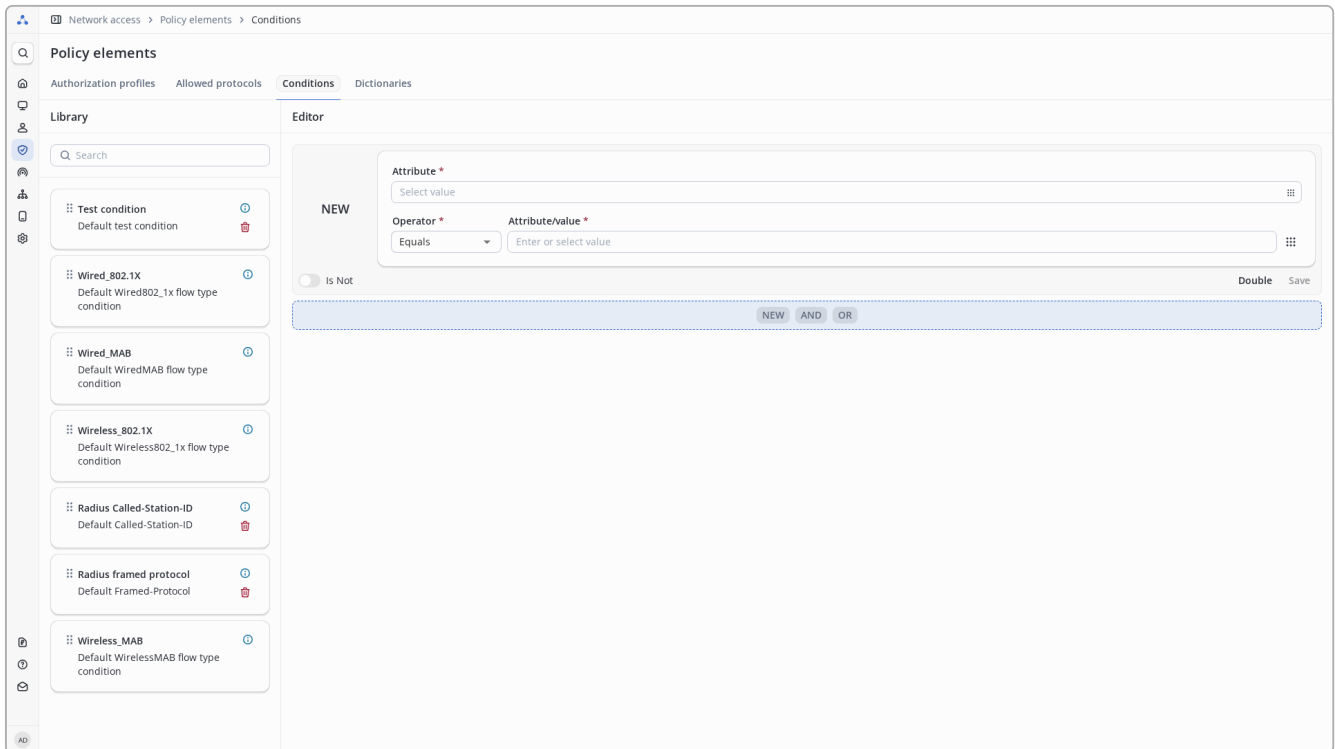


Figure 255. Library of logical conditions

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, there is also support for [regular expressions](#))
 - IP range
 - IP net mask

Empty value

- **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.

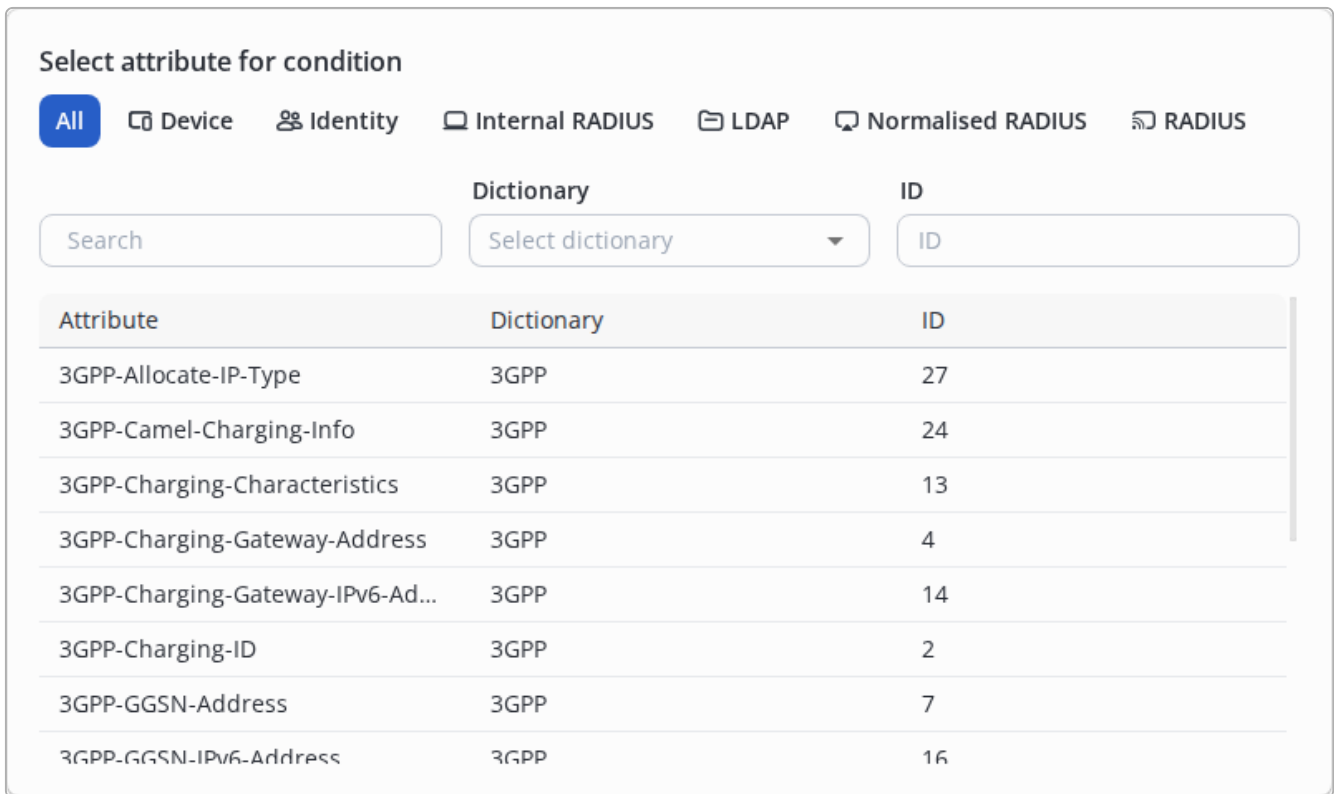


Figure 256. Attribute selection menu

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**.

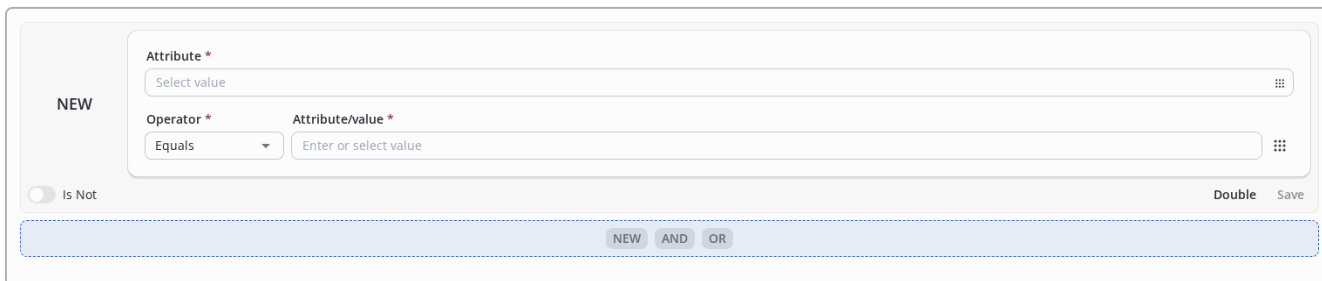



Figure 257. Initial state of Editor

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.

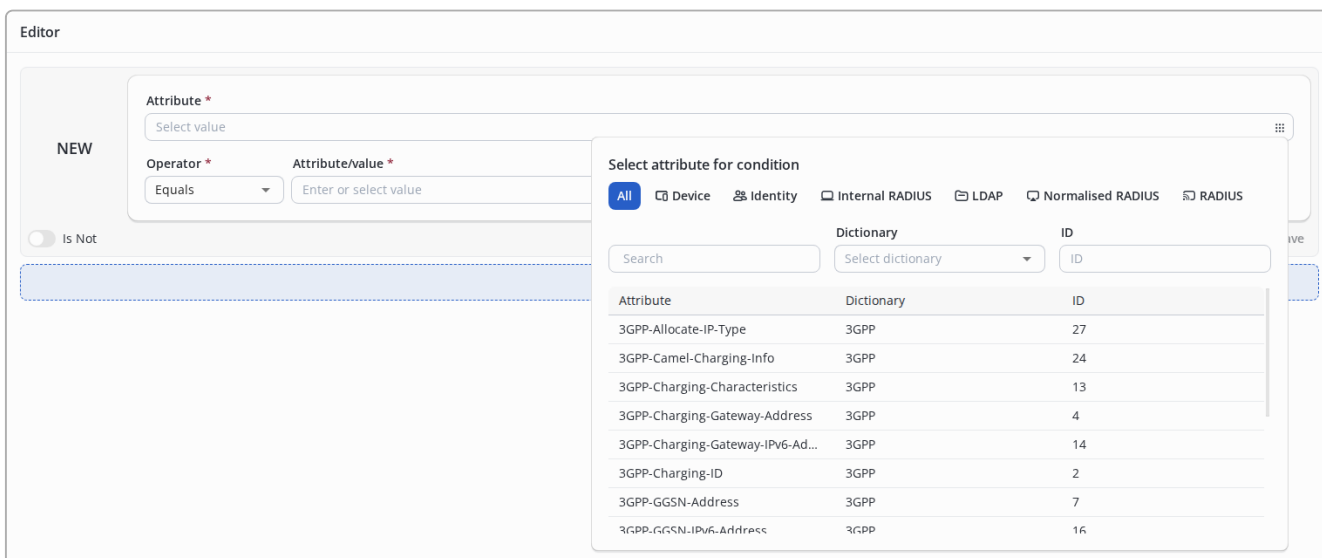


Figure 258. Attribute selection

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, Empty value
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, Empty value
IPv4 address	Equal to, Not equal to, Equal to NULL, Not equal to NULL, IP range, IP net mask, Empty value

Attribute data type	Supported operators
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, Empty value
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 259. 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.

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.

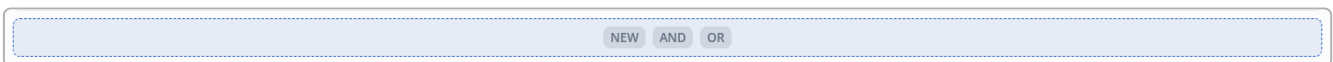


Figure 261. Panel to create an additional logical condition

- **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".

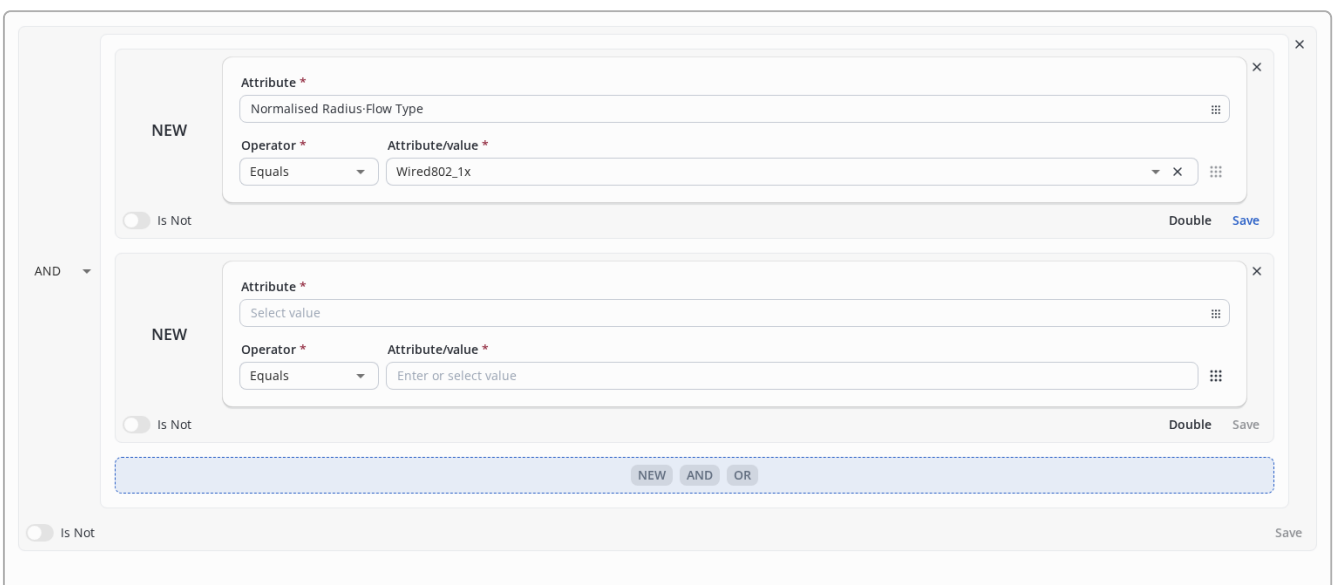




Figure 262. Condition consisting of two conditions combined by a logical "AND"

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.

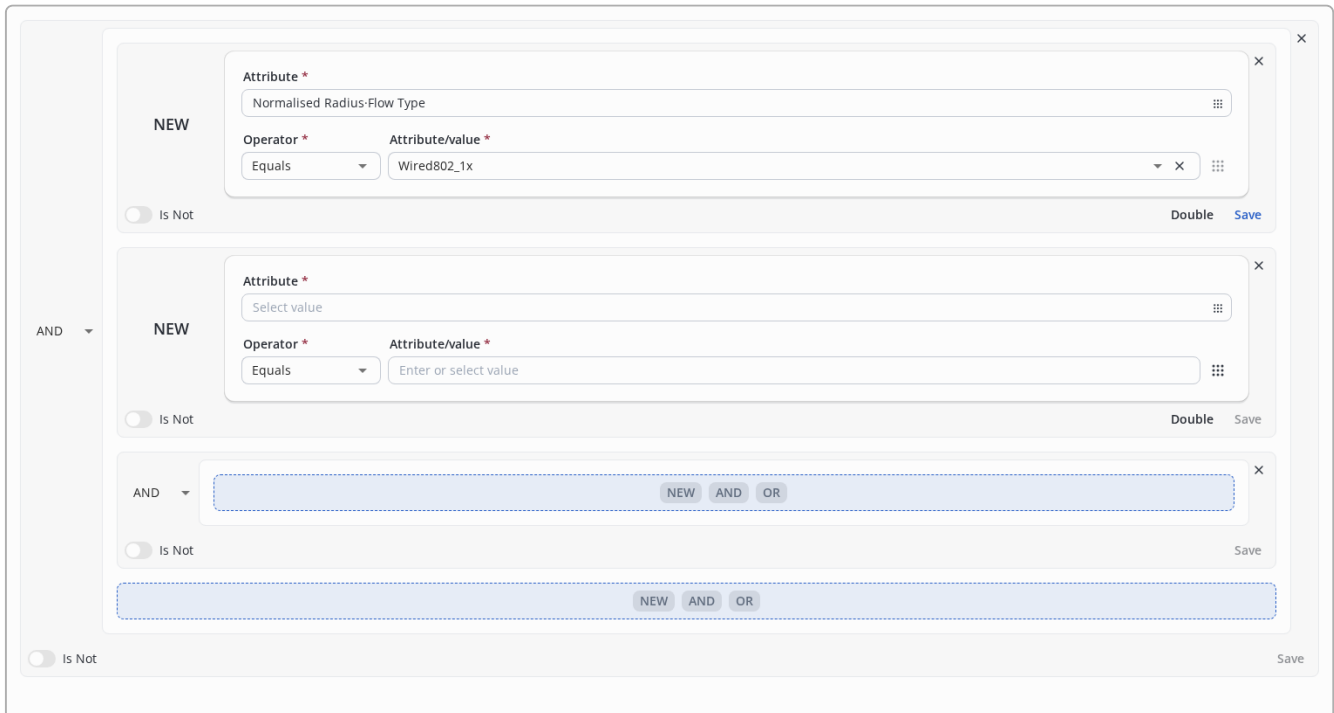


Figure 263. Condition containing nested rules

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

Using regular expressions

Regular expressions can be used when adding a condition to a policy set for attributes with the `matches` operator. This allows you to specify a "pattern" that can match multiple values using just one line.

Example 1. Using regular expressions in logical conditions

Task: You need to apply a policy set to all connections from devices whose names start with the `MES` prefix.

Possible Solution:

In order to select only connections from certain devices, you can use the `RADIUS NAS-Identifier` attribute in the condition. Note that it usually requires configuration on the NAS device to send it.

In order to avoid creating separate `RADIUS NAS-Identifier equals MES1` etc. conditions for each device, you can create one `RADIUS NAS-Identifier matches MES.*` condition.

The `.*` construct means "any number of any characters" after `MES`.

You can also use a more strict expression if, for example, you want `MES` to always be followed by 4 digits and one letter: `MES\d{4}[A-Z]`.

Here:

`\d{4}` — four digits;

`[A-Z]` — one uppercase letter.

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.



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.

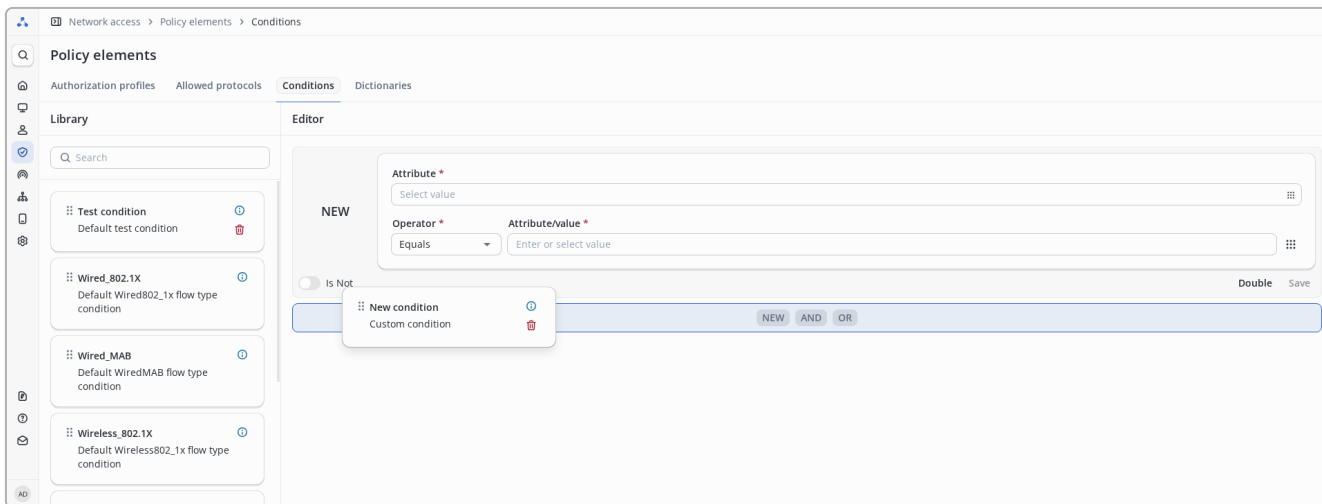


Figure 264. Selecting a logical condition

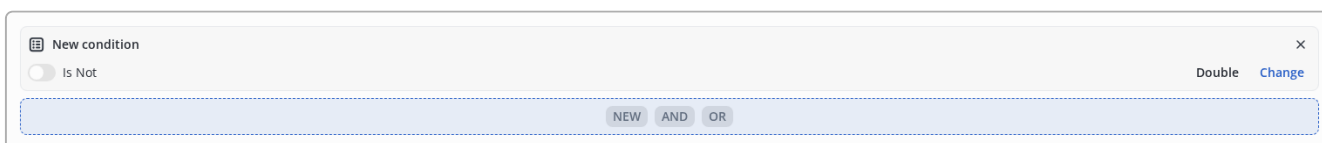



Figure 265. Editing a logical condition

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.

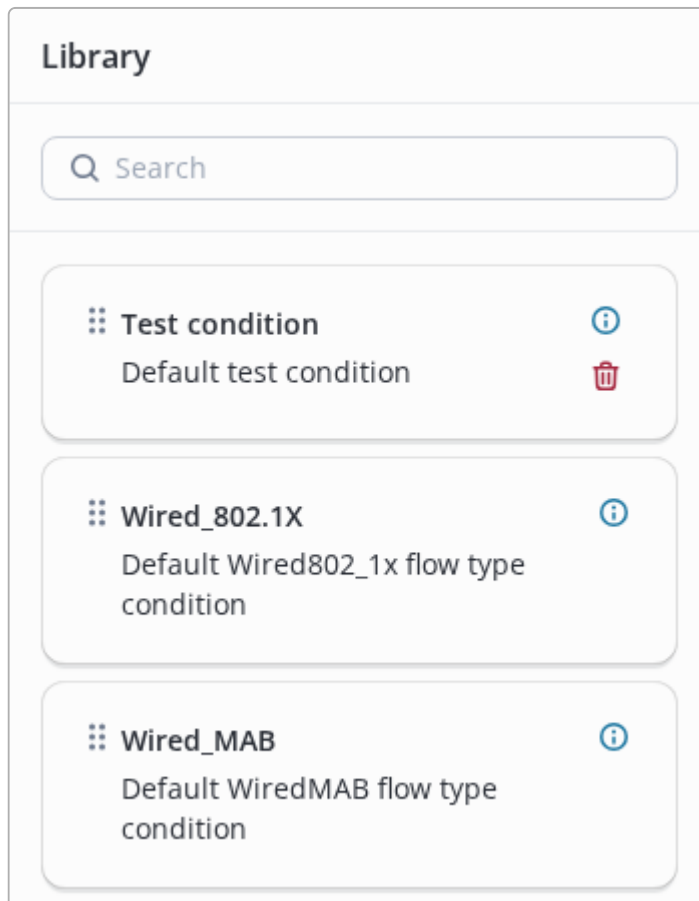


Figure 266. Selecting a condition to delete



Deleting items requires confirmation in the modal window. The selected items will be deleted only after explicit confirmation of the operation.

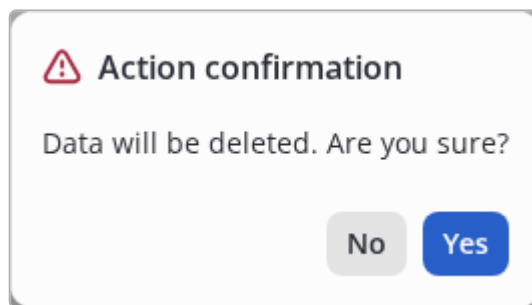


Figure 267. Modal dialog for confirmation



Restrictions:

- some system logical conditions cannot be deleted or edited;
- 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.

RADIUS Session Limits

Description

The simultaneous RADIUS session limiting functionality allows you to control the use of user accounts when connecting to the network. The mechanism limits the number of simultaneously active user sessions and

prevents unauthorized sharing of credentials.

The limit is applied to all identity sources except guest endpoints. Portal redirect sessions are not counted in the limit. The limit is not applied to MAB authentication.



This section is only available when RADIUS Accounting processing is enabled ([System Settings](#) → [Services](#) → [RADIUS](#)).

Configuring RADIUS Session Limits

Identity source	Active sessions limit	Session time limit (hh:mm)
Source 1	100	<input type="checkbox"/> Global 48:00
Source 2	200	<input checked="" type="checkbox"/> Global 00:00
Source 3	50	<input type="checkbox"/> Global 12:00

Figure 268. RADIUS session limits configuration page

At the top of the page is the global parameter:

- **Active session lifetime *** - the maximum lifetime of an active session since its last update. If no events confirming its relevance are received during the specified period, the system considers the session hung and automatically terminates it. Automatic termination frees the quota set for the source for new connections.



The value is specified in `hours:minutes` format and must be greater than `00:00`.

The global session lifetime is applied to identity sources that have the *Global* toggle enabled in the time settings.

Below the global setting is the identity sources table. In the table, you can configure the following parameters for each source:

- **Active session limit** - the maximum number of simultaneously active sessions of one user within this source.
 - `0` - limit is disabled. The system does not check the number of active sessions.
 - `N > 0` - when the limit is reached, the system returns an `Access-Reject` response, and the user does not gain network access.
- **Session time limit** - the active session lifetime for this source, specified in `hours:minutes` format.
 - **Global** - toggle for applying the global session lifetime.
 - **Enabled** - the global lifetime setting is applied to sessions of this source.

- Disabled - a custom lifetime value is specified for this source, independent of the global setting.



When the `Global` toggle is disabled, specifying the session time limit is required.

How Simultaneous RADIUS Session Limit Works

Active Session Count

The NAICE system tracks sessions based on RADIUS Accounting attributes. The number of active sessions for a given user is determined sequentially using the following attribute combinations:

1. **Class-25** - determining connection uniqueness based on an attribute containing a unique connection identifier.
2. **NAS IP + Session-ID** - determining connection uniqueness by the combination of the network device IP address and session identifier.
3. **Identity source + NAS IP + MAC address + Username** - determining connection uniqueness when the authentication source is known. MAC address is not a required attribute, as it may be absent during MAB authentication.
4. **NAS IP + MAC address** - determining connection uniqueness for portal users.
5. **NAS IP + MAC address + Username** - determining connection uniqueness when none of the above attribute combinations were sent by the network device. MAC address is not a required attribute.



The NAICE system uses the first matching attribute combination from the list.

Authentication Check

When authenticating a user, the system identifies them by the combination "*Identity Source + Username*" and checks the number of active RADIUS sessions:

- If the number of active sessions is less than the set limit - access is granted.
- If the number of active sessions exceeds the set limit - the system returns Access-Reject. The reason for rejection is recorded in the [event log](#): simultaneous session limit exceeded.



A session is considered active until a *RADIUS Accounting Stop* packet is received or the session is terminated by timeout. Manual session termination by the administrator also frees the active RADIUS session quota.

RADIUS policies

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:users-and-devices: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.
- RADIUS policies set to `Status Disabled` do not using in the check, the counter in the `Hits count` column does not increase.
- RADIUS policies set to `Status Condition Check` do not using in the check, but the counter in the `Hits count` column increases when the policy is matched.
- 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 in the RADIUS request 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 are checked from top to bottom until a matching condition are found. If no suitable authentication policy is found with a matching condition it will be matched to Default authentication policy at the end of list and identity sequence from this authentication policy will be used to authenticate user.
- A search is performed for the user in the selected [list of identity sequences](#). If no user login will be found in the list of identity sequence the `ACCESS-REJECT` will be sent to the network device.
- Authorization policies are checked from top to bottom until a matching condition are found. If no suitable authorization policy is found with a matching condition, an `ACCESS-REJECT` will be sent to the network device using the Default authorization policy at the end of list. 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

Status	Name*	Description	Conditions*	Allowed protocols*	Hits count
Enabled	Wired network	EAP-PEAP, EAP-TLS	Wired_802.1X	Default protocols	0
Enabled	Wireless network	EAP-PEAP, EAP-TLS	Wireless_802.1X	Default protocols	0
Enabled	Wired network (MAB)	MAC Auth Bypass	Wired_MAB	MAB	0
Enabled	Captive Portal	WiFi	Wired_MAB AND Normalised Radius SSID Equals NAICE-Portal	MAB	0
Default		Default policy set		Default protocols	

Figure 269. View all policy sets

The table displays RADIUS 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. Maximum length - 200 characters.
- **Description** - arbitrary description. Maximum length - 1000 characters.
- **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](#).
- **Hits count** - 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).
- - 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).
- **Hits count** - 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 RADIUS policies are checked in order, as shown on the screen - from top to bottom. RADIUS policies are always displayed on the page fully: **Search** does not hide entries from the list, but only highlight them.

+	Status	Name*	Description	Conditions*	Allowed protocols*	Hits count
⋮	Enabled	Wired network	EAP-PEAP, EAP-TLS	Wired_802.1X 177/1000	Default protocols	0
⋮	Enabled	Wireless network	EAP-PEAP, EAP-TLS	Wireless_802.1X 177/1000	Default protocols	0
⋮	Enabled	Wired network (MAB)	MAC Auth Bypass	Wired_MAB 157/1000	MAB	0

Figure 270. Search for policy set

To change the order, drag the policy by the **⋮** in the **+** column.

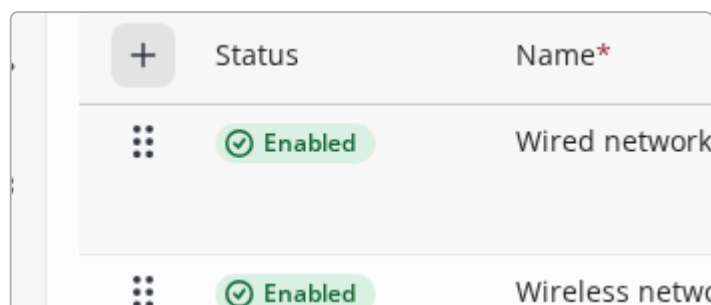


Figure 271. Change policy set order. Drag and drop action



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 policy in the list of RADIUS policies it is demanded to click the **+** button at the top left - the new policy will be added first in the list.

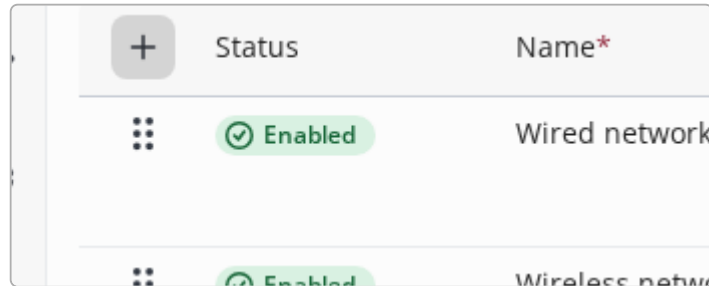


Figure 272. Display new policy. Add action

If it is necessary to add policy to an arbitrary location in list it is demanded to click on the button **⋮** to the right of the selected policy of RADIUS policies list and select **Add on top** or **Add on bottom** in the drop-down menu.

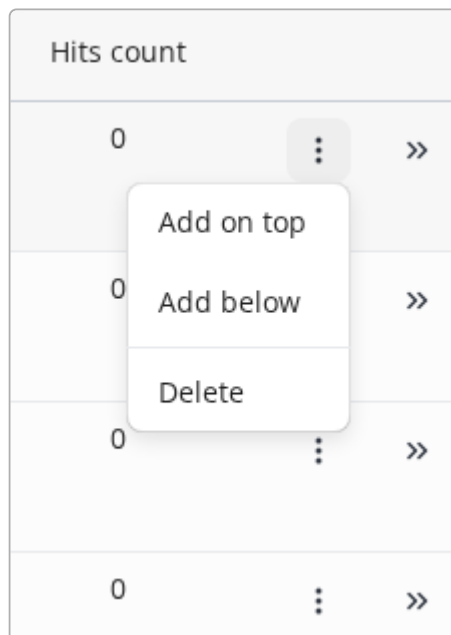


Figure 273. Display policy. Drop-down menus with actions

Information on **Status** :

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

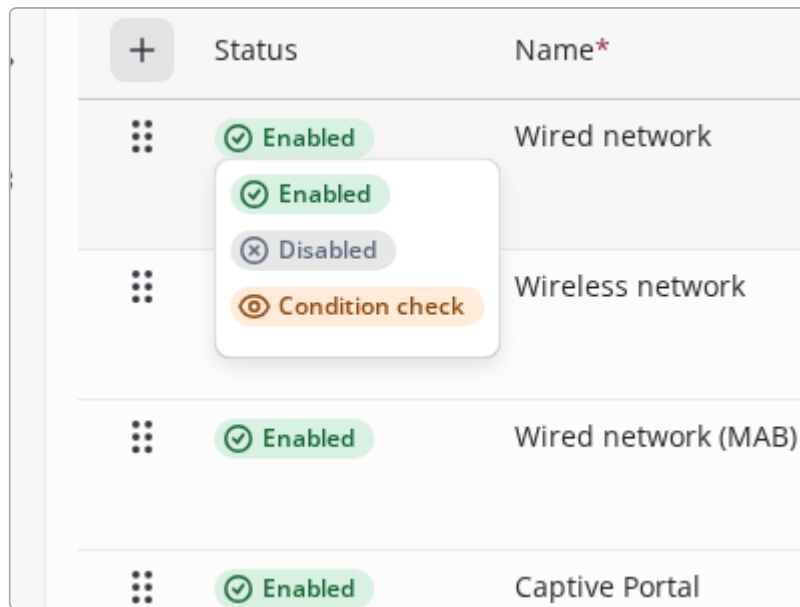


Figure 274. Change policy status

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 275. Displaying the new policy entry. Elements are required

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

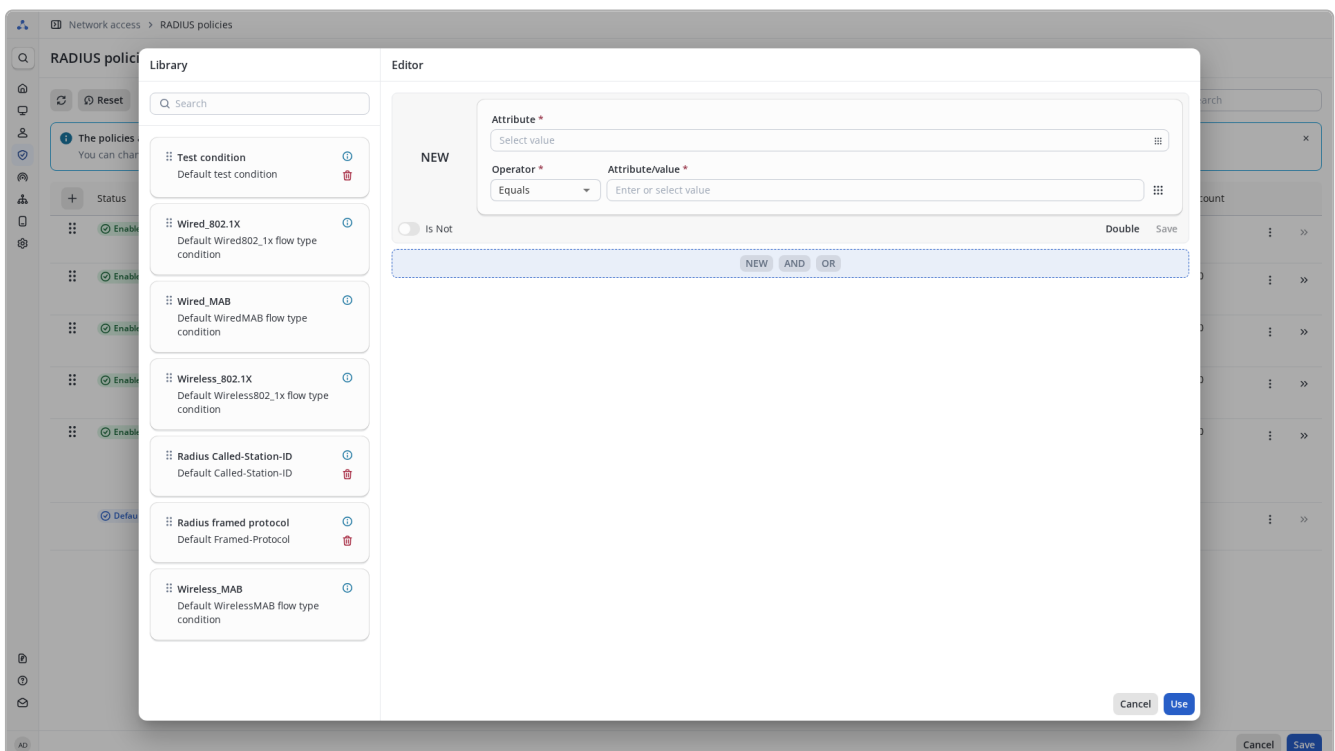


Figure 276. Conditions editor

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.

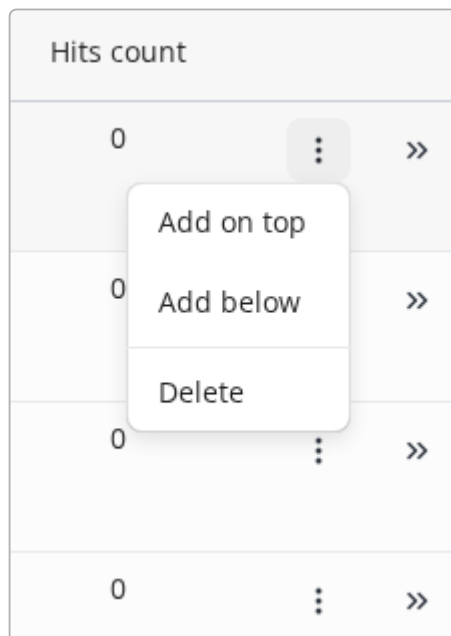


Figure 277. Drop-down menu for deletion of policy set



Deleting items requires confirmation in the modal window. The selected items will be deleted only after explicit confirmation of the operation.

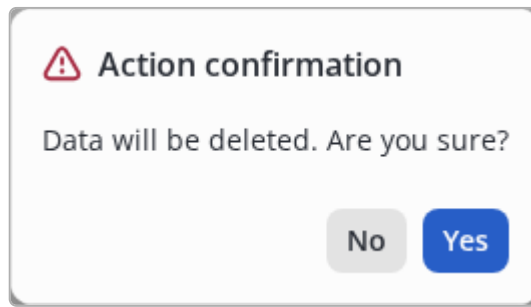


Figure 278. Modal dialog for confirmation

Policy hits count

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



Using the **Condition check** status and observing the trigger counters, you can first fine-tune and debug the condition, and only then put the policy into operation by switching it to the **Enabled** status.

The trigger counters for all policy sets can be reset by clicking on **Reset**. To reset the counter for a specific set, click the number in the **Hits Count** column, click the **Reset** button, and confirm the action.

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](#).

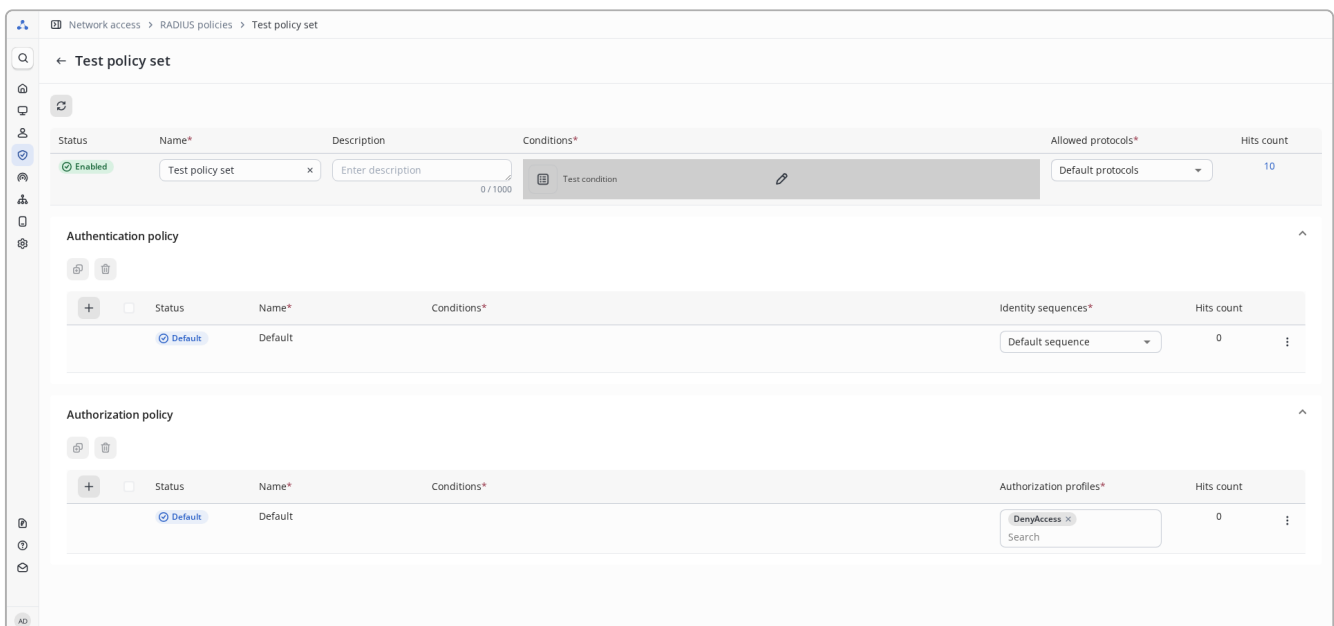


Figure 279. Policy et view and edition page





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 [RADIUS policies](#).
- **Authentication policy** - manages user authentication.
- **Authorization policy** - user authorization management.

Controls:

-  - 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](#).
- **Hits count** - the count of authorization attempts that fall under the specified Conditions. By clicking on the number of operations the counter can be **Reset**.
-  - actions:
 - **Add above** - add a new policy rule *BEFORE* the selected one;
 - **Add below** - add a new policy rule *AFTER* the selected one;
 - **Duplicate** - add a new policy rule, similar to the selected one, before the duplicated rule;
 - **Delete** - delete the selected rule.
- **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 similar to the [RADIUS policies](#) 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 280. "Authentication" policies panel

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

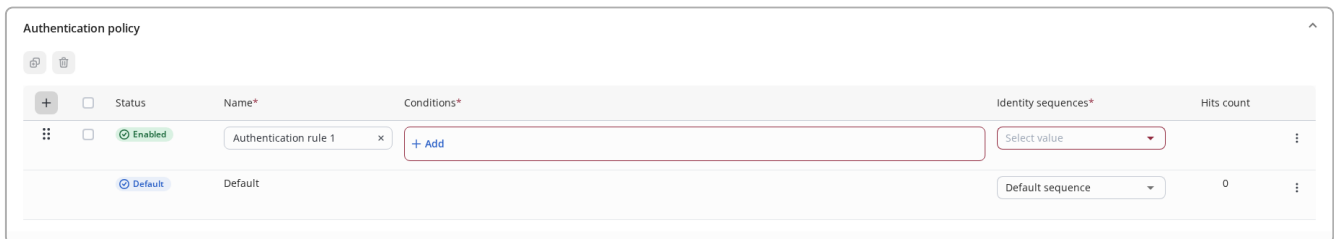


Figure 281. New "Authentication" policy

In the **Name** field, enter the name of the policy rule.

To edit a condition, click **+ Add** - 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**.

A new policy rule can also be created from an existing one by duplicating it. To do this, select the desired rule/rules via , and then click above the table. A new rule will be created above the selected one with similar settings and a name ending with "_copy".

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

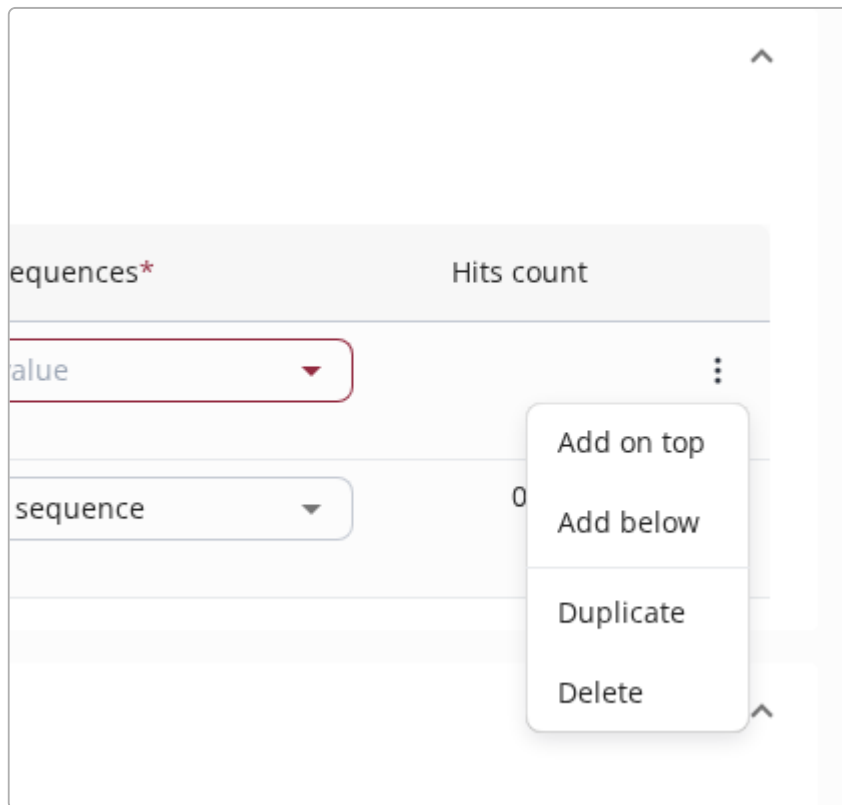


Figure 282. Authentication Policy. Dropdown Menus. Actions

We can also change the policy status.

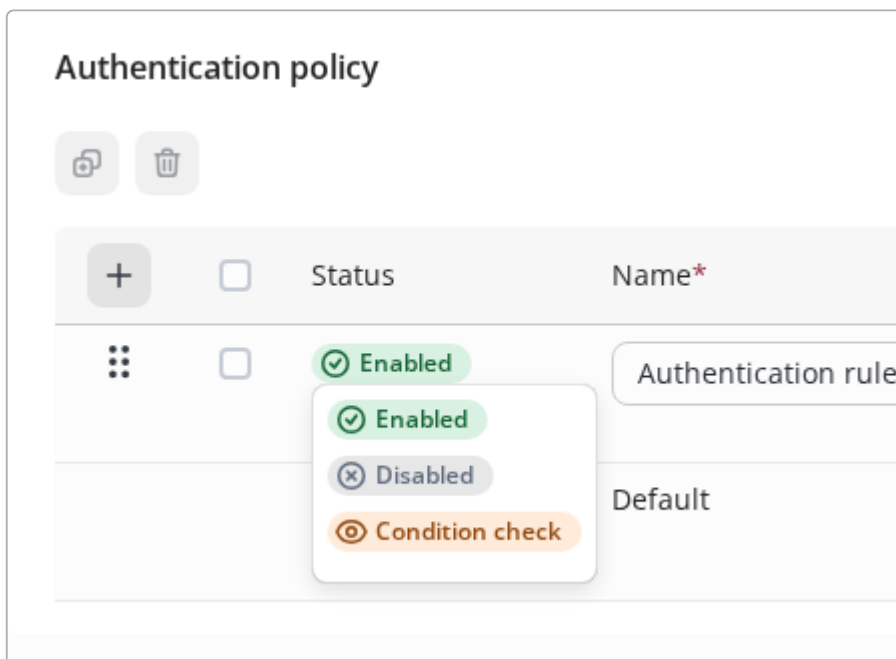


Figure 283. Authentication Policy. Change policy status

Authorization Policy



Figure 284. Policy panel "Authorizations"

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

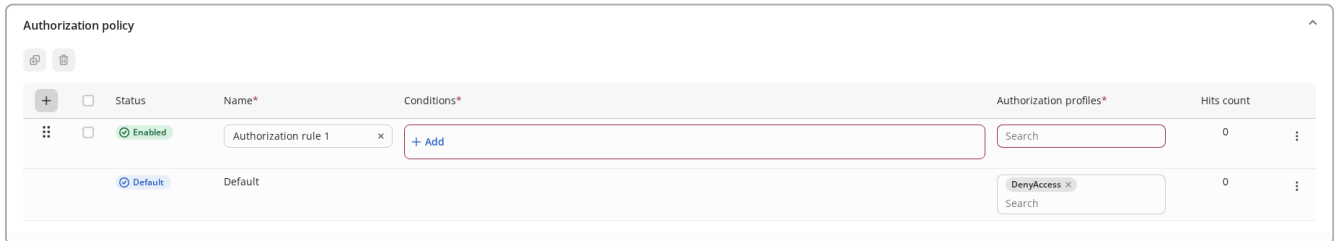


Figure 285. New "Authorization" policy

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

To edit a condition, click **+ Add** - 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.

A new policy rule can also be created from an existing one by duplicating it. To do this, select the desired rule/rules via **□**, and then click **📄** above the table. A new rule will be created above the selected one with similar settings and a name ending with "_copy".

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

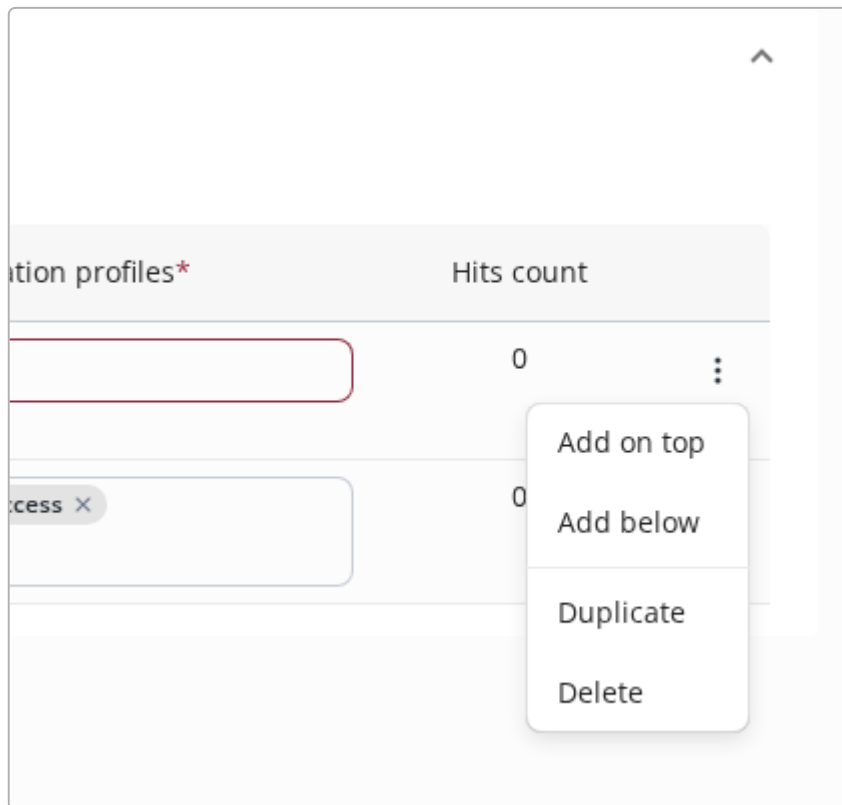


Figure 286. Authorization Policy. Dropdown Menus. Actions

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

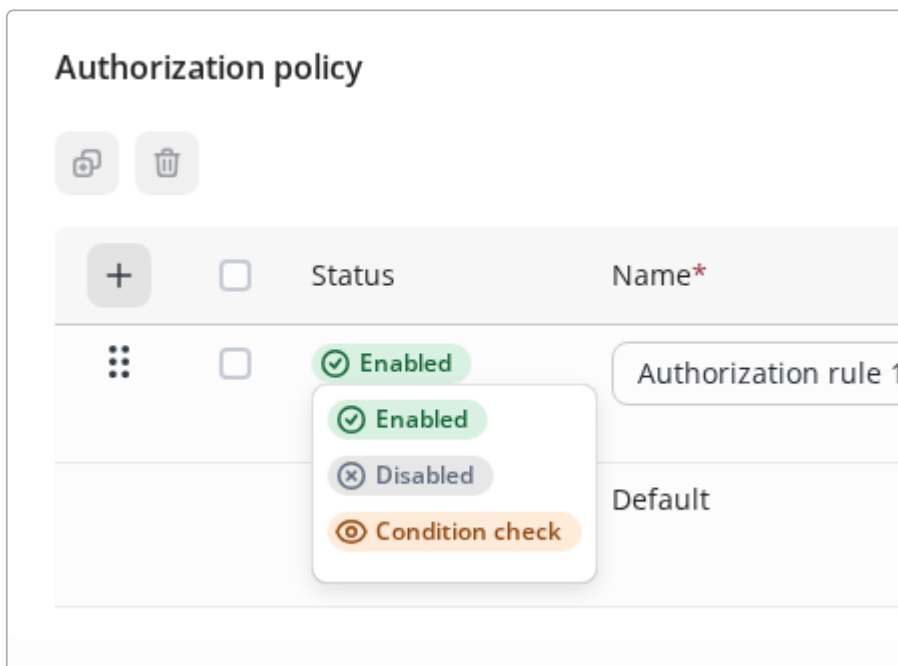


Figure 287. Authorization Policy. Change policy status

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 one policy rule click on the  button and select the **Delete** action.

To delete multiple rules, select them using and then click  above the table of rules.



Deleting items requires confirmation in the modal window.
The selected items will be deleted only after explicit confirmation of the operation.

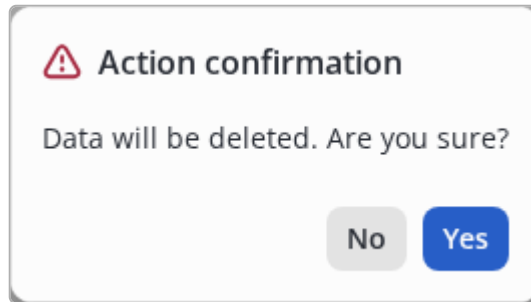


Figure 288. Modal dialog for confirmation

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.

Name ↑	Type	Expression	Description
condition	Created by admin	DHCP probes:Class Id Not equals NULL	Detail description for condition

Figure 289. 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:

- — Add a new element.
- — Duplicate chosen element. Becomes active if only one element in the list is selected.
- — Delete selected elements (inactive until at least one element is selected).
- — Refresh table data.
- — Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).
- — Change the current sort order.
- **Search** — Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.

Adding a Profiling Condition

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

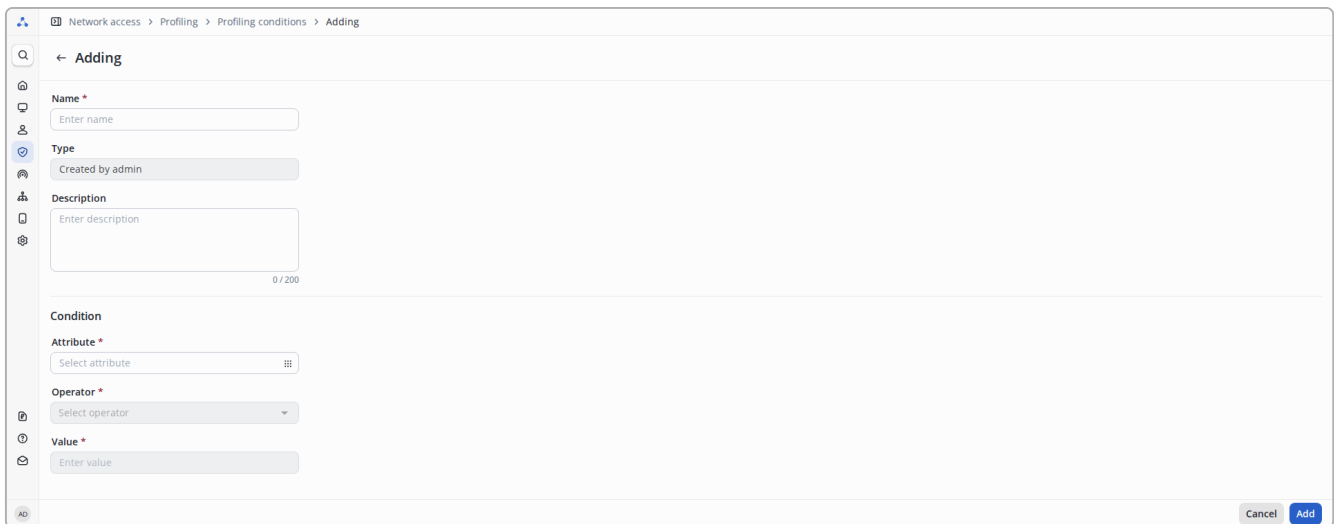



Figure 290. Profiling condition addition page

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

Parameters 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.

Select attribute for condition

All 👤 Profiling

Search Dictionary: Select dictionary ▼ ID: ID

Attribute	Dictionary	ID
Class Id	DHCP probes	60
Client Id	DHCP probes	61
Hostname	DHCP probes	12
Parameter List	DHCP probes	55
Requested address	DHCP probes	50
OUI	MAC	1

Figure 291. 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.

<input type="checkbox"/>	Name ↑
<input type="checkbox"/>	condition

Figure 292. Hyperlink to profiling condition edition page

After this, the editing page will open.

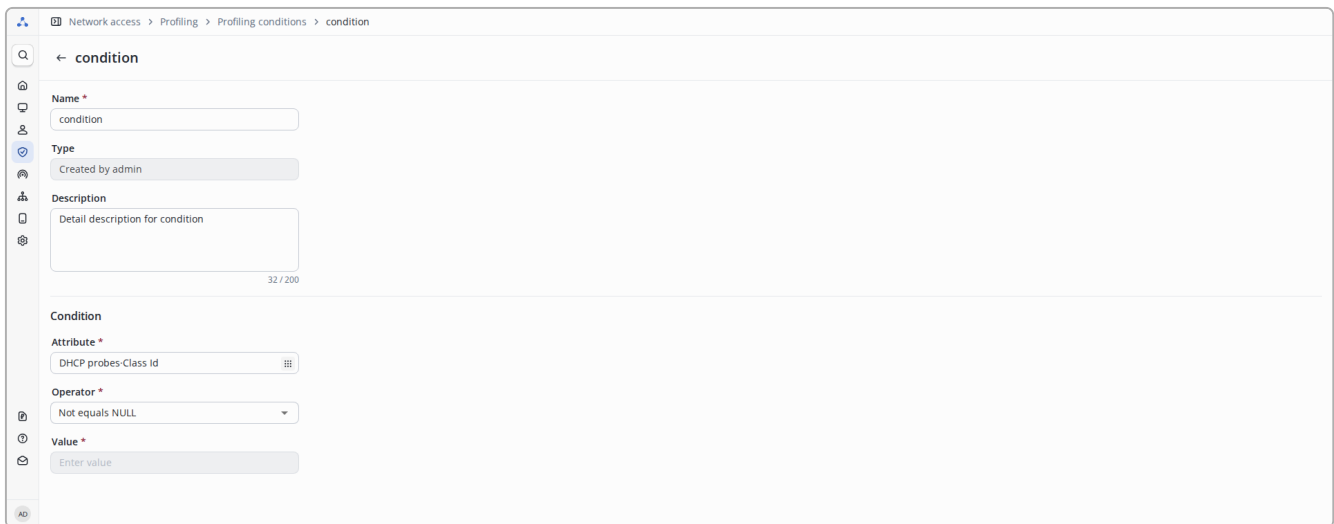



Figure 293. Profiling condition edition page

After editing, click the **"Save"** button. The button is hidden until at least one change is made.

The **"Cancel"** button resets the changes made to their original state.

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.

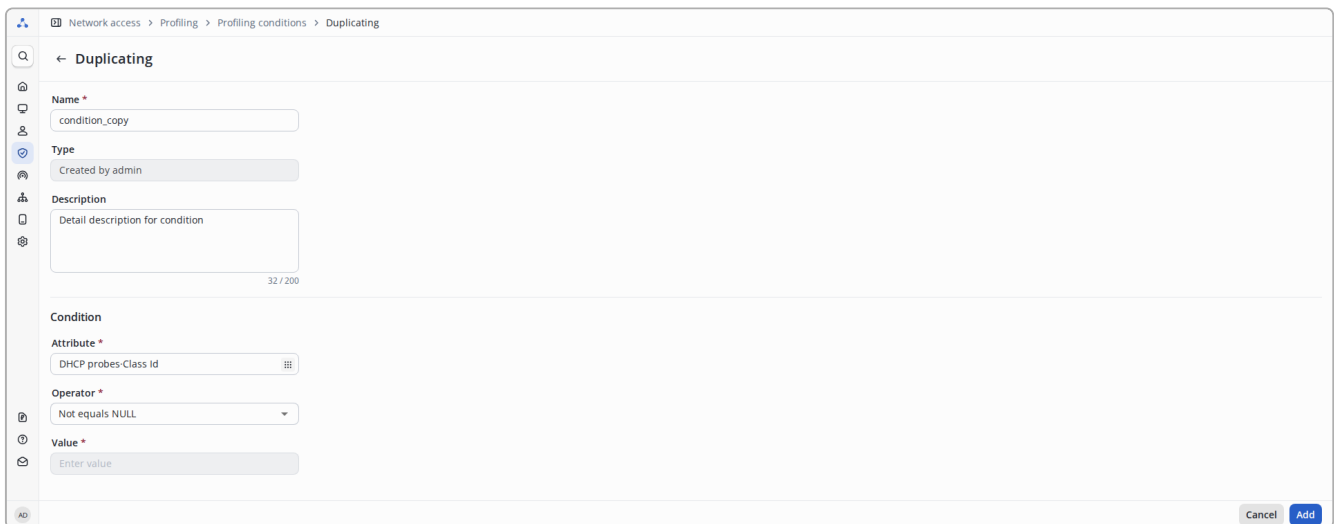


Figure 294. Profiling condition copy page

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.

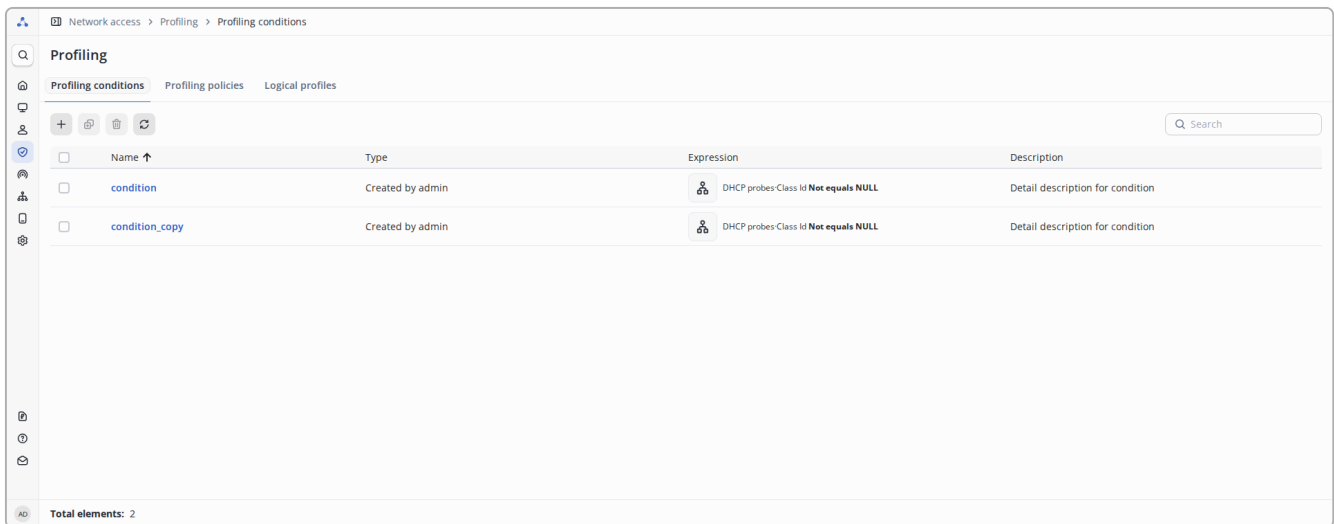


Figure 295. Profiling conditions table after condition copied

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.

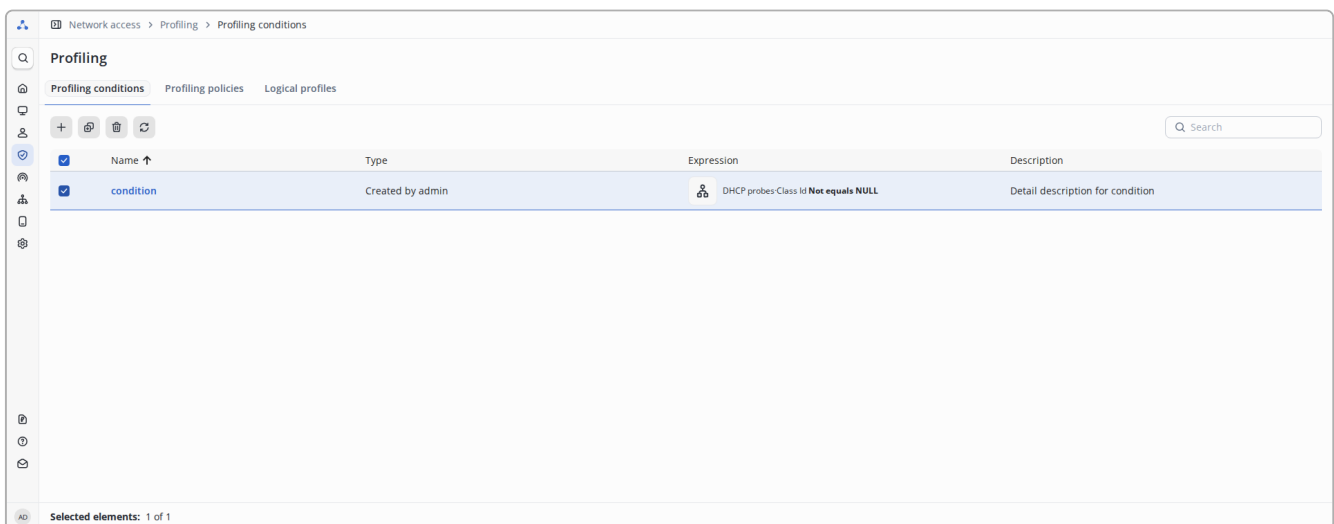


Figure 296. Selecting conditions for deletion



Deleting items requires confirmation in the modal window. The selected items will be deleted only after explicit confirmation of the operation.

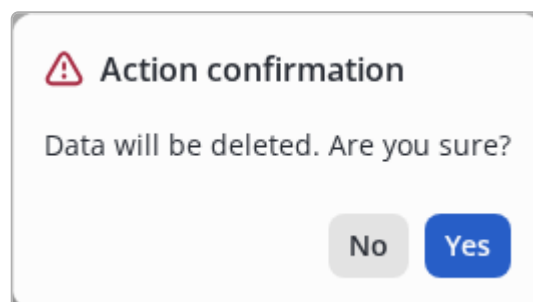


Figure 297. Modal dialog for confirmation

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.

Status	Name ↑	Description	Hits count
Disabled	Eltex	Any Eltex devices	10
Enabled	Eltex-IP-Phone	Eltex any IP Phone profile	0
Enabled	Unknown	Default system profiling policy that is assigned to an endpoint	0

Figure 298. 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.

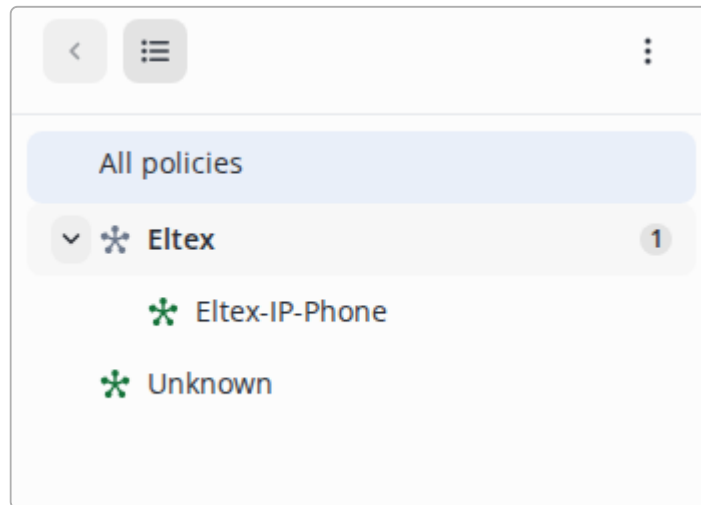









Figure 299. Tree of profiling policies

Contains the following control elements:

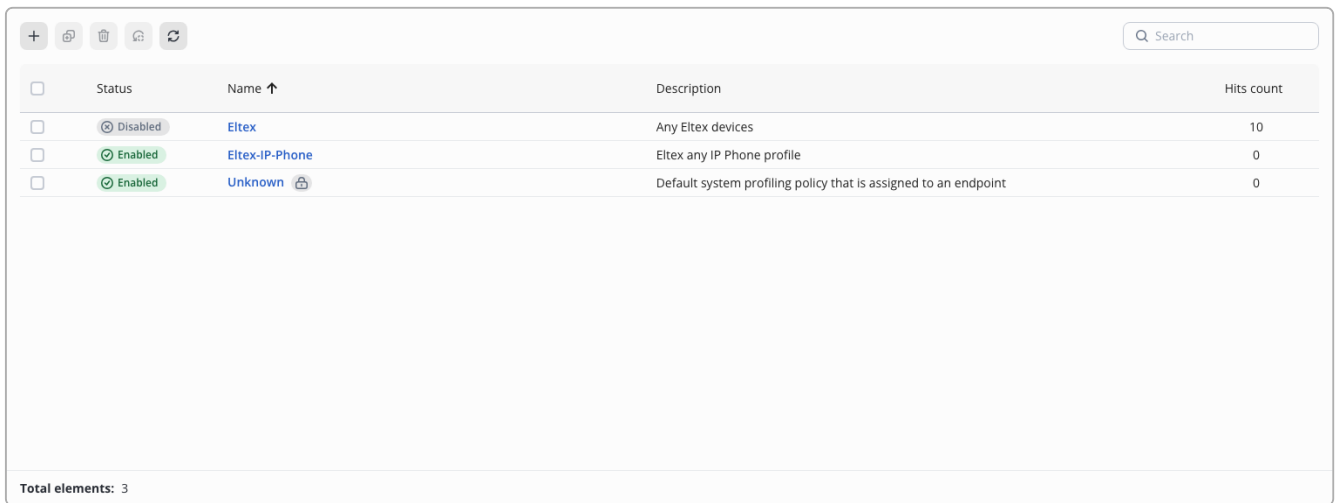
-  - display mode in the form of a tree structure of profiling policies (to switch the mode to the opposite, click on the icon).
-  - display mode in the form of a list of child profiling policies (to switch the mode to the opposite, click on the icon).
-  - adding/duplicating/deleting a policy. The 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.



<input type="checkbox"/>	Status	Name ↑	Description	Hits count
<input type="checkbox"/>	Disabled	Eltex	Any Eltex devices	10
<input type="checkbox"/>	Enabled	Eltex-IP-Phone	Eltex any IP Phone profile	0
<input type="checkbox"/>	Enabled	Unknown	Default system profiling policy that is assigned to an endpoint	0

Total elements: 3

Figure 300. Table listing all profiling policies


The table contains columns:

- **Status** - current status of the profiling policy can take the values **Enabled** or **Disabled** .
- **Name** - name of the profiling policy.
 - - This entity is system and cannot be deleted or edited.
- **Type** - type of profiling policy. The possible value is "Created by admin" or "System".
- **Description** - description of the profiling policy.
- **Hits count** - 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:

- — Add a new element.
- — Duplicate chosen element. Becomes active if only one element in the list is selected.
- — Delete selected elements (inactive until at least one element is selected).
- — Refresh table data.
- — Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).
- — Change the current sort order.
- **Search** — Performs case-insensitive filtering across all columns: only records that satisfy the filtering condition are displayed.
-

 - 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.

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.

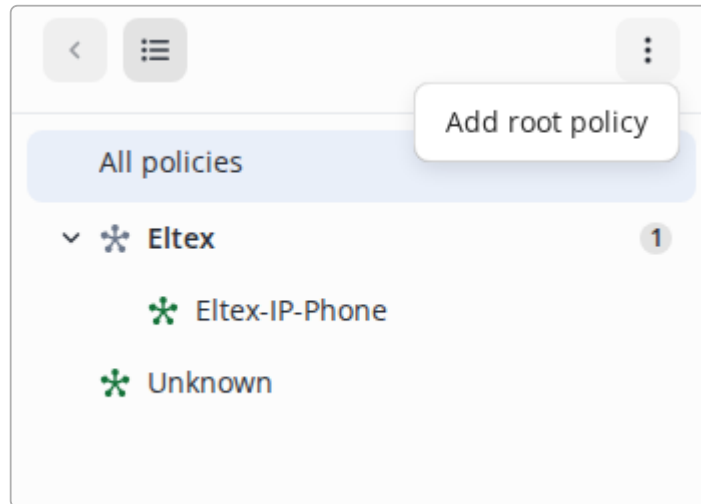


Figure 301. Adding a profiling policy. Actions

- 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.

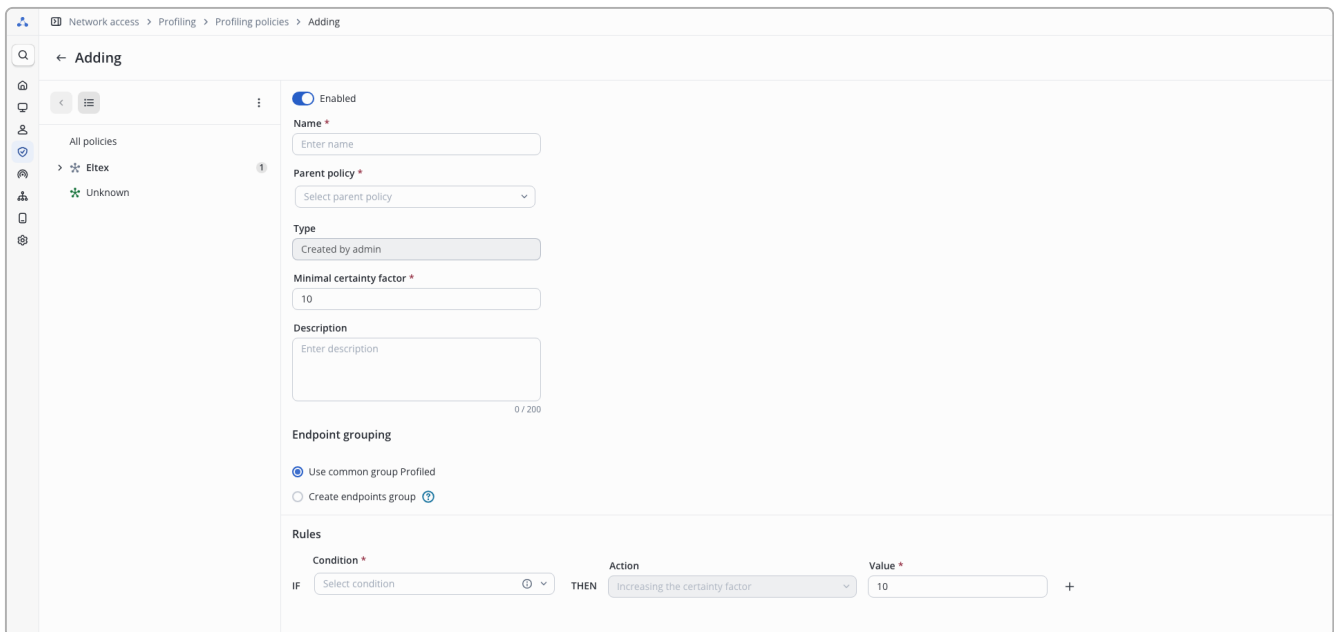


Figure 302. Adding a profiling policy

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 303. 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.

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.

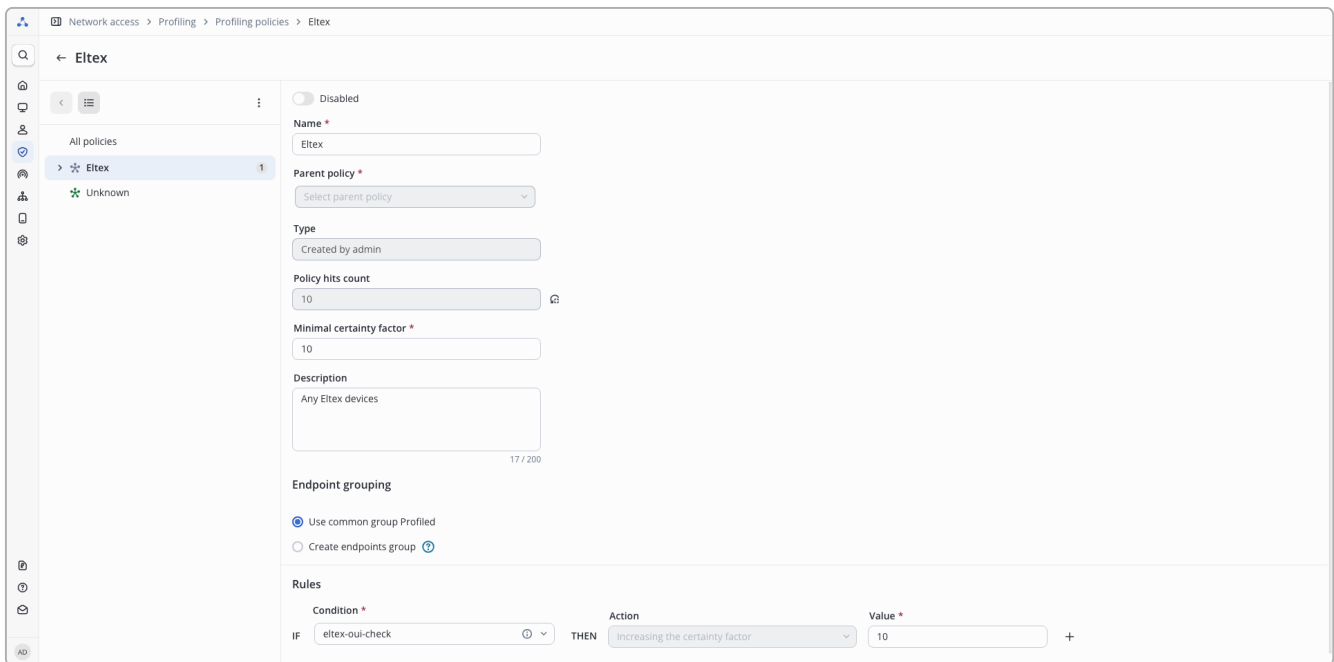


Figure 304. Editing a profiling policy

After editing, click the **"Save"** button. The button is hidden until at least one change is made.

The **"Cancel"** button resets the changes made to their original state.

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.

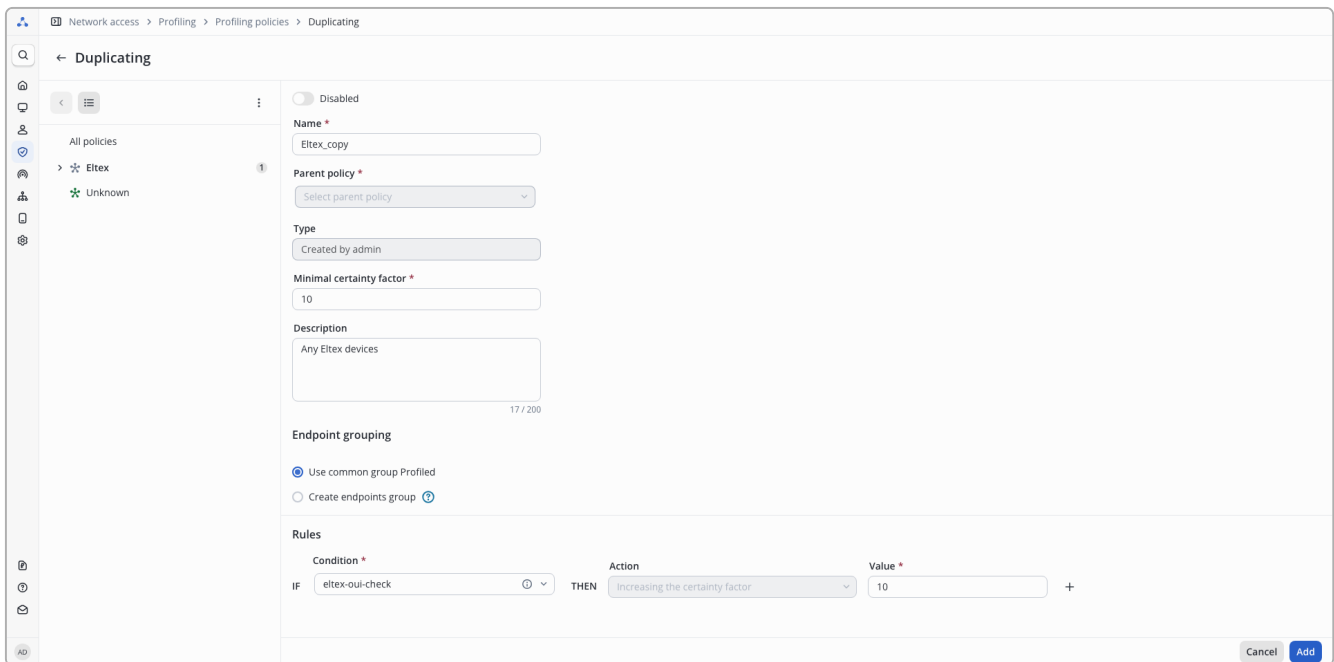




Figure 305. Copying profiling policy

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.



Deleting items requires confirmation in the modal window. The selected items will be deleted only after explicit confirmation of the operation.

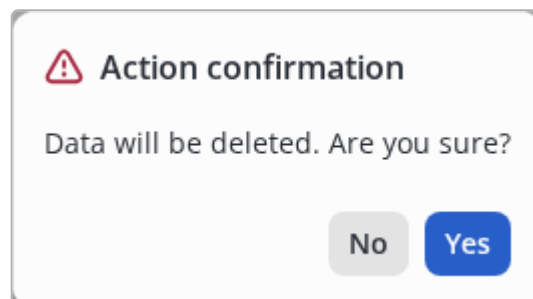


Figure 306. Modal dialog for confirmation



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.

Description of the profiling process

How the certainty factor works

The profiling policy checks whether the conditions added to the **Rules** section match the existing endpoint profiling data:

- For the MAC OUI profiling condition, the vendor MAC name and the value specified in the settings are determined (according to the operator selected). If the check is successful, the endpoint certainty increase the value specified in the **Value** column (10 by default).
- For DHCP profiling conditions, the presence of the corresponding DHCP attribute and its compliance with the specified in the profiling condition are checked. If the check is successful, the endpoint certainty level is increased by the value specified in the **Value** column (default 10).
- After checking all the rules configured in the profiling policy, the value of the endpoint certainty level is generated. This certainty level is the sum of all values specified in the profiling conditions to which the checking endpoint samples match.
- The obtained endpoint certainty level is compared with the value specified in the **Minimal certainty factor** value of the profiling policy.
- If the minimum certainty level of a profiling policy is less than or equal to the certainty level obtained from the endpoint check, the endpoint is considered to be compliant with the policy and is assigned the profiling policy and the endpoint group specified in profiling policy settings.



The certainty level is identified only within one profiling policy, for which the endpoint compliance check is performed. No values from other policies are used!

How the endpoint is checked against profiling policies

An endpoint profiling process contains:

- The root level of profiling policies looks for a suitable profiling policy endpoint from the added by the system user.
- If the endpoint does not match under any profiling policy added by the system user or they are not configured: the default profiling policy * Unknown * is assigned and the endpoint is placed in the * Unknown * group, after that the profiling process ends there.
- If a suitable profiling policy added by the system user is found, it checks if it has child profiling policies - if its do not exist, the endpoint is assigned the found profiling policy and the group specified in its **Endpoint grouping** setting. If the root policy is set to 'use common group Profiled', the endpoint is placed in the * Profiled * system group. The profiling process ends there.
-

If the profiling policy has child policies, the endpoint matches the child policies. If the endpoint does not match any of the child policies, the check stops, the parent policy is assigned to the endpoint, and the group from the parent policy settings.

- If an endpoint matches someone child policy, it is assigned this profiling policy and a group from the settings of this policy. If the `Use parent policy endpoint group` setting is selected in the child policy, the group is assigned according to the parent policy settings.

Restrictions of profiling policy settings

There are the following limitations to consider when configuring profiling policies:

- Multiple policies that an endpoint can match cannot be configured at the same level of root or child profiling policies! In such a situation, it is necessary to change the settings of the profiling policies in order to ensure that only one of them can profiling each endpoint at level! To more detail profiling endpoints, use child policies.
- Within one profiling policy, the minimum trust level cannot be greater (but can be less than or equal to) than the sum of all trust levels specified in its rules.
- After disabling a profiling policy, its child policies are also no longer used for profiling, even if they are enabled.
- The default **Unknown** policy cannot be deleted or changed. Child policies cannot be created for it.
- If the endpoint does not match the requirements of any configured profiling policies, it is considered to comply with the default policy * Unknown *.
- If an endpoint has manually assigned a profiling policy or an endpoint group, those setting cannot be changed based on the results of profiling. To resume auto-profiling disable manual policy assignment or manual group assignment.

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.

Name ↑	Type	Description
IP Phone	Created by admin	Profile for all ip phones

Figure 307. 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:

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

Adding a logical profile

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

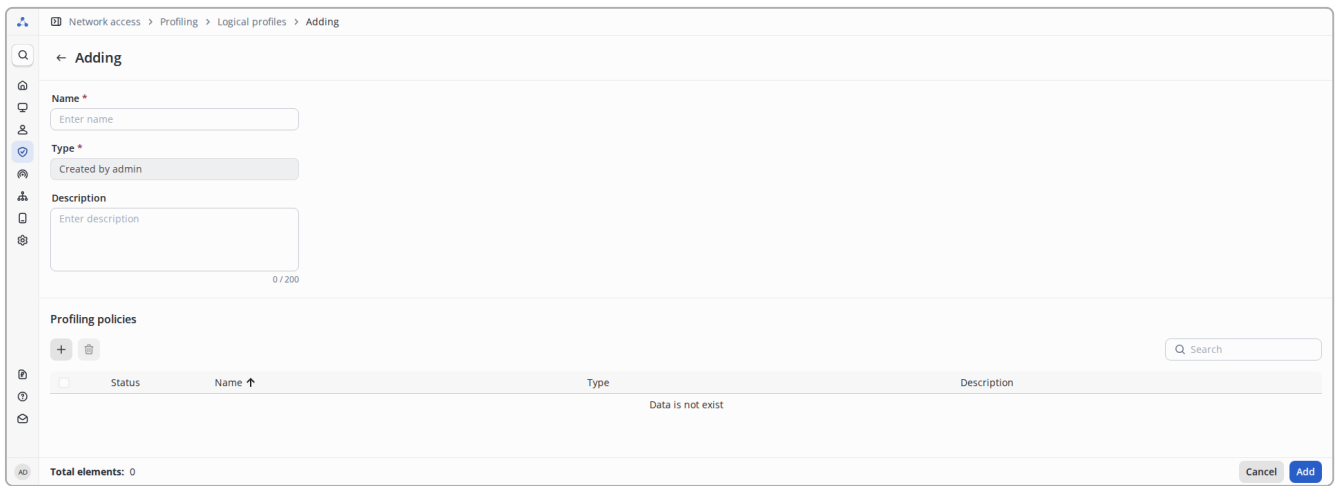


Figure 308. Logical profile addition page

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.
- **+** - 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.

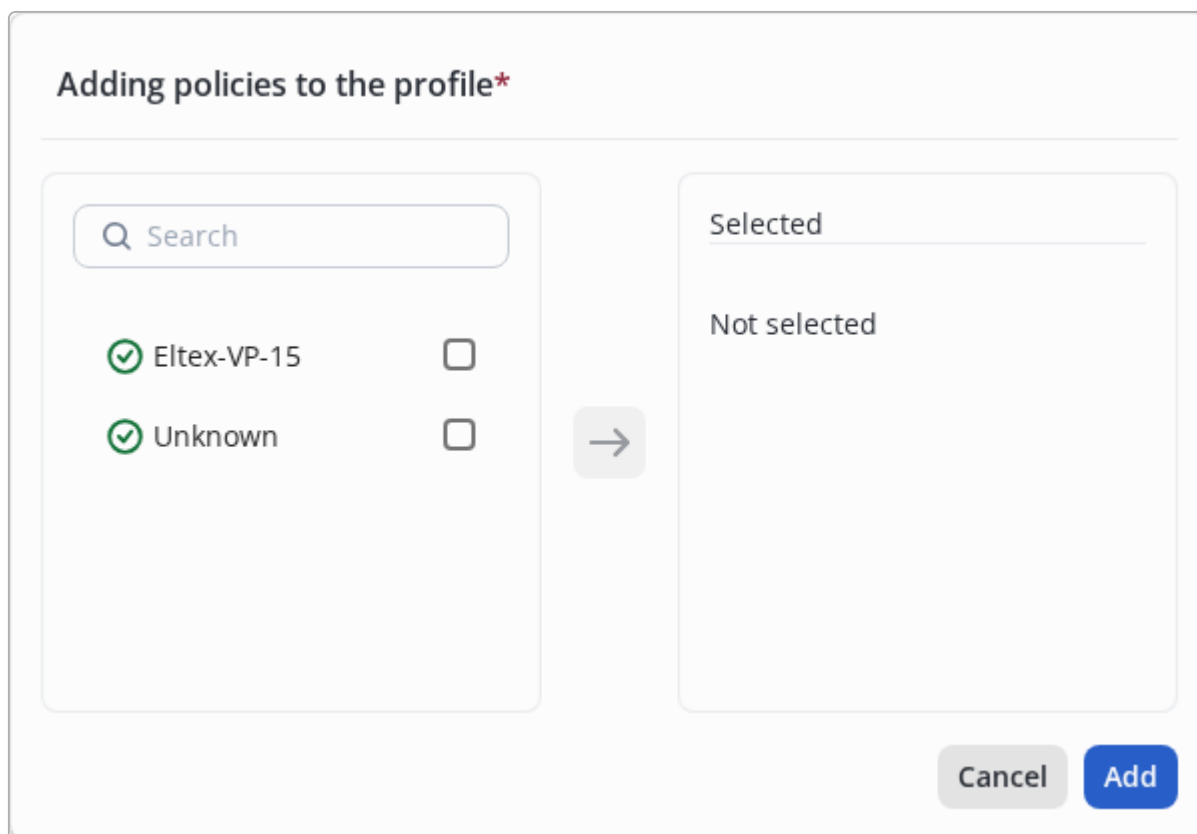




Figure 309. Modal dialog for adding profiling policies

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.

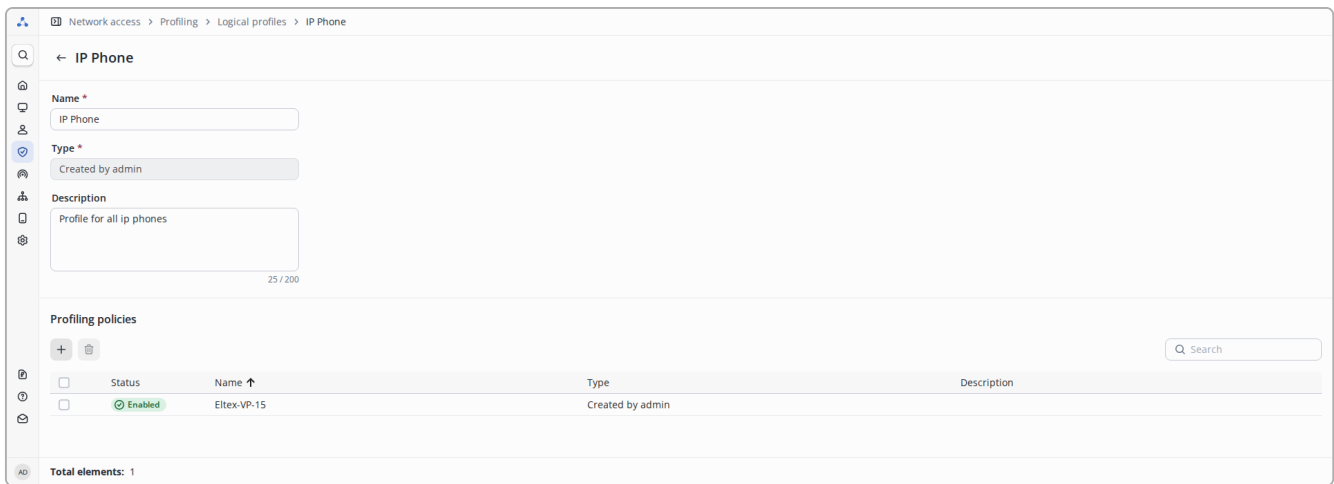


Figure 310. Logical profile edition page

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

The **"Cancel"** button resets the changes made to their original state.

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.

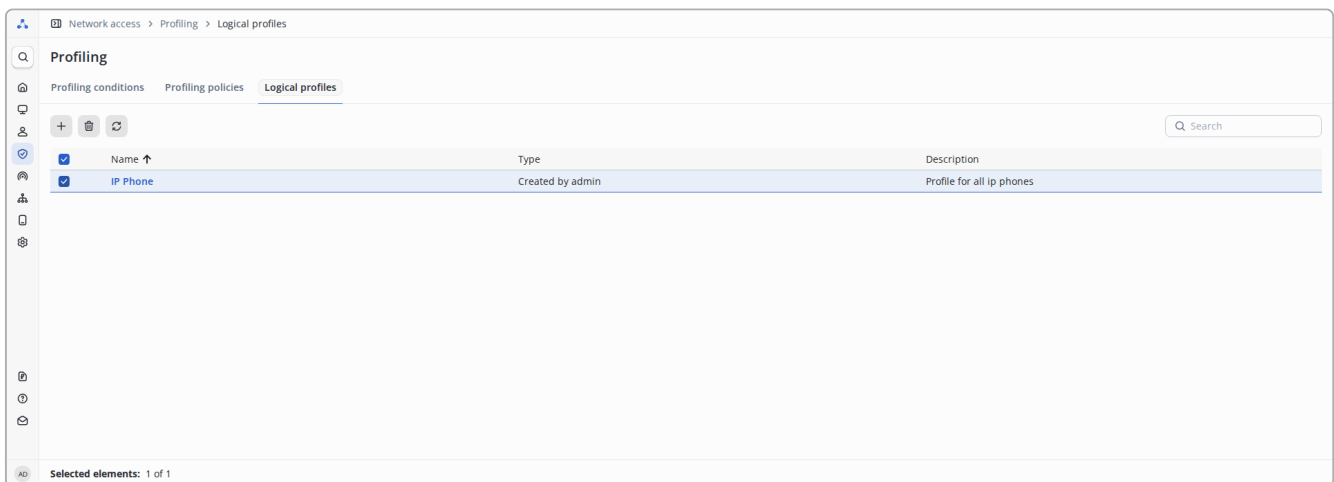


Figure 311. Selecting profiles for deletion



Deleting items requires confirmation in the modal window. The selected items will be deleted only after explicit confirmation of the operation.

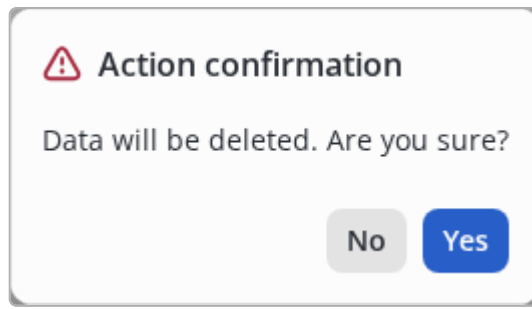


Figure 312. Modal dialog for confirmation



Restrictions:

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

Guest portals

Guest endpoints



This section provides information about functionality available with the **ADVANCED** level license. To purchase this functionality, contact your manager or write to the e-mail address eltex@eltex-co.ru.

Description

Guest endpoints are [endpoints](#) that have passed portal authorization in NAICE. Such endpoints are automatically added to the system and stored for the duration specified in the settings of the [portal](#) through which the user connected. If an endpoint is in the list, the corresponding user can connect to the network without portal authorization (authorization will be performed via MAC Authentication Bypass, or MAB).

A guest endpoint's uniqueness is determined by the combination of the client device's MAC address and the SSID (wireless network identifier) through which the device connects. In practice, this means that when the same user connects from different devices, multiple guest endpoints are created — one for each device. Similarly, multiple guest endpoints are added when the same device connects to several different wireless networks.

Unlike [common endpoints](#), guest endpoints with randomly generated MAC addresses are automatically added to the system.

Manual addition or editing of existing guest endpoints is not available.

Viewing the Endpoint List

<input type="checkbox"/>	Username	Identity source name	Portal name	MAC address	SSID	Last activity date ↓	Creation time
<input type="checkbox"/>	Maria_982	Maria_982 Device	Default Portal	27:ad:7e:b8:da:8d	CompanyWiFi	13.11.2025 03:47:54	10.11.2025 12:36:12
<input type="checkbox"/>	Petr_820	Petr_820 Device	Default Portal	61:a7:2c:4b:13:f2	CompanyWiFi	12.11.2025 20:37:49	09.11.2025 23:01:42
<input type="checkbox"/>	Pavel_160	Petr_820 Device	Default Portal	c4:e1:71:e4:27:fa	CompanyWiFi	14.11.2025 09:05:07	09.11.2025 06:03:59
<input type="checkbox"/>	Petr_657	Petr_820 Device	Default Portal	5c:0e:93:cb:5c:7d	CompanyWiFi	13.11.2025 07:03:32	09.11.2025 15:04:56
<input type="checkbox"/>	Artem_761	Petr_820 Device	Default Portal	ec:7cbc:13:66:eb	CompanyWiFi	14.11.2025 02:53:10	13.11.2025 01:04:52

Figure 313. Viewing the Endpoint List

This page contains a table listing all guest endpoints.

By default, the table includes the following columns:

- **Username** – The username with which the endpoint last authenticated.
- **Identity source name** – The source where the user was found during authentication.
- **Portal name** – The portal where the user authenticated.

MAC address – The endpoint's MAC address in the format "XX:XX:XX:XX:XX:XX".

- SSID – The name of the wireless network to which the user connected during portal authorization.








The network name is obtained from the RADIUS attribute Called-Station-Id, which is expected in the format <AP MAC address>:<SSID>, for example: ec-b1-e0-2b-02-b0:naice-guest-portal-test.

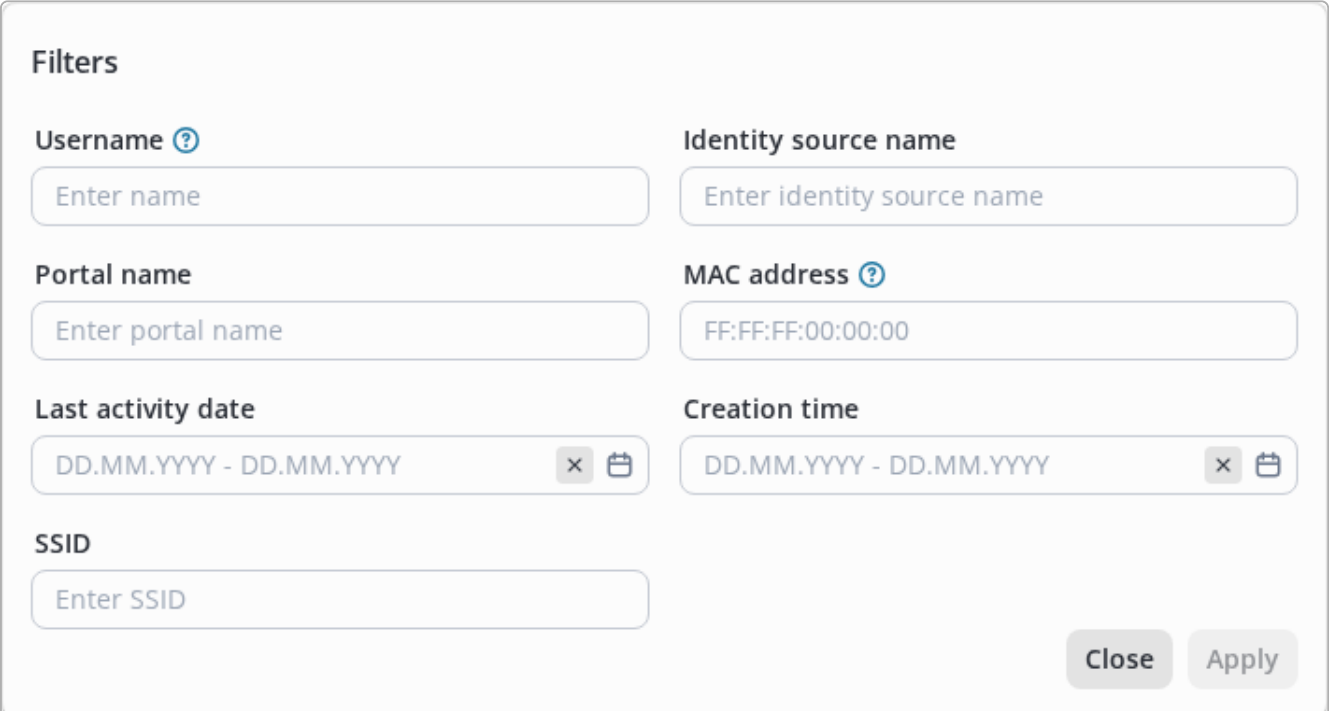
- Last activity date – The time of the endpoint's last authorization or reauthorization.
- Creation time – The time of the endpoint's first portal authorization.

Sorting is available in ascending and descending order for all columns except MAC Address. By default, sorting is applied in ascending order by the Last activity date column.


The page includes the following controls:

-  – Refresh the table data.
-  – Configure the table columns' visibility.
-  – Delete selected items (disabled until at least one item is selected).
-  – Toggle the current sorting order.
- – Checkbox for selecting items to perform further actions (e.g., deletion).
-  **Filters** – Open the filtering settings window for the table data.

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






Filters



Username 

Identity source name

Portal name

MAC address 

Last activity date  

Creation time  

SSID

Close **Apply**

Figure 314. Configuring Table Data Filtering

Filtering is available for all guest endpoint parameters.

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

The **Reset all** button is reset displayed columns to their default state.

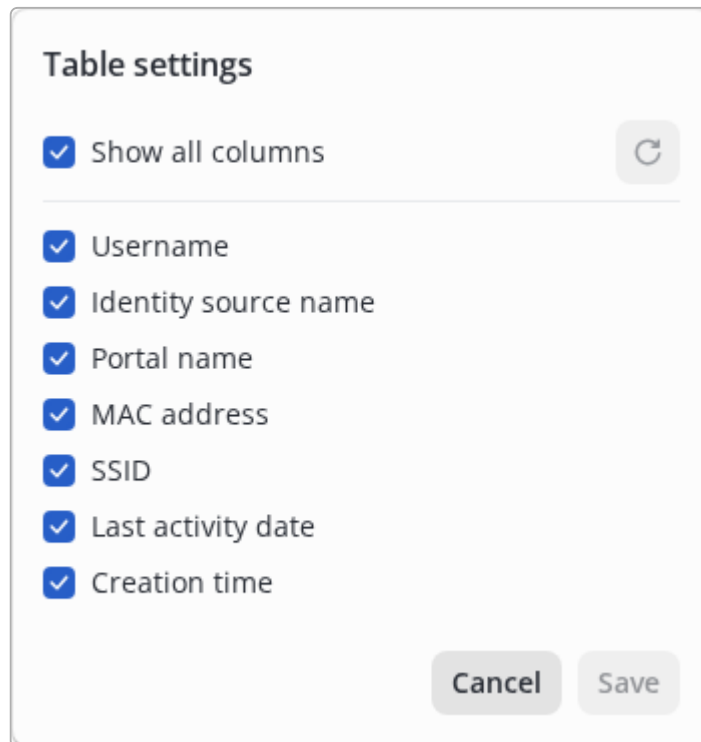


Figure 315. Configuring Visible Table Columns


Deleting an Endpoint



The guest endpoint table is automatically populated during normal NAICE operation as part of endpoint portal authorizations. If an endpoint is deleted, it will be rediscovered upon the next connection attempt. Disabling automatic endpoint learning is not possible.



Deleting a guest endpoint will require the client to reauthorize on the portal upon their next network connection.

To delete an endpoint, go to the viewing page, use the checkbox to select the desired endpoints, and then click  in the upper-left corner above the table.

Username	Identity source name	Portal name	MAC address	SSID	Last activity date ↓	Creation time
<input checked="" type="checkbox"/> Maria_982	Maria_982 Device	Default Portal	27:ad:7e:b8:da:8d	CompanyWiFi	13.11.2025 03:47:54	10.11.2025 12:36:12
<input type="checkbox"/> Petr_820	Petr_820 Device	Default Portal	61:a7:2c:4b:13:f2	CompanyWiFi	12.11.2025 20:37:49	09.11.2025 23:01:42
<input type="checkbox"/> Pavel_160	Petr_820 Device	Default Portal	c4:e1:71:e4:27:fa	CompanyWiFi	14.11.2025 09:05:07	09.11.2025 06:03:59
<input type="checkbox"/> Petr_657	Petr_820 Device	Default Portal	5c:0e:93:cb:6c:7d	CompanyWiFi	13.11.2025 07:03:32	09.11.2025 15:04:56
<input type="checkbox"/> Artem_761	Petr_820 Device	Default Portal	ec:7c:bc:13:66:eb	CompanyWiFi	14.11.2025 02:53:10	13.11.2025 01:04:52

Figure 316. Selecting Endpoints in the Table for Deletion



Deleting items requires confirmation in the modal window. The selected items will be deleted only after explicit confirmation of the operation.

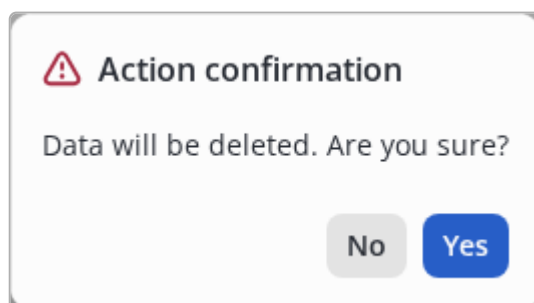


Figure 317. Modal dialog for confirmation

Portal users



This section provides information about functionality available with the **ADVANCED** level license. To purchase this functionality, contact your manager or write to the e-mail address eltex@eltex-co.ru.

Description

Portal users - an internal user source used for portal authentication. When configuring the [identity sequence](#), it appears under the name *Portal*. This source serves as a directory of all guest users regardless of connection success. A user present in this directory can authorize on the network via the specified [portal](#) using the provided username and password.

A key feature of portal users is the **self-registration** mechanism - users who log in via phone number using an SMS code (when this method is enabled in portal settings) are automatically added to this list. All account parameters are automatically filled for them. Besides self-registration, portal users can also be added manually.

Portal users are linked to the [portal](#) where they logged in or will log in later.



To enable authorization on different portals, a user with the same username and password must be added for each portal.



It is assumed that one portal is used for one wireless network ("**1 portal = 1 SSID**"). If the same portal is used in multiple wireless networks, a guest user who successfully authenticates on one SSID will be able to authorize on all SSIDs using this portal.

To prevent this, use an additional condition in [policy](#):

Normalised Radius · SSID Equals <SSID name> .

System users can view the list of registered portal users, delete individual entries, manually add new accounts, or edit existing ones.

Viewing Users

The screenshot shows a web interface for managing portal users. The breadcrumb trail is 'Guest portals > Portals management > Portals users'. The page title is 'Portals management'. There are tabs for 'Guest endpoints', 'Portals users', and 'Portal builder'. A search bar is present. The table has columns for 'Login', 'Portal', 'Notification gateway', 'Description', and 'Creation date'. There are three rows of data.

<input type="checkbox"/>	Login	Portal	Notification gateway	Description	Creation date ↓
<input type="checkbox"/>	Hayley_1	Default portal	gateway_1	Test user	17.11.2025 12:00:00
<input type="checkbox"/>	Zion_2	Default portal	gateway_2	Test user	16.11.2025 12:00:00
<input type="checkbox"/>	Mina_3	Default portal	gateway_3	Test user	15.11.2025 12:00:00

Figure 318. Table of guest users

This page contains a table listing portal user credentials.

The table includes columns:

- **Login** - username (must be unique for the specified portal);
- **Portal** - [portal](#) the user is linked to;
- **Notification gateway** - which [notification gateway](#) was used for self-registration;
- **Description** - optional user description;
- **Creation date** - automatically populated field with time of self-registration or manual user addition.

Sorting (ascending/descending) is available for the **Creation date** column. By default, sorting is in descending order.

Controls:

- — Add a new element.
- — Duplicate chosen element. Becomes active if only one element in the list is selected.
- — Delete selected elements (inactive until at least one element is selected).
- — Refresh table data.
- — Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).

↑ — Change the current sort order.

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

Adding Users

To pre-create an account for portal authentication via username/password, click **+** in the left field above the table.

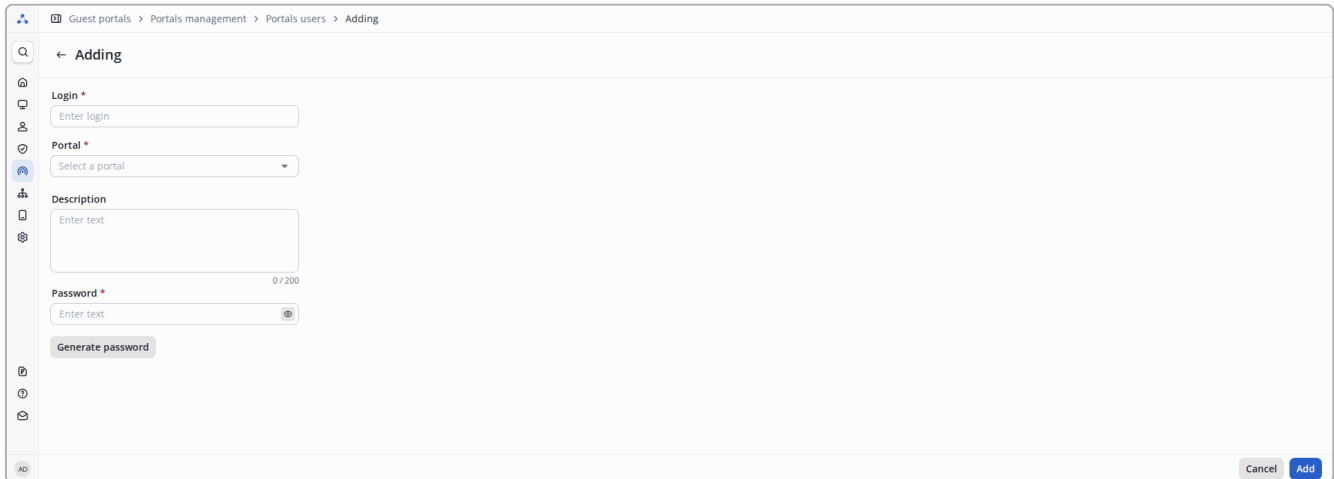




Figure 319. User addition page

The page contains these parameters:

- **Login *** - username. Must be unique per portal. Maximum length: 100 chars.
- **Portal *** - [portal](#) the user is linked to. Credentials only work for authorization on wireless networks using this portal.
- **Description** - optional description. Maximum length: 200 chars.
- **Password *** - user's password. Minimum length: 4 chars, maximum: 100 chars. Click  to toggle password visibility (hidden by default). Random password can be generated via *Generate Password* button and copied via .

Fields marked with * are required.

To add the user, click **Add**. To cancel and return to view page, click **Cancel**.

Editing Users

To edit an existing user, click their username in the table on view page.

An editing page will open, similar to addition page.

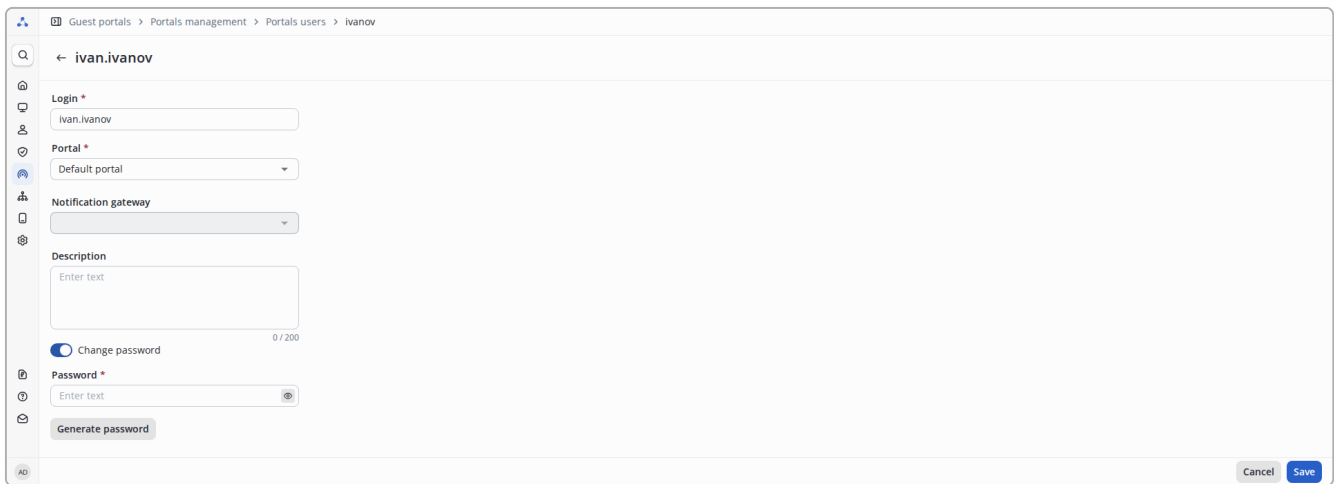


Figure 320. User editing page

When editing a guest user, the Notification gateway parameter - the gateway used for SMS registration - is shown for reference but cannot be edited.

To change password, toggle *Change password* and enter new password in the appearing field.

After editing, click the "Save" button. The button is hidden until at least one change is made.

The "Cancel" button resets the changes made to their original state.

Duplicating Users

A new portal user can be created based on existing one. Select user to copy using checkbox, then click .

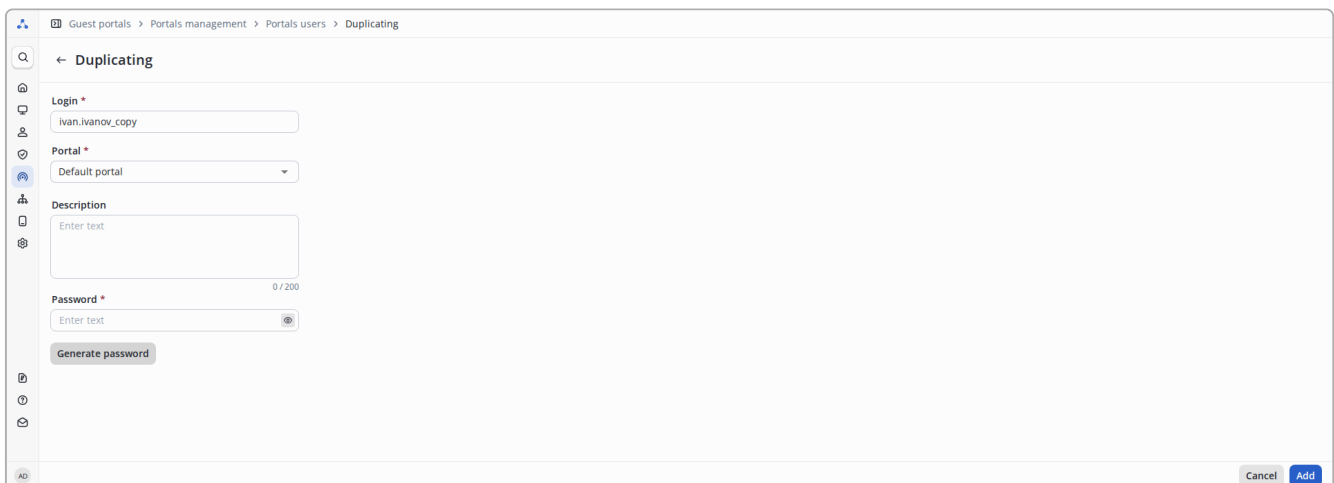


Figure 321. Duplicating a user

A form similar to addition page will open with all fields pre-filled from selected reference. By default "_copy" is appended to Login field. Any unused username can be chosen. Password must be specified.

Deleting Users

To delete users, select desired users using checkbox on view page, then click  in upper-left corner above table.

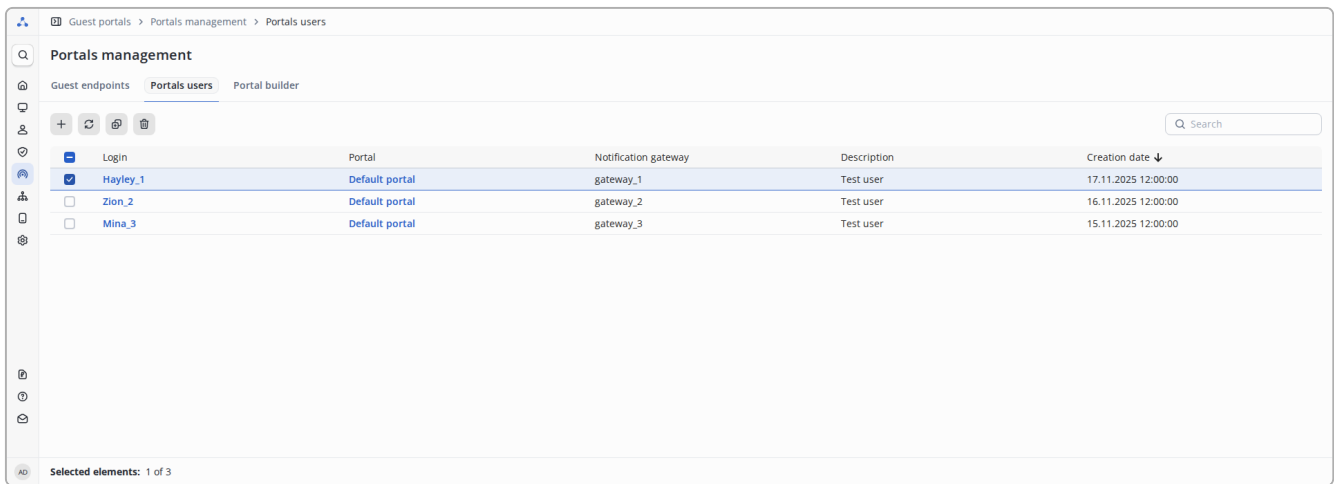


Figure 322. Selecting users for deletion



Deleting items requires confirmation in the modal window. The selected items will be deleted only after explicit confirmation of the operation.

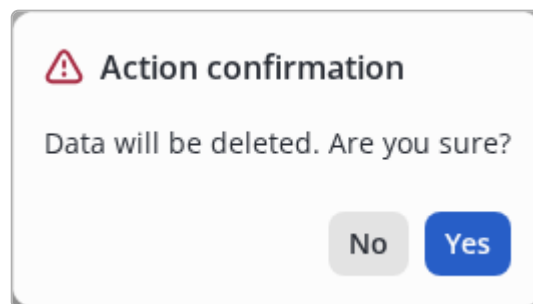


Figure 323. Modal dialog for confirmation



After deleting guest user, previously connected clients may still reconnect via MAB until associated [guest endpoint](#) is removed. Guest endpoint is automatically deleted after period configured in [portal](#) expires or can be manually removed anytime.

Portal builder



This section provides information about functionality available with the **ADVANCED** level license. To purchase this functionality, contact your manager or write to the e-mail address eltex@eltex-co.ru.

Description

The NAICE system includes a WEB portal as one of its components, which implements a hotspot client authorization model. An unknown user can freely connect to the access point (without obtaining a login and password in advance), but when attempting to access the internet via a browser, the user is redirected to the WEB portal page. Here, they can choose to either go through the authorization process or self-registration (e.g., via SMS). During the authorization procedures, the client navigates through various portal pages, the appearance of which can be customized to meet the needs of the wireless network operator.

For customization, the *Portal Builder* is used, allowing system users to configure the workflow and appearance of the portals. System users can create and delete portals, choose their background and content (text, images, color scheme), set up various authorization methods for each portal, and define post-login behavior.

Viewing the Portal List

The screenshot shows a web interface for 'Portals management'. At the top, there are navigation tabs: 'Guest endpoints', 'Portals users', and 'Portal builder'. Below the tabs is a table with the following data:

Status	Name ↑	Login type	Notification gateway	Redirect	Description	Preview
Enabled	guest	Via SMS, Login/password	Demo gateway	https://eltex.loc	Guest portal	Preview icon
Disabled	guest_copy	Login/password		https://eltex.loc	Guest portal	Preview icon
Enabled	test	Via SMS	Demo gateway	https://eltex-co.ru		Preview icon

At the bottom left of the table area, it says 'Total elements: 3'.

Figure 324. Viewing the Portal List

This page contains a table listing all portals.

The table includes the following columns:

- **Status** — the current activation state of the portal: **Enabled** or **Disabled** .
- **Name** — the portal's name.
- **Login type** — the authorization methods configured for the portal.
- **Notification Gateway** — the **gateway** used if SMS-based login is enabled.
- **Redirect** — the final redirect URL for successfully connected users.
- **Description** — an optional description of the portal.
- **Preview** — opens a preview of the portal in a new tab when clicking .

Sorting (ascending/descending) is available for the **Status** and **Name** columns. By default, sorting is applied in ascending order by portal name.

The page includes the following controls:

- — Add a new item.
- — Delete selected items (inactive until at least one item is selected).
- — Duplicate the selected item (becomes active only if a single item is selected).
- — Change the current sorting order.
- — Checkbox for selecting items for further actions (e.g., deletion).

Adding a Portal

To add a new portal, click in the left part of the field above the table on the portal list page. The following page will open:

Figure 325. Portal Global Settings Page

Portal configuration occurs in 3 stages: global settings, appearance settings, and page settings. Only the first stage is mandatory; the remaining two can be skipped. In this case, the portal's appearance and content will remain as per the default settings.

Global Settings

The following parameters are available for configuration:

- **General Parameters**

- **Status** — the current activation state of the portal: ✔ Enabled or ✘ Disabled. Authorization is unavailable on disabled portals.
- **Name *** — the portal's name.
- **Description** — an optional description of the portal.

- **Authentication**

- **Primary login method *** — the authentication method displayed to the user first.
- **Additional login method** — an alternative authentication method.
- **Notification gateway *** — the [gateway](#) used if SMS-based login is enabled.
- **Identity sequence *** — the list and order of sources where user credentials will be searched when using login/password authentication.



Identity sources can include both dedicated [guest users](#) and regular [users](#) or users from [external sources](#).

- **Additional Settings**

User agreement for using the portal — enabling this setting adds a "User agreement" page.

- Confirmation of the user agreement * — requires the user to agree to the User agreement.
- Guest account expiration date — the time after which [guest endpoints](#) associated with this portal will be automatically deleted. Once deleted, the user will need to go through portal authorization again.
- Redirect URL after successful login — the final redirect URL for successfully connected users.



Different client devices may exhibit varying behavior after successful authorization. Some devices may automatically close the pop-up window upon detecting internet access, preventing the user from seeing the final redirect page.

Parameters marked with an asterisk * are mandatory.

After completing the configuration, click **Next** or select the next stage from the top of the page.

Appearance

This stage focuses on configuring the portal's visual parameters, such as color scheme and displayed images.

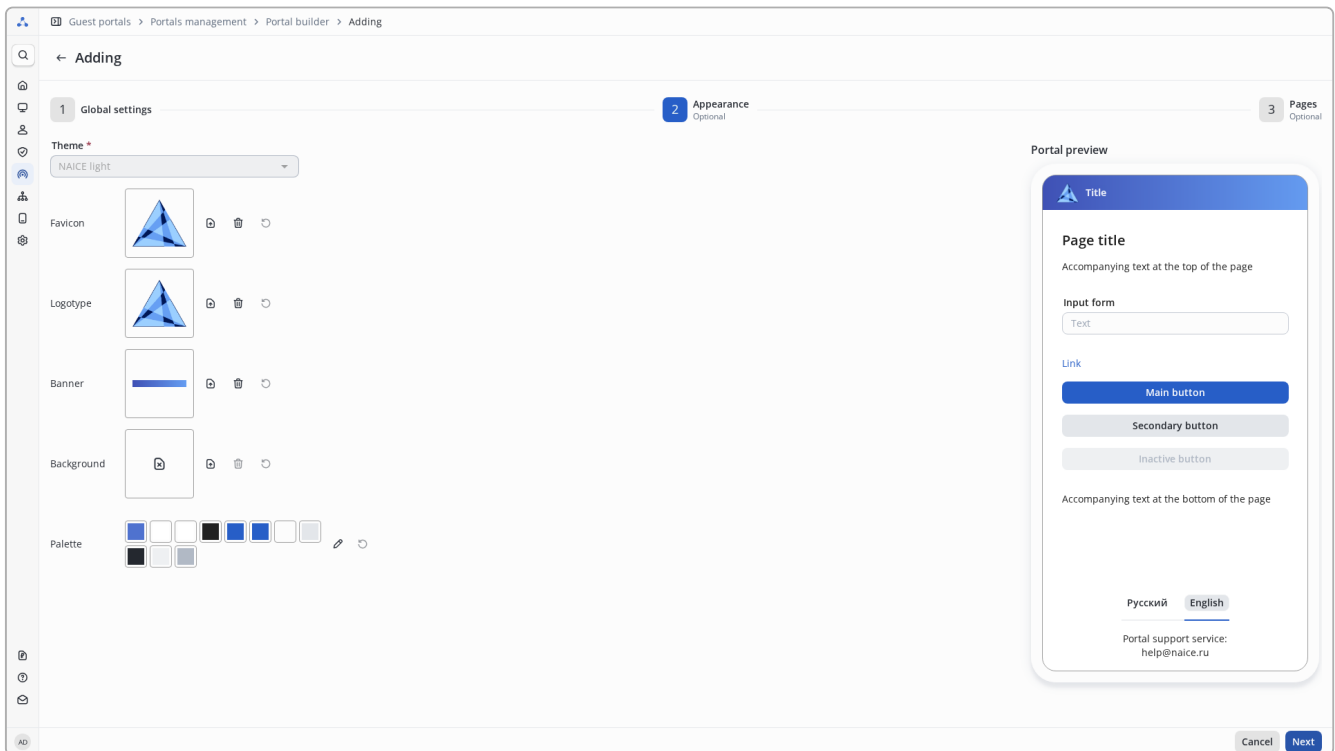


Figure 326. Portal Appearance Settings Page

The following parameters are available for configuration:

- **Favicon** — the icon displayed in the browser tab next to the page title, as well as in other places like bookmarks or search results.
- **Logotype** — the icon displayed in the header at the top of the page.
- **Banner** — the background of the header at the top of the page.
- **Background** — the image displayed as the page background below the header.
- **Palette** — the color scheme settings.

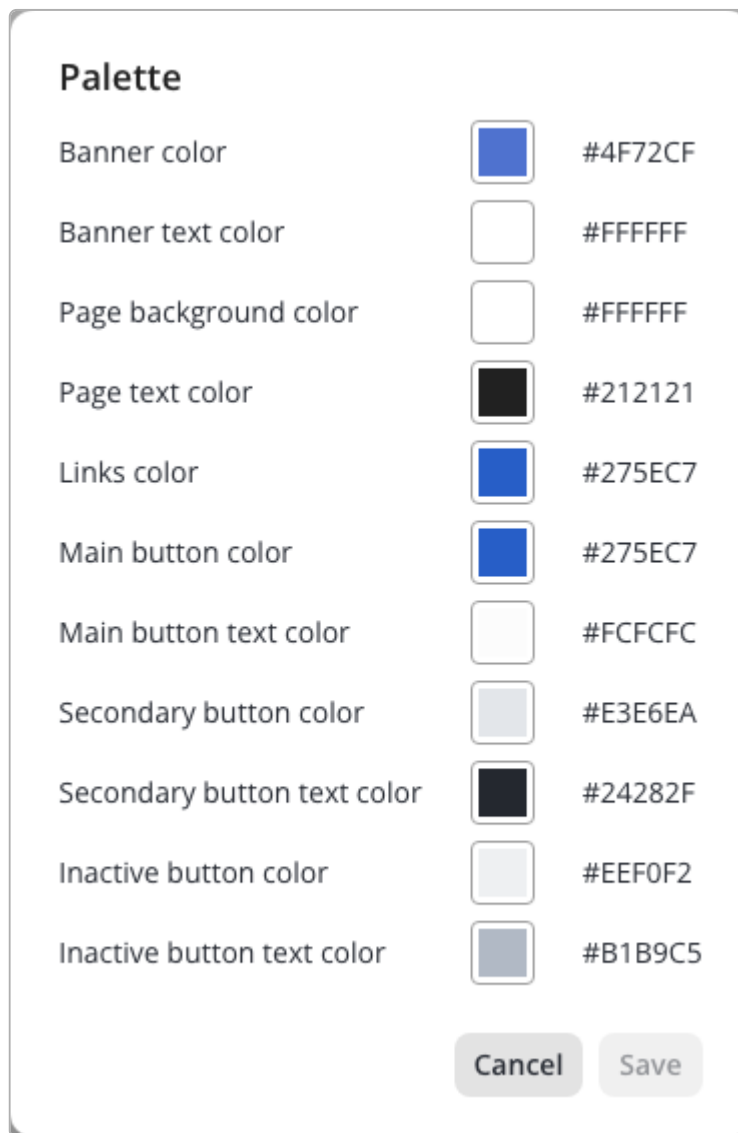






Figure 327. Palette



Banner and background images take precedence over color settings and are displayed on top.

The following controls are used:

-  — upload an image file;
-  — delete an image (it will no longer be displayed);
-  — reset the setting to default;
-  — edit the palette.

By default, the "NAICE light" theme is selected, and its parameters cannot be edited. To configure a custom theme, modify one of the above parameters.

Changes can be previewed in real-time using the preview panel on the right side of the page.

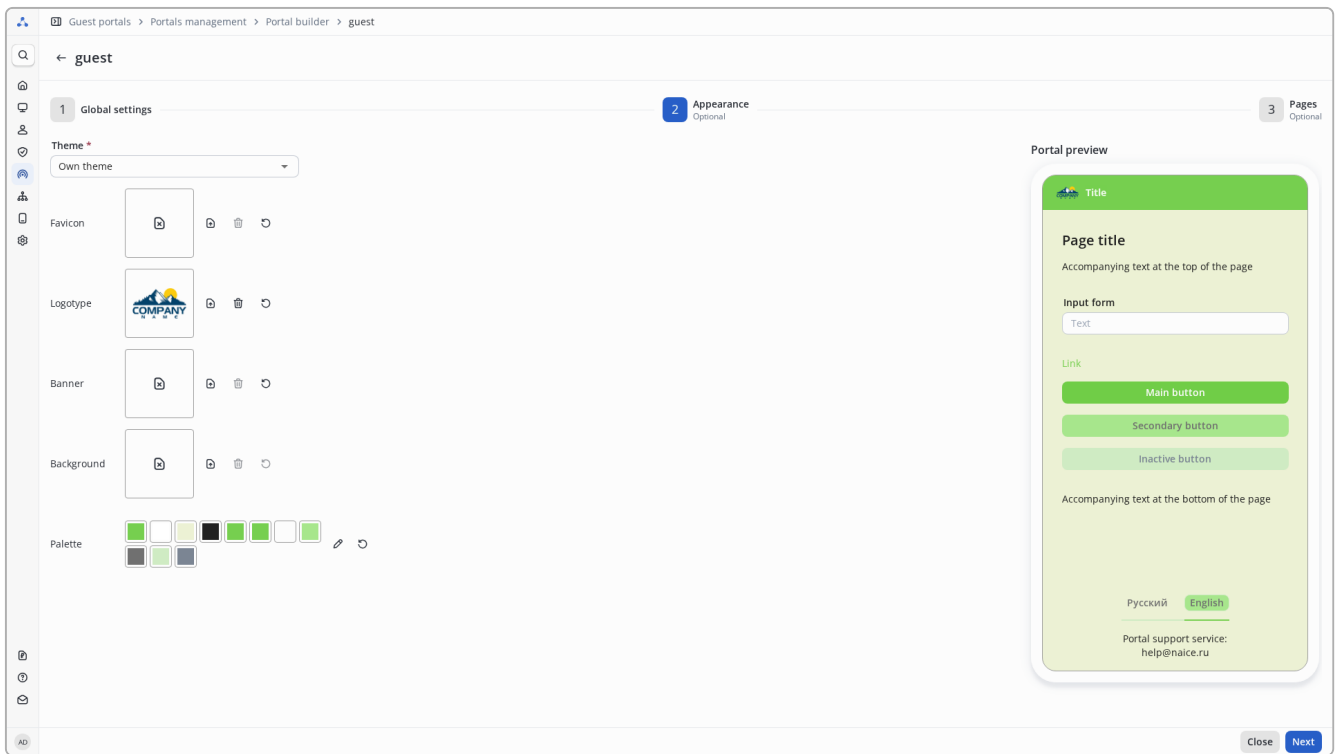


Figure 328. Custom Theme

Pages

This stage defines the text displayed on various portal pages in key functional elements—buttons, headers, info blocks, etc. The layout of these elements is not configurable.

It is important to note that the functionality of elements like buttons is predefined and does not change based on the configured text. For example, changing the text on the "Login" button will not alter its function—it will still trigger an authorization attempt.

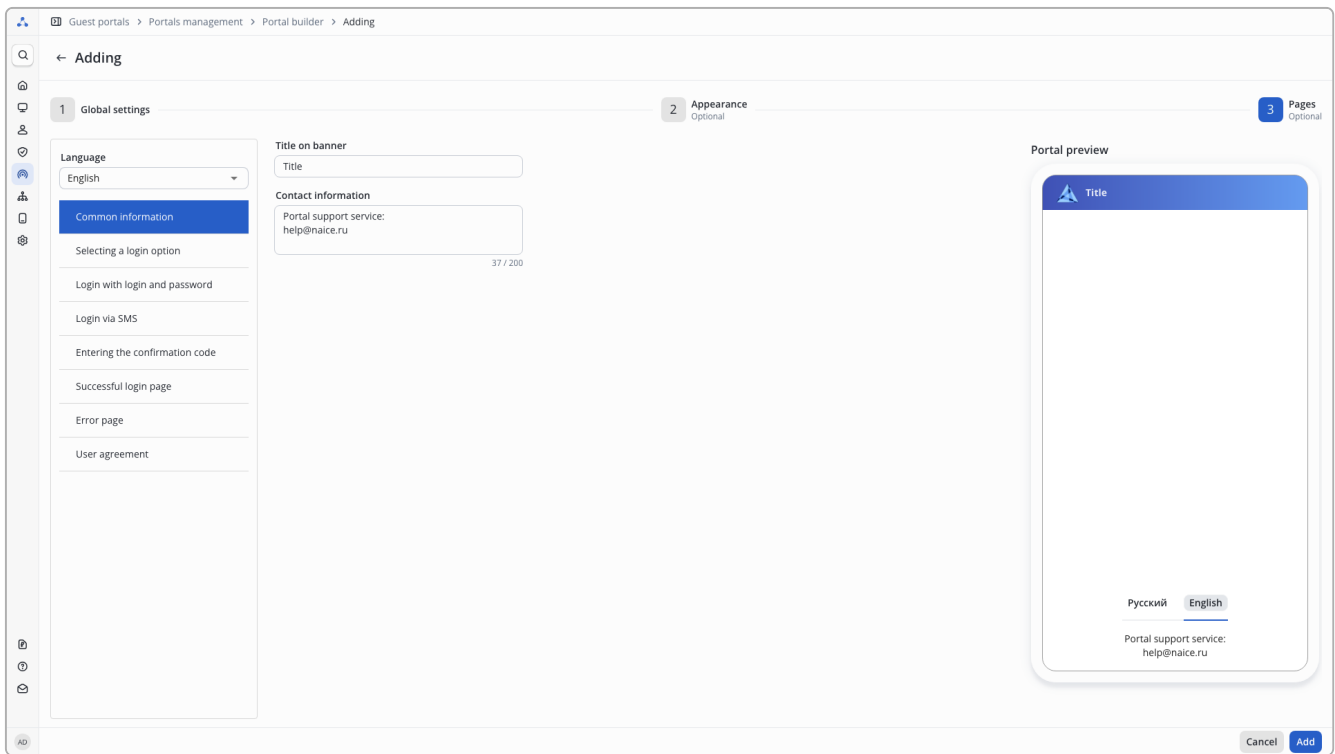


Figure 329. Configuring Page Content

The list of available pages depends on the settings configured in the [Global Settings](#) stage.

- **Common information** — configures the header banner text and footer text on all other pages;
- **Selecting a login option**
- **Login with login and password**
- **Login via SMS** — available only if SMS login is enabled; besides configuring page elements, it also sets the SMS message template sent to the user;
- **Entering the confirmation code**
- **Successful login page**
- **Error page**
- **User agreement** — available only if enabled in global settings; includes a text editor for formatting the terms of use.

Text can be configured separately for each supported language.

Changes can be previewed in real-time using the preview panel on the right side of the page.

After completing the configuration, click **Add**.

CAPTCHA Complexity Settings

When configuring the **Login via SMS** section, an important part of the process is setting the CAPTCHA complexity.

CAPTCHA is a user verification mechanism that requires entering a code from an image distorted by added noise (lines, dots, and high-contrast geometric shapes), the complexity of which varies depending on the

selected level.

The complexity level is configured on the **Login via SMS** page in the corresponding tab:

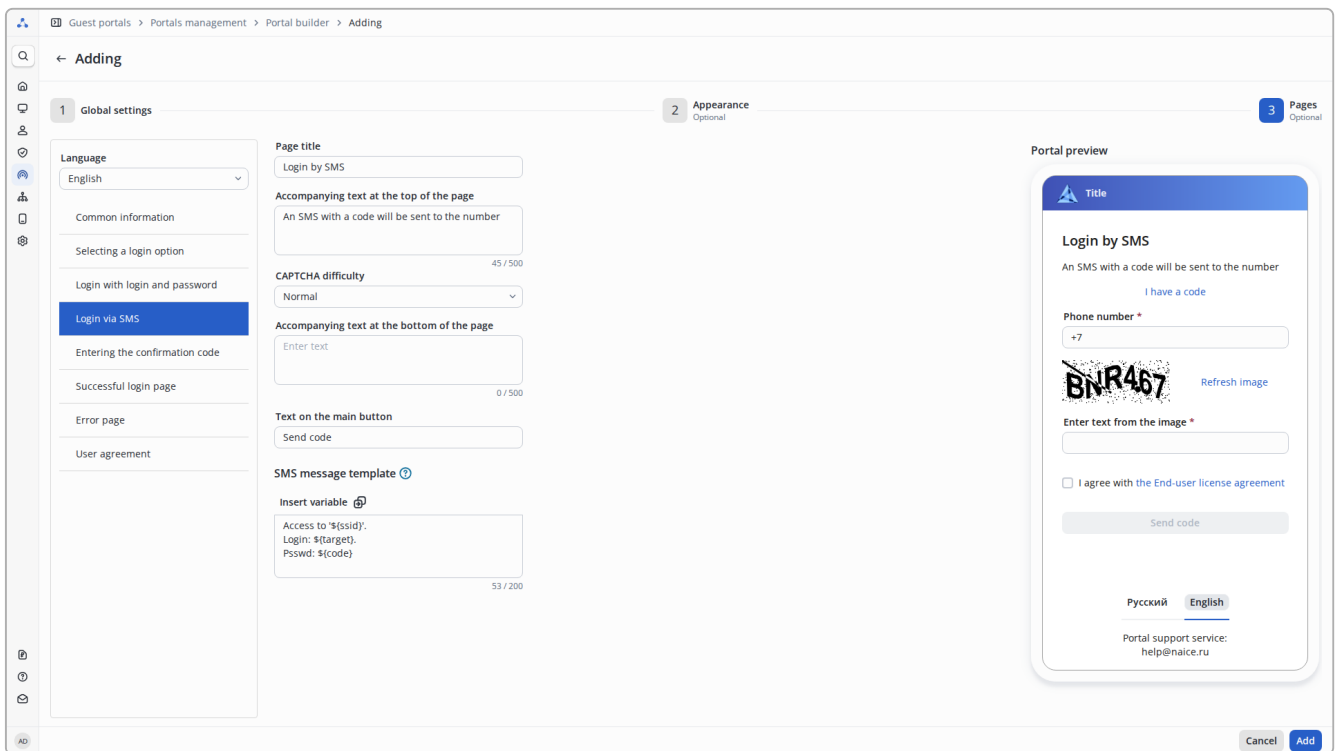


Figure 330. Login via SMS Page

There are four CAPTCHA complexity levels:

- **Disabled** — CAPTCHA is not used during user authorization.
- **Simple** — Minor changes; the code is distorted by a wave effect without additional geometric noise. Readability is high.



Figure 331. Simple CAPTCHA

- **Medium** — Wave distortion is combined with noise in the form of overlapping contrast dots, lines, and geometric shapes. Readability is medium.



Figure 332. Medium CAPTCHA

•

Complex — A larger number of dots is added; high-contrast geometric shapes occupy a larger portion of the code image. Readability is low.



Figure 333. Complex CAPTCHA

Editing a Portal

To edit an existing portal, click its name in the table on the portal list page.

<input type="checkbox"/>	Status	Name ↑	Login type	Notification gateway	Redirect	Description	Preview
<input type="checkbox"/>	Enabled	guest	Via SMS, Login/password	Demo gateway	https://eltex.loc	Guest portal	
<input type="checkbox"/>	Disabled	guest_copy	Login/password		https://eltex.loc	Guest portal	
<input type="checkbox"/>	Enabled	test	Via SMS	Demo gateway	https://eltex-co.ru		

Figure 334. Viewing the Portal List

The editing page will open, which is identical to the portal addition page.

All three configuration stages are immediately available for making changes.



System Behavior When Disabling a Previously Active Portal

- When a portal is disabled, previously connected clients retain the ability to reconnect via MAB until the associated [guest endpoint](#) is deleted. Guest endpoints are automatically deleted after the configured expiration period or can be manually deleted at any time.
- Guest endpoints will be deleted even if the portal is disabled. The current account expiration setting is applied, not the one at the time of portal deactivation.

After editing, click the **"Save"** button. The button is hidden until at least one change is made.

The **"Cancel"** button resets the changes made to their original state.

Duplicating a Portal

A new portal can be created based on an existing one. To do this, select the portal to copy using the checkbox, then click

A form identical to the portal addition form will open, with all fields pre-filled from the selected reference. By default, "_copy" is appended to the `Name` field. You can choose any other name not already in use.

Deleting a Portal

To delete portals, select them using the checkbox on the portal list page, then click  in the top-left corner above the table.



Deleting a portal will also automatically delete associated [guest users](#) and [guest endpoints](#). This will require reauthorization for previously connected clients.

Device access



This section contains information about functionality that is available as part of the additional **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



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

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 [Network 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

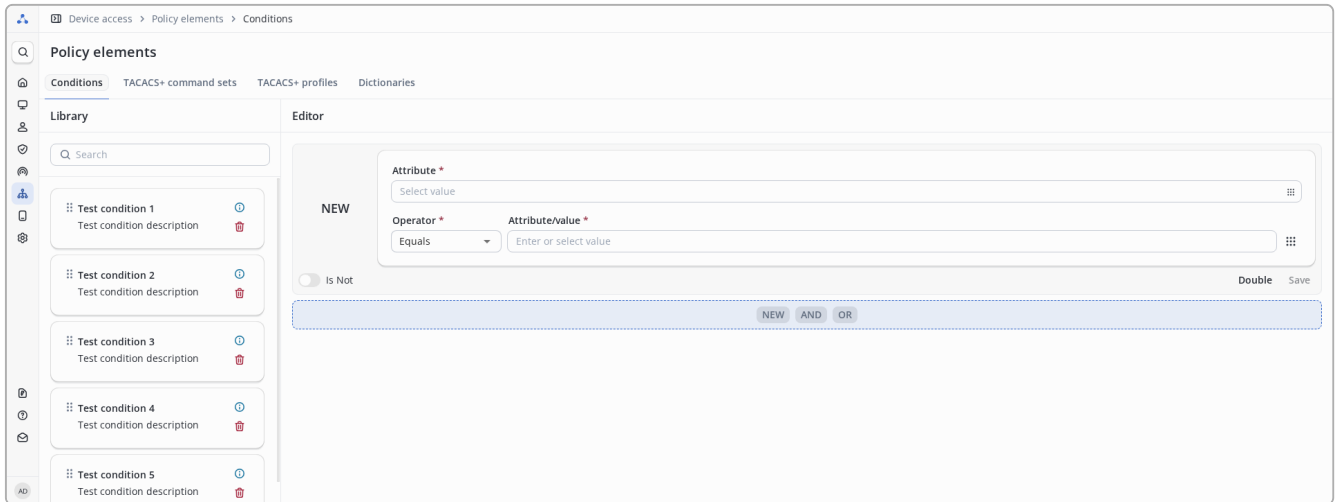


Figure 335. Library of logical conditions

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, there is also support for [regular expressions](#))
 - "IP range"
 - "IP net mask"
 - "Empty value"
- **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.

Select attribute for condition

All
 Device
 Identity
 LDAP
 Network Access
 TACACS+






	Dictionary	ID
<input style="width: 90%;" type="text" value="Search"/>	<input style="border-bottom: 1px solid #ccc;" type="text" value="Select dictionary"/>	<input style="width: 90%;" type="text" value="ID"/>
Attribute	Dictionary	ID
Device Location	Device	4
Device Profile	Device	2
Device Type	Device	3
Model Name	Device	1
Endpoint Group	Endpoint identity	4
Logical Profile	Endpoint identity	6
MAC-Address	Endpoint identity	1
Profiling Policy	Endpoint identity	5

Figure 336. 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**.

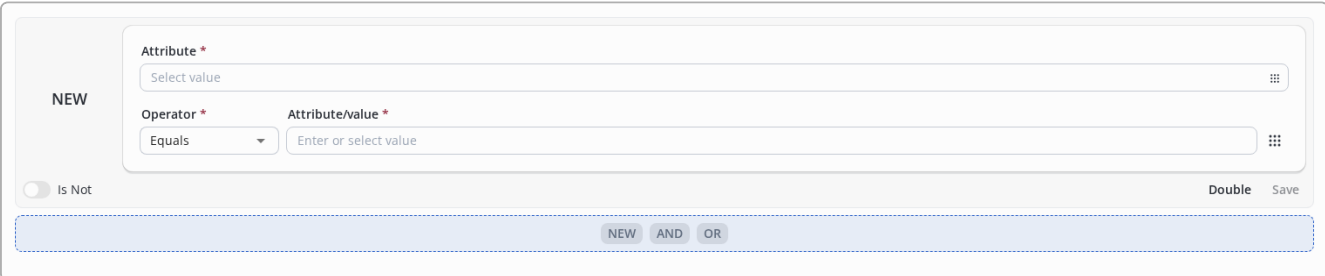



Figure 337. Initial state of Editor

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.

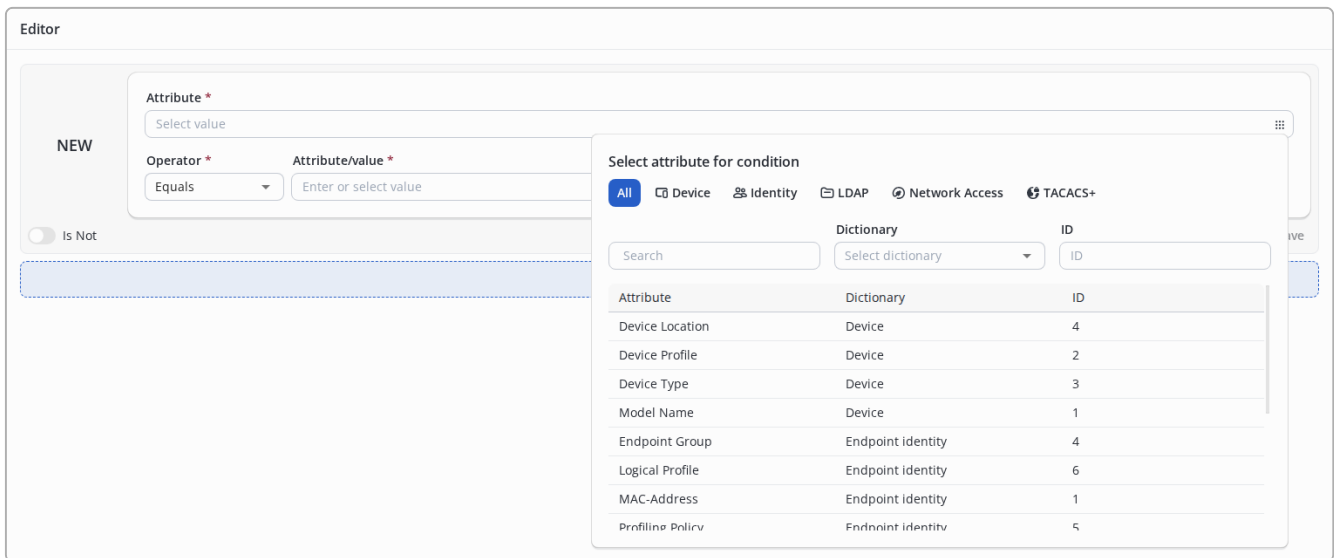


Figure 338. Attribute selection

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, Empty value
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, Empty value
IPv4 address	Equal to, Not equal to, Equal to NULL, Not equal to NULL, IP range, IP net mask, Empty value
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, Empty value
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 339. 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 340. 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 341. 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".

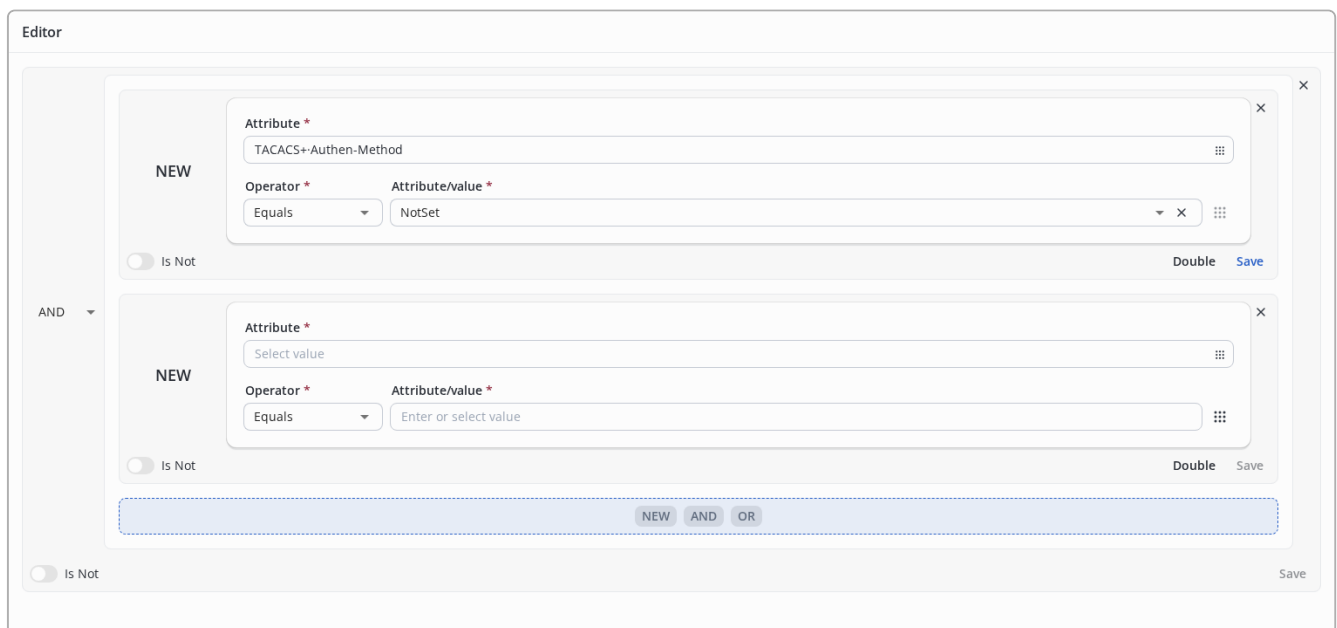


Figure 342. Condition consisting of two conditions combined by a logical "AND"

- 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 **X** at the top right in the condition window.
- To completely clear all conditions in the editor, click **X** 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.

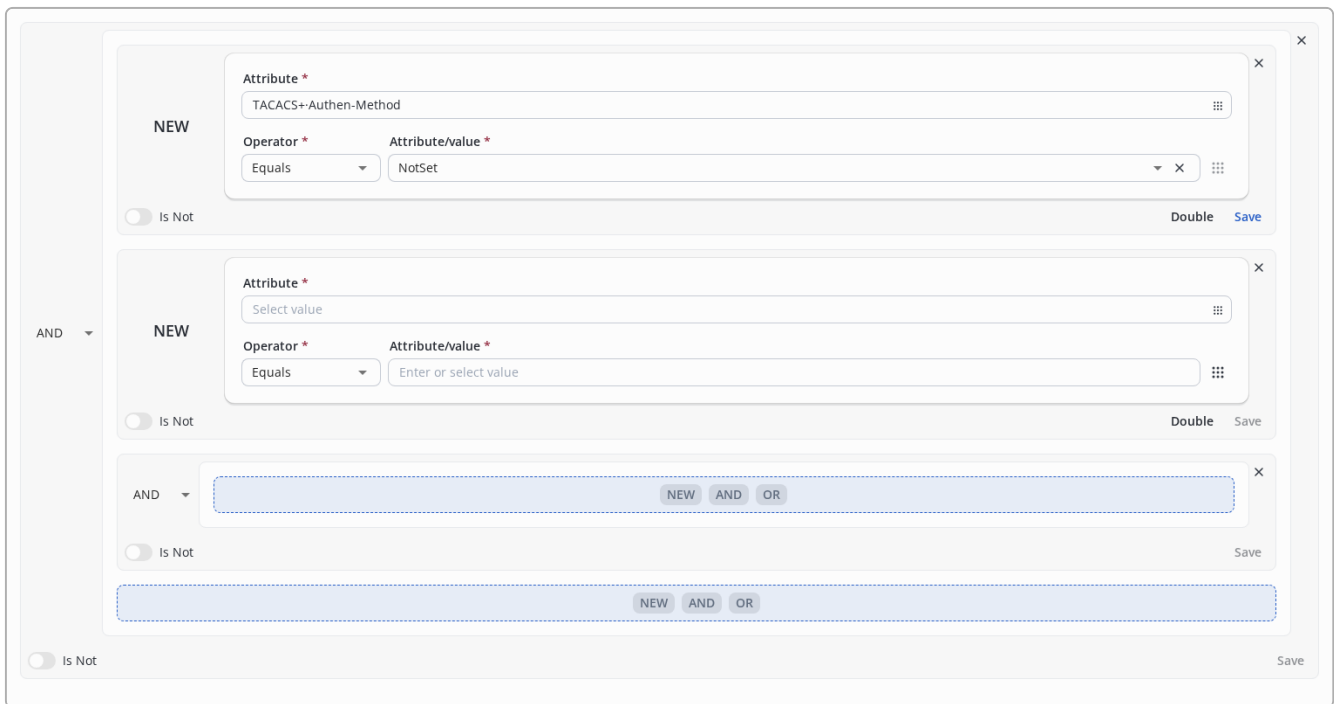


Figure 343. Condition containing nested rules

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

Using regular expressions

Regular expressions can be used when adding a condition to a policy set for attributes with the `matches` operator. This allows you to specify a "pattern" that can match multiple values using just one line.

Example 2. Using regular expressions in logical conditions

Task: You need to apply a policy set to all connections from devices whose names start with the `MES` prefix.

Possible Solution:

In order to select only connections from certain devices, you can use the `RADIUS NAS-Identifier` attribute in the condition. Note that it usually requires configuration on the NAS device to send it.

In order to avoid creating separate `RADIUS NAS-Identifier equals MES1` etc. conditions for each device, you can create one `RADIUS NAS-Identifier matches MES.*` condition.

The `.*` construct means "any number of any characters" after `MES`.

You can also use a more strict expression if, for example, you want `MES` to always be followed by 4 digits and one letter: `MES\d{4}[A-Z]`.

Here:

`\d{4}` — four digits;

`[A-Z]` — one uppercase letter.

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.



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.

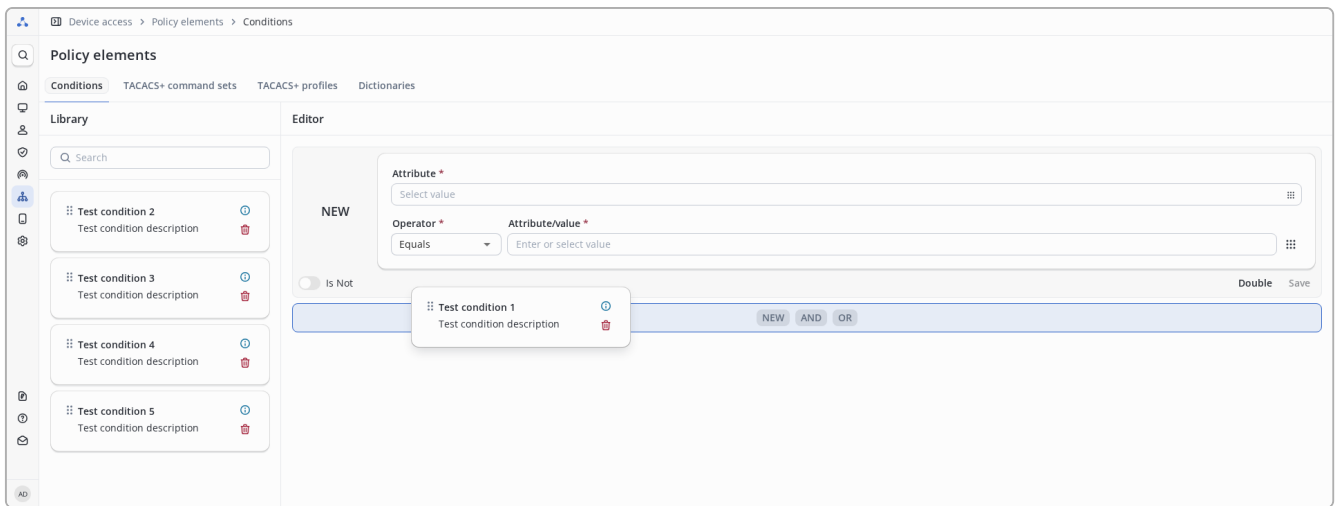


Figure 344. Selecting a logical condition

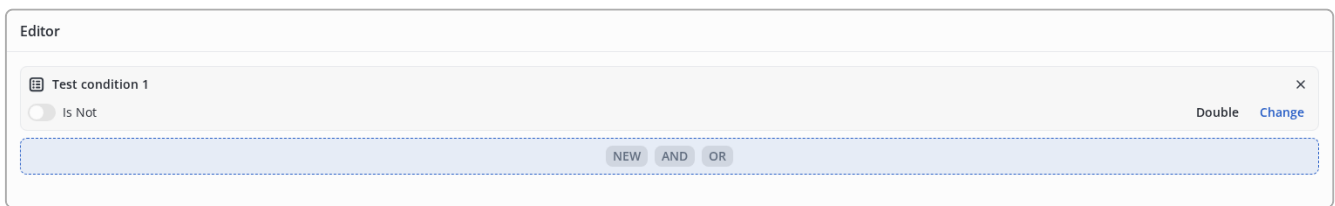



Figure 345. Editing a logical condition

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.

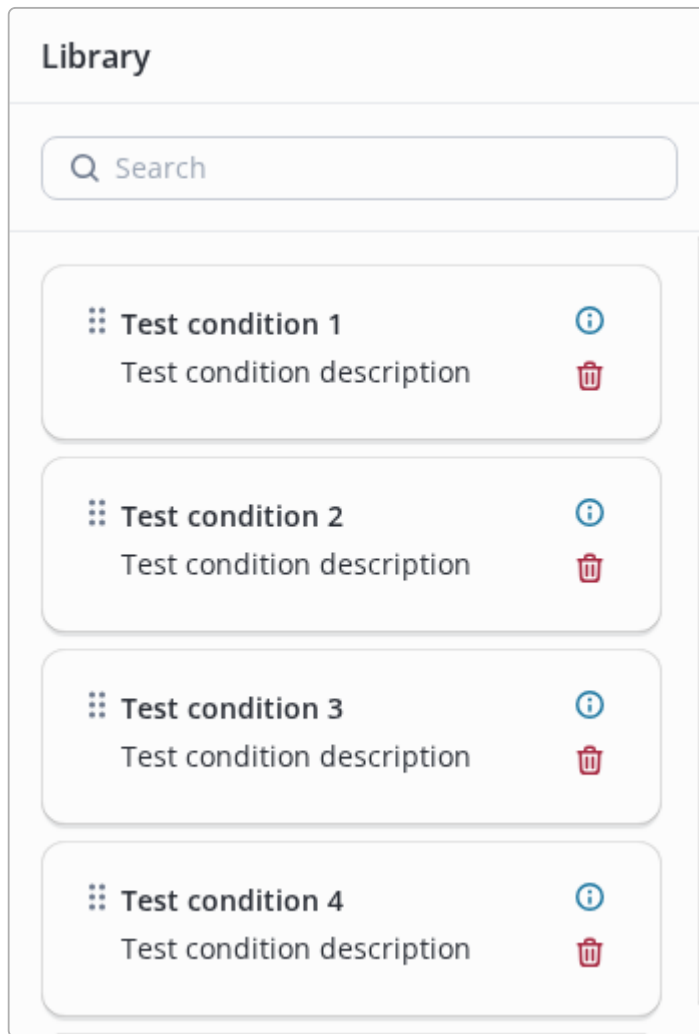


Figure 346. Selecting a condition to delete



Deleting items requires confirmation in the modal window. The selected items will be deleted only after explicit confirmation of the operation.

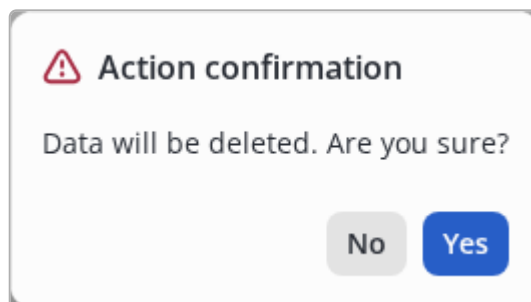


Figure 347. Modal dialog for confirmation



Restrictions:

- some system logical conditions cannot be deleted or edited;
- 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



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

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 [:policy-sets/index.html](http://policy-sets/index.html) when configuring the authorization policy.

Viewing TACACS+ Command Sets

This page contains a table listing all TACACS+ command sets.

Name	Description
Allow all	
Deny all	Deny All
Show only	
MES	
WLC	

Figure 348. Table with a list of TACACS+ command sets on the view page


The table contains columns:


- **Name** - the name of the command set.
 - - This entity is system and cannot be deleted or edited.
- **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:

- - Refresh table data.
- - Add a new element.
- - Duplicate the command set selected by the checkbox.
- - Delete selected elements (inactive until at least one element is selected).
- - Allows you to download data from a csv file.
- - Allows you to upload data to a csv file.
-

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

-  - Change the current sort order.
- - Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).

Adding a new command set

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

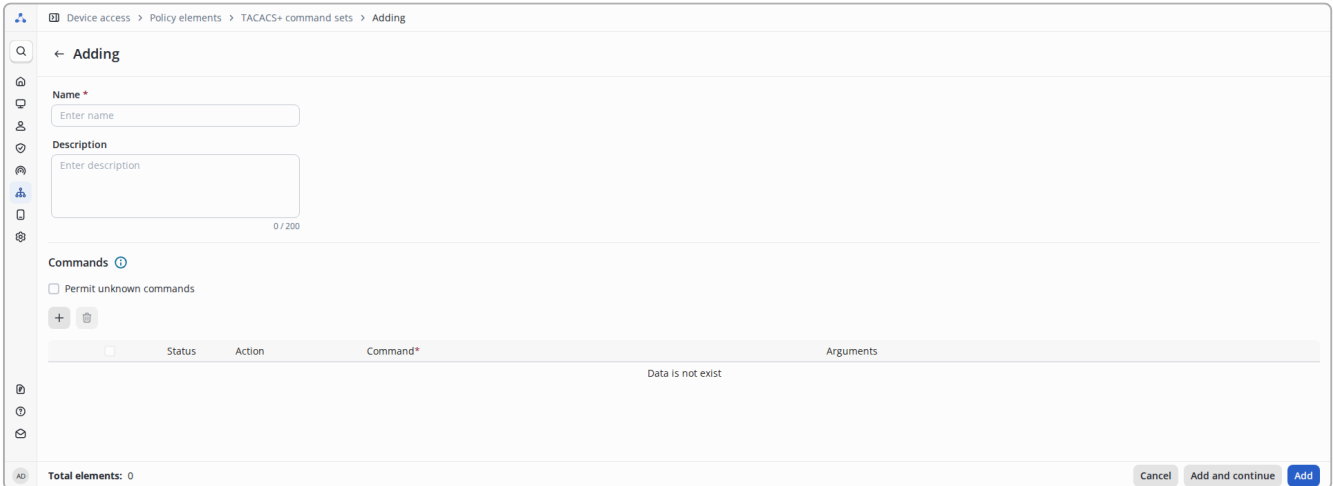



Figure 349. Form for adding a command set

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 in 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 [Using 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 [Using 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.

<input type="checkbox"/>	Name ↑
<input type="checkbox"/>	Allow all 
<input type="checkbox"/>	Deny all 
<input type="checkbox"/>	Show only 
<input type="checkbox"/>	MES
<input type="checkbox"/>	WLC

Figure 350. 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 the **"Save"** button. The button is hidden until at least one change is made.

The **"Cancel"** button resets the changes made to their original state.

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 3. 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 4. 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
<code>show</code>	<code>radius-servers</code>
<code>show</code>	<code>tacacs</code>

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


Command	Arguments
<code>show</code>	<code>(radius-servers) (tacacs)</code>

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.

<input type="checkbox"/>	Name ↑
<input type="checkbox"/>	Allow all
<input type="checkbox"/>	Deny all
<input type="checkbox"/>	Show only
<input checked="" type="checkbox"/>	MES
<input type="checkbox"/>	WLC

Figure 351. Select the set of commands in the table to delete



Deleting items requires confirmation in the modal window. The selected items will be deleted only after explicit confirmation of the operation.

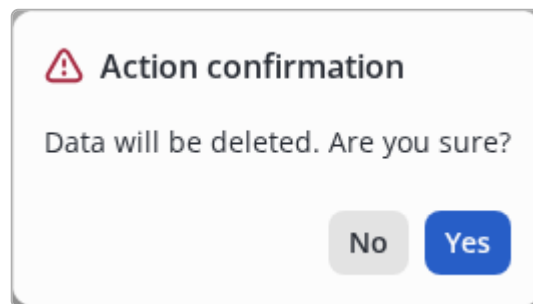


Figure 352. Modal dialog for confirmation



Restrictions:

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

Import

NAICE supports importing data from CSV files.

Preliminary preparation before Import

1. Create or verify the existence of necessary related entities (e.g., device profile).
2. Review the CSV file requirements:
 - Encoding must be UTF-8;
 - Delimiters:
 - Field delimiter: `comma (,)`
 - String/text delimiter: `double quotation mark (")`
 - Headers and values must be enclosed in double quotation marks (`"`)
 - Maximum file size is 2MB.
3. Check the file content for extraneous quotation marks before importing;
4. Check that the values containing the double quotation mark (`"`) or the slash (`/`) are correctly escaped.

- Values containing a double quotation mark (") are escaped using \"
- Values containing the slash (/) are escaped using \/

Correct spelling of values (with escaping using \") using the example of the contents of the file for importing the TACACS Command set

"name:Required"	"description"	"permit_unmatched(true/false)"	"commands(Grant/command/arguments/enabled;...)"
"command_set"	"\"Test command set\""	"false"	"PERMIT/\"show/vlan 1 2 \"/true"


Incorrect spelling of values (without escaping) using the example of the contents of the file for importing the TACACS Command set

"name:Required"	"description"	"permit_unmatched(true/false)"	"commands(Grant/command/arguments/enabled;...)"
"command_set"	"Test command set"	"false"	"PERMIT/show/vlan 1 2 /true"



Failure to escape these characters will lead to incorrect data recognition.

Import procedure

To import data from a CSV file, click on  in the action panel located above the table. This will open the import window:

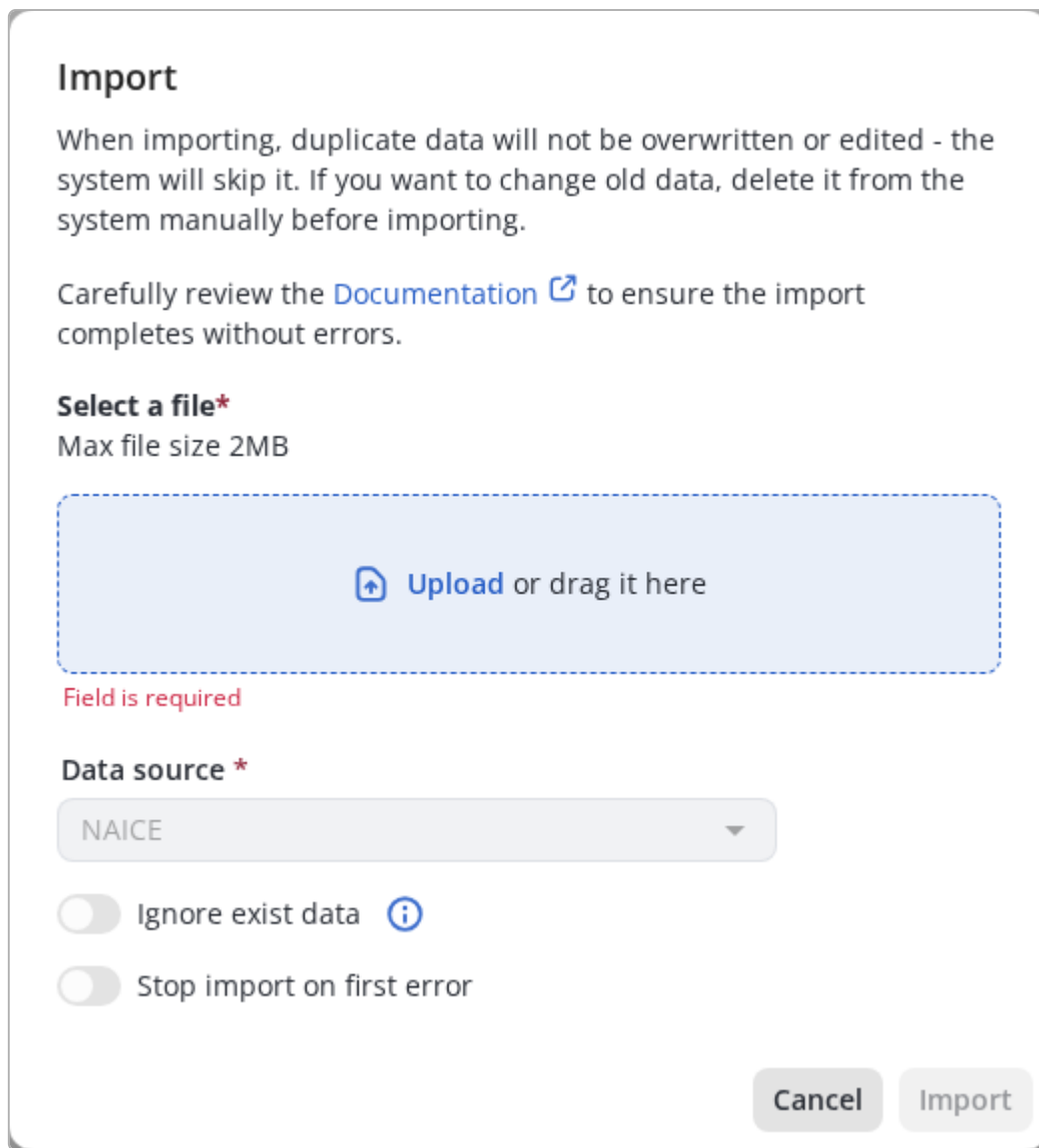


Figure 353. Window Import

Data import proceeds through several steps:

1. Select the required CSV file by dragging it into the upload area or by selecting it through the file explorer by clicking the "Upload";



To apply changes, you must re-upload an updated CSV file.

2. Select the data source (if not predefined);
3. Configure import flags (if needed):

Ignore exist data

- On: Duplicate records trigger warnings.
- Off: Duplicates are treated as errors.

Stop import on first error

- On: Import halts at the first error. Only records that were successfully processed before it occurred will be imported.
-

Off: Erroneous lines are skipped, and the import continues to the end. Only valid records will be imported.

4. To start the import, click the "**Import**".



When importing, duplicate data will not be overwritten or edited - the system will skip it. If you want to change old data, delete it from the system manually before importing.

Viewing the Import report

An import report window opens immediately after file processing.

If all records in the file were processed correctly, you will see the following window:

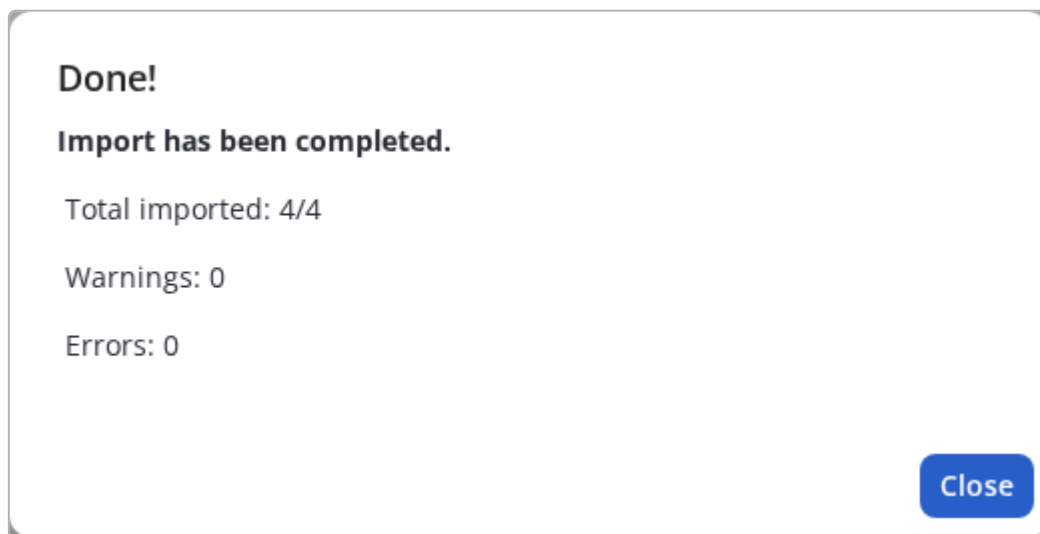


Figure 354. Window Import report (all entries were processed correctly)

The summary block contains:

- **Total Imported** - Counter of records imported (vs. total rows processed);
- **Warnings** - Number of warnings that occurred;
- **Errors** - Number of errors that occurred.

If not all records were processed correctly, you will see the following window:

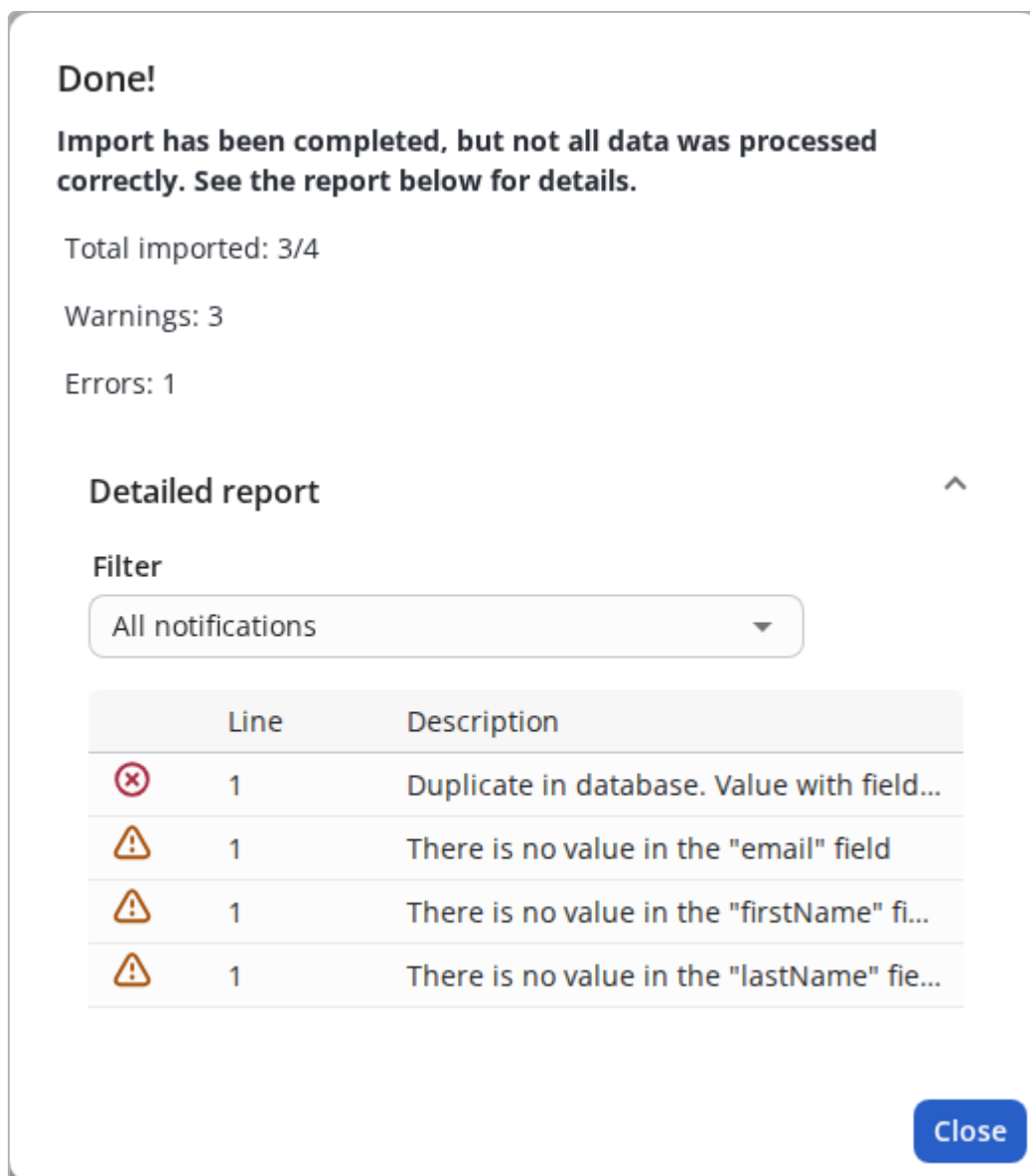


Figure 355. Window Import report (entries processed with errors/warnings)

Detailed report contains the following information:

- **Filter** - Dropdown list allowing you to select which notifications to display (All notifications , Only errors , or Only warnings)

The notification table contains columns:

- **Line** - The line number in the CSV file where an error or warning was detected;
- **Description** - Detailed text explanation of the error or warning.



Hover your cursor over a row in the Description column to view the full error/warning message in a tooltip.

Import particularities for TACACS+ Command sets



For TACACS+ Command sets imports support NAICE and CISCO data sources.

The table below lists the fields, their requirements, descriptions, and requirements:

Field	Description	Requirements
name:Required	Name of the command set	Required Maximum length - 100 characters Must be unique Spaces are not allowed
description	Free-form description	Maximum length - 200 characters
permit_unmatched(true/false)	Permission to execute commands not listed in the commands table	Possible values: • true - status "Enabled" • false - status "Disabled"
commands(Grant/command/arguments/enabled;...)	Configuration block that defines allowed and denied authorization commands	Command separator: ; The requirements for each field will be discussed separately

The column `commands(Grant/command/arguments/enabled;...)` contains the fields `Grant`, `command`, `arguments`, and `enabled`.

The list of fields, their requirements, descriptions, and requirements for the `commands(Grant/command/arguments/enabled;...)` column:

Field	Description	Requirements
Grant	Action performed upon matching compared commands	Required Possible values: • PERMIT • DENY
command	Command	Required Maximum length - 200 characters
arguments	Arguments for the command	Maximum length - 200 characters
enabled	Permission to execute (Status)	Possible values: • true - status "Enabled" • false - status "Disabled"



If a value for the `permit_unmatched(true/false)` field is not found or is incorrect, the default value `false` will be assigned.



If a value for the `commands(enabled)` field is not found or is incorrect, the default value `true` will be assigned.

Example of correctly formatted file content:

"name:Required"	"description"	"permit_unmatch ed(true/false)"	"commands(Grant/command/argume nts/enabled;...)"
"command_set"	"Test command set"	"false"	"PERMIT/\\"show/vlan 1 2 \\"/true;PE RMIT/tacacs-server//true"



As shown in the example, values containing slashes (/) must be escaped with \. Failure to escape will result in incorrect data recognition.

Instructions for obtaining a CSV template file are described later in the **"Export"** section.

Export

NAICE supports exporting data in CSV format. Values and headings are framed by double quotes, the field separator is comma (,).

Export procedure

Two export modes are available:

- **Export all** - Exports all records from the current section. System entities are not included during export.
- **Export selected** - Exports only checked records.

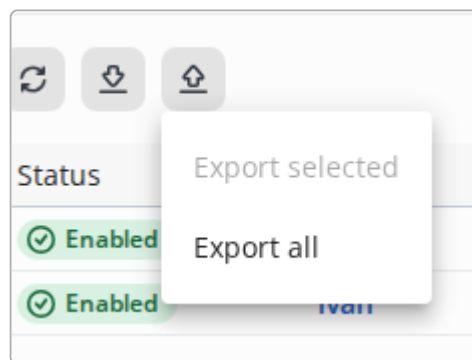



Figure 356. Window export menu



Values containing double quotation marks (") or slashes (/) will be escaped using \.

Export all

On the action panel above the table, click  and select the **"Export all"** mode. In the window that opens, confirm the action by clicking the **"Export"**:

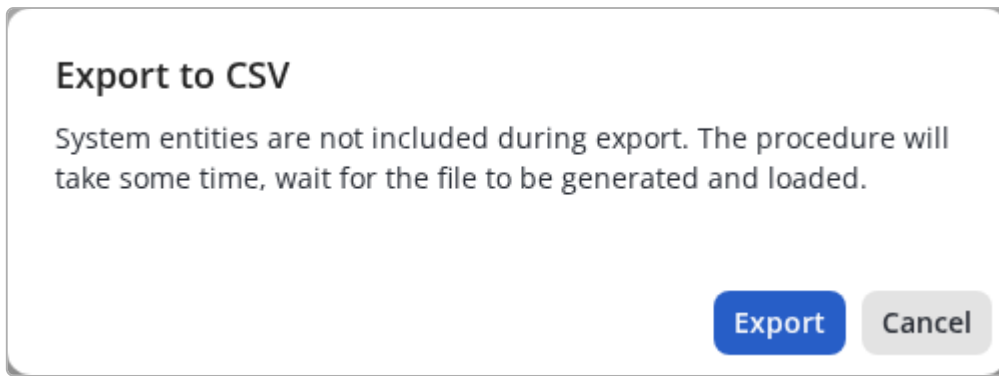



Figure 357. Export all

After clicking the "**Export**", a file containing all records from the current section will be downloaded to your device.

Export selected

On the action panel above the table, click  and select the "**Export selected**" mode. In the window that opens, confirm the action by clicking the "**Export**":

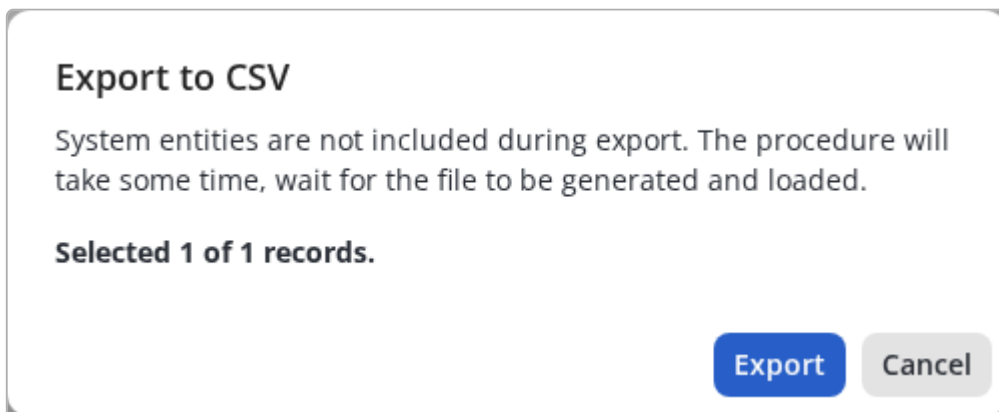


Figure 358. Export selected

After clicking the "**Export**", a file containing only the checked records will be downloaded to your device.



When **opening** CSV files, **always** use a **comma (,)** as the field delimiter. **Double quotation marks (")** or **empty values** may be used as string/text delimiters.

When **saving** CSV files, **always** use a **comma (,)** as the field delimiter, with an **empty value** as the string/text delimiter.



If a double quotation mark (") was used as the line delimiter when opening the file, values containing double quotation marks (") or slashes (/), escaped as \", may receive an extra quotation mark (") upon saving. Please check the file in a text editor and remove any extra quotation marks if they appear.

Template

If there are no records in the table (or only system entities are present), selecting the "**Export all**" mode will generate a CSV file containing only the column headers. This file can be used as a **template** for preparing data prior to import.

Export particularities for TACACS+ Command sets



Values containing a double quote (") or the slash (/), will be escaped using \".

The structure of the csv file for TACACS+ command sets is described in the section "[Import particularities for TACACS+ Command sets](#)".

TACACS+ profiles



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

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

Name	Description
Both privilege	
Deny all shell profile	Deny all shell profile
Maximum privilege	
Minimum privilege	
MES	

Figure 359. TACACS+ profile summary table





This page contains a table listing TACACS+ profiles.

The table contains the following columns:

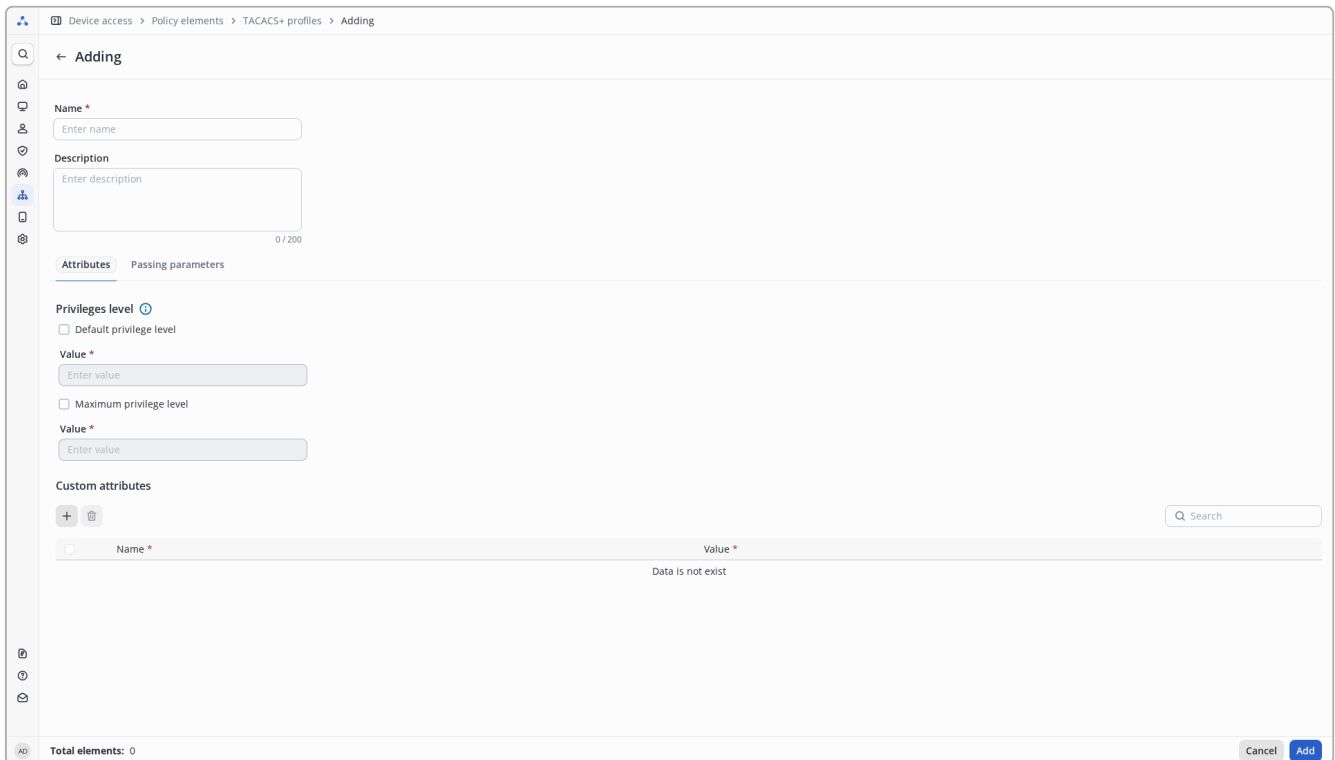
- **Name** - Profile name.
 - - This entity is system and cannot be deleted or edited.
- **Description** - Profile description.

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

Elements of control:


-  - Add TACACS+ profile.
-  - Duplicate TACACS+ profile.
-  - Delete selected (checked) TACACS+ profile.
-  - Refresh profiles table.

Add TACACS+ profile



The screenshot shows the 'Adding' page for a TACACS+ profile. The breadcrumb trail is 'Device access > Policy elements > TACACS+ profiles > Adding'. The page has a search bar and a back arrow. The form fields are: 'Name *' (required), 'Description', and 'Attributes' (with a sub-section for 'Passing parameters'). There are two sections for 'Privileges level': 'Default privilege level' and 'Maximum privilege level', each with a 'Value *' (required) field. Below these is a 'Custom attributes' section with a table that is currently empty, showing a message 'Data is not exist'. The bottom of the page has 'Total elements: 0' and 'Cancel Add' buttons.

Figure 360. TACACS+ Profile Add Page

To add a TACACS+ profile, click .

fill in the following parameters in new window:

- **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).



Parameters marked with * are required.



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:

-  - 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.

Editing a TACACS+ profile

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


<input type="checkbox"/>	Name ↑
<input type="checkbox"/>	Both privilege 
<input type="checkbox"/>	Deny all shell profile 
<input type="checkbox"/>	Maximum privilege 
<input type="checkbox"/>	Minimum privilege 
<input type="checkbox"/>	MES

Figure 361. Hyperlink to the TACACS+ profile editing page



Restriction:

- you cannot edit system profiles TACACS+ ().

This will open the edit page.

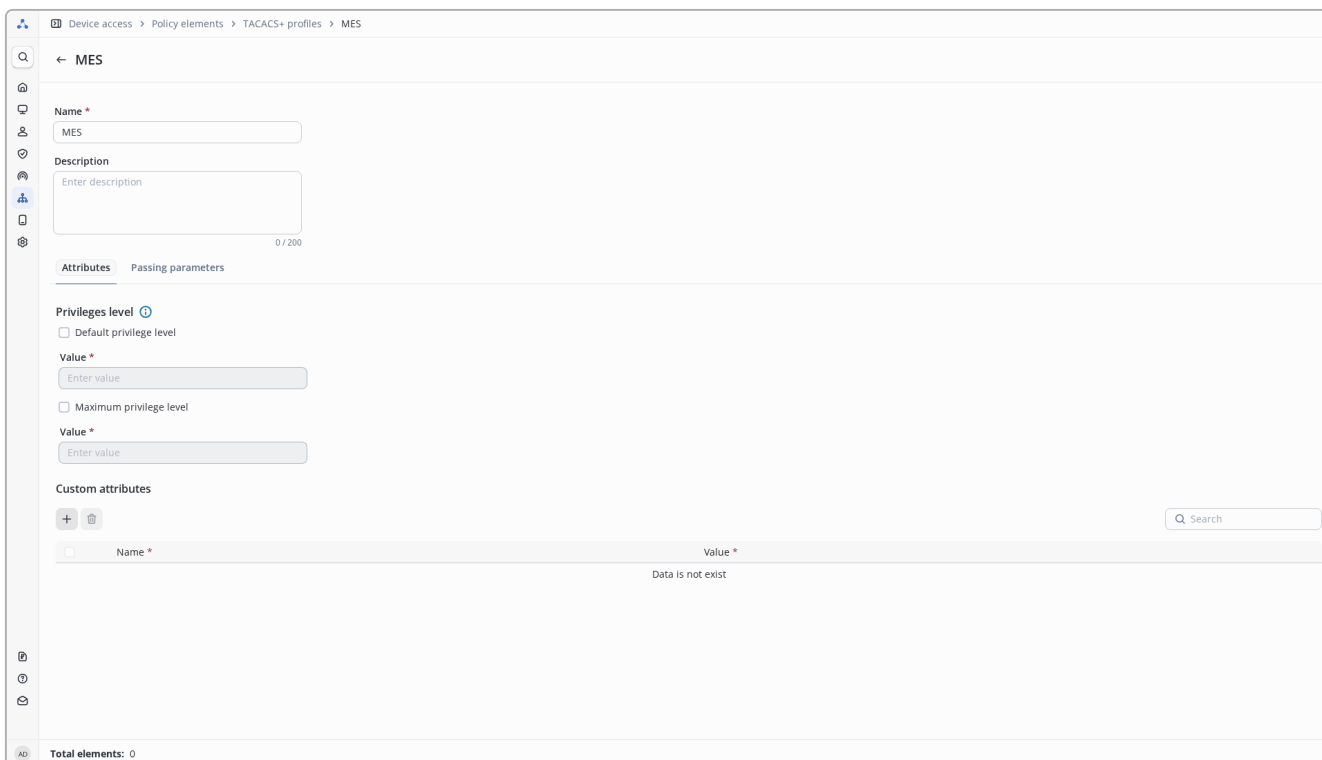



Figure 362. TACACS+ profile editing page

After editing, click the **"Save"** button. The button is hidden until at least one change is made.

The **"Cancel"** button resets the changes made to their original state.

Deleting a TACACS+ profile

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



	Name ↑
<input type="checkbox"/>	Both privilege 
<input type="checkbox"/>	Deny all shell profile 
<input type="checkbox"/>	Maximum privilege 
<input type="checkbox"/>	Minimum privilege 
<input checked="" type="checkbox"/>	MES

Figure 363. Selecting a TACACS+ profile in the table to delete



Deleting items requires confirmation in the modal window. The selected items will be deleted only after explicit confirmation of the operation.

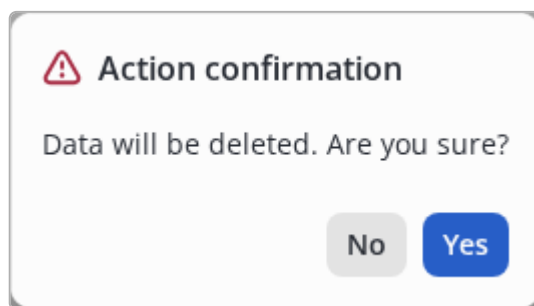


Figure 364. Modal dialog for confirmation



Restriction:

- You cannot delete system profiles TACACS+ (🔒).

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".

The listed profiles are system (🔒) and cannot be edited or deleted.

Network devices policies



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

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 policies table:
 - The authentication or authorization request is checked for compliance with the logical conditions used in the TACACS+ policies.
 - The verification is performed sequentially from top to bottom. Disabled policies are not evaluated and 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 inside that policy.

- 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 uses the **Deny all shell profile** in `TACACS+ Profile settings`, 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:

- Check for compliance with the authentication policy conditions is first performed.
- After determining the authentication policy, a user search is performed within the identity sequence selected for this policy. If the user is not found or their password is incorrect, the connection is rejected, and the request processing ends at this step.
- 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 in `TACACS+ Profile` setting. 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 less or equal to the configured maximum: escalation is granted. If the requested level greater than 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 allowed in the permitted command 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


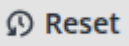




Status	Name*	Description	Conditions*	Protocol	Hits count
Enabled	Test policy set	Description	Test condition	PAPI/ASCII	10
Default	Default	Tacacs default policy set		PAPI/ASCII	5

Figure 365. View all Policies.

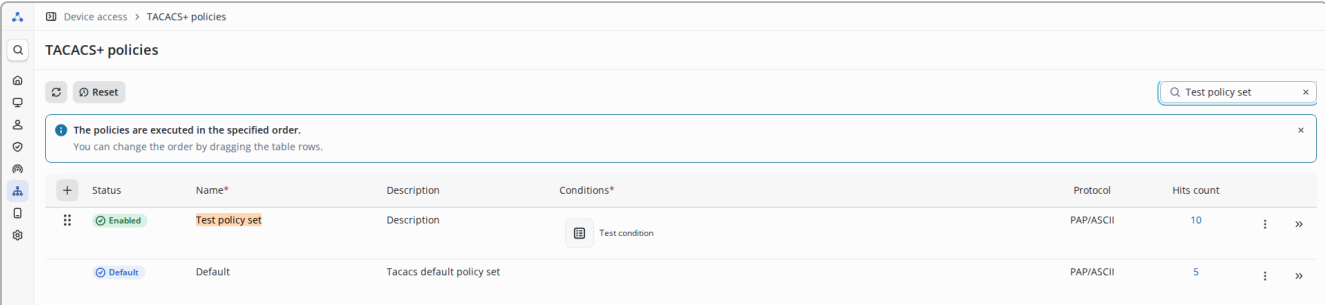
Table Column Descriptions:

- **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 .
- **Hits count** – Number of authorization attempts matching the specified Conditions.

Elements of Control:

-  – refresh data.
-  – delete counters for failed attempts on all policies (attempt counts).
- **Search** – a registered search by name (search results will be highlighted).
-  – add TACACS+ policy (policy will be added first in the list).
-  - element for change policy set order in list by dragging.
- **Hits count** – 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 without removing any policies from the list.



	Status	Name*	Description	Conditions*	Protocol	Hits count		
	Enabled	Test policy set	Description	Test condition	PAP/ASCII	10	:	»
	Default	Default	Tacacs default policy set		PAP/ASCII	5	:	»

Figure 366. Search Policies.

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




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

To view the list of [authentication and authorization policies](#), click  to the right of the selected policy set.

Editing Policy sets list

Add Policy set

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.

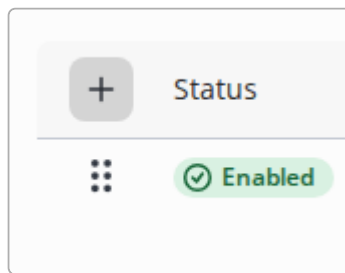



Figure 367. Add Policy icon.

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.

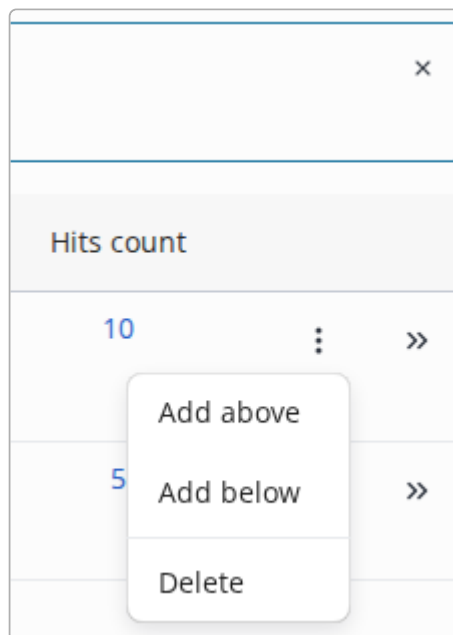





Figure 368. Dropdown Action Menu.

Status Information:

-  **Enabled** – Allows processing requests;
-  **Disabled** – Excludes from processing, does not check the Condition, and does not handle requests;
-  **Condition check** – Allows checking the Condition (and increments the trigger counter) but does not process requests;

- **Default** – Used only for the default policy.

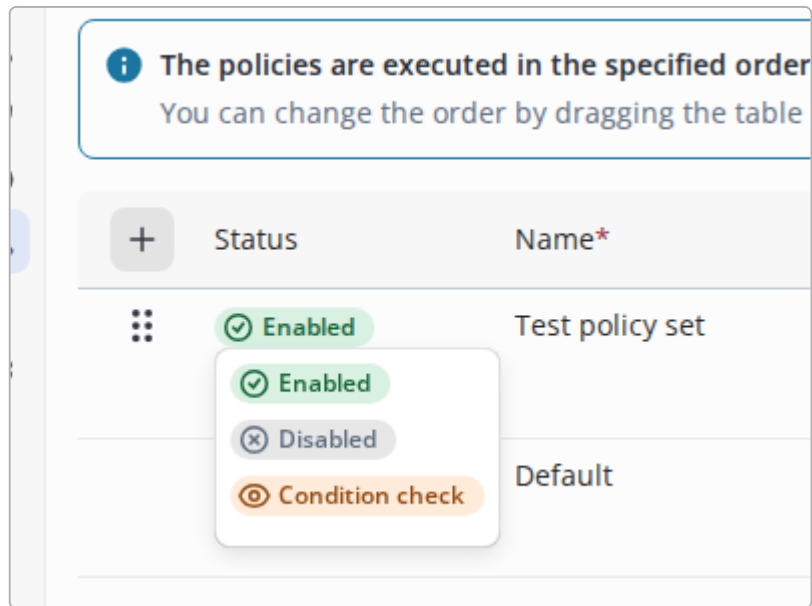


Figure 369. Policy status change.

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

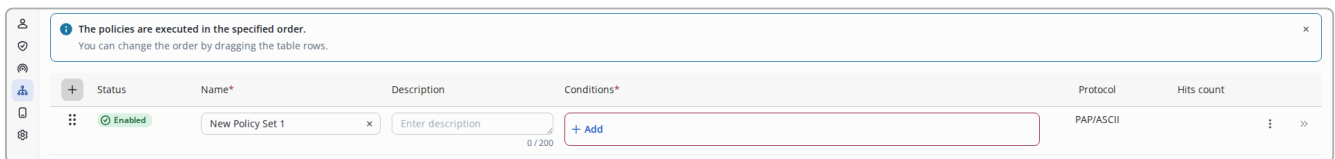


Figure 370. New Policy entry display. Required fields.

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

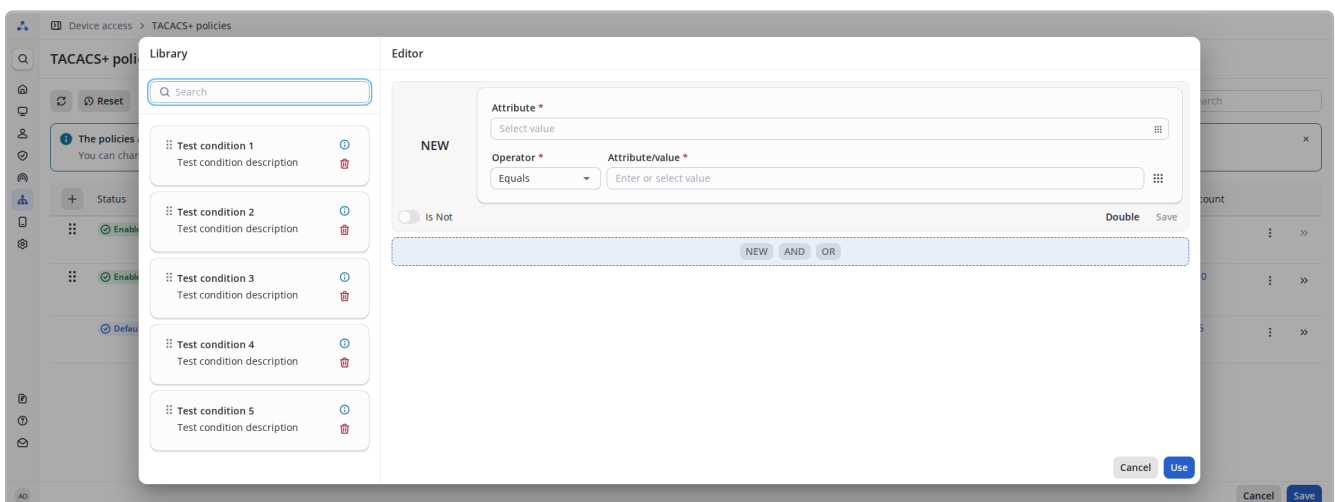


Figure 371. Condition Editor.

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



When configuring a policy set 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 set named `Default` also can be edited.

Policy set deletion

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

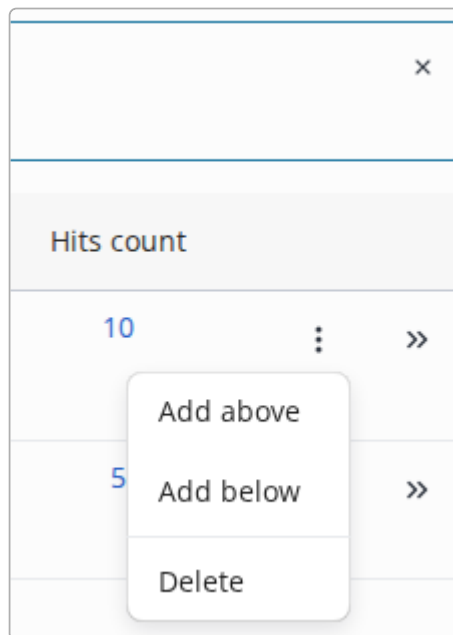


Figure 372. Policy deletion dropdown menu.

Policy hit count

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



Using the **Condition check** status and observing the trigger counters, you can first fine-tune and debug the condition, and only then put the policy into operation by switching it to the **Enabled** status.

The trigger counters for all policy sets can be reset by clicking on **Reset**. To reset the counter for a specific set, click the number in the **Hits Count** column, click the **Reset** button, and confirm the action.

TACACS+ policy configuration



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

Viewing the policies in the selected policy set

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.

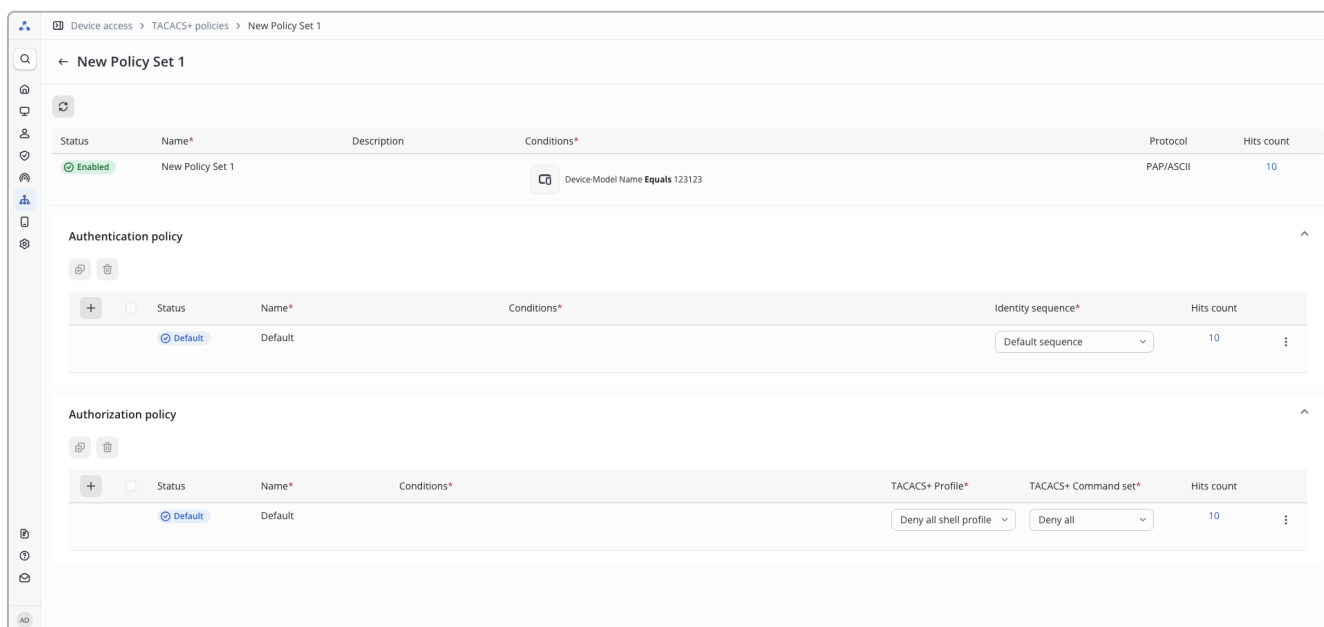


Figure 373. Policy set view & Edit page



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/index.html](http://policy-sets/index.html)
- Authentication Policy - Manages user authentication processes.
- Authorization Policy - Controls User authorization for privilege level and profile access and lists of permitted commands.



Control Elements:

- - 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 .
- Identity sequence * - Selected [identity source chain](#)
- TACACS Profile * - Available [TACACS profiles](#) selection
- TACACS Command Set * - Available [command sets](#) selection
-  - Actions menu:
 - Add Above - Insert policy rule *before* selected one
 - Add Below - Insert policy rule *after* selected one
 - Duplicate - Insert duplicated policy rule
 - Delete - Remove selected policy rule
- Hits count - 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/index.html](#).

Editing policies

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



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



The **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

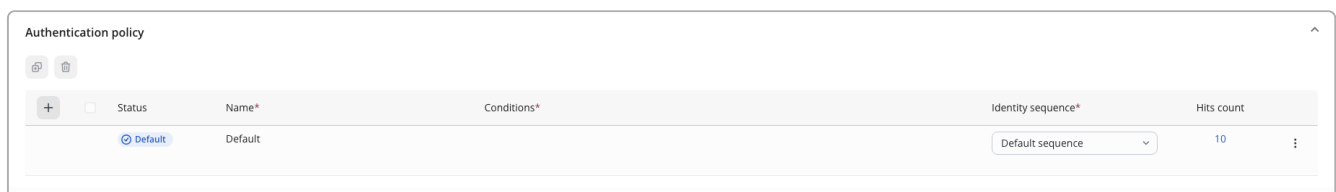


Figure 374. Authentication policy panel.

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

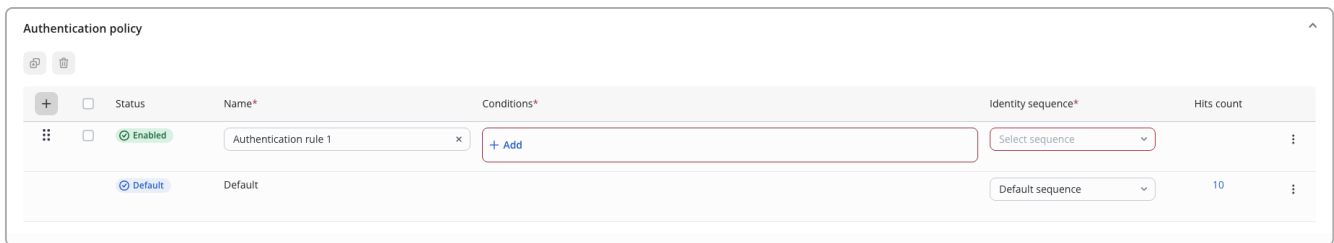


Figure 375. New authentication policy.

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.

In the dropdown menu **Identity sequence**, select the required [chain](#).

A new policy rule can also be created from an existing one by duplicating it. To do this, select the desired rule/rules via , and then click above the table. A new rule will be created above the selected one with similar settings and a name ending with "_copy".

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

Click the **Save** button to save your changes.

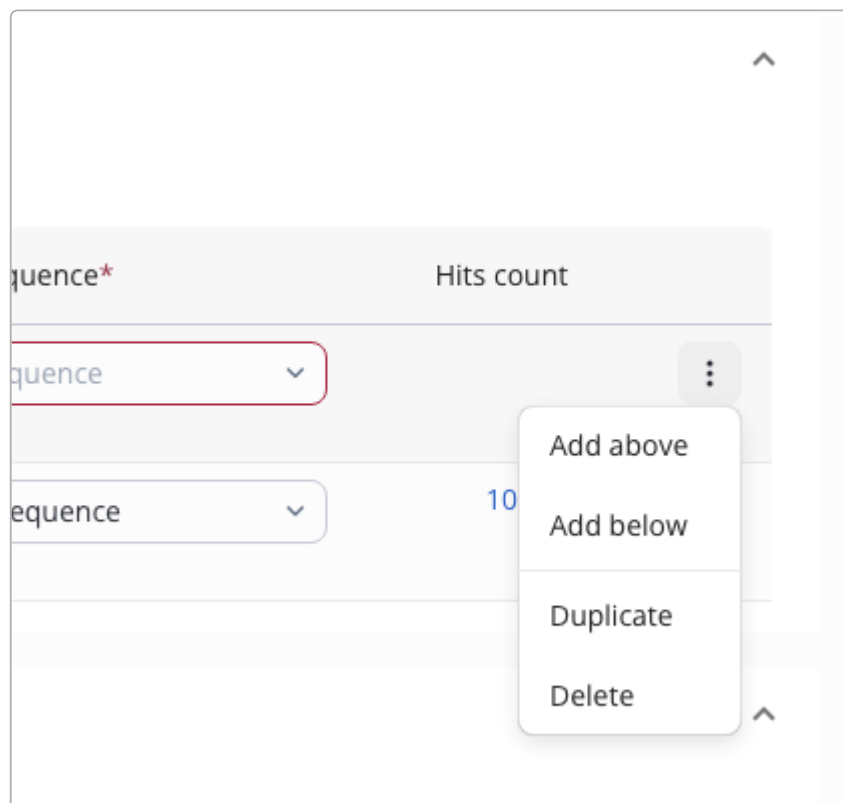


Figure 376. Authentication policy. Dropdown menu - Actions.

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

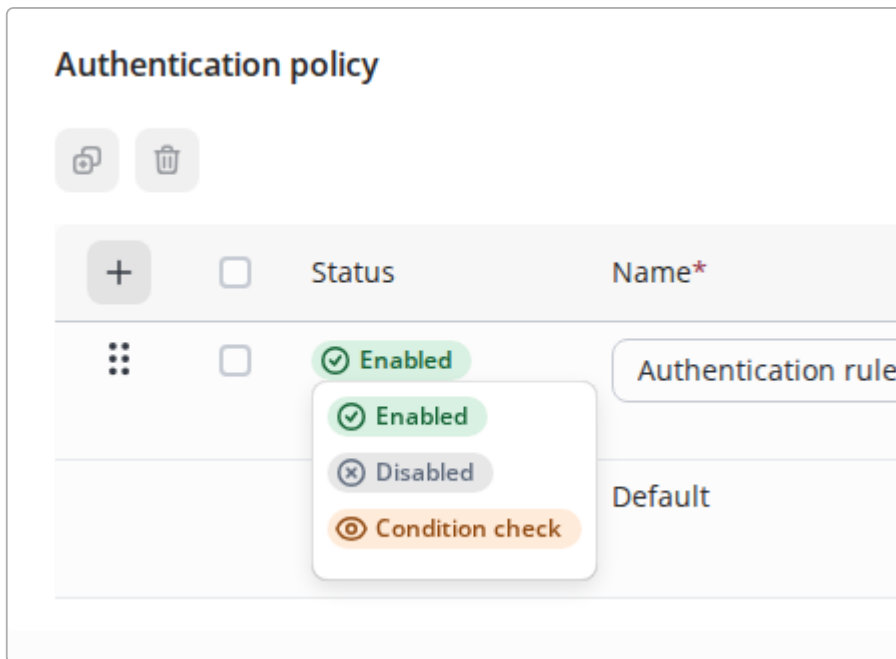


Figure 377. Authentication policy. Status Modification.

Authorization policy



Figure 378. Authorization policies panel.

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

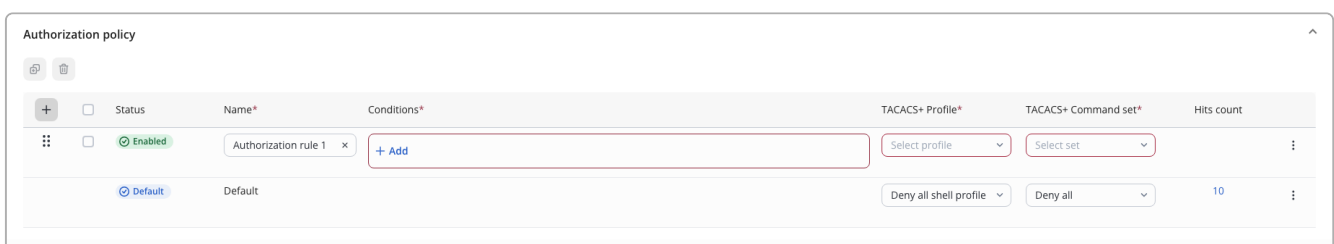


Figure 379. New Authorization policy.

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

To edit the condition, click **+ Add** - 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+`, `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](#).

A new policy rule can also be created from an existing one by duplicating it. To do this, select the desired rule/rules via , and then click above the table. A new rule will be created above the selected one with similar settings and a name ending with "_copy".

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, duplicate or delete the current rule.

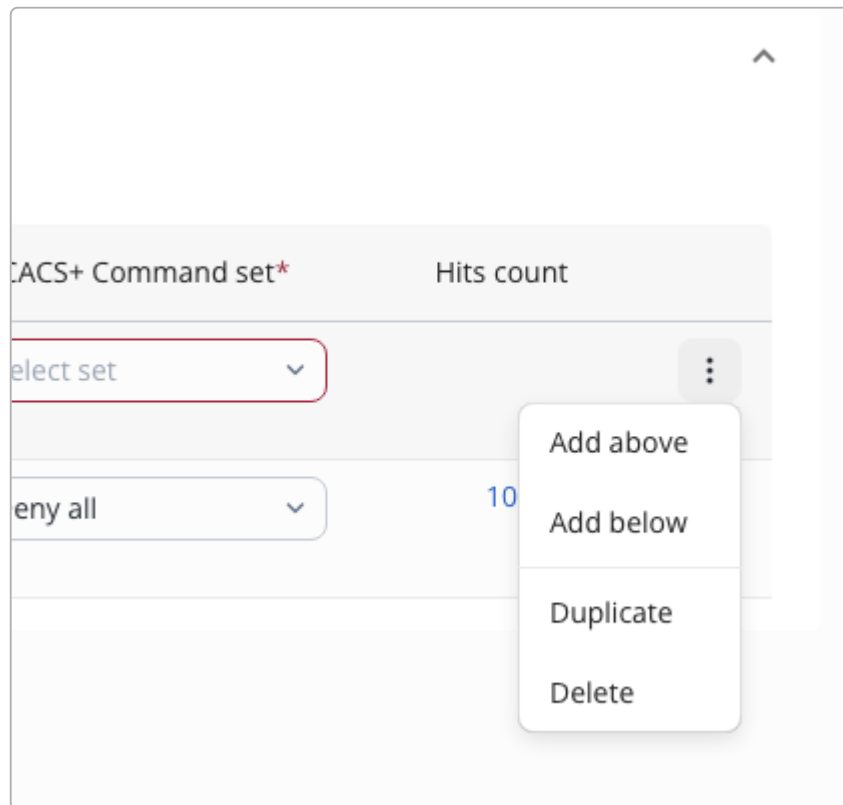


Figure 380. Authorization Policy. Dropdown menu - Actions.

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

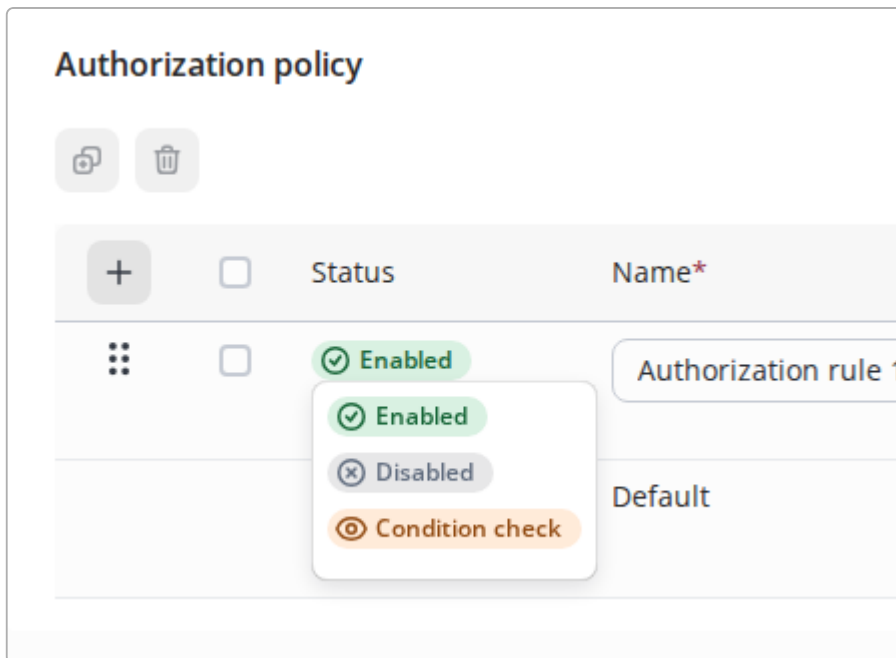


Figure 381. Authorization policy. Status Modification.

To delete multiple rules, select them using and then click  above the table of rules.

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.

Notification gateways

Notification gateways management

Description

Gateway management allows you to create, configure, and use integrations with SMS sending services for portal authorization and mail servers for setting up notifications about the creation and editing of system users. It is possible to configure multiple SMS gateways, which allows for flexible integration settings for each Guest portal.

Currently, integration is only implemented via HTTP/HTTPS protocols for the Guest portal and SMTP for password policies.

View a list of notification gateways

Name	Connection type	Where used
Demo gateway	DEMO	Default portal
Custom gateway	HTTP	Custom portal
Custom smtp gateway	SMTP	Password policies

Figure 382. Table with a list of notification gateways

Below is a table with a list, which contains columns:



- **Name** - The name of the SMS gateway.
 - - This entity is system and cannot be deleted or edited.
- **Connection type** - Gateway connection type. Can take values: DEMO, HTTP, SMTP
- **Where used** - A list of entities in which this gateway is used.

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

- **Description** - Description of the notification gateway.
- **Additional info** - Contains additional data about the existing integration.

Controls:

- - Add a new element.
- - Refresh table data.

-  - Delete selected elements (inactive until at least one element is selected)
-  - Open the settings window for the displayed columns of the table.
- - Checkbox, which is responsible for selecting elements to perform further actions (for example, deletion).

Adding notification gateway

To add a notification gateway, click  .

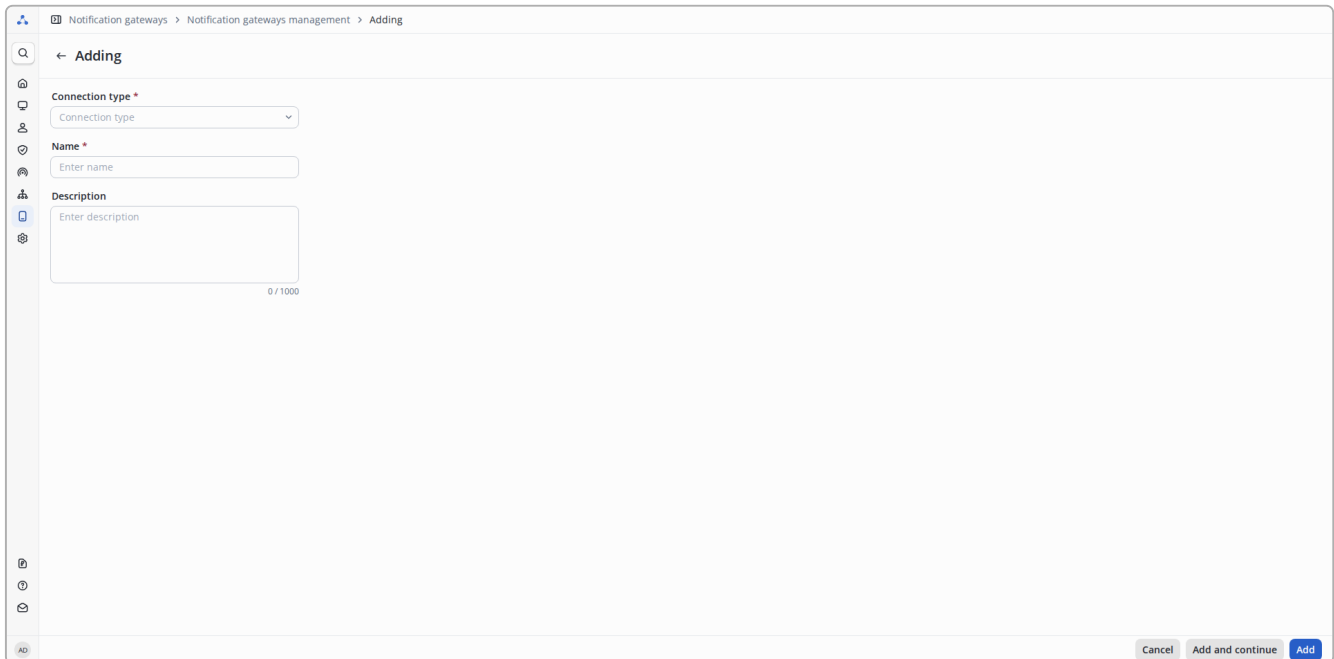


Figure 383. Notification gateway Add Page

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

- **Connection type *** - Gateway connection type. Can take values: DEMO, HTTP, SMTP
- **Name *** - Notification gateway name; must be unique within the gateway list. Maximum length is 200 characters.
- **Description** - Notification gateway description. Maximum length - 1000 characters.

Parameters marked with an asterisk * are required.

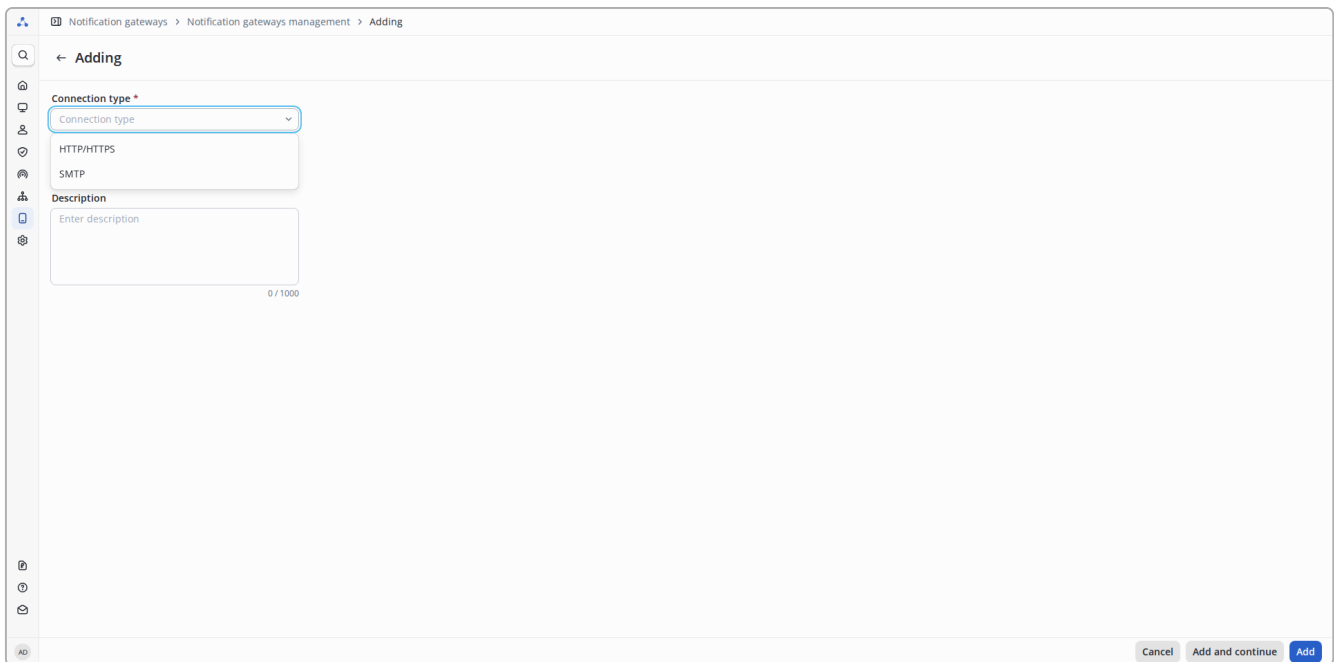


Figure 384. The page for adding a notification gateway with connection type selection

Further gateway configuration depends on the selected connection type. For more information on configuring the [HTTP/HTTPS](#) and [SMTP](#) gateways, see the relevant sections.

For adding a gateway, the system provides two submit buttons that differ in their subsequent behavior:

- **"Add and continue"** — after clicking, the form does not close, and the **"Send test SMS/email"** button becomes available.
- **"Add"** — after clicking, the user is redirected to the notification gateways list page.

Editing notification Gateway

To edit a notification gateway, on the list page, click its name.

<input type="checkbox"/>	Name
<input type="checkbox"/>	Demo gateway
<input type="checkbox"/>	Custom gateway
<input type="checkbox"/>	Custom smtp gateway

Figure 385. Hyperlink to the notification gateway editing page

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



When changes are made to the form, the **"Send test SMS/email"** button becomes unavailable. The button is reactivated only after the changes are saved.

Figure 386. HTTP/HTTPS gateway editing page

Figure 387. SMTP gateway editing page


For saving changes, the system provides two buttons that differ in their subsequent behavior:

- **"Save and continue"** — after clicking, the form does not close, and the **"Send test SMS/email"** button becomes available again.

- **"Save"** — after clicking, the user is redirected to the notification gateways list page.

The **"Cancel"** button resets the changes made to their original state.

Removing a notification gateway

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

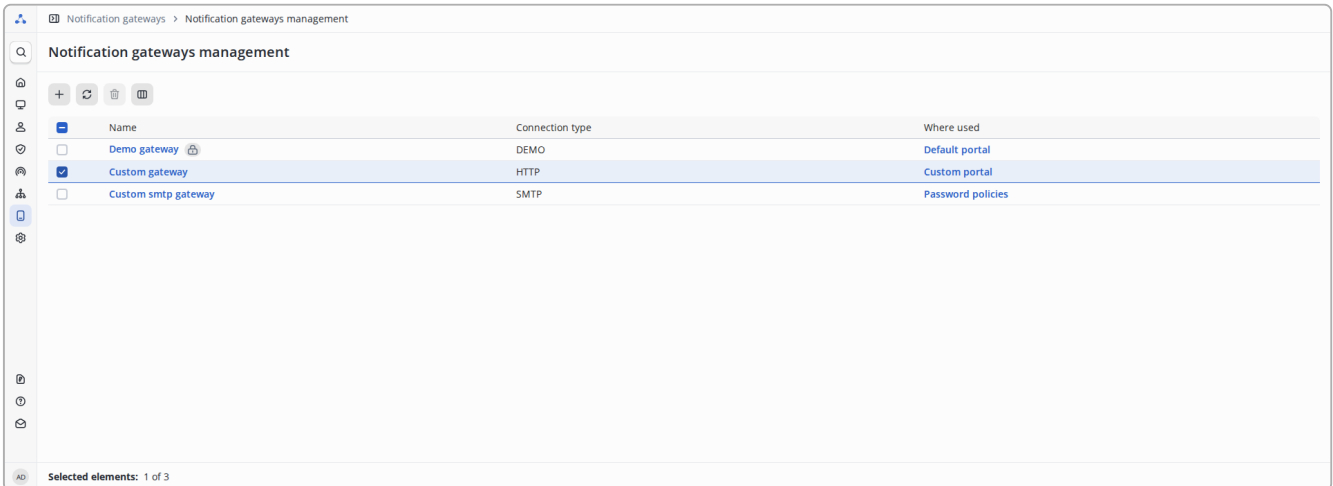


Figure 388. Selecting a gateway in the table to delete



Deleting items requires confirmation in the modal window. The selected items will be deleted only after explicit confirmation of the operation.

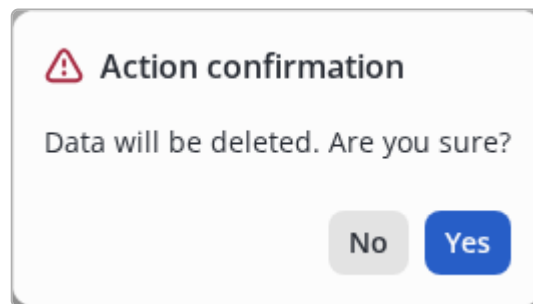


Figure 389. Modal dialog for confirmation

HTTP/HTTPS

Send message request editor

The screenshot shows the 'Adding' gateway configuration page. The breadcrumb trail is 'Notification gateways > Notification gateways management > Adding'. The page title is '← Adding'. The 'Connection type' is set to 'HTTP/HTTPS'. The 'Name' field contains 'Enter name' and the 'Description' field contains 'Enter description'. The 'Message sending request editor' section includes: 'Connection timeout' (3), 'HTTP method' (POST), 'Read timeout' (3), 'URL API' (Enter URL), and 'Request timeout' (3). There is a checkbox for 'SSL/TLS certificate check during HTTP/HTTPS gateway connection' which is unchecked. Below this are tabs for 'User variables', 'Headers', and 'Request body'. A text box contains the instruction: 'System variables can be used as attribute values in parameters, or specify your own as text.' Below this is a table with columns 'Attribute' and 'Attribute value', and a '+' button. At the bottom right are 'Cancel', 'Add and continue', and 'Add' buttons.

Figure 390. HTTP/HTTPS gateway creation page

When you select the HTTP/HTTPS connection type in the gateway creation form, the following options become available:

- **Connection timeout *** - maximum wait time for connection to the server(sec.).The default is 3 seconds.
- **Read timeout *** - maximum wait time for response from the server(sec.).The default is 3 seconds.
- **Request timeout *** - maximum wait time for data from the server(sec.).The default is 3 seconds.
- **HTTP method *** - A drop-down list for selecting the HTTP method for integration. Available options are: GET, POST, and PUT. The default is POST.
- **URL API *** - The address to which the request to send a message within the integration will be executed.

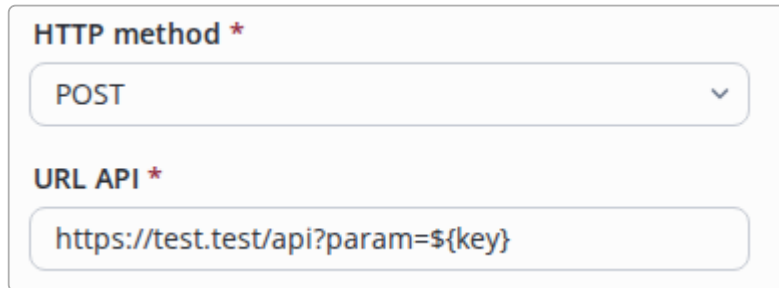
Within the framework of creating SMS integration, flexible configuration of the request for sending a message is available. On the SMS gateway creation page, 3 sections are available for editing the request:

- **User variables** - section for creating user-defined variables required to create a request (for example: login/password/API-key for integration). To create a variable, you must specify its name in the "Attribute" column and its value in the "Attribute value" column. Adding a new variable is done using the **+** button, and deleting it is done using the **🗑** button.
- **Headers** - section for creating HTTP headers for a request by the user. To create a header, you must specify its name in the "Attribute" column and its value in the "Attribute Value" column. The value can also be a variable. To select a variable, click **+** Similar to the section with user variables, adding a new header is done using the **+** button, and deleting it is done using the **🗑** button.
-

Request body - section for editing the request body. Data can be recorded in JSON format. In this section, the use of variables as a value is also allowed.

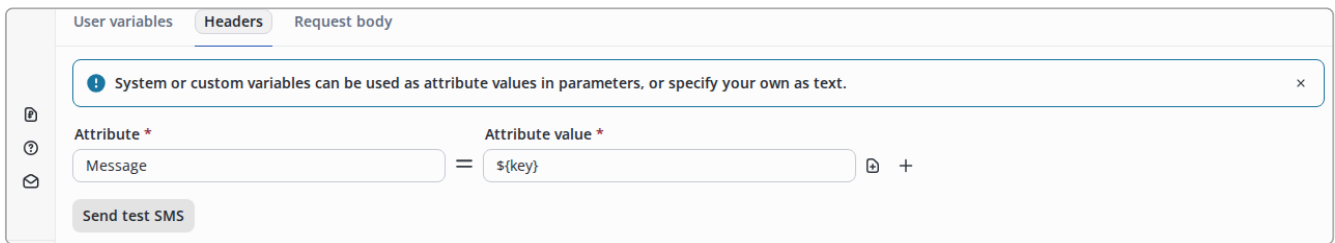
Working with variables

For flexible configuration of SMS integration, it is assumed that user and system variables will be used when composing a request. The system variables are "Message text" and "Phone number". All variables can be used to substitute values into URL, headers, and request body. In addition to user-configurable variables, there are system variables `#{msg}` and `#{target}`, which represent the message text and phone number, respectively.



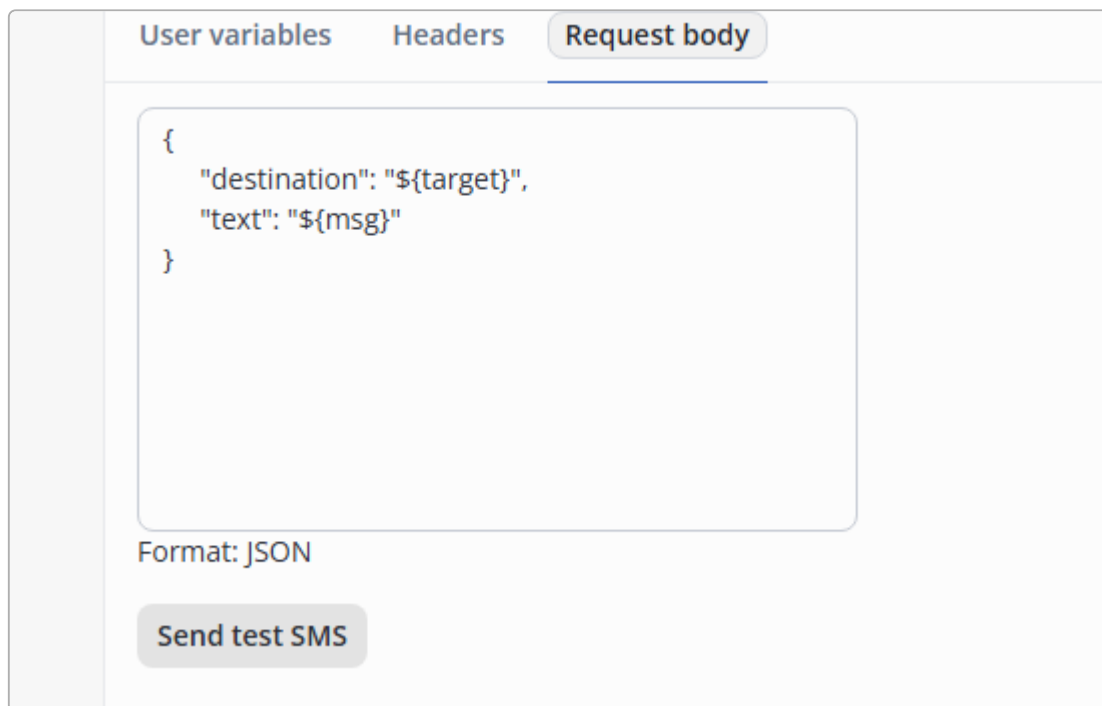
The screenshot shows a configuration panel with two sections. The first section is titled "HTTP method *" and contains a dropdown menu with "POST" selected. The second section is titled "URL API *" and contains a text input field with the URL "https://test.test/api?param=#{key}" entered.

Figure 391. Example of adding a variable to a request URL



The screenshot shows the "Headers" tab in a configuration interface. A tooltip at the top states: "System or custom variables can be used as attribute values in parameters, or specify your own as text." Below this, there is a table with two columns: "Attribute *" and "Attribute value *". The first row contains "Message" in the attribute column and "#{key}" in the attribute value column. A "Send test SMS" button is located at the bottom left.

Figure 392. Example of adding a variable to a request header



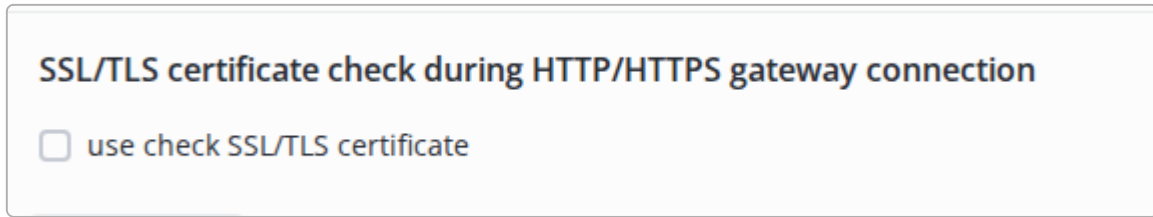
The screenshot shows the "Request body" tab in a configuration interface. The main area contains a JSON object:

```
{  "destination": "#{target}",  "text": "#{msg}"}
```

 Below the JSON editor, it says "Format: JSON". A "Send test SMS" button is located at the bottom left.

Figure 393. Example of adding a variable to a request body

SSL/TLS certificate check during HTTP/HTTPS gateway connection



SSL/TLS certificate check during HTTP/HTTPS gateway connection

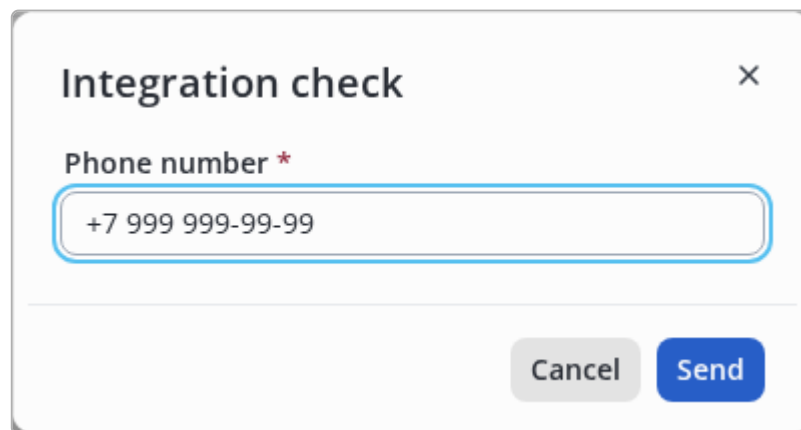
use check SSL/TLS certificate

Figure 394. The setting responsible for certificate validation

If you need to verify the server's certificate when establishing a connection with the HTTP/HTTPS server, you must enable the 'use check SSL/TLS certificate' checkbox. More details can be found in the documentation section for [trusted certificates](#).

Sending a test message

After adding the gateway, the "Send test SMS" button becomes available. Clicking it opens a verification window for the created integration, which includes a phone number input field.



Integration check

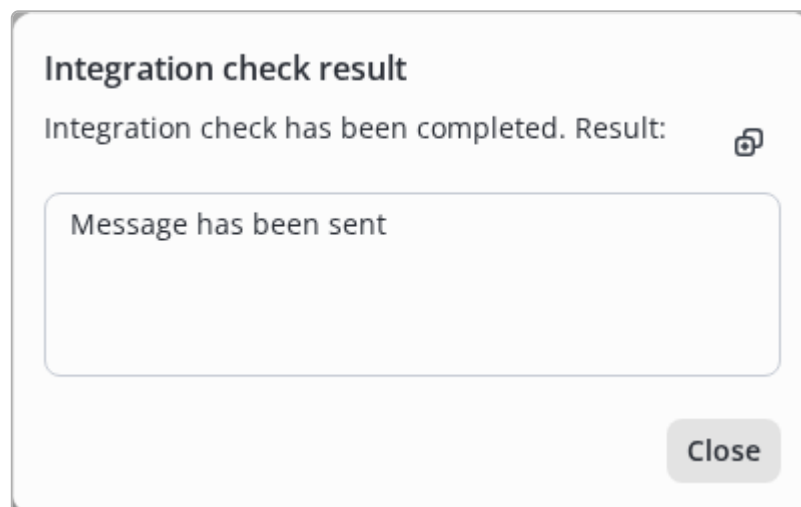
Phone number *

+7 999 999-99-99


Cancel Send

Figure 395. Window for checking the created SMS integration

After filling in the phone number and sending an SMS, a window with the verification result will open for the user.



Integration check result

Integration check has been completed. Result: 

Message has been sent

Close

Figure 396. Result window of checking the created SMS integration

SMTP

SMTP gateway settings

The screenshot shows a web interface for adding a new SMTP gateway. The breadcrumb navigation at the top reads: "Notification gateways > Notification gateways management > Adding". The page title is "← Adding".

The form is divided into several sections:

- Connection type ***: A dropdown menu with "SMTP" selected.
- Name ***: A text input field with the placeholder "Enter name".
- Description**: A text area with the placeholder "Enter description" and a character count of "0 / 1000".
- SMTP gateway settings**:
 - Server address ***: A text input field with the placeholder "Enter name".
 - Port ***: A text input field with the value "25".
 - Sender name ***: A text input field with the placeholder "Enter name".
 - Sender address ***: A text input field with the value "mail@naice.ru".
 - Request timeout ***: A text input field with the value "3".
- SMTP gateway connection authorization**:
 - use authorization
 - User name ***: A text input field with the placeholder "Enter name".
 - Password ***: A text input field with the placeholder "Enter password".
- SSL/TLS certificate check during SMTP gateway connection**:
 - use check SSL/TLS certificate
 -

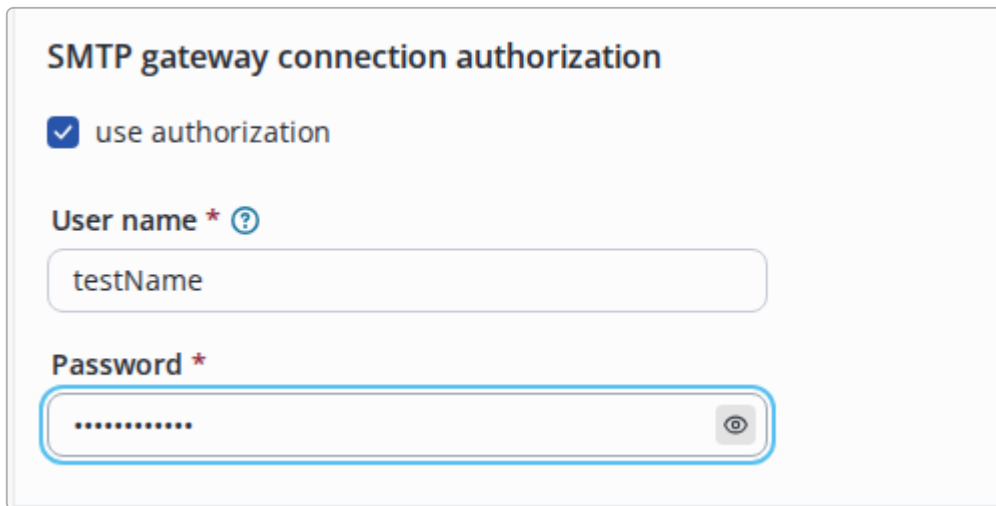
At the bottom right, there are three buttons: "Cancel", "Add and continue", and "Add".

Figure 397. SMTP gateway creation page

When you select the SMTP connection type in the gateway creation form, the following parameters become available:

- **Server name *** - the IP address or domain name of the mail server to be connected.
- **Port *** - SMTP server port to which the request will be made. The default is 25 port.
- **Sender name *** - the sender's name, which will appear in the letter.
- **Sender address *** - the sender's email, which will appear in the letter.
- **Request timeout *** - maximum wait time for data from the server(sec.). The default is 3 seconds.

SMTP gateway connection authorization



The screenshot shows a configuration window titled "SMTP gateway connection authorization". It contains a checked checkbox labeled "use authorization". Below this are two input fields: "User name * ?" with the text "testName" entered, and "Password *" which is currently masked with dots and has a toggle icon on the right.

Figure 398. The setting responsible for user authorization on the SMTP server

If the mail server requires authorization of the user to send a message, then you must enable the 'use authorization' checkbox, after which two more parameters will become available for editing:

- **User name *** - the email address or username that will be used for authorization on the SMTP server.
- **Password *** - the user password that will be used for authorization on the SMTP server.

SSL/TLS certificate check during SMTP gateway connection



The screenshot shows a configuration window titled "SSL/TLS certificate check during SMTP gateway connection". It contains an unchecked checkbox labeled "use check SSL/TLS certificate".

Figure 399. The setting responsible for certificate validation

If you need to verify the server's certificate when establishing a connection with the SMTP server, you must enable the 'use check SSL/TLS certificate' checkbox. More details can be found in the documentation section for [trusted certificates](#).

Send test email

After adding the gateway, the "**Send test email**" button becomes available. Clicking it will open a window for testing the created integration, complete with an email address entry field.

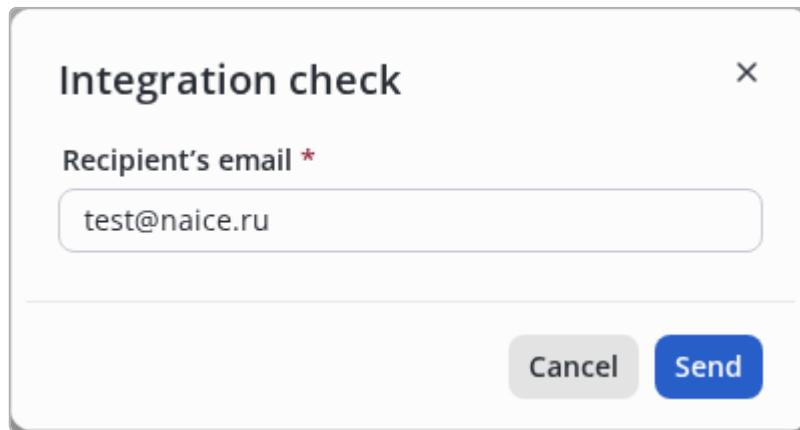


Figure 400. Window for checking the created SMTP integration

After filling in the email address and sending the letter, the user will see a message with the sending status.

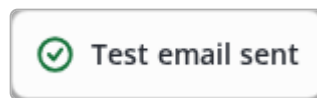


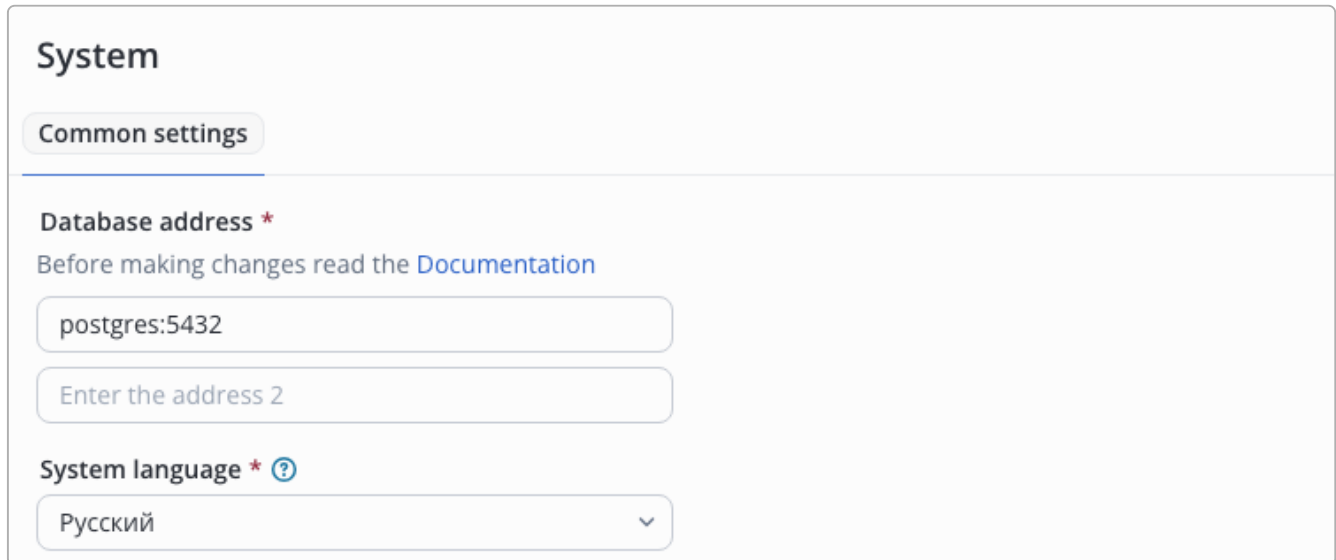
Figure 401. The result window of checking the created SMTP integration

System settings

System

Common settings

The `Common settings` section includes system settings that affect the overall operation of NAICE.



The screenshot shows the 'System' settings page with the 'Common settings' tab selected. Under 'Database address *', there is a text input field containing 'postgres:5432' and a link to 'Documentation'. Below it is another empty text input field with the placeholder 'Enter the address 2'. Under 'System language *', there is a dropdown menu currently set to 'Русский'.

Figure 402. Common settings

Database address

This group of settings allows you to specify one (in the case of a non-redundant installation) or two (in the case of a cluster) PostgreSQL database addresses.



The correct operation of the entire system depends on the correctness of the specified database address/addresses. Specifying an incorrect address may lead to a **complete** loss of access to NAICE.

After deploying NAICE, the settings will be populated with default values, depending on the installation scheme:

- single-host installation without redundancy - `naice-postgres:5432` (the address of the DB docker container in the docker network will be obtained automatically)
- cluster - both addresses will be filled with the values `IPv4-node-address:5432`

Requirements for the specified address

- The address must be specified in the format `domain-name:port` or `IPv4-address:port`.
- If the specified domain name is not a container name in the docker network, resolution of this name must be ensured.
- PostgreSQL with a schema actual for this version of NAICE must be available at the specified address.



Before saving the settings, an attempt is made to read data from the phoca database at the specified address. If only the phoca database is present in PostgreSQL and other databases are absent, the check will pass with a false positive result and the settings will be saved.

Address saving mechanism

1. When the naice-phoca service starts, the database address is read from the environment variables file.
2. When editing the address, the new address is changed in the environment variables file and in PostgreSQL at both the old and new addresses.



Applying the settings will cause the naice-radius service to restart, which will lead to a brief interruption in all types of authorization.

Cluster configuration specifics

When changing database addresses in a redundant installation scheme, it is required that only one node is in the primary state. If both nodes are in the read-only (standby) state, access to NAICE will be lost.

System language

The language used by some services to determine the text localization for the user. This setting affects:

- the default language for new system users (both local and from external sources)
- the language of system events in the [System events](#) section
- the language of email notification texts sent by SMTP-type [notification gateways](#)



The language of the message that is sent to the user during captive portal authorization depends on the portal language selected by the user.



The interface localization for each system user is configured on the page [Account settings](#).+

Services

RADIUS

This page configures the operation of the RADIUS server as part of NAICE.

Services

RADIUS
TACACS+
Event log

General settings

RADIUS authentication port *

RADIUS session storage duration, days *

RADIUS accounting processing

Server certificate * ?

⚠ RADIUS certificate 01

Figure 403. Configuring the RADIUS service

The following parameters are available for configuration:

- **RADIUS authentication port** - the UDP-port on which the RADIUS server listens for RADIUS requests. Default value - 1812.



When saving the configuration, a check is performed only for UDP ports that are used by Docker containers. Ports used by services or applications installed directly on the host machine (outside Docker) are not checked. To avoid conflicts, it is strongly recommended to manually verify, before saving, that the selected port is not in use by other processes on the server.



To apply the configuration, the naive-radius service will be restarted, which will result in a short interruption of RADIUS request processing.

- **RADIUS session storage duration, days** - the number of full days from the RADIUS session creation date during which sessions are stored in the database. After this period expires, sessions are deleted. Default value - 31.



Sessions are periodically checked for expiration and deleted according to a schedule.

- **RADIUS accounting processing** - a flag to enable/disable RADIUS Accounting packet processing. Enabled by default.
 - If processing is enabled: the system accepts and processes Accounting packets, updates the state of active sessions, and terminates them by timeout.
 - If processing is disabled: the system continues to accept packets and responds with correct RADIUS Accounting-Response, but does not perform processing of the received packets.



When RADIUS accounting processing is disabled, the [RADIUS Session Limits](#) section is hidden.

TACACS+

This page configures the operation of the TACACS server as part of NAICE.

Services

RADIUS **TACACS+** Event log

Port TACACS+ * ?

TACACS+ accounting storage duration, days *

TACACS+ session storage duration, days *

Figure 404. Configuring the TACACS service

The following parameters are available for configuration:

- **Port TACACS+** - the TCP-port on which the TACACS server listens for authentication, authorization, and accounting requests via the TACACS+ protocol. Default value - 49.



When saving the configuration, a check is performed only for TCP ports that are used by Docker containers. Ports used by services or applications installed directly on the host machine (outside Docker) are not checked. To avoid conflicts, it is strongly recommended to manually verify, before saving, that the selected port is not in use by other processes on the server.



To apply the setting, the nice-aquila service will be restarted, which will lead to a short interruption in the processing of TACACS+ requests.

- **TACACS+ accounting storage duration, days** - the number of full days from the TACACS accounting session creation date during which they are stored in the database. After this period expires, sessions are deleted. Default value - 31.
- **TACACS+ session storage duration, days** - the number of full days from the TACACS session creation date during which they are stored in the database. After this period expires, sessions are deleted. Default value - 31.



Sessions are periodically checked for expiration and deleted according to a schedule.

Event log

This page configures the operating parameters of the [System events](#) log.

Services

RADIUS TACACS+ **Event log**

Event log storage duration, days * ?

Figure 405. Configuring event log parameters

The following parameters are available for configuration:

- **Event log storage duration, days** - the number of full days from the event creation date during which events are stored in the database. After this period expires, events are deleted. Default value - 31.



Events are periodically checked for expiration and deleted according to a schedule.

Licensing

Connection to ELM

This page configures the NAICE connection parameters to the ELM (Eltex License Manager) license server when licensing through a license server.



For ELM type licenses, when changing licensing related settings, the current active license is reset and its status switches to Backup. This causes the licensed functionality (RADIUS, TACACS+, portal authorization, etc.) paused until the license is reactivated on the [Licensing](#) page.

Go to licensing settings 

Configuring ELM server address

Licensing

Connecting to ELM

! Changing **any** parameter will reset active licenses and suspend authorization functionality. After making changes, manually activate the licenses on the [Licensing page](#).

Address of the ELM licensing server ?

 ?

Use a proxy ?

Figure 406. Configuring connection to ELM without proxy

The ELM server address is configured in the format `domain-name:port` or `IPv4-address:port`, without specifying the protocol used (without "https://"). In the absence of an explicit port specification, port 8099 is automatically applied by the system.

When providing redundant access to the license server, it is possible to specify the address of a second ELM server. If redundancy is not required, configuring a second address is unnecessary.

Using HTTP Proxy

Licensing

Connecting to ELM

! Changing **any** parameter will reset active licenses and suspend authorization functionality. After making changes, manually activate the licenses on the [Licensing page](#).

Address of the ELM licensing server ?

192.0.0.1:8099

Enter host:port ?

Use a proxy ?

Proxy host for ELM *

192.0.0.1:8090

Proxy login for ELM * ?

login

Proxy password for ELM * ?

..... ?

Figure 407. Configuring connection to ELM via HTTP proxy



HTTPS proxy is not supported!

Access to the ELM server via HTTP proxy is supported.

- Proxy host for ELM - the proxy server address in the format domain-name:port or IPv4-address:port, without specifying the protocol used.
- Proxy login for ELM - filled in if authentication is required to work with the proxy server.
- Proxy password for ELM - filled in if authentication is required to work with the proxy server.

Security and access

System Log In

Description

The "System Log In" section is designed for configuring the authentication source through which users gain access to the NAICE system.

By default, system login is performed only using **local accounts**.

If necessary, the use of an external identity source **as the primary authentication source** can be enabled.



Authentication via local accounts always remains available.

Login configuration



To allow users to log in using enterprise accounts from external sources (OpenLDAP, MS Active Directory, etc.), you must first configure an external source in the "[External identity sources](#)" section.

If there are no configured external sources in the system, the source selection option is unavailable. Only login via local accounts is available.

External source

! To configure it, you need to add an external source. x

Add

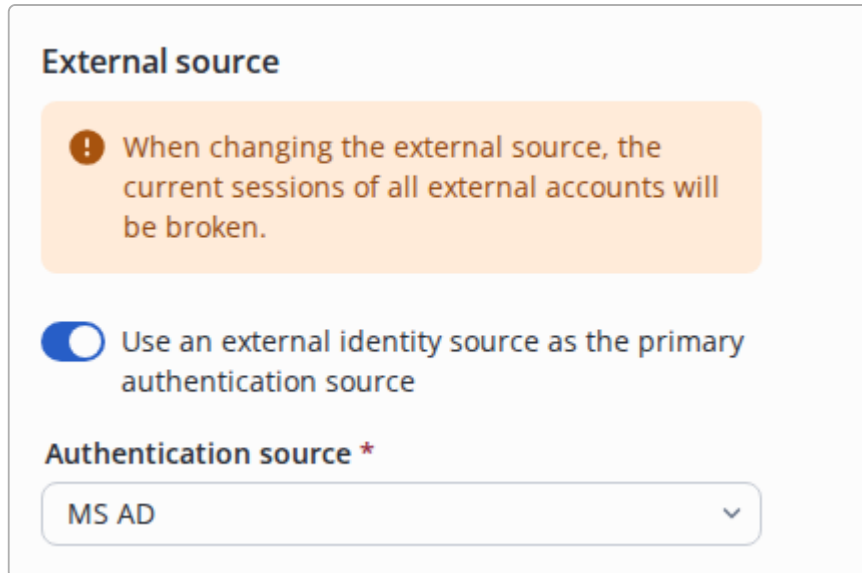
Use an external identity source as the primary authentication source

Figure 408. Login configuration form when no external sources are present



To configure external identity sources, the user role must include the "External sources" privilege with an access level not lower than "Create" (2).

Selecting an external source as the primary authentication source



External source

⚠ When changing the external source, the current sessions of all external accounts will be broken.

Use an external identity source as the primary authentication source

Authentication source *

MS AD

Figure 409. Login configuration form when external sources are present

The following parameters are available in the form:

Use an external identity source as the primary authentication source — a checkbox that enables the use of an external source. When the checkbox is activated, the Authentication source field becomes available:

- Authentication source — selection of an external source from the list added to the system. User credentials will be verified against this source.

To apply the settings, click the "Save" button.

After successful saving, the "Enterprise account" tab appears on the login page for logging in with external accounts:

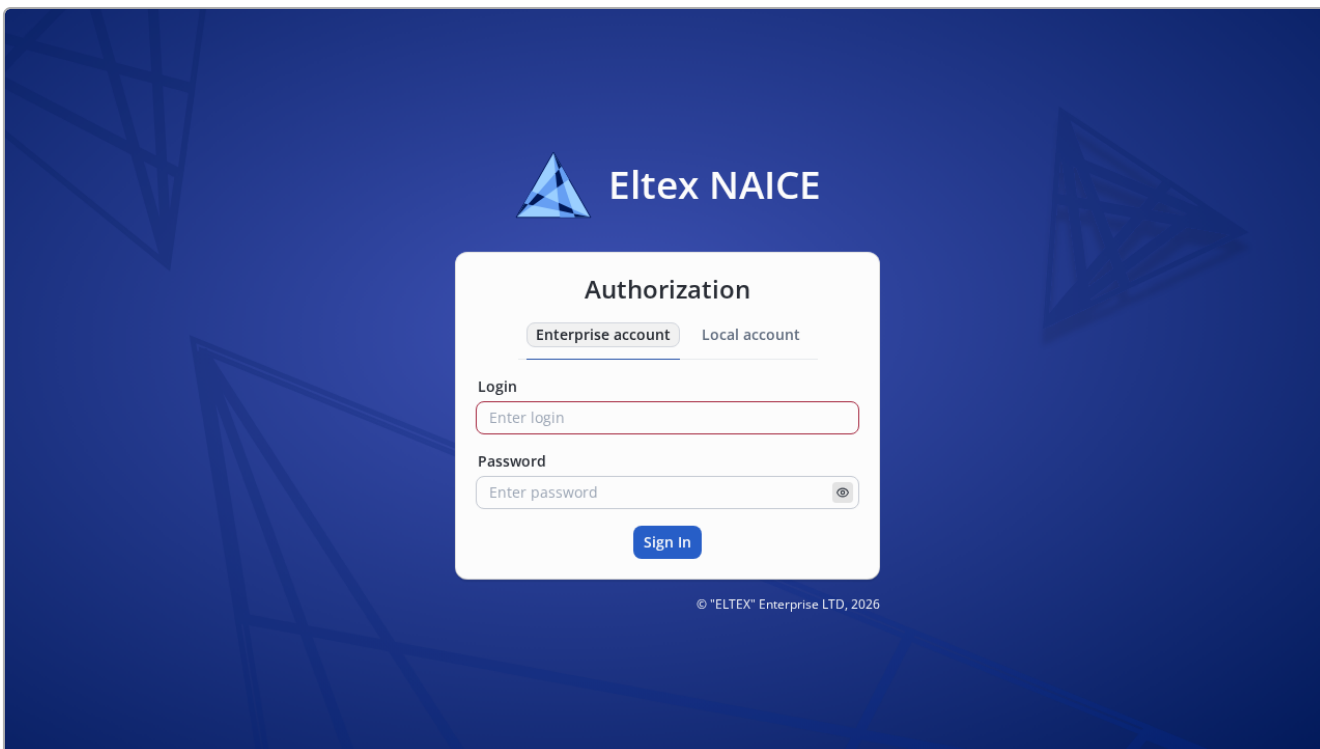


Figure 410. "Enterprise account" tab on the login page



The enterprise account login must not exceed 100 characters.



The "Local account" tab always remains available for authentication using local accounts.

Changing Login Configuration

Any change to the login configuration related to external sources leads to **immediate termination of all active sessions of users authenticated through the old external source**:



- when changing from one external source to another;
- when disabling external authentication (when unchecking the checkbox).

After saving changes, users will need to re-authenticate.

Applying changes to system login settings (changing one external source to another or disabling the use of external authentication) requires confirmation:

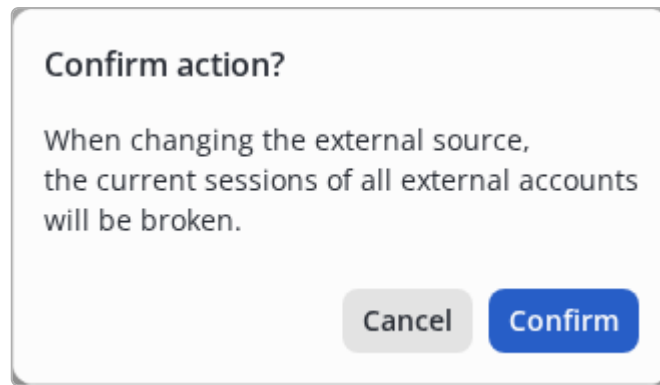


Figure 411. Login configuration change confirmation

Error handling

When problems occur with authentication through an external source, corresponding messages are displayed.

Error "You have no privileges"

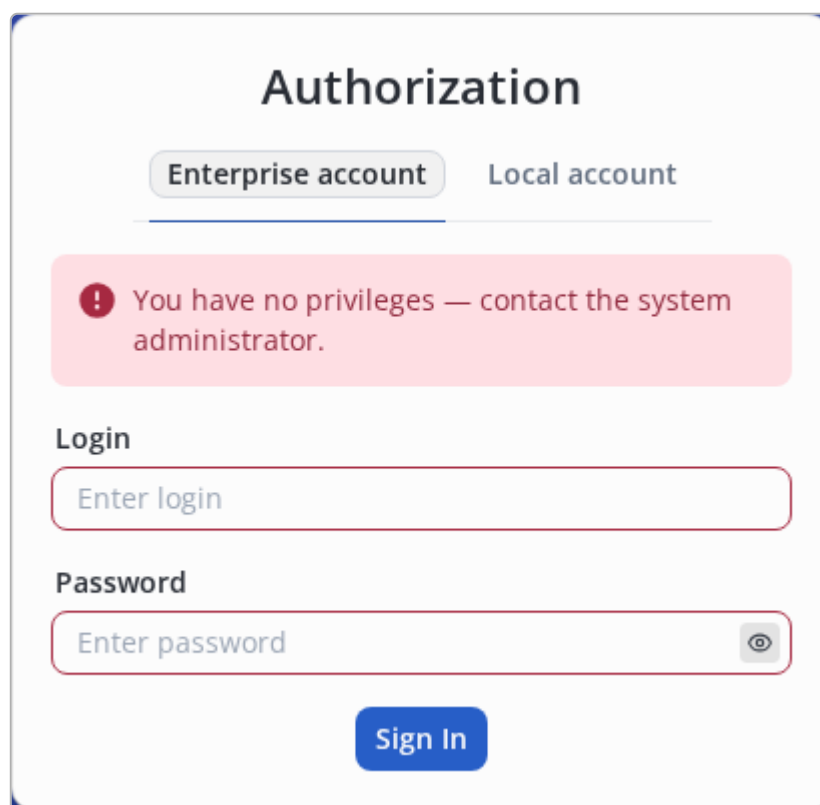


Figure 412. Error when no suitable role is available

Possible reasons:

- No external role matching the user's groups has been configured for the user.
- The configured role has status **Not available** (for example, after changing or disabling the external source).
- User groups are not being read from the external source (issues with attribute configuration).



When using the `CUSTOM` schema for an external source, a situation may occur where groups are not read due to incorrect attribute configuration. This makes group mapping impossible and, consequently, prevents role assignment.

Error "External source is unavailable"

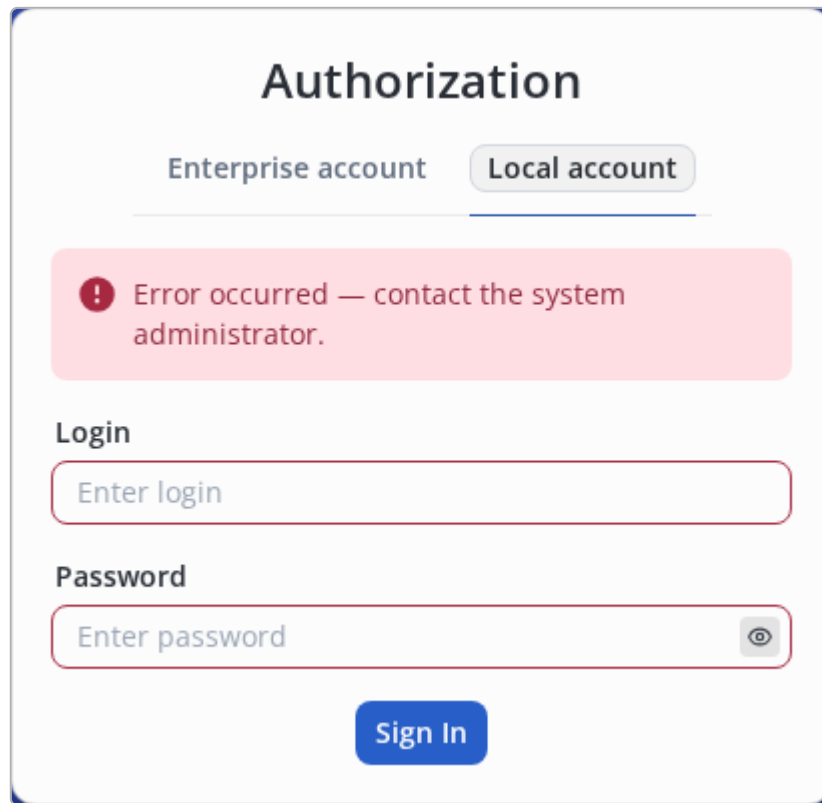
The screenshot shows a web interface titled "Authorization". At the top, there are two tabs: "Enterprise account" (which is selected) and "Local account". Below the tabs, a red error message box contains the text: "External source is unavailable. Contact the administrator or try again later." Underneath the error message, there are two input fields: "Login" with the placeholder text "Enter login" and "Password" with the placeholder text "Enter password" and a toggle icon for visibility. At the bottom of the form is a blue "Sign In" button.

Figure 413. Error when external source is unavailable

Occurs when there is no response from the external source or its configuration is incorrect. Requires checking:

- external source server availability;
- correctness of connection parameters in the source settings;
- network communication between NAICE and the external server.

General authentication error



The screenshot shows a web interface titled "Authorization". At the top, there are two tabs: "Enterprise account" and "Local account", with "Local account" being the active tab. Below the tabs is a red error message box with a white exclamation mark icon, containing the text "Error occurred — contact the system administrator." Underneath the error message, there are two input fields: "Login" and "Password". The "Login" field contains the placeholder text "Enter login". The "Password" field contains the placeholder text "Enter password" and has a small eye icon on the right side. At the bottom of the form is a blue "Sign In" button.

Figure 414. General error when login problems occur

Displayed for other authentication errors not related to roles or source availability.

Troubleshooting



Detailed information about the causes of authentication errors is available on the "[System events](#)" page. The event table records:

- user login attempts;
- role assignment errors;
- connection problems to external sources;
- changes to system login configuration.

Password policies

On this page, you can configure password requirements for [system users](#), as well as notifications regarding system user account actions.

Security and access

System log in
Password policies
Lockout policy
Two-factor authentication
Interaction with /

Password creation requirements

For system users only

Minimum number of characters *

8

The password must contain

- uppercase letters (A-Z)
- lowercase letters (a-z)
- numbers (1-9)
- special symbols ("!@#\$%^&* _+=[])

Additional requirement

- should not contain the login

Notifications

For system users only

- send notifications by email ⓘ

Notifications types *

- creating a new system user ⓘ
- changing system user credentials ⓘ

Gateway for sending *

Notification gateway ▼

Figure 415. Password policy configuration

Password Creation Requirements

- **Minimum number of characters** - the system user's password cannot be shorter than the specified number of characters. The maximum number of characters in a password is 72.
- **Password must contain** - enabling/disabling requirements for the presence of uppercase/lowercase letters, numbers, and special symbols in the password.
- **Additional requirement** - enabling/disabling the requirement that the password should not contain the user's login.



The requirements apply to passwords of newly created users or when changing a user's password. Modifying the password policy does not require previously created users' passwords to be brought into compliance.

Notifications



Settings are displayed only if at least one [notification gateway](#) with an SMTP connection type is configured.

- `send notifications to email` - send emails with the selected notification types to the system user's email address specified in their account.



If the email address is not provided, emails will not be sent.

- Notification types:
 - `creating a new system user` - an email with their account credentials will be sent to the new system user's email address.
 - `changing system user credentials` - notification to the system user about changes to their account.



Configuring email templates is currently unavailable.
The language of the text in emails is configured on the [:system/common-settings.html](#) page, "system language" setting.

- `Gateway for sending` - select one of the existing SMTP gateways in the system through which you plan to send emails.

Lockout policy

The "**Lockout policy**" section is used to configure automatic temporary lockout of system user accounts when the allowed number of unsuccessful sign-in attempts is exceeded.



The lockout policy applies only to system user accounts (administrators).

Configuring the lockout policy

In the "**Account Lockout**" block, the parameters used by the system to determine whether a user account must be temporarily locked can be configured.

To enable the policy, switch the toggle to **Enabled**.

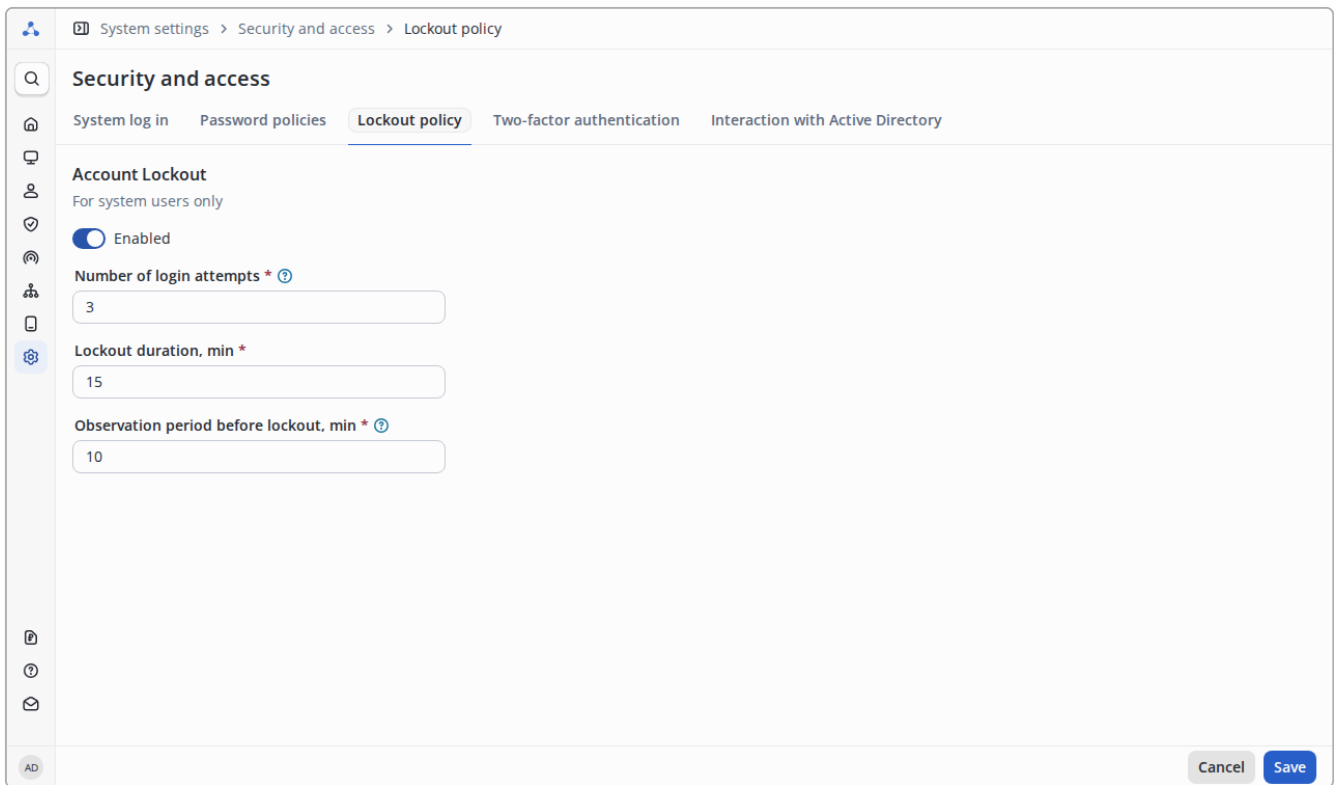


Figure 416. Configuring the lockout policy for system users

If the policy is enabled, the following parameters are available:

Parameter	Description
Number of login attempts	The maximum number of unsuccessful attempts to enter a password or two-factor authentication codes, after which the account will be temporarily locked. The counter is maintained separately for each factor (password, TOTP, Email OTP, backup codes).
Lockout duration, min	The period of time (in minutes) for which the user account is locked. After this time expires, the lockout is automatically removed, and the user can attempt to sign in again.
Observation period before lockout, min	The period of time (in minutes) during which the system counts unsuccessful sign-in attempts. If the number of attempts exceeds the specified threshold within this window, the account is locked.

After changing the lockout policy parameters, save the settings by clicking the "Save" button.

The new rules apply to subsequent user sign-in attempts.



Changing the lockout policy does not terminate currently active user sessions. All new rules take effect from the next sign-in attempt.

How the lockout policy works

The lockout policy protects user accounts from password and two-factor authentication code brute-force attacks. The system records all unsuccessful sign-in attempts, including:

incorrect password;

- incorrect one-time TOTP code;
- incorrect Email OTP code;
- incorrect backup code.

The account is locked if, during the specified **observation period before lockout**, the number of unsuccessful attempts reaches the value specified in the **Number of login attempts** field.

After the lockout, the user cannot sign in to the system until one of the following conditions is met:

- the specified **lockout duration** expires;
- an administrator manually unlocks the account through the "**Accounts**" section (see "[Blocked account](#)").

Example 5. Example of how the lockout policy works

If the following values are specified:

- **Number of login attempts** — 3;
- **Lockout duration** — 15 minutes;
- **Observation period before lockout** — 10 minutes,

then the account will be locked for 15 minutes if the user makes 3 unsuccessful sign-in attempts (entering the password or 2FA codes) within any 10-minute period.



In order for users to receive email notifications about account blocking or unblocking, you need to configure notification delivery in the **System Settings** → **Security and access** → [Password policy](#) section.

Disabling the lockout policy

To disable the lockout policy, switch the toggle to **Disabled** and save the settings.

After the policy is disabled:

- automatic account lockout is **stopped**;
- already locked accounts **remain in the "Blocked" status** until the lockout duration expires or an administrator manually unlocks them;
- unsuccessful attempt counters are **not reset**, but are no longer counted until the policy is re-enabled.



Disabling the lockout policy reduces the level of protection against brute-force attacks. It is recommended to use this function only for diagnostics or in exceptional cases.

Two-factor authentication

Interaction with Active Directory

Description

The *Interaction with Active Directory* page configures periodic automatic password changes for computer accounts used to interact with Active Directory. This setting applies to all computer accounts configured in all identity sources using the Active Directory schema.

Configuring Password Change Schedule

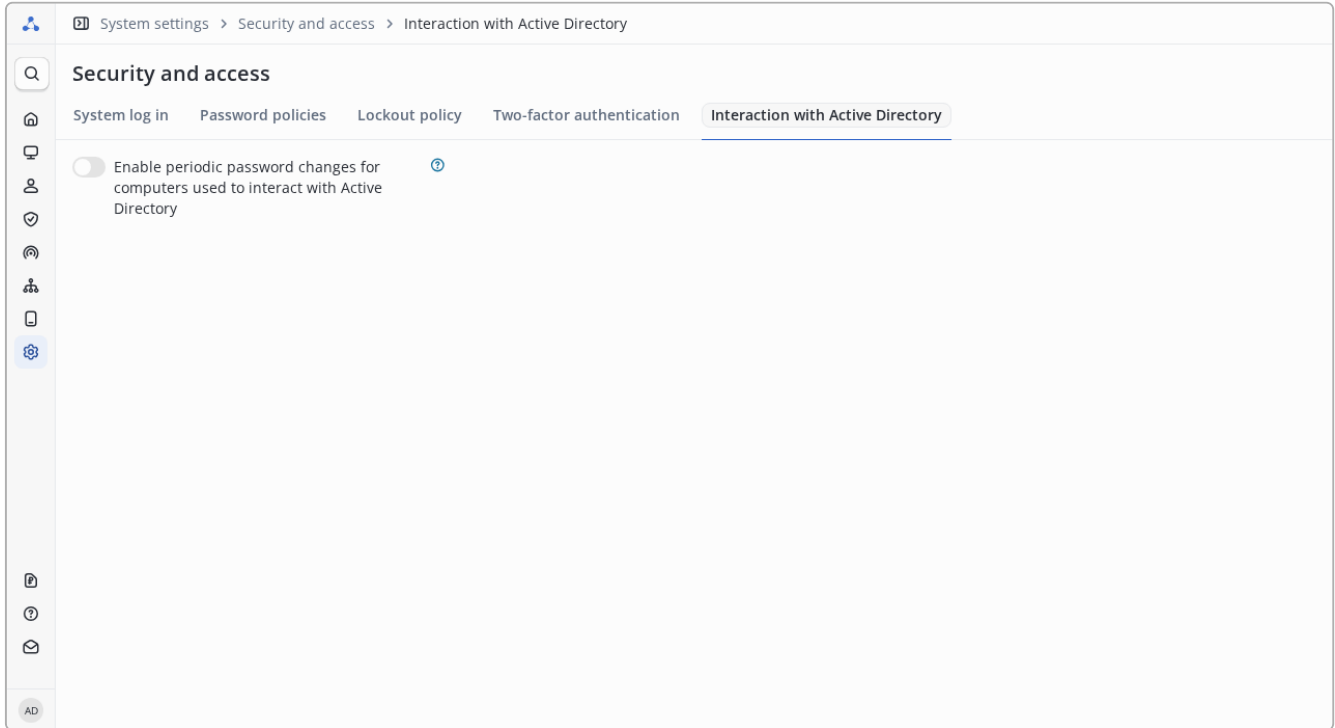



Figure 417. Interaction with Active Directory - disabled

At the top of the page is the toggle:

- Enable periodic password changes for computers used to interact with Active Directory - enables/disables automatic password changes for all computer accounts in all Active Directory identity sources. Hovering over  shows a description of this setting.

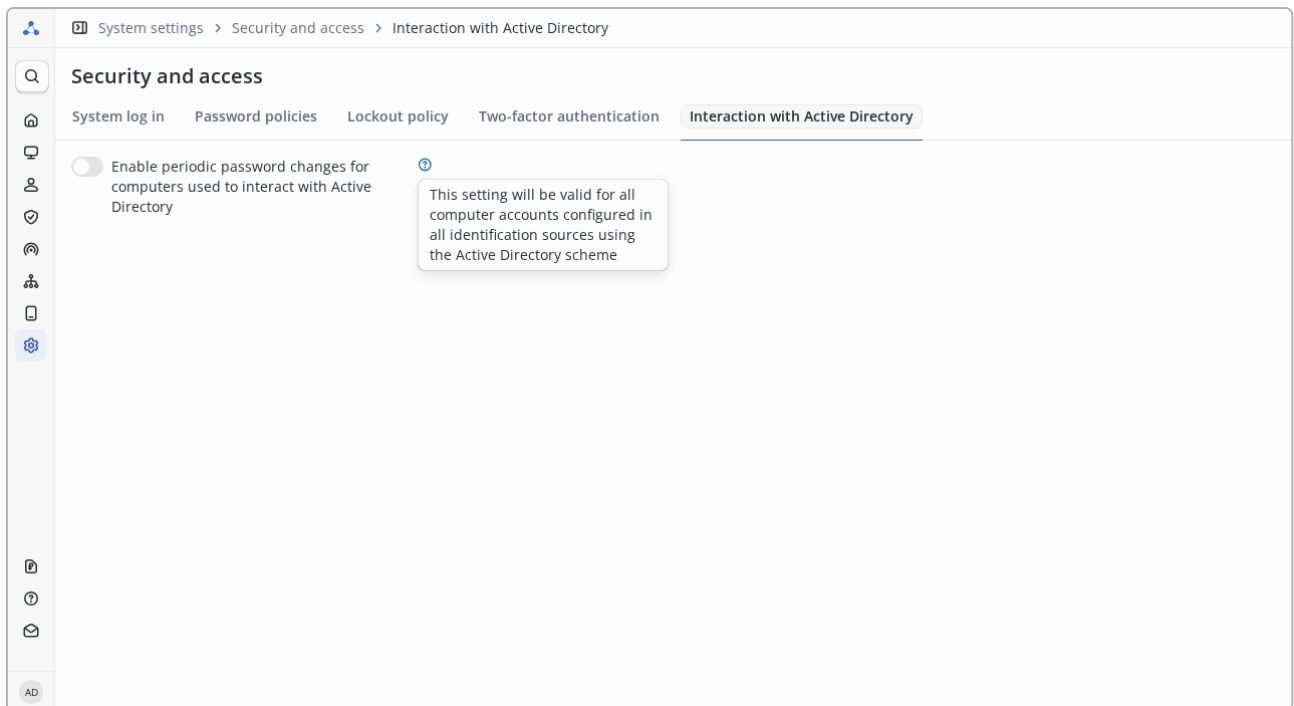


Figure 418. Setting description

When the toggle is enabled, the **Password change schedule** block opens:

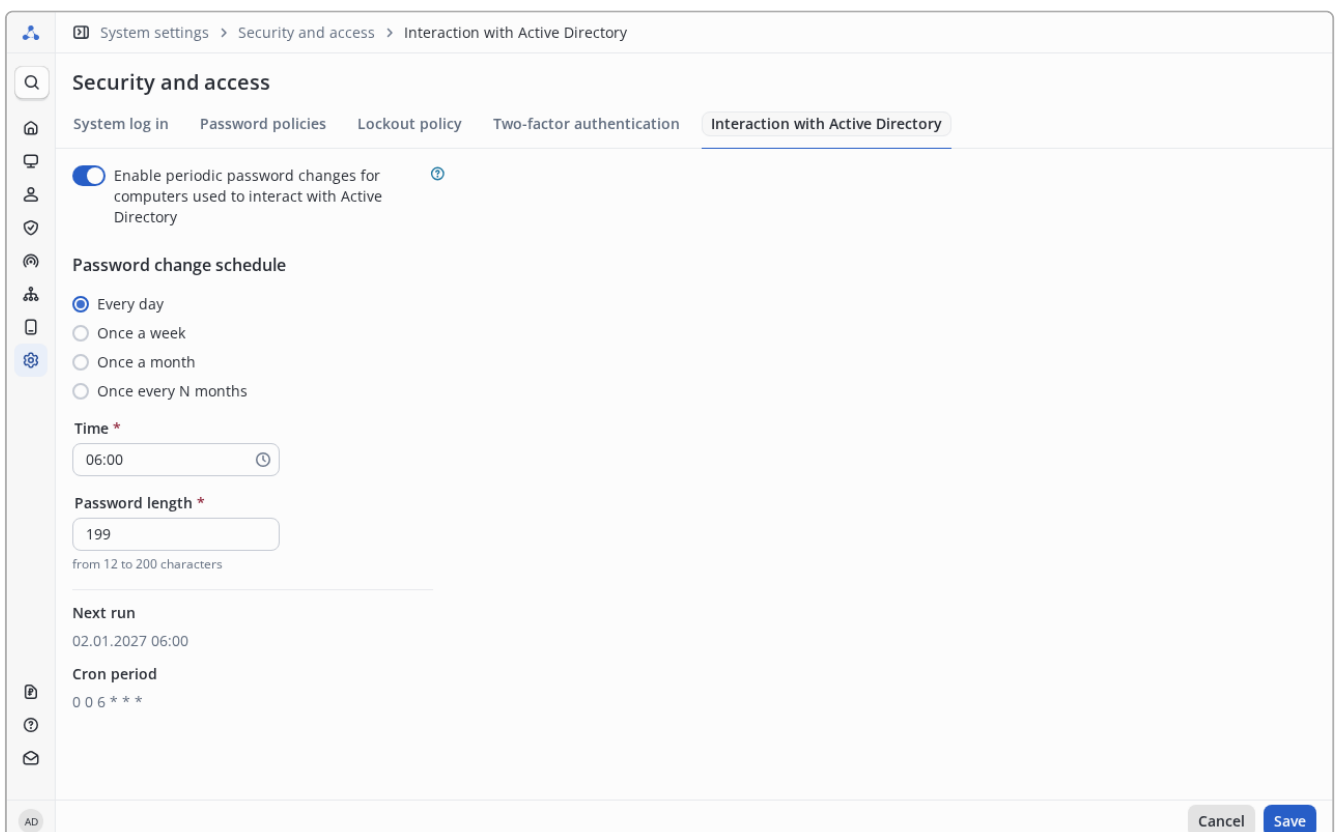


Figure 419. Password change schedule

The schedule block contains the following parameters:

- **Schedule type** - one of the following options:
 - **Every day** - password change is performed daily at the specified time.

- Once a week - an additional Day of week * field appears.

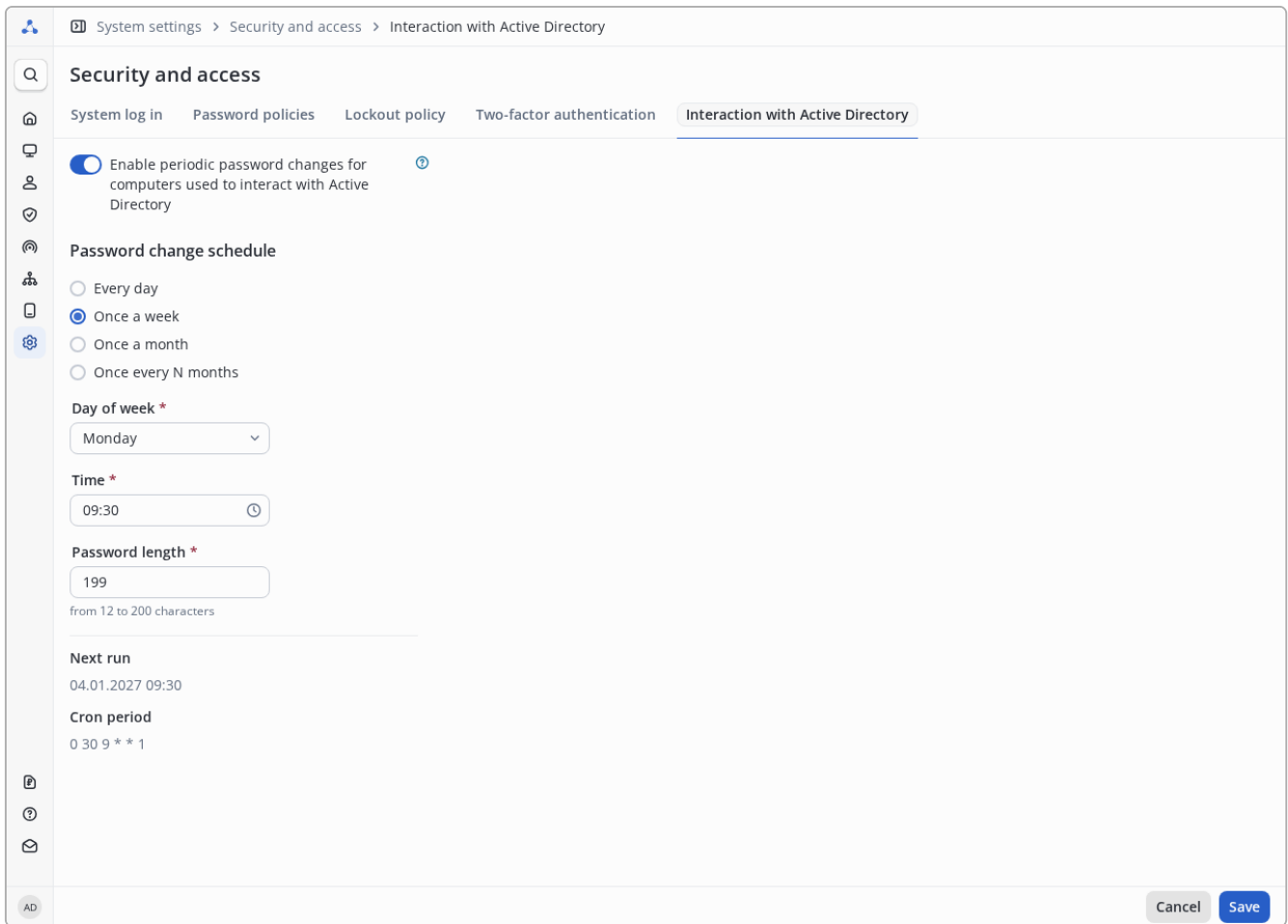


Figure 420. Password change schedule - weekly

- Once a month - an additional Day of month * field appears.

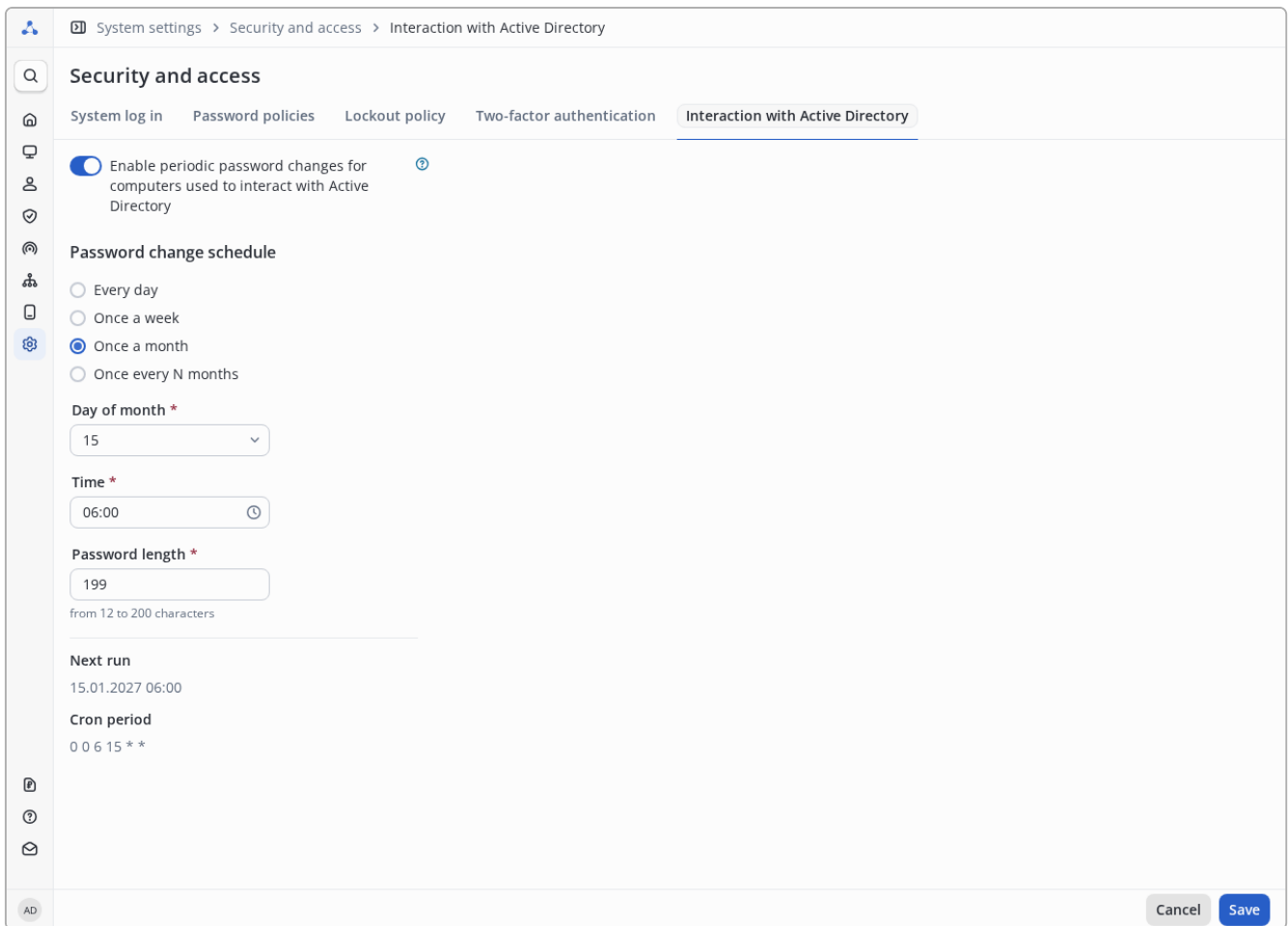


Figure 421. Password change schedule - monthly

- Once every N months - Shift period N * and Day of month * fields appear.

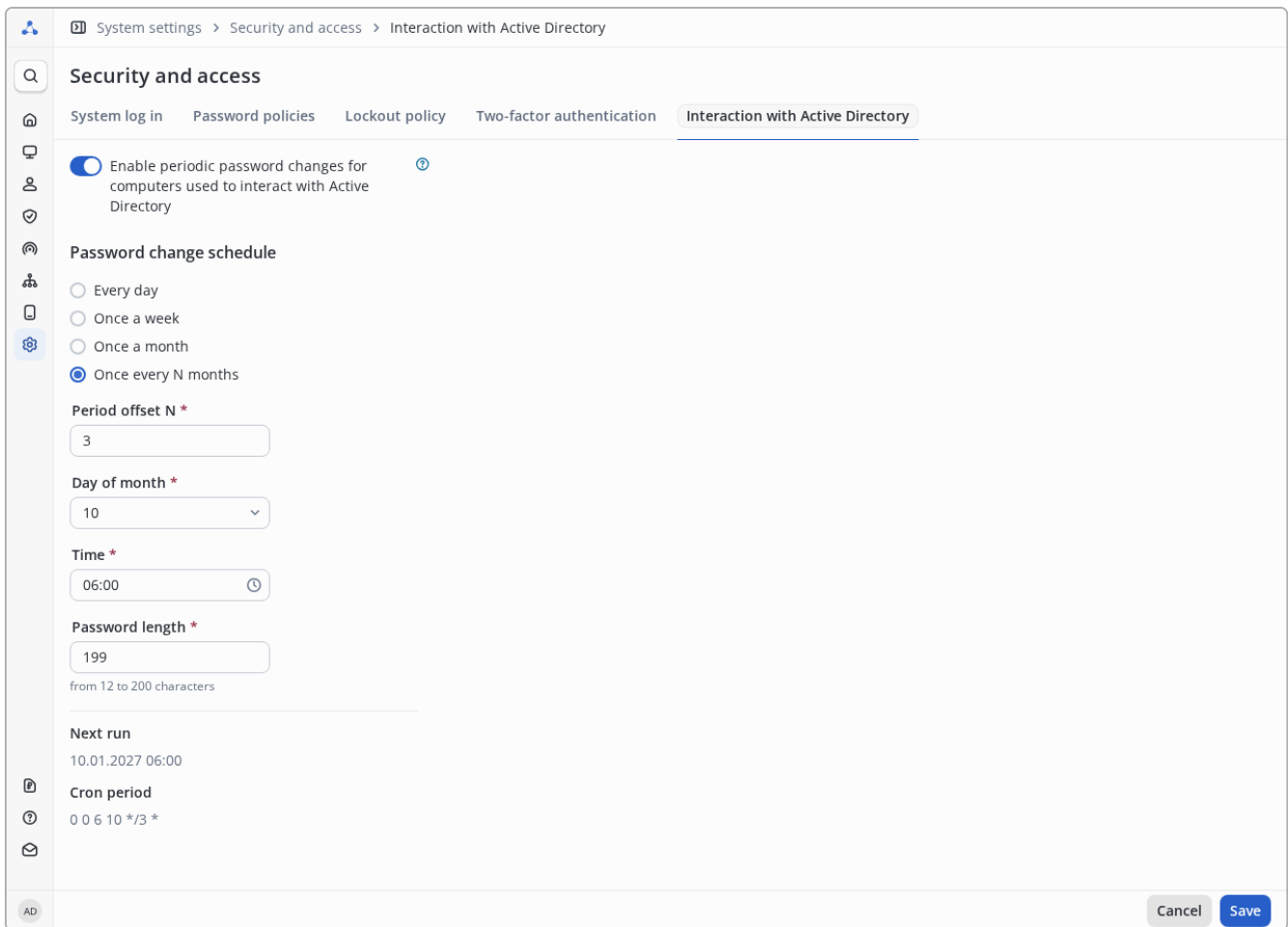


Figure 422. Password change schedule - every N months

- **Time *** - time to perform the password change in hh:mm format.
- **Password length *** - length of the new password. Valid range: from 12 to 200 characters.

Parameters marked with * are required.

At the bottom of the page, additional information is displayed:

- **Next run** - calculated date and time of the next automatic password change.
- **Cron period** - generated Cron expression for the schedule.



If the required parameters are not filled in completely, the value *Unknown* is displayed.

To apply the changes, click the **Save** button. To cancel - click the **Cancel** button.

Certificate store

Trusted Certificates








Description

The **Trusted Certificates** section is intended for managing certificates that the NAICE system trusts when establishing secure connections, for example when connecting to external services.

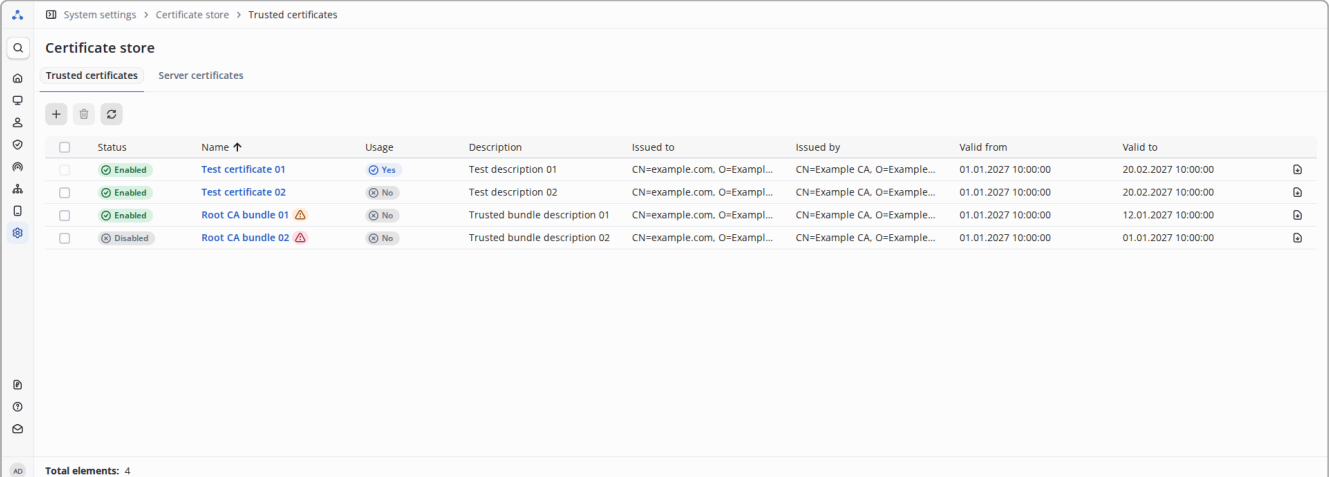
Added certificates form a trusted list used by the system to verify the authenticity of a remote node certificate. The section provides the following operations for working with certificates: viewing, editing, downloading, and deleting.








Controls

Controls in this section are standard and are used similarly to other sections of the system.

-  - Add a new certificate.
-  - Delete selected certificates (inactive until no certificate is selected).
-  - Refresh table data.
- - Checkbox for selecting elements to perform further actions, for example, deletion.
-  - Change the current sorting order.
-  - Download a previously uploaded certificate.
-  - Indicator signaling that the certificate will expire soon.
-  - Indicator signaling that the certificate has expired.

Viewing the list of trusted certificates



<input type="checkbox"/>	Status	Name ↑	Usage	Description	Issued to	Issued by	Valid from	Valid to	
<input type="checkbox"/>	Enabled	Test certificate 01	Yes	Test description 01	CN=example.com, O=Exempl...	CN=Example CA, O=Example...	01.01.2027 10:00:00	20.02.2027 10:00:00	
<input type="checkbox"/>	Enabled	Test certificate 02	No	Test description 02	CN=example.com, O=Exempl...	CN=Example CA, O=Example...	01.01.2027 10:00:00	20.02.2027 10:00:00	
<input type="checkbox"/>	Enabled	Root CA bundle 01 	No	Trusted bundle description 01	CN=example.com, O=Exempl...	CN=Example CA, O=Example...	01.01.2027 10:00:00	12.01.2027 10:00:00	
<input type="checkbox"/>	Disabled	Root CA bundle 02 	No	Trusted bundle description 02	CN=example.com, O=Exempl...	CN=Example CA, O=Example...	01.01.2027 10:00:00	01.01.2027 10:00:00	

Total elements: 4

Figure 423. Table of trusted certificates

The page displays a table with a list of trusted certificates added to the system by the user.

The table contains the following columns:

- **Status** - the current state of the certificate ("Enabled" or "Disabled").
- **Name** - the unique certificate name in the system.
- **Description** - an arbitrary description assigned to the certificate by the user.
- **Issued to** – value from the certificate **Subject** field (certificate owner, the entity to which the certificate was issued).
- **Issued by** – value from the certificate **Issuer** field (certificate issuer).
- **Valid from** - value from the certificate **Not Before** field (start of the certificate validity period).

Valid to - value from the certificate **Not After** field (end of the certificate validity period).

Adding a trusted certificate

To add a new certificate, click **+**.

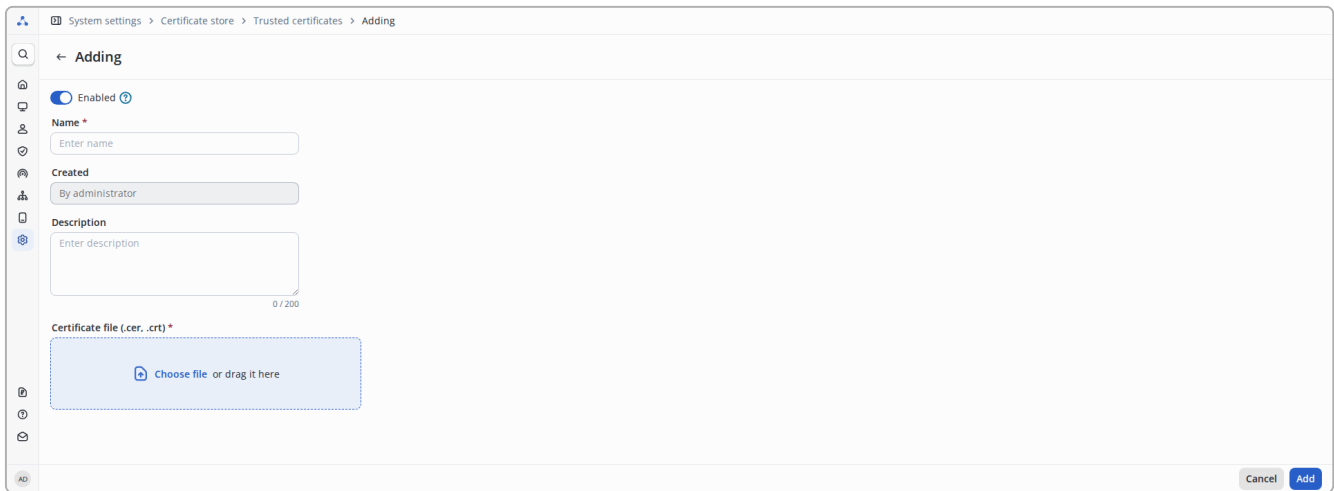


Figure 424. Add trusted certificate window

The add page contains the following parameters:

- **Status** - Determines whether the certificate will be enabled immediately after being added.
- **Name *** - Used to identify the certificate in the interface and events.
- **Description** - An arbitrary description of the certificate.
- **Certificate file (.cer, .crt) *** - Field for adding a certificate file.

Parameters marked with an asterisk ***** are required.

The actual name and extension of the uploaded certificate are also displayed on this page.

Certificate requirements:

- Certificates in **.cer** and **.crt** formats that comply with the **X.509** standard are supported. Certificates in **.pem** format are not supported.
- Private keys do not need to be uploaded to the system.
- Only files containing a single certificate are allowed. Uploading files containing a certificate chain (for example **Root CA** and **Intermediate CA**) or multiple arbitrary certificates is not allowed.
- A certificate for secure LDAP connection must contain a SAN (Subject Alternative Name) field specifying the **domain name** (example **DNS:ldap.example.org**) or **IP address** (example **IP Address:192.168.0.10**) of the host.



Possible errors when uploading certificates to the system

Below are the main errors that may occur when uploading trusted certificates, as well as their causes.



Figure 425. Certificate file is invalid

Reason: The certificate may have an incompatible structure, or the certificate file contains corrupted or incomplete data.

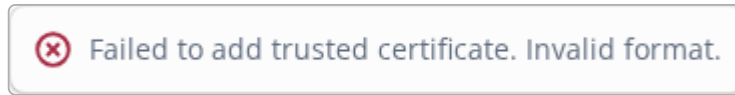


Figure 426. Unsupported certificate format

Reason: The selected file is not a certificate, or an invalid extension was assigned during naming (for example, docx).



Figure 427. Certificate validity period has expired

Reason: The certificate validity period has expired.

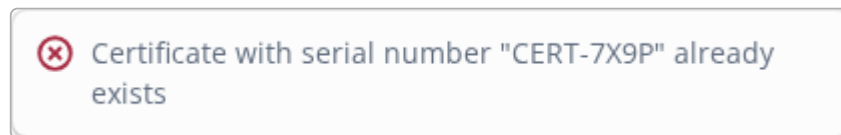


Figure 428. A certificate with the specified serial number already exists

Reason: Attempt to upload a certificate that already exists in the system.

Downloading a certificate from the system

To download a certificate, click  in the table displaying all certificates.





	Valid to	
:00	20.02.2027 10:00:00	
:00	20.02.2027 10:00	 Download certificate
:00	12.01.2027 10:00:00	
:00	01.01.2027 10:00:00	

Figure 429. Downloading a certificate from the system

Viewing a certificate

To view detailed information about a certificate, click its name in the table.

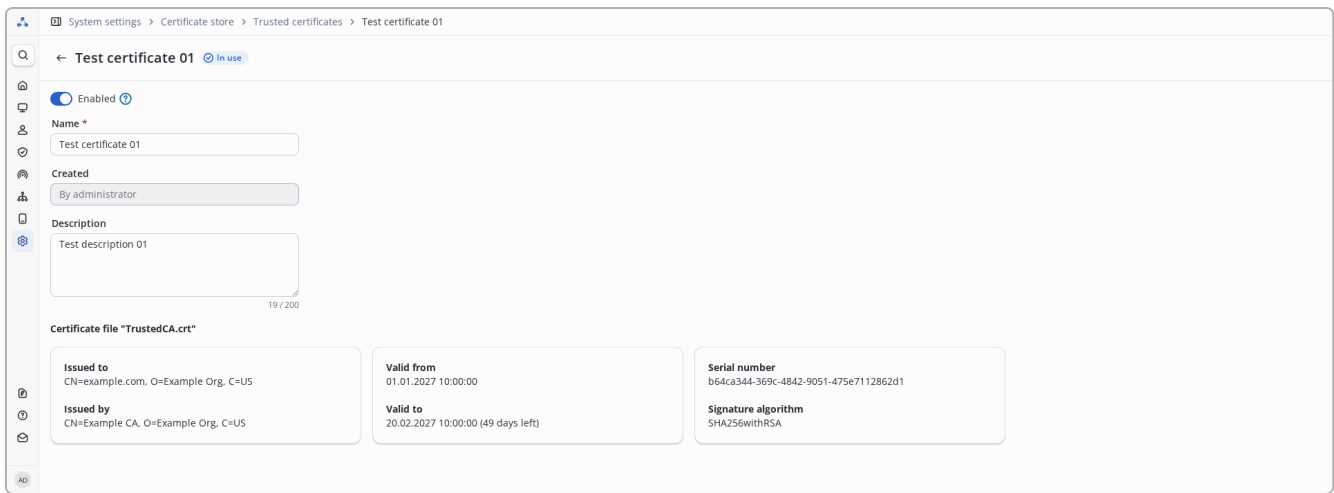


Figure 430. Trusted certificate view page

The following parameters are displayed on the view page:

Main fields

- **Status** - Determines the state of the certificate ("Enabled" or "Disabled").
- **Name *** - Certificate name used for identification in the NAICE system.
- **Description** - An arbitrary description of the certificate created by a NAICE system user.
- **File name** - Name of the uploaded certificate file.

Certificate identification

- **Issued to** – value from the certificate **Subject** field (certificate owner, the entity to which the certificate was issued).
- **Issued by** – value from the certificate **Issuer** field (certificate issuer).
- **Valid from** - value from the certificate **Not Before** field (start of the validity period).
- **Valid to** - value from the certificate **Not After** field (end of the validity period).
- **Serial number** - unique certificate identifier **Serial Number**, assigned by the issuer (CA).
- **Public key algorithm** - algorithm used to sign the certificate - **Signature Algorithm**.

Indication of expiring/expired certificates

Expiring – the certificate validity period is nearing its end and will expire soon. This state is displayed if less than 30 days remain before the certificate expires. In this case, if necessary, the certificate should be replaced in advance to avoid errors when establishing secure connections.



Figure 431. Certificate is expiring

Expired – the current date and time exceed the certificate expiration date. Such a certificate should be replaced immediately with a valid one.

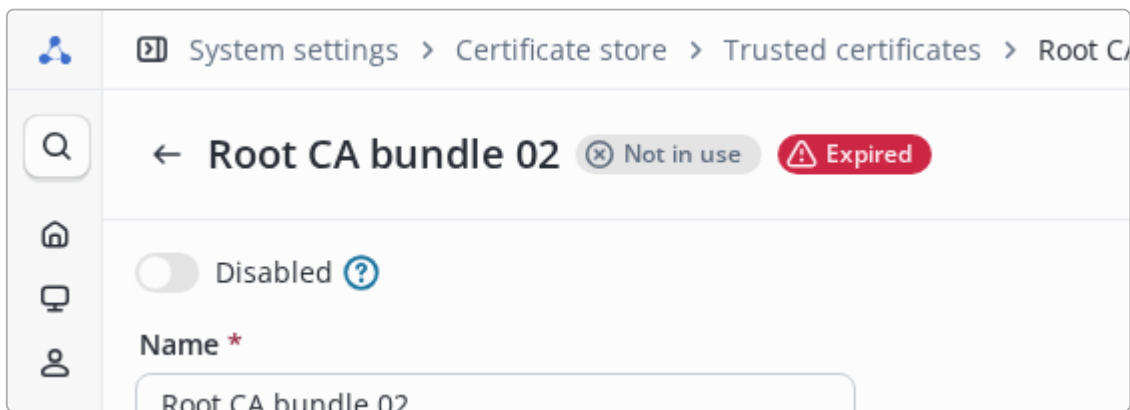


Figure 432. Certificate has expired



Expired certificates can still be used to verify the authenticity of external services while they remain in the "Enabled" state, if this is allowed by the service itself.

Editing a certificate

Editing a selected certificate is performed on its view page, which can be accessed by clicking the certificate name.

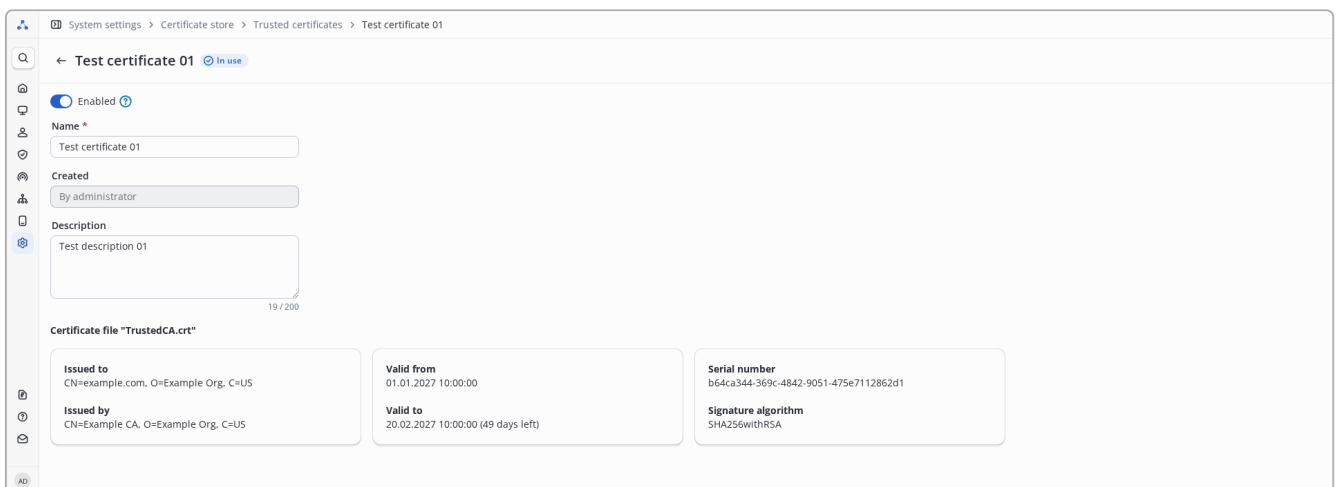


Figure 433. Editing certificate parameters

The following certificate parameters can be changed:

- Name
- Description
- Status



Replacing the certificate file during editing is not supported. To change the certificate contents, delete the entry and upload the certificate again.

Enabling and disabling a certificate

Certificate usage can be suspended without removing it from the system. To do this, change the **Status** field to "Disabled" in the edit form and save the changes.

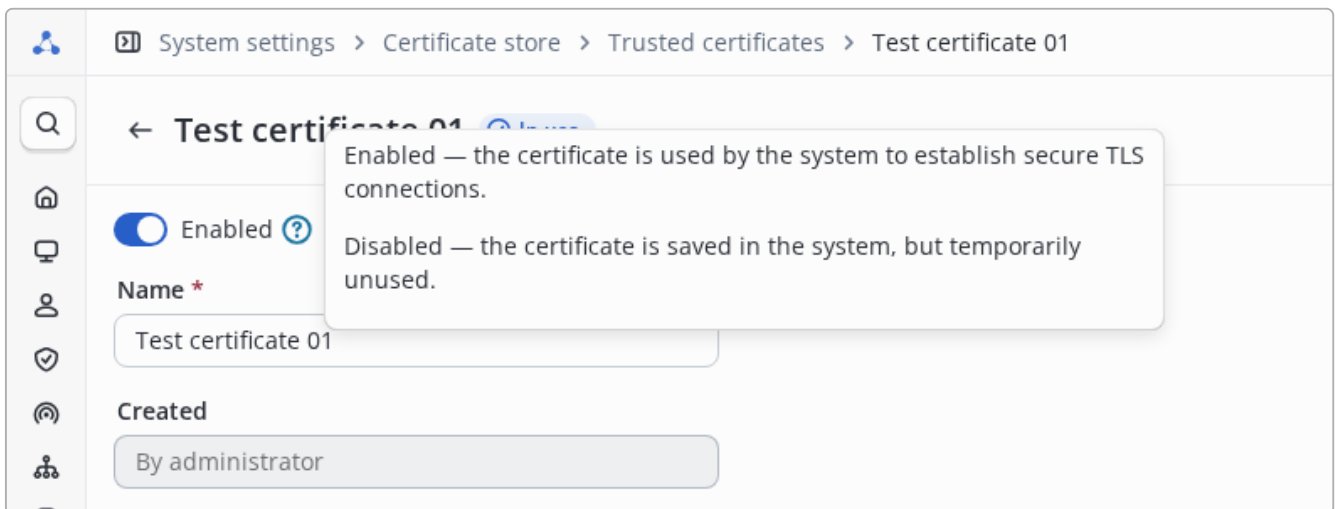


Figure 434. Enabling and disabling a certificate

A disabled certificate:

- Remains in the list;
- Appears in system events;
- Is not used by the system when establishing TLS connections.

Deleting trusted certificates

To delete, select one or more certificates using and click .



Deleting items requires confirmation in the modal window. The selected items will be deleted only after explicit confirmation of the operation.

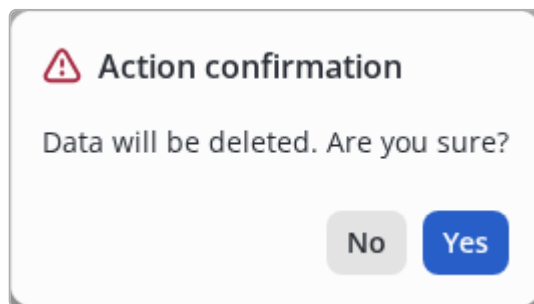


Figure 435. Modal dialog for confirmation



Deleting a certificate is an irreversible operation. Before deletion, make sure that the certificate is not used in the active system configuration, for example, in [external identity sources](#).

Events related to certificates

Operations with trusted certificates are recorded in the [system event log](#).

The following actions are recorded:

- Adding a certificate.
- Editing the certificate name and description.
- Changing the status (enable/disable).
- Deleting certificates.
- Warning about upcoming certificate expiration.
- Warning about certificate expiration.



Warnings about certificate expiration or upcoming expiration in the [system event log](#) are recorded only for certificates in the "Enabled" state. For certificates in the "Disabled" state, such events are not recorded.

Server Certificates

Troubleshooting

Logs

This page configures the logging level for NAICE services. The setting is applied to all services simultaneously; it is not possible to set a different log level for one service compared to the others.



Applying this setting does not require a restart of NAICE services, so changing the value does not cause service interruption.

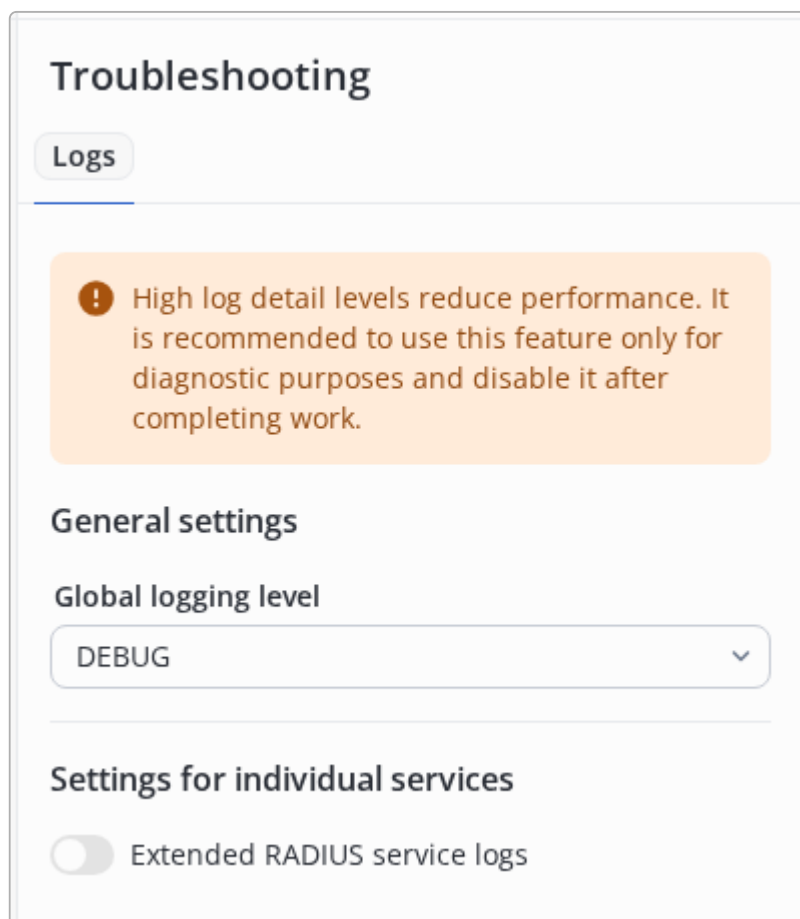


Figure 436. Logging Level Configuration

NAICE services have 6 logging levels. Each subsequent level includes logs from the previous levels, as well as logs specific to that level.

The list of levels in ascending order:

- **FATAL** - Includes only incidents that lead to the stoppage of NAICE services. **Not recommended for configuration**, as the cause of a stop is usually found at the following levels. Minimum number of generated logs.
- **ERROR** - Includes incidents that lead to errors in providing NAICE's core functionality.
- **WARN** - Includes unexpected/suspicious incidents that do not directly lead to a stop in core functionality but could potentially lead to errors.
- **INFO** (default) - Includes both negative and major positive incidents, the tracking of which is planned.
- **DEBUG** - Includes detailed logs necessary for diagnosing problems that arise during NAICE operation. The required log level for problem analysis by technical support.
- **TRACE** - The most detailed log level, used for deep diagnostics of complex problems. **Not recommended for configuration** without a direct instruction from a technical support employee, as it leads to the generation of a huge volume of logs.



It is important to consider that a higher logging level leads to a greater number of generated logs, and consequently, to more frequent log rotation. Log rotation parameters are specified during NAICE installation.

Nodes

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 ELM server address is specified in the system settings under [Connection to ELM](#) and must be accessible at the moment of license activation. The ability to work with the ELM server via an HTTP proxy server (with or without username/password 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 supports 2 license types - **BASIC** and **ADVANCED**. Each subsequent type includes all features of the previous one and adds support for extended functionality.

Licenses for any type can be issued for 1, 3, or 5 years.



For license inquiries, please contact us at eltex@eltex-co.ru.

BASIC License Type

The **BASIC** type provides access to the core service - RADIUS authorization of [endpoints](#). The licensed parameter is **the number of successfully authorized unique endpoints per day**. This quantity is agreed upon during license purchase and depends on the number of client devices in 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.

ADVANCED License Type

At this license type, the functionality required for configuring and operating portal authorization is activated. For any license of this type, the number of [guest endpoints](#) is unlimited, meaning authorization is available for any number of guests.

Additional Modules

The **NAICE-TACACS** add-on module is also available for purchase, which activates the TACACS server within NAICE. Modules are purchased as add-ons to the main license of any type.

Demo mode

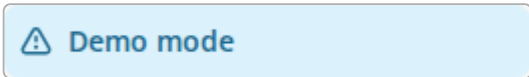
After installation, NAICE is in demo mode. In this mode, all functionality corresponding to the maximum license type and with all additional modules is available, but with the following restrictions:

- the maximum number of [devices](#) added to the system is 15;
- the maximum number of successfully authorized unique [endpoints](#) per day is 15;
- the maximum number of [guest endpoints](#) 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.

A corresponding warning in the lower left part of the navigation menu indicates that the system is in demo mode.



⚠ Demo mode

Figure 437. 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.

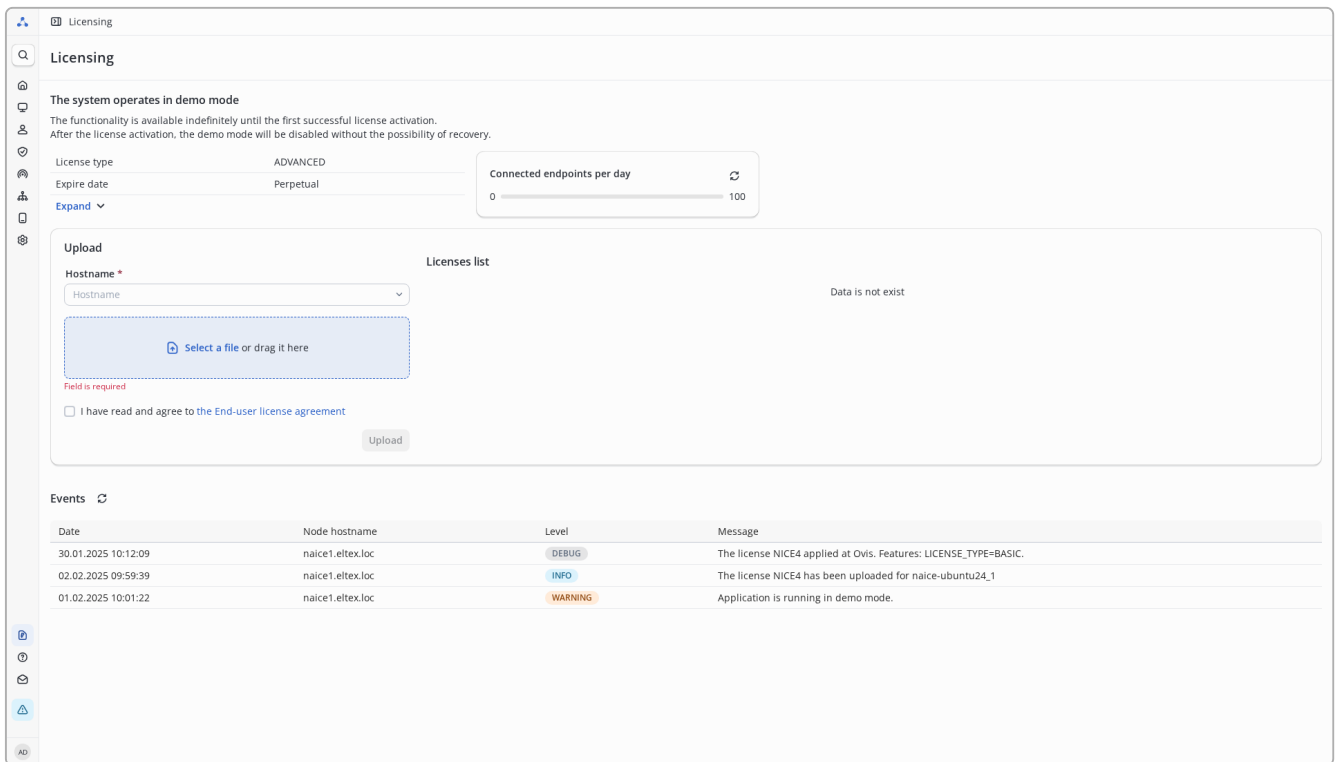


Figure 438. The Licensing in demo mode page

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.

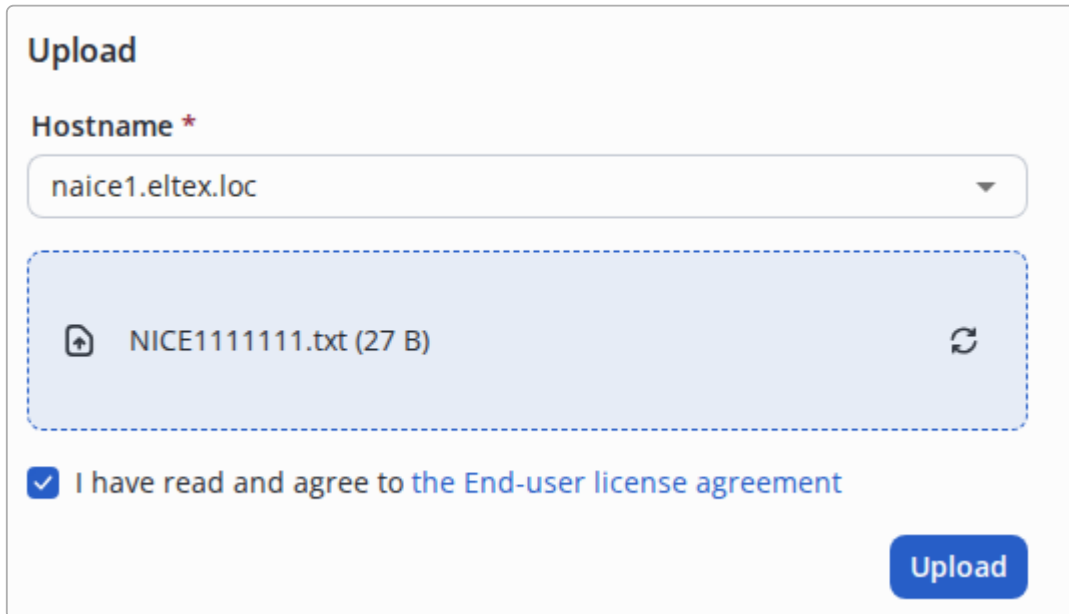


Figure 439. Uploading a product key file

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.

Licenses list				
Hostname	Product ID	Type	Status	Actions
naice1.eltex.loc	NICE1111111	ELM	Active	

Figure 440. 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.

Licenses list				
Hostname	Product ID	Type	Status	Actions
naice1.eltex.loc	FNICE1111111	PLR	Init	

Figure 441. 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**.

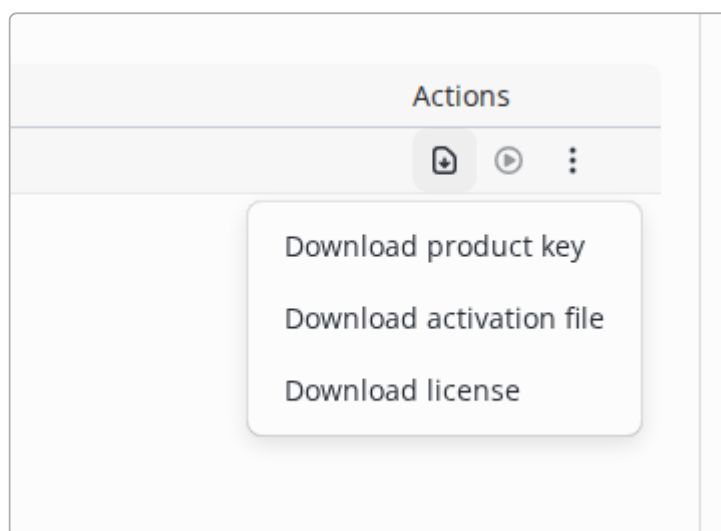


Figure 442. Download menu for licensed files



Activation file name format **request-`<YYYY-MM-DD>-<Product ID>-<NAICE Version>.txt`**, for example - **request-2026-06-17-FNICE1111111-1.2.0.txt**.

2. Send the activation file to the Eltex company to issue a file license corresponding to the provided activation file.

3. Get the license file from the Eltex company.
4. Upload the license file 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.

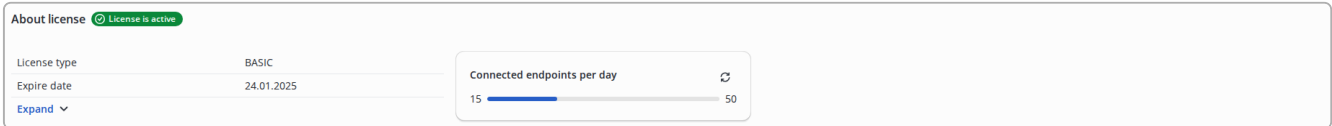


Figure 443. Information about the active license

License activation errors

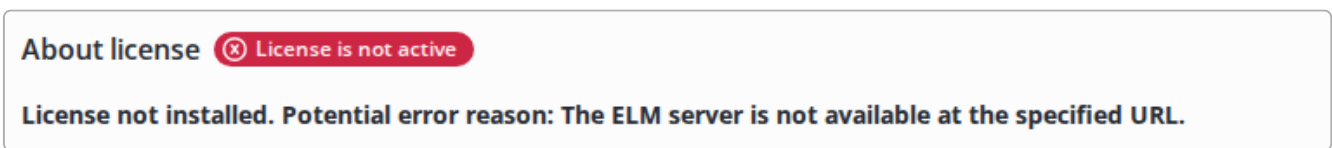




Figure 444. Error when activating the license

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.





Licenses list 				
Hostname	Product ID	Type	Status	Actions
naice1.eltex.loc	NICE1111111	ELM	Ready	  

Figure 445. The license has the Ready status

License is revoked

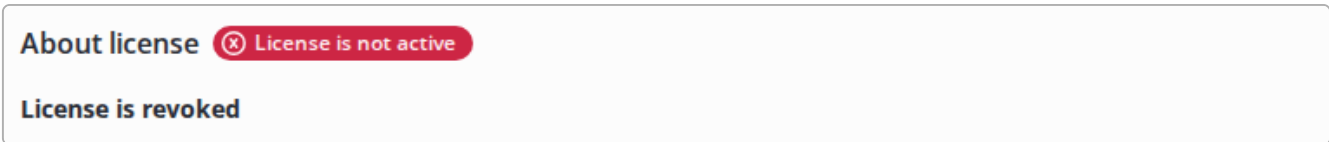


Figure 446. License is revoked

The "License is revoked" error occurs if the activated PLR license is not included in the list of actual PLR licenses. This may happen when the license is revoked by Eltex due to receiving information about its mass distribution on public resources. Older versions of [reactivated](#) or [renewed](#) licenses are also subject to revocation.



If you believe your license was revoked by mistake, please contact your manager, Eltex technical support, or send a request to our email address eltex@eltex-co.ru.

License management and monitoring

After successful activation of the licenses, their status can continue to be monitored on the *Licensing* page.

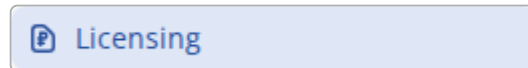


Figure 447. The Licensing item in the navigation menu

Information about the active license

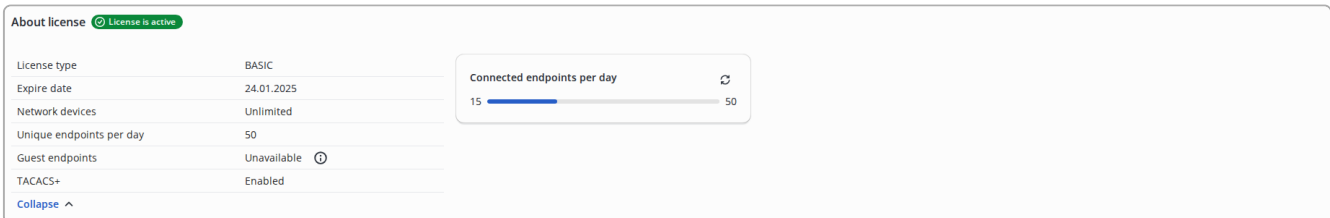



Figure 448. License information

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.

- [Guest endpoints](#) - the limit of the number of [guest endpoints](#).
- [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.
- The [Calling-station-id](#) attribute is used to determine endpoint uniqueness.
- If the specified attribute is missing, indirect determination use the following attributes:
 - [User-Name](#) - This attribute must be present in the RADIUS request.
 - [NAS-IP-Address](#) or [NAS-Identifier](#) - At least one of the specified attributes must be present.
 - [NAS-Port](#) - This attribute is optional.
 - [NAS-Port-Type](#) - This attribute is optional.
- Portal-authorized endpoints ([guest endpoints](#)) are excluded from the count.
- The device is considered connected for exactly 24 hours from the last successful connection. Upon successful re-authorization, the 24-hour countdown is renewing.

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.





Licenses list 				
Hostname	Product ID	Type	Status	Actions
naice1.eltex.loc	NICE1111111	ELM	Ready	  
naice1.eltex.loc	FNICE1111111	PLR	Backup	  

Figure 449. 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;
 - **Revoked** (for PLR only) - the license has been revoked by the Eltex company;
 - **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:

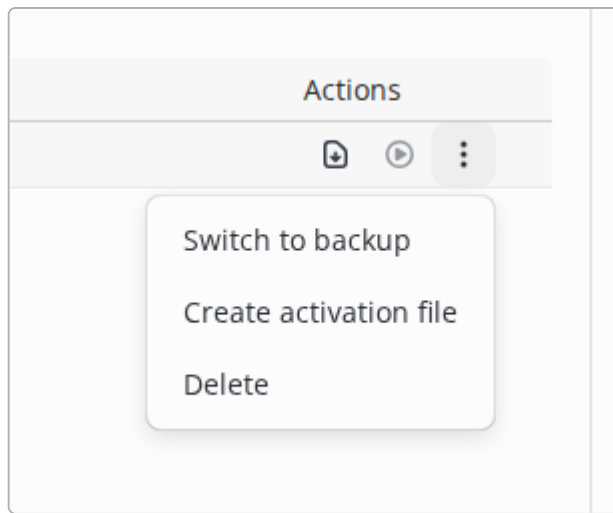





Figure 450. License actions

-  - 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

Date	Node hostname	Level	Message
01.02.2025 20:35:20	naice1.eltex.loc	DEBUG	The license NICE4 applied at Ovis. Features: LICENSE_TYPE=BASIC.
01.02.2025 01:51:07	naice1.eltex.loc	INFO	The license NICE4 has been uploaded for naice-ubuntu24_1
01.02.2025 21:04:05	naice1.eltex.loc	WARNING	Application is running in demo mode.


Figure 451. 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 seconds. 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

The screenshot shows the 'Licensing' page in a web interface. The page is titled 'Licensing' and has a search icon. The main content area is divided into several sections:

- About license:** A green badge indicates 'License is active'. Below this is a table of license details:

License type	BASIC
Expire date	05.02.2025
Network devices	Unlimited
Unique endpoints per day	100 ⚠️
Guest endpoints	Unavailable ℹ️
TACACS+	Enabled
- Connected endpoints per day:** A progress bar shows 91 out of 100 endpoints connected.
- Upload:** A form with a 'Hostname' dropdown menu, a file upload area with the text 'Select a file or drag it here', and a checkbox for 'I have read and agree to the End-user license agreement'. An 'Upload' button is at the bottom right.
- Licenses list:** A table with a warning icon:

Hostname	Product ID
naice1.eltex.loc	NICE11111
naice1.eltex.loc	FNICE1111
- Events:** A table with a refresh icon:

Date	Node hostname	Level
01.02.2025 01:52:41	naice1.eltex.loc	DEBUG
02.02.2025 05:02:41	naice1.eltex.loc	INFO
01.02.2025 22:44:17	naice1.eltex.loc	INFO


A warning message is displayed at the bottom left: 'Less than 10% of unique endpoints are available'.

Figure 452. 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

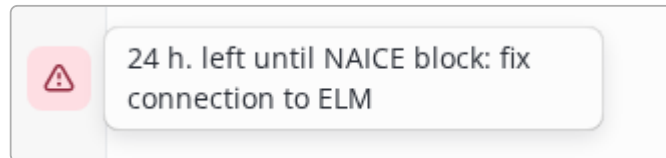


Figure 453. Warning about the unavailability of ELM

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 lower left part of the navigation menu, similar to 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 454. 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 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 reactivate the license according to [Reactivation of the PLR license](#).

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.
2. Send 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.

3. Get a new license file.
4. Upload the license file 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.

Account settings

Description


On this page, you can view/edit credentials of the current system user (under whose account you logged in), as well as change the interface language.

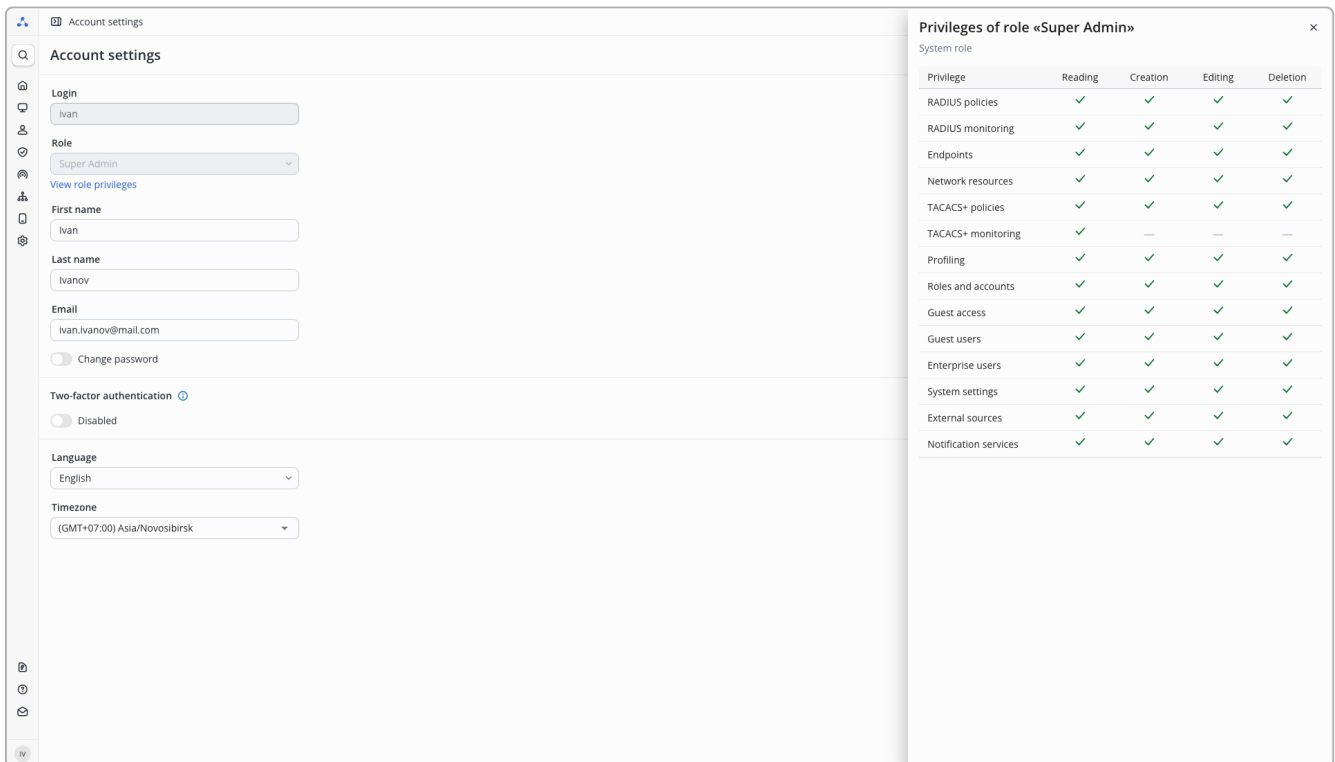


If you logged in as an external system user, only the **Language** and **Timezone** fields will be available for editing.

Setting the timezone affects the displayed time of the last endpoint activity when monitoring connections, the time indicated in the name of the exported file, and the time in the widgets on the dashboard.

Viewing/Editing System User Credentials

The account settings of the current system user are available on any page by clicking on  in the lower left corner of the menu.



The screenshot shows the 'Account settings' page for a user named 'Ivan'. The user's role is 'Super Admin'. The page includes fields for Login, Role, First name, Last name, and Email. There is also a 'Change password' toggle and a 'Two-factor authentication' section which is currently disabled. The 'Language' is set to 'English' and the 'Timezone' is '(GMT+07:00) Asia/Novosibirsk'. On the right side, there is a table titled 'Privileges of role «Super Admin»' showing the permissions for the 'Super Admin' role.

Privilege	Reading	Creation	Editing	Deletion
RADIUS policies	✓	✓	✓	✓
RADIUS monitoring	✓	✓	✓	✓
Endpoints	✓	✓	✓	✓
Network resources	✓	✓	✓	✓
TACACS+ policies	✓	✓	✓	✓
TACACS+ monitoring	✓	—	—	—
Profiling	✓	✓	✓	✓
Roles and accounts	✓	✓	✓	✓
Guest access	✓	✓	✓	✓
Guest users	✓	✓	✓	✓
Enterprise users	✓	✓	✓	✓
System settings	✓	✓	✓	✓
External sources	✓	✓	✓	✓
Notification services	✓	✓	✓	✓

Figure 455. Setting up the account of the current system user

The system user account editing form includes the following fields:

- **Login** — The login of the current system user;
- **Role** — The level of access to the system functionality, which determines the system user's rights;
- **First name** — The system user's personal name (maximum length - 100 characters);
- **Last name** — Last name of the system user (maximum length - 100 characters);
- **Email** — Email address (maximum length - 200 characters);

Language — The language of the system interface (Russian and English are supported);


- Timezone — The time zone for displaying the time in the system.

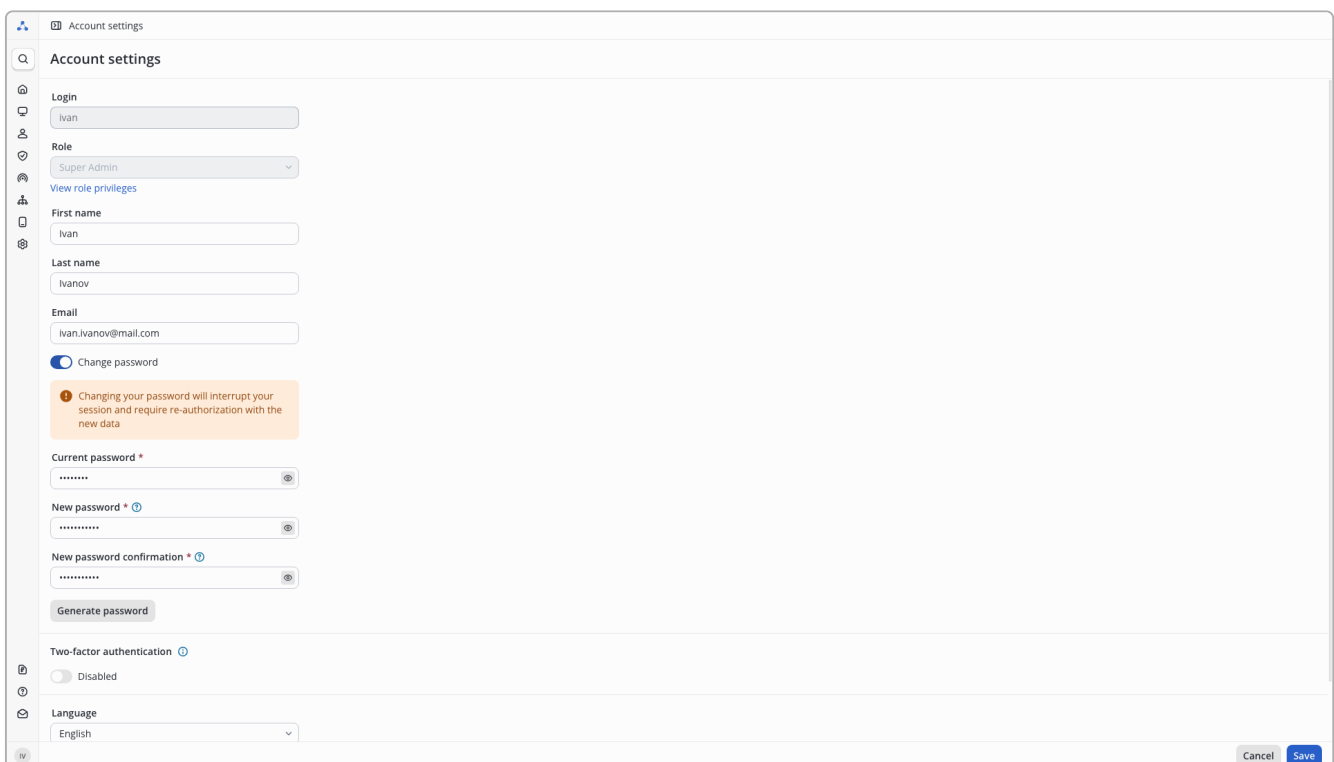
Using the "View role privileges" button, you can open a window with a table of privileges and the rights levels assigned to them for the selected role.

The table for viewing privileges and levels of rights includes:

- Privilege — the name of the privilege;
- Reading, Creation, Editing, Deletion — access levels;
- Statuses of granted rights:
 - ✓ - the user has access,
 - — - access is not provided,
 - ✗ - the user does not have access.

To change the password of the current system user, turn on the switch "Change password", and then enter the current and desired password in the appropriate fields. The password must match the current password policy.

- Current password * — the password under which the current login was performed;
- New password * (maximum length - 72 characters). By clicking on , you can enable the display of the entered password, hidden by default;
- New password confirmation * (maximum length - 72 characters).



The screenshot shows the 'Account settings' interface. The 'Change password' section is active, with a warning message: 'Changing your password will interrupt your session and require re-authorization with the new data'. The 'Current password *' field is filled with dots. The 'New password *' and 'New password confirmation *' fields are also filled with dots. A 'Generate password' button is visible below the password fields. The 'Two-factor authentication' section is disabled. The 'Language' dropdown is set to 'English'. 'Cancel' and 'Save' buttons are at the bottom right.

Figure 456. Changing the password for the current system user



After saving the changes **for the password**, the session will be interrupted and re-login will be required.

After making the changes, click on the **"Save"** button. The button is hidden until at least one field is changed.

After saving the form, you will be returned to the page from which you went to your Account Settings.

The **"Cancel"** button resets the changes made.

Changing the current system user (logout)

To log out on any page, click on the profile icon  in the lower left corner and select **"Logout"**.

Next, you need to confirm the logout by clicking on the **"Logout"** button.