Myra DataHub

User Manual (Versatel)

Version History

Version	Date	Reason for Change
V1.16	08/2026	Updated sections • Networks view • Anomaly history view • Notifications tab • Login
V1.15	08/2026	Updated sections • New sections • Minor corrections Updated sections: • Networks view • Start manual mitigations • Stop manual mitigations • Add account • Change account • Delete account • API tokens tab • Close active web browser sessions • Overview of the Myra DataHub portal • Dashboard view New sections: • Anomaly history view • Notifications tab • Listing all anomalies of the organisation • Changing the notification preference of the authenticated user • Adding a notification address to the organisation • Deleting a notification address from the organisation • Manual as PDF Minor corrections
V1.14	07/2026	Minor corrections
V1.13	06/2026	New sections

Version	Date	Reason for Change
		• API tokens tab
V1.12	06/2026	Updated sections • Network view • Add Network • Edit network • View network
V1.11	04/2026	Minor corrections
V1.10	03/2026	Minor corrections
V1.9	03/2026	Updated sections due to a new **Details** description field • View network • Add Network
V1.8	02/2026	Minor corrections
V1.7	12/2025	New sections • SIEM Settings tab
V1.6	11/2025	New layout
V1.5	09/2025	Updated sections for SIEM • Add Company • Edit company
V1.4	08/2025	Updated sections • Monthly Mitigation Report
V1.3	07/2025	Minor corrections
V1.2	05/2025	Updated sections • New sections Updated sections: • Overview of the Myra DataHub portal • View Business Management New sections: • Add Company

Version	Date	Reason for Change
		• Edit company • Delete company • Add Network • Edit network • Delete network • Report view • Audit log view • View changelog
V1.1	04/2025	Minor corrections
V1.0	03/2025	Initial release

Contents

1. Myra DataHub

1.1 Description

1.1.1 What is the Myra DataHub?

The Myra DataHub is a web-based user interface that provides you with an overview of connected networks, traffic history, and mitigations.

The traffic history contains a presentation of the bandwidth and the packet rate, sorted by destination IP, an overview of source countries, ASN, and packet rates by port. This information can be displayed for various observation periods of up to 24 hours. In addition, you can use the user interface to add and edit new users and to start or stop mitigations manually.

1.1.2 Target Group

The manual is intended for users who want to use the Myra DataHub and its functions as normal users or as admins.

1.2 Getting Started

1.2.1 Activating Your Account

Before you can log in to the Myra DataHub, an admin must create an account for you in the Myra DataHub. Once your new account has been created, you will receive an invitation email.

> Please note that this email is sent from the address **noc@myrasecurity.com**.

Proceed as follows to enable the account:

- Open the invitation email.

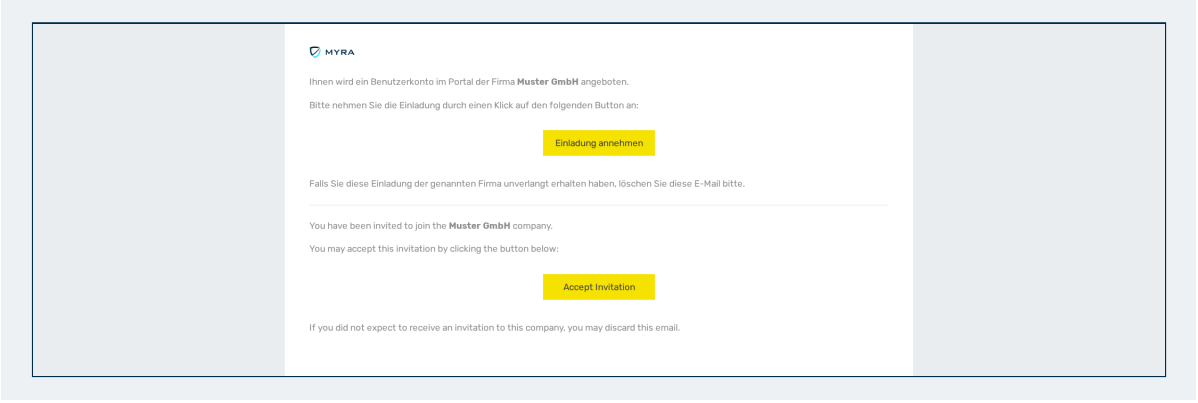


Figure 1: Invitation email

- Click on the **Activate Account** button in the invitation email.
  - ↳ The website of the Myra DataHub opens.

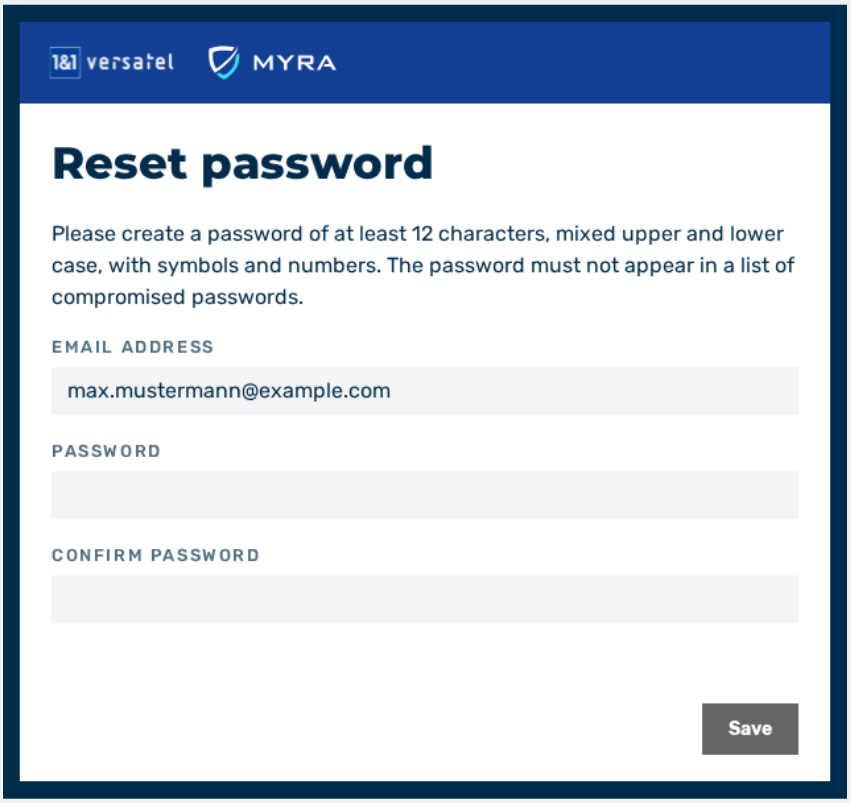


Figure 2: Dialog for changing the password

- ▶ Enter your new password.

> The password must be at least 12 characters long and contain at least one uppercase letter, one number, and one special character.

- ▶ Confirm your new password.
- ▶ Click on the **Save** button.
- ➔ Your new account is now activated.

1.2.2 Registration

Proceed as follows to log in with your credentials:

- ► Open the website.
- ► Enter the following information in the login form:
  - **Email address**
  - **Password**

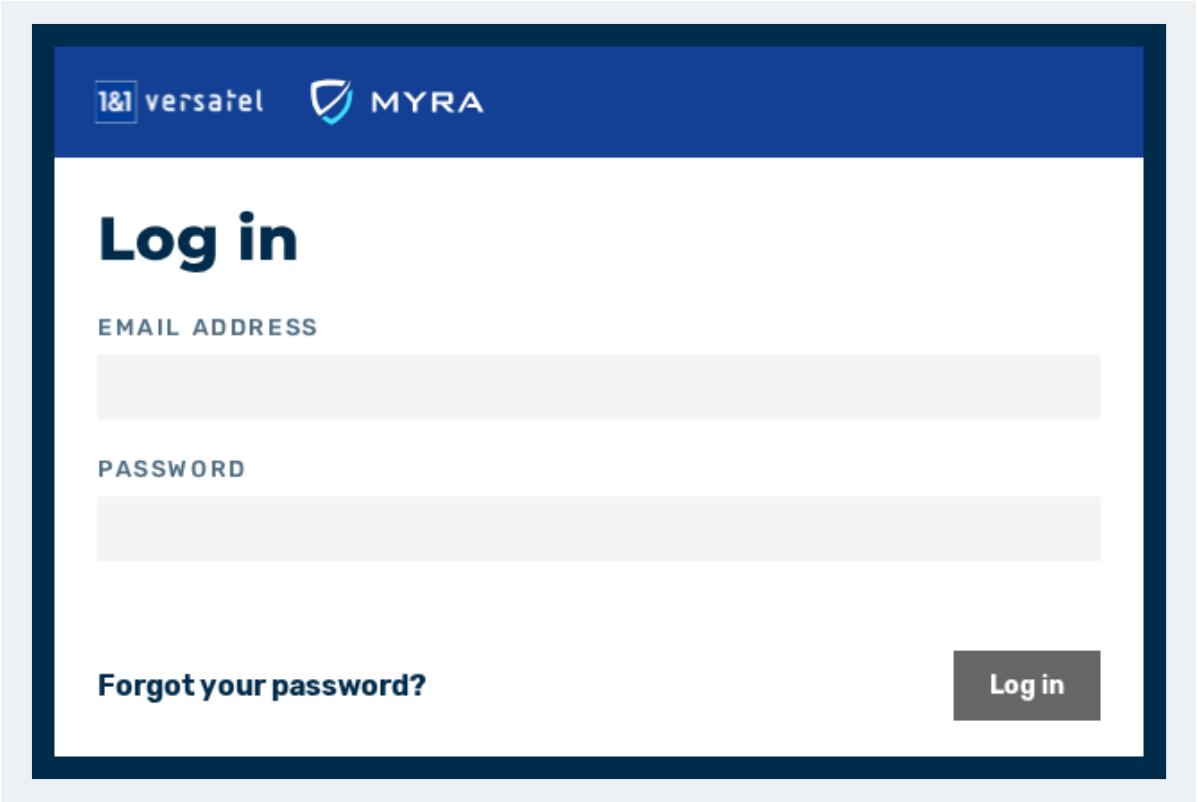


Figure 3: Log in dialog

- ► Click on the **Log in** button.

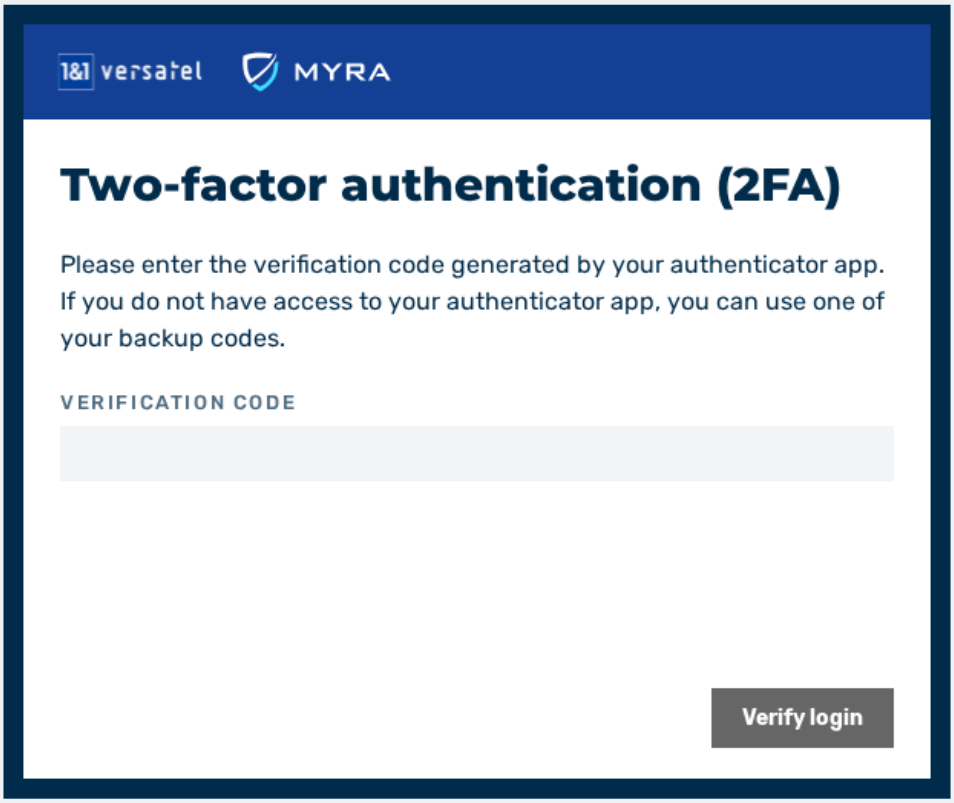


Figure 4: Two-factor authentication (2FA) dialog - Login

- ▶ Enter your 2FA code.
- ▶ Click on the **Verify login** button.
- ➔ The **Company accounts** home page opens.

Two-factor authentication (2FA) is only available if it has been previously enabled in the account. For more information, see **Enabling Two-Factor Authentication**.

1.3 DataHub portal

1.3.1 Overview of the Myra DataHub portal

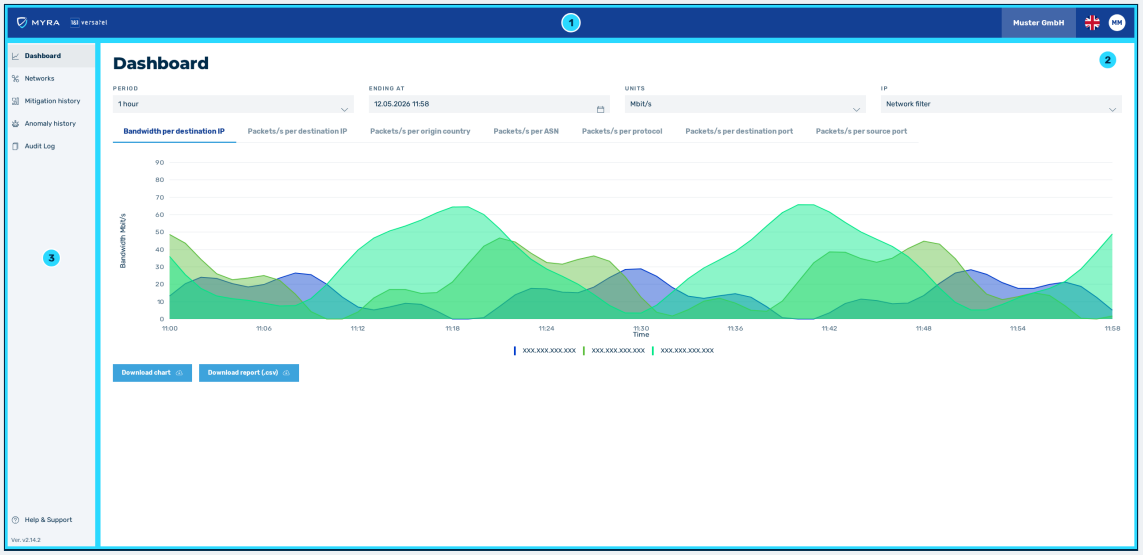


Figure 5: Overview Home

After logging in, the **Dashboard** home page of the Myra DataHub appears.

On the home page, you can find the following information:

- Top menu bar with access to the following buttons (1):
  - Button with the company name for accessing user management
  - Button with flag icon for selecting the user interface language
  - Button with user profile picture for managing your own account settings
  - In the event of maintenance, important information about the type and duration will be shown here as a separate banner.
- Shows the content of the individual views (2)

- Tabs with the following views (3):
  -  Dashboard
  -  Networks
  -  Mitigation history
  - Anomaly history
  -  Audit Log
  - Help & Support for opening the online help
  - Shows the current version number

1.3.2 Company management

1.3.2.1 Dashboard view

Figure 6: Dashboard view

The **Dashboard** view of the respective company provides you with access to various traffic diagrams that give you information about the company's networks.

The following diagrams are available in the **Dashboard** view:

Element	Description
Bandwidth per destination IP	This diagram shows the bandwidth per second for the available destination IPs.
Packets/s per destination IP	This diagram shows how many packets per second were sent to the respective destination IPs.
Packets/s per origin country	This diagram shows the number of packets received per second, grouped by country of origin. The countries of origin of the packets are given with their international country code, for example, DE for Germany or GB for Great Britain.
Packets/s per ASN	This diagram shows how many packets per second were received from a particular source ASN (Autonomous System Number). The legend below the diagram shows the associated names of the ASNs.

Element	Description
Packets/s per protocol	This diagram shows the number of packets received per second, grouped by transmission protocol. The legend below the diagram shows the names of the protocols recorded, for example, ICMP, TCP, UDP.
Packets/s per destination port	This diagram shows the number of packets received per second for the destination port. The numbers of the ports recorded can be found in the legend below the diagrams.
Packets/s per source port	This diagram shows the number of packets received per second for the source port. The numbers of the ports recorded can be found in the legend below the diagrams.
Legend filter	In addition to the filters above the diagrams, there are diagram-specific filters that can be set using the values in the legend. The following filters are available: **IP** : Bandwidth per destination IP and Packets/s per destination IP **Country of origin**: Packets/s per country of origin **ASN**: Packets/s per ASN **Protocol** : Packets/s per protocol **Port** : Packets/s per destination port and Packets/s per source port

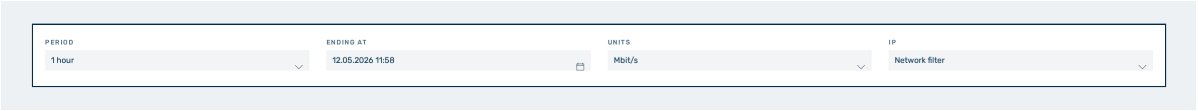


Figure 7: Filters in the dashboard

You can use filters to define the data shown:

Element	Description
Period	shows the data per second for the selected time intervals: 1 hour: shows the data per second for the selected hour. (default value) 2 hours: shows the data per second for the selected 2 hours. 3 hours: shows the data per second for the selected 3 hours. 4 hours: shows the data per second for the selected 4 hours. 6 hours: shows the data per second for the selected 6 hours.

Element	Description
	12 hours: shows the data for the selected 12 hours aggregated in 10-second groups. 24 hours: shows the data for the selected 24 hours aggregated in 10-second groups. 7 days (only available for individual IP addresses): shows the data for the selected 7 days aggregated in groups of one hour.
Ending at	Defines the time period during which the data should be shown according to the time interval defined at **Period**. To change the date, select a date and time using the icon  . ★ If you select **1 hour** as the period and **01.08.2024 12:00** as the end time, the data for the period from 01.08.2024 11:00 to 01.08.2024 12:00 is shown.
Units	For the **Bandwidth per destination IP** diagram, you can choose between the units **Gbit/s**, **Mbit/s**, **Kbit/s**, and **bit/s**. All other charts use the unit packets/s, which cannot be changed.
IP	Allows you to show data for specific IP addresses or entire networks using the following values: If a specific IP address is specified, the chart shows the data for that IP address. If a subnet mask (for example, /24) is entered, the chart shows the data for the entire network.

You can zoom in on any chart, which will enlarge the selected time period. To do this, select the desired area by holding down the left mouse button.

In addition, two buttons can be used to download the data for each diagram:

- **Download chart**: Downloads the chart as a PNG file.
- **Download report (.csv)**: Downloads the data from the chart as a CSV file.

1.3.2.2 Networks view

> To create and delete a network, as well as view and change settings, please contact your Versatel representative.

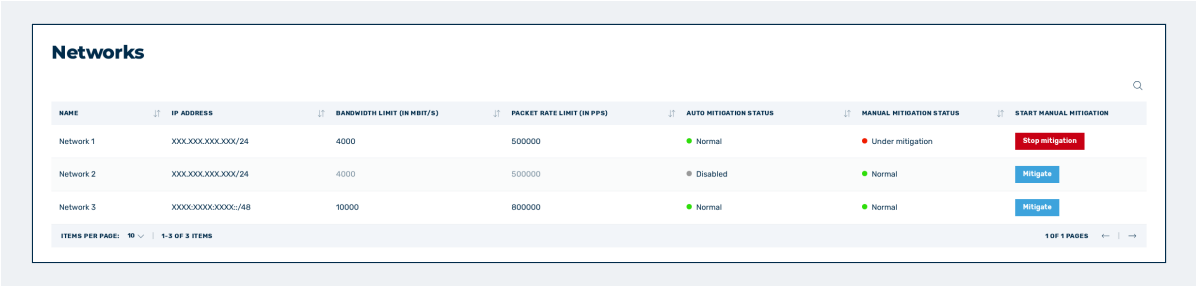


Figure 8: Networks view

The **Networks** view provides an overview of the networks, the IP address ranges of the networks, the configured packet rate limit (in packets/s), the configured bandwidth limit (in MBit/s), and the mitigation status.

The following information is available:

Element	Description
Name	The name of the network.
IP Address	The IP address of the network.
Bandwidth limit (in MBit/s)	The maximum bandwidth allowed for your network. > If the network protection switch under **Auto Actions** is disabled, all values defined prior to deactivation are shown in grey.
Packet rate limit (in PPS)	The maximum number of packets per second allowed on the network. > If the network protection switch under **Auto Actions** is disabled, all values defined prior to deactivation are shown in grey.
Auto mitigation status	Shows the status of mitigation: **Disabled** ⚫: Automatic mitigation is disabled. **Under mitigation** 🔴: Mitigation has been initiated.

Element	Description
	Partially mitigated  : A mitigation is running for only part of the network. ⓘ You can view the currently mitigated IP addresses by moving the mouse pointer over the status indicator. **Normal**  : Mitigation has been completed. ⓘ Automatic mitigations cannot be stopped. If you have any questions about ongoing mitigations, please contact your Versatel representative.
Manual mitigation status	Shows the status of manual mitigation: **Under mitigation**  : A manual mitigation has been initiated. **Partially mitigated**  : A manual mitigation is running for only part of the network. **Normal**  : Manual mitigation has been completed.
START MANUAL MITIGATION	Open the **Mitigate network or IP address(es)** dialog to start mitigation for the selected network.

In addition, you have the following management and configuration options available:

Element	Description
	The icon enables you to search specifically for names, IP addresses, bandwidth, and packet rates.
	The icon allows you to sort individual columns.
	The mitigation icon next to the **Networks** view in the left navigation bar indicates whether at least one mitigation is running.

1.3.2.2.1 Start manual mitigations

Mitigations are possible for the entire network or for individual or multiple IP-addresses.

You need administrator rights to start or stop manual mitigation.

You can only start a manual mitigation if the SOC admin has enabled it for the network.

If you suspect that a company has been targeted by an attack, you can initiate manual mitigation at any time.

Proceed as follows to start a manual mitigation:

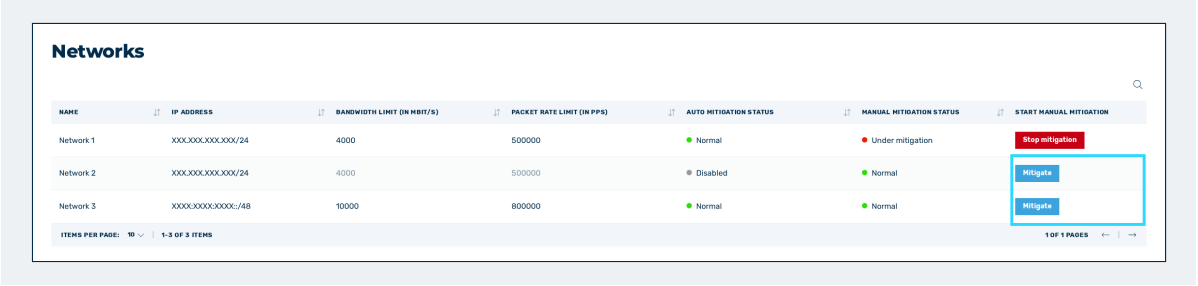


Figure 9: Buttons for initiating mitigation

- ► Click on the **Mitigate** button.
  - ↳ The **Mitigate network or IP address(es)** dialog opens.

► Depending on the type of network, one of two different views is shown:

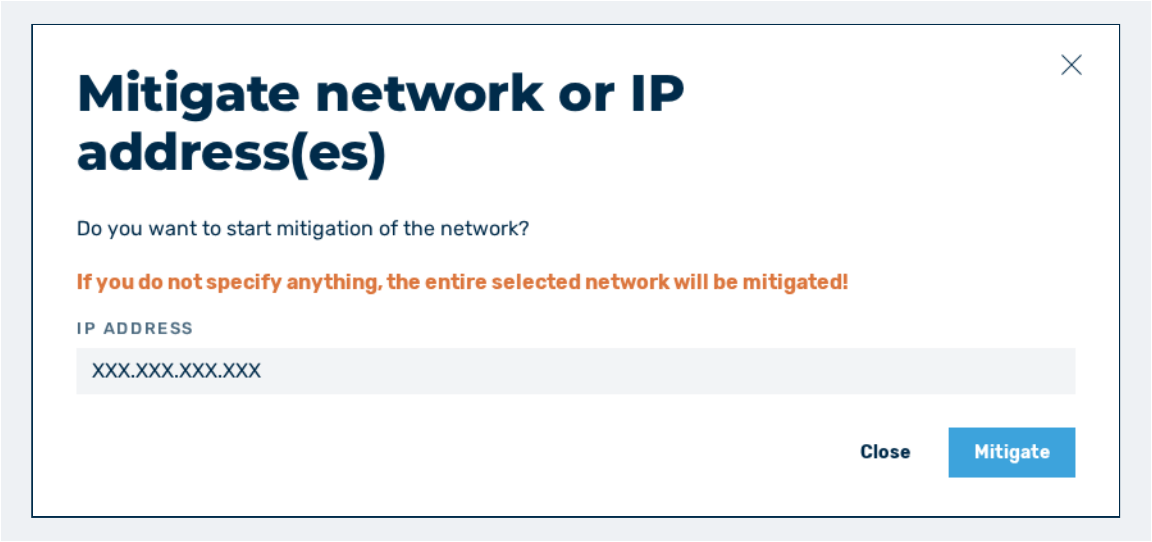


Figure 10: Mitigate network or IP address(es) dialog – variant 1

- For networks with IPv4 /32 and IPv6 /128, only the IP address of the network is displayed.

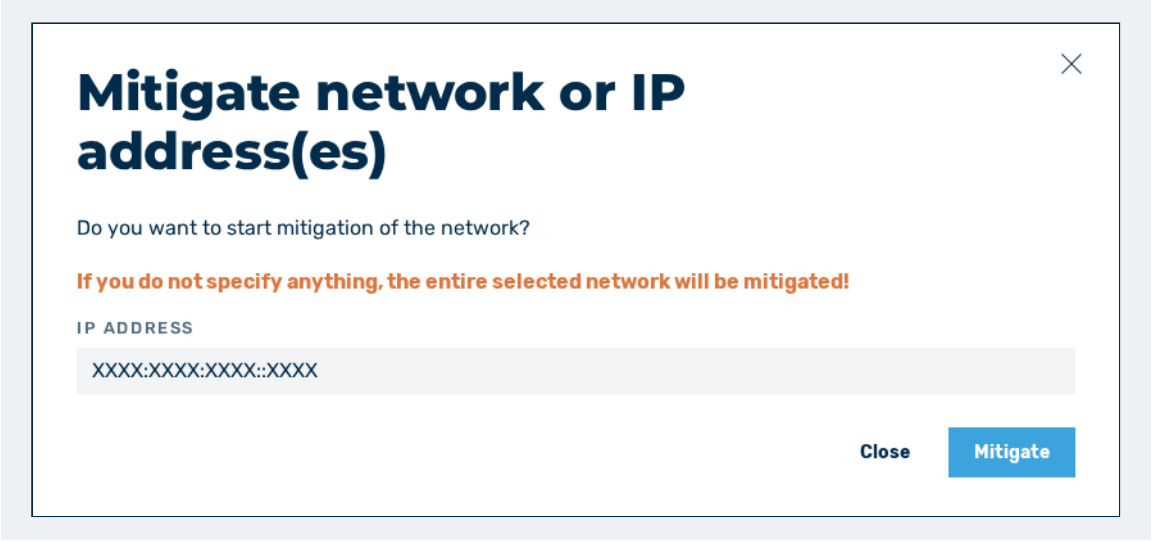


Figure 11: Mitigate network or IP address(es) dialog – variant 2

- For all other networks, you can enter a specific IP address in the right-hand field to run the mitigation for that IP address only. Use the ┼ icon to add further specific IP addresses.

  If you leave the field blank, mitigation will be initiated for the entire network.

> When you enter a specific IP address, the system automatically checks whether this IP address also belongs to the selected network.

► Click on the **Mitigate** button.

➔ A message confirms that mitigation has started successfully.

Next to the **Networks** view in the left navigation bar, the mitigation icon is visible, and in the **Manual mitigation status** column, the status changes to one of the following values:

- **Under mitigation**: Manual mitigation has been initiated for the entire network.
- **Partially mitigated**: The manual mitigation was started for part of the network only.

> Once you have started mitigation for a specific IP address, you can repeat the process for other IP addresses at any time.
>
> To do so, click on the **Additional Mitigation** button to open the dialog for the manual mitigation again.

> After a mitigation has been started successfully, the buttons in the **START MANUAL MITIGATION** column change:
>
> - When a mitigation is started for an entire network: the **Stop mitigation** button appears instead of the **Mitigate** button.
> - When a mitigation is started for a specific IP address: an additional **(X) Stop mitigation(s)** button appears next to the **Mitigate** button. The **X** in brackets indicates the number of IP addresses for which a mitigation has been initiated.

> In the case of manual mitigation, traffic is redirected via the scrubbing center, attacks are mitigated or blocked, and you receive a notification via email.

The mitigation icon next to the **Networks** view in the left navigation bar remains visible for as long as the Myra DataHub is running mitigations. The mitigation icon only disappears once all running mitigations have been stopped.

1.3.2.2.2 Stop manual mitigations

You need administrator rights to start or stop manual mitigation.

Proceed as follows to stop a manually started mitigation:

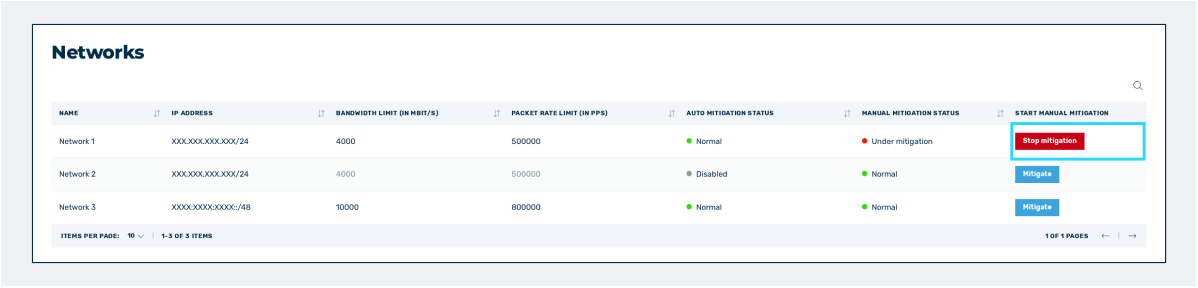


Figure 12: Buttons for ending a mitigation

► Click on the **Stop mitigation** button or the **(X) Stop mitigation(s)** button.

↳ The **Mitigate network or IP address(es)** dialog opens.

► Check which case applies and then proceed as follows:

Figure 13: Dialog for finishing a mitigation - entire network

▷ For the mitigation of an entire network, click on the **Stop mitigation** button.

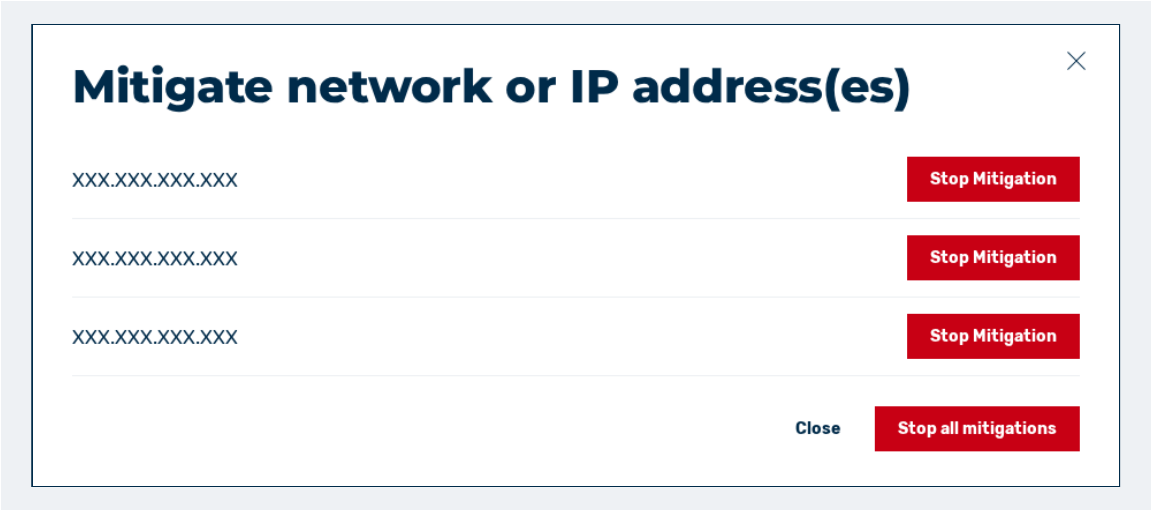


Figure 14: Dialog for finishing a mitigation - individual IP addresses

▷ To stop the mitigation for all IP addresses, click on the **Stop all mitigations** button.

▷ To stop the mitigation for individual IP addresses, click on the **Stop mitigation** button next to the respective entry and then on the **Close** button.

The mitigation icon next to the **Networks** view in the left navigation bar remains visible for as long as the Myra DataHub is running mitigations. The mitigation icon only disappears once all running mitigations have been stopped.

1.3.2.3 Mitigation history view

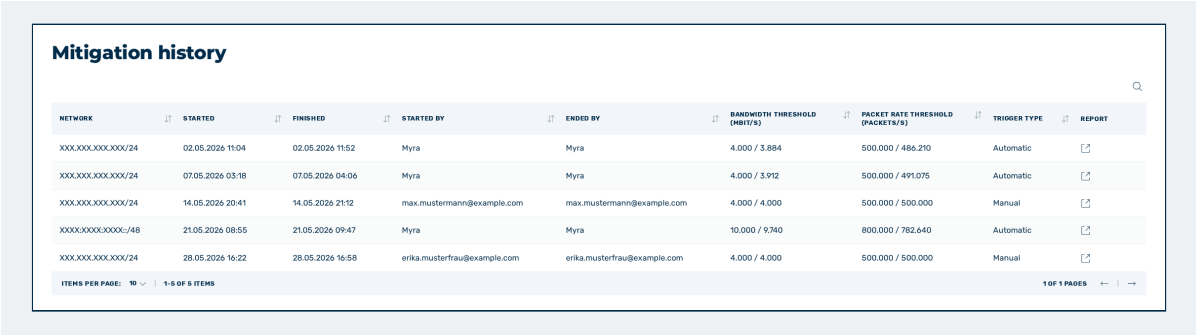


Figure 15: Mitigation history view

In the **Mitigation history** view, you can see an overview of all mitigations that have been triggered automatically or manually. You can retrieve a mitigation report for each completed mitigation.

The following information is available:

Element	Description
Network	The IP address of the network.
Started	The date and time when mitigation was initiated.
Finished	The date and time at which the mitigation was completed.
Started by	Indicates who initiated the manual mitigation.
Ended by	Indicates who stopped the manual mitigation.
Bandwidth Threshold (MBit/s)	Shows the defined bandwidth threshold and threshold exceedance during automatic mitigation.
Packet Rate Threshold (Packets/s)	Shows the defined packet rate threshold and threshold exceedance during automatic mitigation.
Trigger type	Indicates whether mitigation was started manually or automatically.
Report	Enables the mitigation report to be opened in a new window via the icon .

The following options are available:

Element	Description
	The icon enables you to search specifically for names, IP addresses, bandwidth, and packet rates.

1.3.2.3.1 Open mitigation reports

Proceed as follows to open the mitigation report:

- ▶ Click on the icon  in the **Report** column.
- ➔ The **Report - <Report Name> (<Company Name>)** view opens.

1.3.2.3.2 Mitigation reports view

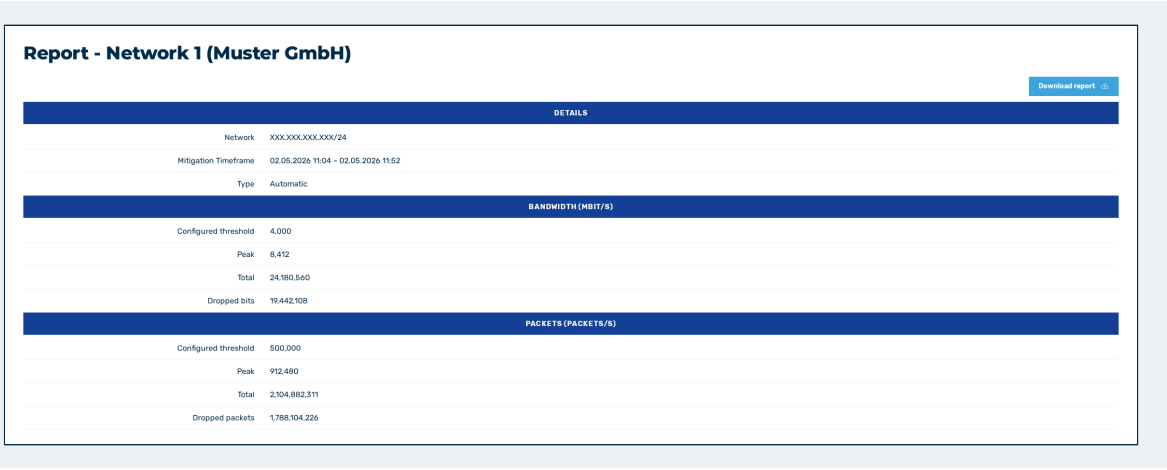


Figure 16: Mitigation reports view

The **Report - <Report Name> (<Company Name>)** view provides an overview of the individual data collected during successful mitigation.

The following information is shown in the **Details** table:

Element	Description
Network	The IP address of the network.
Mitigation Timeframe	Shows the time period during which the mitigation was performed.

Element	Description
Bandwidth - Configured threshold	shows the configured bandwidth threshold at which automatic mitigation is triggered.
Bandwidth - Triggered by	shows the value that triggered automatic mitigation when the bandwidth threshold was exceeded.
Bandwidth - Peak	shows the peak value during mitigation.
Bandwidth – Dropped bits	shows the number of filtered bits.
Packets - Configured threshold	shows the configured packet rate threshold at which automatic mitigation is triggered.
Packets - Triggered by	shows the value that triggered automatic mitigation when the packet rate threshold was exceeded.
Packets - Peak	shows the peak value during mitigation.
Packets – Dropped packets	shows the number of filtered packets.
Type	Indicates whether mitigation was started manually or automatically.

In addition, the mitigation report includes seven charts depicting the following periods:

- Network utilization during the first 24 hours before mitigation began
- Network utilization from the start to the end of mitigation

The following diagrams are available:

Element	Description
Bandwidth per destination IP	This diagram shows the bandwidth per second for the available destination IPs.

Element	Description
Packets/s per destination IP	This diagram shows how many packets per second were sent to the respective destination IPs.
Packets/s per origin country	This diagram shows the number of packets received per second, grouped by country of origin. The countries of origin of the packets are given with their international country code, for example, DE for Germany or GB for Great Britain.
Packets/s per ASN	This diagram shows how many packets per second were received from a particular source ASN (Autonomous System Number). The legend below the diagram shows the associated names of the ASNs.
Packets/s per protocol	This diagram shows the number of packets received per second, grouped by transmission protocol. The legend below the diagram shows the names of the protocols recorded, for example, ICMP, TCP, UDP.
Packets/s per destination port	This diagram shows the number of packets received per second for the destination port. The numbers of the ports recorded can be found in the legend below the diagrams.
Packets/s per source port	This diagram shows the number of packets received per second for the source port. The numbers of the ports recorded can be found in the legend below the diagrams.
Legend filter	In addition to the filters above the diagrams, there are diagram-specific filters that can be set using the values in the legend. The following filters are available: **IP** : Bandwidth per destination IP and Packets/s per destination IP **Country of origin**: Packets/s per country of origin **ASN**: Packets/s per ASN **Protocol** : Packets/s per protocol **Port** : Packets/s per destination port and Packets/s per source port

You can download the reports as PDF files by clicking on the **Download report** button.

1.3.2.4 Anomaly history view

> The **Anomaly history** view appears only if the anomaly feature is enabled for your company.

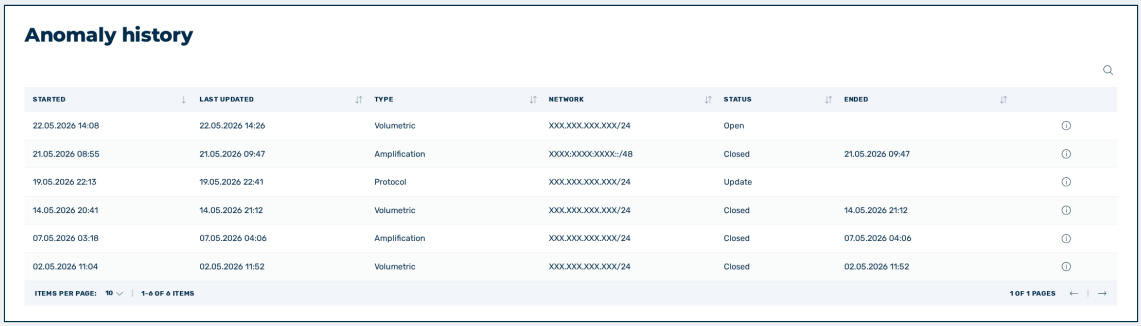


Figure 17: Anomaly history view

In the **Anomaly history** view, you get an overview of all anomalies detected in the traffic of your networks. By default, the entries are sorted in descending order by the start of the anomaly.

The following information is available:

Element	Description
Started	The date and time at which the anomaly was detected.
Last updated	The date and time at which the entry was last updated.
Type	The type of the detected anomaly. The following values are available: **Volumetric**: A traffic flood aimed at saturating your bandwidth or packet capacity by sheer volume, regardless of the protocol used — for example extreme traffic bursts or floods from a large spread of source addresses. **Protocol**: An attack that abuses how a network protocol or connection setup works in order to exhaust connection tables, state, or processing resources rather than bandwidth — for example SYN floods or other anomalous TCP or UDP traffic.

Element	Description
	Amplification: An attack in which third-party servers on the internet are tricked into sending large responses to your address on behalf of a spoofed sender, so a small request turns into a much larger flood — for example DNS reflection. The view can show several types at the same time for one anomaly.
Network	The network in CIDR notation in which the anomaly was detected.
Status	The current status of the anomaly. The following values are available: **Open**: Myra detected the anomaly and the anomaly continues. **Update**: New information about the anomaly is available. **Closed**: The anomaly has ended.
Ended	The date and time at which the anomaly ended.

The following options are available:

Element	Description
	The **View details** icon opens the **Anomaly details** dialog for the selected entry.
	The icon allows you to search by type, network, and status.

If there are no anomalies, the view displays the text **No anomalies found.**

1.3.2.4.1 Anomaly details dialog

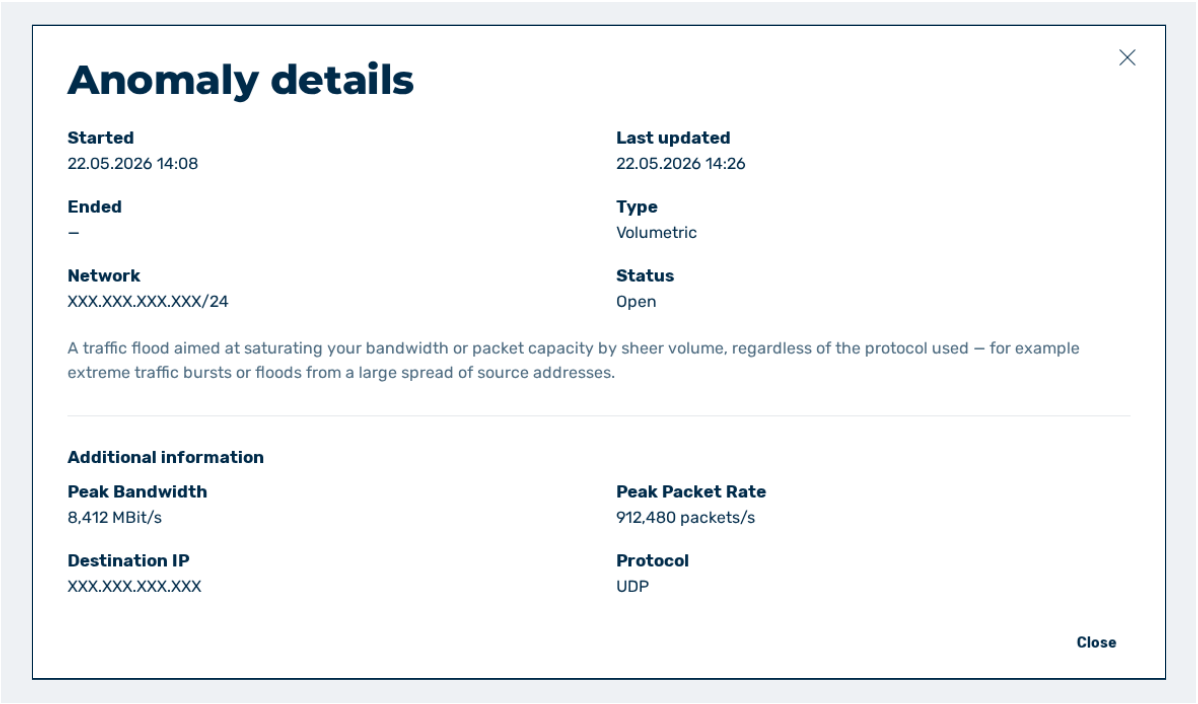


Figure 18: Anomaly details dialog

In the **Anomaly details** dialog, you can view the following information about an anomaly:

Element	Description
Network	The network in CIDR notation in which the anomaly was detected.
Type	The type of the detected anomaly.
Status	The current status of the anomaly.
Started	The date and time at which the anomaly was detected.
Last updated	The date and time at which the entry was last updated.
Ended	The date and time at which the anomaly ended.
Additional information	Further details about the anomaly provided by the detection. ⓘ If no further details are available, the area displays the text **No additional information available.**

1.3.2.5 Audit log view

You need administrator rights to view the audit log.

Figure 19: Audit log view

In the **Audit Log** view, you can find detailed information about all changes made for your own company.

The following information is available:

Element	Description
Created	The time and date when the change was made.
Performed by	The name of the user.
Event	The type of the activity. **CREATED** : A new entry has been created. **UPDATED** : An existing entry has been modified. **DELETED** : An existing entry has been deleted.
Resource	The place of change.
Resource ID	The entry that has been changed.
Parameters	The values of the corresponding entry that have been changed.

The following options are available:

Element	Description
	The symbol filters the reports by names.
Download CSV	The button downloads the complete monthly report as a CSV file.

1.3.3 Company management

If you want to view, add, change, or delete users for your company, proceed as follows:

- ► Open the Myra DataHub.
- ► Log in.
  - ↳ The **Dashboard** home page opens.

Figure 20: Opening user management – Option 1

- ► Click on the company name in the top right corner.
- ➔ The **Company management** view opens.

1.3.3.1 Company management view

In the **Company management** view, you can view, manage, and delete users. You can also customise the SIEM settings for the company and manage the recipients of the notifications.

The view contains the following tabs:

- User management
- SIEM Settings
- Notifications

1.3.3.2 User management tab

1.3.3.2.1 Add account

> You need admin rights to add, edit, or delete an account.

Proceed as follows to add a new account:

- ► Navigate to the **Add company member** area.

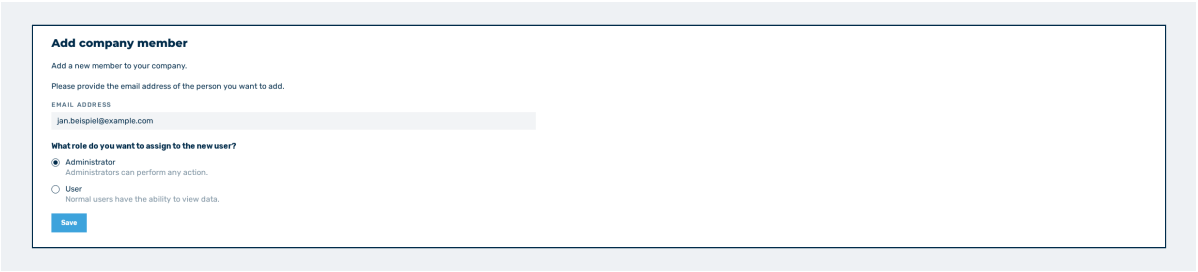


Figure 21: Add company member area

► Under **Email address**, enter the email address of the new user.

> When adding a new user, the name before the @ symbol is stored in the system as the name of the user.
>
> The name can be changed later by users with the **Administrator** role (see **Change account**) or by the users themselves (see **Change username**).

► Under **What role do you want to assign to the new user?**, select the corresponding permission group.

You have two permission groups to choose from:

↳ **Administrator**: Users with the role **Administrator** may use every portal function.

↳ **User**: Users with the role **User** are restricted and may only view data.

► Click on the **Save** button.

➔ A message confirms that the user has been successfully created. The new entry is also visible in the list of accounts.

New users receive an invitation email with an activation link.

1.3.3.2.2 Change account

> You need admin rights to add, edit, or delete an account.

Proceed as follows to change an account:

► Navigate to the **List of User accounts** area.

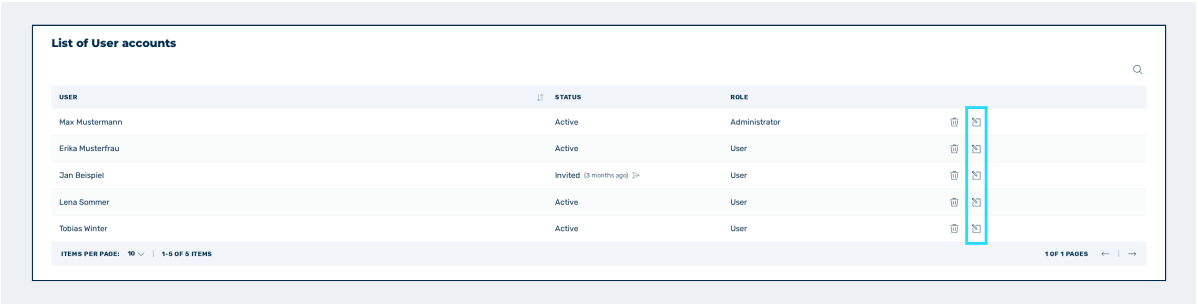


Figure 22: List of user accounts area

- ▶ Click on the icon next to the relevant account.
  - ↳ The **Update company member** dialog opens.

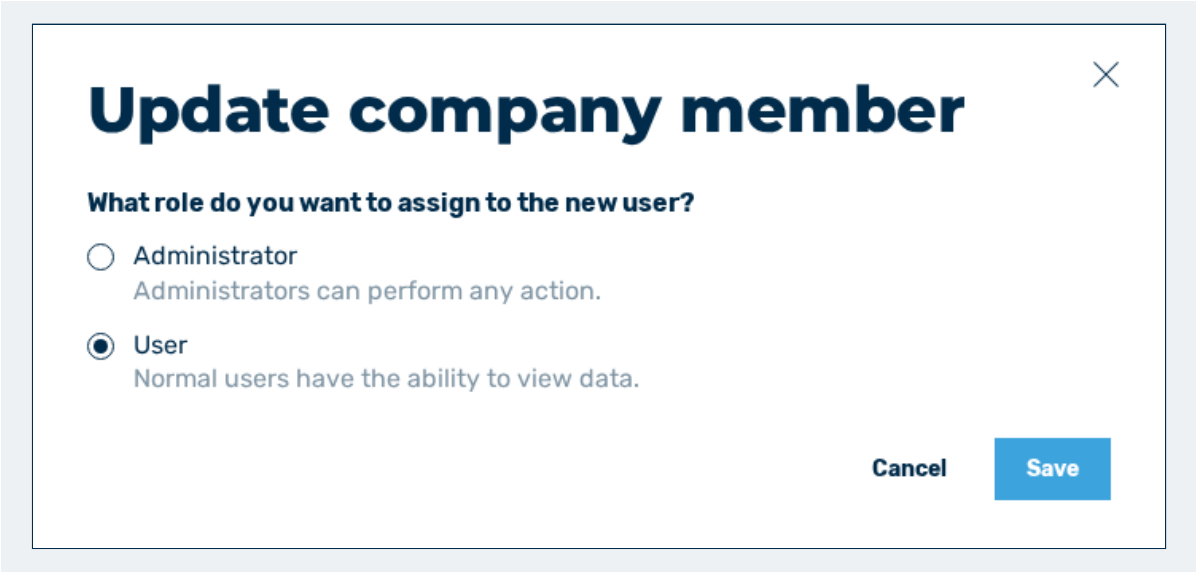


Figure 23: Update company member dialog

- ▶ If necessary, change the name of the user under **Name**.
- ▶ If necessary, change the user's authorization under Role.

  You have two permission groups to choose from:
  - ↳ **Administrator**: Users with the role **Administrator** may use every portal function.
  - ↳ **User**: Users with the role **User** are restricted and may only view data.
- ▶ Click on the **Save** button.
- ➔ A message confirms that the account has been successfully changed.

1.3.3.2.3 Delete account

Deleting an account is permanent, and deleted accounts cannot be restored. To add a deleted account again, you must create it anew.

You need admin rights to add, edit, or delete an account.

Proceed as follows to delete an account:

► Navigate to the **List of User accounts** area.

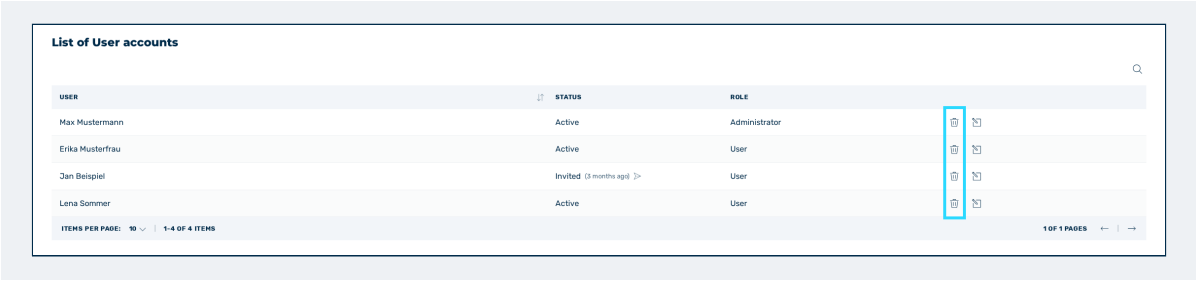


Figure 24: List of user accounts area

► In the **Delete** column, click on the icon.

↳ The **Remove company member** dialog opens.

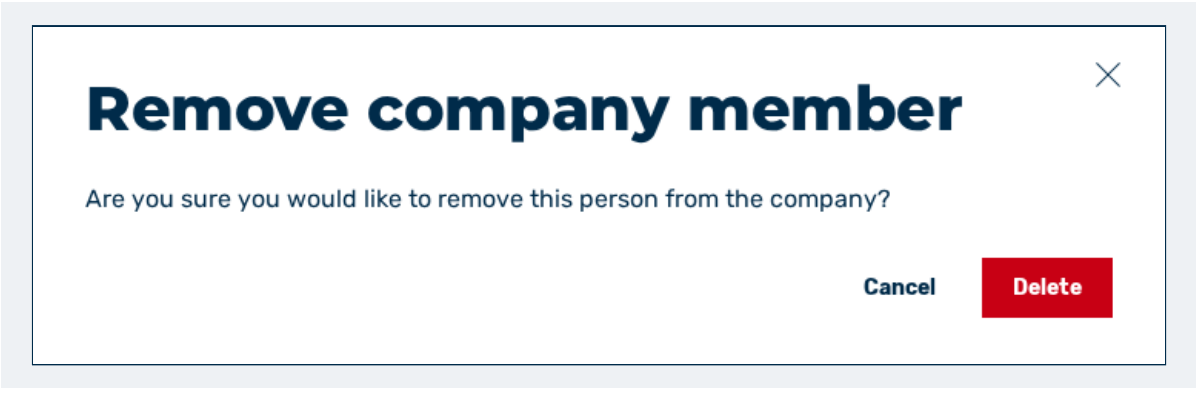


Figure 25: Remove company member dialog

► Click on the **Delete** button.

➔ A message confirms that the account has been deleted. The entry is no longer visible in the list of accounts.

1.3.3.3 SIEM Settings tab

> To view the SIEM Settings tab, the option to use SIEM must be enabled in the organization settings.
>
> If you want to use SIEM, please contact your service partner.

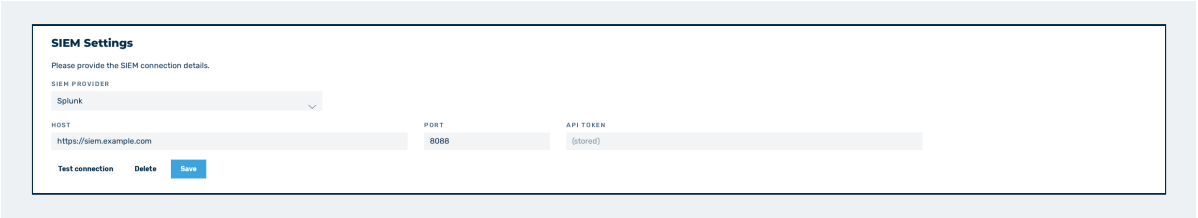


Figure 26: SIEM Settings tab

In the **SIEM Settings** tab, you will find an overview of all the information and settings available to you for managing a company's users.

The following options are available:

Element	Description
SIEM provider	Defines the SIEM provider. Currently, only Splunk is supported as an HTTP Event Collector (HEC).
Host	Defines the name of the host for data transfer.
Port	Defines the port of a host for the connection used to transfer data.
API tokens	Defines the API token for authentication with the host. The API token used must be a HEX token.

The following information is shown in the SIEM log when SIEM is activated:

Data recorded in the SIEM log

Function	Event
Mitigation	Automatic mitigation started
	Automatic mitigation completed

Function	Event
	Start Manual mitigation
	Stop manual mitigation
User management	Add account
	Delete account
	Verify email
	Reset password
	Enable and disable 2FA

1.3.3.4 Notifications tab

> To open the **Notifications** tab, you need administration rights for the company.

In the **Notifications** tab, you can see which users of the company receive email notifications about anomalies and mitigations. You can also add additional recipients that are not users of the application.

The tab is divided into the following areas:

1.3.3.4.1 Notifications area

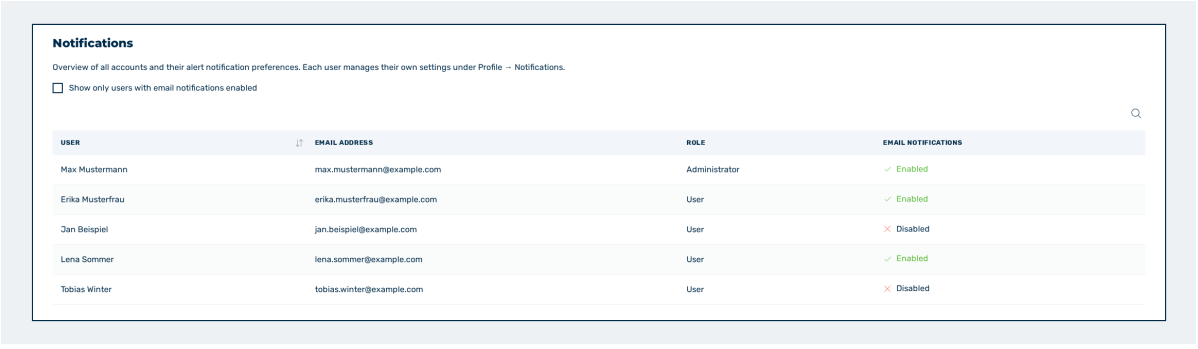


Figure 27: Notifications area

The **Notifications** area contains an overview of all accounts and their alert notification preferences. Each user manages their own settings under **Profile** → **Notifications** (see Notifications tab).

The following information is available:

Element	Description
User	The name of the user.
Email address	The email address of the user.
Role	The role of the user in the company.
Email notifications	Indicates whether the user receives email notifications. The following values are available: **Enabled**: The user receives email notifications. **Disabled**: The user does not receive email notifications.

The following options are available:

Element	Description
Show only users with email notifications enabled	The checkbox hides all users without email notifications enabled.

If the checkbox is selected, a badge next to it shows the number of users with email notifications enabled. If no user matches the selected filter, the area displays the text **No users match the current filter.**

1.3.3.4.2 Additional contacts area

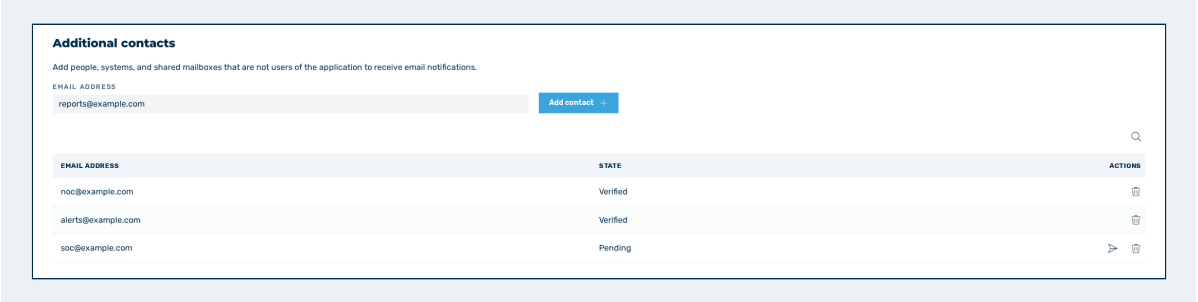


Figure 28: Additional contacts area

In the **Additional contacts** area, you add people, systems, and shared mailboxes that are not users of the application to receive email notifications.

Proceed as follows to add an additional contact:

- ▶ Enter the email address of the contact in the field under **Email address**.
- ▶ Click on the **Add contact** button.
- → The contact is added to the list and a verification email is sent. The contact remains in the **Pending** state until it is confirmed.

The following information is available:

Element	Description
Email address	The email address of the contact.
State	The state of the contact. The following values are available: **Verified**: The contact has confirmed the verification email and receives notifications. **Pending**: The contact has not confirmed the verification email yet.
Actions	The available actions for the contact.

The following options are available:

Element	Description
Resend verification email	The icon sends a new verification email to the contact. ⓘ The icon is only displayed for contacts in the **Pending** state.
Remove contact	The icon opens the **Remove contact** dialog for deleting the selected contact.

ⓘ If no additional contacts have been added yet, the area displays the text **No additional contacts yet.**

1.3.4 Profile

Proceed as follows to view or change your profile information:

- ▶ Open the Myra DataHub.
- ▶ Log in.
  - ↳ The Myra DataHub home page with the company accounts opens.
- ▶ Click on the button with your profile picture in the top right corner.

Figure 29: Options under the profile picture

- ▶ In the menu, click on the **Profile** menu item.
- ➔ The **Profile** view opens.

The **Profile** view has the following tabs:

- Profile
- Notifications
- API tokens

1.3.4.1 Profile tab

In the **Profile** tab, you will find an overview of all the information and settings you can configure for your account.

The view is divided into four areas:

- **Profile information**: Information about view names and email addresses
- **Change password**: settings for setting a new password
- **Two-factor authentication (2FA)**: setting for configuring two-factor authentication
- **Browser sessions**: Overview of all user sessions

1.3.4.1.1 Change username

In the **Profile information** area of the **Profile** view, you can change the name shown in the application.

Figure 30: Personal account area

Proceed as follows to change the name:

- ▶ In the **Name** text field, replace the entered name with the new name.
- ▶ Click on the **Save** button.
- ➔ A message confirms that the name has been successfully changed.

1.3.4.1.2 Change password

In the **Change password** area of the **Profile** view, you can change your password.

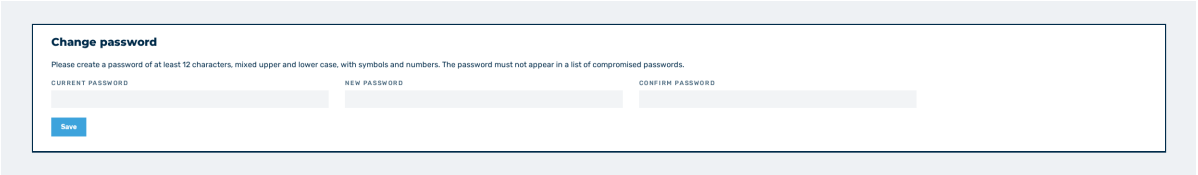


Figure 31: Change password area

Proceed as follows to change your password:

- ▶ Enter the current password in the **Current password** text field.
- ▶ Enter the new password in the **New password** text field.
- ▶ Enter the new password again in the **Confirm password** text field.
- ▶ Click on the **Save** button.
- ➔ A message confirms that the password has been successfully updated.

1.3.4.1.3 Enabling Two-Factor Authentication

On your first login to the Myra DataHub, two-factor authentication is still disabled and must be enabled manually.

In the **Two-factor authentication (2FA)** area in the **Profile** view, you can manage two-factor authentication for your account.

Proceed as follows to enable the two factor authentication:

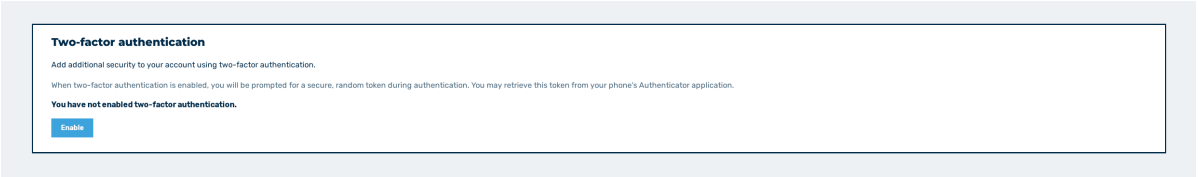


Figure 32: Two-factor authentication (2FA) area

- Click on the **Enable** button.
  - ↳ The **Confirm password** dialog opens.

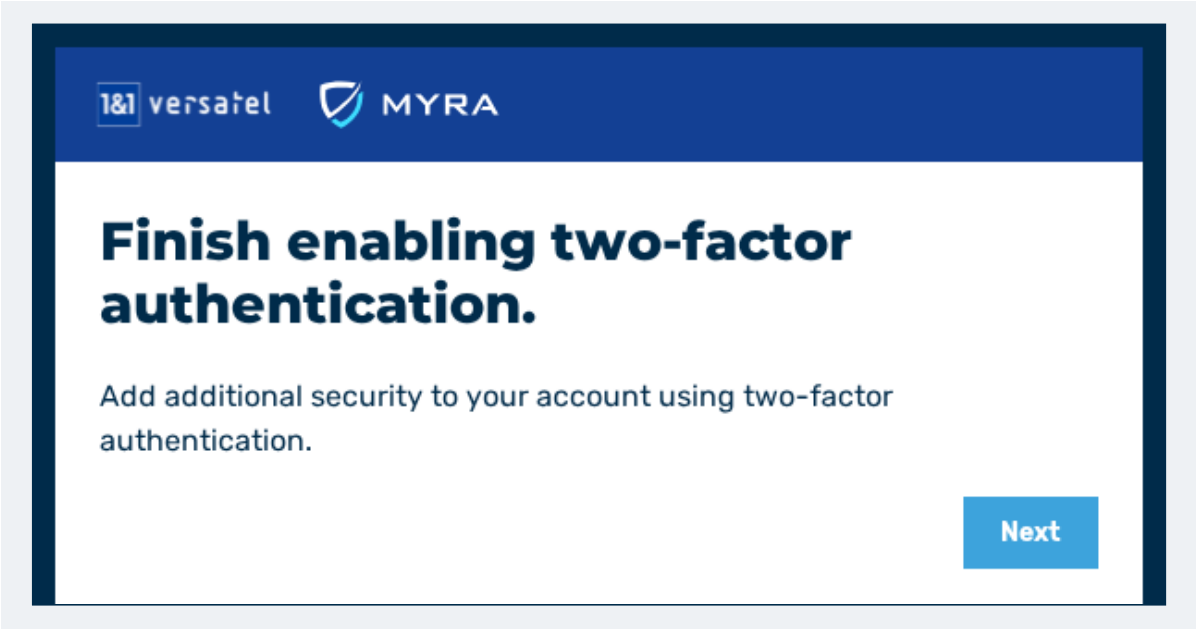


Figure 33: Confirm new password dialog

- Enter your current password in the field under **Password**.
- Click on the **OK** button.
  - ↳ The **Finish enabling two-factor authentication.** dialog with a QR code opens.

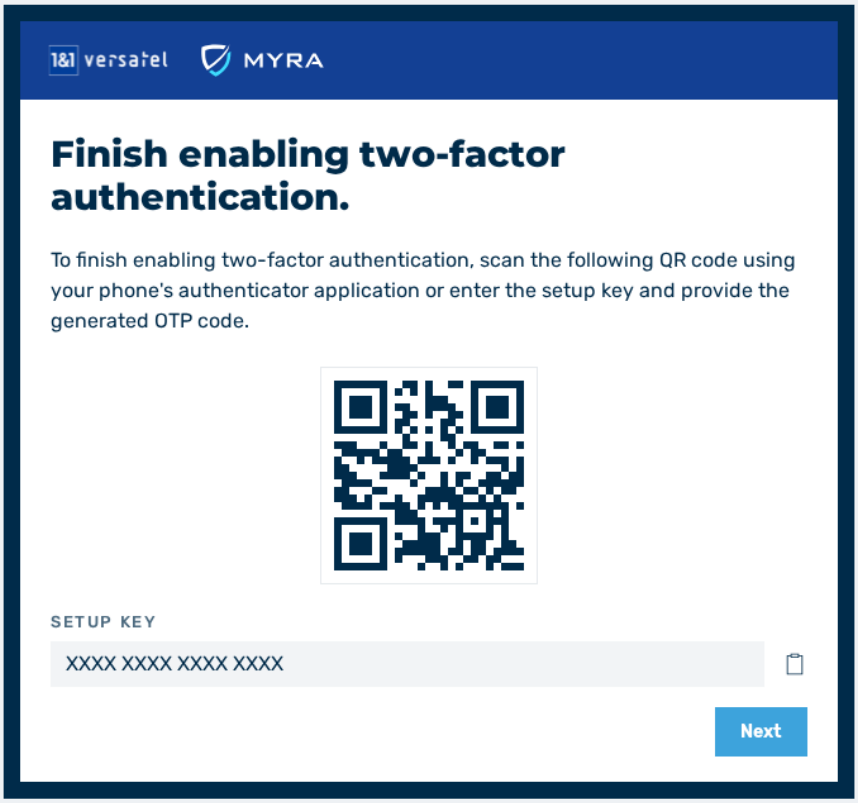


Figure 34: Complete the dialog for activating two-factor authentication.

- Scan the QR code with a TOTP-capable device or program (for example, an authenticator app). Alternatively, you can also use the setup key.
- Click on the **Next** button.

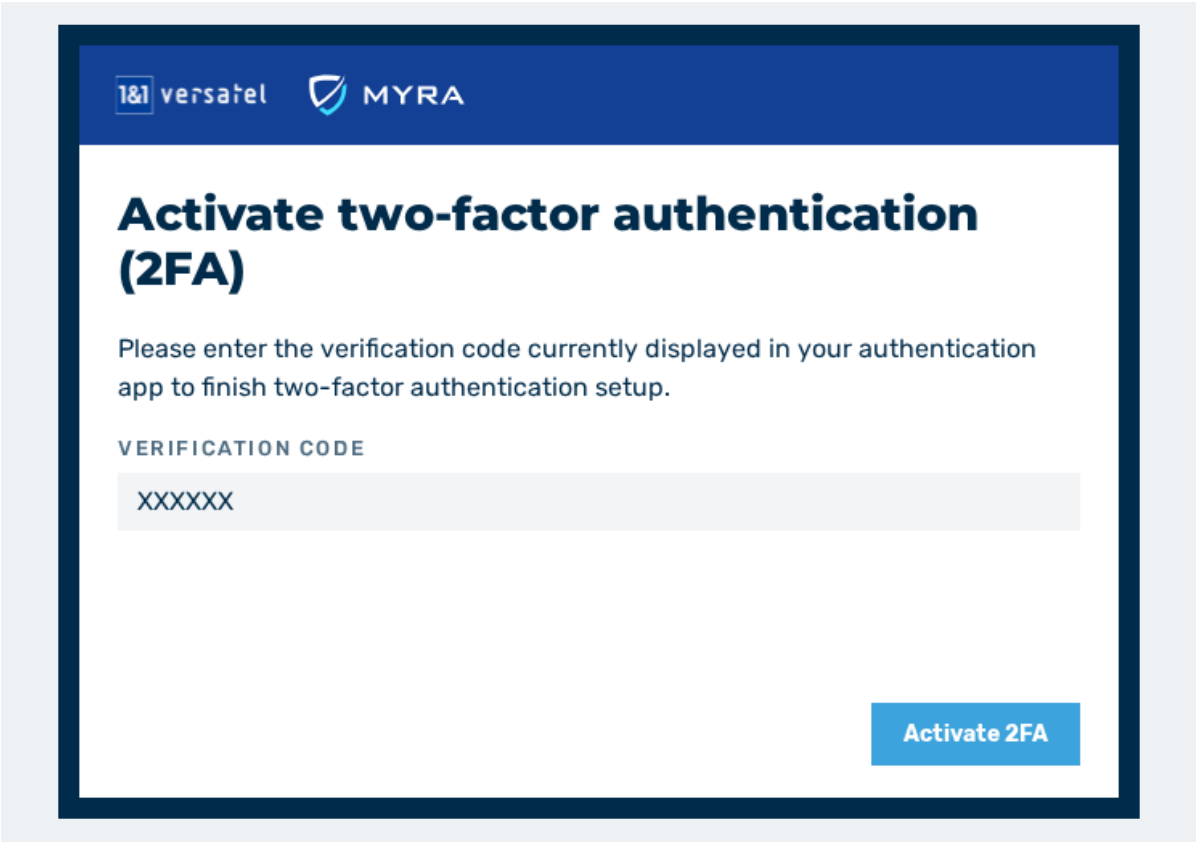


Figure 35: Activate two-factor authentication (2FA) dialog

- ► Click on the **2FA backup codes** button.
  - ↳ The **2FA backup codes** dialog opens.

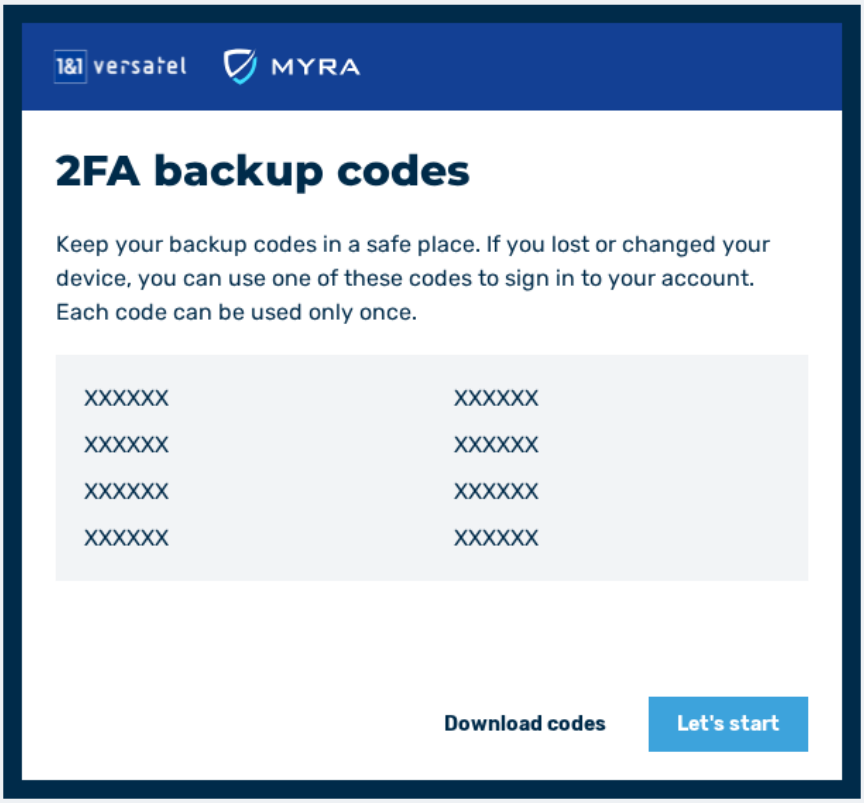


Figure 36: 2FA backup codes dialog

► You have two options:

- Click on the icon to copy the backup codes to the clipboard and save them.
- Download a backup file.

  ▷ Enter your 6-digit verification code in the field under **Verification code**.

  ▷ Click on the **Save codes** button.

  ➔ An HTML file containing the backup codes will be downloaded.

► Click on the **X** in the upper right corner to close the dialog.

➔ Two-factor authentication is set up.

Store or keep the recovery codes in a safe place. Without these codes, you will not be able to access your account if you lose your 2FA device.

You can generate new emergency recovery codes at any time by selecting the **Generate new codes** button. You will then receive eight new one-time codes.

If you want to disable 2FA, you can do so at any time via the **Disable** button in the **Two-factor authentication (2FA)** section of the profile area.

1.3.4.1.4 Close active web browser sessions

In the **Browser sessions** area in the **Profile** view, you can log out of all web browser sessions other than the one currently running in the current browser window.

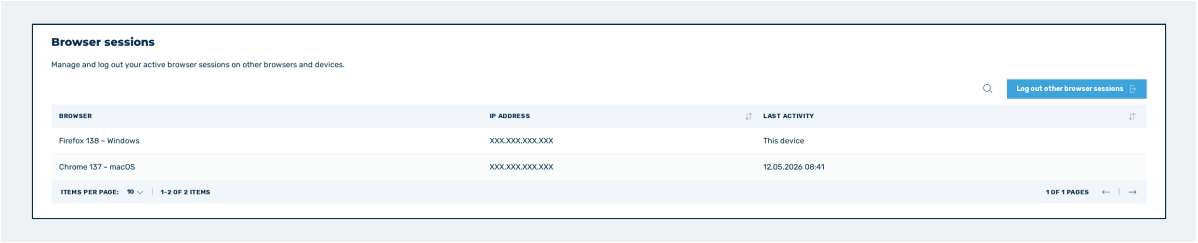


Figure 37: Active sessions area

Proceed as follows to log out of a web browser:

- ► Click on the **Log out other browser sessions** button.
- ➔ A message confirms the successful termination of inactive sessions.

The current session in the current web browser will not be terminated.

1.3.4.2 Notifications tab

The **Notifications** tab appears if you are a member of a company. Myra only sends alerts about traffic anomalies if the anomaly feature is enabled for your company.

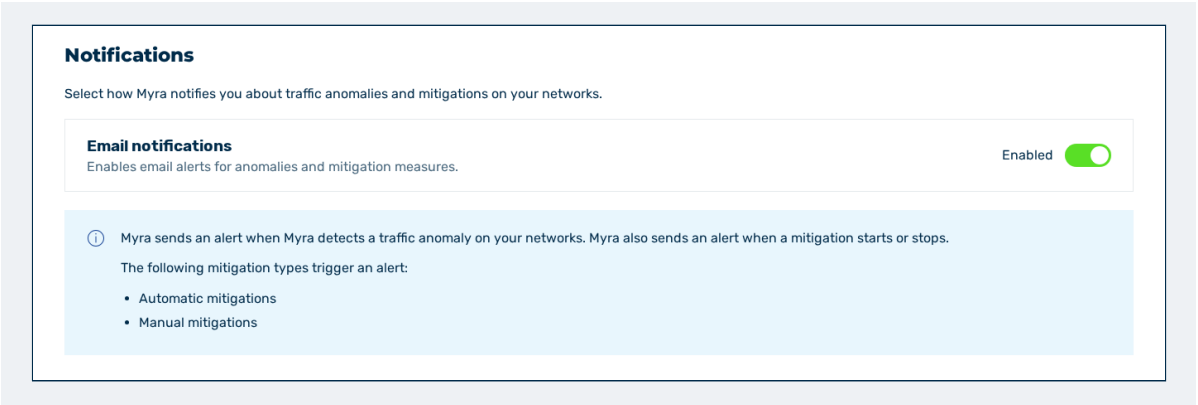


Figure 38: Notifications tab

In the **Notifications** tab, you select how Myra notifies you about traffic anomalies and mitigations on your networks.

Myra sends an alert when Myra detects a traffic anomaly on your networks. Myra also sends an alert when a mitigation starts or stops.

The following types of mitigation trigger a notification:

- Automatic mitigations
- Manual mitigations
- Mitigations that the Myra support team starts

The following options are available:

Element	Description
Email notifications	The switch enables email alerts for anomalies and mitigation measures. The following values are available: **Enabled**: You receive email notifications. **Disabled**: You do not receive email notifications.

Proceed as follows to enable the email notifications:

► Enable the switch under **Email notifications**.

➔ The setting is saved immediately and the **Notifications updated** message appears.

1.3.4.3 API tokens tab

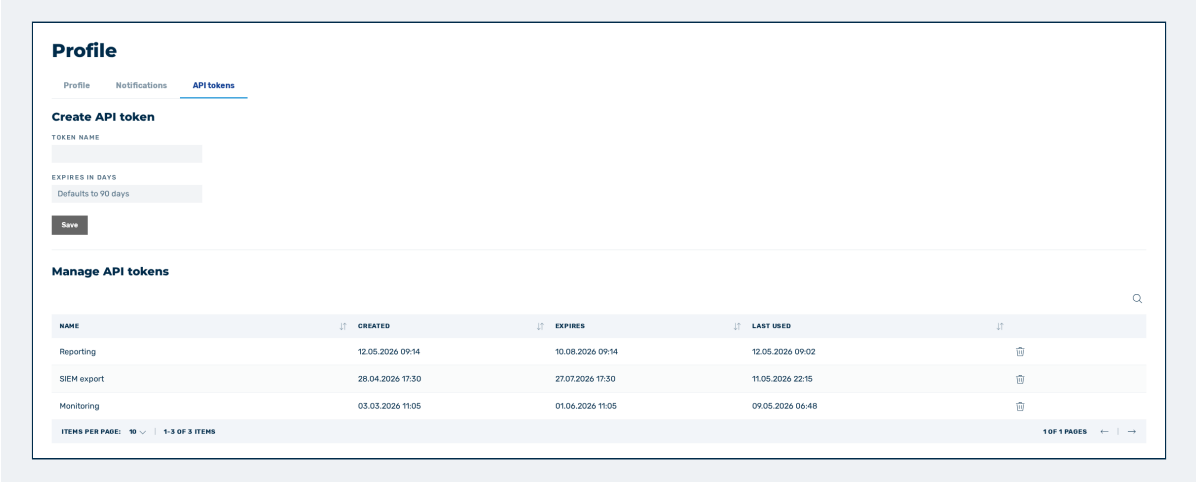


Figure 39: API tokens tab

In the **API tokens** tab, you can create new API tokens, as well as view already added API tokens and delete them.

You need the API token for authentication via bearer tokens to use the API of the Myra DataHub. The token allows you to use Myra's APIv2 easily and securely by specifying the token as a bearer token in the header of your API request.

The tab is split into the following areas:

1.3.4.3.1 Create API token area

In the **Create API token** area, you can create new API tokens and set their validity period.

The following options are available:

Element	Description
Token name	The name of the token.
EXPIRES IN DAYS	The number of days the token is valid.
Save	The button creates the token and opens the **API token created** dialog for copying the token.

1.3.4.3.2 Manage API tokens area

An overview of all tokens.

The following information is available:

Element	Description
Name	The name of the token.
Created	The date and time when the token was generated.
Expires	The number of days the token is valid. ⓘ Specifying an expiration date is optional and does not need to be set when creating an API token. To increase security when using an API token, Myra recommends specifying an expiration date.
Last used	The date and time when the token was last used to execute an API request.

The following options are available:

Element	Description
	The icon opens the **Delete API token** dialog for deleting the selected entry.
Filter field	The field filters entries by names.

1.4 Permissions

1.4.1 Roles and permissions

Pages	Options	User	Admin
Profile	Change name	Yes	Yes
	Change password	Yes	Yes
	Change two-factor authentication	Yes	Yes
	Close web browser session	Yes	Yes
User management	Add account (company)	No	Yes (User & Admin)
	Change account (company)	No	Yes (User & Admin)
	Delete account (business)	No	Yes (User & Admin)
Dashboard	Ansicht **Dashboard**	Yes	Yes
	Download diagrams	Yes	Yes
	Download reports	Yes	Yes
Networks	**Networks** view	Yes	Yes
	Start/stop manual mitigation	No	Yes
	Add Network	No	No
	Show network details	No	No
	Edit network	No	No

Pages	Options	User	Admin
	Delete network	No	No
Mitigation history	**Mitigation history** view	Yes	Yes
	View mitigation report	Yes	Yes
	Download mitigation report	Yes	Yes
Anomaly history	**Anomaly history** view	Yes	Yes
	View anomaly details	Yes	Yes
Notifications	Turn the email notifications of your own account on and off	Yes	Yes
	Notifications tab (company)	No	Yes
	Add/delete additional contact	No	Yes
Audit log (company)	**Audit Log** view	No	Yes
	Download audit log	No	Yes
Language	Change language	Yes	Yes

2. API

2.1 Using the Myra API

The Myra web API is based on REST and uses HTTP requests. Myra supports programmatic access to almost all operations that the user can perform via the web interface. For example, the user can create and configure new domains, manage the cache settings according to the deployment cycle, or change the DNS settings.

Myra's API for the Myra DataHub is available at: **https://versatel.myracloud.com/api/documentation**

Below, we explain the most important steps for registering with APIv2 and sending your first requests.

2.2 General

2.2.1 Getting access to the Myra API

You can authenticate with the Myra API using the following methods.

- Authentication using a bearer token by using an API token

> When you send requests to the Myra DataHub through the API, the API token used has the same permissions as your account.

2.2.2 Authentication using bearer tokens

Proceed as follows to authenticate yourself on the API using a bearer token:

- Creating API token
- Enter bearer token in header

2.2.2.1 Creating API token

Proceed as follows to create an API token:

- Open the Myra DataHub.
- Log in.
- Open your personal account, see **Personal account**.
  - ↳ The **Personal account** view opens.
- Click on the **API tokens** tab.

Figure 40: Enter the name and validity for the API token

- Navigate to the **Create API token** area.
- Enter a name in the text field under **TOKEN NAME**.

> The name of an API token should help you to better identify the different purposes of your API tokens.

- If required, define a validity period for the API token in the text field under **EXPIRES IN DAYS**.

> By default, an API token is valid for 90 days.

- Click on the **Save** button.
  - ↳ The **API token created** dialog opens.

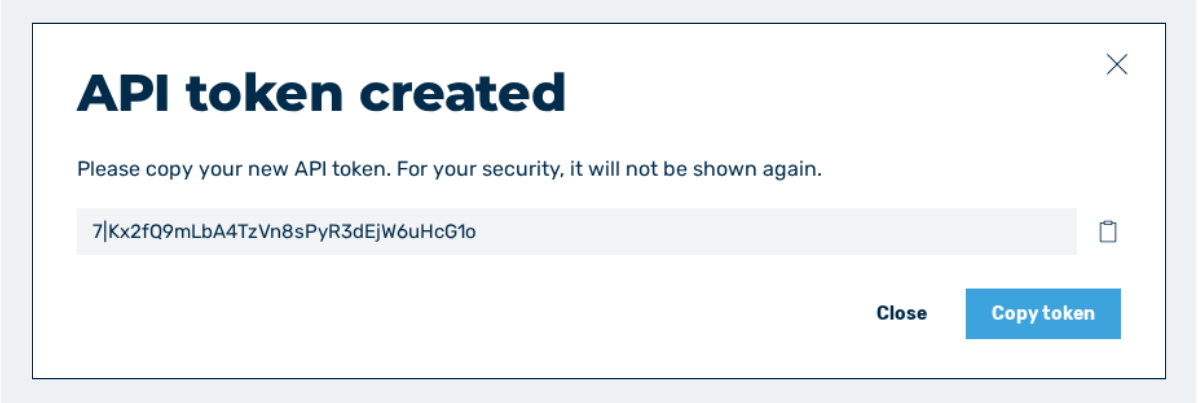


Figure 41: Enter the name and validity for the API token

- ▶ To copy the API token data, click on the icon next to each entry.

> The API token can only be viewed while a new API token is being created and must be stored in a safe place.
>
> As soon as you click on the Close button in the API token created dialog, you can only view the name, the creation date, and the expiry date.
>
> If you have lost the token, you must generate a new API token.

- ▶ To close the dialog, click on the Close button.
- ➔ The new API token appears in the list of all API tokens and can be used immediately.

2.2.2.2 Request to the API using a bearer token

Proceed as follows to send a request to the API using a bearer token:

- ▶ Open the program you want to use to send the request.
- ▶ Add the method for the request.
- ▶ Add the API address together with the URI.

```
https://versatel.myracloud.com/domains/1234
```

- ▶ Add the token as a bearer token to the header as the authentication method.

```
-H „Authorization: Bearer MY_API_TOKEN“
```

- For PUT and POST requests, include a body in JSON format with the required information for the request.

➔ The request should look like this:

```
curl -X GET "https://versatel.myracloud.com/domains/1234"
-H "Authorization: Bearer MY_API_TOKEN"
```

2.2.3 Used API methods

The Myra API for the Myra DataHub uses the following methods:

Element	Description
GET	The GET method allows you to request a specific object or a list of objects with settings and entries in the Myra DataHub.
POST	The POST method allows you to add new settings or entries for specific functions in the Myra DataHub.
PUT	The PUT method allows the user to change specific information of existing settings or entries in the Myra DataHub. Only the attributes `id`, `modified`, and the attributes for changing a specific option must be defined in the body. ⓘ The settings for subdomains are an exception, because changing a setting requires the complete transfer of all attributes of the corresponding object. Attributes that are not defined are reset to the default value.
DELETE	You can use the DELETE method to delete entire entries for an option in the Myra DataHub.

2.2.4 Possible responses to a request

All API requests return a status code and an object that provides information about the success or possible errors, such as missing information or permissions.

2.2.4.1 Possible status codes

Status code	Description	Object
200 OK	The request has succeeded.	QueryVO
201 Created	The request was successful and a new object was created.	ResultVO
202 Accepted	The request was successful but has not yet been completed. This may be the case if the request triggers a process, such as changing a configuration, which takes up to 7 minutes to be implemented.	ResultVO
400 Bad Request	The request was unsuccessful. The request was invalid or information is missing.	ViolationVO
401 Unauthorized	The request was unsuccessful because the request authentication was incorrect.	ViolationVO
403 Forbidden	The request was unsuccessful because the account used does not have the necessary permissions.	ViolationVO

2.2.4.2 Objects used

Element	Description
QueryVO	An object `QueryVO` is returned when a list of objects is received from a GET request.
ResultVO	For successful POST, PUT, and DELETE requests, an object `ResultVO` is returned.
	In the case of invalid requests, an object `ViolationVO` is returned.

Element	Description
Violation **VO**	

2.3 API endpoints

In the following sections, we list all endpoints for our API that you can use to configure the Myra DataHub.

Alternatively, you can find all endpoints in the Swagger documentation of your installation under the path `/api/documentation` .

2.3.1 Organisation management

2.3.1.1 Deleting the SIEM configuration of an organisation

Deleted entries cannot be restored. To use an entry again after deletion, create it anew.

Sends a `DELETE` request to the endpoint `/organisations/{organisation}/siem`.

2.3.1.1.1 Description

The Delete-Organisation-SIEM request deletes the SIEM configuration of the organisation.

2.3.1.1.2 Requirements

Values of the request: **Organisation ID** `{organisation}`

Objects: none

2.3.1.1.3 Request

To delete the SIEM configuration, add the **Organisation ID** `{organisation}` to the path of the request.

No further information is required.

In response to a successful request, the system returns only the HTTP status code 200.

2.3.1.1.4 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	

STATUS CODE	DESCRIPTION
	The request has not succeeded because the user does not have the right permissions.

2.3.1.2 Listing organisations with network and mitigation details

The `OrganisationVO` objects are wrapped in `data`, supplemented by the pagination blocks `links` and `meta`.

Sends a `GET` request to the endpoint `/organisations`.

2.3.1.2.1 Description

The List-Organisations-Paginated request returns a paginated list of all organisations, enriched with network CIDRs and the current mitigation status.

2.3.1.2.2 Requirements

Values of the request: none

Objects: none

2.3.1.2.3 Request

To request a paginated list of all organisations, no additional information is required in the path of the request.

As a result, the user gets one or more objects `OrganisationVO` with the requested information.

The object provides the following information:

Attributes	Description	Values
`id`	The ID of the organisation.	`string`
`name`	The name of the organisation.	`string`
`created_at`	The original creation timestamp in ISO 8601 format.	`string($date-time)`

Attributes	Description	Values
`updated_at`	The last update timestamp in ISO 8601 format.	`string($date-time)`
`users`	The users assigned to the organisation.	`array`
`showReports`	Defines whether mitigation reports are enabled.	`true` `false`
`siemEnabled`	Defines whether the SIEM integration is enabled.	`true` `false`
`customer_id`	The identifier of the customer reference.	`string`
`cidrs`	The comma-separated list of CIDRs.	`string`
`under_mitigation`	Shows whether a network is currently in mitigation.	`true` `false`
`customer_reference`	The grouped customer reference.	`string`

2.3.1.2.4 Example

Example response:


```
{
  "data": [
    {
      "id": "xY9pQ5wR1",
      "name": "Test Organisation",
      "created_at": "2026-01-01T00:00:00+00:00",
      "updated_at": "2026-01-01T00:00:00+00:00",
      "users": [
        {
          "id": "xY9pQ5wR1",
          "name": "Max Mustermann",
          "email": "max@mustermann.de",
          "has2Fa": false,
          "permissions": {},
          "activeOrganisation": {
            "id": "xY9pQ5wR1",
            "name": "Test Organisation"
          },
          "hasActiveMitigations": false,
          "hasSiem": false,
          "invitedSince": "2024-01-15 10:30:00",
```

```
            "status": "active",
            "role": "admin",
            "teams": [
              {
                "id": "xY9pQ5wR1",
                "name": "Test Organisation"
              }
            ],
            "teams_as_admin": [
              {
                "id": "xY9pQ5wR1",
                "name": "Test Organisation"
              }
            ],
            "features": [
              {
                "name": "L_NUMBER",
                "value": null,
                "enabled": 1
              }
            ]
          }
        ],
        "showReports": true,
        "siemEnabled": false,
        "customer_id": "abc",
        "cidrs": "127.0.0.1/32, 10.0.0.0/24",
        "under_mitigation": false,
        "customer_reference": "abc"
      }
    ],
    "links": {
      "first": "https://datahub-api.com/api/networks?page=1",
      "last": "https://datahub-api.com/api/networks?page=5",
      "prev": null,
      "next": "https://datahub-api.com/api/networks?page=2"
    },
    "meta": {
      "current_page": 1,
      "from": 1,
      "last_page": 5,
      "links": [
        {
          "url": "https://datahub-api.com/api/networks?page=2",
          "label": "Next »",
          "active": false
        }
      ],
      "path": "https://datahub-api.com/api/networks",
      "per_page": 15,
      "to": 15,
      "total": 64
    }
  }
```

2.3.1.2.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.

2.3.1.3 Listing all organisations of the user

Sends a `GET` request to the endpoint `/organisations/all`.

2.3.1.3.1 Description

The List-Organisations request returns a list of all organisations to which the user has access.

2.3.1.3.2 Requirements

Values of the request: none

Objects: none

2.3.1.3.3 Request

To request a list of all organisations, no additional information is required in the path of the request.

As a result, the user gets one or more objects `OrganisationVO` with the requested information.

The object provides the following information:

Attributes	Description	Values
`id`	The ID of the organisation.	`string`
`name`	The name of the organisation.	`string`

Attributes	Description	Values
`created_at`	The creation date in ISO 8601 format.	`string($date-time)`
`updated_at`	The last modification date in ISO 8601 format.	`string($date-time)`

The response is not paginated.

2.3.1.3.4 Example

Example response:


```
[
  {
    "id": "xY9pQ5wR1",
    "name": "Test Organisation",
    "created_at": "2026-01-01T00:00:00+00:00",
    "updated_at": "2026-01-01T00:00:00+00:00",
    "users": [
      {
        "id": "xY9pQ5wR1",
        "name": "Max Mustermann",
        "email": "max@mustermann.de",
        "has2Fa": false,
        "permissions": {},
        "activeOrganisation": {
          "id": "xY9pQ5wR1",
          "name": "Test Organisation"
        },
        "hasActiveMitigations": false,
        "hasSiem": false,
        "invitedSince": "2024-01-15 10:30:00",
        "status": "active",
        "role": "admin",
        "teams": [
          {
            "id": "xY9pQ5wR1",
            "name": "Test Organisation"
          }
        ],
        "teams_as_admin": [
          {
            "id": "xY9pQ5wR1",
            "name": "Test Organisation"
          }
        ],
        "features": [
          {
            "name": "L_NUMBER",
```

```
            "value": null,
            "enabled": 1
          }
        ]
      }
    ],
    "showReports": true,
    "siemEnabled": false,
    "customer_id": "abc",
    "cidrs": "127.0.0.1/32, 10.0.0.0/24",
    "under_mitigation": false,
    "customer_reference": "abc"
  }
]
```


2.3.1.3.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.

2.3.1.4 Getting an organisation by ID

Sends a `GET` request to the endpoint `/organisations/{organisation}`.

2.3.1.4.1 Description

The Get-Organisation request returns a single organisation for a specified ID.

2.3.1.4.2 Requirements

Values of the request: **Organisation ID** `{organisation}`

Objects: none

2.3.1.4.3 Request

To request an organisation, add the **Organisation ID** `{organisation}` to the path of the request.

As a result, the user gets an object `OrganisationVO` with the requested information.

The object provides the following information:

Attributes	Description	Values
`id`	The ID of the organisation.	`string`
`name`	The name of the organisation.	`string`
`created_at`	The original creation time in ISO 8601 format.	`string($date-time)`
`updated_at`	The time of the last update in ISO 8601 format.	`string($date-time)`
`users`	The users belonging to the organisation.	`array`
`showReports`	Defines whether mitigation reports are enabled.	`true` `false`
`siemEnabled`	Defines whether the SIEM integration is enabled.	`true` `false`
`customer_id`	The identifier of the customer reference.	`string`
`customer_reference`	The grouped customer reference.	`string`

2.3.1.4.4 Example

Example response:


```
{
  "id": "xY9pQ5wR1",
  "name": "Test Organisation",
  "created_at": "2026-01-01T00:00:00+00:00",
  "updated_at": "2026-01-01T00:00:00+00:00",
  "users": [
    {
      "id": "xY9pQ5wR1",
      "name": "Max Mustermann",
      "email": "max@mustermann.de",
      "has2Fa": false,
      "permissions": {},
      "activeOrganisation": {
        "id": "xY9pQ5wR1",
        "name": "Test Organisation"
```

```
      },
      "hasActiveMitigations": false,
      "hasSiem": false,
      "invitedSince": "2024-01-15 10:30:00",
      "status": "active",
      "role": "admin",
      "teams": [
        {
          "id": "xY9pQ5wR1",
          "name": "Test Organisation"
        }
      ],
      "teams_as_admin": [
        {
          "id": "xY9pQ5wR1",
          "name": "Test Organisation"
        }
      ],
      "features": [
        {
          "name": "L_NUMBER",
          "value": null,
          "enabled": 1
        }
      ]
    }
  ],
  "showReports": true,
  "siemEnabled": false,
  "customer_id": "abc",
  "cidrs": "127.0.0.1/32, 10.0.0.0/24",
  "under_mitigation": false,
  "customer_reference": "abc"
}
```


2.3.1.4.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.

2.3.1.5 Listing all mitigations of an organisation

> The threshold and traffic metrics — `configured_bw`, `configured_pps`, `configured_bw_percentage`, `configured_pps_percentage`, `actual_bw`, `actual_pps`, `peak_bw`, `peak_pps`, `total_bw`, `total_pps` and `dropped_bits` and `dropped_packets` — are only returned for automatic mitigations triggered by detection. They are omitted for manual mitigations, which contain no detection data.

Sends a `GET` request to the endpoint `/organisations/{organisation}/mitigations`.

2.3.1.5.1 Description

The List-Organisation-Mitigations request returns a list of all mitigations for a specified organisation.

2.3.1.5.2 Requirements

Values of the request: **Organisation ID** `{organisation}`

Objects: none

2.3.1.5.3 Request

To request a list of all mitigations, add the **Organisation ID** `{organisation}` to the path of the request.

As a result, the user gets one or more objects `MitigationVO` with the requested information.

The object provides the following information:

Attributes	Description	Values
`id`	The ID of the mitigation.	`string`
`organisation`	The associated organisation, specified as an object.	`object`
`network`	The mitigated network or, in the case of a partial mitigation, the specific IP address.	`string`
	The type of the applied mitigation.	

Attributes	Description	Values
mitigation_type		ACTION_BLACKHOLE ACTION_MITIGATE_ONPREM ACTION_MITIGATE_CLOUD
mitigation_cause	How the mitigation was triggered.	MANUAL_TRIGGER AUTO_TRIGGER OPS_TRIGGER UNKNOWN_TRIGGER
start	The start date of the mitigation in ISO 8601 format.	string($date-time)
end	The end date of the mitigation in ISO 8601 format.	string($date-time)
created_at	The creation date in ISO 8601 format.	string($date-time)
updated_at	The last modification date in ISO 8601 format.	string($date-time)
actual_bw	The actual bandwidth of the mitigation.	number($float)
actual_pps	The actual packets per second of the mitigation.	number($float)
configured_bw	The configured bandwidth of the mitigation.	number($float)
configured_pps	The configured packets per second of the mitigation.	number($float)
	The configured bandwidth as a percentage.	number

Attributes	Description	Values
`configured_bw_percentage`		
`configured_pps_percentage`	The configured packets per second as a percentage.	`number`
`peak_bw`	The peak bandwidth of the mitigation.	`number($float)`
`peak_pps`	The peak packets per second of the mitigation.	`number($float)`
`total_bw`	The total bandwidth of the mitigation.	`number($float)`
`total_pps`	The total packets per second of the mitigation.	`number($float)`
`dropped_bits`	The total bits dropped during the mitigation.	`integer`
`dropped_packets`	The total packets dropped during the mitigation.	`integer`
`has_report`	Shows whether a report is available for the mitigation.	`true` `false`
`start_user`	The users who started the mitigation, specified as an object with ID and display name.	`object`
`end_user`	The users who ended the mitigation, specified as an object with ID and display name. The value is null while the mitigation is still running.	`object`

2.3.1.5.4 Example

Example response:

```
{
  "data": [
    {
```

```
      "id": "xY9pQ5wR1",
      "organisation": {
        "id": "aB3cD4eF5",
        "name": "ACME GmbH"
      },
      "network": "192.0.2.0/24",
      "mitigation_type": "ACTION_MITIGATE_ONPREM",
      "mitigation_cause": "MANUAL_TRIGGER",
      "start": "2026-01-01T00:00:00+00:00",
      "end": "2026-01-01T00:00:00+00:00",
      "created_at": "2026-01-01T00:00:00+00:00",
      "updated_at": "2026-01-01T00:00:00+00:00",
      "actual_bw": 0,
      "actual_pps": 0,
      "configured_bw": 0,
      "configured_pps": 0,
      "configured_bw_percentage": 0,
      "configured_pps_percentage": 0,
      "peak_bw": 0,
      "peak_pps": 0,
      "total_bw": 0,
      "total_pps": 0,
      "dropped_bits": 0,
      "dropped_packets": 0,
      "has_report": true,
      "start_user": {
        "id": "pQ7rS8tU9",
        "name": "Max Mustermann"
      },
      "end_user": {
        "id": "pQ7rS8tU9",
        "name": "Max Mustermann"
      }
    }
  ],
  "links": {
    "first": "https://datahub-api.com/api/networks?page=1",
    "last": "https://datahub-api.com/api/networks?page=5",
    "prev": null,
    "next": "https://datahub-api.com/api/networks?page=2"
  },
  "meta": {
    "current_page": 1,
    "from": 1,
    "last_page": 5,
    "links": [
      {
        "url": "https://datahub-api.com/api/networks?page=2",
        "label": "Next »",
        "active": false
      }
    ],
    "path": "https://datahub-api.com/api/networks",
    "per_page": 15,
    "to": 15,
```

```
    "total": 64
  }
}
```

2.3.1.5.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.

2.3.1.6 Listing all networks of an organisation

> The `pps_limit_percentage` and `bw_limit_percentage` attributes are only present if percentage thresholds are enabled for the organisation.

Sends a `GET` request to the endpoint `/organisations/{organisation}/networks`.

2.3.1.6.1 Description

The List-Organisation-Networks request returns a paginated list of all networks of a specified organisation.

2.3.1.6.2 Requirements

Values of the request: **Organisation ID** `{organisation}`

Objects: none

2.3.1.6.3 Request

To request a list of all networks of an organisation, add the **Organisation ID** `{organisation}` to the path of the request.

As a result, the user gets one or more objects `NetworkVO` with the requested information.

The object provides the following information:

Attributes	Description	Values
`id`	The ID of the network.	`string`
`organisation`	The associated organisation, referenced by ID and name.	`object`
`name`	The name of the network.	`string`
`cidr`	The CIDR range of the network.	`string`
`enabled`	Shows whether automatic mitigation is enabled.	`true` `false`

`mitigation_type`	The mitigation type of the network.	`ACTION_BLACKHOLE`
		`ACTION_MITIGATE_ONPREM`
		`ACTION_MITIGATE_CLOUD`

`auto_mitigation_strategy`	The automatic mitigation strategy of the network.	`string`
`duration`	The duration of the automatic mitigation.	`integer`
`pps_limit`	The configured limit for packets per second.	`integer`
`bw_limit`	The configured bandwidth limit.	`integer`
`autoStatus`	Shows whether the network is currently under automatic mitigation.	`true` `false`
`manualStatus`	Shows whether the network is currently under manual mitigation.	`true` `false`
`active_partial_manual_mitigations`	The active partial manual mitigations.	`array`

Attributes	Description	Values
`active_partial_auto_mitigations`	The active partial automatic mitigations.	`array`
`allow_manual_mitigation`	Shows whether manual mitigations may be started for the network.	`true` `false`
`extra`	Additional custom fields defined for the organisation.	`object`

2.3.1.6.4 Example

Example response:


```
{
  "data": [
    {
      "id": "xY9pQ5wR1",
      "organisation": {
        "id": "aB3cD4eF5",
        "name": "ACME GmbH"
      },
      "name": "Customer-A-Prod",
      "cidr": "192.0.2.0/24",
      "enabled": true,
      "mitigation_type": "ACTION_BLACKHOLE",
      "auto_mitigation_strategy": "IP",
      "duration": 0,
      "pps_limit": 0,
      "bw_limit": 0,
      "autoStatus": true,
      "manualStatus": true,
      "active_partial_manual_mitigations": [
        {}
      ],
      "active_partial_auto_mitigations": [
        {}
      ],
      "allow_manual_mitigation": true,
      "extra": {}
    }
  ],
  "links": {
    "first": "https://datahub-api.com/api/networks?page=1",
    "last": "https://datahub-api.com/api/networks?page=5",
    "prev": null,
    "next": "https://datahub-api.com/api/networks?page=2"
  },
  "meta": {
```

```
    "current_page": 1,
    "from": 1,
    "last_page": 5,
    "links": [
      {
        "url": "https://datahub-api.com/api/networks?page=2",
        "label": "Next »",
        "active": false
      }
    ],
    "path": "https://datahub-api.com/api/networks",
    "per_page": 15,
    "to": 15,
    "total": 64
  }
}
```


2.3.1.6.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.

2.3.1.7 Listing all users of an organisation

Sends a `GET` request to the endpoint `/organisations/{organisation}/users`.

2.3.1.7.1 Description

The List-Organisation-Users request returns a list of all users of a specified organisation, with the exception of agent accounts.

2.3.1.7.2 Requirements

Values of the request: **Organisation ID** `{organisation}`

Objects: none

2.3.1.7.3 Request

To request a list of all users of an organisation, add the **Organisation ID** `{organisation}` to the path of the request.

As a result, the user gets one or more objects `UserV0` with the requested information.

The object provides the following information:

Attributes	Description	Values
`id`	The ID of the user.	`string`
`name`	The full name of the user.	`string`
`email`	The email address of the user.	`string`
`role`	The role of the user within the organisation.	`admin` `editor`
`status`	The current status of the user account.	`string`
`invitedSince`	The date on which the user was invited, or empty if the invitation has already been accepted.	`string($date-time)`
`has2Fa`	Defines whether two-factor authentication is enabled for the user.	`true` `false`

2.3.1.7.4 Example

Example response:


```
[
  {
    "id": "xY9pQ5wR1",
    "name": "Max Mustermann",
    "email": "max@mustermann.de",
    "has2Fa": false,
    "permissions": {},
    "activeOrganisation": {
      "id": "xY9pQ5wR1",
      "name": "Test Organisation"
    },
    "hasActiveMitigations": false,
    "hasSiem": false,
    "invitedSince": "2024-01-15 10:30:00",
    "status": "active",
```

```
    "role": "admin",
    "teams": [
      {
        "id": "xY9pQ5wR1",
        "name": "Test Organisation"
      }
    ],
    "teams_as_admin": [
      {
        "id": "xY9pQ5wR1",
        "name": "Test Organisation"
      }
    ],
    "features": [
      {
        "name": "L_NUMBER",
        "value": null,
        "enabled": 1
      }
    ]
  }
]
```


2.3.1.7.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.

2.3.1.8 Changing the SIEM configuration of an organisation

The body must contain the `id` and `modified` attributes in order to identify the corresponding entry.

The ID of the entry in the request path must match the value of the `id` attribute in the body.

Sends a `PATCH` request to the endpoint `/organisations/{organisation}/siem`.

2.3.1.8.1 Description

The Change-Organisation-SIEM request changes the SIEM connection details of an organisation.

2.3.1.8.2 Requirements

Values of the request: **Organisation ID** `{organisation}`

Objects: `OrganisationVO`

2.3.1.8.3 Request

To change the SIEM connection details, add the **Organisation ID** `{organisation}` to the path of the request.

For a detailed specification of which information is required to change the SIEM connection details, an object `OrganisationVO` with the following attributes must be defined in the body:

Attributes	Description	Values
`id`	The ID of the entry.	`integer`
`modified`	The last modification date in ISO 8601 format.	`string($date-time)`

The following attributes are optional:

Attributes	Description	Values
`siemProvider`	The name of the SIEM provider (for example splunk).	`string`
`siemConnectionDetails`	The connection details for the SIEM provider.	`object`

In response, the system returns the object `OrganisationVO` with the updated information.

The object provides the following information:

Attributes	Description	Values
`id`	The ID of the organisation.	`string`
`name`	The name of the organisation.	`string`
`created_at`	The original creation time.	`string($date-time)`
`updated_at`	The time of the last update.	`string($date-time)`
`users`	The users assigned to the organisation.	`array`
`showReports`	Defines whether mitigation reports are enabled.	`true` `false`
`siemEnabled`	Defines whether the SIEM integration is enabled.	`true` `false`
`customer_id`	The identifier of the customer reference.	`string`
`customer_reference`	The grouped customer reference.	`string`

2.3.1.8.4 Example

Example request body:

```
{
  "siemProvider": "string",
  "siemConnectionDetails": {
    "host": "string",
    "port": 0,
    "apiToken": "string"
  }
}
```

2.3.1.8.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.
422	The request was unsuccessful because the submitted data could not be processed.

2.3.1.9 Changing users within an organisation

> The body must contain the `id` and `modified` attributes in order to identify the corresponding entry.

> The ID of the entry in the request path must match the value of the `id` attribute in the body.

Sends a `PATCH` request to the endpoint `/organisations/{organisation}/users/{user}`.

2.3.1.9.1 Description

The Update-Organisation-User request changes the name and role of a user within a specific organisation.

2.3.1.9.2 Requirements

Values of the request: **Organisation ID** `{organisation}`; **User ID** `{user}`

Objects: none

2.3.1.9.3 Request

To change a user within an organisation, add the **Organisation ID** `{organisation}` and the **User ID** `{user}` to the path of the request.

For a detailed specification of which information is required to change a user, the following attributes must be defined in the body:

Attributes	Description	Values
`id`	The ID of the user.	`string`
`modified`	The last modification date in ISO 8601 format.	`string($date-time)`

The following attributes are optional:

Attributes	Description	Values
`name`	The new name of the user.	`string`
`role`	The new role of the user.	`admin` `editor`

As a result, the user gets an object with the requested information.

The object provides the following information:

Attributes	Description	Values
`id`	The ID of the user.	`string`
`name`	The name of the user.	`string`
`email`	The email address of the user.	`string`
`status`	The current status of the user.	`string`
`invitedSince`	The date on which the user was invited, or empty if the invitation has already been accepted.	`string`
`role`	The role of the user within the organisation.	`admin` `editor`

2.3.1.9.4 Example

Example request body:

```
{
  "name": "string",
  "role": "string"
}
```

2.3.1.9.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.
422	The request was unsuccessful because the submitted data could not be processed.

2.3.1.10 Resending the confirmation email for a notification address

The address must already be registered for the organisation and must not yet be verified; otherwise the request returns a 404 or 409 error.

For this request, you need administration rights for the organisation or SOC rights.

A maximum of five requests per hour to this endpoint is possible.

Sends a `POST` request to the endpoint `/organisations/{organisation}/notification-emails/resend`.

2.3.1.10.1 Description

The Resend-Verification request resends the confirmation email for an unverified notification address of an organisation.

2.3.1.10.2 Requirements

Values of the request: **Organisation ID** `{organisation}`

Objects: none

2.3.1.10.3 Request

To resend the confirmation email, add the **Organisation ID** `{organisation}` to the path of the request and define the target address in the body:

Attributes	Description	Values
`email`	The notification address to which the confirmation email is resent.	`string`

In response to a successful request, the system returns only the HTTP status code 200.

2.3.1.10.4 Example

Example request body:

```
{
  "email": "alerts@example.com"
}
```

2.3.1.10.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.
404	The request was unsuccessful because the requested resource was not found.
409	The request was unsuccessful because there is a conflict with the current state.
422	The request was unsuccessful because the submitted data could not be processed.

2.3.1.11 Adding users to the organisation

The `userId` and `userFullName` attributes are required for Myra deployments.

Sends a `POST` request to the endpoint `/organisations/{organisation}/users/add` .

2.3.1.11.1 Description

The Add-Organisation-User request adds users to a specified organisation.

2.3.1.11.2 Requirements

Values of the request: **Organisation ID** `{organisation}`

Objects: `UserVO`

2.3.1.11.3 Request

To add users to the organisation, add the **Organisation ID** `{organisation}` to the path of the request.

For a detailed specification of which information is required to add users, an object `UserVO` with the following attributes must be defined in the body:

Attributes	Description	Values
`userEmail`	The email address of the user.	`string`
`userRole`	The role of the users.	`admin` `editor`

The following attributes are optional:

Attributes	Description	Values
`userId` (required for Myra deployments)	The MyraCloud ID of the users.	`integer`
`userFullName` (required for Myra deployments)	The full name of the user.	`string`

As a result, the system returns the object `message`, confirming that the users have been added.

The object provides the following information:

Attributes	Description	Values
`message`	The confirmation message of the request.	`string`

2.3.1.11.4 Example

Example request body:

```
{
  "userEmail": "string",
  "userRole": "string",
  "userId": 0,
```

```
  "userFullName": "string"
}
```

2.3.1.11.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.
422	The request was unsuccessful because the submitted data could not be processed.

2.3.1.12 Removing a user from an organisation

> Users cannot remove their own account from an organisation, regardless of their role; such an attempt returns the response `403`.

Sends a `POST` request to the endpoint `/organisations/{organisation}/users/remove`.

2.3.1.12.1 Description

The Remove-Organisation-User request removes a user from a specified organisation.

2.3.1.12.2 Requirements

Values of the request: **Organisation ID** `{organisation}`

Objects: none

2.3.1.12.3 Request

To remove a user from an organisation, add the **Organisation ID** `{organisation}` to the path of the request.

For a detailed specification of which information is required to remove a user from the organisation, the following attribute must be defined in the body:

Attributes	Description	Values
`userId`	The ID of the user to be removed.	`string`

As a result, the user gets an object with a confirmation message.

The object provides the following information:

Attributes	Description	Values
`message`	The confirmation message returned after the user is removed.	`string`

2.3.1.12.4 Example

Example request body:

```
{
  "userId": "string"
}
```

2.3.1.12.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	

STATUS CODE	DESCRIPTION
	The request has not succeeded because the user does not have the right permissions.
404	The request was unsuccessful because the requested resource was not found.

2.3.1.13 Adding a notification address to the organisation

For this request, you need administration rights for the organisation or SOC rights.

The address must not already be registered for the organisation; otherwise the request returns a 422 error.

Sends a `POST` request to the endpoint `/organisations/{organisation}/notification-emails`.

2.3.1.13.1 Description

The Add-Notification-Email request allows you to register an additional notification contact for an organisation that is not a user of the application, for example a shared mailbox or an external partner. A verification email is sent to the address so the contact can confirm the enrolment.

2.3.1.13.2 Requirements

Values of the request: **Organisation ID** `{organisation}`

Objects: none

2.3.1.13.3 Request

To add a notification contact, add the **Organisation ID** `{organisation}` to the path of the request and define the target address in the body:

Attributes	Description	Values
`email`	The notification address to add.	`string`

As a result, you get the created object `NotificationEmail`. The contact remains unverified until the recipient confirms the verification email.

The object provides the following information:

Attributes	Description	Values
`id`	The ID of the notification address.	`string`
`email`	The notification address.	`string`
`verified`	Indicates whether the address has been verified.	`true`, `false`
`verified_at`	The date and time when the address was verified in ISO 8601 format. While the address is unverified, the value is `null`.	`string($date-time)`

2.3.1.13.4 Example

Example request body:

```
{
  "email": "alerts@example.com"
}
```

2.3.1.13.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
201	The request has succeeded and the notification address has been created.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.
422	The request was unsuccessful because the submitted data could not be processed.

2.3.1.14 Deleting a notification address from the organisation

For this request, you need administration rights for the organisation or SOC rights.

Sends a `DELETE` request to the endpoint `/organisations/{organisation}/notification-emails/{notificationEmail}`.

2.3.1.14.1 Description

The Remove-Notification-Email request allows you to remove an additional notification contact from an organisation.

2.3.1.14.2 Requirements

Values of the request: **Organisation ID** `{organisation}`, **Notification address ID** `{notificationEmail}`

Objects: none

2.3.1.14.3 Request

To remove a notification contact, add the **Organisation ID** `{organisation}` and the **Notification address ID** `{notificationEmail}` to the path of the request.

In response to a successful request, the system returns only the HTTP status code 204.

2.3.1.14.4 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
204	The request has succeeded and the response has no content.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.
404	The request was unsuccessful because the requested resource was not found.

2.3.2 Networks

2.3.2.1 Listing all networks with their mitigation status

> The `pps_limit_percentage` and `bw_limit_percentage` attributes are only present if the organisation has percentage thresholds enabled.

> SOC accounts must instead address an organisation explicitly through the `/organisations/{organisation}/networks` endpoint.

Sends a `GET` request to the endpoint `/networks-with-mitigations` .

2.3.2.1.1 Description

The List-Networks-With-Mitigations request returns a list of all networks of the active organisation, including their current mitigation status.

2.3.2.1.2 Requirements

Values of the request: none

Objects: none

2.3.2.1.3 Request

To request a list of all networks with their mitigation status, no additional information is required in the path of the request.

As a result, the user gets one or more objects `NetworkVO` with the requested information.

The object provides the following information:

Attributes	Description	Values
`id`	The ID of the network.	`string`
`organisation`	The associated organisation.	`object`
`name`	The name of the network.	`string`

Attributes	Description	Values
`cidr`	The CIDR of the network.	`string`
`enabled`	Shows whether automatic mitigation is enabled.	`true` `false`

`mitigation_type`	The mitigation type of the network.	`ACTION_BLACKHOLE`
		`ACTION_MITIGATE_ONPREM`
		`ACTION_MITIGATE_CLOUD`

`auto_mitigation_strategy`	The automatic mitigation strategy of the network.	`string`
`duration`	The duration of the automatic mitigation.	`integer`
`pps_limit`	The configured limit for packets per second.	`integer`
`bw_limit`	The configured bandwidth limit.	`integer`
`autoStatus`	Shows whether the network is currently in automatic mitigation.	`true` `false`
`manualStatus`	Shows whether the network is currently in manual mitigation.	`true` `false`
`active_partial_manual_mitigations`	The active partial manual mitigations.	`array`
`active_partial_auto_mitigations`	The active partial automatic mitigations.	`array`
`allow_manual_mitigation`	Shows whether manual mitigations can be started for the network.	`true` `false`
`extra`	Additional custom fields of the organisation.	`object`

2.3.2.1.4 Example

Example response:


```
{
  "data": [
    {
      "id": "xY9pQ5wR1",
      "organisation": {
        "id": "aB3cD4eF5",
        "name": "ACME GmbH"
      },
      "name": "Customer-A-Prod",
      "cidr": "192.0.2.0/24",
      "enabled": true,
      "mitigation_type": "ACTION_BLACKHOLE",
      "auto_mitigation_strategy": "IP",
      "duration": 0,
      "pps_limit": 0,
      "bw_limit": 0,
      "autoStatus": true,
      "manualStatus": true,
      "active_partial_manual_mitigations": [
        {}
      ],
      "active_partial_auto_mitigations": [
        {}
      ],
      "allow_manual_mitigation": true,
      "extra": {}
    }
  ],
  "links": {
    "first": "https://datahub-api.com/api/networks?page=1",
    "last": "https://datahub-api.com/api/networks?page=5",
    "prev": null,
    "next": "https://datahub-api.com/api/networks?page=2"
  },
  "meta": {
    "current_page": 1,
    "from": 1,
    "last_page": 5,
    "links": [
      {
        "url": "https://datahub-api.com/api/networks?page=2",
        "label": "Next »",
        "active": false
      }
    ],
    "path": "https://datahub-api.com/api/networks",
    "per_page": 15,
    "to": 15,
    "total": 64
```

```
    }
  }
```

2.3.2.1.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.

2.3.2.2 Listing all networks of the organisation

SOC accounts must instead address an organisation explicitly through the `/organisations/{organisation}/networks` endpoint.

Sends a `GET` request to the endpoint `/networks` .

2.3.2.2.1 Description

The List-Networks request returns a list of all networks of the organisation.

2.3.2.2.2 Requirements

Values of the request: none

Objects: none

2.3.2.2.3 Request

To request a list of all networks, no additional information is required in the path of the request.

As a result, the user gets one or more objects `NetworkVO` with the requested information.

The object provides the following information:

Attributes	Description	Values
`id`	The ID of the network.	`string`
`organisation`	The associated organisation, referenced by `id` and `name`.	`object`
`name`	The name of the network.	`string`
`cidr`	The IP range of the network in CIDR notation.	`string`
`enabled`	Defines whether automatic mitigation is enabled.	`true` `false`

`mitigation_type`	The type of mitigation applied when the thresholds are exceeded.	`ACTION_BLACKHOLE`
		`ACTION_MITIGATE_ONPREM`
		`ACTION_MITIGATE_CLOUD`

`auto_mitigation_strategy`	The strategy for the automatic mitigation.	`string`
`duration`	The duration of the automatic mitigation in seconds.	`integer`
`pps_limit`	The configured PPS limit.	`integer`
`bw_limit`	The configured bandwidth limit.	`integer`
`autoStatus`	Shows whether the network is currently in automatic mitigation.	`true` `false`
`manualStatus`	Shows whether the network is currently in manual mitigation.	`true` `false`
`active_partial_manual_mitigations`	The active partial manual mitigations of the network.	`array`

Attributes	Description	Values
`active_partial_auto_mitigations`	The active partial automatic mitigations of the network.	`array`
`allow_manual_mitigation`	Shows whether manual mitigations can be started for the network.	`true` `false`
`extra`	Additional custom fields of the organisation.	`object`

2.3.2.2.4 Example

Example response:


```
{
  "data": [
    {
      "id": "xY9pQ5wR1",
      "organisation": {
        "id": "aB3cD4eF5",
        "name": "ACME GmbH"
      },
      "name": "Customer-A-Prod",
      "cidr": "192.0.2.0/24",
      "enabled": true,
      "mitigation_type": "ACTION_BLACKHOLE",
      "auto_mitigation_strategy": "IP",
      "duration": 0,
      "pps_limit": 0,
      "bw_limit": 0,
      "autoStatus": true,
      "manualStatus": true,
      "active_partial_manual_mitigations": [
        {}
      ],
      "active_partial_auto_mitigations": [
        {}
      ],
      "allow_manual_mitigation": true,
      "extra": {}
    }
  ],
  "links": {
    "first": "https://datahub-api.com/api/networks?page=1",
    "last": "https://datahub-api.com/api/networks?page=5",
    "prev": null,
    "next": "https://datahub-api.com/api/networks?page=2"
  },
  "meta": {
```

```
    "current_page": 1,
    "from": 1,
    "last_page": 5,
    "links": [
      {
        "url": "https://datahub-api.com/api/networks?page=2",
        "label": "Next »",
        "active": false
      }
    ],
    "path": "https://datahub-api.com/api/networks",
    "per_page": 15,
    "to": 15,
    "total": 64
  }
}
```


2.3.2.2.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.

2.3.2.3 Getting a network by ID

The `pps_limit_percentage` and `bw_limit_percentage` attributes are only present if the organisation has percentage thresholds enabled.

SOC accounts must instead address an organisation explicitly through the `/organisations/{organisation}/networks` endpoint.

Sends a `GET` request to the endpoint `/networks/{network}`.

2.3.2.3.1 Description

The Get-Network request returns a single network for a specified ID.

2.3.2.3.2 Requirements

Values of the request: **Network ID** `{network}`

Objects: none

2.3.2.3.3 Request

To request a single network, add the **Network ID** `{network}` to the path of the request.

As a result, the user gets an object `NetworkVO` with the requested information.

The object provides the following information:

Attributes	Description	Values
`id`	The ID of the network.	`string`
`organisation`	The associated organisation.	`object`
`name`	The name of the network.	`string`
`cidr`	The CIDR range of the network.	`string`
`enabled`	Defines whether automatic mitigation is enabled.	`true` `false`

`mitigation_type`	The mitigation type of the network.	`ACTION_BLACKHOLE`
		`ACTION_MITIGATE_ONPREM`
		`ACTION_MITIGATE_CLOUD`

`auto_mitigation_strategy`	The automatic mitigation strategy of the network.	`string`
`duration`	The duration of the automatic mitigation.	`integer`
`pps_limit`	The configured PPS limit.	`integer`
`bw_limit`	The configured bandwidth limit.	`integer`

Attributes	Description	Values
`autoStatus`	Defines whether an automatic mitigation is currently running for the network.	`true` `false`
`manualStatus`	Defines whether a manual mitigation is currently running for the network.	`true` `false`
`active_partial_manual_mitigations`	The active partial manual mitigations.	`array`
`active_partial_auto_mitigations`	The active partial automatic mitigations.	`array`
`allow_manual_mitigation`	Shows whether manual mitigations can be started for the network.	`true` `false`
`extra`	Additional custom fields of the organisation.	`object`

2.3.2.3.4 Example

Example response:


```
{
  "id": "xY9pQ5wR1",
  "organisation": {
    "id": "aB3cD4eF5",
    "name": "ACME GmbH"
  },
  "name": "Customer-A-Prod",
  "cidr": "192.0.2.0/24",
  "enabled": true,
  "mitigation_type": "ACTION_BLACKHOLE",
  "auto_mitigation_strategy": "IP",
  "duration": 0,
  "pps_limit": 0,
  "bw_limit": 0,
  "autoStatus": true,
  "manualStatus": true,
  "active_partial_manual_mitigations": [
    {}
  ],
  "active_partial_auto_mitigations": [
    {}
  ],
  "allow_manual_mitigation": true,
```

```
  "extra": {}
}
```

2.3.2.3.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.

2.3.2.4 Listing all mitigations of a network

The threshold and traffic values — `configured_bw`, `configured_pps`, `configured_bw_percentage`, `configured_pps_percentage`, `actual_bw`, `actual_pps`, `peak_bw`, `peak_pps`, `total_bw`, `total_pps` and `dropped_bits` and `dropped_packets` — are only returned for automatic mitigations triggered by detection. They are omitted for manual mitigations, which contain no detection data.

SOC accounts must instead address an organisation explicitly through the `/organisations/{organisation}/mitigations` endpoint.

Sends a `GET` request to the endpoint `/networks/{network}/mitigations`.

2.3.2.4.1 Description

The List-Network-Mitigations request returns a list of all mitigations of a specified network.

2.3.2.4.2 Requirements

Values of the request: **Network ID** `{network}`

Objects: none

2.3.2.4.3 Request

To request a list of all mitigations of a network, add the **Network ID** `{network}` to the path of the request.

As a result, the user gets one or more objects `MitigationVO` with the requested information.

The object provides the following information:

Attributes	Description	Values
`id`	The ID of the mitigation.	`string`
`organisation`	The associated organisation.	`object`
`network`	The network or, in the case of a partial mitigation, the specific IP that is mitigated.	`string`

`mitigation_type`	The type of the mitigation.	`ACTION_BLACKHOLE`
		`ACTION_MITIGATE_ONPREM`
		`ACTION_MITIGATE_CLOUD`

`mitigation_cause`	The way in which the mitigation was triggered.	`MANUAL_TRIGGER`
		`AUTO_TRIGGER`
		`OPS_TRIGGER`
		`UNKNOWN_TRIGGER`

`start`	The start date of the mitigation in ISO 8601 format.	`string($date-time)`
`end`	The end date of the mitigation in ISO 8601 format.	`string($date-time)`

Attributes	Description	Values
`created_at`	The creation date in ISO 8601 format.	`string($date-time)`
`updated_at`	The last modification date in ISO 8601 format.	`string($date-time)`
`actual_bw`	The actual bandwidth of the mitigation.	`number($float)`
`actual_pps`	The actual packets per second of the mitigation.	`number($float)`
`configured_bw`	The configured bandwidth of the mitigation.	`number($float)`
`configured_pps`	The configured packets per second of the mitigation.	`number($float)`
`configured_bw_percentage`	The configured bandwidth as a percentage.	`number`
`configured_pps_percentage`	The configured packets per second as a percentage.	`number`
`peak_bw`	The peak bandwidth of the mitigation.	`number($float)`
`peak_pps`	The maximum packets per second of the mitigation.	`number($float)`
`total_bw`	The total bandwidth of the mitigation.	`number($float)`
`total_pps`	The total packets per second of the mitigation.	`number($float)`
`dropped_bits`	The total bits dropped during the mitigation.	`integer`
`dropped_packets`	The total packets dropped during the mitigation.	`integer`
`has_report`	Shows whether a report is available for the mitigation.	`true` `false`
`start_user`	The users who started the mitigation.	`object`
`end_user`	The users who ended the mitigation. This value is null while the mitigation is running.	`object`

2.3.2.4.4 Example

Example response:


```
{
  "data": [
    {
      "id": "xY9pQ5wR1",
      "organisation": {
        "id": "aB3cD4eF5",
        "name": "ACME GmbH"
      },
      "network": "192.0.2.0/24",
      "mitigation_type": "ACTION_MITIGATE_ONPREM",
      "mitigation_cause": "MANUAL_TRIGGER",
      "start": "2026-01-01T00:00:00+00:00",
      "end": "2026-01-01T00:00:00+00:00",
      "created_at": "2026-01-01T00:00:00+00:00",
      "updated_at": "2026-01-01T00:00:00+00:00",
      "actual_bw": 0,
      "actual_pps": 0,
      "configured_bw": 0,
      "configured_pps": 0,
      "configured_bw_percentage": 0,
      "configured_pps_percentage": 0,
      "peak_bw": 0,
      "peak_pps": 0,
      "total_bw": 0,
      "total_pps": 0,
      "dropped_bits": 0,
      "dropped_packets": 0,
      "has_report": true,
      "start_user": {
        "id": "pQ7rS8tU9",
        "name": "Max Mustermann"
      },
      "end_user": {
        "id": "pQ7rS8tU9",
        "name": "Max Mustermann"
      }
    }
  ],
  "links": {
    "first": "https://datahub-api.com/api/networks?page=1",
    "last": "https://datahub-api.com/api/networks?page=5",
    "prev": null,
    "next": "https://datahub-api.com/api/networks?page=2"
  },
  "meta": {
    "current_page": 1,
    "from": 1,
    "last_page": 5,
    "links": [
      {
```

```
        "url": "https://datahub-api.com/api/networks?page=2",
        "label": "Next »",
        "active": false
      }
    ],
    "path": "https://datahub-api.com/api/networks",
    "per_page": 15,
    "to": 15,
    "total": 64
  }
}
```


2.3.2.4.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.

2.3.2.5 Starting a manual mitigation for a network

If a manual mitigation is already active for the network, a second one cannot be started. The existing mitigation must be stopped first. Data-only networks cannot be mitigated.

A partial mitigation cannot be started for a single-host network (an IPv4 `/32` or IPv6 `/128`), because it covers only a single address. Omit `ip` to mitigate the entire network instead.

Sends a `POST` request to the endpoint `/networks/{network}/mitigation/start`.

2.3.2.5.1 Description

The Start-Manual-Mitigation request starts a manual mitigation for a specified network.

2.3.2.5.2 Requirements

Values of the request: **Network ID** `{network}`

Objects: none

2.3.2.5.3 Request

To start a manual mitigation, add the **Network ID** `{network}` to the path of the request.

The body requires no attributes. The following attributes are optional:

Attributes	Description	Values
`ip`	A list of individual IPs within the network for a partial mitigation. If this information is missing, the entire network CIDR is mitigated. Both IPv4 and IPv6 are accepted.	`array`

As a result, the user gets one or more objects `MitigationVO` with the requested information.

The object provides the following information:

Attributes	Description	Values
`id`	The ID of the mitigation.	`string`
`organisation`	The associated organisation.	`object`
`network`	The network, or the specific IP that is mitigated in the case of a partial mitigation.	`string`

`mitigation_type`	The type of the mitigation.	`ACTION_BLACKHOLE`
		`ACTION_MITIGATE_ONPREM`
		`ACTION_MITIGATE_CLOUD`

Attributes	Description	Values

`mitigation_cause`	How the mitigation was triggered.	`MANUAL_TRIGGER`
		`AUTO_TRIGGER`
		`OPS_TRIGGER`
		`UNKNOWN_TRIGGER`

`start`	The start date of the mitigation in ISO 8601 format.	`string($date-time)`
`end`	The end date of the mitigation in ISO 8601 format.	`string($date-time)`
`created_at`	The creation date in ISO 8601 format.	`string($date-time)`
`updated_at`	The last modification date in ISO 8601 format.	`string($date-time)`
`actual_bw`	The actual bandwidth.	`number($float)`
`actual_pps`	The actual packets per second.	`number($float)`
`configured_bw`	The configured bandwidth.	`number($float)`
`configured_pps`	The configured packets per second.	`number($float)`
`configured_bw_percentage`	The configured bandwidth as a percentage.	`number`
`configured_pps_percentage`	The configured packets per second as a percentage.	`number`
`peak_bw`	The peak bandwidth.	`number($float)`
`peak_pps`	The maximum packets per second.	`number($float)`
`total_bw`	The total bandwidth.	`number($float)`
`total_pps`	The total packets per second.	`number($float)`
`has_report`	Shows whether a report is available for the mitigation.	`true` `false`

Attributes	Description	Values
`start_user`	The person who started the mitigation.	`object`
`end_user`	The person who ended the mitigation. This value is null while the mitigation is running.	`object`

2.3.2.5.4 Example

Example request body:

```
{
  "ip": [
    "192.0.2.1"
  ]
}
```

2.3.2.5.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
304	The resource has not changed since the last request.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.
422	The request was unsuccessful because the submitted data could not be processed.

2.3.2.6 Stopping the active manual mitigation of a network

Sends a `POST` request to the endpoint `/networks/{network}/mitigation/stop`.

2.3.2.6.1 Description

The Stop-Mitigation request stops the active manual mitigation for a specified network.

2.3.2.6.2 Requirements

Values of the request: **Network ID** `{network}`

Objects: none

2.3.2.6.3 Request

To stop the active manual mitigation, add the **Network ID** `{network}` to the path of the request.

The following attributes are optional:

Attributes	Description	Values
`ip`	A list of individual IPs within the network for which the mitigation is to be stopped. If this information is missing, the mitigation is stopped for the entire network CIDR.	`array`

As a result, the user gets one or more objects `MitigationVO` with the requested information.

The object provides the following information:

Attributes	Description	Values
`id`	The ID of the mitigation.	`string`
`organisation`	The associated organisation.	`object`
`network`	The network or, in the case of a partial mitigation, the specific IP that is mitigated.	`string`

`mitigation_type`	The type of the mitigation.	`ACTION_BLACKHOLE`
		`ACTION_MITIGATE_ONPREM`
		`ACTION_MITIGATE_CLOUD`

Attributes	Description	Values

`mitigation_cause`	How the mitigation was triggered.	`MANUAL_TRIGGER`
		`AUTO_TRIGGER`
		`OPS_TRIGGER`
		`UNKNOWN_TRIGGER`

`start`	The start date of the mitigation in ISO 8601 format.	`string($date-time)`
`end`	The end date of the mitigation in ISO 8601 format.	`string($date-time)`
`created_at`	The creation date in ISO 8601 format.	`string($date-time)`
`updated_at`	The last modification date in ISO 8601 format.	`string($date-time)`
`actual_bw`	The actual bandwidth.	`number($float)`
`actual_pps`	The actual packets per second.	`number($float)`
`configured_bw`	The configured bandwidth.	`number($float)`
`configured_pps`	The configured packets per second.	`number($float)`
`configured_bw_percentage`	The configured bandwidth as a percentage.	`number`
`configured_pps_percentage`	The configured packets per second as a percentage.	`number`
`peak_bw`	The peak bandwidth.	`number($float)`
`peak_pps`	The maximum packets per second.	`number($float)`
`total_bw`	The total bandwidth.	`number($float)`
`total_pps`	The total packets per second.	`number($float)`
`has_report`	Whether a report is available for the mitigation.	`true` `false`

Attributes	Description	Values
`start_user`	The users who started the mitigation.	`object`
`end_user`	The users who ended the mitigation; null while the mitigation is running.	`object`

2.3.2.6.4 Example

Example request body:

```
{
  "ip": [
    "string"
  ]
}
```

2.3.2.6.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
304	The resource has not changed since the last request.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.
422	The request was unsuccessful because the submitted data could not be processed.

2.3.3 Mitigations

2.3.3.1 Listing all mitigations of the organisation

> The threshold and traffic metrics — `configured_bw`, `configured_pps`, `configured_bw_percentage`, `configured_pps_percentage`, `actual_bw`, `actual_pps`, `peak_bw`, `peak_pps`, `total_bw`, `total_pps` and `dropped_bits` and `dropped_packets` — are only returned for automatic mitigations triggered by detection. They are omitted for manual mitigations, which contain no detection data.

> SOC accounts must instead address an organisation explicitly through the `/organisations/{organisation}/mitigations` endpoint.

Sends a `GET` request to the endpoint `/mitigations`.

2.3.3.1.1 Description

The List-Mitigations request returns a list of all mitigations of the organisation.

2.3.3.1.2 Requirements

Values of the request: none

Objects: none

2.3.3.1.3 Request

To request a list of all mitigations, no additional information is required in the path of the request.

As a result, the user gets one or more objects `MitigationVO` with the requested information.

The object provides the following information:

Attributes	Description	Values
`id`	The ID of the mitigation.	`string`

Attributes	Description	Values
`organisation`	The associated organisation.	`object`
`network`	The mitigated network, or a single IP address in the case of a partial mitigation.	`string`

`mitigation_type`	The type of the applied mitigation.	`ACTION_BLACKHOLE`
		`ACTION_MITIGATE_ONPREM`
		`ACTION_MITIGATE_CLOUD`

`mitigation_cause`	How the mitigation was triggered.	`MANUAL_TRIGGER`
		`AUTO_TRIGGER`
		`OPS_TRIGGER`
		`UNKNOWN_TRIGGER`

`start`	When the mitigation started.	`string($date-time)`
`end`	When the mitigation ended; null while it is still running.	`string($date-time)`
`created_at`	The creation date of the entry in ISO 8601 format.	`string($date-time)`
`updated_at`	The date of the last update of the entry in ISO 8601 format.	`string($date-time)`
`actual_bw`	The measured bandwidth at the start of the mitigation.	`number($float)`
`actual_pps`	The measured packet rate at the start of the mitigation.	`number($float)`
`configured_bw`	The bandwidth threshold configured at the start of the mitigation.	`number($float)`
`configured_pps`	The packet rate threshold configured at the start of the mitigation.	`number($float)`

Attributes	Description	Values
`configured_bw_percentage`	The bandwidth threshold as a percentage of the calculated baseline.	`number`
`configured_pps_percentage`	The packet rate threshold as a percentage of the calculated baseline.	`number`
`peak_bw`	The peak bandwidth observed during the mitigation.	`number($float)`
`peak_pps`	The peak packet rate observed during the mitigation.	`number($float)`
`total_bw`	The total bits processed during the mitigation.	`number($float)`
`total_pps`	The total packets processed during the mitigation.	`number($float)`
`dropped_bits`	The total bits dropped during the mitigation.	`integer`
`dropped_packets`	The total packets dropped during the mitigation.	`integer`
`has_report`	Defines whether a detailed mitigation report is available.	`true` `false`
`start_user`	Who started the mitigation.	`object`
`end_user`	Who ended the mitigation; null while it is still running.	`object`

2.3.3.1.4 Example

Example response:


```
{
  "data": [
    {
      "id": "xY9pQ5wR1",
      "organisation": {
        "id": "aB3cD4eF5",
        "name": "ACME GmbH"
      },
      "network": "192.0.2.0/24",
```

```
      "mitigation_type": "ACTION_MITIGATE_ONPREM",
      "mitigation_cause": "MANUAL_TRIGGER",
      "start": "2026-01-01T00:00:00+00:00",
      "end": "2026-01-01T00:00:00+00:00",
      "created_at": "2026-01-01T00:00:00+00:00",
      "updated_at": "2026-01-01T00:00:00+00:00",
      "actual_bw": 0,
      "actual_pps": 0,
      "configured_bw": 0,
      "configured_pps": 0,
      "configured_bw_percentage": 0,
      "configured_pps_percentage": 0,
      "peak_bw": 0,
      "peak_pps": 0,
      "total_bw": 0,
      "total_pps": 0,
      "dropped_bits": 0,
      "dropped_packets": 0,
      "has_report": true,
      "start_user": {
        "id": "pQ7rS8tU9",
        "name": "Max Mustermann"
      },
      "end_user": {
        "id": "pQ7rS8tU9",
        "name": "Max Mustermann"
      }
    }
  ],
  "links": {
    "first": "https://datahub-api.com/api/networks?page=1",
    "last": "https://datahub-api.com/api/networks?page=5",
    "prev": null,
    "next": "https://datahub-api.com/api/networks?page=2"
  },
  "meta": {
    "current_page": 1,
    "from": 1,
    "last_page": 5,
    "links": [
      {
        "url": "https://datahub-api.com/api/networks?page=2",
        "label": "Next »",
        "active": false
      }
    ],
    "path": "https://datahub-api.com/api/networks",
    "per_page": 15,
    "to": 15,
    "total": 64
  }
}
```

2.3.3.1.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.

2.3.3.2 Getting a mitigation by ID

The threshold and traffic values — `configured_bw`, `configured_pps`, `configured_bw_percentage`, `configured_pps_percentage`, `actual_bw`, `actual_pps`, `peak_bw`, `peak_pps`, `total_bw`, `total_pps` and `dropped_bits` and `dropped_packets` — are only returned for automatic mitigations triggered by detection. They are omitted for manual mitigations, which contain no detection data. You need at least READ permissions for the selected period.

SOC accounts must instead address an organisation explicitly through the `/organisations/{organisation}/mitigations` endpoint.

Sends a `GET` request to the endpoint `/mitigations/{mitigation}`.

2.3.3.2.1 Description

The Get-Mitigation request returns a single mitigation for a specified ID.

2.3.3.2.2 Requirements

Values of the request: **Mitigation ID** `{mitigation}`

Objects: none

2.3.3.2.3 Request

To request a mitigation, add the **Mitigation ID** `{mitigation}` to the path of the request.

As a result, the user gets an object `MitigationVO` with the requested information.

The object provides the following information:

Attributes	Description	Values
`id`	The ID of the mitigation.	`string`
`organisation`	The associated organisation of the mitigation.	`object`
`network`	The network, or the specific IP address that is mitigated in the case of a partial mitigation.	`string`

`mitigation_type`	The applied mitigation type.	`ACTION_BLACKHOLE`
		`ACTION_MITIGATE_ONPREM`
		`ACTION_MITIGATE_CLOUD`

`mitigation_cause`	How the mitigation was triggered.	`MANUAL_TRIGGER`
		`AUTO_TRIGGER`
		`OPS_TRIGGER`
		`UNKNOWN_TRIGGER`

`start`	The start date of the mitigation in ISO 8601 format.	`string($date-time)`
`end`	The end date of the mitigation in ISO 8601 format.	`string($date-time)`
`created_at`	The creation date in ISO 8601 format.	`string($date-time)`
`updated_at`	The last modification date in ISO 8601 format.	`string($date-time)`
`actual_bw`	The actual bandwidth of the mitigation.	`number($float)`

Attributes	Description	Values
`actual_pps`	The actual packets per second of the mitigation.	`number($float)`
`configured_bw`	The configured bandwidth of the mitigation.	`number($float)`
`configured_pps`	The configured packets per second of the mitigation.	`number($float)`
`configured_bw_percentage`	The configured bandwidth as a percentage value.	`number`
`configured_pps_percentage`	The configured packets per second as a percentage value.	`number`
`peak_bw`	The peak bandwidth of the mitigation.	`number($float)`
`peak_pps`	The peak value of the packets per second of the mitigation.	`number($float)`
`total_bw`	The total bandwidth of the mitigation.	`number($float)`
`total_pps`	The total number of packets per second of the mitigation.	`number($float)`
`dropped_bits`	The total number of bits dropped during the mitigation.	`integer`
`dropped_packets`	The total number of packets dropped during the mitigation.	`integer`
`has_report`	Shows whether a report is available for the mitigation.	`true` `false`
`start_user`	The user who started the mitigation.	`object`
`end_user`	The user who ended the mitigation; null while the mitigation is running.	`object`
`peaks`	The breakdown of the peak traffic of the mitigation.	`object`

2.3.3.2.4 Example

Example response:


```
{
  "id": "string",
  "organisation": {},
  "network": "string",
  "mitigation_type": "ACTION_BLACKHOLE",
  "mitigation_cause": "MANUAL_TRIGGER",
  "start": "2026-01-01T00:00:00+00:00",
  "end": "2026-01-01T00:00:00+00:00",
  "created_at": "2026-01-01T00:00:00+00:00",
  "updated_at": "2026-01-01T00:00:00+00:00",
  "actual_bw": 0,
  "actual_pps": 0,
  "configured_bw": 0,
  "configured_pps": 0,
  "configured_bw_percentage": 0,
  "configured_pps_percentage": 0,
  "peak_bw": 0,
  "peak_pps": 0,
  "total_bw": 0,
  "total_pps": 0,
  "dropped_bits": 0,
  "dropped_packets": 0,
  "has_report": true,
  "start_user": {},
  "end_user": {},
  "peaks": {}
}
```


2.3.3.2.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.

2.3.3.3 Getting graph data of a mitigation

> SOC accounts cannot call this endpoint with a personal access token. There is no organisation-related token equivalent for it. Use the access options provided by the web application (session authentication) instead.

Sends a `GET` request to the endpoint `/mitigations/{mitigation}/data/{dataType}/{field}`.

2.3.3.3.1 Description

The Get-Mitigation-Data request returns the graph data for a specific mitigation, filtered by data type and field.

2.3.3.3.2 Requirements

Values of the request: **Mitigation ID** `{mitigation}`; **Data type** `{dataType}`; **Field** `{field}`

Objects: none

2.3.3.3.3 Request

To request the graph data of a mitigation, add the **Mitigation ID** `{mitigation}`, the **Data type** `{dataType}`, and the **Field** `{field}` to the path of the request.

Data type `{dataType}` defines the type of data to retrieve, for example `bandwidth` or `protocol`.

Field `{field}` defines the field to retrieve, for example `bits` or `packets`.

As a result, the user gets an array of series for a graphical visualisation.

The object provides the following information:

Attributes	Description	Values
`name`	The name of the series.	`string`
`data`	The array of data points of the series. Each point provides the attributes `x` and `y`.	`array`

2.3.3.3.4 Example

Example response:


```
[
  {
    "data": [
      {
        "x": 0,
        "y": 0
      }
    ],
    "name": "string"
  }
]
```


2.3.3.3.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.

2.3.3.4 Stopping a manual mitigation by ID

Sends a `POST` request to the endpoint `/mitigations/{mitigation}/stop`.

2.3.3.4.1 Description

The Stop-Mitigation request stops a specific manual mitigation by its ID.

2.3.3.4.2 Requirements

Values of the request: **Mitigation ID** `{mitigation}`

Objects: none

2.3.3.4.3 Request

To stop a manual mitigation, add the **Mitigation ID** `{mitigation}` to the path of the request. No further information is required.

As a result, the user gets an object `MitigationVO` with the information about the stopped mitigation.

The object provides the following information:

Attributes	Description	Values
`id`	The ID of the mitigation.	`string`
`organisation`	The associated organisation.	`object`
`network`	The network, or the specific IP that is mitigated in the case of a partial mitigation.	`string`

`mitigation_type`	The type of the mitigation.	`ACTION_BLACKHOLE`
		`ACTION_MITIGATE_ONPREM`
		`ACTION_MITIGATE_CLOUD`

`mitigation_cause`	How the mitigation was triggered.	`MANUAL_TRIGGER`
		`AUTO_TRIGGER`
		`OPS_TRIGGER`
		`UNKNOWN_TRIGGER`

`start`	The start date in ISO 8601 format.	`string($date-time)`
`end`	The end date in ISO 8601 format.	`string($date-time)`
`created_at`	The creation date in ISO 8601 format.	`string($date-time)`
`updated_at`	The last modification date in ISO 8601 format.	`string($date-time)`

Attributes	Description	Values
`actual_bw`	The actual bandwidth.	`number($float)`
`actual_pps`	The actual packets per second.	`number($float)`
`configured_bw`	The configured bandwidth.	`number($float)`
`configured_pps`	The configured packets per second.	`number($float)`
`configured_bw_percentage`	The configured bandwidth as a percentage.	`number`
`configured_pps_percentage`	The configured packets per second as a percentage.	`number`
`peak_bw`	The peak bandwidth.	`number($float)`
`peak_pps`	The maximum packets per second.	`number($float)`
`total_bw`	The total bandwidth.	`number($float)`
`total_pps`	The total packets per second.	`number($float)`
`has_report`	Shows whether a report is available for the mitigation.	`true` `false`
`start_user`	The person who started the mitigation.	`object`
`end_user`	The person who ended the mitigation. This value is null while the mitigation is running.	`object`

2.3.3.4.4 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
304	The resource has not changed since the last request.
401	The request has not succeeded because the user authentication was incorrect.

STATUS CODE	DESCRIPTION
403	The request has not succeeded because the user does not have the right permissions.

2.3.4 Anomalies

2.3.4.1 Listing all anomalies of the organisation

> The anomalies feature must be enabled for the organisation. When it is disabled, the endpoint responds with the status code 403.

> SOC accounts cannot call this endpoint with a personal access token. Use the access via the web application (session authentication) instead.

Sends a `GET` request to the endpoint `/anomalies`.

2.3.4.1.1 Description

The List-Anomalies request allows you to request a paginated list of all historical anomalies of the organisation.

2.3.4.1.2 Requirements

Values of the request: none

Objects: none

2.3.4.1.3 Request

To request a list of all anomalies, no additional information needs to be added to the path of the request. To paginate, sort, and filter the list, you can append the following optional query parameters:

Attributes	Description	Values
`page`	The page to return.	`integer`, minimum `1`, default `1`
`perPage`	The number of anomalies per page.	`integer`, `1` to `100`, default `10`
`orderBy`	The attribute to sort by.	

Attributes	Description	Values
		`started_at` , `last_updated_at` , `ended_at` , `status` , `cidr` , `types` , default `started_at`
`orderDir`	The sort direction.	`asc` , `desc` , default `desc`
`search`	The free-text search over the `cidr` , `status` , and `types` attributes.	`string`
`status`	Only returns anomalies with this status.	`OPEN` , `UPDATE` , `CLOSED`
`type`	Only returns anomalies that contain this type.	`VOLUMETRIC` , `PROTOCOL` , `AMPLIFICATION`

As a result, you get one or more objects `AnomalyVO` with the requested information.

The object provides the following information:

Attributes	Description	Values
`id`	The ID of the anomaly.	`string`
`cidr`	The network or single IP address affected by the anomaly, in CIDR notation.	`string`
`types`	The detected anomaly types. An anomaly can carry more than one type.	`VOLUMETRIC` , `PROTOCOL` , `AMPLIFICATION`
`status`	The status of the anomaly.	`OPEN` , `UPDATE` , `CLOSED`
`started_at`	The date and time when the anomaly started in ISO 8601 format.	`string($date-time)`
`last_updated_at`	The date and time when the anomaly was last updated in ISO 8601 format.	`string($date-time)`

Attributes	Description	Values
`ended_at`	The date and time when the anomaly ended in ISO 8601 format. While the anomaly is ongoing, the value is `null`.	`string($date-time)`
`metadata`	Additional details about the anomaly, provided as a list of key-value entries.	`array`

Metadata entries flagged as private by the detecting system are never returned. The `metadata` attribute only contains public entries.

2.3.4.1.4 Example

Example response:


```
{
  "data": [
    {
      "id": "aB3xY9",
      "cidr": "203.0.113.0/24",
      "types": [
        "VOLUMETRIC"
      ],
      "status": "OPEN",
      "started_at": "2026-01-01T00:00:00+00:00",
      "last_updated_at": "2026-01-01T00:15:00+00:00",
      "ended_at": null,
      "metadata": [
        {
          "key": "attack_vector",
          "value": "UDP_Reflection"
        }
      ]
    }
  ]
}
```

2.3.4.1.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.
422	The request was unsuccessful because the submitted data could not be processed.

2.3.5 Mitigation reports

2.3.5.1 Listing mitigation statistics for a month

This request is available to super admin users only.

Sends a `GET` request to the endpoint `/mitigation-statistic-group/{group}`.

2.3.5.1.1 Description

The Get-Mitigation-Statistics request returns the mitigation statistics for a specified month of the organisation.

2.3.5.1.2 Requirements

Values of the request: **Month** `{group}`

Objects: none

2.3.5.1.3 Request

To request the mitigation statistics, add the **Month** `{group}` (in the format `YYYY-MM`) to the path of the request.

As a result, the user gets one or more objects `MitigationStatisticVO` with the requested information.

The object provides the following information:

Attributes	Description	Values
`org`	The name of the organisation.	`string`
`network`	The IP address or the CIDR of the mitigated network.	`string`
`start`	The date and time of the start of the mitigation, in ISO 8601 format.	`string($date-time)`
`end`	The date and time of the end of the mitigation, in ISO 8601 format.	`string($date-time)`
`trigger`		`1`

Attributes	Description	Values
	The trigger type of the mitigation: `1` started manually, `2` started automatically, `3` started by operations.	`2` `3`
`actual_bw`	The measured bandwidth in Mbps at the start of the mitigation.	`integer`
`configured_bw`	The configured bandwidth threshold in Mbps.	`integer`
`actual_pps`	The measured packets per second at the start of the mitigation.	`integer`
`configured_pps`	The configured packet rate threshold.	`integer`
`peak_bw`	The peak bandwidth observed during the mitigation, in Mbps.	`integer`
`peak_pps`	The peak packet rate observed during the mitigation.	`integer`
`total_bw`	The total bandwidth received during the mitigation, in bits.	`integer`
`total_pps`	The total packets received during the mitigation.	`integer`
`dropped_bits`	The total bits dropped by the mitigation.	`integer`
`dropped_packets`	The total packets dropped by the mitigation.	`integer`

2.3.5.1.4 Example

Example response:


```
{
  "data": [
    {
      "org": "Test Organisation",
      "network": "172.0.0.1",
      "start": "2026-01-01T00:00:00+00:00",
```

```
      "end": "2026-01-01T00:00:00+00:00",
      "trigger": 1,
      "actual_bw": 100,
      "configured_bw": 200,
      "actual_pps": 1500,
      "configured_pps": 2000,
      "peak_bw": 400,
      "peak_pps": 3000,
      "total_bw": 123456,
      "total_pps": 78910,
      "dropped_bits": 10000,
      "dropped_packets": 2000
    }
  ],
  "links": {
    "first": "https://datahub-api.com/api/networks?page=1",
    "last": "https://datahub-api.com/api/networks?page=5",
    "prev": null,
    "next": "https://datahub-api.com/api/networks?page=2"
  },
  "meta": {
    "current_page": 1,
    "from": 1,
    "last_page": 5,
    "links": [
      {
        "url": "https://datahub-api.com/api/networks?page=2",
        "label": "Next »",
        "active": false
      }
    ],
    "path": "https://datahub-api.com/api/networks",
    "per_page": 15,
    "to": 15,
    "total": 64
  }
}
```


2.3.5.1.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.

STATUS CODE	DESCRIPTION
403	The request has not succeeded because the user does not have the right permissions.

2.3.5.2 Listing all months with mitigation statistics

This endpoint is available to super admin users only.

Sends a `GET` request to the endpoint `/mitigation-statistic-groups`.

2.3.5.2.1 Description

The List-Mitigation-Statistic-Groups request returns a paginated list of all months for which mitigation statistics of the organisation are available.

2.3.5.2.2 Requirements

Values of the request: none

Objects: none

2.3.5.2.3 Request

To request a list of all months with mitigation statistics, no additional information is required in the path of the request.

As a result, the user gets one or more objects `MitigationStatisticGroupVO` with the requested information.

The object provides the following information:

Attributes	Description	Values
`id`	The month identifier of the entry in the format `YYYY-MM`.	`string`

2.3.5.2.4 Example

Example response:


```
{
  "data": [
    {
      "id": "2026-02"
    }
  ],
  "meta": {
    "current_page": 0,
    "last_page": 0,
    "per_page": 0,
    "total": 0
  }
}
```


2.3.5.2.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.

2.3.6 Country packet reports

2.3.6.1 Getting the country packet report for the current month

This endpoint does not use the regular DataHub API authentication. Authentication is performed with a separate static token (configuration value `COUNTRY_STATS_API_TOKEN`) that is transmitted as a Bearer token in the `Authorization` header.

Sends a `GET` request to the endpoint `/country-packet-reports`.

2.3.6.1.1 Description

The List-Country-Packet-Reports request allows the user to request the aggregated country packet report for the current month. For each country, the report contains the sum of the packets from the mitigations that ended in the reporting month, sorted by packet count in descending order.

The system re-aggregates the data every hour. The aggregation requires the feature flag `COUNTRY_STATS_ENABLED`; otherwise, the report stays empty.

2.3.6.1.2 Requirements

Values of the request: none

Objects: none

2.3.6.1.3 Request

To request the report for the current month, no additional information needs to be added to the path of the request.

As a result, the user gets a list of country entries in `data` and a `meta` object with details about the reporting period.

The country entries provide the following information:

Attributes	Description	Values
`country`	The ISO country code of the country.	`string`

Attributes	Description	Values
`packets`	The aggregated number of packets for the country in the reporting month.	`integer`

The `meta` object provides the following information:

Attributes	Description	Values
`period_start`	The first day of the reporting month in the format `YYYY-MM-DD`.	`string($date)`
`period_end`	The last day of the reporting month in the format `YYYY-MM-DD`.	`string($date)`
`last_updated_at`	The date and time of the last aggregation in ISO 8601 format; `null` if no data has been aggregated yet.	`string($date-time)`

2.3.6.1.4 Example

Example response:


```
{
  "data": [
    {
      "country": "DE",
      "packets": 3023924
    },
    {
      "country": "US",
      "packets": 953069
    },
    {
      "country": "NL",
      "packets": 561701
    }
  ],
  "meta": {
    "period_start": "2026-06-01",
    "period_end": "2026-06-30",
    "last_updated_at": "2026-06-30T23:05:00+00:00"
  }
}
```

2.3.6.1.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the `Authorization` header is missing or does not contain a Bearer token.
403	The request has not succeeded because the transmitted token is invalid.

2.3.6.2 Getting the country packet report for a specific month

This endpoint does not use the regular DataHub API authentication. Authentication is performed with a separate static token (configuration value `COUNTRY_STATS_API_TOKEN`) that is transmitted as a Bearer token in the `Authorization` header.

Sends a `GET` request to the endpoint `/country-packet-reports/{period}`.

2.3.6.2.1 Description

The Get-Country-Packet-Report request allows the user to request the aggregated country packet report for a specific month. For each country, the report contains the sum of the packets from the mitigations that ended in the reporting month, sorted by packet count in descending order.

2.3.6.2.2 Requirements

Values of the request: **Month** `{period}`

Objects: none

2.3.6.2.3 Request

To request the report for a specific month, add the **Month** `{period}` in the format `YYYY-MM` to the path of the request. A value in a different format leads to a 404 error.

As a result, the user gets a list of country entries in `data` and a `meta` object with details about the reporting period. The structure of the response is identical to the request for the current month. See **Getting the country packet report for the current month**.

For months without aggregated data, the response contains an empty `data` list; `last_updated_at` is `null` in this case.

2.3.6.2.4 Example

Example response:

```
{
  "data": [
    {
      "country": "DE",
      "packets": 3023924
    },
    {
      "country": "FR",
      "packets": 529490
    }
  ],
  "meta": {
    "period_start": "2026-05-01",
    "period_end": "2026-05-31",
    "last_updated_at": "2026-06-01T00:35:00+00:00"
  }
}
```

2.3.6.2.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the `Authorization` header is missing or does not contain a Bearer token.
403	The request has not succeeded because the transmitted token is invalid.
404	

STATUS CODE	DESCRIPTION
	The request was unsuccessful because the specified month does not have a valid format.

2.3.6.3 Getting the country packet report for the current day

This endpoint does not use the regular DataHub API authentication. Authentication is performed with a separate static token (configuration value `COUNTRY_STATS_API_TOKEN`) that is transmitted as a Bearer token in the `Authorization` header.

Sends a `GET` request to the endpoint `/country-packet-daily-reports`.

2.3.6.3.1 Description

The List-Country-Packet-Reports request allows the user to request the aggregated country packet report for the current day. For each country, the report contains the sum of the packets from the mitigations that ended on the reporting day, sorted by packet count in descending order.

The system re-aggregates the data every hour. The aggregation requires the feature flag `COUNTRY_STATS_ENABLED`; otherwise, the report stays empty.

2.3.6.3.2 Requirements

Values of the request: none

Objects: none

2.3.6.3.3 Request

To request the report for the current day, no additional information needs to be added to the path of the request.

As a result, the user gets a list of day entries in `data`. Each entry contains the date and the country entries in `countries`.

The entries provide the following information:

Attributes	Description	Values
`date`	The day for which the report is created.	`string($date)`
`country`	The ISO country code of the country.	`string`
`packets`	The aggregated number of packets for the country on the reporting day.	`integer`

2.3.6.3.4 Example

Example response:


```
{
  "data": [
    {
      "date": "2026-06-08",
      "countries": [
        {
          "country": "DE",
          "packets": 3023924
        },
        {
          "country": "US",
          "packets": 953069
        },
        {
          "country": "NL",
          "packets": 561701
        }
      ]
    }
  ]
}
```

2.3.6.3.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the `Authorization` header is missing or does not contain a Bearer token.
403	The request has not succeeded because the transmitted token is invalid.

2.3.6.4 Getting the country packet report for a specific day

This endpoint does not use the regular DataHub API authentication. Authentication is performed with a separate static token (configuration value `COUNTRY_STATS_API_TOKEN`) that is transmitted as a Bearer token in the `Authorization` header.

Sends a `GET` request to the endpoint `/country-packet-daily-reports/{period}`.

2.3.6.4.1 Description

The Get-Country-Packet-Report request allows the user to request the aggregated country packet report for a specific day. For each country, the report contains the sum of the packets from the mitigations that ended on the reporting day, sorted by packet count in descending order.

2.3.6.4.2 Requirements

Values of the request: **Day** `{period}`

Objects: none

2.3.6.4.3 Request

To request the report for a specific day, add the **Day** `{period}` in the format `YYYY-MM-DD` to the path of the request. A value in a different format leads to a 404 error.

As a result, the user gets a list of day entries in `data`. Each entry contains the date and the country entries in `countries`. The structure of the response is identical to the request for the current day. See **Getting the country packet report for the current day**.

For days without aggregated data, the response contains an empty `data` list.

2.3.6.4.4 Example

Example response:

```
{
  "data": [
    {
      "date": "2026-06-08",
      "countries": [
        {
          "country": "DE",
          "packets": 3023924
        },
        {
          "country": "US",
          "packets": 953069
        },
        {
          "country": "NL",
          "packets": 561701
        }
      ]
    }
  ]
}
```

2.3.6.4.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the `Authorization` header is missing or does not contain a Bearer token.
403	

STATUS CODE	DESCRIPTION
	The request has not succeeded because the transmitted token is invalid.
404	The request was unsuccessful because the specified day does not have a valid format.

2.3.7 Audit logs

2.3.7.1 Listing all audit log entries of the organisation

SOC accounts cannot call this endpoint with a personal access token. There is no organisation-related token equivalent. Use access through the web application (session authentication) instead.

Sends a `GET` request to the endpoint `/auditLogs`.

2.3.7.1.1 Description

The List-Audit-Logs request returns a list of all audit log entries of the organisation.

2.3.7.1.2 Requirements

Values of the request: none

Objects: none

2.3.7.1.3 Request

To request a list of all audit log entries, no additional information is required in the path of the request.

As a result, the user gets one or more objects `AuditLogVO` with the requested information.

The object provides the following information:

Attributes	Description	Values
`event`	The type of the logged event.	`string`
`resource`	The type of the resource affected by the event.	`string`
`resource_identifier`	The identifier of the affected resource.	`string`
`performed_by`	The name of the user who performed the action.	`string`
`parameters`		`object`

Attributes	Description	Values
	Additional parameters and details of the logged event.	
`created_at`	The date and time when the event was logged, in ISO 8601 format.	`string($date-time)`

2.3.7.1.4 Example

Example response:


```
{
  "data": [
    {
      "event": "string",
      "resource": "string",
      "resource_identifier": "string",
      "performed_by": "string",
      "parameters": {},
      "created_at": "2026-01-01T00:00:00+00:00"
    }
  ],
  "links": {
    "first": "https://datahub-api.com/api/networks?page=1",
    "last": "https://datahub-api.com/api/networks?page=5",
    "prev": null,
    "next": "https://datahub-api.com/api/networks?page=2"
  },
  "meta": {
    "current_page": 1,
    "from": 1,
    "last_page": 5,
    "links": [
      {
        "url": "https://datahub-api.com/api/networks?page=2",
        "label": "Next »",
        "active": false
      }
    ],
    "path": "https://datahub-api.com/api/networks",
    "per_page": 15,
    "to": 15,
    "total": 64
  }
}
```

2.3.7.1.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.

2.3.8 User management

2.3.8.1 Getting the account information of the authenticated user

Sends a `GET` request to the endpoint `/users/me`.

2.3.8.1.1 Description

The Get-Logged-User request returns the account information of the currently authenticated user.

2.3.8.1.2 Requirements

Values of the request: none

Objects: none

2.3.8.1.3 Request

To request the account information of the currently authenticated user, no additional information is required in the path of the request.

As a result, the user gets an object `UserVO` with the requested information.

The object provides the following information:

Attributes	Description	Values
`id`	The ID of the user.	`string`
`name`	The full name of the user.	`string`
`email`	The email address of the user.	`string`
`activeOrganisation`	The organisation context in which the token is used.	`object`

2.3.8.1.4 Example

Example response:

```
{
  "id": "xY9pQ5wR1",
```

```
  "name": "Max Mustermann",
  "email": "max@mustermann.de",
  "activeOrganisation": {
    "id": "xY9pQ5wR1",
    "name": "Test Organisation"
  }
}
```

2.3.8.1.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.

2.3.8.2 Changing the notification preference of the authenticated user

The notification preference is only available for an organisation with the anomalies feature enabled, and only for users who are neither a SOC administrator nor a SOC user. SOC administrators and SOC users add their email address to the notification recipient list of the relevant organisation instead.

Sends a `PATCH` request to the endpoint `/users/me/notification-preferences`.

2.3.8.2.1 Description

The Change-Notification-Preferences request allows you to change the mitigation and anomaly notification email preference of the authenticated user.

2.3.8.2.2 Requirements

Values of the request: none

Objects: `NotificationPreferencesV0`

2.3.8.2.3 Request

To change the notification preference, no additional information needs to be added to the path of the request.

For a detailed specification of which information is required to change the notification preference, define the object `NotificationPreferencesVO` with the following attributes in the body:

Attributes	Description	Values
`notificationsEnabled`	Indicates whether the user is opted in to mitigation and anomaly notification emails.	`true` , `false`

The system responds by returning the object `ApiUser` with the updated information.

The object provides the following information:

Attributes	Description	Values
`id`	The ID of the user.	`string`
`name`	The full name of the user.	`string`
`email`	The email address of the user.	`string`
`notificationsEnabled`	Indicates whether the user is opted in to mitigation and anomaly notification emails.	`true` , `false`
`activeOrganisation`	The organisation context the token operates in.	`object`

2.3.8.2.4 Example

Example request body:

```
{
  "notificationsEnabled": true
}
```

2.3.8.2.5 Responses

The following responses are available:

STATUS CODE	DESCRIPTION
200	The request has succeeded.
401	The request has not succeeded because the user authentication was incorrect.
403	The request has not succeeded because the user does not have the right permissions.
422	The request was unsuccessful because the submitted data could not be processed.

3. Troubleshooting

This chapter lists the messages of the Myra DataHub portal, their cause, and how to resolve them.

The portal reports an error in three places:

- **Below the input field** – as long as a value is not valid. The message disappears as soon as the value is correct.
- **As a notification at the edge of the screen** – after an action has failed. It names the action that failed.
- **As a page of its own** – when the application cannot carry out the request at all, for example because a permission is missing.

If the general message **There was an unexpected issue.** appears, the server did not answer the request. Repeat the action. If the message persists, note the time, the view, and the action before you report the error.

The messages appear in the language selected in the portal. This chapter quotes the English wording.

3.1 Login

Login fails

The login screen checks the email address and the password together. It therefore does not state which of the two entries is wrong.

Message	Cause	Remedy
We weren't able to log you in. Please check your login credentials.	The email address or the password is wrong.	Enter both again. Watch the capitalisation of the password and check whether the caps lock key is active.
These credentials do not match our records.	No user account exists for this email address.	Check the spelling of the email address. If the account does not exist yet, ask a person with administration rights to create it.
The provided password is incorrect.	The user account exists, but the password does not belong to it.	Reset the password using **Forgot your password?**.
Too many login attempts. Please try again in n seconds.	Per email address and IP address, 15 login attempts per minute are allowed.	Wait for the time stated. The block ends by itself; a further attempt does not extend it.

The login procedure is described in **Login**.

Two-factor authentication

Message	Cause	Remedy
The authentication code is not valid.	The code that you entered does not match or is no longer valid.	A code is valid for a short time only. Wait until the authenticator application generates the next code and enter that one. Also check whether the time on the device is correct — a deviating time produces invalid codes.

Message	Cause	Remedy
The provided two factor authentication code was invalid.	The same error when enabling two-factor authentication later on the **Profile** tab.	Repeat the entry with the next code.
Two-factor authentication is required to use this website.	Two-factor authentication is mandatory for this portal but is not set up for the user account yet.	Set up two-factor authentication. Without it, the portal remains locked.
You have not enabled two-factor authentication.	An action requires two-factor authentication, for example, the display of the recovery codes.	Enable two-factor authentication first.

The second factor is limited as well: after five entries per minute, the portal rejects further attempts. In that case, wait one minute.

If the authenticator application is unavailable — for example, after you changed the device — log in with **Use a recovery code** and one of the emergency recovery codes that you stored during the setup. Each code is valid once. If all codes are used or lost, only a person with administration rights can reset the user account.

The setup is described in **Enabling two-factor authentication**.

Resetting the password

Forgot your password? requests an email containing a reset link.

Message	Cause	Remedy
We have received your request to reset your password. You will receive an email with further instructions shortly.	The portal accepted the request.	Open the link in the email. If the email is missing, check the spam folder.

Message	Cause	Remedy
We can't find a user with that email address.	No user account exists for this email address.	Check the spelling. Use the address the invitation was sent to.
Please wait before retrying.	You made the request too soon after the previous one.	Wait a moment and request the link again.
This password reset token is invalid.	The link expired or someone already used it.	Request a new link and open it immediately after you receive it.
The token has expired. Please restart the process.	The link that activates the account or sets the password expired.	Start the procedure again from the beginning.

The password is not accepted

The new password must meet all of the following rules; if it breaks one, the screen names exactly that rule.

Message	Requirement
The password must be at least 12 characters long.	at least 12 characters
The password must contain at least one lowercase letter.	at least one lowercase letter
The password must contain at least one uppercase letter.	at least one uppercase letter
The password must contain at least one number.	at least one digit
The password must contain at least one these symbols: !@#$%^&*.	at least one of the characters `!@#$%^&*`
The password is not valid.	

Message	Requirement
	The password does not meet the rules, or it does not match the confirmation.

In addition, the portal checks the password against known data breaches. A password that appears there is rejected even if it meets all rules. Choose a different password in that case.

When you change the password on the **Profile** tab, **Incorrect password. Please try again.** refers to the current password, not to the new one.

3.2 Access and display

The portal shows an error page

If the portal cannot carry out a request, it replaces the view with an error page offering the **Back to dashboard** button.

Page	Message	Cause	Remedy
Access Denied	**Sorry, you don't have access to this page.**	The user account does not hold the role this view requires, or the view belongs to a different company.	Return to the dashboard. If you need the view for your work, ask a person with administration rights to check your role. Which role opens which view is listed under **Roles and permissions**.
Page not found	**Sorry, the page you are looking for doesn't exist or has been moved.**	The address is misspelled, or the object behind it has been deleted — a network whose address is still stored as a bookmark, for example.	Open the view through the navigation instead of through a bookmark.
Internal Server Error	**Sorry, an internal server error occurred.**	The request failed on the server.	Repeat the action after a short while. If the error persists, note the time and the action and report it.

The session has expired

If an action unexpectedly returns you to the login screen, the session has expired. Without activity, a session ends after 120 minutes by default; the operator of the portal can change this value. Closing the web browser does not end the session.

- Log in again.
- Carry out the action once more. Entries you made before the session expired and did not save are lost.

On the **Profile** tab, **Browser sessions** shows which sessions are still open; **Log out other browser sessions** ends them. If you feel your user account has been compromised, end the other sessions and change your password immediately.

A view stays empty

An empty list is not an error: the portal shows only the data of the company you are currently logged in to, and only the selected period.

Message	Meaning	Remedy
No data currently available.	No measurements exist for the selected period.	Select a longer observation period.
No networks found.	No network is assigned to the company.	Ask the SOC to assign the network.
There is no mitigation history.	No mitigation was carried out in the selected period.	Extend the period.
No reports found.	No mitigation report has been generated yet.	A report is created only after a mitigation has finished.
No audit log found.	No change subject to logging was made in the selected period.	Extend the period or reset the filter.
No anomalies found.	No anomaly was detected in the selected period.	Extend the period.

If a view stays empty although data is expected, first check whether you are logged in to the correct company.

3.3 Networks and mitigations

A manual mitigation cannot be started

Message	Cause	Remedy
Cannot change the manual mitigation setting while there is an ongoing manual mitigation.	A manual mitigation is already running for the network.	End the running mitigation and change the setting afterwards.
This IP address doesn't belong to the selected network.	The IP address entered lies outside the address range of the network.	Enter an address from the range of the network. Leave the field empty to mitigate the entire network.
Invalid ip.	The entry is not a valid IP address.	Enter a complete IPv4 or IPv6 address without spaces.
The network(s) couldn't be mitigated.	The job failed on the server.	Repeat the start after a short while. Before that, check whether a mitigation is already running for the network.

If the **Start mitigation** button is missing entirely, manual mitigation is not enabled for this network, or your user account does not hold administration rights. Only the SOC can change either.

A mitigation cannot be stopped

If the portal reports **The mitigation(s) couldn't be stopped.**, the server did not accept the job. Repeat it after a short while.

Only manually started mitigations can be stopped. A mitigation triggered automatically ends by itself once the attack subsides.

3.4 User accounts

An account cannot be added

Message	Cause	Remedy
This user already belongs to the company.	A user account already exists for this email address in the company.	Look for the account in the list. If it is to receive different rights, change the role instead of creating a second account.
Failed to add the user to the company.	The server did not create the account.	Check the email address and repeat the procedure.
This field is required.	A mandatory field is empty.	Fill in the marked field.
The value can be up to 255 characters long.	The entry is too long.	Shorten the value to 255 characters at most.
The changes couldn't be saved.	The server did not apply the change.	Repeat the procedure. Afterwards, check in the list whether the change has been applied.

The procedure is described in **Adding an account**.

The invited person receives no email

A newly created account stays in the **Pending** state until the invited person accepts the invitation and sets a password.

- ▶ Check the spelling of the email address in the list.
- ▶ Ask the recipient to check their spam folder.
- ▶ Send the invitation again using the **Resend invitation** icon.
- ➔ The portal confirms with **The invitation has been successfully sent to the user.**

If the portal reports **The invitation couldn't be resent to the user.** instead, sending has failed. Repeat it after a short while. If the invitation link has already expired for the

recipient — recognisable by the message **The token has expired. Please restart the process.** — send the invitation again as well.

The SIEM connection cannot be established

The **SIEM Settings** tab checks the connection only when you click.

Message	Cause	Remedy
The connection couldn't be established.	The host, the port, or the API token is wrong, or the destination cannot be reached from the portal.	Check the host and the port. Enter the API token again — a stored token is only shown as **(stored)** and cannot be read back. Then have someone check whether a firewall is blocking the connection.
The connection could be established.	The entries are correct.	Save the settings.

Further details on the tab are given in **SIEM Settings tab**.

3.5 API access

An API token cannot be created

Message	Cause	Remedy
Must be a whole number between 1 and 90.	The validity period lies outside the permitted range.	Enter a whole number between 1 and 90 days.
This field is required.	The name of the token is missing.	Assign a name by which you will recognise the token later.
There was a problem creating the token. Please try again.	The server did not create the token.	Repeat the procedure.
There was a problem deleting the token. Please try again.	The server did not delete the token.	Repeat the procedure.

Please copy your new API token. For your security, it will not be shown again. If you did not copy the token before closing the dialog, it cannot be read back afterwards. Delete it and create a new one.

The procedure is described in **Creating an API token**.

The API rejects a request

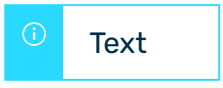
Response	Cause	Remedy
`400 Bad Request`	The request is incomplete or contains an invalid value.	The returned `ViolationVO` object names the field and the reason. Correct the value and send the request again.
`401 Unaut`	The bearer token is missing, misspelled, or expired.	Check the `Authorization: Bearer <token>` header. A

Response	Cause	Remedy
`horized`		token is valid for 90 days at most; after that, create a new one.
`403 Forbidden`	The user account behind the token lacks the permission for this endpoint — or the identifier in the path does not exist or belongs to a different company. The API answers both the same way so that it does not disclose identifiers of others.	First check the identifier in the path, then the role of the user account.
`429 Too Many Requests`	240 requests per minute are allowed, counted per user account.	Spread the requests over time. Evaluate the `Retry-After` header of the response and repeat the request afterwards.

The complete list is given in **Possible responses to a request**.

4. Reference

4.1 Notational conventions

Formatting	Description
Text in bold	Identifies screen elements from the graphical user interface.
Links	Identifies references to chapters and sections within the manual, as well as external sources.
`Text in monospace`	Identifies commands, code, and input.
`<ABC>`	Identifies placeholders to be filled in by the customer or the system.
☑	Indicates prerequisite steps that users must fulfill before performing a procedure.
▶	Indicates steps that users should perform.
▷	Indicates subordinate steps that users should perform.
↳	Indicates the interim result for checking after one or more steps have been performed.
➔	Indicates the result that should be obtained after performing several steps.
	Identifies important information to support users.
	Identifies particularly important information that, if not observed, can lead to incorrect settings or data loss.
	Identifies examples to support users.

4.2 Configuration via YAML

In addition to managing companies and users through the graphical interface of the Myra DataHub, you can also make all configurations by means of YAML files.

In order for the creation of companies, their users, and their networks to function, the instructions must be submitted as YAML in the following format.

```yaml
custname: 'Client A'
timestamp: 2025-02-27 143232
portal:
  enabled: true
  email: noc@myrasecurity.com
  lastname: Myra
  forename: Security
1.1.1.1/32:
  enabled: true
  email:
    - noc@myrasecurity.com
  pps_limit: 500000
  bw_limit: 4000
  duration: 14400
  type: ACTION_BLACKHOLE
  wholenet:
    enabled: true
  nettype: RIPE (PI)
  extra:
    INTERNET-SERVICEKENNUNG: L2220001
    CUSTNETNAME: Network 1
    DIENST-ID: HWDDSxxx
    DEBITOR: Debitor 2
    CHANNEL: 1000
    DETAILS: Description for the network
```

You can only add companies and one user with admin rights each using the YAML file. Changing and deleting is not possible via YAML and must be done in the graphical user interface.

You can use the YAML file to add, modify, or delete one or more networks for a company.

> You cannot enable the SIEM (Security Information and Event Management) integration with the YAML file for companies. SIEM can only be enabled for a company through the graphical user interface of the Myra DataHub.

The values transferred in YAML format correspond to the information in the graphical user interface of the Myra DataHub and can be assigned as follows:

Element	Description
Company accounts	

NAME	CUSTOMER ID
Muster GmbH	10024

YAML - Company accounts

Element	Description
User management	

EMAIL ADDRESS
max.mustermann@example.com

YAML - User Management 1

NAME	ROLE
Max Mustermann	Administrator

YAML - User Management 2

Element	Description
Networks	

NAME	IP ADDRESS	NETWORK TYPE
Network 1	XXX.XXX.XXX.XXX/24	RIPE (PI)
Network 2	XXX.XXX.XXX.XXX/24	RIPE (LIR)

YAML - Networks

Below you will find a table showing the assignment of all values in the YAML file and on the graphical user interface:

Comparison of the fields in the Myra DataHub UI with the YAML file

Myra DataHub UI	YAML	Description
Company		
Name	`Custname`	Customer name
Customer ID	`Name der YAML-Datei`	Customer's unique ID
User management		
Email Address	`Portal: email`	Email address of the first admin account. **Note:** When adding a new company via the YAML file, only one user with admin rights is created. Additional accounts can only be added via the graphical user interface.
Name	`portal: lastname`	Name of the first admin account.
Name	`portal: forename`	First name of the first admin account.
	`portal: enabled`	Only in YAML: Defines whether an admin account is created for the new company. The following values are available: `true` : An admin account is created. `false` : An admin account is not created.
Networks		
Name	`extra: CUSTNETNAME`	The name of the network.
IP	`CIDR`	The IP address of the network.
Packet Rate	`pps_limit`	The threshold value for the maximum number of packets allowed per second.

Myra DataHub UI	YAML	Description
Threshold (Packets/s)		
Dienst-ID	`extra: DIENST-ID`	A Versatel-specific value.
CHANNEL	`extra: CHANNEL`	A Versatel-specific value.
Network type	`nettype`	The network type for the corresponding network. The following values are available: `RIPE` : Uses the Regional Internet Registry for Europe (RIPE) as the network type. `RIPE (PI)` : Uses the Provider Independent Address Space (PI address space) as the network type. `RIPE (LIR)` : Uses the Local Internet Registry (LIR) as the network type. `RIPE (AS8881)` : Uses Versatel's autonomous system (AS) as the network type. `SUBNET` or `Subnet` : Uses a self-defined IP address range as the network type.
Network Reference	`extra: INTERNET-SERVICEKENNUNG`	Contains the unique L-number for the Internet line through which customers are connected to Versatel.
Bandwidth Threshold (MBit/s)	`bw_limit`	The threshold value for the maximum possible bandwidth.
Duration to Maintain Mitigation (in Sec)	`duration`	The duration of mitigation in seconds after traffic has fallen below the thresholds.

Myra DataHub UI	YAML	Description
Debitor	`extra: DEBITOR`	A Versatel-specific value.
Details	`extra: DETAILS`	A custom comment on the description of the network.
Mitigation type	`type`	Defining how mitigation will be carried out. The following values are available: **ACTION_BLACKHOLE**: If the threshold value is exceeded, all traffic is discarded. **ACTION_MITIGATE_ONPREM**: If the threshold value is exceeded, the traffic is filtered via the internal servers. **ACTION_MITIGATE_CLOUD**: If the threshold is exceeded, the traffic is cleaned via the Myra Scrubbing Center.
Mitigation Strategy	Wholenet: enabled	Defines whether only a single IP address or the entire network is automatically mitigated. The following values are available: `IP` : Only a single IP address of the network is automatically mitigated. `CIDR` : The entire network is automatically mitigated.
Notification email address	email	The email address of the user to whom mitigation notifications are sent.
Auto Actions	enabled	Indicates whether automatic mitigation is performed for the selected network or not. The following values are available: `true` : Automatic mitigation is enabled. `false` : Automatic mitigation is disabled.

4.3 Glossary

Element	Description
Scrubbing	Scrubbing refers to the process of filtering Internet traffic, particularly at OSI layers ¾, in such a way that valid clean traffic is distinguished from harmful attack traffic.
Scrubbing Center	A scrubbing center is a high-performance Internet node (point of presence/ PoP) consisting of hardware, software, and broadband connectivity that is capable of performing scrubbing efficiently using Myra technology.
Myra Partner	An ISP is a Myra customer that uses the Myra product Network DDoS Protection (on-prem) and has implemented it within its own network.
End customer	An end customer is the customer of a Myra partner that uses the volumetric DDoS protection service for OSI layers ¾ **powered by Myra**.
Network DDoS Protection (cloud)	Cloud scrubbing is a service provided by Myra in the form of Security-as-a-Service (SaaS) that protects the network of the Myra partner from volumetric DDoS attacks on OSI layers ¾. **Functionality:** As soon as parameters defined in advance are exceeded, the (attack) traffic is briefly rerouted into a cloud scrubbing center by means of Border Gateway Protocol (BGP) rerouting and **washed clean** of unwanted traffic there, so that only clean traffic is forwarded to the recipient over a secured connection. **Advantages:** Network DDoS Protection (cloud) can reliably defend against DDoS attacks with a bandwidth of several Tbit/s. This defence bandwidth is always available to the Myra partner, even if it exceeds the total line capacity (bandwidth) of the Myra partner's own physical connection. It is irrelevant

Element	Description
	whether the entire line capacity of the Myra partner is physically implemented by one line provider or by several (multi-vendor strategy). This DDoS protection is also retained if the Myra partner changes line provider in the future or adds further ones. **Restriction:** For technical reasons, protection through Network DDoS Protection (cloud) is only possible for individual /24 prefixes with IPv4 and /48 prefixes with IPv6. Because of the restriction to exactly these sizes that generally applies on the public internet, networks smaller than /24 or /48 cannot be protected through cloud scrubbing.
Network DDoS Protection (on-premises)	Myra provides its partner with one or more physical scrubbing centers, which are integrated into the network infrastructure of the Myra partner. This ensures that all routers involved in routing relevant to scrubbing are controlled by Myra or the Myra partner. This also makes it possible to define valid routes for smaller prefixes (that is, networks smaller than /24 or /48) without causing problems for public routing.
Network DDoS Protection (hybrid)	Network DDoS Protection (hybrid) is a combination of the OnPrem and Cloud network DDoS protection solutions. If the bandwidth of a DDoS attack exceeds the line capacity (of one or of several physical connections) of the Myra partner, the resources of Myra can be used as a second line of defence and a switch can be made from Network DDoS Protection (on-prem) to Network DDoS Protection (cloud), in order to reliably defend against volumetric DDoS attacks on OSI layers ¾ with bandwidths of several Tbit/s as well. This enables Myra partners to ensure that their own servers and networks, as well as those of their end customers, remain accessible even during DDoS attacks with extremely high bandwidths.
Myra Flow-	The Myra Flow Application is an application that detects DDoS attacks on the basis of the data supplied by the edge routers of the Myra partner and thresholds defined beforehand. The Flow-Monitoring reports detected attacks to downstream instances to automatically initiate countermeasures.

Element	Description
Application	The application is operated in the network infrastructure of the Myra partner, usually on a virtual machine.
Uplink	An uplink is a dedicated channel for returning the cleaned traffic to the Myra partner after scrubbing has been completed. This channel is necessary to avoid a routing loop. Uplinks can be set up redundantly as direct connect (physical) or as VLAN, IPsec, GRE (virtual).
On Demand	On demand means that traffic filtering is only activated once an attack exceeds the specified thresholds. Normally, traffic does not flow through the scrubbing center. With automatic attack detection, routing is changed and data traffic is processed there. After 24 hours, regular routing is restored – a period recommended by Myra to prevent unnecessary route flapping.
Route flapping	Route flapping refers to the state of different announced routes on the internet at the same time. This is dangerous and has far-reaching negative consequences for routing on the public Internet.
Myra Data Hub	The Myra DataHub is a web-based user interface (WebGUI) for Myra partners to view an overview of end customers. This shows the end customers with the connected networks and their created accounts. Within this WebGUI, end customers have an overview of traffic history, the networks that have been activated, and the mitigation reports that have been collected. Within the traffic history view, it is possible to filter between bandwidth and packet rate, sorted by destination IP, overview of source countries, ASN, and packet rates by port. In addition, various viewing periods of up to 24 hours can be defined. The set thresholds can also be viewed via the WebGUI. In addition, the functionality of the Myra DataHub includes the option of initiating manual mitigation and configuring the defined companies, networks, and users by the Myra partner.