Control Panel Manual for Administrators

Contents

General Information

About this Manual

This manual is intended for Control Panel administrators. It contains information on its usage as well as on administrative tasks.

The administrative rights are divided into two levels:

- Customer-level administrator: Is responsible for a primary domain and all corresponding alias domains and email addresses.
- Partner-level administrator: Is responsible for several customers. Each customer consists of a primary domain and all corresponding alias domains and email addresses.

Notice:

The modules and functions to which a user has access depend on their permissions. Therefore, some of the modules and functions described herein may not be available to some users.

First, this manual provides the following basic information about the Control Panel: The Control Panel is the user interface for using and configuring our services (see Introduction on page 8) and is supported by various browsers (see Prerequisites on page 8).

The Control Panel is updated on a regular basis to introduce new features and improvements. The current version number can be retrieved from the Control Panel (see Checking the Version Number on page 9). Changes to a version are summarized in the release notes (see Version Information on page 9). In addition, users can contact our support via the Control Panel (see Submitting a Support Request by Chat).

Additionally, this manual explains the first steps in the Control Panel: To access the Control Panel, users must first log in (see Logging in on page 10). Each user has their own user settings and can edit them (see User Settings on page 21). Administrators can also manage the permissions of users (see Rights Management in the Control Panel on page 49).

Later in this manual, the modules of the Control Panel are described in detail:

- **Email Live Tracking** (see Email Live Tracking on page 58)
- **Service Dashboard** (see About the Service Dashboard on page 97)
- **Reporting & Compliance** (see Reporting & Compliance on page 156)
- **Web Filter** (see Downloading the Web Filter)
- **Customer Settings** (see Customer Settings on page 210)
- **Backup** (see #unique_15)
- **Deny & Allow Lists** (see About Deny & Allow Lists on page 308)
- **Security Settings** (see Security Settings)
- **Customization** (see Control Panel Customization on page 593)

The classification reasons based on which emails are assigned to a category in the Control Panel are also presented (see Classification reasons on page 612).

Basic Information on the Control Panel

Introduction

The Control Panel is the user interface for using and configuring our services. The main functionality of the Control Panel is to monitor and control emails.

The Control Panel supports users in handling received emails and in evaluating email traffic. For example, users can report emails as spam and deliver emails previously reported as spam. You can also add senders to the deny or allow list (see Email Actions on page 87).

The Control Panel is developed as a web application in responsive design and can therefore be operated from mobile devices as well as from desktop computers.

Prerequisites

Control Panel is supported by the following browsers:

- Google Chrome version 55

- Mozilla Firefox version 50
- Microsoft Edge version 38 and higher
- Apple Safari version 9

Important:

The private mode of the listed browsers is not supported.

Version Information

The Control Panel is updated on a regular basis to introduce new features and improvements. Every version is assigned a version number (see Checking the Version Number on page 9). The enhancements and improvements of a version are described in release notes. The current release notes are available here. A link to the release notes can also be found below the version number in the Control Panel.

Checking the Version Number

In the Control Panel, you can check the number of the current Control Panel version. Below the version number, there is also a link to the release notes (see Version Information on page 9).

1. Log in to the Control Panel with your credentials.
2. Click on ℹ next to the user settings in the upper right corner of the window.

   ➜

   The current version number is displayed in the lower right corner of the Control Panel. Below the version number, there is a link to the release notes.
3. Optional: If you would like to open the release notes, click on the link below the version number.

   ➜

   A page with the release notes opens.

✓

The version number has been checked.

First Steps in the Control Panel

Logging in

Your administrator has added your mailbox to the Control Panel (see Adding a Mailbox on page 216).

> **Notice:**
>
> Administrators can also deactivate user mailboxes in the Control Panel (see Activating or Deactivating a Mailbox on page 236). Users with deactivated mailboxes cannot log in to the Control Panel.

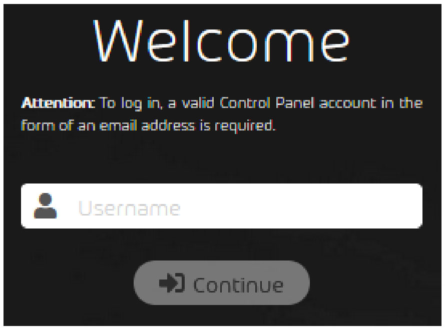
In order to access the Control Panel, you must log in to the Control Panel.

> **Notice:**
>
> For security reasons, a user is notified by email when multiple login attempts have failed for their account in a row. The first notification is sent after 5 failed login attempts. Another notification is sent after 8 failed login attempts, whereupon access is blocked for 24 hours. After each additional failed login attempt, another notification is sent and access is blocked again for 24 hours.

1. Enter the URL of the Control Panel website in your browser to log in to the Control Panel.

   ➔

   The login page is displayed.



Welcome

Attention: To log in, a valid Control Panel account in the form of an email address is required.

Figure 1: Control Panel login

2. Enter your username in the **Username** field.

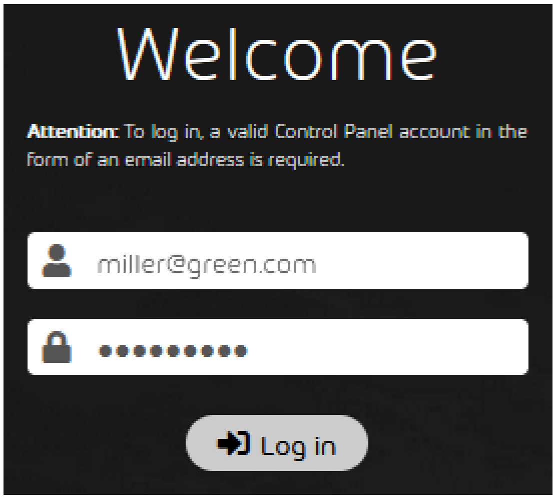
> **Notice:**
>
> Enter your personal email address as the username. After a new registration, you will receive your credentials from your partner or Support.

3. Click on **Continue**.

> **Notice:**
>
> If you have forgotten your password and your mailbox is not synchronized with a directory service via LDAP in the Control Panel, you can reset your password (see Resetting a Password on page 18).

4. Follow these steps if your password is managed in the Control Panel or if you log in to the Control Panel with your credentials from a directory service via LDAP.

   a) Enter your password in the **Password** field.



Welcome

Attention: To log in, a valid Control Panel account in the form of an email address is required.

miller@green.com

●●●●●●●●●

Figure 2: Enter password

   b) Click on **Log in**.

➜

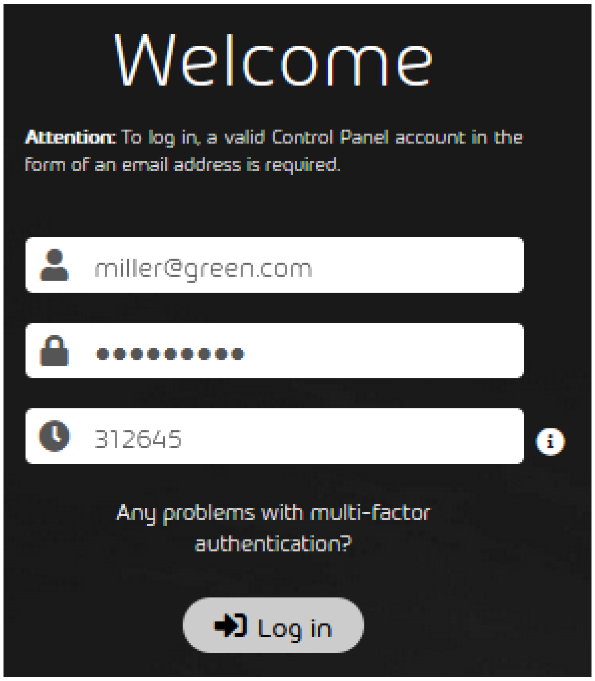
If multi-factor authentication is not configured for the account, the Control Panel opens. When you log in to the Control Panel for the first time, a window for selecting a timezone, a language, a date format and a time format is displayed.

If the login is performed for an administrator account and multi-factor authentication is being enforced for administrators (see "Enforcing Multi-Factor Authentication for Administrators" in the Control Panel manual), the administrator must configure multi-factor authentication for their account (see Configuring Multi-Factor Authentication from step 7 on page 28).

If multi-factor authentication is configured for the account (see Configuring Multi-Factor Authentication on page 26) the **One-time password** field is displayed. To log in using multi-factor authentication, more steps are required.

c) If multi-factor authentication is configured for your account, open your authenticator app on your mobile device.

d) Enter the current one-time password from the authenticator app in the **One-time password** field.



Welcome

Attention: To log in, a valid Control Panel account in the form of an email address is required.

miller@green.com

●●●●●●●●●

312645

Figure 3: Enter one-time password

e) Click on **Log in**.

Notice:

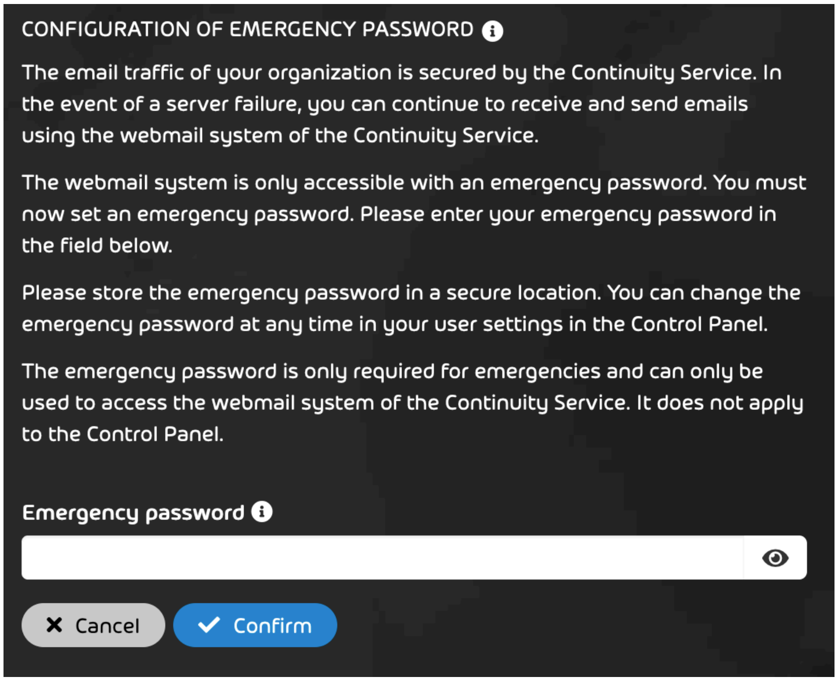
If you experience problems with multi-factor authentication, the administrator can reset multi-factor authentication for the account (see Troubleshooting: Problems with Multi-Factor Authentication on page 20 and "Resetting Multi-Factor Authentication" in the Control Panel manual).

➔

The Control Panel opens. If the partner has published an end-user license agreement and a data processing agreement, the agreements are displayed. When you log in to the Control Panel for the first time, a window for selecting a timezone, a language, a date format and a time format is displayed.

5. If you are prompted to set an emergency password, enter a password in the **Emergency password** field. You can use this password to log in to our webmail system in case your

organization's email server fails. After setting the emergency password for the first time, you can change it in your user settings (see Changing the Emergency Password on page 24).



CONFIGURATION OF EMERGENCY PASSWORD

The email traffic of your organization is secured by the Continuity Service. In the event of a server failure, you can continue to receive and send emails using the webmail system of the Continuity Service.

The webmail system is only accessible with an emergency password. You must now set an emergency password. Please enter your emergency password in the field below.

Please store the emergency password in a secure location. You can change the emergency password at any time in your user settings in the Control Panel.

The emergency password is only required for emergencies and can only be used to access the webmail system of the Continuity Service. It does not apply to the Control Panel.

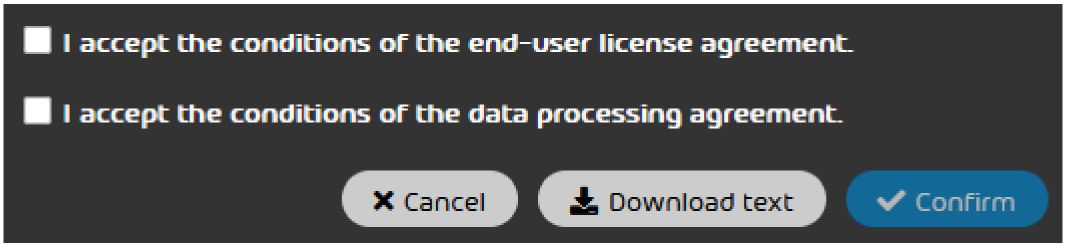
Figure 4: Set emergency password

6. **Important:**

   Partners can publish an end-user license agreement and a data processing agreement in the Control Panel (see "Terms and Conditions" in the Control Panel manual). Every user must accept the end-user license agreement once in order to access the Control Panel.

   If an end-user license agreement and a data processing agreement are displayed, agree to their terms.

   a) Tick the **I accept the conditions of the end-user license agreement.** checkbox.



□ I accept the conditions of the end-user license agreement.

□ I accept the conditions of the data processing agreement.

Figure 5: Accept the end-user license agreement

   b) **Important:**

   The agreements will not be displayed in the Control Panel again after the user has accepted them.

   Optional: If you would like to save the text of the agreements, click on **Download text**.

   ➜

   The agreements are exported as a .txt file and provided for download.

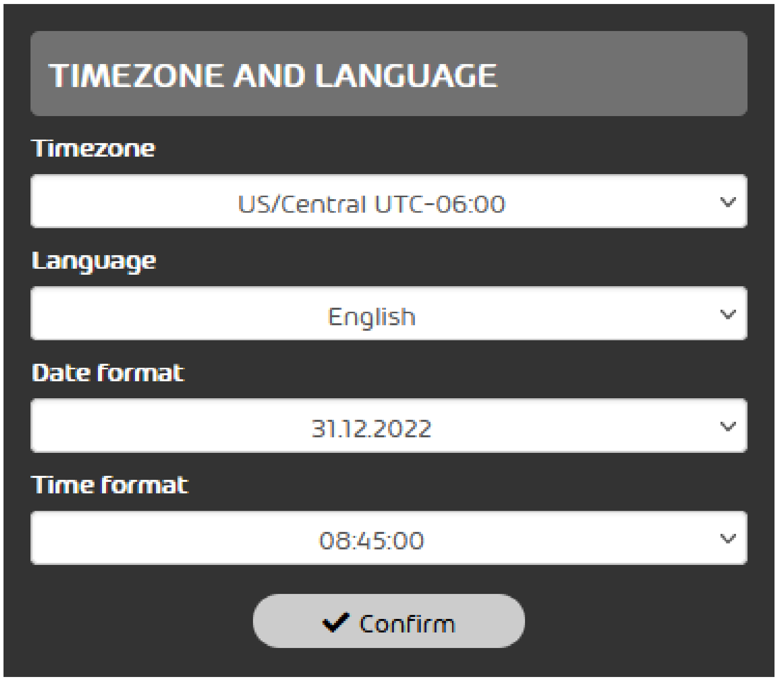
   c) Optional: If you have downloaded the text of the agreements, save the .txt file on your file system.

   d) Click on **Confirm**.

   ➜

   The terms are accepted.

7. If you log in to the Control Panel for the first time, select a timezone, language, date format and time format from the drop-down menus and click on **Confirm**.



TIMEZONE AND LANGUAGE

Timezone: US/Central UTC-06:00

Language: English

Date format: 31.12.2022

Time format: 08:45:00

Figure 6: Select settings

Notice:

For more information on the settings, see Changing the Timezone and Language on page 35. You can change the settings at any time in your user settings.

The Control Panel login has been performed.

Notice:

You will be automatically logged out of the Control Panel after 24 hours of inactivity if you do not log yourself out before.

Resetting a Password

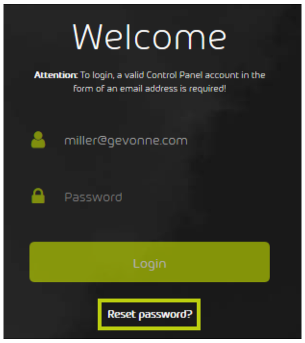
Your account is not synchronized via LDAP.

Notice:

If your account is synchronized via LDAP, you cannot reset your password by yourself. To reset your password, contact your administrator.

If you forget your password for the Control Panel, you can reset it.

1. Open the Control Panel login page.
2. Enter your email address.
3. Click on **Reset password?**.



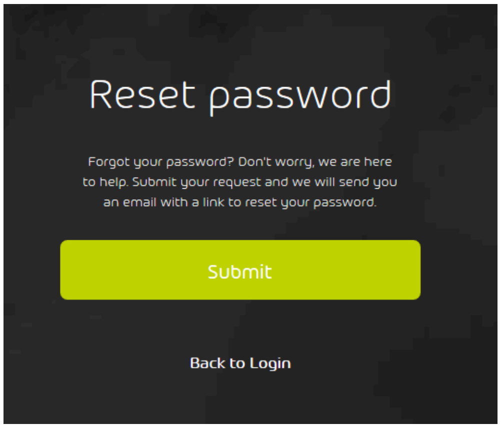
Welcome

Attention: To login, a valid Control Panel account in the form of an email address is required!

miller@gevonne.com

Figure 7: Reset password

4. Click on **Submit**.



Reset password

Forgot your password? Don't worry, we are here to help. Submit your request and we will send you an email with a link to reset your password.

Figure 8: Confirm resetting the password

➜

You get an email with a new password and a link to reset your password.

> **Notice:**
>
> The link is valid for one hour.

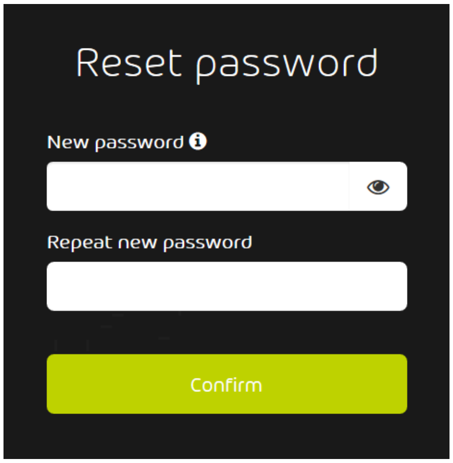
5. Open the email and click on the link.

➜

A window with the application form for the Control Panel opens.

6. Enter a new password and repeat it.

7. Click on **Submit**.



Reset password

New password

Repeat new password

Figure 9: Repeat the new password

✓

The password has been changed. You can now log in to the Control Panel with your new password.

- If the link for resetting your password has expired, click again on **Submit**. You will receive a new link.

Troubleshooting: Problems with Multi-Factor Authentication

Problem

Multi-factor authentication is configured for your Control Panel account (see Configuring Multi-Factor Authentication on page 26). You cannot log in to the Control Panel.

Reason

You cannot retrieve the one-time password that is required for the Control Panel login from your authenticator app on your mobile device because you no longer have access to the app or the mobile device.

Solution

Contact your administrator.

➔

The administrator resets multi-factor authentication for the account (see chapter "Resetting Multi-Factor Authentication" in the Control Panel manual). The configuration of multi-factor authentication is deleted for the account. From now on, only the Control Panel password is required to log in to the Control Panel. It is possible to reconfigure multi-factor authentication (see Configuring Multi-Factor Authentication on page 26).

User Settings

In the user settings, users can manage their personal settings. The user settings can be accessed via the gear wheel icon in the upper right corner of the Control Panel (see Opening the User Settings on page 22). The user settings contain general settings regarding a user's password, their emergency password for the webmail system of the Continuity Service (see About the Continuity Service on page 588), multi-factor authentication, basic data, timezone and language. Furthermore, API tokens, out of office notes and settings for quarantine reports can be managed.

Users whose passwords are managed in the Control Panel can change their password (see Changing the Password on page 23). If the administrator allows it (see "Enabling Multi-Factor Authentication" in the Control Panel manual), users whose passwords are managed in the Control Panel or in a directory service via LDAP can configure multi-factor authentication for their account (see Configuring Multi-Factor Authentication on page 26). This increases security for the Control Panel login. If desired, users can also deactivate multi-factor authentication for their account again (see Deactivating Multi-Factor Authentication on page 31).

Users whose mailboxes are not synchronized with a directory service via LDAP in the Control Panel can edit their basic data (see Editing Basic Data on page 37). For users of LDAP mailboxes (see Mailbox Types on page 215), the basic data is synchronized with the directory service. Users with these mailboxes can view their basic data but cannot edit them.

Each user can select a timezone, language, date format and time format (see Changing the Timezone and Language on page 35). The settings apply to the Control Panel display and to automatic emails from the Control Panel.

Administrators and users with the **Service Desk** role can create API tokens that allow applications to access the Control Panel through the API (see Creating an API Token on page 39). API tokens can also be deleted from the Control Panel again (see Deleting an API Token on page 42), which makes them invalid.

Furthermore, users can create out of office notes (see Creating an Out-of-Office Note on page 43) to automatically inform the senders of their incoming emails about their absences. If the administrator allows it, users can also edit the settings for their own quarantine reports (see Configuring Quarantine Reports on page 45).

Opening the User Settings

You can open your user settings (see User Settings on page 21) in the Control Panel. In the user settings, you can manage general settings such as your timezone and your language (see Changing the Timezone and Language on page 35) as well as API tokens (see Creating an API Token on page 39 and Deleting an API Token on page 42), out of office notes (see Creating an Out-of-Office Note on page 43) and settings for your quarantine reports (see Configuring Quarantine Reports on page 45).

1. Log in to the Control Panel with your credentials.
2. Click on ⚙ in the upper right corner of the Control Panel.

➜

The user settings are displayed.

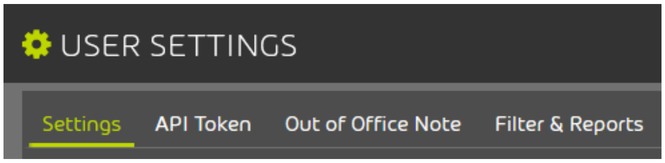


Figure 10: User settings

✓

The user settings have been opened.

Settings

Changing the Password

If your mailbox is not synchronized with a directory service via LDAP, you can change your Control Panel password in your user settings (see User Settings on page 21).

Notice:

Users of LDAP mailboxes (see Mailbox Types on page 215) can log in to the Control Panel with their credentials from the directory service. Thus, these users cannot change their passwords in the Control Panel. The password settings are hidden for these users.

1. Log in to the Control Panel with your credentials.
2. Click on ⚙ in the upper right corner of the Control Panel.

   ➜

   The user settings are displayed.

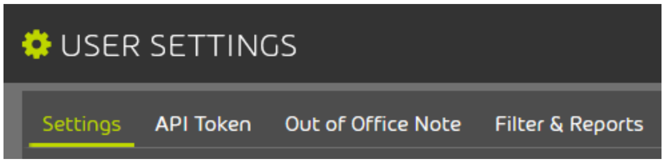
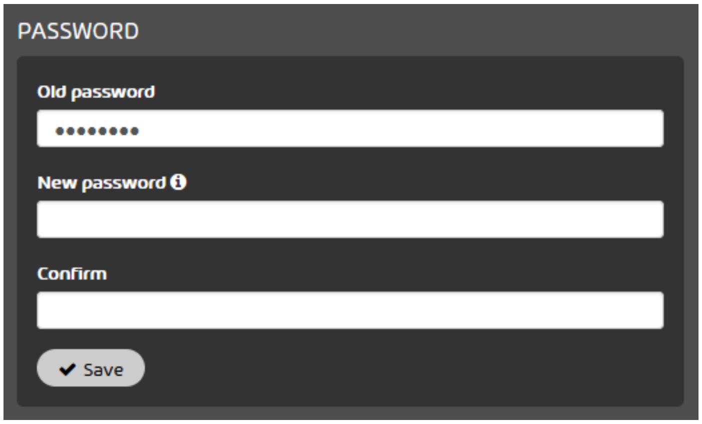


Figure 11: User settings

3. Select the **Settings** tab.

4. Enter your current password in the **Old password** field.



PASSWORD

Old password

••••••••

New password ℹ

Confirm

✔ Save

Figure 12: Enter the old password

5. Enter your new password in the **New password** field.

> **Important:**
>
> New passwords must contain at least one uppercase letter, one lowercase letter, one digit and one special character. Additionally, new passwords must have a minimum length that has been set by a customer-level or partner-level administrator. In any case, passwords must consist of at least 8 characters.

6. Repeat the new password in the **Confirm** field.

7. Click on **Save**.

   The new password is saved. For security reasons, the user is notified by email when the password is changed.

The password has been changed.

Changing the Emergency Password

1. Log in to the Control Panel with your credentials.
2. Click on ⚙ in the upper right corner of the Control Panel.

   ➜

   The user settings are displayed.

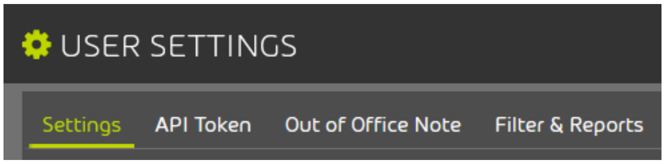


Figure 13: User settings

3. Select the **Settings** tab.
4. Enter your new emergency password in the **Emergency password** field.

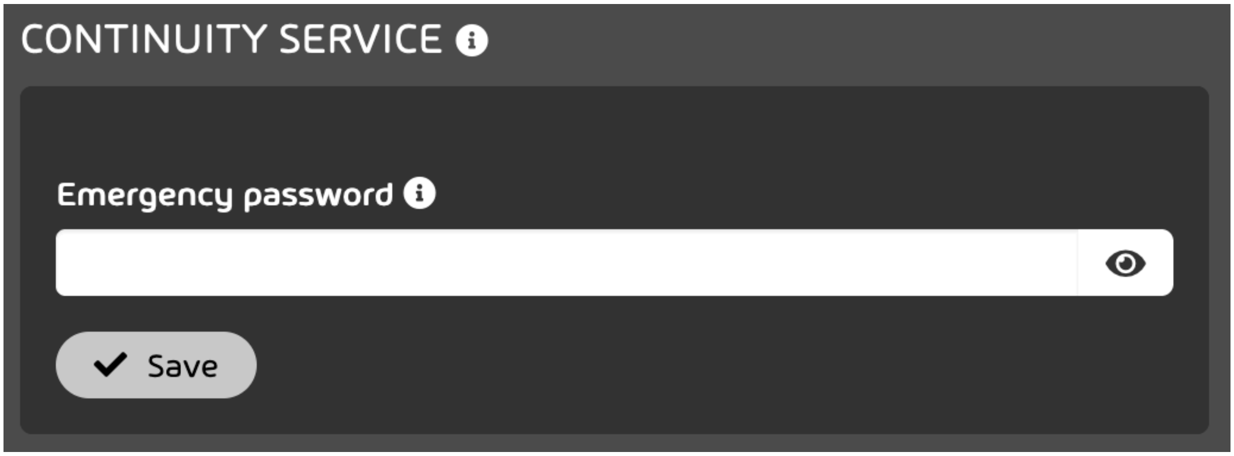


Figure 14: Change emergency password

5. Click on **Save**.

   ➜

   The new emergency password is saved.

✓

The new emergency password has been changed.

Configuring Multi-Factor Authentication

Your Control Panel credentials are managed in the Control Panel or in a directory service via LDAP. Your administrator has enabled multi-factor authentication for the users of your domain (see "Enabling Multi-Factor Authentication" in the Control Panel manual). You have installed a TOTP authenticator app (e.g., Microsoft Authenticator, Google Authenticator) on your mobile device.

You can configure multi-factor authentication for your Control Panel account. Multi-factor authentication increases security for the Control Panel login. We recommend in particular that administrators use multi-factor authentication.

Multi-factor authentication in the Control Panel uses the TOTP method. TOTP stands for time-based one-time passwords. In order to log in to the Control Panel using multi-factor authentication, you must enter a one-time-password from an authenticator app in addition to the Control Panel password (see Logging in on page 10).

1. Log in to the Control Panel.
2. Click on ⚙ in the upper right corner of the Control Panel.

   ➔

   The user settings are displayed.

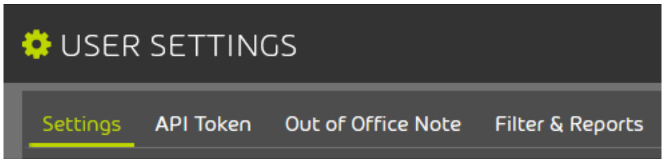
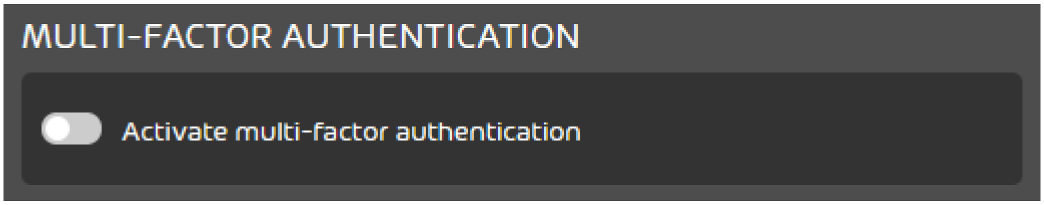


Figure 15: User settings

3. Select the **Settings** tab.

4. Toggle the switch **Activate multi-factor authentication** under **Multi-Factor Authentication**.



MULTI-FACTOR AUTHENTICATION

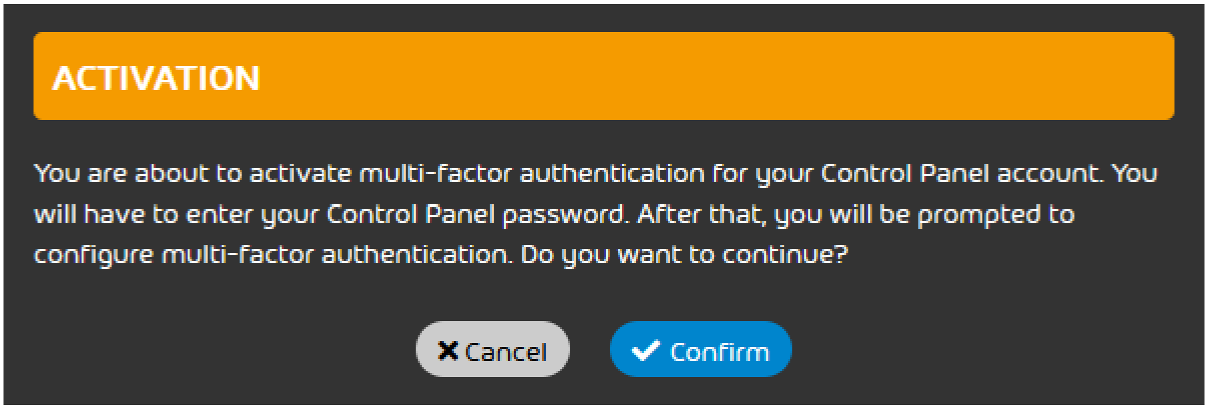
Activate multi-factor authentication

Figure 16: Activate multi-factor authentication

➜

The button turns green and a confirmation window opens.

5. Click on **Confirm**.



ACTIVATION

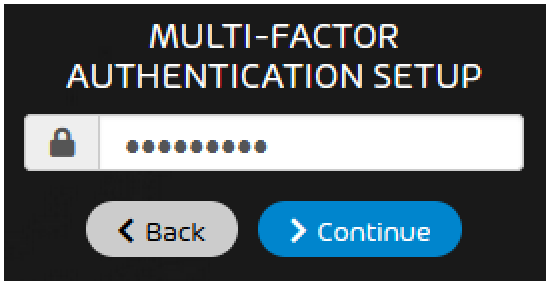
You are about to activate multi-factor authentication for your Control Panel account. You will have to enter your Control Panel password. After that, you will be prompted to configure multi-factor authentication. Do you want to continue?

Figure 17: Confirm

➜

The page **Multi-factor authentication setup** is displayed.

6. Enter your Control Panel password in the input field.



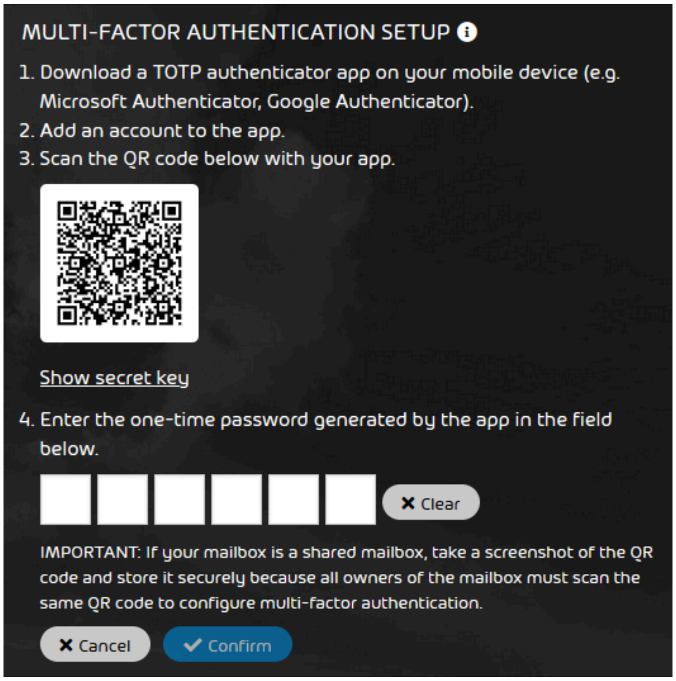
MULTI-FACTOR AUTHENTICATION SETUP

Figure 18: Enter password

7. Click on **Continue**.

➜

A page with instructions on how to configure multi-factor authentication is displayed.



MULTI-FACTOR AUTHENTICATION SETUP

1. Download a TOTP authenticator app on your mobile device (e.g. Microsoft Authenticator, Google Authenticator).
2. Add an account to the app.
3. Scan the QR code below with your app.

Show secret key

4. Enter the one-time password generated by the app in the field below.

IMPORTANT: If your mailbox is a shared mailbox, take a screenshot of the QR code and store it securely because all owners of the mailbox must scan the same QR code to configure multi-factor authentication.

Figure 19: Multi-factor authentication setup

8. Open your authenticator app on your mobile device.

> **Notice:**
>
> Some browsers support authenticator plug-ins. Users who do not have a mobile device at their disposal can use an authenticator plug-in in the browser on their PC instead of an authenticator app.

9. Add a new account to the authenticator app.

10.

> **Important:**
>
> A QR code or secret key is required to configure multi-factor authentication. The QR code is displayed only once in the Control Panel. The secret key can also be displayed only once in the Control Panel.
>
> If multi-factor authentication is configured for a shared mailbox, all owners of the mailbox must use the same QR code or secret key to configure multi-factor authentication in their authenticator app. Thus, the first person to configure multi-factor authentication for the mailbox must take a screenshot of the QR code or save the secret key and make it available to the other owners of the mailbox.

Optional: If you would like to configure multi-factor authentication with the QR code, proceed as follows.

a) If your mailbox is a shared mailbox, create a screenshot of the QR code from the Control Panel and store it safely.

b) Scan the QR code from the Control Panel with the authenticator app.

➡

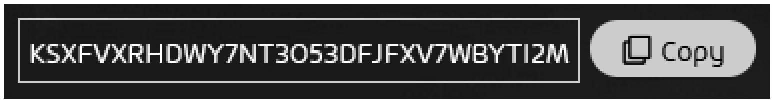
The authenticator app generates a new six-digit one-time password every 30 seconds.

11. Optional: If you would like to configure multi-factor authentication with the secret key, proceed as follows.

a) Click on **Show secret key**.

➜

The secret key is displayed.



KSXFVXRHDWY7NT3O53DFJFXV7WBYTI2M

Figure 20: Secret key

b) Click on **Copy**.

➜

The secret key is copied to the clipboard.

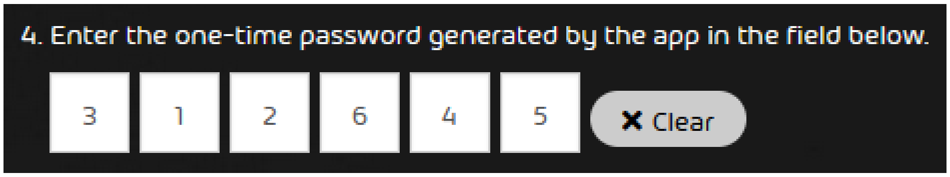
c) If your mailbox is a shared mailbox, save the secret key and store it safely.

d) Enter the secret key in the authenticator app.

➜

The authenticator app generates a new six-digit one-time password every 30 seconds.

12. Enter the current one-time password from the authenticator app in the input mask in the Control Panel.



4. Enter the one-time password generated by the app in the field below.

3 1 2 6 4 5

Figure 21: Enter one-time password

13. Optional: If you would like to empty the input mask in order to be able to enter a different one-time password, click on **Clear**.

    ➜

    The input mask is cleared.

14. Click on **Confirm**.

    ➜

    Multi-factor authentication is configured. From now on, the Control Panel login uses multi-factor authentication.

✓

Multi-factor authentication has been configured.

Next, you can log in to the Control Panel using multi-factor authentication (see Logging in on page 10). If you no longer want to use multi-factor authentication, you can deactivate multi-factor authentication for your account (see Deactivating Multi-Factor Authentication on page 31).
If you have problems with multi-factor authentication, you can contact your administrator (see Troubleshooting: Problems with Multi-Factor Authentication on page 20).

Deactivating Multi-Factor Authentication

You have configured multi-factor authentication for your Control Panel account (see Configuring Multi-Factor Authentication on page 26).

If you no longer want to use multi-factor authentication, you can deactivate multi-factor authentication for your Control Panel account. Multi-factor authentication increases security for the Control Panel login because a one-time password from an authenticator app is required in addition to the Control Panel password.

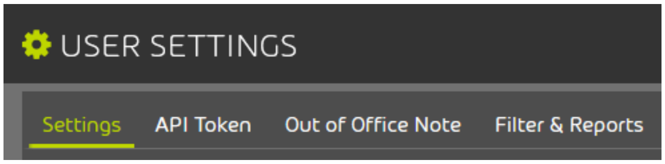
> **Notice:**
>
> We recommend in particular that administrators use multi-factor authentication.

1. Log in to the Control Panel.

2. Click on ⚙ in the upper right corner of the Control Panel.

   ➜

   The user settings are displayed.

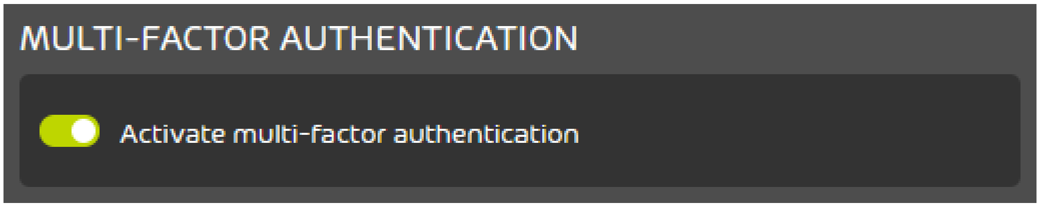


USER SETTINGS

Settings | API Token | Out of Office Note | Filter & Reports

Figure 22: User settings

3. Select the **Settings** tab.
4. Toggle the switch **Activate multi-factor authentication** under **Multi-Factor Authentication**.



MULTI-FACTOR AUTHENTICATION

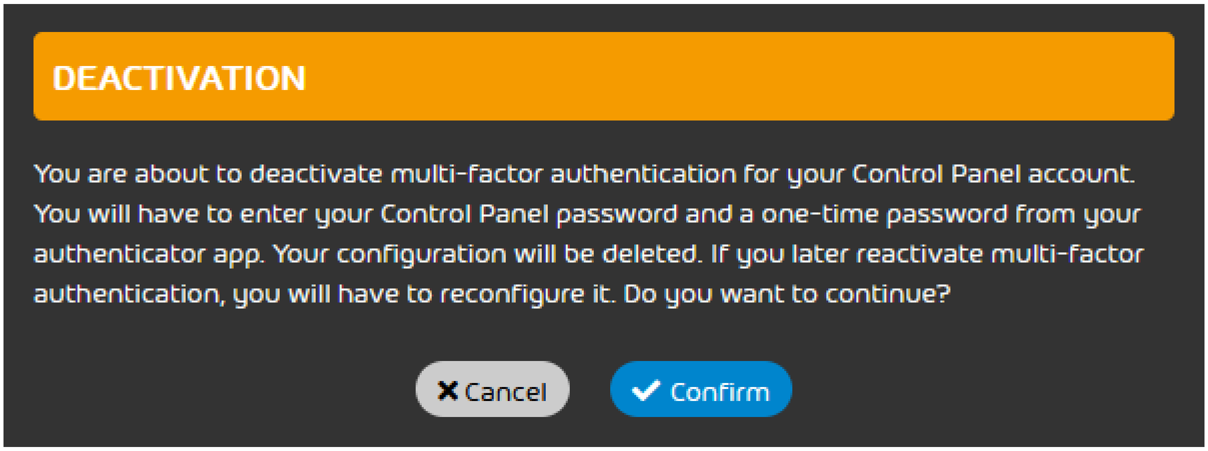
Activate multi-factor authentication

Figure 23: Deactivate multi-factor authentication

➜

The switch is grayed out and a confirmation window opens.

5. Click on **Confirm**.



DEACTIVATION

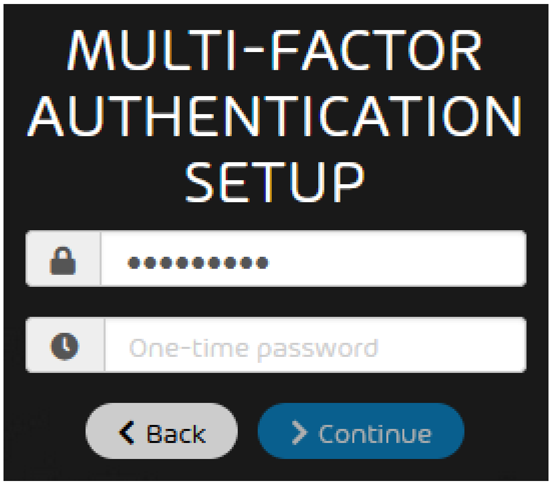
You are about to deactivate multi-factor authentication for your Control Panel account. You will have to enter your Control Panel password and a one-time password from your authenticator app. Your configuration will be deleted. If you later reactivate multi-factor authentication, you will have to reconfigure it. Do you want to continue?

Figure 24: Confirm

➜

The page **Multi-factor authentication setup** is displayed.

6. Enter your Control Panel password in the upper field.

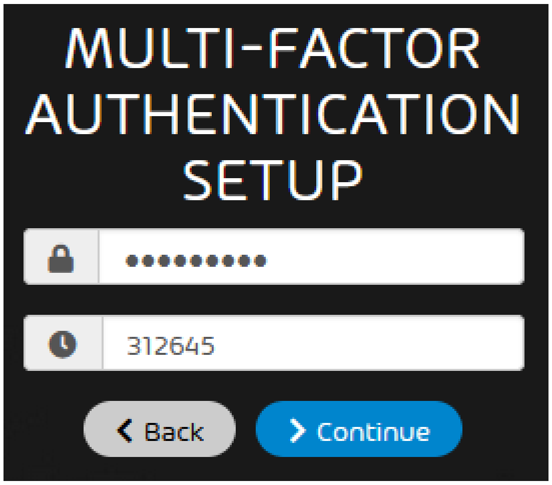


MULTI-FACTOR AUTHENTICATION SETUP

Figure 25: Enter password

7. Open your authenticator app on your mobile device.

8. Enter the current one-time password from the authenticator app in the lower field.



MULTI-FACTOR AUTHENTICATION SETUP

●●●●●●●●●●

312645

Figure 26: Enter one-time password

➜

The button **Continue** is enabled.

9. Click on **Continue**.

➜

Multi-factor authentication has been deactivated for the account. The configuration of multi-factor authentication is deleted for the account. From now on, the Control Panel login no longer requires a one-time password from an authenticator app.

10. Optional: Delete the account for multi-factor authentication from your authenticator app.

✓

Multi-factor authentication has been deactivated for the account.

Next, you can log in to the Control Panel without using multi-factor authentication (see Logging in on page 10). If you would like to later use multi-factor authentication again, you can reconfigure multi-factor authentication (see Configuring Multi-Factor Authentication on page 26).

Changing the Timezone and Language

In your user settings (see User Settings on page 21) you can change the timezone, language, date format and time format. These settings apply to the Control Panel display and to automatic emails from the Control Panel.

Notice:

Each user selects a timezone, language, date format and time format the first time they log in to the Control Panel. Users can change these settings at any time in the user settings.

1. Log in to the Control Panel with your credentials.
2. Click on ⚙ in the upper right corner of the Control Panel.

➔

The user settings are displayed.

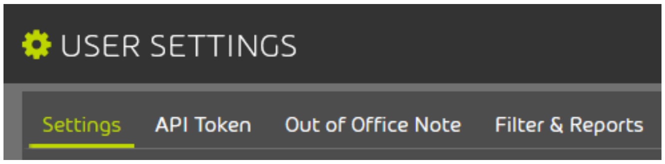
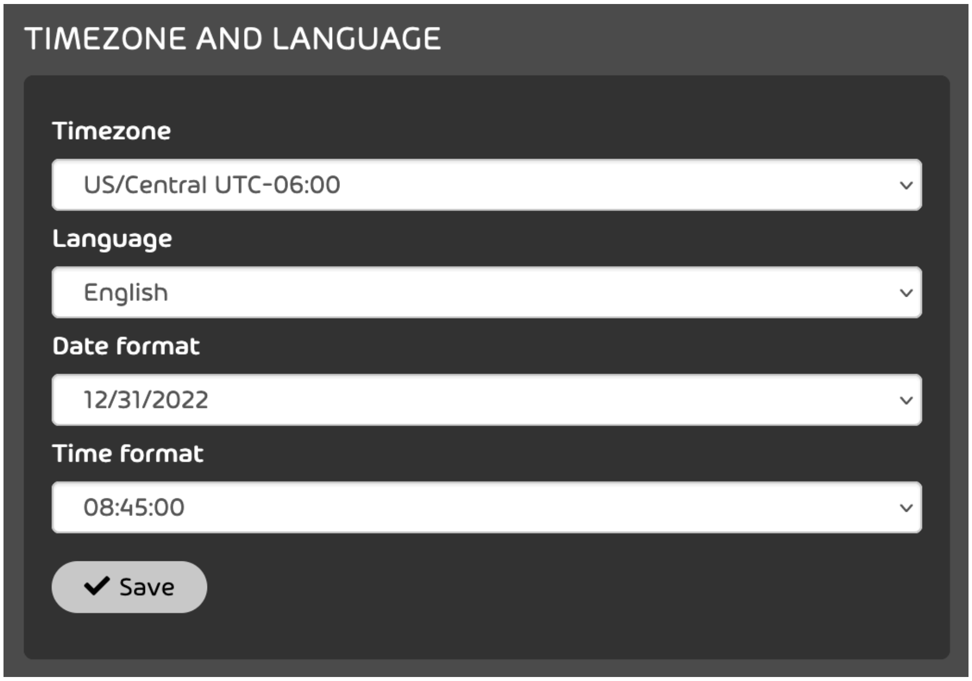


Figure 27: User settings

3. Select the **Settings** tab.

   ➡

   The section **Timezone and language** displays the settings for the timezone, language, date format and time format.



TIMEZONE AND LANGUAGE

Timezone: US/Central UTC-06:00

Language: English

Date format: 12/31/2022

Time format: 08:45:00

Figure 28: Timezone and language

4. Select a timezone from the drop-down menu **Timezone**.

> **Notice:**
>
> The timezone determines the number format in the Control Panel and in automatic emails from the Control Panel.

5. Select a language from the drop-down menu **Language**.

6. Select a date format from the drop-down menu **Date format**.

> **Notice:**
>
> The date format determines the order in which the available details of a date are displayed. If information is not available for all details, the missing details will not be displayed.

7. Select a time format from the drop-down menu **Time format**.

> **Notice:**
>
> The time format determines the order in which the available details of a time are displayed. If information is not available for all details, the missing details will not be displayed.

8. Click on **Save**.

   The changes are saved.

The timezone, language, date format and time format have been changed.

Editing Basic Data

Under **User Settings** (see User Settings on page 21), you can edit the basic data of your mailbox. The basic data contains information about the owner of a mailbox.

> **Notice:**
>
> Users of LDAP mailboxes (see Mailbox Types on page 215) cannot edit their basic data in the Control Panel. If basic data is stored for these mailboxes in the directory service, this data is displayed in the Control Panel.

1. Log in to the Control Panel with your credentials.

2. Click on ⚙ in the upper right corner of the Control Panel.

   ➔

   The user settings are displayed.

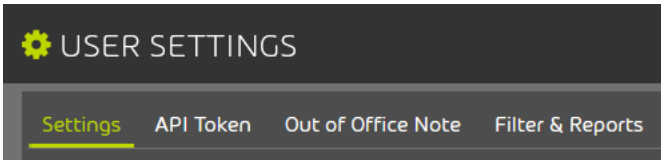


Figure 29: User settings

3. Select the **Settings** tab.

   ➔

   In the upper area of the page, the **Basic data** section is displayed.

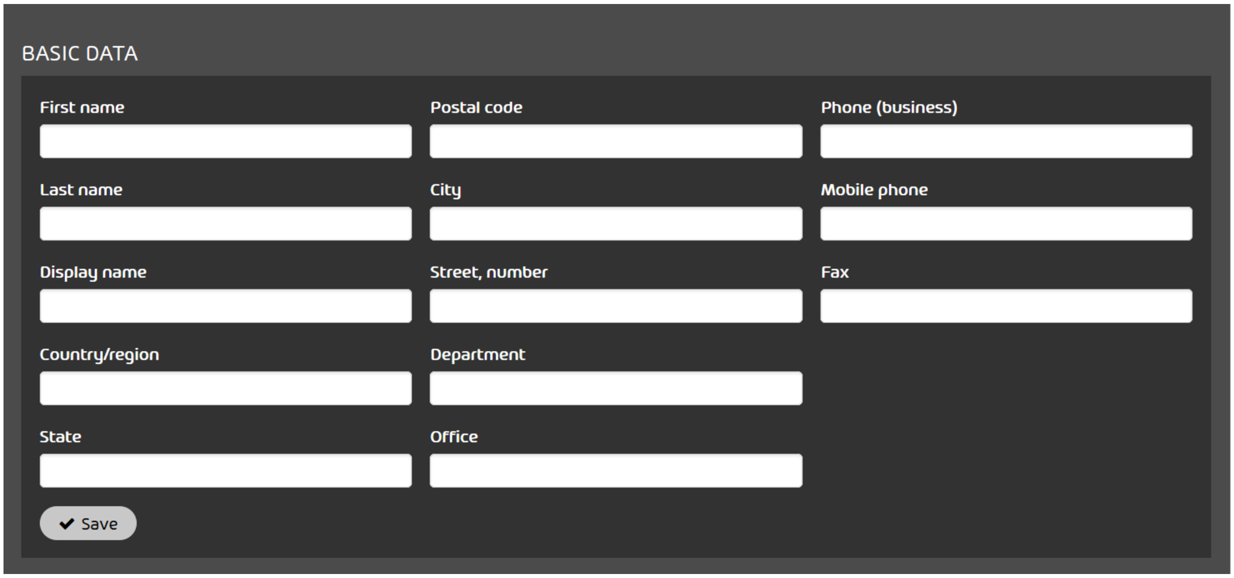


Figure 30: Basic data

4. **Notice:**

   All fields are optional.

   Enter your data in the fields. The fields have the following meanings:

   - **First name**: your first name
   - **Last name**: your last name
   - **Display name**: your display name in the Control Panel
   - **Country/Region**: country or region where your company is based
   - **State**: state where your company is based
   - **Postal code**: postal code of your company
   - **City**: city where your company is based
   - **Street, number**: street and house number where your company is based
   - **Department**: department to which you belong
   - **Office**: office in which you work
   - **Phone (business)**: your business phone number
   - **Mobile phone**: your mobile phone number
   - **Fax**: your fax number

5. Click on **Save**.

   ➜

   The changes are saved.

✓

The basic data has been edited.

Creating an API Token

With an API token, you can grant applications access to the Control Panel API. Each application needs its own token. In your user settings (see User Settings on page 21), you can create an API token for authorization in the Control Panel.

1. Log in to the Control Panel with your administrative credentials.
2. Click on ⚙ in the upper right corner of the Control Panel.

   ➜

   The user settings are displayed.

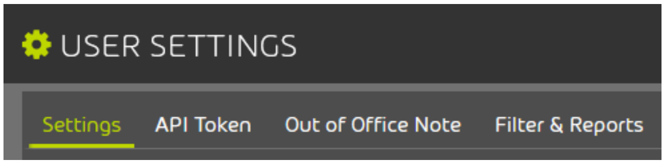
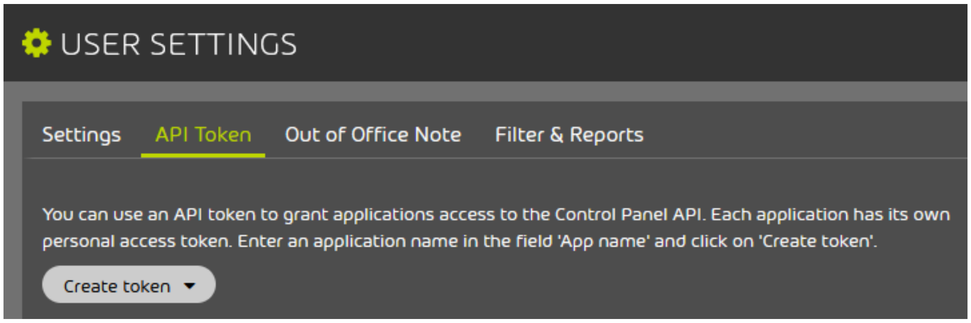


Figure 31: User settings

3. Select the **API Token** tab.
4. Click on **Create token**.



You can use an API token to grant applications access to the Control Panel API. Each application has its own personal access token. Enter an application name in the field 'App name' and click on 'Create token'.

Figure 32: Create token

➜

Additional settings are displayed.

5. In the **App Name** field, enter a name for the application that will use the token.

> **Notice:**
>
> The actions performed with this token will be recorded in the **Auditing 2.0** module under the name of the user who created the token.

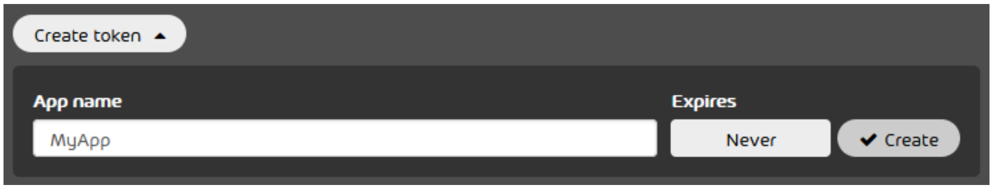


Figure 33: Enter app name

6. Optional: Under **Expires**, select an expiration date for the token.

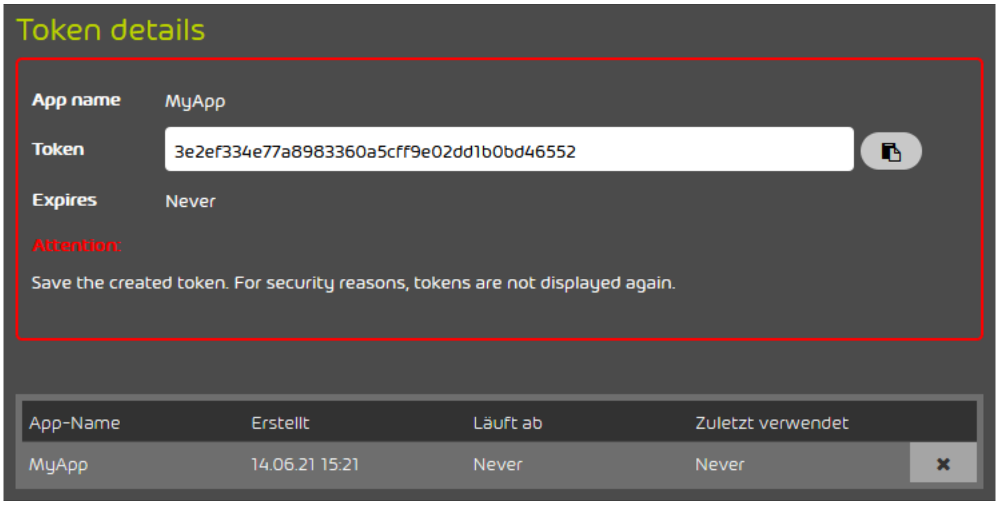
> **Notice:**
>
> **Never** is selected as the default value.

7. **CAUTION:**

   For security reasons, the token is only displayed once. If you do not save the token, it will be lost. Please save the token right away.

   Click on **Create**.

   The API token is created and displayed.



Token details

App name: MyApp

Token: 3e2ef334e77a8983360a5cff9e02dd1b0bd46552

Expires: Never

Attention:

Save the created token. For security reasons, tokens are not displayed again.

App-Name	Erstellt	Läuft ab	Zuletzt verwendet	
MyApp	14.06.21 15:21	Never	Never	✖

Figure 34: Created token

An API token has been created.

If you no longer need an API token, you can delete it from the Control Panel (see Deleting an API Token on page 42).

Deleting an API Token

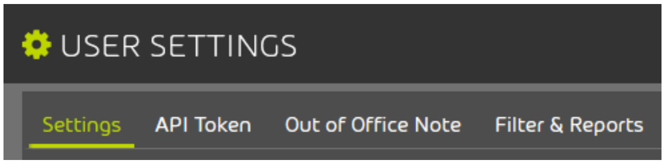
You have created an API token (see Creating an API Token on page 39).

If you no longer need an API token before its expiration date, you can delete it from your user settings in the Control Panel (see User Settings on page 21). This action invalidates the token. The API token can then no longer be used to access the API of the Control Panel.

1. Log in to the Control Panel with the credentials of the user who originally created the token.
2. Click on ⚙ in the upper right corner of the Control Panel.

   ➔

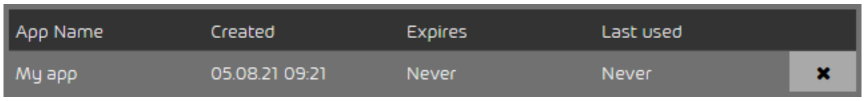
   The user settings are displayed.



USER SETTINGS

Figure 35: User settings

3. Select the **API Token** tab.
4. Select the token that you would like to delete from the list.



App Name	Created	Expires	Last used	
My app	05.08.21 09:21	Never	Never	✖

Figure 36: Select token

5. Click on the cross next to the token.

   ➔

   The token is deleted from the system.

✓

An API token has been deleted from the system and invalidated.

Creating an Out-of-Office Note

You can add a personal out-of-office note to your email account in your user settings (see User Settings on page 21). You can write a custom text for the out-of-office note, and activate or deactivate the out-of-office note at any time. Once you activate the out-of-office note, all senders of your incoming emails will receive an automatic reply about your absence.

1. Log in to the Control Panel with your credentials.
2. Click on ⚙ in the upper right corner of the Control Panel.

   ➔

   The user settings are displayed.

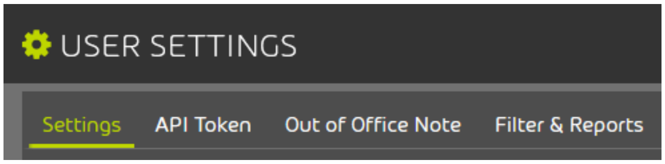
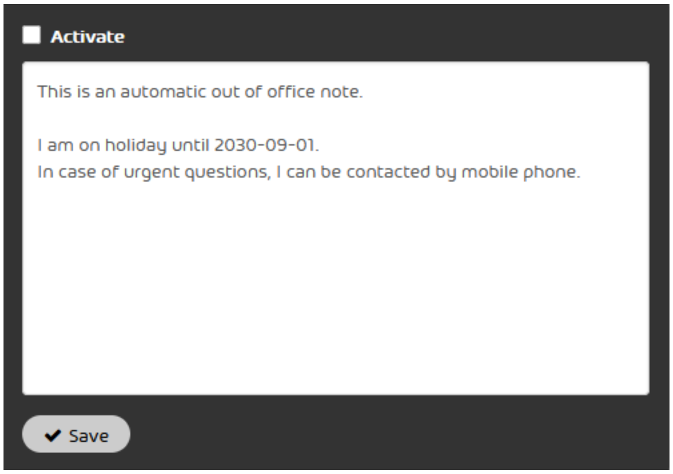


Figure 37: User settings

3. Select the **Out of Office Note** tab.
4. Enter a text for the out-of-office note in the text field.



This is an automatic out of office note.

I am on holiday until 2030-09-01.
In case of urgent questions, I can be contacted by mobile phone.

Figure 38: Enter text

5. Click on **Save**.

   ➔

   The text of the out-of-office note is saved.

6. Optional: To activate the out-of-office note, tick the checkbox **Activate**.

   ➜

   The out-of-office note is activated. From now on, automatic emails with the out-of-office note are sent to the senders of incoming emails.

✓

An out-of-office note has been created.

Configuring Quarantine Reports

If your administrator has allowed it, you can activate or deactivate the infomail filter for your own mailbox as well as adjust the settings of your quarantine reports. You can edit these settings in your user settings (see User Settings on page 21).

If the infomail filter is activated, incoming emails classified as **Infomail** will either be stored in quarantine and listed in your quarantine reports or they will be tagged and directly delivered to you, depending on your administrator's settings. The category **Infomail** includes advertising emails, especially newsletters.

You can change the delivery times of your quarantine reports. Furthermore, you can exclude emails by senders who are on your own deny list or on the deny list of the domain from your quarantine reports.

1. Log in to the Control Panel with your credentials.
2. Click on ⚙ in the upper right corner of the Control Panel.

   ➜

   The user settings are displayed.

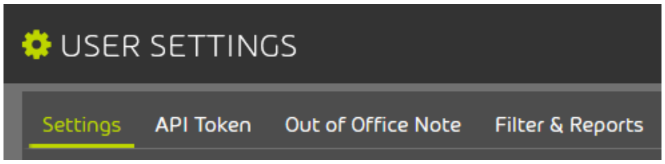


Figure 39: User settings

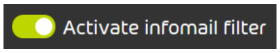
3. Select the **Filter & Reports** tab.

   ➜

   The settings for quarantine reports open. The settings of the administrator are predefined.

4. > **Notice:**
   >
   > Users can only change the settings if their administrator has allowed it.

   Toggle the switch to activate or deactivate the infomail filter.



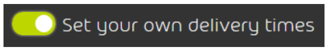
Activate infomail filter

Figure 40: Activate the infomail filter

   ➜

   If the switch is highlighted in green, the infomail filter is activated and emails classified as **Infomail** are either stored in quarantine and listed in quarantine reports or they are tagged and directly delivered. The administrator decides how the emails are handled.

5. In order to change the settings of your quarantine reports, toggle the switch **Set your own delivery times**.



Set your own delivery times

Figure 41: Set your own delivery times

   ➜

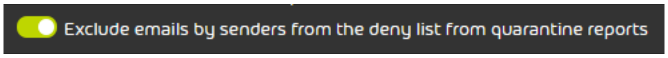
   The quarantine report settings are enabled.

> **Notice:**
>
> The Quarantine Report module is set up at the level of the primary mailbox. Quarantine reports are generated and delivered for each primary mailbox. If alias mailboxes are assigned to a primary mailbox, emails to these alias mailboxes will be listed on a single quarantine report together with the emails addressed to the primary mailbox.

6. **Important:**

   This setting can only be changed if delivery times have been set for quarantine reports.

   If you would like to exclude emails by senders who are on your deny list or on the deny list of the domain from quarantine reports, toggle the switch **Exclude emails by senders from the deny list from quarantine reports**.



Exclude emails by senders from the deny list from quarantine reports

Figure 42: Exclude emails by senders from the deny list from quarantine reports

Notice:

If this option is activated, emails from senders who are on the user's deny list or the deny list of the domain (see chapter "About Deny & Allow Lists" in the Control Panel manual) are not listed in the user's quarantine reports.

If the administrator has selected the layout **Inbox Manager with email preview and exclude option** for their users' quarantine reports (see "Layouts for Quarantine Reports" in the Control Panel manual), this option is activated and cannot be deactivated. Quarantine reports with this layout contain the button **Never show sender**. With this button, users can add a sender to their own deny list so emails by this sender will no longer be listed in future quarantine reports. Users cannot select the layout for their quarantine reports themselves.

➜

The switch is highlighted in green. Future quarantine reports will not contain any emails by senders who are on the deny list of the mailbox or the domain.

7. If you would like to deactivate quarantine reports for your mailbox, activate the **Deactivate** button.

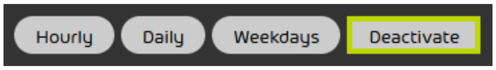


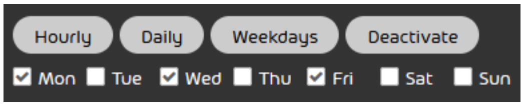
Figure 43: Deactivate the Quarantine Report

➜

All delivery times and delivery days are deactivated for the mailbox. No more quarantine reports will be sent. No further adjustments are required.

8. If quarantine reports remain activated for your mailbox, select the days on which quarantine reports shall be delivered. Select at least one day.

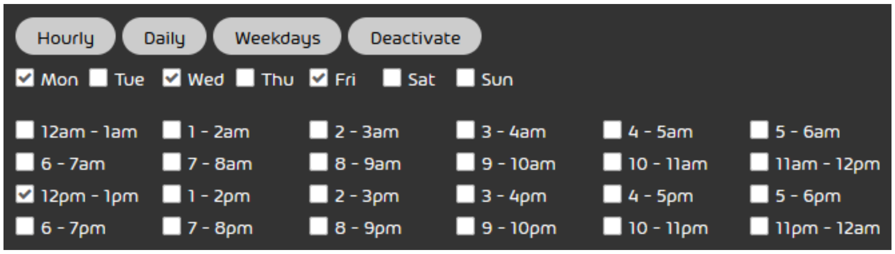
   - To deliver quarantine reports every day, activate the button **Daily**.
   - To deliver quarantine reports every day from Monday to Friday, activate the button **Weekdays**.
   - Tick the checkboxes of the desired days.



☑ Mon □ Tue ☑ Wed □ Thu ☑ Fri □ Sat □ Sun

Figure 44: Select days

9. Select the times at which the quarantine reports shall be delivered. Select at least one time.
   - To deliver quarantine reports every day, activate the button **Hourly**.
   - Tick the checkboxes of the desired times.



☑ Mon □ Tue ☑ Wed □ Thu ☑ Fri □ Sat □ Sun

□ 12am - 1am	□ 1 - 2am	□ 2 - 3am	□ 3 - 4am	□ 4 - 5am	□ 5 - 6am
□ 6 - 7am	□ 7 - 8am	□ 8 - 9am	□ 9 - 10am	□ 10 - 11am	□ 11am - 12pm
☑ 12pm - 1pm	□ 1 - 2pm	□ 2 - 3pm	□ 3 - 4pm	□ 4 - 5pm	□ 5 - 6pm
□ 6 - 7pm	□ 7 - 8pm	□ 8 - 9pm	□ 9 - 10pm	□ 10 - 11pm	□ 11pm - 12am

Figure 45: Select times

Notice:

A quarantine report is sent at the selected delivery times only if new emails have been placed in quarantine since the last quarantine report.

The infomail filter and quarantine reports have been configured for the mailbox.

Rights Management in the Control Panel

In the Control Panel, there are various permission profiles referred to as "roles" (see Roles on page 49). The permissions are assigned for different scopes that the authorized users can select in the scope selection (see Scope Selection on page 54). In the Control Panel, every user is assigned a role.

Roles

In the Control Panel, every user is assigned a role. Each role has different permissions in the Control Panel. Depending on their permissions, users have access to different scopes of Control Panel (see Scope Selection on page 54).

In the Control Panel, the following standard roles are defined:

- **User**: This role is automatically assigned if no other role has been assigned. This role cannot be assigned manually.
- **Administrator**: This role has comprehensive administrative rights.
- **Service Desk**: This role is aimed at support employees.
- **Reporting**: This role has only access to statistics.
- **Marketing**: This role is aimed at employees who create and edit signatures and disclaimers. It can be assigned in addition to any of the other default roles to grant an employee access to the module **Signature and Disclaimer**. It is not necessary to assign the role in addition to the role **Administrator**, since administrators already have access to the module. This role is only available at customer level.
- **Security Awareness**: This role is aimed at employees who configure and manage the Security Awareness Service for a customer. It can be assigned in addition to any of the other default roles to grant an employee access to the module **Security Awareness Service**. It is not necessary to assign the role in addition to the role **Administrator**, since administrators already have access to the module. This role is only available at customer level.

The following table shows to which Control Panel modules the standard roles have access. An **x** indicates that the role has access to the module.

Table 1: Standard roles and modules

MODULE	USER	ADMINISTRATOR	SERVICE DESK	REPORTING	MARKETING	SECURITY AWARENESS
Email Live Tracking	x	x	x			
Service Dashboard		x				
Reporting & Compliance	x	x	x	x		

MODULE	USER	ADMINISTRATOR	SERVICE DESK	REPORTING	MARKETING	SECURITY AWARENESS
Web Filter		x				
Customer Settings		x				
Backup		x Customer-level administrators only have access to this module if partner-level administrators have granted them access.				
Deny & Allow Lists	x	x	x			
Security Awareness Service		x				x

MODULE	USER	ADMINISTRATOR	SERVICE DESK	REPORTING	MARKETING	SECURITY AWARENESS
Security Settings		x			The role only has access to the module **Signature and Disclaimer**.	
Customization		x				
User Settings	x					

Different email actions are available to the standard roles that have access to the **Email Live Tracking** module. The following table shows which email actions (see Email Actions on page 87) each of these standard roles can perform.

Notice:

The following table also includes actions that are only available after booking additional services and are thus not mentioned in the chapter Email Actions on page 87.

Table 2: Standard roles and email actions

EMAIL ACTION	USER	ADMINISTRATOR	SERVICE DESK
Deliver email	X Users can deliver emails classified as **Clean**. The administrator can allow users to deliver emails of other categories.	X	X
Report as spam	X	X	X
Report as infomail	X	X	X
Add sender to deny list	X	X	X
Add sender to allow list & deliver email	X	X	X
Add to deny list for all users		X	
Add to allow list for all users		X	
Send email to admin	X	X	X
Deliver to support	X	X	
Mark as private	X	X	X

EMAIL ACTION	USER	ADMINISTRATOR	SERVICE DESK
Email preview	x	This action is only available for the user's own emails if the user is selected in the scope selection.	This action is only available for the user's own emails if the user is selected in the scope selection.
ATP scan		x	x
ATP report		x	x
Info	x	x	x

Scope Selection

By default, each user only sees their own settings and emails in the Control Panel. However, administrators and other users with a role with permissions on customer level or partner level (see Roles on page 49) can change the scope in the Control Panel using the scope selection (see Use of the Scope Selection on page 56) in order to access the settings to a different scope. The scope selection is a drop-down menu in the upper right corner of the Control Panel.

Notice:

Regular users cannot change the scope.

Figure 46: Scope selection

If no scope is selected in the scope selection, the settings and emails of the logged-in user are displayed in the Control Panel, and the user can manage the settings of their own mailbox.

Administrators and users with a role with permissions on customer level or partner level can select different scopes depending on their permissions. The scopes are hierarchically organized and are explained in the following table.

Table 3: Scopes

SCOPE	EXPLANATION
Partner	The partner scope is the widest scope in the Control Panel. Sub-partners or customers can be assigned to a partner. **Notice:** Under sub-partners, no other partners can be added, only customers. In this scope, administrators can add and delete sub-partners and customers. Parent settings that are inherited to sub-partners and customers can also be managed in this scope.
Customer	Customers are companies that use our services. Customers are assigned to partners. In the Control Panel, customers are managed on a primary domain basis. In this scope, administrators can view a customer's email traffic. Administrators can also manage the customer's mailboxes, groups and alias domains, as well as configure our services for the customer. The customer's deny list and allow list can be managed in this scope. A customer parents the mailboxes that belong to its primary domain and alias domains.

SCOPE	EXPLANATION
User	Users are the narrowest scope in the Control Panel. Users correspond to mailboxes. Users are assigned to the customers to whose primary domains or alias domains their mailboxes belong. In this scope, administrators can view the user's email traffic. Administrators can also manage the user's deny list and allow list.

Use of the Scope Selection

If a user has been assigned an additional role, they can easily change the scope of their role in the Control Panel.

The **Scope selection** is located in the upper window area:

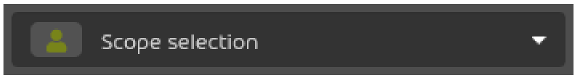


Figure 47: Scope selection

The scope selection contains all scopes relevant to the roles assigned to the logged-in user. The scope can be selected in two ways. The first option is to select the partner, customer or user directly from the drop-down menu:

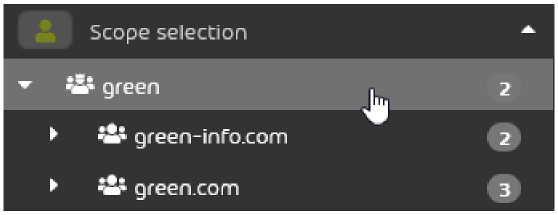
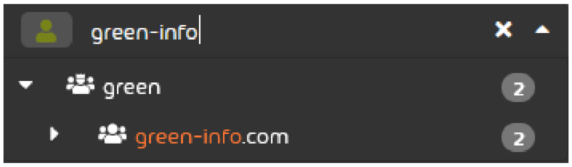


Figure 48: Select the scope

The second option is to enter the name of the partner, customer or user in the search bar.



green-info

green 2

green-info.com 2

Figure 49: Search in the scope selection

It is not necessary to write out the name of the desired scope in full: It is enough to enter a part of the name to limit the selection list to the elements that contain this string.

By default, the search is limited to partners and customers. In order to also include users in the search, the user search must be enabled.

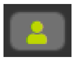


Figure 50: Enable the user search

Notice:

Once the **@** character is inserted in the scope search, the search for users is automatically enabled.

To limit the search to partners and customers, the user search must be disabled.

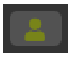


Figure 51: Disable the user search

Email Live Tracking

In the **Email Live Tracking** module, each user can monitor their own email traffic. Each user can view information about their own incoming and outgoing emails and perform actions on their emails. In addition to emails of the primary mailbox, emails of alias addresses are displayed.

Administrators also see their own emails in the **Email Live Tracking** module directly after logging in to the Control Panel. However, in contrast to regular users, administrators can change the view. Customer-level administrators can view the email traffic of their primary domain and their alias domains.

Notice:

To change the view, administrators can select a domain or a partner from the scope selection in the upper right corner of the Control Panel. If nothing is selected in the scope selection, administrators only see their own emails in the **Email Live Tracking** module.

Only emails of domains that have been verified for a customer (see Domain Verification on page 289) are displayed in the module.

The **Email Live Tracking** module is divided into the following sections: filter, email view and category statistics (see Overview of the Email Live Tracking on page 59).

Users can adjust the email view in the module (see Customizing the Email View on page 61), and search and filter the displayed emails (see Filtering Emails on page 65). The **Email Live Tracking** module contains detailed information (see Email Details on page 72) and more general information about the emails (see Email Fields on page 79). Emails are also assigned to categories (see Email Categories on page 82). Different actions can be performed on the emails (see Email Actions on page 87). Furthermore, the data of all or selected emails can be exported as a CSV file (see Exporting Email Data as a CSV file on page 94).

Overview of the Email Live Tracking

The **Email Live Tracking** module is divided into the following three sections: filter, email view and category statistics. These sections are described below.

Filter

You can filter your emails in different ways (see Filtering Emails on page 65).

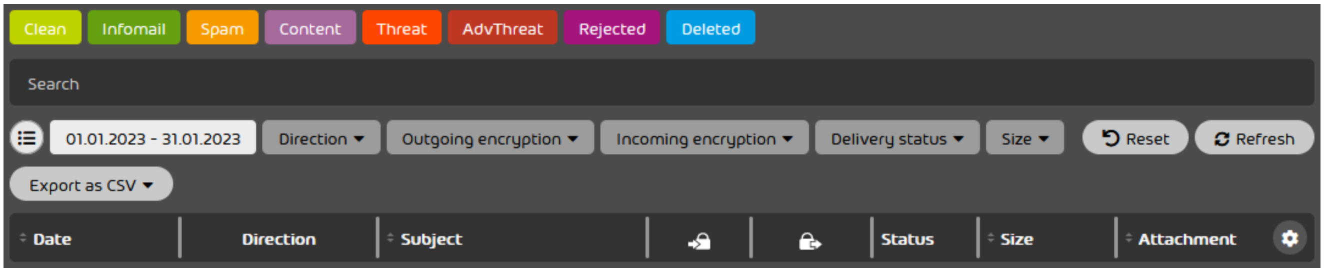
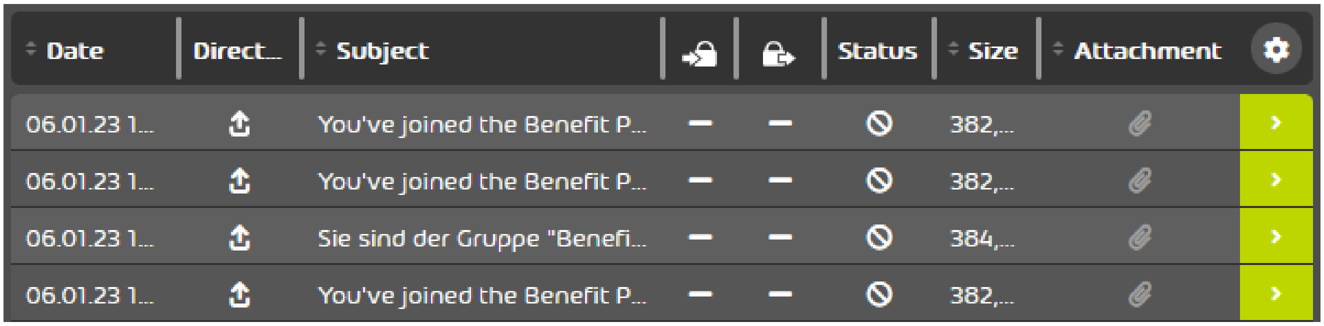


Figure 52: Filter selection

Email View

The email view is the main window of Email Live Tracking. Here, all emails are displayed. The previously selected filters determine the emails to be displayed.



Date	Direct...	Subject			Status	Size	Attachment	
06.01.23 1...	⇧	You've joined the Benefit P...	—	—	⊘	382,...	📎	›
06.01.23 1...	⇧	You've joined the Benefit P...	—	—	⊘	382,...	📎	›
06.01.23 1...	⇧	Sie sind der Gruppe "Benefi...	—	—	⊘	384,...	📎	›
06.01.23 1...	⇧	You've joined the Benefit P...	—	—	⊘	382,...	📎	›

Figure 53: Email View

You can customize the view individually (see Customizing the Email View on page 61).

All emails that match your filter settings can be exported with the function Export as CSV ▾. You can select the fields to be exported (see Exporting Email Data as a CSV file on page 94).

Extensive email lists can be browsed using the page navigation menu. The page navigation menu is located in the center of the lower display area. The number of elements displayed per page can be selected from the drop-down menu on the right. To access a specific page, the user can enter the page number in the input field and then confirm with Enter. To the right of the input field, the total number of available pages is displayed. The single arrow icons to the left and to the right of the input field allow the user to access the previous or the next page. With the double arrow icons, the user can access the first and the last page.

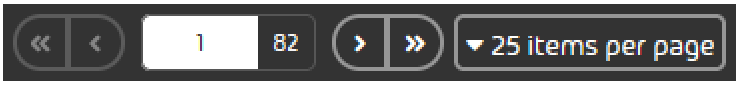


Figure 54: Page navigation menu

Notice:

The display is limited to 10000 records, which corresponds to 200 pages with default settings. If more results are returned by a search query, a plus sign is added to the total number of available pages. In order to get more accurate results, the displayed emails can be narrowed down with the filter functions (see Filtering Emails on page 65).

Category Statistics

The statistics evaluate the categories of your emails shown in the email view. The statistics can be hidden and displayed using the arrow ⌄ in the lower right area of the email view.

Notice:

The applied filters are included in the statistics.

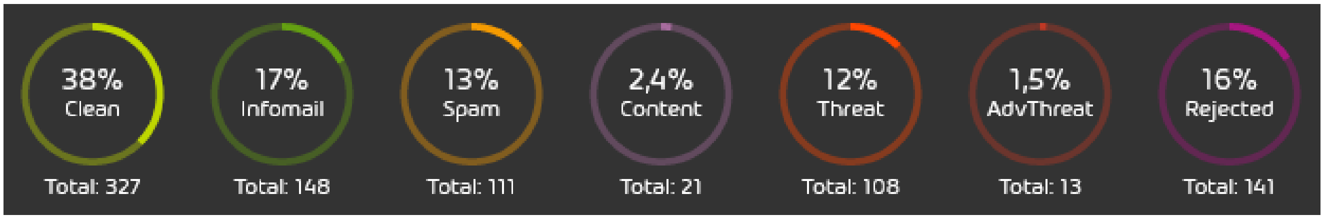


Figure 55: Category statistics

Customizing the Email View

Users can customize the email view in the following ways:

- Selecting which fields shall be displayed (see Customizing the Displayed Columns on page 61).
- Resizing the fields (see Resizing the Fields on page 63).
- Changing the positions of the fields (see Changing the Order of the Email Fields on page 64).

Customizing the Displayed Columns

The **Email Live Tracking** module (see Email Live Tracking on page 58) contains an overview of your incoming and outgoing emails.

Notice:

Instead of their own emails, customer-level administrators can view the emails of their primary domain and alias domains by selecting the domain from the scope selection in the upper right corner of the Control Panel.

The emails are displayed in a table. The table contains information about the emails. You can select the information to be displayed in the **Email Live Tracking** module. For more information about the available columns, see Email Fields on page 79.

1. Log in to the Control Panel with your credentials.
2. Navigate to the **Email Live Tracking** module.

3. Click on the table icon ⚙ in the upper right corner of the table.

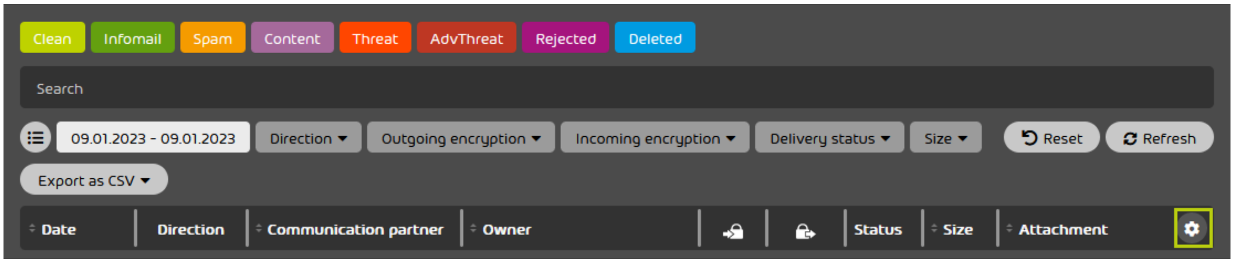


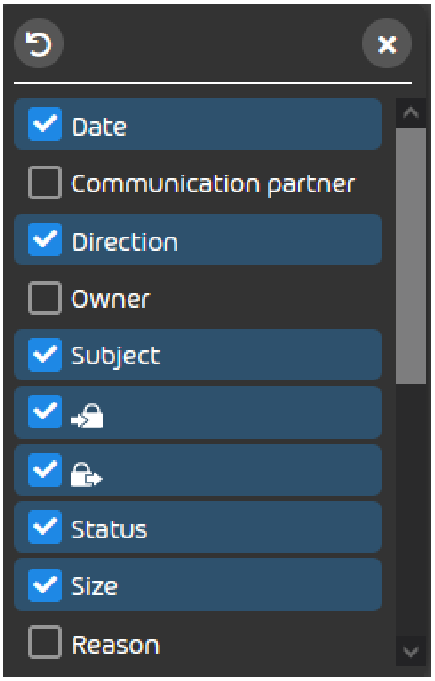
Figure 56: Open the email fields

➜

A list with the available email fields is displayed.

4. Select the desired fields.

Notice: The selected fields are highlighted in blue.



- ☑ Date
- □ Communication partner
- ☑ Direction
- □ Owner
- ☑ Subject
- ☑
- ☑
- ☑ Status
- ☑ Size
- □ Reason

Figure 57: Select email fields

The displayed email fields have been customized.

Next, you can resize the displayed fields (see Resizing the Fields on page 63) and adjust the field order (see Changing the Order of the Email Fields on page 64).

Resizing the Fields

You have customized the displayed email information (see Customizing the Displayed Columns on page 61).

You can resize the fields in the **Email Live Tracking** module (see Email Live Tracking on page 58).

1. Log in to the Control Panel with your credentials.
2. Navigate to the **Email Live Tracking** module.
3. Place the mouse pointer between two fields.

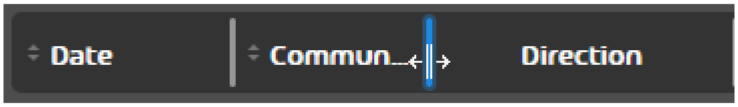


Figure 58: Adjust the size

A blue line is displayed between the fields.

4. Drag the field to the left or to the right to resize it as desired.

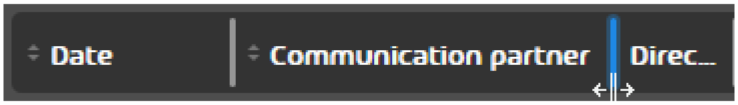


Figure 59: Adjust the size

The fields have been resized.

Next, you can adjust the field order (see Changing the Order of the Email Fields on page 64).

Changing the Order of the Email Fields

You have customized the displayed email information (see Customizing the Displayed Columns on page 61).

You can change the order of the email fields in the **Email Live Tracking** module (see Email Live Tracking on page 58).

1. Log in to the Control Panel with your credentials.
2. Navigate to the **Email Live Tracking** module.
3. Click on a field and press and hold the mouse button.

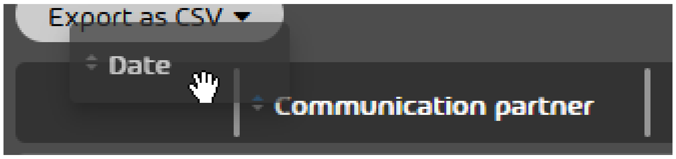


Figure 60: Change the order 1

4. Drag the field to the desired position and release the mouse button.

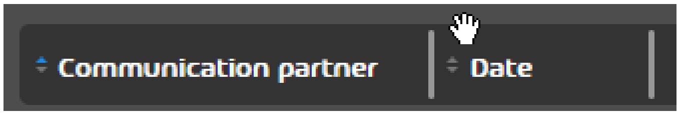


Figure 61: Change the order 2

The order of the email fields has been changed.

Next, you can resize the fields (see Resizing the Fields on page 63).

Filtering Emails

The email search allows filtering of the emails displayed in the overview and searching for specific emails. The following options are available:

- Filtering emails by category (see Filtering Emails by Category on page 65).
- Using other email filters (see Field Filters on page 69).
- Searching emails via the search bar and limiting the search to certain email fields (see Search Bar on page 66).
- Resetting or repeating the search (see Resetting or Repeating the Search on page 71).
- Using the advanced search function (see Advanced Search on page 68).

Filtering Emails by Category

You can filter the emails in the **Email Live Tracking** module (see Email Live Tracking on page 58) by categories.

1. Log in to the Control Panel with your credentials.
2. From the scope selection, select the domain whose mailboxes you would like to display.
3. Navigate to the **Email Live Tracking** module.

4. Activate or deactivate the desired categories in the filter menu.

> **Notice:**
>
> To only display emails of a specific category, double-click on the desired category. All other categories are deactivated.

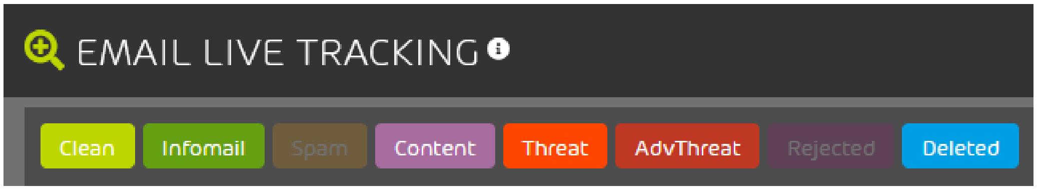


Figure 62: Activate/deactivate email categories

Only emails of active categories are displayed in the table.

The emails in the **Email Live Tracking** module have been filtered by categories.

Search Bar

By entering a string in the search bar of the **Email Live Tracking** module (see Email Live Tracking on page 58), users can search for emails (see Searching Emails on page 66). The search can be limited to certain fields (see Limiting the Search to Certain Fields on page 67). Moreover, the search bar contains an advanced search function that completes search queries (see Advanced Search on page 68).

Searching Emails

You can search emails in the **Email Live Tracking** module (see Email Live Tracking on page 58).

1. Log in to the Control Panel with your credentials.

2. Optional: If you would like to search the emails of a domain instead of your own emails, select the domain from the scope selection.
3. Navigate to the **Email Live Tracking** module.
4. Enter a string in the search field.

> **Important:**
>
> You must enter at least three characters to use the search.

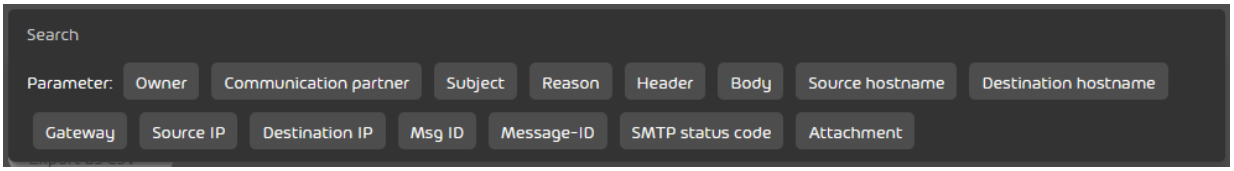


Figure 63: Search bar

The results are updated in real time.

The emails in the **Email Live Tracking** module have been searched.

Limiting the Search to Certain Fields

You can limit the email search in the **Email Live Tracking** module (see Searching Emails on page 66) to certain fields; only these fields are searched for the entered string.

1. Log in to the Control Panel with your credentials.
2. Optional: If you would like to search the emails of a domain instead of your own emails, select the domain from the scope selection.
3. Navigate to the **Email Live Tracking** module.
4. Select a field from the search suggestions.

5. Enter a character string for which the selected field shall be searched.

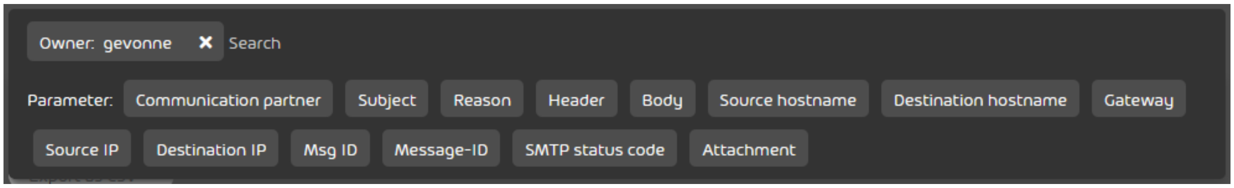


Figure 64: Limit search to certain fields

✓

The email search has been limited to certain fields.

Advanced Search

The full text search searches all email fields in the module. It is also possible to search combinations of individual email fields.

The search field in the **Email Live Tracking** module (see Email Live Tracking on page 58) completes search queries. Thus, users can also search for the beginning of words. The search is not intended to search within words.

In the email fields, different delimiters are used to separate words.

The following table shows examples for valid and invalid search queries. The delimiters for the specified email fields are also described.

Notice:

Attachments are only searched if the search has been limited to the **Attachment** field (see Limiting the Search to Certain Fields on page 67).

Table 4: Examples for complex search queries

TYPE	DELIMITER	EXAMPLE	VALID SEARCH QUERY	INVALID SEARCH QUERY
email address	"@" and last "."	info@test.com	info; test; com	o@test; nfo@
Hostname	"-" and "."	gateway07-rz01.test.com	gate; rz01; test; com	eway; 07; 01;
Attachments	";"	text.txt; image.jpg	text.txt; image.jpg	text; txt; xt; mage; image; jpg; pg
Text	Special character	We ensure that your online communications are both smooth and secure.	ensure; secure; online	nsure; ecure; nline
Reason	":"	linktag: lt_exprx_15_10_442: auto	linktag; lt_exprx; auto	tag; exprx; 10_442

Field Filters

The filters **Date**, **Direction**, **Encryption**, **Delivery status**, and **Size** can be applied to emails in the **Email Live Tracking** module. These are described in the table below.

Table 5: Filter

PROPERTY	DESCRIPTION
Date	Select a time interval from the drop-down menu or define a custom range. The default setting is **Today**. If a time interval (**Last month**, **This year**, etc.) is selected, the time zone UTC is applied regardless of the user's settings. Thus, if a different time zone than UTC is set for the user, emails from the last calendar day before the selected time interval may also be displayed among the results. **Notice:** The time interval must not exceed 365 days. Longer time intervals cannot be selected from the drop-down menu. Manually entering a longer time interval will result in an error message.
Direction	Select the direction of the emails to be displayed. The default setting is to display both directions.
Encryption	Limit the displayed emails to a certain encryption method. You can also select multiple encryption methods.
Delivery status	Specify the status of the emails to be displayed. You can choose from: **Delivered**, **Deferred**, **Rejected** and **No status**.

PROPERTY	DESCRIPTION
Size	Limit the emails to different sizes. Select the size from the drop-down menu.

Resetting or Repeating the Search

You have performed a search in the **Email Live Tracking** module (see Searching Emails on page 66 or Limiting the Search to Certain Fields on page 67) and/or applied certain field filters (see Field Filters on page 69) and are still in the **Email Live Tracking** module (see Email Live Tracking on page 58).

After you have searched the emails in the **Email Live Tracking** module, you can either reset your search settings (see Searching Emails on page 66, Limiting the Search to Certain Fields on page 67 and Field Filters on page 69) or perform a new search with your current search settings in order to refresh the search results.

Reset your search settings or perform a new search with your current search settings. To do so, click on one of the following buttons:

- **Reset**: The search settings are reset.
- **Refresh**: A new search is performed with the current search settings.

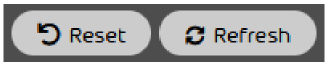


Figure 65: Reset the search settings or repeat the search

The search settings have been reset or the search has been repeated with the current search settings.

Email Details

The email view in the **Email Live Tracking** (see Email Live Tracking on page 58) shows the details of single emails.

Furthermore, actions for the selected email can be performed via the email details (see Performing an Action for a Single Email on page 72). In general, the following actions can be performed:

- Reporting an email as spam (see **Report as spam**)
- Reporting an email as infomail (see **Report as infomail**)
- Delivering an email (see **Deliver email**)
- Performing an ATP scan (see Initiating an ATP Scan on page 74)

Depending on which products are activated and which actions have been enabled by the administrator, additional actions may be available (see Email Actions on page 87).

Metadata, headers and the SMTP dialog of the email are displayed in the email details (see Extended Email Information on page 77).

Performing an Action for a Single Email

If you want to perform an action for a single email, proceed as follows.

> **Notice:**
>
> Alternatively, you can perform an action for multiple emails at once (see Selecting an Action for Multiple Emails on page 84).

1. Log in to the Control Panel.
2. Optional: If you would like to view the emails of a domain instead of your own emails, select the domain from the scope selection.
3. Navigate to the **Email Live Tracking** module.

4. Click on the arrow at the end of the row of the desired email.

Notice:

The color indicates the category of the email.

A menu opens.

5. Click on the action that you would like to perform.

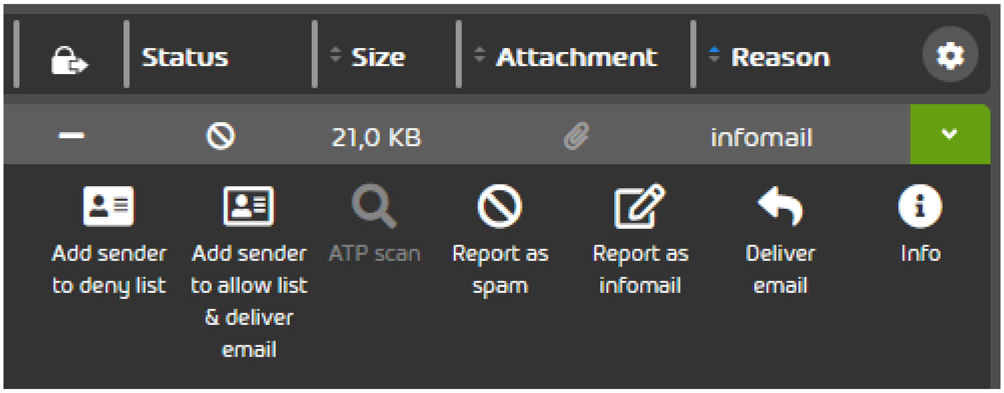


Figure 66: Email actions

Notice:

You will find further actions in the email selection (see Selecting an Action for Multiple Emails on page 84).

Notice:

For an overview of the email actions, see Email Actions on page 87.

An action has been performed for a single email.

Initiating an ATP Scan

You have activated Advanced Threat Protection (see Activating ATP on page 356).

With the ATP scan (see chapter "ATP Scan" in the Control Panel manual), you can manually check emails with executable attachments for malicious content in the **Email Live Tracking** module (see chapter "Email Live Tracking" in the Control Panel manual).

Notice:

The ATP scan can only be applied to emails with executable attachments (e.g., .exe files).

Attention:

If you have not booked Advanced Threat Protection (see chapter "Structure and Functions of ATP" in the Control Panel manual), you can perform two ATP scans per month for free. You can only perform further ATP scans, if you have booked ATP.

1. Log in to the Control Panel with your credentials.
2. If you would like to view the emails of a domain instead of your own emails, select the domain from the scope selection.
3. Navigate to the **Email Live Tracking** module.
4. Click on the arrow symbol to the right of the desired email.

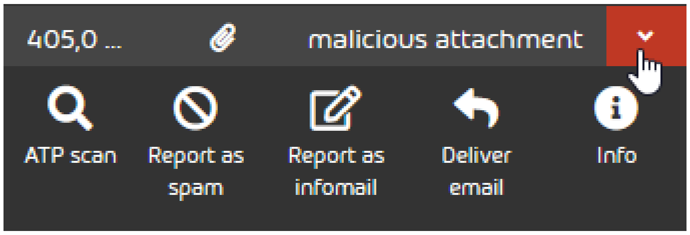


Figure 67: ATP scan in the Email Live Tracking

The detail view opens.

5. Click on **ATP scan** to start the scan.

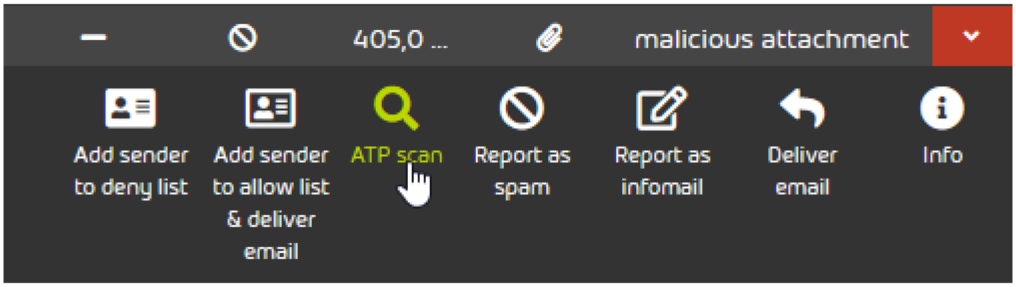
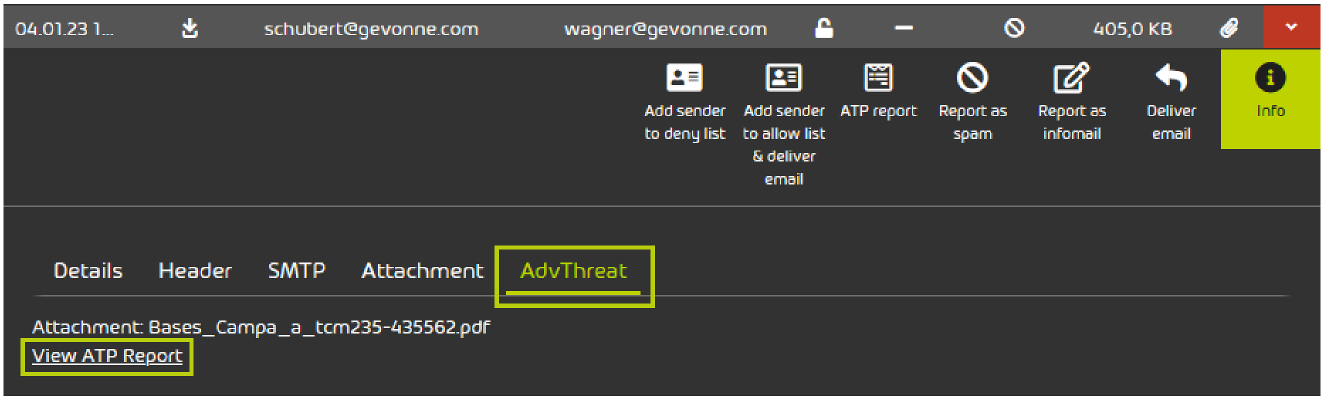


Figure 68: Initiate ATP scan

The ATP scan has been initiated for the email.

Once the ATP scan is complete, you can view the ATP report in the extended function view of the email under **ATP scan** (see ATP Report on page 75).


04.01.23 1... schubert@gevonne.com wagner@gevonne.com – 405,0 KB

Attachment: Bases_Campa_a_tcm235-435562.pdf

Figure 69: Open ATP report

ATP Report

The ATP report is a detailed report that is created after an email has been analyzed with the ATP scan (see chapter "ATP Scan" in the Control Panel manual and Initiating an ATP Scan on page 74). The ATP report provides information about the analyzed email. ATP reports are available for analyzed emails in the **Email Live Tracking** module (see Email Live Tracking on page 58). The ATP report of an email can be accessed under the menu item **ATP report** or **Info** of the **AdvThreat** tab of the email menu.

The ATP report is divided into four main sections:

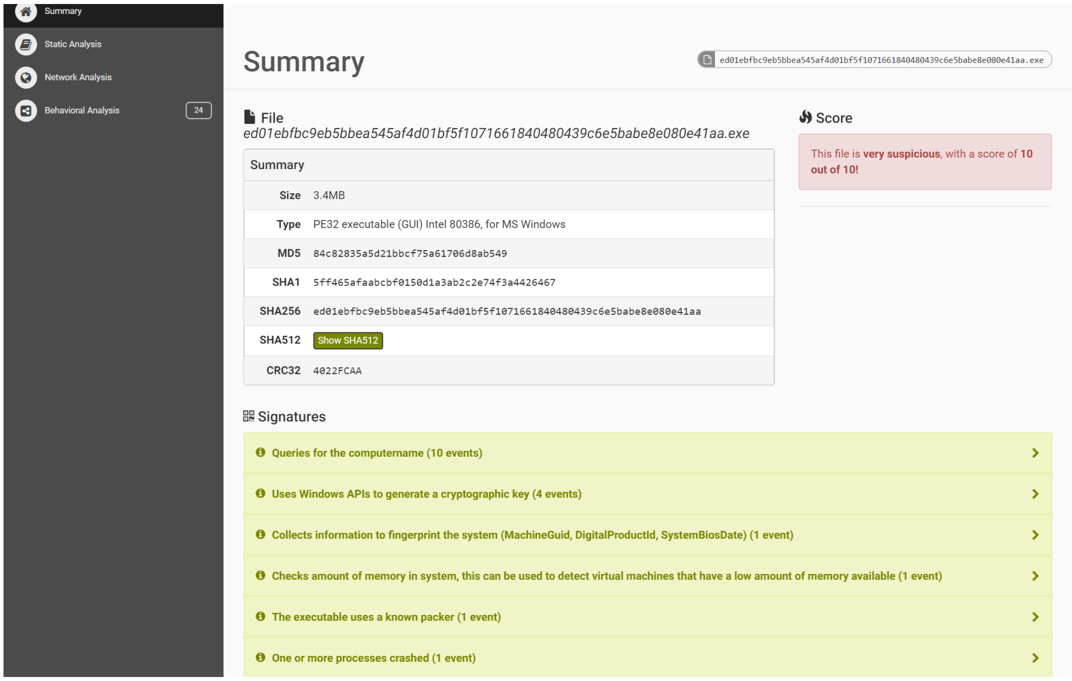
Summary

Here you will find an overview of the analyzed file. In addition, the file is assigned a **Score** from 0 to 10. 0 means "no danger", and 10 is the highest danger level.

Under the **Signatures** section, the file is assigned one of the following categories according to its behavior:

- Information (green)
- Attention (yellow)
- Warning (red)

When you click on a signature, extended process information is displayed.



Summary

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

File
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

Summary	
Size	3.4MB
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	84c82835a5d21bbcf75a61706d8ab549
SHA1	5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
SHA256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
SHA512	Show SHA512
CRC32	4022FCAA

Score

This file is **very suspicious**, with a score of **10 out of 10!**

Signatures

- Queries for the computername (10 events)
- Uses Windows APIs to generate a cryptographic key (4 events)
- Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate) (1 event)
- Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event)
- The executable uses a known packer (1 event)
- One or more processes crashed (1 event)

Figure 70: ATP Report Overview

Static Analysis

The static analysis is divided into three subcategories:

- Static Analysis – Static analysis of the file. It depends on the format of the file.
- Strings – Output of the strings contained in the file.
- Antivirus – Analysis of the file by different antivirus programs.

Network Analysis

In the network analysis, the entire network's traffic is analyzed and listed by protocol (e.g., HTTP, TCP, UDP).

Behavioral Analysis

The behavioral analysis monitors the behavior of the file at runtime.

It displays all system API calls and processes logged during dynamic sandbox analysis.

The results are divided into two sections:

- Process Tree – Here, the processes are displayed in hierarchical order.
- Process Contents – If you select a process from the process tree, the executed API queries are displayed here in chronological order.

Extended Email Information

In the **Email Live Tracking** module (see Email Live Tracking on page 58), you can find information about the selected email in the email details under **Info**. The detailed information about an email is divided into the following three sections: **Details**, **Header**, and **SMTP**.

Details

This section contains the following information about the selected email:

- **Owner**: Control Panel user who has received or sent the email

- **Communication partner**: Communication partner of the owner of the email (can be the recipient or the sender)
- **Incoming encryption**: Encryption method of incoming emails from the perspective of our servers. These emails arrive at our servers from Control Panel users or their communication partners.
- **Outgoing encryption**: Encryption method of outgoing emails from the perspective of our servers. These emails are sent from our servers to Control Panel users or their communication partners.
- **Classification**: Category that has been assigned to the email in the Control Panel (see Email Categories on page 82)
- **Subject**: Subject of the email
- **Reason**: Reason for the email classification (see Classification reasons on page 612)
- **Source hostname**: Server name of the sender
- **Message-ID**: Identifier assigned to the email by the sender's original server
- **SMTP status code**: Information from our server's last response in the SMTP dialog. This information is only displayed for emails with the delivery status **Delivered** or **Deferred** (see Field Filters on page 69). It contains the following information:
  - Timestamp of the transaction
  - Used protocol (SMTP, TLS or EmiG)
  - Hostname and IPv4 address of the receiving server
  - SMTP code and, if available, SMTP message
  - **END-SEND**: This value indicates that the SMTP client has issued the SMTP command **QUIT**. The value indicates that the communication has finished correctly.
  - **CIPHER**: This field is only displayed if TLS is used, and it refers to the strength of the used ciphers. Possible values are **NONE** (if the communication has taken place via an unencrypted channel), **WEAK** (if the communication has taken place using a TLS version older than 1.2 or a cipher that we consider to be weak) and **STRONG** (other).
  - **IDENTITY**: This field is only displayed if TLS is used, and it refers to the identification method used. The value **NONE** indicates that the communication has taken place via an unencrypted channel. The value **EMIG_VERIFIED** indicates that authentication has been performed with EmiG. The value **CA_VERIFIED** indicates that the communication partner's TLS certificate

has been validated. The value **SELF_ISSUED** indicates that the communication partner's TLS certificate has not been validated because it is either self-signed or the validation has been performed only partially. In very infrequent cases, the value **UNKNOWN** indicates a program error.

- **Domain of the owner**: Domain of the user who has received or sent the email..

Notice:

For older emails that were received or sent before the implementation of the domain verification process (see "Domain Verification" in the Control Panel manual), this field is empty.

Header

Here, the header section of the selected email is displayed. The header of rejected emails cannot be displayed.

SMTP

In this section, the result of the email transmission is displayed. For more information, see the explanation under **Details** > **SMTP status code**. If several delivery attempts have been made, several messages are displayed here.

Attachment

Here, a table with the attachments of the email is displayed. For each attachment, the file name is displayed in the **Attachment** column, and its hash value in the **Attachment hash** column.

Email Fields

The following table describes the columns that can be displayed in the email table in the **Email Live Tracking** module (see Email Live Tracking on page 58). Most names and meanings of the columns match those of the email information fields (see Extended Email Information on page 77).

Table 6: Email fields

FIELD	DESCRIPTION
Gateway	Used gateway
Subject	Subject of the email
Reason	Reason for the email classification (see Classification reasons on page 612)
Communication partner	Communication partner of the owner of the email (can be the recipient or the sender) **Notice:** For incoming emails, the field contains the header From and, for outgoing emails, the header To of the email. For incoming emails of the category **Rejected**, the field contains the envelope From of the email. It is possible that the envelope From contains a string that is not an email address.
Source hostname	Server name of the sender

FIELD	DESCRIPTION
Owner	Control Panel user who has received or sent the email **Notice:** For incoming emails, the field contains the header To and, for outgoing emails, the header From of the email. For incoming emails of the category **Rejected**, the field contains the envelope To of the email.
Destination hostname	Server name of the recipient
Destination IP	Recipient's IP address (only for delivered emails)
Message-ID	Identifier assigned to the email by the sender's original server
Source IP	Sender's IP address
Msg ID	Identifier assigned to the email by our servers
Date	Date and time of the email
Direction	Direction of the message from the owner's point of view. ⬇ stands for "incoming" and ⬆ for "outgoing".

FIELD	DESCRIPTION
→🔒	Encryption method of incoming emails from the perspective of our servers. These emails arrive at our servers from Control Panel users or their communication partners. A lock icon indicates that the incoming email is encrypted. To see the encryption method of the email, move the cursor over the lock icon or open the email details.
🔒→	Encryption method of outgoing emails from the perspective of our servers. These emails are sent from our servers to Control Panel users or their communication partners. The encryption state and encryption method are displayed as described in →🔒.
Status	Delivery status of the email (see Field Filters on page 69)
Size	Size of the email including the attachment
Attachment	An icon indicates if the email has attachments.

Email Categories

The emails of users are divided into the following categories in the **Email Live Tracking** module (see Email Live Tracking on page 58):

Table 7: Email categories

CATEGORY	DESCRIPTION
Clean	These emails are assumed to be desired by the recipient and not to pose any danger.
Infomail	These emails are promotional. Infomail includes newsletters that are sent by email. You can classify these emails as **Spam** or **Clean**. In the following cases, an email is not directly classified as **Clean**, but as **Infomail**: • This email was sent from a well-known newsletter sender. • Newsletters are sent out regularly from the sender's IP range. • This email contains a keyword or string that points to a newsletter. • The email has several characteristics that in combination point to a newsletter.
Spam	These emails are unwanted and are often promotional or fraudulent. The emails are sent simultaneously to a large number of recipients.
Content	These emails have an invalid attachment. The administrators define in the **Content Control** module which attachments are invalid.
Threat	These emails contain dangerous content, such as malicious attachments or links, or they are sent to commit crimes, such as phishing.

CATEGORY	DESCRIPTION
AdvThreat	Advanced Threat Protection has detected a threat in these emails. The emails are used for illegal purposes and involve sophisticated technical means that can only be fended off using advanced dynamic procedures.
Rejected	Our email server rejects these emails directly during the SMTP dialog because of external characteristics, such as the identity of the sender, and the emails are not analyzed further.

Selecting an Action for Multiple Emails

If you would like to perform an action in the **Email Live Tracking** module (see Email Live Tracking on page 58) for multiple emails at once, proceed as follows.

> **Notice:**
>
> Alternatively, you can perform an action for a single email (see Performing an Action for a Single Email on page 72).

1. Log in to the Control Panel.
2. If you would like to view the emails of a domain instead of your own emails, select the domain from the scope selection.
3. Navigate to the **Email Live Tracking** module.

4. Click on the button below the filters to open a bar with actions.

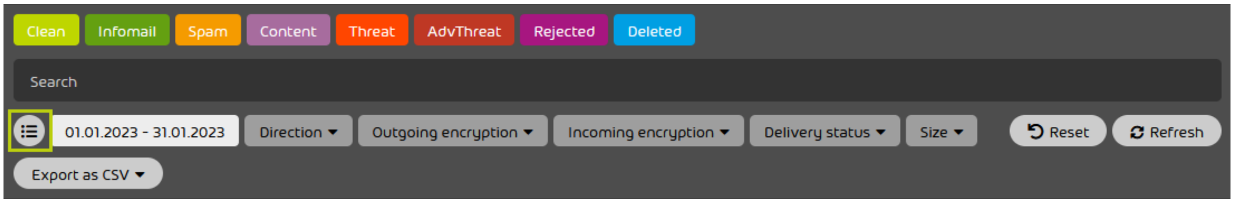
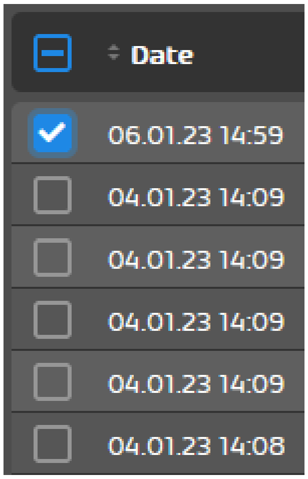


Figure 71: Open actions

5. Click on the desired emails to select them.

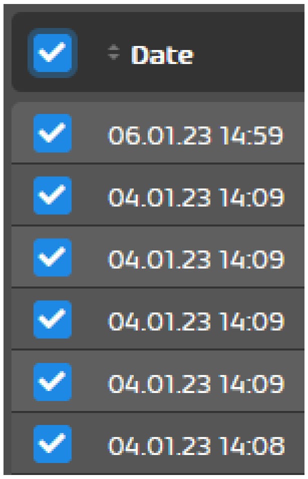


⊟	Date
☑	06.01.23 14:59
☐	04.01.23 14:09
☐	04.01.23 14:09
☐	04.01.23 14:09
☐	04.01.23 14:09
☐	04.01.23 14:08

Figure 72: Select email

Notice:

You can also select all displayed emails at the same time.



☑	Date
☑	06.01.23 14:59
☑	04.01.23 14:09
☑	04.01.23 14:09
☑	04.01.23 14:09
☑	04.01.23 14:09
☑	04.01.23 14:08

Figure 73: Select all displayed emails

6. Click on an action to perform it on the selected emails.

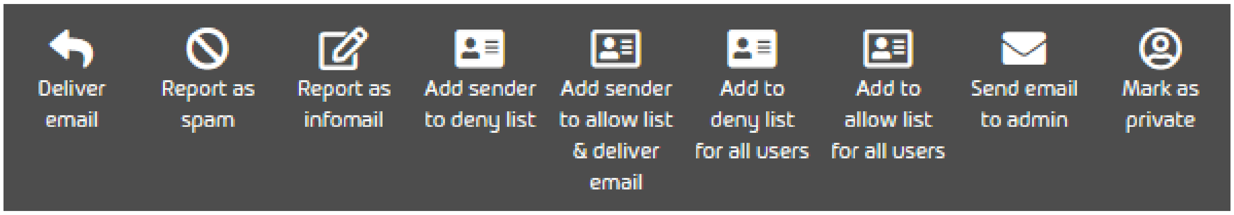


Figure 74: Select action

The action is applied to the selected emails.

An action has been performed for multiple emails at once.

Email Actions

For emails in the **Email Live Tracking** module (see Email Live Tracking on page 58), various actions, such as adding senders to the deny list, can be performed. The actions that can be performed for emails in the **Email Live Tracking** module are described in the following table.

Notice:

The availability of the email actions depends on which actions have been enabled by the administrator and which products have been activated.

Table 8: Email actions

ACTION	DESCRIPTION
Deliver email	The selected emails are delivered, triggering a process of re-evaluation of the classification on our part. For users, however, this action is only available for emails classified as **Infomail**, **Spam**, **Content** and **Threat** if their administrator has enabled their delivery (see Allowing and Forbidding User Actions on page 454). Only administrators and users with the **Service Desk** role can deliver emails classified as **AdvThreat**. The additional line **x-hornetsecurity-delivered:** is added to the headers of the delivered emails, containing information about the role of the user who triggered this action. Support employees, partner-level administrators, customer-level administrators and basic users are tagged with the words **support**, **reseller**, **admin** and **user**, respectively.

ACTION	DESCRIPTION
Email preview	In a new window, an encrypted link opens a web service where the content of the selected email is displayed in a secure way. Images, links and other active content from the email are deactivated or replaced by secure placeholders. If necessary and possible, the layout and encoding of the email are slightly modified to display the content of the email. **Notice:** This action is only visible when no scope is selected in the scope selection and emails from the active user's mailbox are displayed in Email Live Tracking (see Scope Selection on page 54). **Notice:** Control Panel users can apply this action to emails of which they are the owner. Delegates can additionally view a preview of the emails of the mailboxes for which they have been registered as delegates (see Entering a Delegate on page 239). **Notice:** This action can only be performed for a single email (see Performing an Action for a Single Email on page 72). **Important:** The email preview opens in a pop-up window. Browsers may block pop-

ACTION	DESCRIPTION
Report as spam	The support and quality management system is informed about the selected emails and the emails are reclassified. This is the preferred method of dealing with emails that have been classified incorrectly. **Notice:** The email action **Report as spam** can be used to report all emails that have been classified incorrectly (false negative).
Report as infomail	The selected emails are classified as infomail. The options for dealing with infomail are individually adjustable.
Add sender to deny list	The senders of the selected emails are added to the user's deny list. Any future emails from these senders will be automatically classified as spam.
Add sender to allow list & deliver email	The senders of the selected emails are added to the user's allow list and the emails are delivered. All other emails from the senders will be automatically delivered.
Add to deny list for all users	The senders of the selected emails are added to the deny list for all users of the domain and incoming emails are classified as spam.

ACTION	DESCRIPTION
Add to allow list for all users	The senders of the selected emails are added to the allow list for all users. All incoming emails from the senders will be automatically delivered.
Send email to admin	The selected emails are sent to the email address of the person to whom the contact **send_email_to_admin** has been assigned under **Service Dashboard** > **Role management and contacts** (see Assigning a Contact for Email Delivery on page 102).

Notice:

The deny list and allow list entries are processed in the following order:

- Administrator deny list
- Administrator allow list
- User deny list
- User allow list

An administrator adds the account example@example.com to the global deny list. A user adds the same account to his allow list. All emails from the account will be delivered to the user, but not to any users who have not added the account to their allow lists.

Email Preview

The email preview in the **Email Live Tracking** module (see Email Live Tracking on page 58) allows users and delegates to view the content of emails of the following categories (see Email Categories on page 82):

- **Spam**
- **Threat**

- **AdvThreat**
- **Content**
- **Infomail**
- **Clean**

The email preview is supported by the following browsers in their latest version:

- Edge
- Chrome
- Firefox
- Safari

The email preview can be accessed in the **Email Live Tracking** module and in quarantine reports (see the chapter "About Quarantine Report" in the Control Panel manual). In the **Email Live Tracking** module, the email preview for a user is available only for emails that either belong to the user or belonged to a mailbox that was removed and subsequently assigned to that user. Delegates can view previews for emails of the mailbox to which they are assigned as a delegate (see Entering a Delegate on page 239). For more information, see Email Actions on page 87. In quarantine reports, the email preview is only available if the administrator has selected a layout with email preview and if quarantine reports are generated for each user of the domain (see Configuring the Quarantine Report for a Domain on page 416).

The email preview can be opened by clicking on a button in the **Email Live Tracking** module and in quarantine reports. Once a user opens the email preview, an encrypted link opens a web service in a new browser window.

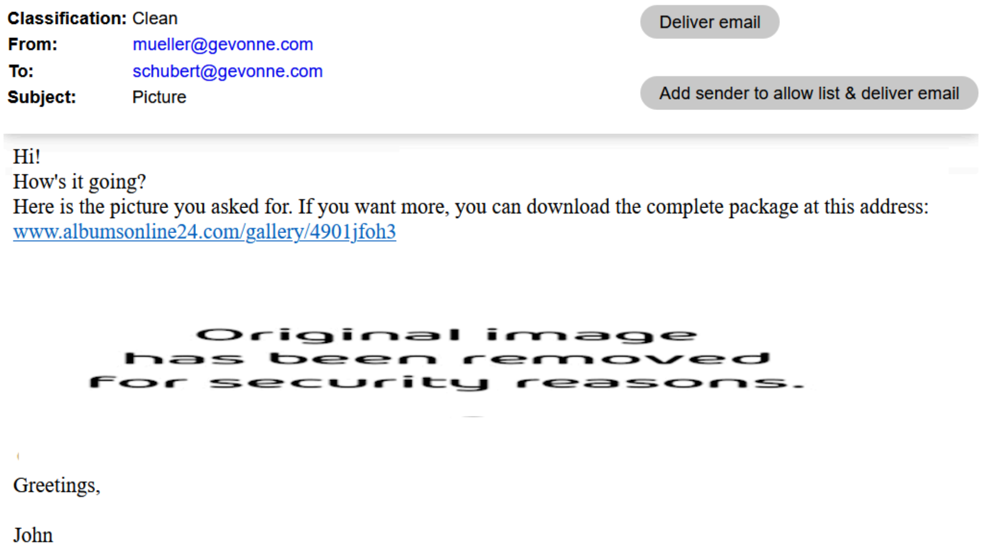
The encrypted link is only valid for a limited time. In the **Email Live Tracking** module, the encrypted link is generated as soon as the user requests the email preview. This link can only be used once. The user can generate a new link in the module as often as desired. By default, this option is available for six months. Links from quarantine reports are valid for 14 days and can be used an unlimited number of times during this period. The links in quarantine reports cannot be generated again.

In the web service, the content of the selected email is displayed in a secure way. Images from the email are replaced by secure placeholders showing the text **Original image has been removed**

for security reasons.. Links and other active content are deactivated. If necessary and possible, the layout and encoding of the email are slightly modified to display the content of the email.

Important:

The email preview opens in a pop-up window. Browsers may block pop-up windows. Pop-up windows can be allowed in the browser settings.



Classification: Clean
From: mueller@gevonne.com
To: schubert@gevonne.com
Subject: Picture

Hi!
How's it going?
Here is the picture you asked for. If you want more, you can download the complete package at this address:
www.albumsonline24.com/gallery/4901jfoh3

Original image
has been removed
for security reasons.

Greetings,

John

Figure 75: Preview of an email

Users can have emails delivered from the email preview. In order to do this, users have the following options, which they can trigger via buttons at the top of the email preview:

- **Deliver email**: The email is delivered. For more information, see the explanation of the email action **Deliver email** under Email Actions on page 87.
- **Add sender to allow list & deliver email**: The sender of the email is added to the user's allow list and the email is delivered. All incoming emails from the sender will be automatically delivered.

Exporting Email Data as a CSV file

You can export the current search results in the **Email Live Tracking** module (see Email Live Tracking on page 58) as a CSV file. The search results depend on the filters that have been set (see Field Filters on page 69). The rows in the export file are sorted in the same way as the data in the **Email Live Tracking** module.

Notice:

If a time interval (**Last month**, **This year**, etc.) is selected, the time zone UTC is applied regardless of the user's settings. Thus, if a different time zone than UTC is set for the user, data from the last calendar day before the selected time interval may also be exported.

1. Log in to the Control Panel with your credentials.
2. Optional: If you would like to view the emails of a domain instead of your own emails, select the domain from the scope selection.
3. Navigate to the **Email Live Tracking** module.
4. Optional: If you only want to export certain emails, filter the displayed emails (see Filtering Emails on page 65).

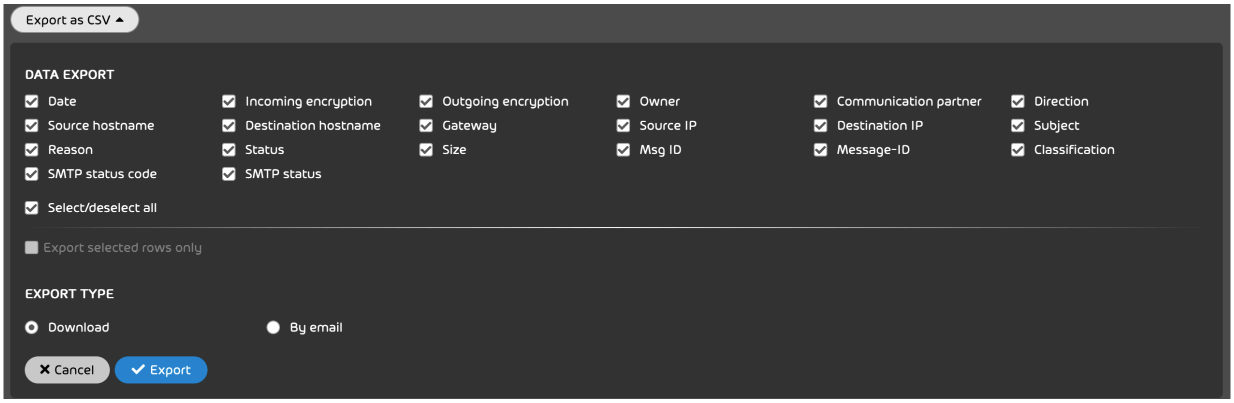
   ➜

   In the **Email Live Tracking** module, only emails are displayed that match the search settings.

5. Click on **Export as CSV**.

   ➜

   A submenu with advanced settings opens.



Export as CSV ▲

DATA EXPORT

☑ Date
☑ Source hostname
☑ Reason
☑ SMTP status code
☑ Incoming encryption
☑ Destination hostname
☑ Status
☑ SMTP status
☑ Outgoing encryption
☑ Gateway
☑ Size
☑ Owner
☑ Source IP
☑ Msg ID
☑ Communication partner
☑ Destination IP
☑ Message-ID
☑ Direction
☑ Subject
☑ Classification

☑ Select/deselect all

□ Export selected rows only

EXPORT TYPE

● Download ○ By email

✕ Cancel ✓ Export

6. Select the table columns that you would like to export.

> **Notice:**
>
> For more information about the email fields, see Extended Email Information on page 77.

7. Select the desired export type:

   - **Download**
   - **By email**

8. Click on **Export** to export the email data from the selected table columns as a CSV file.

> **Notice:**
>
> This function enables the export of a maximum of 10,000 entries per file. If the search results contain more than 10,000 entries, only the first 10,000 entries are exported according to the current sorting.

✓

Email data has been exported as a CSV file.

Service Dashboard

About the Service Dashboard

The Service Dashboard offers administrators an overview on administrative activities.

The Service Dashboard displays an overview of all created roles of individual user domains .

In the **Role management and contacts** section, partner-level and customer-level administrators can create new role assignments (see Roles on page 49) and manage existing role assignments (see Role Management and Contacts on page 97). Administrators can also assign contact data to several positions of their company (see Adding Contact Data on page 100).

In the **Secondary environments** section, customer-level administrators can manage their secondary environments to route the inbound email traffic of individual mailboxes of a domain to other destination servers (see Secondary Environments on page 107).

In the **LDAP Connection** tab, customer-level administrators can configure the LDAP connection in the Control Panel (see LDAP Connection on page 116).

Furthermore, partner-level and customer-level administrators can set default values for the timezone, the language, the date format and the time format for all their subordinate partners, customers and users in the **Default Timezone and Language** tab (see Setting Default Values for Timezone and Language on page 140).

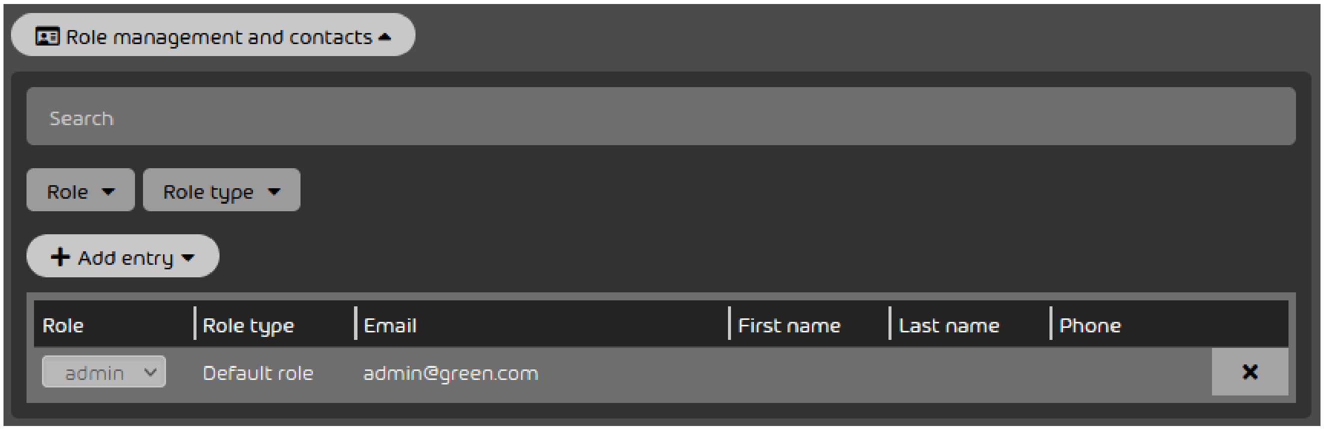
Moreover, partner-level administrators can define an end-user license agreement and a data processing agreement in the **Terms and Conditions** tab (see Terms and Conditions on page 142) in order to have their customers' users agree to their terms.

Role Management and Contacts

In the **Service Dashboard** module, administrators can manage their users' role assignments as well as contacts within their company. Users with an assigned role have other permissions than simple users (see the chapter "Roles" in the Control Panel manual). Contacts are people to contact for a department of the company.

Under **Role management and contacts**, you can perform the following actions:

- Assigning a role to a user (see Assigning a Role on page 98)
- Setting a user as a contact (see Adding Contact Data on page 100)
- Setting a user as a contact for email delivery (see Assigning a Contact for Email Delivery on page 102)
- Filtering roles and contacts (see Filtering Roles and Contacts on page 103)
- Deleting a role assignment or a contact (see Deleting a Role Assignment or Contact on page 105)



Role	Role type	Email	First name	Last name	Phone
admin	Default role	admin@green.com			

Figure 76: Overview of the role management and contacts

Assigning a Role

Users with a role assigned (see Roles on page 49) have different permissions than simple users. In the **Service Dashboard** module (see About the Service Dashboard on page 97), you can assign roles to your users in order to grant them additional permissions.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain to whose users you would like to assign roles.
3. Navigate to **Service Dashboard**.

4. Select the **Administration** tab.
5. Click on **Role management and contacts** > **Add entry**.

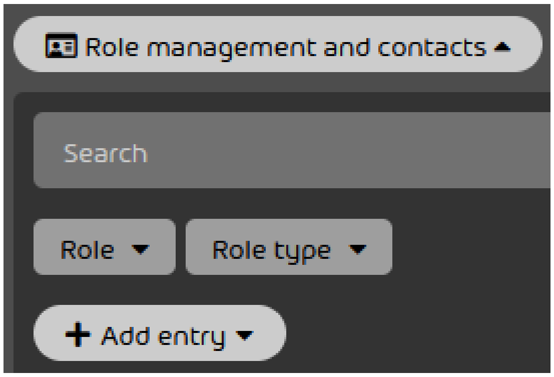


Figure 77: Add entry

6. Under **Select user**, enter the user to whom you would like to assign a new role.
7. In the drop-down menu, select which permission(s) you would like to assign to the user.

> **Notice:**
>
> For an explanation of the roles, see chapter Roles on page 49.

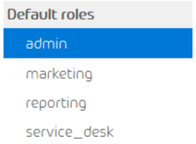


Figure 78: Select role

8. Click on **Confirm**.

The role is assigned to the user. The user is displayed in the table with the assigned role.

A role has been assigned to a user.

Adding Contact Data

In the **Service Dashboard** module (see About the Service Dashboard on page 97), you can add contact data for different positions of your company by assigning users as contacts to those positions. The contact data of those users is stored for those positions.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain at whose level you would like to set users as contacts.
3. Navigate to **Service Dashboard**.
4. Select the **Administration** tab.
5. Click on **Role management and contacts** > **Add entry**.

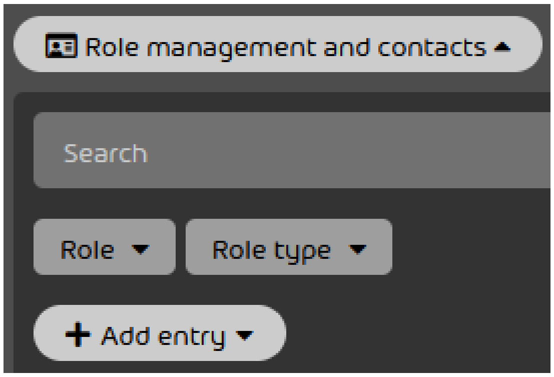


Figure 79: Add entry

6. Select a role from the drop-down menu to which you would like to assign a user's contact data.

   You can select one of the following roles:

   - it_director
   - helpdesk
   - sales
   - license_management
   - emergency
   - personal_contact
   - send_email_to_admin

   Important:

   The contact role **send_email_to_admin** is different from the role **admin**. With the action **Send email to admin** under **Email Live Tracking**, emails are only sent to the person assigned to the contact role **send_email_to_admin** (see Assigning a Contact for Email Delivery on page 102).

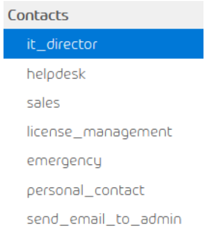


Figure 80: Select unit

7. Under **Select user**, select the user whose contact data you would like to assign to the selected position.
8. Click on **Confirm**.

   ➜

   The selected user's data is assigned to the position. The entry is displayed in the table and is labeled as **Role type** under **Contact**.

A user has been set as a contact for a position.

Assigning a Contact for Email Delivery

You can assign the **send_email_to_admin** contact to a user in order to enable your users to deliver emails to that user (see Email Live Tracking on page 58) in the **Email Live Tracking** module. If the **send_email_to_admin** contact is assigned to a user, users can deliver emails to the assigned user in the **Email Live Tracking** module with the **Send email to admin** action (see Email Actions on page 87). Otherwise, this email action is not available to the users of the domain and is hidden in the Control Panel.

> **Notice:**
>
> The **send_email_to_admin** contact is automatically assigned to the first administrator that has been set for a customer. However, administrators can delete this contact if they wish (see Deleting a Role Assignment or Contact on page 105).

You can assign the **send_email_to_admin** contact manually to a user.

1. Log in to the Control Panel with your administrative credentials.
2. Navigate to **Service Dashboard**.
3. Select the **Administration** tab.
4. Click on **Role management and contacts** > **Add entry**.

   An extended view opens.
5. Select **send_email_to_admin** from the drop-down menu.

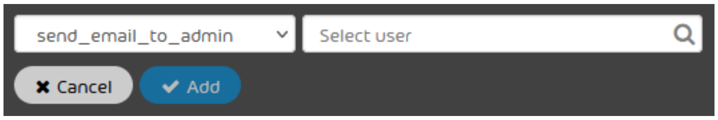


Figure 81: Select the contact role

6. Under **Select user**, enter the administrative user to whom you would like to assign the contact role.

   The button **Add** is enabled.

7. Click on **Add**.

   The contact role is assigned to the user. The assignment is added to the table below.

   > **Notice:**
   >
   > If the **send_email_to_admin** contact was not assigned to any user previously, the users of the domain must log out of the Control Panel and log in again in order for the changes to become effective.

The **send_email_to_admin** contact has been assigned to a user. From now on, users can forward emails to the assigned user in the module **Email Live Tracking** with the action **Send email to admin**.

Filtering Roles and Contacts

You have assigned roles to users (see Assigning a Role on page 98) and you have set users as contacts (see Adding Contact Data on page 100).

In the **Service Dashboard** module (see About the Service Dashboard on page 97), you can filter roles (see Roles on page 49) and contacts by the assigned role or role type in order to manage roles and contacts more easily.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain at whose level you would like to filter roles and contacts.
3. Navigate to **Service Dashboard**.

4. Select the **Administration** tab.
5. Click on **Role management and contacts**.
6. Filter by roles or role types.

   - To filter by a role, select the role from the drop-down menu **Role**.
   - To filter by a role type, select the role type from the drop-down menu **Role type**.

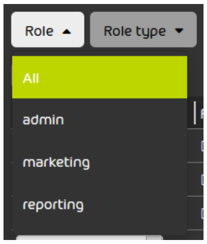


Figure 82: Filter by role

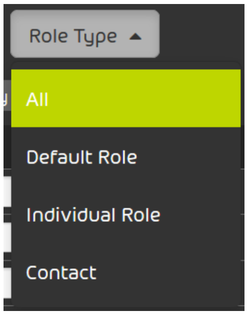


Figure 83: Filter by role type

The filtered entries are displayed in the table.

Roles and contacts have been filtered.

Deleting a Role Assignment or Contact

✓ You have assigned a role to a user (see Assigning a Role on page 98) or you have set a user as a contact (see Adding Contact Data on page 100).

In the **Service Dashboard** module (see About the Service Dashboard on page 97), users can be assigned roles (see Roles on page 49) and be set as contacts (see Adding Contact Data on page 100). Users with an assigned role have different permissions than simple users. Contacts are people to contact for a department of the company. If an existing role assignment or contact is no longer valid, you can delete the role assignment or contact.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for whose users you would like to delete role assignments or contacts.
3. Navigate to **Service Dashboard**.
4. Select the **Administration** tab.

5. **Important:**

   If the last **send_email_to_admin** contact is deleted, the email action **Send email to admin** is hidden for the users of the domain in the **Email Live Tracking** module and is no longer available to them.

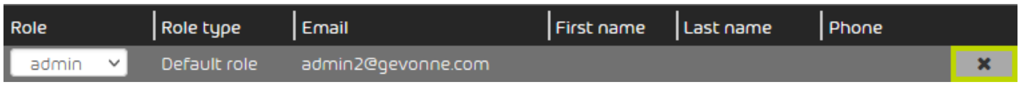
   Important:

   The role **admin** must be assigned to at least one user. You can only delete the assignment of this role to a user if the role is assigned to another user.

   Notice:

   Users with the **admin** role can delete their own assignments of the **admin** role.

   Click on the cross to the right of the role assignment or the contact to be deleted.

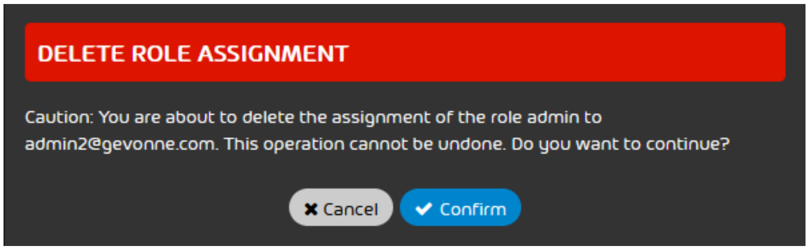


Role	Role type	Email	First name	Last name	Phone	
admin	Default role	admin2@gevonne.com				✖

Figure 84: Delete entry

➔

A warning message is displayed.



DELETE ROLE ASSIGNMENT

Caution: You are about to delete the assignment of the role admin to admin2@gevonne.com. This operation cannot be undone. Do you want to continue?

Figure 85: Warning message

6. Confirm the deletion of the entry with **Confirm**.

   The entry is deleted.

   > **Notice:**
   >
   > If the last **send_email_to_admin** contact is deleted, the users of the domain must log out of the Control Panel and log in again in order for the changes to become effective.

A role assignment or contact has been deleted.

Secondary Environments

By default, the inbound email traffic of all mailboxes of a domain is routed to the destination server that has been defined in the **Spam and Malware Protection** module (see Adjusting the Primary Environment Settings on page 441). This destination server is called the primary environment.

The inbound email traffic of individual mailboxes of a domain can be routed to other destination servers. These other destination servers are managed as secondary environments in the Control Panel. There are several types of secondary environments (see Types of Secondary Environments on page 107). In the **Service Dashboard** module, secondary environments can be created (see Creating a Secondary Environment on page 110), edited (see Editing a Secondary Environment on page 112) and deleted (see Deleting a Secondary Environment on page 114).

Types of Secondary Environments

In addition to the primary environment (see "Primary Environment Settings" in the Control Panel manual), to which the inbound email traffic of the mailboxes of a domain is routed by default, secondary environments can be managed in the Control Panel. Secondary environments are destination servers to which the inbound email traffic of individual mailboxes of a domain shall be routed instead of the primary environment. In the **Service Dashboard** module (see About the Service Dashboard on page 97), the following types of secondary environments can be managed:

- **Individual**: This type of secondary environments allows administrators to define their own destination servers. To do so, they can specify the IPv4 addresses or the hostnames of the destination servers. Administrators can create several secondary environments of this type.

Synchronization of Secondary Environments

By default, mailboxes that are synchronized a directory service via LDAP are assigned to the primary environment (see “Primary Environment Settings” in the Control Panel manual). Unlike non-synchronized mailboxes, synchronized mailboxes cannot be manually assigned to a secondary environment (see Secondary Environments on page 107) in the Control Panel.

However, it is possible to assign these mailboxes to secondary environments automatically. This requires that the mailbox belongs to a group in the directory service whose name matches the name of the secondary environment in the Control Panel. It does not matter whether this group exists in the Control Panel.

During the synchronization of a mailbox in the Control Panel, the names of its groups in the directory service are compared with the names of the secondary environments one after another. Once a match is found, the processing of further groups is stopped and the mailbox is assigned to the secondary environment. Further matches are therefore not taken into account.

Notice:

The order in which the groups are processed is based on the Unicode table. The following characters, for example, are sorted in the following order. However, the following list only contains some characters and is therefore not intended to be exhaustive.

1. Exclamation mark !
2. Hash #
3. Asterisk *
4. Plus sign +
5. Minus sign -
6. Digits
7. Less-than sign <
8. Greater-than sign >
9. Underscore _
10. Lowercase letters
11. Tilde ~
12. Lowercase letters with diacritical marks

All letters in the names of groups and secondary environments are treated as lowercase letters.

To ensure that a synchronized mailbox is assigned to the correct secondary environment, we recommend the following procedure: The administrator assigns the mailbox in the directory service to exactly one group whose name matches the name of a secondary environment in the Control Panel. This is the secondary environment to which the mailbox shall be assigned.

Important:

For a synchronized mailbox to be assigned to the primary environment, the mailbox must not belong to any group in the directory service whose name matches the name of a secondary environment in the Control Panel.

Creating a Secondary Environment

By default, the inbound email traffic of all mailboxes of a domain is routed to the destination server that has been defined as the primary environment (see Adjusting the Primary Environment Settings on page 441) in the **Spam and Malware Protection** module (see Spam and Malware Protection on page 434). If the inbound email traffic of individual mailboxes of a domain shall be routed to other destination servers instead, you can create secondary environments for these destination servers.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to create a secondary environment.
3. Navigate to **Service Dashboard**.
4. Select the tab **Administration**.
5. Click on **Add secondary environment** under **Secondary environments**.

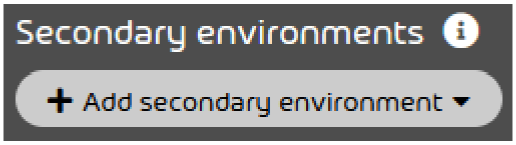


Figure 86: Add secondary environment

➜

A menu opens.

6. Select the tab corresponding to the type of secondary environment that you would like to create (see Types of Secondary Environments on page 107). You can choose from the following types of secondary environments:

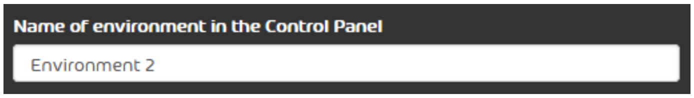
   - **Individual**

7. **Important:**

   LDAP mailboxes (see chapter "Mailbox Types" in the Control Panel manual) are automatically assigned to secondary environments during synchronization in the Control Panel if they are assigned to a group in the directory service whose name matches the name of a secondary environment in the Control Panel. The mailboxes are assigned to the secondary environment with that name.

   The names of the groups are processed and compared one after another with the names of the secondary environments according to the order of the Unicode table. Each mailbox is assigned to the secondary environment whose name is first matched. For more information, see Synchronization of Secondary Environments on page 108.

   In the field **Name of environment in the Control Panel**, enter the name under which the secondary environment shall be displayed in the Control Panel.

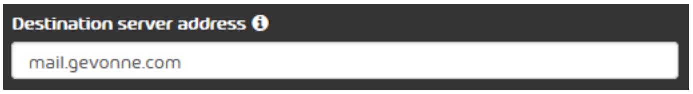


Name of environment in the Control Panel

Environment 2

Figure 87: Enter name of secondary environment

8. Optional: If you have selected the tab **Individual**, enter the IPv4 address or the hostname of the destination server in the field **Destination server address**.

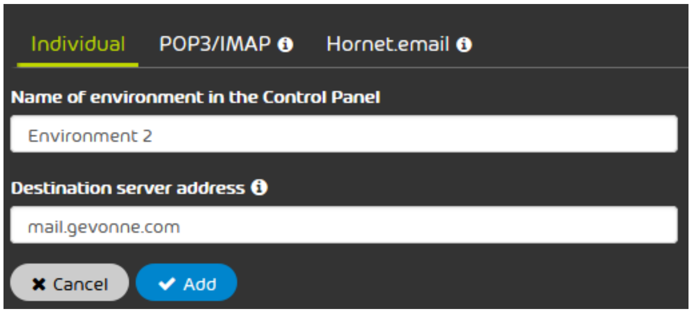


Destination server address

mail.gevonne.com

Figure 88: Enter address of destination server

9. Click on **Add**.



Name of environment in the Control Panel

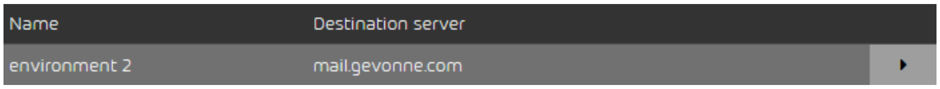
Environment 2

Destination server address

mail.gevonne.com

Figure 89: Add secondary environment

The secondary environment is created and added to the table under **Secondary environments**.



Name	Destination server
environment 2	mail.gevonne.com

Figure 90: List of secondary environments

A secondary environment has been created.

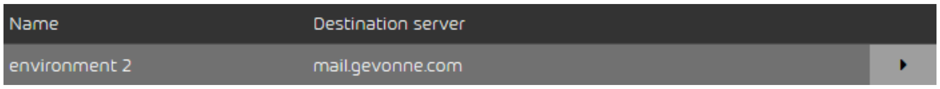
Next, you can assign the secondary environment to mailboxes of your domain (see Changing an Environment on page 252). If you no longer need the secondary environment, you can delete it (see Deleting a Secondary Environment on page 114).

Editing a Secondary Environment

You have created a secondary environment (see Creating a Secondary Environment on page 110).

You can edit existing secondary environments. However, you cannot change the type of secondary environment (see Types of Secondary Environments on page 107) in this process.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to edit an existing secondary environment.
3. Navigate to **Service Dashboard**.
4. Select the **Administration** tab.
5. Select the secondary environment from the list under **Secondary environments** and click on the menu arrow next to the secondary environment.



Name	Destination server
environment 2	mail.gevonne.com

Figure 91: Open menu

➜

A menu opens.

6. Click on **Edit entry**.

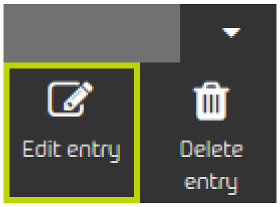
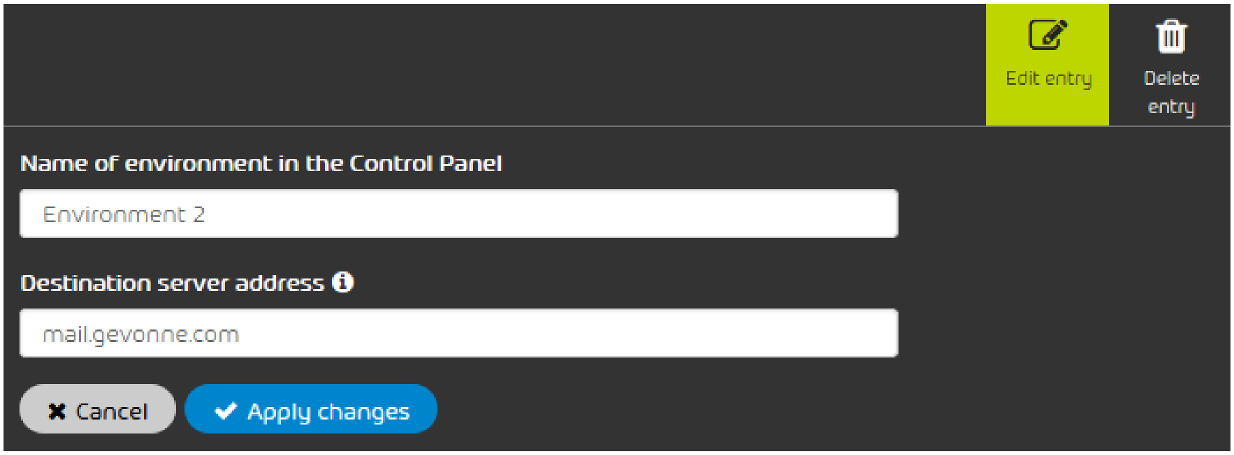


Figure 92: Edit entry

➜

A menu with the current settings of the secondary environment opens.

7. Edit the settings of the secondary environment as desired (see Creating a Secondary Environment on page 110).



Name of environment in the Control Panel

Environment 2

Destination server address

mail.gevonne.com

Figure 93: Edit secondary environment

8. Click on **Apply changes**.

   The changes are saved and applied to all mailboxes to which the secondary environment is assigned.

A secondary environment has been edited.

Deleting a Secondary Environment

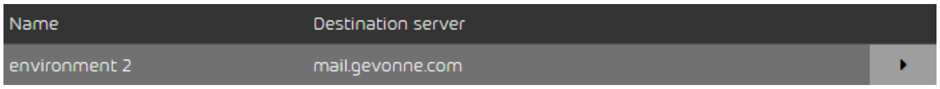
You have created a secondary environment (see Creating a Secondary Environment on page 110).

If you no longer need a secondary environment, you can delete it. When you delete a secondary environment, the mailboxes to which the secondary environment had been assigned are assigned the primary environment instead (see Primary Environment Settings on page 440).

Important:

If the mailboxes of the primary environment are synchronized with a directory service via LDAP, the mailboxes from the deleted secondary environment are assigned to the primary environment, but not synchronized.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to delete a secondary environment.
3. Navigate to **Service Dashboard**.
4. Select the **Administration** tab.
5. Select the secondary environment from the list under **Secondary environments** and click on the menu arrow next to the secondary environment.



Name	Destination server	
environment 2	mail.gevonne.com	▸

Figure 94: Open menu

➔

A menu opens.

6. Click on **Delete entry**.

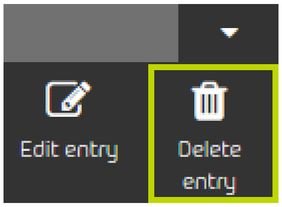
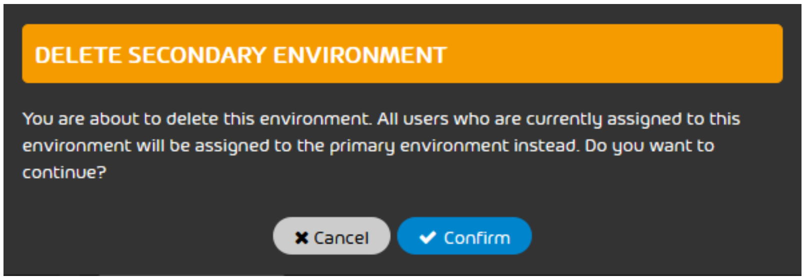


Figure 95: Delete entry

➔

A notification is displayed.

7. Click on **Confirm**.



DELETE SECONDARY ENVIRONMENT

You are about to delete this environment. All users who are currently assigned to this environment will be assigned to the primary environment instead. Do you want to continue?

Figure 96: Delete secondary environment

The secondary environment is deleted. The mailboxes of the domain to which the secondary environment had been assigned are assigned the primary environment instead.

A secondary environment has been deleted.

LDAP Connection

In the **LDAP Connection** tab of the **Service Dashboard** module, customer-level administrators can connect a directory service, such as Microsoft Active Directory (AD), to the Control Panel via LDAP. The LDAP connection can only be applied to the primary environment (see chapter "Primary Environment Settings" in the Control Panel manual).

To connect a directory service to the Control Panel, customer-level administrators must first configure the LDAP attributes of the directory service in the Control Panel (see Configuring LDAP Attributes on page 117). After that, administrators can add an LDAP connection (see Adding an LDAP Connection on page 119). This establishes a connection between the Control Panel and a directory service. It is possible to add multiple LDAP connections for different directory services. When adding an LDAP connection, administrators can further secure the LDAP connection by setting LDAPS as the access protocol. As an additional protection measure, administrators can restrict the access of their directory service to our IP address range (see Limiting the Directory Service to our

IP Address Range on page 128). Administrators can also define whether users and groups from the directory service will be synchronized in the Control Panel. Administrators can check the result of the synchronization by viewing a list of the users and groups to be synchronized.

Once there is at least one active LDAP connection, customer-level administrators can configure that their users can use their credentials from the directory service to log in to the Control Panel (see Configuring the Control Panel Login via LDAP on page 129). Administrators can use a test function to check whether logging in with credentials from the directory service is actually possible.

Customer-level administrators can edit existing LDAP connections at a later stage (see Editing an LDAP Connection on page 133). If an LDAP connection shall be temporarily suspended, administrators can deactivate the LDAP connection (see Deactivating the LDAP Connection on page 135). If an LDAP connection is no longer required, administrators can delete it (see Deleting an LDAP Connection on page 138).

Configuring LDAP Attributes

In the **LDAP Connection** tab (see LDAP Connection on page 116) of the **Service Dashboard** module (see chapter "About the Service Dashboard" in the Control Panel manual), the LDAP attributes are preset with default values for the Microsoft Active Directory. If the actual attributes names of your directory service differ, you can change them under **LDAP attributes**. The LDAP attributes apply to all LDAP connections of the customer in the Control Panel (see Adding an LDAP Connection on page 119).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to configure the LDAP attributes.
3. Navigate to **Service Dashboard**.
4. Select the **LDAP Connection** tab.

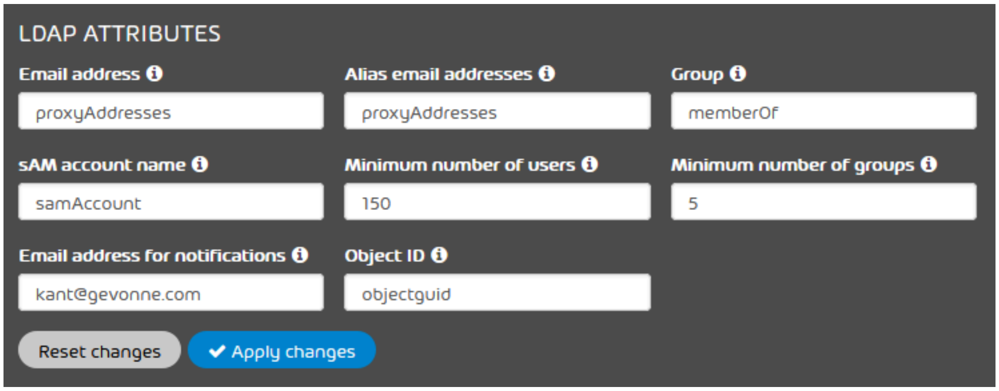
5. Fill out the form under **LDAP attributes**. The fields have the following meanings:

    - **Email address**: Attribute of the directory service under which the email addresses of users are stored. In a Microsoft Active Directory, the default attribute **proxyAddresses** is used.
    - **Alias email addresses**: Attribute of the directory service under which the alias email addresses of users are stored. In a Microsoft Active Directory, the default attribute **proxyAddresses** is also used for that.
    - **Group**: Attribute of the directory service under which the groups are stored. In a Microsoft Active Directory, the default attribute **memberOf** is used.
    - **sAM account name**: Attribute of the directory service under which the name of the SAM account is stored. In a Microsoft Active Directory, the default attribute **sAMAccountname** is used.
    - **Minimum number of users**: Minimum amount of users expected during the LDAP synchronization. This value refers to the total number of synchronized users of all active LDAP connections. This value can be used as a criterion for the quality of the synchronization. If this value is not reached during a synchronization process, an email will be sent to the email address specified under **Email address for notifications** to notify the user about possible synchronization problems. The default value is **1**.
    - **Minimum number of groups**: Similar to **Minimum number of users**, but for groups instead of users. The default value is **0**.
    - **Email address for notifications**: Email address to which notifications about the LDAP synchronization should be delivered.
    - **Object ID**: Attribute of the directory service used for the unique external identification of mailboxes. In a Microsoft Active Directory, the default attribute **objectguid** is used.
    - **Positions and languages for the Security Awareness Service**: Custom attribute of the directory service that contains the users' positions and languages for the Security

Awareness Service (see Synchronizing the Position and Language for the Security Awareness Service). The desired attribute can be selected from a drop-down menu.

Notice:

This field is only displayed if the Security Awareness Service (see About the Security Awareness Service) is activated.



LDAP ATTRIBUTES

Email address	Alias email addresses	Group
proxyAddresses	proxyAddresses	memberOf
sAM account name	Minimum number of users	Minimum number of groups
samAccount	150	5
Email address for notifications	Object ID	
kant@gevonne.com	objectguid	

Figure 97: Fill in the form

6. Click on **Apply changes**.

   The changes are saved.

The LDAP attributes of a customer's directory service have been configured in the Control Panel.

Next, you can add an LDAP connection to the Control Panel (see Adding an LDAP Connection on page 119).

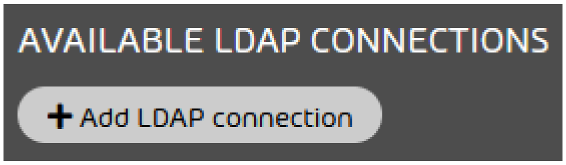
Adding an LDAP Connection

You have configured the LDAP attributes of your directory service in the Control Panel (see Configuring LDAP Attributes on page 117).

In the **LDAP Connection** tab (see LDAP Connection on page 116) of the **Service Dashboard** module (see chapter "About the Service Dashboard" in the Control Panel manual) you can add an LDAP connection to the Control Panel. This establishes a connection between the Control Panel and a directory service. You can configure that users and groups from the directory service are synchronized in the Control Panel. You can add multiple LDAP connections for different directory services to the Control Panel.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to add an LDAP connection.
3. Navigate to **Service Dashboard**.
4. Select the **LDAP Connection** tab.

5. Click on **Available LDAP connections** under **Add LDAP connection**.



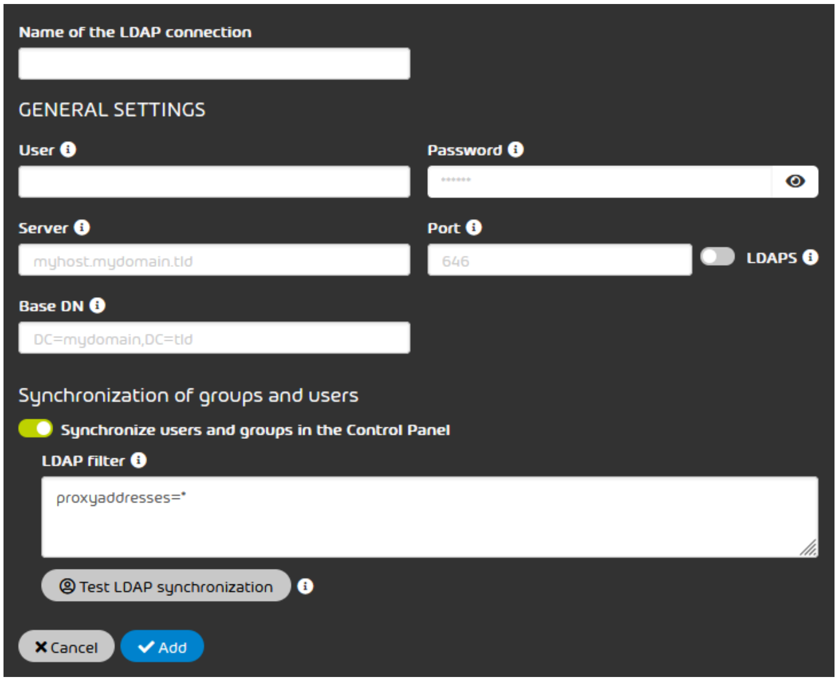
AVAILABLE LDAP CONNECTIONS

+ Add LDAP connection

Figure 98: Add an LDAP connection

➜

An extended view opens.



Name of the LDAP connection

GENERAL SETTINGS

User ⓘ

Password ⓘ ••••••

Server ⓘ myhost.mydomain.tld

Port ⓘ 646

LDAPS ⓘ

Base DN ⓘ DC=mydomain,DC=tld

Synchronization of groups and users

Synchronize users and groups in the Control Panel

LDAP filter ⓘ proxyaddresses=*

Figure 99: Extended view

6. Enter a name for the LDAP connection in the **Name of the LDAP connection** field.

7. Fill out the fields under **General settings**. The fields have the following meanings.

   - **User**: User name of an LDAP user with read rights over the directory structure under the base DN. Alternatively, the user's email address or LDAP path can be entered.

     > ℹ **Notice:**
     >
     > In the Microsoft Active Directory, users are granted the required rights by being assigned to the group **RAS and IAS Servers**.

     > ℹ **Notice:**

   - **Password**: The user's password
   - **Server**: IPv4 address or hostname of the destination server of the directory service
   - **Port**: Port of the destination server of the directory service. The default ports for the different LDAP protocols are:
     - LDAP: Port 389
     - LDAPS: Port 636
     - GC_LDAP: Port 3268
     - GC_LDAPS: Port 3269
   - **Base DN**: LDAP base distinguished name under which the user can be found. For example: **DC=myDomain,DC=tld**.

8. Optional: If your directory service is reached via LDAPS, toggle the switch **LDAPS**.

Notice:

The LDAPS protocol secures the LDAP connection with TLS/SSL. The LDAP connection can be additionally protected by limiting the directory service to our IP address range (see Limiting the Directory Service to our IP Address Range on page 128).

➜

The switch is highlighted in green.

9. Optional: If the users and groups from the directory service are not to be synchronized in the Control Panel, toggle the **Synchronize users and groups in the Control Panel** switch.

Notice:

The synchronization of users and groups is activated by default.

The synchronization of users and groups transfers the users and their group memberships from the directory service to the Control Panel. If users or group memberships are deleted or changed in the directory service, these changes are also applied in the Control Panel.

Mailboxes that have been created manually in the Control Panel or come from other sources than LDAP (see chapter "Mailbox Types" in the Control Panel manual) remain in the Control Panel when an LDAP synchronization is performed. During synchronization, only mailboxes that have been created in the Control Panel during a previous LDAP synchronization and are no longer available in the directory service are deleted from the Control Panel.

Notice:

The group memberships of LDAP mailboxes are only managed in the directory service. LDAP mailboxes thus cannot be added manually to groups or removed from groups in the Control Panel. In order to assign the users in the Control Panel to the groups from the directory service, groups with the same names must be created manually in the Control Panel. For more information on how to create groups, see "Groups" in the Control Panel manual. However, mailboxes of secondary environments can be added to or imported into groups that are synchronized from a directory service in the Control Panel (see "Managing Members" and "Importing Group Members from a CSV File" in the Control Panel manual).

Notice:

During the synchronization of users from the directory service, alias addresses are automatically assigned. The advantage is that only one quarantine report (see "About Quarantine Report" in the Control Panel manual) is sent out for each primary address, including all corresponding alias addresses.

➜

The switch is grayed out. The **LDAP filter** field is hidden.

10. If the synchronization of users and groups is activated, enter the LDAP filter used to find the users and groups in the directory service in the **LDAP filter** field.

> **Notice:**
>
> The LDAP filter **proxyaddresses=*** is set by default. By default, this LDAP filter finds the users and groups in the Microsoft Active Directory.

> **Notice:**
>
> To change the filter, you must use the following syntax:
>
> (|(xxxxxxxxxx=xxxxxxxxxx)(xxxxxxxxxx=xxxxxxxxxx))
>
> The entire filter, as well as each attribute-value pair, must be enclosed in parentheses. The preceding **|** defines an OR relation between the parameters in the following brackets. Therefore, only one defined parameter must match. An AND operation between the parameters can be built by adding an **&** at the beginning.
>
> In addition, at least one entry must be enclosed in the brackets.

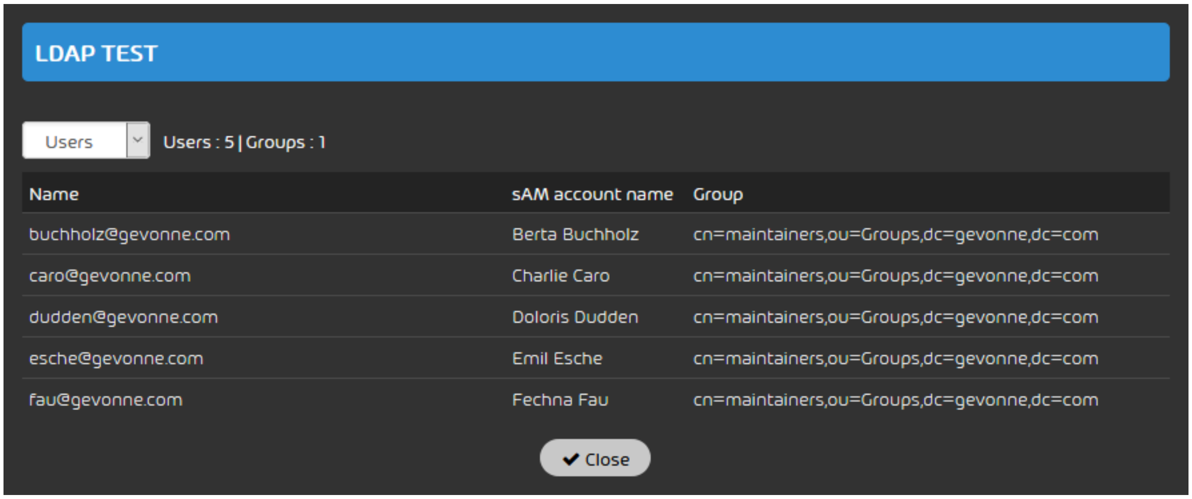
> **Notice:**
>
> The expression **(|(sAMAccountType=805306368)(sAMAccountType=268435456)(sAMAccountType=268435457)(objectclass=publicFolder))** finds all users from a Microsoft Active Directory.

11. Optional: If you would like to check which users and groups to be synchronized are found in the directory service using the entered LDAP filter, proceed as follows.

a) Click on **Test LDAP synchronization**.

➜

The **LDAP test** window opens.



Name	sAM account name	Group
buchholz@gevonne.com	Berta Buchholz	cn=maintainers,ou=Groups,dc=gevonne,dc=com
caro@gevonne.com	Charlie Caro	cn=maintainers,ou=Groups,dc=gevonne,dc=com
dudden@gevonne.com	Doloris Dudden	cn=maintainers,ou=Groups,dc=gevonne,dc=com
esche@gevonne.com	Emil Esche	cn=maintainers,ou=Groups,dc=gevonne,dc=com
fau@gevonne.com	Fechna Fau	cn=maintainers,ou=Groups,dc=gevonne,dc=com

Figure 100: LDAP check

b) From the drop-down menu, select the option for which you would like to view more information. You can choose from the following options.

- **Users**: The users who are found in the directory service using the LDAP filter and who can be synchronized are displayed.
- **Groups**: The groups that are found in the directory service using the LDAP filter and that can be synchronized are displayed.
- **Log**: The log of the LDAP test is displayed.

c) Check whether the displayed data corresponds to your expectations regarding the content of your directory service.

d) Click on **Close**.

➜

The window closes.

12. Click on **Apply changes**.

➜

The settings are saved. The LDAP connection is added to the Control Panel and activated.

> **Notice:**
>
> The synchronization of data from the directory service is performed hourly. For this reason, the result of the settings may not be effective for up to two hours.

✓

An LDAP connection has been added to the Control Panel. If the synchronization of users and groups is activated, the users and groups from the directory service will be regularly synchronized in the Control Panel. The synchronized users are added to the Control Panel as LDAP mailboxes (see chapter "Mailbox Types" in the Control Panel manual).

Next, you can configure that users of LDAP mailboxes will use the credentials from the directory service to log in to the Control Panel (see Configuring the Control Panel Login via LDAP on page 129). You can edit an existing LDAP connection at a later stage (see Editing an LDAP Connection on page 133). You can also temporarily deactivate an LDAP connection (see Deactivating the LDAP Connection on page 135) or delete it from the Control Panel (see Deleting an LDAP Connection on page 138).

Limiting the Directory Service to our IP Address Range

You can limit the access of your directory service (see LDAP Connection on page 116) our IP address range. By entering our IP address ranges in the firewall of your directory service, you can prevent requests from other IP addresses from being accepted by your directory service.

Add the following IP address ranges to the firewall of your directory service:

- First Range: **83.246.65.0/24** With subnet mask **255.255.255.0**, corresponding to the addresses from 83.246.65.1 to 83.246.65.255.

- Second Range: **94.100.128.0/20** With subnet mask **255.255.240.0**, corresponding to the addresses from 94.100.128.1 to 94.100.143.255.
- Third Range: **185.140.204.0/22** With subnet mask **255.255.252.0**, corresponding to the addresses from 185.140.204.1 to 185.140.207.255.
- Fourth Range: **173.45.18.0/24** With subnet mask **255.255.255.0**, corresponding to the addresses from 173.45.18.1 to 173.45.18.255.

Notice:

Customers in Canada must additionally enter the following IP ranges:

- Fifth Range: **108.163.133.224/27** With subnet mask **255.255.255.224**, corresponding to the addresses from 108.163.133.224 to 108.163.133.255.
- Sixth Range: **199.27.221.64/27** With subnet mask **255.255.255.224**, corresponding to the addresses from 199.27.221.64 to 199.27.221.95.
- Seventh Range: **209.172.38.64/27** With subnet mask **255.255.255.224**, corresponding to the addresses from 209.172.38.64 to 209.172.38.95.
- Eighth Range: **216.46.2.48/29** With subnet mask **255.255.255.248**, corresponding to the addresses from 216.46.2.48 to 216.46.2.55.
- Ninth Range: **216.46.11.224/27** With subnet mask **255.255.255.224**, corresponding to the addresses from 216.46.11.224 to 216.46.11.255.

✓

The valid IP address range in your firewall has been limited to our IP address ranges.

Configuring the Control Panel Login via LDAP

You have added an active LDAP connection to the Control Panel (see Adding an LDAP Connection on page 119).

In the **LDAP Connection** tab of the **Service Dashboard** module, you can configure that users of LDAP mailboxes (see chapter “Mailbox Types” in the Control Panel manual) will use the credentials from the directory service to log in to the Control Panel.

Notice:

The users of all active LDAP connections can log in with the credentials from the directory service.

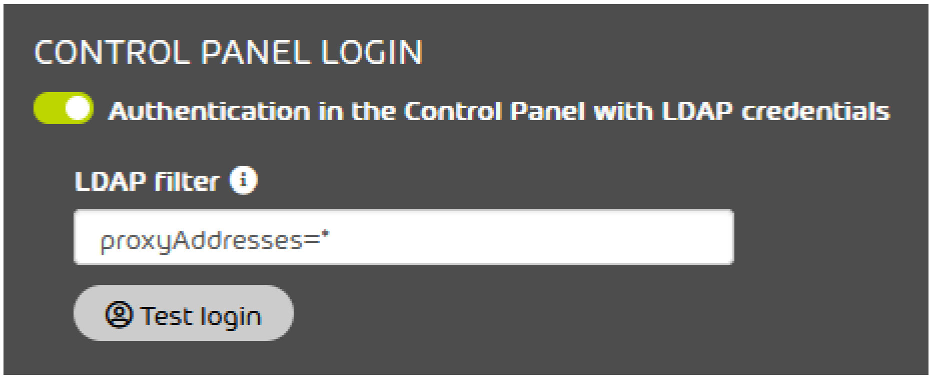
Notice:

If the credentials from the directory service are used for the Control Panel login, users cannot change their password in the Control Panel (see chapter "Changing the Password" in the Control Panel manual).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for whose users you would like to activate the authentication with credentials from the directory service.
3. Navigate to **Service Dashboard**.
4. Select the **LDAP Connection** tab.
5. Toggle the switch **Authentication in the Control Panel with LDAP credentials** under **Control Panel login**.

➜

The additional field **LDAP filter** is displayed below the switch.



CONTROL PANEL LOGIN

● Authentication in the Control Panel with LDAP credentials

LDAP filter

proxyAddresses=*

Figure 101: LDAP filter for the Control Panel login

6. In the **LDAP filter** field, enter a filter for the users or groups from the directory service that shall log in to the Control Panel with their credentials from the directory service.

   Notice:

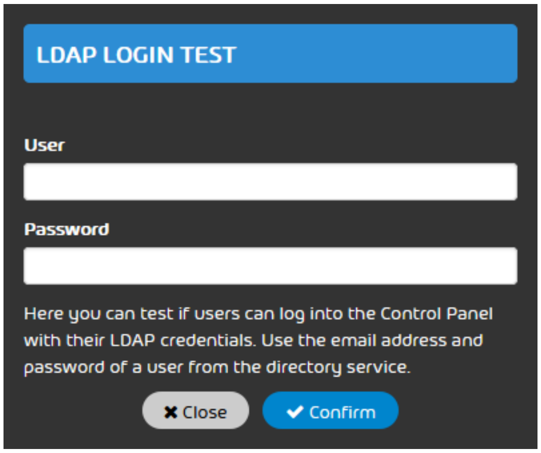
   The LDAP filter **proxyaddresses=*** is set by default. This expression selects all users from a Microsoft Active Directory.

7. If you would like to check whether the login to the Control Panel works with credentials from the directory service, proceed as follows.

   a) Click on **Test login**.

      ➡

      The **LDAP login test** window opens.



Here you can test if users can log into the Control Panel with their LDAP credentials. Use the email address and password of a user from the directory service.

Figure 102: LDAP login test

   b) In the **User** field, enter the email address of the user for whom you would like to test the Control Panel login.

   c) In the **Password** field, enter the user's password from the directory service.

   d) Click on **Confirm**.

      ➡

      The test is performed and the result is displayed at the bottom of the window.

   e) Click on **Close**.

      ➡

      The window closes.

8. Click on **Apply changes**.

   The changes are saved.

   > **Notice:**
   >
   > The synchronization of data from the directory service is performed hourly. For this reason, the result of your settings may not be effective for up to two hours.

The Control Panel login with credentials from the directory service has been configured.

> **Important:**
>
> Logging in via LDAP only applies to users with LDAP mailboxes (see chapter "Mailbox Types" in the Control Panel manual). Users with mailboxes from a secondary environment can still log in with their credentials managed in the Control Panel.

Editing an LDAP Connection

You have added an LDAP connection to the Control Panel (see Adding an LDAP Connection on page 119).

In the **LDAP Connection** tab (see LDAP Connection on page 116) of the **Service Dashboard** module (see About the Service Dashboard on page 97), you can edit an existing LDAP connection.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain whose LDAP connection you would like to edit.
3. Navigate to **Service Dashboard**.
4. Select the **LDAP Connection** tab.

5. Under **Available LDAP connections**, select the LDAP connection that you would like to edit and click on the menu arrow next to the LDAP connection.

Figure 103: Open menu

➔

A menu opens.

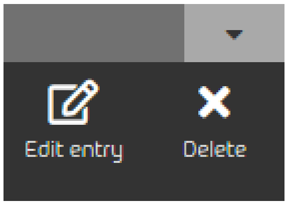


Figure 104: Menu

6. Click on **Edit entry**.

   ➔

   The settings of the LDAP connection are displayed.

7. Edit the settings as desired (see Adding an LDAP Connection on page 119).

8. Click on **Apply changes**.

   ➔

   The changes are saved.

   Notice:

   The synchronization of data from the directory service is performed hourly. For this reason, the result of the settings may not be effective for up to two hours.

✓

An existing LDAP connection has been edited.

Deactivating the LDAP Connection

You have added an active LDAP connection to the Control Panel (see Adding an LDAP Connection on page 119).

In the **LDAP Connection** tab (see LDAP Connection on page 116) of the **Service Dashboard** module (see About the Service Dashboard on page 97) you can deactivate an existing LDAP connection if you no longer want to synchronize users and group memberships from the directory service in the Control Panel. If users previously used their credentials from the directory service to log in to the Control Panel, the last synchronized password remains stored in the Control Panel and users can change their password in the Control Panel. The settings will be kept in case you want to reactivate the LDAP connection later.

Notice:

After the deactivation of the LDAP connection, the user data in the Control Panel will no longer be synchronized with the directory service. Once data in the directory service changes, the set of data in the Control Panel and the set of data in the directory service will differ. For example, passwords in the Control Panel will no longer be automatically renewed, mailboxes of new users from the directory service will not be added to the Control Panel or mailboxes of deleted users will not be deleted from the Control Panel.

However, mailboxes in the Control Panel that have been previously synchronized via LDAP will still be protected by our services and will still be treated as LDAP mailboxes (see chapter "Mailbox Types" in the Control Panel manual).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain whose LDAP connection you would like to deactivate.
3. Navigate to **Service Dashboard**.
4. Select the **LDAP Connection** tab.

5. Under **Available LDAP connections**, select the LDAP connection that you would like to deactivate and click on the menu arrow next to the LDAP connection.

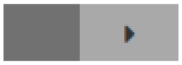


Figure 105: Open the menu

➜ A menu opens.

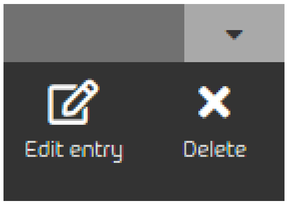


Figure 106: Menu

6. Click on **Edit entry**.

   ➜ The settings of the LDAP connection are displayed.

7. Toggle the switch **Activate LDAP connection**.

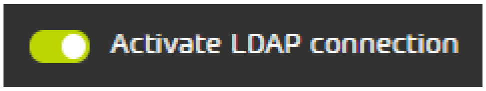


Figure 107: Deactivating the LDAP Connection

➜ The switch is grayed out. The **Test LDAP synchronization** button under **Synchronization of groups and users** is disabled.

8. Click on **Apply changes**.

   ➜ The settings are saved.

An LDAP connection has been deactivated.

Activating the LDAP Connection

You have deactivated an existing LDAP connection (see Deactivating the LDAP Connection on page 135).

In the **LDAP Connection** tab (see LDAP Connection on page 116) of the **Service Dashboard** module (see About the Service Dashboard on page 97), you can activate an existing LDAP connection to establish a connection between the Control Panel and a directory service. After activating the LDAP connection, it is again possible to synchronize the users and their group memberships from the directory service in the Control Panel (see Adding an LDAP Connection on page 119) and to use the credentials from the directory service to log in to the Control Panel (see Configuring the Control Panel Login via LDAP on page 129).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain whose LDAP connection you would like to activate.
3. Navigate to **Service Dashboard**.
4. Select the **LDAP Connection** tab.
5. Toggle the switch **Activate LDAP connection**.

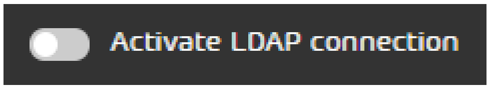


Figure 108: Deactivating the LDAP Connection

The switch is highlighted in green. The **Test LDAP synchronization** button under **Synchronization of groups and users** is enabled.

6. Click on **Apply changes**.

   ➔

   The settings are saved.

   > **Notice:**
   >
   > The synchronization of data from the directory service is performed hourly. For this reason, the result of the settings may not be effective for up to two hours.

✓

An existing LDAP connection has been activated.

Deleting an LDAP Connection

You have added an LDAP connection to the Control Panel (see Adding an LDAP Connection on page 119).

In the **LDAP Connection** tab (see LDAP Connection on page 116) of the **Service Dashboard** module (see About the Service Dashboard on page 97), you can delete an existing LDAP connection if it is no longer needed. After the deletion, the users whose mailboxes were previously synchronized with the directory service remain in the Control Panel as LDAP mailboxes. However, the mailboxes are no longer synchronized. If users previously used their credentials from the directory service to log in to the Control Panel, the last synchronized password remains stored in the Control Panel and users can change their password in the Control Panel.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain whose LDAP connection you would like to delete.
3. Navigate to **Service Dashboard**.
4. Select the **LDAP Connection** tab.

5. Under **Available LDAP connections**, select the LDAP connection that you would like to delete and click on the menu arrow next to the LDAP connection.

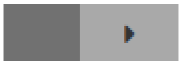


Figure 109: Open menu

➜

A menu opens.

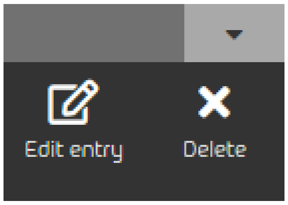


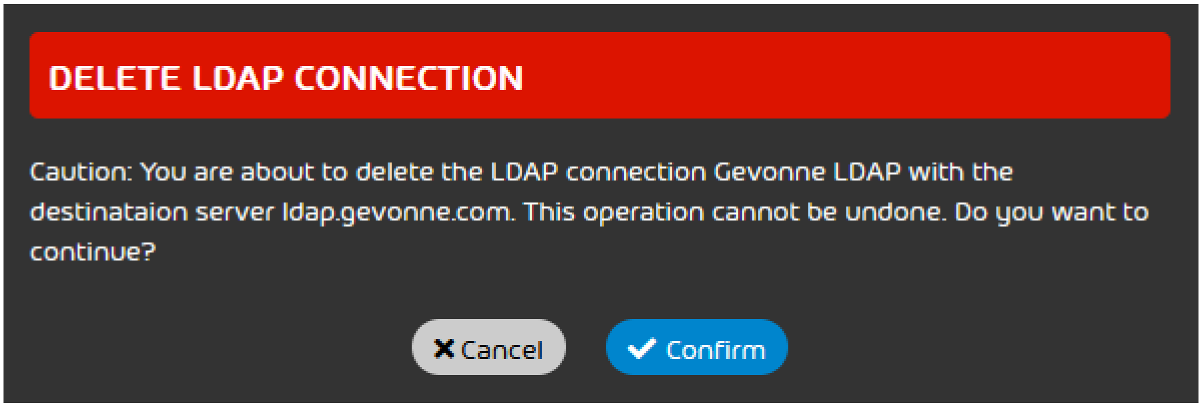
Figure 110: Menu

6. Click on **Delete**.

➜

A warning message is displayed.

7. Click on **Confirm**.



DELETE LDAP CONNECTION

Caution: You are about to delete the LDAP connection Gevonne LDAP with the destinataion server ldap.gevonne.com. This operation cannot be undone. Do you want to continue?

Figure 111: Confirm deletion

The LDAP connection is deleted from the list under **Available LDAP connections**.

An LDAP connection has been deleted from the Control Panel.

Setting Default Values for Timezone and Language

In the **Service Dashboard** module (see About the Service Dashboard on page 97), you can set default values for the timezone, language, date format and time format for a customer. The settings apply to the Control Panel display and to automatic emails from the Control Panel.

Notice:

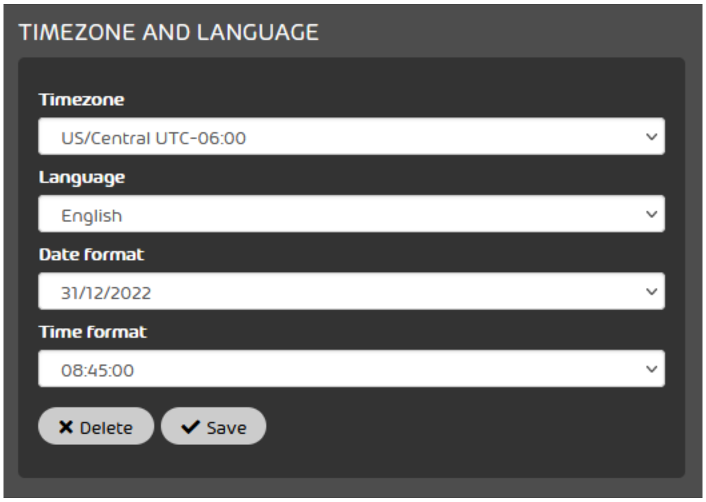
The default values are inherited by all subordinate users. As soon as a user of the customer adjusts their own settings, the default values are overwritten for the user. Users can change the settings in their user settings (see chapter 'Changing the Timezone and Language' in the Control Panel manual).

1. Log in to the Control Panel with your administrative credentials.

2. From the scope selection, select the customer for whom you would like to set default values.
3. Navigate to **Service Dashboard**.
4. Select the **Default Timezone and Language** tab.

➜

The section **Timezone and language** displays the settings for the timezone, language, date format and time format.



TIMEZONE AND LANGUAGE

Timezone: US/Central UTC-06:00

Language: English

Date format: 31/12/2022

Time format: 08:45:00

Figure 112: Timezone and language

5. Select a timezone from the drop-down menu **Timezone**.

> **Notice:**
>
> The timezone determines the number format in the Control Panel and in automatic emails from the Control Panel.

6. Select a language from the drop-down menu **Language**.

7. Select a date format from the drop-down menu **Date format**.

   Notice:

   The date format determines the order in which the available details of a date are displayed. If information is not available for all details, the missing details will not be displayed.

8. Select a time format from the drop-down menu **Time format**.

   Notice:

   The time format determines the order in which the available details of a time are displayed. If information is not available for all details, the missing details will not be displayed.

9. Click on **Save**.

   ➜

   The changes are saved.

✓

Default values for the timezone, language, date format and time format have been set for a customer.

Terms and Conditions

In the **Terms and Conditions** tab in the **Service Dashboard** module (see About the Service Dashboard on page 97), partner-level administrators can define an end-user license agreement and a data processing agreement in order to have their customers' users agree to their terms.

Once a partner's end-user license agreement and data processing agreement have been published, the agreements are displayed to the customers' users the next time they log in to the Control Panel. In order to access the Control Panel, the users must agree to the end-user license agreement once. Administrators can also accept the data processing agreement. By default, the acceptance of the data processing agreement is optional. However, partner-level administrators can make the acceptance of the data processing agreement mandatory, too.

In order to be able to define terms and conditions, partner-level administrators must first enable Terms and Conditions (see Enabling Terms and Conditions on page 143). This enables the settings of the partner's terms and conditions. The administrators can then make the acceptance of the data processing agreement mandatory for their customers' administrators (see Making the Data Processing Agreement Mandatory on page 144), and create and publish an end-user license agreement and a data processing agreement (see Creating an End-User License Agreement and a Data Processing Agreement on page 146). The agreements can be created in all languages of the Control Panel. If a partner's terms change, the partner's administrators can publish a new version of the agreements.

Notice:

Previous versions of the agreements are not stored in the Control Panel. In the **Terms and Conditions** tab in the **Service Dashboard** module, only the current version of the agreements is displayed.

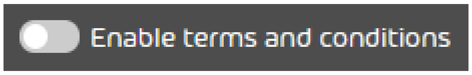
Partner-level administrators can export the text of the current version of the end-user license agreement and the data processing agreement from the Control Panel (see Exporting the End-User License Agreement and the Data Processing Agreement on page 153) in order to still have access to these agreements in the future. If a partner no longer wants to use Terms and Conditions in the Control Panel, the partner's administrators can deactivate Terms and Conditions (see Deactivating Terms and Conditions on page 154).

Changes to Terms and Conditions are audited in the **Reporting & Compliance** > **Auditing 2.0** module (see chapter "Auditing 2.0" in the Control Panel manual).

Enabling Terms and Conditions

If you would like to have your customers' users agree to an end-user license agreement and a data processing agreement in the Control Panel, you must first enable Terms and Conditions for the partner in the **Terms and Conditions** tab (see Terms and Conditions on page 142) in the **Service Dashboard** module (see About the Service Dashboard on page 97).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the partner for whom you would like to enable Terms and Conditions.
3. Navigate to **Service Dashboard**.
4. Select the **Terms and Conditions** tab.
5. Toggle the switch **Enable terms and conditions**.



Enable terms and conditions

Figure 113: Enable Terms and Conditions

The switch is highlighted in green. All other settings in the **Terms and Conditions** tab are enabled.

> **Notice:**
>
> If settings had already been configured in the **Terms and Conditions** tab, the settings become effective again.

Terms and Conditions have been enabled for a partner.

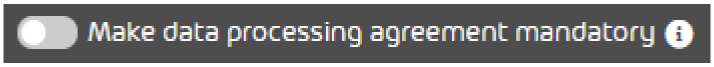
Next, you can make the acceptance of the data processing agreement mandatory for your customers' administrators (see Making the Data Processing Agreement Mandatory on page 144), and create and publish an end-user license agreement and a data processing agreement (see Creating an End-User License Agreement and a Data Processing Agreement on page 146).

Making the Data Processing Agreement Mandatory

You have enabled Terms and Conditions (see Enabling Terms and Conditions on page 143).

If you publish an end-user license agreement and a data processing agreement in the **Terms and Conditions** tab (see Terms and Conditions on page 142) in the **Service Dashboard** module (see About the Service Dashboard on page 97), your customers' users must agree to the end-user license agreement the next time they log in to the Control Panel. The customers' administrators can also accept the data processing agreement. By default, the acceptance of the data processing agreement is optional. However, you can require your customers' administrators to accept the end-user license agreement, too.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the partner for whom you would like to enable Terms and Conditions.
3. Navigate to **Service Dashboard**.
4. Select the **Terms and Conditions** tab.
5. Toggle the switch **Make data processing agreement mandatory**.



Make data processing agreement mandatory

Figure 114: Make the acceptance of the data processing agreement mandatory

The switch is highlighted in green. If an end-user license agreement and the data processing agreement have been published for the partner, the administrators of the partner's subordinate customers must accept not only the end-user license agreement but also the data processing agreement in order to access the Control Panel.

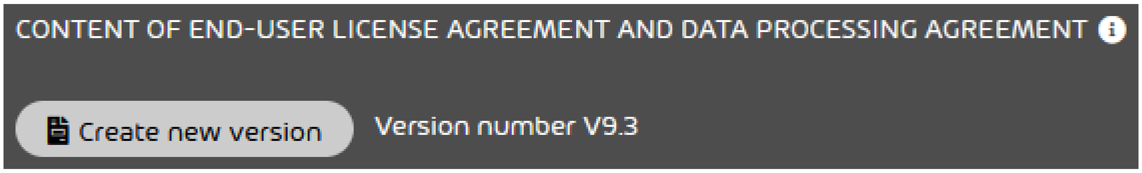
The acceptance of the data processing agreement has been made mandatory.

Next, you can create and publish an end-user license agreement and a data processing agreement (see Creating an End-User License Agreement and a Data Processing Agreement on page 146).

Creating an End-User License Agreement and a Data Processing Agreement

In the **Terms and Conditions** tab (see Terms and Conditions on page 142) in the **Service Dashboard** module (see About the Service Dashboard on page 97), you can create and publish an end-user license agreement and a data processing agreement. The agreements will be displayed to your customers' users the next time they log in to the Control Panel. In order to access the Control Panel, the users must accept the end-user license agreement once. The customers' administrators can also accept the data processing agreement. If the terms change, you can create and publish a new version of the agreements. Once a new version has been published, users must agree to the terms again.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the partner for whom you would like to enable Terms and Conditions.
3. Navigate to **Service Dashboard**.
4. Select the **Terms and Conditions** tab.
5. Click on **Create new version** under **Content of end-user license agreement and data processing agreement**.


CONTENT OF END-USER LICENSE AGREEMENT AND DATA PROCESSING AGREEMENT
Create new version

Version number V9.3

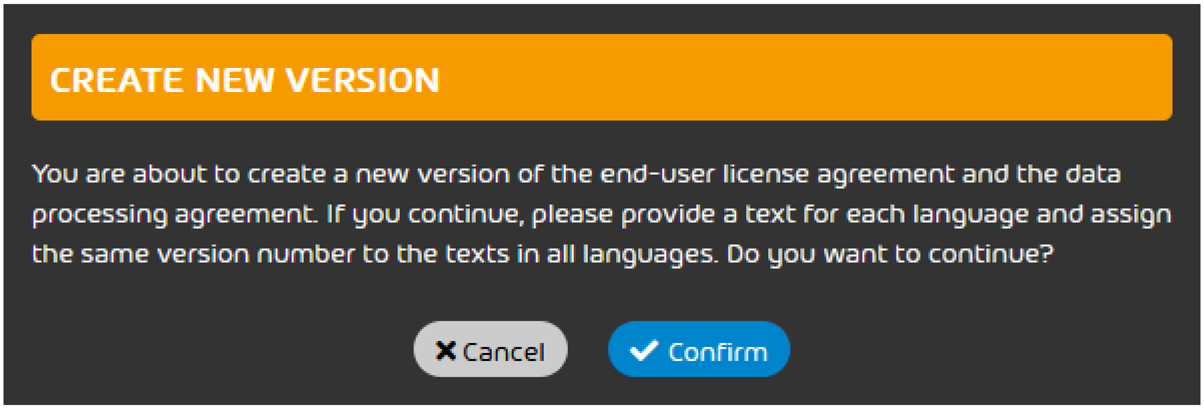
Figure 115: Create a new version

> **Notice:**
>
> If a version already exists, the current version number is displayed on the right to the button **Create new version**.

➜

A confirmation window is displayed.

6. Click on **Create new version**.



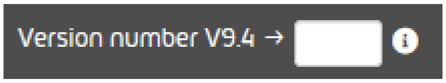
CREATE NEW VERSION

You are about to create a new version of the end-user license agreement and the data processing agreement. If you continue, please provide a text for each language and assign the same version number to the texts in all languages. Do you want to continue?

Figure 116: Confirm the creation of a new version

➜

Next to the current version number, an input field for the new version number is displayed.



Version number V9.4 →

Figure 117: Input field for the new version number

7. Enter the version number of the new version in the input field.

Notice:

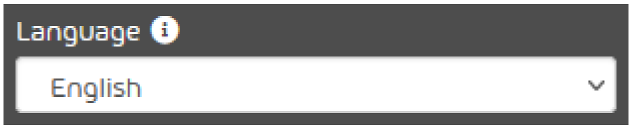
Version numbers that have already been assigned to previous versions are not accepted.

The version number may contain the following characters:

- Dots
- Letters
- Digits

Dots are not allowed at the beginning or at the end. Two or more consecutive dots are not allowed.

8. From the drop-down menu **Language**, select the language for which you would like to create a text.



Language

English

Figure 118: Select a language

Notice:

The text of the end-user license agreement and the data processing agreement can be created in any language of the Control Panel. The agreements are displayed to all users of the subordinate customers, regardless if the text is available in the display language of the concrete user.

➜

The text editor is displayed empty.

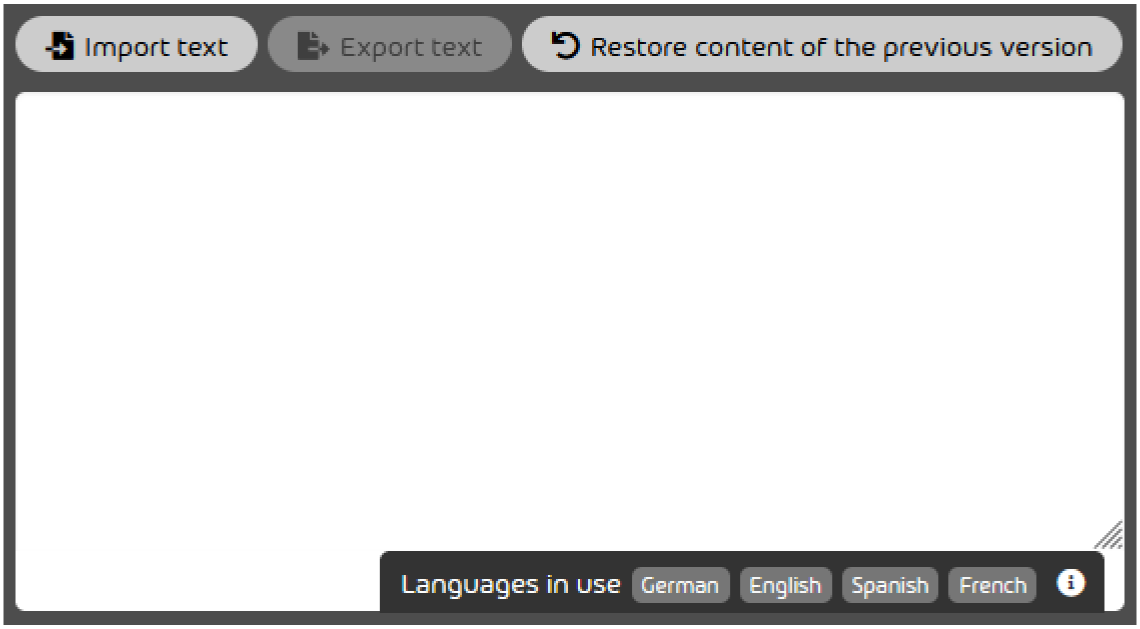


Figure 119: Text editor

Notice:

At the bottom of the text editor, the display languages of the Control Panel are displayed. Languages for which a text of this version has already been published are highlighted in white. Unused languages are grayed out.

9. Optional: If you would like to copy the text of the previous version into the text editor, click on **Restore content of the previous version**.

   ➔

   If a text has been published for the previous version in the selected language, this text is displayed in the text editor.

10. Optional: If you would like to import a text from your file system into the text editor, follow the following steps.

    a) Click on **Import text**.

    ➔

    An extended view opens.

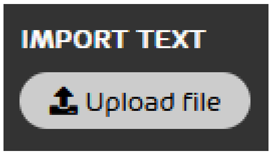


Figure 120: Extended view

    b) Click on **Upload file**.

    ➔

    A file selection window opens.

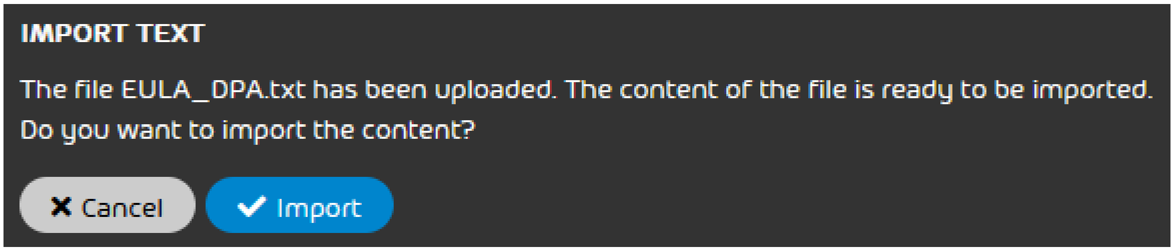
    c) Select the file whose content you would like to import.

    > **Notice:**
    >
    > Only .txt files can be imported.

    ➔

    The Control Panel reads the file and prepares the content of the file for the import.

    d) Click on **Import**.



The file EULA_DPA.txt has been uploaded. The content of the file is ready to be imported. Do you want to import the content?

Figure 121: Confirm the import

➜

The text from the imported file is displayed in the text editor.

11. Optional: Enter the text of the end-user license agreement and the data processing agreement in the text editor or edit the existing text as desired.

> **Notice:**
>
> The text cannot be formatted.

12. Once the text is ready to be published, click on **Publish** under the text editor.

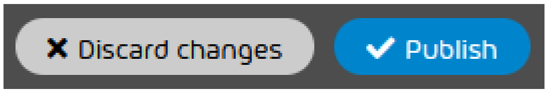
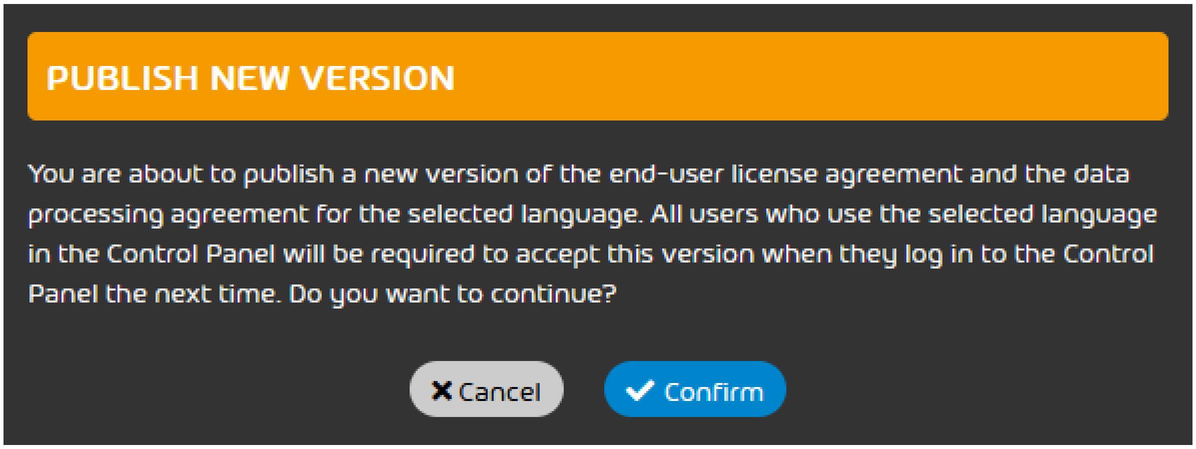


Figure 122: Publish the text

➜

A confirmation window is displayed.

13. Click on **Confirm**.



PUBLISH NEW VERSION

You are about to publish a new version of the end-user license agreement and the data processing agreement for the selected language. All users who use the selected language in the Control Panel will be required to accept this version when they log in to the Control Panel the next time. Do you want to continue?

Figure 123: Confirm the publication

➔

The text is published in the selected language. The new version of the end-user license agreement and the data processing agreement will be displayed to all users of the subordinate customers the next time they log in to the Control Panel. The users must accept the end-user license agreement once in order to access the Control Panel. The administrators of the subordinate customers can also accept the data processing agreement.

14. Repeat the steps 8 on page 148 to 13 on page 152 for all languages in which you would like to add a text of the end-user license agreement and the data processing agreement.

✓

A new version of the end-user license agreement and the data processing agreement has been created and published.

Next, you can export the end-user license agreement and the data processing agreement of the current version (see Exporting the End-User License Agreement and the Data Processing Agreement on page 153).

Exporting the End-User License Agreement and the Data Processing Agreement

You have created and published an end-user license agreement and a data processing agreement (see Creating an End-User License Agreement and a Data Processing Agreement on page 146).

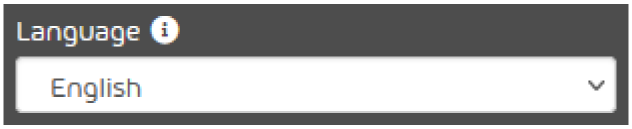
In the **Terms and Conditions** tab (see Terms and Conditions on page 142) in the **Service Dashboard** module (see About the Service Dashboard on page 97), you can export the current version of the end-user license agreement and the data processing agreement. This allows you to store the agreements outside the Control Panel so you can access them again later.

Notice:

Previous versions of the agreements are not stored in the Control Panel. In the **Terms and Conditions** tab in the **Service Dashboard** module, only the current version of the agreements is displayed.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the partner for whom you would like to enable Terms and Conditions.
3. Navigate to **Service Dashboard**.
4. Select the **Terms and Conditions** tab.

5. From the drop-down menu **Language**, select the language whose text you would like to export.



Language

English

Figure 124: Select a language

In the text editor, the text of the end-user license agreement and the data processing agreement is displayed in the selected language.

6. Click on **Export text** above the text editor.

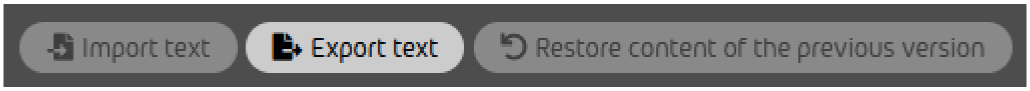


Figure 125: Export the text

The text of the end-user license agreement and the data processing agreement in the selected language is exported as a .txt file and provided as a download.

7. Save the exported file on your file system.
8. Repeat the steps 5 on page 154 to 7 on page 154 for all languages whose texts you would like to export.

The text of the current version of the end-user license agreement and the data processing agreement has been exported.

Deactivating Terms and Conditions

You have enabled Terms and Conditions (see Enabling Terms and Conditions on page 143).

In the **Terms and Conditions** tab (see Terms and Conditions on page 142) in the **Service Dashboard** module (see About the Service Dashboard on page 97), you can deactivate Terms and Conditions. Once Terms and Conditions have been deactivated, all other settings in the **Terms and Conditions** tab are disabled. No end-user license agreement and no data processing agreement will be displayed to your customers' users anymore when they log in to the Control Panel.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the partner for whom you would like to enable Terms and Conditions.
3. Navigate to **Service Dashboard**.
4. Select the **Terms and Conditions** tab.
5. Toggle the switch **Enable terms and conditions**.

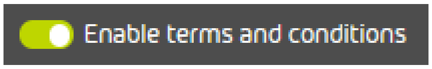

Enable terms and conditions

Figure 126: Deactivate Terms and Conditions

The switch is grayed out. All other settings in the **Terms and Conditions** tab are disabled. No end-user license agreement and no data processing agreement will be displayed to the users of the subordinate customers anymore when they log in to the Control Panel.

> **Notice:**
>
> The current settings in the **Terms and Conditions** tab will be kept in case Terms and Conditions are enable again later (see Enabling Terms and Conditions on page 143).

Terms and Conditions have been deactivated.

Next, you can enable Terms and Conditions again (see Enabling Terms and Conditions on page 143).

Reporting & Compliance

Reporting & Compliance

The **Reporting & Compliance** module displays information about email traffic, attacks on the users of a domain, and actions performed in the Control Panel.

In the submodule **Email Statistics**, users can view statistics about their own email traffic (see Email Statistics on page 156). Customer-level administrators, and users with the **Service Desk** or the **Reporting** role (see Roles on page 49) can alternatively view statistics about their domain's email traffic or the email traffic of a user from their domain.

The submodule **Threat Live Report** is available for customer-level administrators and for users with the **Service Desk** or the **Reporting** role if Advanced Threat Protection is activated for the customer. The module contains information about attacks on users of the domain (see About Threat Live Report on page 171).

The submodule **Auditing 2.0** is available for customer-level and partner-level administrators. This submodule logs actions performed by users in the Control Panel (see Auditing 2.0 on page 185).

Email Statistics

Users can view statistics about their own email traffic in the **Email Statistics** module. Customer-level administrators can also view statistics about the email traffic of their domain or of a user of their domain.

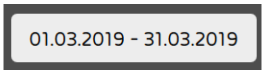
Users can select which date range and email direction the statistics in the module should refer to (see Filtering Email Statistics on page 157). The statistics are presented in two diagrams. The first diagram shows how the emails are distributed across the email categories in the Control Panel (see Emails by Type on page 159). The second diagram shows how the emails are distributed over time (see Emails by Time on page 160). The data of the second diagram can also be exported as a CSV file (see Exporting Email Statistics as a CSV File on page 162). Customer-level administrators can also see how the emails of the users of a domain are distributed across the email categories from the Control Panel (see Emails by User on page 163).

Furthermore, a domain's email statistics can be summarized in a report every month (see Monthly Report on page 164). Customer-level administrators can define to which mailboxes the monthly report should be sent (see Adding Recipients on page 165). Instead of adding recipients individually, administrators can also import a list of recipients from a CSV file (see Importing Recipients from a CSV File on page 167). Furthermore, administrators can remove previous recipients (see Removing Recipients on page 170).

Filtering Email Statistics

In the **Email Statistics** module, statistics about your email traffic are displayed (see Emails by Type on page 159 and Emails by Time on page 160).Customer-level administrators, as well as users with the **Service Desk** or the **Reporting** role, you can also view the data of a customer's domain instead of your own data. For a domain, you can also see how the emails of the users of the domain are distributed across the email categories in the Control Panel (see Emails by User on page 163). You can filter the data in the **Email Statistics** module by a date range and an email direction.

1. Log in to the Control Panel with your credentials.
2. Optional: If you would like to see the data of a domain or of a user of a domain instead of your own data, select the domain or the user in the scope selection.
3. Navigate to **Reporting & Compliance** > **Email Statistics**.
4. Click on the date range.



01.03.2019 - 31.03.2019

Figure 127: Click on the date range

➔

A calendar is displayed.

5. **Important:**

   At most, the data of the last 3 months can be displayed.

   Select a date range.

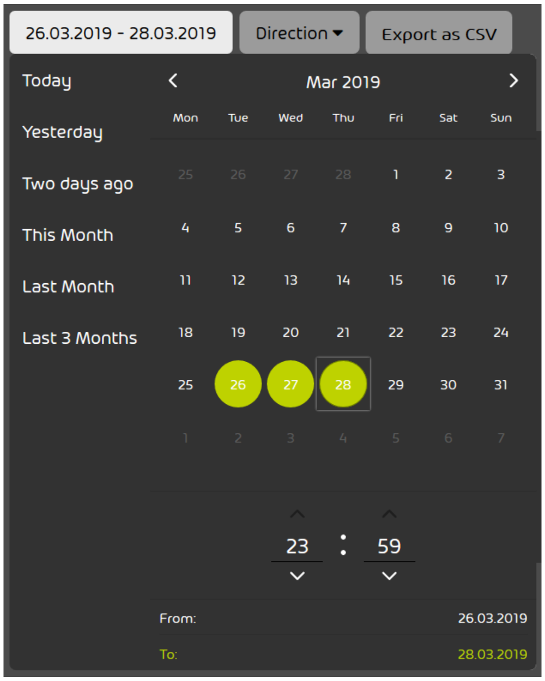


Figure 128: Select a period

➜

In the **Email Statistics** module, only data on emails from the selected date range is displayed.

6. Optional: In the drop-down menu **Direction**, select the direction of the emails that are to be included in the statistics. You can choose from the following options:

   - **Both**: Incoming and outgoing emails are included in the statistics.
   - **Incoming**: Only incoming emails are included in the statistics.
   - **Outgoing**: Only outgoing emails are included in the statistics.

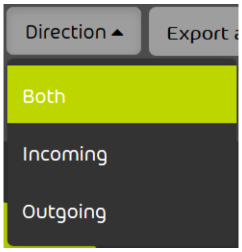


Figure 129: Select a direction

➜

In the **Email Statistics** module, only data on emails with the selected direction is displayed.

✓

The data in the **Email Statistics** module has been filtered by a date range and an email direction.

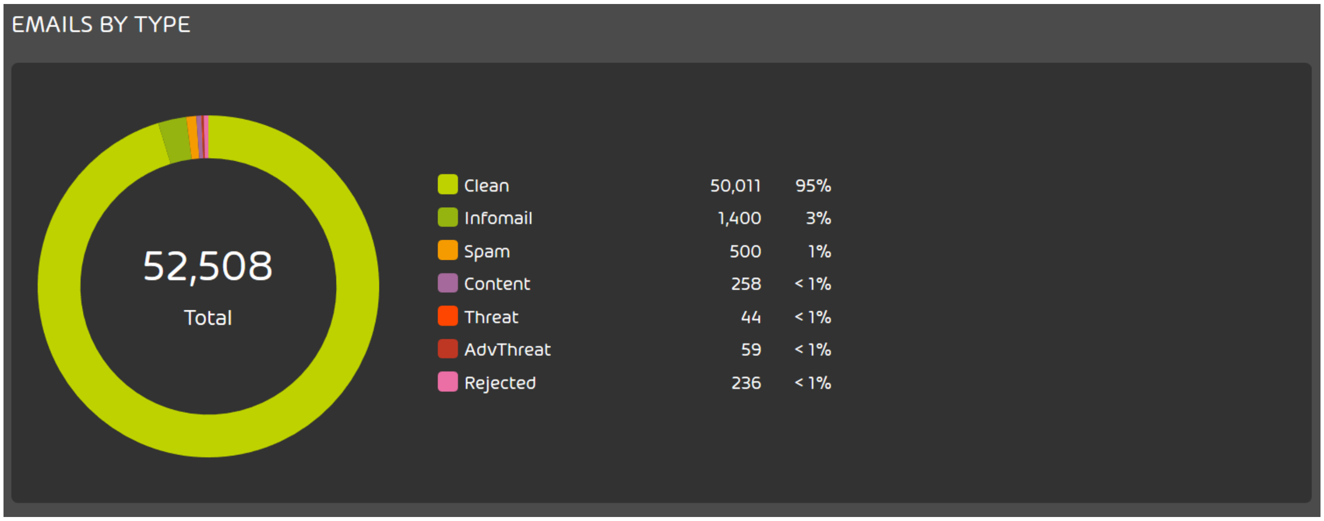
Emails by Type

The diagram **Emails by type** in the **Reporting & Compliance** > **Email Statistics** module shows how a user's emails or a domain's emails are distributed across the email categories in the Control Panel (see Email Categories on page 82).

Notice:

Regular users can view data about their own email traffic in the diagram.Customer-level administrators, as well as users with the **Service Desk** or the **Reporting** role (see Roles on page 49) can also see a domain's data or data of a user from a domain instead of their own data. The displayed data can be filtered by date range and email direction (see Filtering Email Statistics on page 157).

The diagram shows the total number of emails that were received and/or sent during the selected date range. Furthermore, the diagram shows the number and percentage of the emails that are assigned to each email category in the Control Panel.



Clean	50,011	95%
Infomail	1,400	3%
Spam	500	1%
Content	258	< 1%
Threat	44	< 1%
AdvThreat	59	< 1%
Rejected	236	< 1%

Figure 130: Emails by type

Emails by Time

The diagram **Emails by time** shows an overview of incoming and/or outgoing emails in the selected period. The numbers of emails per category are shown in absolute numbers.

Notice:

Regular users can view data about their own email traffic in the diagram.Customer-level administrators, as well as users with the **Service Desk** or the **Reporting** role (see Roles on page 49) can also see a domain's data or data of a user from a domain instead of their own data. The displayed data can be filtered by date range and email direction (see Filtering Email Statistics on page 157).

The diagram shows how many emails have been received and/or sent at different times during the selected date range. The diagram is divided into different colors by email category (see Email Categories on page 82).

Once the mouse pointer points to a position in the diagram, an overview is displayed for the nearest time, indicating how many emails of each category were received and/or sent at this time. Furthermore, a vertical line is displayed at the position of this time with dots for the different email categories. Once the mouse pointer points to one of these dots, the number of emails of this category is displayed.

Additionally, the data from the diagram can be exported as a CSV file (see Exporting Email Statistics as a CSV File on page 162).

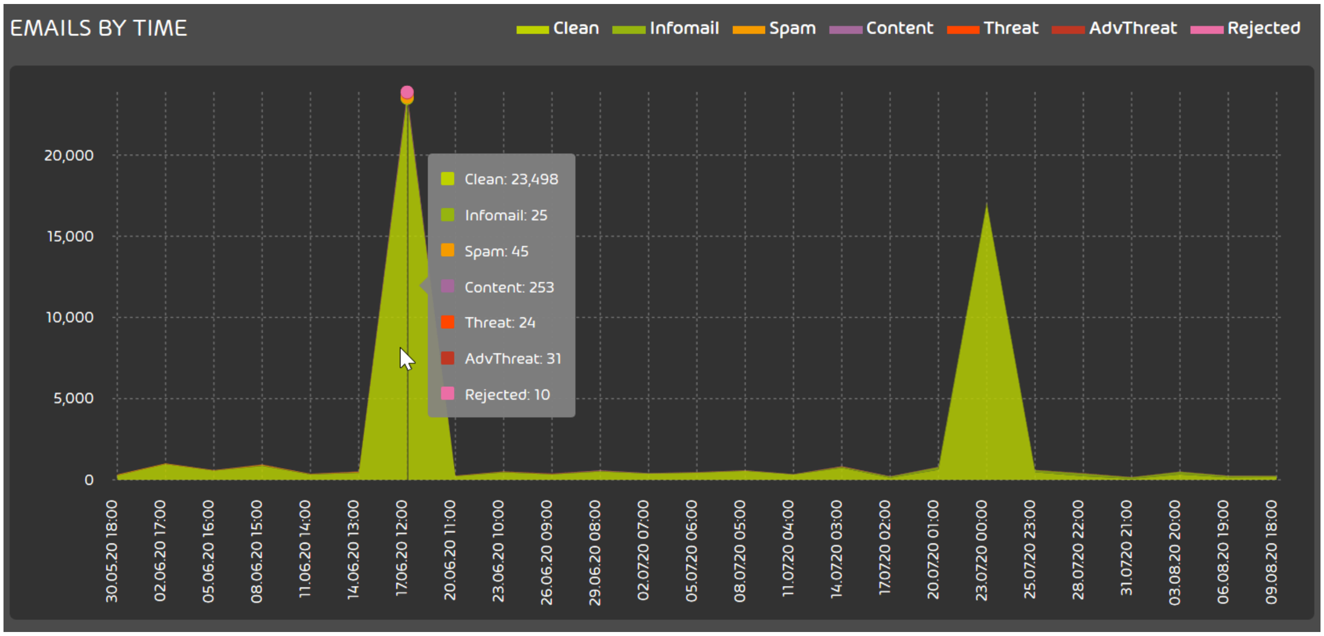


Figure 131: Emails by time

Exporting Email Statistics as a CSV File

The **Email Statistics** module contains a diagram that shows how emails are distributed over time (see Emails by Time on page 160). You can export the data of this diagram as a CSV file.As a customer-level administrator or a user with the **Service Desk** or the **Reporting** role (see Roles on page 49), you can export your own data, your domain's data or the data of a user from your domain.

1. Log in to the Control Panel with your credentials.
2. Optional: If you would like to export a domain's data or the data of a user from a domain instead of your own data, select the domain or the user in the scope selection.
3. Navigate to **Reporting & Compliance** > **Email Statistics**.
4. Select a date range and an email direction for the statistics (see Filtering Email Statistics on page 157).

   ➜

   Only emails from the selected date range and with the selected direction are included in the statistics.

5. Click on **Export as CSV**.

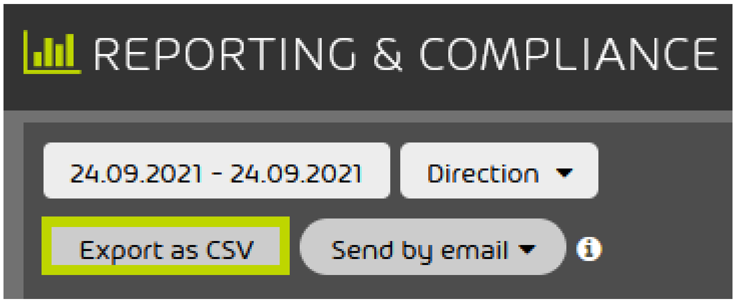


Figure 132: Export as a CSV file

➜

A CSV file with the data from the diagram on the distribution of emails over time is made available for download.

6. Download the file.

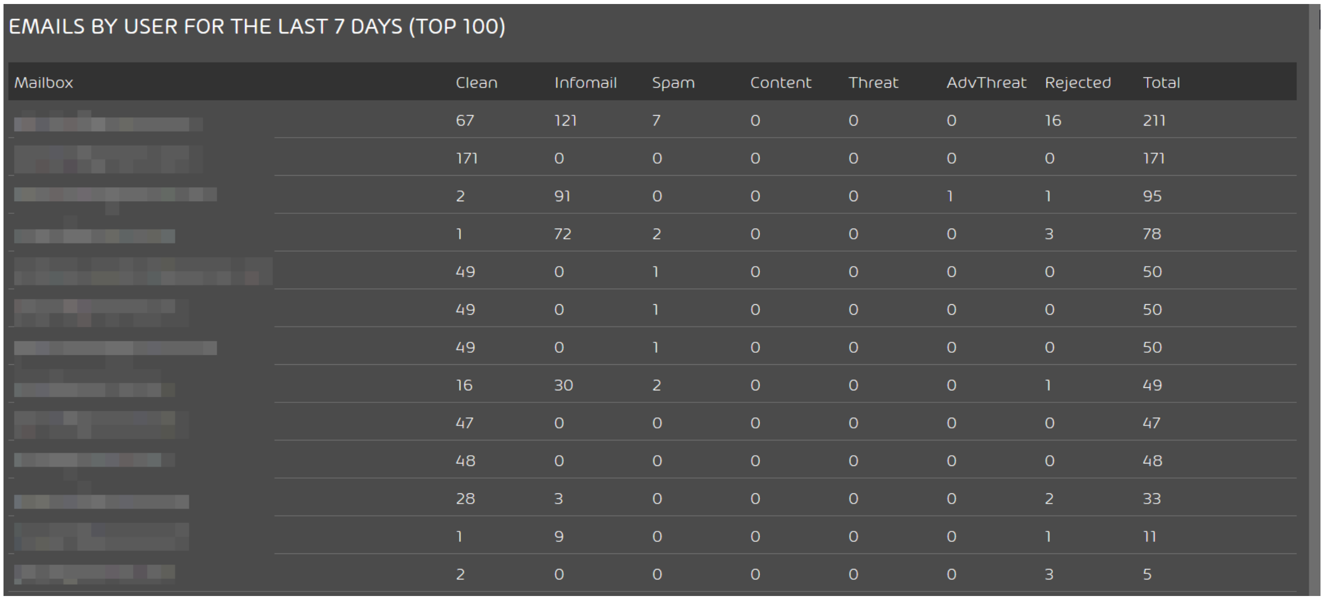
✓

The data of the diagram on the distribution of emails over time has been downloaded.

Emails by User

The statistics **Emails by user for the last 7 days (top 100)** in the **Reporting & Compliance** > **Email Statistics** module are available for customer-level administrators, as well as for users with the **Service Desk** or the **Reporting** role (see Roles on page 49). The statistics are only displayed if a domain has been selected in the scope selection (see Filtering Email Statistics on page 157). The statistics can be filtered by the email direction (see Filtering Email Statistics on page 157).

The statistics will list the 100 users of the domain who have received and/or sent emails the most in the last 7 days. Those users are sorted by the total number of their emails. Moreover, the number of emails on each email category (see Email Categories on page 82) is displayed.



EMAILS BY USER FOR THE LAST 7 DAYS (TOP 100)

Mailbox	Clean	Infomail	Spam	Content	Threat	AdvThreat	Rejected	Total
[redacted]	67	121	7	0	0	0	16	211
[redacted]	171	0	0	0	0	0	0	171
[redacted]	2	91	0	0	0	1	1	95
[redacted]	1	72	2	0	0	0	3	78
[redacted]	49	0	1	0	0	0	0	50
[redacted]	49	0	1	0	0	0	0	50
[redacted]	49	0	1	0	0	0	0	50
[redacted]	16	30	2	0	0	0	1	49
[redacted]	47	0	0	0	0	0	0	47
[redacted]	48	0	0	0	0	0	0	48
[redacted]	28	3	0	0	0	0	2	33
[redacted]	1	9	0	0	0	0	1	11
[redacted]	2	0	0	0	0	0	3	5

Figure 133: Emails by user

Monthly Report

The email statistics of a domain can be summarized in a report every month. The monthly report is sent to selected recipients at the beginning of each month and summarizes the email statistics of the past month.

Customer-level administrators can select the recipients to which the monthly report shall be sent. The monthly report can be sent both to users of the domain and to external mailboxes. Administrators can add recipients individually (see Adding Recipients on page 165) or import a list of recipients from a CSV file (see Importing Recipients from a CSV File on page 167). These CSV files must meet certain requirements (see CSV Files for Recipient Import on page 169). When a recipient is no longer required, administrators can remove them (see Removing Recipients on page 170).

Adding Recipients

Once a month, a report with the email statistics (see Email Statistics on page 156) of the past month is sent to selected recipients for each domain. You can add single users of your domain and external mailboxes as recipients.

Notice:

Control Panel users receive the monthly report in the language that is set in their user settings (see chapter "Changing the Timezone and Language" in the Control Panel manual). External recipients receive the monthly report in English.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for whose monthly report you would like to define recipients.
3. Navigate to **Reporting & Compliance** > **Email Statistics**.
4. Click on **Send by email**.

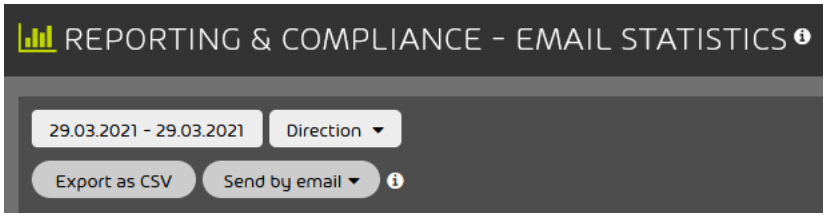


Figure 134: Open monthly report settings

➜

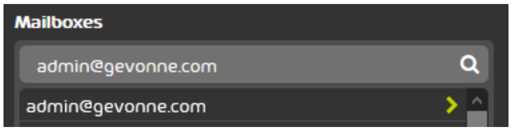
The settings of the monthly report are displayed.

5. Optional: If you would like to set a user of the domain as a recipient, proceed as follows.

   a) Enter the user's email address in the search field under **Mailboxes** and press Enter.

      ➡

      The search results are displayed in the list under the search field.



Mailboxes

admin@gevonne.com

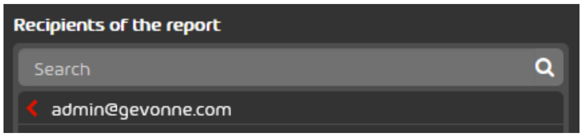
admin@gevonne.com

Figure 135: Search results

   b) Click on the user's email address in the list.

      ➡

      The email address is added to the list of recipients.



Recipients of the report

Search

admin@gevonne.com

Figure 136: List of recipients

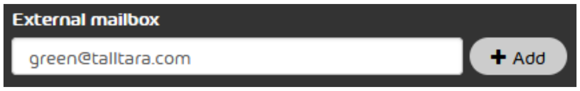
6. Optional: If you would like to set an external mailbox as a recipient, proceed as follows.

   a) Enter the external email address in the **External mailbox** field.

      ➡

      The button **Add** is enabled.

   b) Click on **Add**.



External mailbox

green@talltara.com

+ Add

Figure 137: Add an external mailbox

➡ The external email address is added to the list of recipients.

7. Click on **Apply changes**.

   ➔

   The changes are applied.

✓

Individual recipients of the monthly report have been defined.

Importing Recipients from a CSV File

Once a month, a report with the email statistics (see Email Statistics on page 156) of the past month is sent to selected recipients for each domain. You can import new recipients from a CSV file. The CSV file can contain both users of the domain and external mailboxes.

> **Notice:**
>
> Control Panel users receive the monthly report in the language that is set in their user settings (see chapter "Changing the Timezone and Language" in the Control Panel manual). External recipients receive the monthly report in English.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for whose monthly report you would like to define recipients.
3. Navigate to **Reporting & Compliance** > **Email Statistics**.

4. Click on **Send by email**.

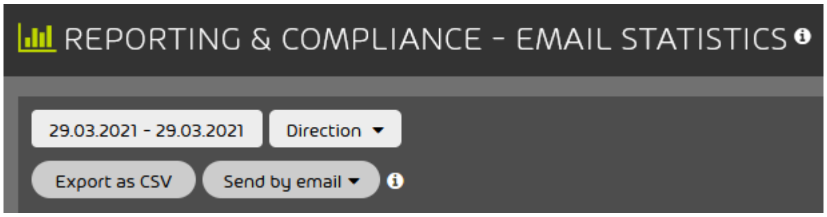


Figure 138: Open monthly report settings

➜

The settings of the monthly report are displayed.

5. Click on **Import list from CSV file**.

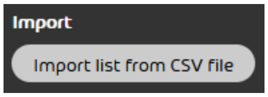


Figure 139: Import list from CSV file

➜

A file selection window opens.

6. **Important:**

   To ensure that an external CSV file can be imported into the Control Panel without errors, rules regarding the file format, structure of its contents as well as a valid syntax must be observed (see CSV Files for Recipient Import on page 169).

   Select the desired CSV file.

➜

The email addresses from the CSV file are added to the list of recipients.

✓

Monthly report recipients have been imported from a CSV file.

CSV Files for Recipient Import

A list of recipients for the monthly report can be imported from a CSV file (see Importing Recipients from a CSV File on page 167). To ensure that an external CSV file containing recipients of the monthly report can be imported into the Control Panel without errors, rules regarding the file extension and content structure must be observed. The CSV file can contain both email addresses of Control Panel users and email addresses of external mailboxes.

Rule for the file extension

- The extension of the import file is **.csv**. Other file extensions, such as .txt or .docx, will not be accepted.

Rules for columns and rows

- The CSV file contains only one column.
- The first row contains the column name. The column name can be freely defined.
- From the second row on, the CSV file contains a recipient's email address in each row.
- The rows end without any punctuation sign.

Rule for the formatting of email addresses

- The email addresses are correctly formatted (according to the pattern "local-part@hostname.top-level-domain").

Important:

Incorrectly formatted addresses are not considered during the import.

Rule for duplicated entries

- Duplicated entries do not affect the processing of the CSV file, but should be avoided.

Removing Recipients

You have defined recipients for the monthly report (see Adding Recipients on page 165 or Importing Recipients from a CSV File on page 167).

If a recipient of the monthly report does not need to receive any more reports in the future, you can remove the recipient.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for whose monthly report you would like to define recipients.
3. Navigate to **Reporting & Compliance** > **Email Statistics**.
4. Click on **Send by email**.

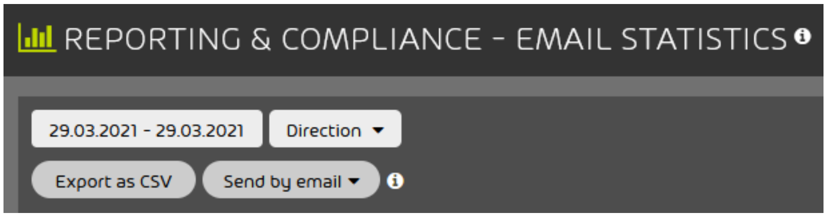


Figure 140: Open monthly report settings

The settings of the monthly report are displayed.

5. In the list of recipients, click on the recipient that you would like to remove.

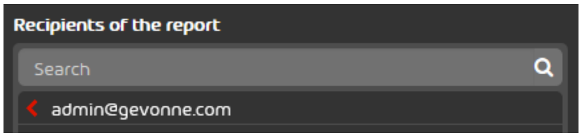


Figure 141: Removing Recipients

The recipient is removed from the list.

A recipient of the monthly report has been removed.

Threat Live Report

About Threat Live Report

> **Important:**
>
> Threat Live Report is available for customers who have booked **Advanced Threat Protection**.

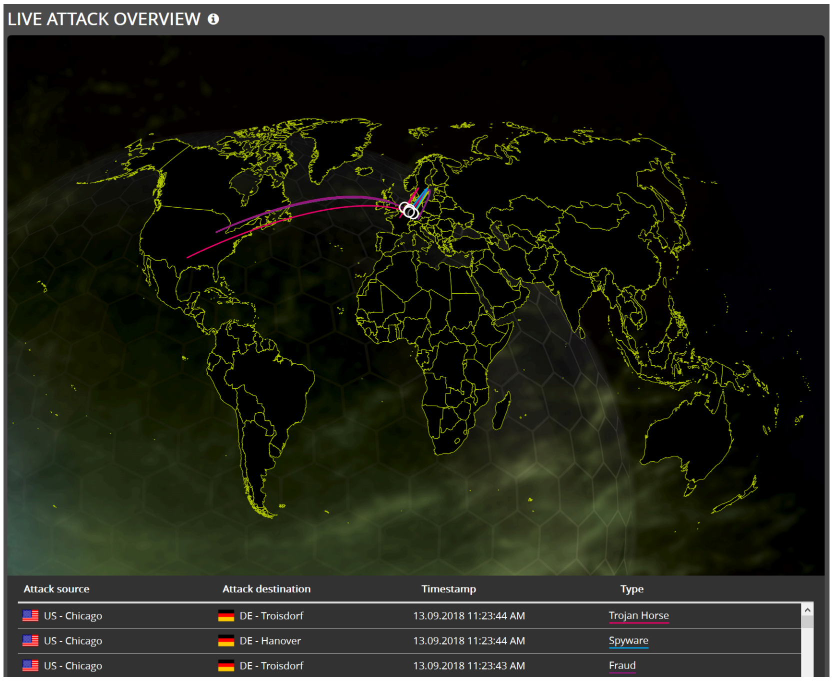
Information on the charts is also given directly in the interface. Place the mouse pointer on the ⓘ behind the name of the corresponding statistics or diagram.

Description of Statistics

Live Attack Overview

The **Live Attack Overview** under **Threat Live Report** shows all attacks against your company or all users of the Control Panel that are being prevented in real time (see Switching between Global and Domain-Specific Data on page 182). The source, target and attack type are displayed in a table.

You can find a description of all possible attack types under Description of Attack Types on page 178.



Attack source	Attack destination	Timestamp	Type
US - Chicago	DE - Troisdorf	13.09.2018 11:23:44 AM	Trojan Horse
US - Chicago	DE - Hanover	13.09.2018 11:23:44 AM	Spyware
US - Chicago	DE - Troisdorf	13.09.2018 11:23:43 AM	Fraud

Figure 142: Live Attack Overview

Attempted Attacks - Attack Type by Date

The statistics **Attack type by date** under **Threat Live Report** show how many attacks per attack type took place at a certain time in the selected period. The data can refer either to the currently selected domain or to all customers (see Switching between Global and Domain-Specific Data on page 182).

To view the absolute numbers of attacks per attack type at a certain time, you can move the cursor over the vertical lines. If the cursor is placed over one of the points of an attack type, only the corresponding chart and information about the number of attacks will be displayed.

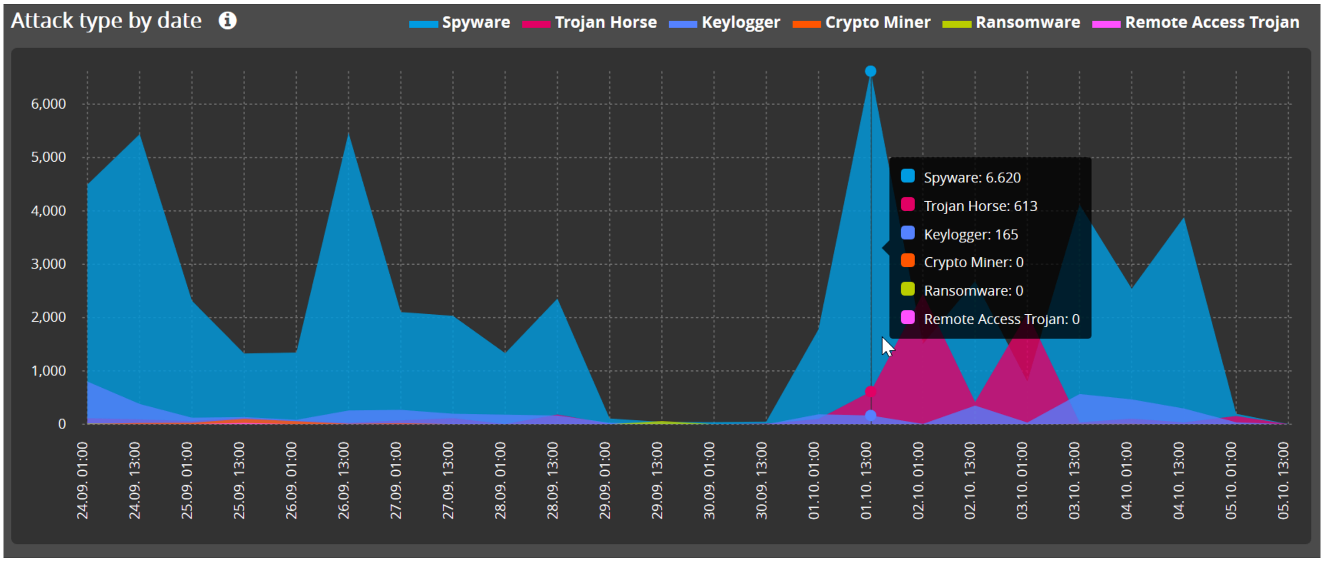


Figure 143: Attempted attacks - attack type by date

Threat Statistics by Attack Type

The chart **By attack type** under **Threat Live Report** shows the distribution of attacks at a certain time by their attack type. In the center, the total number of attacks that took place in the selected period is displayed. The data can refer either to the currently selected domain or to all customers (see Switching between Global and Domain-Specific Data on page 182). You can find a description of the attack types under Description of Attack Types on page 178.

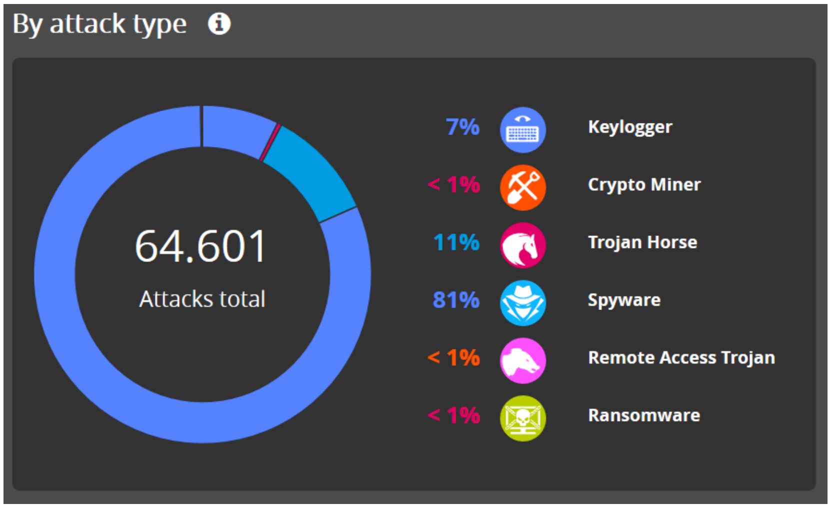


Figure 144: Threat statistics by attack type

Threat Statistics by Attack Vector

The chart **By attack vector** under **Threat Live Report** shows the distribution of attacks at a certain time by their attack vector. In the center, the total number of attacks that took place in the selected period is displayed. The data can refer either to the currently selected domain or to all customers (see Switching between Global and Domain-Specific Data on page 182). You can find a description under Description of Attack Vectors on page 181.

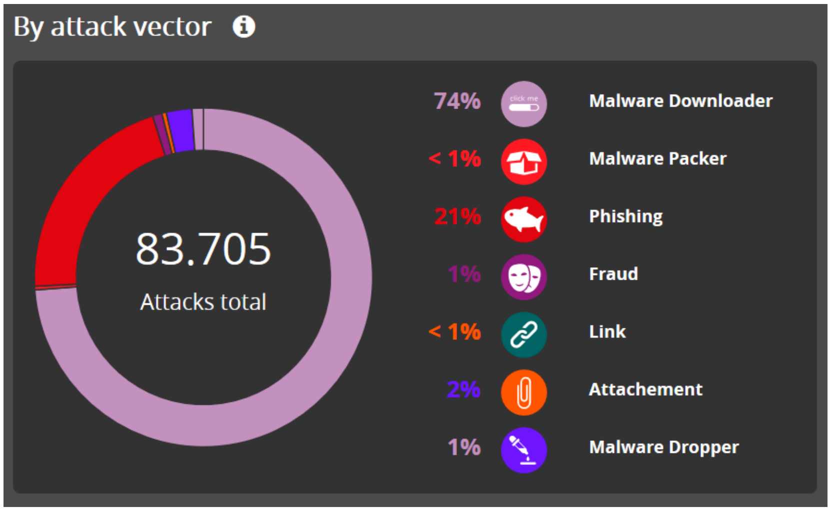


Figure 145: Threat statistics by attack vector

Attempted Attacks - Attack Vector by Date

The statistics **Attack vectors by date** under **Threat Live Report** show how many attacks per attack vector took place at a certain time in the selected period. The data can refer either to the currently selected domain or to all customers (see Switching between Global and Domain-Specific Data on page 182).

To view the absolute numbers of attacks per attack vector at a certain time, you can move the cursor over the vertical lines. If the cursor is placed over one of the points of an attack vector, only the corresponding chart and information about the number of attacks will be displayed.

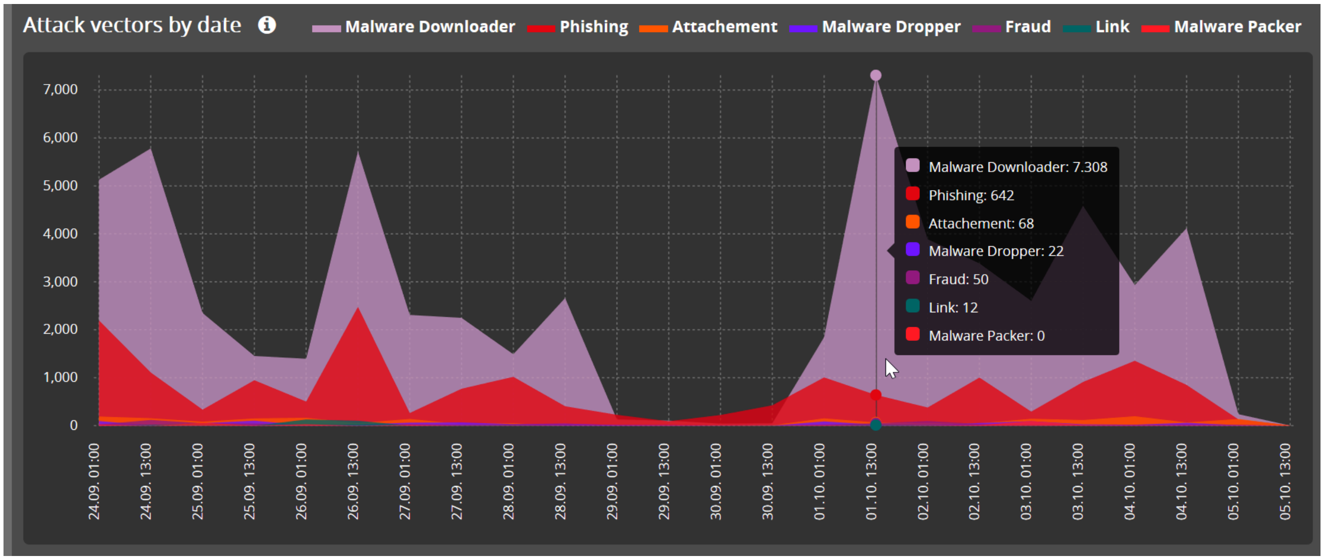


Figure 146: Threat statistics - attack vectors by date

URL Rewriting Statistics

The statistics and charts under **Secure Links Statistics** each represent the number of clicked links in emails rewritten by the URL Rewriting engine in the selected time period. This refers to global data for all customers and is not rectricted to data for the selected domain. Under **Secure Links Statistics**, the following statistics and charts are displayed:

- The statistics **Clicks by time of day** show the distribution of clicks on links in emails by time of day in percent.

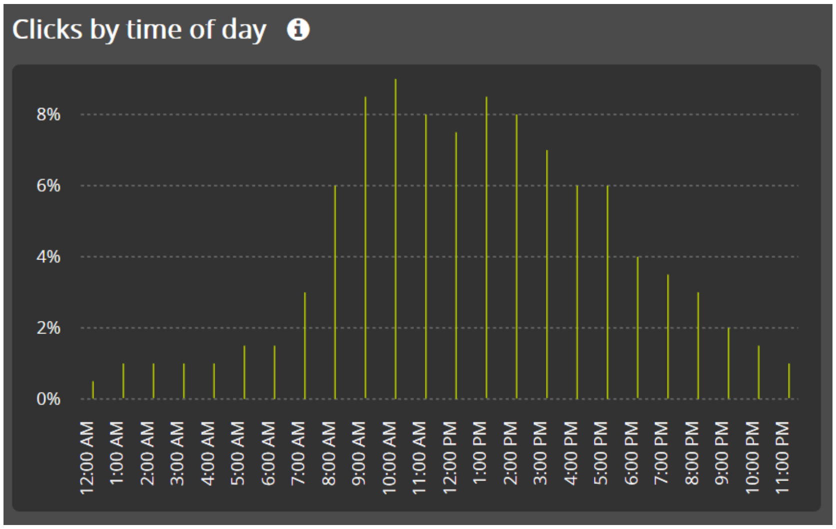


Figure 147: Clicks by time of day

- The statistics **Clicks by device** show the distribution of clicks by device in percent.

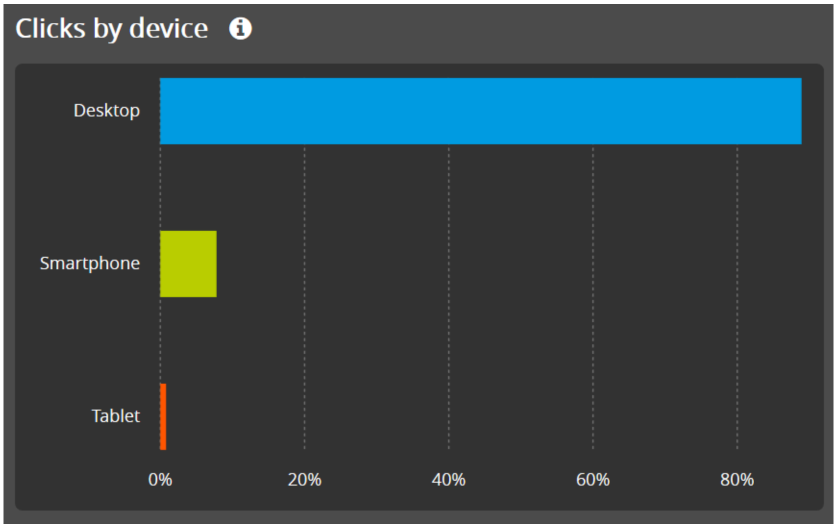


Figure 148: Clicks by device

- The chart **Clicks by operating system (OS)** shows the distribution of clicks by operating system in percent.

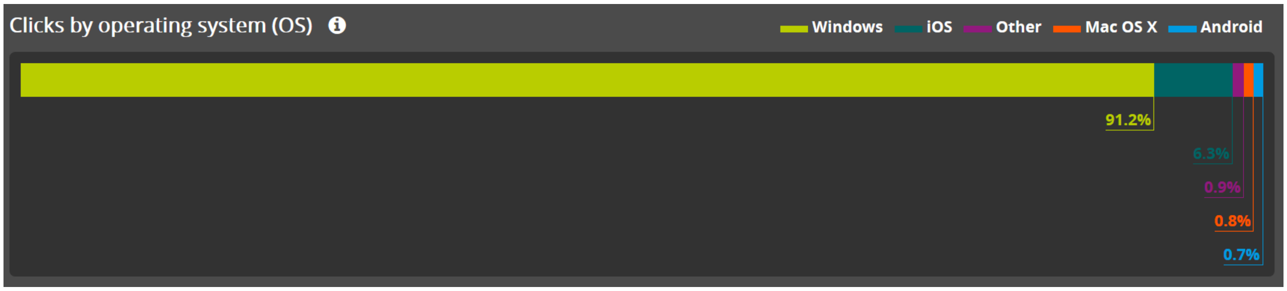


Figure 149: Clicks by operating system (OS)

Attack Types and Vectors

Description of Attack Types

Table 9: Attack types

NAME OF THE ATTACK TYPE	EXPLANATION
Backdoor	A backdoor malware has a similar goal as a remote access Trojan but uses a different approach. The attackers use so-called backdoors, which are sometimes deliberately placed in programs or operating systems. However, they may also have been installed secretly. The peculiarity of backdoors is the fact that they bypass the usual defense mechanisms and are therefore very attractive for cyber criminals. For example, they are very popular for creating botnets.
Banking Trojan	Banking trojans are a malware type that attempts to steal sensitive data such as bank details or email data. Attackers often succeed by combining this with phishing attacks, where a website pretends to be an official bank website.

NAME OF THE ATTACK TYPE	EXPLANATION
Bot	A bot does not always have to be a malware, initially a bot is a computer program that executes tasks independently and automatically. If several bots communicate with each other, this is called a botnet. Botnets are large collections of infected computers that an attacker builds up. An attacker can send commands to all computers simultaneously to trigger activities. The deceptive thing is that the owners of the computers do not notice the "membership" in a botnet until it executes externally controlled activities.
Crypto Miner	A crypto miner is a malware used to mine digital currencies. Criminals infect computers with crypto miners to take advantage of their computing power or cloud CPU load. This reduces the performance of the computer as well as the lifespan. Furthermore, entire company networks can be shut down by crypto miners.
Keylogger	Keyloggers are malware types that can be implemented by hardware or software. Keyloggers record a user's keystrokes and speech and are able to access sensitive data or passwords.
Point-of-Sale Trojan	Point-of-sale Trojans are a type of malware that attacks sales systems in which transactions with sensitive payment data take place. Cyber criminals use point-of-sale Trojans to gain access to unencrypted customer data from bank and credit cards.
Ransomware	Ransomware is an attack that encrypts files on the target system. The files cannot be opened without a key. The attackers demand a large sum of ransom money to hand over the key. Even if only one computer is infected initially, Ransomware can spread across the entire network.

NAME OF THE ATTACK TYPE	EXPLANATION
Remote Access Trojans	A remote access Trojan (RAT) allows attackers to take over computers and control them remotely. This allows them to execute commands on the victim's systems and distribute RATs to other computers with the goal of building a botnet.
Root Kit	A root kit can be used to hide malicious code from detection. This form of attack involves the attacker intruding deeply into the computer system, gaining root privileges and general access rights. Cyber criminals then change the system so that the user no longer recognizes when processes and activities are started. Attacks based on rootkit obfuscations are therefore very difficult to detect.
Spyware	Spyware is malware that collects information on the victim's computer. This information can be, for example, access data for user accounts, sensitive banking data or surfing behavior. Users usually do not know that they have become victims of spyware.
Trojan horses	Trojan horses are programs that disguise themselves as benign but contain harmful code. The user only detects the clean application, while the background execution of malicious code infects the system. The user can no longer influence the effects from this point on.

Description of Attack Vectors

Table 10: Attack Vectors

NAME OF THE ATTACK VECTOR	EXPLANATION
Attachment	An attachment of an email is a file that can contain malware.
Link	A link in an email is a connection to another website. Malware can hide behind this link.
Link Dropper	Link Droppers are links that serve as carriers for malware. The link itself is not harmful but allows the malware behind it to execute itself.
Link Downloader	Link downloaders are links in emails that contain malware. If the victim clicks on this link, the malware is downloaded.
Malware Downloader	Malware downloaders are considered Trojans because they secretly download malicious files from a remote server.
Malware Dropper	Malware Droppers are not malware, but transport malware into the system. From the outside, the Malware Dropper appears harmless and can camouflage itself as a file. However, the files it contains can run themselves and infect the system with malware.
Malware Packer	Malware packers are a malware type in which criminals compress their malicious programs using a variety of methods. This is an attempt to bypass malware analysis.

NAME OF THE ATTACK VECTOR	EXPLANATION
Fraud	Fraud in relation to the Internet means obtaining sensitive data, money or bank details of users through Internet services. For example, websites or transactions can pretend to be real, but are programmed by cybercriminals. A well-known variant is CEO fraud, in which criminals pose as managing directors and contact the accounting department of a company by phone or email to instruct the transfer of large sums of money.
Phishing	Phishing is a combination of the words "password" and "fishing" and thus refers to "fishing for passwords." Cyber criminals claim that emails or websites are genuine and thus cause users to enter sensitive data there. Users thus voluntarily disclose their data without knowing that the data will fall into the hands of the criminals.

Actions in Threat Live Report

Switching between Global and Domain-Specific Data

☑ You have not yet toggled the **global** switch under **Threat Live Report**.

In the **Live Attack Overview** section and the charts and statistics under **Attempted Attacks** and **Threat Statistics**, you can choose between displaying global data for all customers or data for the domain currently selected in the scope selection. The display of domain-specific data is selected by default.

Notice:

In contrast, the charts under **Secure Links Statistics** always display only global data for all customers and cannot be modified.

1. Select a domain from the scope selection.

   The **Threat Live Report** module under **Reporting & Compliance** is enabled.

2. Navigate to **Reporting & Compliance** > **Threat Live Report**.
3. Toggle the switch **global**.

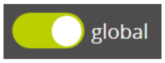


Figure 150: Switch global highlighted in green

   The switch **global** is highlighted in green. The charts and statistics under **Live Attack Overview**, **Attempted Attacks** and **Threat Statistics** now use global data for all customers.

4. Toggle the **global** switch again.

   The **global** switch is grayed out. The charts and statistics under **Live Attack Overview**, **Attempted Attacks** and **Threat Statistics** now use data for the domain selected in the scope selection.

The display of charts and statistics under **Threat Live Report** has been switched from global to domain-specific data (or vice versa).

Selecting a Display Period

You can select a display period for the charts and statistics under **Attempted Attacks**, **Threat Statistics** and **Secure Links Statistics**.

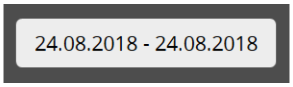
Notice:

The **Live Attack Overview** section always displays real-time data and is not affected by the selected period.

1. Select a domain from the scope selection.

   ➔

   The **Threat Live Report** module under **Reporting & Compliance** is enabled.
2. Navigate to **Reporting & Compliance** > **Threat Live Report**.
3. Click on the date selection button.



24.08.2018 - 24.08.2018

Figure 151: Click on the date selection button

   ➔

   A date selection calendar is displayed.
4. Select the desired period manually.

   a) Click on the first day of the desired period in the calendar.

   b) Click on the last day next to the desired period.

      ➔

      The desired period is selected.

   ➔

   The charts and statistics mentioned above only display data from the selected period.

5. Select a predefined period. You have the following options:

    - **Today**: The period is limited to the present day.
    - **Yesterday**: The period is limited to the day before the present day.
    - **Two days ago**: The period is limited to the day two days before the present day.
    - **This month**: The current calendar month is selected as the period.
    - **Last month**: The calendar month before the current calendar month is selected as the period.
    - **Last 3 months**: The current calendar month and the two preceding calendar months are selected as the period.
    - **This year**: The current calendar year is selected as the period.
    - **Last 12 months**: The last 12 months are selected as the period.

    The charts and statistics mentioned above only display data from the selected period.

The display period has been selected.

Auditing 2.0

Auditing 2.0

In the **Auditing 2.0** module, the activities of the Control Panel users are documented in an audit log. The audit log allows customer-level and partner-level administrators to track their users' activities. Administrators can determine, for example, which user is responsible for deleting a record and at what time this action was performed. This enables administrators to undo the actions if required.

Each log entry represents an event that was performed by a Control Panel user. Information on several categories is stored for each event (see Categories on page 186). Administrators can select which of these categories are displayed in the audit log (see Selecting the Displayed Categories on page 188).

To facilitate the search for entries, administrators can filter the entries in the audit log. Administrators can specify the period for which entries are displayed in the audit log (see Selecting a Display Period on page 190). Administrators can also filter entries by actions (see Filtering by Action on page 191) and events (see Filtering by Events on page 193). If desired, administrators can reset the filter settings back to default (see Resetting the Settings on page 203). In addition, administrators can search the audit log entries for search terms (see Searching Entries on page 204).

To view which values have changed due to an event in the Control Panel, administrators can open the entry of the event (see Opening an Entry on page 205). Furthermore, administrators can export the displayed entries as a CSV file (see Exporting Entries on page 206).

Categories

In the **Auditing 2.0** module (see Auditing 2.0 on page 185), events performed by Control Panel users are documented in an audit log. Information on several categories is stored for each log entry. Each column of the audit log corresponds to a category. The categories are explained in the table listed below.

Table 11: Categories in the audit log

CATEGORY	EXPLANATION
Timestamp	Shows at which time the action was performed.
User	Shows which user has performed the action.
Target	Shows the user for whom the action was performed.
Event	Shows the event, e.g. a change of user settings, deny list, allow list, credentials or a login.
Action	Explains if an action has created, updated or deleted something. Success or failure indicate if a login was successful.

CATEGORY	EXPLANATION
Target path	Shows under which domain the user is created for whom the action was performed.
App ID	Shows the identification numbers of the applications that use the API. Applications can communicate with our Services via the API. For more information about the API, see the manual "Application Programming Interface (API)".
App version	Shows the version of the application which communicates with the API.
IP	Shows the IPv4 address of the user who performed the action.
URL	Shows the path to the API endpoint which is used.

The following categories are displayed in the audit log by default:

- **Timestamp**
- **User**
- **Target**
- **Event**
- **Action**

In addition, administrators can have the following categories displayed in the audit log (see Selecting the Displayed Categories on page 188):

- **Target path**
- **App ID**
- **App version**
- **IP**
- **URL**

Selecting the Displayed Categories

The audit log in the **Auditing 2.0** module (see Auditing 2.0 on page 185) contains information on different categories (see Categories on page 186). You can select which categories are displayed in the audit log. Each table column of the audit log corresponds to a category.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the customer whose audit log you would like to open.
3. Navigate to **Reporting & Compliance** > **Auditing 2.0**.

4. Click on the ▣ button in the upper right corner of the table.

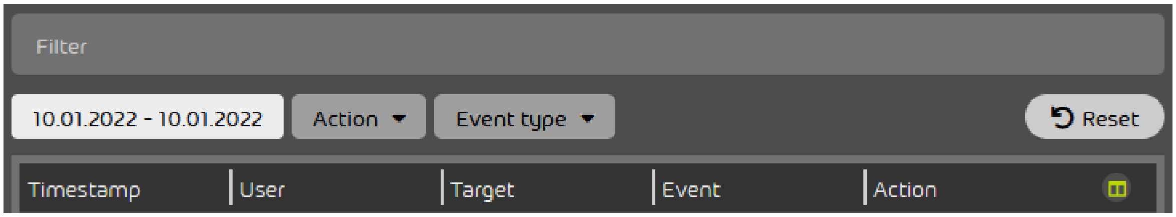


Figure 152: Open the overview of available categories

➔

A list of all available categories is displayed. The categories that are currently displayed in the audit log are highlighted in green.

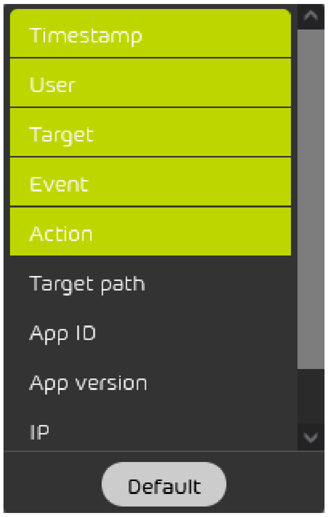


Figure 153: Available categories

5. To display a category that is currently hidden in the audit log, click on the category.

➔

The category is highlighted in green.

6. To hide a category that is currently displayed from the audit log, click on the category.

   The category is no longer highlighted in green.

7. Optional: To reset the table columns of the audit log to the default settings, click on **Default**.

   The table columns of the audit log are reset to the default settings.

8. Click in the window outside the list to close it.

   The list is closed. The selected categories are displayed in the audit log.

Categories to be displayed in the audit log have been selected.

Filtering of Entries

Selecting a Display Period

In the **Auditing 2.0** module (see Auditing 2.0 on page 185), you can select a display period for the audit log.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the customer whose audit log you would like to open.
3. Navigate to **Reporting & Compliance** > **Auditing 2.0**.

4. Click on the displayed date range.

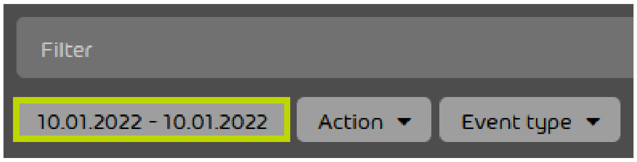


Figure 154: Select a period

➔

A calendar opens.

5. In the calendar, select the period for which events are to be displayed in the audit log.

➔

All days of the selected period are highlighted in the calendar. The start date and the end date are displayed below the calendar.

6. Click in the window outside the calendar to close it.

➔

The calendar closes. Only events from the selected period are displayed in the audit log.

✓

A display period has been selected for the audit log.

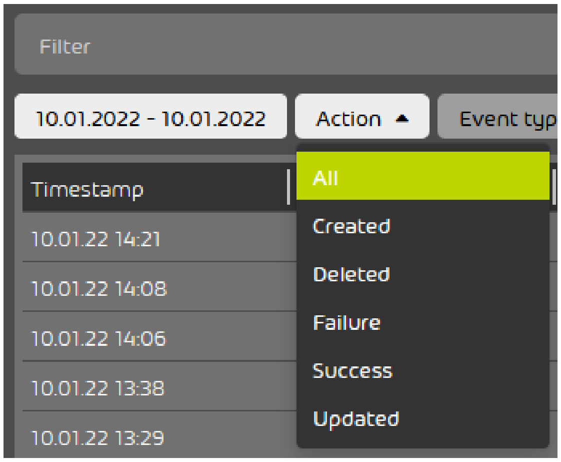
Filtering by Action

Actions to filter by

Administrators can filter the entries from the audit log in the **Auditing 2.0** module (see Auditing 2.0 on page 185) by actions. To do so, administrators can select an action from the **Action** drop-down menu. After the selection, only entries of the selected action are displayed.

Notice:

It is only possible to filter by one action at a time.



10.01.22 14:21
10.01.22 14:08
10.01.22 14:06
10.01.22 13:38
10.01.22 13:29

Figure 155: Filter by Action

The following table lists the actions that administrators can filter by.

Table 12: Actions

ACTION	EXPLANATION
All	Shows all actions that took place in the selected period.
Updated	Shows all actions that updated something.
Success	Shows all logins that were successful.
Created	Shows all actions that created something.
Failure	Shows all logins that failed.
Deleted	Shows all actions that deleted something.

Filtering by Events

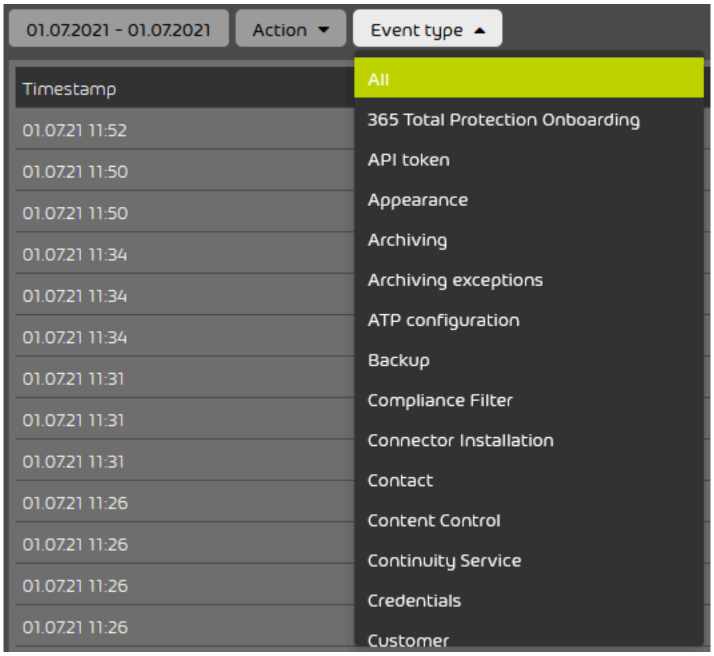
Events to filter by

Administrators can filter the entries from the audit log in the **Auditing 2.0** module (see Auditing 2.0 on page 185) by events. Administrators can select an event from the drop-down menu **Event type**. Once an event has been selected, only the entries for this event are displayed.

> **Notice:**
>
> It is only possible to filter by one event at a time.

In the **Auditing 2.0** module, administrators can view all events that have taken place at the level of the currently selected partner or customer, as well as all subordinate scopes. Entries for the **Email action** event are audited at the level of the highest scope accessible to the user who caused the event.

> **Notice:**
>
> With the exception of the **Email action** event, all entries are audited at the level of the scope that was selected in the scope selection when the event took place (see chapter 'Scope Selection' in the Control Panel manual).



Timestamp
01.07.21 11:52
01.07.21 11:50
01.07.21 11:50
01.07.21 11:34
01.07.21 11:34
01.07.21 11:34
01.07.21 11:31
01.07.21 11:31
01.07.21 11:31
01.07.21 11:26
01.07.21 11:26
01.07.21 11:26
01.07.21 11:26

Figure 156: Filter by event

The following table lists the events that administrators can filter by.

Table 13: Events to filter by

EVENT	EXPLANATION
All	Shows all modifications in the Control Panel.
General LDAP settings	Filters for events that have led to an update of the general settings for all LDAP connections in the **Service Dashboard** module.
Out of office note	Filters by events that have led to an update of the settings for out of office notes in the **User Settings** module.
Credentials	Filters by events that have led to an update of the credentials of a user.

EVENT	EXPLANATION
Login	Filters by successful and failed Control Panel logins.
API token	Filters by events that have led to the creation or deletion of API tokens in the **API Token** tab in the **User Settings** module.
ATP configuration	Filters by events that have led to an update of the settings in the **Advanced Threat Protection** module.
Appearance	Filters by events that have led to an update of the settings in the **Control Panel** tab in the **Customization** module.
Quarantine report appearance	Filters for events that have led to an update of the appearance of quarantine reports. This includes changes in the **Customization** and **Quarantine Report** modules.
Auto logout: configuration	Filters by events that have led to the creation, an update or the deletion of custom settings for the auto logout of inactive users in the **Customer Settings** > **Authentication policies & IPs** module.
Backup	Filters for events that have led to the activation of data backup and restore services.

EVENT	EXPLANATION
User actions	Filters by events that have led to the creation, an update or the deletion of the settings for the allowed actions in the **User Rights** tab in the **Spam and Malware Protection** module.
User settings	Filters by events that have led to the creation, an update or the deletion of settings under **User Settings**. Changes to a partner's or customer's default values for the timezone, language, date format and time format in the **Service Dashboard** module (see chapter "Setting Default Values for Timezone and Language" in the Control Panel manual) are also audited under this event.
Deny & Allow Lists	Filters by events that have led to an update of the settings in the **Deny & Allow Lists** module.
Compliance Filter	Filters by events that have led to the creation, an update or the deletion of rules as well as an update of the settings in the **Compliance Filter** module.
Connector Installation	Filters by events that have led to the installation of connectors.
Content Control	Filters by events that have led to the creation or an update of the settings in the **Content Control** module.
Continuity Service	Filters by events that have led to an update of the settings in the **Continuity Service** module.

EVENT	EXPLANATION
Domain	Filters by events that have led to the creation, an update or the deletion of domains in the **Domains** module.
Email address	Filters by events that have led to the creation, an update or the deletion of email addresses in the **Mailboxes** module.
Email action	Filters by events related to email actions in the **Email Live Tracking** module. The following email actions are recorded with the status **Updated**: · **Report as spam** · **Report as infomail** · **Mark as private** The email action **Delete email** is recorded with the status **Deleted**. The following email actions are recorded with the status **Success**: · **Deliver email** · **Add sender to deny list** · **Add sender to allow list & deliver email** · **Add to deny list for all users** · **Add to allow list for all users** · **Send email to admin** · **ATP scan**

EVENT	EXPLANATION
Email information	Filters by events that have led to an update of the settings in the **Email information** tab in the **Customization** module.
Email statistics recipients	Filters by events that have led to the addition or removal of mailboxes to or from the email statistics recipient list in the **Email Statistics** module.
Email preview	Filters by events that have led to the creation of an email preview in the **Email Live Tracking** module.
Email Authentication	Filters by events that have led to the creation or deletion of exceptions as well as to the update of the settings in the **Email Authentication** module.
Terms and Conditions	Filters by events that have led to the creation or an update of the settings in the **Terms and Conditions** tab in the **Service Dashboard** module.
Group	Filters by events that have led to the creation, an update or the deletion of groups in the **Groups** module.
Content of terms and conditions	Filters by events that have led to the creation of a text of the end-user license agreement and the data processing agreement in the **Terms and Conditions** tab in the **Service Dashboard** module.

EVENT	EXPLANATION
Outlook Add-in	Filters by events that have led to an update of the settings in the Outlook Add-In.
Contact	Filters by events that have led to the creation, an update or the deletion of contacts in the **Service Dashboard** module.
Customer	Filters by events that have led to the creation or deletion of customers in the **Service Dashboard** module.
LDAP connection	Filters for events that have led to the creation, an update or the deletion of the settings of an LDAP connection in the **Service Dashboard** module.
Migration of a single mailbox	Filters by events that have led to an update or the deletion of a data migration job for a single mailbox during mailbox migration in the **365 Total Protection** module.
Migration of several mailboxes	Filters by events that have led to the creation, an update or the deletion of a data migration job for several mailboxes during mailbox data migration in the **365 Total Protection** module.

EVENT	EXPLANATION
Multi-factor authentication	Filters by events that have led to the creation, an update or the deletion of settings related to multi-factor authentication. Creation means that multi-factor authentication has been enabled for the users of a domain in the **Customer Settings** > **Authentication policies & IPs** module. Update means that a user has configured multi-factor authentication for their own account under **User settings**. Deletion means that a user has deactivated multi-factor authentication for their own account under **User settings**, that an administrator has reset multi-factor authentication for a user in the **Customer Settings** > **Mailboxes** module or that an administrator has deactivated multi-factor authentication for the users of a domain in the **Customer Settings** > **Authentication policies & IPs** module.
Newsletter	Filters by events that have led to the subscription of newsletters for customers or partners in the **Service Dashboard** module.
Partner	Filters by events that have led to the creation or deletion of partners in the **Service Dashboard** module.
Mailbox	Filters by events that have led to the creation or an update of mailboxes in the **Mailboxes** module.

EVENT	EXPLANATION
Quarantine Report	Filters by events that have led to an update of the settings in the **Quarantine Report** module.
Role assignment	Filters by events that have led to the creation, an update or the deletion of role assignments in the **Service Dashboard** module.
Spam and Malware Protection	Filters by events that have led to an update of the settings in the **Spam and Malware Protection** module.
Support information	Filters by events that have led to an update of the settings in the **Support information** tab in the **Customization** module.
Targeted Fraud Forensics Filter groups	Filters by events that have led to the creation or deletion of groups for the Targeted Fraud Forensics Filter in the **Advanced Threat Protection** module.
Environment	Filters by events that have led to the creation, an update or the deletion of secondary environments in the **Service Dashboard** module.
Environment validation	Filters by events that have led to the creation or deletion of an environment validation for mailbox migration in the **365 Total Protection** module.

EVENT	EXPLANATION
Environment assignment	Filters by events that have led to the creation, an update or the deletion of environment assignments to mailboxes in the **Customer Settings** > **Mailboxes** module. Creation means that a newly created mailbox has been assigned to an environment for the first time. Update means that a mailbox has been assigned to a different environment than the one it had been assigned before. Deletion means that the environment assignment of a mailbox has been deleted because the mailbox itself has been deleted.
Restrictions	Filters by events that have led to an update of the settings in the **Authentication policies & IPs** module.
Credentials for mailbox migration	Filters by events that have led to the creation or deletion of the credentials of an on-premise Exchange server for mailbox migration in the **365 Total Protection** module.

Additional events

The following table lists events by which administrators cannot filter, but which are nonetheless displayed in the **Auditing 2.0** module.

Table 14: Events that cannot be filtered by

EVENT	EXPLANATION
Basic data	Filters by events that have led to the creation, an update or the deletion of the basic data for mailboxes in the **Mailboxes** module.

Resetting the Settings

You have changed the settings for displaying the audit log in the **Auditing 2.0** module (see Selecting a Display Period on page 190, Filtering by Action on page 191 and Filtering by Events on page 193). You are currently in the **Auditing 2.0** module.

You can reset the settings for displaying the audit log in the **Auditing 2.0** module (see Auditing 2.0 on page 185) to the default settings.

Click on **Reset**.

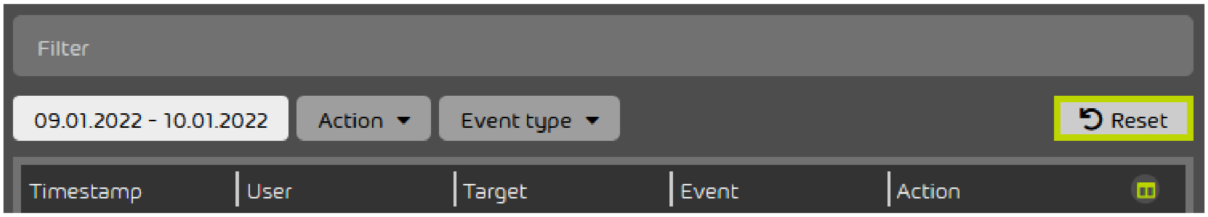


Figure 157: Reset settings

The settings are reset.

The settings for displaying the audit log have been reset to the default settings.

Searching Entries

Administrators can filter the entries from the audit log in the **Auditing 2.0** module (see Auditing 2.0 on page 185) by search terms. Administrators can search for search terms in the following parameters:

- **User**
- **Target path**
- **Target**
- **App ID**
- **App version**
- **Old values**
- **New values**
- **IP**
- **URL**

Except for the **Old values** and **New values** parameters, all parameters correspond to categories of the audit log (see Categories on page 186). In contrast, the **Old values** and **New values** parameters refer to the old and new values stored in the audit log entries under the menu item **Info**.

Administrators can enter a search term in the search bar. To search a specific parameter for the search term, administrators can then click on the desired parameter below the search bar. Otherwise, all parameters are searched for the search term. Administrators can start the search by pressing the Enter key. Only the entries that meet the search criteria are displayed in the audit log.

Notice:

Administrators can use multiple parameters at the same time. Administrators can enter one search term for each used parameter. The search results contain only entries that meet all search criteria.

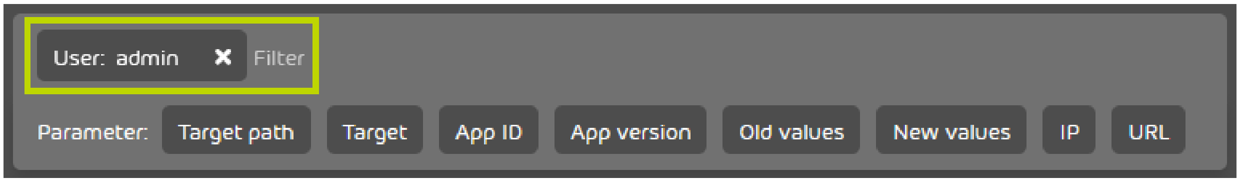


Figure 158: Searching entries

Opening an Entry

You can open an entry from the audit log in the **Auditing 2.0** module to see which values were valid before and after an event.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the customer whose audit log you would like to open.
3. Navigate to **Reporting & Compliance** > **Auditing 2.0**.
4. Optional: To search for an entry, filter the entries in the audit log (see Selecting a Display Period on page 190, Filtering by Action on page 191, Filtering by Events on page 193 or Searching Entries on page 204).
5. Click on the menu arrow next to the entry that you would like to open.

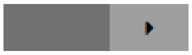


Figure 159: Open menu

➔

A menu opens.

6. Click on **Info**.

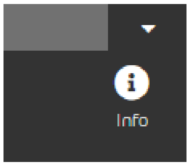
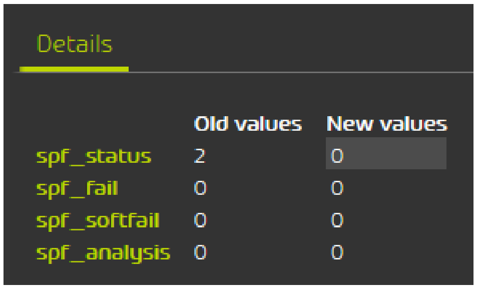


Figure 160: Open information

The entry is opened. If available, the old and new values of the event are displayed.


Details

	Old values	New values
spf_status	2	0
spf_fail	0	0
spf_softfail	0	0
spf_analysis	0	0

Figure 161: Event values

> **Notice:**
>
> The value that has changed due to the event is highlighted in gray.

An entry from the audit log has been opened.

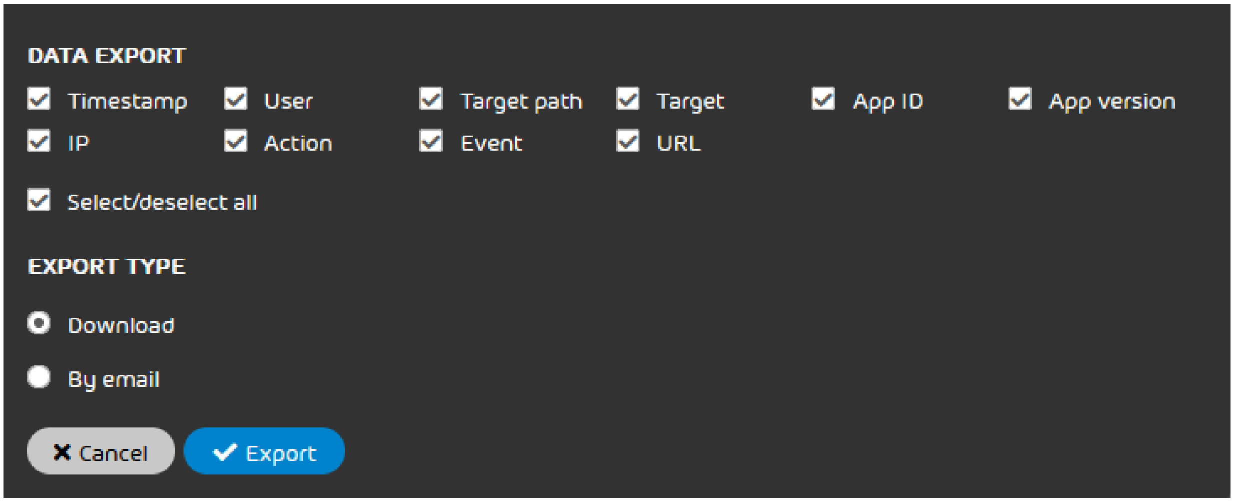
Exporting Entries

In the **Auditing 2.0** module (see Auditing 2.0 on page 185), you can export the entries of the audit log as a CSV file. During the export, all entries displayed in the **Auditing 2.0** module are exported. You can select the columns whose data should be exported.

1. Log in to the Control Panel with your administrative credentials.

2. From the scope selection, select the customer whose audit log you would like to open.
3. Navigate to **Reporting & Compliance** > **Auditing 2.0**.
4. Select the period whose entries are to be exported as the display period (see Selecting a Display Period on page 190).
5. Filter the displayed entries by actions (see Filtering by Action on page 191).
6. Filter the displayed entries by events (see Filtering by Events on page 193).
7. Click on **Export as CSV**.

   A form for exporting audit log entries opens.



DATA EXPORT

☑ Timestamp ☑ User ☑ Target path ☑ Target ☑ App ID ☑ App version
☑ IP ☑ Action ☑ Event ☑ URL

☑ Select/deselect all

EXPORT TYPE

◉ Download

○ By email

Figure 162: Form

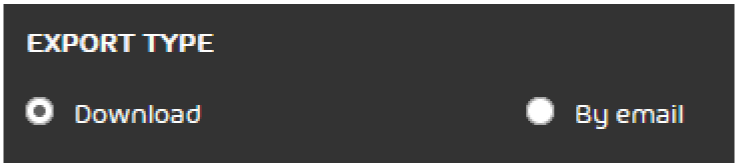
8. Tick the checkboxes of the categories whose data you would like to export from the audit log. You have the following options:

   - **Timestamp**
   - **User**
   - **Target path**
   - **Target**
   - **App ID**
   - **App version**
   - **IP**
   - **Action**
   - **Event**
   - **URL**

   > **Notice:**
   >
   > Each category corresponds to a column of the audit log (see Categories on page 186). By default, all categories in the form are preselected.

9. Under **Export type**, select whether the CSV file shall be provided as a download or sent by email.

   - **Download**: The CSV file is provided as download.
   - **By email**: The CSV file is sent by email.



EXPORT TYPE

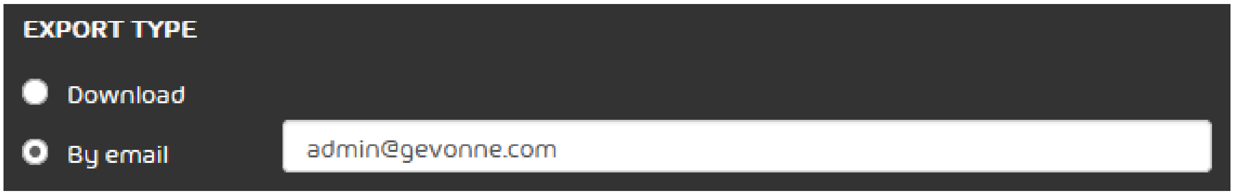
◉ Download ○ By email

Figure 163: Select export type

➜

If the option **By email** has been selected, an additional field is displayed.

10. Optional: If you have selected the option **By email**, enter the email address to which the CSV file shall be sent in the field.



EXPORT TYPE

○ Download

● By email admin@gevonne.com

Figure 164: Enter an email address

11. Click on **Export**.

➜

The CSV file is provided as a download or sent by email.

✓

Audit log entries have been exported.

Customer Settings

Customer Settings

In the **Customer Settings** module, customer-level administrators can view and manage the basic settings for mailboxes, groups, domains, as well as restrictions for passwords and IP addresses. The **Customer Settings** module is divided into the following submodules:

- **Mailboxes**: In the Control Panel, users are managed as mailboxes. In order for our services to be applied to mailboxes, these must be added to the Control Panel. In this module, customer-level administrators can add their domains' mailboxes to the Control Panel and manage them (see Mailboxes on page 210).
- **Groups**: Mailboxes can be combined into groups in the Control Panel in order to create group-wide settings for different services. In this module, customer-level administrators can create and manage groups (see Groups on page 262).
- **Domains**: In the Control Panel, alias domains can be added to a primary domain so mailboxes of alias domains can also be added to the Control Panel. In this module, customer-level administrators can add alias domains to the Control Panel, export them and delete them (see Domains on page 280).
- **Authentication policies & IPs**: In this module, customer-level administrators can define restrictions for passwords and IP addresses for the Control Panel login (see Authentication Policies and IPs on page 292).

Mailboxes

In the **Customer Settings** > **Mailboxes** module, all mailboxes registered under the selected domain are displayed and managed. This module is only available for customer-level administrators.

Mailboxes are the license basis for all services. A primary mailbox represents a single user. In addition to a primary mailbox, several associated alias addresses can be created without additional cost (see Adding an Alias Address on page 237).

In order for our services to be applied to a mailbox, the mailbox must be available in the Control Panel. Customer-level administrators can add mailboxes individually to the Control Panel (see Adding a Mailbox on page 216) or import several mailboxes (see CSV Files for Mailbox Import on page 223) from a CSV file (see Importing Mailboxes from a CSV File on page 219) into the Control Panel. Mailboxes can also be added automatically to the Control Panel (see Automatic Creation of Mailboxes on page 216).

Furthermore, customer-level administrators can create forward mailboxes (see Adding a Forward Mailbox on page 231) whose incoming emails are forwarded to other mailboxes (see Mailbox Types on page 215). Recipients for forward mailboxes can be imported from a CSV file (see CSV Files for the Import of Recipients for Forward Mailboxes on page 244).

Mailboxes from the Control Panel can be exported as a CSV file (see Exporting Mailboxes as a CSV File on page 228) and can later be imported again into the Control Panel using the CSV import.

If our services are no longer to be applied to one or several mailboxes, they can be removed from the Control Panel (see Removing a Mailbox on page 257 and Removing Multiple Mailboxes on page 259).

The existing mailboxes can be sorted in the **Mailboxes** module by their type and their environment (see Primary Environment Settings on page 440 and Secondary Environments on page 107). The drop-down menu **All types** allows you to filter the mailboxes by their type (see Mailbox Types on page 215).

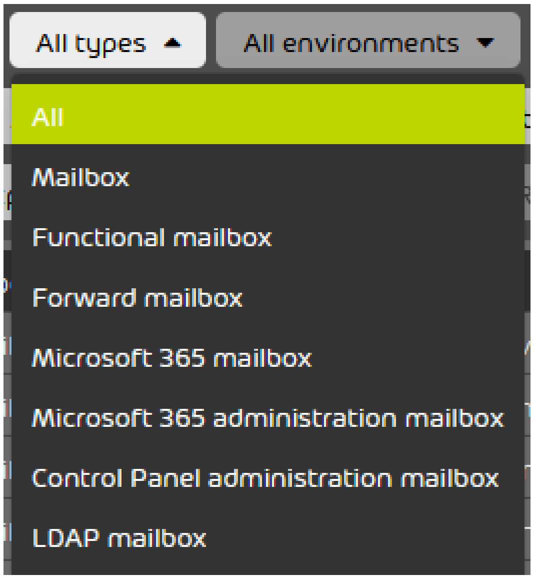


Figure 165: Filtering by type

The drop-down menu **All environments** allows you to filter the mailboxes by their environment. The drop-down menu contains the primary environment and the secondary environments of the domain.

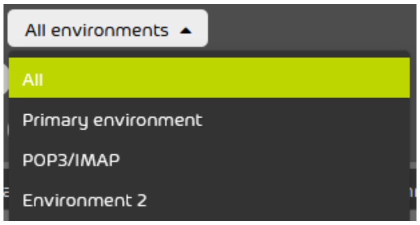


Figure 166: Filtering by environment

The drop-down menu **Multi-factor authentication** is only displayed if a customer-level administrator has enabled multi-factor authentication for the customer's mailboxes (see Enabling Multi-Factor Authentication on page 296). This drop-down menu allows you to filter the mailboxes by their configuration of multi-factor authentication.

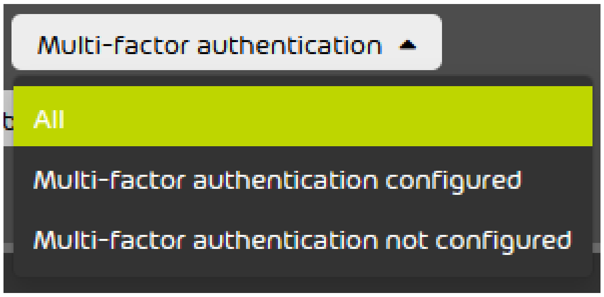

Multi-factor authentication ▲
All
Multi-factor authentication configured
Multi-factor authentication not configured

Figure 167: Filtering by multi-factor authentication

Furthermore, the **Mailboxes** module offers customer-level administrators the following options for managing individual mailboxes in the mailbox menu.

Table 15: Manage mailboxes

SYMBOL	NAME	DESCRIPTION
👥	Groups	Adding the mailbox to a group (see Groups on page 262 and Adding a Mailbox to a Group on page 233) as well as removing the mailbox from a group (see Removing a Mailbox from a Group on page 234).
🔧	Timezone & language	Changing the timezone, language, date format and time format of the mailbox (see Setting the Timezone and Language of a Mailbox on page 244)
🪪	Basic data	Changing the basic data of the mailbox (see Editing the Basic Data of a Mailbox on page 247)
🪧	Change environment	Change of the environment of a mailbox (see Changing an Environment on page 252)
🔑	Change password	Password change (see Changing the Password on page 253)

SYMBOL	NAME	DESCRIPTION
⌨	Reset multi-factor authentication	Resetting multi-factor authentication for the mailbox (see Resetting Multi-Factor Authentication on page 255) **Notice:** This action is only visible if multi-factor authentication is enabled for the domain (see Enabling Multi-Factor Authentication on page 296).
◉	Active or Inactive	Activation or deactivation of the mailbox (see Activating or Deactivating a Mailbox on page 236)
👥	Aliases	Addition of alias addresses to primary mailboxes (see Adding an Alias Address on page 237)
👤	Delegate	Addition of delegates to mailboxes (see Entering a Delegate on page 239)
⏷	Quarantine Report	Configuring the Quarantine Report for the mailbox (see Configuring the Quarantine Report for a Mailbox on page 421)
☒	Remove	Removal of the mailbox (see Removing a Mailbox on page 257)

Notice:

Some of the described functions cannot be applied to LDAP mailboxes or can only be applied to them to a limited extent. This is pointed out in the chapters on the affected functions.

Mailbox Types

The Control Panel distinguishes between the following mailbox types.

Table 16: Mailbox types

MAILBOX TYPE	EXPLANATION
Mailbox	This mailbox has been created manually in the Control Panel. The mailbox is not synchronized with any directory service via LDAP. For information on how to create mailboxes of this type, see Adding a Mailbox on page 216.
Functional mailbox	Mailboxes of this type are currently not detected in the Control Panel.
Forward mailbox	A forward mailbox is a virtual mailbox that is linked to at least one mailbox in the Control Panel. Incoming emails of the forward mailbox are forwarded to its linked mailboxes. For information on how to create forward mailboxes, see Adding a Forward Mailbox on page 231.
Control Panel administration mailbox	Mailboxes of this type are assigned the **admin** role in the Control Panel (see chapter "Roles" in the Control Panel manual).
LDAP mailbox	The user data of this mailbox is synchronized with a directory service via LDAP in the Control Panel. For information on the synchronization of mailboxes via LDAP, see Synchronizing Users and Groups with LDAP.

Automatic Creation of Mailboxes

Instead of adding mailboxes manually to the Control Panel (see Adding a Mailbox on page 216) or importing them into the Control Panel (see Importing Mailboxes from a CSV File on page 219), mailboxes can be created automatically in the Control Panel in two ways:

- LDAP mailboxes (see Mailbox Types on page 215) are synchronized with a directory service.
- Mailboxes are automatically identified and created based on the recipient addresses of emails that are accepted by the customer's email server. For each recipient address, a mailbox is created in the Control Panel. The automatic creation of mailboxes is enabled by default.

CAUTION:

To prevent the creation of unnecessary mailboxes and their additional costs, a user check that only accepts emails to valid mailboxes must be set up (see Adjusting the Primary Environment Settings on page 441).

CAUTION:

Even if a user check is enabled, the mechanism for the automatic creation of mailboxes cannot distinguish alias addresses from primary mailboxes unless the mailbox data is synchronized with a directory service. In order to prevent unnecessary mailboxes from being automatically created in the Control Panel because of incoming emails to valid alias addresses, the alias addresses must be manually added to the Control Panel (see Adding an Alias Address on page 237) if no synchronization is performed.

Adding a Mailbox

Our services can be applied to mailboxes that are listed under your domain in the Control Panel. In the **Customer Settings** > **Mailboxes** module, you can add mailboxes to your domain in the Control Panel.

Important:

Customers who have configured the synchronization of the mailboxes of their primary environment with a directory service via LDAP can only add new mailboxes manually if they have created a secondary environment (see Creating a Secondary Environment on page 110). Manually added mailboxes are not synchronized via LDAP.

Important:

If a new mailbox that has the same name as a previously deleted mailbox (see Removing a Mailbox on page 257) is added, this new mailbox will not be related to the previously deleted mailbox in the Control Panel.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain to which you would like to add a new mailbox.
3. Navigate to **Customer Settings** > **Mailboxes**.
4. Click on **Add mailbox**.

➜

A form opens.

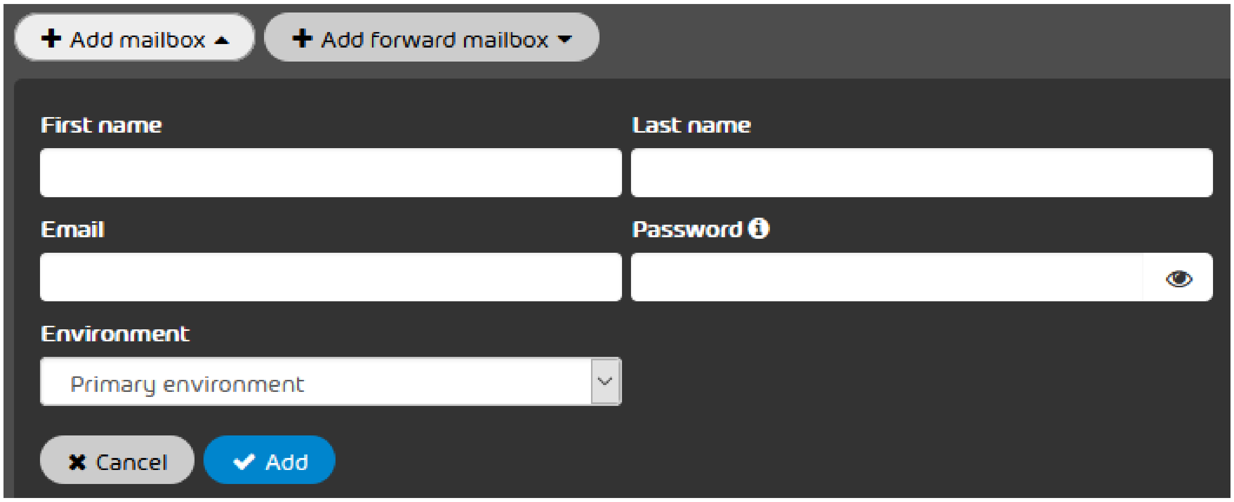


Figure 168: Form

5. Enter the mailbox owner's first name in the field **First name**.
6. Enter the mailbox owner's last name in the field **Last name**.
7. Enter the email address of the mailbox in the field **Email**.

> **Notice:**
>
> The following special characters are supported in email addresses:
>
> - Hash #
> - Ampersand &
> - Apostrophe '
> - Plus sign +
> - Slash /
> - Equals sign =
> - Question mark ?
> - Grave accent `
> - Vertical bar |
>
> The following special characters are not supported:
>
> - Asterisk *
> - Exclamation mark !
> - Percent sign %
> - Whitespace
> - Comma ,

8\.

> **Important:**
>
> The password must comply with the password policies. The password policies are displayed once the mouse pointer is moved over the ⓘ icon above the field.

In the field **Password**, enter a password that the mailbox owner can use to log in to the Control Panel as a user.

9. From the drop-down menu under **Environment**, select the environment to which the inbound email traffic of the mailbox shall be routed.

   Notice:

   The environment determines to which destination server the inbound email traffic of a mailbox is routed. The inbound email traffic can be routed to the primary environment (see Adjusting the Primary Environment Settings on page 441) or to a secondary environment (see Secondary Environments on page 107) of the domain. Customers who have configured the synchronization of the mailboxes of their primary environment with a directory service can select secondary environments only.

10. Click on **Add**.

    ➜

    The mailbox is created and added to the list of mailboxes.

✓

A mailbox has been added to the domain in the Control Panel.

Importing Mailboxes from a CSV File

Instead of entering mailboxes manually in the Control Panel, you can import mailboxes from a CSV file in the **Customer Settings** > **Mailboxes** module. You can import mailboxes both initially, before any other mailboxes have been created in the Control Panel, and additionally at a later time. You can either update or remove the entries that already exist in the Control Panel. During the import, primary mailboxes are imported together with their alias mailboxes and environments into the Control Panel.

Notice:

LDAP mailboxes (see Mailbox Types on page 215) cannot be imported from a CSV file.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to import mailboxes.
3. Navigate to **Customer Settings** > **Mailboxes**.

4. Click on **Import CSV**.

   ➡

   A menu opens.

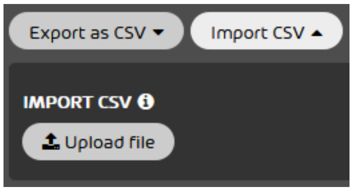


Figure 169: Menu for the CSV import of mailboxes

5. Click on **Upload file**.

   ➡

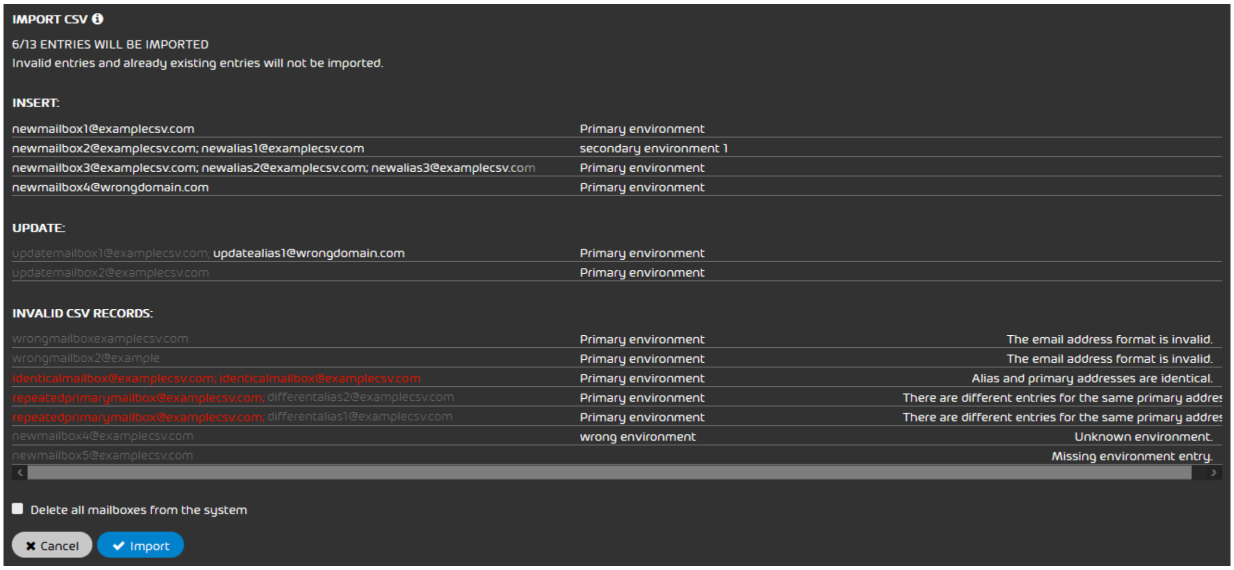
   A file selection window opens.

6. **Important:**

   To ensure that an external CSV file can be imported into the Control Panel without errors, rules regarding the file format, structure of its contents as well as a valid syntax must be observed (see CSV Files for Mailbox Import on page 223). The CSV file may contain up to 200 entries.

   Select the desired CSV file.

   The Control Panel reads the CSV file and displays a summary of the mailboxes to be added and updated as well as the invalid CSV entries and the error type.



IMPORT CSV

6/13 ENTRIES WILL BE IMPORTED
Invalid entries and already existing entries will not be imported.

INSERT:

newmailbox1@examplecsv.com	Primary environment
newmailbox2@examplecsv.com; newalias1@examplecsv.com	secondary environment 1
newmailbox3@examplecsv.com; newalias2@examplecsv.com; newalias3@examplecsv.com	Primary environment
newmailbox4@wrongdomain.com	Primary environment

UPDATE:

updatemailbox1@examplecsv.com; updatealias1@wrongdomain.com	Primary environment
updatemailbox2@examplecsv.com	Primary environment

INVALID CSV RECORDS:

wrongmailboxexamplecsv.com	Primary environment	The email address format is invalid.
wrongmailbox2@example	Primary environment	The email address format is invalid.
identicalmailbox@examplecsv.com; identicalmailbox@examplecsv.com	Primary environment	Alias and primary addresses are identical.
repeatedprimarymailbox@examplecsv.com; differentalias2@examplecsv.com	Primary environment	There are different entries for the same primary addres
repeatedprimarymailbox@examplecsv.com; differentalias1@examplecsv.com	Primary environment	There are different entries for the same primary addres
newmailbox4@examplecsv.com	wrong environment	Unknown environment.
newmailbox5@examplecsv.com		Missing environment entry.

□ Delete all mailboxes from the system

Notice:

For more information about the errors listed here, see Mailbox Import Errors on page 226.

7. **CAUTION:**

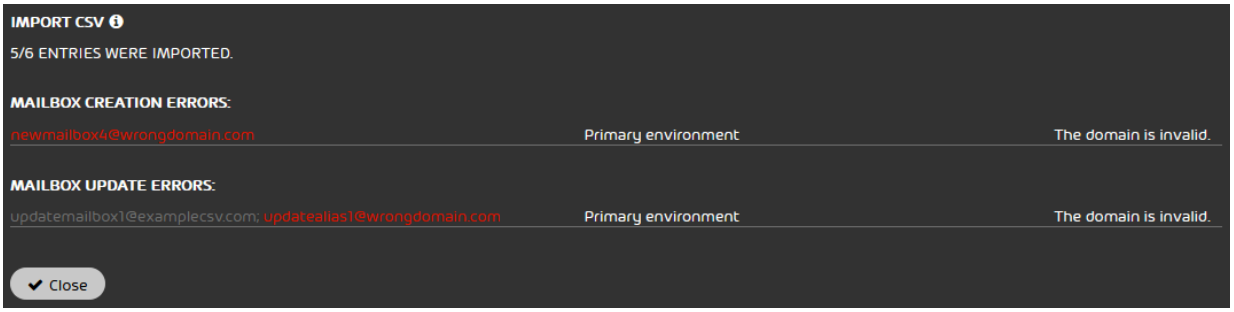
   During a CSV import with the option **Delete all mailboxes from the system**, the existing mailboxes in the Control Panel are overwritten.

   To prevent data loss, export the available mailboxes before performing the import.

   Optional: To delete all mailboxes from the system before importing new mailboxes, tick the **Delete all mailboxes from the system** checkbox.

8. Click on **Import**.

   The mailboxes listed in the summary are added or updated. The results of the import are then displayed.

   IMPORT CSV

   5/6 ENTRIES WERE IMPORTED.

   MAILBOX CREATION ERRORS:

   newmailbox4@wrongdomain.com — Primary environment — The domain is invalid.

   MAILBOX UPDATE ERRORS:

   updatemailbox1@examplecsv.com; updatealias1@wrongdomain.com — Primary environment — The domain is invalid.

   ✓ Close

   Notice:

   For more information about the errors listed here, see Mailbox Import Errors on page 226.

9. Click on **Close**.

   The summary of the import is closed.

Mailboxes have been imported from a CSV file and added to the domain in the Control Panel.

CSV Files for Mailbox Import

To ensure that an external CSV file containing mailbox information can be imported into the Control Panel without errors (see Importing Mailboxes from a CSV File on page 219), rules regarding the file extension and content structure must be observed.

Rule for the file extension

- The extension of the import file is **.csv**. Other file extensions, such as .txt or .docx, will not be accepted.

Rule for columns and rows

- The CSV file contains three columns separated from each other by a semicolon.
- The first row contains the column names. The first column is for primary mailboxes, the second one is for alias mailboxes and the third one is for the environments of the mailboxes.
- The rows of the CSV file end without any punctuation sign.
- The CSV file contains up to 200 entries.

Column names:

name;aliases;environment

Rule for the formatting of mailbox addresses

- The mailbox addresses are correctly formatted (according to the pattern "local-part@hostname.top-level-domain").

> ! **Important:**
>
> Incorrectly formatted addresses are not considered during the import.

- The mailbox addresses belong to domains that have been defined for the customer in the Control Panel.

> **Important:**
>
> Mailbox addresses from other domains are not imported into the Control Panel.

Rule for primary mailboxes

- From the second row on, the CSV file contains an address of a primary mailbox in each row of the first column.
- The first column must not be empty in any row.

Rules for alias mailboxes

- From the second row on, the addresses of alias mailboxes defined for the primary mailboxes listed in the left column can be entered in the second column.
- In case of primary mailboxes that do not have any alias mailbox assigned, the second column stays empty.
- If a cell of the second column contains several alias mailboxes, the addresses are separated from each other with commas.

Primary mailbox without an alias mailbox and with the primary environment:

```
primarymailbox@only.com;;primary
```

Primary mailbox with an alias mailbox and the primary environment:

```
primarymailbox@example.com;aliasmailbox@example.com;primary
```

Primary mailbox with several alias mailboxes and the primary environment:

```
primarymailbox@example.com;alias1@example.com,alias2@example.com;primary
```

Rules for environments

- From the second row on, the third column contains the names of the environments that shall be assigned to the mailboxes listed in the left column in the Control Panel.

> **Notice:**
>
> The environment determines to which destination server the inbound email traffic of a mailbox is routed (see Secondary Environments on page 107).

- Each row contains the name of an environment. For the primary environment, the name **primary** is used. For secondary environments, the name under which the secondary environment is displayed in the Control Panel is used. The names of the environments are not case-sensitive.

> **Important:**
>
> Records with secondary environments can only be imported from a CSV file if the secondary environments have been previously created in the Control Panel (see Creating a Secondary Environment on page 110).

- The third column must not be empty in any row.

Primary mailbox with an alias mailbox and the primary environment:

```
primarymailbox@example.com;aliasmailbox@example.com;primary
```

Primary mailbox with an alias mailbox and a secondary environment:

```
primarymailbox@example.com;aliasmailbox@example.com;environment 2
```

Rules for duplicated entries

- Duplicated entries do not affect the processing of the CSV file, but should be avoided.
- The file must not contain rows with the same content as others in the left column, but different content in the other columns.

Important:

Rows with the same primary mailbox are not imported if the CSV file contains another row with the same primary mailbox but with different alias mailboxes or a different environment.

Invalid rows with the same primary mailbox, different alias mailboxes and the primary environment:

```
primarymailbox@example.com;alias1@example.com,alias2@example.com;primary
 primarymailbox@example.com;alias3@example.com;primary
```

Mailbox Import Errors

When importing mailboxes (see Importing Mailboxes from a CSV File on page 219), the Control Panel performs two different checks, which can result in different errors.

The first check is performed after the user has selected a CSV file for mailbox import. The mailbox addresses are checked for the correct format and for repetitions. It is also checked if the environments exist in the Control Panel. The following errors are possible and are listed in the summary under **Invalid CSV records:**:

1. **The email address format is invalid.**: The listed addresses contain format errors (see valid format under CSV Files for Mailbox Import on page 223).

   Important:

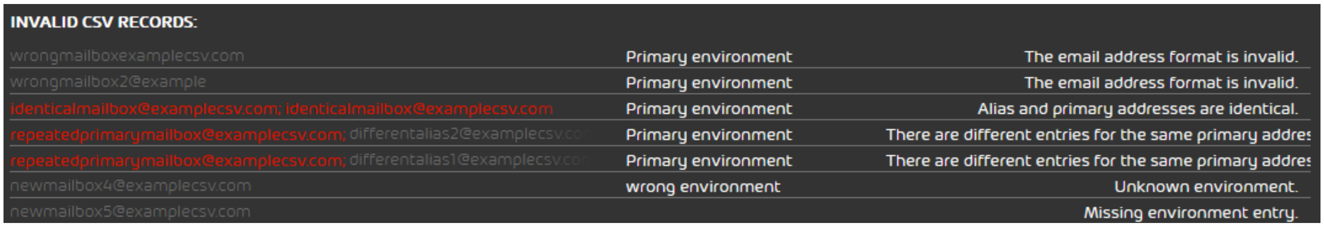
   If these errors occur while updating existing mailboxes, no other contents of the affected CSV records are imported, even if they are valid.

2. **Alias and primary addresses are identical.**: In the affected record, the same address is listed as the primary mailbox and as the alias mailbox.

3. **There are different entries for the same primary address.**: The CSV file contains several records with different alias mailboxes or environments for one primary mailbox. None of these records are imported into the Control Panel.

4. **Unknown environment.**: An environment (see Primary Environment Settings on page 440 and Secondary Environments on page 107) with this name does not exist for the domain in the Control Panel. For the correct spelling of the names of the primary environment and the secondary environments, see CSV Files for Mailbox Import on page 223. The record is not imported into the Control Panel.

5. **Missing environment entry.**: No environment has been defined for this mailbox. The record is not imported into the Control Panel.

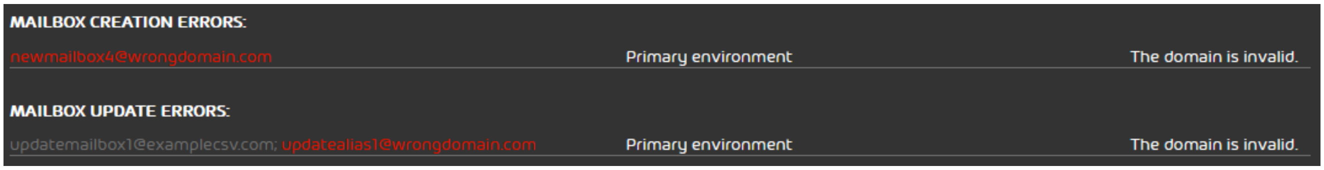


INVALID CSV RECORDS:

wrongmailboxexamplecsv.com	Primary environment	The email address format is invalid.
wrongmailbox2@example	Primary environment	The email address format is invalid.
identicalmailbox@examplecsv.com; identicalmailbox@examplecsv.com	Primary environment	Alias and primary addresses are identical.
repeatedprimarymailbox@examplecsv.com; differentalias2@examplecsv.co	Primary environment	There are different entries for the same primary addres
repeatedprimarymailbox@examplecsv.com; differentalias1@examplecsv.co	Primary environment	There are different entries for the same primary addres
newmailbox4@examplecsv.com	wrong environment	Unknown environment.
newmailbox5@examplecsv.com		Missing environment entry.

Figure 170: Error display after CSV file selection

The second check takes place after the administrator has triggered the import. The domains of the mailboxes to be imported are checked. If a mailbox belongs to a domain that has not been defined under **Customer Settings** > **Domains** (see Domains on page 280), an import error occurs. In the resulting view of import results, these errors are listed in sorted order either under **Mailbox creation errors:** or under **Mailbox update errors:**.



MAILBOX CREATION ERRORS:

newmailbox4@wrongdomain.com	Primary environment	The domain is invalid.

MAILBOX UPDATE ERRORS:

updatemailbox1@examplecsv.com; updatealias1@wrongdomain.com	Primary environment	The domain is invalid.

Figure 171: Error display after mailbox import from a CSV file

Notice:

If these errors occur, the error-free contents of the affected CSV entries are imported.

Exporting Mailboxes as a CSV File

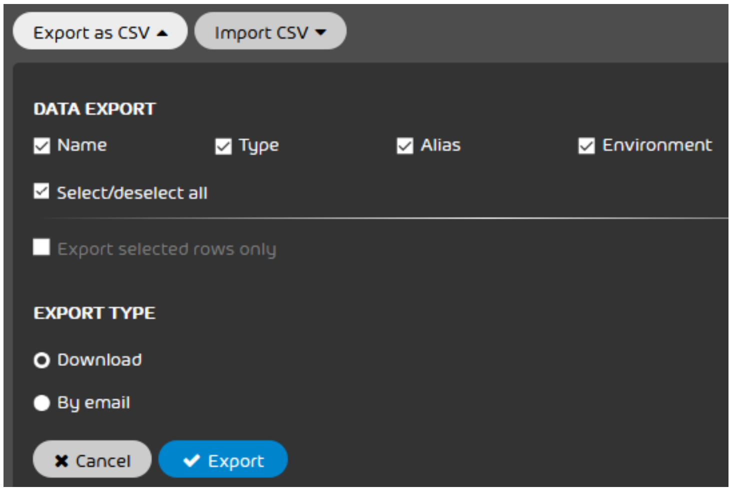
You have added mailboxes to the Control Panel (see Adding a Mailbox on page 216 and Importing Mailboxes from a CSV File on page 219).

To prevent the loss of data related to the mailboxes of your domain, you can export the data of the mailboxes as a CSV file. During the export, the data of all mailboxes available under the domain in the Control Panel is exported.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain whose mailboxes you would like to export.
3. Navigate to **Customer Settings** > **Mailboxes**.
4. Click on **Export as CSV**.

   ➜

   A form is displayed.



Export as CSV ▲ Import CSV ▼

DATA EXPORT

☑ Name ☑ Type ☑ Alias ☑ Environment

☑ Select/deselect all

□ Export selected rows only

EXPORT TYPE

● Download

○ By email

✖ Cancel ✔ Export

Figure 172: Form for CSV export

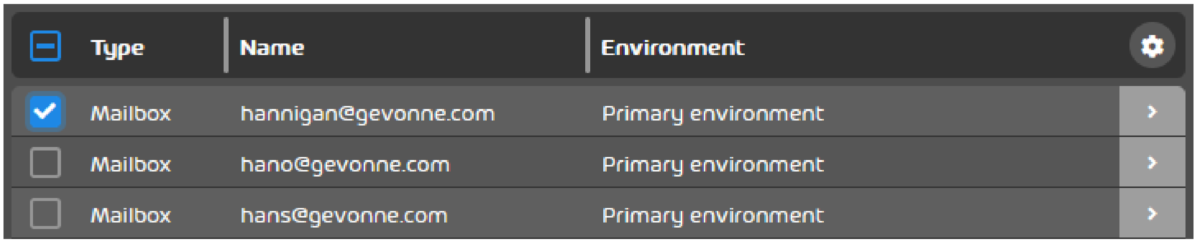
5. Under **Data export**, tick the checkboxes of the data you would like to export.
   - **Name**: The addresses of the primary mailboxes are exported.
   - **Type**: The types of the primary mailboxes are exported (see Mailboxes on page 210).
   - **Alias**: If alias mailboxes are assigned to primary mailboxes, the addresses of the alias mailboxes are exported.
   - **Environment**: The environments of the mailboxes are exported (see Adding a Mailbox on page 216).
   - **Select/deselect all**: All previously described checkboxes are ticked or unticked.
6. Optional: If you only want to export data of selected mailboxes, proceed as follows:

   a) Click on ☰ at the top of the module.

   ➔

   A column with checkboxes is displayed in the table.

   b) Select the rows from which you would like to export data.



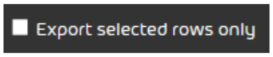
⊟	Type	Name	Environment
☑	Mailbox	hannigan@gevonne.com	Primary environment
□	Mailbox	hano@gevonne.com	Primary environment
□	Mailbox	hans@gevonne.com	Primary environment

Figure 173: Select rows

➔

In the form, the **Export selected rows only** checkbox is enabled.

   c) Tick the **Export selected rows only** checkbox.



□ Export selected rows only

Figure 174: Export selected rows

7. Under **Export type**, select whether the CSV file shall be provided as a download or sent by email.

   - **Download**: The CSV file is provided as download.
   - **By email**: The CSV file is sent by email.

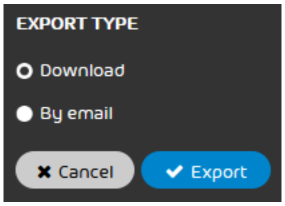
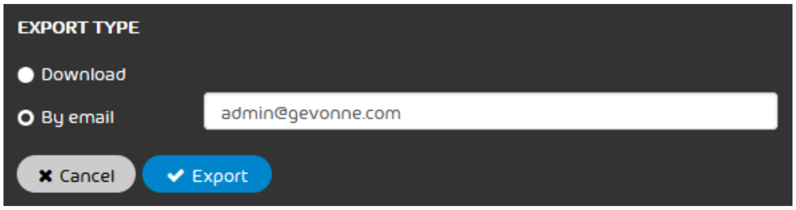


Figure 175: Select export type

➔

If the option **By email** has been selected, an additional field is displayed.

8. Optional: If you have selected the option **By email**, enter the email address to which the CSV file shall be sent in the field.



admin@gevonne.com

Figure 176: Enter an email address

9. Click on **Export**.

   ➔

   The CSV file is provided as a download or sent by email.

✓

Mailboxes have been exported as a CSV file.

Next, you can import the exported mailboxes again if required (see Importing Mailboxes from a CSV File on page 219).

Adding a Forward Mailbox

You have added a mailbox to the Control Panel (see Adding a Mailbox on page 216 and Importing Mailboxes from a CSV File on page 219).

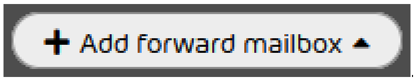
In the **Customer Settings** > **Mailboxes** module, you can set up forward mailboxes for existing mailboxes. Forward mailboxes can forward email traffic to one to 100 internal or external mailboxes.

Important:

The maximum allowed size for emails forwarded to forward mailboxes is limited and depends on the number of forward recipients. The following table breaks down the allowed size for forwarded emails depending on the number of recipients.

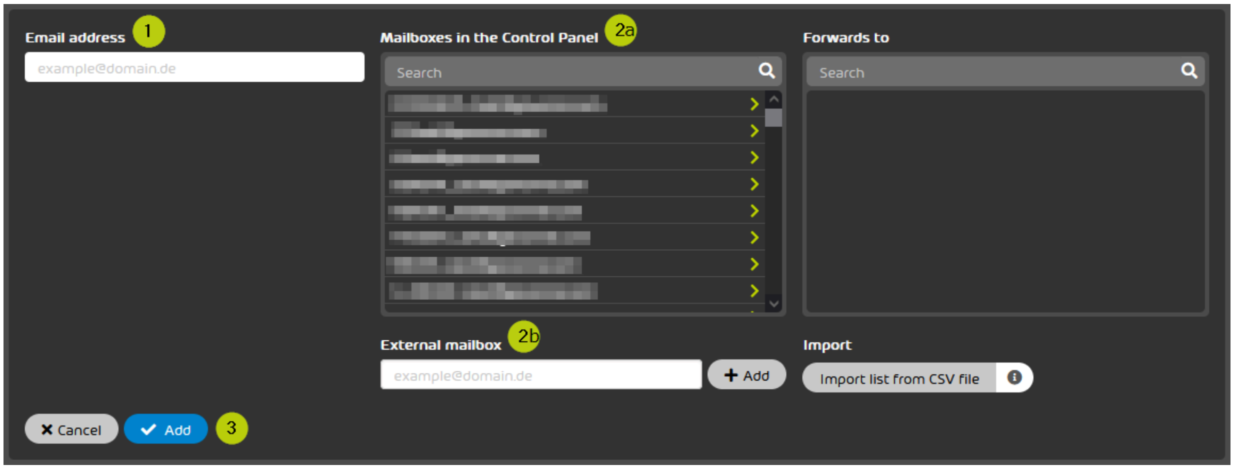
NUMBER OF RECIPIENTS	MAXIMUM ALLOWED EMAIL SIZE (MB)
1	100
2-9	50
10-24	25
25-49	15
50-100	10

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain to which you would like to add a forward mailbox.
3. Navigate to **Customer Settings** > **Mailboxes**.

4. Click on 

.

A drop-down menu opens.



5. Under **Email address**, enter the mailbox for which you want to set up forwarding. (1)
6. In order to add a forward mailbox,
   - select a registered mailbox from the list (2a) or
   - enter a valid address in the field **External mailbox** (2b) and confirm with **Add**

Notice:

Repeat this step to add more forward mailboxes.

The mailboxes appear in the list **Forwards to**.

7. Click on **Add** mailbox (3) to set up the forwarding.

A forward mailbox has been added.

Adding a Mailbox to a Group

You have added a mailbox to the Control Panel (see Adding a Mailbox on page 216 and Importing Mailboxes from a CSV File on page 219). You have created a group (see Creating a Group on page 262).

Instead of adding mailboxes to a group in the **Groups** module (see Managing Members on page 270), you can add a mailbox to a group (see Groups on page 262) in the **Mailboxes** module.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain containing the group to which you would like to add a mailbox.
3. Navigate to **Customer Settings** > **Mailboxes**.
4. Click on the menu arrow next to the mailbox that you would like to add to a group.

   ➜

   A menu opens.

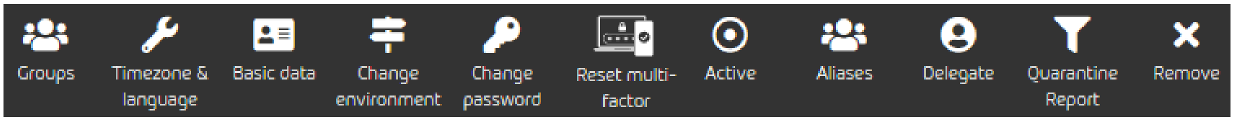
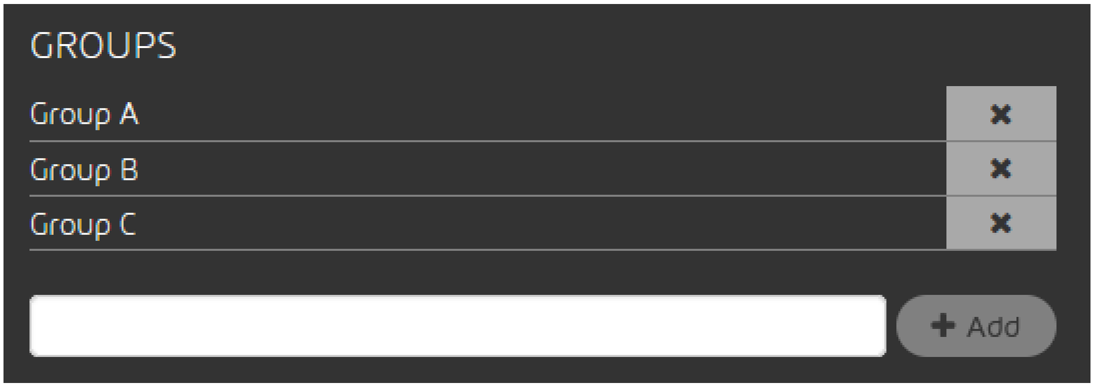


Figure 177: Actions for mailboxes

5. Click on **Groups**.

   A menu for group management opens. Here, all groups to which the mailbox belongs are displayed.



GROUPS

Group A	✖
Group B	✖
Group C	✖

Figure 178: Group menu

6. In the input field, enter the name of the group to which you would like to add the mailbox.
7. Click on **Add**.

   The mailbox is added to the group. The group is displayed in the group list.

A mailbox has been added to a group.

Next, you can remove the mailbox from the group (see Removing a Mailbox from a Group on page 234).

Removing a Mailbox from a Group

You have added a mailbox to a group (see Adding a Mailbox to a Group on page 233).

Instead of removing mailboxes from a group in the **Groups** module (see Managing Members on page 270), you can remove a mailbox from a group in the **Mailboxes** module (see Groups on page 262).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain containing the group from which you would like to remove a mailbox.
3. Navigate to **Customer Settings** > **Mailboxes**.
4. Click on the menu arrow next to the mailbox that you would like to remove from a group.

   ➔

   A menu opens.

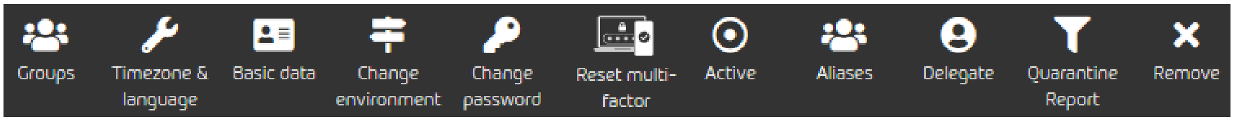


Figure 179: Actions for mailboxes

5. Click on **Groups**.

   ➔

   A menu for group management opens. Here, all groups to which the mailbox belongs are displayed.

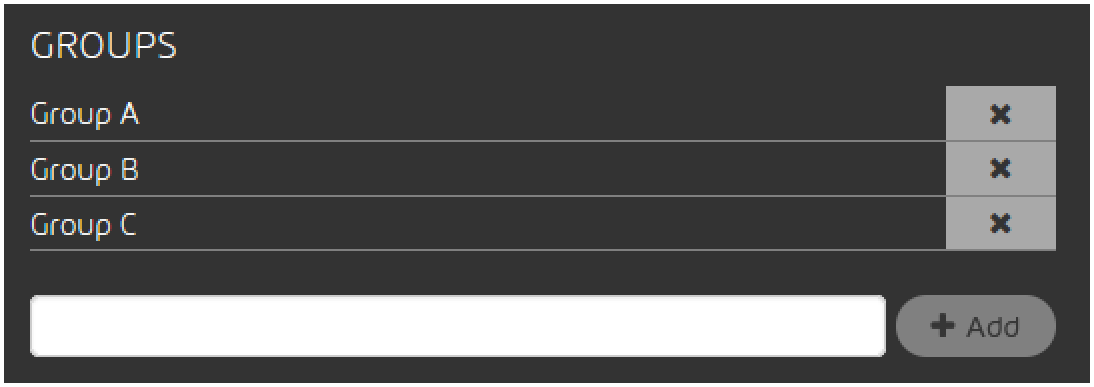


Figure 180: Group menu

6. Click on the cross icon next to the group from which you would like to remove the mailbox.

   ➔

   The mailbox is removed from the group. The group is removed from the group list.

✓

A mailbox has been removed from a group.

Activating or Deactivating a Mailbox

You have added a mailbox to the Control Panel (see Adding a Mailbox on page 216 and Importing Mailboxes from a CSV File on page 219).

Only users whose mailboxes have been activated in the Control Panel can log in to the Control Panel. Our services are equally applied and billed for activated and deactivated mailboxes. You can activate and deactivate mailboxes in the Control Panel.

1. Log in to the Control Panel with your administrative credentials.
2. Select the domain from the scope selection.
3. Navigate to **Customer Settings** > **Mailboxes**.
4. Click on the menu arrow next to the mailbox you want to activate or deactivate.

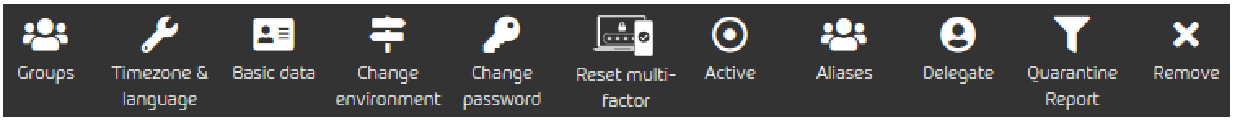


Figure 181: Open menu

   ➔

   A menu opens.

5. Click on the button **Active** or **Inactive**.

   ➔

   A drop-down menu opens.

6. Click on **Activate** under **Deactivate**.

   The mailbox is activated or deactivated. Depending on the activation status, the symbol is displayed in white (activated) or red (deactivated).

A mailbox has been activated or deactivated.

Adding an Alias Address

You have added a mailbox to the Control Panel (see Adding a Mailbox on page 216 and Importing Mailboxes from a CSV File on page 219).

In the **Customer Settings** > **Mailboxes** module, you can add alias addresses to a primary mailbox. An alias address is assigned to a primary mailbox. The owner of a primary mailbox can see both the emails of the primary mailbox and the emails of the alias addresses in the **Email Live Tracking** module (see Email Live Tracking on page 58). You can add several alias addresses to a primary mailbox. Alias addresses are free of charge.

Notice:

No alias addresses can be assigned to LDAP mailboxes (see Mailbox Types on page 215).

Attention:

If a customer's mailbox data is not synchronized with a directory service, the customer must add all alias addresses from the domain to the Control Panel manually (see Adding a Mailbox on page 216 and Importing Mailboxes from a CSV File on page 219). Otherwise, the alias addresses would not be identified as alias addresses of existing primary mailboxes but as new primary mailboxes during the automatic creation of mailboxes (see Automatic Creation of Mailboxes on page 216). This would lead to chargeable primary mailboxes being created for the alias addresses in the Control Panel (see Mailboxes on page 210).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain containing the primary mailbox to which you would like to add an alias address.
3. Navigate to **Customer Settings** > **Mailboxes**.
4. Click on the menu arrow next to the mailbox to which you want to add an alias address.

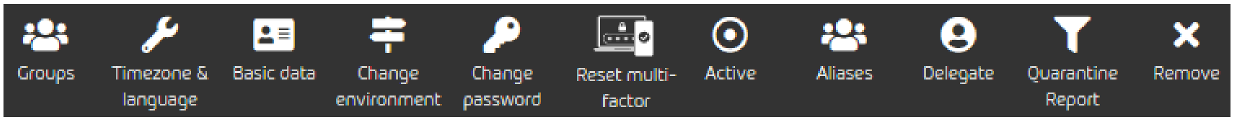


Figure 182: Open menu

➜

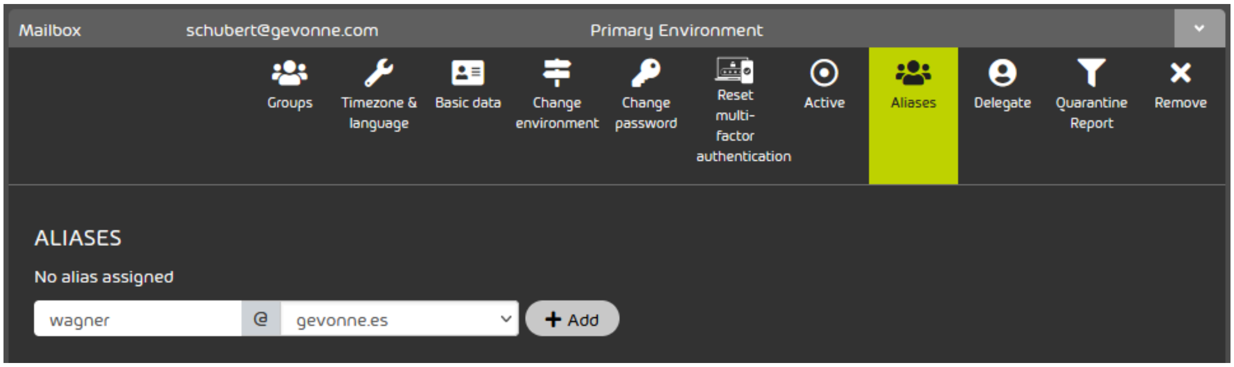
A menu opens.

5. Click on **Aliases**.

➜

A menu opens.

6. Enter the desired alias under **Alias**, followed by the domain, and click on **Add**.



Mailbox schubert@gevonne.com Primary Environment

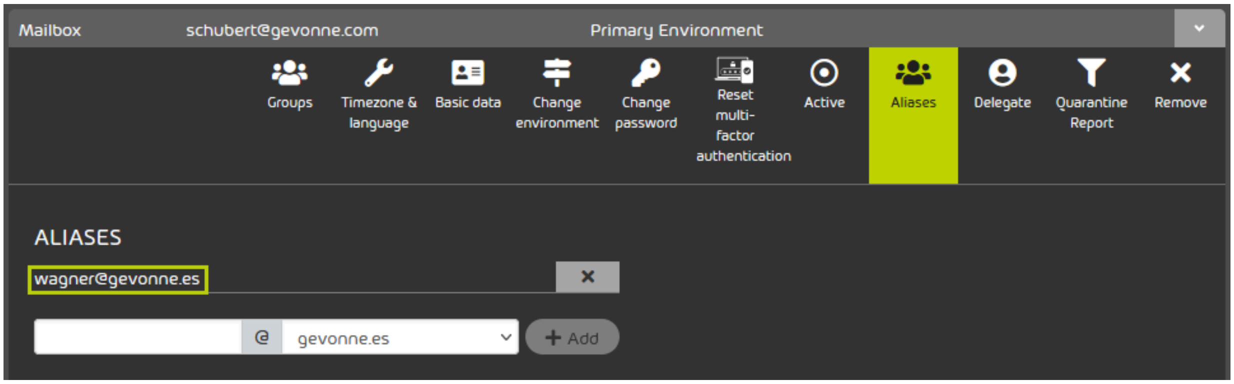
ALIASES

No alias assigned

wagner @ gevonne.es

Figure 183: Enter an alias address

The alias address is added.



Mailbox schubert@gevonne.com Primary Environment

ALIASES

wagner@gevonne.es

@ gevonne.es

Figure 184: Added alias address

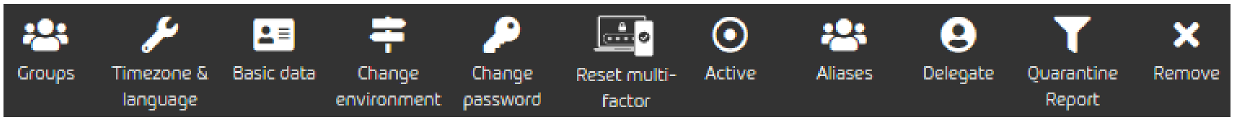
An alias address is added to a primary mailbox.

Entering a Delegate

You have added a mailbox to the Control Panel (see Adding a Mailbox on page 216 and Importing Mailboxes from a CSV File on page 219).

In the **Customer Settings** > **Mailboxes** module, you can enter a delegate for an existing primary mailbox. In the **Email Live Tracking** module (see Email Live Tracking on page 58), delegates have access to the emails of the mailboxes for which they have been registered as delegates, and can perform email actions for these emails.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain containing the mailbox for which you would like to enter a delegate.
3. Navigate to **Customer Settings** > **Mailboxes**.
4. Click on the menu arrow next to the desired mailbox.



5. Click on **Delegate**.

   ➜

   A drop-down menu opens.
6. Activate the checkbox **Activate delegate access**.

   ➜

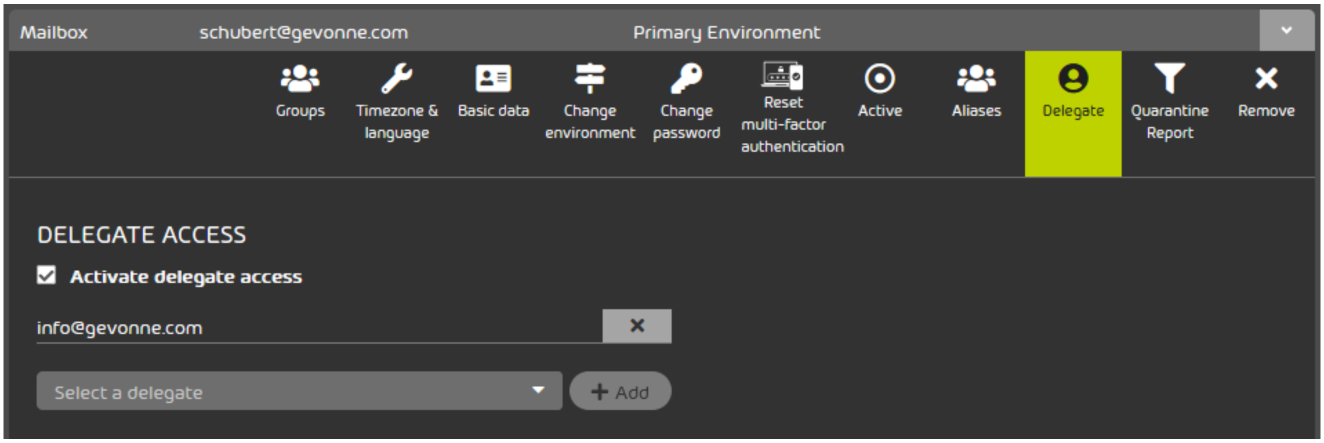
   A list of the registered users appears.
7. Select a delegate from the list and click on **Add**.

   ➜

   The delegate is added to the mailbox. For security reasons, the user to whose mailbox the delegate has been assigned is notified by email about the delegate assignment.

✓

A delegate has been entered for a mailbox.



DELEGATE ACCESS

☑ Activate delegate access

info@gevonne.com

Select a delegate

+ Add

Importing Recipients for Forward Mailboxes from a CSV File

Instead of entering recipients for forward mailboxes manually, you can import them from a CSV list in the **Customer Settings** > **Mailboxes** module. This can be done both initially, before any data has been entered, and additionally during operation.

Notice:

No forward mailboxes can be assigned to LDAP mailboxes (see Mailbox Types on page 215). Thus, no recipients for forward mailboxes can be imported from a CSV file for these mailboxes.

1. Log in to the Control Panel with your administrative credentials.
2. Select the domain from the scope selection.
3. Navigate to **Customer Settings** > **Mailboxes**.

4. Click on **Add**.

   ➜

   A new form is displayed.

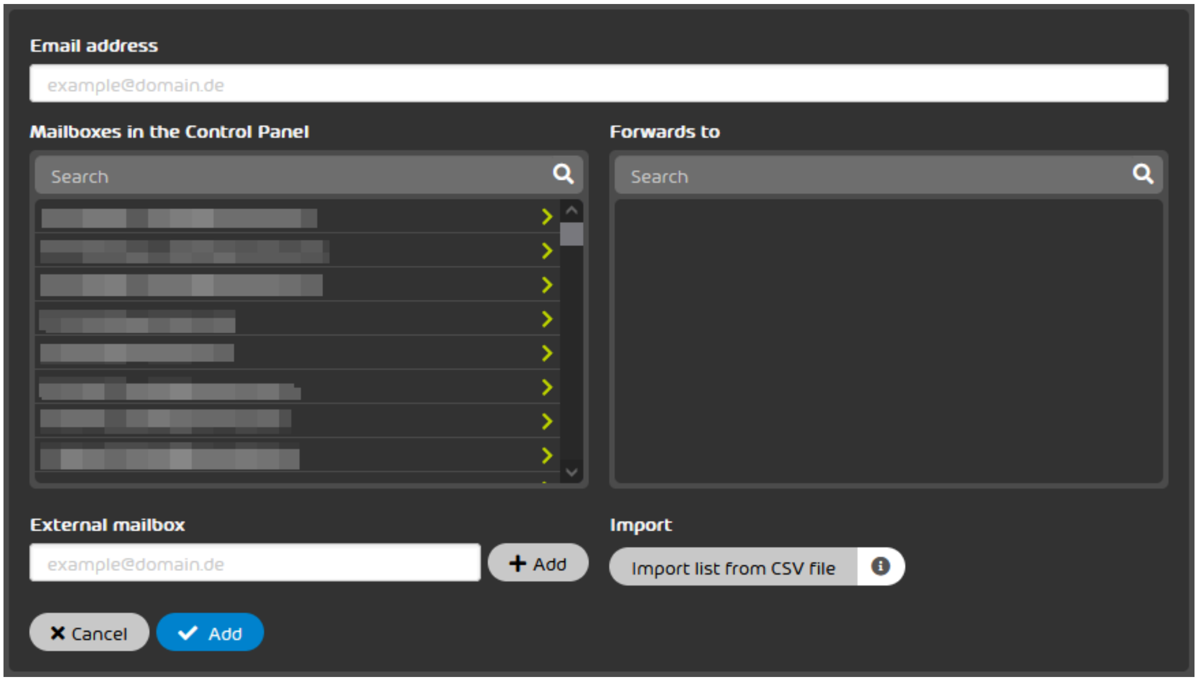


Figure 185: Import recipients for a forward mailbox from a CSV file

5. Enter the email address of the forward mailbox under **Email address**.
6. Click on **Import list from CSV file**.

   ➜

   A file selection window opens.

7. Select the desired CSV file.

> **Important:**
>
> To ensure that an external CSV file can be imported into the Control Panel without errors, special rules regarding the file format, the content structure as well as a valid syntax must be observed (see CSV Files for the Import of Recipients for Forward Mailboxes on page 244).

8. Click on **Import list from CSV file**.

➔

The addresses from the CSV file are imported and displayed in the **Forwards to** section.

> **Notice:**
>
> The following rules apply to the import of recipients for forward mailboxes:
>
> - Recipients that are already displayed under **Forwards to** are not deleted.
> - Only entries from the CSV file that are not already displayed under **Forwards to** are imported.
> - Duplicated entries from the CSV file are imported only once.
> - Not correctly-formated list entries are ignored and do not lead to the termination of the process. However, after the import an error message is displayed if invalid entries are present.
> - If the CSV file does not contain any valid addresses that are not already present in the **Forwards to** section, a corresponding error message is displayed and no addresses are imported.

9. Click on **Add**.

✓

Recipients for forward mailboxes have been imported from a CSV file.

CSV Files for the Import of Recipients for Forward Mailboxes

To ensure that an external CSV file with recipients for forward mailboxes can be imported into the Control Panel without errors (see Importing Recipients for Forward Mailboxes from a CSV File on page 241), special rules regarding the file extension and content structure must be observed.

Rules for creating a CSV file for the import of recipients

- The extension of the import file is always **.csv**. Other file extensions, such as .txt or .docx, are not allowed and will not be accepted.
- The CSV file contains only one column, in which individual entries are entered one below the other.
- The first row always contains the column name and can be named individually.
- The recipients' addresses must be correctly formatted (according to the pattern "local-part@hostname.top-level-domain").

> **Important:**
>
> Incorrectly formatted addresses are not considered during the import.

- Each row may contain only one address.
- Duplicated entries do not affect the processing of the file, but should be avoided.

Setting the Timezone and Language of a Mailbox

✓ You have added a mailbox to the Control Panel (see Adding a Mailbox on page 216 and Importing Mailboxes from a CSV File on page 219).

In the **Customer Settings** > **Mailboxes** module (see Mailboxes on page 210), you can set a different timezone, language, date format and time format for a single mailbox than for the domain (see chapter "Setting Default Values for Timezone and Language" in the Control Panel manual). The settings apply to the Control Panel display and to automatic emails from the Control Panel. The data from this module is synchronized with the user's data in the section **Timezone and language** under **User Settings** (see Changing the Timezone and Language on page 35).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain containing the mailbox whose settings you would like to change.
3. Navigate to **Customer Settings** > **Mailboxes**.
4. Click on the menu arrow next to the mailbox whose settings you would like to change.

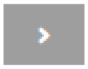


Figure 186: Open menu

➜

A menu opens.

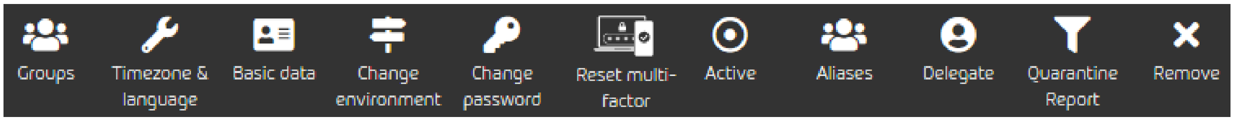
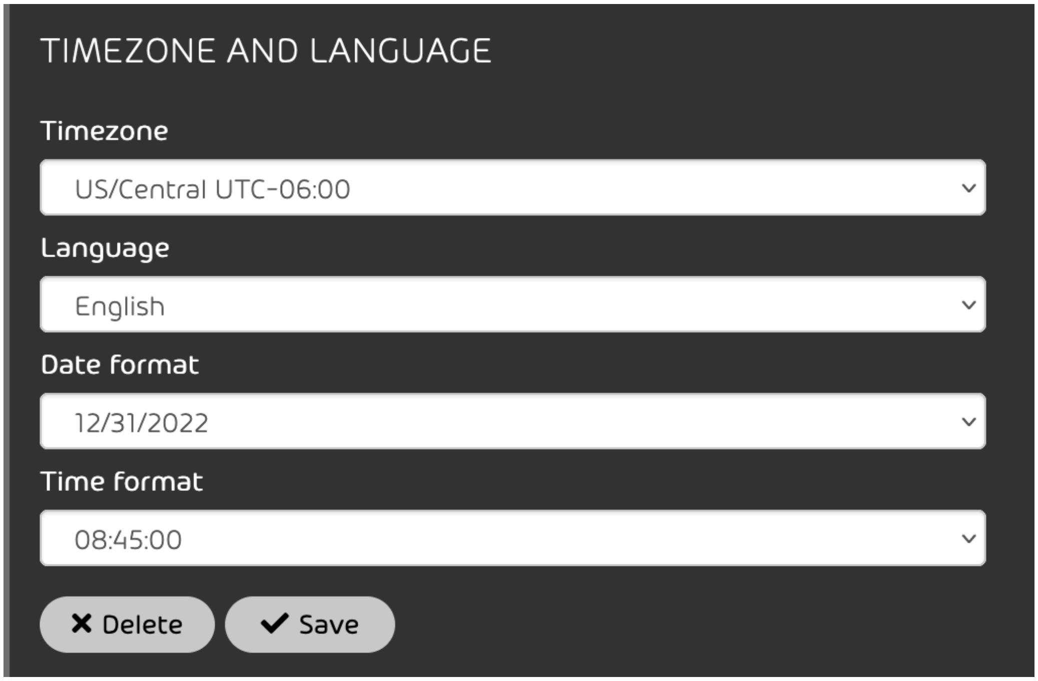


Figure 187: Menu

5. Click on **Timezone & language**.

   ➜

   A form is displayed.



TIMEZONE AND LANGUAGE

Timezone: US/Central UTC-06:00

Language: English

Date format: 12/31/2022

Time format: 08:45:00

Figure 188: Timezone & language

6. Select a timezone from the drop-down menu **Timezone**.

> **Notice:**
>
> The timezone determines the number format in the Control Panel and in automatic emails from the Control Panel.

7. Select a language from the drop-down menu **Language**.

8. Select a date format from the drop-down menu **Date format**.

   > **Notice:**
   >
   > The date format determines the order in which the available details of a date are displayed. If information is not available for all details, the missing details will not be displayed.

9. Select a time format from the drop-down menu **Time format**.

   > **Notice:**
   >
   > The time format determines the order in which the available details of a time are displayed. If information is not available for all details, the missing details will not be displayed.

10. Click on **Save**.

    The changes are saved.

    > **Notice:**
    >
    > The changes will not be applied until the user for whom the changes were made refreshes the page or logs back in to the Control Panel.

The timezone, language, date format and time format of a mailbox have been set.

Editing the Basic Data of a Mailbox

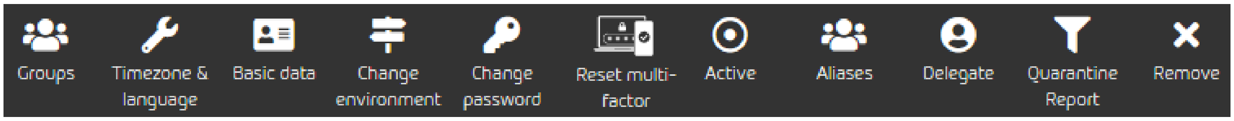
You have added a mailbox to the Control Panel (see Adding a Mailbox on page 216 and Importing Mailboxes from a CSV File on page 219).

The basic data contains information about the owner of a mailbox. In the **Customer Settings** > **Mailboxes** module, you can edit the basic data of a mailbox.

Notice:

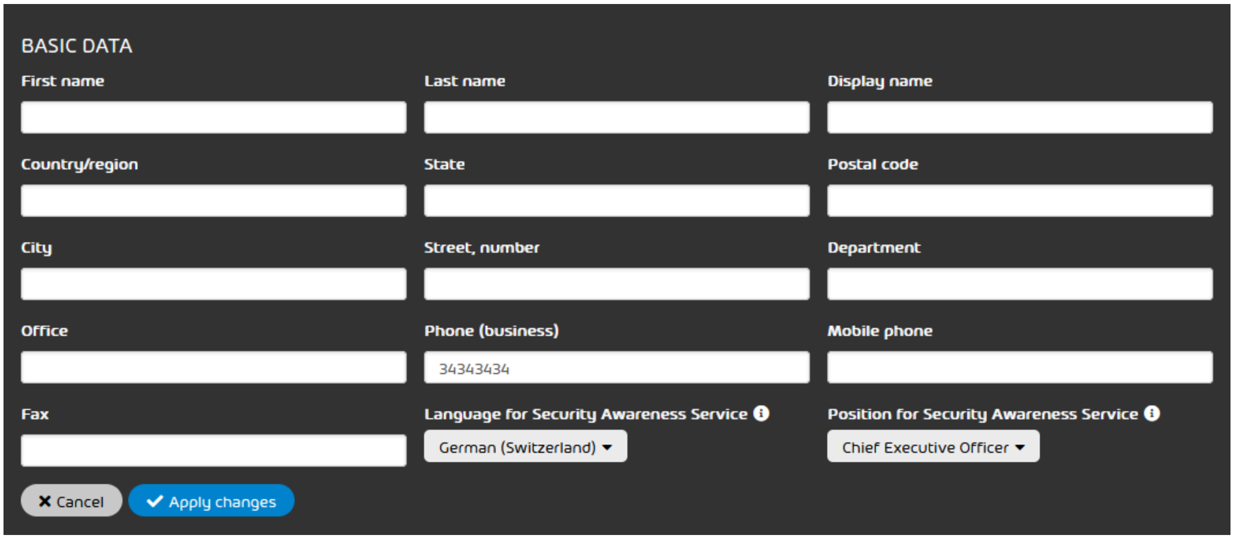
You cannot edit the basic data of LDAP mailboxes (see Mailbox Types on page 215) in the Control Panel. If basic data for a mailbox is stored in a directory service synchronized via LDAP, this data is displayed in the Control Panel.

1. Log in to the Control Panel with your administrative credentials.
2. Select the customer from the scope selection.
3. Navigate to **Customer Settings** > **Mailboxes**.
4. Click on the menu arrow next to the mailbox for which you want to edit the basic data.



5. Click on **Basic data**.

A form is displayed.



BASIC DATA

First name	Last name	Display name
Country/region	State	Postal code
City	Street, number	Department
Office	Phone (business): 34343434	Mobile phone
Fax	Language for Security Awareness Service: German (Switzerland)	Position for Security Awareness Service: Chief Executive Officer

✕ Cancel ✓ Apply changes

Figure 189: Basic data

6. **Notice:**

   All fields are optional.

   Notice:

   In the **Phone (business)**, **Mobile phone** and **Fax** fields, the phone or fax numbers must be entered in the following format:

   a. Country code: 00 or + and two-digit country code. Optionally, the country code can be in parentheses. Some examples of correct country codes are: **(0034)**, **(+34)**, **0049**, **+49**.

   b. Whitespace, period, or hyphen to separate country code from area code (optional).

   c. Maximum five-digit area or mobile code.

   d. Whitespace, period, or hyphen to separate area or mobile codes from the phone number (optional).

   e. Phone number consisting of any number of digits.

   Here are some examples of correct phone or fax numbers:

   (0034) 7432 1354913

   +49.157.1354913

   0049 157-1354913

   Enter the data of the user who owns the mailbox in the form. The fields have the following meanings:

   - **First name**: the user's first name
   - **Last name**: the user's last name
   - **Display name**: the user's display name in the Control Panel
   - **Country/Region**: country or region where the user's company is based

- **State**: state where the user's company is based
- **Postal code**: postal code of the user's company
- **City**: city where the user's company is based
- **Street, number**: street and house number where the user's company is based
- **Department**: department to which the user belongs
- **Office**: office in which the user works
- **Phone (business)**: the user's business phone number
- **Mobile phone**: the user's mobile phone number
- **Fax**: the user's fax number

7. Click on **Apply changes**.

   The changes are saved.

The basic data of a mailbox has been edited.

Changing the Emergency Password

Your mailboxes are synchronized via LDAP and forced your users to set an emergency password (see Activating Emergency Passwords).

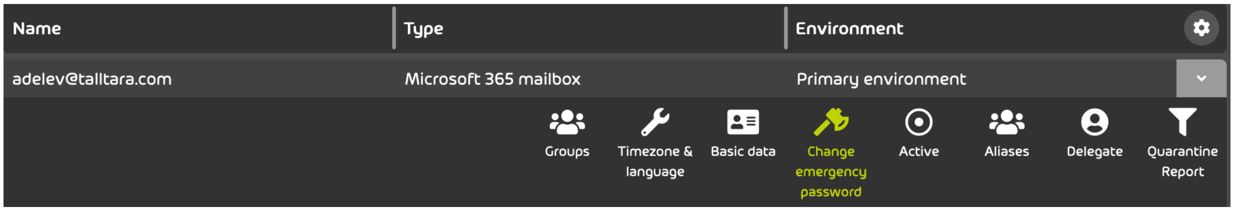
In the **Customer Settings** > **Mailboxes** module, you can change the emergency password for a mailbox.

Notice:

Emergency passwords can only be edited for LDAP mailboxes (see Mailbox Types on page 215).

1. Log in to the Control Panel with your administrative credentials.
2. Select the domain from the scope selection.

3. Navigate to **Customer Settings** > **Mailboxes**.
4. Click the menu arrow next to the mailbox whose emergency password you want to change.



Name	Type	Environment
adelev@talltara.com	Microsoft 365 mailbox	Primary environment

5. Click on **Change emergency password**.

   ➜

   An input field is displayed.
6. Enter the new emergency password in the input field.

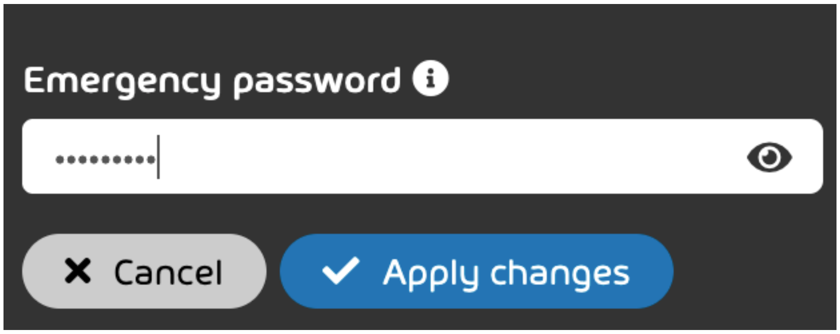


Figure 190: Change emergency password

7. Click on **Apply changes**.

   ➜

   The emergency password is saved.

✓

The emergency password of a mailbox has been changed.

Changing an Environment

You have added a mailbox to the Control Panel (see Adding a Mailbox on page 216 and Importing Mailboxes from a CSV File on page 219). You have defined the destination server to which the inbound email traffic of the mailbox shall be routed as the primary (see Adjusting the Primary Environment Settings on page 441) or a secondary environment (see Creating a Secondary Environment on page 110).

The environment of a mailbox determines to which destination server the inbound email traffic of the mailbox is routed. By default, mailboxes of a domain are assigned its primary environment (see Primary Environment Settings on page 440). If the inbound email traffic of individual mailboxes of the domain are to be routed to a different destination server instead, you can assign a secondary environment (see Secondary Environments on page 107) instead of the primary environment to these mailboxes. In the **Customer Settings** > **Mailboxes** module, you can change the environments of mailboxes of your domain. You cannot assign any environments to forward mailboxes (see Mailbox Types on page 215) and synchronized mailboxes in the Control Panel, since forward mailboxes are managed without any environments in the Control Panel and the environments of synchronized mailboxes are fetched from the source system.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain containing the mailbox whose environment you would like to change.
3. Navigate to **Customer Settings** > **Mailboxes**.
4. Click on the menu arrow next to the mailbox whose environment you would like to change.

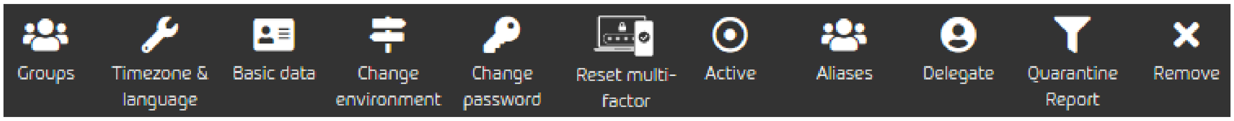


Figure 191: Open menu

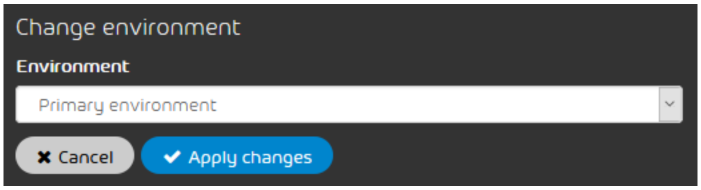
➔

A menu opens.

5. Click on **Change environment**.

   A form is displayed.

6. From the drop-down menu under **Environment**, select the environment to which the inbound email traffic of the mailbox shall be routed.



Change environment

Environment: Primary environment

Figure 192: Select environment

7. Click on **Apply changes**.

The environment of a mailbox has been changed.

Changing the Password

You have added a mailbox to the Control Panel (see Adding a Mailbox on page 216 and Importing Mailboxes from a CSV File on page 219).

In the **Customer Settings** > **Mailboxes** module, you can change the password for a manually created mailbox (see Mailbox Types on page 215).

Notice:

The passwords for LDAP mailboxes cannot be changed in the Control Panel.

1. Log in to the Control Panel with your administrative credentials.
2. Select the domain from the scope selection.
3. Navigate to **Customer Settings** > **Mailboxes**.

4. Click on the menu arrow next to the mailbox whose password you want to change.

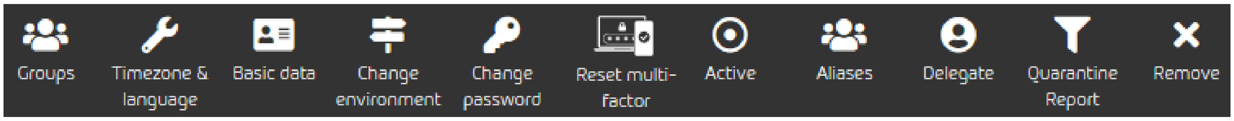


Figure 193: Open menu

A menu opens.

5. Click on **Change password**.

A menu opens.

6. Enter the new password in the **New password** field.

> **Important:**
>
> The new password must comply with the password polices from the **Authentication policies & IPs** module (see Authentication Policies and IPs on page 292).

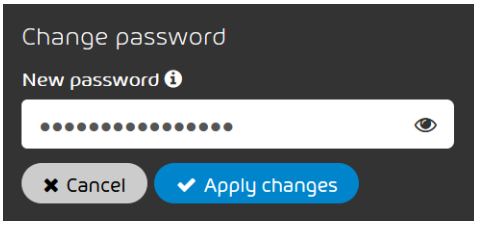


Figure 194: Enter a password

7. Click on **Apply changes**.

The password is saved. A confirmation message is displayed. For security reasons, the user is notified by email when the password is changed.

The password for a manually created mailbox has been changed.

Resetting Multi-Factor Authentication

You have enabled multi-factor authentication for the users of a domain (see Enabling Multi-Factor Authentication on page 296). A user of the domain has configured multi-factor authentication for their Control Panel account (see "Configuring Multi-Factor Authentication" in the Control Panel manual).

If a user experiences problems with multi-factor authentication (see "Troubleshooting: Problems with Multi-Factor Authentication" in the Control Panel manual), you can reset multi-factor authentication for the user. By doing so, multi-factor authentication is deactivated for the user and their configuration of multi-factor authentication is deleted.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain of the user for whom you would like to reset multi-factor authentication.
3. Navigate to **Customer Settings** > **Mailboxes**.
4. Click on the menu arrow next to the mailbox for which you would like to reset multi-factor authentication.

   ➜

   A menu opens.

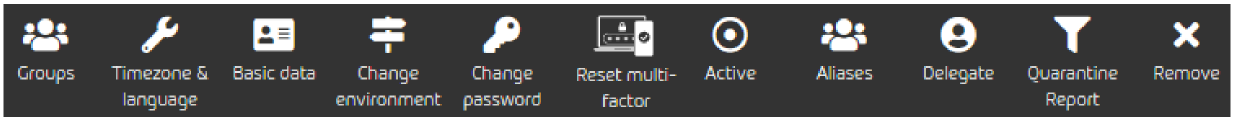


Figure 195: Menu

5. Click on **Reset multi-factor authentication**.

   ➜

   An extended view opens.

6. Click on **Reset multi-factor authentication**.

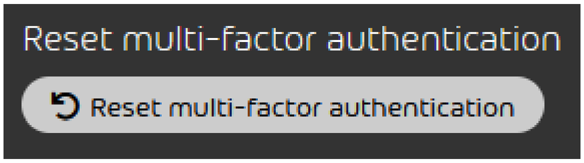
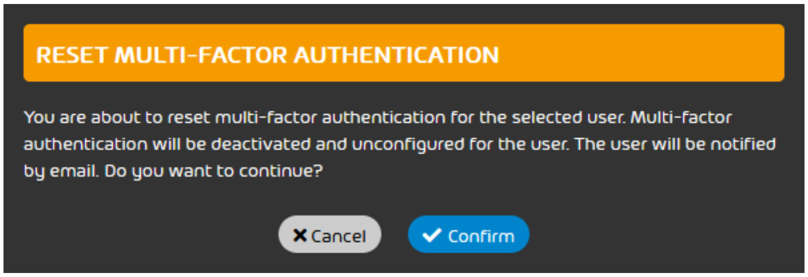

Reset multi-factor authentication
Reset multi-factor authentication

Figure 196: Resetting multi-factor authentication

A confirmation window opens.

7. Click on **Confirm**.



You are about to reset multi-factor authentication for the selected user. Multi-factor authentication will be deactivated and unconfigured for the user. The user will be notified by email. Do you want to continue?

Figure 197: Confirm

Multi-factor authentication is deactivated for the user and their configuration of multi-factor authentication is deleted. The user is informed by email that multi-factor authentication has been deactivated for their account. From now on, the user can log in to the Control Panel without using multi-factor authentication.

Multi-factor authentication has been reset for a user.

The user can reconfigure multi-factor authentication for their account (see "Configuring Multi-Factor Authentication" in the Control Panel manual).

Removing a Mailbox

You have added a mailbox to the Control Panel (see Adding a Mailbox on page 216 and Importing Mailboxes from a CSV File on page 219).

In the **Customer Settings** > **Mailboxes** module, you can remove manually created mailboxes (see Mailbox Types on page 215) from the Control Panel.

All settings of a mailbox are lost after its deletion. This has the following effects:

- The connection to the Control Panel is lost and future emails from the mailbox will not be processed by our services any longer.
- Owners of removed mailboxes will no longer be able to log in to the Control Panel with their credentials.
- Deleted mailboxes are removed from the groups (see Groups on page 262) to which they belong.
- Role assignments (see Roles on page 49) to users of deleted mailboxes are deleted.
- Alias addresses (see Adding an Alias Address on page 237) of deleted mailboxes are deleted.
- Deleted mailboxes are removed from forwarding lists of forward mailboxes (see Adding a Forward Mailbox on page 231).
- Deleted mailboxes are removed from delegate lists (see Entering a Delegate on page 239) of other mailboxes. Delegations to the deleted mailboxes are deleted.

The data related to emails to and from deleted mailboxes is kept in the Control Panel and is visible to administrators and to users to whom the deleted mailboxes are assigned.

Notice:

Deleting a mailbox in the Control Panel only affects the data and settings stored for that mailbox in the Control Panel. The mailbox itself remains.

Important:

LDAP mailboxes cannot be manually removed from the Control Panel.

Notice:

Instead of removing mailboxes individually, administrators can also remove multiple mailboxes at once (see Removing Multiple Mailboxes on page 259).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain from which you would like to delete a mailbox.
3. Navigate to **Customer Settings** > **Mailboxes**.
4. Click on the menu arrow next to the desired mailbox.

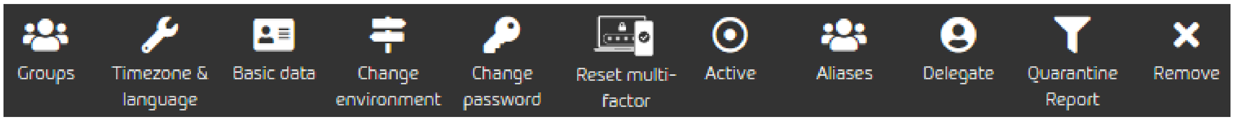


Figure 198: Open menu

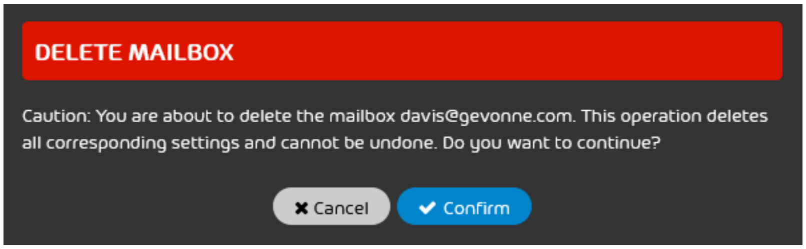
➜

A menu opens.

5. Click on **Remove**.

➜

A confirmation window opens.



DELETE MAILBOX

Caution: You are about to delete the mailbox davis@gevonne.com. This operation deletes all corresponding settings and cannot be undone. Do you want to continue?

Figure 199: Remove a mailbox

6. Click on **Confirm**.

➜

The mailbox is removed from the Control Panel. A confirmation message is displayed.

A manually created mailbox has been removed from the Control Panel.

Removing Multiple Mailboxes

You have added mailboxes to the Control Panel (see Adding a Mailbox on page 216 and Importing Mailboxes from a CSV File on page 219).

In the **Customer Settings** > **Mailboxes** module, you can remove multiple manually created mailboxes (see Mailbox Types on page 215) from the Control Panel at once.

All settings of a mailbox are lost after its deletion. This has the following effects:

- The connection to the Control Panel is lost and future emails from the mailbox will not be processed by our services any longer.
- Owners of removed mailboxes will no longer be able to log in to the Control Panel with their credentials.
- Deleted mailboxes are removed from the groups (see Groups on page 262) to which they belong.
- Role assignments (see Roles on page 49) to users of deleted mailboxes are deleted.
- Alias addresses (see Adding an Alias Address on page 237) of deleted mailboxes are deleted.
- Deleted mailboxes are removed from forwarding lists of forward mailboxes (see Adding a Forward Mailbox on page 231).
- Deleted mailboxes are removed from delegate lists (see Entering a Delegate on page 239) of other mailboxes. Delegations to the deleted mailboxes are deleted.

The data related to emails to and from deleted mailboxes is kept in the Control Panel and is visible to administrators and to users to whom the deleted mailboxes are assigned.

Notice:

Deleting a mailbox in the Control Panel only affects the data and settings stored for that mailbox in the Control Panel. The mailbox itself remains.

Important:

LDAP mailboxes cannot be manually removed from the Control Panel.

Notice:

Instead of removing multiple mailboxes at once, administrators can also remove mailboxes individually.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to remove mailboxes.
3. Navigate to **Customer Settings** > **Mailboxes**.
4. Click on ☰ at the top of the module.

   ➜

   A column with checkboxes is displayed in the list of domains.
5. Tick the checkboxes of the mailboxes that you would like to remove.

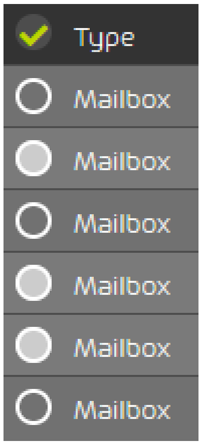


Figure 200: Select mailboxes

➜

The button **Remove** is enabled.

6. Click on **Remove**.

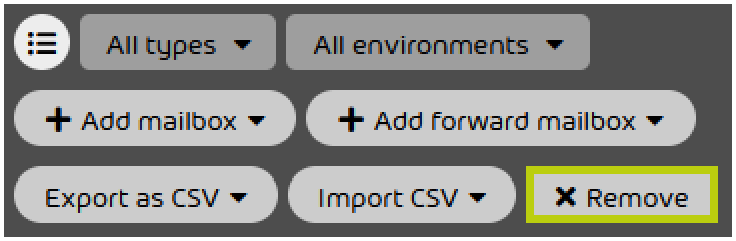
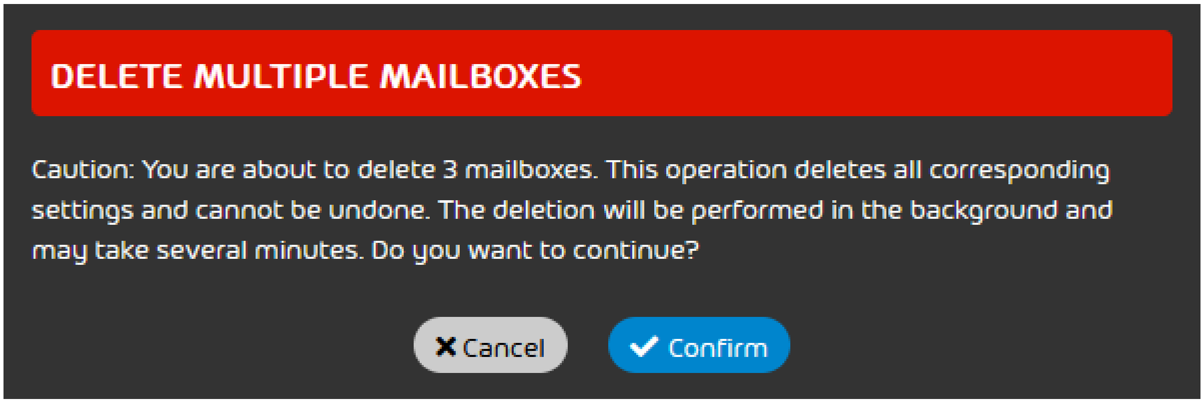


Figure 201: Remove the mailboxes

➜

A confirmation window is displayed.

7. Click on **Confirm**.



DELETE MULTIPLE MAILBOXES

Caution: You are about to delete 3 mailboxes. This operation deletes all corresponding settings and cannot be undone. The deletion will be performed in the background and may take several minutes. Do you want to continue?

Figure 202: Confirm deletion

➜

The mailboxes are removed from the Control Panel. The deletion is performed in the background and may take a few minutes.

✓

Multiple manually created mailboxes have been removed from the Control Panel.

Groups

In the Control Panel, mailboxes can be added to groups. Some services in the Control Panel can only be applied to groups. Some other services offer group-wide settings. Thus, groups simplify the configuration of services in the Control Panel.

In the **Customer Settings** > **Groups** module, customer-level administrators can create groups and add members individually (see Creating a Group on page 262), as well as manage existing groups. Already existing lists of group members can be imported from CSV files (see Importing Group Members from a CSV File on page 265). These CSV files must meet special requirements (see CSV Files for Group Member Import on page 269). It is also possible to export member lists of existing groups as CSV files (see Exporting Groups as a CSV File on page 276).

For customer-level administrators, the following options for managing groups are available in the group menu.

Table 17: Manage groups

SYMBOL	NAME	DESCRIPTION
ℹ	Details	Detailed information about the group
👥	Manage members	Adding/deleting members (see Managing Members on page 270)
A	Rename	Changing the group name (see Renaming a Group on page 272)
✎	Customize description	Customizing the group description (see Customizing a Group Description on page 274)
✖	Delete	Deleting the group (see Deleting a Group on page 278)

Creating a Group

In the **Customer Settings** > **Groups** module, you can create a new group from existing mailboxes.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to create a group.
3. Navigate to **Customer Settings** > **Groups**.
4. Click on **Add**.

➔

A drop-down menu opens.

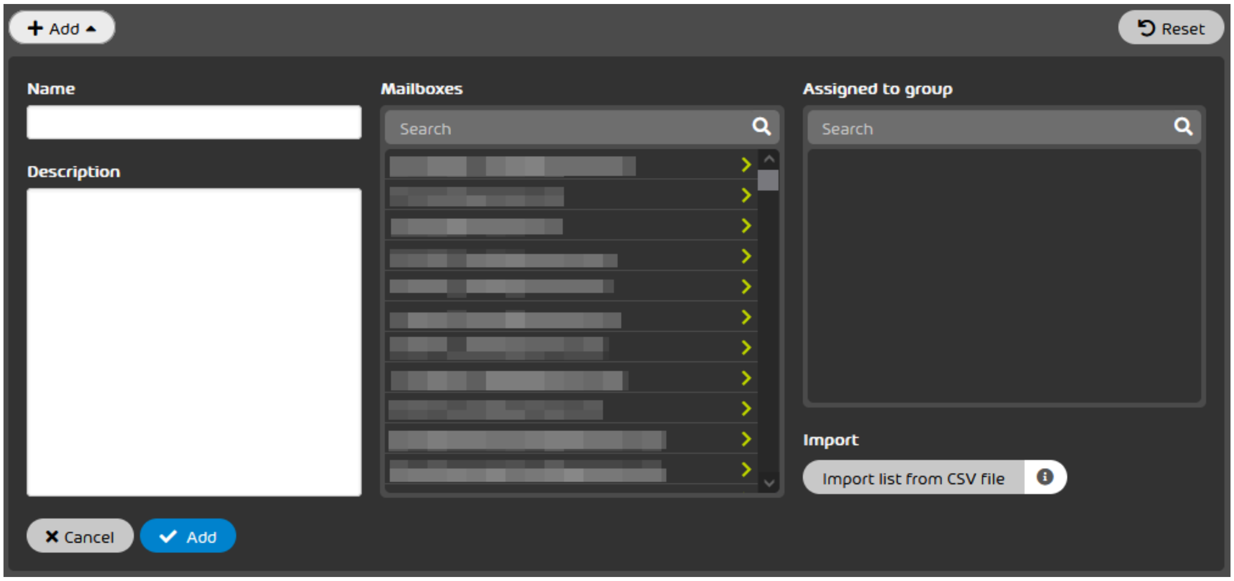


Figure 203: Add a new group

5. Enter a group name under **Name**.
6. Optional: Describe the group in the **Description** field.

7. Add mailboxes to the new group. You have two options:

   - Under **Mailboxes**, select at least one mailbox to add to the group. To add a mailbox to the group, click on the mailbox.

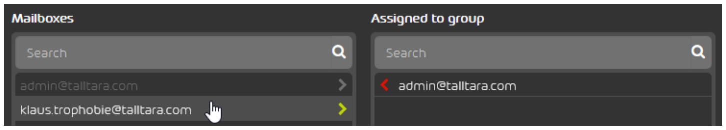


Figure 204: Add a single mailbox

   - Import an existing list of members from a CSV file (see Importing Group Members from a CSV File on page 265). With each import, you can only import members for a single group.

   The selected or imported mailboxes are displayed under **Assigned to group**.

8. Click on **Add**.

   The group is saved. The mailboxes under **Assigned to group** are assigned to the group.

A group has been created.

Next, you can manage the group members (see Managing Members on page 270 and Importing Group Members from a CSV File on page 265), rename the group (see Renaming a Group on page 272), change the group description (see Customizing a Group Description on page 274), export the group as a CSV file (see Exporting Groups as a CSV File on page 276) or delete the group (see Deleting a Group on page 278).

Importing Group Members from a CSV File

Instead of adding users manually to a group, you can add users from a CSV list in the **Customer Settings** > **Groups** module. With a CSV list, you can assign users to both newly-created and existing groups.

Notice:

With each import, you can only import members for a single group.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain containing the group to which you would like import members.
3. Navigate to **Customer Settings** > **Groups**.

4. You have two options:

   - Create a new group and import members from a CSV file (see Section a)
   - Add members from a CSV file to an existing group (see Section b)

a) Click on **Add**.

➜

A form is displayed.

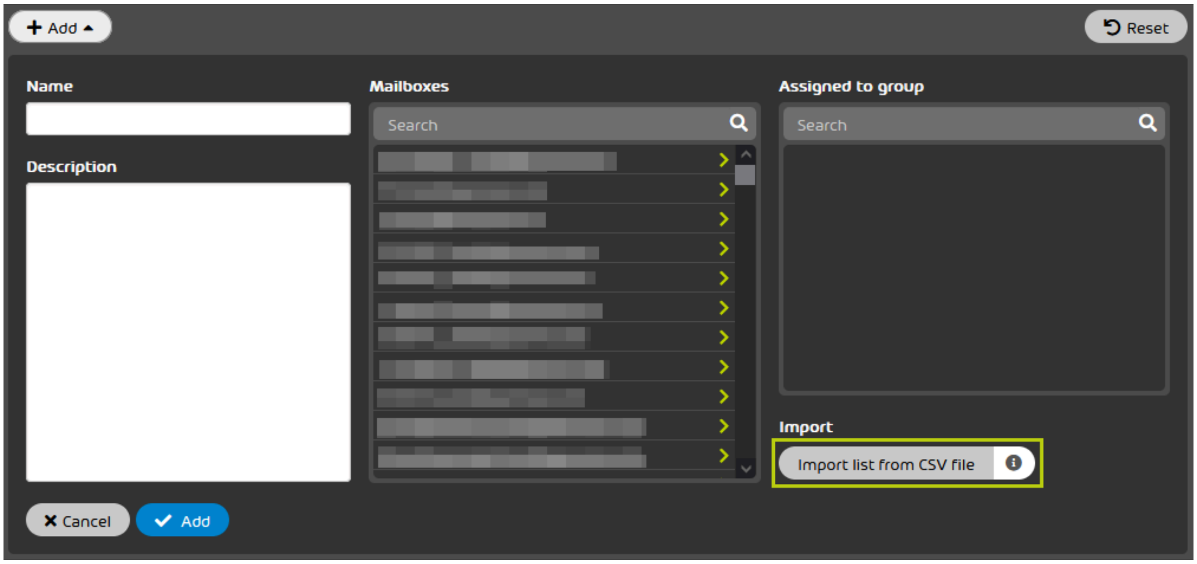


Figure 205: Import group members for a new group from a CSV file

b) Select an existing group at the bottom of the page and click on **Manage members**.

➜

A form is displayed.

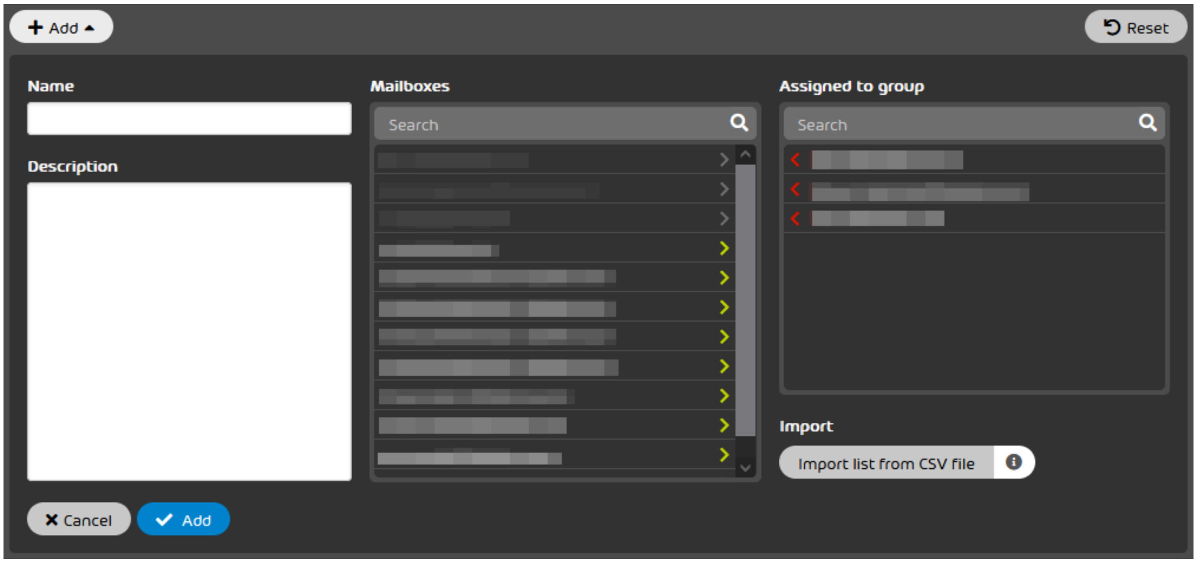


Figure 206: Import group members for an existing group from a CSV file

5. Click on **Import list from CSV file**.

Notice:

Only group members for the group that is currently selected are imported from the CSV file.

A file selection window opens.

6. Select the desired CSV file.

Important:

To ensure that an external CSV file with group members can be imported into the Control Panel without errors, special rules regarding the file format and content structure as well as a valid syntax must be observed (see CSV Files for Group Member Import on page 269).

➔

All group members imported from the CSV file are displayed under **Assigned to group**.

Notice:

The following rules apply to the import of group members from CSV files:

- Group members that are already assigned to another group are also imported from a CSV file. The group members are displayed under **Assigned to group**.
- If entries are imported from multiple CSV files, duplicate entries are automatically detected within different CSV files. Duplicate entries are imported only once and displayed under **Assigned to group**.
- Duplicate entries within a single CSV file are imported only once and displayed under **Assigned to group**.
- Invalid entries are also imported from a CSV file and displayed under **Assigned to group**. As soon as you save the group, the system checks whether the entries are valid. If the list contains invalid entries, an error message appears. Remove all invalid entries (see CSV Files for Group Member Import on page 269) and save the group.

7. Click on **Add** or **Apply changes** to save your changes.

   The group is saved.

   > **Important:**
   >
   > If the list under **Assigned to group** contains invalid entries or group members of other groups, an error message appears. Remove group members of other groups and invalid entries from the list and save the group.

Group members have been imported from a CSV file and added to a group.

CSV Files for Group Member Import

To ensure that an external CSV file with information about group members can be imported into the Control Panel without errors (see Importing Group Members from a CSV File on page 265), special rules regarding the file extension and content structure must be observed.

Rules for creating a CSV file for group member import

- The extension of the import file is always **.csv**. Other file extensions, such as .txt or .docx, are not allowed and will not be accepted.
- The CSV file contains only one column, in which individual entries are entered one below the other.
- The first row always contains the column name and can be named individually.
- Group members are listed by their email addresses. The addresses must be correctly formatted (according to the pattern "local-part@hostname.top-level-domain").

> **Important:**
>
> Incorrectly formatted addresses are not considered during the import.

- Each row may contain only one address.

- Duplicated entries do not affect the processing of the file, but should be avoided.

Managing Members

✓ You have created a group (see Creating a Group on page 262).

In the **Customer Settings** > **Groups** module, you can add manually created mailboxes (see Mailbox Types on page 215) to groups or remove them from groups. It does not matter if the group is synchronized or not.

> **Notice:**
>
> LDAP mailboxes cannot be added to groups or removed from groups in the Control Panel. Their group memberships are only managed in the directory service.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to manage group members.
3. Navigate to **Customer Settings** > **Groups** and click on the menu arrow for the desired group.

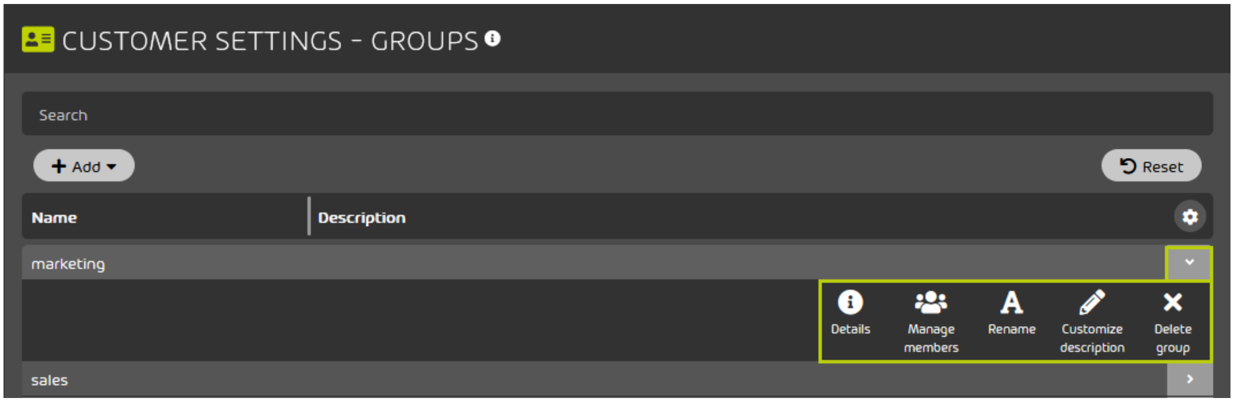


Figure 207: Open Groups menu

4. Click on **Manage members**.

➔

A drop-down menu with two windows opens, showing all registered mailboxes on the left and all mailboxes assigned to the group on the right.

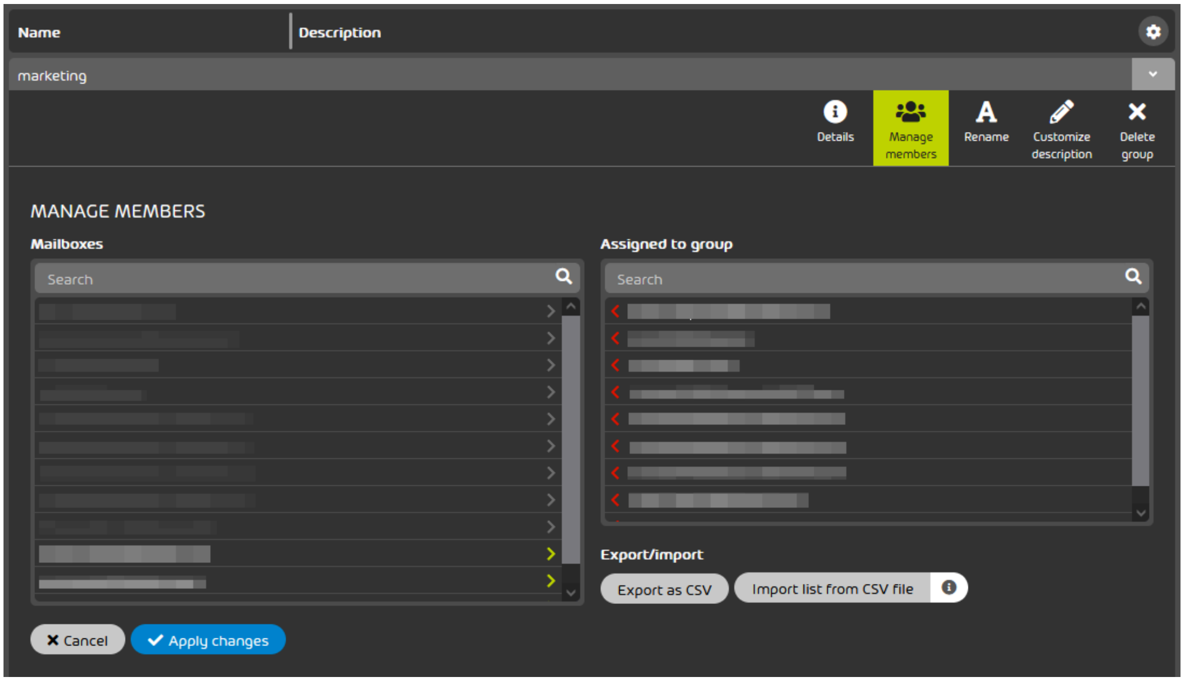


Figure 208: Manage group members

5. Manage the members of a group:

   - If you would like to add more members to the group, click on the members to be added in the table **Mailboxes** (on the left). You can also import existing group lists as a CSV file (see Importing Group Members from a CSV File on page 265).
   - If you would like to remove members from the group, click on the group members to be removed in the table **Assigned to group** (on the right).

   > **Notice:**
   >
   > LDAP mailboxes are grayed out in the tables **Mailboxes** and **Assigned to group**, and cannot be moved from one table to the other.

   ➜

   The members are added to the group or removed from the group.

6. Click on **Apply changes**.

   ➜

   The changes are saved in the Control Panel.

   > **Notice:**
   >
   > Changes to synchronized groups are not transferred to the directory service during synchronization, but they will persist in the Control Panel.

✓

The members of the group have been managed.

Renaming a Group

You have created a group (see Creating a Group on page 262).

Under **Customer Settings** > **Groups**, you can rename groups (see Groups on page 262).

Important:

Groups that are synchronized from a directory service will no longer be synchronized after they have been renamed.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain of the group you would like to rename.
3. Navigate to **Customer Settings** > **Groups** and click on the menu arrow for the desired group.

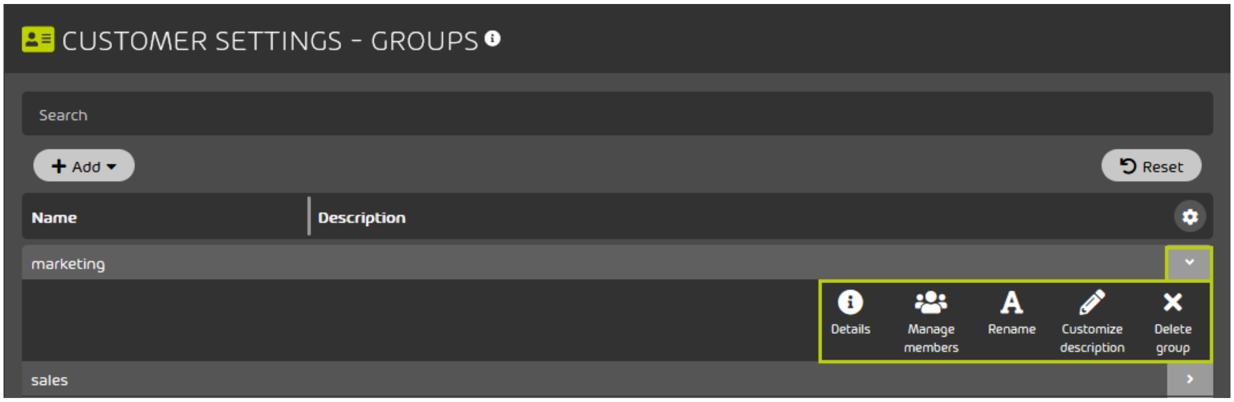
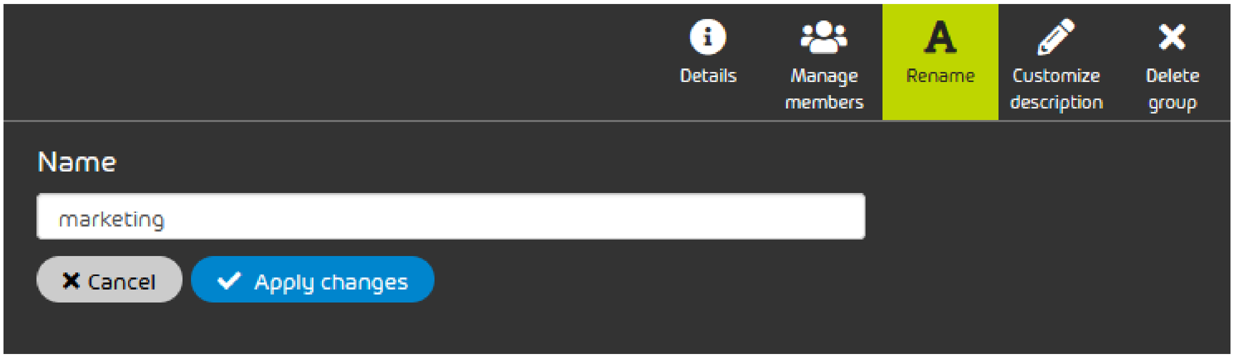


Figure 209: Open Groups menu

4. Click on **Rename**.

A drop-down menu opens.



Name: marketing

5. **Important:**

   If a non-synchronized group is given the name of a group from a directory service that is synchronized via LDAP, the group will be synchronized subsequently. Synchronized mailboxes that are assigned to the group in the directory service are assigned to the group in the Control Panel. The group membership of synchronized mailboxes is continuously synchronized. Non-synchronized mailboxes that have been manually assigned to the group in the Control Panel remain assigned to the group and are not affected by synchronizations.

   Enter the new group name in the input field.
6. Click on **Apply changes**.

✓

A group has been renamed.

Customizing a Group Description

☑ You have created a group (see Creating a Group on page 262).

In the **Customer Settings** > **Groups** module, you can customize group descriptions.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain of the group whose description you would like to customize.

3. Navigate to **Customer Settings** > **Groups** and click on the menu arrow for the desired group.

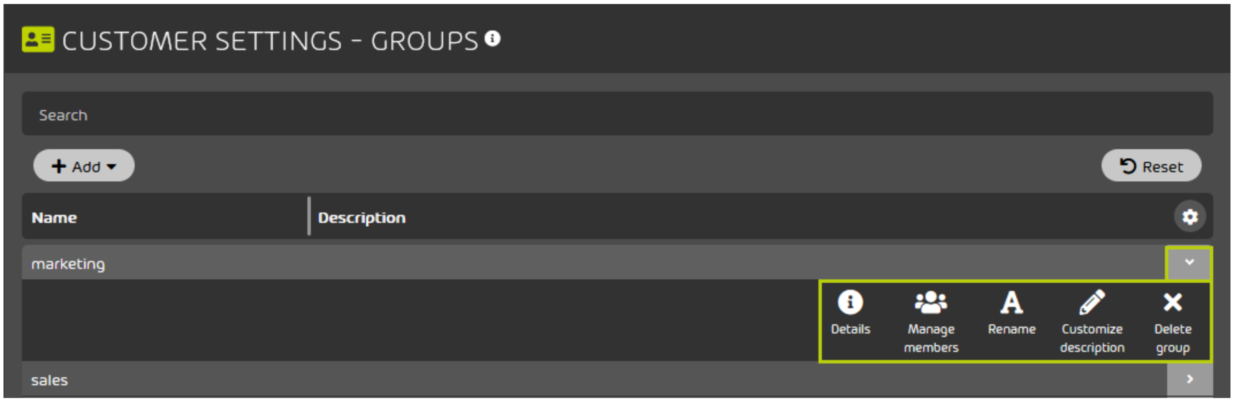
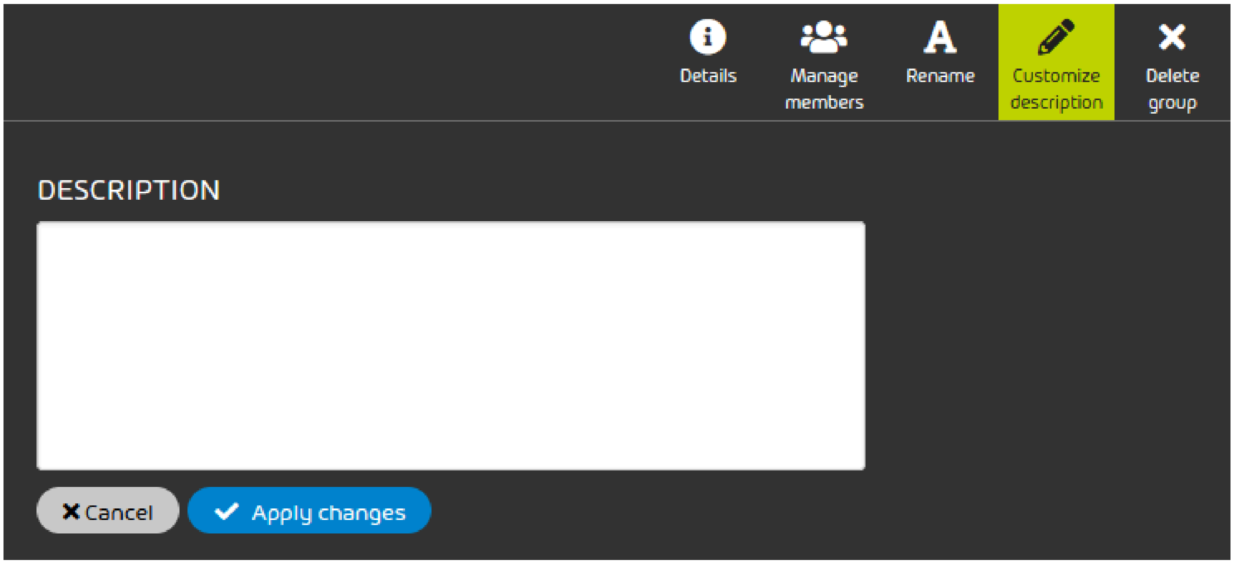


Figure 210: Open Groups menu

4. Click on **Customize description**.

A drop-down menu opens.



5. Enter the desired description for the group and click on **Apply changes**.

A group description has been customized.

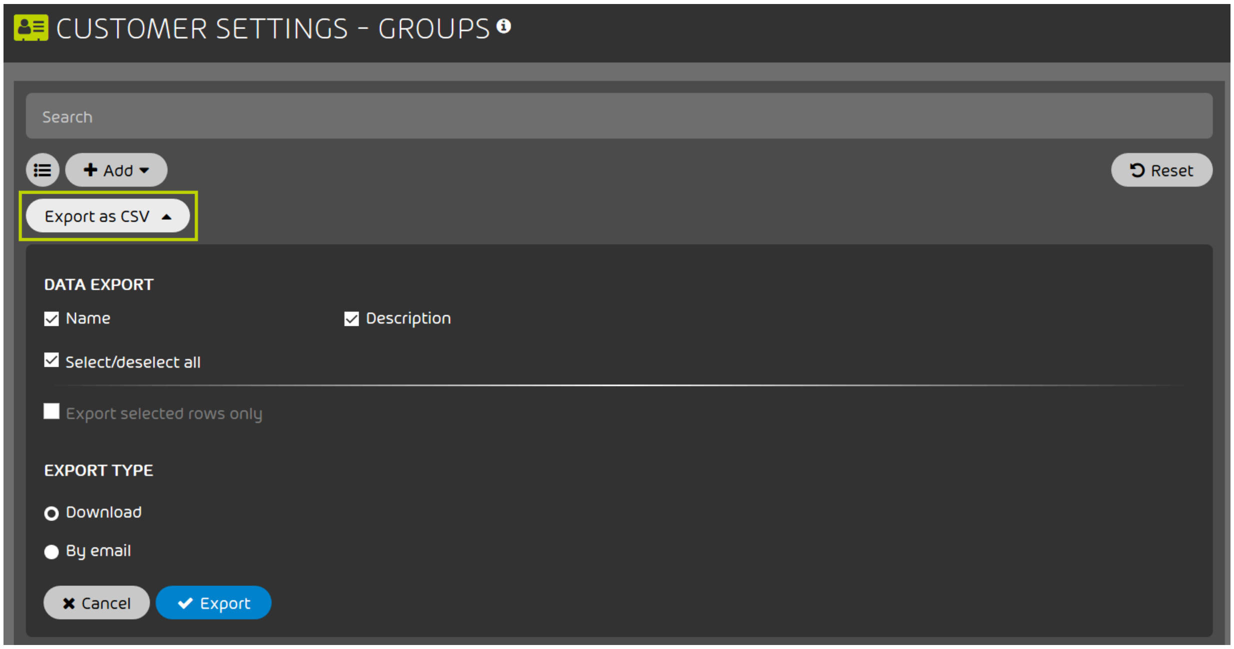
Exporting Groups as a CSV File

You have created a group (see Creating a Group on page 262).

In the **Customer Settings** > **Groups** module, you can export groups as a CSV file.

1. Log in to the Control Panel with your administrative credentials.
2. Select a domain from the scope selection.
3. Navigate to **Customer Settings** > **Groups**.
4. Click on **Export as CSV**.

   An extended view opens.



DATA EXPORT

☑ Name ☑ Description

☑ Select/deselect all

□ Export selected rows only

EXPORT TYPE

● Download

○ By email

Figure 211: Select data for the export

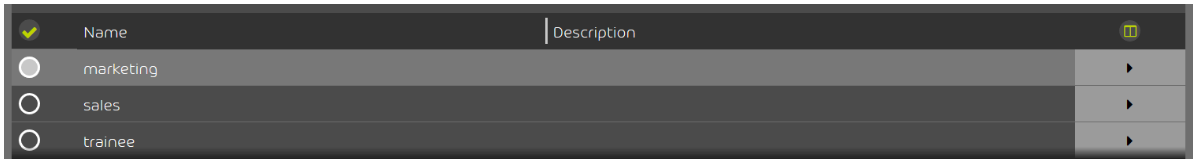
5. Under **Data export**, tick the checkboxes of the data you would like to export.
   - **Name**: The names of the groups are exported.
   - **Description**: The descriptions of the groups are exported.
   - **Select/deselect all**: All previously described checkboxes are activated or deactivated.
6. Optional: If you only want to export data of selected groups, proceed as follows:

   a) Click on ☰ at the top of the module.

   ➜

   A column with checkboxes is displayed in the table.

   b) Tick the checkboxes of the rows from which you would like to export data.



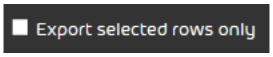
✓	Name	Description	◫
○	marketing		▸
○	sales		▸
○	trainee		▸

Figure 212: Select rows

   ➜

   The checkbox **Export selected rows only** is enabled in the extended view.

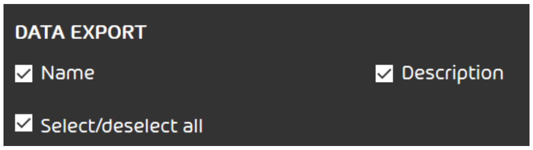
   c) Tick the enabled checkbox **Export selected rows only**.



☐ Export selected rows only

Figure 213: Export selected rows

7. Optional: Select under **Data export** whether you want to export both the **Name** and the **Description** column.



DATA EXPORT

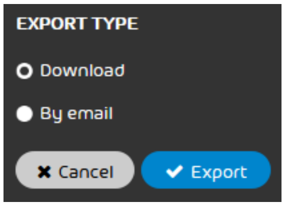
☑ Name ☑ Description

☑ Select/deselect all

Figure 214: Select columns

8. Under **Export type**, select if the CSV file should be made available for download or delivered by email.

   - **Download**: The CSV file is provided as download.
   - **By email**: The CSV file is sent by email.



EXPORT TYPE

◉ Download

○ By email

Figure 215: Select export type

9. Click on **Export**.

The data of a group has been exported as a CSV file.

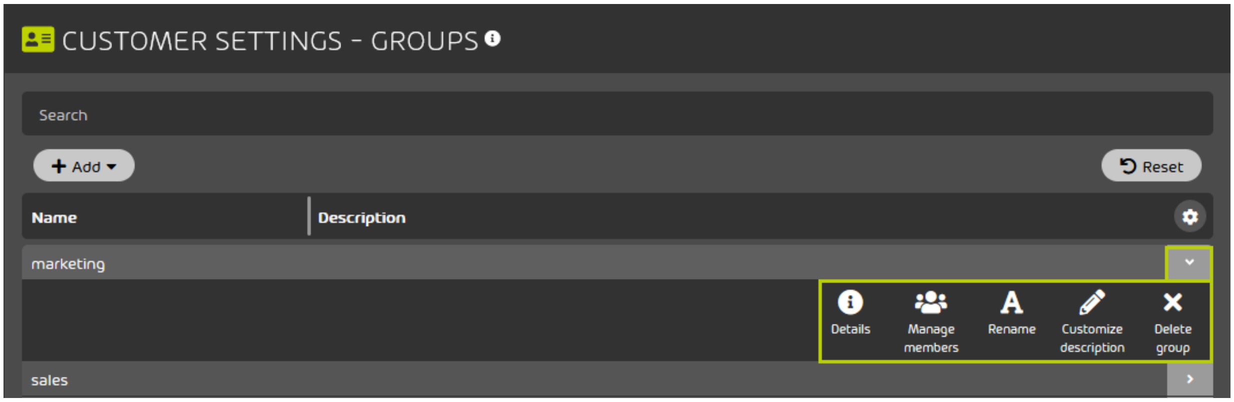
Deleting a Group

You have created a group (see Creating a Group on page 262).

In the **Customer Settings** > **Groups** module, you can delete an existing group (see Groups on page 262).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to delete a group.

3. Navigate to **Customer Settings** > **Groups** and click on the menu arrow for the desired group.



CUSTOMER SETTINGS - GROUPS

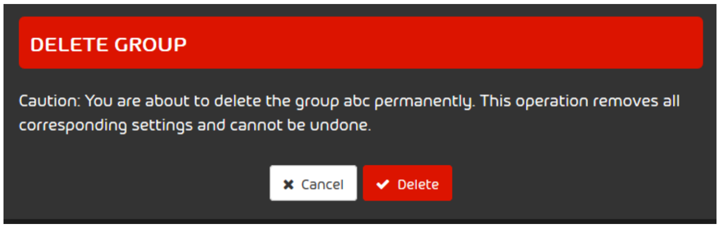
Figure 216: Open Groups menu

4. Click on **Confirm**.

CAUTION:

Deleting the group irrevocably deletes all settings and all group members!

A warning message is displayed.



DELETE GROUP

Caution: You are about to delete the group abc permanently. This operation removes all corresponding settings and cannot be undone.

5. Confirm the warning message by clicking on **Confirm**.

A group has been deleted.

Domains

In the **Customer Settings** > **Domains** module, a customer's primary domain and alias domains are displayed and managed.

Notice:

Alias domains can, for example, be applied if several top-level domains exist for one domain. For instance, an administrator can specify the top-level domains **.de** and **.es** for the primary domain **customer_domain.com**. In this case, **customer_domain.de** and **customer_domain.es** would be alias domains of the primary domain.

Alias domains do not incur any costs.

Customer-level administrators can create new alias domains (see Adding an Alias Domain on page 280) and delete existing alias domains (see Deleting an Alias Domain on page 287) in this module. The primary domain cannot be deleted. Furthermore, administrators can export the displayed domains in CSV format (see Exporting Domains as a CSV File on page 284) and import new alias domains from CSV files (see Importing Alias Domains from a CSV File on page 282). These CSV files must meet special requirements (see CSV Files for the Import of Alias Domains on page 283).

For security reasons, we check whether a customer is entitled to manage the domains added to the Control Panel (see Domain Verification on page 289).

Adding an Alias Domain

As a customer-level administrator, you can add alias domains to a customer's primary domain in the **Customer Settings** > **Domains** module. The procedure described here allows you to add alias domains individually. Alternatively, you can import a list of alias domains from a CSV file (see Importing Alias Domains from a CSV File on page 282).

Notice:

Alias domains can, for example, be applied if several top-level domains exist for one domain. For instance, an administrator can specify the top-level domains **.de** and **.es** for the primary domain **customer_domain.com**. In this case, **customer_domain.de** and **customer_domain.es** would be alias domains of the primary domain.

Alias domains do not incur any costs.

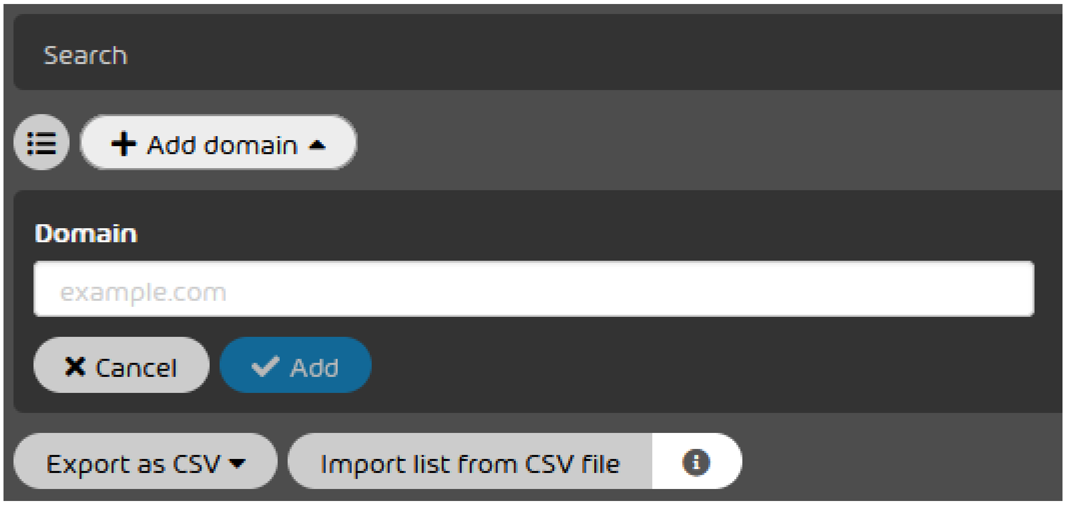
1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the customer to whose primary domain you would like to add an alias domain.
3. Navigate to **Customer Settings** > **Domains**.
4. Click on **Add domain**.

   ➔

   Additional settings are displayed.
5. **Important:**

   The alias domain must be a valid domain.

   Enter the alias domain in the **Domain** field.



6. Click on **Add**.

   The alias domain is added to the list of domains. The alias domain is first assigned the state **Not verified** in the **Verified** column. After a few minutes, we check whether the alias domain can be verified (see Domain Verification on page 289).

An alias domain has been added to a customer's primary domain.

Next, you can export the customer's domains as a CSV file (see Exporting Domains as a CSV File on page 284) or delete the alias domain (see Deleting an Alias Domain on page 287).

Importing Alias Domains from a CSV File

Instead of adding alias domains individually to a primary domain (see Adding an Alias Domain on page 280), you can import alias domains in the **Customer Settings** > **Domains** module from a CSV list. You can import alias domains from a CSV list both initially, before any data has been entered, as well as anytime later.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the customer to whose primary domain you would like to add alias domains.
3. Navigate to **Customer Settings** > **Domains**.
4. Click on **Import list from CSV file**.

   A file selection window opens.

5. Select the desired CSV file.

> **Important:**
>
> To ensure that an external CSV file with alias domains can be imported into the Control Panel without errors, special rules regarding the file format and content structure as well as a valid syntax must be observed (see CSV Files for the Import of Alias Domains on page 283).

➜

If the CSV file contains alias domains that are not yet available in the Control Panel, they will be added to the list of domains.

✓

Alias domains have been imported from a CSV file and added to the customer's primary domain.

Next, you can export the customer's domains as a CSV file (see Exporting Domains as a CSV File on page 284) or delete alias domains (see Deleting an Alias Domain on page 287).

CSV Files for the Import of Alias Domains

To ensure that an external CSV file with alias domains can be imported into the Control Panel without errors (see Importing Alias Domains from a CSV File on page 282), special rules regarding the file extension and content structure must be observed.

Rules for creating a CSV file to import alias domains

- The extension of the import file is always **.csv**. Other file extensions, such as .txt or .docx, are not allowed and will not be accepted.
- The CSV file contains only one column, in which individual entries are entered one below the other.
- The first row always contains the column name and can be named individually.

- The domain names must be correctly formatted.

Important:

Incorrectly formatted domain names lead to an immediate termination of the import. Correct entries will not be imported if the import is aborted.

- Each row may contain only one domain name.
- The file must no contain duplicate entries.

Important:

Duplicate entries lead to an immediate termination of the import. Correct entries will not be imported if the import is aborted.

Exporting Domains as a CSV File

In the **Customer Settings** > **Domains** module, you can export a customer's domains as a CSV file. The exported CSV file contains two columns. The first column contains the domain names. The second column contains the domain types. Here, a distinction is made between the primary domain and the alias domains. You can export all domains of a customer or only selected domains.

Notice:

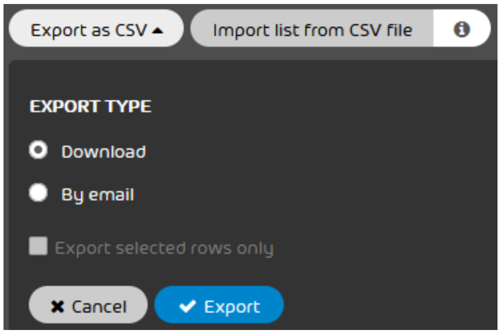
The exported CSV files cannot be used to import alias domains (see Importing Alias Domains from a CSV File on page 282 and CSV Files for the Import of Alias Domains on page 283).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the customer whose domains you would like to export.
3. Navigate to **Customer Settings** > **Domains**.

4. Click on **Export as CSV**.

   ➜

   The CSV export settings are displayed.



EXPORT TYPE

● Download

○ By email

□ Export selected rows only

Figure 217: CSV export settings

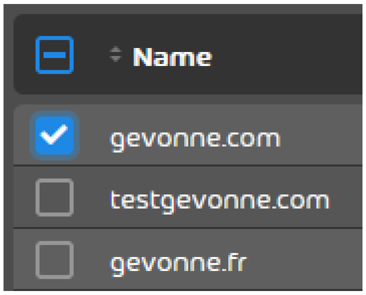
5. Optional: If you only want to export selected domains, proceed as follows:

   a) Click on ☰ at the top of the module.

      ➔

      A column with checkboxes is displayed in the list of domains.

   b) Activate the checkboxes of the rows that you would like to export.



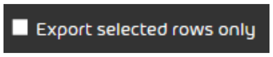
⊟	Name
☑	gevonne.com
☐	testgevonne.com
☐	gevonne.fr

Figure 218: Select rows

      ➔

      In the CSV export settings, the **Export selected rows only** checkbox is enabled.

   c) Tick the **Export selected rows only** checkbox.



☐ Export selected rows only

Figure 219: Export selected rows

6. Under **Export type**, select whether the CSV file shall be provided as a download or sent by email.

   - **Download**: The CSV file is provided as download.
   - **By email**: The CSV file is sent by email.

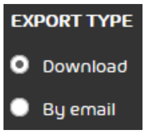


Figure 220: Select export type

If the **By email** option has been selected, an input field is displayed.

7. If you have selected the **By email** option, enter the email address to which the CSV file should be sent in the input field.
8. Click on **Export**.

   The domains are exported as a CSV file. The CSV file is provided as a download or sent by email.

All or selected domains of a customer have been exported as a CSV file.

Deleting an Alias Domain

You have added alias domains to a customer's primary domain (see Adding an Alias Domain on page 280 and Importing Alias Domains from a CSV File on page 282).

You can delete a customer's existing alias domains from the Control Panel.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the customer for whom you would like to delete an alias domain.

3. Navigate to **Customer Settings** > **Domains**.
4. Click on the menu arrow next to the alias domain that you would like to delete.

   ➜

   A menu opens.
5. **CAUTION:**

   Once the alias domain is deleted, all email addresses and settings of the alias domain will be permanently deleted.

   If an email address of the deleted domain has been the primary address of a mailbox to which an email address of a different domain is assigned as an alias address, the alias address becomes the new primary address of the mailbox. If several alias addresses are assigned to the mailbox, the alias address that was created first becomes the primary address and the other alias addresses remain. In the future, the user of the mailbox must use the new primary address as their username in the Control Panel.

   Click on **Delete domain**.

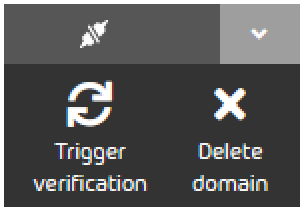
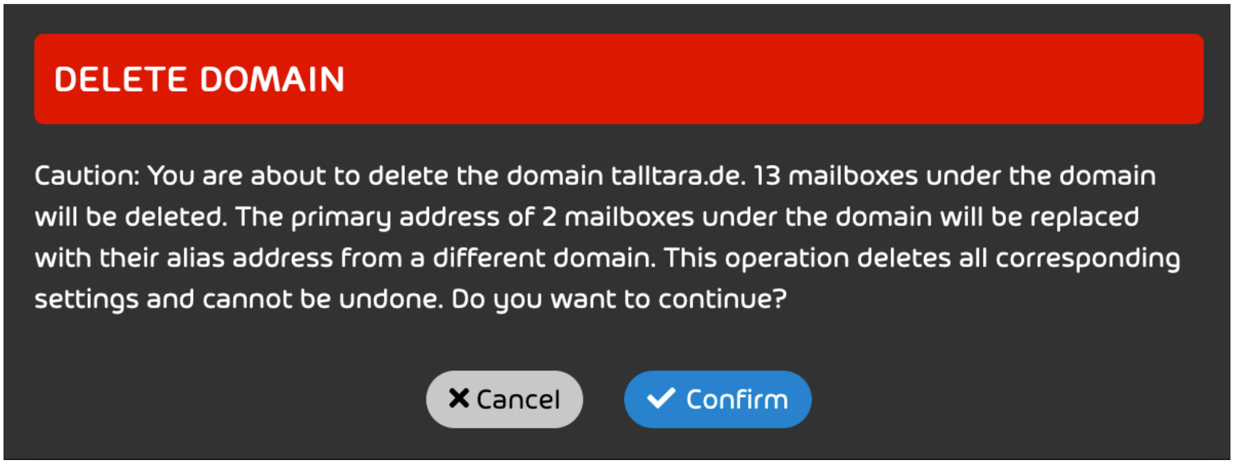


Figure 221: Delete domain

➜

A warning message is displayed.

6. Click on **Confirm**.



DELETE DOMAIN

Caution: You are about to delete the domain talltara.de. 13 mailboxes under the domain will be deleted. The primary address of 2 mailboxes under the domain will be replaced with their alias address from a different domain. This operation deletes all corresponding settings and cannot be undone. Do you want to continue?

Figure 222: Confirm deletion

➜

The alias domain, its mailboxes and the settings of the alias domain are deleted from the Control Panel. The alias domain is added to the list of domains.

✓

The alias domain has been deleted from the Control Panel.

Domain Verification

For security reasons, we check whether a customer is entitled to manage the domains added to the Control Panel. We thus check the domains that are entered for a customer in the **Customer Settings** > **Domains** module (see Domains on page 280).

Notice:

Customer-level administrators can access this module if they select the customer's primary domain from the scope selection (see Scope Selection on page 54).

If a domain passes the check, the domain is verified. The verification state is indicated by a symbol in the **Verified** column of the **Customer Settings** > **Domains** module. A domain can only be verified for a single customer in the Control Panel.

Table 18: Domain Verification

SYMBOL	EXPLANATION
✓	The domain is verified.
🔌	The domain is not verified.

We check a domain for the first time a few minutes after it was added to the Control Panel. During this process, we determine whether the MX records of the domain point to us (see "Changing the MX Records""Initial Service Setup in the manual Initial Service Setup). For unverified domains, the check is repeated once a day. However, customer-level administrators can manually start the check of an unverified domain at any time (see Triggering a Verification on page 291).

Notice:

If any problems occur during the verification of a domain, the customer can contact Support or their contact person.

Domain verification affects the **Email Live Tracking** module (see Email Live Tracking on page 58). The module only displays emails for mailboxes of verified domains. The domain of the mailbox is displayed for each email in the **Domain of the owner** field in the email details (see Extended Email Information on page 77). Once a domain is verified, the **Email Live Tracking** module displays all emails for mailboxes of the domain that have been sent to our infrastructure.

Notice:

Older emails for which the **Domain of the owner** field is empty are also displayed in the **Email Live Tracking** module.

Emails of the category **Rejected** are also displayed in the module. This prevents a loss of emails that had been sent to our infrastructure before the domain was created in the Control Panel, and were thus rejected by us.

Triggering a Verification

For unverified domains in the **Customer Settings** > **Domains** module, we automatically check whether the domains can be verified once a day (see Domain Verification on page 289). In addition, you can start the check of an unverified domain manually at any time.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the primary domain of the customer for whom you would like to check a domain.
3. Navigate to **Customer Settings** > **Domains**.
4. Click on the menu arrow next to the unverified domain for which you would like to start a check.

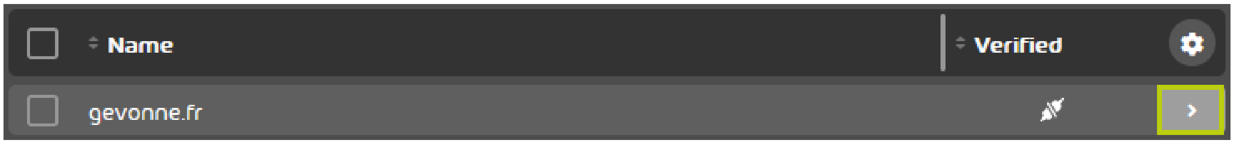


Figure 223: Open menu

A menu opens.

5. Click on **Trigger verification**.

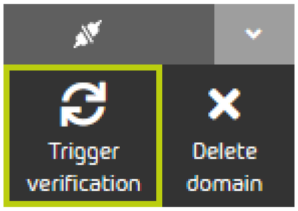


Figure 224: Start check

➜

We check whether the MX records of the domain point to us. If the domain passes the check, the status of the domain in the column **Verified** changes to **Verified**.

✓

The check of an unverified domain has been started.

Authentication Policies and IPs

In the **Customer Settings** > **Authentication policies & IPs** module, administrators can configure settings for the Control Panel login.

Customer-level and partner-level administrators can define a password policy for the Control Panel accounts of users (see Setting the Password Length on page 294). If desired, administrators can later reset the password policy back to default (see Resetting the Password Length on page 295).

Notice:

The password policies only apply to passwords managed in the Control Panel (see Mailbox Types on page 215).

For LDAP mailboxes, customer-level administrators can specify whether the users' credentials from the directory service will be used for the Control Panel login (see Configuring the Control Panel Login via LDAP on page 129) or whether the users' passwords will be managed in the Control Panel instead.

Customer-level administrators can enable multi-factor authentication for a customer's users (see Enabling Multi-Factor Authentication on page 296). This enables users to configure multi-factor authentication for their account (see chapter "Configuring Multi-Factor Authentication" in the Control Panel manual). Multi-factor authentication increases security for the Control Panel login because a one-time password from an authenticator app is required in addition to the Control Panel password. It is also possible to enforce multi-factor authentication for administrators (see Enforcing Multi-Factor Authentication for Administrators on page 297). Administrators can later deactivate multi-factor authentication for a customer's users again (see Deactivating Multi-Factor Authentication on page 299).

Notice:

Only users whose passwords are managed in the Control Panel or in a directory service via LDAP can configure multi-factor authentication in the Control Panel.

For security reasons, inactive users are by default automatically logged out of the Control Panel after 24 hours. Customer-level administrators can set a shorter time until auto logout or deactivate auto logout for their users (see Configuring Auto Logout on page 301). If desired, customer-level administrators can later reset the settings to default (see Resetting Auto Logout to Default on page 304).

By default, the Control Panel login is possible from any IPv4 address. However, in order to increase security, partner-level and customer-level administrators can specify that users may only access the Control Panel from certain IPv4 addresses or IPv4 ranges. Administrators can limit the login to certain IPv4 addresses or IPv4 ranges by adding the IPv4 addresses or IPv4 ranges to the **Customer Settings** > **Authentication policies & IPs** module (see Assigning an IP Address on page 305). Administrators can also delete IPv4 addresses and IPv4 ranges from the module again (see Deleting an IP Address on page 306). If no IPv4 address or IPv4 range is provided in the module, a login is possible from any IPv4 address. Otherwise, the login is limited to the provided IPv4 addresses and IPv4 ranges.

Setting the Password Length

You can also see the minimum requirements for new passwords as defined by the Control Panel.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to define password policies.
3. Navigate to **Customer Settings** > **Authentication policies & IPs**.

   Important:

   The password policies are inherited from partners to their customers. The subordinate customers can strengthen, but not weaken the password policies. For example, the subordinate customers can increase, but not reduce the password length.

4. Enter the minimum password length in the **Password length** input field.

   Notice:

   The minimum password length must be at least 8 characters.

   Notice:

   Other requirements for new passwords are displayed. These are defined by the Control Panel and cannot be changed. They establish that new passwords must contain at least one uppercase letter, one lowercase letter, one digit and one special character.

5. Click on **Save** to apply the settings.

   The minimum password length is updated in the Control Panel.

   > **Notice:**
   >
   > The new minimum password length is obligatory for all new passwords and does not affect any existing passwords.

The minimum password length has been set for a domain.

Next, you can reset the password policies (see Resetting the Password Length on page 295).

Resetting the Password Length

You have set a minimum password length for a domain (see Setting the Password Length on page 294).

In the **Customer Settings** > **Authentication policies & IPs** module, you can reset the minimum password length for a domain to default. Default settings are settings that have been specified by parent administrators.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to reset the minimum password length.
3. Navigate to **Customer Settings** > **Authentication policies & IPs**.
4. Click on **Default settings** to reset the minimum password length to default.
5. Click on **Save** to apply the settings.

The minimum password length for a domain has been reset to default.

Enabling Multi-Factor Authentication

You can enable multi-factor authentication for the users of a domain. This enables users of the domain to configure multi-factor authentication for their Control Panel account (see chapter "Configuring Multi-Factor Authentication" in the Control Panel manual).

Notice:

Only users whose passwords are managed in the Control Panel or in a directory service via LDAP can configure multi-factor authentication in the Control Panel.

Multi-factor authentication increases security for the Control Panel login because a one-time password from an authenticator app is required in addition to the Control Panel password. We recommend in particular that administrators configure multi-factor authentication for their account.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to enable multi-factor authentication.
3. Navigate to **Customer Settings** > **Authentication policies & IPs**.
4. Toggle the switch **Enable users to use multi-factor authentication** under **Multi-Factor Authentication**.

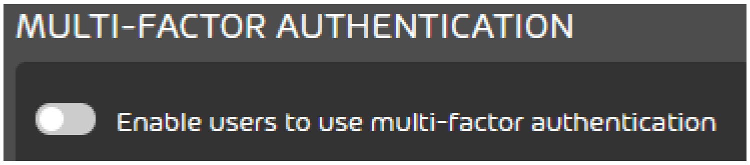
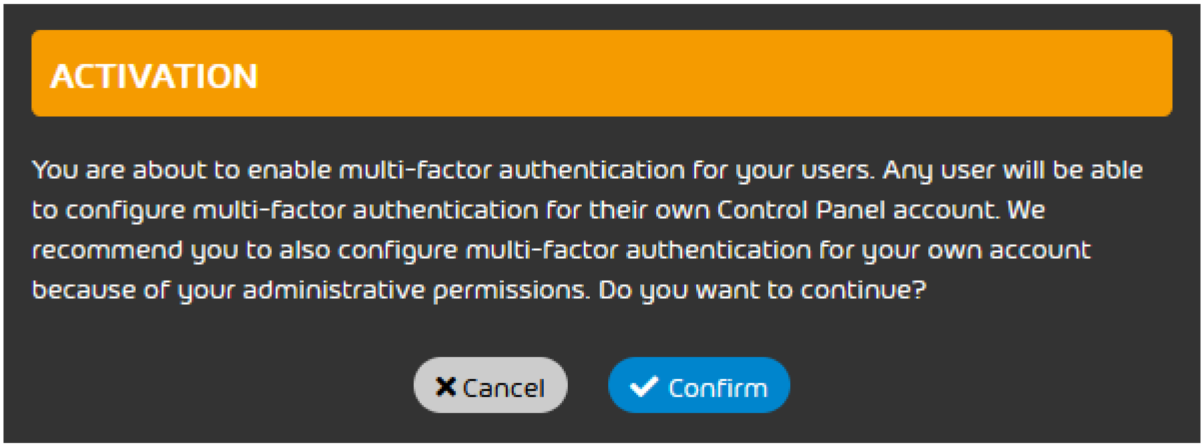

MULTI-FACTOR AUTHENTICATION
Enable users to use multi-factor authentication

Figure 225: Enable multi-factor authentication

➜

The button turns green and a confirmation window opens.

5. Click on **Confirm**.



ACTIVATION

You are about to enable multi-factor authentication for your users. Any user will be able to configure multi-factor authentication for their own Control Panel account. We recommend you to also configure multi-factor authentication for your own account because of your administrative permissions. Do you want to continue?

Figure 226: Confirm

Multi-factor authentication is enabled for the users of the domain.

Multi-factor authentication has been enabled for the users of a domain.

Next, the users of the domain can configure multi-factor authentication for their Control Panel account (see chapter "Configuring Multi-Factor Authentication" in the Control-Panel manual). If a user experiences problems with multi-factor authentication, you can reset multi-factor authentication for the user (see Resetting Multi-Factor Authentication on page 255).

Enforcing Multi-Factor Authentication for Administrators

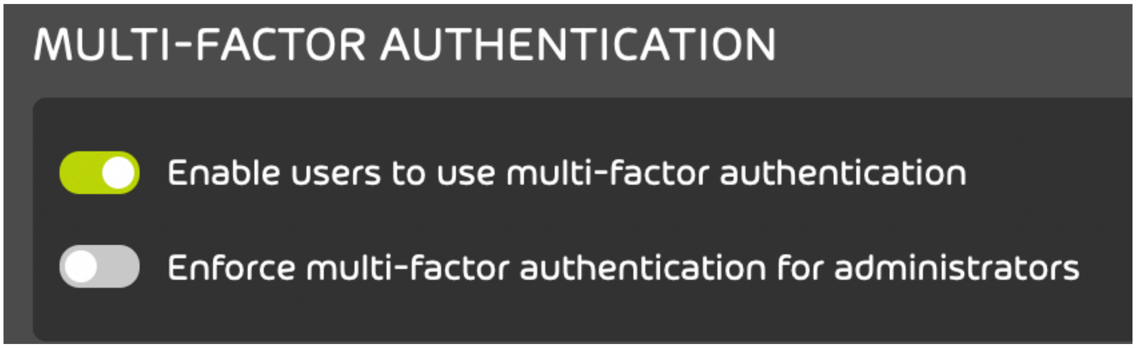
You have enabled multi-factor authentication (see Enabling Multi-Factor Authentication on page 296).

You can enforce multi-factor authentication for a customer's administrators. This forces all administrators of the customer to configure multi-factor authentication for their Control Panel account (see chapter "Configuring Multi-Factor Authentication" in the Control Panel manual).

Notice:

Only users whose passwords are managed in the Control Panel or in a directory service via LDAP can configure multi-factor authentication in the Control Panel.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for whose administrators you would like to enforce multi-factor authentication.
3. Navigate to **Customer Settings** > **Authentication policies & IPs**.
4. Toggle the switch **Enforce multi-factor authentication for administrators** under **Multi-Factor Authentication**.



MULTI-FACTOR AUTHENTICATION

Enable users to use multi-factor authentication

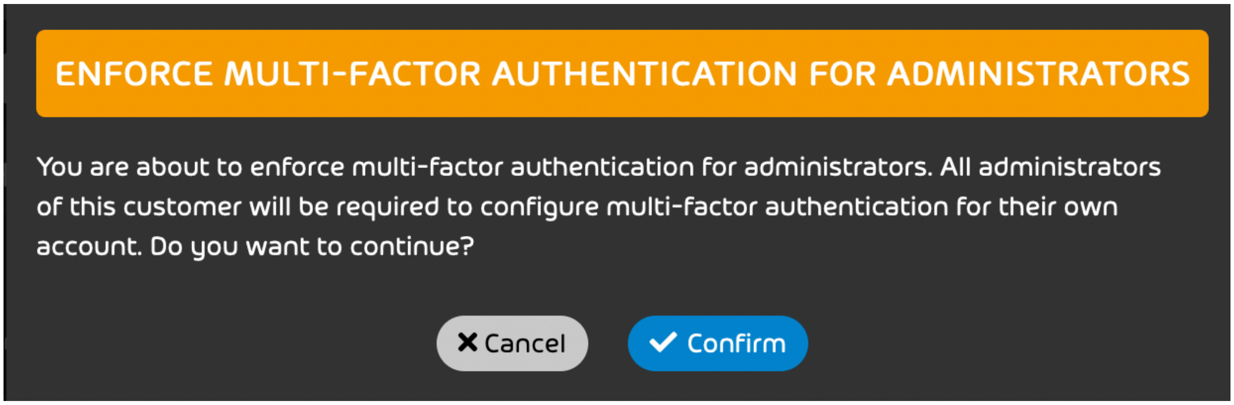
Enforce multi-factor authentication for administrators

Figure 227: Enforce multi-factor authentication for administrators

➔

The switch is highlighted in green. A confirmation window opens.

5. Click on **Confirm**.



ENFORCE MULTI-FACTOR AUTHENTICATION FOR ADMINISTRATORS

You are about to enforce multi-factor authentication for administrators. All administrators of this customer will be required to configure multi-factor authentication for their own account. Do you want to continue?

Figure 228: Confirm

➜

Multi-factor authentication is enforced for all administrators of the customer.

✓

Multi-factor authentication has been enforced for all administrators of a customer.

Once the customer's administrators log in to the Control Panel the next time, they must configure multi-factor authentication for their Control Panel account (see Configuring Multi-Factor Authentication from step 7 on page 28chapter "Configuring Multi-Factor Authentication" from step 7 on page 28 in the Control Panel manual).

Deactivating Multi-Factor Authentication

You have enabled multi-factor authentication for the users of a domain (see Enabling Multi-Factor Authentication on page 296).

You can deactivate multi-factor authentication for the users of a domain. Users are then no longer enabled to configure multi-factor authentication for their Control Panel account. For users who had multi-factor authentication already configured, the configuration is deleted.

Notice:

Only users whose passwords are managed in the Control Panel or in a directory service via LDAP can configure multi-factor authentication in the Control Panel.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for whose users you would like to deactivate multi-factor authentication.
3. Navigate to **Customer Settings** > **Authentication policies & IPs**.
4. Toggle the switch **Enable users to use multi-factor authentication** under **Multi-Factor Authentication**.

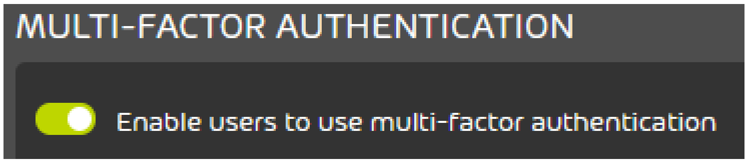
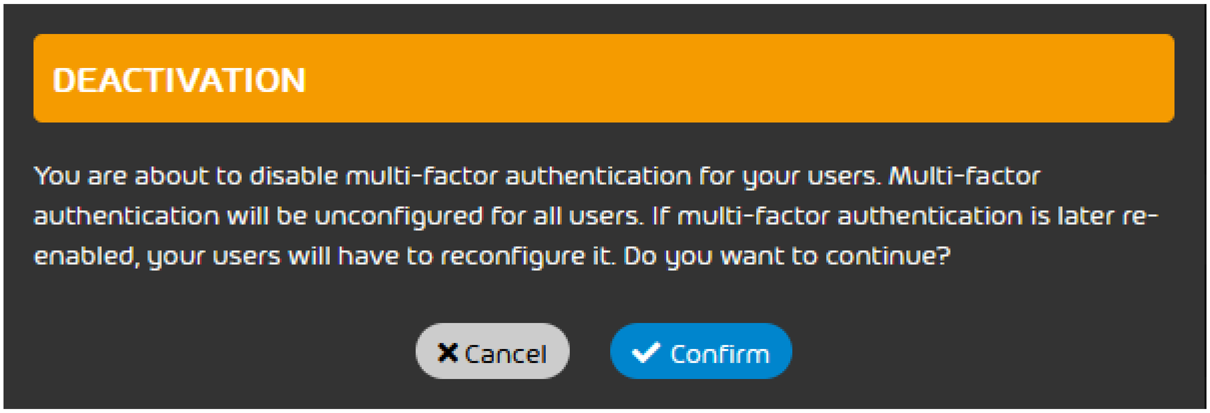

MULTI-FACTOR AUTHENTICATION
Enable users to use multi-factor authentication

Figure 229: Deactivate multi-factor authentication

➜

The switch is grayed out and a confirmation window opens.

5. Click on **Confirm**.



DEACTIVATION

You are about to disable multi-factor authentication for your users. Multi-factor authentication will be unconfigured for all users. If multi-factor authentication is later re-enabled, your users will have to reconfigure it. Do you want to continue?

Figure 230: Confirm

Multi-factor authentication is deactivated for the users of the domain. For users who had multi-factor authentication already configured, the configuration is deleted. From now on, the users must only enter their Control Panel password when they log in to the Control Panel.

> **Notice:**
>
> If multi-factor authentication is later re-enabled for the users of the domain (see Enabling Multi-Factor Authentication on page 296), the users can reconfigure multi-factor authentication (see chapter "Configuring Multi-Factor Authentication" in the Control-Panel manual).

Multi-factor authentication has been deactivated for the users of a domain.

Configuring Auto Logout

For security reasons, inactive users are automatically logged out of the Control Panel.

Notice:

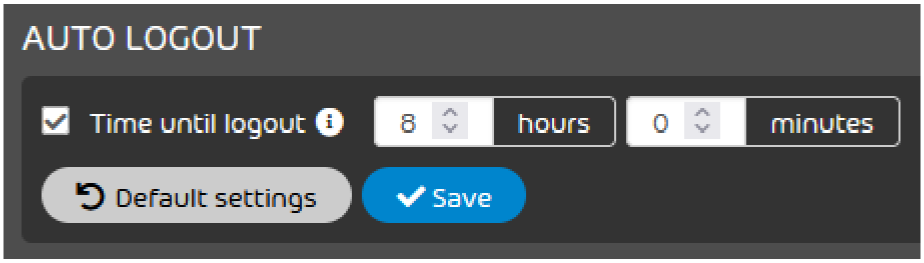
By default, inactive users are automatically logged out of the Control Panel after 24 hours.

In the **Customer Settings** > **Authentication policies & IPs** module (see Authentication Policies and IPs on page 292), you can set a shorter auto logout time or deactivate the auto logout for a customer's users.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to change the auto logout settings.
3. Navigate to **Customer Settings** > **Authentication policies & IPs**.
4. If you would like to set a shorter time until auto logout, set the desired time in the fields **hours** and **minutes** under **Auto logout**.

   Notice:

   The time until auto logout must not exceed 24 hours.

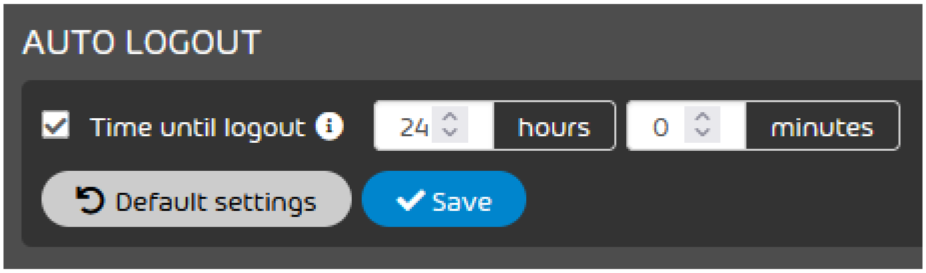


AUTO LOGOUT

☑ Time until logout: 8 hours 0 minutes

Figure 231: Set a time

5. If you would like to deactivate auto logout, untick the **Time until logout** checkbox under **Auto logout**.



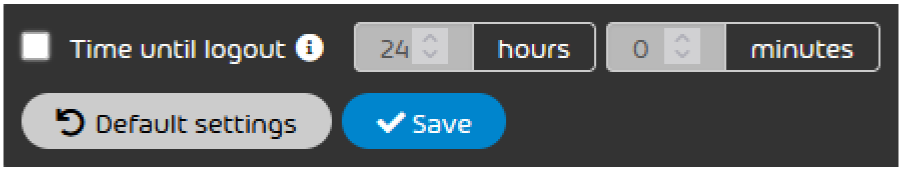
AUTO LOGOUT

☑ Time until logout 24 hours 0 minutes

Figure 232: Deactivate auto logout

➔

The tick is removed and the time settings are grayed out.



□ Time until logout 24 hours 0 minutes

Figure 233: No auto logout

6. Click on **Save**.

➔

The settings are saved. A success message is displayed.

✓

The settings for the auto logout of a customer's users have been edited.

Next, you can reset the auto logout settings to default (see Resetting Auto Logout to Default on page 304).

Resetting Auto Logout to Default

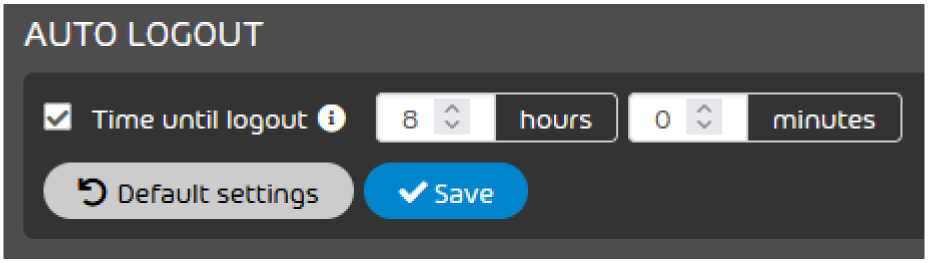
You have changed the settings for the auto logout of a customer's users (see Configuring Auto Logout on page 301).

In the **Customer Settings** > **Authentication policies & IPs** module (see Authentication Policies and IPs on page 292), you can reset the settings for the auto logout of a customer's users to default.

> **Notice:**
>
> By default, inactive users are automatically logged out of the Control Panel after 24 hours.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to reset the auto logout settings to default.
3. Navigate to **Customer Settings** > **Authentication policies & IPs**.

4. Click on **Default settings** under **Auto logout**.

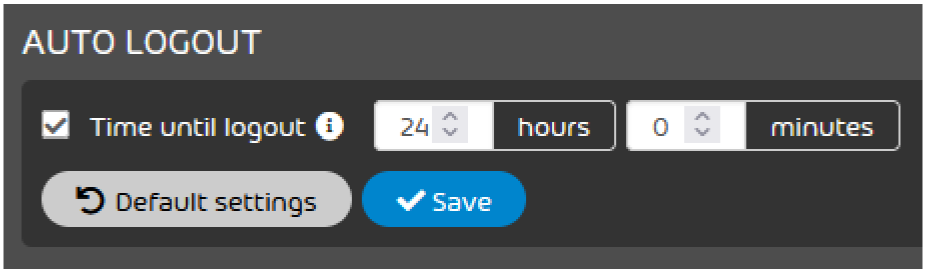


AUTO LOGOUT

☑ Time until logout: 8 hours 0 minutes

Figure 234: Reset to default

The auto logout settings are reset to default. A success message is displayed.



AUTO LOGOUT

☑ Time until logout: 24 hours 0 minutes

Figure 235: Default configuration

The settings for the auto logout of a customer's users have been reset to default.

Assigning an IP Address

In the **Customer Settings** > **Authentication policies & IPs** module, you can allow the Control Panel login for a domain only from selected IP addresses or IP address ranges.

> **Notice:**
>
> If no IP addresses are defined, all IP addresses are allowed to log in to the Control Panel.

1. Log in to the Control Panel with your administrative credentials.
2. Select the desired domain from the scope selection.
3. Navigate to **Customer Settings** > **Authentication policies & IPs**.
4. Click on **Add restriction** under **Allowed IPs for Control Panel Login**.
5. Enter a valid IPv4 address or range of IPv4 addresses and click on **Add**.

For a domain, an IP address or IP address range for the Control Panel login has been added.

Next, you can delete the specified IP address (see Deleting an IP Address on page 306).

Deleting an IP Address

You have limited the Control Panel to certain IPv4 addresses or IPv4 address ranges (see Assigning an IP Address on page 305) login for a domain.

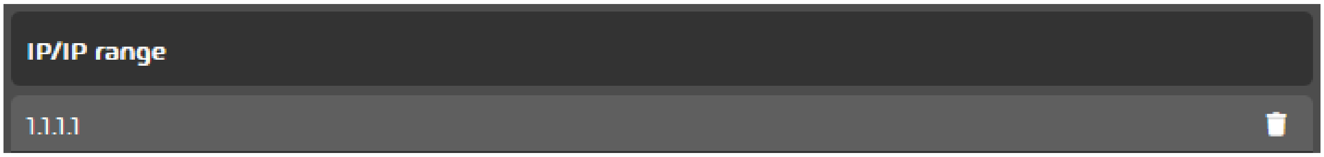
In the **Customer Settings** > **Authentication policies & IPs** module, you can delete specified IP addresses or IP address ranges for a domain so it is no longer possible to log in to the Control Panel from that IP address or IP address range. The Control Panel login is only possible from specified IP addresses and IP address ranges.

Notice:

If no IPv4 addresses are defined, all IPv4 addresses are allowed to log in to the Control Panel.

1. Log in to the Control Panel with your administrative credentials.
2. Select the desired domain from the scope selection.
3. Navigate to **Customer Settings** > **Authentication policies & IPs**.
4. Click on the menu arrow to the right of the IP address or the IP address range to be deleted.
5. Click on **Delete** to delete the IP address or IP address range.

An IP address or an IP address range has been deleted from the list of IP addresses that are allowed for the Control Panel login. If the list still contains other entries, a Control Panel login is no longer possible from the deleted IP address or IP address range. If the list is empty, a Control Panel login is possible from any IP address.



IP/IP range
1.1.1.1

Allow & Deny Lists

About Deny & Allow Lists

The **Deny & Allow Lists** module contains a user's or a customer's deny list and allow list. Each user has their own deny list and allow list, which they can manage themselves. Customer-level administrators can also access their users' personal deny lists and allow lists by selecting the users from the scope selection. Additionally, customer-level administrators can manage a deny list and allow list for their whole domain. The deny list and allow list at domain level shows not only entries that apply to all users of the domain but also entries of individual users of the domain. The deny lists and allow lists are processed in a specific order (see Hierarchy of Deny and Allow List Entries on page 347).

With the deny list, users and customer-level administrators can define that certain incoming emails of a user or of all users of a customer are classified as spam by spam filtering. Emails classified as **Spam** are not directly delivered to the recipient but stored in quarantine. If they wish to do so, recipients can deliver emails classified as **Spam** from quarantine in the **Email Live Tracking** module or from quarantine reports.

Notice:

In the **Email Live Tracking** module (see chapter "Email Live Tracking" in the Control Panel manual), emails are shown even if the senders are on the deny list.

Whether emails from senders on the deny list are displayed in quarantine reports (see chapter "About Quarantine Report" in the Control Panel manual), depends on the quarantine report settings. Users can check in their user settings whether emails from senders on the deny list are excluded from their quarantine reports (see chapter "Configuring Quarantine Reports" in the Control Panel manual). If the administrator allows it, users can change this setting themselves.

With the allow list, users and customer-level administrators can define that spam filtering and/or other filtersare bypassed for certain incoming emails of a user or all users of a domain.

Important:

An allow list at user level only bypasses spam filtering. If a sender is on the allow list, their emails that would usually be classified as **Spam** are delivered to the recipient as **Clean**. However, if an email from a sender on the allow list is classified as **Content**, **Threat**, **AdvThreat** or **Rejected**, it will not be delivered.

For allow list entries at domain level, customer-level administrators can, in contrast, select which filters should be bypassed by an allow list entry. Besides spam filtering, other filters can be selected (see Creating an Allow List Entry for a Domain on page 316). At the level of a domain, customer-level administrators can create allow list entries for an entire domain as well as allow list entries for individual users of a customer.

Users and customer-level administrators can create deny list and allow list entries directly in the **Deny & Allow Lists** module (see Creating a Deny List Entry for a User on page 310 and Creating an Allow List Entry for a User on page 312 for the creation of entries for a user and Creating a Deny List Entry for a Domain on page 314 and Creating an Allow List Entry for a Domain on page 316 for the creation of entries for all users of a domain). Alternatively, users and customer-level administrators can import deny list and allow list entries from a CSV file (see Importing Deny List and Allow List Entries from a CSV File on page 322). The CSV files must follow a certain structure.CSV files for importing deny list and allow list entries at user level or deny list entries at domain level have different structural requirements (see CSV Files for the Import of Deny List and Allow List Entries on page 327) than CSV files for importing allow list entries at domain level (see CSV File for the Import of Allow List Entries for a Domain on page 327).

Notice:

Customer-level administrators can import allow list entries for individual users in addition to allow list entries for a domain using the CSV import at domain level (see CSV File for the Import of Allow List Entries for a Domain on page 327). At this level, allow list entries that bypass filters other than spam filtering can also be imported for individual users (see CSV File for the Import of Allow List Entries for a Domain on page 327).

In order to manage deny list and allow list entries more easily, users and customer-level administrators can export entries from the deny list or allow list as a CSV file (see Exporting Deny List or Allow List Entries as a CSV File on page 343). Furthermore, the deny list and allow list entries in the Control Panel can be searched (see Searching Deny List or Allow List Entries on page 347). Entries that are no longer required, can be removed (see Deleting a Deny List or Allow List Entry on page 345).

Creating a Deny List Entry for a User

In the **Deny & Allow Lists** module (see About Deny & Allow Lists on page 308), you can add email addresses, domains or IPv4 addresses to your deny list or to the deny list of a user of your domain. Incoming emails of the user that originate from these email addresses, domains and IP addresses are classified as spam by spam filtering.

Notice:

Customer-level administrators can also create deny list entries for all users of their domain (see Creating a Deny List Entry for a Domain on page 314).

Notice:

Instead of creating deny list entries individually, users and customer-level administrators can also import a list of deny list entries from a CSV file (see Importing Deny List and Allow List Entries from a CSV File on page 322).

1. Log in to the Control Panel with your administrative credentials.
2. If you would like to create an entry for the deny list of a user of your domain instead of an entry for your own deny list, select the user from the scope selection.

   Notice:

   If no scope is selected in the scope selection, the logged-in user is selected.

3. Navigate to **Deny & Allow Lists**.

4. Select the tab **Deny list**.
5. Click on **Add entry**.

   ➔

   An extended view opens.

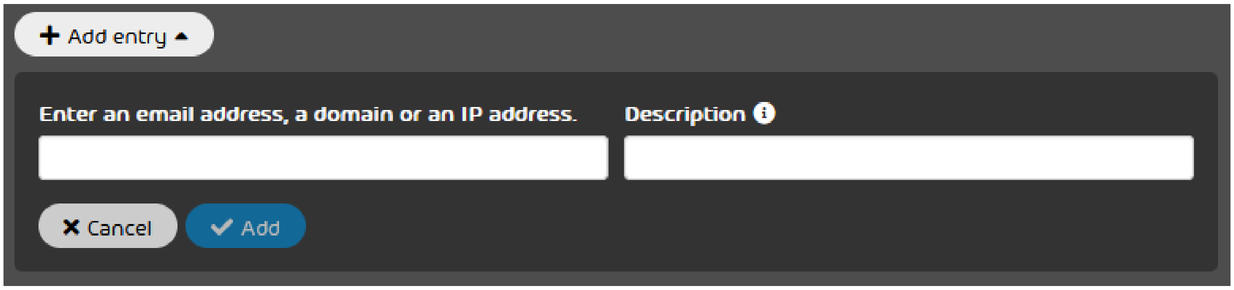


Figure 236: Extended view

6. In the left field, enter the email address, the domain or the IPv4 address whose emails shall be classified as spam by spam filtering.

   Notice:

   Domains must have the syntax **domainname.tld**.

7. Optional: Enter a description of the deny list entry in the field **Description**.

   Notice:

   The description is limited to 100 characters.

8. Click on **Add**.

   ➔

   The entry is created and added to the table of the user's deny list entries.

   Notice:

   The deny list entry is also displayed in the deny list of the user's domain.

A deny list entry has been created for a user.

Next, you can export deny list entries as a CSV file (see Exporting Deny List or Allow List Entries as a CSV File on page 343). If you no longer need a deny list entry, you can delete it (see Deleting a Deny List or Allow List Entry on page 345).

Creating an Allow List Entry for a User

In the **Deny & Allow Lists** module (see About Deny & Allow Lists on page 308), you can add email addresses, domains or IPv4 addresses to your allow list or to the allow list of a user of your domain. Incoming emails of the user that originate from these email addresses, domains and IPv4 addresses bypass spam filtering.

Notice:

Customer-level administrators can additionally create allow list entries for all users of their domain (see Creating a Deny List Entry for a Domain on page 314).

Important:

An allow list at user level only bypasses spam filtering. If a sender is on the allow list, their emails that would usually be classified as **Spam** are delivered to the recipient as **Clean**. However, if an email from a sender on the allow list is classified as **Content**, **Threat**, **AdvThreat** or **Rejected**, it will not be delivered.

For allow list entries at domain level, customer-level administrators can, in contrast, select which filters should be bypassed by an allow list entry. Besides spam filtering, other filters can be selected (see Creating an Allow List Entry for a Domain on page 316). At the level of a domain, customer-level administrators can create allow list entries for an entire domain as well as allow list entries for individual users of a customer.

Notice:

Instead of creating allow list entries individually, users and customer-level administrators can also import a list of allow list entries from a CSV file (see **Importing Deny List and Allow List Entries from a CSV File** on page 322).

1. Log in to the Control Panel with your administrative credentials.
2. If you would like to create an entry for the allow list of a user of your domain instead of an entry for your own allow list, select the user from the scope selection.

   Notice:

   If no scope is selected in the scope selection, the logged-in user is selected.

3. Navigate to **Deny & Allow Lists**.
4. Select the **Allow list** tab.
5. Click on **Add entry**.

➜

An extended view opens.

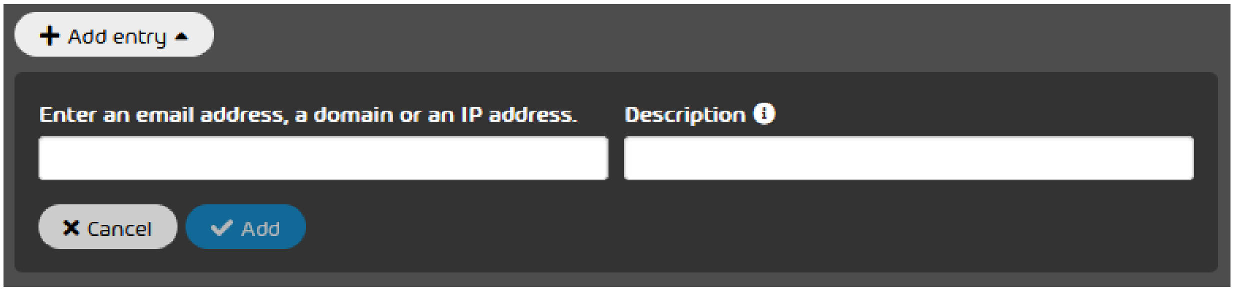


Figure 237: Extended view

6. In the left field, enter the email address, the domain or the IPv4 address whose emails shall not be marked as spam by spam filtering.

> **Notice:**
>
> Domains must have the syntax **domainname.tld**.

7. Optional: Enter a description of the allow list entry in the field **Description**.

> **Notice:**
>
> The description is limited to 100 characters.

8. Click on **Add**.

➜

The entry is created and added to the table of the user's allow list entries.

> **Notice:**
>
> The allow list entry is also displayed in the allow list of the user's domain.

Next, you can export allow list entries as a CSV file (see Exporting Deny List or Allow List Entries as a CSV File on page 343). If you no longer need an allow list entry, you can delete it (see Deleting a Deny List or Allow List Entry on page 345).

Creating a Deny List Entry for a Domain

In the **Deny & Allow Lists** module (see About Deny & Allow Lists on page 308), you can add email addresses, domains or IPv4 addresses to the deny list of your domain. Incoming emails of the users of your domain that originate from these email addresses, domains and IP addresses are classified as spam by spam filtering.

Notice:

Instead of creating deny list entries individually, customer-level administrators can also import a list of deny list entries from a CSV file (see Importing Deny List and Allow List Entries from a CSV File on page 322).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to create a deny list entry.
3. Navigate to **Deny & Allow Lists**.
4. Select the tab **Deny list**.
5. Click on **Add entry**.

➔

An extended view opens.

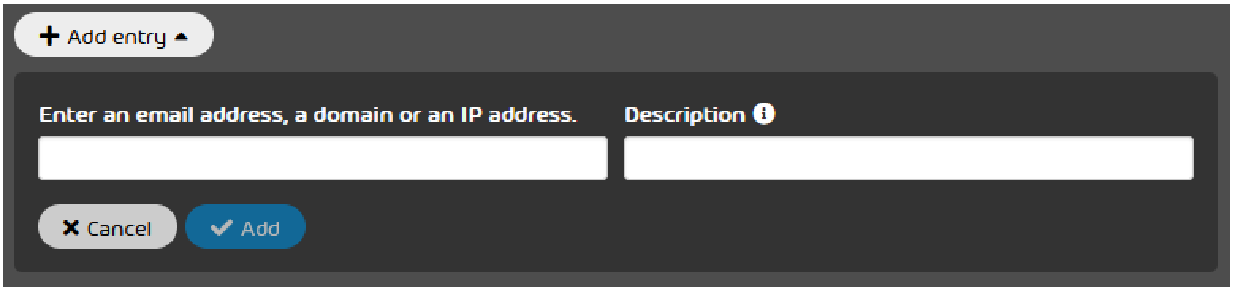


Figure 238: Extended view

6. In the left field, enter the email address, the domain or the IPv4 address whose emails shall be classified as spam by spam filtering.

Notice:

Domains must have the syntax **domainname.tld**.

7. Optional: Enter a description of the deny list entry in the field **Description**.

> **Notice:**
>
> The description is limited to 100 characters.

8. Click on **Add**.

   ➜

   The entry is created and added to the table of deny list entries of the domain.

✓

A deny list entry has been created for a domain.

Next, you can export deny list entries as a CSV file (see Exporting Deny List or Allow List Entries as a CSV File on page 343). If you no longer need a deny list entry, you can delete it (see Deleting a Deny List or Allow List Entry on page 345).

Creating an Allow List Entry for a Domain

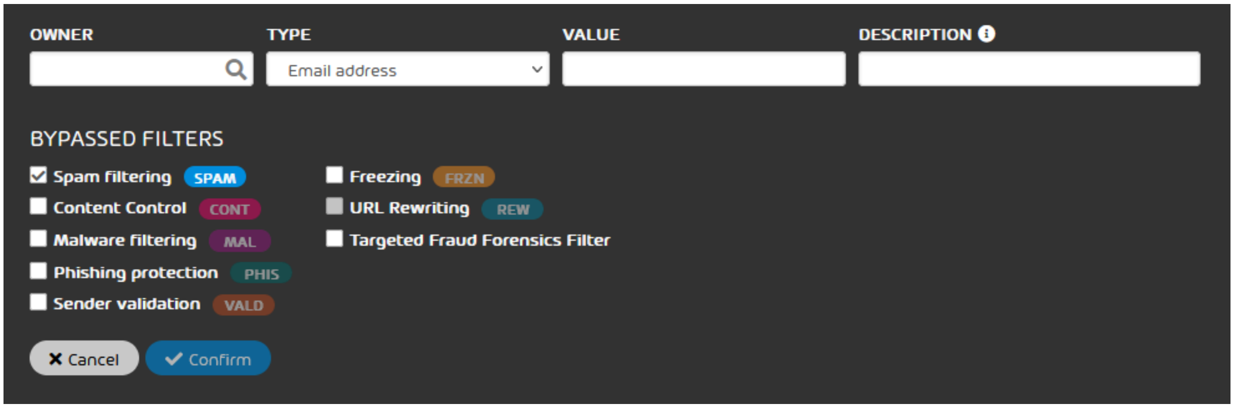
In the **Deny & Allow Lists** module (see About Deny & Allow Lists on page 308), you can create allow list entries at the level of a domain. You can create allow list entries for your domain that apply to all users of the customer, as well as entries for individual users of the customer. The allow list entry defines that certain incoming emails bypass selected filters. Unlike for allow list entries that are created at the level of a user (see Creating an Allow List Entry for a User on page 312), at the level of a domain, you can select which filters an allow list entry bypasses.

> **Notice:**
>
> Instead of creating allow list entries individually, customer-level administrators can also import a list of allow list entries from a CSV file (see Importing Deny List and Allow List Entries from a CSV File on page 322).

1. Log in to the Control Panel with your administrative credentials.

2. From the scope selection, select the domain for which you would like to create an allow list entry.
3. Navigate to **Deny & Allow Lists**.
4. Select the **Allow list** tab.
5. Click on **Add entry**.

An extended view opens.



OWNER:

TYPE: Email address

VALUE:

DESCRIPTION:

BYPASSED FILTERS

☑ Spam filtering SPAM
□ Content Control CONT
□ Malware filtering MAL
□ Phishing protection PHIS
□ Sender validation VALD
□ Freezing FRZN
□ URL Rewriting REW
□ Targeted Fraud Forensics Filter

Figure 239: Extended view

6. Optional: If the allow list entry should only apply only to a specific user of the customer, enter the user's email address in the **Owner** field. To trigger the automatic suggestion function, enter at least three consecutive characters.

> **Notice:**
>
> If the field is left empty, the allow list entry applies to the customer's domain. In this case, the allow list entry applies to all users of the customer.

7. From the drop-down menu **Type**, select which information of an email the allow list entry shall refer to. You have the following options:

   - **Email address**: The allow list entry applies to emails that have been sent from a specific email address.
   - **Domain**: The allow list entry applies to emails that have been sent from an email address of a specific domain.
   - **IP address or range**: The allow list entry applies to emails that have been sent from a specific IPv4 address or from a specific IPv4 range.
   - **URL (only for Secure Links)**: An allow list entry of this type only bypasses the engine URL Rewriting of Advanced Threat Protection (see chapter "Description of the ATP Engines" in the Control Panel manual) This allow list entry prevents URLs in incoming emails that point to a specific domain from being rewritten by the engine URL Rewriting. The allow list entry can also be extended to the subdomains of the domain. Alternatively, it is possible to enter a specific URL instead of a domain. In this case, only links with this URL are not rewritten.

   ➜

   If the option **URL (only for Secure Links)** has been selected, the checkbox **Include subdomains** is displayed under the field **Value**. Furthermore, for this option, the checkbox **Secure Links** under **Bypassed filters** is ticked and all other checkboxes are grayed out. If a different option has been selected, the checkbox **Spam filtering** is ticked.

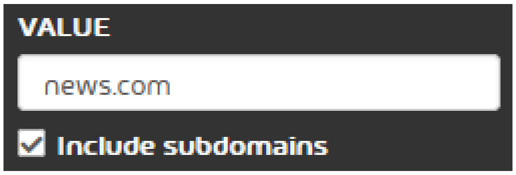
8. In the field **Value**, enter the value of the emails to which the allow list entry shall apply. Depending on the selection in step 7 on page 318, enter one of the following values:

   - **Email address**: the sender's email address
   - **Domain**: the sender's domain
   - **IP address or range**: IPv4 address or IPv4 range from which the email has been sent
   - **URL (only for Secure Links)**: domain of the URL or a specific URL included in the email

   ➜

   The button **Confirm** is enabled.

9. Optional: If you have selected the option **URL (only for Secure Links)** in step 7 on page 318 and the allow list entry shall also apply to URLs with a subdomain of the domain entered in step 8 on page 318, tick the checkbox **Include subdomains**.



VALUE

news.com

☑ Include subdomains

Figure 240: Include subdomains

10. Optional: Enter a description of the allow list entry in the field **Description**.

Notice:

The description is limited to 100 characters.

11. Under **Bypassed filters**, tick the checkboxes of the filters that the allow list entry shall bypass for an email. You have the following options:

    - **Spam filtering**: Spam filtering of Spam and Malware Protection is bypassed. The allow list entry prevents emails from being classified as spam by spam filtering.

      > **Notice:**
      >
      > Except for allow list entries of the type **URL (only for Secure Links)**, this filter is the only one selected by default, which corresponds to the configuration of users' allow list entries (see Creating an Allow List Entry for a User on page 312).

    - **Content Control**: The filter Content Control (see chapter "About Content Control" in the Control Panel manual) of Spam and Malware Protection is bypassed. The allow list entry prevents emails from being classified as **Content**.
    - **Malware filtering**: Malware filtering of Spam and Malware Protection is bypassed. The allow list entry prevents emails that contain malware from being classified as **Threat**.
    - **Phishing protection**: Phishing protection of Spam and Malware Protection is bypassed. The allow list entry prevents phishing emails from being classified as **Threat**.
    - **Sender validation**: The sender validation of Spam and Malware Protection is bypassed. The allow list entry prevents emails that have failed the sender validation from being rejected by our email server.
    - **Freezing**: The engine Freezing (see chapter "Description of the ATP Engines" in the Control Panel manual) of Advanced Threat Protection is bypassed.
    - **Secure Links**: The engine URL Rewriting (see chapter "Description of the ATP Engines" in the Control Panel manual) of Advanced Threat Protection is bypassed.

      > **Notice:**
      >
      > The engine URL Rewriting can only be bypassed for allow list entries of the type **URL (only for Secure Links)** (see step 7 on page 318). The engine URL Rewriting will not be applied to URLs of the entered domain (see step 8 on page 318) in the owner's incoming emails.

- **Targeted Fraud Forensics Filter**: The engine Targeted Fraud Forensics Filter (see chapter 'Description of the ATP Engines' in the Control Panel manual) of Advanced Threat Protection is bypassed for a specific Control Panel user. The engine Targeted Fraud Forensics Filter does not check for certain emails from an external email address whether they appear to have been sent in the name of a specific Control Panel user. For any other Control Panel user, the engine Targeted Fraud Forensics Filter is applied as usual.

  Notice:

  In the following example, it might be useful to bypass the engine Targeted Fraud Forensics Filter for a user: A user of the customer communicates on a regular basis with other employees of the company using a different email address (e.g., their private email address) than the email address under which the user exists in the Control Panel. In order to prevent these emails from being classified as **AdvThreat**, the customer's administrator can create an allow list entry for this alternative email address and bypass the engine Targeted Fraud Forensics Filter for the related user in the Control Panel.

Notice:

The filters are part of services. If one of these services is not activated for the customer, the corresponding filter cannot be activated for the customer either. In this case, a yellow warning triangle is displayed next to the filter, Bypassing the filter has no impact then. However, it is nonetheless possible to select the filter.

➜

12. If you have selected the option **Targeted Fraud Forensics Filter**, enter the email address of the user for whom the engine Targeted Fraud Forensics Filter shall be bypassed in the field **Related Control Panel user**.
13. Click on **Confirm**.

➜

The allow list entry is saved and added to the table of allow list entries.

An allow list entry has been created at the level of a domain.

Next, you can export allow list entries as a CSV file (see Exporting Deny List or Allow List Entries as a CSV File on page 343). If you no longer need an allow list entry, you can delete it (see Deleting a Deny List or Allow List Entry on page 345).

Importing Deny List and Allow List Entries from a CSV File

Instead of creating deny list and allow list entries individually for a user (see Creating a Deny List Entry for a User on page 310 and Creating an Allow List Entry for a User on page 312) or for a domain (see Creating a Deny List Entry for a Domain on page 314 and Creating an Allow List Entry for a Domain on page 316), you can import multiple deny list and allow list entries from a CSV file in the **Deny & Allow Lists** module (see About Deny & Allow Lists on page 308).

1. Log in to the Control Panel with your administrative credentials.
2. If you would like to import entries for the deny list of your domain or for a user of the domain, select the domain or the user from the scope selection.

> **Notice:**
>
> If no scope is selected in the scope selection, the logged-in user is selected.

3. Navigate to **Deny & Allow Lists**.
4. If you would like to import deny list entries, select the tab **Deny list**. If you would like to import allow list entries, select the tab **Allow list**.

5. Click on **Import CSV**.

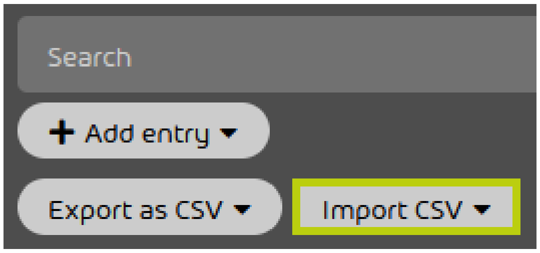


Figure 241: Import CSV file

➔

An extended view opens.

6. Click on **Upload file**.

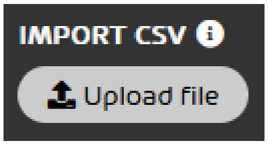


Figure 242: Upload file

7.

Important:

The CSV file must meet structural requirements. The requirements for the import of deny list and allow list entries for a user and for the import of deny list entries for a domain (see CSV Files for the Import of Deny List and Allow List Entries on page 327) are different than those for the import of allow list entries at the level of a domain (see CSV File for the Import of Allow List Entries for a Domain on page 327).

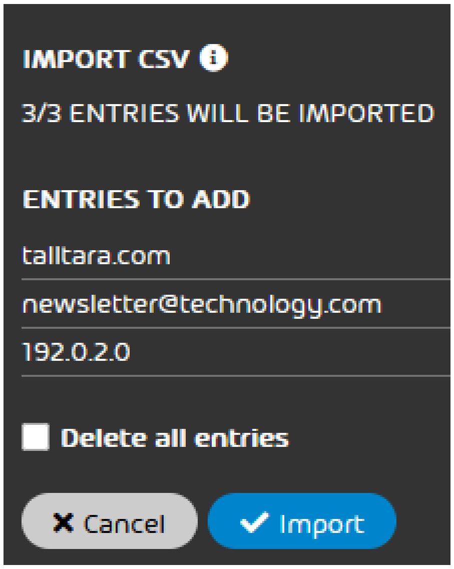
Select the CSV file from your file system and click on **Open**.

➡

It is determined how many valid entries can be imported from the CSV file.

Notice:

If an entry cannot be imported, a warning is displayed for the entry.



IMPORT CSV

3/3 ENTRIES WILL BE IMPORTED

ENTRIES TO ADD

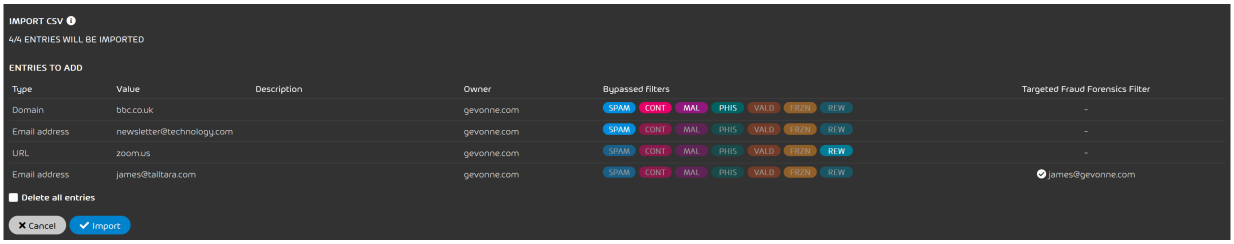
talltara.com

newsletter@technology.com

192.0.2.0

□ Delete all entries

Figure 243: Entries to be added for a user



IMPORT CSV

4/4 ENTRIES WILL BE IMPORTED

ENTRIES TO ADD

Type	Value	Description	Owner	Bypassed filters	Targeted Fraud Forensics Filter
Domain	bbc.co.uk		gevonne.com	SPAM CONT MAL PHIS VALD FRZN REW	-
Email address	newsletter@technology.com		gevonne.com	SPAM CONT MAL PHIS VALD FRZN REW	-
URL	zoom.us		gevonne.com	SPAM CONT MAL PHIS VALD FRZN REW	-
Email address	james@talltara.com		gevonne.com	SPAM CONT MAL PHIS VALD FRZN REW	✓ james@gevonne.com

□ Delete all entries

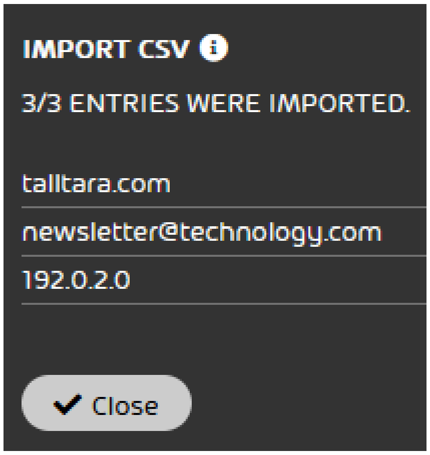
Figure 244: Entries to be added for the allow list of a domain

8. Optional: If you want to remove all existing entries from the deny or allow list in the Control Panel, click on **Delete all entries**.

   Once step 9 on page 326 has been performed, all existing entries from the deny list or allow list are removed and the entries from the CSV file are imported to the deny list or allow list.

9. Click on **Import**.

The entries from the CSV file are imported to the deny list or allow list. Invalid entries and already existing entries will not be imported.



IMPORT CSV

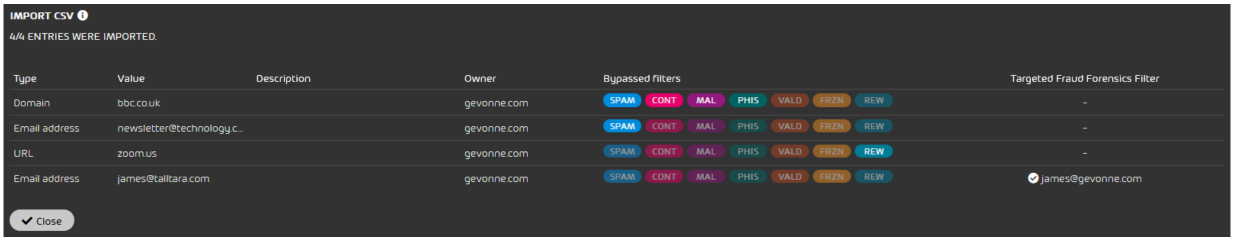
3/3 ENTRIES WERE IMPORTED.

talltara.com

newsletter@technology.com

192.0.2.0

Figure 245: Imported entries for a user



IMPORT CSV

4/4 ENTRIES WERE IMPORTED.

Type	Value	Description	Owner	Bypassed filters	Targeted Fraud Forensics Filter
Domain	bbc.co.uk		gevonne.com	SPAM CONT MAL PHIS VALD FRZN REW	-
Email address	newsletter@technology.c...		gevonne.com	SPAM CONT MAL PHIS VALD FRZN REW	-
URL	zoom.us		gevonne.com	SPAM CONT MAL PHIS VALD FRZN REW	-
Email address	james@talltara.com		gevonne.com	SPAM CONT MAL PHIS VALD FRZN REW	✓ james@gevonne.com

Figure 246: Imported entries for the allow list of a domain

Deny list or allow list entries have been imported from a CSV file.

Next, you can export deny list or allow list entries as a CSV file (see Exporting Deny List or Allow List Entries as a CSV File on page 343). If you no longer need an entry, you can delete it (see Deleting a Deny List or Allow List Entry on page 345).

CSV Files for the Import of Deny List and Allow List Entries

CSV files for the import of deny list and allow list entries (see About Deny & Allow Lists on page 308) must meet structural requirements. The import file must meet the following conditions:

- The extension of the import file is .csv. Other file extensions, such as .txt or .docx, will not be accepted.
- The first row contains the column name **value**.
- The rows below contain domains, email addresses or IPv4 addresses.
- Multiple entries within a row are separated from each other with semicolons.

CSV File for the Import of Allow List Entries for a Domain

CSV files for the import of allow list entries (see About Deny & Allow Lists on page 308) for a domain must meet structural requirements. The import file must meet the following conditions.

Rule for the file extension

- The extension of the import file is .csv. Other file extensions, such as .txt or .docx, will not be accepted.

Rules for columns and rows

- The CSV file contains to 14 columns.
- The columns are separated from each other by a semicolon
- The first row contains the column names (see table Table 19: Columns on page 328).
- From the second row on, each row corresponds to an allow list entry.
- From the second row on, each column contains a value (see table Table 19: Columns on page 328).
- The rows end without any punctuation sign.

Table 19: Columns

NUMBER	COLUMN NAME	VALUE
1	value	This column may contain an email address, a domain, a URL, an IPv4 address or an IPv4 range. The value corresponds to the input in the field **Value** if an allow list entry is created manually (see Creating an Allow List Entry for a Domain on page 316). Which type of value must be entered, depends on the type of the allow list entry, i.e. the value in the column 4**entry_type**. For more information on the possible inputs, see step 8 on page 318 in chapter Creating an Allow List Entry for a Domain on page 316.

NUMBER	COLUMN NAME	VALUE
2	description	This column contains the description of an allow list entry. This column corresponds to the input in the field **Description** if an allow list entry is created manually (see Creating an Allow List Entry for a Domain on page 316). The description is limited to 100 characters. The description is optional. Thus, the column may also be empty.
3	owner	This column contains the owner of the allow list entry. If the allow list entry is to be applied to all users of a customer, the value is the customer's primary domain. However, it is also possible to enter a user of the customer as the owner. If the allow list entry is to be applied to a user of the customer, the value is the user's email address.

NUMBER	COLUMN NAME	VALUE
4	entry_type	This column contains the type of the allow list entry. This column corresponds to the field **Type** if an allow list entry is created manually (see Creating an Allow List Entry for a Domain on page 316). The following values are available: - **EMAIL**: This value corresponds to the option **Email address**. - **DOMAIN**: This value corresponds to the option **Domain**. - **IP**: This value corresponds to the option **IP address or range**. - **URL**: This value corresponds to the option **URL (only for Secure Links)**. For more information on the options, see step 7 on page 318 in chapter Creating an Allow List Entry for a Domain on page 316. **Important:** If this column contains the value **URL**, the allow list entry only bypasses the engine URL Rewriting. Therefore, the column

NUMBER	COLUMN NAME	VALUE
5	spam_protection	The value in this column indicates whether the allow list entry shall bypass spam filtering (see step 11 on page 320 in chapter Creating an Allow List Entry for a Domain on page 316). The column may contain the value **0** or **1**. The value **0** means that spam filtering shall not be bypassed. The value **1** means that spam filtering shall be bypassed. **Important:** If the column 4**entry_type** contains the value **URL**, this filter cannot be bypassed and the value in this column must be **0**.

NUMBER	COLUMN NAME	VALUE
6	content_filter	The value in this column indicates whether the allow list entry shall bypass Content Control (see step 11 on page 320 in chapter Creating an Allow List Entry for a Domain on page 316). The column may contain the value **0** or **1**. The value **0** means that Content Control shall not be bypassed. The value **1** means that Content Control shall be bypassed. **Important:** If the column 4**entry_type** contains the value **URL**, this filter cannot be bypassed and the value in this column must be **0**.

NUMBER	COLUMN NAME	VALUE
7	malware_protection	The value in this column indicates whether the allow list entry shall bypass malware filtering (see step 11 on page 320 in chapter Creating an Allow List Entry for a Domain on page 316). The column may contain the value **0** or **1**. The value **0** means that malware filtering shall not be bypassed. The value **1** means that malware filtering shall be bypassed. ❗ **Important:** If the column 4**entry_type** contains the value **URL**, this filter cannot be bypassed and the value in this column must be **0**.

NUMBER	COLUMN NAME	VALUE
8	phishing_protection	The value in this column indicates whether the allow list entry shall bypass phishing protection (see step 11 on page 320 in chapter Creating an Allow List Entry for a Domain on page 316). The column may contain the value **0** or **1**. The value **0** means that phishing protection shall not be bypassed. The value **1** means that phishing protection shall be bypassed. **Important:** If the column 4**entry_type** contains the value **URL**, this filter cannot be bypassed and the value in this column must be **0**.

NUMBER	COLUMN NAME	VALUE
9	sender_validation	The value in this column indicates whether the allow list entry shall bypass the sender validation (see step 11 on page 320 in chapter Creating an Allow List Entry for a Domain on page 316). The column may contain the value **0** or **1**. The value **0** means that the sender validation shall not be bypassed. The value **1** means that the sender validation shall be bypassed. **Important:** If the column 4**entry_type** contains the value **URL**, this filter cannot be bypassed and the value in this column must be **0**.

NUMBER	COLUMN NAME	VALUE
10	email_freezing	The value in this column indicates whether the allow list entry shall bypass the engine Freezing of Advanced Threat Protection (see step 11 on page 320 in chapter Creating an Allow List Entry for a Domain on page 316). The column may contain the value **0** or **1**. The value **0** means that the engine Freezing shall not be bypassed. The value **1** means that the engine Freezing shall be bypassed. **Important:** If the column 4**entry_type** contains the value **URL**, this filter cannot be bypassed and the value in this column must be **0**.

NUMBER	COLUMN NAME	VALUE
11	atp_url_rewriting	The value in this column indicates whether the allow list entry shall bypass the engine URL Rewriting of Advanced Threat Protection (see step 11 on page 320 in chapter Creating an Allow List Entry for a Domain on page 316). The column may contain the value **0** or **1**. The value **0** means that the engine URL Rewriting shall not be bypassed. The value **1** means that the engine URL Rewriting shall be bypassed. **Important:** If the column entry_type contains the value **URL**, this column must contain the value **1**.

NUMBER	COLUMN NAME	VALUE
12	atp_tfff	The value in this column indicates whether the engine Targeted Fraud Forensics Filter of Advanced Threat Protection shall be bypassed (see step 11 on page 320 in chapter Creating an Allow List Entry for a Domain on page 316). The column may contain the value **0** or **1**. The value **0** means that the engine Targeted Fraud Forensics Filter shall not be bypassed. The value **1** means that the engine Targeted Fraud Forensics Filter shall be bypassed. **Important:** If the column 4**entry_type** contains the value **URL**, this filter cannot be bypassed and the value in this column must be **0**.

NUMBER	COLUMN NAME	VALUE
13	atp_tfff_related_user	**Important:** This column may only contain a value if the engine Targeted Fraud Forensics Filter shall be bypassed, i.e. the column 12**atp_tfff** contains the value **1**. Otherwise, this column must be empty. The value in this column must be the email address of the Control Panel user for whom the engine Targeted Fraud Forensics Filter shall be bypassed. This column corresponds to the input in the field **Related Control Panel user** if an allow list entry is created manually (see Creating an Allow List Entry for a Domain on page 316).

NUMBER	COLUMN NAME	VALUE
14	atp_url_rewriting_include_subdomains	**Important:** This column may only contain the value **1** if the allow list entry refers to a URL for URL Rewriting, i.e. the column **entry_type** contains the value **URL**. The value in this column indicates whether the engine URL Rewriting shall also be bypassed for URLs with a subdomain of the domain entered in the column 1**value**. This column corresponds to the field **Include subdomains** if an allow list entry is created manually (see Creating an Allow List Entry for a Domain on page 316). The column may contain the value **0** or **1**. The value **0** means that the engine URL Rewriting shall not be bypassed for URLs with a subdomain. The value **1** means that the engine URL Rewriting shall also be bypassed for URLs with a subdomain.

Rule for duplicated entries

- Duplicate entries do not affect the processing of the CSV file.

Editing an Allow List Entry for a Domain

You have created (see Creating an Allow List Entry for a Domain on page 316) or imported allow list entries from a CSV file (see Importing Deny List and Allow List Entries from a CSV File on page 322).

In the **Deny & Allow Lists** module (see About Deny & Allow Lists on page 308), you can edit existing allow list entries for a domain. This way, you can, for instance, change the filters that are bypassed by an allow list entry.

Notice:

At domain level, customer-level administrators can also edit existing allow list entries of the users of their domain. Allow list entries that have been created at user level (see Creating an Allow List Entry for a User on page 312) only bypass spam filtering. However, at domain level, customer-level administrators can edit the users' allow list entries in such a way that they bypass other filters than spam filtering. Regardless of the bypassed filters, the entries will still be displayed at user level and can be deleted by the users (see Deleting a Deny List or Allow List Entry on page 345).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to edit an allow list entry.
3. Navigate to **Deny & Allow Lists**.
4. Select the tab **Allow list**.

5. Click on the menu arrow next to the allow list entry that you would like to edit.

Figure 247: Open the menu

➔

A menu opens.

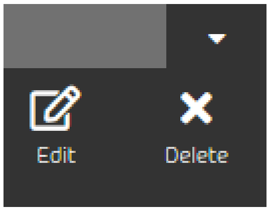
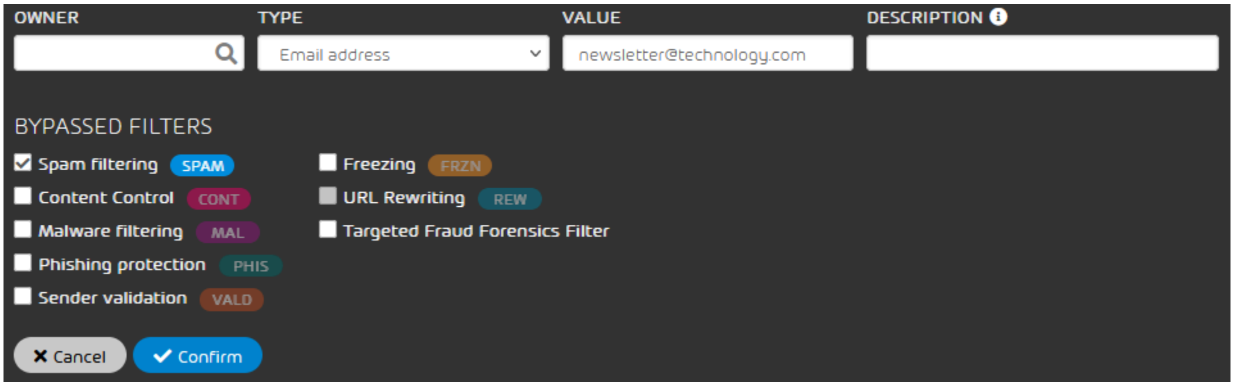


Figure 248: Menu

6. Click on **Edit**.

➔

A form with the settings of the allow list entry opens.



OWNER

TYPE: Email address

VALUE: newsletter@technology.com

DESCRIPTION

BYPASSED FILTERS

☑ Spam filtering SPAM
□ Content Control CONT
□ Malware filtering MAL
□ Phishing protection PHIS
□ Sender validation VALD
□ Freezing FRZN
□ URL Rewriting REW
□ Targeted Fraud Forensics Filter

Figure 249: Settings of the allow list entry

7. Edit the settings as desired (see Creating an Allow List Entry for a Domain on page 316).

8. Click on **Confirm**.

   The changes are saved.

An allow list entry has been edited.

Exporting Deny List or Allow List Entries as a CSV File

You have created deny list or allow list entries (see Creating a Deny List Entry for a User on page 310 and Creating an Allow List Entry for a User on page 312 for the creation of deny list and allow list entries for a user and Creating a Deny List Entry for a Domain on page 314 and Creating an Allow List Entry for a Domain on page 316 for the creation of deny list and allow list entries for a domain) or imported them from a CSV file (see Importing Deny List and Allow List Entries from a CSV File on page 322).

In the **Deny & Allow Lists** module (see About Deny & Allow Lists on page 308), you can export all existing deny list or allow list entries as a CSV file.

1. Log in to the Control Panel with your administrative credentials.
2. If you would like to export the entries from the deny list or the allow list of your domain or of a user of the domain instead of your own entries, select the domain or the user from the scope selection.

   Notice:

   If no scope is selected in the scope selection, the logged-in user is selected.
3. Navigate to **Deny & Allow Lists**.
4. If you would like to export the entries from the deny list, select the tab **Deny list**. If you would like to export the entries from the allow list, select the tab **Allow list**.

5. Click on **Export as CSV**.

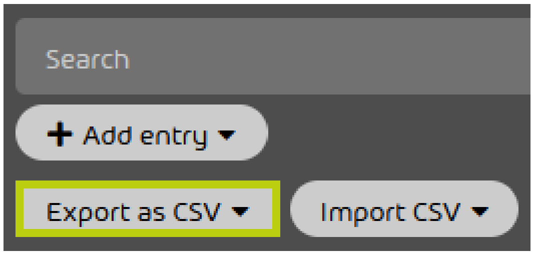


Figure 250: Export the entries as a CSV File

The CSV export settings are displayed.

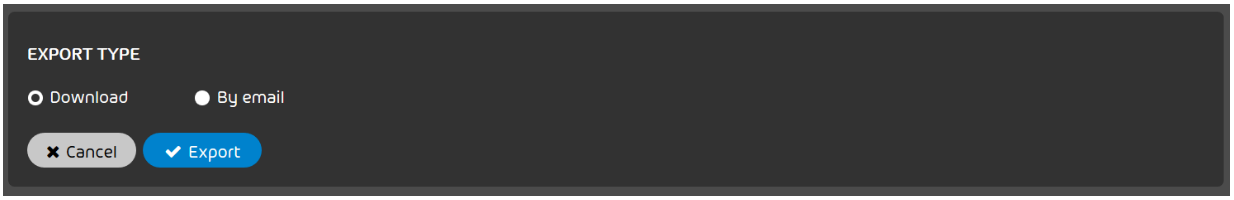


Figure 251: CSV export settings

6. Under **Export type**, select whether the CSV file shall be provided as a download or sent by email.

   - **Download**: The CSV file is provided as download.
   - **By email**: The CSV file is sent by email.

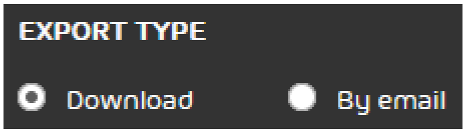


Figure 252: Select export type

If the **By email** option has been selected, an input field is displayed.

7. Optional: If you have selected the **By email** option, enter the email address to which the CSV file should be sent in the input field.
8. Click on **Export**.

   The entries from the deny list or allow list are exported as a CSV file. The CSV file is provided as a download or sent by email.

The entries from the deny list or allow list have been exported as a CSV file.

Deleting a Deny List or Allow List Entry

You have created deny list or allow list entries (see Creating a Deny List Entry for a User on page 310 and Creating an Allow List Entry for a User on page 312 for the creation of deny list and allow list entries for a user and Creating a Deny List Entry for a Domain on page 314 and Creating an Allow List Entry for a Domain on page 316 for the creation of deny list and allow list entries for a domain) or imported them from a CSV file (see Importing Deny List and Allow List Entries from a CSV File on page 322).

If you no longer need a deny list or allow list entry, you can delete the entry in the **Deny & Allow Lists** module (see About Deny & Allow Lists on page 308).

1. Log in to the Control Panel with your administrative credentials.
2. If you would like to delete an entry from the deny list or allow list of your domain or from of a user of your domain, select the domain or the user from the scope selection.

   Notice:

   If no scope is selected in the scope selection, the logged-in user is selected.

3. Navigate to **Deny & Allow Lists**.

4. If you would like to delete a deny list entry, select the tab **Deny list**. If you would like to delete an allow list entry, select the tab **Allow list**.
5. If you would like to delete a user's deny list or allow list entry or the deny list entry of a domain, click on the cross next to the deny list or allow list entry. If you would like to delete the allow list entry of a domain, click on the menu arrow next to the allow list entry.

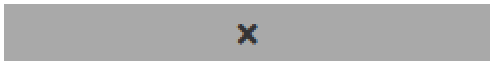


Figure 253: Delete a deny list or allow list entry of a user or a deny list entry of a domain

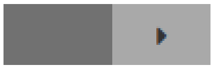


Figure 254: Open the menu for the allow list of a domain

If a user's deny list or allow list entry or a deny list entry of a domain has been selected, the deny list or allow list entry is deleted. If an allow list entry of a domain has been selected, a menu opens.

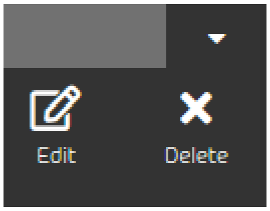


Figure 255: Menu for the allow list of a domain

6. If you would like to delete an allow list entry of a domain, click on **Delete**.

The allow list entry is deleted.

A deny list or allow list entry has been deleted.

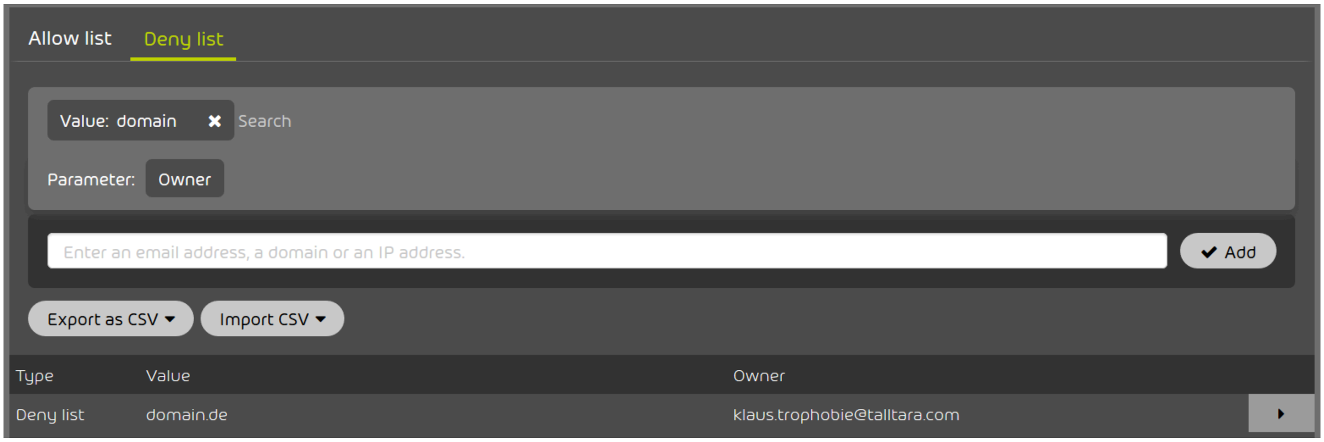
Searching Deny List or Allow List Entries

In the **Deny & Allow Lists** module (see About Deny & Allow Lists on page 308), you can search deny list and allow list entries. The search in the **Deny & Allow Lists** module works in a similar way to the search in the **Email Live Tracking** module (see "Searching Emails" in the Control Panel manual).

Search terms can be entered in the search bar. The entries are filtered dynamically.

Example: Search entries in the deny list and allow list module

The deny list of the user **klaus.trophobie@talltara.com** is searched for the term **test**. Only results starting with **test** are shown.



Value: domain ✖

Parameter: Owner

Type	Value	Owner
Deny list	domain.de	klaus.trophobie@talltara.com

Figure 256: Search the deny list

Hierarchy of Deny and Allow List Entries

Deny list and allow list entries (see About Deny & Allow Lists on page 308) are processed in the following order from the highest to the lowest priority:

- User allow list
- User deny list
- Domain and group allow list

- Domain and group deny list

Notice:

It is no longer possible to create deny list and allow list entries at partner level or for groups. However, such deny and allow lists might still exist for existing customers.

If the system finds a suitable entry on either list, the execution is stopped and the remaining entries are not checked.

Example: Processing hierarchy of deny list and allow list entries

An administrator adds the sender **example@example.com** to the domain deny list. A user adds this sender address to his allow list. All emails from the sender **example@example.com** will be delivered to this user, but no emails will be delivered to any users of the domain who have not added this sender to their allow list.

Security Settings

Security Settings

- Advanced Threat Protection
- Quarantine Report
- Spam and Malware Protection
- Content Control
- Compliance Filter
- Signature and Disclaimer
- Continuity Service

Advanced Threat Protection (ATP)

Structure and Functions of ATP

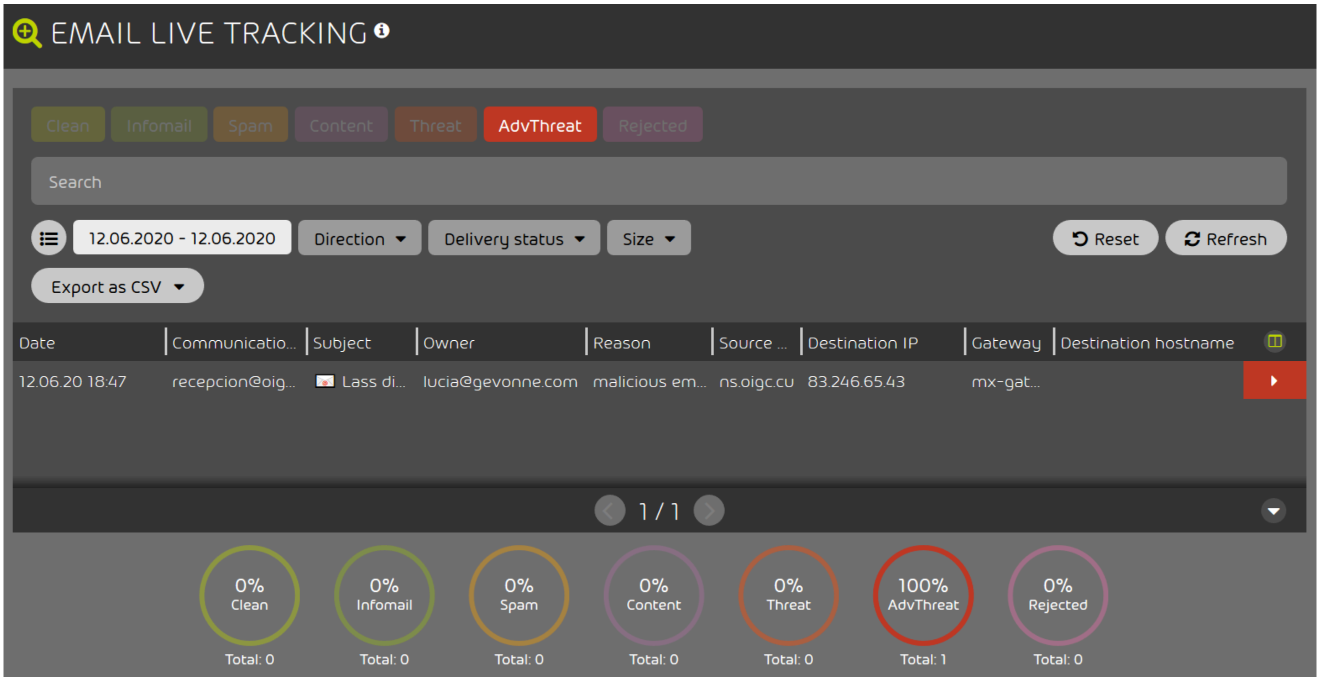
Advanced Threat Protection (ATP) protects against targeted and individual attacks.

Advanced Threat Protection (ATP) protects companies against targeted and individual attacks. Innovative forensic analysis engines ensure that attacks are stopped immediately. At the same time, this solution provides companies with detailed information about the attacks.

ATP consists of the following analysis engines (see Description of the ATP Engines on page 351):

- Sandbox Engine
- URL Rewriting
- URL Scanning
- Freezing
- Targeted Fraud Forensics

Emails intercepted by ATP are categorized as **AdvThreat** and placed in quarantine. Typically, they can be delivered manually by users with administrative rights (see chapter "Roles" in the Control Panel manual).



Date	Communicatio...	Subject	Owner	Reason	Source ...	Destination IP	Gateway	Destination hostname
12.06.20 18:47	recepcion@oig...	Lass di...	lucia@gevonne.com	malicious em...	ns.oigc.cu	83.246.65.43	mx-gat...	

0% Clean	0% Infomail	0% Spam	0% Content	0% Threat	100% AdvThreat	0% Rejected
Total: 0	Total: 0	Total: 0	Total: 0	Total: 0	Total: 1	Total: 0

Figure 257: Category "AdvThreat"

ATP notifies the security officers of companies about security-related events at two points in time:

- Immediately after the arrival of triggering emails with Real-Time Alert (see Real-Time Alert on page 355).
- Immediately after the detection of new threats in already delivered emails with Ex Post Alert (see Ex Post Alert on page 355).

The following chart shows the role of ATP in the processing of emails by our infrastructure.

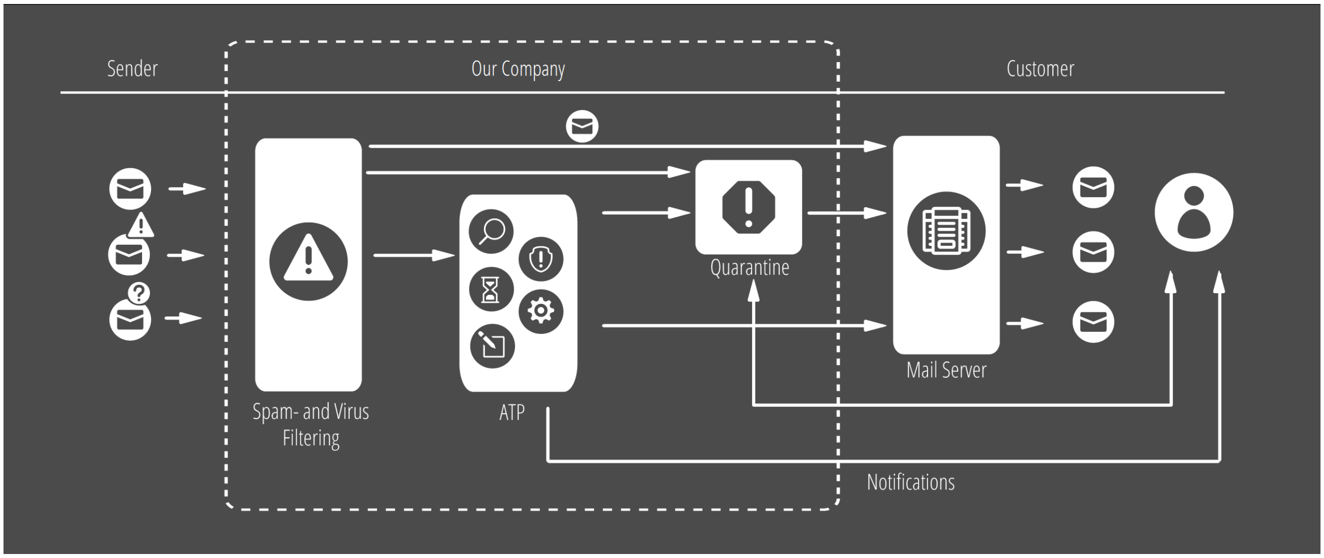


Figure 258: Operating principle of ATP

In addition to the automatic analysis of emails, both upon their arrival and subsequently with Ex Post Alert, ATP offers the possibility of performing manual analyses of emails with executable attachments. With the so-called ATP scans (see ATP Scan on page 369), the user does not only increase security, but also obtains detailed information about the affected emails through the ATP reports (see ATP Report on page 75).

In order for a customer to be able to use Advanced Threat Protection, an administrator must activate the service (see Activating ATP on page 356). After that, the recipients of notifications from Real-Time Alert and Ex Post Alert can be managed (see Adding a Recipient of Alerts on page 358 and Removing Recipients of Alerts on page 360). The engines URL Rewriting and Targeted Fraud Forensics Filter must be activated separately (seeActivating URL Rewriting on page 363 and Activating the Targeted Fraud Forensics Filter on page 364). Furthermore, administrators can define to which user groups the Targeted Fraud Forensics Filter shall be applied (see Adding a Group to the TFFF Group List on page 366 and Removing a Group from the TFFF Group List on page 368).

Description of the ATP Engines

Advanced Threat Protection uses a number of engines to detect and fend off attacks.

Table 20: ATP engines

ATP ENGINES	OPERATING PRINCIPLE AND ADVANTAGES
Sandbox Engine	Attachments are executed in a variety of system environments and their behavior is analyzed. If they turn out to be malware, you are notified. It protects against ransomware and blended attacks.
URL Rewriting	URL Rewriting prevents users from being directed to malicious websites by links in emails. If URL Rewriting is enabled for a customer, links in the users' incoming emails are rewritten as soon as the emails reach our infrastructure. The rewrite allows URL Rewriting to check the website subsequently. When a user clicks on a rewritten link in an email, URL Rewriting checks the website against our domain and URL intelligence databases. These databases contain billions of phishing and malware records and are continuously expanded. If the website passes the first check, URL Rewriting analyzes it for other indicators that it may pose a threat. These include embedded links to malware or phishing forms. Only if the website passes both checks, the user will be redirected to the website. This engine must be activated separately (see Activating URL Rewriting on page 363).

ATP ENGINES	OPERATING PRINCIPLE AND ADVANTAGES
URL Scanning	A document (e. g., PDF, Microsoft) attached to an email may contain links. However, the links cannot be replaced as this would damage the integrity of the document. The URL Scanning engine leaves the document in its original form and only checks the target of such links.
QR Code Analyzer	Images (e. g., PGN, JPEG, GIF and BMP) attached to an email may contain QR codes. The QR Code Analyzer checks the targets of QR codes and blocks an email if its QR code leads to a dangerous web page.
Freezing	Emails which cannot be immediately and conclusively assigned to a category but look suspicious are retained for a short period by Freezing. An additional scan with updated signatures is performed later. It protects against ransomware, blended attacks, and phishing attacks.

ATP ENGINES	OPERATING PRINCIPLE AND ADVANTAGES
Targeted Fraud Forensics Filter	The Targeted Fraud Forensics Filter detects targeted personalized attacks carried out without malware or links. It uses the following detection mechanisms: • Intention Recognition System: It alerts on content patterns that might hint at malicious intent. • Fraud Attempt Analysis: It checks the authenticity and integrity of metadata and email contents. • Identity Spoofing Recognition: Detection and blocking of forged sender identities. • Spy-Out Detection: Protects against attacks trying to obtain sensitive information. • Feign Facts Identification: Content analysis of messages based on provision of feigned facts. • Targeted Attack Detection: Detection of targeted attacks on individuals. This engine must be activated separately (see Activating the Targeted Fraud Forensics Filter on page 364). The Targeted Fraud Forensics Filter is applied to selected user groups that are managed in a group list (see Adding a Group to the TFFF Group List on page 366 and Removing a Group from the TFFF Group List on page 368).

Real-Time Alert

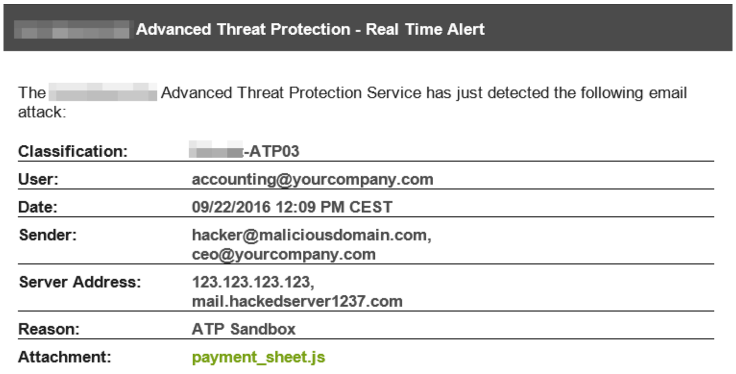
Real-Time Alert is a notification function of Advanced Threat Protection that informs about the reason why emails have been intercepted.

Once Advanced Threat Protection detects an attack, Real-Time Alert sends a notification about a possible threat to the customer's company. The person in charge receives information on the type of the attack, its target, the sender and the reason why the email was intercepted.

Notifications are sent in the following cases:

- The Sandbox Engine has found malicious code (see Sandbox Engine).
- URL Rewriting has blocked a website or a download (see URL Rewriting).
- URL Scanning has found a malicious URL (see URL Scanning).
- The Targeted Fraud Forensics Filter has filtered out emails (see Targeted Fraud Forensics Filter).

Recipients of notifications can be added (see Adding a Recipient of Alerts on page 358) or removed (see Removing Recipients of Alerts on page 360) under **Security Settings** > **Advanced Threat Protection**.



[redacted] Advanced Threat Protection - Real Time Alert

The [redacted] Advanced Threat Protection Service has just detected the following email attack:

Classification:	[redacted]-ATP03
User:	accounting@yourcompany.com
Date:	09/22/2016 12:09 PM CEST
Sender:	hacker@maliciousdomain.com, ceo@yourcompany.com
Server Address:	123.123.123.123, mail.hackedserver1237.com
Reason:	ATP Sandbox
Attachment:	payment_sheet.js

Figure 259: Real-Time Alert

Ex Post Alert

With Ex Post Alert, IT security teams receive notifications if already delivered emails are classified as malicious at a later point.

Recipients of Ex Post Alert will receive a detailed evaluation of the attack so they can immediately initiate actions such as checking their systems or raising the awareness of their own employees.

Recipients of notifications can be added (see Adding a Recipient of Alerts on page 358) or removed (see Removing Recipients of Alerts on page 360) under **Security Settings** > **Advanced Threat Protection**.

Notice:

Once Advanced Threat Protection is activated, Ex Post Alert is activated for all mailboxes of the customer.

Basic configuration

Activating ATP

You have activated Spam and Malware Protection.

You can activate Advanced Threat Protection to protect your company in real time against targeted and individual cyberattacks.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to activate Advanced Threat Protection.
3. Navigate to **Security Settings** > **Advanced Threat Protection**.
4. Toggle the switch **Activate Advanced Threat Protection**.

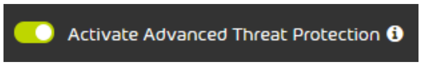


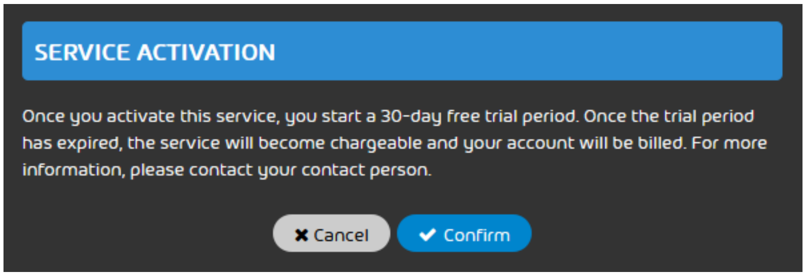
Figure 260: Activate Advanced Threat Protection

A confirmation window is displayed.

5. **Attention:**

   Once Advanced Threat Protection is activated, a 30-day free trial period starts. Once the trial period has expired, the service becomes chargeable and your account is billed.

   Click on **Confirm**.



SERVICE ACTIVATION

Once you activate this service, you start a 30-day free trial period. Once the trial period has expired, the service will become chargeable and your account will be billed. For more information, please contact your contact person.

Figure 261: Confirm

✓

Advanced Threat Protection has been activated for the domain.

Important:

By activating Advanced Threat Protection, you activate all ATP engines (see Description of the ATP Engines on page 351) except URL Rewriting and the Targeted Fraud Forensics Filter for the domain. URL Rewriting and the Targeted Fraud Forensics Filter must be activated separately.

Next, you can manage the recipients of notifications from Advanced Threat Protection (see Adding a Recipient of Alerts on page 358 and Removing Recipients of Alerts on page 360). Furthermore, you can activate the engines URL Rewriting and Targeted Fraud Forensics Filter (see Activating URL Rewriting on page 363 and Activating the Targeted Fraud Forensics Filter on page 364).

Adding a Recipient of Alerts

You have activated Advanced Threat Protection (see Activating ATP on page 356).

In the **Security Settings** > **Advanced Threat Protection** module, you can add email addresses of users who shall receive notifications from Real-Time Alert (see Real-Time Alert on page 355) and Ex Post Alert (see Ex Post Alert on page 355).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to add recipients of alerts.
3. Navigate to **Security Settings** > **Advanced Threat Protection**.
4. Click on **Add recipient**.

Notice:

It is strongly recommended that you register the security officers of your company as recipients.

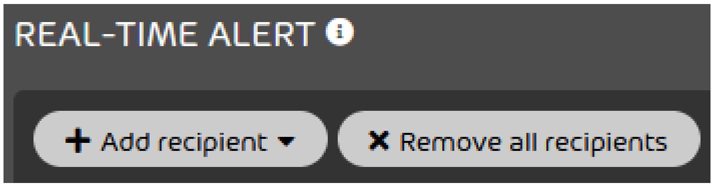
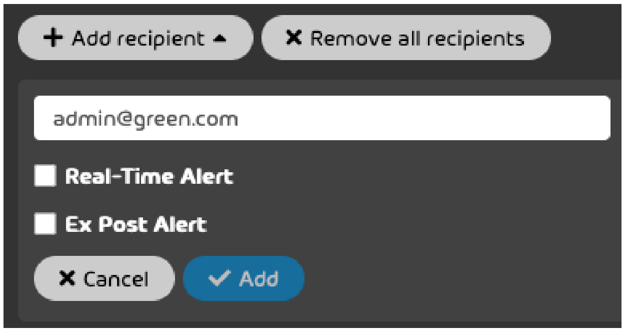


Figure 262: Add recipient

An extended view opens.

5. Enter the desired email address in the input field.



admin@green.com

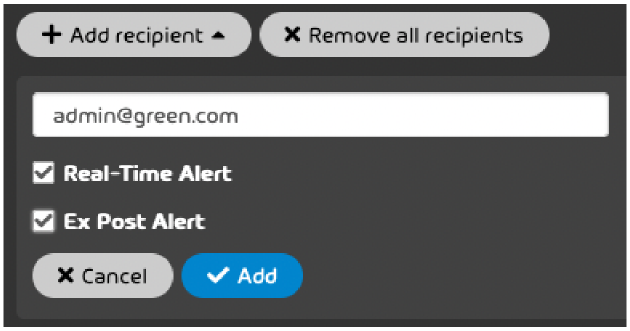
☐ Real-Time Alert

☐ Ex Post Alert

Figure 263: Enter an email address

6. Tick the checkboxes of the notification types that the recipient shall receive. You have the following options.

   - **Real-Time Alert** (see Real-Time Alert on page 355)
   - **Ex Post Alert** (see Ex Post Alert on page 355)



admin@green.com

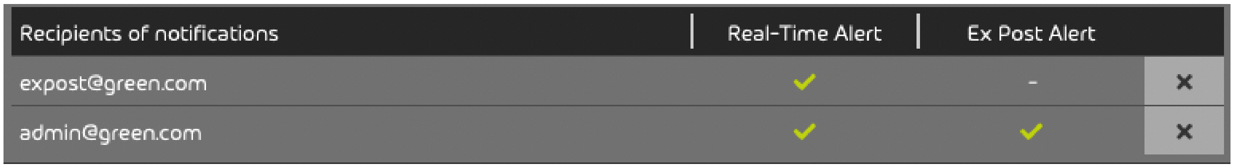
☑ Real-Time Alert

☑ Ex Post Alert

Figure 264: Select notification types

7. Click on **Add**.

The email address is added to the list **Recipients of notifications**. Checkmarks in the columns **Ex Post Alert** and **Real-Time Alert** indicate that the recipient receives notifications of this type.



Recipients of notifications	Real-Time Alert	Ex Post Alert	
expost@green.com	✓	-	✕
admin@green.com	✓	✓	✕

Figure 265: Added recipient

An email address for notifications from Real-Time Alert and/or Ex Post Alert has been added.

Removing Recipients of Alerts

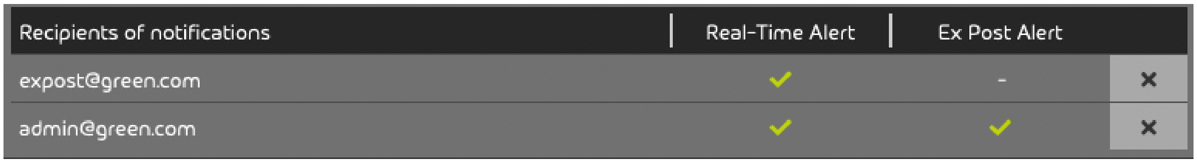
You have activated Advanced Threat Protection (see Activating ATP on page 356) and added alert recipients (see Adding a Recipient of Alerts on page 358).

In the **Security Settings** > **Advanced Threat Protection** module, you can remove email addresses from the recipient list for alerts from Advanced Threat Protection (see Structure and Functions of ATP on page 349). You can either delete individual email addresses or delete all email addresses at once.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to remove a recipient of alerts from Advanced Threat Protection.
3. Navigate to **Security Settings** > **Advanced Threat Protection**.

4. To remove a single recipient, follow these steps:

   a) From the **Recipients of notifications** list, select the email address that you would like to remove.



Recipients of notifications	Real-Time Alert	Ex Post Alert	
expost@green.com	✓	-	✕
admin@green.com	✓	✓	✕

Figure 266: Select an email address

   b) Click on the cross in the row of the email address that you would like to remove.

➜

The email address is removed from the list.

5. To remove all recipients at once, follow these steps:

   a) Click on **Remove all recipients**.

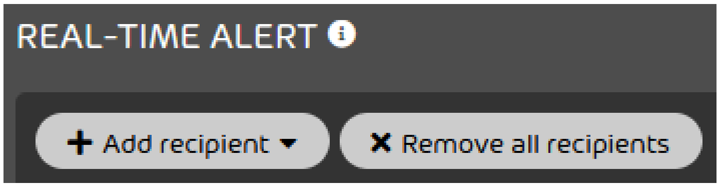
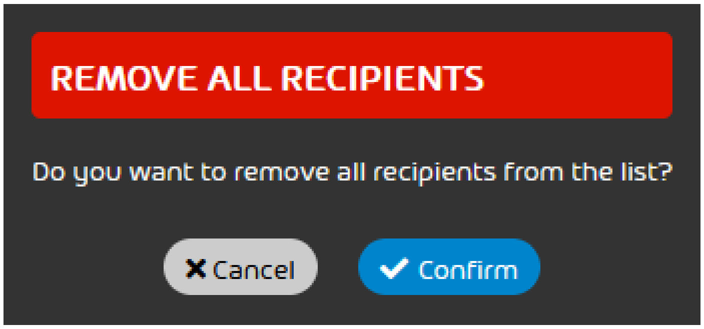


Figure 267: Remove all recipients

A confirmation window opens.

   b) Click on **Confirm**.


REMOVE ALL RECIPIENTS

Do you want to remove all recipients from the list?

Figure 268: Confirm

All email addresses are removed from the list.

Individual or all email addresses have been removed from the recipient list for alerts from Advanced Threat Protection.

Activating URL Rewriting

You have activated Advanced Threat Protection (see Activating ATP on page 356).

In the **Security Settings** > **Advanced Threat Protection** module, you can activate the ATP engine URL Rewriting (see Description of the ATP Engines on page 351). URL Rewriting is activated by default for all users of your primary domain and alias domains.

Notice:

If URL Rewriting shall not be applied to individual users of a domain, those exceptions must be communicated to Support.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to activate URL Rewriting.
3. Navigate to **Security Settings** > **Advanced Threat Protection** in the Control Panel.
4. Toggle the switch **Activate Secure Links** under **SECURE LINKS**.

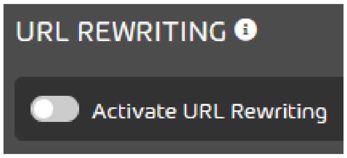


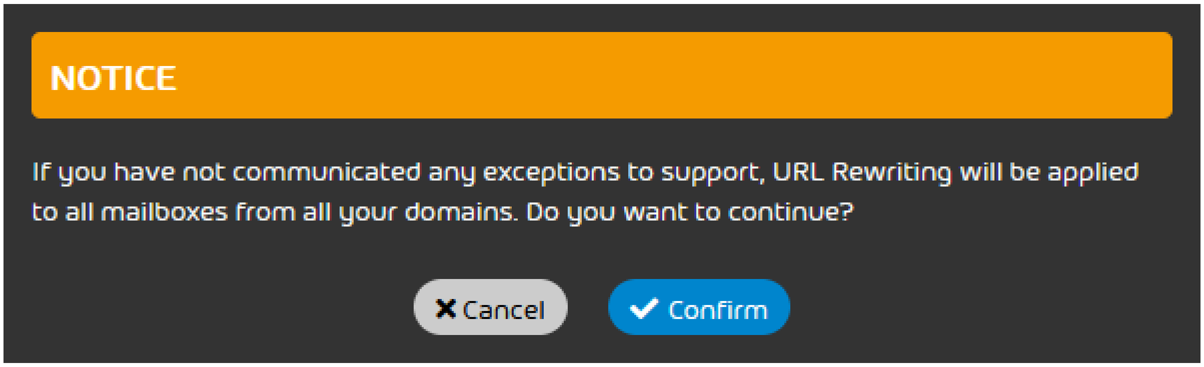
Figure 269: Activate URL Rewriting

The button turns green and a confirmation window opens.

Notice:

URL Rewriting is activated by default for all mailboxes of your primary domain and alias domains. If you do not want to activate URL Rewriting for all domains, please contact Support before the activation and let them know which domains you want to exclude from the activation.

5. Click on **Confirm**.



NOTICE

If you have not communicated any exceptions to support, URL Rewriting will be applied to all mailboxes from all your domains. Do you want to continue?

Figure 270: Confirm

✓

URL Rewriting has been activated for all mailboxes of your primary domain and alias domains that have not been defined as exceptions.

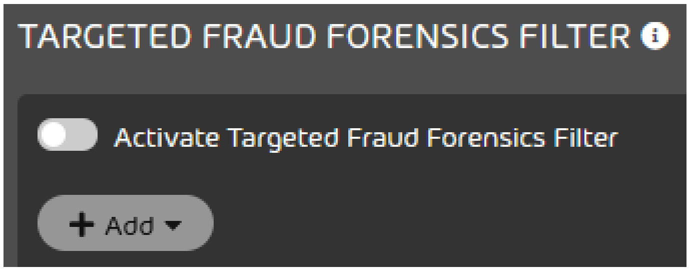
Activating the Targeted Fraud Forensics Filter

You have activated Advanced Threat Protection (see Activating ATP on page 356) and created user groups (see chapter "Groups" in the Control Panel manual). You have activated the SPF check (see chapter "Activating the SPF Check" in the Control Panel manual).

In the **Security Settings** > **Advanced Threat Protection** module, you can activate the ATP engine Targeted Fraud Forensics Filter (see Description of the ATP Engines on page 351) for selected user groups.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to activate the Targeted Fraud Forensics Filter.
3. Navigate to **Security Settings** > **Advanced Threat Protection** in the Control Panel.

4. Toggle the switch **Activate Targeted Fraud Forensics Filter** under **TARGETED FRAUD FORENSICS FILTER**.



TARGETED FRAUD FORENSICS FILTER

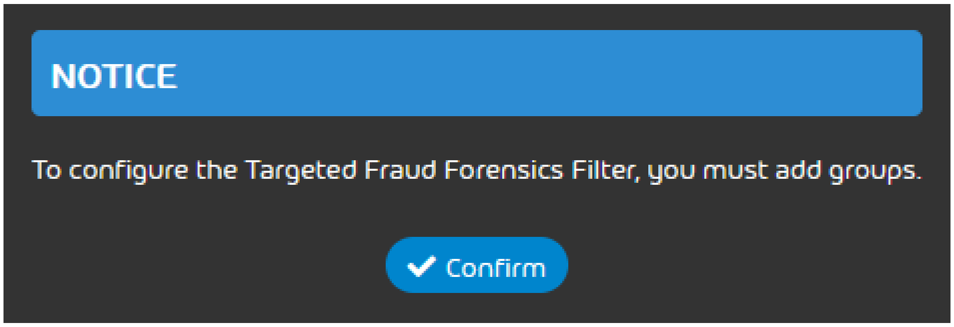
Activate Targeted Fraud Forensics Filter

Figure 271: Activate the Targeted Fraud Forensics Filter

➔

The switch is highlighted in green. The Targeted Fraud Forensics Filter is activated but not yet applied to any user groups. The **Add** button is enabled and a message is displayed.

5. Click on **Confirm**.



NOTICE

To configure the Targeted Fraud Forensics Filter, you must add groups.

Figure 272: Confirm

6. Add the desired user groups to the group list (see Adding a Group to the TFFF Group List on page 366).

➔

The Targeted Fraud Forensics Filter is applied to all added user groups.

✓

The ATP engine Targeted Fraud Forensics Filter has been activated.

Next, you can add groups to the Targeted Fraud Forensics Filter (see Adding a Group to the TFFF Group List on page 366) or remove them from the Targeted Fraud Forensics Filter (see Removing a Group from the TFFF Group List on page 368).

Adding a Group to the TFFF Group List

You have activated the Targeted Fraud Forensics Filter (see Activating the Targeted Fraud Forensics Filter on page 364) and created user groups (see chapter "Groups" in the Control Panel manual).

The Targeted Fraud Forensics Filter is not applied to domains but to user groups. To apply the Targeted Fraud Forensics Filter to a group, you must add the group to the Targeted Fraud Forensics Filter group list.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to add a group to the Targeted Fraud Forensics Filter.
3. Navigate to **Security Settings** > **Advanced Threat Protection** in the Control Panel.

4. In the **TARGETED FRAUD FORENSICS FILTER** area, click on **Add**.

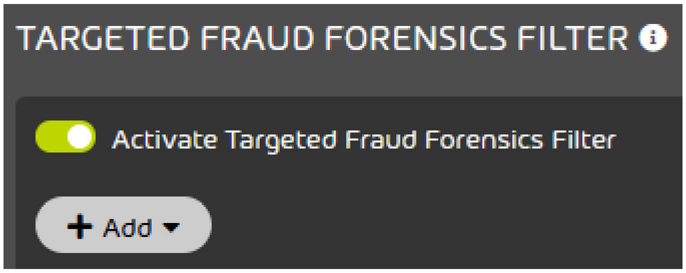

TARGETED FRAUD FORENSICS FILTER
Activate Targeted Fraud Forensics Filter
+ Add

Figure 273: Add a group

➜

An extended view opens.

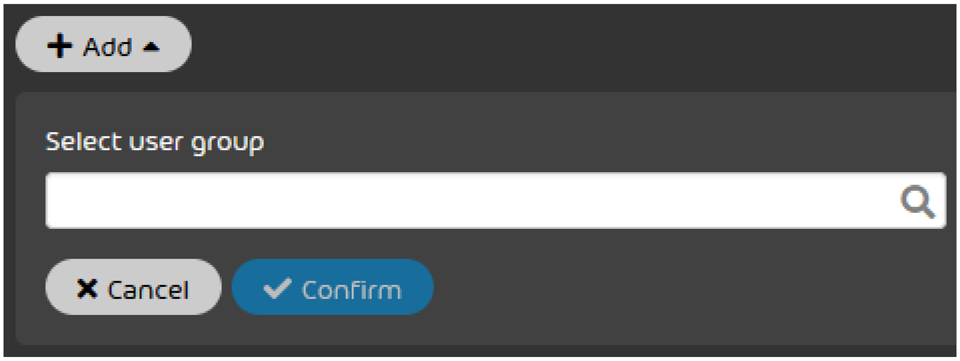


Figure 274: Extended view

5. Enter the name of the desired group in the search field.

➜

A drop-down menu with the search results opens.

6. Select the user group.

7. Click on **Confirm**.

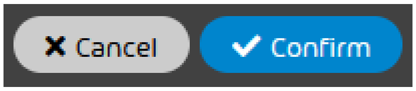


Figure 275: Confirm

The group is added to the group list. From now on, the Targeted Fraud Forensics Filter is applied to all mailboxes of this group.

A group has been added to the group list of the Targeted Fraud Forensics Filter.

Next, you can remove the group from the group list of the Targeted Fraud Forensics Filter (see Removing a Group from the TFFF Group List on page 368).

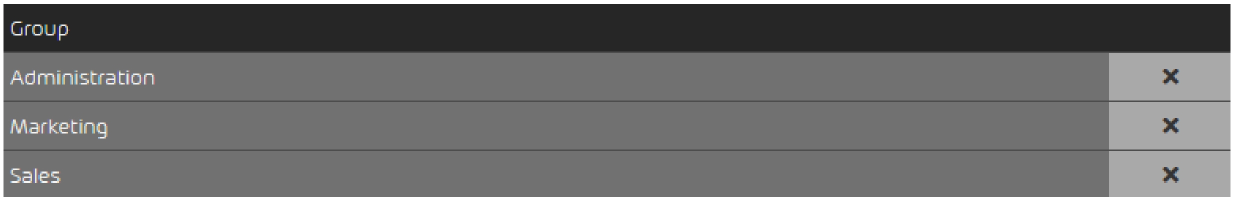
Removing a Group from the TFFF Group List

You have activated the Targeted Fraud Forensics Filter (see Activating ATP on page 356) and added user groups to the group list (see Adding a Group to the TFFF Group List on page 366).

The Targeted Fraud Forensics Filter is applied to user groups. To stop applying the Targeted Fraud Forensics Filter to a group, you must remove the group from the Targeted Fraud Forensics Filter group list.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to remove a group from the Targeted Fraud Forensics Filter.
3. Navigate to **Security Settings** > **Advanced Threat Protection**.

4. Select the desired user group from the group list in the section **TARGETED FRAUD FORENSICS FILTER**.



Group	
Administration	×
Marketing	×
Sales	×

Figure 276: Select a group

5. Click on the cross next to the group that you would like to remove.

   The group is removed from the group list. From now on, the Targeted Fraud Forensics Filter is no longer applied to the mailboxes of this group.

A group has been removed from the group list of the Targeted Fraud Forensics Filter.

ATP Scan

With the ATP scan, administrators can perform an additional analysis of emails. The ATP scan is triggered manually (see **Initiating an ATP Scan** on page 74) and analyzes emails with executable attachments for malicious content. The selected email is analyzed with the Sandbox Engine, and a detailed report is generated for the email: the ATP report (see **ATP Report** on page 75).

Customers who have not booked ATP can also run the ATP scan. For these customers, however, the monthly number of analyses is limited.

Since emails from ATP customers are already automatically analyzed with the Sandbox Engine (see **Description of the ATP Engines** on page 351), for ATP customers, the ATP scan is mainly an additional security measure (for example, before manual delivery of emails categorized as **AdvThreat**). On top of that, ATP customers receive additional information with the ATP report.

Initiating an ATP Scan

You have activated Advanced Threat Protection (see Activating ATP on page 356).

With the ATP scan (see chapter "ATP Scan" in the Control Panel manual), you can manually check emails with executable attachments for malicious content in the **Email Live Tracking** module (see chapter "Email Live Tracking" in the Control Panel manual).

Notice:

The ATP scan can only be applied to emails with executable attachments (e.g., .exe files).

Attention:

If you have not booked Advanced Threat Protection (see chapter "Structure and Functions of ATP" in the Control Panel manual), you can perform two ATP scans per month for free. You can only perform further ATP scans, if you have booked ATP.

1. Log in to the Control Panel with your credentials.
2. If you would like to view the emails of a domain instead of your own emails, select the domain from the scope selection.
3. Navigate to the **Email Live Tracking** module.
4. Click on the arrow symbol to the right of the desired email.

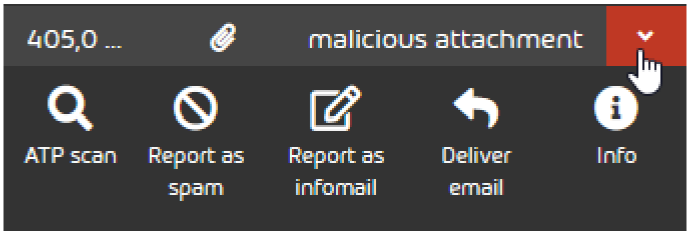
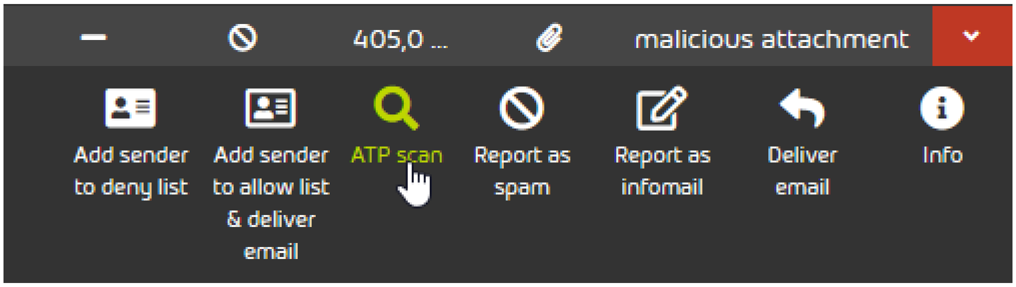


Figure 277: ATP scan in the Email Live Tracking

The detail view opens.

5. Click on **ATP scan** to start the scan.



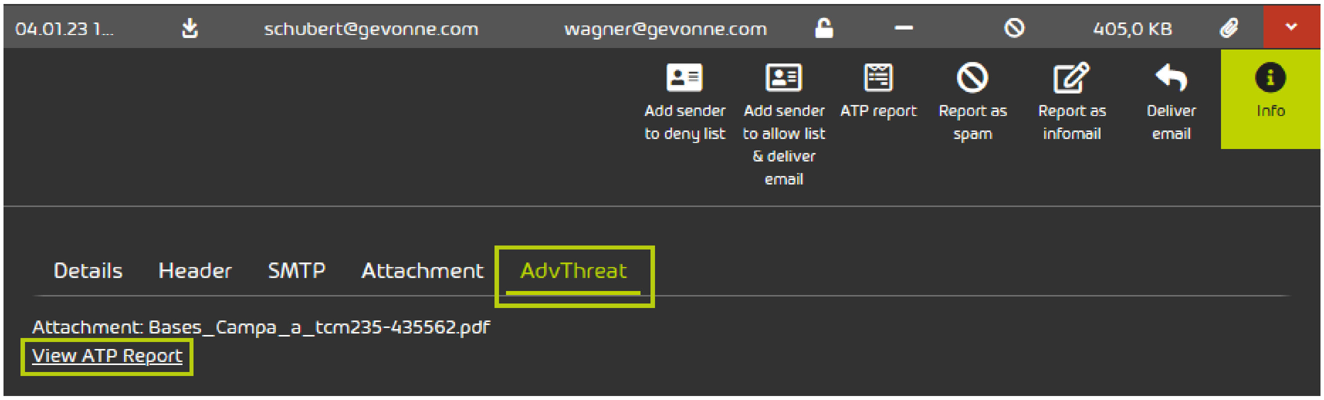
405,0 ...

malicious attachment

Figure 278: Initiate ATP scan

The ATP scan has been initiated for the email.

Once the ATP scan is complete, you can view the ATP report in the extended function view of the email under **ATP scan** (see ATP Report on page 75).



04.01.23 1... schubert@gevonne.com wagner@gevonne.com 405,0 KB

Attachment: Bases_Campa_a_tcm235-435562.pdf

View ATP Report

Figure 279: Open ATP report

ATP Report

The ATP report is a detailed report that is created after an email has been analyzed with the ATP scan (see chapter "ATP Scan" in the Control Panel manual and Initiating an ATP Scan on page 74). The ATP report provides information about the analyzed email. ATP reports are available for analyzed emails in the **Email Live Tracking** module (see Email Live Tracking on page 58). The ATP report of an email can be accessed under the menu item **ATP report** or **Info** of the **AdvThreat** tab of the email menu.

The ATP report is divided into four main sections:

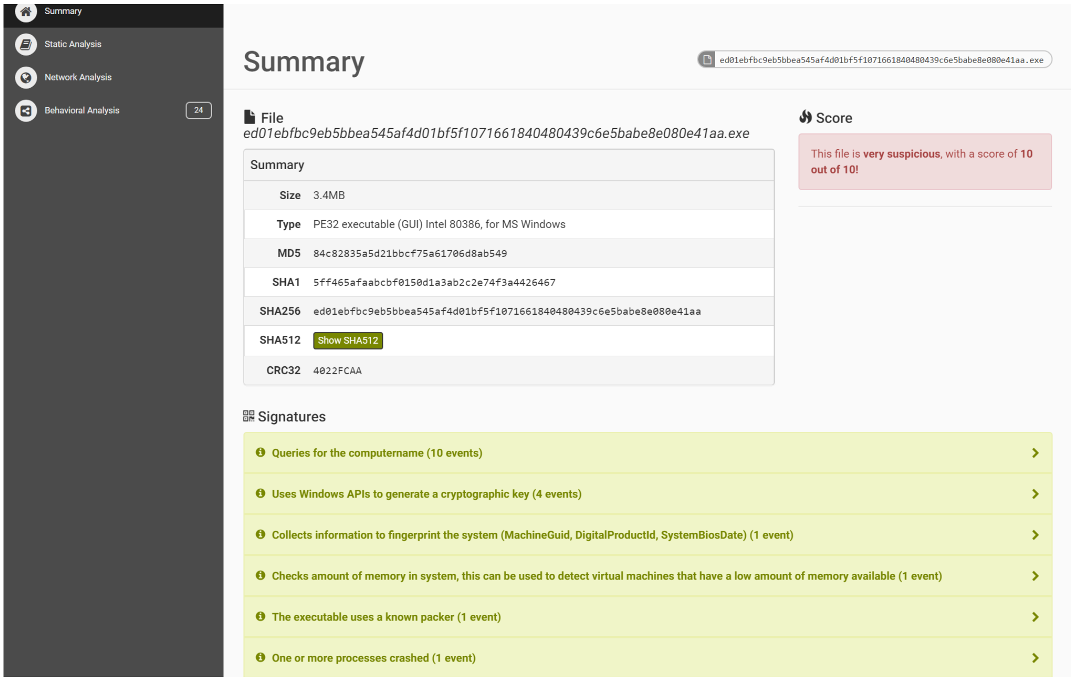
Summary

Here you will find an overview of the analyzed file. In addition, the file is assigned a **Score** from 0 to 10. 0 means "no danger", and 10 is the highest danger level.

Under the **Signatures** section, the file is assigned one of the following categories according to its behavior:

- Information (green)
- Attention (yellow)
- Warning (red)

When you click on a signature, extended process information is displayed.



Summary

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

File
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

Summary	
Size	3.4MB
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	84c82835a5d21bbcf75a61706d8ab549
SHA1	5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
SHA256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
SHA512	Show SHA512
CRC32	4022FCAA

Score

This file is **very suspicious**, with a score of **10 out of 10!**

Signatures

- Queries for the computername (10 events)
- Uses Windows APIs to generate a cryptographic key (4 events)
- Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate) (1 event)
- Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event)
- The executable uses a known packer (1 event)
- One or more processes crashed (1 event)

Figure 280: ATP Report Overview

Static Analysis

The static analysis is divided into three subcategories:

- Static Analysis – Static analysis of the file. It depends on the format of the file.
- Strings – Output of the strings contained in the file.
- Antivirus – Analysis of the file by different antivirus programs.

Network Analysis

In the network analysis, the entire network's traffic is analyzed and listed by protocol (e.g., HTTP, TCP, UDP).

Behavioral Analysis

The behavioral analysis monitors the behavior of the file at runtime.

It displays all system API calls and processes logged during dynamic sandbox analysis.

The results are divided into two sections:

- Process Tree – Here, the processes are displayed in hierarchical order.
- Process Contents – If you select a process from the process tree, the executed API queries are displayed here in chronological order.

Email Authentication

About Email Authentication

Email Authentication offers customer-level administrators different methods to authenticate email senders (see Methods for Sender Authentication on page 375). The following methods are available:

- SPF check (Sender Policy Framework) (see SPF check on page 376)
- DKIM validation and DKIM signing (DomainKeys Identified Mail) (see DKIM Validation and DKIM Signing on page 388)

- DMARC validation (Domain-based Message Authentication, Reporting and Conformance) (see DMARC Validation on page 393)

Email Authentication can only be used if Spam and Malware Protection has been activated (see "Activating Spam and Malware Protection" in the Control Panel manual). Before customer-level administrators can activate sender authentication methods, they must check the DNS settings of their own domains (see Checking the DNS Settings of Your Own Domains on page 374).

Checking the DNS Settings of Your Own Domains

You have activated Spam and Malware Protection (see "Activating Spam and Malware Protection" in the Control Panel manual).

Notice:

You can only check the DNS settings of the domains for which Spam and Malware Protection is activated.

Before setting up sender authentication methods, you must check whether the DNS settings of your domains are correctly configured. In this process, the SPF, DKIM and DMARC settings of your domains will be checked.

Important:

You can only activate the SPF check (see SPF check on page 376), the DKIM validation (see DKIM Validation and DKIM Signing on page 388) and the DMARC validation (see DMARC Validation on page 393) for those of your domains for which the corresponding DNS settings are correctly configured.

Notice:

To find out how to set an SPF record, see Setting an SPF Record on page 379.

To find out how to set a CNAME record, see Setting a CNAME Record on page 388.

1. Log in to the Control Panel with your administrative credentials.

2. Select your domain from the scope selection.
3. Navigate to **Security Settings** > **Email Authentication**.
4. Click on **Refresh DNS settings** to check the status of the DNS settings of your domains.

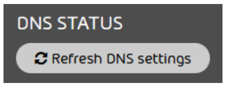


Figure 281: Update DNS settings

The status of the DNS settings of your domains is displayed in a table. The following three results are possible:

✓	The settings of the domain are correctly configured.
!	No records have been set for the domain.
✗	The settings of the domain are not correctly configured.

The DNS settings of your domains have been checked.

Next, you can activate sender authentication methods (see Methods for Sender Authentication on page 375).

Methods for Sender Authentication

Customer-level administrators can activate different methods for the authentication of email senders for their domains. The following methods are available:

- SPF check on page 376
- DKIM Validation and DKIM Signing on page 388

- DMARC Validation on page 393

These methods enhance the protection of a company's email infrastructure against spam and phishing. Customer-level administrators can use these methods individually or combine them.

Combining several methods delivers the best protection. For instance, on servers that only use DKIM, spam can be distributed by an email with a valid DKIM signature. As long as this email is not altered, the email can be sent with a valid DKIM signature in bulk to different people. To prevent this, SPF can be added. SPF checks the origin of the email. The IPv4 address and the domain name of the mail server are checked. SPF rejects emails from unauthorized servers. This prevents the distribution of spam via emails with a valid DKIM signature.

Furthermore, customer-level administrators can exclude some of their domains from the application of these methods by defining exceptions (see Adding Exceptions on page 404).

Emails that have failed the sender authentication are rejected or marked as spam. Emails that have failed the SPF check, the DKIM validation or the DMARC validation are assigned specific classification reasons in the Control Panel (see Classification Reasons of Email Authentication on page 405).

SPF check

SPF (Sender Policy Framework) is a sender authentication method that checks whether the sender address of an email has been faked. With an SPF check, the incoming server checks whether an incoming email has been sent by an authorized server. For this purpose, the incoming server checks whether the IP address of the outgoing server is registered in an SPF record in the DNS zone of the sender's domain. An SPF record contains the IP addresses of the servers that are authorized to send emails from a domain. For more information on the SPF check logic, see SPF Check Logic on page 377.

Customer-level administrators can set up the SPF check for incoming emails of their domains. To do so, administrators must first set the SPF records (see Setting an SPF Record on page 379) for all their domains to whose incoming emails SPF checks shall be applied. Administrators must then activate the SPF check (see Activating the SPF Check on page 379) and configure the advanced options (see Configuring Advanced Options for SPF Check on page 383).

The chapter Troubleshooting on page 386 explains how to resolve errors related to SPF checks.

SPF Check Logic

The logic of SPF checks is described below.

When an email is received on a destination server, the IP address of the sending server is compared with the records stored in the TXT record of the domain of the sender's email address. If the IP address of the sending server is not included in the TXT record, an error is returned. Depending on the severity, the check of the TXT record returns either a hardfail or a softfail.

Customer-level administrators can decide which measures shall be taken for each type of fail (see Activating the SPF Check on page 379). If no errors occur, the email is delivered as usual.

Notice:

The following explanations are based on the assumption that both the sender details from the envelope (MAIL FROM) and the sender details from the header (From) are being checked. If only one of these specifications is to be checked, a single check takes place and its fail type is decisive.

The following logic is considered when checking the TXT record:

1. In the first step, the domains that are given in the envelope (MAIL FROM) and the header (From) are checked simultaneously. If one of the checks fails, the type of its fail is considered in the next step. If both checks fail, the most serious type of fail is considered in the next step. There are three possible cases.

   Table 21: Case 1 - Both SPF checks end with a softfail

   If both the SPF check for the envelope and the SPF check for the header end with a softfail, a softfail is considered in the next step.

PART OF THE EMAIL	CONFIGURATION	TYPE OF FAIL
Envelope (MAIL FROM)	~all	Softfail

PART OF THE EMAIL	CONFIGURATION	TYPE OF FAIL
Header (From)	~all	Softfail

Table 22: Case 2 - Both SPF checks end with a hardfail

If both the SPF check for the envelope and the SPF check for the header end with a hardfail, a hardfail is considered in the next step.

PART OF THE EMAIL	CONFIGURATION	TYPE OF FAIL
Envelope (MAIL FROM)	-all	Hardfail
Header (From)	-all	Hardfail

Table 23: Case 3 - The SPF checks end with different fails

If the SPF checks for the envelope and the header end with different fails, a hardfail is considered in the next step.

PART OF THE EMAIL	CONFIGURATION	TYPE OF FAIL
Envelope (MAIL FROM)	-all	Hardfail
Header (From)	~all	Softfail

2. The second step is to check which measures you have set for a hardfail or a softfail. These are the measures which will be applied.

Notice:

In the SPF check, only the qualifiers **-** and **~** are supported. The qualifier **-** represents the result code hardfail and the qualifier **~** represents the result code softfail. The qualifier **?** is not supported.

Setting an SPF Record

You can set an SPF record in your domain's DNS zone to authorize our servers to send emails on behalf of your domain. Spam and Malware Protection (see "Spam and Malware Protection" in the Control Panel manual) can detect deception attempts such as spoofing based on the SPF entry in time. Recipients outside your organization can use the SPF record to perform SPF checks on emails from your domain. You also need the SPF record to enable Email Authentication to perform SPF checks (see "SPF check" in the Control Panel manual) on incoming emails.

Important:

Register all servers that are authorized to send emails from your domain in the SPF record.

Notice:

Our SPF record is not required for customers who have configured their primary environment with the **IP/Hostname** option but have not specified any relay server addresses for outgoing emails. For more information on how to set the primary environment, see .

You must set the SPF Record in the DNS zone of your domain yourself. For more information on how to correctly set the SPF record in the DNS zone, please contact Support.

Activating the SPF Check

You have set valid SPF records in the DNS zone of your domains (see Setting an SPF Record on page 379). You have activated Spam and Malware Protection for your domain (see "Activating Spam and Malware Protection" in the Control Panel manual).

Important:

SPF checks are only performed for domains with valid SPF records.

Important:

The SPF check can only be enabled if the customer meets one of the following conditions:

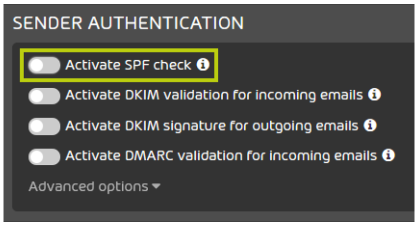
- The customer has configured their primary environment with the **IP/Hostname** option and defined relay server IP addresses for outgoing emails. The customer has set our SPF record in the DNS zone in addition to their own SPF records (see Setting an SPF Record on page 379).
- The customer has configured their primary environment with the **IP/Hostname** option but has not defined relay server IP addresses for outgoing emails. The customer has set their own SPF records in the DNS zone.

For more information on how to set the primary environment, see the chapter "Adjusting the Primary Environment Settings" in the Control Panel manual.

You can activate the SPF check to check whether the IP address of the outgoing server of an incoming email is specified in the SPF records of the sender's domain and is authorized to send emails from the domain.

1. Log in to the Control Panel with your administrative credentials.
2. Select your domain from the scope selection.
3. Navigate to **Security Settings** > **Email Authentication**.

4. Tick the **Activate SPF check** checkbox under **Sender Authentication**.



SENDER AUTHENTICATION

Activate SPF check

Activate DKIM validation for incoming emails

Activate DKIM signature for outgoing emails

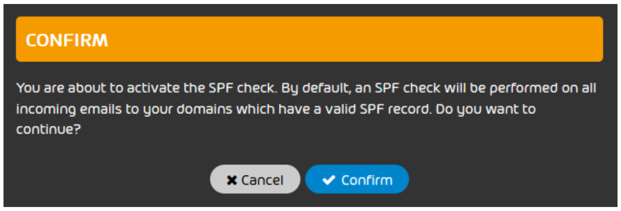
Activate DMARC validation for incoming emails

Figure 282: Enable SPF check

➔

A warning message is displayed.

5. Click on **Confirm**.



CONFIRM

You are about to activate the SPF check. By default, an SPF check will be performed on all incoming emails to your domains which have a valid SPF record. Do you want to continue?

Figure 283: Confirm

➔

The SPF check is activated for all domains that are under the selected domain and for which correct SPF records have been set.

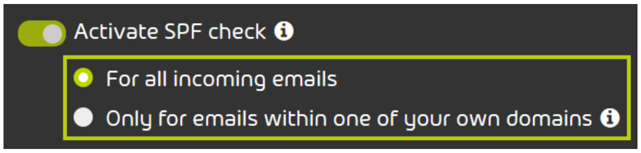
6. Select in which situations an SPF check shall be performed.

   - To check all incoming emails that have an SPF record set for their sender's domain, select **For all incoming emails**.

     > **Notice:**
     >
     > This option is recommended if there is generally a high volume of address forgery from different sender domains. If you use this variant, the false positive rate may increase if several communication partners have not configured their SPF records correctly.

   - To only check incoming emails sent from the recipient's domain or one of their alias domains, select **Only for emails within one of your own domains**.

     > **Notice:**
     >
     > Only internal emails are checked. This option is recommended to prevent targeted attacks under fake email addresses from your own domain.



Activate SPF check

● For all incoming emails

○ Only for emails within one of your own domains

Figure 284: Select emails for SPF check

➜

The SPF check is activated.

> **Notice:**
>
> Due to DNS caching, it may take up to 72 hours for the change to take effect.

✓

The SPF check has been activated.

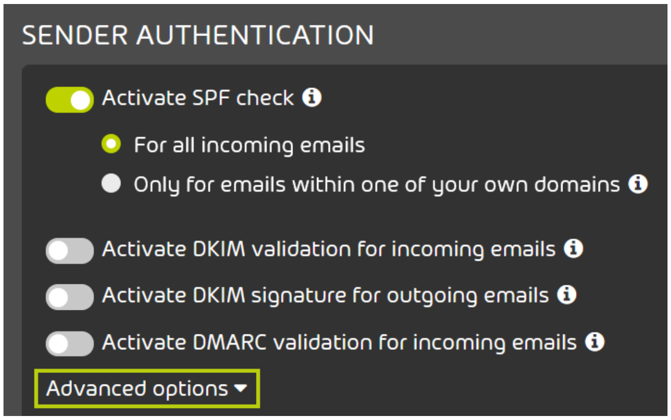
Next, you can configure the advanced options for the SPF check (see Configuring Advanced Options for SPF Check on page 383).

Configuring Advanced Options for SPF Check

You have activated the SPF check (see Activating the SPF Check on page 379).

In the **Security Settings** > **Email Authentication** module, you can configure how to proceed depending on the results of SPF checks (see SPF check on page 376).

1. Log in to the Control Panel with your administrative credentials.
2. Select your domain from the scope selection.
3. Navigate to **Security Settings** > **Email Authentication**.
4. Click on **Advanced options**.



SENDER AUTHENTICATION

- ☑ Activate SPF check
  - ● For all incoming emails
  - ○ Only for emails within one of your own domains
- ☐ Activate DKIM validation for incoming emails
- ☐ Activate DKIM signature for outgoing emails
- ☐ Activate DMARC validation for incoming emails

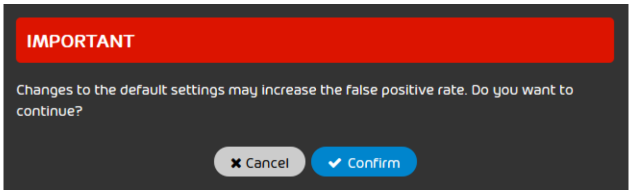
Figure 285: Open advanced options

A warning message is displayed.

5. **Important:**

   Changes to the advanced options can result in the delivery of malicious emails.

   To change the advanced options, click on **Confirm**.



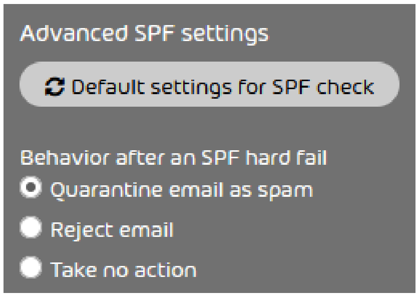
IMPORTANT

Changes to the default settings may increase the false positive rate. Do you want to continue?

Figure 286: Confirm

6. Optional: Under **Behavior after an SPF hard fail**, define what shall happen after an SPF hardfail. You have the following options:

   - **Quarantine email as spam**: The email is marked as spam and stored in quarantine.
   - **Reject email**: The email is rejected. The email is neither delivered to the recipient nor stored in quarantine.
   - **Take no action**: The SPF hardfail does not trigger any action. Subsequently, the email is checked by other filters of our services.



Advanced SPF settings

Behavior after an SPF hard fail

● Quarantine email as spam

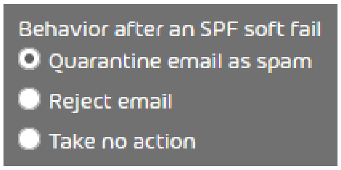
○ Reject email

○ Take no action

Figure 287: Select behavior after an SPF hardfail

7. Optional: Under **Behavior after an SPF soft fail**, define what shall happen after an SPF softfail. You have three options:

   - **Quarantine email as spam**: The email is marked as spam and stored in quarantine.
   - **Reject email**: The email is rejected. The email is neither delivered to the recipient nor stored in quarantine.
   - **Take no action**: The SPF softfail does not trigger any action. Subsequently, the email is checked by other filters of our services.



Behavior after an SPF soft fail

● Quarantine email as spam

○ Reject email

○ Take no action

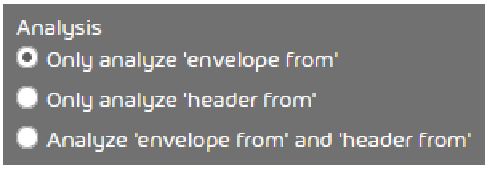
Figure 288: Select behavior after an SPF softfail

8. Optional: Under **Analysis**, determine which email elements shall be analyzed. You have the following options:

   - **Only analyze 'envelope from'**
   - **Only analyze 'header from'**
   - **Analyze 'envelope from' and 'header from'**

Notice:

If both elements are checked, this increases security, but also the false-positive rate.



Analysis

● Only analyze 'envelope from'

○ Only analyze 'header from'

○ Analyze 'envelope from' and 'header from'

Figure 289: Configure analysis

9. Optional: To reset the SPF settings to the default settings, click on **Default settings for SPF check**.

   Notice:

   The default settings are to store emails as spam in quarantine after an SPF hardfail and an SPF softfail and to only analyze the envelope from.

   ➜

   The changes are saved.

   Notice:

   Due to DNS caching, it may take up to 72 hours for the change to take effect.

✓

The advanced options for the SPF check have been configured.

Troubleshooting

The following errors related to SPF checks can be resolved:

- Errors related to SPF checks while sending emails (see Troubleshooting: Problems When Sending Emails with an SPF Entry Set Up on page 386)
- Errors related to SPF checks while receiving emails (see Troubleshooting: Problems When Receiving Emails with SPF Checks on page 387)

Troubleshooting: Problems When Sending Emails with an SPF Entry Set Up

Condition:

One of the following conditions is fulfilled:

- SPF checks are only performed if the sender's domain and the recipient's domain are the same. Incoming internal emails are incorrectly declared invalid.

- Your communication partner informs you that emails from your domain are declared invalid by SPF checks.

Cause: Your own TXT record is wrong

The IP addresses of your email servers registered in the TXT record are wrong or missing.

Remedy: Editing the TXT entry

Add the missing IPv4 addresses of your email servers to the TXT record or correct the IPv4 addresses.

Troubleshooting: Problems When Receiving Emails with SPF Checks

Condition:

SPF checks are performed for all incoming emails for whose sender's domain a TXT record is set. Incoming emails of certain domains are incorrectly declared invalid.

Cause: Errors in TXT entry of the communication partner

Remedy: Informing your communication partner

Inform the communication partner about a possible incorrect SPF configuration.

Remedy: Adding IP addresses to the allow list

1. Open the Control Panel.
2. Select the affected domain from the scope selection.
3. Navigate to **Deny & Allow Lists**.
4. Select the **Allow list** tab.
5. Enter the IPv4 address of the communication partner in the field **Add entry**.
6. Click on **Add** to confirm your input.

DKIM Validation and DKIM Signing

DKIM (DomainKeys Identified Mail) is an email authentication method that checks whether emails have been manipulated during transfer. DKIM signing adds a DKIM signature to the email header of an outgoing email. Once a server receives an email with a DKIM signature and performs a DKIM validation, the receiving server queries the public key that has been entered in the DNS zone of the sending domain in a TXT record. This key is used to check whether the DKIM signature is correct. The DKIM validation reveals if an email was altered during delivery.

The senders of incoming emails can be authenticated with DKIM validations. To do so, customer-level administrators must first activate the DKIM validation (see Activating the DKIM Validation on page 389) and then configure the advanced options (see Configuring Advanced Options for DKIM Validation on page 390).

Customer-level administrators can enable the recipients of their domains' outgoing emails to perform DKIM validations. To do so, administrators must first set CNAME records that point to our DKIM records in the DNS zone of their domains (see Setting a CNAME Record on page 388). Administrators must then activate DKIM signatures for outgoing emails of their domains (see Activating the DKIM Signing on page 392). This ensures that outgoing emails that are routed through our infrastructure are signed with DKIM.

Setting a CNAME Record

If you would like to use DKIM (see DKIM Validation and DKIM Signing on page 388), you must set CNAME records in the DNS zone of your domain. These records point to our DKIM records. The recipients of emails from your domain query these records in order to obtain the public key for encrypting our DKIM signature and other information required to perform a DKIM validation.

1. Contact Support to get the CNAME records.
2. Set the CNAME records in the DNS zone of your domain.

CNAME records have been set in the DNS zone of your domain.

Next, you can activate the DKIM validation (see Activating the DKIM Validation on page 389).

Activating the DKIM Validation

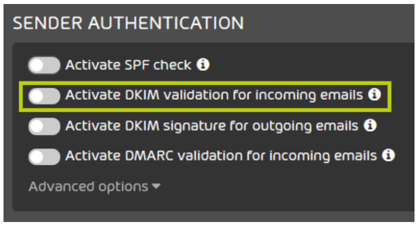
You have activated Spam and Malware Protection for your domain (see "Activating Spam and Malware Protection" in the Control Panel manual).

You can activate the DKIM validation (see DKIM Validation and DKIM Signing on page 388) to check the DKIM signatures of incoming emails.

1. Log in to the Control Panel with your administrative credentials.
2. Select your domain from the scope selection.
3. Navigate to **Security Settings** > **Email Authentication**.
4. **Important:**

   The DKIM validation can only be activated for your domains that have valid DKIM settings.

   Activate the checkbox **Sender Authentication** under **Activate DKIM validation for incoming emails**.



SENDER AUTHENTICATION

○ Activate SPF check

○ Activate DKIM validation for incoming emails

○ Activate DKIM signature for outgoing emails

○ Activate DMARC validation for incoming emails

Figure 290: Activating the DKIM Validation

The DKIM validation is activated for incoming emails.

Notice:

Due to DNS caching, it may take up to 72 hours for the change to take effect.

The DKIM validation of incoming emails has been activated for your domain.

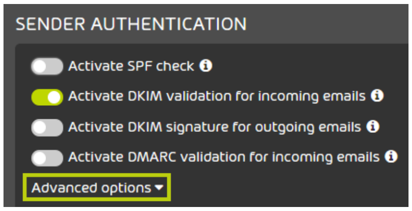
Next, you can configure the advanced options for the DKIM validation (see Configuring Advanced Options for DKIM Validation on page 390).

Configuring Advanced Options for DKIM Validation

You have activated the DKIM validation (see Activating the DKIM Validation on page 389).

In the **Security Settings** > **Email Authentication** module, you can configure how to proceed depending on the results of DKIM validations (see DKIM Validation and DKIM Signing on page 388).

1. Log in to the Control Panel with your administrative credentials.
2. Select your domain from the scope selection.
3. Navigate to **Security Settings** > **Email Authentication**.
4. Click on **Advanced options**.



SENDER AUTHENTICATION

- Activate SPF check
- Activate DKIM validation for incoming emails
- Activate DKIM signature for outgoing emails
- Activate DMARC validation for incoming emails

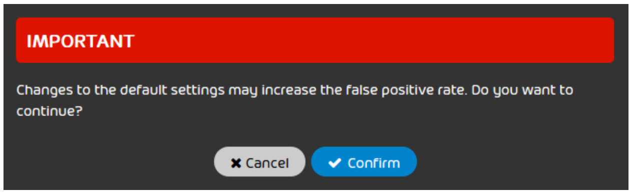
Figure 291: Open advanced options

A warning message is displayed.

5. **Important:**

   Changes to the advanced options can result in the delivery of malicious emails.

   To change the advanced options, click on **Confirm**.



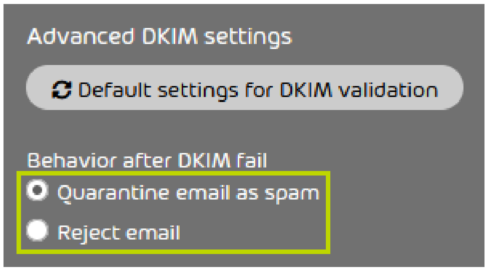
IMPORTANT

Changes to the default settings may increase the false positive rate. Do you want to continue?

Figure 292: Confirm

6. Optional: Under **Advanced DKIM settings**, define what shall happen after a DKIM fail. You have the following options:

   - **Quarantine email as spam**: The email is marked as spam and stored in quarantine.
   - **Reject email**: The email is rejected. The email is neither delivered to the recipient nor stored in quarantine.



Advanced DKIM settings

Behavior after DKIM fail

● Quarantine email as spam

○ Reject email

Figure 293: Select advanced options

7. Optional: To reset the DKIM settings to the default settings, click on **Default settings for DKIM validation**.

Notice:

The default setting is to store emails after a DKIM fail as spam in quarantine.

➜

The changes are saved.

Notice:

Due to DNS caching, it may take up to 72 hours for the change to take effect.

✓

The advanced options for the DKIM validation have been configured.

Activating the DKIM Signing

You have set valid CNAME records in the DNS zone of your domain (see Setting a CNAME Record on page 388). You have activated Spam and Malware Protection for your domain (see "Activating Spam and Malware Protection" in the Control Panel manual).

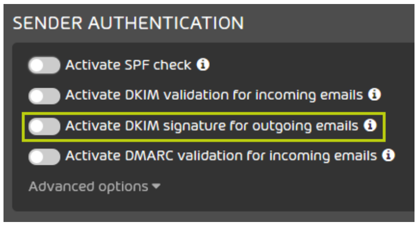
In the **Security Settings** > **Email Authentication** module, you can activate DKIM signing for outgoing emails of your domains to enable the recipients of the emails to perform DKIM validations.

1. Log in to the Control Panel with your administrative credentials.
2. Select your domain from the scope selection.
3. Navigate to **Security Settings** > **Email Authentication**.

4. **Important:**

   The DKIM validation can only be activated for your domains that have valid DKIM records.

   Tick the checkbox **Sender Authentication** under **Activate DKIM signature for outgoing emails**.



SENDER AUTHENTICATION

- ○ Activate SPF check
- ○ Activate DKIM validation for incoming emails
- ○ Activate DKIM signature for outgoing emails
- ○ Activate DMARC validation for incoming emails

Advanced options ▾

Figure 294: Activate DKIM signing

DKIM signing is activated for outgoing emails.

Notice:

Due to DNS caching, it may take up to 72 hours for the change to take effect.

DKIM signing has been activated for outgoing emails.

DMARC Validation

DMARC (Domain-based Message Authentication, Reporting & Conformance) defines how an incoming email should be handled depending on the results of the SPF check and the DKIM validation as well as other alignments of addresses and domains.

A DMARC validation checks if an incoming email corresponds to what the recipient knows about the sender. The DMARC validation is performed after the SPF check and the DKIM validation. Based on the results of the SPF check and the DKIM validation as well as the results of the alignment of addresses in the envelope from and in the header from of the email (SPF alignment) on the one hand, and the alignment of domains in the header from and in the DKIM signature (DKIM alignment) on the other hand, the DMARC validation decides how to handle the email. For more information on the DMARC decision matrix, see DMARC Decision Matrix on page 397.

Customer-level administrators can set up the DMARC validation for incoming emails of their domains. To do so, customers must first set a DMARC record in the DNS zone of their domains (see Setting a DMARC Record on page 394 and Tags in DMARC Records on page 395), then activate the DMARC validation (see Activating the DMARC Validation on page 399) and finally configure the advanced options (see Configuring Advanced Options for DMARC Validation on page 401).

Setting a DMARC Record

A DMARC record is required to perform DMARC validations (see DMARC Validation on page 393) on emails from a domain. You can set a DMARC record for your domain.

1. Create a TXT record with the following name in the DNS zone of your domain. Replace **<domain.tld>** with your domain.
   _dmarc.<domain.tld>
2. Define the DMARC policy according to the following sample pattern in the TXT record. Replace **<username@domain.tld>** with an email address.
   v=DMARC1;p=quarantine;pct=100;rua=mailto:<username@domain.tld>

> **Important:**
>
> The chapter Tags in DMARC Records on page 395 provides an overview and explanation of the tags that can be used in DMARC records.

> **Notice:**
>
> The specifications from the DMARC record are applied to emails sent to recipients outside the domain. The settings for emails sent to recipients within the domain can be configured in the **Email Authentication** module.

✓

A DMARC record has been set in the DNS zone of the domain.

Tags in DMARC Records

DMARC records are made up of tags. The tags of a DMARC record contain specifications for DMARC validations of emails sent from the domain to recipients outside the domain.

The following table provides an overview and explanation of the tags that can be used in DMARC entries. All tags but **v** and **p** are optional.

> **Important:**
>
> The tags **v** and **p** are required.

TAG	EXPLANATION	POSSIBLE VALUES
v	This tag determines which DMARC protocol version is used.	**v=DMARC1** **Notice:** The only possible value for this tag is **v=DMARC1**.
p	This tag determines how to handle an email from the domain in case its DMARC validation fails.	**p=quarantine**: The email is stored in quarantine. **p=reject**: The email is rejected. **p=none**: No measures are taken for the email. **Notice:** We recommend the value **p=quarantine**.

TAG	EXPLANATION	POSSIBLE VALUES
pct	This tag determines the percentage of emails for which DMARC validations are performed. Possible values for this tag are numbers from 1 to 100.	**pct=100** **Notice:** We recommend the value **pct=100** so that DMARC validations are performed on all emails from the domain.
rua	This tag determines the email address to which daily aggregate reports about failed DMARC validations are sent.	**rua=mailto:<username@domain.com>** **<username@domain.com>** should be replaced with the email address to which the aggregate reports are to be sent.
ruf	This tag determines the email address to which forensic reports about single emails for which the DMARC validation has failed are sent.	**ruf=mailto:<username@domain.com>** **<username@domain.com>** should be replaced with the email address to which the forensic reports should be sent.
sp	This tag determines how to handle an email from a subdomain of the domain if the DMARC validation for the email fails.	**sp=quarantine**: The email is stored in quarantine. **sp=reject**: The email is rejected. **sp=none**: No measures are taken for the email.

TAG	EXPLANATION	POSSIBLE VALUES
adkim	This tag determines the alignment mode for DKIM signatures (see DKIM Validation and DKIM Signing on page 388). The alignment mode determines the degree of accuracy with which an email must match the DKIM signature in order to be accepted.	**adkim=r**: The alignment mode is relaxed. A partial match is enough. **adkim=s**: The alignment mode is strict. An exact match is required.
aspf	This tag determines the alignment mode for the domains in the header from and the envelope from of an email (see SPF check on page 376). The alignment mode determines the degree of accuracy with which both domains must match in order for the email to be accepted.	**aspf=r**: The alignment mode is relaxed. A partial match is enough. **aspf=s** The alignment mode is strict. An exact match is required.

DMARC Decision Matrix

The DMARC decision matrix indicates how incoming emails are handled after successful or failed SPF checks and DKIM validations.

Table 24: DMARC decision matrix

SPF CHECK	DKIM VALIDATION	SPF ALIGNMENT	DKIM ALIGNMENT	DMARC RESULT	ACTION
Pass	Pass	Pass	Pass	Pass	Deliver
Pass	Pass	Pass	Fail	Pass	Deliver
Pass	Pass	Fail	Pass	Pass	Deliver
Pass	Pass	Fail	Fail	Fail	Store as spam in quarantine or reject
Pass	Fail	Pass	Pass	Pass	Deliver
Pass	Fail	Pass	Fail	Pass	Deliver
Pass	Fail	Fail	Pass	Fail	Store as spam in quarantine or reject
Pass	Fail	Fail	Fail	Fail	Store as spam in quarantine or reject
Fail	Pass	Pass	Pass	Pass	Deliver
Fail	Pass	Pass	Fail	Fail	Store as spam in quarantine or reject
Fail	Pass	Fail	Pass	Pass	Deliver
Fail	Pass	Fail	Fail	Fail	Store as spam in quarantine or reject

SPF CHECK	DKIM VALIDATION	SPF ALIGNMENT	DKIM ALIGNMENT	DMARC RESULT	ACTION
Fail	Fail	Pass	Pass	Fail	Store as spam in quarantine or reject
Fail	Fail	Pass	Fail	Fail	Store as spam in quarantine or reject
Fail	Fail	Fail	Pass	Fail	Store as spam in quarantine or reject
Fail	Fail	Fail	Fail	Fail	Store as spam in quarantine or reject

The DMARC result is only positive if both the SPF check (see SPF check on page 376) or DKIM validation (see DKIM Validation and DKIM Signing on page 388) and the corresponding alignment (SPF alignment or DKIM alignment) have been passed. If the DMARC result is positive, the email will be delivered. Otherwise, the email will be either stored as spam in quarantine or rejected, depending on the settings in the **Email Authentication** module (see About Email Authentication on page 373) in the Control Panel.

Activating the DMARC Validation

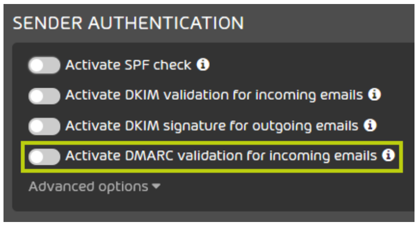
You have set valid SPF, DKIM and DMARC records for at least one of your domains (see Setting an SPF Record on page 379, Setting a CNAME Record on page 388 and Setting a DMARC Record on page 394). You have activated Spam and Malware Protection for your domain (see "Activating Spam and Malware Protection" in the Control Panel manual).

You can activate the DMARC validation to specify how incoming emails are handled depending on the results of SPF checks (see SPF check on page 376) and DKIM validations (see DKIM Validation and DKIM Signing on page 388).

1. Log in to the Control Panel with your administrative credentials.
2. Select your domain from the scope selection.
3. Navigate to **Security Settings** > **Email Authentication**.
4. **Important:**

   The DMARC validation can only be activated for your domains that have valid SPF, DKIM and DMARC records.

   Tick the checkbox **Sender Authentication** under **Activate DMARC validation for incoming emails**.



SENDER AUTHENTICATION

- Activate SPF check
- Activate DKIM validation for incoming emails
- Activate DKIM signature for outgoing emails
- Activate DMARC validation for incoming emails

Figure 295: Activate the DMARC validation

The DMARC validation is activated for incoming emails.

Notice:

Due to DNS caching, it may take up to 72 hours for the change to take effect.

The DMARC validation has been activated for incoming emails.

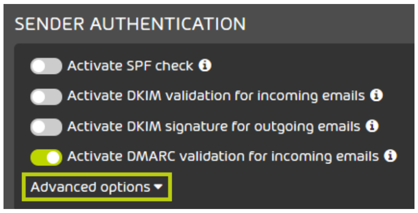
Next, you can configure the advanced options for the DMARC validation (see Configuring Advanced Options for DMARC Validation on page 401).

Configuring Advanced Options for DMARC Validation

You have activated the DMARC validation (see Activating the DMARC Validation on page 399).

In the **Security Settings** > **Email Authentication** module, you can configure how to proceed depending on the results of DMARC validations (see DMARC Validation on page 393).

1. Log in to the Control Panel with your administrative credentials.
2. Select your domain from the scope selection.
3. Navigate to **Security Settings** > **Email Authentication**.
4. Click on **Advanced options**.



SENDER AUTHENTICATION

○ Activate SPF check
○ Activate DKIM validation for incoming emails
○ Activate DKIM signature for outgoing emails
● Activate DMARC validation for incoming emails

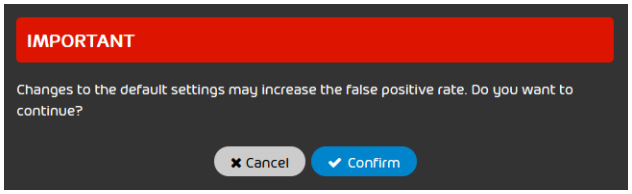
Figure 296: Open advanced options

A warning message is displayed.

5. **Important:**

   Changes to the advanced options can result in the delivery of malicious emails.

   To change the advanced options, click on **Confirm**.



IMPORTANT

Changes to the default settings may increase the false positive rate. Do you want to continue?

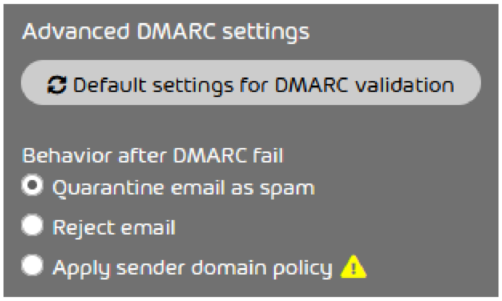
Figure 297: Confirm

6. Optional: Under **Advanced DMARC settings**, define what shall happen after a DMARC fail. You have the following options:

   - **Quarantine email as spam**: The email is marked as spam and stored in quarantine.
   - **Reject email**: The email is rejected. The email is neither delivered to the recipient nor stored in quarantine.
   - **Apply sender domain policy**: After a DMARC Fail, the email is handled according to the DMARC policy of the sender's domain.

   Notice:

   If you select this option, you trust the DMARC policies of third parties.



Advanced DMARC settings

Default settings for DMARC validation

Behavior after DMARC fail

● Quarantine email as spam

○ Reject email

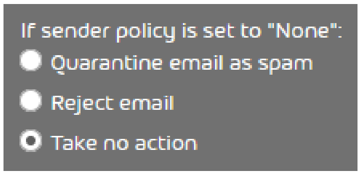
○ Apply sender domain policy ⚠

Figure 298: Select behavior after a DMARC fail

If the option **Apply sender domain policy** has been selected, additional settings are displayed.

7. If you have selected the option **Apply sender domain policy**, select under **If sender policy is set to "None":** the behavior to apply if the DMARC policy of the sender's domain has been set to "None". You have the following options:

   - **Quarantine email as spam**: The email is marked as spam and stored in quarantine.
   - **Reject email**: The email is rejected. The email is neither delivered to the recipient nor stored in quarantine.
   - **Take no action**: The DMARC fail does not trigger any action. Subsequently, the email is checked by other filters of our services.



If sender policy is set to "None":
○ Quarantine email as spam
○ Reject email
● Take no action

Figure 299: Behavior if sender policy is set to "None"

8. Optional: To reset the DMARC settings to the default settings, click on **Default settings for DMARC validation**.

> **Notice:**
>
> The default setting is to store emails after a DMARC fail as spam in quarantine.

➜

The changes are saved.

> **Notice:**
>
> Due to DNS caching, it may take up to 72 hours for the change to take effect.

✓

The advanced options for the DMARC validation have been configured.

Adding Exceptions

You have activated sender authentication methods (see Methods for Sender Authentication on page 375) in the **Email Authentication** module.

If you have activated the SPF check (see SPF check on page 376), the DKIM validation (see DKIM Validation and DKIM Signing on page 388) and/or the DMARC validation (see DMARC Validation on page 393), and would like to deactivate these for one of your domains, you must an exception.

1. Log in to the Control Panel with your administrative credentials.
2. Select your domain from the scope selection.
3. Navigate to **Security Settings** > **Email Authentication**.
4. Click on **Add exception** under **Exceptions**.

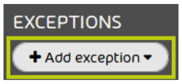


Figure 300: Add exception

➔

An extended view opens.

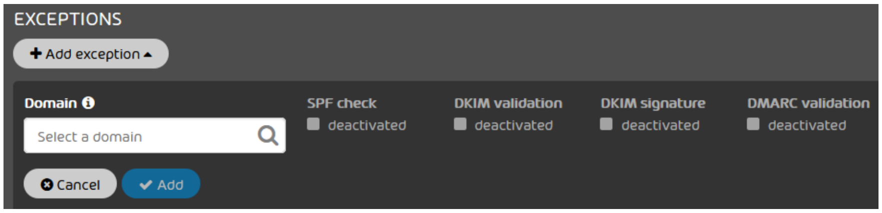


Figure 301: Extended view

5. Under **Domain**, select the domain for which you would like to add the exception.

> **Notice:**
>
> You can only select domains for which Spam and Malware Protection is activated.

6. Activate the checkbox under the name of the check that you would like to deactivate for the domain.

   > **Notice:**
   >
   > You can only deactivate the SPF check, the DKIM validation or the DMARC validation for a domain if the domain has the corresponding valid DNS settings. For all other domains, no checks are performed.

7. Click on **Add**.

   ➜

   The exception is added and appears in the table below.

   > **Notice:**
   >
   > Due to DNS caching, it may take up to 72 hours for the change to take effect.

✓

An exception has been added to Email Authentication.

Classification Reasons of Email Authentication

For emails that have failed the sender authentication of Email Authentication, certain classification reasons are used in the Control Panel. For information on other classification reasons, see chapter "Classification reasons" in the Control Panel manual.

SPF

Emails found not to have been sent by a server registered in the DNS during an SPF check will be stored as spam in quarantine, rejected or delivered, depending on your settings (see Configuring Advanced Options for SPF Check on page 383).

In the **Email Live Tracking** module in the Control Panel, these emails are displayed with the reasons **Envelope SPF Failure** and **Message Header SPF Failure** regardless of the measure performed.

DKIM

Emails that have failed the DKIM validation are stored as spam in quarantine or rejected depending on your settings (see Configuring Advanced Options for DMARC Validation on page 401).

In the **Email Live Tracking** module in the Control Panel, these emails are displayed with the reason **DKIM Failure**.

DMARC

Emails found in a DMARC check not to comply with the SPF and/or DKIM policies are stored as spam in quarantine or rejected, depending on your settings (see Configuring Advanced Options for DMARC Validation on page 401).

In the **Email Live Tracking** module in the Control Panel, these emails are displayed with the reason **DMARC Failure**.

Quarantine Report

About Quarantine Report

Quarantine Report is a feature of Spam and Malware Protection (see chapter "Spam and Malware Protection" in the Control Panel manual) that allows customer-level administrators to configure quarantine reports for the users of their domains.

A quarantine report is a report which is either created individually for a user or for an entire domain and is delivered to the recipient by email. Customer-level administrators can select a quarantine report layout (see Layouts for Quarantine Reports on page 407). The quarantine report lists all emails categorized as **Spam** and **Infomail** (see chapter "Email Categories" in the Control Panel manual), as well as emails that have not been delivered to the user but put in quarantine. If the recipient of a quarantine report has the required permissions, they can later have those emails delivered on demand (see Email Actions in Quarantine Reports on page 412).

Notice:

In the **Spam and Malware Protection** module, you can choose which emails can be delivered by the users (see chapter 'Allowing and Forbidding User Actions' in the Control Panel manual).

Notice:

The number of listed emails is limited. Up to 1000 emails are displayed in a quarantine report.

Quarantine reports are generated for each primary mailbox. If a user has alias mailboxes, he receives a single quarantine report listing emails addressed both to the primary mailbox and to the alias mailboxes. Once the user delivers an email from a quarantine report (see Delivering an Email from a Quarantine Report on page 430), the mailbox to which the email is addressed is displayed.

Customer-level administrators can activate the **Quarantine Report** module for a domain (see Activating the Quarantine Report for a Domain on page 414) and configure it (see Configuring the Quarantine Report for a Domain on page 416). Furthermore, administrators can configure the **Quarantine Report** module differently for an individual mailbox (see Configuring the Quarantine Report for a Mailbox on page 421). If needed, administrators can also deactivate the **Quarantine Report** module for a domain (see Deactivating the Quarantine Report for a Domain on page 429).

Layouts for Quarantine Reports

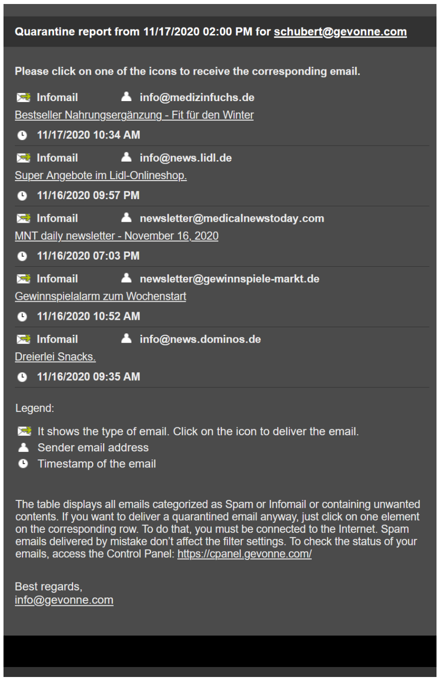
In the **Quarantine Report** module (see About Quarantine Report on page 406), customer-level administrators can select a layout for their domains' quarantine reports (see Configuring the Quarantine Report for a Domain on page 416). The layout determines which email actions the recipients can trigger from their quarantine reports (see Email Actions in Quarantine Reports on page 412).

Notice:

In the footer of quarantine reports, the support information from the **Customization** module is displayed (see chapter "Adding Support Information to the Control Panel" in the Control Panel manual).

The following layouts are available:

- **Default layout**: This layout is our default layout.



Quarantine report from 11/17/2020 02:00 PM for schubert@gevonne.com

Please click on one of the icons to receive the corresponding email.

✉ **Infomail** 👤 **info@medizinfuchs.de**
Bestseller Nahrungsergänzung - Fit für den Winter
🕒 **11/17/2020 10:34 AM**

✉ **Infomail** 👤 **info@news.lidl.de**
Super Angebote im Lidl-Onlineshop.
🕒 **11/16/2020 09:57 PM**

✉ **Infomail** 👤 **newsletter@medicalnewstoday.com**
MNT daily newsletter - November 16, 2020
🕒 **11/16/2020 07:03 PM**

✉ **Infomail** 👤 **newsletter@gewinnspiele-markt.de**
Gewinnspielalarm zum Wochenstart
🕒 **11/16/2020 10:52 AM**

✉ **Infomail** 👤 **info@news.dominos.de**
Dreierlei Snacks.
🕒 **11/16/2020 09:35 AM**

Legend:

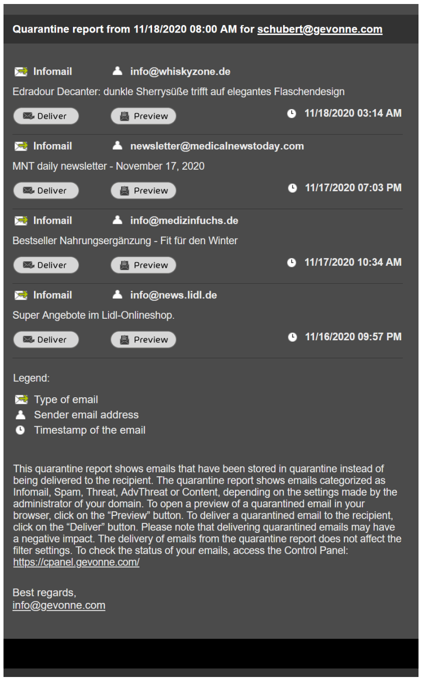
✉ It shows the type of email. Click on the icon to deliver the email.
👤 Sender email address
🕒 Timestamp of the email

The table displays all emails categorized as Spam or Infomail or containing unwanted contents. If you want to deliver a quarantined email anyway, just click on one element on the corresponding row. To do that, you must be connected to the Internet. Spam emails delivered by mistake don't affect the filter settings. To check the status of your emails, access the Control Panel: https://cpanel.gevonne.com/

Best regards,
info@gevonne.com

Figure 302: Default layout

- **Default layout with email preview**: This layout is our default layout with additional buttons for the delivery and preview of emails (see Email Preview on page 91).



Quarantine report from 11/18/2020 08:00 AM for schubert@gevonne.com

Infomail info@whiskyzone.de
Edradour Decanter: dunkle Sherrysüße trifft auf elegantes Flaschendesign
11/18/2020 03:14 AM

Infomail newsletter@medicalnewstoday.com
MNT daily newsletter - November 17, 2020
11/17/2020 07:03 PM

Infomail info@medizinfuchs.de
Bestseller Nahrungsergänzung - Fit für den Winter
11/17/2020 10:34 AM

Infomail info@news.lidl.de
Super Angebote im Lidl-Onlineshop.
11/16/2020 09:57 PM

Legend:

Type of email
Sender email address
Timestamp of the email

This quarantine report shows emails that have been stored in quarantine instead of being delivered to the recipient. The quarantine report shows emails categorized as Infomail, Spam, Threat, AdvThreat or Content, depending on the settings made by the administrator of your domain. To open a preview of a quarantined email in your browser, click on the “Preview” button. To deliver a quarantined email to the recipient, click on the “Deliver” button. Please note that delivering quarantined emails may have a negative impact. The delivery of emails from the quarantine report does not affect the filter settings. To check the status of your emails, access the Control Panel: https://cpanel.gevonne.com/

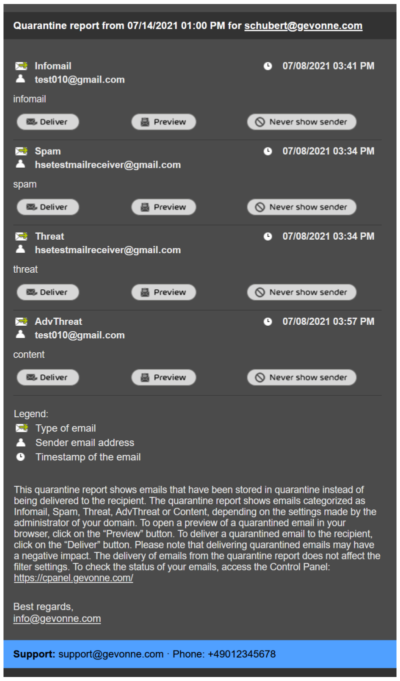
Best regards,
info@gevonne.com

Figure 303: Default layout with email preview

- **Inbox Manager with email preview and exclude option**: This layout is our default layout with additional buttons for the delivery and preview of emails and for excluding a sender's emails from future quarantine reports. Quarantine reports with this layout do not list any emails by senders who are on the user's deny list or the deny list of the domain. To exclude a sender's emails from future quarantine reports, the recipient of the quarantine report can add the sender of a quarantined email to their own deny list (see chapter "About Deny & Allow Lists" in the Control Panel manual) using the button **Never show sender**.

Important:

This layout is only displayed and can only be selected if the option **Exclude emails by senders from the deny list from quarantine reports** has been enabled in the quarantine reports settings. For more information on how to configure quarantine reports, see Configuring the Quarantine Report for a Domain on page 416.



Quarantine report from 07/14/2021 01:00 PM for schubert@gevonne.com

Infomail 07/08/2021 03:41 PM
test010@gmail.com
infomail

Spam 07/08/2021 03:34 PM
hsetestmailreceiver@gmail.com
spam

Threat 07/08/2021 03:34 PM
hsetestmailreceiver@gmail.com
threat

AdvThreat 07/08/2021 03:57 PM
test010@gmail.com
content

Legend:
✉ Type of email
👤 Sender email address
🕓 Timestamp of the email

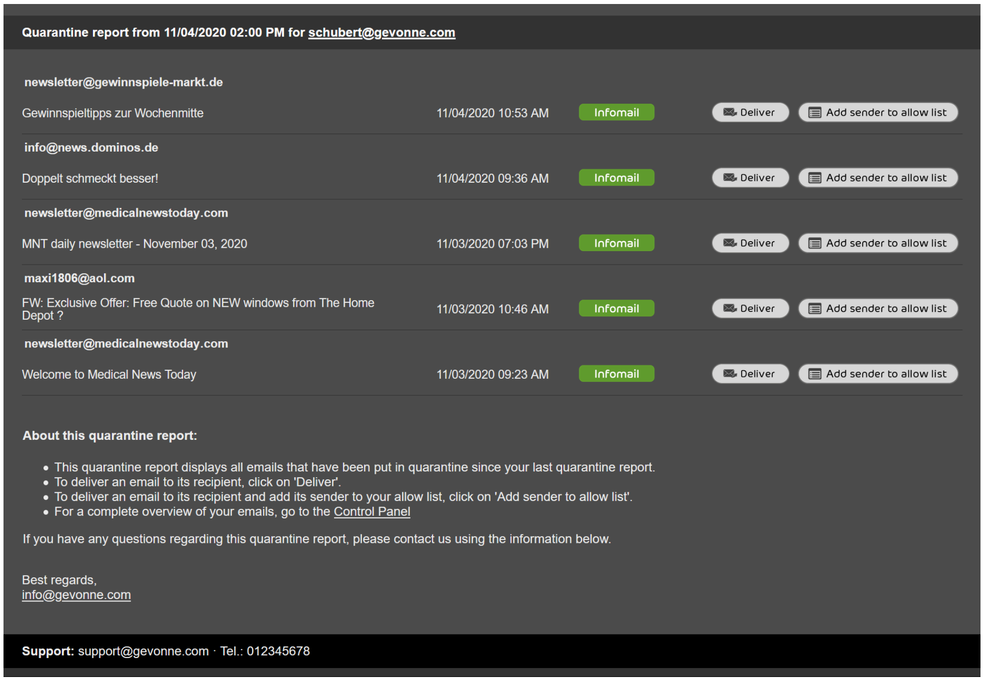
This quarantine report shows emails that have been stored in quarantine instead of being delivered to the recipient. The quarantine report shows emails categorized as Infomail, Spam, Threat, AdvThreat or Content, depending on the settings made by the administrator of your domain. To open a preview of a quarantined email in your browser, click on the "Preview" button. To deliver a quarantined email to the recipient, click on the "Deliver" button. Please note that delivering quarantined emails may have a negative impact. The delivery of emails from the quarantine report does not affect the filter settings. To check the status of your emails, access the Control Panel: https://cpanel.gevonne.com/

Best regards,
info@gevonne.com

Support: support@gevonne.com · Phone: +49012345678

Figure 304: Inbox Manager with email preview and exclude option

- **Layout for desktop**: This layout is optimal for desktop PCs because it fully utilizes the screen width. The quarantine reports contain buttons for the delivery of emails and for the addition of recipients to the allow list.



Quarantine report from 11/04/2020 02:00 PM for schubert@gevonne.com

newsletter@gewinnspiele-markt.de

Gewinnspieltipps zur Wochenmitte 11/04/2020 10:53 AM Infomail

info@news.dominos.de

Doppelt schmeckt besser! 11/04/2020 09:36 AM Infomail

newsletter@medicalnewstoday.com

MNT daily newsletter - November 03, 2020 11/03/2020 07:03 PM Infomail

maxi1806@aol.com

FW: Exclusive Offer: Free Quote on NEW windows from The Home Depot ? 11/03/2020 10:46 AM Infomail

newsletter@medicalnewstoday.com

Welcome to Medical News Today 11/03/2020 09:23 AM Infomail

About this quarantine report:

- This quarantine report displays all emails that have been put in quarantine since your last quarantine report.
- To deliver an email to its recipient, click on 'Deliver'.
- To deliver an email to its recipient and add its sender to your allow list, click on 'Add sender to allow list'.
- For a complete overview of your emails, go to the Control Panel

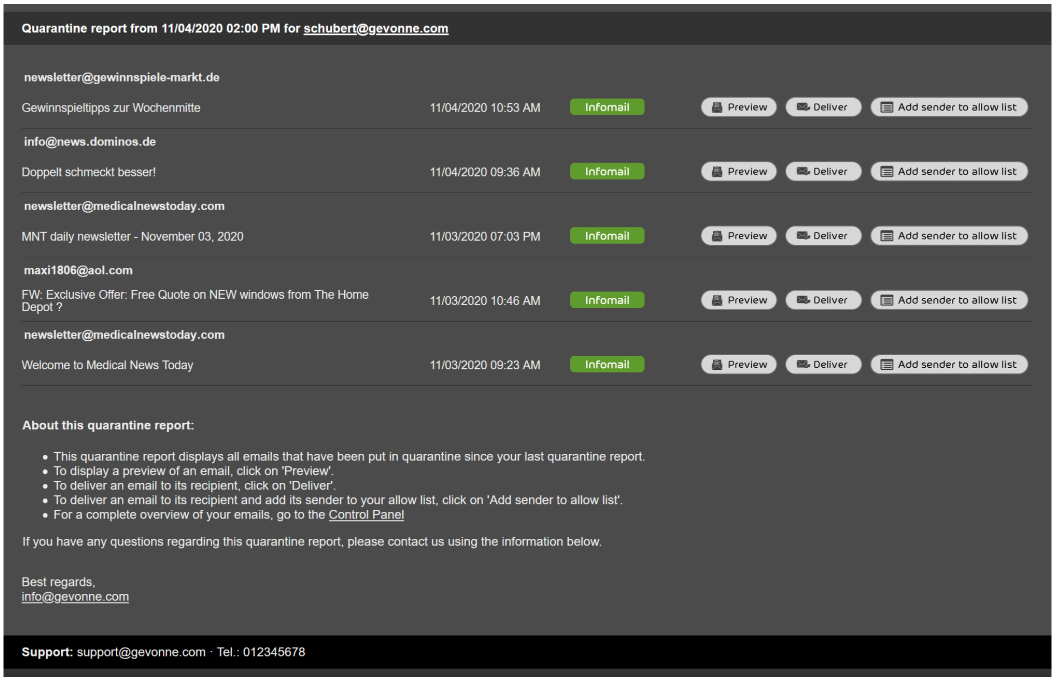
If you have any questions regarding this quarantine report, please contact us using the information below.

Best regards,
info@gevonne.com

Support: support@gevonne.com · Tel.: 012345678

Figure 305: Layout for desktop

- **Layout for desktop with email preview**: This layout is our layout for desktops with additional buttons for the preview of emails (see Email Preview on page 91).



Quarantine report from 11/04/2020 02:00 PM for schubert@gevonne.com

newsletter@gewinnspiele-markt.de			
Gewinnspieltipps zur Wochenmitte	11/04/2020 10:53 AM	Infomail	Preview · Deliver · Add sender to allow list
info@news.dominos.de			
Doppelt schmeckt besser!	11/04/2020 09:36 AM	Infomail	Preview · Deliver · Add sender to allow list
newsletter@medicalnewstoday.com			
MNT daily newsletter - November 03, 2020	11/03/2020 07:03 PM	Infomail	Preview · Deliver · Add sender to allow list
maxi1806@aol.com			
FW: Exclusive Offer: Free Quote on NEW windows from The Home Depot ?	11/03/2020 10:46 AM	Infomail	Preview · Deliver · Add sender to allow list
newsletter@medicalnewstoday.com			
Welcome to Medical News Today	11/03/2020 09:23 AM	Infomail	Preview · Deliver · Add sender to allow list

About this quarantine report:

- This quarantine report displays all emails that have been put in quarantine since your last quarantine report.
- To display a preview of an email, click on 'Preview'.
- To deliver an email to its recipient, click on 'Deliver'.
- To deliver an email to its recipient and add its sender to your allow list, click on 'Add sender to allow list'.
- For a complete overview of your emails, go to the Control Panel

If you have any questions regarding this quarantine report, please contact us using the information below.

Best regards,
info@gevonne.com

Support: support@gevonne.com · Tel.: 012345678

Figure 306: Layout for desktop with email preview

Email Actions in Quarantine Reports

Quarantine reports contain buttons that allow you to perform some email actions from the **Email Live Tracking** module. The available actions depend on the layout of the quarantine reports (see Layouts for Quarantine Reports on page 407). The following table explains the actions and lists the layouts in which the actions are available.

Table 25: Email Actions in Quarantine Reports

ACTION	LAYOUT	EXPLANATION
Deliver	Default layout Default layout with email preview Inbox Manager with email preview and exclude option Layout for desktop Layout for desktop with email preview	The selected emails are delivered, triggering a process of re-evaluation of the classification on our part. For more information, see chapter "Email Actions" in the Control Panel manual.
Add sender to allow list	Layout for desktop Layout for desktop with email preview	The senders of the selected emails are added to the user's allow list and the emails are delivered. All other emails from the senders will be automatically delivered.

ACTION	LAYOUT	EXPLANATION
Preview	**Default layout with email preview** **Inbox Manager with email preview and exclude option** **Layout for desktop with email preview**	In a new window, an encrypted link opens a web service where the content of the selected email is displayed in a secure way. Images, links and other active content from the email are deactivated or replaced by secure placeholders. If necessary and possible, the layout and encoding of the email are slightly modified to display the content of the email. For more information, see chapter "Email Preview" in the Control Panel manual.
Never show sender	**Inbox Manager with email preview and exclude option**	The sender of the selected email is added (see chapter "About Deny & Allow Lists" in the Control Panel manual) to the recipient's deny list (see chapter "Email Actions" in the Control Panel manual). Emails from this sender will not be listed in the user's future quarantine reports.

Activating the Quarantine Report for a Domain

✓ You have activated Spam and Malware Protection (see chapter "Activating Spam and Malware Protection" in the Control Panel manual).

You can activate the **Quarantine Report** module (see About Quarantine Report on page 406) for a domain so that its users can receive quarantine reports.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to activate the **Quarantine Report** module.
3. Navigate to **Security Settings** > **Quarantine Report**.
4. **Important:**

   If you want to customize the quarantine reports, enter all required information into the **Customization** module before activating the **Quarantine Report** module. The quarantine reports are automatically customized based on the information from this module. If you have not entered any information into the module, the quarantine reports will not be customized.

   Toggle the switch **Activate Quarantine Report**.

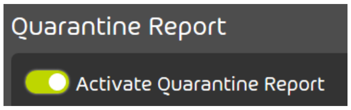


Figure 307: Activate the Quarantine Report

The switch is highlighted in green.

The **Quarantine Report** module has been activated for a domain.

Next, you can configure the **Quarantine Report** module for the domain (see Configuring the Quarantine Report for a Domain on page 416).

Configuring the Quarantine Report for a Domain

You have activated the **Quarantine Report** module for the domain (see Activating the Quarantine Report for a Domain on page 414).

You can configure the quarantine reports for a domain in the **Quarantine Report** module (see About Quarantine Report on page 406).

1. Log in to the Control Panel with your administrative credentials.
2. Navigate to **Security Settings** > **Quarantine Report**.
3. **Important:**

   By default, all users of the domain receive individual quarantine reports at their own email addresses. Alternatively, you can generate a quarantine report for the whole domain. If a quarantine report is generated for the whole domain, its users do not receive any quarantine report.

   Optional: To generate a quarantine report for the whole domain, toggle the switch **Generate a quarantine report for the whole domain**.

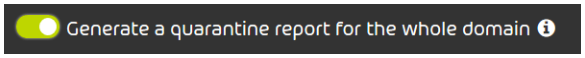
   

   Figure 308: Generate a quarantine report for the whole domain

   The **Recipient address for the quarantine report** field is displayed.
4. **Important:**

   The email address in the field **Recipient address for the quarantine report** may not belong to the recipient of quarantine reports of another customer.

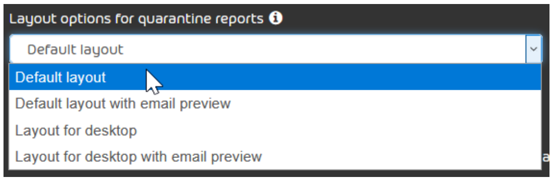
   Optional: Enter the email address to which the quarantine report will be delivered into the field **Recipient address for the quarantine report**.

5. Select a quarantine report layout under **Layout options for quarantine reports**(see Layouts for Quarantine Reports on page 407).

   - **Default layout**
   - **Default layout with email preview**
   - **Inbox Manager with email preview and exclude option**

     > **Important:**
     >
     > This layout is only displayed and can only be selected if the option **Exclude emails by senders from the deny list from quarantine reports** has been enabled in the quarantine reports settings.

   - **Layout for desktop**
   - **Layout for desktop with email preview**



Layout options for quarantine reports ℹ

Default layout

Default layout

Default layout with email preview

Layout for desktop

Layout for desktop with email preview

Figure 309: Select a layout

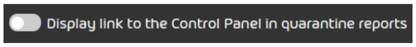
> **Notice:**
>
> Layouts with email preview are not available for quarantine reports that are generated for the whole domain.

> **Notice:**
>
> For more information about the email preview, see chapter "Email Preview" in the Control Panel manual.

6. Optional: If you want to remove references to the Control Panel from quarantine reports, toggle the switch **Display link to the Control Panel in quarantine reports**.

   Notice:

   By default, the Control Panel is referred to in quarantine reports.



○ Display link to the Control Panel in quarantine reports

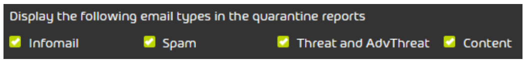
Figure 310: Remove link to Control Panel

➔

The switch is grayed out.

7. Tick the checkboxes of the email types to be displayed in the quarantine reports. You can choose from the following email types.

   - **Infomail**
   - **Spam**
   - **Threat and AdvThreat**
   - **Content**

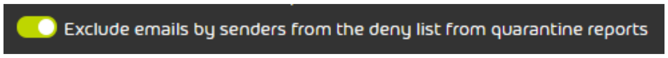


Display the following email types in the quarantine reports

☑ Infomail ☑ Spam ☑ Threat and AdvThreat ☑ Content

Figure 311: Select email types

8. If you would like to exclude emails by senders who are on the recipient's deny list or the deny list of the domain from quarantine reports, toggle the switch **Exclude emails by senders from the deny list from quarantine reports**.



Exclude emails by senders from the deny list from quarantine reports

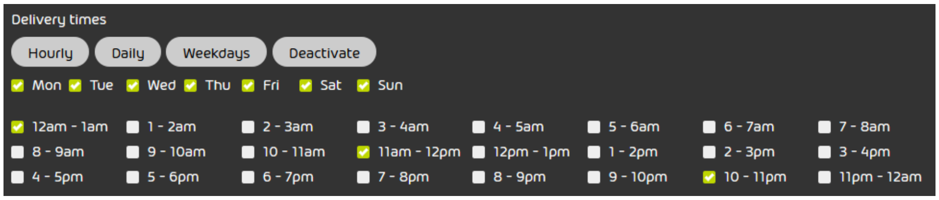
> **Important:**
>
> If a quarantine report is generated for the whole domain (see above), only emails originating from senders who are on the deny list of the domain are excluded. The recipients' deny lists are not taken into account.

Figure 312: Exclude emails by senders from the deny list from quarantine reports.

➜ The switch is activated. The **Inbox Manager with email preview and exclude option** layout is enabled in the **Layout options for quarantine reports** drop-down menu.

9. Under **Delivery times**, select the times at which the quarantine reports shall be delivered. You can tick the checkboxes of the desired days and times or click on the following buttons:

   - **Hourly**: All times are selected.
   - **Daily**: All days are selected.
   - **Weekdays**: All days from Monday to Friday are selected.
   - **Deactivate**: No days or times are selected. The quarantine reports are deactivated for all users of the domain by default.



☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun

☑ 12am - 1am □ 1 - 2am □ 2 - 3am □ 3 - 4am □ 4 - 5am □ 5 - 6am □ 6 - 7am □ 7 - 8am
□ 8 - 9am □ 9 - 10am □ 10 - 11am ☑ 11am - 12pm □ 12pm - 1pm □ 1 - 2pm □ 2 - 3pm □ 3 - 4pm
□ 4 - 5pm □ 5 - 6pm □ 6 - 7pm □ 7 - 8pm □ 8 - 9pm □ 9 - 10pm ☑ 10 - 11pm □ 11pm - 12am

Figure 313: Select times

Notice:

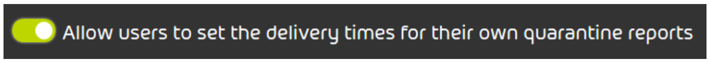
A quarantine report is sent at the selected delivery times only if new emails have been placed in quarantine since the last quarantine report.

10. **Important:**

    By default, the users of the domain receive quarantine reports at the times set for the domain. If delivery times have been selected for the domain, the users cannot change the delivery times for their own quarantine reports by default.

    If no delivery times have been selected, the users can change the delivery times for their own quarantine reports. This permission cannot be revoked.

    Optional: To allow the users of the domain to change the delivery times of their quarantine reports, toggle the switch **Allow users to set the delivery times for their own quarantine reports**.

    Allow users to set the delivery times for their own quarantine reports

    Figure 314: Allow users to change the delivery times

    The switch is highlighted in green.

11. Create a custom text in each language in which quarantine reports are to be delivered (see Creating a Custom Text for Quarantine Reports on page 425).
12. To apply the changes, click on **Save**.

The **Quarantine Report** module has been configured for a domain.

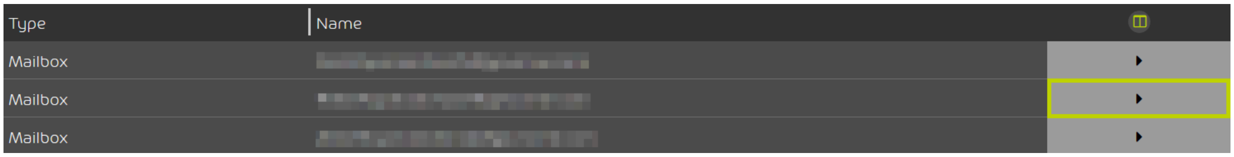
Next, you can configure quarantine reports differently for a mailbox of the domain (see Configuring the Quarantine Report for a Mailbox on page 421).

Configuring the Quarantine Report for a Mailbox

You have activated the **Quarantine Report** module for the domain (see Activating the Quarantine Report for a Domain on page 414). You have configured the **Quarantine Report** module for the domain (see Configuring the Quarantine Report for a Domain on page 416).

In the **Customer Settings** > **Mailboxes** module, you can configure the quarantine reports for a mailbox differently than for the rest of the domain's mailboxes (see Configuring the Quarantine Report for a Domain on page 416).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain of the mailbox for which you want to configure the **Quarantine Report** module.
3. Navigate to **Customer Settings** > **Mailboxes**.
4. Select the mailbox from the list and click on the arrow next to the mailbox.



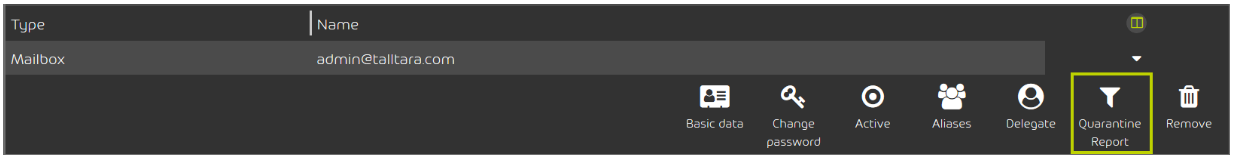
Type	Name	
Mailbox	[redacted]	▸
Mailbox	[redacted]	▸
Mailbox	[redacted]	▸

Figure 315: Display advanced settings

➜

A menu opens.

5. In the menu, click on **Quarantine Report**.



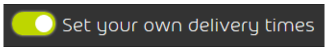
Type	Name
Mailbox	admin@talltara.com

Figure 316: Menu

➜

The settings of the **Quarantine Report** module for the mailbox are displayed. If you have not yet configured the settings of the **Quarantine Report** module for the mailbox, the settings for the domain are displayed here by default.

6. To configure the **Quarantine Report** module for the mailbox, toggle the switch **Set your own delivery times**.



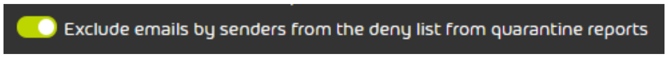
Set your own delivery times

Figure 317: Set your own delivery times

➜

The switch is highlighted in green. You can deactivate the **Quarantine Report** module for your mailbox or change the delivery times of quarantine reports.

7. If you would like to exclude emails by senders who are on the recipient's deny list or the deny list of the domain from quarantine reports, toggle the switch **Exclude emails by senders from the deny list from quarantine reports**.



Exclude emails by senders from the deny list from quarantine reports

Figure 318: Exclude emails by senders from the deny list from quarantine reports

➜

The switch is highlighted in green.

8. If you would like to deactivate the **Quarantine Report** module for the mailbox, activate the button **Deactivate**.

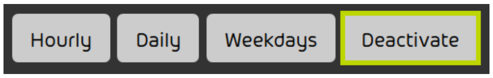


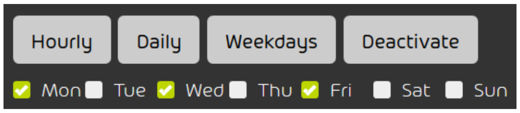
Figure 319: Deactivate the Quarantine Report

➜

All delivery times and delivery days are deactivated for the mailbox. No quarantine reports are delivered to the mailbox. No further adjustments are required.

9. If the **Quarantine Report** module remains activated for the mailbox, select the days on which the quarantine reports shall be delivered. Select at least one day.

   - To deliver quarantine reports every day, activate the button **Daily**.
   - To deliver quarantine reports every day from Monday to Friday, activate the button **Weekdays**.
   - Tick the checkboxes of the desired days.

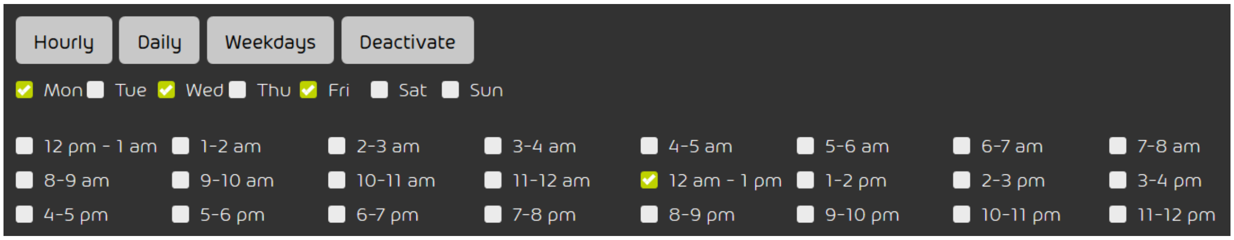


☑ Mon ☐ Tue ☑ Wed ☐ Thu ☑ Fri ☐ Sat ☐ Sun

Figure 320: Select days

10. Select the times at which the quarantine reports shall be delivered. Select at least one time.

    - To deliver quarantine reports every day, activate the button **Hourly**.
    - Tick the checkboxes of the desired times.



☑ Mon ☐ Tue ☑ Wed ☐ Thu ☑ Fri ☐ Sat ☐ Sun

☐ 12 pm - 1 am	☐ 1-2 am	☐ 2-3 am	☐ 3-4 am	☐ 4-5 am	☐ 5-6 am	☐ 6-7 am	☐ 7-8 am
☐ 8-9 am	☐ 9-10 am	☐ 10-11 am	☐ 11-12 am	☑ 12 am - 1 pm	☐ 1-2 pm	☐ 2-3 pm	☐ 3-4 pm
☐ 4-5 pm	☐ 5-6 pm	☐ 6-7 pm	☐ 7-8 pm	☐ 8-9 pm	☐ 9-10 pm	☐ 10-11 pm	☐ 11-12 pm

Figure 321: Select times

Notice:

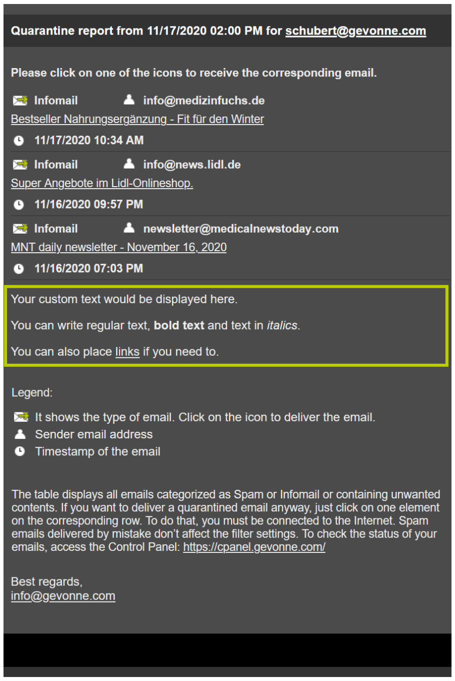
A quarantine report is sent at the selected delivery times only if new emails have been placed in quarantine since the last quarantine report.

The **Quarantine Report** module has been configured for a mailbox.

Creating a Custom Text for Quarantine Reports

You have activated the **Quarantine Report** module (see Activating the Quarantine Report for a Domain on page 414).

In the **Quarantine Report** module (see About Quarantine Report on page 406), you can customize quarantine reports of your domain with a custom text in any language supported by the Control Panel. In the quarantine reports, the text is displayed below the list of emails.



Quarantine report from 11/17/2020 02:00 PM for schubert@gevonne.com

Please click on one of the icons to receive the corresponding email.

Infomail **info@medizinfuchs.de**
Bestseller Nahrungsergänzung - Fit für den Winter
11/17/2020 10:34 AM

Infomail **info@news.lidl.de**
Super Angebote im Lidl-Onlineshop.
11/16/2020 09:57 PM

Infomail **newsletter@medicalnewstoday.com**
MNT daily newsletter - November 16, 2020
11/16/2020 07:03 PM

Your custom text would be displayed here.

You can write regular text, **bold text** and text in *italics*.

You can also place links if you need to.

Legend:

- It shows the type of email. Click on the icon to deliver the email.
- Sender email address
- Timestamp of the email

The table displays all emails categorized as Spam or Infomail or containing unwanted contents. If you want to deliver a quarantined email anyway, just click on one element on the corresponding row. To do that, you must be connected to the Internet. Spam emails delivered by mistake don’t affect the filter settings. To check the status of your emails, access the Control Panel: https://cpanel.gevonne.com/

Best regards,
info@gevonne.com

Figure 322: Example of custom text

1. Log in to the Control Panel with your administrative credentials.
2. Navigate to **Security Settings** > **Quarantine Report**.

3. Toggle the switch **Use custom text in quarantine reports**.

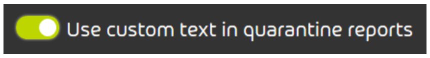


Figure 323: Use custom text

➔

The switch is highlighted in green. The area for creating custom texts is enabled.

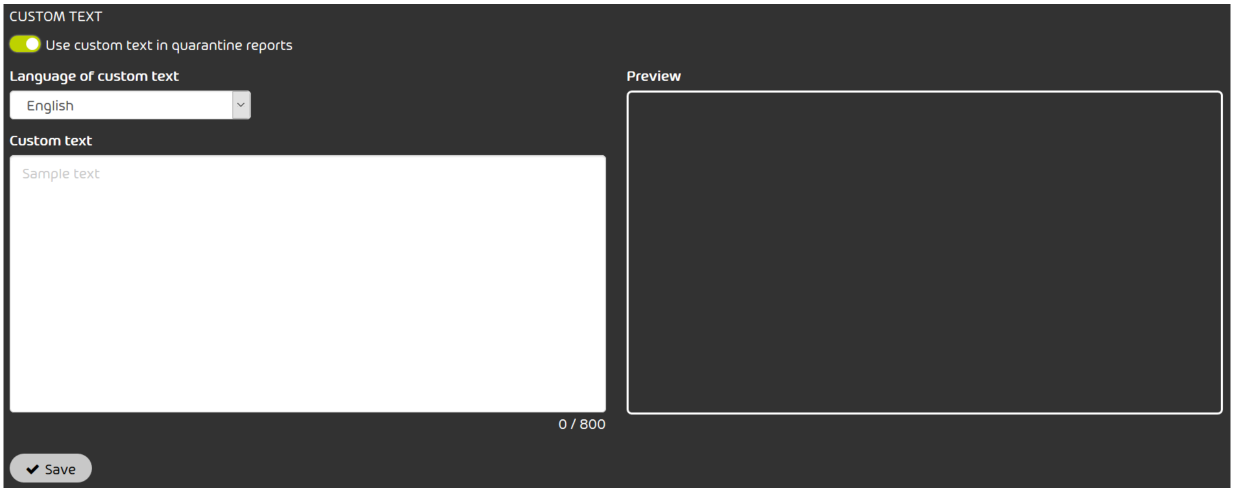


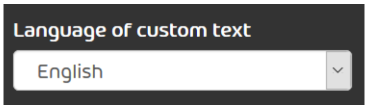
Figure 324: Text editor

4. **Important:**

   Each user receives their quarantine reports in the language that is set under **User Settings** (see Changing the Timezone and Language on page 35). This language can differ from the default language of the domain in the **Service Dashboard** module (see Setting Default Values for Timezone and Language on page 140).

   A custom text can be created for each available language. Custom texts are added to quarantine reports in the same language. If no custom text is available for a language, quarantine reports in this language are sent without a custom text.

   Select the language of the custom text under **Language of custom text**.



Language of custom text

English

Figure 325: Language of custom text

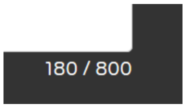
Notice:

If you select a different language while writing a text, the text you have written so far will be preserved as long as you do not leave the page. As soon as you deactivate the **Use custom text in quarantine reports** switch and save the changes, all custom texts in all languages will be erased at once.

5. Create a custom text in the selected language.

Notice:

There is a length limit of 800 characters. You can check the current length by looking at a counter below the input field.



180 / 800

Figure 326: Character count

6. Optional: Format your text as you please. You can use some formatting options of the Markdown markup language.

Notice:

The following formatting options are supported:

- Single asterisks for italics: *Italics*.
- Double asterisks for bold: **Bold**.
- A line break is represented by an empty line. Without this empty line, the quarantine report would display a single line. Example:

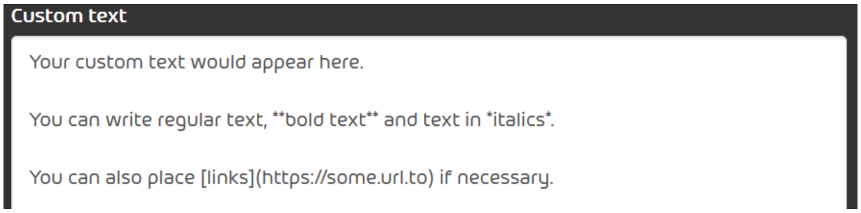
  This is a paragraph. This is another paragraph.
- A bulleted list can be added by starting each list item as a separate line with a hyphen and a space. An empty line between two list elements is optional and increases the spacing between the list elements. However, the first list item must be separated from the preceding text by an empty line. The last list item must also be separated from the following text by an empty line. Example:

  - First list item

  - Second list item

  - Third list item
- Links can be added with square brackets around the displayed text and round brackets for the URL. Example:

  Click [here](https://a.url.tld).



Your custom text would appear here.

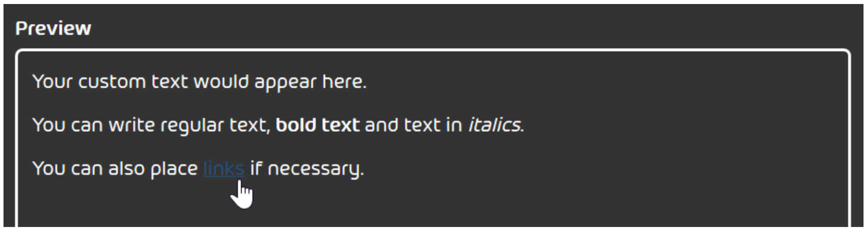
You can write regular text, **bold text** and text in *italics*.

You can also place [links](https://some.url.to) if necessary.

Figure 327: Sample text in the input field

7. Once you have finished your input in all desired languages, save your texts with **Save**.

   Your custom texts will be saved and used for the next delivery of quarantine reports. The preview shows the result in the currently selected language after you have clicked on **Save**.



Preview

Your custom text would appear here.

You can write regular text, **bold text** and text in *italics*.

You can also place links if necessary.

Figure 328: Sample text in preview field

Custom texts have been created for quarantine reports.

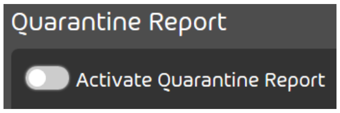
Deactivating the Quarantine Report for a Domain

You have activated the **Quarantine Report** module for the domain (see Activating the Quarantine Report for a Domain on page 414).

If quarantine reports shall no longer be generated for the mailboxes of a domain, you can deactivate the **Quarantine Report** module (see About Quarantine Report on page 406) for that domain.

1. Log in to the Control Panel with your administrative credentials.
2. Select a domain from the scope selection.
3. Navigate to **Security Settings** > **Quarantine Report**.

4. Toggle the switch **Activate Quarantine Report**.



Quarantine Report

Activate Quarantine Report

Figure 329: Deactivate the Quarantine Report

➜

The switch is grayed out.

✓

The **Quarantine Report** module has been activated for a domain.

Delivering an Email from a Quarantine Report

✓ You have activated the **Quarantine Report** module for the domain (see Activating the Quarantine Report for a Domain on page 414).

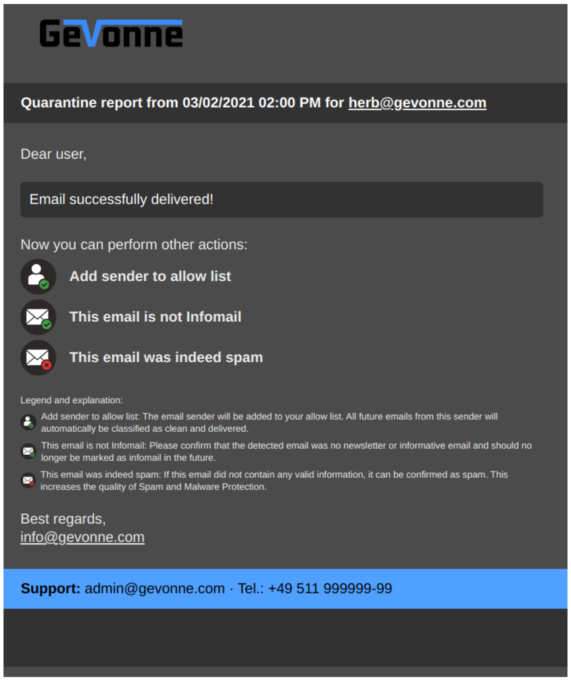
You can deliver emails that are listed in quarantine reports (see About Quarantine Report on page 406).

1. Open the quarantine report in your email client.
2. In the quarantine report, select the email to be delivered.

3. Click on **Deliver**.

➜

The email is delivered to the recipient. A delivery notification is displayed in the browser.



Quarantine report from 03/02/2021 02:00 PM for herb@gevonne.com

Dear user,

Email successfully delivered!

Now you can perform other actions:

- **Add sender to allow list**
- **This email is not Infomail**
- **This email was indeed spam**

Legend and explanation:

- Add sender to allow list: The email sender will be added to your allow list. All future emails from this sender will automatically be classified as clean and delivered.
- This email is not Infomail: Please confirm that the detected email was no newsletter or informative email and should no longer be marked as infomail in the future.
- This email was indeed spam: If this email did not contain any valid information, it can be confirmed as spam. This increases the quality of Spam and Malware Protection.

Best regards,
info@gevonne.com

Support: admin@gevonne.com · Tel.: +49 511 999999-99

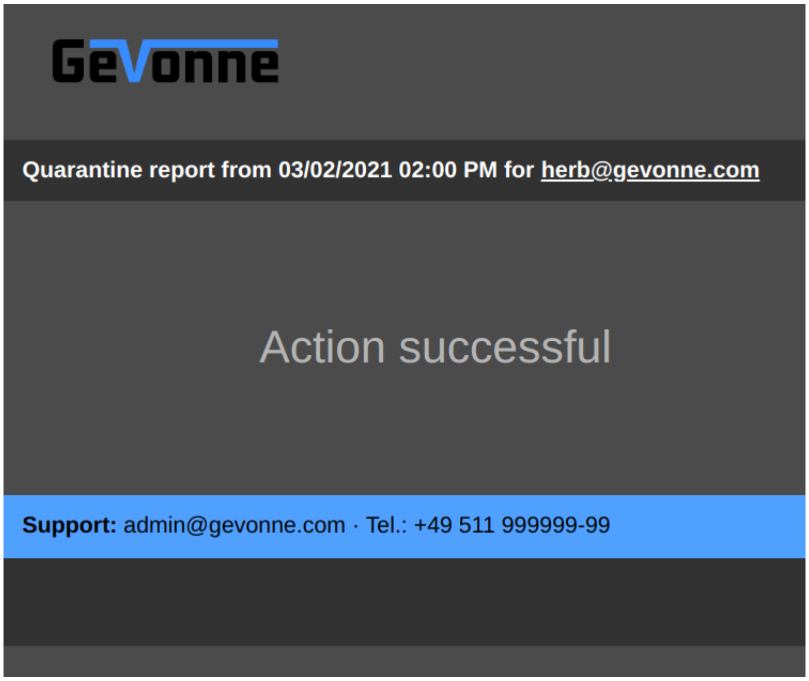
Figure 330: Delivery notification

Notice:

Quarantine reports are generated for each primary mailbox. If alias mailboxes are assigned to a primary mailbox, emails to these alias mailboxes will be listed on a single quarantine report together with the emails addressed to the primary mailbox. Once an email is delivered from a quarantine report, the mailbox to which the email is addressed is displayed at the top of the delivery notification.

4. Click on one of the advanced options:
   - **Add sender to allow list**: The sender is added to the user's allow list.
   - **This email is not Infomail**: The email is reclassified as **Clean**.
   - **This email was indeed spam**: The email is reclassified as **Spam** if it was previously classified as infomail.

The selected action is performed. Instead of the delivery notification, a confirmation is displayed in the browser.



GeVonne

Quarantine report from 03/02/2021 02:00 PM for herb@gevonne.com

Action successful

Support: admin@gevonne.com · Tel.: +49 511 999999-99

Figure 331: Confirmation window

5. Close the delivery notification.

An email from a quarantine report has been delivered.

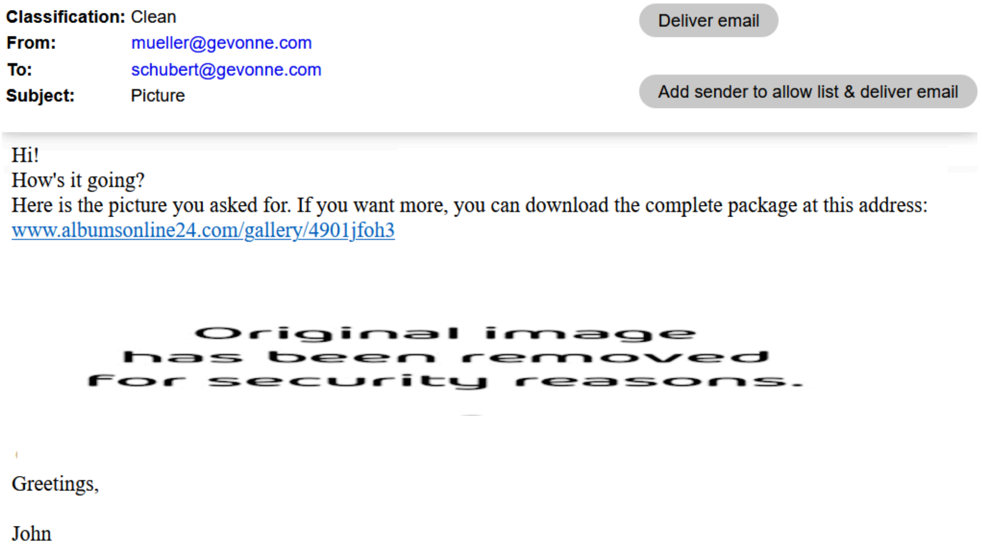
Displaying an Email Preview

You can display a preview for emails listed in quarantine reports (see About Quarantine Report on page 406) if you are their owner. For more information about the email preview, see chapter "Email Preview" in the Control Panel manual.

1. Open the quarantine report in your email client.
2. Select the email you would like to preview.
3. Click on **Preview**.

   ➔

   A simplified preview of the email is displayed in the browser.



Classification: Clean
From: mueller@gevonne.com
To: schubert@gevonne.com
Subject: Picture

Hi!
How's it going?
Here is the picture you asked for. If you want more, you can download the complete package at this address:
www.albumsonline24.com/gallery/4901jfoh3

Original image
has been removed
for security reasons.

Greetings,

John

Figure 332: Email preview

4. Close the email preview.

✓

A preview for an email from a quarantine report has been displayed.

Spam and Malware Protection

Spam and Malware Protection

Spam and Malware Protection is a service that blocks spam and emails containing viruses before they enter the recipient's mailbox. Furthermore, infomail (e.g., newsletters) can be detected and, depending on the settings, be delivered, put in quarantine or tagged.

With the following features, Spam and Malware Protection offers protection against threats, spam and infomail:

- Virus analysis of emails with automatic updates of the virus signatures and an early alert system for new and yet unknown viruses.
- Link tracking: Incoming and outgoing emails are automatically checked for malicious URLs.
- Phishing mail detection: Different mechanisms, such as link tracking and malicious script command detection, prevent phishing attacks.
- Outbound filtering: Outgoing emails are checked for spam and viruses in order to prevent the customer from involuntarily sending or forwarding malware and spam.
- Bounce management: Spam and Malware Protection rejects bounce messages that are sent in return to spam with fake sender addresses.

The following settings related to Spam and Malware Protection can be configured under **Security Settings** > **Spam and Malware Protection**:

- Activating Spam and Malware Protection (see **Activating Spam and Malware Protection** on page 437)
- Adjusting the Primary Environment Settings (see **Primary Environment Settings** on page 440)
- Configuring the handling of spam and infomail (see **Email Filter Settings** on page 446)
- Allowing and Forbidding User Actions (see **Allowing and Forbidding User Actions** on page 454)
- Deactivating Spam and Malware Protection (see **Deactivating Spam and Malware Protection** on page 455)

Spam and Malware Protection allows the administrator to decide how spam and infomail are handled (see **Email Filter Settings** on page 446). If emails have been classified incorrectly, users can trigger the delivery of spam and infomail under **Email Live Tracking** (see Email Actions on page 87), depending on the administrator's settings.

Furthermore, the services **Content Control** (see About Content Control on page 458) and **Compliance Filter** (see About the Compliance Filter on page 472) are part of Spam and Malware Protection and can be activated if desired. The order of rules (see Order of Rules Across All Services on page 435) shows the order of filters for all services.

Order of Rules Across All Services

The rules of Spam and Malware Protection (see "Spam and Malware Protection" in the Control Panel manual) are processed according to specific priorities. Once a rule with a higher priority applies, no rules with lower priorities are processed. This can lead to emails being blocked despite an allow list entry having been set for its sender's address because the IPv4 address of the sending server is on the RBL deny list.

Rule order (from top to bottom in descending priority):

Incoming emails

1. RBL list (block)
2. Mass spam detection (block)
3. Compliance Filter
4. Check for malicious content (quarantine)
5. Content Control if activated (quarantine)
6. User-based allow list (deliver)
7. User-based deny list (quarantine)

8. Administrative allow list (deliver)

   Notice:

   The administrative allow list is a special case among the rules. This is because administrators can select which filters will be bypassed by allow list entries at domain level (see "Creating a Deny List Entry for a Domain" in the Control Panel manual). While being processed, the affected emails thus skip the selected filters. This also applies to filters that are listed before the administrative allow list. The position where the administrative allow list is placed in the list refers to the default configuration of allow list entries at domain level. By default, the entries only bypass spam filtering.

9. Administrative deny list (quarantine)

10. General allow list (deliver)

11. General spam rules (quarantine)

12. Infomail filter (quarantine)

Notice:

The Compliance Filter (see **About the Compliance Filter** on page 472) is applied before Content Control (see **About Content Control** on page 458). This allows administrators to create exceptions for Content Control with filter rules of the Compliance Filter that categorize emails as **Clean**.

For Content Control, exceptions can neither be created using user-based allow and deny lists nor administrative deny lists because these rules are applied after Content Control. Only administrative allow lists can be used to bypass Content Control.

Outgoing emails

1. RBL list

2. Compliance Filter

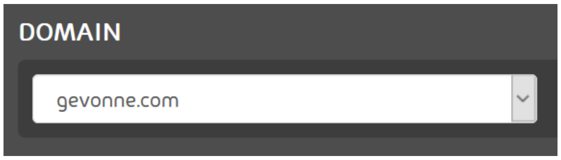
3. Check for malicious content

4. Content Control if activated

Activating Spam and Malware Protection

In the **Security Settings** > **Spam and Malware Protection** module, you can activate Spam and Malware Protection (see Spam and Malware Protection on page 434) for a domain.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to activate Spam and Malware Protection.
3. Navigate to **Security Settings** > **Spam and Malware Protection**.
4. Under **Domain**, select the domain for which you would like to activate Spam and Malware Protection.



DOMAIN

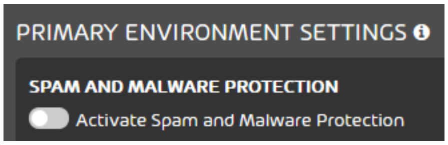
gevonne.com

Figure 333: Select domain

Notice:

Spam and Malware Protection can only be configured for alias domains if it is activated for the corresponding primary domain. By default, the settings of the primary domain are inherited to the alias domains.

5. Toggle the switch **Activate Spam and Malware Protection** under **Primary Environment Settings**.



PRIMARY ENVIRONMENT SETTINGS

SPAM AND MALWARE PROTECTION

Activate Spam and Malware Protection

Figure 334: Activate Spam and Malware Protection

➔

A confirmation window is displayed.

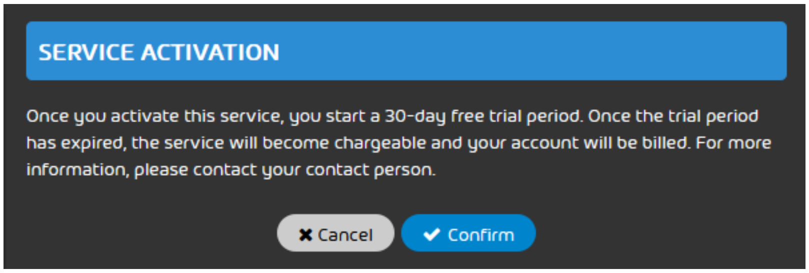
6. **Attention:**

   Once Spam and Malware Protection is activated, a 30-day free trial period starts. Once the trial period has expired, the service becomes chargeable and your account is billed.

   Important:

   Administrators cannot deactivate Spam and Malware Protection for a primary domain by themselves. Only Support can deactivate Spam and Malware Protection for the primary domain.

   Click on **Confirm**.



SERVICE ACTIVATION

Once you activate this service, you start a 30-day free trial period. Once the trial period has expired, the service will become chargeable and your account will be billed. For more information, please contact your contact person.

Figure 335: Confirm

The switch turns green and additional control elements are unlocked under **Primary Environment Settings** and **Email Filter Settings**.

7. Optional: If you want to adjust the environment settings and the email filter settings before Spam and Malware Protection is activated, you can adjust the settings now (see Adjusting the Primary Environment Settings on page 441 and Email Filter Settings on page 446).
8. Click on **Save**.

Spam and Malware Protection has been activated for the domain.

Next, you can adjust the settings of your primary environment (see Primary Environment Settings on page 440) and configure email filter settings (see Email Filter Settings on page 446).

Primary Environment Settings

In the **Spam and Malware Protection** module (see Spam and Malware Protection on page 434), the primary environment settings of a customer domain are managed.

Spam and Malware Protection requires several primary environment settings related to receiving and sending emails. Under **Primary Environment Settings**, customer-level administrators can set the destination of incoming emails, specify IPv4 addresses for other relay servers, activate the bounce management and configure the user check.

For more clarity, the available options are explained below. More configuration details are described under Adjusting the Primary Environment Settings on page 441.

- **Destination**: Under **Destination**, you must enter the destination of incoming emails which are to be processed by Spam and Malware Protection. The following options are available:
  - **IP/Hostname**: This is the standard option. It refers to the customer's email servers. Either the corresponding IPv4 addresses or the corresponding hostnames must be specified. If you enter a hostname, an MX record resolution is performed first, followed by an A record resolution.
- **IP addresses of relay servers for outgoing emails**: If Spam and Malware Protection is activated, outgoing emails are filtered, too. Under **IP addresses of relay servers for outgoing emails**, you can specify the IPv4 addresses of the customer's relay servers from which outgoing emails are sent to our servers so that Spam and Malware Protection can verify if an email was in fact sent by the customer.

  Here, you can enter several addresses with suffixes not longer than /24 for relay servers, separated from each other by commas. There is a length limit of 65,535 characters. It is also possible to enter CIDR ranges. If an email is sent from one of the specified IP addresses, Spam and

Malware Protection intervenes. If this option is disabled, Spam and Malware Protection filters all outgoing emails from the email addresses of the domain.

Important:

The relay server IP addresses specified here are also required for signing and encrypting emails with Signature and Disclaimer. If no addresses are specified, neither of the services will be able to process any emails. Even if these services are not used, we recommend customer-level administrators to specify their relay server IP addresses here.

- **Restrict email sending to the relay server IP addresses**: This setting ensures that outgoing emails from email addresses of the domain are only sent via our infrastructure if they have been sent from one of the entered relay server addresses.
- **Bounce management (recommended)**: Bounce management is a feature that checks incoming bounce messages to determine whether the emails that prompted them were actually sent via the domain's relay servers or via a fake sender address as the result of a spam attack. In the second case, the bounce messages are rejected.
- **User check**: With the user check, Spam and Malware Protection checks if the recipient addresses of incoming emails exist. If the recipient address of an email does not exist, Spam and Malware Protection rejects the email. This prevents our mail servers from accepting emails addressed to non-existing recipients under our customers' domains, which could be exploited for DDoS attacks. The user check can be based on the users lists of the Control Panel or it can be carried out by directly sending an SMTP request to the email servers of a customer's domain that are specified under **Destination**.

Adjusting the Primary Environment Settings

You have activated Spam and Malware Protection.

Spam and Malware Protection (see **Spam and Malware Protection** on page 434) requires several primary environment settings related to receiving and sending emails. For more information about the functions, see **Primary Environment Settings** on page 440.

1. Log in to the Control Panel with your administrative credentials.

2. From the scope selection, select the domain for which you would like to adjust the primary environment settings.
3. Navigate to **Security Settings** > **Spam and Malware Protection**.
4. Under **Domain**, select the domain for which you would like to adjust the primary environment settings.
5. Optional: If you have selected an alias domain that inherits the settings from the primary domain, toggle the **Inherit from primary domain** switch.

   ➜

   The switch is grayed out. The settings in the module are enabled.
6. Under **Destination**, set the destination server of incoming emails. You have the following options:
   - If you have your own email server, tick the **IP/Hostname** checkbox and enter the IPv4 address or the hostname of the destination server in the field. Enter at least one IPv4 address or hostname. Optionally, you can also enter the port number and priority. Follow the input format **IPv4/Hostname:Port#Priority** and use a semicolon to separate multiple entries from each other.

Notice:

This destination server is called the primary environment in the Control Panel. By default, the inbound email traffic of the mailboxes of the domain is routed to the primary environment. To route the inbound email traffic of an individual mailbox to a different destination server instead, the mailbox can be assigned a secondary environment (see "Secondary Environments" in the Control Panel manual) instead of the primary environment (see Changing an Environment on page 252).

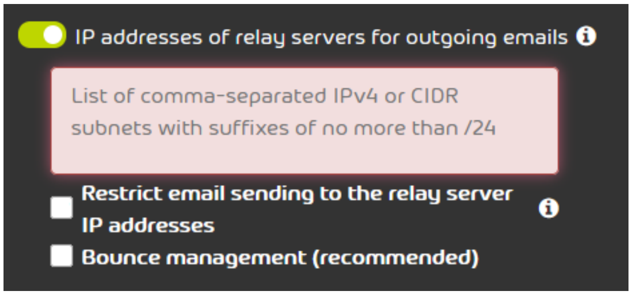
7. **Notice:**

   This step is optional but highly recommended. The relay IP addresses specified under **IP addresses of relay servers for outgoing emails** are also required for signing emails with Signature and Disclaimer. If no addresses are specified, neither of the services will be able to process any emails.

   Optional: If you want to enter the IP addresses of your relay servers manually, toggle the switch **IP addresses of relay servers for outgoing emails**.

   ➜

   An input field for IPv4 addresses is displayed.



IP addresses of relay servers for outgoing emails

List of comma-separated IPv4 or CIDR subnets with suffixes of no more than /24

□ Restrict email sending to the relay server IP addresses

□ Bounce management (recommended)

Figure 336: Define relay server IP addresses for outgoing emails

8. Optional: Enter the IPv4 addresses of your relay servers in the field under the switch **IP addresses of relay servers for outgoing emails**. If the switch is on, this field may not remain empty.

   Notice:

   Here, you can enter several relay server IPv4 addresses with suffixes no larger than /24, separated from each other by commas. The field may only contain up to 65,535 characters.

9. Optional: To ensure that outgoing emails from the domain are sent exclusively via the entered relay server IP addresses, tick the checkbox **Restrict email sending to the relay server IP addresses**.

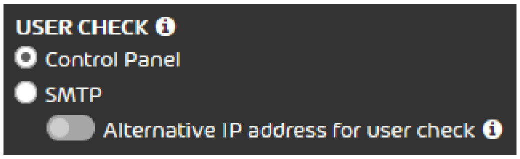
> **Notice:**
>
> This setting is activated by default. The setting ensures that outgoing emails from the domain's email addresses are only sent via our infrastructure if they have been sent from one of the entered relay server IPv4 addresses.

10. Optional: If you want to activate bounce management to prevent incorrect bounce messages, tick the checkbox **Bounce management (recommended)**.

11. **Notice:**

    This step is only possible for customers who have selected **IP/Hostname** as the destination of their primary environment.

    Optional: Set up the user check under the section **User check**. You have the following options:



USER CHECK

● Control Panel

○ SMTP

Alternative IP address for user check

Figure 337: Set up user check

- **Control Panel**: If you tick this checkbox, Spam and Malware Protection checks whether the recipient address is listed in the user list of the Control Panel. This setting prevents the automatic creation of mailboxes in the Control Panel (see Mailboxes on page 210).

  Notice:

  If this option is selected, all desired mailboxes and their alias addresses must be available in the Control Panel. Mailboxes can either be added manually to the Control Panel or synchronized with a directory service via LDAP.

- **SMTP**: If you tick this checkbox, Spam and Malware Protection checks the recipient address using an SMTP callback. To do so, Spam and Malware Protection asks the destination server of the recipient address whether the recipient address is valid. Usually, the destination server is determined on the basis of the domain part. If you would like to use a different destination server for the user check with SMTP, toggle the switch **Alternative IP address for user check** and enter the IPv4 address in the input field. You can enter an IPv4 or CIDR subnet.

  Notice:

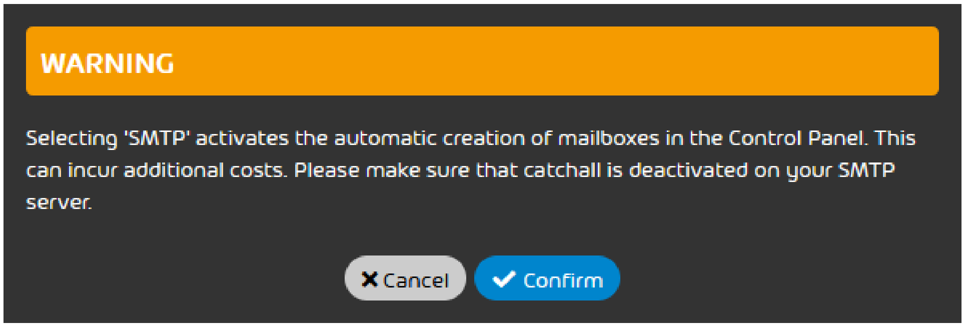
  Please contact Support if the user check causes any problems.

12. Click on **Save**.

    ➜

    If the **SMTP** option has been selected for the user check, a warning message is displayed. Otherwise, the settings are saved.

13. If you have selected the **SMTP** option for the user check, click on **Confirm**.



WARNING

Selecting 'SMTP' activates the automatic creation of mailboxes in the Control Panel. This can incur additional costs. Please make sure that catchall is deactivated on your SMTP server.

Figure 338: Confirm

➜

The settings are saved.

✓

The primary environment settings of Spam and Malware Protection have been adjusted.

Next, you can adjust the email filter settings (see Email Filter Settings on page 446) or allow or forbid user actions (see Allowing and Forbidding User Actions on page 454).

Email Filter Settings

In the **Email Filter Settings** section of the **Spam and Malware Protection** module (see Spam and Malware Protection on page 434), customer-level administrators can make various settings for the email filter.

Under **Security Settings** > **Spam and Malware Protection** > **Email Filter Settings**, customer-level administrators have the following options:

- Configuring the handling of spam (see **Configuring the Handling of Spam** on page 447).
- Activating the infomail filter (see **Activating the Infomail Filter** on page 449).
- Configuring the infomail filter (see **Configuring the Infomail Filter** on page 450).
- Configuring the handling of infomail (see **Configuring the Handling of Infomail** on page 451).

Configuring the Handling of Spam

You have activated **Spam and Malware Protection** (see Activating Spam and Malware Protection on page 437).

Under **Spam Handling** in the **Spam and Malware Protection** module (see Spam and Malware Protection on page 434), you can decide how to handle spam messages that have been filtered out by the email filter.

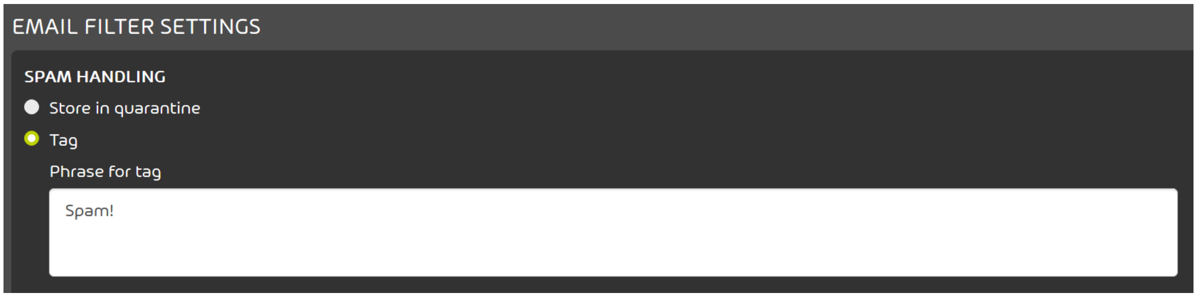
1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to configure the handling of spam.
3. Navigate to **Security Settings** > **Spam and Malware Protection**.
4. Under **Domain**, select the domain for which you would like to configure the handling of spam.
5. Optional: If you have selected an alias domain that inherits the settings from the primary domain, toggle the **Inherit from primary domain** switch.

   ➜

   The switch is grayed out. The settings in the module are enabled.

6. Select the desired option for spam handling under **Email Filter Settings** > **Spam Handling**. You have two options:

   - If you want to store spam messages in quarantine, select **Store in quarantine**. For emails stored in quarantine, the module **Email Live Tracking** offers several actions.
   - If you want to tag emails with a personalized phrase, select **Tag**. After that, the input field **Phrase for tag** is displayed. Enter the phrase with which spam messages shall be tagged.



EMAIL FILTER SETTINGS

SPAM HANDLING

○ Store in quarantine

● Tag

Phrase for tag

Spam!

Figure 339: Tag spam

Notice:

Emails classified as **Spam** are only displayed in quarantine reports (see chapter "About Quarantine Report" in the Control Panel manual) if they have been put in quarantine and the email category has been selected to be displayed in quarantine reports (see chapter "Configuring the Quarantine Report for a Domain" in the Control Panel manual).

7. Click on **Save**.

✓

The handling of spam has been configured.

Next, you can configure the handling of infomail (see Activating the Infomail Filter on page 449) or allow or forbid user actions (see Allowing and Forbidding User Actions on page 454).

Activating the Infomail Filter

You have activated **Spam and Malware Protection**(see Activating Spam and Malware Protection on page 437).

Under **Infomail Filter Settings** in the **Spam and Malware Protection** module (see Spam and Malware Protection on page 434), you can activate the infomail filter for a primary domain and make other settings. The settings will also apply to the alias domains of the primary domain.

The infomail filter detects infomail and carries out different actions, depending on the settings. The infomail filter is one of the email filter's features of **Spam and Malware Protection**. To use the infomail filter, you have to activate it first.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to activate the infomail filter.
3. Navigate to **Security Settings** > **Spam and Malware Protection**.
4. Under **Domain**, select the primary domain for which you would like to activate the infomail filter.
5. Toggle the switch **Activate infomail filter**.

   ➜

   The switch turns green and a form containing more settings is displayed.
6. Click on **Save**.

✓

The infomail filter has been activated for a primary domain and its alias domains.

Next, you can configure the infomail filter (see Configuring the Infomail Filter on page 450).

Configuring the Infomail Filter

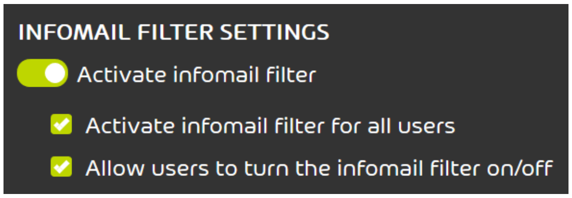
You have activated **Spam and Malware Protection** and the infomail filter (see Activating Spam and Malware Protection on page 437 and Activating the Infomail Filter on page 449).

Under **Infomail Filter Settings** in the **Spam and Malware Protection** module (see "Spam and Malware Protection" in the Control Panel manual), you can configure the infomail filter to define its scope for a customer. The settings apply both to the customer's primary domain and their alias domains.

You can either activate or deactivate the infomail filter by default for all users of the customer. Furthermore, you can specify whether users can turn the infomail filter on and off (see "Configuring Quarantine Reports" in the Control Panel manual). This way, users can decide themselves whether they would like to use the infomail filter.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to configure the infomail filter.
3. Navigate to **Security Settings** > **Spam and Malware Protection**.
4. Under **Domain**, select the primary domain for which you would like to configure the infomail filter.
5. If you would like to activate the infomail filter by default for all users of the customer, tick the **Activate infomail filter for all users** checkbox under **Email Filter Settings** > **Infomail Filter Settings**.
6. If you would like to allow the customer's users to turn the infomail filter on and off, tick the **Allow users to turn the infomail filter on/off** checkbox. If the checkbox is ticked, users are allowed to activate and deactivate the infomail filter under **User settings** > **Filter & Reports** (see "Configuring Quarantine Reports" in the Control Panel manual). By combining the two checkboxes, you have the following options:
   - **Activate infomail filter for all users** activated, **Allow users to turn the infomail filter on/off** deactivated: The infomail filter is activated for all users. The users cannot turn off the infomail filter.

- **Activate infomail filter for all users** activated, **Allow users to turn the infomail filter on/off** deactivated: The infomail filter is activated for all users by default. The users can turn off the infomail filter.
- **Activate infomail filter for all users** deactivated, **Allow users to turn the infomail filter on/off** activated: The infomail filter is deactivated for all users by default. The users can turn on the infomail filter.
- **Activate infomail filter for all users** deactivated **Allow users to turn the infomail filter on/off** deactivated: The infomail filter is deactivated for all users. The users cannot turn on the infomail filter. As soon as you apply the changes, the switch **Activate infomail filter** turns gray and the advanced settings disappear.



INFOMAIL FILTER SETTINGS

Activate infomail filter

☑ Activate infomail filter for all users

☑ Allow users to turn the infomail filter on/off

Figure 340: Configure the infomail filter

7. Click on **Save**.

✓

The infomail filter has been configured.

Next, you can configure the handling of infomail (see Configuring the Handling of Infomail on page 451) or allow or forbid user actions (see Allowing and Forbidding User Actions on page 454).

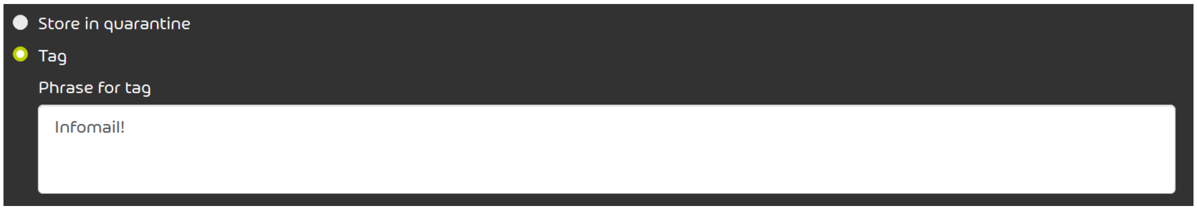
Configuring the Handling of Infomail

You have activated **Spam and Malware Protection** and the infomail filter (see Activating Spam and Malware Protection on page 437 and Activating the Infomail Filter on page 449).

Under **Infomail Filter Settings** in the **Spam and Malware Protection** module (see Spam and Malware Protection on page 434), you can decide how to handle infomail messages that have been filtered out by the email filter.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to configure the handling of infomail.
3. Navigate to **Security Settings** > **Spam and Malware Protection**.
4. Under **Domain**, select the domain for which you would like to configure the handling of infomail.
5. Optional: If you have selected an alias domain that inherits the settings from the primary domain, toggle the **Inherit from primary domain** switch.

6. Select the desired option for infomail handling under **Email Filter Settings** > **Infomail Filter Settings**. You have two options:
   - If you want to store infomail messages in quarantine, select **Store in quarantine**. For emails stored in quarantine, the module **Email Live Tracking** (see Email Live Tracking on page 58) offers several actions (see Email Actions on page 87).
   - If you want to tag infomail messages with a personalized phrase, select **Tag**. After that, the input field **Phrase for tag** is displayed. Enter the phrase with which infomail messages shall be tagged therein.



○ Store in quarantine
● Tag
Phrase for tag
Infomail!

Figure 341: Tag infomail

Notice:

Regardless of this setting, all emails categorized as **Infomail** will be listed in quarantine reports. This only applies if you have activated the infomail filter and have selected emails categorized as **Infomail** to be displayed in quarantine reports (see Configuring the Quarantine Report for a Domain on page 416).

7. Click on **Save**.

Infomail handling has been configured.

Next, you can allow or forbid user actions (see Allowing and Forbidding User Actions on page 454).

Allowing and Forbidding User Actions

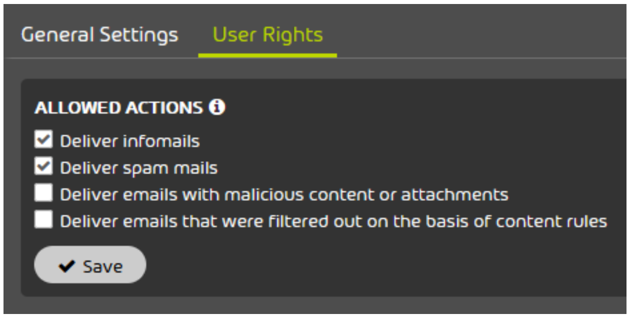
Under **User Rights** in the **Spam and Malware Protection** module (see Spam and Malware Protection on page 434), you can allow or forbid the users of your domain to perform actions on emails intercepted by Spam and Malware Protection.

In the **Email Live Tracking** module (see Email Live Tracking on page 58) and the quarantine reports (see About Quarantine Report on page 406), some actions are available to the users in order to deliver their own emails intercepted by Spam and Malware Protection. You can allow or forbid these actions. Regardless of these settings, administrators at the customer level can deliver all emails from the **Email Live Tracking** module.

1. Log in to the Control Panel with your administrative credentials.
2. Select a domain from the scope selection.
3. Navigate to **Security Settings** > **Spam and Malware Protection**.
4. Select the tab **User rights**.

   ➔

   The tab **User rights** opens.



ALLOWED ACTIONS

☑ Deliver infomails

☑ Deliver spam mails

☐ Deliver emails with malicious content or attachments

☐ Deliver emails that were filtered out on the basis of content rules

Figure 342: User rights

5. Under **Allowed actions**, tick the checkboxes of the actions you want to allow the users of the domain to perform. Untick the checkboxes of the actions you want to forbid the users of your domain to perform. Following actions are available:

   - **Deliver infomails**.
   - **Deliver spam mails**.
   - **Deliver emails with malicious attachments**.
   - **Deliver emails that were filtered out on the basis of content rules**.

   Notice:

   Regardless of these settings, users cannot deliver emails classified as **AdvThreat**. Only administrators and users with the **Service Desk** role can deliver emails from this category.

6. Click on **Save**.

User actions on emails intercepted by Spam and Malware Protection have been allowed or forbidden.

Next, you can activate the infomail filter (see Activating the Infomail Filter on page 449).

Deactivating Spam and Malware Protection

You have activated Spam and Malware Protection (see Spam and Malware Protection on page 434) for a primary domain. You have reset the MX records in the DNS zone of your domain so that they point to your email server again.

If you no longer want to use Spam and Malware Protection, you can deactivate Spam and Malware Protection for your alias domains by yourself in the Control Panel and ask support to deactivate it for the primary domain. The settings will be kept in case you want to reactivate Spam and Malware Protection later.

Warning:

If Spam and Malware Protection is deactivated and the MX records in the DNS zone of your domain have not been reset to point to your email server beforehand, your incoming emails will not be forwarded to your email server and may be lost.

Before deactivating Spam and Malware Protection, make sure that the MX records in the DNS zone of your domain point to your email server.

DANGER:

Once Spam and Malware Protection is deactivated, the following services can no longer be used even if they appear to be activated in the Control Panel:

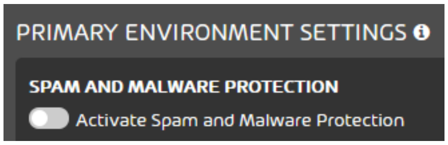
- Advanced Threat Protection (see Structure and Functions of ATP on page 349)
- Compliance Filter (see About the Compliance Filter on page 472)
- Content Control (see About Content Control on page 458)
- Continuity Service (see About the Continuity Service on page 588)
- Email Authentication (see About Email Authentication on page 373)
- Quarantine Report (see About Quarantine Report on page 406)

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the primary for which and for whose alias domains you would like to deactivate Spam and Malware Protection.
3. Navigate to **Security Settings** > **Spam and Malware Protection**.

4. Under **Domain**, select an alias domain with custom settings for which you would like to deactivate Spam and Malware Protection.

> **Notice:**
>
> For alias domains that inherit the Spam and Malware Protection settings from the primary domain, Spam and Malware Protection is automatically deactivated once it is deactivated for the primary domain. Therefore, it is not necessary to deactivate Spam and Malware Protection separately for these alias domains.

5. Toggle the switch **Activate Spam and Malware Protection** under **Primary Environment Settings**.



PRIMARY ENVIRONMENT SETTINGS ℹ

SPAM AND MALWARE PROTECTION

○ Activate Spam and Malware Protection

Figure 343: Deactivate Spam and Malware Protection

➜ The switch is grayed out.

6. Click on **Save**.

➜ Spam and Malware Protection is deactivated for the alias domain.

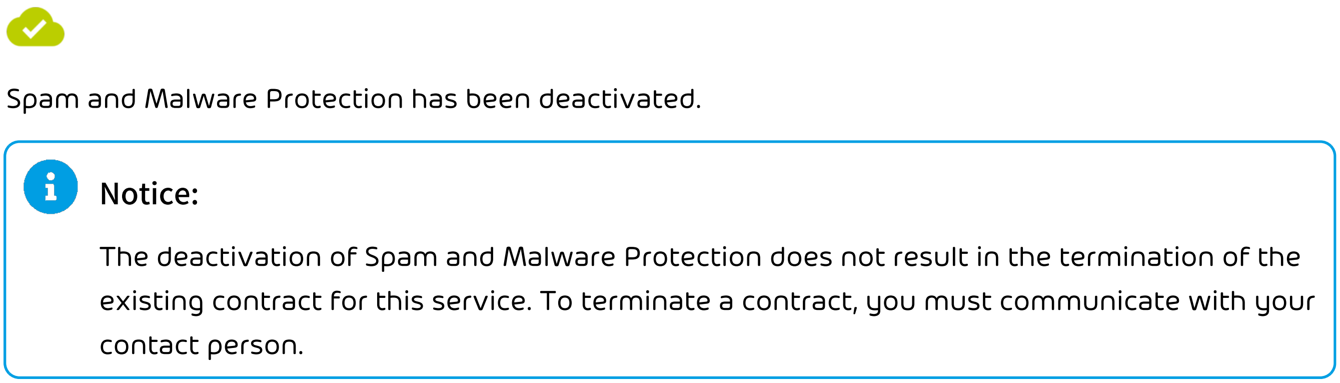
7.

> **Important:**
>
> Once Spam and Malware Protection is deactivated for the primary domain, the Spam and Malware Protection settings of the alias domains can no longer be modified. Thus, make sure that Spam and Malware Protection is configured correctly for the alias domains before Spam and Malware Protection is deactivated for the primary domain.

Tell support or your contact person that you want to deactivate Spam and Malware Protection for the primary domain.

➜

Support handles the deactivation request.



Spam and Malware Protection has been deactivated.

Notice:

The deactivation of Spam and Malware Protection does not result in the termination of the existing contract for this service. To terminate a contract, you must communicate with your contact person.

Content Control

About Content Control

Content Control allows customer-level administrators to manage the handling of attachments of incoming and outgoing emails.

Before Content Control can be used, a customer-level administrator must activate Content Control (see Activating Content Control on page 460). After that, customer-level administrators can configure Content Control (see Configuring Content Control on page 463).

Customer-level administrators can define a maximum allowed email size. Emails that exceed this size are filtered out. Furthermore, administrators can choose which attachment types shall be filtered out. The following attachment types can be selected:

- Encrypted attachments
- Executable attachments
- Office files with macros

Additionally, administrators can forbid file types based on their file extension. Forbidden file types can be defined both for directly attached files and for files in archives. Moreover, categories (see Overview of Categories on page 459) can be used to forbid several file types at once.

Customer-level administrators can choose whether the filtered-out attachments are stored in quarantine or whether the emails are delivered to the recipients without attachments. In the second case, the recipients are notified that the attachments have been cut off.

Settings can be made either for all mailboxes of the domain or for groups of mailboxes (see "Groups" in the Control Panel manual). To configure settings for a group, the group must be added to Content Control (see Adding a Group to Content Control on page 461). In Content Control, groups are sorted according to their priority and processed in this order. If a mailbox belongs to several groups, the settings of the group with the highest priority are applied to it. Administrators can change the priorities of the groups (see Changing Priorities of Groups on page 468). If the general settings of the domain shall be applied to the mailboxes of a group again, administrators can remove the group from Content Control (see Removing a Group from Content Control on page 470).

Overview of Categories

The following table shows the categories by which customer-level administrators can filter out groups of file types in attachments using Content Control (see About Content Control on page 458).

CATEGORY	FILTERED OUT FILE TYPES
.executable	.action .apk .app .bas .bat .bin .cab .chm .cmd .com .command .cpl .csh .dll .exe .gadget .hta .inf .ins .inx .ipa .isu .job .jar .js .jse .ksh .lnk .msc .msi .msp .mst .osx .paf .pcd .pif .prg .ps1 .reg .rgs .run .scr .sct .sh .shb .shs .u3p .vb .vba .vbe .vbs .vbscript. vbx .workflow .ws .wsc .wsf .wsh
.mediafile	.aif .flv .mp1 .mid .mp5 .mpa .wma .mp2 .mpe .swf .wmf .wav .mp4 .wmv .mpg .avi .mov .mp3 .mpv2 .mp2v .aiff .mpeg
.docmacro	Microsoft Word files with macros. Attached Microsoft Word files are searched for macro patterns with heuristic analysis. This filter does not cover all kinds of macros.
.xlsmacro	Microsoft Excel files with macros. Attached Microsoft Excel files are searched for macro

CATEGORY	FILTERED OUT FILE TYPES
	patterns with heuristic analysis. This filter does not cover all kinds of macros.
.pptmacro	Microsoft PowerPoint files with macros. Attached Microsoft PowerPoint files are searched for macro patterns with heuristic analysis. This filter does not cover all kinds of macros.

Activating Content Control

You have activated Spam and Malware Protection (see "Activating Spam and Malware Protection" in the Control Panel manual).

In the **Security Settings** > **Content Control** module, you can activate Content Control (see About Content Control on page 458) to manage the handling of attachments of incoming and outgoing emails for the users of a domain.

1. Log in to the Control Panel with your administrative credentials.
2. Select a domain from the scope selection.
3. Navigate to **Security Settings** > **Content Control**.
4. Toggle the switch **Activate Content Control**.

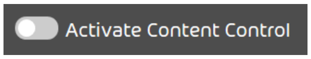


Figure 344: Activate Content Control

The switch is highlighted in green.

Content Control has been activated for the selected domain. The default settings of Content Control are applied to all users of the domain.

Next, you can adjust the default settings of Content Control for the domain (see Configuring Content Control on page 463). If you would like to configure settings for groups, you must first add groups to Content Control (see Adding a Group to Content Control on page 461). If you no longer want to use Content Control, you can deactivate Content Control (see Deactivating Content Control on page 471).

Adding a Group to Content Control

You have activated Content Control (see Activating Content Control on page 460). You have created a group under the domain (see "Creating a Group" in the Control Panel manual).

By default, the settings in the **Content Control** module apply to all users of a domain. However, under **Security Settings** > **Content Control**, you can add a group to Content Control to configure Content Control differently for the group than for other users under the domain.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to add a group to Content Control.
3. Navigate to **Security Settings** > **Content Control**.
4. Click on the drop-down menu under **Affected groups**.

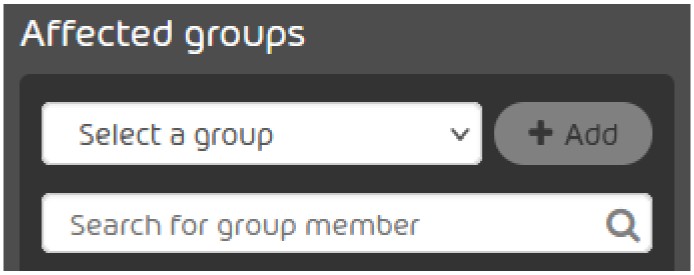


Figure 345: Select a group

The drop-down menu opens. The drop-down menu contains the groups of the domain.

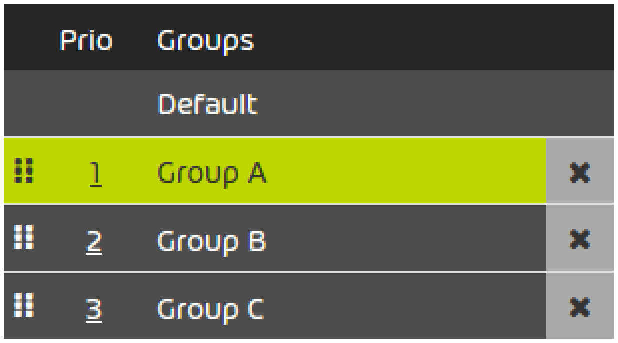
5. From the drop-down menu, select the group that you would like to add to Content Control.

6. Click on **Add**.

The group is added to the group list below. The group is added to the end of the list.

Notice:

The groups are sorted by their priority. The priorities are listed in the column **Prio**. The lower the number, the higher the priority of a group. To a mailbox that belongs to multiple groups in the **Content Control** module, the rules of the group with the highest priority are applied. The priorities of the groups can be changed (see Changing Priorities of Groups on page 468).



	Prio	Groups	
		Default	
⠿	1	Group A	✖
⠿	2	Group B	✖
⠿	3	Group C	✖

Figure 346: Group list

A group has been added to Content Control.

Next, you can configure Content Control for the group (see Configuring Content Control on page 463), change the priority of the group (see Changing Priorities of Groups on page 468) or remove the group from Content Control (see Removing a Group from Content Control on page 470).

Configuring Content Control

You have activated Content Control (siehe Activating Content Control on page 460).

In the **Security Settings** > **Content Control** module, you can configure Content Control. You can modify the default settings for the domain as well as the settings for single groups.

1. Log in to the Control Panel with your administrative credentials.
2. Select a domain from the scope selection.
3. Navigate to **Security Settings** > **Content Control**.
4. Under **Affected groups**, choose whether you want to modify the default settings or the settings for a group.

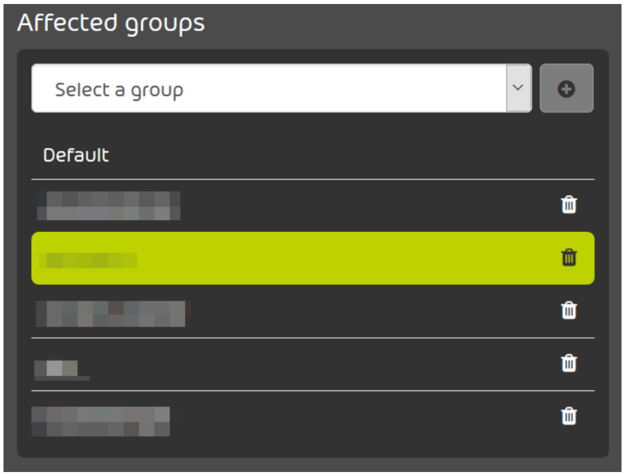


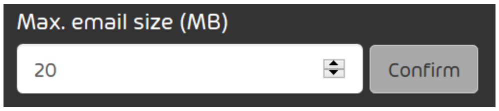
Figure 347: Select default or group settings

- To modify the settings for all users of the domain that are not included in any of the listed groups, select **Default**.
- To modify the settings for a group, select that group.

Your selection is highlighted in green.

5. Go to **Settings** > **For incoming emails** to configure Content Control for incoming emails.

6. Under **Max. email size (MB)**, enter the maximum allowed email size in megabytes.



Max. email size (MB)

20

Figure 348: Enter maximum email size

Notice:

The maximum email size must not exceed the size limit of your email server. The maximum email size refers to the payload of the email. The payload is the size of the email and its attachments on the recipient's computer. The actual size of the email, including additional data required to transmit it, can be approximately one-third larger. Since the size limit of your email server refers to this actual size, the value in the **Max. email size (MB)** field must be determined from the maximum actual size. As a guideline, this value should be 67% of the maximum actual size.

Example: If the size limit of the destination server is 10 MB, a maximum email size of 6.7 MB should be entered in the field.

Notice:

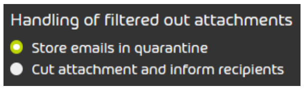
The field **Max. email size (MB)** accepts values up to 150 MB.

7. Click on **Confirm** to save the changes.

8. **Notice:**

   This option is only available for incoming emails. Outgoing emails with filtered-out attachments are blocked and the sender receives a non-delivery report.

   Under **Handling of filtered out attachments**, select how to deal with emails with filtered-out attachments.



Handling of filtered out attachments

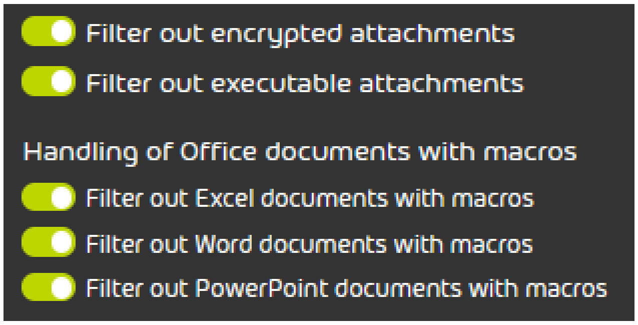
● Store emails in quarantine

○ Cut attachment and inform recipients

Figure 349: Select how to handle filtered-out attachments

- To save emails with filtered-out attachments in the quarantine and prevent them from being delivered to the recipients, select **Store emails in quarantine**.
- To cut filtered-out attachments from the emails and deliver the emails with automatically generated attachments containing references to the removed attachments instead, select **Cut attachment and inform recipients**.

9. Select which attachments should be filtered out. To filter out attachments, toggle the corresponding switch.



Filter out encrypted attachments

Filter out executable attachments

Handling of Office documents with macros

Filter out Excel documents with macros

Filter out Word documents with macros

Filter out PowerPoint documents with macros

Figure 350: Filter out attachments

- Select **Filter out encrypted attachments**to filter out encrypted attachments with the following file extensions:
  - .dot
  - .doc
  - .docx
  - .xls
  - .xlsx
  - .ppt
  - .pptx
  - .pptx
  - .pdf
  - .rar
  - .7z
  - .gz
- Select **Filter out executable attachments** to filter out all file types from the category .executable (see Overview of Categories on page 459).
- Select **Filter out Excel documents with macros** to filter out all file types from the category .xslmacro (see Overview of Categories on page 459).

- Select **Filter out Word documents with macros** to filter out all file types from the category .docmacro (see Overview of Categories on page 459).
- Select **Filter out PowerPoint documents with macros** to filter out all file types from the category .pptmacro (see Overview of Categories on page 459).

10.

Notice:

You can use categories to filter out groups of file types (see Overview of Categories on page 459).

Important:

Content Control does not only check the file extension but also checks the MIME type of the files. The MIME type can differ from the file extension.

If you filter out .gz files, you also filter out files with the MIME type application/gz.

Figure 351: Example

In order to filter out files of other file types, enter the file extension in the field under **Forbidden file extensions (e.g. '.jpg')** (e.g., '.jpg') and click on **Add**.

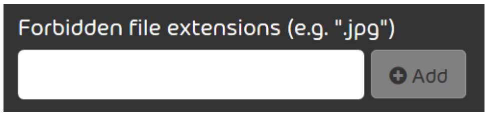


Figure 352: Filter out file types

➜

The file type is listed below.

11. **Important:**

    Content Control opens and scans archive files in the formats .rar, .zip, and .7z. Archive files in other formats are not checked. If archive files are nested, Content Control checks archive files up to the 4th level. On each level, Content Control checks a maximum of 8 archive files. For each email, Content Control checks a maximum of 1000 files inside archive files.

    To filter out files of certain file types from archive files, proceed as follows.

    - To use the file types listed above, mark the checkbox **Forbidden file extensions in archives (e.g. '.png')** under **Inherit forbidden file extensions from above**.
    - In order to filter out files of other file types, enter the file extension in the field under **Forbidden file extensions in archives (e.g. '.png')** and click on **Add**.
12. Go to **Settings** > **For outgoing emails** to configure Content Control for outgoing emails.
13. Configure Content Control for outgoing emails.
    - To apply the settings of incoming emails to outgoing emails, toggle the switch **Use the same settings as for incoming emails**.
    - To create different settings for outgoing emails than for incoming emails, follow the same procedure as in the previous steps for incoming emails.

Content Control has been configured.

Changing Priorities of Groups

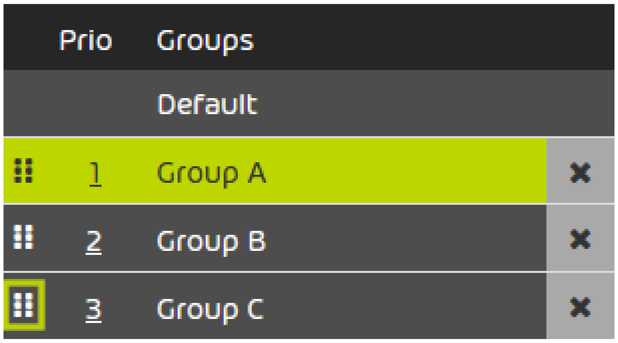
You have added several groups to Content Control (see Adding a Group to Content Control on page 461).

In the **Security Settings** > **Content Control** module, groups are sorted by their priority. The priorities of the groups are displayed under **Affected groups** in the column **Prio**. The lower the number, the higher the priority of a group. If a mailbox belongs to several groups in the **Security Settings** >

Content Control module, the rules of the group with the highest priority are applied to it. You can change the priorities of groups.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain containing the groups whose priorities you would like to change in the **Content Control** module.
3. Navigate to **Security Settings** > **Content Control**.
4. Under **Affected groups**, select the group whose priority you would like to change.
5. Optional: Change the priority of the group by moving the group within the list.

a) Click on the six points next to the group, and press and hold the left mouse button.



Prio	Groups	
	Default	
1	Group A	✖
2	Group B	✖
3	Group C	✖

Figure 353: Move the group

b) Drag the group to the position corresponding to the new priority.

c) Release the left mouse button.

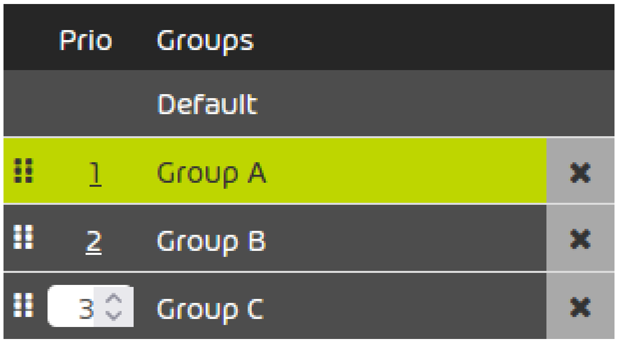
➔

The group is placed at the new position. The priorities of all groups that have moved within the list are updated.

6. Overwrite the priority of the group.

   a) Double-click on the priority next to the group.

      The number can be edited.



Prio	Groups	
	Default	
1	Group A	✖
2	Group B	✖
3	Group C	✖

Figure 354: Input field for the priority

   b) Enter the number of the new priority in the input field or select the number with the selection arrows.

   c) Confirm the new priority with the enter key.

   The priority of the group is saved. The group is placed at the position that corresponds to the new priority. The priorities of all groups that have moved within the list are updated.

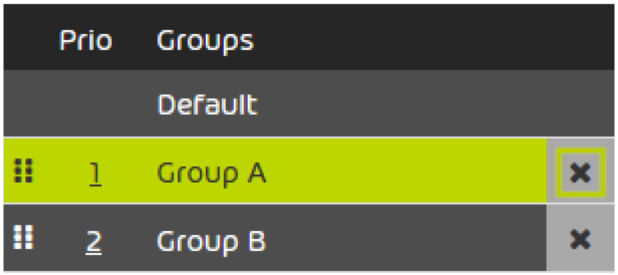
The priorities of the groups have been changed.

Removing a Group from Content Control

You have added a group to Content Control (see Adding a Group to Content Control on page 461).

In the **Security Settings** > **Content Control** module, you can remove a group from Content Control so the default settings of Content Control are again applied to the members of the group.

1. Log in to the Control Panel with your administrative credentials.
2. Select a domain from the scope selection.
3. Navigate to **Security Settings** > **Content Control**.
4. Click on the cross icon next to the group.



Prio	Groups	
	Default	
1	Group A	✖
2	Group B	✖

Figure 355: Remove a group

A warning message is displayed.

5. Click on **Confirm**.

The group is removed from Content Control.

A group has been removed from Content Control. The default settings of Content Control are applied to the group members.

Deactivating Content Control

You have activated Content Control (siehe Activating Content Control on page 460).

In the **Security Settings** > **Content Control** module, you can deactivate Content Control for a domain.

1. Log in to the Control Panel with your administrative credentials.
2. Select a domain from the scope selection.
3. Navigate to **Security Settings** > **Content Control**.
4. Toggle the switch **Activate Content Control**.

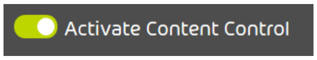
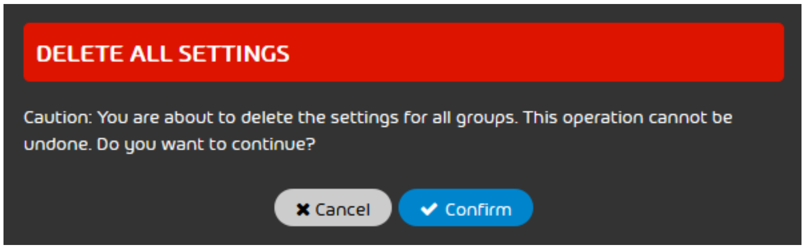


Figure 356: Deactivate Content Control

➜

A warning message is displayed.

5. Click on **Confirm** to permanently delete all settings of Content Control for the domain.


DELETE ALL SETTINGS

Caution: You are about to delete the settings for all groups. This operation cannot be undone. Do you want to continue?

Figure 357: Confirm

✓

Content Control has been deactivated for a domain. All settings of Content Control have been permanently deleted for the domain.

Compliance Filter

About the Compliance Filter

With the Compliance Filter, customer-level administrators can define their own filter rules, for example, to classify incoming emails as **Clean**, **Spam** or **Threat** (see "Email Categories" in the Control Panel manual). Furthermore, emails can be rejected, redirected through a different server or forwarded to other recipients. For the ranking of the filter rules of the Compliance Filter in the rule order of all our services, see Order of Rules Across All Services on page 435

CAUTION:

Incorrect filter rules have a negative impact on the email traffic and can override our services.

The Compliance Filter is not designed to rewrite addresses.

The Compliance Filter can check both incoming and outgoing emails. After the activation of the Compliance Filter (see Activating Compliance Filter on page 475), customer-level administrators can define filter rules of the following types:

- **Header**
- **Body**
- **Advanced**

Regular expressions can be used in the conditions of the filter rules (see Regular Expressions on page 524). Customer-level administrators assign an action to each filter rule. This action is automatically applied to the emails that match the filter rule. For more information on filter rules, see Filter Rules on page 476. In total, up to 1500 filter rules can be defined per customer.

Besides filter rules for individual expressions, more complex and precise filter rules can be created using dictionaries, each of which may contain up to 15000 literal expressions or up to 1000 regular expressions (see Dictionaries on page 515). Customer-level administrators can create and maintain up to 250 dictionaries for their primary domain. Dictionaries with regular expressions in particular significantly reduce the effort required to create and maintain filter rules.

In order to activate and configure the Compliance Filter for a domain, Spam and Malware Protection (see 'Spam and Malware Protection' in the Control Panel manual) must be activated for the domain.Once Spam and Malware Protection is deactivated, the Compliance Filter is also deactivated and can no longer be configured.

Customer-level administrators can deactivate the Compliance Filter if they no longer want to use it (see Deactivating Compliance Filter on page 537).

Order of Rules Across All Services

The rules of Spam and Malware Protection (see "Spam and Malware Protection" in the Control Panel manual) are processed according to specific priorities. Once a rule with a higher priority applies, no rules with lower priorities are processed. This can lead to emails being blocked despite an allow list entry having been set for its sender's address because the IPv4 address of the sending server is on the RBL deny list.

Rule order (from top to bottom in descending priority):

Incoming emails

1. RBL list (block)
2. Mass spam detection (block)
3. Compliance Filter
4. Check for malicious content (quarantine)
5. Content Control if activated (quarantine)
6. User-based allow list (deliver)
7. User-based deny list (quarantine)
8. Administrative allow list (deliver)

> **Notice:**
>
> The administrative allow list is a special case among the rules. This is because administrators can select which filters will be bypassed by allow list entries at domain level (see "Creating a Deny List Entry for a Domain" in the Control Panel manual). While being processed, the affected emails thus skip the selected filters. This also applies to filters that are listed before the administrative allow list. The position where the administrative allow list is placed in the list refers to the default configuration of allow list entries at domain level. By default, the entries only bypass spam filtering.

9. Administrative deny list (quarantine)

10. General allow list (deliver)
11. General spam rules (quarantine)
12. Infomail filter (quarantine)

> **Notice:**
>
> The Compliance Filter (see About the Compliance Filter on page 472) is applied before Content Control (see About Content Control on page 458). This allows administrators to create exceptions for Content Control with filter rules of the Compliance Filter that categorize emails as **Clean**.
>
> For Content Control, exceptions can neither be created using user-based allow and deny lists nor administrative deny lists because these rules are applied after Content Control. Only administrative allow lists can be used to bypass Content Control.

Outgoing emails

1. RBL list
2. Compliance Filter
3. Check for malicious content
4. Content Control if activated

Activating Compliance Filter

You have activated Spam and Malware Protection for the domain (see "Activating Spam and Malware Protection" in the Control Panel manual) for which you would like to activate the Compliance Filter.

In the **Security Settings** > **Compliance Filter** module, you can activate the Compliance Filter to create your own rules for filtering emails (see Filter Rules on page 476).

1. Log in to the Control Panel with your administrative credentials.

2. From the scope selection, select the domain for which you would like to activate the Compliance Filter.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Toggle the **Activate Compliance Filter** switch.

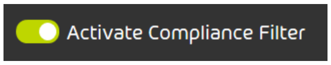


Figure 358: Activating Compliance Filter

The Compliance Filter is activated.

The Compliance Filter has been activated. Once filter rules have been created, the Compliance Filter can be used.

Next, you can create filter rules (see Filter Rules on page 476) and dictionaries (see Dictionaries on page 515) for the Compliance Filter.

Filter Rules

The Compliance Filter checks the emails of a domain. In the **Compliance Filter** module, customer-level administrators can manage filter rules for incoming and outgoing emails. Administrators can create filter rules for incoming (see Creating a Filter Rule for Incoming Emails on page 477) and outgoing emails (see Creating a Filter Rule for Outgoing Emails on page 484). The created filter rules are displayed in two tables (see Display of Filter Rules on page 491).

Notice:

Up to 1500 filter rules can be created for a primary domain.

Customer-level administrators can select an action (see Actions in Filter Rules on page 493) for each filter rule. The action is performed once an email matches the filter rule.

Customer-level administrators also select a type (see Types of Filter Rules on page 495) for each filter rule. The type of the filter rule determines to which emails the filter rule applies.

One of the possible conditions for filter rules regards the recipients to whom an email is sent. If an email is sent to multiple recipients and a filter rule applies to some of them, the action only affects the delivery of the email to the recipients to which the filter rule applies. Thus, different actions can be performed for different recipients of the same email.

Customer-level administrators can edit filter rules at a later stage (see Editing a Filter Rule on page 501). Furthermore, administrators can change the priorities of the filter rules (see Changing the Priority of a Filter Rule on page 503). The priority affects the order in which the filter rules of the Compliance Filter are processed. For more information on the order of the filter rules of the Compliance Filter, see Order of Filter Rules on page 505.

If a filter rule shall be temporarily suspended, customer-level administrators can deactivate it (see Deactivating a Filter Rule of the Compliance Filter on page 513). Deactivated filter rules can be reactivated later (see Activating a Filter Rule on page 512).

Once a filter rule is no longer required, customer-level administrators can delete the filter rule (see Deleting a Filter Rule of the Compliance Filter on page 514).

Creating a Filter Rule for Incoming Emails

You have activated the Compliance Filter for the selected domain (see Activating Compliance Filter on page 475).

In the **Security Settings** > **Compliance Filter** module, you can create filter rules of the Compliance Filter (see About the Compliance Filter on page 472) for incoming emails.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to create the filter rule.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Select the **Rules** tab.

5. Click on **Add rule** under **Rules for incoming emails**.

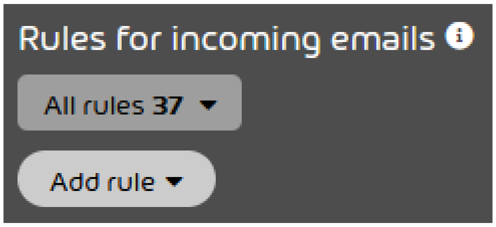


Figure 359: Add a rule

6. Under **Action**, select what shall happen to the emails that match the filter rule. You can choose from the following actions:

   - **Reject**
   - **Change recipient**
   - **Reroute**
   - **Add BCC**
   - **Tag as 'Clean'**
   - **Tag as 'Spam'**
   - **Tag as 'Threat'**

Notice:

For an overview of the actions, see Actions in Filter Rules on page 493.

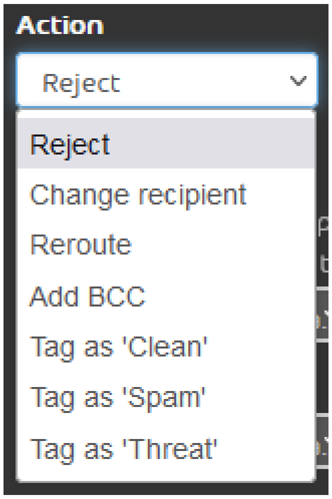


Figure 360: Select action

If the selected action requires additional information, an additional field appears under the drop-down menu. For more information about the additional fields of the actions, see Actions in Filter Rules on page 493.

7. Select the type of the filter rule under **Conditions**. You have the following options:

   - **Header**: The filter rule matches all emails with a header that contains a specified search term.
   - **Body**: The filter rule matches all emails with a body that contains a specified search term.
   - **Advanced**: You can specify the sender, the recipient, the IPv4 address and the hostname for the emails. You can also define search terms for the subject and attachment of the emails and a maximum email size. The filter rule matches all emails with the defined properties.

Notice:

The type of the filter rule determines to which emails the filter rule shall apply.

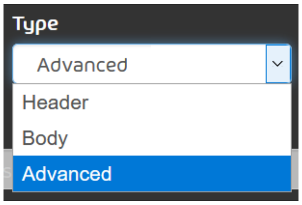


Figure 361: Select the type of the filter rule

➜

Under the drop-down menu, fields for the configuration of the filter rule are displayed. The selected filter rule type determines which fields are displayed.

Notice:

Under Types of Filter Rules on page 495, you can find an overview and explanations of the fields that are available for each filter rule type.

8. If you have selected the **Advanced** type, follow the following steps:

a) Under **Conditions**, select the logical operator between the conditions to which the filter rule shall apply. You have the following options:

- **Match all conditions**: All selected conditions must match in order for the filter rule to be applied to an email. This relation corresponds to a logical AND operation.
- **Match any condition** : It suffices that one of the selected conditions matches for the filter rule to be applied to an email. This relation corresponds to a logical OR operation.

b) Tick the checkboxes of the conditions that shall apply to the filter rule.

The input fields of the selected conditions are enabled.

c) If the input field of the selected condition contains a drop-down menu, select which type of data you would like to enter. You have the following options:

- **Literal / regular expression**: The entered value is interpreted as a literal or a regular expression.
- **Contained in dictionary**: The entered value is interpreted as the name of a dictionary (see Dictionaries on page 515) that is referenced in the condition. The condition is fulfilled if the corresponding value of the email matches an entry from the referenced dictionary.
- **Not contained in dictionary**: The entered value is interpreted as the name of a dictionary (see Dictionaries on page 515) that is referenced in the condition. The

condition is fulfilled if the corresponding value of the email does not match any entry from the referenced dictionary.

d) If you have selected the conditions **Sender** or **Recipient**, select to which field of the email the entered value shall refer. You have the following options:

- **According to envelope**: The entered value must match the address that has been passed as the parameter of **MAIL FROM:** (sender address) or **RCPT TO:** (recipient address) during the email transfer.
- **According to header**: The entered value must match the address that has been passed in the field **From** (sender address) or **To** in the header of the email.
- **According to both**: The entered sender address must either be given as a parameter of **MAIL FROM:** or in the field **From** in the header of the email. The entered recipient address must either be given as a parameter of **RCPT TO:** or in the field **To** in the header of the email.

9. Depending on the input type, enter a search term, a value or the name of a directory in the input fields of the conditions

> **Notice:**
>
> A search term is found as a literal or a regular expression even if it is surrounded by text.

> **Notice:**
>
> To define more accurate and flexible rules, you can use regular expressions. For a description of the structure and functionality of regular expressions, see Regular Expressions on page 524 and Explanation of Regular Expressions on page 526. Under Exceptions to Regular Expressions on page 533, you will find an overview of unsupported characters.
>
> Regular expressions can only be used in rules of type **Advanced**.

> **Notice:**
>
> In the field **Larger than**, enter the maximum email size in megabytes.

10. Optional: Enter a description of the filter rule under **Description (optional)**.

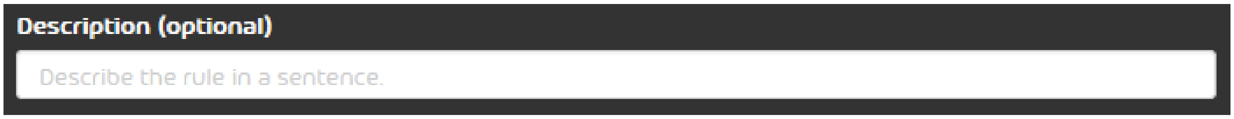
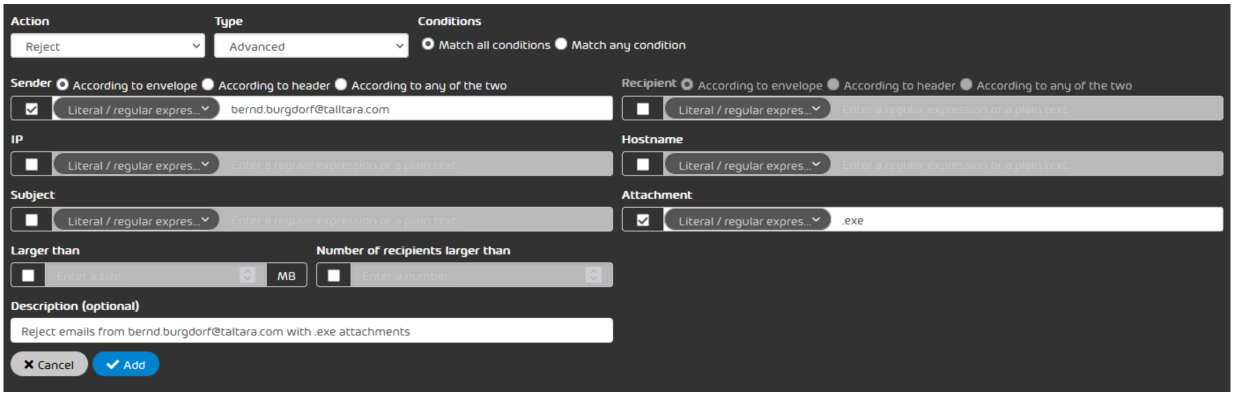


Figure 362: Describe filter rule

11. Click on **Add**.



Action: Reject
Type: Advanced
Conditions: ● Match all conditions ○ Match any condition

Sender ● According to envelope ○ According to header ○ According to any of the two
☑ Literal / regular expres... bernd.burgdorf@talltara.com

Recipient ● According to envelope ○ According to header ○ According to any of the two
□ Literal / regular expres... Enter a regular expression or a plain text.

IP
□ Literal / regular expres... Enter a regular expression or a plain text.

Hostname
□ Literal / regular expres... Enter a regular expression or a plain text.

Subject
□ Literal / regular expres... Enter a regular expression or a plain text.

Attachment
☑ Literal / regular expres... .exe

Larger than
□ Enter a size. MB

Number of recipients larger than
□ Enter a number.

Description (optional)
Reject emails from bernd.burgdorf@taltara.com with .exe attachments

Figure 363: Add filter rule

The filter rule is added to the table under **Rules for incoming emails** (see Display of Filter Rules on page 491). The filter rule is assigned the lowest priority of all existing filter rules and is placed at the end of the table. The filter rule is activated.

A filter rule for incoming emails has been created.

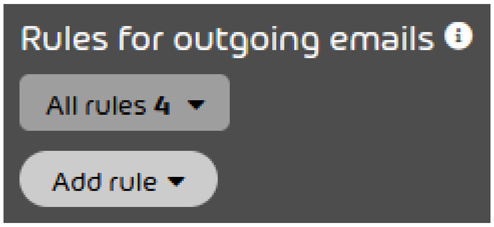
Next, you can edit the filter rule (see Editing a Filter Rule on page 501), change the priority of the filter rule (see Changing the Priority of a Filter Rule on page 503), temporarily deactivate the filter rule (see Deactivating a Filter Rule of the Compliance Filter on page 513) or delete it (see Deleting a Filter Rule of the Compliance Filter on page 514).

Creating a Filter Rule for Outgoing Emails

You have activated the Compliance Filter for the selected domain (see Activating Compliance Filter on page 475).

In the **Security Settings** > **Compliance Filter** module, you can create filter rules of the Compliance Filter (see About the Compliance Filter on page 472) for outgoing emails.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to create the filter rule.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Select the tab **Rules**.
5. Click on **Add rule** under **Rules for outgoing emails**.



Rules for outgoing emails

Figure 364: Add a rule

6. Under **Action**, select what shall happen to the emails that match the filter rule. You can choose from the following actions:

   - **Reject**
   - **Change recipient**
   - **Reroute**
   - **Add BCC**
   - **Notify sender**

   Notice:

   For an overview of the actions, see Actions in Filter Rules on page 493.

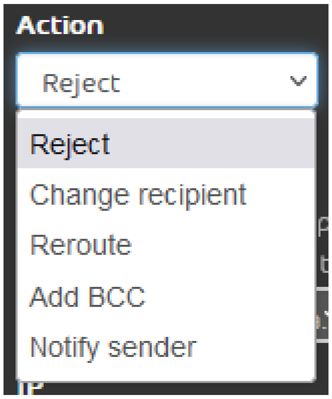


Figure 365: Select action

If the selected action requires additional information, an additional field appears under the drop-down menu. For more information about the additional fields of the actions, see Actions in Filter Rules on page 493.

7. Select the type of the filter rule under **Type**. It determines to which emails the filter rule shall apply. You have the following options:

   - **Header**: The filter rule matches all emails with a header that contains a specified search term.
   - **Body**: The filter rule matches all emails with a body that contains a specified search term.
   - **Advanced**: You can specify the sender, the recipient, the IPv4 address and the hostname for the emails. You can also define search terms for the subject and attachment of the emails and a maximum email size. The filter rule matches all emails with the defined properties.

Notice:

The type of the filter rule determines to which emails the filter rule shall apply.

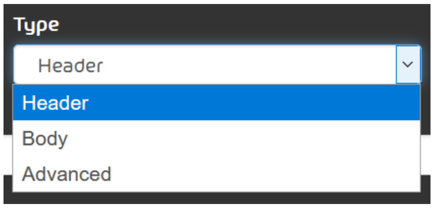

Type: Header

Figure 366: Select the type of the filter rule

➜

Under the drop-down menu, fields for the configuration of the filter rule are displayed. The selected filter rule type determines which fields are displayed.

Notice:

Under Types of Filter Rules on page 495, you can find an overview and explanations of the fields that are available for each filter rule type.

8. If you have selected the **Advanced** type, follow the following steps:

a) Under **Conditions**, select the logical operator between the conditions to which the filter rule shall apply. You have the following options:

- **Match all conditions**: All selected conditions must match in order for the filter rule to be applied to an email. This relation corresponds to a logical AND operation.
- **Match any condition** : It suffices that one of the selected conditions matches for the filter rule to be applied to an email. This relation corresponds to a logical OR operation.

b) Tick the checkboxes of the conditions that shall apply to the filter rule.

➜

The input fields of the selected conditions are enabled.

c) If the input field of the selected condition contains a drop-down menu, select which type of data you would like to enter. You have the following options:

- **Literal / regular expression**: The entered value is interpreted as a literal or a regular expression.
- **Contained in dictionary**: The entered value is interpreted as the name of a dictionary (see Dictionaries on page 515) that is referenced in the condition. The condition is fulfilled if the corresponding value of the email matches an entry from the referenced dictionary.
- **Not contained in dictionary**: The entered value is interpreted as the name of a dictionary (see Dictionaries on page 515) that is referenced in the condition. The

condition is fulfilled if the corresponding value of the email does not match any entry from the referenced dictionary.

d) If you have selected the conditions **Sender** or **Recipient**, select to which field of the email the entered value shall refer. You have the following options:

- **According to envelope**: The entered value must match the address that has been passed as the parameter of **MAIL FROM:** (sender address) or **RCPT TO:** (recipient address) during the email transfer.
- **According to header**: The entered value must match the address that has been passed in the field **From** (sender address) or **To** in the header of the email.
- **According to both**: The entered sender address must either be given as a parameter of **MAIL FROM:** or in the field **From** in the header of the email. The entered recipient address must either be given as a parameter of **RCPT TO:** or in the field **To** in the header of the email.

9. Depending on the input type, enter a search term, a value or the name of a directory in the input fields of the conditions

   Notice:

   A search term is found as a literal or a regular expression even if it is surrounded by text.

   Notice:

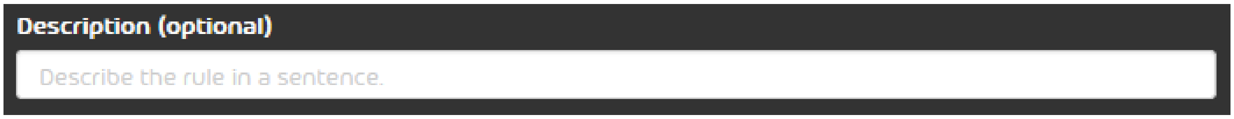
   To define more accurate and flexible rules, you can use regular expressions. For a description of the structure and functionality of regular expressions, see Regular Expressions on page 524 and Explanation of Regular Expressions on page 526. Under Exceptions to Regular Expressions on page 533, you will find an overview of unsupported characters.

   Regular expressions can only be used in rules of type **Advanced**.

   Notice:

   In the field **Larger than**, enter the maximum email size in megabytes.

10. Optional: Enter a description of the filter rule under **Description (optional)**.

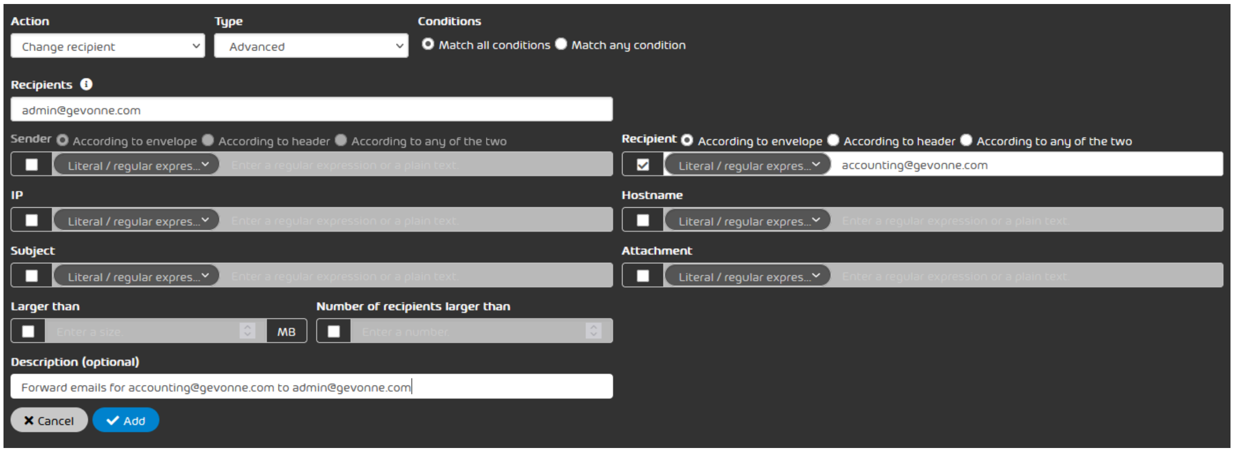


Description (optional)

Describe the rule in a sentence.

Figure 367: Describe filter rule

11. Click on **Add**.



Action: Change recipient

Type: Advanced

Conditions: ● Match all conditions ○ Match any condition

Recipients: admin@gevonne.com

Sender ● According to envelope ○ According to header ○ According to any of the two

□ Literal / regular expres... Enter a regular expression or a plain text.

Recipient ● According to envelope ○ According to header ○ According to any of the two

☑ Literal / regular expres... accounting@gevonne.com

IP

□ Literal / regular expres... Enter a regular expression or a plain text.

Hostname

□ Literal / regular expres... Enter a regular expression or a plain text.

Subject

□ Literal / regular expres... Enter a regular expression or a plain text.

Attachment

□ Literal / regular expres... Enter a regular expression or a plain text.

Larger than

□ Enter a size MB

Number of recipients larger than

□ Enter a number

Description (optional)

Forward emails for accounting@gevonne.com to admin@gevonne.com

Figure 368: Add filter rule

The filter rule is added to the table under **Rules for outgoing emails** (see Display of Filter Rules on page 491). The filter rule is assigned the lowest priority of all existing filter rules and is placed at the end of the table. The filter rule is activated.

A filter rule for outgoing emails has been created.

Next, you can edit the filter rule (see Editing a Filter Rule on page 501), change the priority of the filter rule (see Changing the Priority of a Filter Rule on page 503), temporarily deactivate the filter rule (see Deactivating a Filter Rule of the Compliance Filter on page 513) or delete it (see Deleting a Filter Rule of the Compliance Filter on page 514).

Display of Filter Rules

After filter rules for incoming and outgoing emails have been created, they will be displayed in the corresponding table in the sections **Rules for incoming emails** and **Rules for outgoing emails**.

Both tables contain the following columns:

- **Priority**: Application priority of the filter rule. A filter rule with a lower number in this field is applied before a filter rule with a higher number. The filter rules are sorted by their priority in descending order.
- **Active**: If the checkbox is ticked, this means that the filter rule is activated.
- **Action**: Here, the action is indicated that is performed by the filter rule.
  - Actions for incoming emails: **Change recipient**, **Reroute**, **Add BCC**, **Tag as 'Clean'**, **Tag as 'Spam'**, **Tag as 'Threat'**.
  - Actions for outgoing emails: **Reject**, **Change recipient**, **Reroute**, **Add BCC**, **Notify sender**.

> **Notice:**
>
> The available actions are described in chapter Actions in Filter Rules on page 493.

- **Type**: Here, the type of the filter rule is indicated.
- **Conditions**: Here, the filter conditions are indicated in the configured system language. If a dictionary is referenced in an advanced rule, this is indicated by the abbreviation **D**. In the following example, the rule takes into account senders from the dictionary **forbiddensenders**: **Sender: ?A=?D=forbiddensenders**. Furthermore, the entries of a dictionary can be negated. In the following example, the rule does not take into account senders from the dictionary **forbiddensenders**: **Sender: ?A=?D!=forbiddensenders**.

> **Note:**
>
> For the filter rules **Sender** and **Recipient**, the field or the fields to which the entered value refers is also indicated (**According to envelope**, **According to header** and **According to both** as described in chapter Types of Filter Rules on page 495). This is indicated by the abbreviations **E** (for **Envelope**), **H** (for **Header**) and **A** (for **Any**), regardless of the language.
>
> For instance, **Sender:?E=miller@gevonne.com** would mean that a filter rule shall be applied to emails with the envelope sender **miller@gevonne.com**.

- **Description**: Description written by the creator of the filter rule.
- **ID**: Number that was automatically generated by the system to identify the filter rule.

Actions in Filter Rules

An action is assigned to each filter rule of the Compliance Filter (see About the Compliance Filter on page 472). Once an email matches the filter rule, this action is performed.

Different actions are available for incoming and outgoing emails.

The following actions are only available for incoming emails:

- **Tag as 'Clean'**
- **Tag as 'Spam'**
- **Tag as 'Threat'**

The action **Notify sender** is only available for outgoing emails.

The following table describes all actions for filter rules in the **Compliance Filter** module. If an action is selected that requires additional information in the **Compliance Filter** module, an additional field is displayed for the action. These fields are also described in the table.

Table 26: Actions for filter rules

ACTION	DESCRIPTION
Reject	! **Attention:** The email is rejected. The sending email server is informed about the disconnection error with an error code and a text (**554 5.6.9 customer rule based reject by Compliance-Filter**). For more information, see "Classification reasons" in the Control Panel manual. The sending email server is in charge of notifying the sender.

ACTION	DESCRIPTION
Change recipient	The email is delivered to one or more other email addresses instead of the original recipient. If this action is selected, the **Send email to:** field is displayed. Customer-level administrators must enter all email addresses the email shall be forwarded to in this field. Administrators can enter as many email addresses as needed in the field. If multiple email addresses are entered, they must be separated from each other with semicolons.
Reroute	The email is redirected through another IPv4 address or hostname. If this action is selected, the **IP or hostname** field is displayed. Customer-level administrators must enter the IPv4 address or the hostname through which the email shall be redirected in this field. Administrators can only enter one IPv4 address or one hostname.
Add BCC	One or more BCC recipients are automatically added to the email. If this action is selected, the **Send email to:** field is displayed. Customer-level administrators must enter the email addresses to which blind copies of the email shall be sent in this field. Administrators can enter as many email addresses as needed in the field. If multiple email addresses are entered, they must be separated from each other with semicolons.

ACTION	DESCRIPTION
Notify sender	The sender of the email is automatically notified once the outgoing email has been accepted by the destination server.
Tag as 'Clean'	The incoming email is classified as **Clean**.
Tag as 'Spam'	The incoming email is classified as **Spam**.
Tag as 'Threat'	The incoming email is classified as **Threat**.

Types of Filter Rules

When creating filter rules in the **Compliance Filter** module (see About the Compliance Filter on page 472), customer-level administrators can select a type for the filter rule. With the type of the filter rule, administrators define the properties of the emails the rule should be applied to. In the **Compliance Filter** module, fields for different properties are displayed for each filter rule type.

The following tables give an overview of the fields that are available for each filter rule type. The tables contain descriptions of the properties and examples for possible input.

Notice:

To define more accurate and flexible rules, regular expressions can be used. For a description of the structure and functionality of regular expressions, see Regular Expressions on page 524 and Explanation of Regular Expressions on page 526. For an overview of all unsupported characters, see Exceptions to Regular Expressions on page 533.

Notice:

In order to manage conditions more easily, customer-level administrators can collect multiple expressions in dictionaries. Dictionaries can be referenced in the input fields of filter rule conditions. For more information on the functions, the creation and the management of dictionaries, see Dictionaries on page 515.

Table 27: Type Header

FIELD	DESCRIPTION	EXAMPLE FOR INPUT
Filter: header	The header of the email is searched for the entered search term.	Invoice

Table 28: Type Body

FIELD	DESCRIPTION	EXAMPLE FOR INPUT
Filter: body	The decoded body of the email is searched for the entered search term. **Notice:** Attachments are excluded from the search in the email body.	Payment order

Table 29: Type Advanced

FIELD	DESCRIPTION	EXAMPLE FOR INPUT
Sender	The sender address of the email is searched for the entered search term or for the entries in the referenced dictionary (see Dictionaries on page 515). **Notice:** Customer-level administrators have the following options to select which type of sender address is searched (see Creating a Filter Rule for Incoming Emails): - **According to envelope**: Sender address from the envelope (**MAIL FROM:**) - **According to header**: Sender address from the header (**To:**) - **According to both**: any of the two sender addresses	**user@gevonne.com**

FIELD	DESCRIPTION	EXAMPLE FOR INPUT
Recipient	The recipient addresses are searched for the entered search term or for the entries in the referenced dictionary. **Notice:** Customer-level administrators have the following options to select which type of recipient address is searched (see Creating a Filter Rule for Incoming Emails): - **According to envelope**: Recipient address from the envelope (**RCPT TO:**) - **According to header**: Recipient address from the header (**From:**) - **According to both**: any of the two recipient addresses **Notice:** If an email is sent to multiple recipients and a filter rule applies to some of them, the action only affects the	**user.extern@yahoo.com**

FIELD	DESCRIPTION	EXAMPLE FOR INPUT
IP	The public IPv4 address of the sending email server is searched for the entered search term or for the entries in the referenced dictionary. **Notice:** Enter the IPv4 address without the subnet mask as a search term.	Right: **0.0.0.0** Wrong: **0.0.0.0/24**
Hostname	The hostname (PTR record) obtained through a reverse lookup of the IPv4 address of the email server, is searched for the entered search term or for the entries in the referenced dictionary. Depending on whether the rule applies to incoming or outgoing emails, this is the hostname of the source server or the destination server,	**mailserver.domain.com**
Subject	The subject of the email is searched for the entered search term or for the entries in the referenced dictionary.	**Spam**

FIELD	DESCRIPTION	EXAMPLE FOR INPUT
Attachment	The file names and the file extensions of the email attachments are searched for the entered search term or for the entries in the referenced dictionary. **Notice:** It is possible to search for a file extension or for a part of the file name. To search for a file extension, the file extension must be entered as the search term. To search for a part of the file name, the part to be searched must be entered as the search term. **Notice:** The collective terms for attachments cannot be used for the Compliance Filter.	.jpg express

FIELD	DESCRIPTION	EXAMPLE FOR INPUT
Larger than	It is checked whether the email exceeds the entered size. **Notice:** The maximum email size is given in megabytes.	**500**
Number of recipients larger than	It is checked whether the number of recipients exceeds the entered size.	**10**

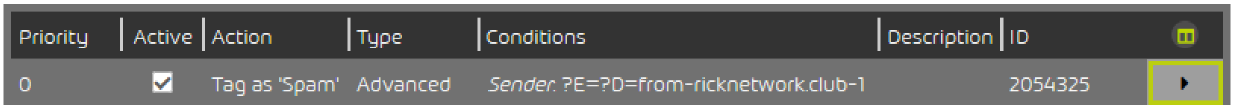
Editing a Filter Rule

You have activated the Compliance Filter for the selected domain (see Activating Compliance Filter on page 475) and have created filter rules for the Compliance Filter (see Creating a Filter Rule for Incoming Emails on page 477 or Creating a Filter Rule for Outgoing Emails on page 484)

In the **Security Settings** > **Compliance Filter** module, you can edit filter rules of the Compliance Filter (see About the Compliance Filter on page 472).

1. Log in to the Control Panel with your administrative credentials.
2. Select a domain from the scope selection.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Select the **Rules** tab.

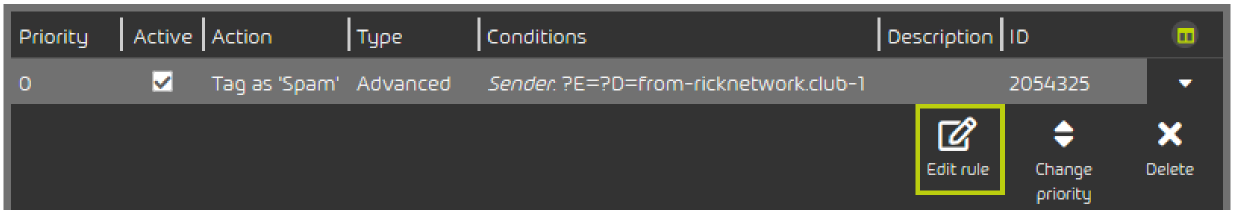
5. In the list of filter rules for incoming or outgoing emails, click on the menu arrow next to the filter rule you would like to edit.



Priority	Active	Action	Type	Conditions	Description	ID
0	☑	Tag as 'Spam'	Advanced	*Sender:* ?E=?D=from-ricknetwork.club-1		2054325

Figure 369: Open the menu

6. Click on **Edit rule**.



Priority	Active	Action	Type	Conditions	Description	ID
0	☑	Tag as 'Spam'	Advanced	*Sender:* ?E=?D=from-ricknetwork.club-1		2054325

Figure 370: Editing a Filter Rule

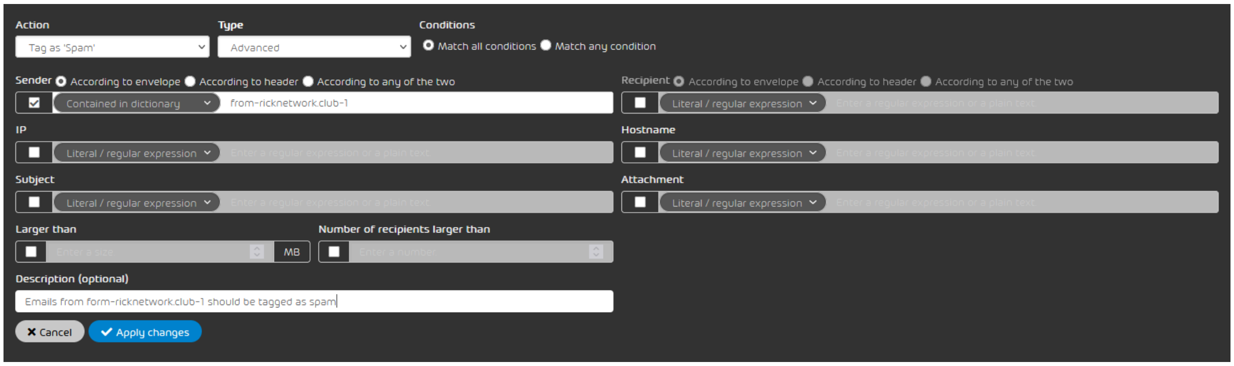
A menu with the current filter rule settings opens.

7. Edit the settings as desired.

Notice:

For more information, see Creating a Filter Rule for Incoming Emails on page 477 or Creating a Filter Rule for Outgoing Emails on page 484.

8. Click on **Apply changes**.



Action: Tag as 'Spam'
Type: Advanced
Conditions: ● Match all conditions ○ Match any condition

Sender ● According to envelope ○ According to header ○ According to any of the two
☑ Contained in dictionary: from-ricknetwork.club-1

Recipient ● According to envelope ○ According to header ○ According to any of the two
□ Literal / regular expression: Enter a regular expression or a plain text

IP
□ Literal / regular expression: Enter a regular expression or a plain text

Hostname
□ Literal / regular expression: Enter a regular expression or a plain text

Subject
□ Literal / regular expression: Enter a regular expression or a plain text

Attachment
□ Literal / regular expression: Enter a regular expression or a plain text

Larger than
□ Enter a size MB

Number of recipients larger than
□ Enter a number

Description (optional)
Emails from form-ricknetwork.club-1 should be tagged as spam

Figure 371: Apply changes

The changes are applied.

A filter rule has been edited.

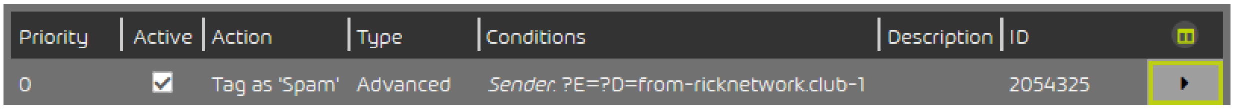
Changing the Priority of a Filter Rule

You have activated the Compliance Filter for the selected domain (see Activating Compliance Filter on page 475) and have created filter rules for the Compliance Filter (see Creating a Filter Rule for Incoming Emails on page 477 or Creating a Filter Rule for Outgoing Emails on page 484)

In the **Security Settings** > **Compliance Filter** module, you can change the order in which the filter rules of the Compliance Filter (see About the Compliance Filter on page 472) are processed. To change the order of the filter rules, change the priorities of the filter rules.

> **Important:**
>
> The order in which the filter rules of the Compliance Filter are processed depends not only on the priorities but also on the type of the filter rules (see Order of Filter Rules on page 505).

1. Log in to the Control Panel with your administrative credentials.
2. Select a domain from the scope selection.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Select the **Rules** tab.
5. In the list of filter rules for incoming or outgoing emails, click on the menu arrow next to the filter rule for which you would like to change the priority.



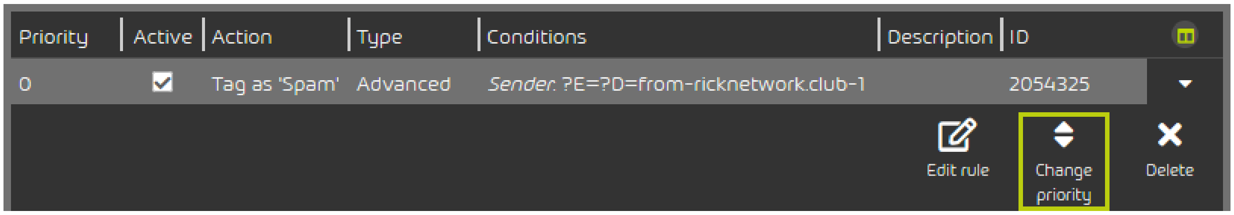
Priority	Active	Action	Type	Conditions	Description	ID	
0	☑	Tag as 'Spam'	Advanced	*Sender:* ?E=?D=from-ricknetwork.club-1		2054325	▸

Figure 372: Open the menu

➜

A menu opens.

6. Click on **Change priority**.



Priority	Active	Action	Type	Conditions	Description	ID	
0	☑	Tag as 'Spam'	Advanced	*Sender:* ?E=?D=from-ricknetwork.club-1		2054325	▾

Figure 373: Change priority

➜

A menu opens.

7. Enter the new priority of the filter rule under **Priority**.

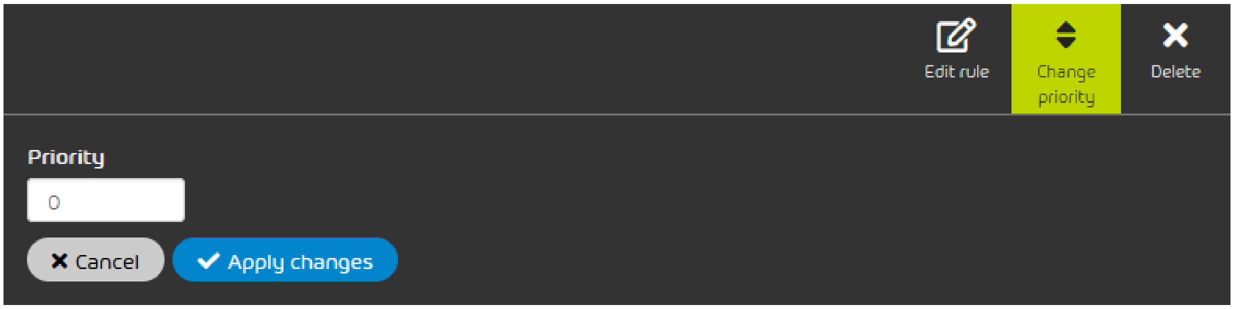


Figure 374: Enter priority

8. Click on **Apply changes**.

   ➜

   The new priority is assigned to the filter rule. The filter rule will be moved to the position that complies with the new priority.

✓

The priority of a filter rule has been changed. Thus, the order in which the filter rules are processed has changed.

Order of Filter Rules

> **Important:**
>
> Please note how the Compliance Filter ranks in the order of our services (see Order of Rules Across All Services on page 435). Once a rule of one of the services matches an email, the processing of other rules is stopped. No other rules are applied to the email.
>
> This order allows you to create exceptions for Content Control with filter rules of the Compliance Filter that categorize emails as **Clean**.

The filter rules of the Compliance Filter (see About the Compliance Filter on page 472) are processed according to their type (see Types of Filter Rules on page 495) in the following order:

1. Body
2. Header
3. Advanced

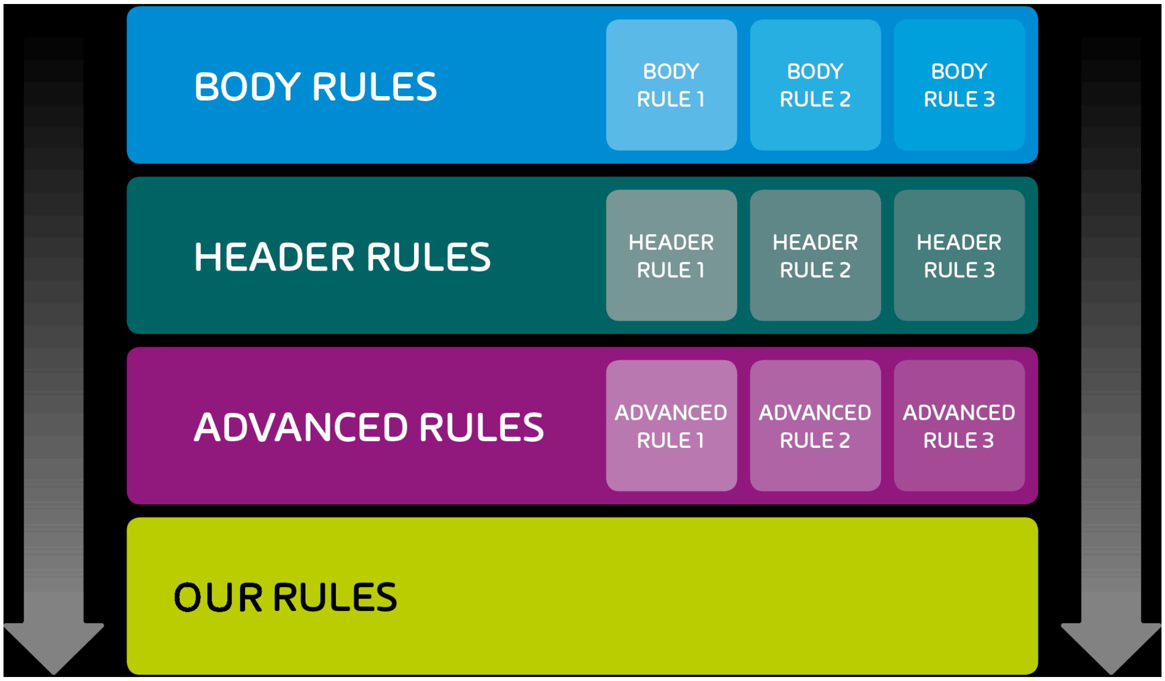


Figure 375: Order of filter rules by type

Filter rules of the same type are sorted according to their priority and processed in this order.

Notice:

The higher the number, the lower the priority of the filter rule.

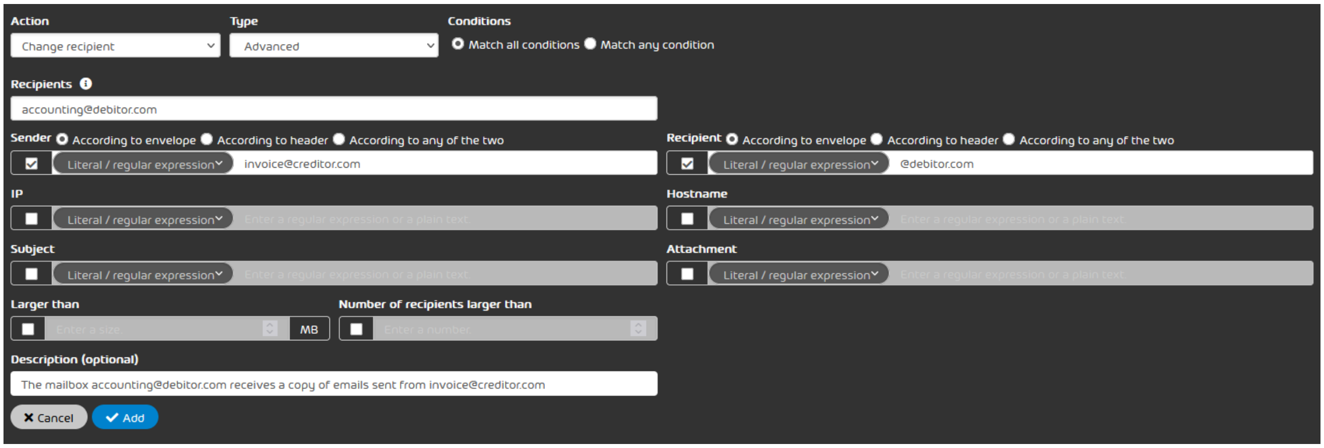
Customer-level administrators can change the priority of a filter rule (see Changing the Priority of a Filter Rule on page 503).

The following examples illustrate the order in which the rules are processed.

Simple processing of filter rules

Initial situation:

A customer-level administrator has defined filter rules for the Compliance Filter. No rules of other services apply to this case.



Action: Change recipient
Type: Advanced
Conditions: ◉ Match all conditions ○ Match any condition

Recipients: accounting@debitor.com

Sender ◉ According to envelope ○ According to header ○ According to any of the two
☑ Literal / regular expression: invoice@creditor.com

Recipient ◉ According to envelope ○ According to header ○ According to any of the two
☑ Literal / regular expression: @debitor.com

IP
☐ Literal / regular expression: Enter a regular expression or a plain text.

Hostname
☐ Literal / regular expression: Enter a regular expression or a plain text.

Subject
☐ Literal / regular expression: Enter a regular expression or a plain text.

Attachment
☐ Literal / regular expression: Enter a regular expression or a plain text.

Larger than
☐ Enter a size. MB

Number of recipients larger than
☐ Enter a number.

Description (optional): The mailbox accounting@debitor.com receives a copy of emails sent from invoice@creditor.com

Figure 376: Filter rule: Forward

Procedure:

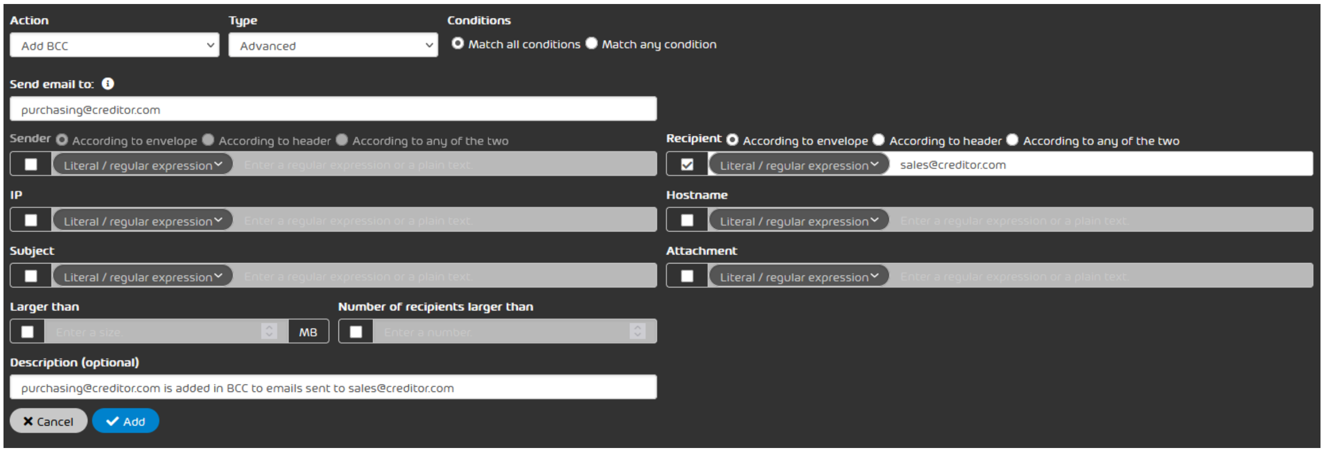
1. An email from **invoice@creditor.com** is sent to any user of the domain debitor.com.
2. The Compliance Filter first searches the filter rules of the type **Body**, then the filter rules of the type **Header** and finds a match in the filter rules of the type **Advanced**.
3. The filter rule is applied. The Compliance Filter does not search for any other matches in other filter rules.

Conflict between several filter rules of the same type

Initial situation:

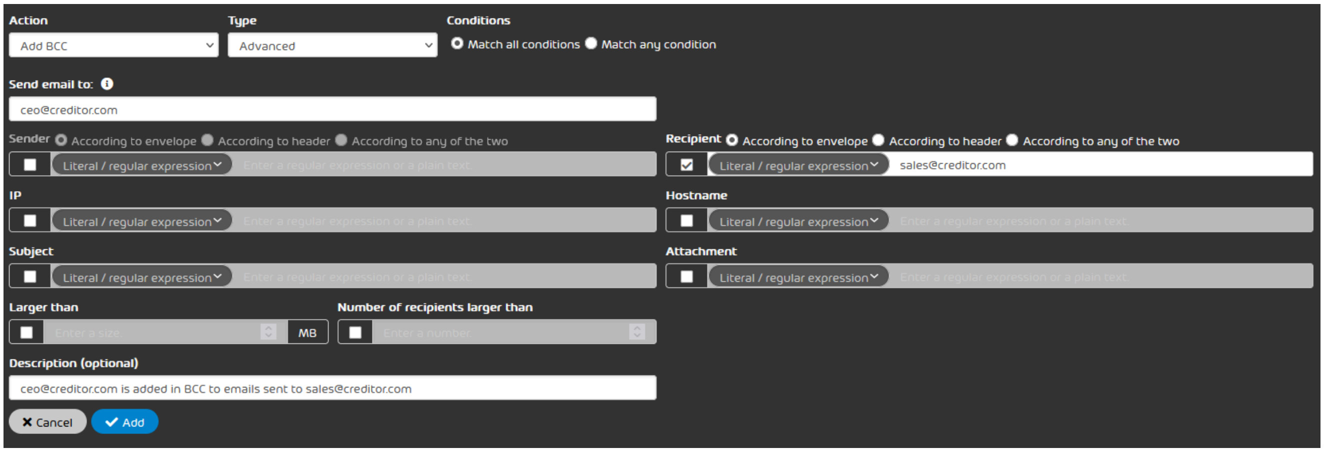
A customer-level administrator has defined two different filter rules of the type **Advanced** for the Compliance Filter for the event that an outgoing email is sent to **sales@creditor.com**.

Both filter rules cause a BCC to be added to the email. For one filter rule the BCC recipient is **purchasing@creditor.com**, for the other one it is **ceo@creditor.com**. The filter rule with the BCC recipient **purchasing@creditor.com** has a higher priority than the filter rule with the BCC recipient **ceo@creditor.com**, and is listed above the other filter rule in the overview of filter rules. No other filter rules apply to this case.



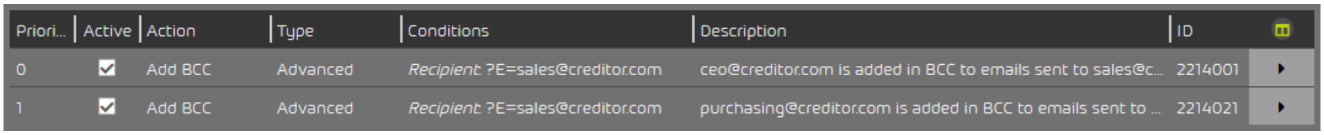
Action: Add BCC
Type: Advanced
Conditions: ● Match all conditions ○ Match any condition
Send email to: purchasing@creditor.com
Sender ● According to envelope ○ According to header ○ According to any of the two
□ Literal / regular expression — Enter a regular expression or a plain text
Recipient ● According to envelope ○ According to header ○ According to any of the two
☑ Literal / regular expression — sales@creditor.com
IP: □ Literal / regular expression — Enter a regular expression or a plain text
Hostname: □ Literal / regular expression — Enter a regular expression or a plain text
Subject: □ Literal / regular expression — Enter a regular expression or a plain text
Attachment: □ Literal / regular expression — Enter a regular expression or a plain text
Larger than: □ Enter a size MB
Number of recipients larger than: □ Enter a number
Description (optional): purchasing@creditor.com is added in BCC to emails sent to sales@creditor.com

Figure 377: Filter rule: add purchasing@creditor.com as BCC recipient



Action: Add BCC
Type: Advanced
Conditions: ● Match all conditions ○ Match any condition
Send email to: ceo@creditor.com
Sender ● According to envelope ○ According to header ○ According to any of the two
□ Literal / regular expression — Enter a regular expression or a plain text
Recipient ● According to envelope ○ According to header ○ According to any of the two
☑ Literal / regular expression — sales@creditor.com
IP: □ Literal / regular expression — Enter a regular expression or a plain text
Hostname: □ Literal / regular expression — Enter a regular expression or a plain text
Subject: □ Literal / regular expression — Enter a regular expression or a plain text
Attachment: □ Literal / regular expression — Enter a regular expression or a plain text
Larger than: □ Enter a size MB
Number of recipients larger than: □ Enter a number
Description (optional): ceo@creditor.com is added in BCC to emails sent to sales@creditor.com

Figure 378: Filter rule: add ceo@creditor.com as BCC recipient



Priori...	Active	Action	Type	Conditions	Description	ID	
0	☑	Add BCC	Advanced	*Recipient:* ?E=sales@creditor.com	ceo@creditor.com is added in BCC to emails sent to sales@c...	2214001	▸
1	☑	Add BCC	Advanced	*Recipient:* ?E=sales@creditor.com	purchasing@creditor.com is added in BCC to emails sent to ...	2214021	▸

Figure 379: Order of filter rules

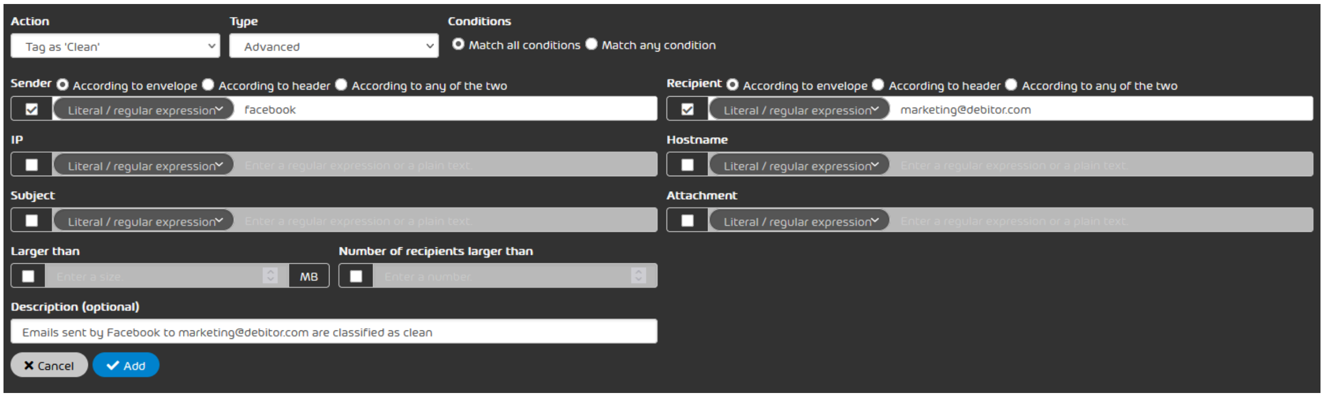
Procedure:

1. An email from any sender is sent to **sales@creditor.com**.
2. The Compliance Filter first searches the filter rules of the type **Body**, then the filter rules of the type **Header** and finds a match in the filter rules of the type **Advanced**.
3. The filter rule with the higher priority (BCC to **purchasing@creditor.com**) is applied. The Compliance Filter does not search for any other matches in other filter rules. The filter rule with the lower priority (BCC to **ceo@creditor.com**) is not applied.

Conflict between rules of different types

Initial situation:

A customer-level administrator has defined a filter rule establishing that incoming emails with a link to Facebook should be categorized as **Spam**. In another filter rule, the administrator had defined an exception for the recipient **marketing@debitor.com**. The exception defined by the administrator causes emails sent directly from Facebook to **marketing@debitor.com** to be categorized as **Clean**. The filter rule with the exception for **marketing@debitor.com** has a higher priority than the filter rule for emails with links to Facebook, and is listed above the other filter rule in the overview of filter rules. No other filter rules apply to this case.



Action: Tag as 'Clean'

Type: Advanced

Conditions: ● Match all conditions ○ Match any condition

Sender ● According to envelope ○ According to header ○ According to any of the two

☑ Literal / regular expression facebook

Recipient ● According to envelope ○ According to header ○ According to any of the two

☑ Literal / regular expression marketing@debitor.com

IP

□ Literal / regular expression Enter a regular expression or a plain text.

Hostname

□ Literal / regular expression Enter a regular expression or a plain text.

Subject

□ Literal / regular expression Enter a regular expression or a plain text.

Attachment

□ Literal / regular expression Enter a regular expression or a plain text.

Larger than

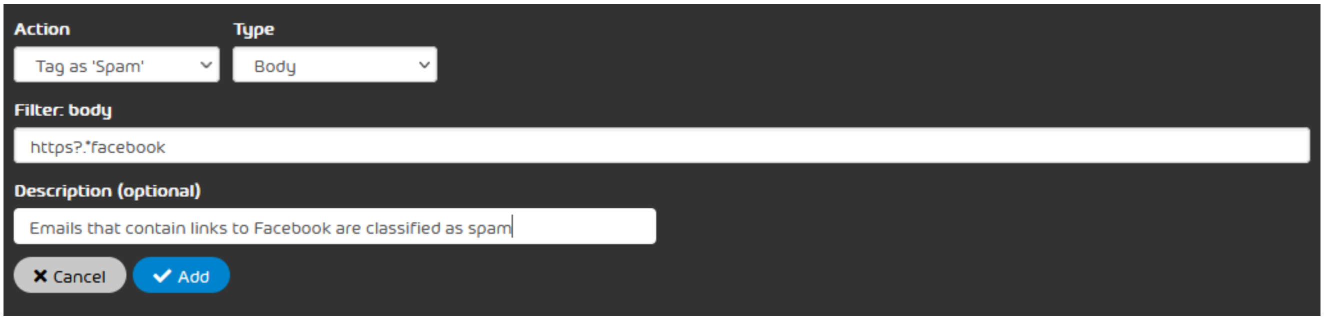
□ Enter a size. MB

Number of recipients larger than

□ Enter a number.

Description (optional): Emails sent by Facebook to marketing@debitor.com are classified as clean

Figure 380: Filter rule: Tag as clean



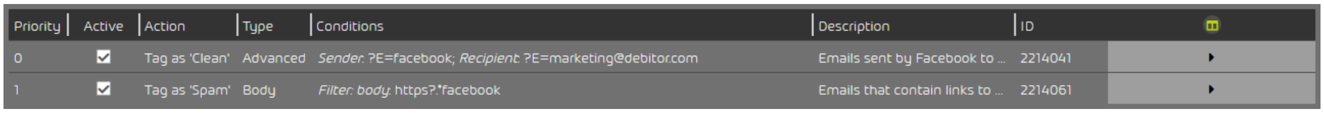
Action: Tag as 'Spam'

Type: Body

Filter: body: https?.*facebook

Description (optional): Emails that contain links to Facebook are classified as spam

Figure 381: Filter rule: Tag as spam



Priority	Active	Action	Type	Conditions	Description	ID
0	☑	Tag as 'Clean'	Advanced	*Sender:* ?E=facebook; *Recipient:* ?E=marketing@debitor.com	Emails sent by Facebook to ...	2214041
1	☑	Tag as 'Spam'	Body	*Filter: body:* https?.*facebook	Emails that contain links to ...	2214061

Figure 382: Order of filter rules

Procedure:

1. Facebook sends an email with a link to **marketing@debitor.com**.

2. The Compliance Filter first searches the filter rules of the type **Body** and finds a match in the filter rule for emails that contain links to Facebook.

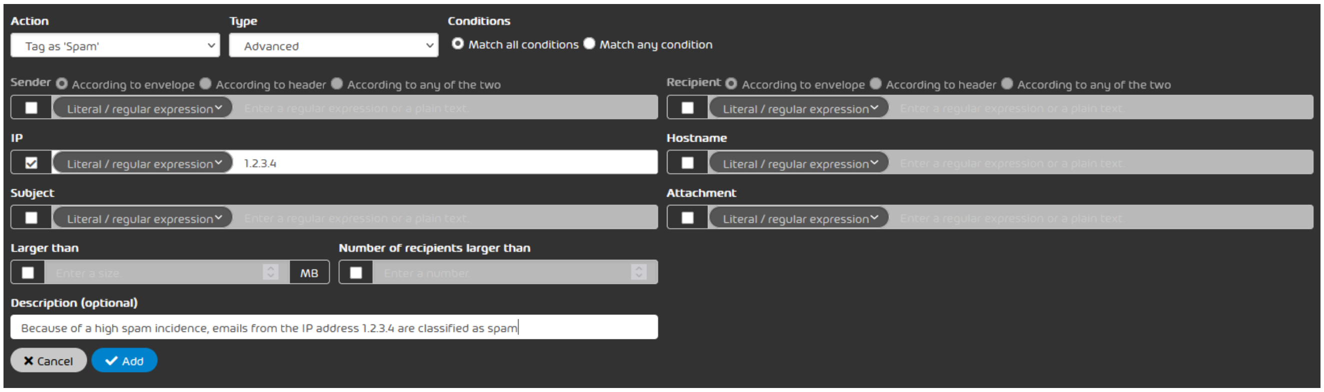
3. The filter rule is applied to the email and the email is categorized as **Spam**. The Compliance Filter does not search for any other matches in other filter rules. Despite its higher priority, the

filter rule with the exception for **marketing@debitor.com** is not applied because the filter rules of the type **Body** take precedence over the filter rules of other types.

Conflict between the Compliance Filter and our filter rules

Initial situation:

Due to a high spam volume from one IPv4 address, a customer-level administrator has defined a filter rule establishing that emails from this IP address should be tagged as spam. No other filter rules of the Compliance Filter apply to this case. In addition to the filter rule of the Compliance Filter, a filter rule defined by us applies to this case.



Action: Tag as 'Spam'
Type: Advanced
Conditions: ● Match all conditions ○ Match any condition
Sender: ● According to envelope ○ According to header ○ According to any of the two
□ Literal / regular expression — Enter a regular expression or a plain text.
Recipient: ● According to envelope ○ According to header ○ According to any of the two
□ Literal / regular expression — Enter a regular expression or a plain text.
IP: ☑ Literal / regular expression — 1.2.3.4
Hostname: □ Literal / regular expression — Enter a regular expression or a plain text.
Subject: □ Literal / regular expression — Enter a regular expression or a plain text.
Attachment: □ Literal / regular expression — Enter a regular expression or a plain text.
Larger than: □ Enter a size. MB
Number of recipients larger than: □ Enter a number.
Description (optional): Because of a high spam incidence, emails from the IP address 1.2.3.4 are classified as spam

Figure 383: Filter rule: Tag emails from an IPv4 address as spam

Procedure:

1. A sender from the domain behind the IPv4 address sends an email to any recipient.
2. The Compliance Filter first searches the filter rules of the type **Body**, then the filter rules of the type **Header** and finds a match in the filter rules of the type **Advanced**.
3. The filter rule is applied to the email and the email is categorized as **Spam**. The Compliance Filter does not search for any other matches in other filter rules.
4. We have already defined a more precise filter rule for this case. The high spam volume could be narrowed down to the sender **info@**. Other email addresses of the domain do not send any spam emails. Since our filter rules are not searched anymore, the filter rule defined by the

customer-level administrator, the scope of which is too extensive, is applied. A clean email could thus be tagged as spam.

Activating a Filter Rule

You have deactivated a filter rule of the Compliance Filter (see Deactivating a Filter Rule of the Compliance Filter on page 513).

If you would like to apply a deactivated rule of the Compliance Filter (see About the Compliance Filter on page 472) again, you can activate the filter rule in the **Security Settings** > **Compliance Filter** module.

1. Log in to the Control Panel with your administrative credentials.
2. Select a domain from the scope selection.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Select the **Rules** tab.
5. Select the desired filter rule from the list of filter rules for incoming or outgoing emails and activate the checkbox in the column **Active**.

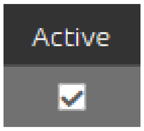


Figure 384: Activate filter rule

The filter rule is activated. The filter rule is applied to the email traffic of the domain.

A filter rule of the Compliance Filter has been activated.

Deactivating a Filter Rule of the Compliance Filter

You have activated the Compliance Filter for the selected domain (see Activating Compliance Filter on page 475) and have created filter rules for the Compliance Filter (see Creating a Filter Rule for Incoming Emails on page 477 or Creating a Filter Rule for Outgoing Emails on page 484)

If you would like to temporarily suspend a filter rule of the Compliance Filter (see About the Compliance Filter on page 472), you can deactivate it in the **Security Settings** > **Compliance Filter** module.

1. Log in to the Control Panel with your administrative credentials.
2. Select a domain from the scope selection.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Select the **Rules** tab.
5. Select the desired rule from the list of filter rules for incoming or outgoing emails, and deactivate the checkbox in the column **Active**.

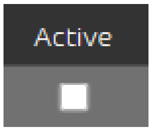


Figure 385: Deactivate the filter rule

The filter rule is deactivated. The filter rule is applied to the email traffic of the domain.

A filter rule of the Compliance Filter has been deactivated.

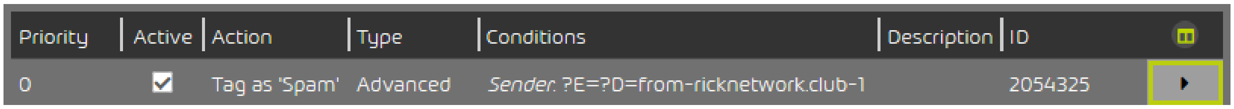
Next, you can reactivate the filter rule if it should be applied again (see Activating a Filter Rule on page 512).

Deleting a Filter Rule of the Compliance Filter

You have activated the Compliance Filter for the selected domain (see Activating Compliance Filter on page 475) and have created filter rules for the Compliance Filter (see Creating a Filter Rule for Incoming Emails on page 477 or Creating a Filter Rule for Outgoing Emails on page 484)

In the **Security Settings** > **Compliance Filter** module, you can delete filter rules of the Compliance Filter that you no longer need.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to delete a filter rule.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Select the **Rules** tab.
5. In the list of rules for incoming or outgoing emails, click on the menu arrow next to the filter rule you would like to delete.

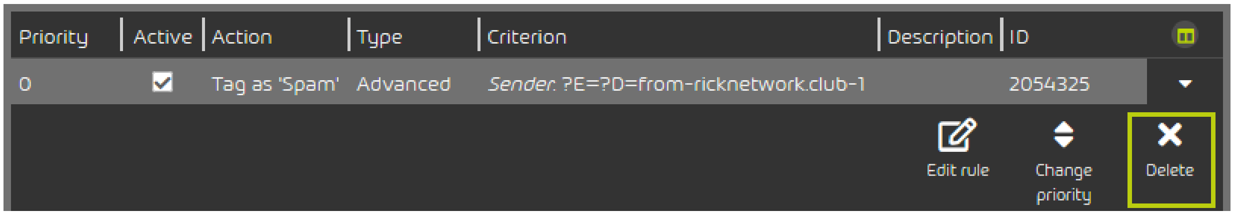


Priority	Active	Action	Type	Conditions	Description	ID	
0	☑	Tag as 'Spam'	Advanced	*Sender:* ?E=?D=from-ricknetwork.club-1		2054325	▸

Figure 386: Open the menu

A menu opens.

6. Click on **Delete**.

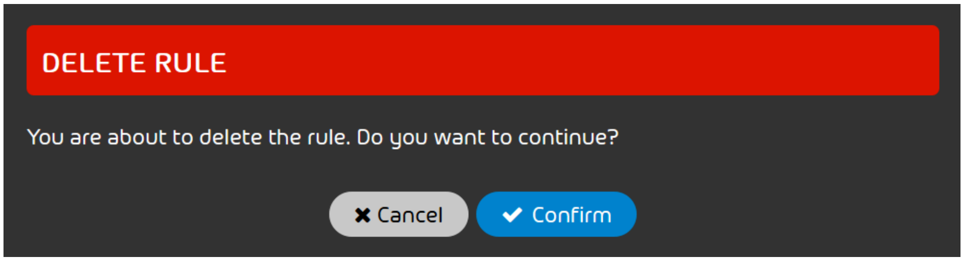


Priority	Active	Action	Type	Criterion	Description	ID
0	☑	Tag as 'Spam'	Advanced	*Sender*: ?E=?D=from-ricknetwork.club-1		2054325

Figure 387: Delete filter rule

A warning message is displayed.

7. Click on **Confirm**.



DELETE RULE

You are about to delete the rule. Do you want to continue?

Figure 388: Confirm deletion

The filter rule is deleted.

A filter rule of the Compliance Filter has been deleted.

Dictionaries

Dictionaries are sets of expressions that can be used to create filter rules in the **Security Settings** > **Compliance Filter** module (see About the Compliance Filter on page 472). The expressions of a dictionary can either all be interpreted as literal or as regular expressions. Regular expressions are more accurate and reduce the number of entries to be created and maintained.

Notice:

Up to 250 dictionaries can be created for a primary domain.

Dictionaries with regular expressions can contain up to 1000 entries whereas dictionaries with literal expressions can contain up to 15000 entries.

When creating filter rules of the type **Advanced** (see Creating a Filter Rule for Incoming Emails on page 477 or Creating a Filter Rule for Outgoing Emails on page 484), customer-level administrators can reference a dictionary in some conditions instead of entering a single expression. In order to reference an existing dictionary, administrators must enter the name of the dictionary in the input field of the condition and select from a drop-down menu how the expressions of the dictionary shall be interpreted by the filter rule. With the **Contained in dictionary** option, the filter rule applies if at least one expression from the dictionary matches an email. The expressions of the dictionary are thus logically linked with an OR within the condition. With the **Not contained in dictionary** option, the filter rule applies if no expression matches.

Dictionaries facilitate the creation of filter rules of the Compliance Filter because a single filter rule can apply to emails with different values for a condition. For instance, a single filter rule could mark emails from the senders **@facebook**, **@instagram** or **@tiktok** that are sent to email addresses from the marketing department as clean if a dictionary with these three terms is created and referenced in the condition **Sender** (see Types of Filter Rules on page 495). In order to have the same behavior of the Compliance Filter without referencing a dictionary, either three different filter rules containing one literal expression for a sender each or a single filter rule containing a regular expression with OR operators between the different senders would be required. The latter solution might be impractical for a high number of specified senders.

Another use case is to reject all incoming emails containing swear words. To do this, a customer-level administrator would create a dictionary of swear words and reference it in a filter rule for incoming emails. Creating and maintaining individual filter rules for each swear word instead would be much more time-consuming.

Customer-level administrators can create dictionaries (see Creating a Dictionary on page 517), edit existing dictionaries (see Editing a Dictionary on page 520) and delete them (see Deleting a Dictionary on page 522).

Creating a Dictionary

You have activated the Compliance Filter for the selected domain (see Activating Compliance Filter on page 475).

In the **Compliance Filter** > **Dictionaries** module, you can create dictionaries (see Dictionaries on page 515) for the Compliance Filter. Dictionaries allow you to easily create complex filter rules (see Creating a Filter Rule for Incoming Emails on page 477 and Creating a Filter Rule for Outgoing Emails on page 484).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to create a dictionary.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Select the tab **Dictionaries**.

5. Click on **Add**.

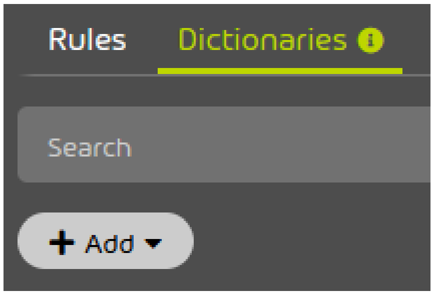
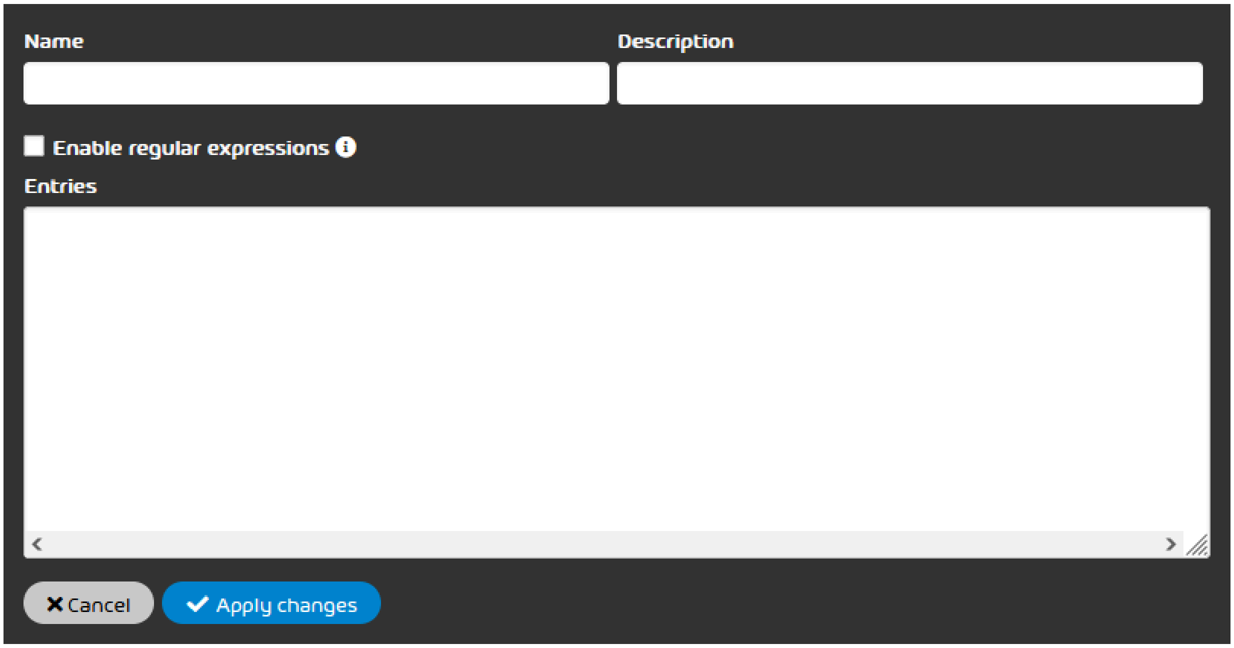


Figure 389: Add a dictionary

➜

A form for creating a dictionary is displayed.


Name

Description

□ Enable regular expressions

Entries

Figure 390: Form for a dictionary

6. Enter a name for the dictionary in the field **Name**.

> **Notice:**
>
> The name may only contain the following characters:
>
> - Latin lower case letters from a-z
> - digits from 0-9
> - Special characters **- _ . , =**
>
> Whitespaces and colons are not allowed.

7. Optional: Enter a description for the dictionary in the field **Description**.
8. Optional: If the entries of the dictionary are to be interpreted as regular expressions, tick the checkbox **Enable regular expressions**.

> **Notice:**
>
> If this option is selected, all entries of the dictionary must comply with the rules of regular expressions (see Explanation of Regular Expressions on page 526) and their exceptions (see Exceptions to Regular Expressions on page 533).

9. Enter the desired exceptions in the field **Entries**.

> **Notice:**
>
> Each line corresponds to an entry. The maximum line length is 1000 characters. The number of entries is limited to 15000 literal expressions and to 1000 regular expressions. Blank lines and duplicate entries are ignored and removed when the dictionary is saved.

10. Click on **Apply changes**.

    ➜

    If the checkbox **Enable regular expressions** is ticked, we check whether the regular expressions are correct.

    The form is closed, the dictionary is saved and added to the table of dictionaries.

✓

A dictionary has been created.

Next, you can edit (see Editing a Dictionary on page 520) or delete (see Deleting a Dictionary on page 522) the dictionary. You can reference the dictionary in filter rules of the Compliance Filter (see Creating a Filter Rule for Incoming Emails on page 477 and Creating a Filter Rule for Outgoing Emails on page 484).

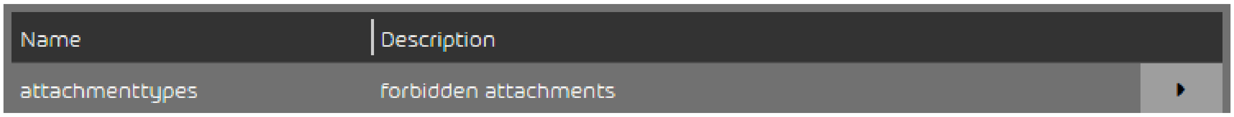
Editing a Dictionary

You have created a dictionary (see Creating a Dictionary on page 517).

In the **Security Settings** > **Compliance Filter** module, you can edit existing dictionaries (see Dictionaries on page 515) of the Compliance Filter (see About the Compliance Filter on page 472).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to edit a dictionary.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Select the tab **Dictionaries**.

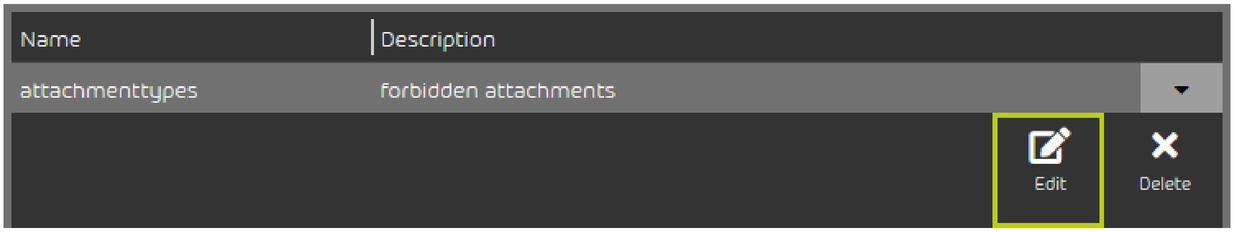
5. In the list of dictionaries, click on the menu arrow next to the dictionary that you would like to edit.



Name	Description
attachmenttypes	forbidden attachments

Figure 391: Open the menu

6. Click on **Edit**.



Name	Description
attachmenttypes	forbidden attachments

Figure 392: Edit the dictionary

➜

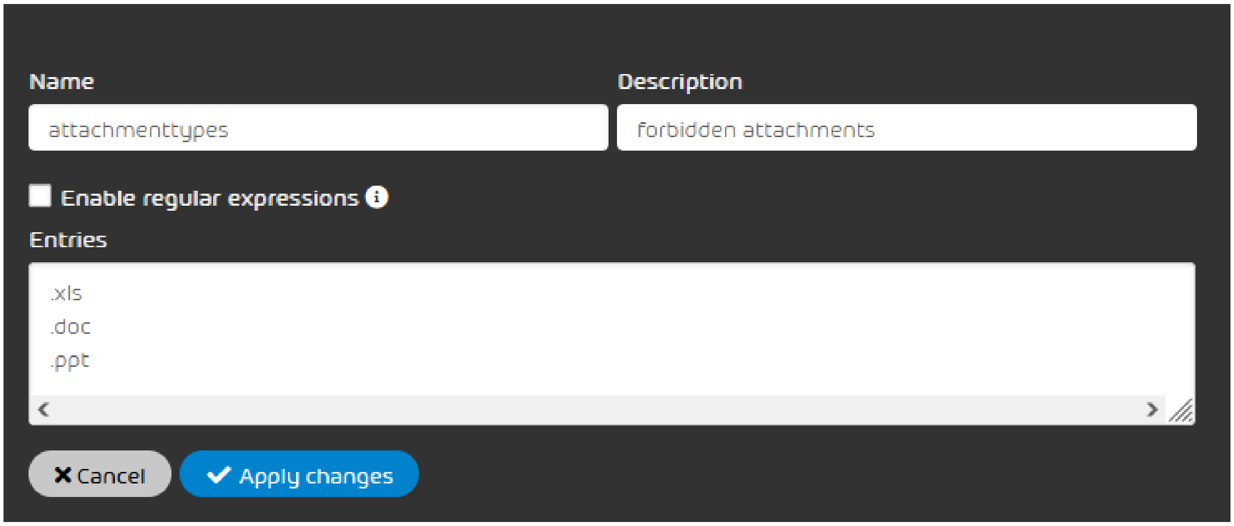
A form with the current settings of the dictionary opens.

7. Edit the settings as desired.

Notice:

For more information, see Creating a Dictionary on page 517.

8. Click on **Apply changes**.



Name

attachmenttypes

Description

forbidden attachments

□ Enable regular expressions

Entries

.xls
.doc
.ppt

Figure 393: Apply changes

The changes are applied.

Notice:

If the dictionary has been renamed and it is already referenced in filter rules, the name of the dictionary will also be updated in these filter rules.

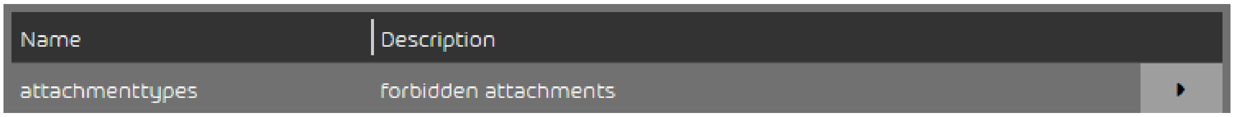
A dictionary has been edited.

Deleting a Dictionary

You have created a dictionary (see Creating a Dictionary on page 517). The dictionary is not referenced in any filter rule of the Compliance Filter.

If you no longer need an existing dictionary (see Dictionaries on page 515) of the Compliance Filter (see About the Compliance Filter on page 472), you can delete it in the **Security Settings** > **Compliance Filter** module.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to delete a dictionary.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Select the tab **Dictionaries**.
5. In the list of dictionaries, click on the menu arrow next to the dictionary that you would like to delete.

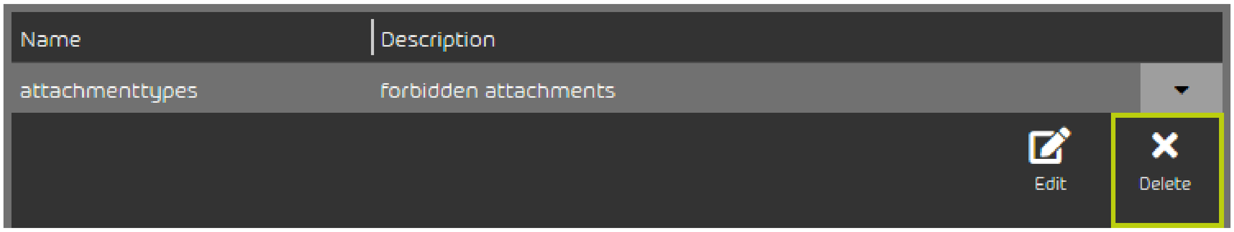


Name	Description
attachmenttypes	forbidden attachments

Figure 394: Open the menu

A menu opens.

6. Click on **Delete**.

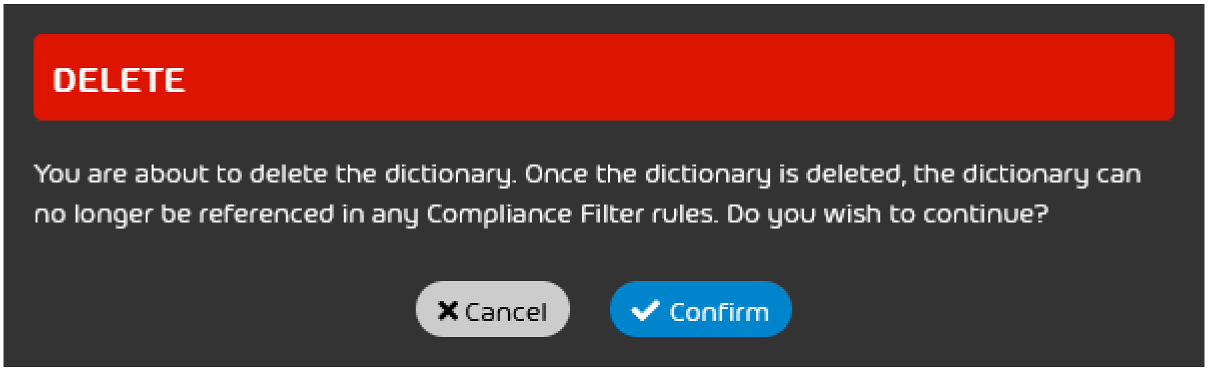


Name	Description
attachmenttypes	forbidden attachments

Figure 395: Delete the dictionary

A warning message is displayed.

7. Click on **Confirm**.



DELETE

You are about to delete the dictionary. Once the dictionary is deleted, the dictionary can no longer be referenced in any Compliance Filter rules. Do you wish to continue?

Figure 396: Confirm deletion

We check whether the dictionary is referenced in any filter rules of the Compliance Filter. If it is not referenced anywhere, the dictionary is deleted.

A dictionary has been deleted.

Regular Expressions

In the filter rules of the Compliance Filter (see Filter Rules on page 476), regular expressions (RegEx for short) can be used to extract information from strings. This way, it is possible to recognize patterns in the subject or other components of an email, and to filter emails.

Notice:

The system automatically adds the sequence **.*** at the beginning and the end of regular expressions in the **Compliance Filter** module unless the regular expression starts with **^** or ends with **$**.

Notice:

By appending a question mark, the quantifiers **+** and ***** (see table Syntax elements and special characters in chapter Explanation of Regular Expressions on page 526) are automatically made lazy before the regular expressions are evaluated.

"Lazy" is the opposite of "greedy" and means that the search ends with the shortest possible match. For instance, the greedy regular expression **a.*b** would find the match **aabcaab** in the string **aabcaabcdf**. In contrast, the lazy expression **a.*?b** would find the match **aab** twice in the same string.

Important:

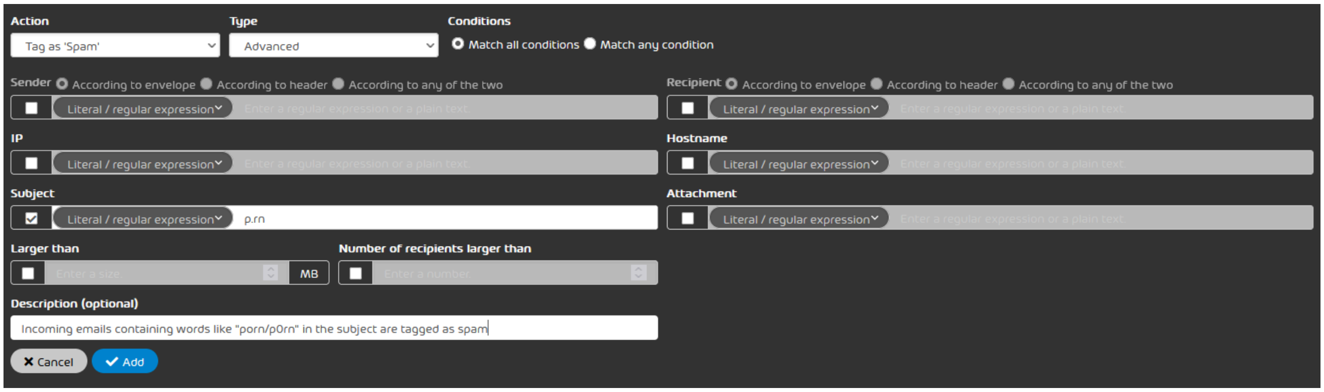
In the **Compliance Filter** module, regular expressions can only be used in filter rules of the type **Advanced** (see Types of Filter Rules on page 495) and in dictionaries (see Dictionaries on page 515).

For an explanation and examples of regular expressions, see Explanation of Regular Expressions on page 526 and Examples for Complex Regular Expressions on page 536.

Within the Compliance Filter, regular expressions according to Perl Compatible Regular Expressions can be defined. Other libraries are not supported. For more information, see: http://www.pcre.org/. In addition, there are special restrictions that are explained in Exceptions to Regular Expressions on page 533.

Example: Using regular expressions in the Compliance Filter

Users often received emails with the word "porn" in the subject. A filter rule was defined to mark them as spam. Recently, an increased volume of spam emails using leetspeak to bypass this filter was observed. For example, incoming emails with the subject "p0rn" were not tagged by the Compliance Filter. In this case, the use of a regular expression is more effective:



Action: Tag as 'Spam'

Type: Advanced

Conditions: ● Match all conditions ○ Match any condition

Sender ● According to envelope ○ According to header ○ According to any of the two

□ Literal / regular expression

Recipient ● According to envelope ○ According to header ○ According to any of the two

□ Literal / regular expression

IP

□ Literal / regular expression

Hostname

□ Literal / regular expression

Subject

☑ Literal / regular expression p.rn

Attachment

□ Literal / regular expression

Larger than

□ MB

Number of recipients larger than

□

Description (optional)

Incoming emails containing words like "porn/p0rn" in the subject are tagged as spam

Figure 397: Use of a regular expression in the Compliance Filter

The dot matches any character. The filter is not limited to an "o" in this place, but reacts to any letter, digit and special character.

Explanation of Regular Expressions

In the following examples for regular expressions, the text in the left column is validated against the regular expression in the right column. The text marked in bold is matched by the regular expression.

Individual characters

Table 30: Matching letters

TEXT	REGEX
abcdef	**abc**
abcde	
Abcd	

With letters, you can search anywhere inside a text for matches.

Table 31: Matching characters from a selection of characters

TEXT	REGEX
ac**bde**f	[abc]de
adefg	

A selection of characters searches individually for each of the characters that are bundled together by square brackets to form a selection.

Table 32: Matching characters from character ranges

TEXT	REGEX
1 Word	[1-5] [A-Z]
7 Words	
2 different words	

Square brackets can also be used to specify character ranges. The first and the last character of the range are separated by a hyphen. The character order is the same as in the ASCII table. Capital letters thus come before lower-case letters. Therefore, the regular expression **[A-z]** finds all ASCII characters from the capital letter A to the lower-case letter z. In contrast, the regular expression **[a-Z]** is invalid and does not find any matches.

Important:

The character range **[A-z]** contains only Latin letters. The following characters are excluded from the character range:

- umlauts (äöü)
- letters with accents (e.g., áéíóú)
- language-specific letters (e.g., ñ or ß)

Table 33: Matching digits

TEXT	REGEX
number = **123**	123 or \d\d\d
var number = **123**	
ab**123**fg	

Digits have the same effect as letters. Instead of a specific digit, the character **\d** can be used to match any digit.

Table 34: Matching letters

TEXT	REGEX
a12**b**34**c**	\w

The expression **\w** matches any Latin letter from A to z (see above) without special characters or language-specific letters.

Table 35: Matching any character

TEXT	REGEX
bob.	···\.
tom.	
?!a.	
abc1	

A single "." matches any character. In order to match a dot, the dot must be escaped with "\.".

Table 36: Matching multiple characters

TEXT	REGEX
abcc	**ab*c**
a**abbbbbc**c	
bb**ac**cc	

Repetitions

The trailing asterisk means that the preceding character may occur any number of times. The character may thus occur not at all, once or multiple times.

Table 37: Matching at least one character

TEXT	REGEX
aaaaaaaaa**abc**	**ab+c**
a**abbbc**	
ac	

The trailing plus sign means that the character must occur at least once and may occur multiple times. If it does not occur, there is no match.

Table 38: Defining the number of character repetitions

TEXT	REGEX
12 **123 4544 1564**14	**\d{3,4}**

A given number or an interval for the number of repetitions of the preceding character can be specified in curly brackets. The example above searches for character sequences that contain only digits and consist of 3 to 4 characters. The following combinations are possible:

- {m}: The preceding character must occur exactly m times.
- {m,}: The preceding character must occur at least m times.
- {m,n}: The preceding character must occur at least m times and at most n times.

Table 39: Optional characters

TEXT	REGEX
3 users online	**\d+ users? online**
150 users online	
20 users online	
1 user online	
no user online	

By appending a "?", the leading character is declared as optional.

Groups

Table 40: Grouping regular expressions

TEXT	REGEX
dump025.csv	**\w+\d+\.(\w+)**
dump026.csv	

Parentheses around a part of the regular expression group the enclosed elements. In the example above, the file extension after the dot is a group. Several operators handle groups like individual characters. Therefore, trailing quantifiers such as ?, *, + or curly brackets have an effect on the group as a whole and not only on the last character. For instance, the whole group **(abc)?** would be optional. Besides, groups allow advanced operations such as backreferencing (see below). Another advantage is that groups make the expressions easier to read.

Table 41: Matching either/or

TEXT	REGEX
data.csv	**.*\.(exe|xlsx)**
bild.jpg	
moving.gif	
document.pdf	
virus.exe	
locky.xlsx	

A vertical bar **|** within parentheses separates character sequences from each other that are to be searched for alternatively.

Table 42: Backreferencing

TEXT	REGEX
From: "local@domain.com" <local@domain.com>	**From: "(*@.*\.com)" <\1>**
"local@domain.com" <hacker@hackeddomain.com>	

The backreference \1 stands for the group definition (.*@.*\.com). A match is only made if the match of the group appears again at the referenced place.

Syntax elements and special characters

The following syntax elements can be used to define regular expressions in the Compliance Filter:

Table 43: Syntax elements

WILDCARD/CHARACTER CLASS	FUNCTION
abc...	Letters
123...	Digits
[abc]	Any of the characters a, b or c
[a-z]	Any ASCII character from the specified range
\d	Any digit
.	Any character
. **/** \ *****	Escaping the characters in bold
\w	Any alphanumeric character
*	0 or more repetitions of the preceding expression
+	1 or more repetitions of the preceding expression
?	The preceding expression is optional
{m}	Exactly m repetitions of the preceding expression
{m,}	At least m repetitions of the preceding expression

WILDCARD/CHARACTER CLASS	FUNCTION
{m, n}	m to n repetitions of the preceding expression
\s	Any whitespace
(…)	Extraction group
(.*)	All
(abc|def)	abc or def
^	Beginning of the string
$	End of the string

The special characters from the table above are interpreted as part of a regular expression by default. However, it is also possible to search for these special characters literally. To do so, the functions of these special characters must be bypassed with a preceding backslash ****. For instance, the expression **a*** does not find any number of As but the literal character sequence **a***.

Exceptions to Regular Expressions

The creation of regular expressions for filter rules of the Compliance Filter (see **About the Compliance Filter** on page 472 and **Filter Rules** on page 476) differs from the creation of PCRE-compliant expressions because not all their syntax elements can be used in the Compliance Filter. Basically, characters from the extended ASCII table are allowed. When checking regular expressions, no distinction is made between upper and lower case.

Different restrictions apply to expressions that are entered directly in the input fields of filter rules in the **Compliance Filter** module and to those in dictionaries (see **Dictionaries** on page 515).

The following characters **cannot** be used in the input fields of filter rules in the **Compliance Filter** module whose values are interpreted as regular expressions:

- Semicolon ;

- Degree sign °
- Asterisk * at the beginning of an entry
- Slash / (unless it is escaped with \)

The following characters **cannot** be used in dictionaries of the **Compliance Filter** module whose entries are interpreted as regular expressions:

- Degree sign °
- Slash / (unless it is escaped with \)

Notice:

The vertical bar | (pipe) is both in input fields of filter rules and in dictionaries only allowed inside a group between parentheses. Furthermore, a single vertical bar | is used whenever it has the meaning OR. Two vertical bars || are interpreted as a wildcard and mean that all characters will be accepted.

Common Use Cases of Regular Expressions

In the following, sample regular expressions (see Explanation of Regular Expressions on page 526) of common use cases in the Compliance Filter (see About the Compliance Filter on page 472) are presented.

Different hostnames with the same ending

When creating filter rules for emails that are sent from or to the email servers of different subdomains of a specific domain, the condition **Hostname** in the **Security Settings** > **Compliance Filter** module can be used to search for strings with a certain ending.

The following regular expression can be used for this search:

String^

The circumflex means that the string that is searched for must be found at the end of the checked hostname. For instance, the regular expression **.*domain\.tld^** would find emails from or to the email servers of the domain **domain.tld** and all its subdomains (e.g., **marketing.domain.tld**, **sales.domain.tld**, **accounting.domain.tld**)

Numbered hostnames of email servers

Often, the only difference between the different email servers of a domain is their number. In order to process emails from and to these email servers using filter rules of the Compliance Filter, the condition **Hostname** can search for strings that only differ in their numbering.

The following regular expression can be used for this search:

(string before numbering)\d+(string after numbering)

Notice:

The brackets in this expression are optional and were used for clarity.

The sequence **\d+** stands for "at least one digit". For instance, the regular expression **mx\d+\.domain\.tld** would find emails from or to the following email servers: **mx3.domain.tld**, **mx30.domain.tld**, **mx100.domain.tld**.

Several specific email addresses of a domain

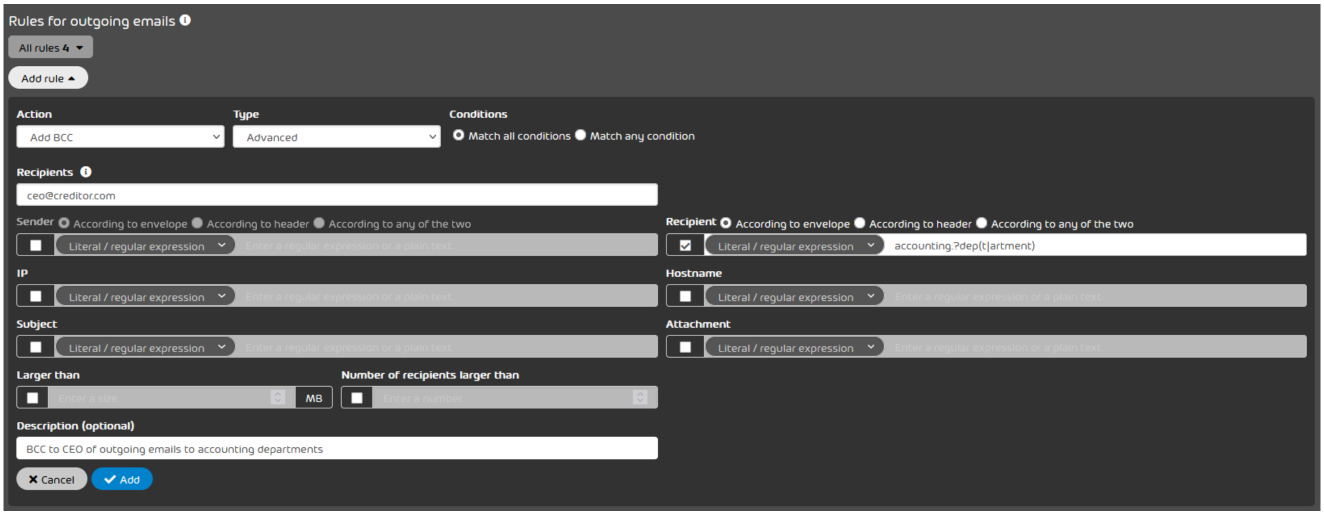
In order for a filter rule to be applied to a small number of email addresses of a domain, a regular expression with the following pattern can be used for the condition **Sender** or **Recipient**:

(user1|user2|user3)@domain

The symbol **|** separates several alternative strings from each other, one of which must be found. The alternative strings must be in brackets. For instance, the regular expression **(evan|peter|sandra)@domain.com** would find emails from and to the following email servers: **evan@domain.com**, **peter@domain.com**, **sandra@domain.com**.

Examples for Complex Regular Expressions

To conclude, we are taking a look at the usage of complex regular expressions (see Explanation of Regular Expressions on page 526) within filter rules of the Compliance Filter (see About the Compliance Filter on page 472).



Rules for outgoing emails

All rules 4

Add rule

Action: Add BCC

Type: Advanced

Conditions: ◉ Match all conditions ○ Match any condition

Recipients: ceo@creditor.com

Sender ◉ According to envelope ○ According to header ○ According to any of the two
□ Literal / regular expression: Enter a regular expression or a plain text.

Recipient ◉ According to envelope ○ According to header ○ According to any of the two
☑ Literal / regular expression: accounting.?dep(t|artment)

IP
□ Literal / regular expression: Enter a regular expression or a plain text.

Hostname
□ Literal / regular expression: Enter a regular expression or a plain text.

Subject
□ Literal / regular expression: Enter a regular expression or a plain text.

Attachment
□ Literal / regular expression: Enter a regular expression or a plain text.

Larger than
□ Enter a size. MB

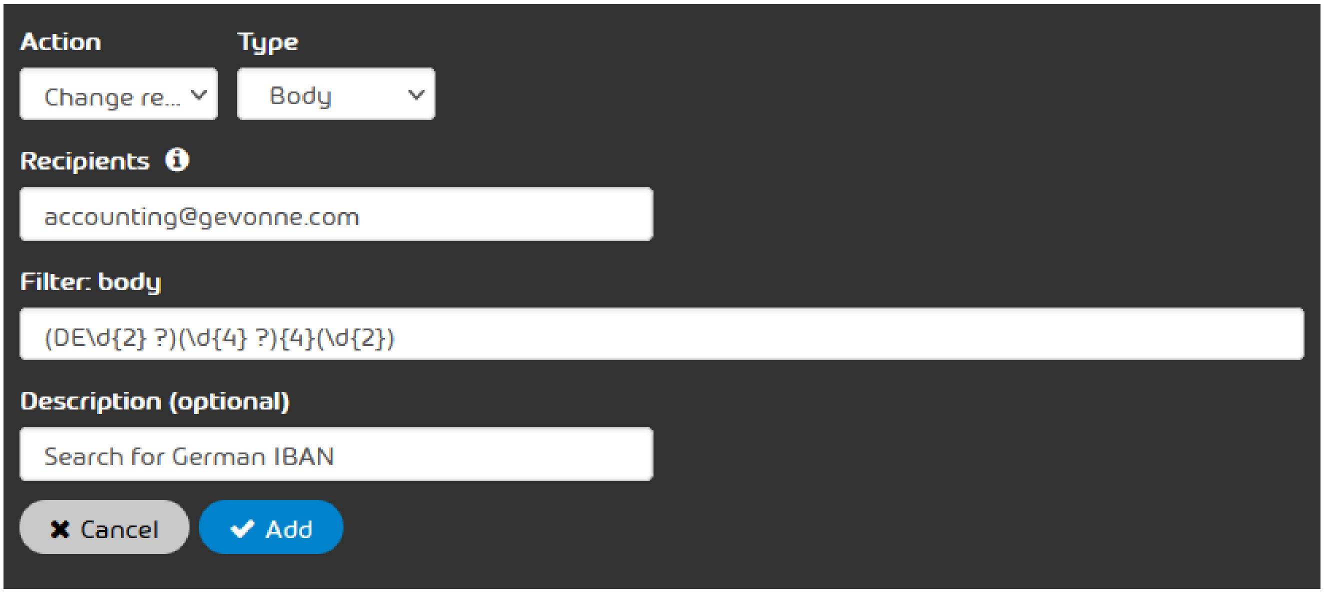
Number of recipients larger than
□ Enter a number.

Description (optional): BCC to CEO of outgoing emails to accounting departments

Figure 398: Search for recipients

In this first example, a customer would like their CEO to receive blind copies of outgoing emails that are sent to the accounting departments of the company's customers. These email addresses follow a certain pattern. The regular expression **accounting.?dep(t|artmen)** finds the following text segments and many other combinations:

- **accountingdepartment@test.com**
- **accounting_department@test.com**
- **accounting_dept@test.com**
- **accounting.department@anothertest.com**



Action: Change re...

Type: Body

Recipients: accounting@gevonne.com

Filter: body: (DE\d{2} ?)(\d{4} ?){4}(\d{2})

Description (optional): Search for German IBAN

Figure 399: Search for IBAN in email body

In this example, a customer would like to forward all incoming emails that contain German IBAN account numbers in the email body to their accounting department. The regular expression **(DE \d{2} ?)(\d{4} ?){4}(\d{2})** can be used to search for German IBAN numbers. This regular expression finds both German IBAN account numbers without whitespaces and German IBAN account numbers that are divided into 4-character blocks and a 2-character block at the end according the usual notation.

- **DE12345678901234567890**
- **DE12 3456 7890 1234 5678 90**

Deactivating Compliance Filter

If you no longer want to use the filter rules of the Compliance Filter (see About the Compliance Filter on page 472), you can deactivate the Compliance Filter in the **Security Settings** > **Compliance Filter** module. This action deletes all created rules.

1. Log in to the Control Panel with your administrative credentials.

2. From the scope selection, select the domain for which you would like to deactivate the Compliance Filter.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Toggle the switch **Activate Compliance Filter**.

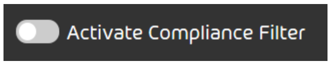
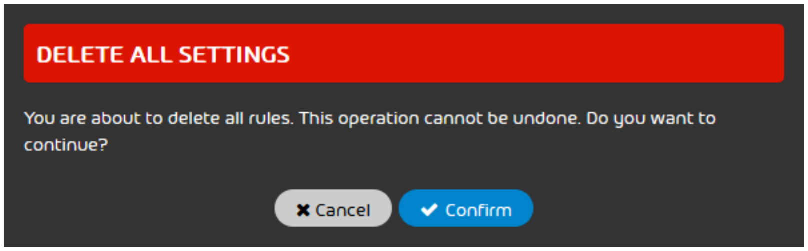


Figure 400: Deactivate Compliance Filter

➜

A confirmation window opens.

5. Click on **Confirm**.



DELETE ALL SETTINGS

You are about to delete all rules. This operation cannot be undone. Do you want to continue?

Figure 401: Confirm

➜

The Compliance Filter is deactivated. All rules are deleted. The settings in the **Compliance Filter** module are disabled. No further input is possible.

✓

The Compliance Filter has been deactivated.

Signature and Disclaimer

About Signature and Disclaimer

Signature and Disclaimer controls the automated and centralized provision of email signatures and disclaimers. Signatures and disclaimers can be created either for all mailboxes of a domain or only for the mailboxes of a certain group (see 'Groups' in the Control Panel manual). The tool dynamically generates user specific signatures, matching the Active Directory. The signatures are based on predefined templates and are included automatically after the current text of the email. For this purpose, Active Directory variables (AD variables) are used. These variables are integrated into the signature or disclaimer and retrieve information from the corresponding Active Directory attributes. For mailboxes that have been manually created in the Control Panel and that are not synchronized with LDAP (see chapter "Mailbox Types" in the Control Panel manual), the AD variables are used to retrieve basic data of the mailbox.

Only customers whose users and groups are synchronized with LDAP from a Microsoft Active Directory can use AD variables. Other directory services are not supported.

Notice:

Signatures and disclaimers are added to all emails sent via our relay servers. Signatures and disclaimers are thus also added to emails sent within a company as long as they are routed through are infrastructure.

Customer-level administrators and users with the **Marketing** role (see Access to the Signature and Disclaimer Module on page 540) can configure signatures and disclaimers. The functions of Signature and Disclaimer are also available for mobile phones (see Mobile Use of Signature and Disclaimer on page 540).

Before Signature and Disclaimer can be used, the service must be activated (see Activating Signature and Disclaimer on page 540). After that, signatures and disclaimers for groups can be created in an editor (see Creating Signatures and Disclaimers on page 542), edited or deleted (see Editing or Deleting a Signature or Disclaimer on page 551). The priority of groups can be changed (see Changing Priorities of Groups on page 547). The editor displays the signatures and disclaimers as they will later be issued (see WYSIWYG Editor on page 554). Images can also be embedded in signatures and disclaimers (see Embedding of Images in Signatures and Disclaimers on page 569). If group-based signatures and disclaimers are created, the priorities of the groups can be changed (see Changing Priorities of Groups on page 547).

If Signature and Disclaimer shall no longer be used, the service can be deactivated (see Deactivating Signature and Disclaimer on page 552).

For more information on how to resolve frequent errors, see Troubleshooting on page 584.

Mobile Use of Signature and Disclaimer

If Signature and Disclaimer is activated, signatures and disclaimers are also attached to emails sent from mobile devices.

Notice:

We support the current latest versions of the operating systems Android and iOS. With older versions, signatures and disclaimers may not be displayed correctly.

Access to the Signature and Disclaimer Module

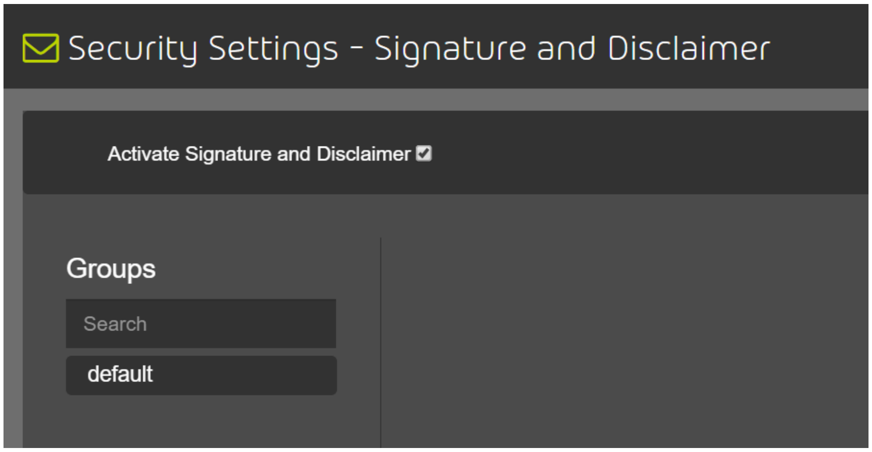
If users without administrative permissions shall create and edit signatures and disclaimers, customer-level administrators can assign them the **Marketing** role (see "Roles" in the Control Panel manual). With the **Marketing** role, users have access to the **Signature and Disclaimer** module (see About Signature and Disclaimer on page 539).

Activating Signature and Disclaimer

You have activated LDAP synchronization (see "Activating the LDAP Connection" in the Control Panel manual) for the domain for which you would like to activate Signature and Disclaimer (see About Signature and Disclaimer on page 539).

In the **Security Settings** > **Signature and Disclaimer** module, you can activate Signature and Disclaimer (see About Signature and Disclaimer on page 539).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to activate Signature and Disclaimer.
3. Navigate to **Security Settings** > **Signature and Disclaimer**.
4. Tick the **Activate Signature and Disclaimer** checkbox.



Security Settings - Signature and Disclaimer

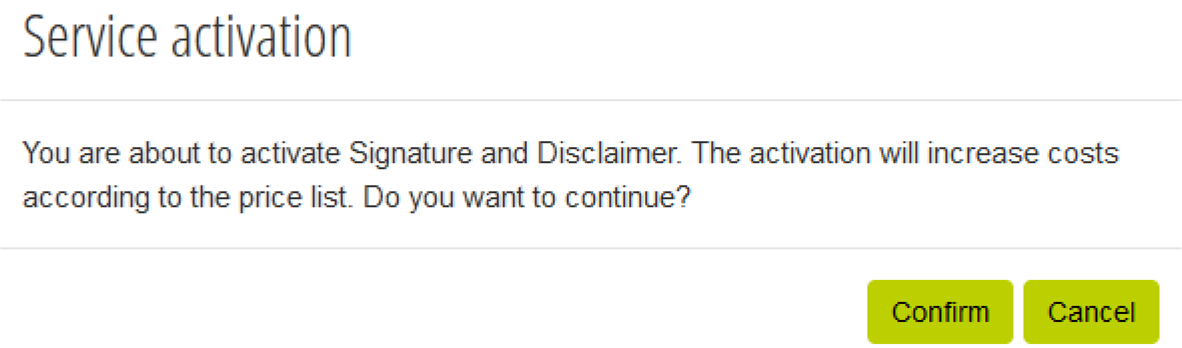
Activate Signature and Disclaimer ☑

Figure 402: Activate Signature and Disclaimer

➜

A confirmation window is displayed.

5. Click on **Confirm**.



Service activation

You are about to activate Signature and Disclaimer. The activation will increase costs according to the price list. Do you want to continue?

Figure 403: Confirm activation

➜

Signature and Disclaimer is activated.

✓

Signature and Disclaimer has been activated.

Next, you can change the priorities of the groups (see Changing Priorities of Groups on page 547). Furthermore, you can create (see Creating Signatures and Disclaimers on page 542), edit or delete (see Editing or Deleting a Signature or Disclaimer on page 551) signatures and disclaimers. If Signature and Disclaimer shall no longer be used, you can deactivate the service (see Deactivating Signature and Disclaimer on page 552).

Creating Signatures and Disclaimers

✓ You have activated Signature and Disclaimer (see Activating Signature and Disclaimer on page 540).

In the **Security Settings** > **Signature and Disclaimer** module, you can create group-based signatures or disclaimers. The groups are visible on the left side of the main window. If you have not created any groups for the domain, you can select the group **default** to assign the same signature or disclaimer to all users.

Notice:

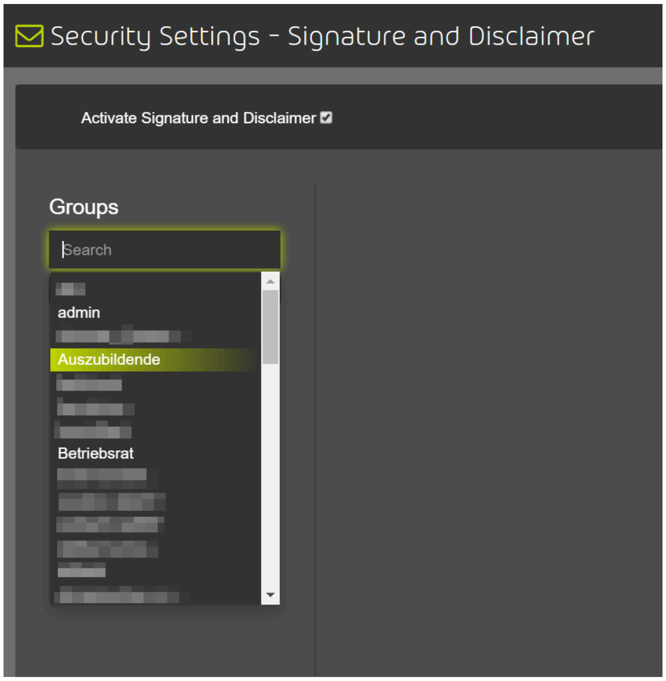
In the Control Panel, you can create new groups under **Customer Settings** > **Groups**. For more information, see the Control Panel manual under "Groups".

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to create signatures and disclaimers.
3. Navigate to **Security Settings** > **Signature and Disclaimer**.

4. Under **Groups**, add a group from the group selection on the left side of the main window.

Notice:

If you click on the field **Search**, a drop-down menu with all created groups is displayed. Additionally, you can search here for defined groups.



Security Settings - Signature and Disclaimer

Activate Signature and Disclaimer ☑

Groups

Search

admin

Auszubildende

Betriebsrat

Figure 404: Add a Group

5. Select the added group.

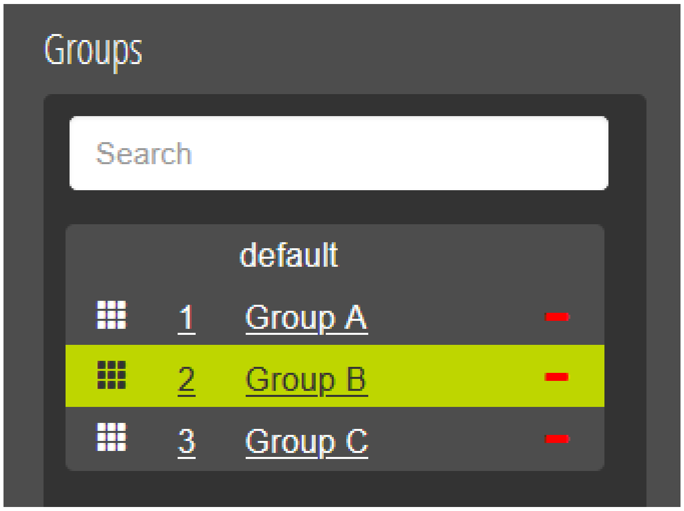


Figure 405: Select a group

On the right hand side of the main window, the selection of signatures and disclaimers appears.

6. On the right side, click on **+** under **disclaimer** or **Signature** to create a new template.

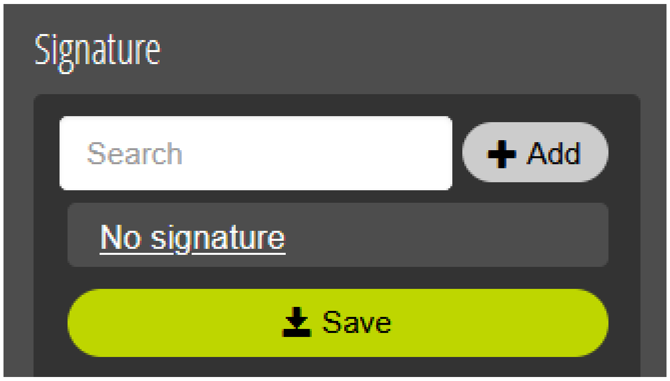


Figure 406: Add a new template

7. Enter a name for the new template.

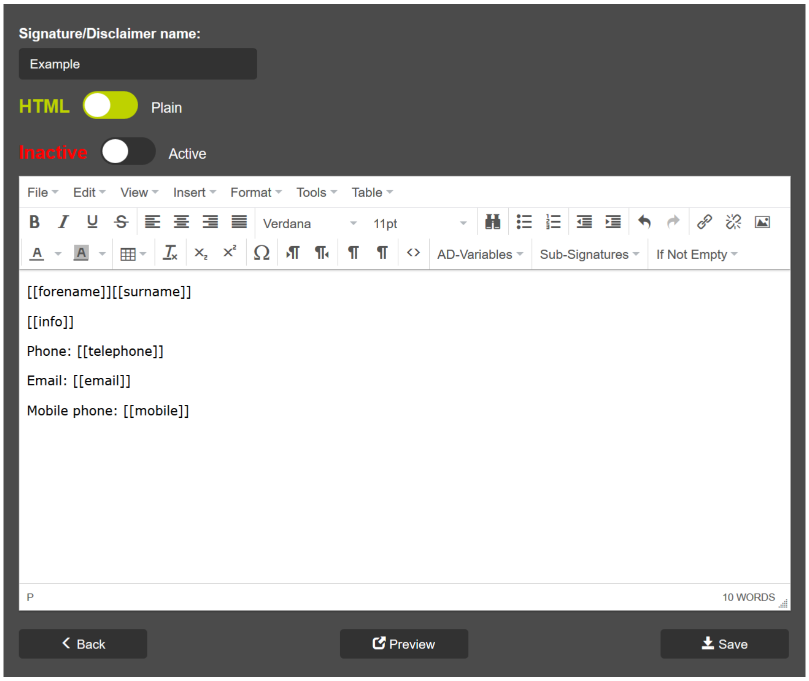
You can create templates for signatures or disclaimers in HTML and plain format at the same time. The templates are created separately.

8. Select the format for which you want to create the template:
    - HTML
    - Plain

Notice:

While editing, you can switch between the formats.

9. Define your template in the What You See Is What You Get editor (WYSIWYG editor) (see WYSIWYG Editor on page 554).



[[forename]][[surname]]

[[info]]

Phone: [[telephone]]

Email: [[email]]

Mobile phone: [[mobile]]

Figure 407: Define a template in the WYSIWYG editor

10. Save the template.

11. Select the template from the main window.

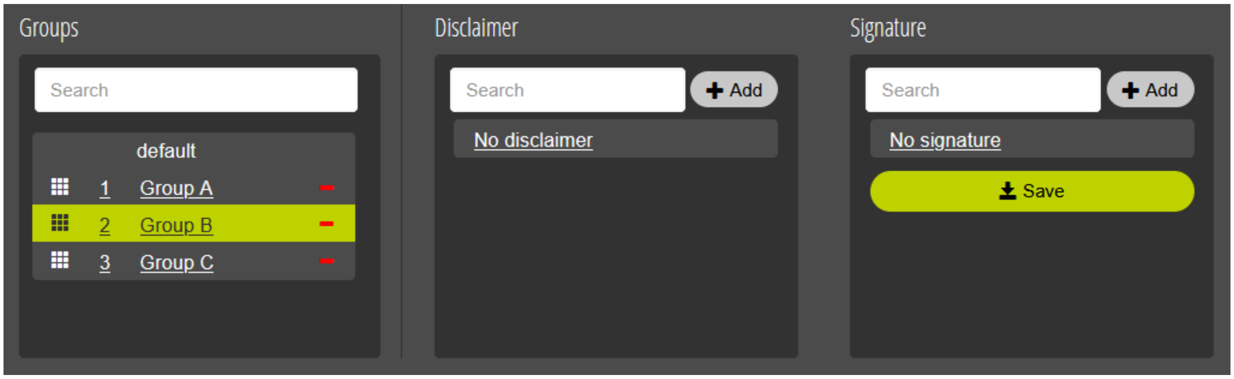


Figure 408: Select a signature from the main window

12. In the overview, click on **Save** to assign the previously selected template to the selected group.

A signature and/or a disclaimer has been created and assigned to a group.

Notice:

Signatures and disclaimers are only added to emails that are sent via the relay IP addresses specified under **Spam and Malware Protection** (see "Primary Environment Settings" in the Control Panel manual).

Notice:

A user's signature and disclaimer are added only once to an email thread. If possible, the repetition of signatures and disclaimers is avoided later in the thread.

Changing Priorities of Groups

You have added several groups to the **Signature and Disclaimer** module (see Creating Signatures and Disclaimers on page 542).

In the **Signature and Disclaimer** module, groups are sorted by their priority. The priorities of the groups are displayed in the group table under **Groups**. The lower the number, the higher the priority of a group. If a mailbox belongs to several groups in the **Signature and Disclaimer** module, the outgoing emails of the mailbox are sent with the signature and disclaimer of the group with the highest priority.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain containing the groups whose priorities you would like to change in the **Signature and Disclaimer** module.
3. Navigate to **Security Settings** > **Signature and Disclaimer**.
4. Under **Groups**, select the group whose priority you would like to change.

5. Optional: Change the priority of the group by moving the group within the list.

   a) Click on the nine points symbol next to the group, and press and hold the left mouse button.

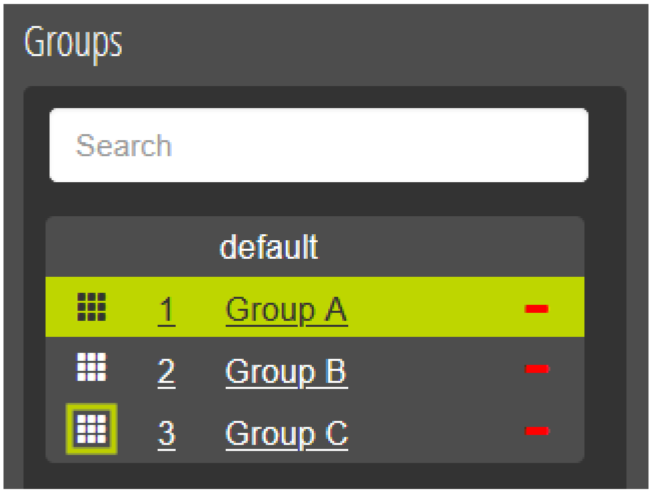


Figure 409: Move the group

   b) Drag the group to the position corresponding to the new priority.

   c) Release the left mouse button.

➔

The group is placed at the new position. The priorities of all groups that have moved within the list are updated.

6. Overwrite the priority of the group.

   a) Double-click on the priority next to the group.

   The number can be edited.

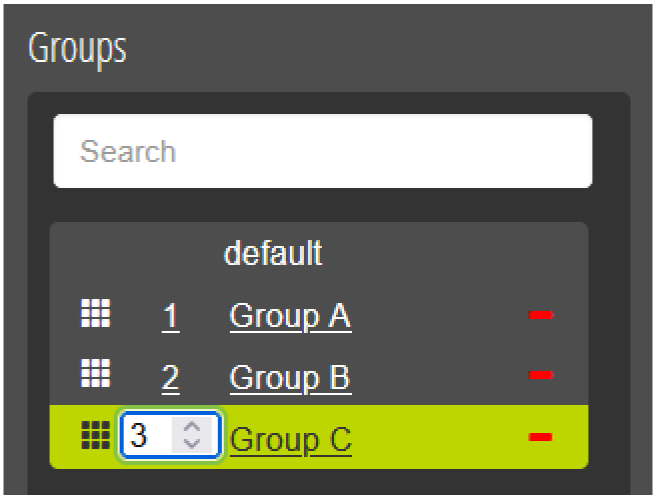


Figure 410: Input field for the priority

   b) Enter the number of the new priority in the input field or select the number with the selection arrows.

   c) Confirm the new priority with the enter key.

   The priority of the group is saved. The group is placed at the position that corresponds to the new priority. The priorities of all groups that have moved within the list are updated.

The priorities of the groups have been changed.

Editing or Deleting a Signature or Disclaimer

You have activated Signature and Disclaimer (see Activating Signature and Disclaimer on page 540) and created a signature or a disclaimer (see Creating Signatures and Disclaimers on page 542).

In the **Security Settings** > **Signature and Disclaimer** module, you can edit or delete existing signatures or disclaimers.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to edit or delete a signature or a disclaimer.
3. Navigate to **Security Settings** > **Signature and Disclaimer**.
4. Click on the field **Search** in the main window under **Signature** or **Disclaimer** and select the desired template.

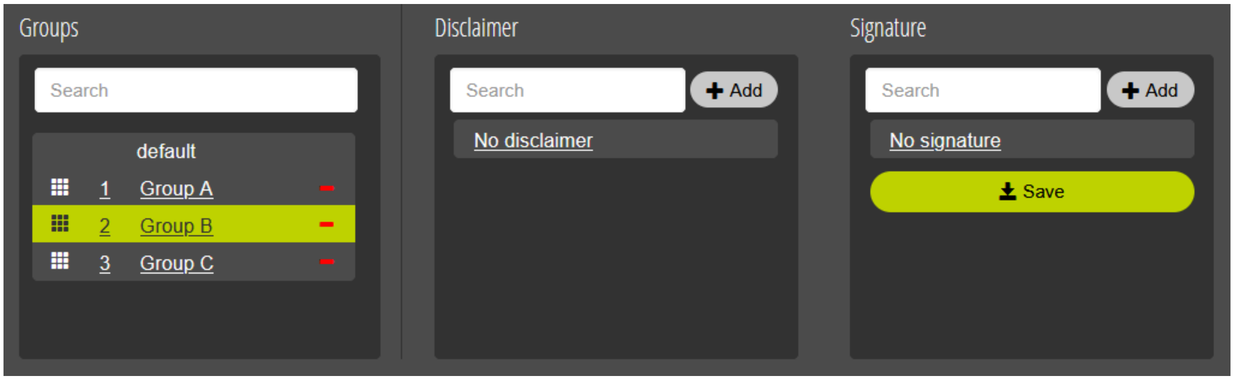


Figure 411: Select a signature from the main window

5. Select one of the following actions:

   - To edit the selected template, click on the pen next to the template's name. The editor appears and you can edit the template.

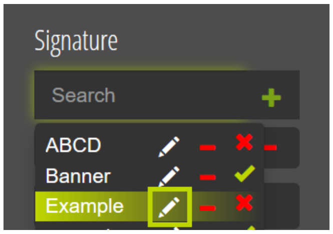


Figure 412: Edit a template

   - To delete the selected template, click on the red **–** sign. Confirm your input with **OK**.

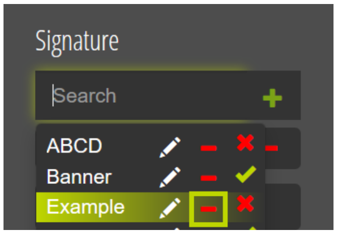


Figure 413: Delete a template

A signature or a disclaimer has been edited or deleted.

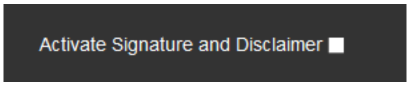
Deactivating Signature and Disclaimer

You have activated Signature and Disclaimer (see Activating Signature and Disclaimer on page 540).

If you no longer want to use Signature and Disclaimer (see About Signature and Disclaimer on page 539), you can deactivate the service. Your group settings, signatures and disclaimers will be kept in case you later want to reactivate Signature and Disclaimer.

1. Log in to the Control Panel with your administrative credentials.

2. From the scope selection, select the domain for which you would like to deactivate Signature and Disclaimer.
3. Navigate to **Security Settings** > **Signature and Disclaimer**.
4. Untick the **Activate Signature and Disclaimer** checkbox.

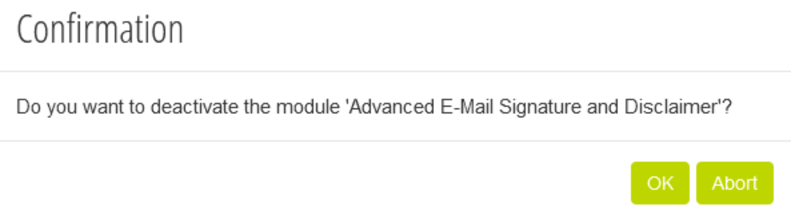


Activate Signature and Disclaimer □

Figure 414: Deactivating Signature and Disclaimer

➔ A confirmation window opens.

5. Click on **OK**.



Confirmation

Do you want to deactivate the module 'Advanced E-Mail Signature and Disclaimer'?

Figure 415: Confirm deactivation

➔

Signature and Disclaimer is deactivated.

✓

Signature and Disclaimer has been deactivated.

Notice:

The deactivation of Signature and Disclaimer does not result in the termination of the existing contract for this service. To terminate a contract, you must communicate with your contact person.

WYSIWYG Editor

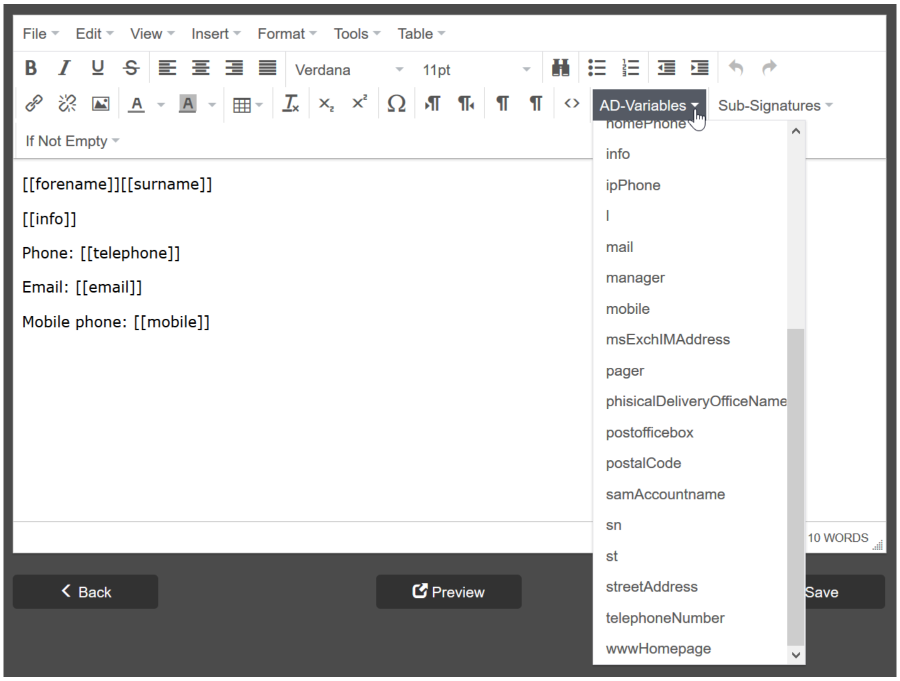
In the WYSIWYG editor, templates for signatures and disclaimers can be easily created and edited.

For this purpose, simple formatting options, such as paragraph alignment, font style and bulleting, are available to customer-level administrators and users with the **Marketing** role (see Access to the Signature and Disclaimer Module on page 540). Furthermore, Active Directory variables can be used to access attributes from the Active Directory or basic data of manually created mailboxes (see chapter "Mailbox Types" in the Control Panel manual) in order to add, for instance, the first and last name defined for a mailbox to signatures or disclaimers. The available attributes depend on the use case:

- If the LDAP connection is activated (see "LDAP Connection" in the Control Panel manual), numerous attributes from the Active Directory are available (see Synchronized Attributes from the Active Directory on page 555). If no value has been assigned to an attribute, it can be hidden in signatures and disclaimers (see Hiding Empty Active Directory Elements on page 560).
- For manually created mailboxes, the basic data of the mailboxes (see Basic Data Request with AD Variables on page 559) is available.

> **Important:**
>
> To use AD variables, they must have been defined in the Active Directory.

Signatures and disclaimers can be formatted using HTML source text (see Inserting HTML Source Code on page 567). In addition, existing signatures can be included in other signatures as subsignatures (see Including Subsignatures on page 563) and graphics can be added to signatures and disclaimers (see Embedding of Images in Signatures and Disclaimers on page 569). A preview function can be used to display a signature or a disclaimer as they will later be issued (see Displaying a Preview of a Signature or a Disclaimer on page 568).



[[forename]][[surname]]

[[info]]

Phone: [[telephone]]

Email: [[email]]

Mobile phone: [[mobile]]

Figure 416: WYSIWYG Editor

Synchronized Attributes from the Active Directory

If the LDAP connection (see "LDAP Connection" in the Control Panel manual) is activated, numerous attributes are synchronized with the Active Directory from Microsoft that can be used in the **Signature and Disclaimer** module (see About Signature and Disclaimer on page 539). Once data changes in the Active Directory, it is also updated in the Control Panel (see Data Synchronization via LDAP on page 557).

The following attributes from the Active Directory are synchronized for LDAP mailboxes (see chapter "Mailbox Types" in the Control Panel manual) and can be used to create signatures and disclaimers:

AD VARIABLE	DESCRIPTION
cn	Common name
company	Company

AD VARIABLE	DESCRIPTION
countryCode	Country/Region
department	Department
description	Description
directReports	Employee
displayName	Display name – complete name
facsimileTelephoneNumber	Fax
givenName	First name
homePhone	Private phone number
info	Job title/Position **Notice:** The field Title is often used for other purposes. Therefore, the term Info is used here for the LDAP attribute Title (Job title/Position).
ipPhone	IP phone number
l (lower case L)	City
mail	Email address
manager	Manager
mobile	Mobile phone number

AD VARIABLE	DESCRIPTION
msExchIMAddress	IM address
pager	Pager number
physicalDeliveryOfficeName	Office
postalCode	Postal code
postOfficeBox	Mailbox
samAccountName	User account name
sn	Last name
st	State
streetAddress	Street
telephoneNumber	Phone number
wwwHomepage	website

Data Synchronization via LDAP

If you change the Active Directory, these changes will be synchronized.

The changes in the Active Directory are tracked using the **USNChangedNr** attribute. If the value changes, the dataset is synchronized.

> **Important:**
>
> If you perform a backup, the **USNChangedNr** is not increased but reset to an earlier value. The dataset is then also synchronized again.

Synchronized Attributes from the Azure Active Directory

With the Azure Active Directory of Microsoft, certain attributes are synchronized for Signature and Disclaimer (see About Signature and Disclaimer on page 539).

Important:

For manually created mailboxes, basic data (see Basic Data Request with AD Variables on page 559) is used. LDAP attributes are not synchronized and cannot be used.

The following attributes are synchronized and can be used to create signatures and disclaimers:

AD VARIABLE	DESCRIPTION
countryCode	Country/Region
department	Department
displayName	Complete name
givenName	First name
info	Job title/Position **Notice:** The field Title is often used for other purposes. Therefore, the term Info is used here for the LDAP attribute Title (Job title/Position).
l (lower case L)	City
mail	Email address
mobile	Mobile phone number

AD VARIABLE	DESCRIPTION
postalCode	Postal code
sn	Last name
st	State
streetAddress	Street
telephoneNumber	Phone number

Basic Data Request with AD Variables

Important:

For manually created mailboxes, the basic data of the mailboxes that is described below can be used as AD variables.

The AD variables and the basic data of a mailbox relate to each other as follows:

AD VARIABLE	BASIC DATA
countryCode	**Country/Region**
department	**Department**
displayName	**Display name**
facsimileTelephoneNumber	**Fax**
givenName	**First name**
l (lower case L)	**City**

AD VARIABLE	BASIC DATA
mail	Email address of the mailbox
mobile	**Mobile phone**
postalCode	**Postal code**
physicalDeliveryOfficeName	**Office**
sn	**Last name**
st	**State**
streetAddress	**Street, number**
telephoneNumber	**Phone (business)**

Hiding Empty Active Directory Elements

You have activated Signature and Disclaimer (see Activating Signature and Disclaimer on page 540).

In the **Security Settings** > **Signature and Disclaimer** module, you can use the **If Not Empty** function of the WYSIWYG editor (see WYSIWYG Editor on page 554) to hide content in signatures and disclaimers if certain AD variables are not filled for users.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to create signatures and disclaimers.
3. Navigate to **Security Settings** > **Signature and Disclaimer**.
4. Create or edit a signature or a disclaimer (see Creating Signatures and Disclaimers on page 542 or Editing or Deleting a Signature or Disclaimer on page 551).
5. Select the line in the editor in which you want to insert the AD variable.

6. Click on **If Not Empty**.

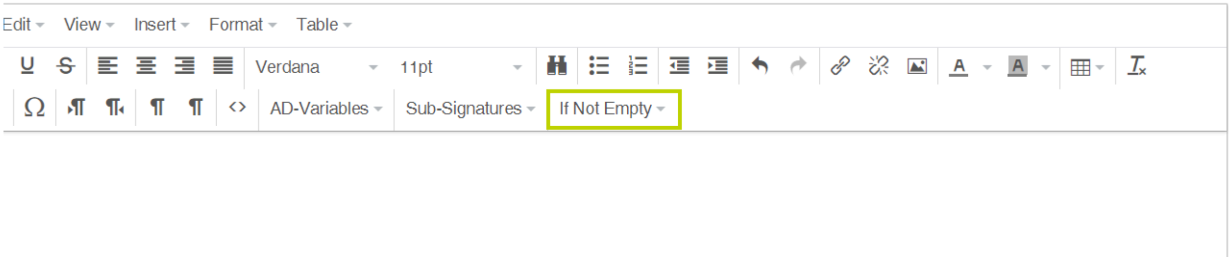


Figure 417: Open the selection

7. Select the desired AD variable from the field Variable.

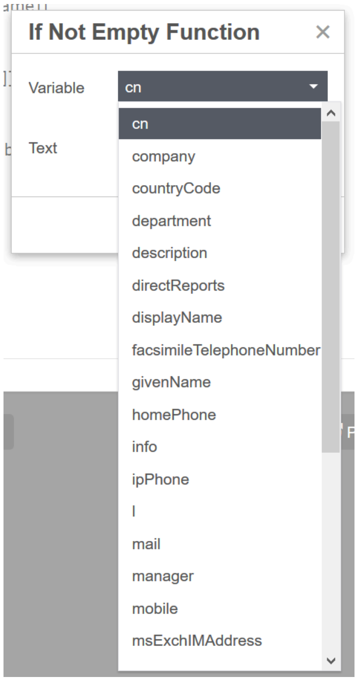


Figure 418: Select AD variable

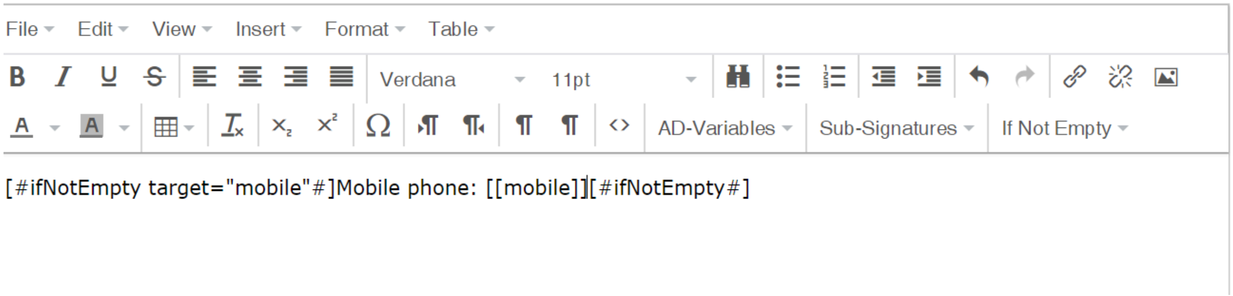
8. Enter the text that you want to hide if the element is not filled for the user.

9. Confirm with **OK**.

10. It is also possible to enter an AD variable in the text to be hidden:

    a) Click on the position in the editor between the If Not Empty tag at which you want to insert the AD variable to be hidden.

    b) Select the AD variable from the drop-down menu.



```
[#ifNotEmpty target="mobile"#]Mobile phone: [[mobile]][#ifNotEmpty#]
```

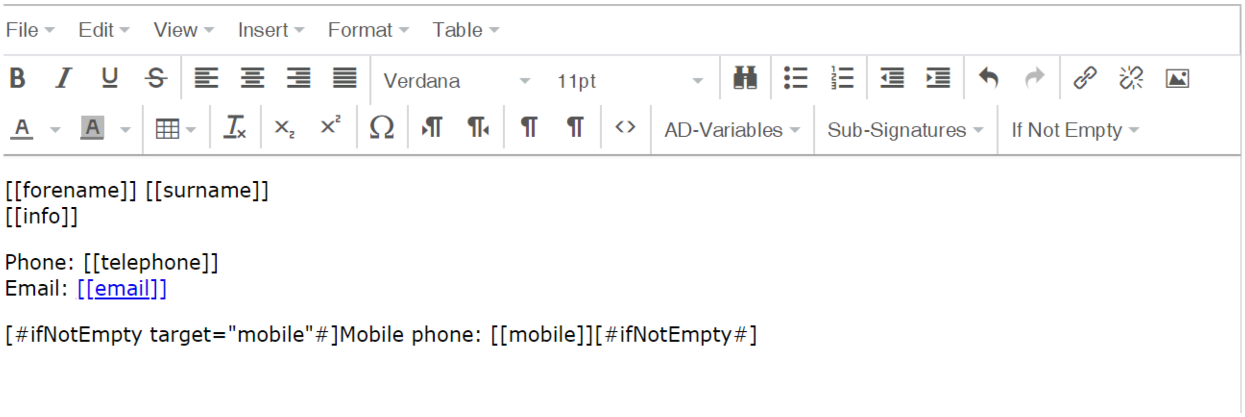
Figure 419: If Not Empty - Mobile phone

11. Click on **Save** to save the signature or disclaimer.

✓ Empty elements of the Active Directory have been hidden in a signature or a disclaimer.

Example: Hiding non-existent AD variables

The following signature is created for all users:



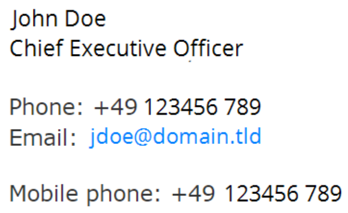
```
[[forename]] [[surname]]
[[info]]

Phone: [[telephone]]
Email: [[email]]

[#ifNotEmpty target="mobile"#]Mobile phone: [[mobile]][#ifNotEmpty#]
```

Figure 420: Signature in the editor

The following signature is displayed for users with a mobile phone number:



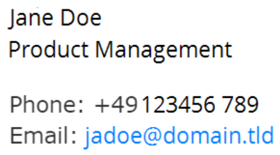
John Doe
Chief Executive Officer

Phone: +49 123456 789
Email: jdoe@domain.tld

Mobile phone: +49 123456 789

Figure 421: Signature with mobile phone number

The following signature is displayed for users without a mobile phone number:



Jane Doe
Product Management

Phone: +49123456 789
Email: jadoe@domain.tld

Figure 422: Signature without mobile phone number

Including Subsignatures

You have activated Signature and Disclaimer (see Activating Signature and Disclaimer on page 540). You have created a signature (see Creating Signatures and Disclaimers on page 542).

In the **Security Settings** > **Signature and Disclaimer** module, you can use the **Sub-Signatures** function of the WYSIWYG editor (see WYSIWYG Editor on page 554) to include an existing signature as a subsignature in another signature of Signature and Disclaimer (see About Signature and Disclaimer on page 539).

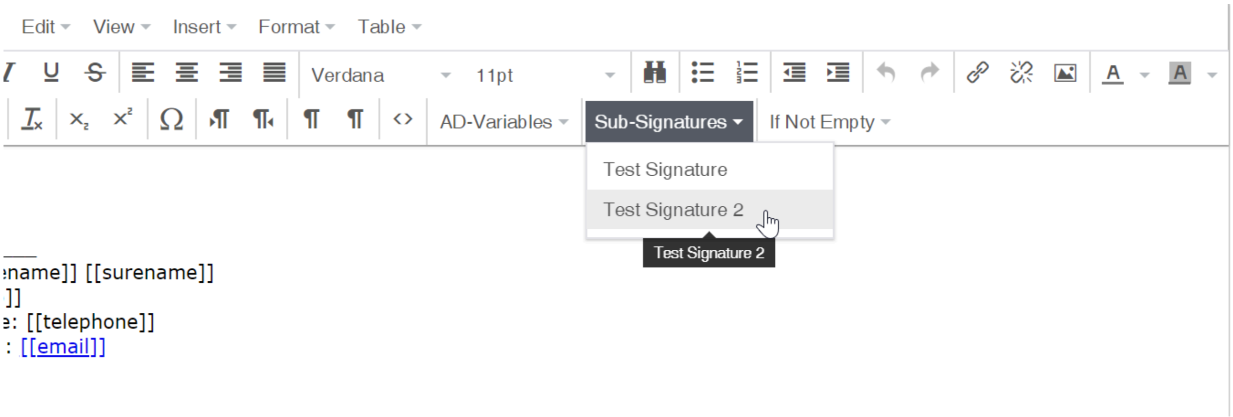
Important:

Subsignatures can only be used in signatures. At least one signature must exist that you can include as a subsignature.

1. Log in to the Control Panel with your administrative credentials.

2. From the scope selection, select the domain for which you would like to create a signature.
3. Navigate to **Security Settings** > **Signature and Disclaimer**.
4. Create or edit a signature (see Creating Signatures and Disclaimers on page 542 or Editing or Deleting a Signature or Disclaimer on page 551).
5. Select the line in the editor, in which you want to insert the subsignature.

6. Click on **Sub-Signatures** and select the subsignature from the existing signatures.

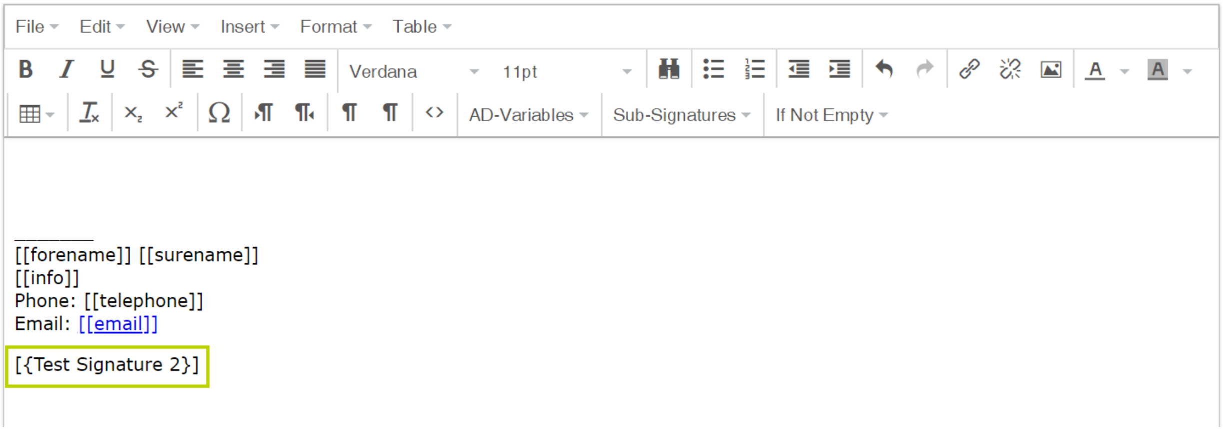


:name]] [[surename]]
]]
:: [[telephone]]
: [[email]]

Figure 423: Select a subsignature

➜

A placeholder is inserted for the subsignature.



[[forename]] [[surename]]
[[info]]
Phone: [[telephone]]
Email: [[email]]

[{Test Signature 2}]

Figure 424: Subsignature placeholder

7. Click on **Save** to save the signature with subsignature.

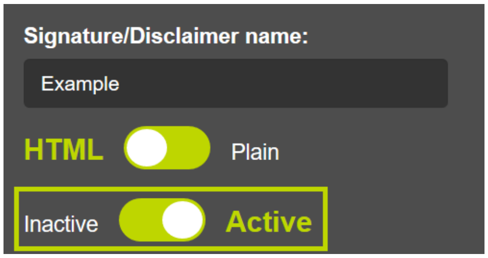
8. **Important:**

   In order to use a signature as a subsignature, it must be activated first.

   To activate a signature to use as a subsignature:

   a) Open the edit mode of the signature you want to use as a subsignature.

   b) Toggle the switch to **Encryption active**.



Signature/Disclaimer name: Example

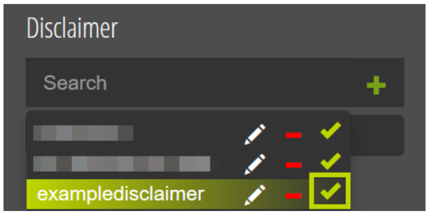
HTML ● Plain

Inactive ● Active

Figure 425: Activate subsignatures

➡

Activated and deactivated signatures are marked in the selection.



Disclaimer

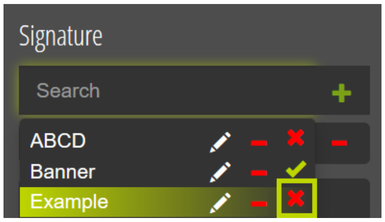
Search +

[redacted] ✓

[redacted] ✓

exampledisclaimer ✓

Figure 426: Active signature in the selection



Signature

Search +

ABCD ✗

Banner ✓

Example ✗

Figure 427: Inactive signature in the selection

A subsignature has been included in a signature.

Inserting HTML Source Code

You have activated Signature and Disclaimer (see Activating Signature and Disclaimer on page 540).

In the **Security Settings** > **Signature and Disclaimer** module, you can add HTML source code to signatures and disclaimers using the WYSIWYG editor.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to create a signature or a disclaimer.
3. Navigate to **Security Settings** > **Signature and Disclaimer**.
4. Create or edit a signature or a disclaimer (see Creating Signatures and Disclaimers on page 542 or Editing or Deleting a Signature or Disclaimer on page 551).
5. In the WYSIWYG editor select the tab **Tools** and click on **Source Code**.

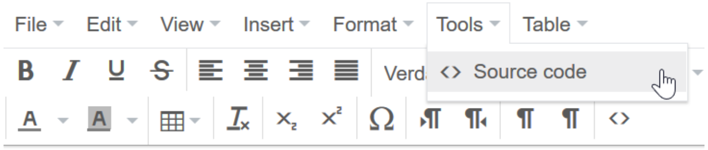
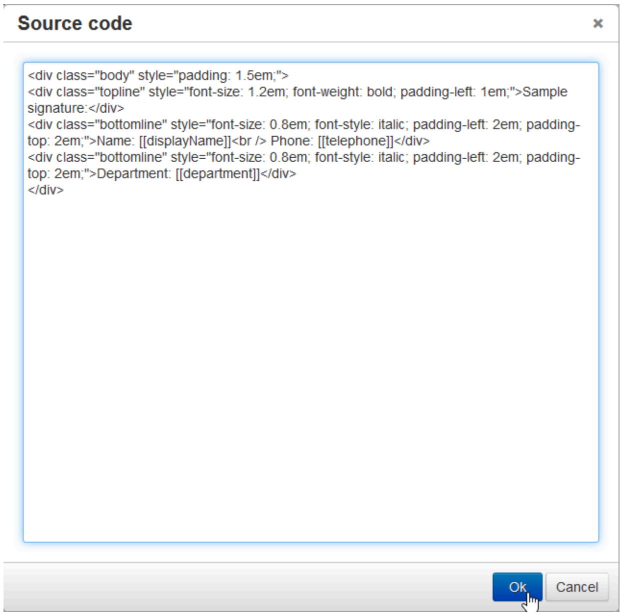


Figure 428: Source code editor

A new window for text input appears.

6. Enter the desired HTML source code and confirm with **OK**.



```
<div class="body" style="padding: 1.5em;">
<div class="topline" style="font-size: 1.2em; font-weight: bold; padding-left: 1em;">Sample
signature:</div>
<div class="bottomline" style="font-size: 0.8em; font-style: italic; padding-left: 2em; padding-
top: 2em;">Name: [[displayName]]<br /> Phone: [[telephone]]</div>
<div class="bottomline" style="font-size: 0.8em; font-style: italic; padding-left: 2em; padding-
top: 2em;">Department: [[department]]</div>
</div>
```

Figure 429: Insert source code

7. In the editor click on **Save** to save your changes.

✓

HTML source code has been added to a signature or a disclaimer.

Displaying a Preview of a Signature or a Disclaimer

You have activated Signature and Disclaimer (see Activating Signature and Disclaimer on page 540).

In the **Security Settings** > **Signature and Disclaimer** module, you can display a preview of a signature or a disclaimer.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to create a signature or a disclaimer.
3. Navigate to **Security Settings** > **Signature and Disclaimer**.

4. Create or edit a signature or a disclaimer (see Creating Signatures and Disclaimers on page 542 or Editing or Deleting a Signature or Disclaimer on page 551).
5. Click on **Preview** at the bottom of the WYSIWYG editor.

   A preview window for signatures and disclaimers opens.
6. Select a mailbox from the list on the left side of the window.

   A preview of the selected user's signature and/or disclaimer is displayed on the right side of the window.

A preview of a signature and/or disclaimer has been displayed.

Embedding of Images in Signatures and Disclaimers

With the WYSIWYG editor, images can be embedded in signatures and disclaimers. Images that shall be used for all mailboxes of a group can either be directly copied into the WYSIWYG editor via drag and drop (see Inserting and Linking an Image via Drag and Drop on page 574) or embedded as a URL using an input window (see Embedding an Image Using a URL on page 569). Furthermore, different images can be embedded in signatures and disclaimers for different mailboxes of a group (see Embedding Different Images for Different Mailboxes on page 577).

Embedding an Image Using a URL

You have activated Signature and Disclaimer (see Activating Signature and Disclaimer on page 540).

In the **Security Settings** > **Signature and Disclaimer** module, you can embed an image in a signature or a disclaimer of Signature and Disclaimer (see About Signature and Disclaimer on page 539) using a URL.

1. Log in to the Control Panel with your administrative credentials.

2. From the scope selection, select the domain for which you would like to create a signature or a disclaimer.
3. Navigate to **Security Settings** > **Signature and Disclaimer**.
4. Create or edit a signature or a disclaimer (see Creating Signatures and Disclaimers on page 542 or Editing or Deleting a Signature or Disclaimer on page 551).
5. When creating or editing a signature or a disclaimer in the WYSIWYG editor, click on the position where you would like to insert the image.
6. Within the editor, navigate to **Insert** > **Image**.

   ➜

   An input window with further parameters opens.

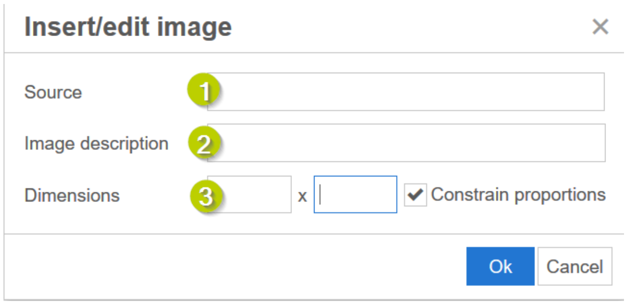


Figure 430: Input window for images

7. Under **Source** (1), enter the address of the image that should be displayed. Search the internet for the desired image and copy the stored image location.

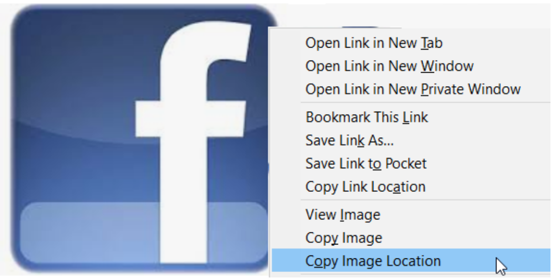
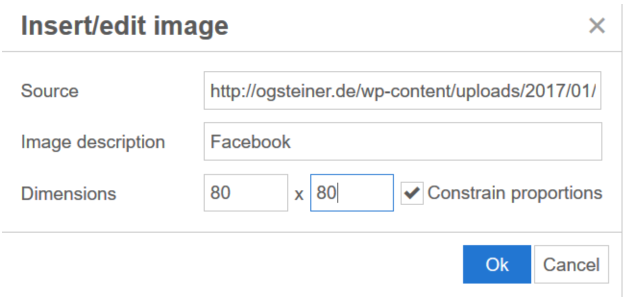


Figure 431: Copy the location of the representative image and paste under Source.

➜

The location of the desired image is stored.

8. Alternatively, enter a description under **Image description** (2).
9. If necessary, adjust the size of the image individually under **Dimensions** and save your input with **Ok**.



Source: http://ogsteiner.de/wp-content/uploads/2017/01/

Image description: Facebook

Dimensions: 80 x 80 ☑ Constrain proportions

Figure 432: Resize the image

➜

The parameters are stored and the image is displayed in the editor.

10. Right-click on the image and select **Link** to enter a specific URL.

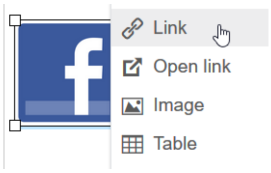
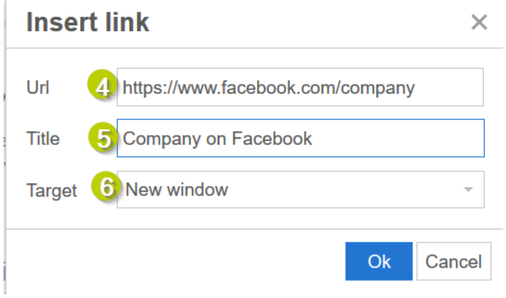


Figure 433: Link an image

An input window with further parameters opens.



Url 4 https://www.facebook.com/company

Title 5 Company on Facebook

Target 6 New window

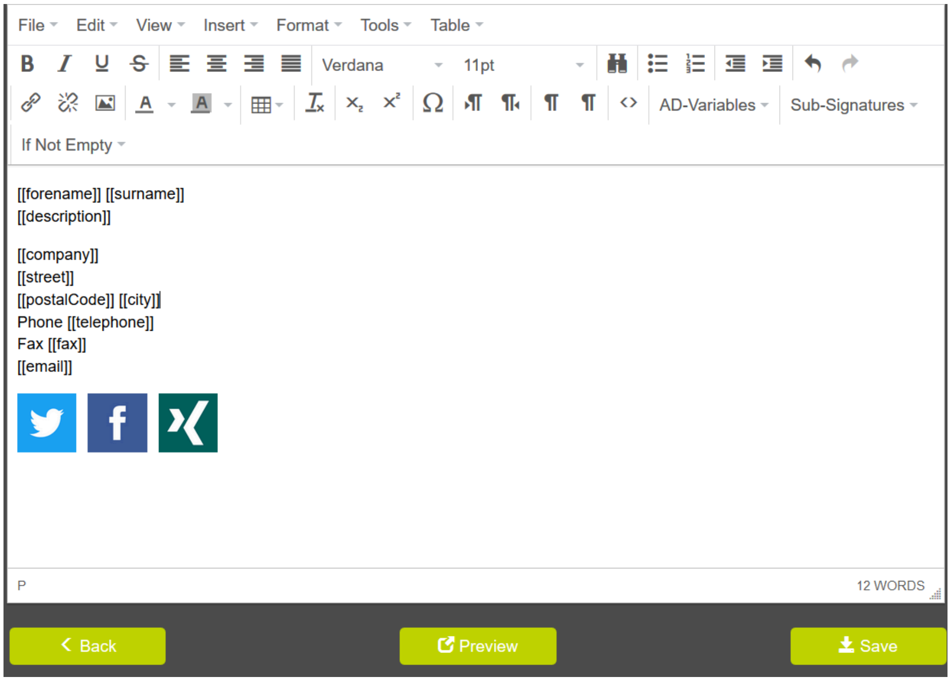
Figure 434: Enter a URL

11. Enter the destination address of the desired website under **URL** (4).
12. Alternatively, enter a text under **Title** (5) which should be displayed over the image when the mouse hovers over it.
13. Under **Target** (6) select **New window** to open the linked website in a new tab to leave.
14. Click on **Ok** and then on **Save** to save all data.

Notice:

If necessary, repeat steps 1-10 if you want to insert several images.

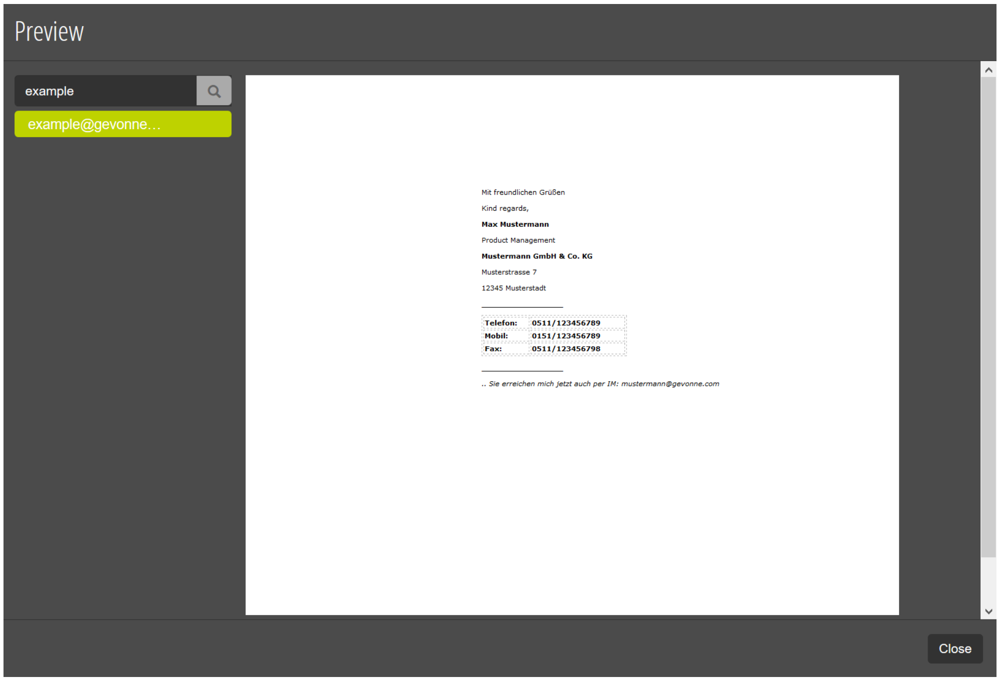
An image has been embedded in a signature or a disclaimer using a URL.



[[forename]] [[surname]]
[[description]]

[[company]]
[[street]]
[[postalCode]] [[city]]
Phone [[telephone]]
Fax [[fax]]
[[email]]

Figure 435: Assignment of variables with linked images



Mit freundlichen Grüßen

Kind regards,

Max Mustermann

Product Management

Mustermann GmbH & Co. KG

Musterstrasse 7

12345 Musterstadt

Telefon:	**0511/123456789**
Mobil:	**0151/123456789**
Fax:	**0511/123456798**

.. Sie erreichen mich jetzt auch per IM: mustermann@gevonne.com

Figure 436: Preview of a signature with linked images

Inserting and Linking an Image via Drag and Drop

In the **Security Settings** > **Signature and Disclaimer** module, you can insert and link an image in a signature or a disclaimer of Signature and Disclaimer (see About Signature and Disclaimer on page 539) via drag and drop.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to create a signature or a disclaimer.
3. Navigate to **Security Settings** > **Signature and Disclaimer**.
4. Create or edit a signature or a disclaimer (see Creating Signatures and Disclaimers on page 542 or Editing or Deleting a Signature or Disclaimer on page 551).
5. When creating or editing a signature or a disclaimer in the WYSIWYG editor, click on the position where you would like to insert the image.

6. Drag the image to the desired position.

➜

The image is inserted at the desired position via drag and drop.

7. Right-click on the image and select **Link** to enter a specific URL.

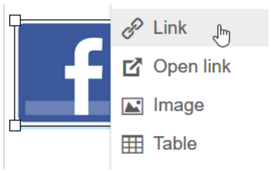
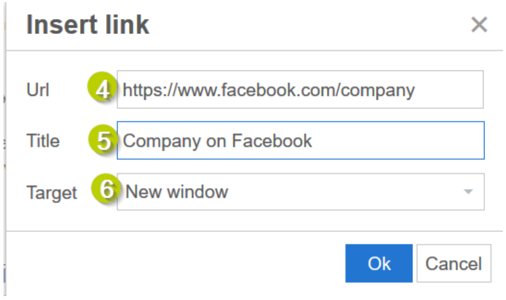


Figure 437: Link image

➜

An input window with further parameters opens.



Insert link

Url (4) https://www.facebook.com/company

Title (5) Company on Facebook

Target (6) New window

Figure 438: Enter a URL

8. Enter the destination address of the desired website under **URL** (4).

9. Alternatively, enter a text under **Title** (5) which should be displayed over the image when the mouse hovers over it.

10. Under **Target** (6) select **New window** to open the linked website in a new tab to leave.

11. Click on **Ok** and close the input window.

➜

The image is linked.

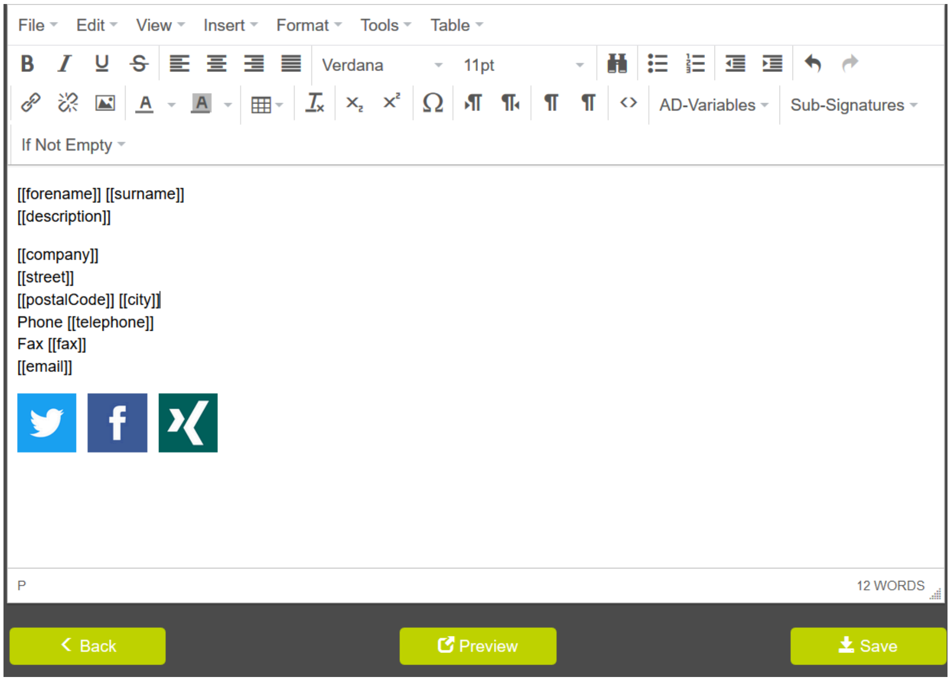
12. Optional: Right-click on the added image and select **Image** to resize the image in the field **Dimensions**.

13. Click on **Ok** and then on **Save** to save all data.

> **Notice:**
>
> If necessary, repeat steps 1-9 if you would like to insert several images.

✓

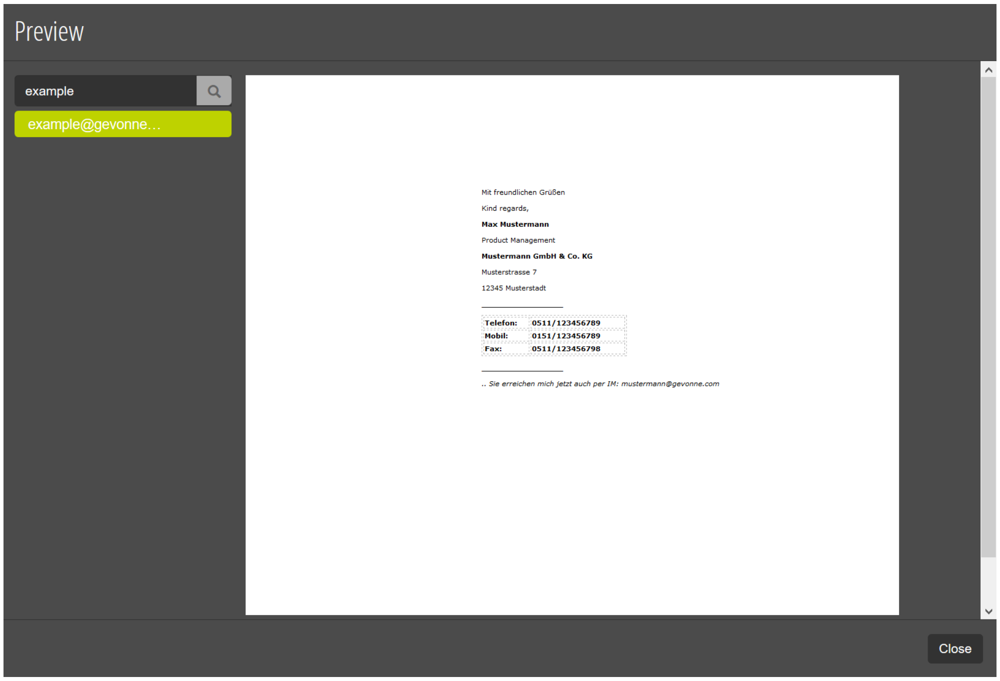
An image has been added to a signature or a disclaimer via drag and drop.



[[forename]] [[surname]]
[[description]]

[[company]]
[[street]]
[[postalCode]] [[city]]
Phone [[telephone]]
Fax [[fax]]
[[email]]

Figure 439: Assignment of variables with linked images



Mit freundlichen Grüßen

Kind regards,

Max Mustermann

Product Management

Mustermann GmbH & Co. KG

Musterstrasse 7

12345 Musterstadt

Telefon:	**0511/123456789**
Mobil:	**0151/123456789**
Fax:	**0511/123456798**

.. Sie erreichen mich jetzt auch per IM: mustermann@gevonne.com

Figure 440: Preview of a signature with linked images

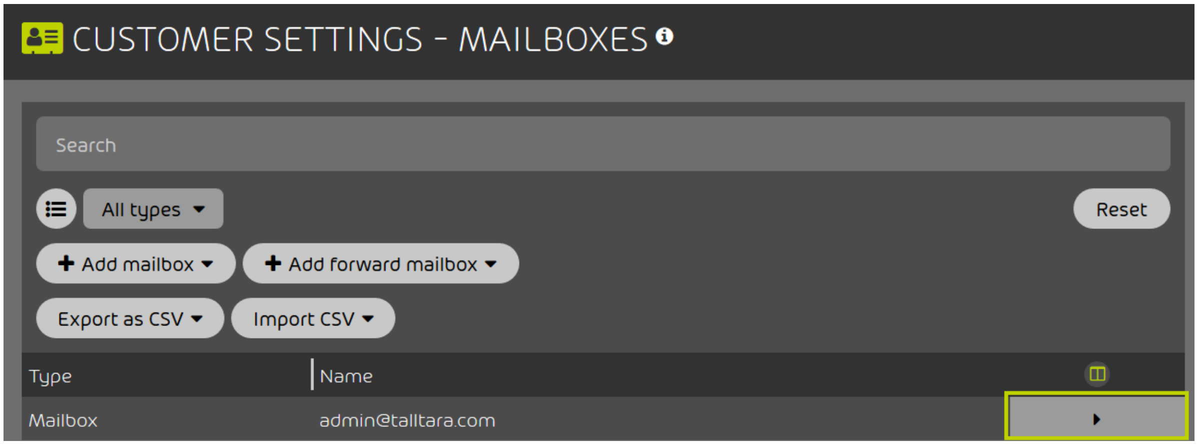
Embedding Different Images for Different Mailboxes

You have activated Signature and Disclaimer (see Activating Signature and Disclaimer on page 540). You have created a mailbox (see "Adding a Mailbox" in the Control Panel manual) and have added it to a group (see "Adding a Mailbox to a Group" in the Control Panel manual).

Via the modules **Customer Settings** > **Mailboxes** and **Security Settings** > **Signature and Disclaimer** (see About Signature and Disclaimer on page 539), you can embed different images in the signatures of the different mailboxes of a group.

1. Log in to the Control Panel with your administrative credentials.
2. Select the desired domain from the scope selection.
3. Navigate to **Customer Settings** > **Mailboxes**.

4. Click on the menu arrow next to the desired mailbox.



Type	Name
Mailbox	admin@talltara.com

Figure 441: Open the menu

➜

A menu opens.

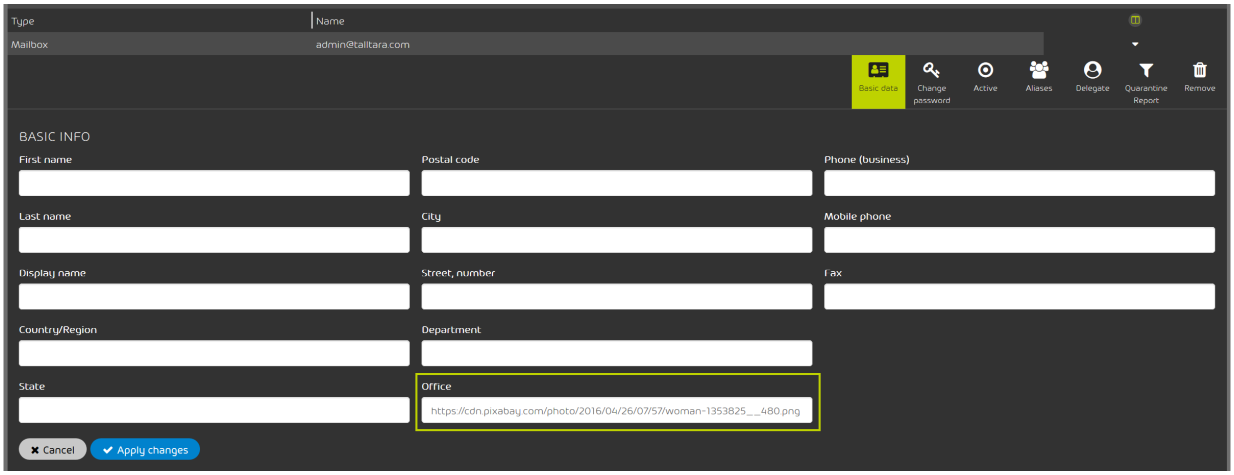
5. Click on **Basic info**.

➜

A drop-down menu opens.

6. Enter the URL of an image in any unfilled field within the **Basic info**.

➔



Type: Mailbox

Name: admin@talltara.com

Office: https://cdn.pixabay.com/photo/2016/04/26/07/57/woman-1353825__480.png

Figure 442: Enter the URL of an image in Office

7. Click on **Apply changes**.

➔

The changes are saved.

8. Repeat the procedure for each mailbox of the group.
9. Navigate to **Security Settings** > **Signature and Disclaimer**.
10. Select the group containing the previously edited mailbox.

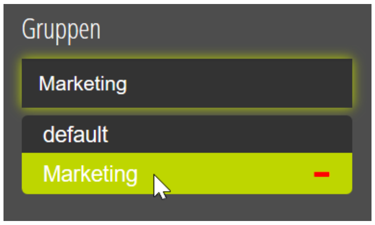
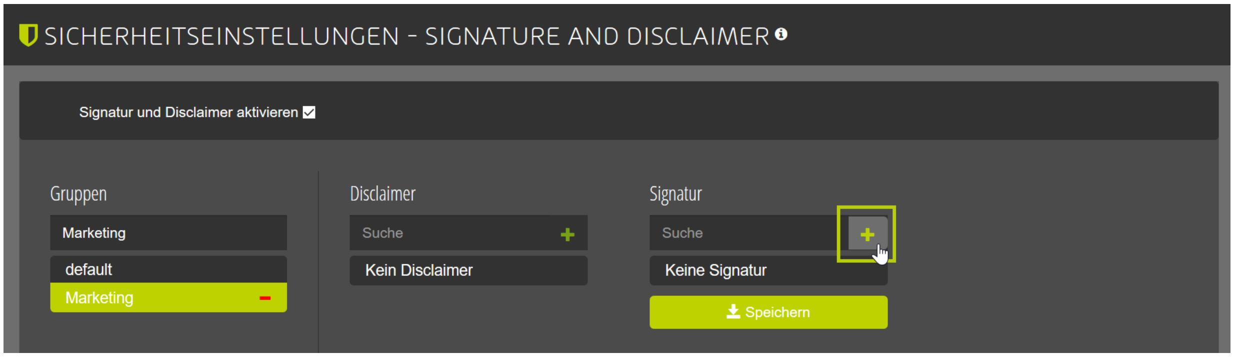


Figure 443: Select a group

➔

The group is selected.

11. Click on the plus sign button under the Headline **Signature**.



The **Signature** window opens.

12. Click on the button **Source code** in the **Signature** window.

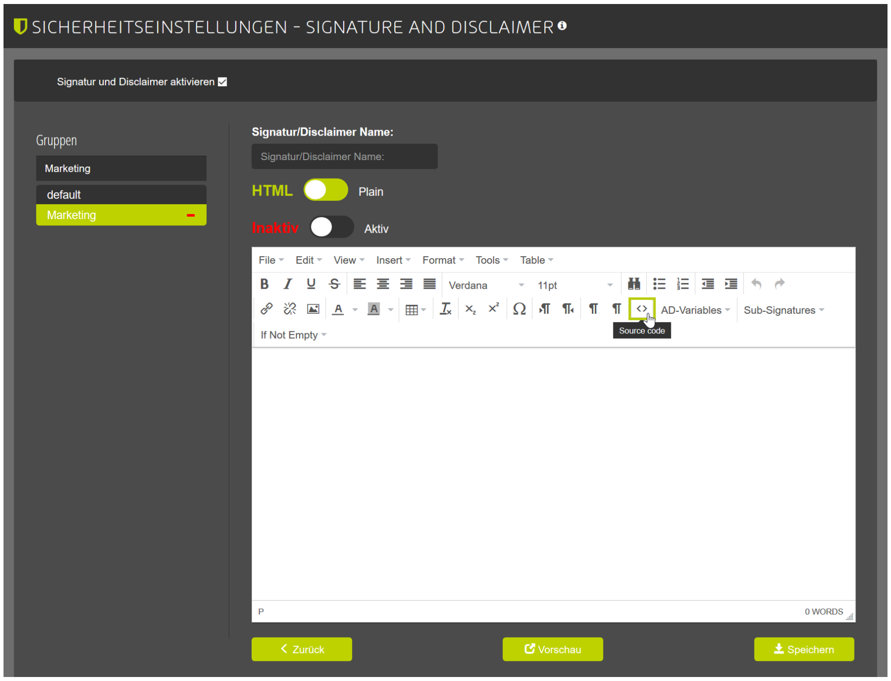


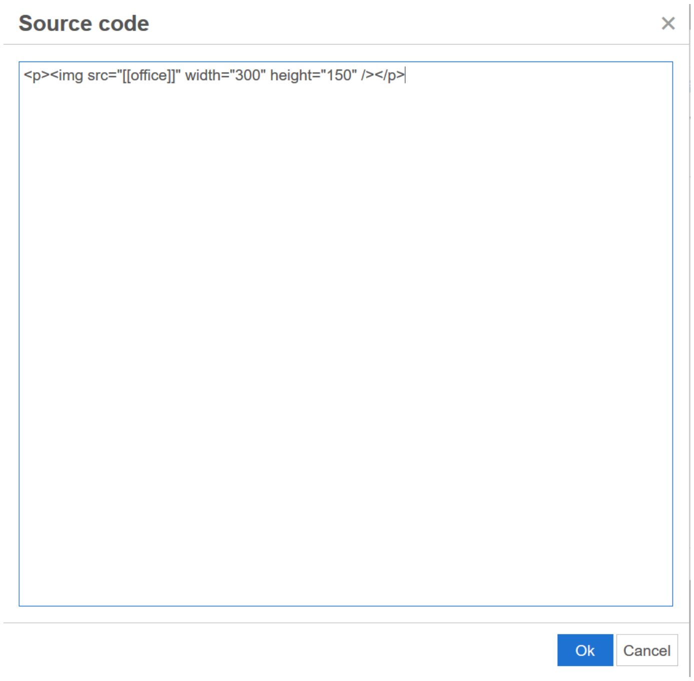
Figure 444: Display source code

13. **Notice:**

    In the attribute **src**, enter the name of the basic data field in which you have entered the URL of the image. The following are examples of field names:

    - **Department**: department
    - **Display name**: displayname
    - **Office**: office
    - **State**: state
    - **Fax**: fax
    - **Country/Region**: country
    - **City**: city
    - **Postal code**: postalcode
    - **Street, number**: street
    - **Phone (business)**: telephone
    - **Mobile phone**: mobile

    To embed images, enter an HTML code snippet according to the following pattern: **<img src="[[...]]" width="..." height="..."/>**.



```
<p><img src="[[office]]" width="300" height="150" /></p>
```

Figure 445: Embedding of an image URL from the Office field in the Signature window

14. Click on **OK**.

➔

The **Source code** window closes and the **Signature** window is displayed.

15. Optional: Click on the button **Preview** and select the mailbox whose signature you have edited the last.

   ➜

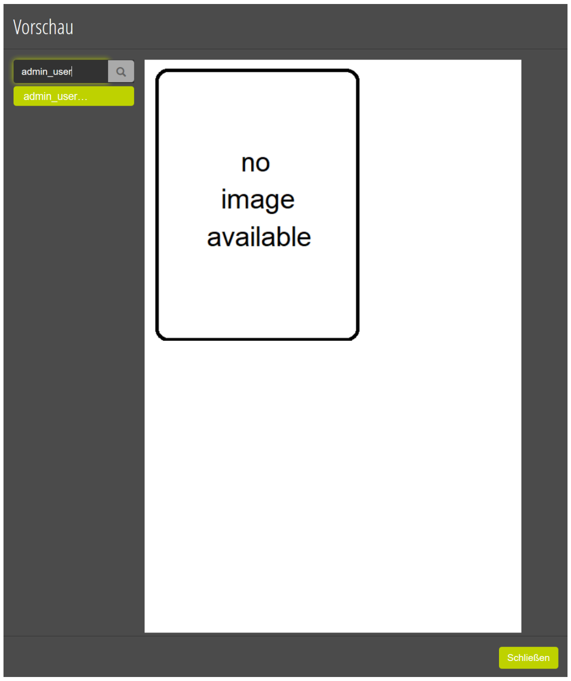


Figure 446: Preview of the new signature

16. Optional: Click on **Close**.

   ➜

   The preview closes.

17. Enter a name for the signature you have edited in the **Signature/Disclaimer name** field.

18. Click on **Save**.

   ➜

   The signature is saved.

✓

Different images have been embedded in the signatures of the different mailboxes of a group.

Troubleshooting

While using Signature and Disclaimer, errors may occur that are caused by an incorrect configuration. In the following chapters, the causes of and solutions for frequent errors are explained:

- Troubleshooting: Variables Are Not Referenced on page 584
- Troubleshooting: Missing HTML Signature in Emails Sent from Mail (Apple) or Thunderbird on page 585

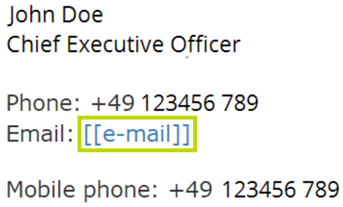
Troubleshooting: Variables Are Not Referenced

Condition:

You have inserted an AD variable or a subsignature (see Including Subsignatures on page 563) and it is displayed incorrectly in the created signature.

Cause: AD Variable does not exist

The variable is not defined in the Active Directory.



John Doe
Chief Executive Officer

Phone: +49 123456 789
Email: [[e-mail]]

Mobile phone: +49 123456 789

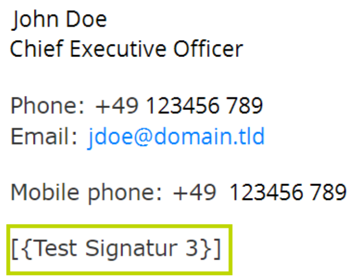
Figure 447: Example of a non-existent AD variable

Remedy

Select the AD variables in the editor from the drop-down menu.

Cause: Subsignature does not exist

The referenced signature does not exist or the name of the signature has been changed. Therefore, it cannot be included.



John Doe
Chief Executive Officer

Phone: +49 123456 789
Email: jdoe@domain.tld

Mobile phone: +49 123456 789

[{Test Signatur 3}]

Figure 448: Example for the integration of a non-existent signature

Remedy

Select the signature to be included again from the **Sub-Signatures** drop-down menu.

Troubleshooting: Missing HTML Signature in Emails Sent from Mail (Apple) or Thunderbird

Condition

Emails sent from Thunderbird or Mail (Apple) do not attach the HTML signature, but the plain signature. If you have not specified a signature for plain text, the email will be sent without a signature.

Reason

Some email clients such as Mail (Apple) and Thunderbird send emails by default as plain text and not in HTML format. Thus, the plain template is loaded in the **Signature and Disclaimer**.

Remedy for Mail (Apple) on MacOS

See Using plain or rich text in emails in Mail on Mac and follow the instructions of the manufacturer.

Workaround for Mail (Apple) on iOS

Format one or more characters bold, italic or underlined in your email text.

The client sends the email in HTML format and **Signature and Disclaimer** attaches the HTML signature.

Remedy for Thunderbird

- For single emails: Select **Write** > **Options** > **Delivery Format** > **Rich Text (HTML) Only**.

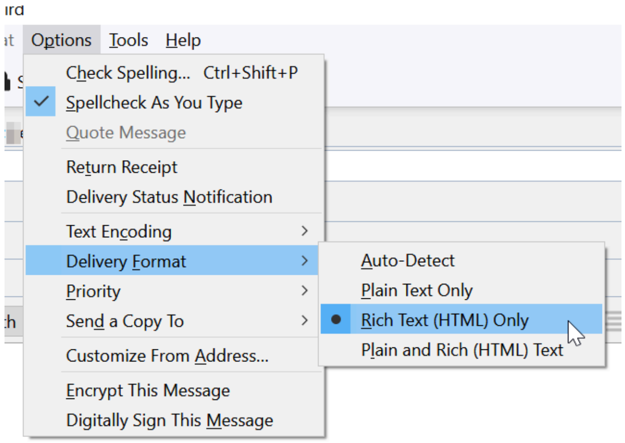
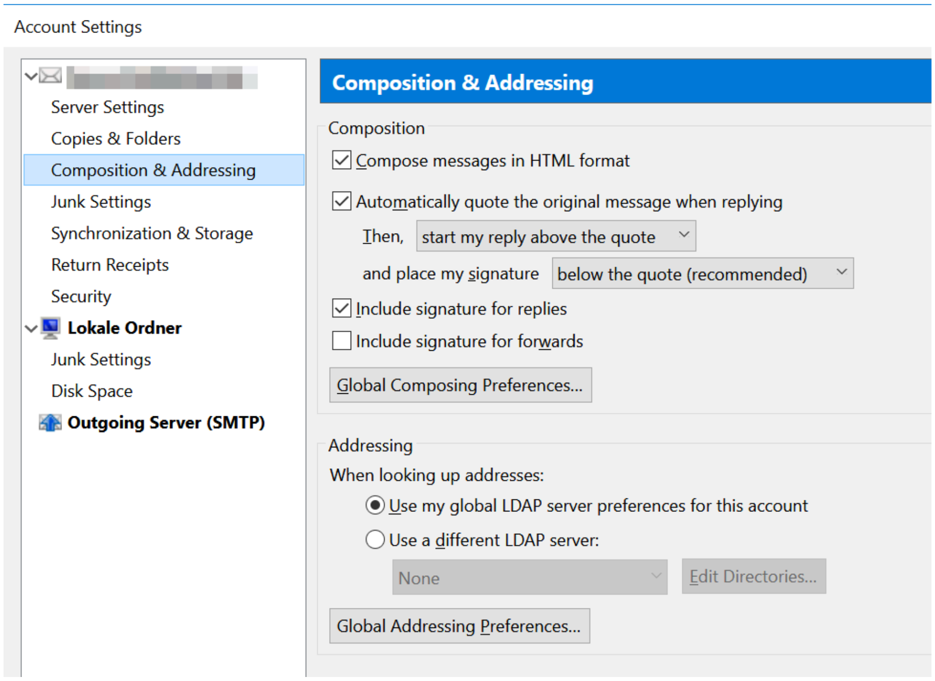


Figure 449: Options for a single email

- For all emails: Select **Write** > **Tools** > **Account Settings** > **Composition & Addressing** and activate **Compose messages in HTML format**.



Account Settings

[redacted]
Server Settings
Copies & Folders
Composition & Addressing
Junk Settings
Synchronization & Storage
Return Receipts
Security
Lokale Ordner
Junk Settings
Disk Space
Outgoing Server (SMTP)

Composition & Addressing

Composition

☑ Compose messages in HTML format

☑ Automatically quote the original message when replying

Then, start my reply above the quote

and place my signature below the quote (recommended)

☑ Include signature for replies

□ Include signature for forwards

Addressing

When looking up addresses:

● Use my global LDAP server preferences for this account

○ Use a different LDAP server:

None

Figure 450: Settings for all emails

Troubleshooting:

Condition

Rooms can no longer be booked in Microsoft 365 once Signature and Disclaimer is activated.

Reason

In order to book rooms, Microsoft 365 uses dedicated mailboxes called room mailboxes that only accept mailboxes from within the same organization. Once Signature and Disclaimer is activated, emails are redirected via our servers in order for signatures and disclaimers to be attached. Emails that are redirected via our servers are regarded as external emails and are not accepted by room mailboxes.

Remedy

1. Open the Exchange Management Shell.
2. Run the following command:

   ```
   Set-CalendarProcessing "" -ProcessExternalMeetingMessages $True
   ```

   ➔

   Room mailboxes are allowed to accept external emails.

Continuity Service

About the Continuity Service

With the Continuity Service, users can continue to receive and send emails if your own email server fails. Once the Continuity Service is configured for a domain or a single user, the Continuity Service is set to be automatically activated when the email server fails.

If users are synchronized via LDAP, they must set an emergency password (see Activating Emergency Passwords) to access the webmail system of the Continuity Service.

> **Important:**
>
> The Continuity Service is a standby system. If a customer activates the service after their own email server has already failed, the Continuity Service will only take effect after a delay of several hours. Therefore, emails sent in the meantime may be lost. To reliably keep the email traffic up and running, the Continuity Service must be permanently activated.

For domains for which the Continuity Service is activated, the emails of the last three months are stored in the email archive. Furthermore, the user can see in the **Email Live Tracking** module (see "Email Live Tracking" in the Control Panel manual) which of their emails have been delivered by the Continuity Service.

Notice:

Emails delivered by the Continuity Service retain the status **Deferred** after delivery.

In the following, the configuration options of the Continuity Service are described:

- Activating the Continuity Service (see Activating the Continuity Service)
- Adding All Users of a Domain to the Continuity Service (see Adding All Users of a Domain to the Continuity Service on page 589)
- Adding Single Users to the Continuity Service (see Adding Single Users to the Continuity Service on page 590)
- Excluding Users from the Continuity Service (see Excluding Users from the Continuity Service on page 592)
- Activating Emergency Passwords (see Activating Emergency Passwords)
- Deactivating the Continuity Service (see Deactivating the Continuity Service)

Adding All Users of a Domain to the Continuity Service

You have activated the Continuity Service (see Activating the Continuity Service).

In the **Security Settings** > **Continuity Service** module, you can add all users of a domain to the Continuity Service (see About the Continuity Service on page 588) to keep the email traffic for their mailboxes up and running in case your own email server fails.

1. Log in to the Control Panel with your administrative credentials.
2. Select the domain from the scope selection.
3. Navigate to **Security Settings** > **Continuity Service**.

4. **Important:**

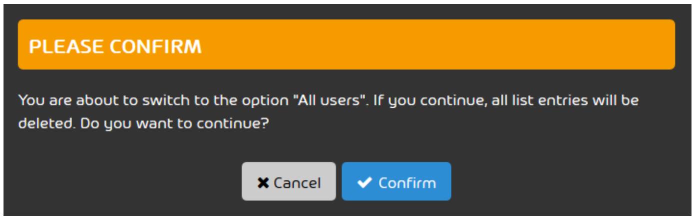
   If you switch from the option **Selected users only** to the option **All users**, all previously added users are removed.

   To activate the Continuity Service for all users of the domain, activate the checkbox **All users**.

   ➜

   If you have previously added single users to the Continuity Service, a warning message appears.

5. If a warning message appears, click on **Confirm**.



PLEASE CONFIRM

You are about to switch to the option "All users". If you continue, all list entries will be deleted. Do you want to continue?

Figure 451: Confirm

➜

The Continuity Service is applied to all users of the domain.

All users of a domain have been added to the Continuity Service.

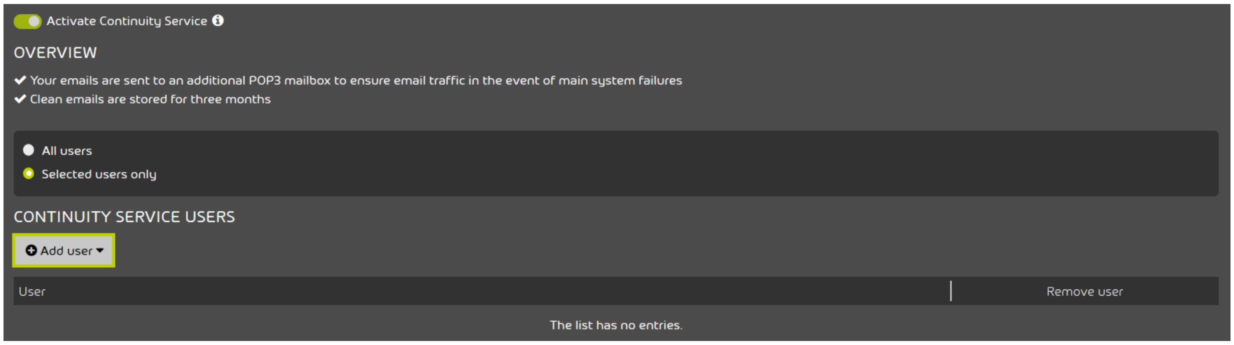
Adding Single Users to the Continuity Service

You have activated the Continuity Service (see Activating the Continuity Service).

In the **Security Settings** > **Continuity Service** module, you can add single users of a domain to the Continuity Service (see About the Continuity Service on page 588) to keep the email traffic for their mailboxes up and running in case your own email server fails.

1. Log in to the Control Panel with your administrative credentials.

2. Select the domain from the scope selection.
3. Navigate to **Security Settings** > **Continuity Service**.
4. Activate the checkbox **Selected users only**.
5. Click on **Add** under **Continuity Service Users**.



Activate Continuity Service

OVERVIEW

✓ Your emails are sent to an additional POP3 mailbox to ensure email traffic in the event of main system failures
✓ Clean emails are stored for three months

○ All users
● Selected users only

CONTINUITY SERVICE USERS

User	Remove user

The list has no entries.

Figure 452: Add user

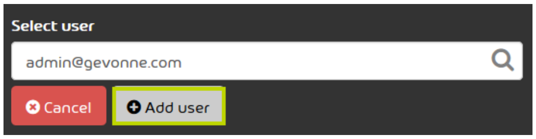
An extended view opens.

6. Enter the email address of the user who you want to add under **Select user**.

Notice:

To trigger the automatic suggestion function, enter at least three consecutive characters.

7. Click on **Add**.



Select user

admin@gevonne.com

Figure 453: Enter user

The user is added and appears in the table. The Continuity Service is applied to the user.

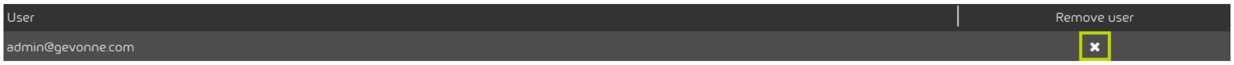
A single user has been added to the Continuity Service.

Excluding Users from the Continuity Service

You have added single users to the Continuity Service (see Adding Single Users to the Continuity Service on page 590).

In the **Security Settings** > **Continuity Service** module, you can exclude users so they will no longer be secured by the Continuity Service.

1. Log in to the Control Panel with your administrative credentials.
2. Select the domain from the scope selection.
3. Navigate to **Security Settings** > **Continuity Service**.
4. To exclude a user from the Continuity Service, click on the cross under **Remove user** next to the user.



User	Remove user
admin@gevonne.com	✖

Figure 454: Remove user

The user is removed from the list. The Continuity Service is no longer applied to the user.

A user has been excluded from the Continuity Service.

Customization

Control Panel Customization

In the **Customization** module, administrators can customize the Control Panel on two levels.

On the one hand, administrators can determine the appearance of emails sent by the Control Panel (see Customizing the Email Template on page 600), and store the contact details (see Customizing Email Information on page 597) that are to be displayed in them.

Notice:

Websafe email notifications (see "Websafe" in the Control Panel manual) are also customized according to these settings.

On the other hand, administrators can customize the appearance of both the website of the Control Panel and the Progressive Web App and define a new URL and a new name for them (see Customizing the Control Panel on page 604).

The customization is displayed to all users who log in via the specified domain.

Attention:

Using a customized Control Panel will increase costs according to the price list.

Important:

If a customer-level administrator has not saved any settings for their domain in one of the tabs of the **Customization** module, the settings of the parent partner who has made changes to their settings, will be applied to their domain. If no settings have been saved at the level of their partner or the partner's parent partner, no customization will be performed.

Important:

Support information (see Adding Support Information to the Control Panel on page 594) must be added even if no other customization options are used. The support information is displayed for the users in the Control Panel.

Adding Support Information to the Control Panel

In the **Support information** tab of the **Customization** module (see Control Panel Customization on page 593), you can add the support information of your company for it to be displayed to the users in the Control Panel. This setting is independent of the Control Panel customization, which requires an additional fee. The data that is specified here is also displayed in the default version of the Control Panel.

Notice:

A partner's settings are also applied to their sub-partners and customers if the sub-partners and customers have not changed any settings themselves.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain that you would like to customize.

3. Navigate to **Customization** > **Support information**.

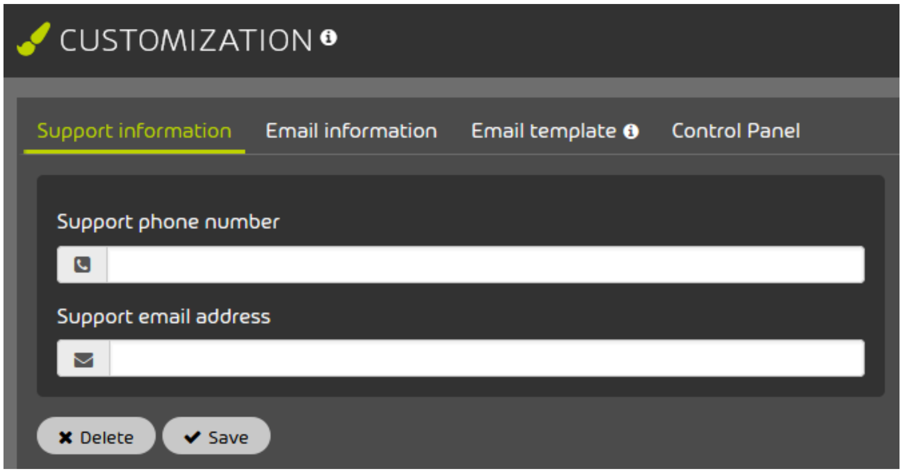
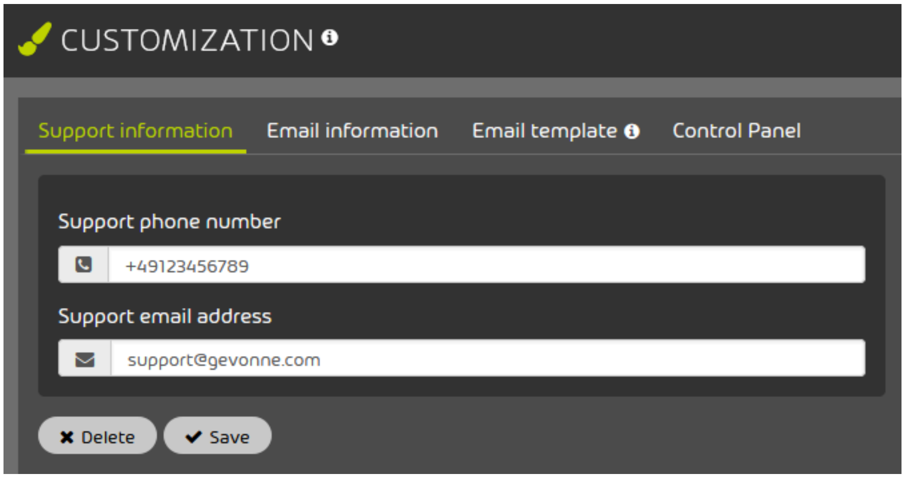


Figure 455: Select support information

4. Enter the support phone number of your company in the field **Support phone number**.

> **Notice:**
>
> If one of the fields described here is empty for a customer or partner, the value set by the next parent partner will be used for this field. If this field is empty for all parent partners, the default values of the Control Panel are used.

5. Enter the support email address of your company in the field **Support email address**.



Support phone number: +49123456789

Support email address: support@gevonne.com

Figure 456: Add support information

6. Click on **Save**.

The support information has been added to the Control Panel.

Next, you can customize the emails sent by the Control Panel for your company (see **Customizing Emails from the Control Panel** on page 596), and customize the appearance of the Control Panel (see **Customizing the Control Panel** on page 604).

Customizing Emails from the Control Panel

In different situations, the Control Panel automatically sends emails (for example, when a user requests a new password (see "Resetting a Password" in the Control Panel manual). You can customize both the appearance of emails sent by the Control Panel and the information therein according to your company.

1. Customize the email information according to your company (see Customizing Email Information on page 597).

   The emails sent by the Control Panel contain a custom legal notice, the name of a contact person from your company and a custom sender address.

2. Customize the appearance of the emails to fit your corporate image (see Customizing the Email Template on page 600).

   The color of the footers, the color scheme (theme) of the emails and the logo in the header of the emails are customized.

The appearance of the emails sent by the Control Panel and the information therein have been customized.

Next, you can customize the appearance of the Control Panel (see Customizing the Control Panel on page 604).

Customizing Email Information

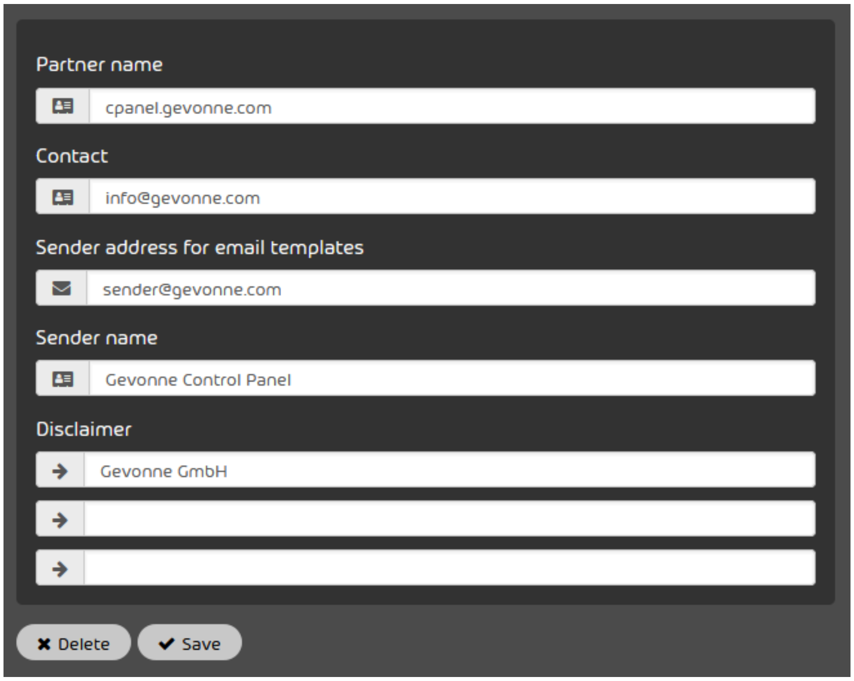
Under **Email information** in the **Customization** module (see Control Panel Customization on page 593), you can specify a greeting formula, contact information, a sender address and a disclaimer for emails sent by the Control Panel.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain that you would like to customize.

3. Navigate to **Customization** > **Email information**.

   ➜

   A form is displayed.



Partner name

cpanel.gevonne.com

Contact

info@gevonne.com

Sender address for email templates

sender@gevonne.com

Sender name

Gevonne Control Panel

Disclaimer

Gevonne GmbH

Figure 457: Email information

4. Fill in the form. The fields have the following meanings:

   - **Partner name**: Here you can enter the name of the company to be mentioned in the greeting at the beginning of the emails (e.g., "Dear <company name> customer,").
   - **Contact**: Here you can enter the signature text that will be displayed below the closing formula in emails (e.g., "Your Control Panel Team").
   - **Sender address for email templates**: Here you can enter the sender address for emails sent by the Control Panel.

     Notice:

     This sender address is not applied to emails sent by the Websafe (see chapter "Websafe" in the Control Panel manual).

     Notice:

     If a customer has activated the SPF check (see chapter "Activating the SPF Check" in the Control Panel manual), our SPF record must have been set in the DNS zone of the domain of the sender address (see chapter "Setting an SPF Record" in the Control Panel manual). Otherwise, the SPF checks on emails sent by the Control Panel will return errors (see chapter "SPF Check Logic" in the Control Panel manual).
   - **Sender name**: Here you can enter the display name of the sender.
   - **Disclaimer**: Here you can enter the company's legal notice.

   Notice:

   If one of these fields is empty for a customer or partner, the value set by the next parent partner will be used for this field. If this field is empty for all parent partners, the default values of the Control Panel are used.

5. Click on **Save**.

✓

The email information has been customized.

Next, you can customize the appearance of emails sent by the Control Panel for your company (see Customizing the Email Template on page 600), and the appearance of the Control Panel (see Customizing the Control Panel on page 604).

Customizing the Email Template

In the **Email template** tab of the **Customization** module (see Control Panel Customization on page 593), you can adjust the appearance of the emails sent by the Control Panel to your corporate image. The customization of the email template does not incur any additional costs and can be done independently of the Control Panel customization, which requires an additional fee. However, if the Control Panel is customized, the primary color, theme and logo from the tab **Email template** will also be used in the Control Panel (see Customizing the Appearance and URL of the Control Panel on page 605).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain that you would like to customize.
3. Navigate to **Customization** > **Email template**.

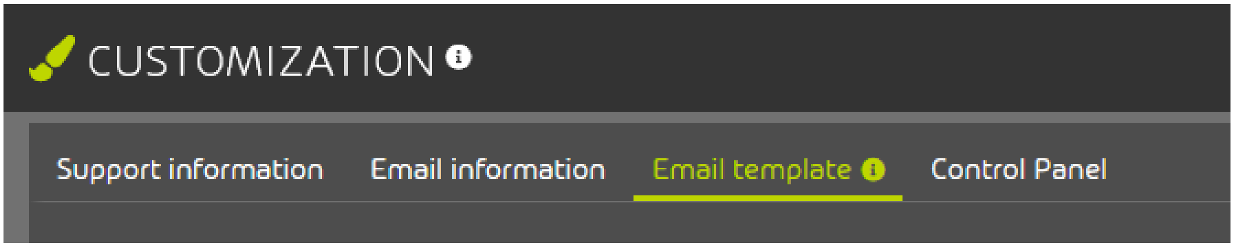
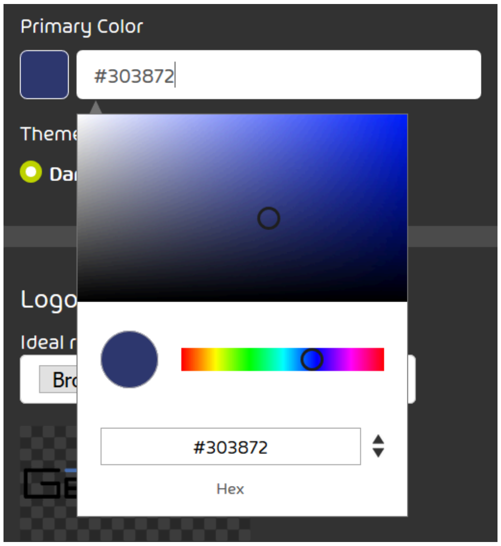


Figure 458: Select tab

4. Select a color for the footer of emails sent by the Control Panel.

   a) Click in the field under **Primary color**.



Primary Color: #303872

Hex: #303872

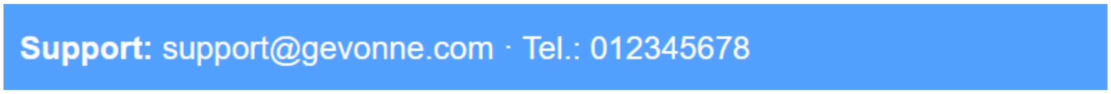
Figure 459: Select color

   b) Select a color. You can either click on the color in the gradient field or enter the color code in HEX, RGB or HSL into the field.

> **Notice:**
>
> If the Control Panel is customized, the selected color will also be used as the primary color of the Control Panel (see **Customizing the Appearance and URL of the Control Panel** on page 605).

➔

The selected color is displayed in the circle and the color code is displayed in HEX, RGB or HSL.

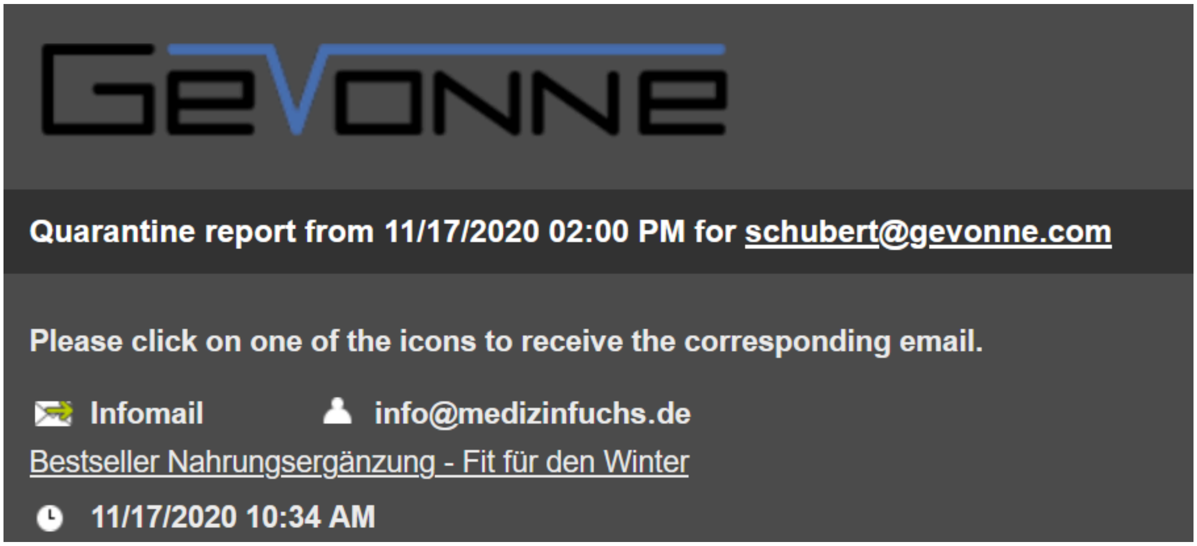


Support: support@gevonne.com · Tel.: 012345678

Figure 460: Colored footer in a quarantine report

5. Under **Theme**, select a theme for your emails. You have two options:

   - **Dark**: A dark theme is selected. Emails are displayed in dark colors.



Quarantine report from 11/17/2020 02:00 PM for schubert@gevonne.com

Please click on one of the icons to receive the corresponding email.

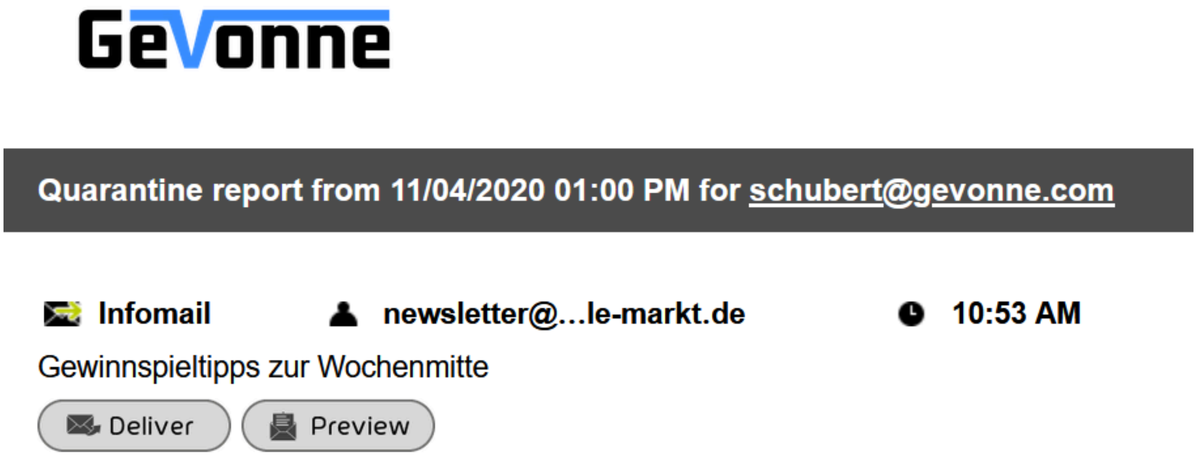
Infomail info@medizinfuchs.de

Bestseller Nahrungsergänzung - Fit für den Winter

11/17/2020 10:34 AM

Figure 461: Email with a dark theme

   - **Bright**: A bright theme is selected. Emails are displayed in bright colors.



Quarantine report from 11/04/2020 01:00 PM for schubert@gevonne.com

Infomail newsletter@...le-markt.de 10:53 AM

Gewinnspieltipps zur Wochenmitte

Figure 462: Email with a bright theme

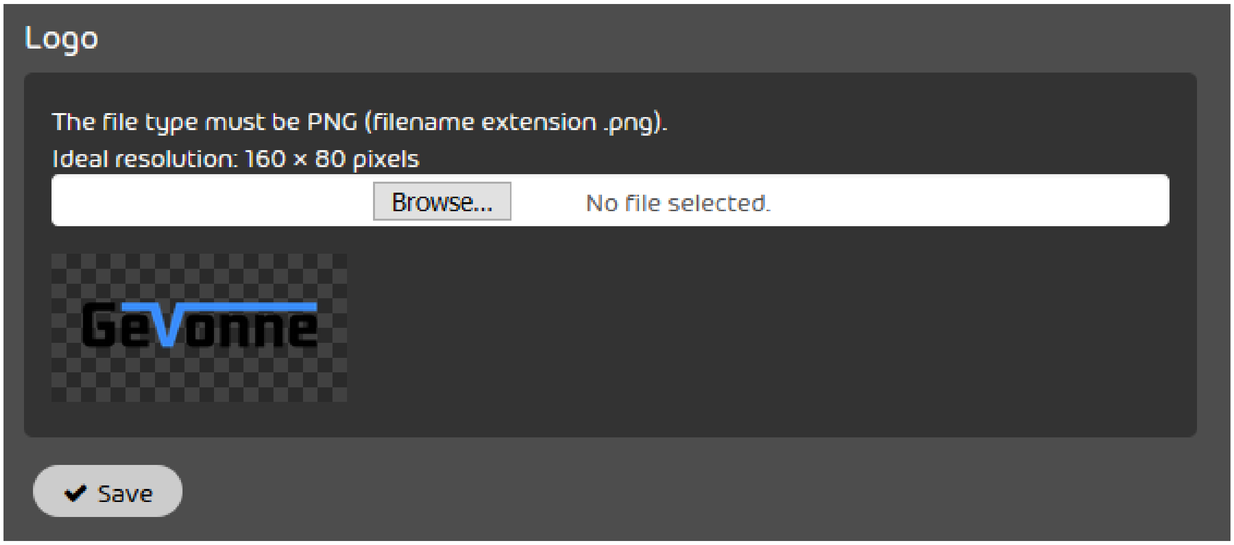
6. Under **Logo**, click on **Search** and select your logo.

Notice:

A logo with a resolution of 160 × 80 pixels delivers the best results.

Only the file format .png is supported.

The logo is displayed in the header of emails sent by the Control Panel.


Logo

The file type must be PNG (filename extension .png).

Ideal resolution: 160 × 80 pixels

Figure 463: Select logo

7. Click on **Save**.

✓

The appearance of the emails sent by the Control Panel has been customized.

Next, you can adjust the information shown on emails sent by the Control Panel to your company (see Customizing Email Information on page 597), and the appearance of the Control Panel (see Customizing the Control Panel on page 604).

Customizing the Control Panel

You can customize the URL and the appearance of the Control Panel by entering a URL of your domain and by incorporating your corporate colors, your logo and your favicon.

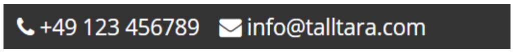
1. Choose a URL of your domain for the Control Panel and configure a redirection to the default URL of the Control Panel in a CNAME record in the DNS zone of your domain.

   In the next example, a CNAME record is set for **controlpanel.customerdomain.com**:

   controlpanel.customerdomain.com IN CNAME <default URL>

   > **Notice:**
   >
   > You can ask Support for the default URL of the Control Panel.

2. Customize the appearance and the URL of the Control Panel website (see Customizing the Appearance and URL of the Control Panel on page 605 and Customizing the Email Template on page 600).
3. Customize the app name and the app icon of the progressive web app to fit your corporate image (see Customizing the Progressive Web App on page 609).
4. Add the support information (phone number and email address) to be displayed to the users in the Control Panel (see Adding Support Information to the Control Panel on page 594).



☎ +49 123 456789 ✉ info@talltara.com

> **Notice:**
>
> This setting is independent of the Control Panel customization, which requires an additional fee. The contact data that is specified here is also displayed in the default version of the Control Panel.

Figure 464: Contact data in the Control Panel

5. **Attention:**

   Creating a customized version of the Control Panel will increase costs according to the price list.

   CAUTION:

   Make sure that you have entered all data and the URL for your customized Control Panel in the module **Customization**.

   To implement the customization of the Control Panel with the data and files you have provided, contact our support.

The Control Panel has been customized.

Customizing the Appearance and URL of the Control Panel

You have customized the email template (see Customizing the Email Template on page 600).

In the **Control Panel** tab of the **Customization** module (see Control Panel Customization on page 593), you can customize the appearance of the Control Panel to fit your corporate image. The primary color, theme and logo for the customized Control Panel are taken over from the settings in the tab **Email template**.

Notice:

Here are some examples of how the settings from the tab **Email template** affect the customized Control Panel (see Customizing the Email Template on page 600).

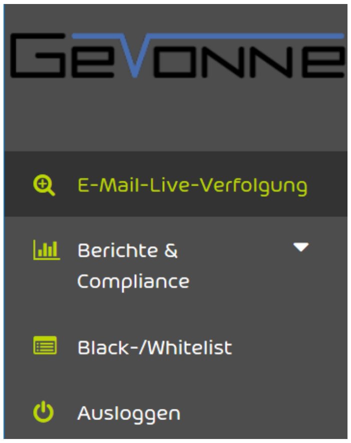


Figure 465: View of the Control Panel with a dark theme and a customized logo

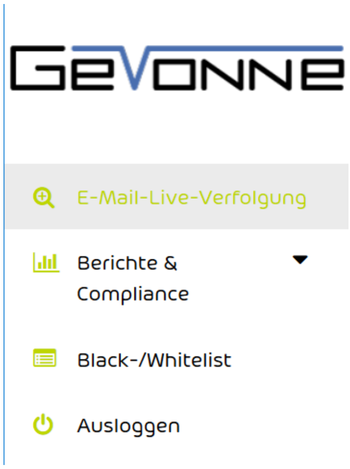


Figure 466: View of the Control Panel with a bright theme and a customized logo

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain that you would like to customize.

3. Navigate to **Customization** > **Control Panel**.

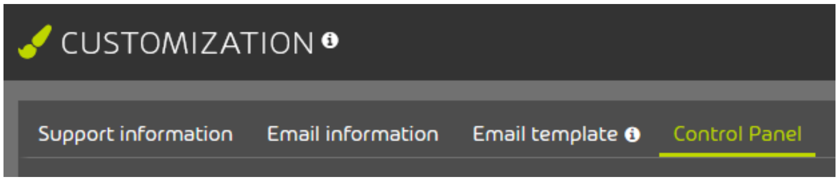


Figure 467: Select tab

4. **Important:**

   The Control Panel customization is only possible for partners or customers with at least 5,000 users.

   Toggle the switch **Activate customization of the Control Panel**.

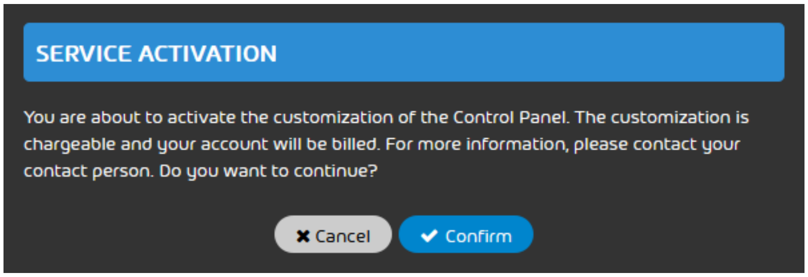
   ➜

   A confirmation window is displayed.

5. **Attention:**

   The Control Panel customization is chargeable.

   Click on **Confirm**.



SERVICE ACTIVATION

You are about to activate the customization of the Control Panel. The customization is chargeable and your account will be billed. For more information, please contact your contact person. Do you want to continue?

Figure 468: Confirm

➜

The settings in the tab **Control Panel** are enabled.

6. **CAUTION:**

   The Control Panel customization only works if the URL of the customized Control Panel points with a CNAME record to the URL of the default version of the Control Panel.

   Make sure that the URL points to the URL of the default version of the Control Panel through a CNAME record (see Customizing the Control Panel on page 604).

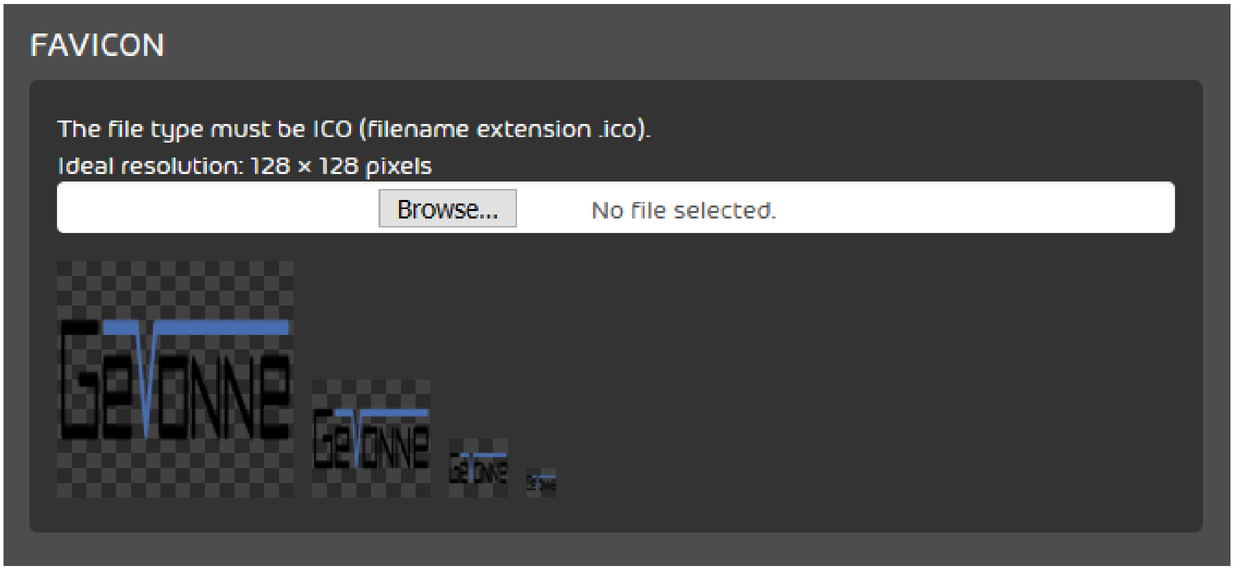
   Enter the URL of your domain to your customized Control Panel in the field **URL**.

   The URL must match the following pattern: **controlpanel.customerdomain.com**

7. Under **Favicon**, click on **Search** and select your favicon.

   Notice:

   The favicon must be uploaded in the ICO file format (filename extension *.ico). An optimal representation is achieved with a resolution of at least 128 × 128 pixels.



FAVICON

The file type must be ICO (filename extension .ico).
Ideal resolution: 128 × 128 pixels

Figure 469: Select favicon

8. Customize the Progressive Web App (see Customizing the Progressive Web App on page 609).

9. Click on **Save**.

> **Notice:**
>
> The deployment of the customization takes no more than 5 minutes.

10. Refresh the website to see your customization.

> **Notice:**
>
> The changes are only visible under the URL of the customized Control Panel.

✓

The appearance and URL of the Control Panel have been customized for a fee.

Next, you can customize the appearance of the Progressive Web App (see Customizing the Progressive Web App on page 609) and add support information (see Adding Support Information to the Control Panel on page 594).

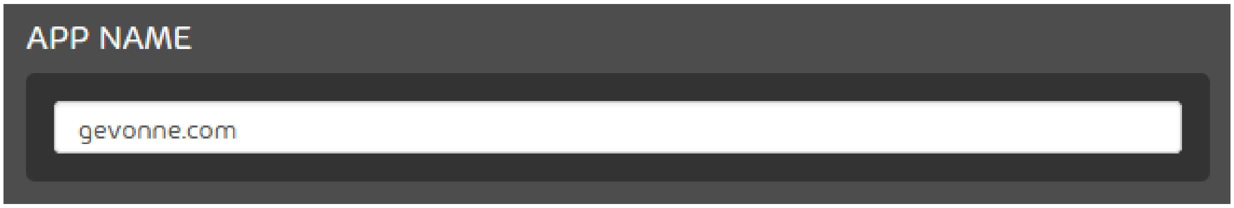
Customizing the Progressive Web App

You have activated the Control Panel customization (see Customizing the Appearance and URL of the Control Panel on page 605).

In the **Control Panel** tab of the **Customization** module (see Control Panel Customization on page 593), you can customize the app name and the app icon of the Progressive Web App to fit your corporate image.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain that you would like to customize.
3. Navigate to **Customization** > **Control Panel**.

4. Under **App name**, enter the name to be displayed on the home screen of mobile devices.



APP NAME

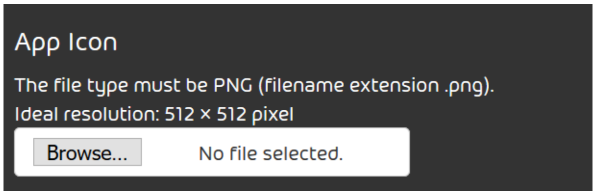
gevonne.com

Figure 470: Enter app name

5. Upload a picture under **App icon**.

Notice:

Only the file format .png is supported.



App Icon

The file type must be PNG (filename extension .png).
Ideal resolution: 512 × 512 pixel

Figure 471: Upload app icon

➔

Below the selection of the app icon, a preview of the icon in various sizes is displayed. In addition, a preview of the start screen is displayed under **Splash screen**. The splash screen is displayed while loading the progressive web app and contains the image file uploaded under **Logo**.

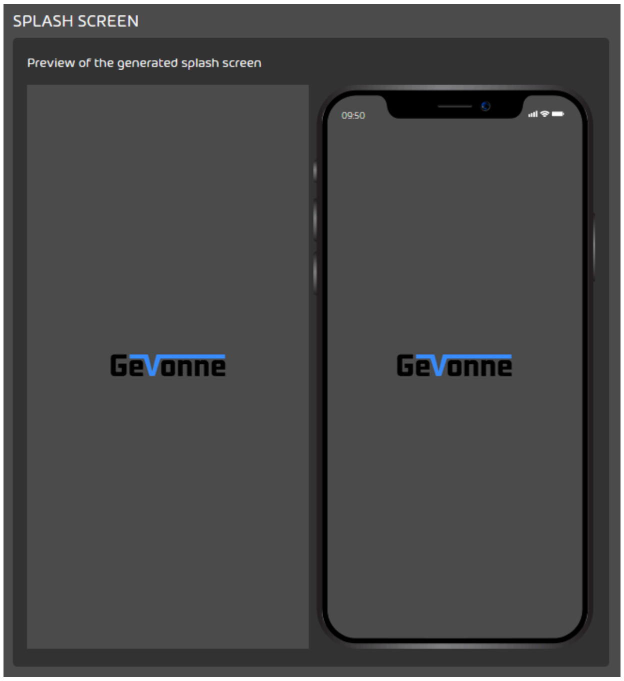


Figure 472: Preview of splash screen

6. Click on **Save**.

✓

The name and the logo of the progressive web app have been customized.

Next, you can customize the appearance of the of the Control Panel (see Customizing the Appearance and URL of the Control Panel on page 605) and add support information (see Adding Support Information to the Control Panel on page 594).

Email Classification Reasons

Classification reasons

In the Control Panel, each email is assigned to a category (see "Email Categories" in the Control Panel manual). The reasons for the classification of the emails are specified in the **Reason** column of the **Email Live Tracking** module (see "Email Live Tracking" in the Control Panel manual).

The following table shows the classification reasons together with the related email categories and explains them.

Table 44: Classification reasons

REASON	CATEGORY	DEFINITION
450 4.5.5 E-Mail deferred because of Spam sending to unlock goto [URL]	Rejected	The email has been temporarily rejected because spam had been sent from the email address of the sender. You can unlock the email address by clicking on the displayed URL.
450 4.5.5 too many false recipients rate-limited;	Rejected	The email has been temporarily rejected because it contains too many false recipients.
450 4.5.5 unblock [URL]	Rejected	The email has been temporarily rejected due to contents in its header. You can unlock the email address by clicking on the displayed URL.
450 4.5.6 busy try again later;	Rejected	The email has been temporarily rejected due to server overload.

REASON	CATEGORY	DEFINITION
450 4.5.7 busy try again later by {gateway}	Rejected	The email has been temporarily rejected due to server overload. The hostname of our gateway is displayed.
450 4.5.7 loop detected, by {relay};	Rejected	The email has been temporarily rejected because a loop has been detected. The hostname of our relay is displayed.
450 4.5.8 no mail data, by {relay};	Rejected	The email has been temporarily rejected because it does not have any content. The hostname of our relay is displayed.
450 4.5.8 no mail data;	Rejected	The email has been temporarily rejected because it does not have any content.
450 4.5.8 too much load try next hop;	Rejected	The email has been temporarily rejected because due to server overload. The delivery should be tried through a different hop.
450 4.5.9 Connection PID broken $CLEANUPID by $(hostname);	Rejected	The email has been temporarily rejected because of a system error.
450 4.5.9 Greylisted, please try again later;	Rejected	The email has been temporarily rejected because of greylisting.

REASON	CATEGORY	DEFINITION
450 4.5.9 no resources please take next hop. by {relay};	Rejected	The email has been temporarily rejected because no resources were available for the reception. The delivery should be tried through a different hop. The hostname of our relay is displayed.
450 4.5.9 no smtp resources, please take next hop. by {relay};	Rejected	The email has been temporarily rejected because no SMTP resources were available for the reception. The hostname of our relay is displayed.
450 5.5.6 loop detected;	Rejected	The email has been temporarily rejected because a loop has been detected.
454 4.7.1 {the sender's email address}: Relay access denied	Deferred	The email has been deferred because it was not sent from any of the relay server IP addresses defined in the **Spam and Malware Protection** module (see "Spam and Malware Protection" in the Control Panel manual). Through our infrastructure, the customer may only send emails originating from one of the specified IP addresses. The delivery of the email will be stopped after one day.

REASON	CATEGORY	DEFINITION
504 5.5.2 Recipient address rejected: need fully-qualified address	Rejected	The email has been rejected because the recipient's email address was incomplete.
523 5.2.3 E-Mail rejected, e-mail is too large by company rule {rule ID};	Rejected	The email has been rejected because it exceeded a size limit defined by the customer. The rule ID is displayed.
550 5.1.1 Recipient address rejected: undeliverable address	Rejected	The email has been rejected because the recipient's email address does not exist.
552 5.2.2 Mailbox not available. For more information visit {URL};	Rejected	The email has been rejected due to the recipient's or the sender's email address. The hostname of our gateway is displayed.
552 5.5.2 Message size exceeds fixed maximum message size. Size: {email size}, Max size: {maximum size} by {gateway};	Rejected	The email has been rejected because it exceeds the size limit at the gate. The hostname of our gateway is displayed.
552 5.5.2 Size: {email size}	Rejected	The email has been rejected according to the Content Control policies (see "About Content Control" in the Control Panel manual) because it does not comply with the applicable size limits. The email size is specified.

REASON	CATEGORY	DEFINITION
552 5.5.8 utilize Smarthost instead of MX by {gateway};	Rejected	The email has been rejected because it should be sent via a smarthost and not directly to the gate. The hostname of our gateway is displayed.
554 5.5.4 Your IP {IP address} address has a bad reputation. To unblock visit {URL};	Rejected	The email has been rejected because your IP address has a negative reputation. You can unlock your email address by following the given URL.
554 5.5.5 E-Mail rejected Spam found, for support contact {URL};	Rejected	The email has been rejected because it contains spam. To send a request to support, click on the given URL.
554 5.6.0 unblock {URL};	Rejected	The email has been rejected because its header is too big. To send a request to support, click on the given URL.
554 5.6.1 E-Mail rejected because of Spam-Header to unlock goto {URL};	Rejected	Your email has been rejected because it has been identified as spam based on its header. You can unlock the email address by clicking on the displayed URL.

REASON	CATEGORY	DEFINITION
554 5.6.1 Your mailheader contains SPAM. To unblock visit {URL}	Rejected	Your email has been rejected because it has been identified as spam based on its header. You can unlock the email address by clicking on the displayed URL.
554 5.6.2 E-Mail rejected because of Spam-http-Link to unlock goto {URL};	Rejected	Your email has been rejected because it has been identified as spam based on a link. You can unlock the email address by clicking on the displayed URL.
554 5.6.2 Your mail contains a SPAM-LINK. To unblock visit {URL};	Rejected	Your email has been rejected because it has been identified as spam based on a link. You can unlock the email address by clicking on the displayed URL.
554 5.6.3 E-Mail rejected because of Spam-Body to unlock goto {URL};	Rejected	Your email has been rejected because it has been identified as spam based on its text. You can unlock the email address by clicking on the displayed URL.

REASON	CATEGORY	DEFINITION
554 5.6.3 Your mail contains SPAM. To unblock visit {URL};	Rejected	The email has been rejected because it contains spam. You can unlock the email address by clicking on the displayed URL.
554 5.6.4 E-Mail rejected, forbidden attachment by company rule Attachments {rule ID}	Rejected	The email has been rejected because it contains a forbidden attachment according to rules defined by the customer. The rule ID is displayed.
554 5.6.4 E-Mail rejected Virus found, for support contact {URL}	Rejected	The email has been rejected because it contains viruses. To send a request to support, click on the given URL.
554 5.6.9, customer rule based reject by antispameurope Compliancfilter ID={rule ID}	Rejected	The email has been rejected by the specified Compliance Filter rule (see "About the Compliance Filter" in the Control Panel manual). The rule ID is displayed.
554 5.6.9 Compliance rule based reject by antispameurope Compliancefilter ID={rule ID} by {gateway};	Rejected	The email has been rejected by the specified Compliance Filter rule of the specified host (see "About the Compliance Filter" in the Control Panel manual). The rule ID and the hostname of our gateway are displayed.

REASON	CATEGORY	DEFINITION
554 5.6.9 Compliance rule based reject by Compliancefilter ID={rule ID} by {gateway};	Rejected	The email has been rejected by the specified Compliance Filter rule of the specified host (see "About the Compliance Filter" in the Control Panel manual). The rule ID and the hostname of our gateway are displayed.
554 5.7.0 Sender address rejected: {sender address} sending out spam;	Rejected	The email has been rejected because the sender distributed spam.
554 5.7.12 SPF fail by customer policy. {Gateway};	Rejected	The email has been rejected because of an SPF fail according to a setting made by the customer (see "SPF check" in the Control Panel manual). The hostname of our gateway is displayed.

REASON	CATEGORY	DEFINITION
554 5.7.1 Domain / User unknown	Rejected	The email has been rejected because the specified domain or the specified mailbox is not available in the Control Panel (see "Domains" in the Control Panel manual and "Mailboxes" in the Control Panel manual). **Notice:** The creation and synchronization of new mailboxes may take up to 90 minutes. If emails are sent to a mailbox before its creation has been completed, the emails are rejected.
554 5.7.2 Sender address rejected: Access denied;	Rejected	The email has been rejected because the sender's IP address is not registered in our system.
Allowed by User Policy	Clean	The sender or sending host of the email is on the recipient's allow list (see 'About Deny & Allow Lists' in the Control Panel manual).
Bad Host Reputation	Spam	The sending host of the email has a negative reputation.

REASON	CATEGORY	DEFINITION
Bad IP Reputation	Spam	The IP address of the sending host of the email has a negative reputation.
Bad Sender Reputation	Spam	The sender of the email has a negative reputation.
Bad URL Reputation	Spam	The email contains at least one link to a web server with a negative reputation.
Block by Compliance Filter Policy ID={rule ID}	Rejected	The email has been blocked by a Compliance Filter rule as Threat (see "About the Compliance Filter" in the Control Panel manual). The rule ID is displayed.
Business Email Compromise	AdvThreat	The email is a fraudulent email with a fake sender from your own company.
Clean by Compliance Rule ID={rule ID}	Clean	The email has been classified as clean by a Compliance Filter rule (see "About the Compliance Filter" in the Control Panel manual). The rule ID is displayed.

REASON	CATEGORY	DEFINITION
Denied by User Policy	Spam	The sender or sending host of the email is on the recipient's deny list (see 'About Deny & Allow Lists' in the Control Panel manual).
Detached by Content Control Policy	Content	At least one attachment is forbidden according to the settings of Content Control (see "About Content Control" in the Control Panel manual).
DKIM Failure	Spam	The DKIM validation failed (see "DKIM Validation and DKIM Signing" in the Control Panel manual).
DMARC Failure	Spam	The DMARC validation failed (see "DMARC Validation" in the Control Panel manual).
Envelope SPF Failure	Rejected , Spam	The SPF check in the envelope of the email failed (see "SPF check" in the Control Panel manual). **Reject email** or **Quarantine email as spam** was defined as the action after a fail.
Good Sender Reputation	Clean	The sender or sending host of the email has a positive reputation.

REASON	CATEGORY	DEFINITION
Ham	Clean	Ham is the opposite of spam. Ham is thus a desired email that matches the pattern of a valid email.
Impersonation attempt by customer policy	AdvThreat , Threat	The email sender's display name matches the display name of a registered Control Panel user. However, the email address in the header from differs from the email address that is registered for this user.
Malicious Attachment	AdvThreat , Rejected, Threat	At least one attachment of the email is malicious.
Malicious Email Content	AdvThreat , Rejected, Threat	The email contains malicious content.
Malicious URL	AdvThreat , Rejected, Threat	The email contains links to malicious websites or documents.
Massive Attack Prevention	AdvThreat , Threat	The email matches the pattern of a starting malware campaign.

REASON	CATEGORY	DEFINITION
Message Header SPF Failure	Rejected , Spam	The SPF check in the header of the email failed (see "SPF check" in the Control Panel manual). **Reject email** or **Quarantine email as spam** was defined as the action after a fail.
Phishing	AdvThreat , Threat	The email contains characteristics of a phishing attack.
RBL	Rejected	The sending host of the email has a negative reputation.
Rejected by Content Filter	Content	The email has been rejected according to the Content Control policies (see "About Content Control" in the Control Panel manual) because it contains at least one forbidden attachment.
Sandbox	AdvThreat	At least one attachment of the email has been dynamically analyzed by the Sandbox Engine of Advanced Threat Protection and has been rated as malicious (see "Description of the ATP Engines" in the Control Panel manual).

REASON	CATEGORY	DEFINITION
Sender Allowed by Domain Policy	Clean	The sender or sending host of the email is on the allow list of the customer administrator (see "About Deny & Allow Lists" in the Control Panel manual).
Sender Denied by Domain Policy	Spam	The sender or sending host of the email is on the deny list of the customer administrator (see "About Deny & Allow Lists" in the Control Panel manual).
Spam by Compliance Rule ID={rule ID}	Spam	The email has been classified as spam by a Compliance Filter rule (see "About the Compliance Filter" in the Control Panel manual). The rule ID is displayed.
Spam Content	Spam	The email contains content that is classified as spam.
SPF Failure	Rejected	The email has been rejected because of an SPF fail (see "SPF check" in the Control Panel manual).
Statusmail	Clean	The email is an automatically generated system notification, such as a quarantine report (see "About Quarantine Report" in the Control Panel manual).

REASON	CATEGORY	DEFINITION
Targeted Fraud	AdvThreat	The email matches the pattern of a targeted fraud attack.
Threat by Compliance Rule ID={rule ID}	Threat	The email has been classified as Threat by a Compliance Filter rule (see "About the Compliance Filter" in the Control Panel manual). The rule ID is displayed.
Unsolicited Email	Spam	The email has been rated as unwanted because it contains, for instance, an unrequested offer.

Index

WatchGuard®