2020-05-20

HORNETSECURITY

CONTROL PANEL MANUAL FOR PARTNERS

www.hornetsecurity.com

THE CLOUD SECURITY PIONEER

Contents

About this Manual 9

Introduction 10

- Requirements 10
- Version Information 10
- Viewing the Version Number 11

Logging in 12

- Resetting the Password 15

User Settings 17

- Opening the User Settings 17
- Settings 17
  - Changing the Password 17
  - Changing the Location and the Language 18
- Creating an API Token 19
- Creating an Out of Office Note 21
- Configuring the Spam Report 22

Rights Management in the Control Panel 25

- Roles 25
- Application Scopes 26
  - Selection of Scopes 26

Email Live Tracking 29

- Overview 29
- Customizing the Email Display 31
  - Customizing Email Fields 31
  - Resizing Fields 32
  - Changing the Position of Email Fields 33
- Filtering Emails 34
  - Filtering Emails by Category 34
  - Search Bar 34

Email Field Filters....35
Filtering Results from the Email Display....36
Resetting All Filters....36
Advanced Search....36
Email Details....37
Opening the Email Details....37
Initiating an ATP Scan Manually....38
ATP Report....40
Extended Email Information....42
Email Fields....43
Processing Emails....44
Email Actions....45
Exporting a List as CSV....47

Service Dashboard....49
About the Service Dashboard....49
Administration of Partners and Customers....49
Filtering Entries....50
Creating Customers or Sub-Partners....51
Deleting a Customer....52
Role Management....53
Assigning a Role....53
Delete role assignment....54
Basic Settings....55
LDAP Connection....55
Contact Data....65

365 Total Protection....69
365 Total Protection....69
Description of 365 Total Protection....69
Onboarding of Microsoft 365 Customers....69
Setting up 365 Total Protection....72
Configuration of Microsoft Services....75
Email Encryption....92
Activating the Continuity Service (365 Total Protection Enterprise only)....93
Group Management in the Control Panel....94
Ordering 365 Total Protection....98
Offboarding after Termination of the Trial Period or Cancellation....98
365 Total Encryption....102

About 365 Total Encryption....102
Activating 365 Total Encryption for a domain....103
Filtering mailboxes by status....105
Activating the Mailbox Encryption....106
Notifying users again....108
Deactivating the Mailbox Encryption....109
Configuration as User....110
Master Key....159

Reporting & Compliance....166
Email Statistics....166
Filtering Diagrams and Statistics....166
Emails by Type....167
Emails by Time....168
Emails by User....168
Threat Live Report....169
About Threat Live Report....169
Displaying Global Data....170
Selecting the Period....170
Statistic Descriptions....171
Description of Attack Types....177
Description of Attack Vectors....179
Auditing 2.0....180
About this manual....180
Auditing....180
Description of Categories....180
Filtering Events....181
Resetting Settings....186
Auditing....187

Web Filter....188
Editing Settings in the Web Filter Module....188
Release Requests....188
Blocked Sites....189
Valid Sites....190
Reporting an Incorrectly Categorized Website....191
Grouping of URLs....192
Black & White Lists....193
Blocking or Releasing Domains via Black or White List....193

Releasing a Website Specifically....196
Locking Websites Specifically....196
Configuration....197
Activating Web Filter for an Individual Domain....197
Gruppeneinstellungen....200
Web Filter Categories....206
Web Filter Templates....209
Exceptions....210
Statistics....211
Web Filter Statistics....211

Customer Settings....213
Mailboxes....214
Adding a Mailbox....215
Importing Mailboxes from a CSV File....215
Adding a forward mailbox....222
Activating or Deactivating a Mailbox....223
Adding an Alias Address....224
Entering a Delegate....225
Importing Recipients for Forward Mailboxes from a CSV File....226
Groups....229
Adding a group....229
Importing Group Members from a CSV File....230
Manage members....233
Renaming a Group....234
Customizing a Description....235
Deleting a Group....236
Domains....238
Adding a Domain....238
Importing Domains from a CSV File....239
Deleting Domains....241
Password Policy & IPs....241
Assign Password Policies....242
Resetting Password Policies....243
Assigning an IP Address....243
Deleting an IP Restriction....244

Black & White Lists....245
About Black & White Lists....245

Creating Black and White List Entries....245
Deleting Black or White List Entries....247
Searching for Black and White List entries....248
Processing hierarchy of black list and white list entries....249

Security Settings....250
Security Settings....250
Advanced Threat Protection (ATP)....250
Advanced Threat Protection functionality....250
Basic Settings....256
ATP scan....263
ATP Report....265
Spam Report....267
About the Spam Report....267
Activating the Spam Report for a Domain....267
Configuring the Spam Report for a Domain....268
Configuring the Spam Report for a Mailbox....270
Deactivating the Spam Report for a Domain....272
Spam and Malware Protection....273
Spam and Malware Protection....273
Content Control....285
About Content Control....285
Activating Content Control....285
Adding a group....285
Deleting a Group....286
Setting up Content Control....287
Overview of Categories....291
Deactivating Content Control....292
Compliance Filter....293
Compliance Filter....293
Setting up the Compliance Filter....293
Compliance Filter Rule Creation....295
Filter Sequence and Classification....299
Regular Expressions....306
Ruleset order....312
Setting up Advanced Routing....313
Signature and Disclaimer....314
Introduction....314
Mobile Use of Signature & Disclaimer....315

Activating LDAP for Signature & Disclaimer ... 315
Activating Signature & Disclaimer in the Web Interface ... 317
Creating Signatures and Disclaimers ... 317
Editing or Deleting Signature and Disclaimer Templates ... 321
Using the WYSIWYG Editor ... 322
Embed Images in Signature & Disclaimer ... 333
Data Synchronization via LDAP ... 340
Troubleshooting ... 341
Archiving Audit Access Management ... 344
Archiving Audit Access Management ... 344
Setting up and Activating Audit Accesses ... 345
Archiving ... 347
Setting up and Activating Archiving ... 348
Adding Exceptions ... 349
Deactivating Archiving ... 350
Continuity Service ... 350
Encryption ... 351
Activating Email Encryption ... 352
Checking the Encryption Capability ... 352
Encryption Methods ... 353
Sequence of Encryption Methods ... 354
Subject Tagging for Encryption ... 354
Setting Deviating Encryption Policies ... 355
Combination of Encryption Methods ... 359
Certificates ... 361
Websafe ... 363
Using Keywords in the Email Subject ... 367
Hornetdrive ... 367
About Hornetdrive ... 367
Performing Actions ... 368
Account Area ... 374

Whitelabeling ... 379
Control Panel Customization (Whitelabel) ... 379
Prerequisites to Customize the Control Panel ... 379
Customizing the Control Panel ... 379
Customizing the Progressive Web App ... 383
Example: Customizing the Control Panel ... 386
Fallback Design ... 387

Displayed Email Information....387
Adding Email Information....387
Contact Data in the Control Panel....388
Adding Support Information in the Control Panel....389

Email Categories....390

Classification Reasons....391
Classifications ATP, Rejected, Virus....391
Classification Content....392
Classification Valid....392
Classification Spam....393
Deprecated Email Classification Reasons....394
Classification ATP/Content/Virus....394
Classification Rejected....396
Classification Quarantined....397
Classification Valid....398

Index....400

About this Manual

This manual is for both users and administrators of the Control Panel. It describes the usage as well as the administrative tasks.

The administrative roles are divided into two levels:

- Domain administrator: Is responsible for a primary email domain, the related alias email domains and all email addresses.
- Partner: Is responsible for several clients. Each client corresponds to a primary email domain, its alias email domains and all email addresses.

Notice:

Depending on the level of rights assigned to you, it is possible that you cannot see all the menus described.

Introduction

The main functionality of the Control Panel is to monitor and control the flow of your emails.

The Control Panel is designed for handling incoming emails and evaluating the email traffic. For example, you can mark emails as spam or release emails that have been marked as spam. You can also blacklist or whitelist senders. It provides you with an easy-to-use web interface with a responsive design. Thus you can use it on your desktop and on your mobile device from everywhere you are.

Notice:

Email Live Tracking has been enhanced with several features compared to the old "email search". You can use all other modules of the Control Panel as usual, as they are integrated from the old version of the Control Panel until they are completed.

Requirements

The support of the browsers starts with the following versions:

- Google Chrome version 55
- Mozilla Firefox version 50
- Internet Explorer version 11
- Microsoft Edge version 38
- Apple Safari version 9

Important:

The private mode of the listed browsers is not supported.

Version Information

The linked version information on the Website contains information about new features and solved problems in the respective Control Panel release.

You find the latest version information Here.

Viewing the Version Number

1. Open the Control Panel and log in.
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.

Logging in

1. Enter the URL of the Control Panel website in your browser to log in to the Control Panel.
   ➔ The following login screen appears:

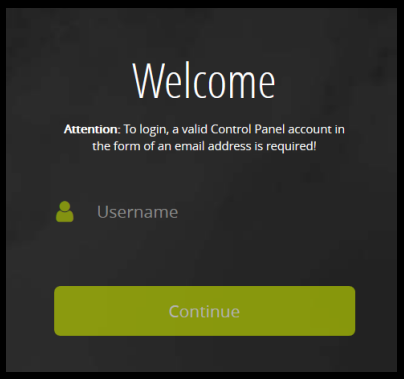


Figure 1: Control Panel login

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

> **Notice:**
>
> Enter your personal email address as the username. You can change the scope after you have logged in. After a new registration, you will receive your access data from your partner or support.

3. Click on **Continue**.
4. Perform the following steps if your account is synchronized with LDAP or was created directly in the Control Panel. If your account is synchronized with Microsoft 365, go to step 5.

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

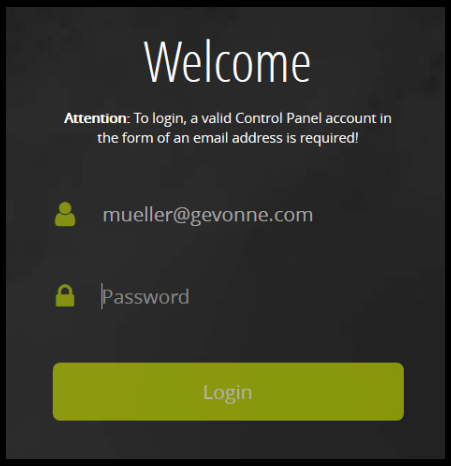


Figure 2: Enter Password

b) Click on **Login**.

➔ You have logged in to the Control Panel.

> **Notice:**
>
> When you log in for the first time, you must select a time zone that determines the language of the Control Panel as well as the time and date. You can change the time zone and the language at any time in the user settings.

5. If your account is synchronized with Microsoft 365, follow these steps.

   a) Enter your email address again in the Microsoft login window.

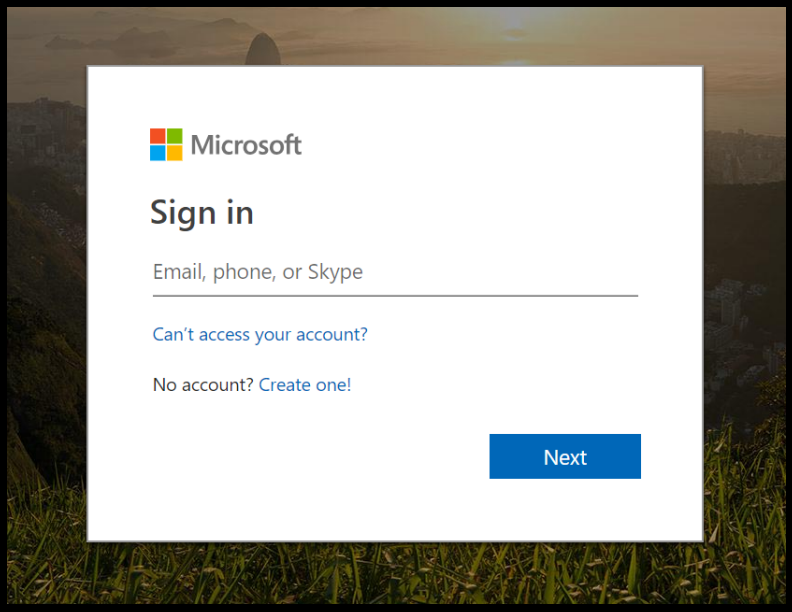


Figure 3: Microsoft Login

b) Click on **Next**.

c) Enter your password.

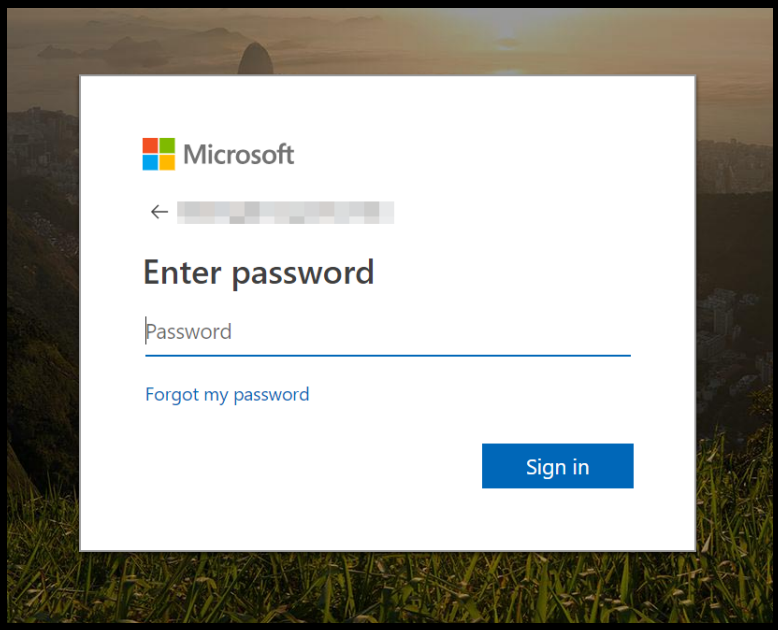


Figure 4: Enter Password

d) Click on **Sign in**.

e) Select whether you want to stay logged in.

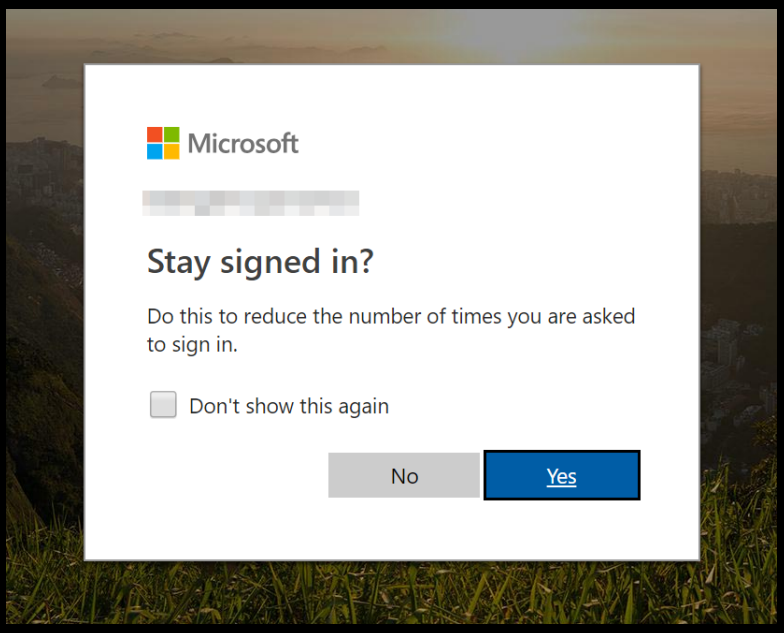


Figure 5: Options

You have logged in to the Control Panel.

Notice:

When you log in for the first time, you must select a time zone that determines the language of the Control Panel as well as the time and date. You can change the time zone and the language at any time in the user settings.

Resetting the Password

Reset your password for your account if you forgot it.

Prerequisite: Your account is not synchronized via LDAP or Microsoft 365.

You cannot reset your password if your account is synchronized via LDAP or Microsoft 365. If you want to reset your password, contact your administrator.

1. Click on **Reset password?**.

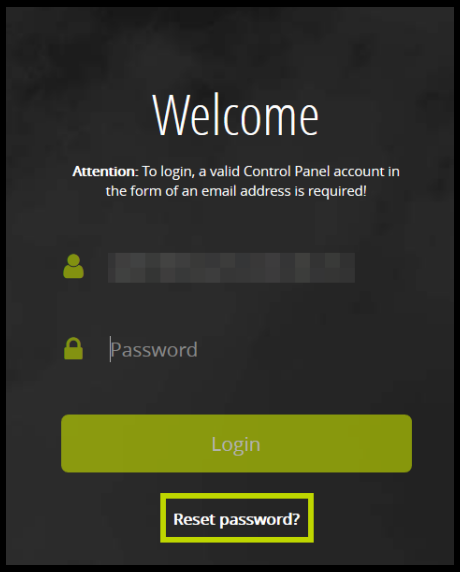


Figure 6: Reset password

➔ You get an email with a new password and an activation link.

2. Click on the activation link in the email.
   ➔ A window with the application form for the Control Panel opens.
3. Enter the password which you got in the email.
   ➔ You are logged in.

Passwort has been reset.

User Settings

You can change your password and your location in the user settings. The location is responsible for the language and timezone used in the Control Panel.

Notice:

It is possible to change the settings individually or all at once.

Opening the User Settings

Click on ⚙ in the upper right corner of the window.

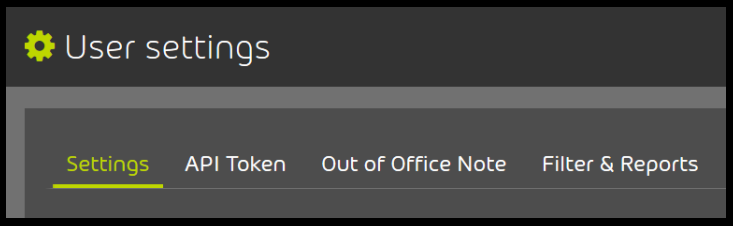


Figure 7: User Settings

The user settings have been opened.

Settings

Changing the Password

1. Enter your current password in the text field Old Password.
2. Enter your new password in the text fields New Password and Repeat.
3. Click on Save, to save your new password.

Password has been changed.

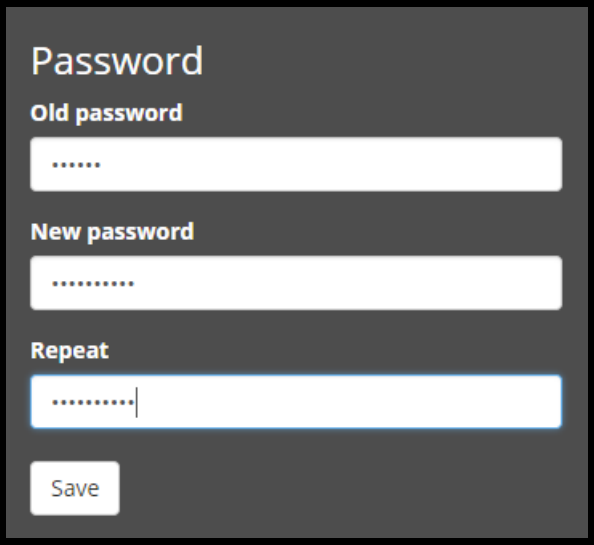


Figure 8: Changing the password

Changing the Location and the Language

The location and language are selected independently and do not influence each other.

Notice:

You select a location and a language at your first login but you can change these in the user settings at any time.

1. **Notice:** The selected location determines the time zone to which the time entries in the Control Panel are adapted.

   Select the location in the upper dropdown menu.
2. Select the language in the lower dropdown menu.
3. Click on **Save** to save the changes.

The location and the language have been changed.

Figure 9: Changing the location and the language

Creating an API Token

You can use an API token to grant applications access to the Control Panel API. Each application has its own personal access token.

1. Click on to open the user settings.
2. Select the tab **API Token**.
3. Click on **Create Token**.

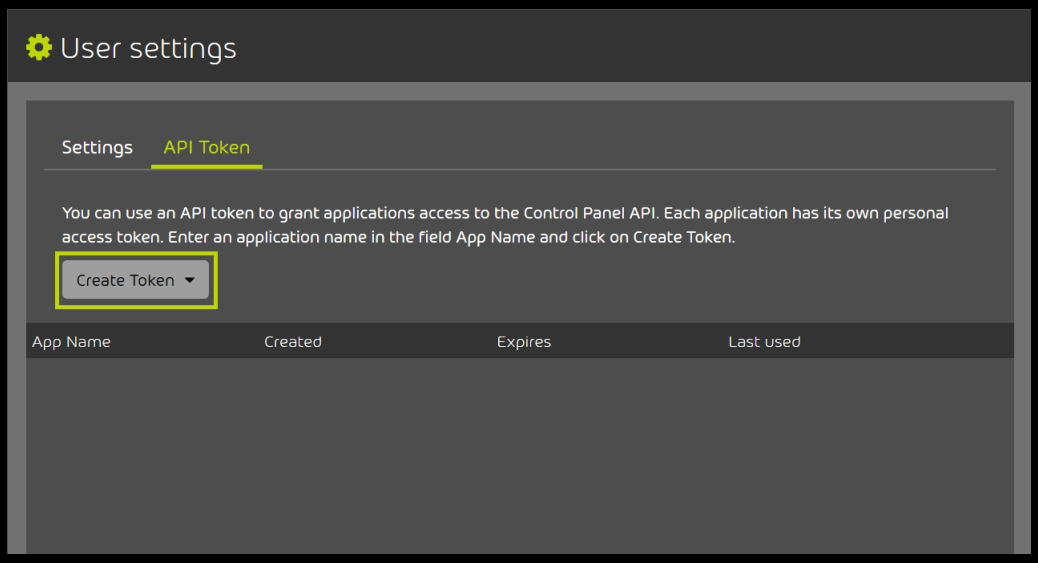


Figure 10: Create token

4. In the App Name field, enter a name for the application that uses the token.

   The actions performed are recorded in Auditing under the app name entered.

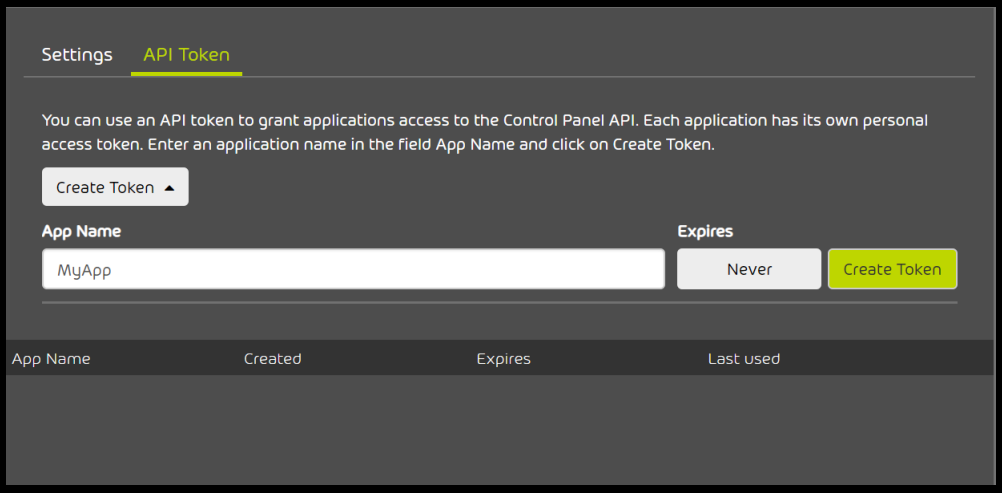


Figure 11: Enter app name

5. Optional: Enter app name Under Expires you can select an expiration date for the token. **Never** is selected as the default value.
6. Click on **Create Token**.

The API token has been created.

Important:

Be sure to save the token directly. It will not be displayed again for security reasons.

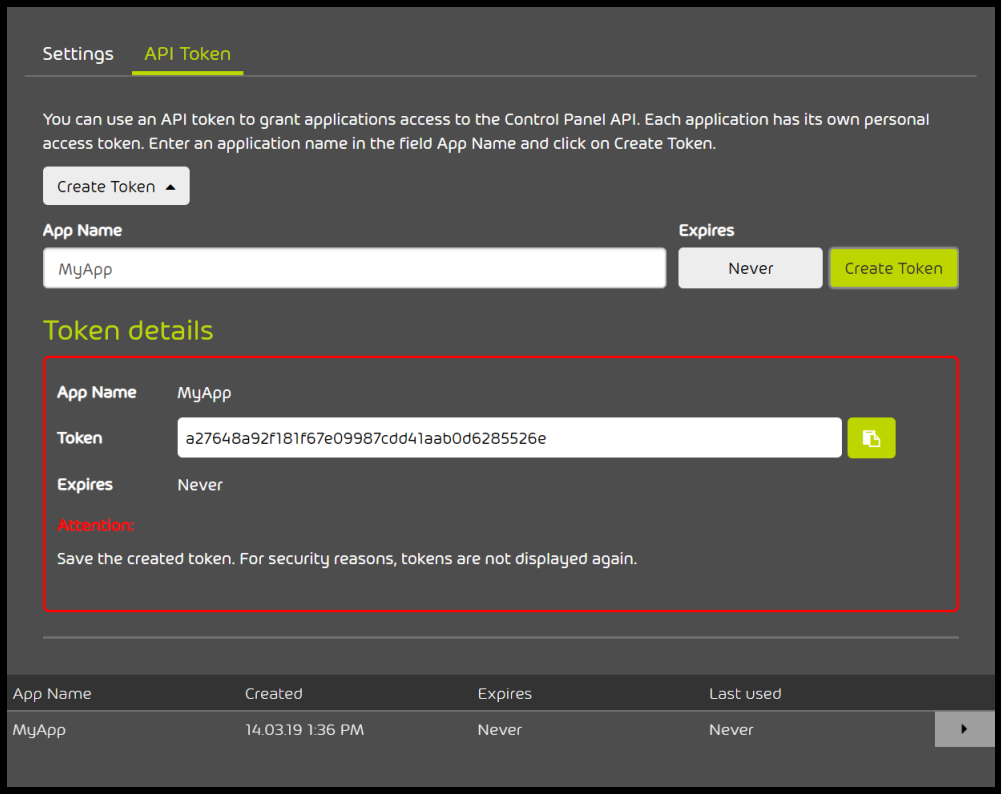


Figure 12: Token created

Creating an Out of Office Note

You have the option to add a personal out of office note to your existing email account.

When you activate the personal out of office note, all incoming email senders automatically receive feedback on your absence. The out of office note can be written individually and activated or deactivated at any time.

1. Click on ⚙ in the upper right corner of the window to open the user settings.
2. Select the tab **Out of Office Note** .
3. Write an individual text about your absence.
4. Click on **Save** to save the out of office note.
   ➔ Your Out of Office Note is saved.
5. Click the **Activate** check box to activate or deactivate the out of office note.

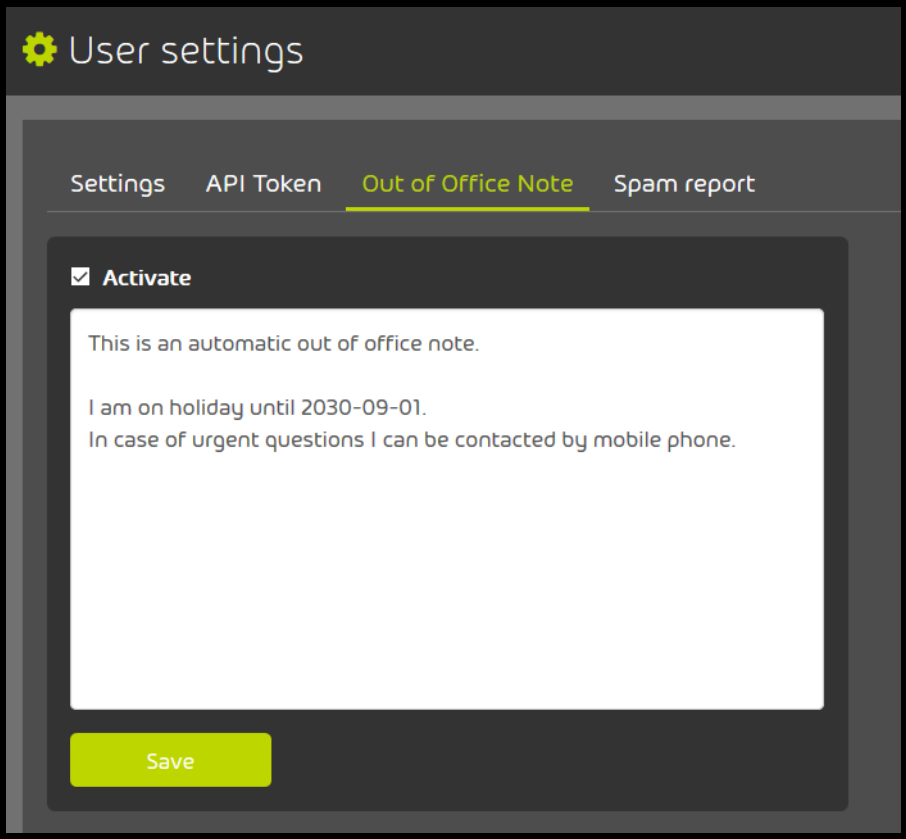


Figure 13: Create an out of office note

Your out of office note has been created.

Configuring the Spam Report

If your administrator has allowed it, you can activate or deactivate the infomail filter, deactivate the Spam Report as well as adjust the delivery times of the Spam Report as a user.

1. Open the user settings .
2. Select **Filter & Reports**.

   The Spam Report settings open. The settings of the administrator are predefined.
3. **Notice:**

   You can only adjust the settings if your administrator has allowed it.

   Activate or deactivate the infomail filter.

- To classify advertising emails as infomail, activate the switch **Activate infomail filter**.
- To stop classifying advertising emails as infomail, deactivate the switch **Activate infomail filter**.

Figure 14: Activate infomail filter

If the infomail filter is activated, the emails classified as infomail are either stored in quarantine and listed in the Spam Report or they are tagged and delivered directly. The administrator decides how the emails are handled.

4. To configure the Spam Report for your mailbox, activate the switch **Set your own delivery times**.

Figure 15: Set your own delivery times

You can deactivate the Spam Report for your mailbox or change the delivery times of the Spam Report.

5. If you would like to deactivate the Spam Report for your mailbox, activate the button **Deactivate**.

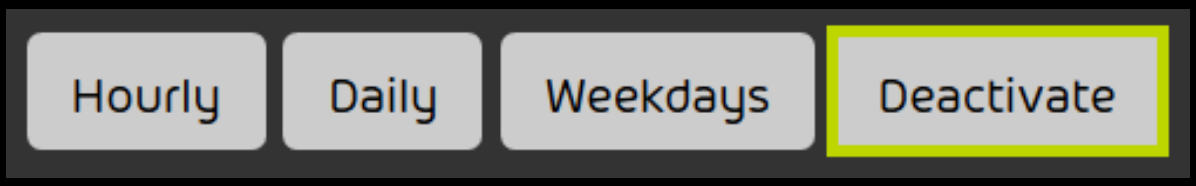


Figure 16: Deactivate the Spam Report

All delivery days and delivery times are deactivated for your mailbox. You will not receive any spam reports. No further adjustments are required.

6. If the Spam Report remains activated for your mailbox, select the days on which the spam reports shall be delivered. Select at least one day.

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

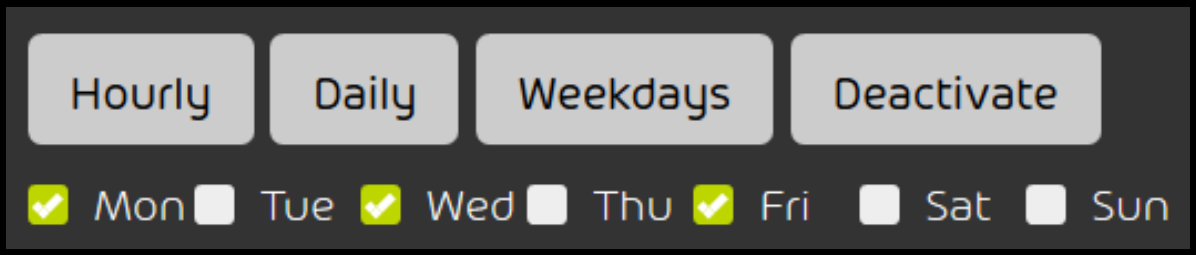


Figure 17: Select days

7. Select the times at which the spam reports shall be delivered. Select at least one time.
   - To deliver the spam reports every hour, activate the button **Hourly**.
   - Activate the checkboxes of the desired times.

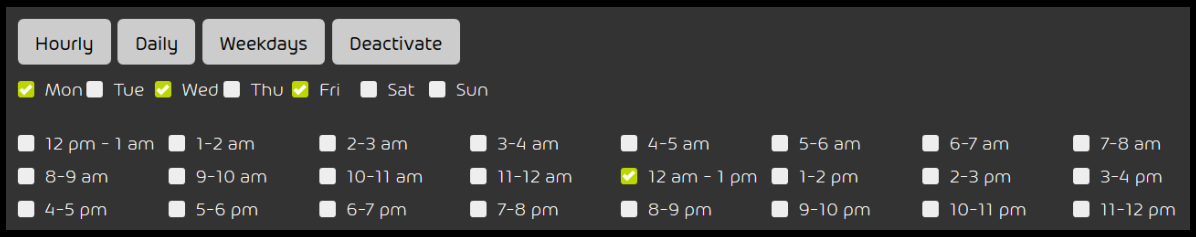


Figure 18: Select times

You have configured the Spam Report for your mailbox.

Rights Management in the Control Panel

In the Control Panel, there are various authorization profiles referred to as roles. The corresponding rights are assigned to different scopes, which the authorized users can then select in the scope selection.

Roles

Standard roles with different rights are defined in the Control Panel.

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.

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
Email Live Tracking	x	x	x	
Service Dashboard		x		
365 Total Protection		x	x	
Reporting & Compliance	x	x	x	x
Web Filter		x		
Customer Settings		x		

Module	User	Administrator	Service Desk	Reporting
Black & White Lists	x	x	x	
Security Settings		x		
Whitelabeling		x		
User Settings	x			

Application Scopes

In the Control Panel, there are three types of scopes which can be selected by users with sufficient rights. These scopes are organized hierarchically:

1. Partner: Is the top-level scope. It can contain customers and additional partners.
2. Customer: This scope corresponds to a domain and is below a partner. It contains all mailboxes that belong to a domain.
3. User: This scope corresponds to a mailbox and is below a customer.

Selection of Scopes

If you have been assigned a role other than the user role, the Control Panel provides an easy way to change the scope of your role.

You can find the **Scope selection** in the upper right corner:

Figure 19: Scope selection

The scope selection contains all scopes of the roles assigned to you. You have two options for selecting the scope. The first option is to select the partner, customer, or user directly from the drop-down menu:

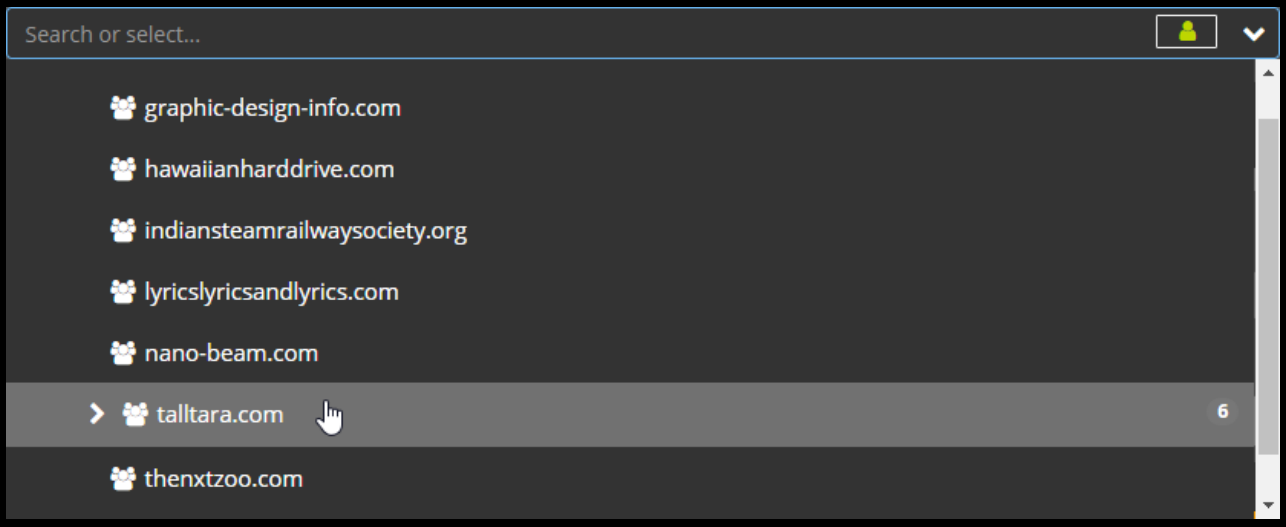


Figure 20: Select the scope

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

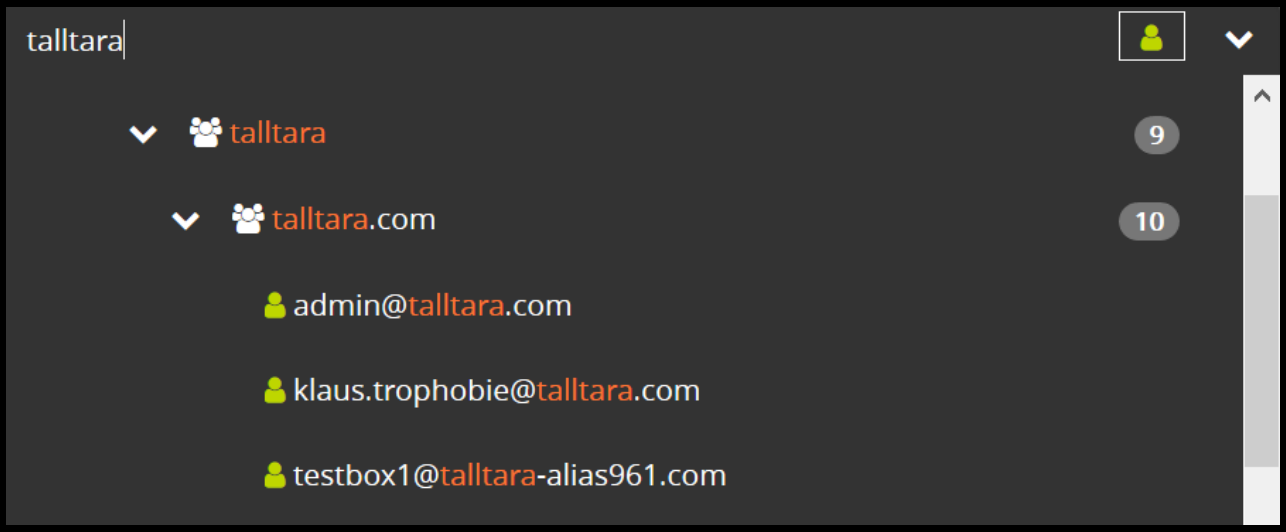


Figure 21: Search in the scope selection

You do not need to spell out the name of the scope you are looking for: It is also enough if you 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. To search for users as well, enable the user search.

Figure 22: Enable the user search

Notice:

As soon as you insert the @ character in the scope search, the search for users is automatically enabled.

To limit the search for partners and customers, deactivate the search for users.

Figure 23: Disable the user search

Email Live Tracking

In the Email Live Tracking, you can examine your email traffic.

Notice:

You can only see the emails, which correspond to your level of authorization.

- Users will only see their own emails including the emails of their alias addresses.
- Domain administrators can see all emails of the domain they administrate, including the alias domains.
- Partners can see all emails of their clients' domains.

All users including the administrators will view their own personal emails after logging in. To administrate emails, you must change the scope.

The following sections start with an overview of the Email Live Tracking. The functionalities are explained individually afterwards.

Overview

The Email Live Tracking is divided into three sections:

Filter Section

You can filter the emails shown in the email display. The different functions are described in Filtering Emails. The filter section inherits the selection and processing actions for emails.

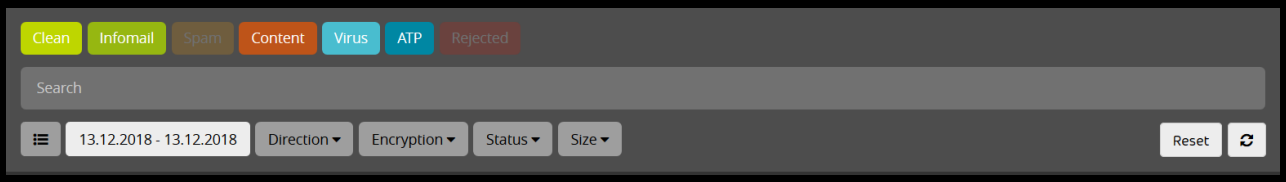


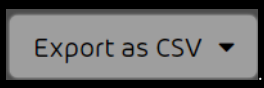
Figure 24: Filter selection

Email Display

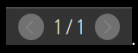
The email display is the main component of the window and shows all the emails following your search and filter criteria.

Figure 25: Email Display

You can customize the email display individually by customizing email fields (see Customizing Email Fields on page 31).

All emails that match your filter definition can be exported using the 

. You can select the fields to be exported.

Extensive email lists can be searched with the scroll function 

. The scroll function is located in the center of the lower display area. By selecting the arrow at the bottom right, the statistics can be hidden and displayed.

Email Category Statistics

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

Notice:

The applied filters are reflected in the statistics.

Figure 26: Category Statistics

Customizing the Email Display

You can customize the email display individually by

- Selecting and deselecting email fields.
- Changing the positions of email fields.
- Resizing the fields.

Customizing Email Fields

1. Click on the button on the right.

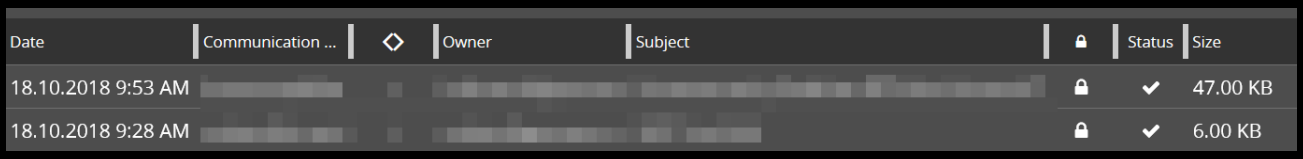


Figure 27: Customizing button

2. Select the desired field from the pop-up window.

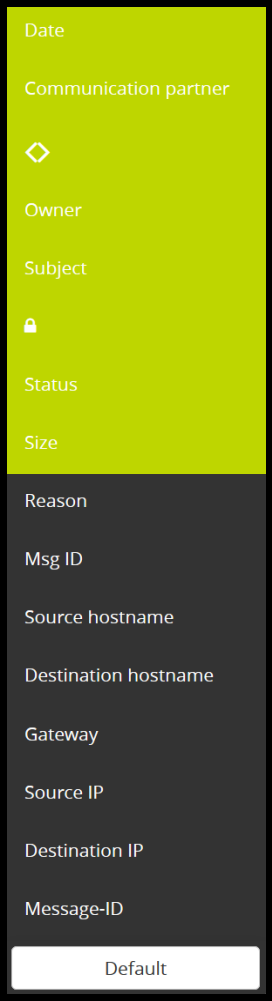


Figure 28: Customizing fields

Email fields have been customized.

Resizing Fields

1. Place the mouse between two fields.

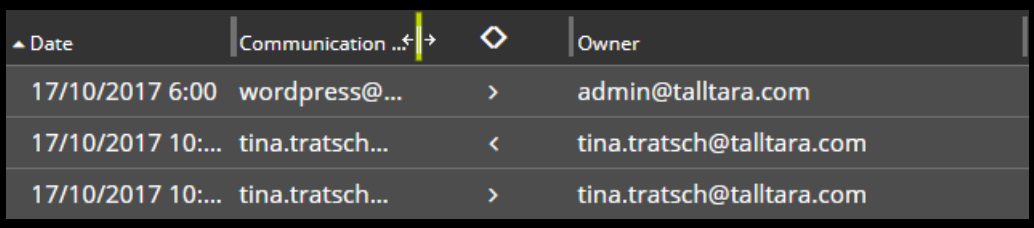


Figure 29: Resizing

A green line appears.

2. Drag the line and resize the field as desired.

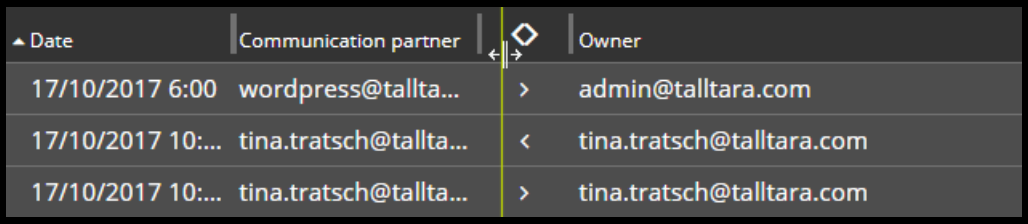


Figure 30: Resizing

Fields have been resized.

Changing the Position of Email Fields

1. Drag the field you want to reposition.

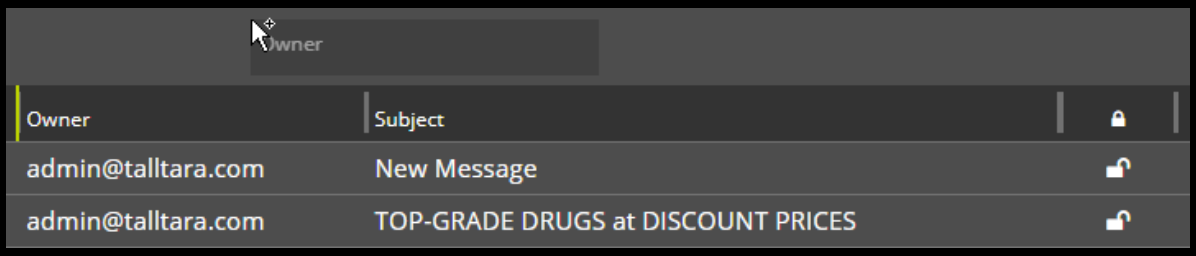


Figure 31: Changing the position of fields 1

2. Drop it in the position you desire.

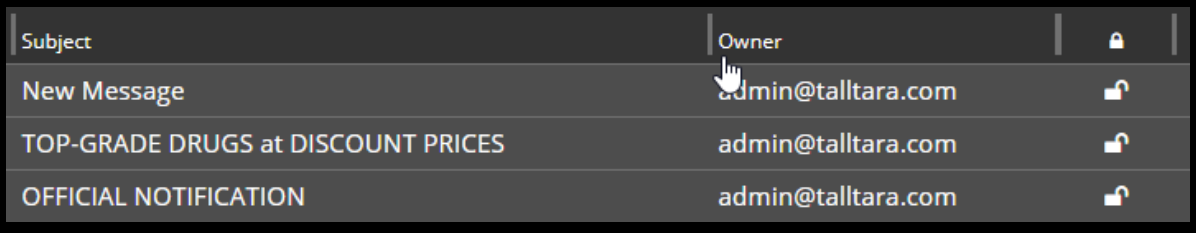


Figure 32: Changing the position of fields 2

Position of email fields has been changed.

Filtering Emails

The Email search in the Email Live Tracking module provides various filter functions. You can use them individual or in combination on your emails.

Filtering Emails by Category

Select or deselect the category in the filter section.

Notice:

To only display emails of a specific category, double-click on the desired category and all other categories will be disabled.

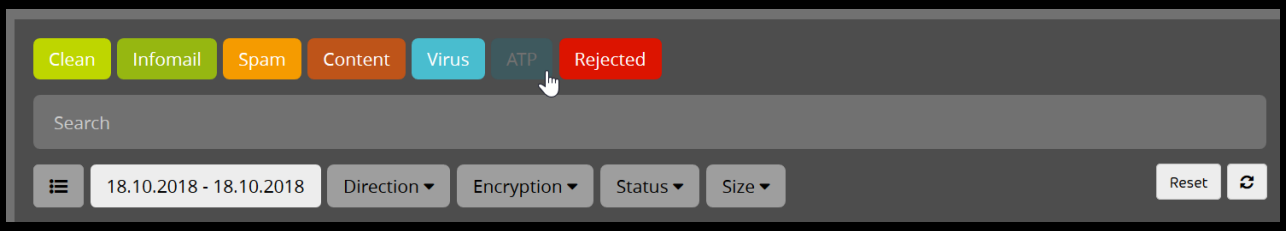


Figure 33: E-Mail-Kategorien de-/aktivieren

Email fields have been changed by their categories.

Search Bar

You can filter your results entering terms in the search bar. All email fields are searched unless you select a field suggested to search for.

Searching Emails

Enter a term in the search bar.

Important:

You must enter at least three characters to use the search.

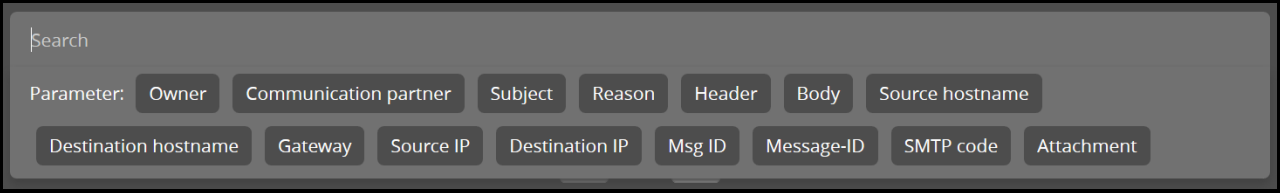


Figure 34: Search bar

The results in the email display are filtered while typing.

Searching Only in Certain Fields

1. Select a field from the suggestions.
2. Enter a term in the field to be searched for.

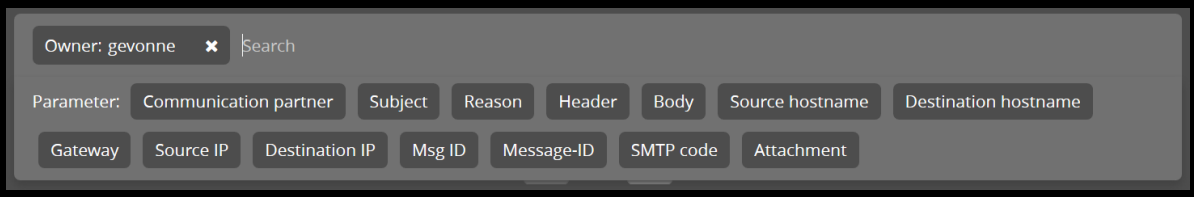


Figure 35: Limit the search to certain fields

You are searching only in selected fields.

Email Field Filters

Filter your results with the following email field filters:

Field	Filter Description
Date	You can select a time interval from the dropdown menu or define a custom range. The current day ("Today") is the default setting.
Direction	Filter for incoming or outgoing emails. The default is both.
Encryption	Select the encryption type you want to filter for, multiselection is possible. The default includes all encryption types and no encryption.
Status	Filter for delivered, deferred or rejected emails.

Field	Filter Description
Size	Filter for emails with a specific size, selected from the dropdown menu.

Filtering Results from the Email Display

You can directly select a value of an email from the email display to filter for.

Double-click on the desired field value (e.g. Communication-Partner) of an email.

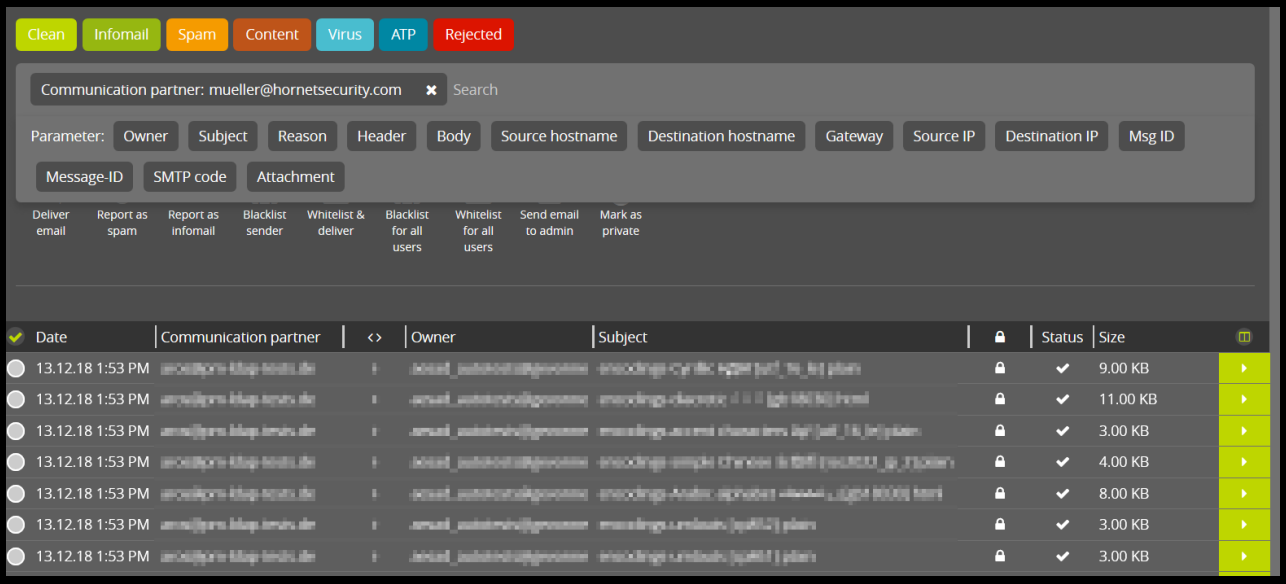


Figure 36: Filter for information of certain fields

Results are filtered from Email Display.

Resetting All Filters

Click on Reset Filter/Search.

All filters have been reset.

Advanced Search

In the Email Live Tracking, you can search the individual email fields combined or use the full-text search to search in all fields at once. Defining queries, the search is completing and you can search for word beginnings. It is not intended to search within words.

For each individual field, there are delimiters to separate words.

The following table shows examples for valid and invalid queries as well as the delimiters for the individual fields.

Table 2: 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	";" and last "."	text.txt; image.jpg	text; txt; image.jpg	xt; mage; pg
Text	special characters	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

Email Details

You can view the details of a single email and perform the following actions:

- Report the email as spam.
- Report the email as infomail.
- Deliver the email.

The email details contain meta information, that are described in Email Fields, as well as the email header and the SMTP dialog for the email.

Opening the Email Details

1. Click on the arrow symbol.

Notice:

The color indicates the category of the email.

2. Click on the action that you would like to perform on the email.

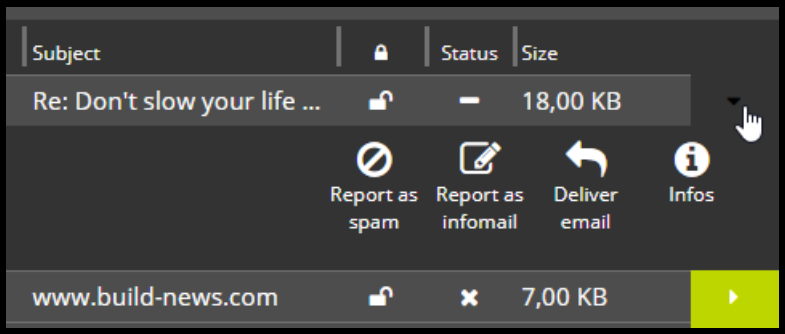


Figure 37: Open the details

Notice:

To blacklist or whitelist the email sender, use the Selection.

Email details are displayed.

Initiating an ATP Scan Manually

Analyze emails with executable attachments (e. g., .Exe files) manually with the ATP Scan.

With the ATP Scan, you can perform an analysis on emails with executable attachments.

Notice:

The ATP scan is only available for emails with executable attachments (e.g. .exe file). Furthermore, clean emails that have already been delivered can only be scanned when the products Archiving or the Hornetsecurity Continuity Service are active.

Attention:

If you have not booked Advanced Threat Protection, you can perform two ATP scans per month. You can only perform further ATP scans, if you have booked ATP.

1. Navigate to **Email Live Tracking** in the Control Panel.
2. Click on the arrow symbol right to the desired email.

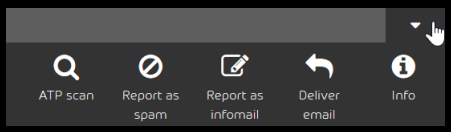


Figure 38: ATP scan in the Email Live Tracking module

The detail view opens.

3. Click on **ATP**, to start the scan.

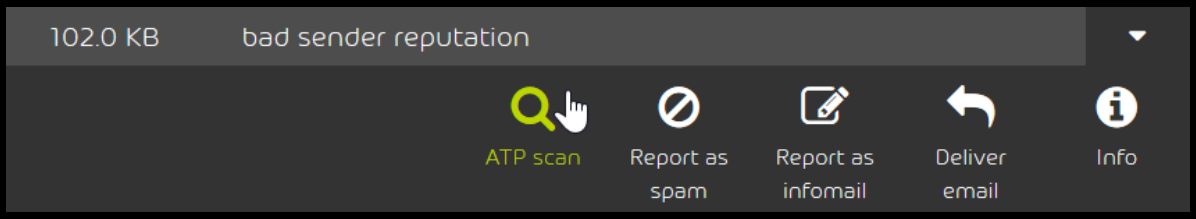


Figure 39: Initiating an ATP Scan Manually

You have started the ATP scan for the email.

Once the ATP scan is complete, you can view the ATP report in the detail view of the email under **Info**.

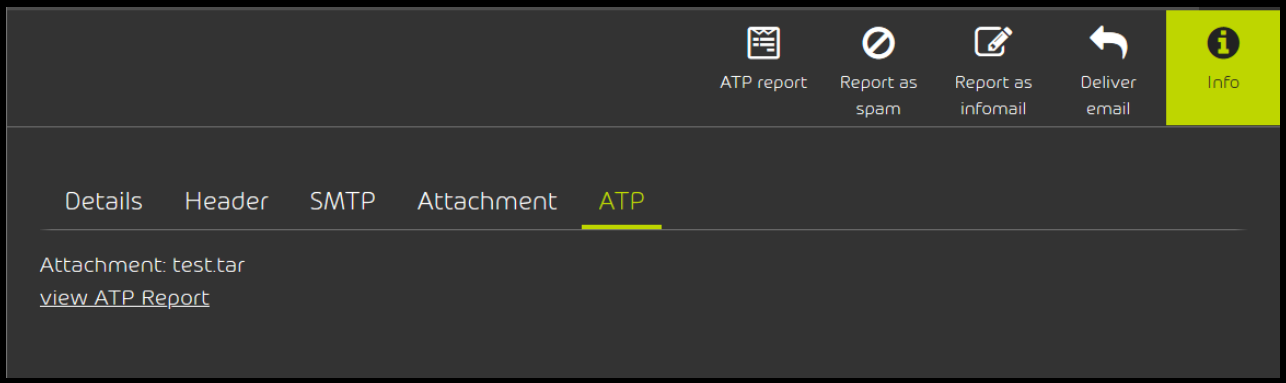


Figure 40: Open ATP report

ATP Report

The ATP report is a detailed report on the files analyzed with the ATP Scan.

The ATP report is a detailed report which is created as soon as an email has been analyzed with the ATP Scan (see ATP scan on page 263). The ATP report provides information about the analyzed email.

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.

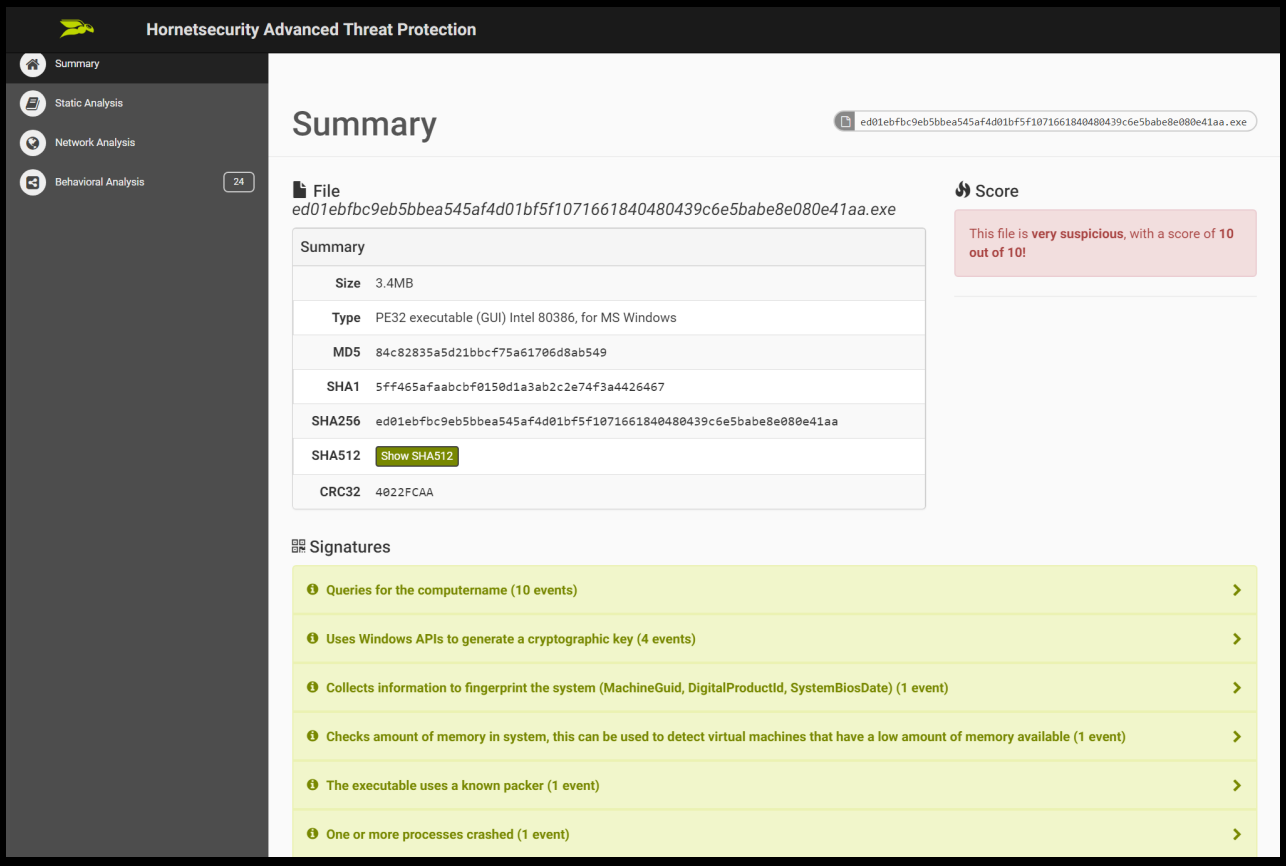


Figure 41: ATP Report Overview

Static Analysis

The static analysis is divided into three subcategories:

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

Network Analysis

In the network analysis, all network traffic is analyzed and listed according to protocols (e.g. HTTP, TCP, UDP).

Behavioral Analysis

The behavior analysis analyzes the behavior of the file at runtime.

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.
- If you select a process from the Process Tree, the executed API queries are displayed here in chronological order.

Extended Email Information

You can find detailed information about the selected email under Infos. The detailed information of a specific email is separated in three sections.

Notice:

You can find a description of the shown email fields under Email fields.

Details

Here, you can find further information concerning the selected email.The following email fields are shown:

- Owner
- Communication Partner
- Subject
- Message-ID
- Category filter
- Reason
- Connect
- SMTP-Code
- Encryption
- Date

Header

The header tab provides the header information of the selected email. The header is not shown for rejected emails.

SMTP

In the SMTP tab, the whole SMTP-Dialog is shown. The last row is also shown in the details under SMTP-Code

Email Fields

The following table describes the email fields shown in the email display and the email details.

Feld	Beschreibung
Date	The date and time when the email was sent. Depending on the selected time zone.
Communication partner	The owner's communication partner. Sender or receiver of emails to/from the owner.
Direction <>	Incoming or outgoing message from the owner's point of view.
Owner	The email was sent or received by the owner.
Subject	The subject of the email.
Encryption	The lock only shows, whether the email is encrypted or not. You can see the encryption type in the email details.
Status	Indicates, whether the email is delivered, deferred or rejected.
Size	Size of the email.
Reason	The reason, why the email has been classified as spam, virus etc.
msg ID	Internal id of the email.
source Hostname	Outgoing server hostname.
destination Hostname	Incoming server hostname.
Gateway	The gateway.
source IP	Sender's IP address.
destination IP	Receiver's IP address.
message ID	The id of the email.
Connect	Depending on the direction of the email, the hostname of the incoming or outgoing mail server is shown.

Feld	Beschreibung
SMTP-Code	Shows the last row of the SMTP dialog.

Processing Emails

1. Click on the button in the filter section. A tool bar opens.

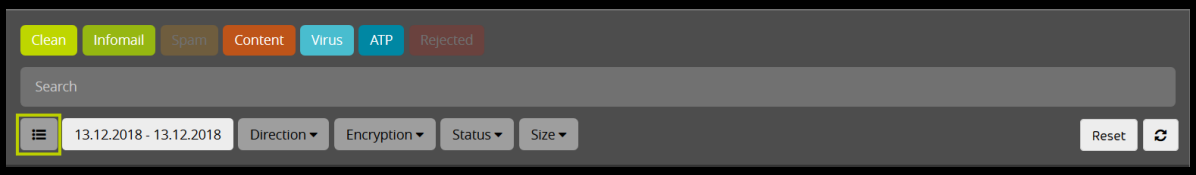


Figure 42: Selection button

2. Click on the emails in the result display to select them.

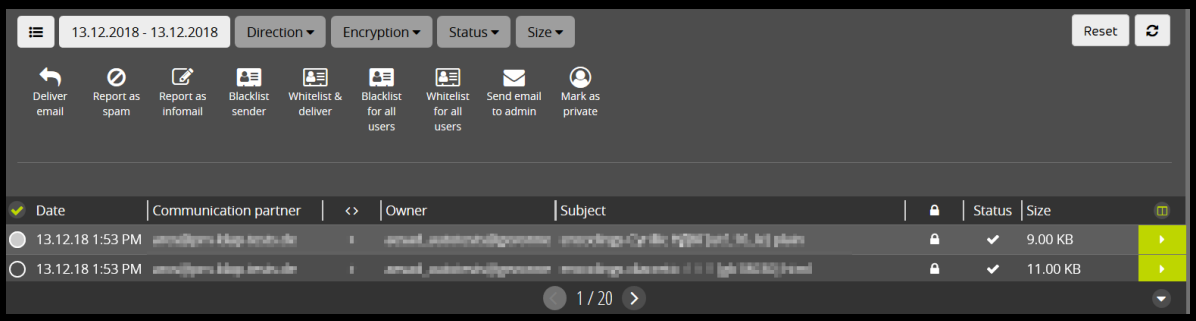
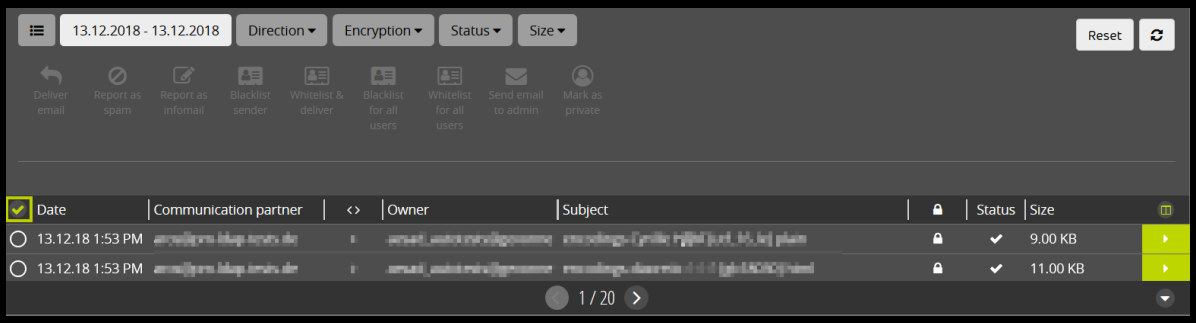


Figure 43: Selecting emails

> **Notice:**
>
> You can select and process multiple emails at once.

Furthermore, it is possible to select all displayed emails at once:



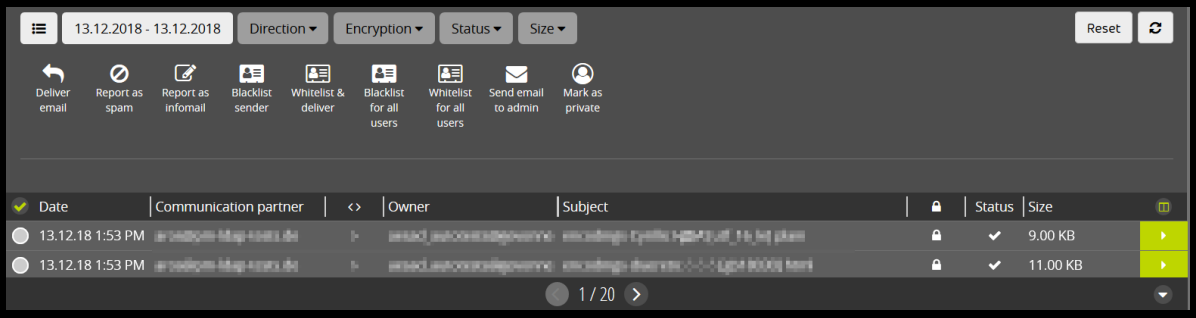


Figure 44: Select all displayed emails

3. Click on the action you want to perform for the selected emails.

Email Actions

For emails in Email Live Tracking, various actions, such as blacklisting, can be performed.

The actions are described in the following table.

Action	Description
Deliver email	The selected emails are delivered, triggering a process of re-evaluation of the classification on our part. This option can always be applied to emails classified as **Clean** and **Infomail** if you have booked Archiving. For emails classified as **Spam**, **Content**, **Virus**, and **ATP**, the option is independent from Archiving. However, the option is only available for emails with these classifications if the administrator has enabled the delivery. 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 of Hornetsecurity, partners, customers and basic users are tagged with the words **support**, **reseller**, **admin** and **user**, respectively.
Report as spam	The selected emails are classified as spam, and the support and quality management system

Action	Description
	is informed. This is the preferred method of dealing with spam emails.
Report as infomail	The selected emails are classified as infomail. The options for dealing with infomail are individually adjustable.
Blacklist sender	The senders of the selected emails are added to the user's black list. Any future emails from these senders will be automatically classified as spam.
Whitelist & deliver	The senders of the selected emails are added to the user's white list and the emails are delivered. All other emails from the senders will be automatically delivered.
Blacklist for all users	The senders of the selected emails are added to the black list for all users of the domain and incoming emails are classified as spam.
Whitelist for all users	The senders of the selected emails are added to the white 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 provided under **Service Dashboard**#→ **Data**.
Mark as private	The selected emails are treated as private emails. Thus, the access to them is blocked and can only be restored by the support. With an audit access, emails marked as private cannot be read. However, emails marked as private are exported with the Aeternum Export Manager.

Notice:

The blacklist and whitelist entries are processed in the following order:

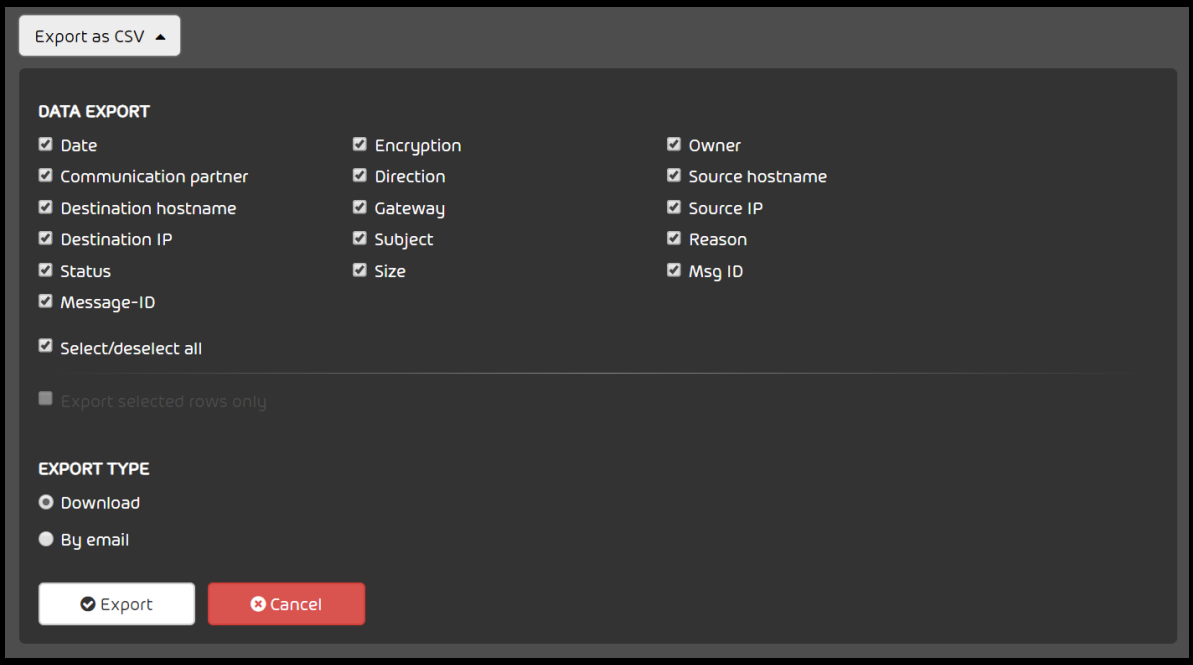
- Administrator black list
- Administrator white list
- User black list
- User white list

An administrator adds the account elpmaxe@elpmaxe.moc to the global black list. A user adds the same account to his white list. All emails from the account will be delivered to the user, but not to any users who have not whitelisted the account.

Exporting a List as CSV

1. Click on the button Export as CSV.

   A submenu with advanced settings opens.



2. Select the table columns that you want to export to your list.
3. Select the desired export type: **Download** or **by Email**.

4. Click on **Export**, to export the email data of the selected table columns as CSV.

You have exported the email data as CSV.

Service Dashboard

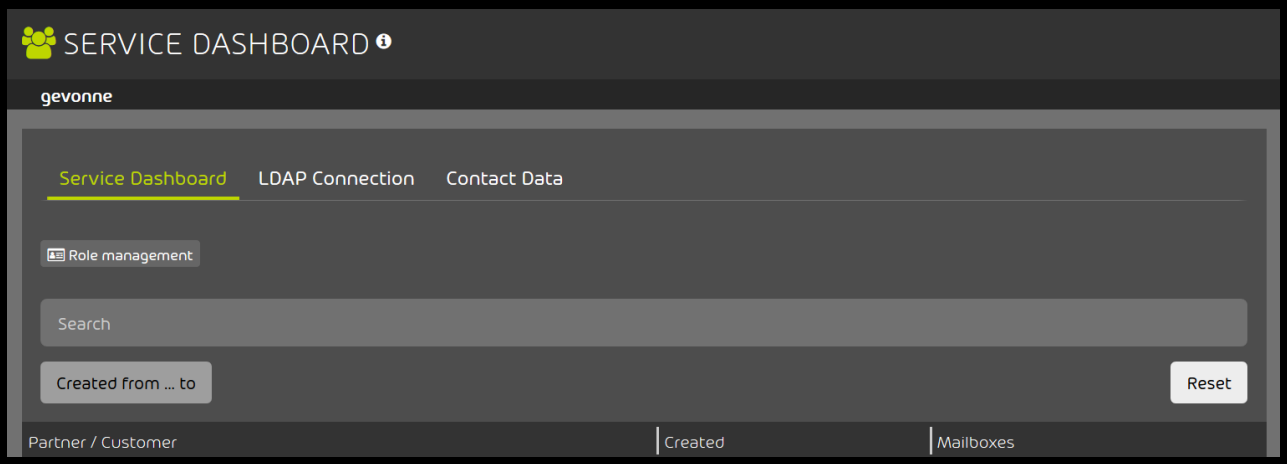
About the Service Dashboard

The Service Dashboard offers you the possibility to have an overview of the administrative activities.

The Service Dashboard displays an overview of all created roles of individual user domains as well as assignments of partners and customers in the form of containers. The arrangement of the containers, and thus the hierarchical dependency of created objects, is always read from left (parent object) to right (child object). Depending on the assigned rights, the stored objects can be combined with other objects, deleted from parent objects or assigned to other objects. This allows you, for instance, to create new customers under existing partners or to remove customers from partners.

The role administration allows you to create new role assignments and manage existing role assignments (see Role Management on page 53).

In the Service Dashboard, you can also configure the LDAP connection in the Control Panel (see #unique_46) and enter the contact data of your company (see Contact Data on page 65).



Administration of Partners and Customers

In the Service Dashboard, you can create new partners and customers as well as delete existing partners and customers.

You can see all of your subordinate partners and customers, and the date on which the partner or customer has been created. The date under **Created at** refers to the partner or customer with

a gray background. The **Mailboxes** column shows the number of mailboxes created under the customer. You have the possibility to delete subordinate partners or customers and to create new ones.

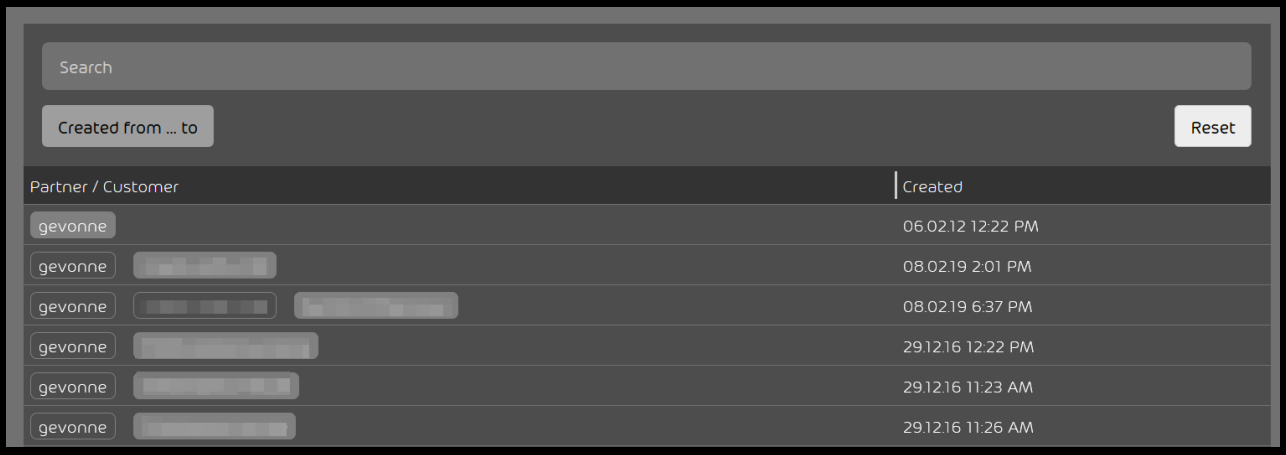


Figure 45: Entries of a partner

In the following chapters, the configuration of the Service Dashboard is explained:

- Filtering Entries on page 50
- Creating Customers or Sub-Partners on page 51
- Deleting a Customer on page 52

Filtering Entries

Filter the entries by date and keywords.

Select one of the following options to filter your entries:

- In order to filter your entries by keywords, enter the name of the partner or customer you are looking for in the field **Search**. Type in at least 3 consecutive letters to trigger the automatic search and suggestion function.

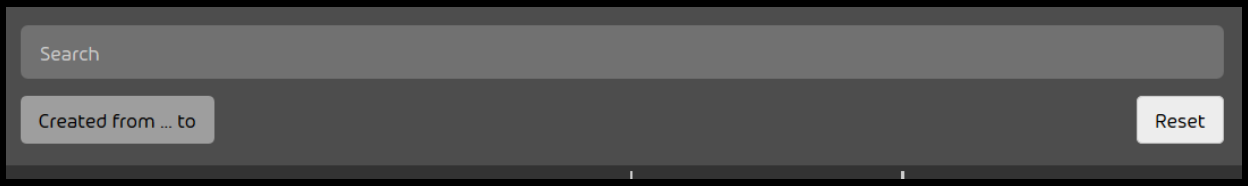


Figure 46: Enter keyword

- In order to filter your entries by date, click on the button **Created from ... to** and select a period.

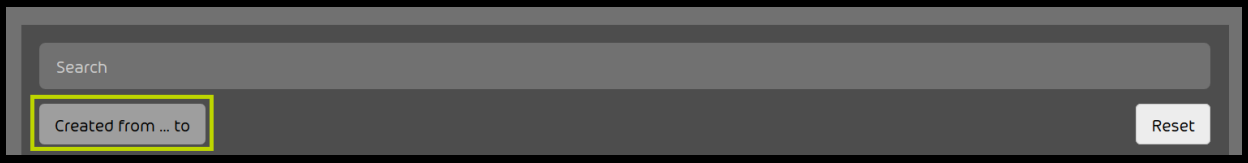


Figure 47: Select date

Your entries have been filtered.

Creating Customers or Sub-Partners

Create new partners or customers or assign an existing customer to a partner.

1. Log in to the Control Panel with your administrative credentials.
2. Select a partner from the scope selection.
3. Navigate to **Service Dashboard**.
4. Select the tab **Service Dashboard**.
5. From the list, select the partner you would like to create a customer or sub-partner for and click on the arrow on the right side of the partner.

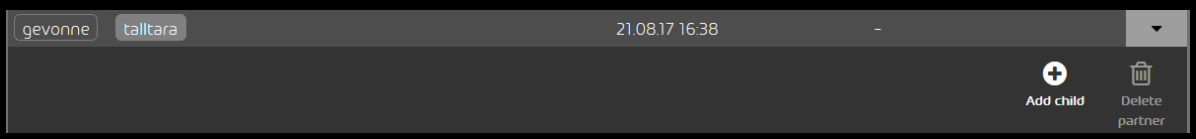


Figure 48: Select partner

An menu opens.

6. Click on **Add child**.
7. **Notice:**

   Under sub-partners, no other partners can be added, only customers.

   Under **Type**, select whether you want to add a partner or customer.
8. Enter the data of the customer or partner:
   - Enter a valid top-level domain for a customer under **Display name (domain) in the Control Panel**.
   - For a partner, enter the name of the partner under **Name in the Control Panel**.

   a) Enter the company name under **Company**.

b) Under **E-mail address**, enter a valid email address that exists in the Control Panel.

> **Notice:**
>
> Start the domain name with a lower case letter.

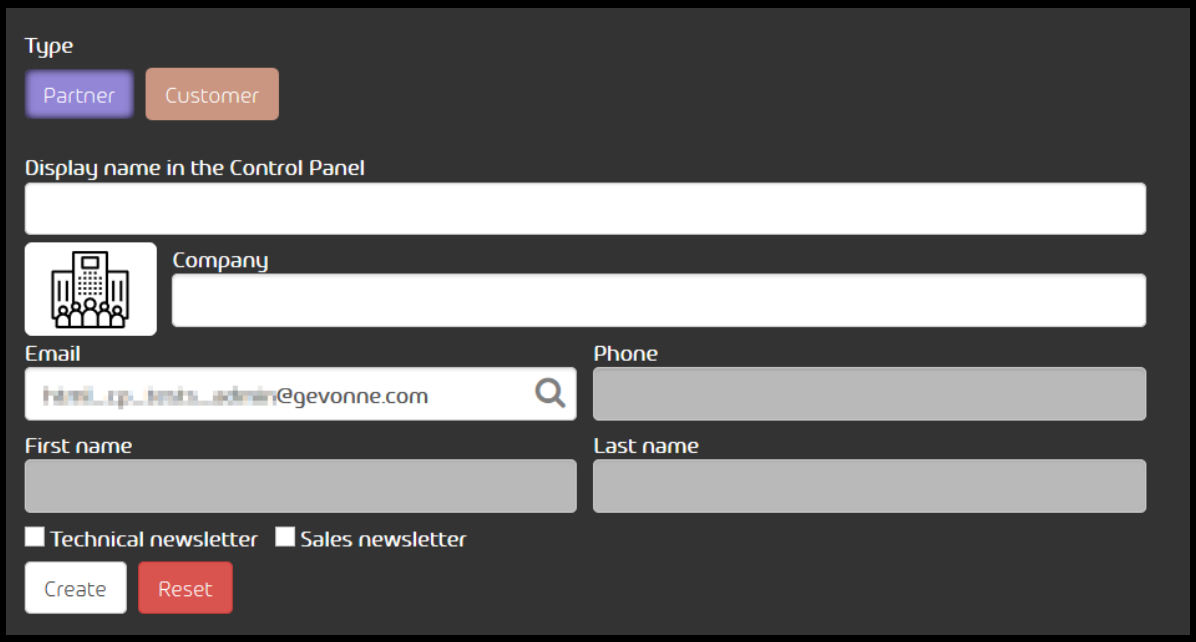
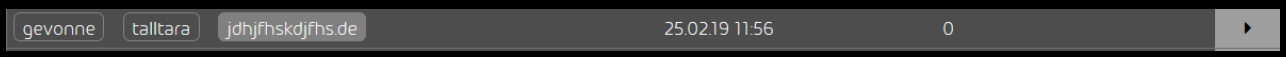


Figure 49: Enter customer data

9. Click on **Create**.

The customer or sub-partner has been created under the selected partner.



Deleting a Customer

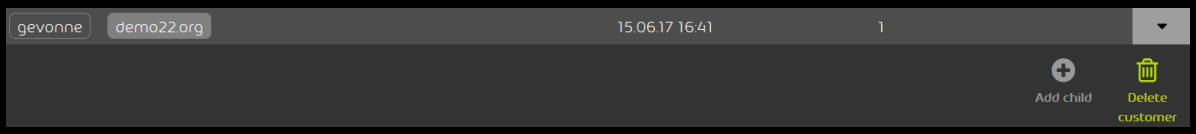
As a partner, you can delete your subordinate customers.

1. Log in to the Control Panel with your administrative credentials.
2. Select your partner role from the scope selection.
3. Select **Service Dashboard**.
4. Click on the drop-down menu next to the customer to be deleted.

5. **CAUTION:**

   All data for this customer will be permanently deleted from the Control Panel!

   Click on **Delete customer** to delete the selected customer.



The customer has been permanently deleted.

Role Management

You can create new roles and manage existing roles using role management.

Under **Role management** the following actions can be performed:

- Assigning a Role on page 53.
- Delete role assignment on page 54.

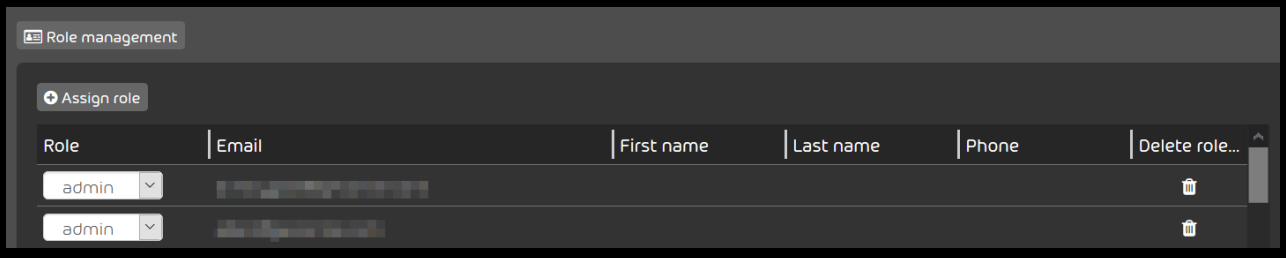


Figure 50: Overview of role management

Assigning a Role

1. Log in to the Control Panel with your administrative credentials.
2. Open the **Service Dashboard**.
3. Click on **Role management#→Assign role**.

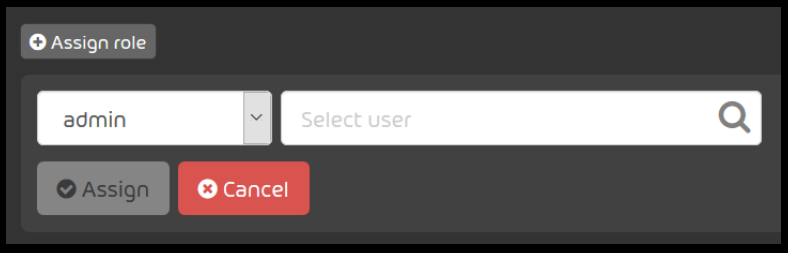


Figure 51: Assigning a Role

4. Under **Select user**, enter the user to whom you would like to assign a new role.
5. In the drop-down menu, select the role which you would like to assign to the user.
6. Click on **Assign**.

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

Delete role assignment

1. Log in to the Control Panel with your administrative credentials.
2. Open the **Service Dashboard**.
3. To delete a role assignment, click on the icon to the right of the row of the role assignment to be deleted.

A warning message appears.

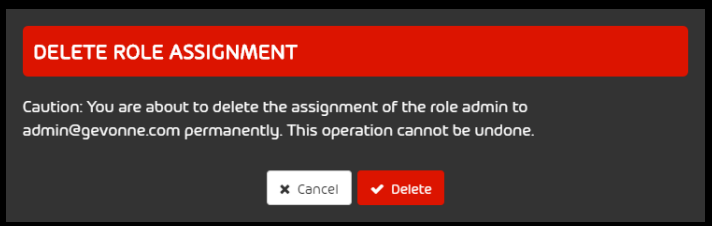


Figure 52: Warning message

4. Confirm the deletion of the role assignment with **Delete**.

The role assignment has been deleted.

Basic Settings

Under **Service Dashboard**, you can adjust the basic settings for the corresponding partner/ customer.

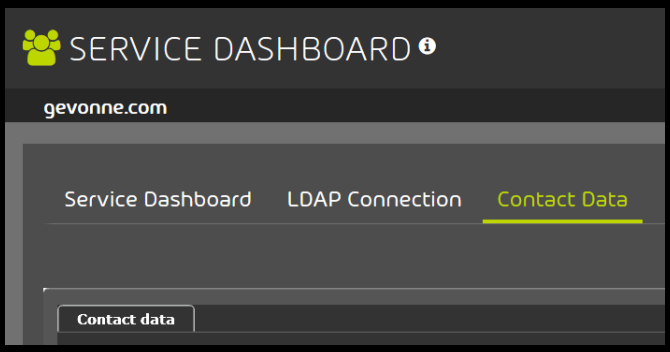


Figure 53: Navigation in the Control Panel

LDAP Connection

Your directory service, e. g. the Microsoft Active Directory, is directly connected with the Hornetsecurity service via LDAP.

With LDAP you can authenticate your login to the Hornetsecurity Control Panel and the web filter through your directory service and configure an additional user and group synchronization for the managed service. Furthermore, you can activate the service Advanced Email Signature and Disclaimer.

Important:

You cannot use LDAP and the Microsoft 365 synchronization of attributes simultaneously. For Microsoft 365 customers, only the attributes from the Azure Active Directory are synchronized (see Synchronized Attributes from the Azure Active Directory on page 97).

Activating the LDAP Connection

Activate the LDAP connection to connect to your directory service.

First, create a new user in your directory service.

Notice:

The user must be authorized to look up email addresses and to compare passwords. In the Microsoft Active Directory Service, this is ensured by assigning the user to the group **RAS and IAS Servers**.

Notice:

You can choose any name for the user. For standardization, the user name **Hornetsecurity** is recommended.

For implementing your directory service in the Control Panel of Hornetsecurity, the following information is required:

- The password of the created user.
- The LDAP base distinguished name under which the user can be found.
- The hostname or the IP address of your directory server.
- The port and the protocol (LDAP or LDAPS) for reaching the server.

In the Control Panel of Hornetsecurity, navigate to **Service Dashboard** and select the primary domain for which you would like to activate the service.

1. Select the tab **LDAP Connection**.
2. Mark **LDAP connection activated**.
3. Enter the user for your directory service in the field **User**.

   Notice:

   If you have created the user **Hornetsecurity**, enter his username.
4. Enter the password for the user in the field **Password**.
5. Enter the hostname or the IP address of your directory server in the field **Server**.
   Example: **myhost.mydomain.tld**
6. Enter the port of your directory server in the field **Port**.

   The default ports for the protocols are:

   - LDAP: Port 389
   - LDAPS: Port 636
   - GC LDAP: Port 3268
   - GC LDAPS: Port 3269

7. Optional: Activate the checkbox **LDAPs** if your connection is established via LDAPS.
8. Enter the desired LDAP base distinguished name in the field **Base-DN**.
   DC=myDomain,DC=tld
9. Click on **Save** at the bottom of the window.

You have configured the connection to your directory server.

In the following example, an LDAP connection is established for the user **hornetsecurity@mydomain.tld** on the directory server **myhost.mydomain.tld** via the LDAP default port **389** with the LDAP base distinguished name **mydomain.tld**.

Figure 54: LDAP configuration

Next, you can:

- Configure the user authentication for the Control Panel via LDAP.
- Configure the user and group synchronization via LDAP.
- Configure the Web Filter login via LDAP.
- Activate Signature and Disclaimer.

Securing the LDAP Connection

It is possible to secure the LDAP connection through different methods.

To protect the transmitted data and the LDAP connection from unauthorized access, you have the following options:

- Encrypt the communication with LDAPS through TLS/SSL.

  Notice:

  If you are using LDAPS, configure the port and activate LDAPS as shown in Activating the LDAP Connection on page 55.

- Restrict the IP address range for connections to Hornetsecurity only.

Limiting the Directory Service to the IP Address Range of Hornetsecurity

Limit the IP address range of your directory service in your firewall to connections to Hornetsecurity only.

Add the following IP address ranges to your firewall:

- First range: 83.246.65.0/24 with subnet mask 255.255.255.0, corresponding to the addresses between 83.246.65.1 and 83.246.65.255
- Second range: 94.100.128.0/20 with subnet mask 255.255.240.0, corresponding to the addresses between 94.100.128.1 and 94.100.143.255
- Third range: 185.140.204.0/22 with subnet mask 255.255.252.0, corresponding to the addresses between 185.140.204.1 and 185.140.207.255
- Fourth range: 173.45.18.0/24 with subnet mask 255.255.255.0, corresponding to the addresses between 173.45.18.1 and 173.45.18.255

Logging in to the Control Panel via LDAP

Configure the Control Panel authentication to use the credentials from your Active Directory.

Notice:

The Control Panel login is only possible through an Microsoft Active Directory (AD).

1. In the advanced settings under **Control Panel login**, activate the checkbox **Control Panel authentication with LDAP credentials**.

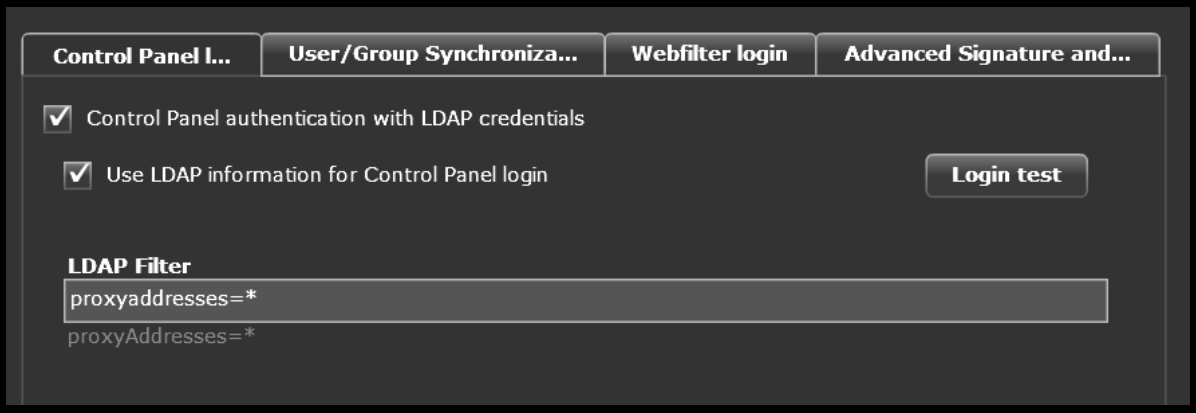


Figure 55: Activate Control Panel login with LDAP credentials

2. **Notice:**

   If you want to use a different LDAP server for the Control Panel login:

   Optional: Deactivate the checkbox **Use LDAP information for Control Panel login**.

   a) Define the logon information in the appearing fields.

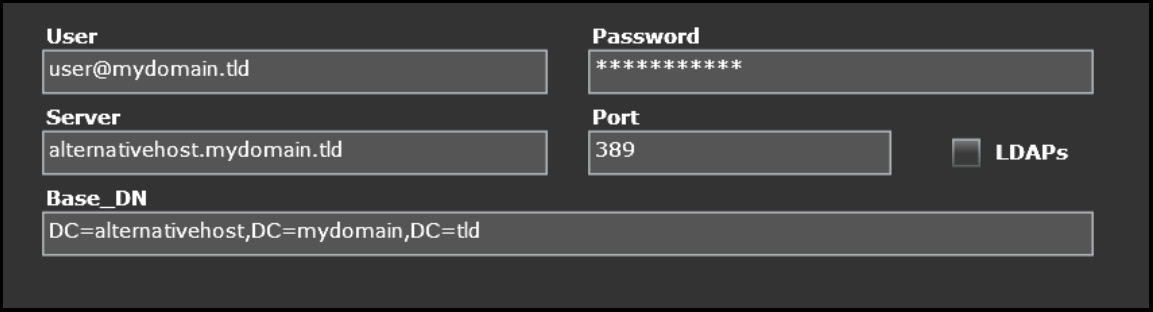


Figure 56: Selecting a different LDAP server

3. Optional: You can filter users in the field **LDAP Filter**.

> **Notice:**
>
> The default filter **proxyAddresses=*** gets all users from an Active Directory.

4. Optional: Click on **Login test**, to test the login for a specific user from your Active Directory.
   a) Enter the email address and the password of an Active Directory user.
   b) Click on **Ok**.

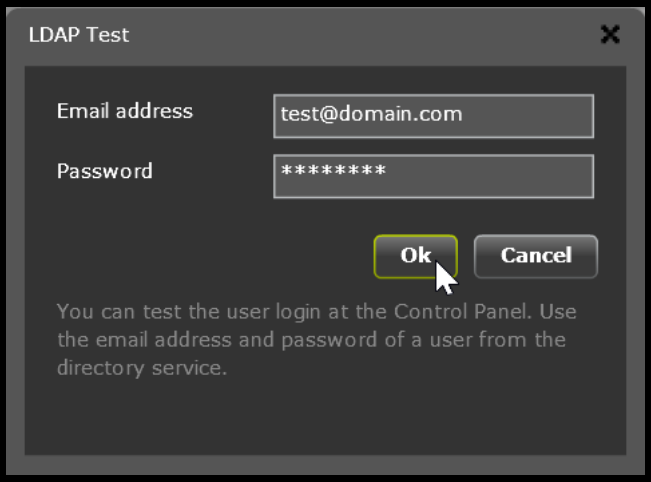


Figure 57: Login-Test

→ The authentication is checked and you will get a notification.

5. Click on **Save** in the lower left corner of the window.

You have configured the Control Panel login through LDAP.

Synchronizing Users with LDAP

Synchronize users from your directory service with LDAP.

With the synchronization of users from your directory service, alias addresses are automatically assigned. The benefit is that only one spam report is sent out for the primary email address including all alias addresses.

Notice:

To import users, you must create your directory service groups inside the Control Panel manually.

To assign users to the correct groups, the groups must have exactly the same group names as in your directory service.

For additional information about adding groups see "Groups".

1. Activate the checkbox **Synchronize user/group into Control Panel**.
2. **Notice:**

   If you want to use a different directory service for the user and group synchronization:

   Deactivate the checkbox **Use LDAP information for User/Group Synchronization**.

   a) Define the logon information in the appearing fields.

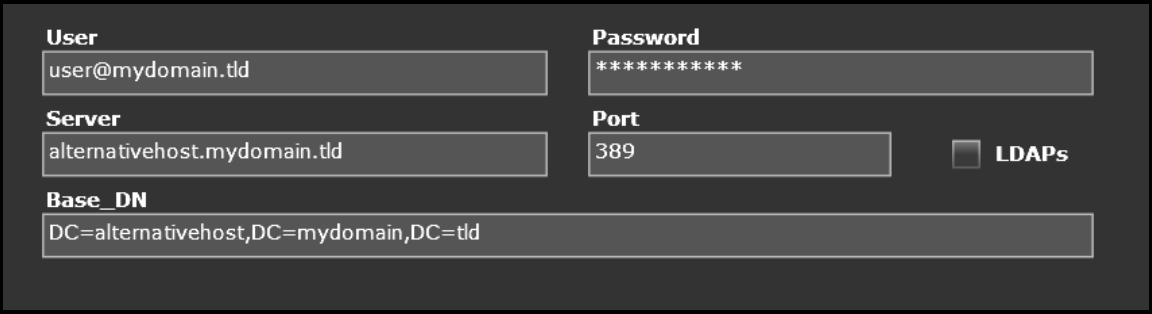


Figure 58: Selecting a different LDAP server

3. Enter the LDAP filter for the user objects and exceptions in the field **LDAP Filter**.

Notice:

The default entry:

(|(sAMAccountType=805306368)(sAMAccountType=268435456)(sAMAccountType=268435457)(objectclass=publicFolder))

selects all users of an Active Directory.

If you want to change the filter, use the following syntax:

(|(xxxxxxxxxx=xxxxxxxxxx)(xxxxxxxxxx=xxxxxxxxxx))

The preceding **|** defines an OR relation between the parameters in the following brackets. Therefore, only one parameter must match. If you want an AND relation between the parameters, you must use a preceding **&**.

In addition, at least one entry must stand in the brackets.

4. Enter the LDAP attributes in the corresponding fields.

Table 3: LDAP fields

Attribute	Description
Email	The attribute where the email addresses are stored in your directory service. In an Active Directory this is the attribute **proxyaddresses=***.
E-Mail aliases	The attribute, where the email alias addresses are stored.
Group	The attribute, where the groups are stored.
sAM Account Name	The attribute where the users' account names are stored.
min. user	Minimum number of users, that have to be captured by the LDAP synchronization for a change.
min. groups	Minimum number of groups, that have to be captured by the LDAP synchronization for a change.

Attribute	Description
E-mail for alerts	Notifications are sent to this email address.
Alert after x minutes without Update	Minutes without synchronization, after that a notification is sent.

5. Click on **Save** in the lower left corner of the window.

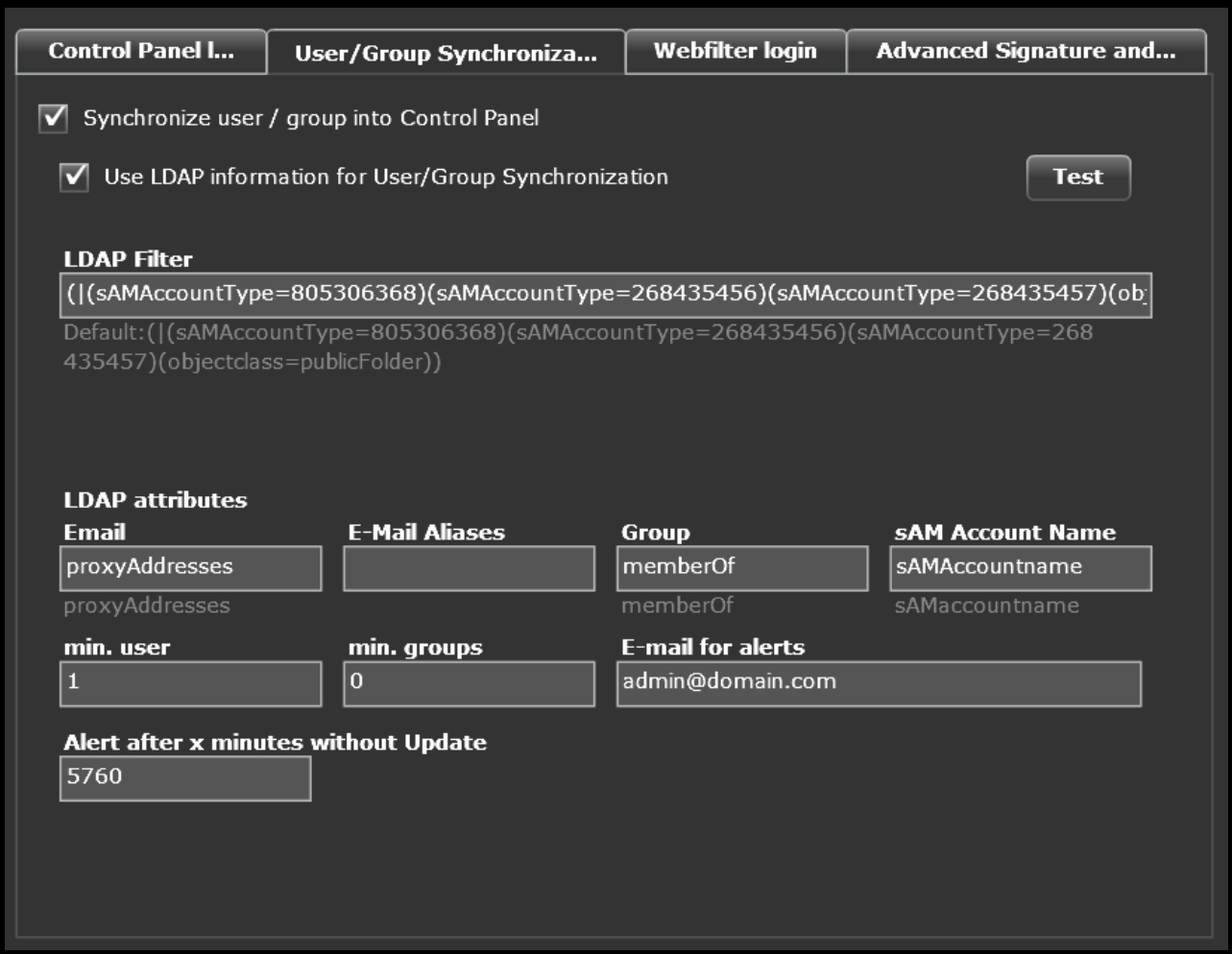


Figure 59: User and Group Synchronization

Logging in to the **Webfilter** via LDAP

Activate the Web Filter login via LDAP.

1. Navigate in the lower window area to the tab **Web Filter login**.
2. Activate the checkbox **Activate Web Filter login**.

3. **Notice:**

   If you want to use a different directory service for the **Web Filter** login:

   Deactivate the checkbox **Use LDAP information for Web Filter login**.

   a) Define the logon information in the appearing fields.

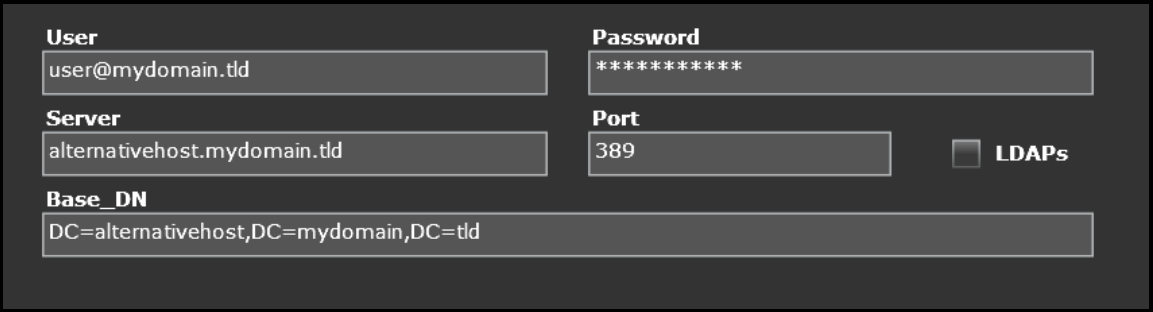


Figure 60: Selecting a different LDAP server

4. Optional: Enter the LDAP filter for the email addresses of the **Web Filter** user.

   Notice:

   The filter for all users in the Microsoft Active Directory: **proxyAddresses=*** is set as default. If your directory service has a different structure, you can change the filter individually.

5. Click on **Save** in the lower left corner of the window.

The **Web Filter** login via your directory service is now set up.

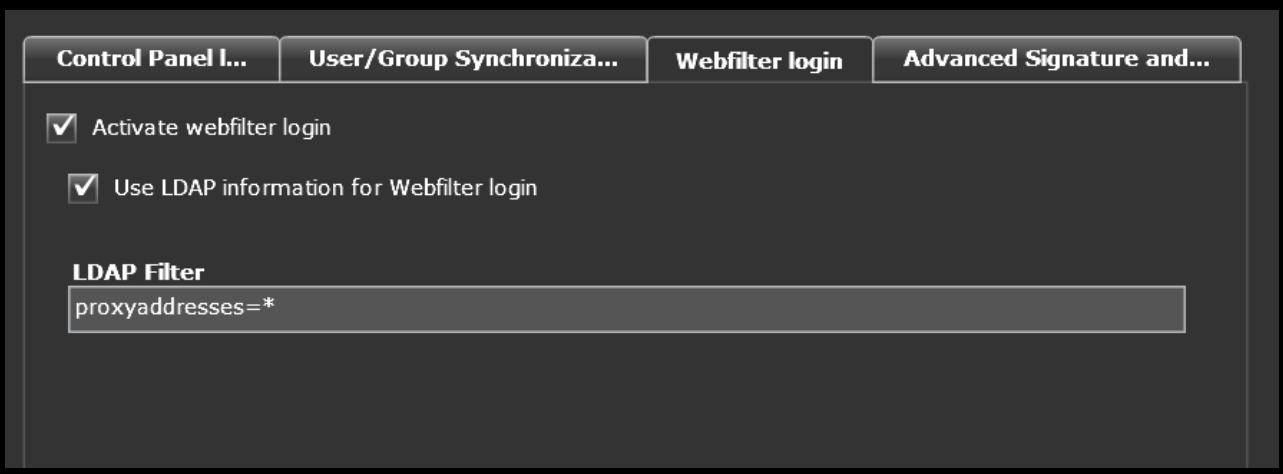


Figure 61: Web Filter login via LDAP

Activating LDAP for Signature & Disclaimer

To use Signature & Disclaimer, activate it in the Control Panel. After the activation, optionally configure a different LDAP server for the synchronization and enter filters for the user synchronization.

Important:

Do not follow the steps in this chapter if you are an Microsoft 365 customer. You cannot use LDAP and the Microsoft 365 synchronization of attributes simultaneously. Follow the steps in the chapter Activating Signature & Disclaimer in the Web Interface on page 317

To use Signature & Disclaimer, you must activate it in the Control Panel.To use Signature & Disclaimer, activate it in the Control Panel. After the activation, optionally configure a different LDAP server for the synchronization and enter filters for the user synchronization.

1. Select **Service Dashboard#→LDAP connection#→Advanced Signature and Disclaimer** in the Control Panel.
2. Activate the checkbox **Activate Signature and Disclaimer**.

   Attention:

   Activating Signature & Disclaimer could be additionally charged depending on your license.

   a) Confirm the notification with **OK**.
3. **Notice:**

   Follow this step if you want to use a different directory service for the user synchronization with Signature and Disclaimer.

   Optional: Deactivate the checkbox **Use LDAP information for Signature and Disclaimer**.

   a) Define the logon information in the appearing fields.

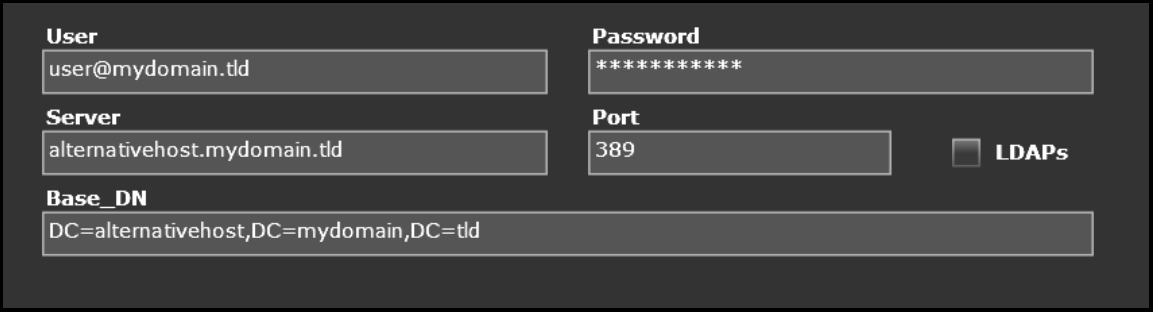


Figure 62: Selecting a different LDAP server

4. Optional: Enter the desired filter in the field **LDAP Filter**.

> **Notice:**
>
> The value **proxyaddresses=*** selects all users in an Active Directory. If your template does not comply with your directory structure, you can customize it here individually.

5. Click on **Save** in the lower left corner of the window.

You have activated LDAP for Signature & Disclaimer in the Control Panel.

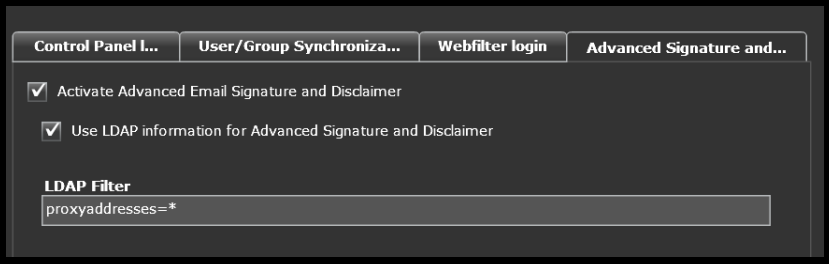


Figure 63: Activate Signature & Disclaimer

Now you can configure Signature & Disclaimer for users and groups of your directory service.

Contact Data

The master data of companies and contact persons can be added under the tab **Contact Data**. This data can be accessed by Hornetsecurity. The company data is required for billing purposes. The data for contact persons is used in support requests to check whether the requester is authorized to submit an request.

Important:

Support requests can only be processed by persons authorized to give instructions in accordance with the Order Processing Contract (AVV, Art. 28 GDPR)! No requests can be accepted by the support in case of missing authorizations! Under **Contact Data**, enter the persons who are authorized to provide support requests for the registered customer according to the AVV.

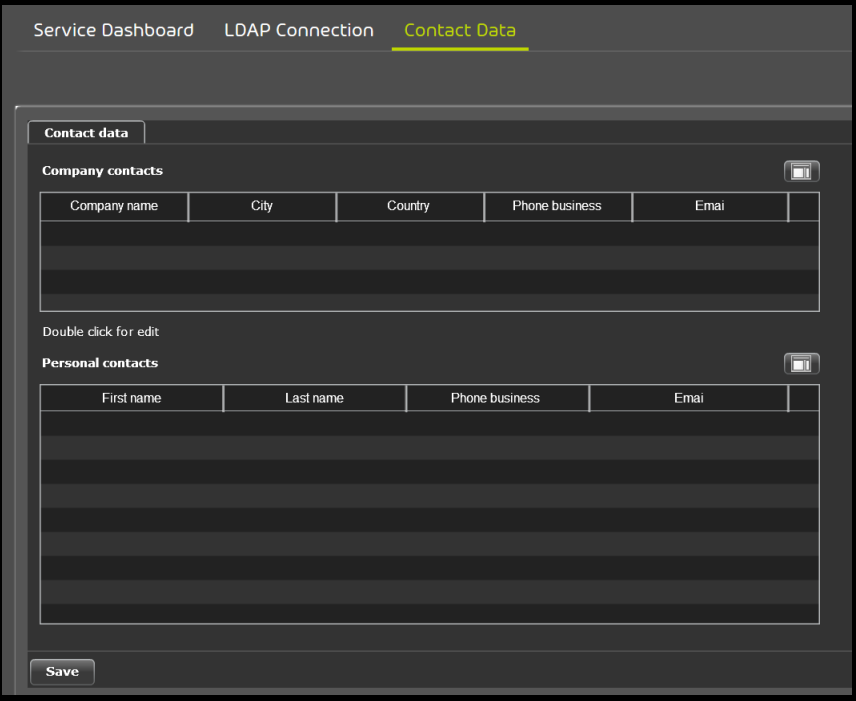


Figure 64: Management of contact data

Adding Contact Data

Under **Service Dashboard#→Contact Data**, you can enter master data about your company and contact persons for support requests.

1. Navigate to **Service Dashboard#→Contact Data**
2. Click on **Add**.
3. Enter the desired contact data and confirm with **Add**:

   a) Select the tab **Company** to add contact data for a company.

Figure 65: Contact data form for a company

b) Select the tab **Person** to add contact data for a person.

Figure 66: Contact data form for a person

4. Save your data with **Save**.

The contact data has been added.

365 Total Protection

365 Total Protection

Description of 365 Total Protection

365 Total Protection from Hornetsecurity offers comprehensive protection for Microsoft cloud services – specially developed for Microsoft 365 and seamlessly integrated. Benefit from the fact that it is easy to set up and extremely intuitive to use, simplifying your IT Security management from the very start.

Here you get all the information you need to set up 365 Total Protection.

Notice:

The 365 Total Protection onboarding addresses new customers. Existing customers and domains cannot be created again.

Onboarding of Microsoft 365 Customers

With 365 Total Protection domains and users of a customer are synchronized automatically into the Control Panel.

If your customer has an Microsoft 365 account, you have the option to set up 365 Total Protection automatically using the Control Panel. All of the customer's domains and users created in Microsoft 365 are automatically transferred and displayed in the control panel.

Notice:

Groups are synchronized from Microsoft 365 as well but cannot be used at the moment. For more information on how to add groups manually, see the chapter Group Management in the Control Panel on page 94.

There are two ways to set up the customer: You can either log in to Microsoft with the customer's administrative credentials and perform the onboarding process yourself, or you can send the customer an onboarding link to do the setup themselves.

Afterwards, some DNS settings must be configured for the domains to redirect the email traffic.

Creating an Onboarding Link

Create a link for your customers so that they can perform the setup process themselves.

1. Open the Control Panel.
2. In the scope selection, select the partner account under which you want to create the new customer.
3. Select **365 Total Protection**.
4. Click on **Create onboarding link for customers**.

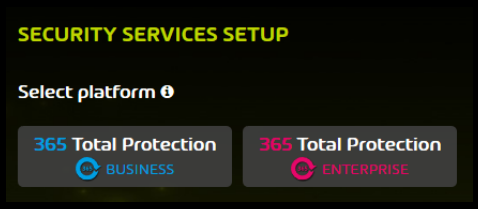


Figure 67: Select product

A unique link is then created which you can use several times.

5. Select the desired version of **365 Total Protection**.

Figure 68: Select version

6. Click on to copy the link to the clipboard.

You can use the generated link multiple times and deliver it to customers to take them directly to the onboarding form.

Onboarding 365 Customers in the Control Panel

Onboard the customer directly via the Control Panel if you have the administrative credentials for the Microsoft 365 environment of the customer you are setting up.

1. Open the Control Panel.
2. In the scope selection, select the partner under which the new customer is to be created.

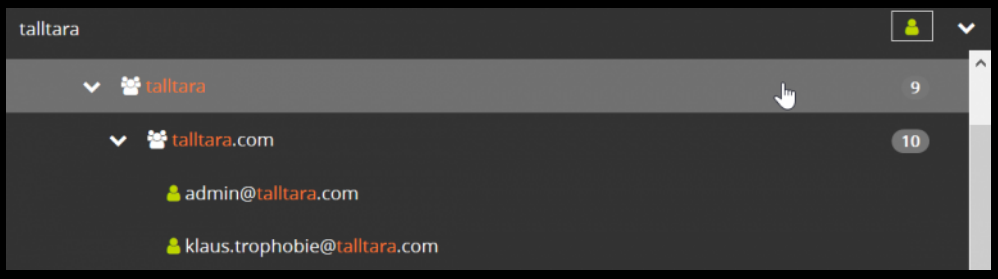


Figure 69: Select partner in the scope selection

3. Select **365 Total Protection**.

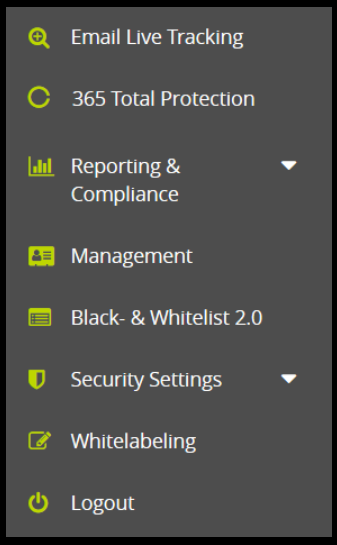


Figure 70: 365 Total Protection

4. Click on the desired product.

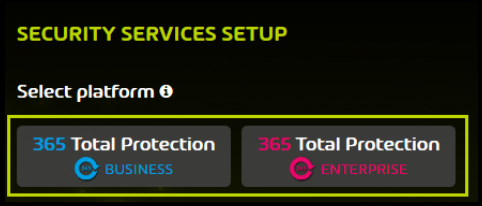


Figure 71: Select product

5. You will then be redirected to the onboarding form.

Setting up 365 Total Protection

Enter your contact details in the onboarding form so that we can contact you in case of problems or questions.

1. Enter your contact data.

> **Important:**
>
> Enter your primary domain in the field **Display name (domain) in the Control Panel**. This domain will be displayed in the Control Panel. Do not enter your .onmicrosoft domain!

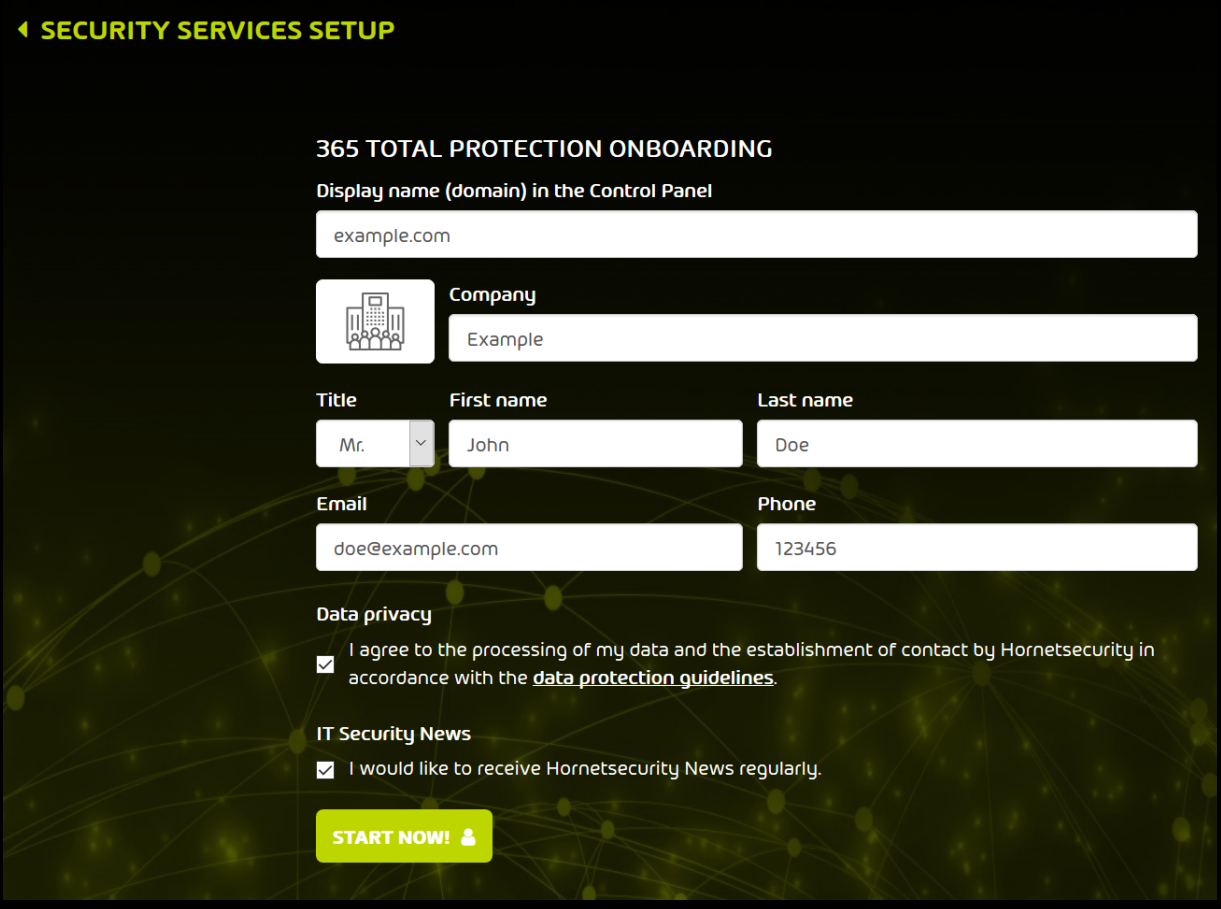


Figure 72: Fill in contact data

2. Then click on **START NOW!** to start the process.

3. Log in to Microsoft 365 with administrative rights.

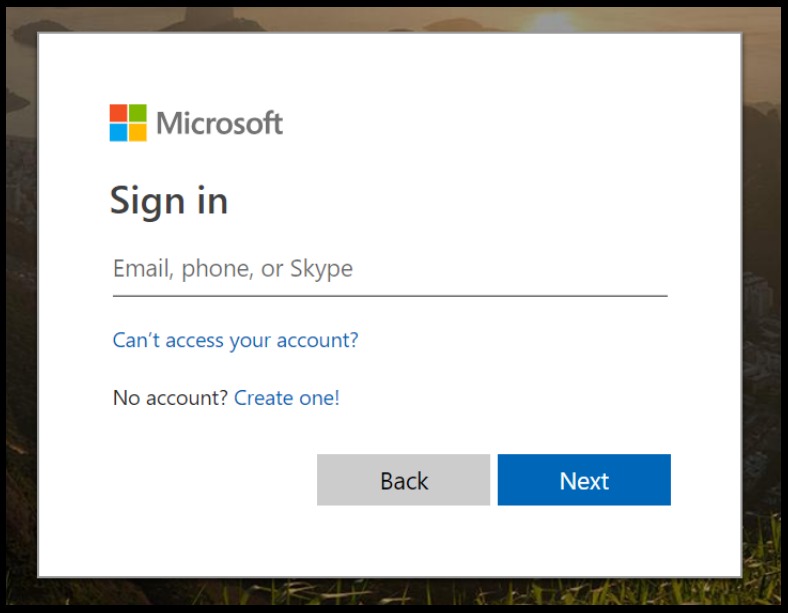


Figure 73: Enter Microsoft credentials

Notice:

During the subsequent synchronization, only the domains and mailboxes are transferred. No changes are made to Microsoft's configuration settings. Groups are synchronized from Microsoft 365 as well but cannot be used at the moment. For more information on how to add groups manually, see the chapter Group Management in the Control Panel on page 94.

4. Accept the requested permissions to connect our services with Microsoft.

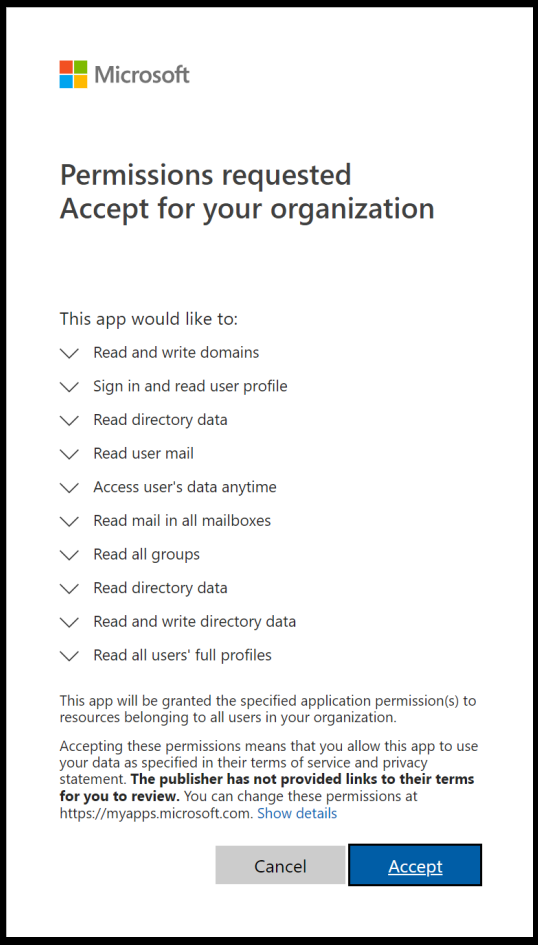


Figure 74: Accept permissions

Your domains and mailboxes are created in the Control Panel.

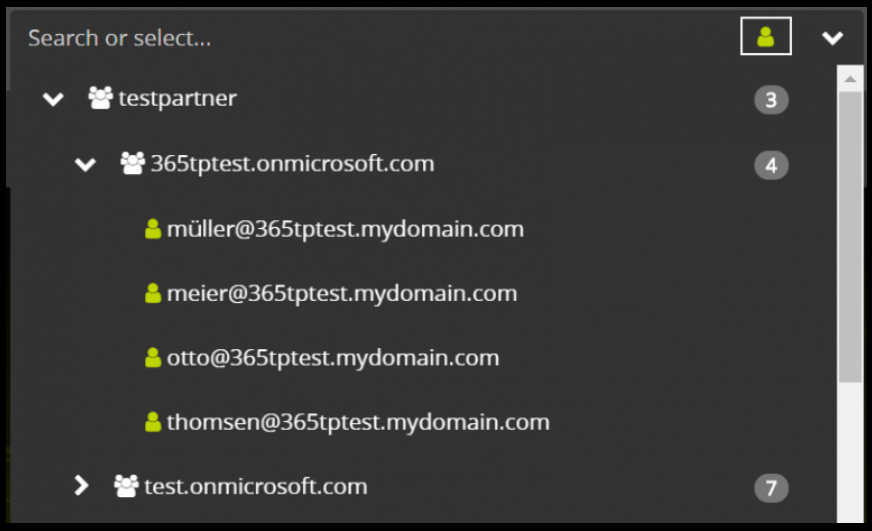


Figure 75: Registered onmicrosoft domains

Your domains and mailboxes are created in the Control Panel. From now on, you can use your Microsoft 365 credentials to log in to the Control Panel and configure the services.

After synchronization, you must set up the Microsoft services (see Configuration of Microsoft Services on page 75) so you can make full use of our services.

Configuration of Microsoft Services

To take advantage of all 365 Total Protection services, you must customize the configuration of Microsoft 365.

Configuring the Email Traffic Automatically

Configure the in- and outbound email traffic automatically.

Notice:

The automatic configuration of the outbound email traffic also configures the inbound email traffic automatically.

On the status page click on **CONFIGURE AUTOMATICALLY** to start the automatic configuration of the outbound email traffic.

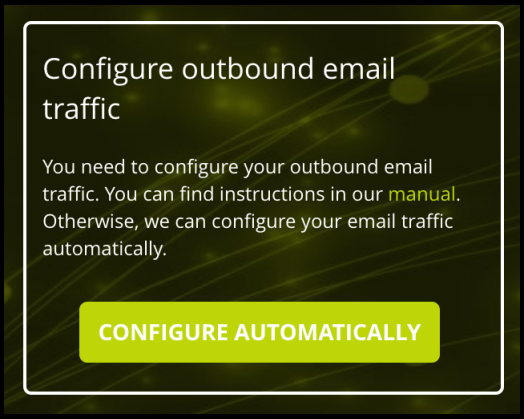
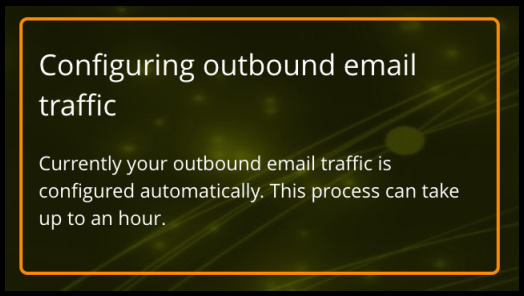


Figure 76: Configure automatically

The outbound email traffic is configured.



The outbound email traffic was successfully configured.

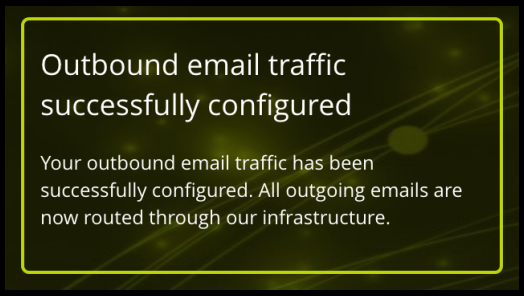


Figure 77: Successful configuration

Important:

Already installed connectors can cause errors in the automatic configuration of the outbound email traffic.

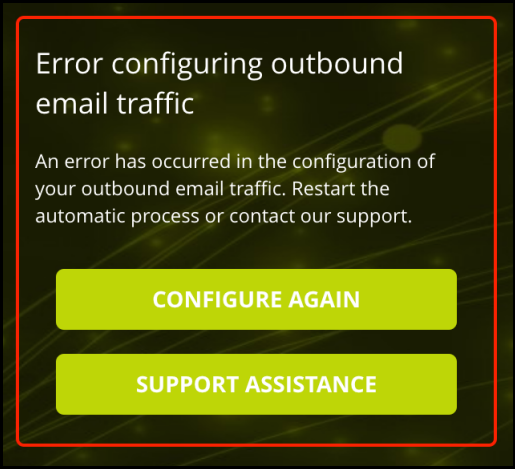


Figure 78: Errors in configuration

Troubleshooting

- Delete already configured connectors and click on **CONFIGURE AGAIN** to start the configuration OR
- click on **SUPPORT ASSISTANCE** to contact the support.

Deactivate the Microsoft 365 spam filter for the IP address range of Hornetsecurity

Deactivate the spam filter of Microsoft 365 to set up filtering through our services.

The spam filter of Microsoft 365 must be deactivated to prevent incoming emails from being classified as spam. The spam filtering is done by us.

Notice:

The email authentication with SPF by Hornetsecurity is not activated automatically. For more information about the configuration of the email authentication, see "Email Authentication Methods". Setting up email authentication is not mandatory, but recommended.

1. Log in to office.com with your administrative credentials.
2. Click on **Admin**.

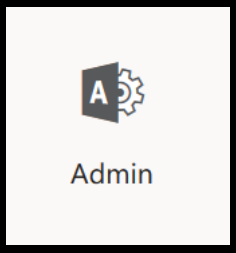


Figure 79: Admin button

3. Select **Admin centers**→**Exchange**→**protection**→**connection filter**.
4. Select **Default**.
5. Click on **Edit**.

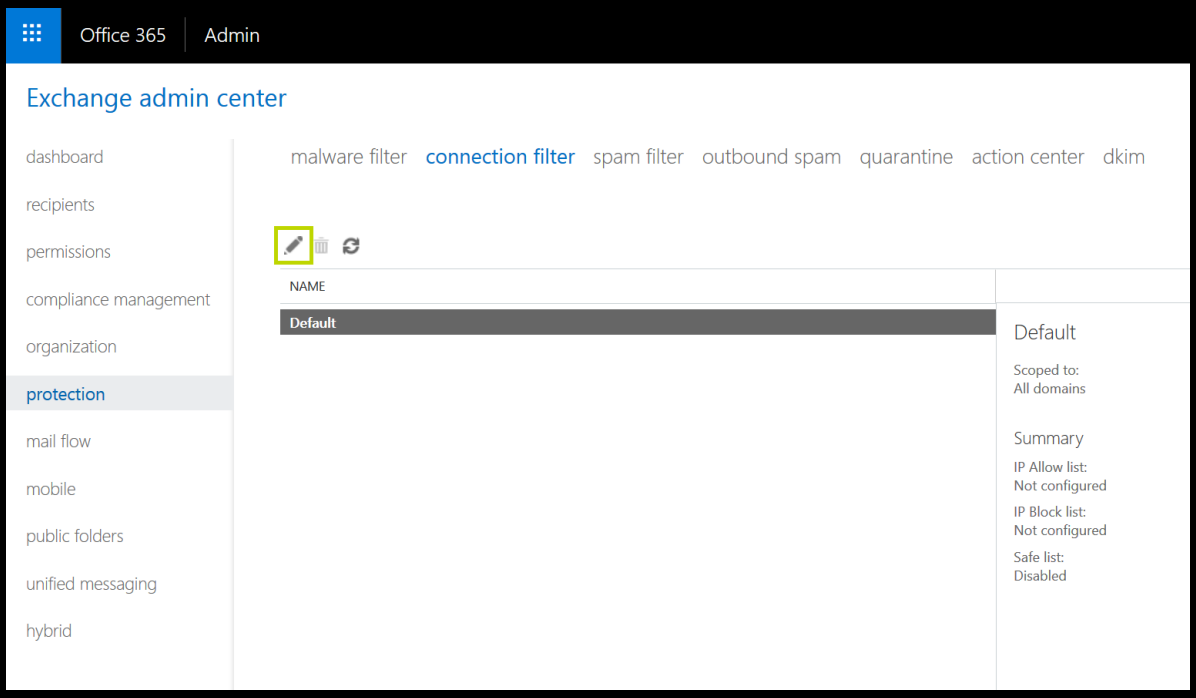


Figure 80: Configure connection filtering of Microsoft 365

6. Select **Connection filtering**.
7. Under **IP Allow list** click on **+**.
8. Enter the following IP addresses in the field **Allowed IP Address**:

   83.246.65.0/24, 94.100.128.0/24, 94.100.129.0/24, 94.100.130.0/24, 94.100.131.0/24, 94.100.132.0/24, 94.100.133.0/24, 94.100.134.0/24, 94.100.135.0/24, 94.100.136.0/24, 94.100.137.0/24, 94.100.138.0/24, 94.100.139.0/24, 94.100.140.0/24, 94.100.141.0/24, 94.100.142.0/24, 94.100.143.0/24, 185.140.207.0/24, 185.140.206.0/24, 185.140.205.0/24, 185.140.204.0/24, 173.45.18.0/24

9. Activate the checkbox **Enable safe list**.

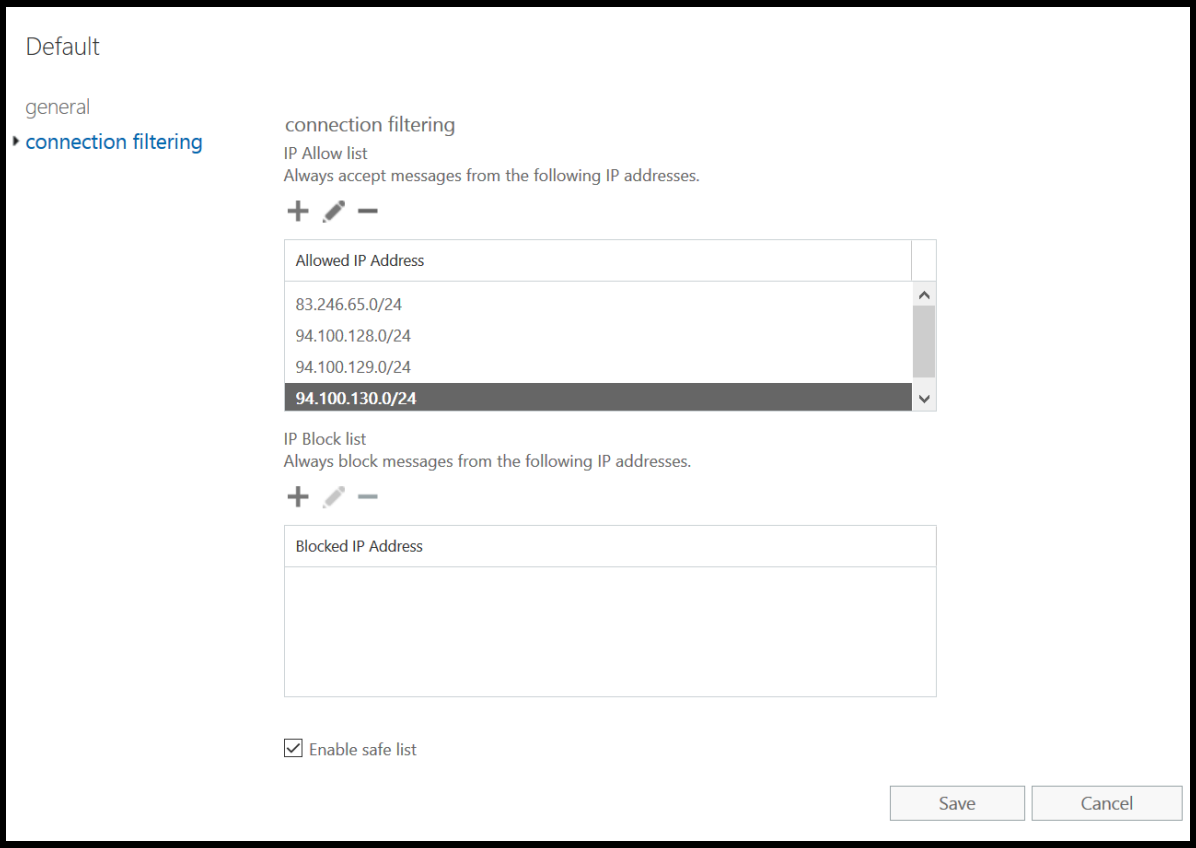


Figure 81: Settings connection filtering

10. Save your settings.

The Microsoft 365 spam filter is deactivated for the IP address range of Hornetsecurity.

Adjusting the SPF Records

To make sure that emails routed through the Hornetsecurity Services are not filtered as spam, add Hornetsecurity as a valid sender for your domain.

1. Open the Microsoft 365 Admin Center.
2. Navigate to **Setup#→Domains**.
3. Select the domain you have registered with Hornetsecurity.
4. Include the following SPF/TXT record: **TXT "v=spf1 include:spf.protection.outlook.com include:spf.hornetsecurity.com ~all"**

> **Important:**
>
> If you have additional systems, which send outbound emails for the corresponding domain, include them to the SPF Record as well.

The configuration of the inbound email traffic is complete.

Setting MX records

To route and filter email traffic through our infrastructure, adjust the MX records of all synchronized domains.

1. > **Important:**
   >
   > Set the following MX records in the DNS settings of your domains in the Microsoft 365 Admin Center: If you are note sure, please contact the support.

   Set the MX records in the DNS settings as follows:

   Table 4: MX records

Domain	Class	TYPE	PRIORITY	Mailserver
customerdomain.tld	IN	MX	10	mx01.hornetsecurity.com
customerdomain.tld	IN	MX	20	mx02.hornetsecurity.com
customerdomain.tld	IN	MX	30	mx03.hornetsecurity.com
customerdomain.tld	IN	MX	40	mx04.hornetsecurity.com

   > **Notice:**
   >
   > Enter your actual domain for **customerdomain.tld**.

2. To check if the MX records are set correctly, click on **SHOW CONFIGURATION**.

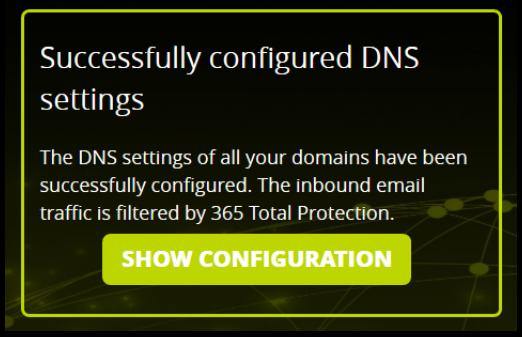


Figure 82: Show configuration

The status report shows the successful update of the MX records.

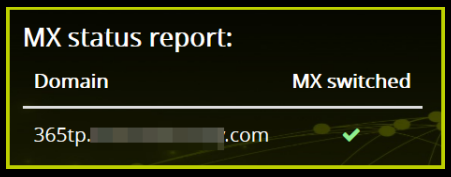


Figure 83: Status report

MX-records have been added.

Configuring Autodiscover

Setting the Autodiscover service facilitates the process of setting up user accounts in email clients. Users do not need to enter a server name or port number, this information is automatically shared by the Autodiscover service.

Set a CNAME record for the Autodiscover service:

Table 5: Add MX records

TYPE	PRIORITY	HOSTNAME	POINTS TO	TTL
CNAME		autodiscover	autodiscover.hornetsecurity.com	1 hour

You have set the Autodiscover service for 365 Total Protection.

Archiving for Internal Emails

There are two options to archive internal emails with the archiving service of Hornetsecurity: Either you forward internal emails to Hornetsecurity or you use a journal postbox.

Important:

You cannot use both options at the same time.

Figure 84: Archiving of domains in Hornetsecurity Control Panel

Important:

Also make sure to have the archiving service enabled within the Hornetsecurity Control Panel for all domains before you continue.

Option A: Using Hornetsecurity for Relaying Internal Traffic

With this option all internal emails leave your Microsoft 365 environment and are routed to Hornetsecurity. These emails are redirected to Microsoft 365 after archiving.

1. In the Exchange Admin Center, select **mail flow#→rules#→Create a new rule...**.

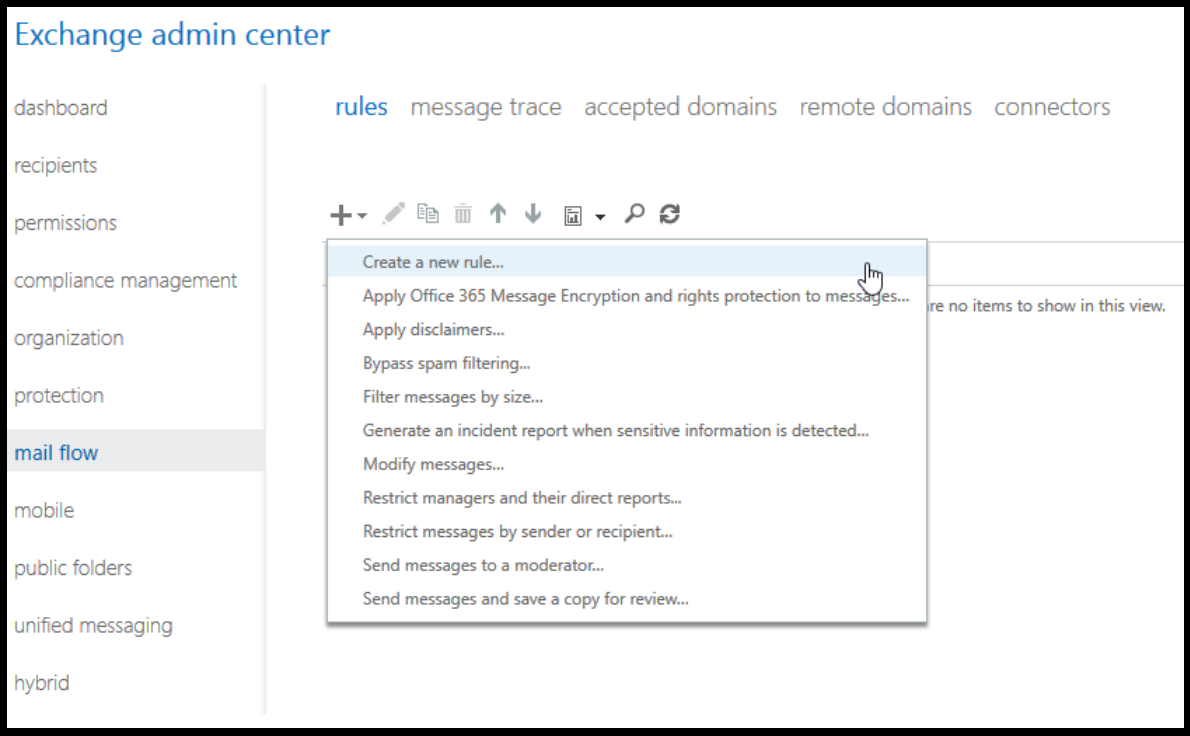


Figure 85: Create new rule

2. Select **More options...**.

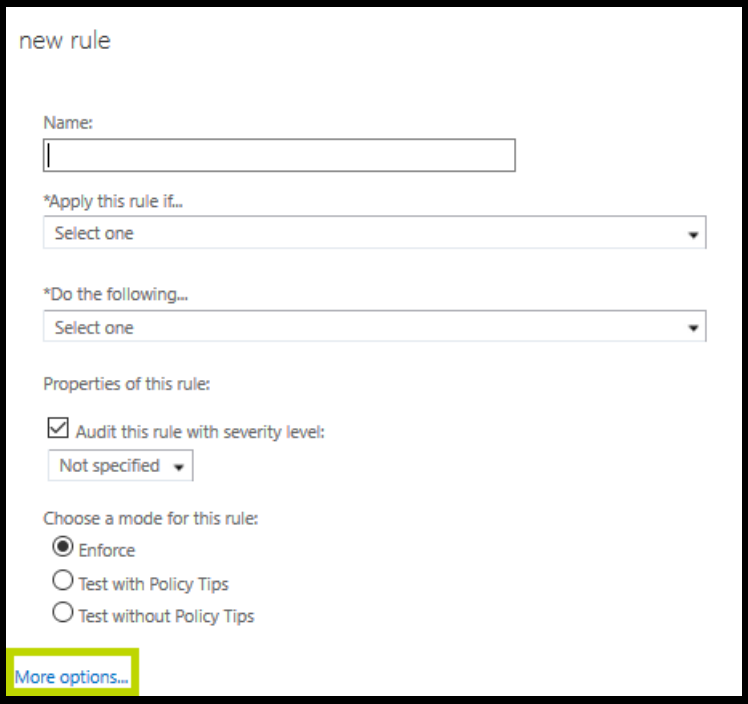


Figure 86: More options

3. Define a name for the new rule.
4. In the drop-down menu **Apply this rule if...** select**The recipient is located...#→Inside the organization...**.

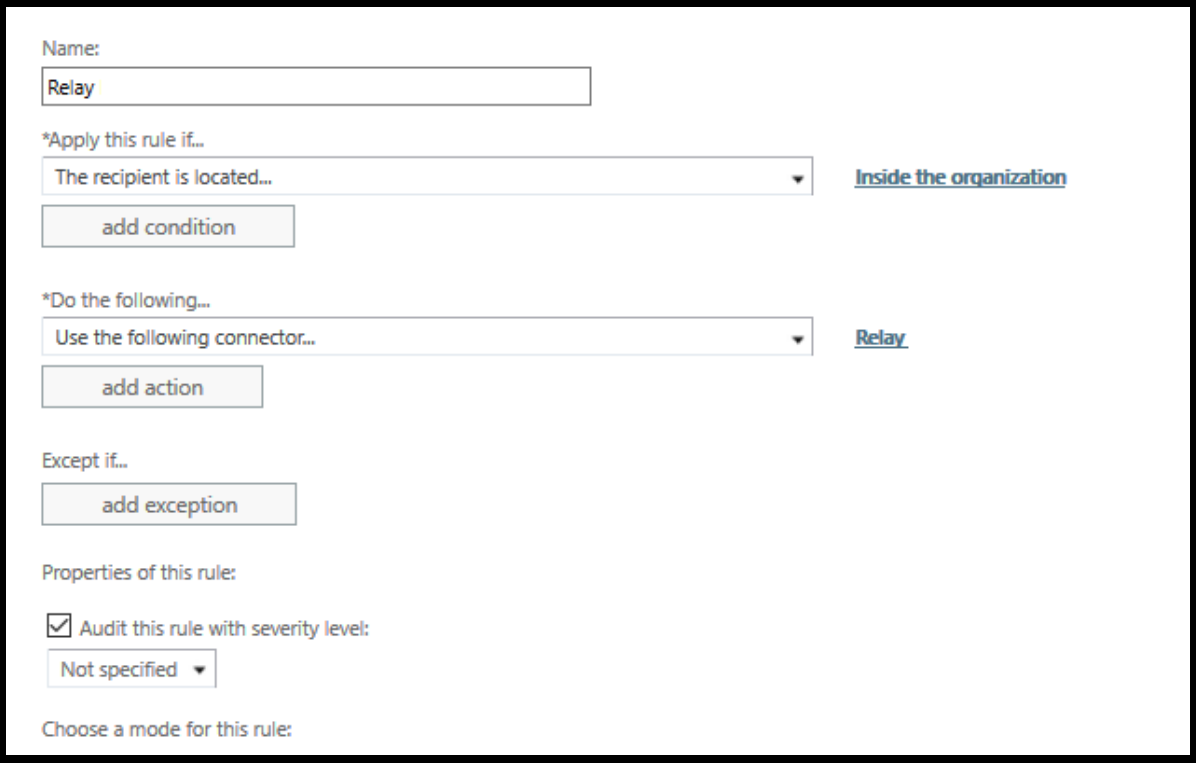


Figure 87: Setup new rule

5. In the drop-down menu **Do the following....**, select **Redirect the message to...#→The following connector**.
6. Select the connector created in Configuring Connector for Outbound Email Traffic.

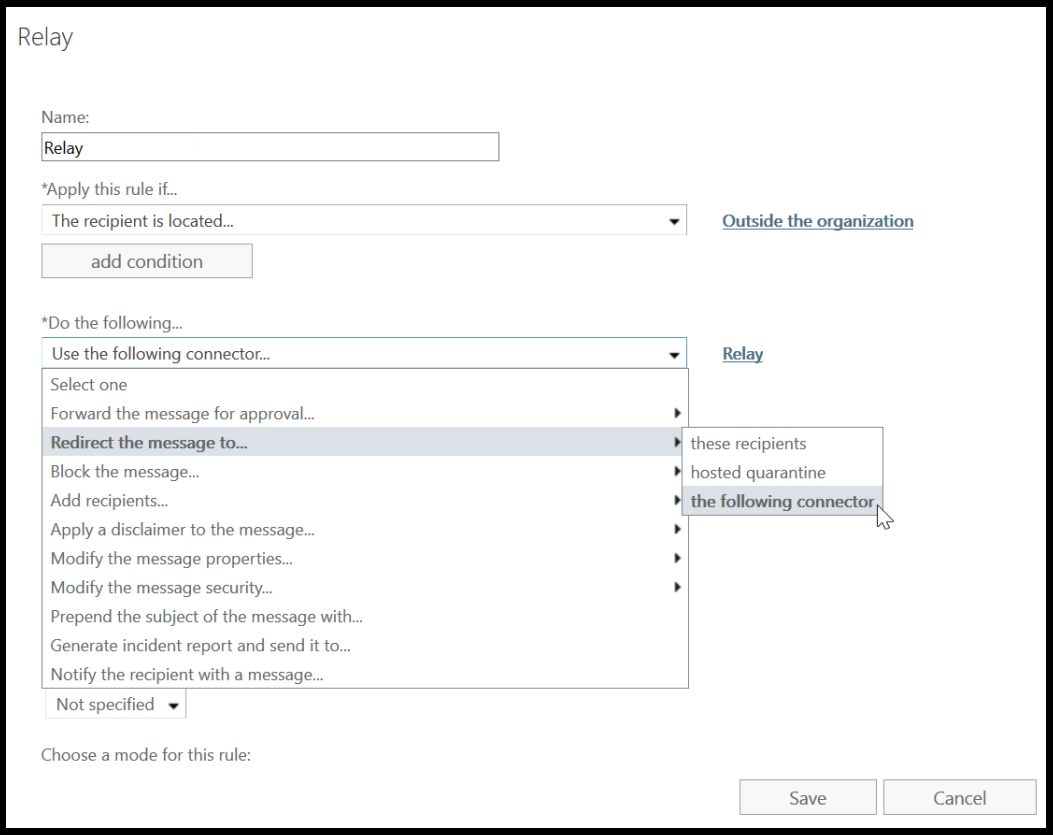


Figure 88: Select connector

7. Click on **Add exception** and, in the drop-down menu **Except if...**, select the point **The sender is located... Outside the organization...**.

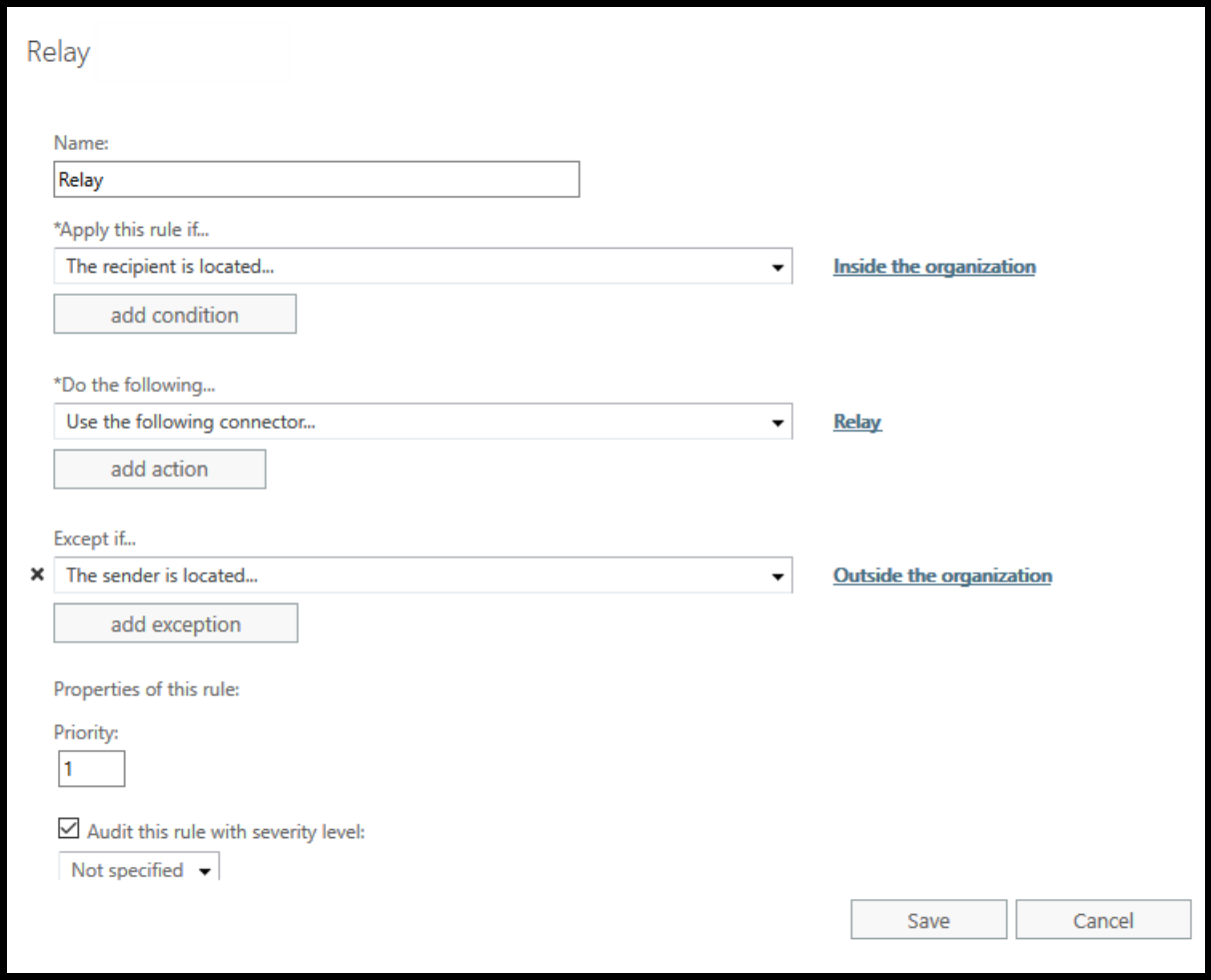


Figure 89: Add exception

8. Save your settings.

Hornetsecurity is used for Relaying Internal Traffic.

Option B: Use Journaling to Archive Internal Emails

Another option for archiving internal emails is the journaling feature.

That means that Microsoft 365 generates a journal report for each internal email and sends it to Hornetsecurity while keeping your internal email routing within your organization.

Creating a Journal Rule

Create a journal rule to send journal reports to our domain.

1. Open the **Exchange Admin Center**.

2. Select **Compliance management#→Journal rules**.
3. Click on **New**.
4. Define an email address for undeliverable journal reports.

   This can belong to any user in the Microsoft 365 environment.
5. Define a name in the field **Name**.
6. Enter following in the input field **Send journal reports to: <customer_domain.tld> 2007@journal.antispameurope.com**

> **Notice:**
>
> The placeholder **<customer_domain.tld>** represents the main domain which is defined in the Hornetsecurity Control Panel.

7. Select **[Apply to all messages]** in the drop-down menu **If the message is sent to or received from...**.
8. Select **Internal messages only** in the drop-down menu **Journal the following messages...**.

Figure 90: Apply new journal rule

9. Click on **Save**.

New Journal Rule has been created.

Creating a New Connector for Journal Reports

Create a connector for journal reports to forward emails via our smart host.

1. Select **Mail flow#→Connectors#→New**.

2. Select **Microsoft 365** in the drop-down menu **From:**.
3. Select **Partner organization** in the drop-down menu **To:**.

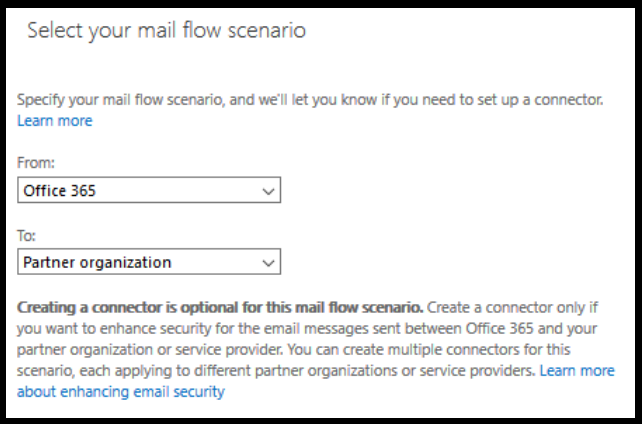


Figure 91: Select destination server

4. Click on **Next**.
5. Define a name for the new connector (e. g., Relay (Journal)).

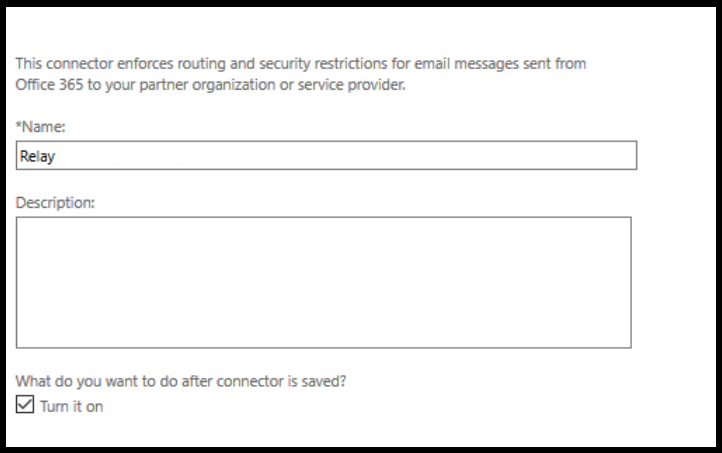


Figure 92: Define name

6. Click on **Next**.
7. Select **Only when email messages are sent to these domains** and enter the following domain: **journal.antispameurope.com**

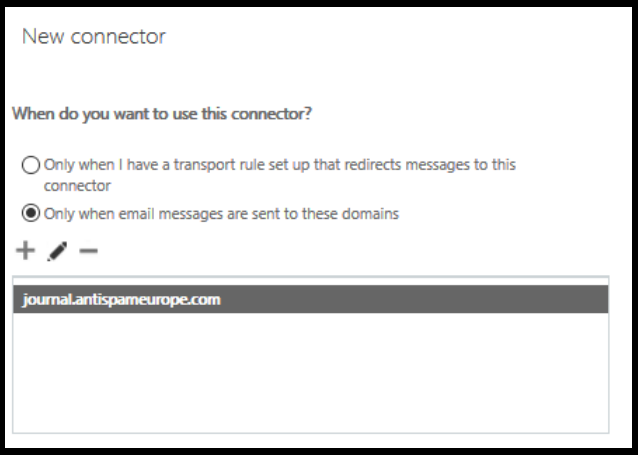


Figure 93: Setup application

8. Click on **Next**.
9. Select **Route email through these smart hosts** and enter following domain: **relay-cluster-eu01.hornetsecurity.com**.

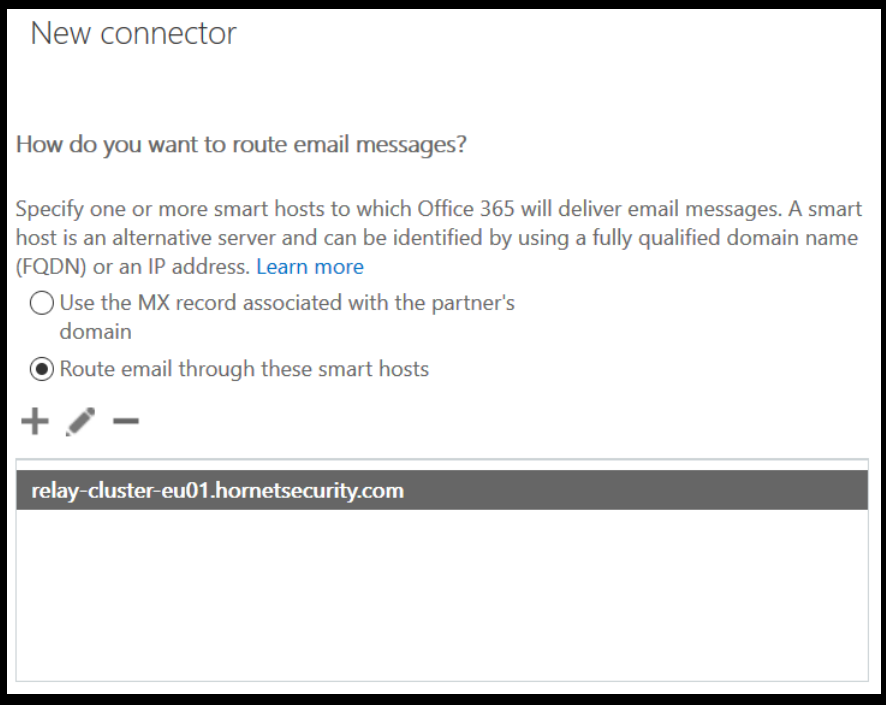


Figure 94: Add smart host

10. Click on **Next** on the following TLS configuration without making adjustments.

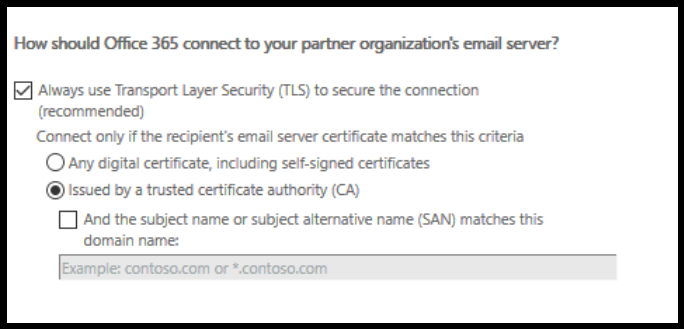


Figure 95: TLS configuration

You can see a review of the configured connector. This should look similar to this:

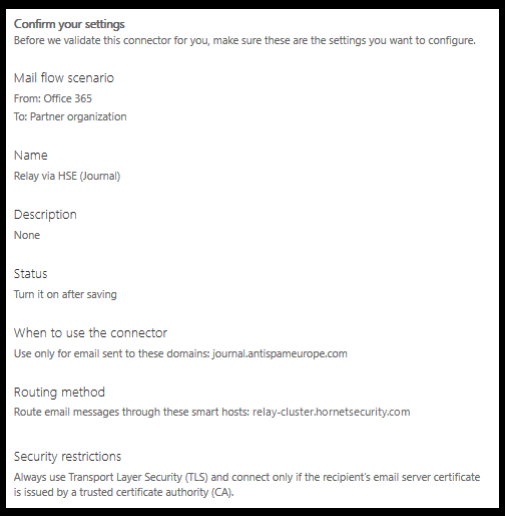


Figure 96: Overview of configured connector

11. Click on **Next**.
12. To confirm that the connector is working as intended, send a test email using the following email address scheme for this test email: <customer_domain.tld>_2007@journal.antispameurope.com

Notice:

Replace **<customerdomain.tld>** with your actual domain.

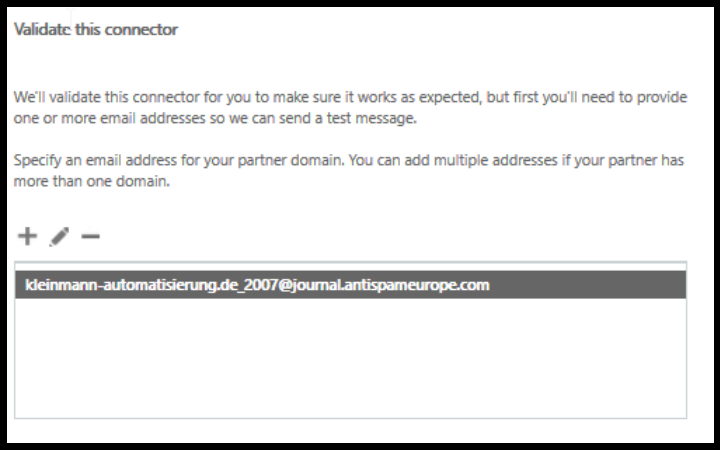


Figure 97: Validate connector

13. Save your settings, if the test was successful.

New Connector for Journal Reports has been created.

Email Encryption

The email encryption is part of the products 365 Total Protection Business and Enterprise. Encryption must be activated manually because some settings must be configured here.

Follow the instructions in the chapter "Encryption" .

Activating Email Encryption

Attention:

The activation of Email Encryption will increase costs according to the price list.

1. Navigate to **Security Settings#→Email Encryption**.
2. Mark the checkbox **Activate policy**.

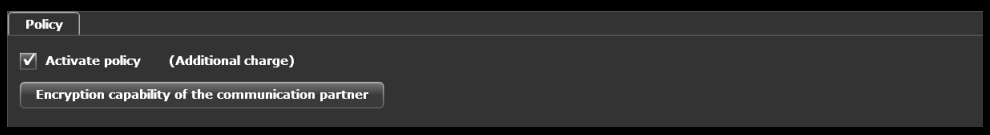


Figure 98: Activating Email Encryption

You have activated Email Encryption.

Notice:

Only emails which are sent from one of the relay IP addresses specified under Spam and Malware Encryption can be signed and encrypted with Email Encryption (see Environment Settings on page 276).

Activating the Continuity Service (365 Total Protection Enterprise only)

Activate the Continuity Service to receive emails in case of a service disruption.

If the Microsoft services fail or the services be temporarily unavailable, this also affects your access to your mailbox. Emails can then be neither sent nor received which can harm your entire business processes. In such an event, Continuity Service is your stand-by system which – activated in mere seconds – keeps your email correspondence up and running.

Notice:

Continuity Service is only included in 365 Total Protection Enterprise and you must activate it manually to configure the settings.

1. Navigate to **Security Settings#→Continuity Service**.
2. Activate the checkbox **Continuity Service, stores clean Emails for 3 months**. With 365 Total Protection Enterprise you do not have to pay any additional fees for this service.
3. Select whether all mailboxes of the domain or only certain mailboxes should be covered by the service:

   a) If you select **All users**, all mailboxes of the domain will be covered.

   b) If you select **Selected users only**, the click on **Select** and select the mailboxes you want.

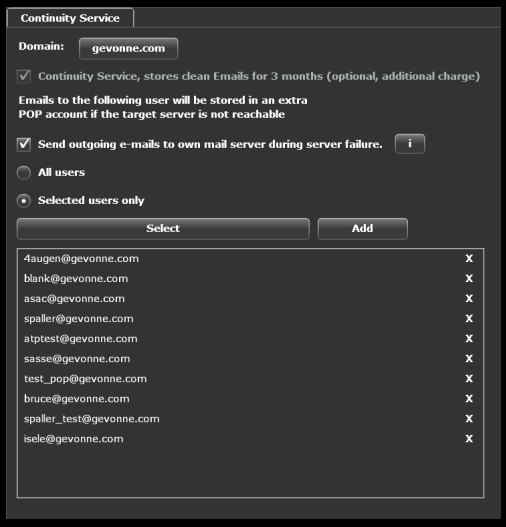


Figure 99: Continuity Service, activating

You have activated Continuity Service.

Group Management in the Control Panel

The groups you want to use in the Control Panel have to be created again because Microsoft 365 allows a different group management than our services.

The chapter "Groups" of the Control Panel explains how to create groups in the Control Panel.

Adding a group

Create a new group from existing mailboxes.

1. Navigate to **Customer Settings#→Groups**.
2. Click on Add group
   A drop-down menu opens.

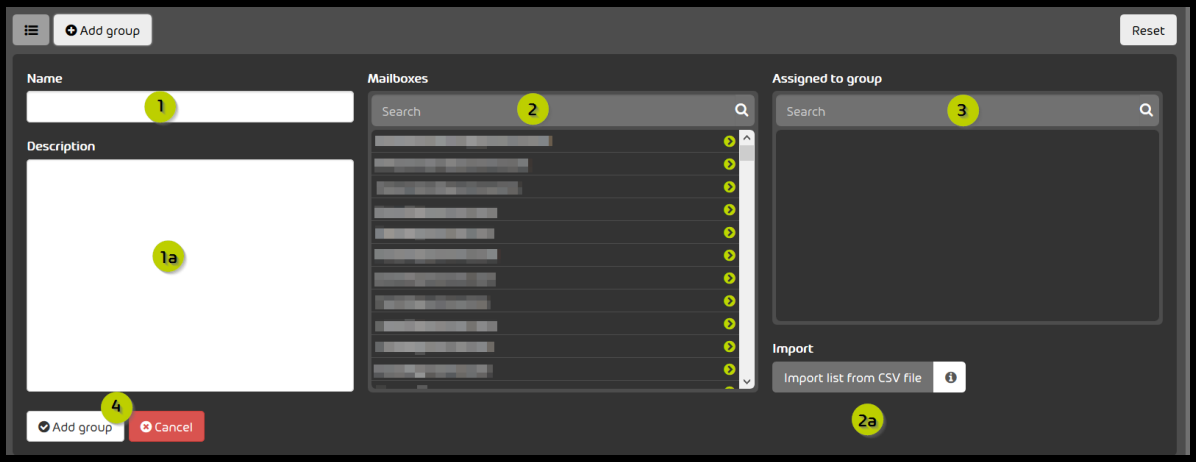


Figure 100: Add a new group

3. Assign a group name under **Name** (1). You can optionally add a description to the group in the field **Description** (1a).
4. Under **Mailboxes** (2), select at least one mailbox to add to the group.

> **Notice:**
>
> Previous member lists can be imported here from a CSV file (see Importing Group Members from a CSV File on page 230) (2a).

→ The selected mailbox is displayed in the window **Assigned to group** (3).

5. Click on **Add Group** to combine the selected mailboxes into one group (4).

You have created a group from selected mailboxes.

Manage members

Manage the members of an existing group.

1. Navigate to **Customer Settings#→Groups** and click on the arrow for the desired group.

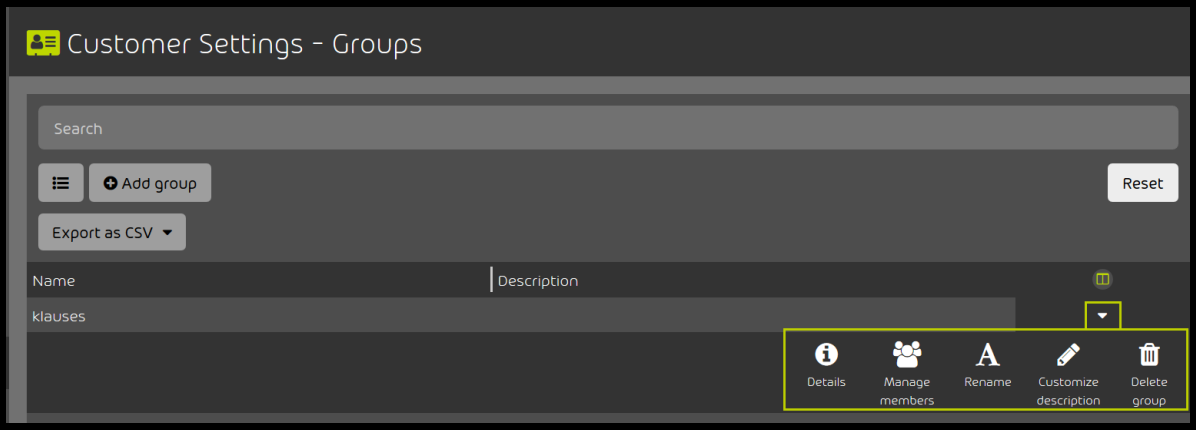


Figure 101: Open groups menu

2. Click on **Manage members**.

   A drop-down menu with two windows will open, showing all registered mailboxes (left) and all mailboxes assigned to the group (right).

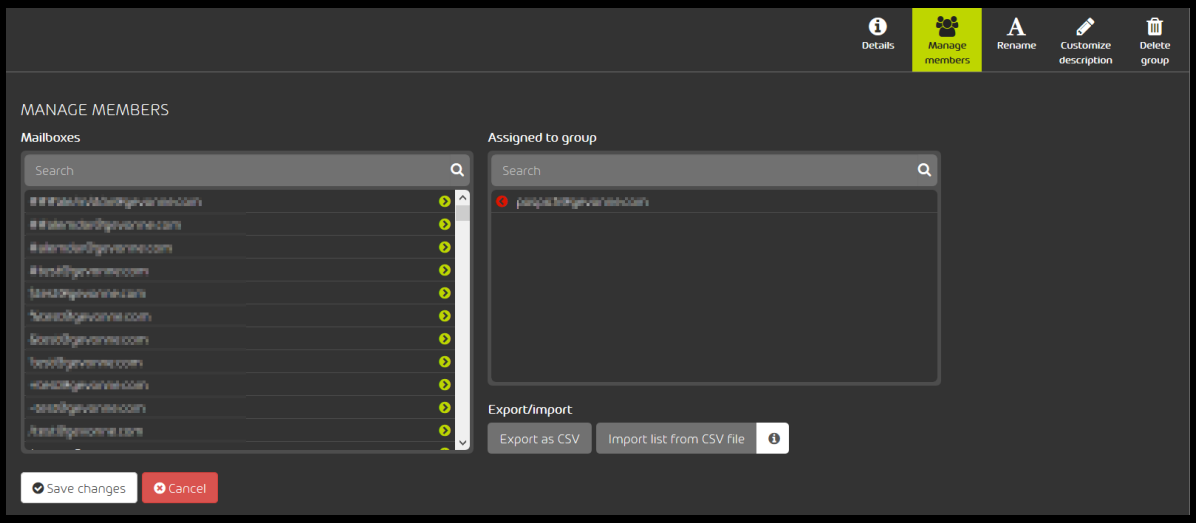


Figure 102: Manage group members

3. Manage the members of a group:

   - If you want to add more members to the group, click on the members to be added in the **Mailboxes** (left) window. You can also import existing group lists as a CSV file (see Importing Group Members from a CSV File on page 230).
   - If you want to remove already existing members from the group, click within the window **Assigned to Group** (right) on the group members to be removed.

   You have assigned or removed members from the selected group.

4. Click **Save Changes** to save the updated group.

You have successfully managed the group.

Synchronized Attributes from the Azure Active Directory

With the Azure Active Directory of Microsoft only certain attributes are synchronized for Signature & Disclaimer.

Important:

It is not possible to use LDAP and attribute synchronization via Microsoft 365 at the same time. For Microsoft 365 customers, only the attributes in the table below are synchronized. The LDAP attributes are not synchronized.

The following attributes are synchronized and can be used to create signatures and disclaimers:

AD-Variable	Description
countryCode	Country code
department	Department
displayName	Complete name
givenName	First name
info	Jobtitle/Position **Notice:** The field Title is often used for other purposes. Therefore, the term Info is used here for the LDAP-attribute Title (Jobtitle/Position).
l (lower case L)	City
mail	Email address
mobile	Mobile phone number
postalCode	Postal code
sn	Surname

AD-Variable	Description
st	State
streetAddress	Street
telephoneNumber	Phone number

Ordering 365 Total Protection

If you would like to use the product after 14-day test, order 365 Total Protection in the Control Panel directly.

1. Select **365 Total Protection**.
2. Click on **BUY NOW**.
   An overview showing the amount of mailboxes and the price appears.

3. Click on **ORDER NOW CHARGEABLE** to buy 365 Total Protection.
   You get a confirmation email with an overview of the product.

Offboarding after Termination of the Trial Period or Cancellation

Delete the configuration for Microsoft 365 to get emails if you do not use 365 Total Protection anymore.

At the end of the 365 Total Protection trial period, if you no longer wish to use the product, or if you canceled 365 Total Protection at any time, you will need to make some settings in your Microsoft 365 configuration to ensure that your emails are delivered.

1. Delete or deactivate the connector for the inbound email traffic. (firewall setting)

2. If you have changed the outbound email traffic, delete or deactivate this connector as well. (Relaying)

> **Notice:**
>
> Information on how to delete or disable the connectors in your Microsoft 365 environment can be found here: Deleting or Deactivating Connector on page 99.

3. Remove the MX records in the DNS zone of your domains.

Your emails will then no longer be routed through our services.

Deleting or Deactivating Connector

Delete or deactivate the connector.

1. Open Office.com and log in with your administrative credentials.
2. Navigate to **Admin**#→**Admin centers**#→**Exchange**.
3. Select **mail flow** and click on the tab **connectors**.
4. Select the connector, you want to delete or deactivate.
5. You can delete or deactivate the connector:
   - To delete the connector, click on **Delete**.
   - To deactivate the connector, click on **Deactivate** in the connector overview.

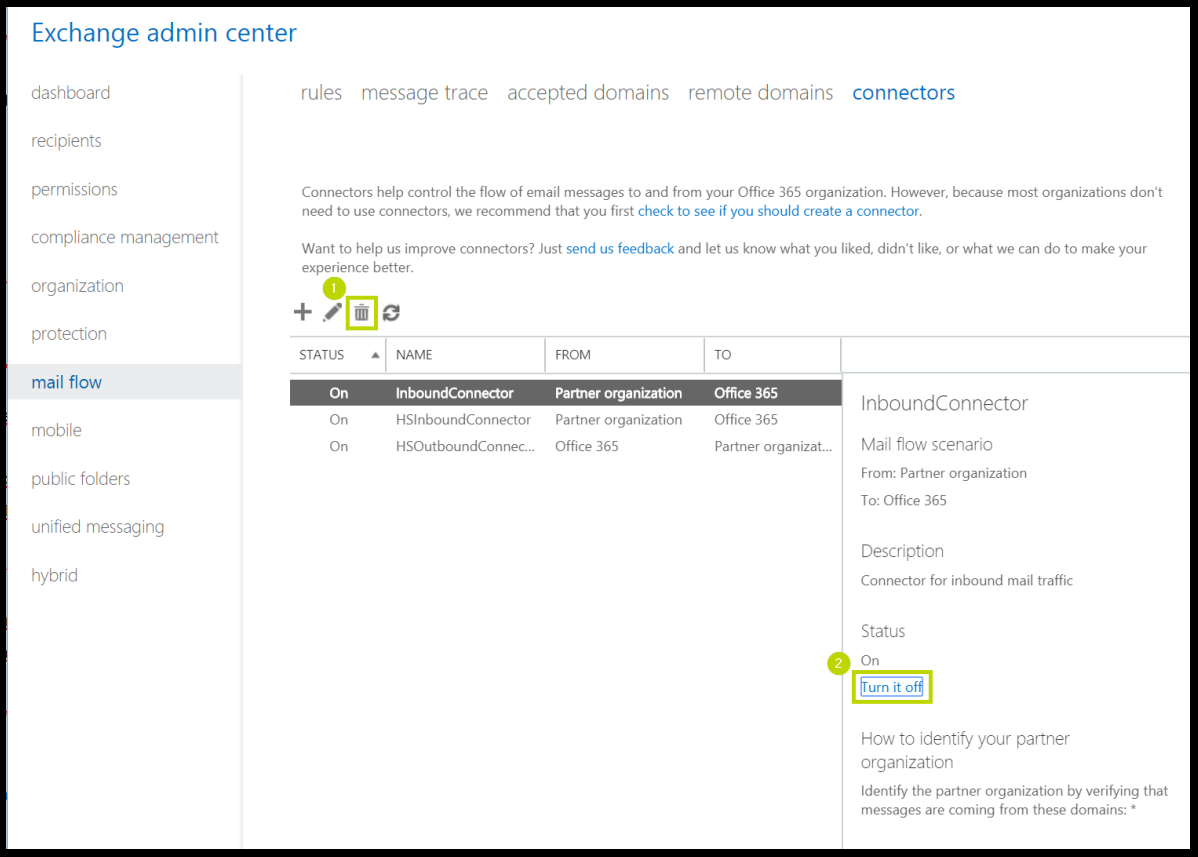


Figure 103: Delete or deactivate Connector

6. Confirm the notification with **Yes**.

Connector has been deleted or deactivated.

Deleting a Customer in the Test Stage

Delete a customer in the test stage from the 365 Total Protection environment.

Depending on your rights, you can delete an existing customer in the test stage of 365 Total Protection from the 365 Total Protection environment.

CAUTION:

The selected customer will be deleted permanently! There is no possibility to restore the customer's data!

1. In the scope selection in the top right corner of the Control Panel, select the desired **.onmicrosoft** customer.

- The product **365 Total Protection appears in the main navigation on the left.**.

2. Click on **365 Total Protection** in the main navigation on the left.
   - The page with the setup status of **365 Total Protection** is displayed.
3. Scroll with the mouse to the lower position of the status page.
   - You will see the contract status and the buttons **BUY NOW** and **DELETE CUSTOMER**.

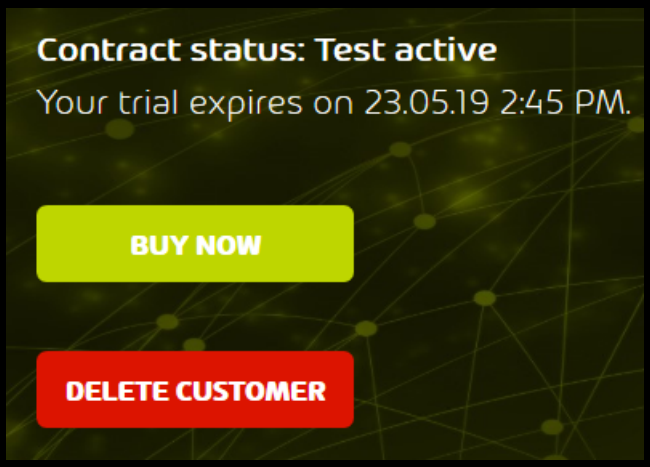


Figure 104: Button DELETE CUSTOMER

4. Click on the button **DELETE CUSTOMER**.
   - A warning about the deletion of the existing customer is displayed.

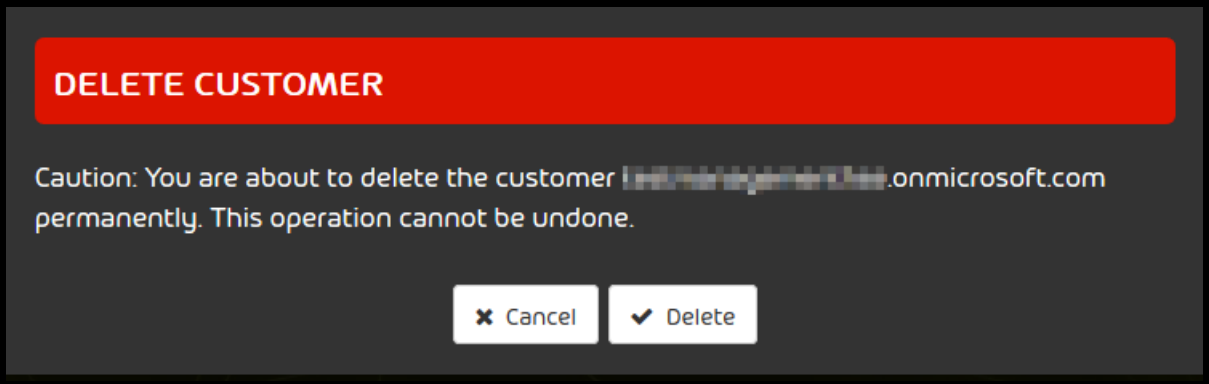


Figure 105: Delete customer

5. Click on **Delete** to permanently delete the selected customer.

- You have successfully deleted the selected 365 Total Protection customer.

365 Total Encryption

About 365 Total Encryption

365 Total Encryption is an additional feature for 365 Total Protection which encrypts all existing and future incoming and outgoing email messages. Follow the steps in this manual in order to activate 365 Total Encryption for your domain.

365 Total Encryption has the following functions:

- All incoming and outgoing emails are encrypted before they enter the Microsoft Cloud.
- In Microsoft 365, all emails are stored encrypted so that only the authorized person with the private key can have access.
- Existing mailboxes are automatically subsequently encrypted when 365 Total Protection is activated.

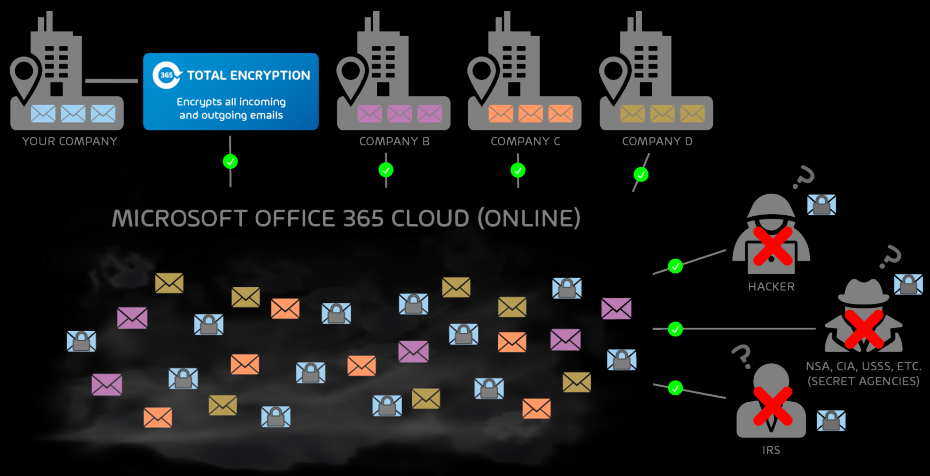


Figure 106: How 365 Total Encryption works:

365 Total Encryption has the following advantages:

- Confidential company data in emails is protected.
- The data is safe even if an account has been hijacked successfully.
- Authorities and secret services cannot spy out your data.

Activating 365 Total Encryption for a domain

You have activated 365 Total Protection.

1. Log in to the Control Panel with your administrative credentials.
2. In the role selection, select the domain containing the users you want to activate 365 Total Encryption for.
3. Navigate to **365 Total Protection**#→**365 Total Encryption**.

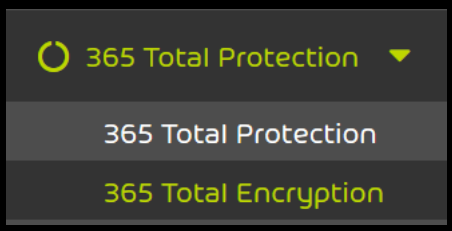


Figure 107: Select 365 Total Encryption

4. Click on **Encryption activated** to activate 365 Total Encryption.

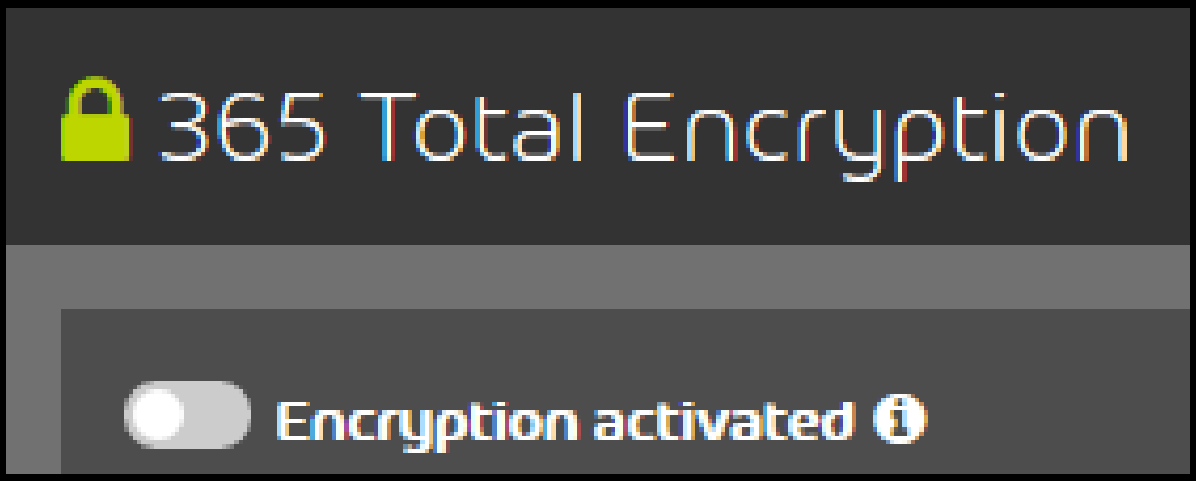


Figure 108: Activate Encryption

5. **Attention:**
   The activation of 365 Total Encryption will increase costs according to the price list.

   Click on **Activate** to confirm the activation.

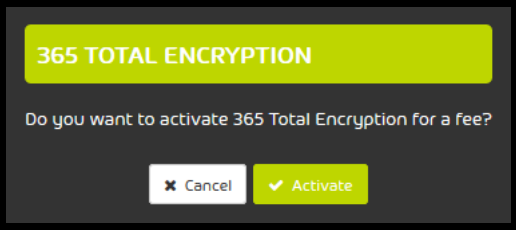


Figure 109: Confirm activation

You are redirected to a Microsoft login page.

6. **Notice:**

   Logging in to Microsoft is used for two-factor authentication.

   Log in with your administrative credentials.

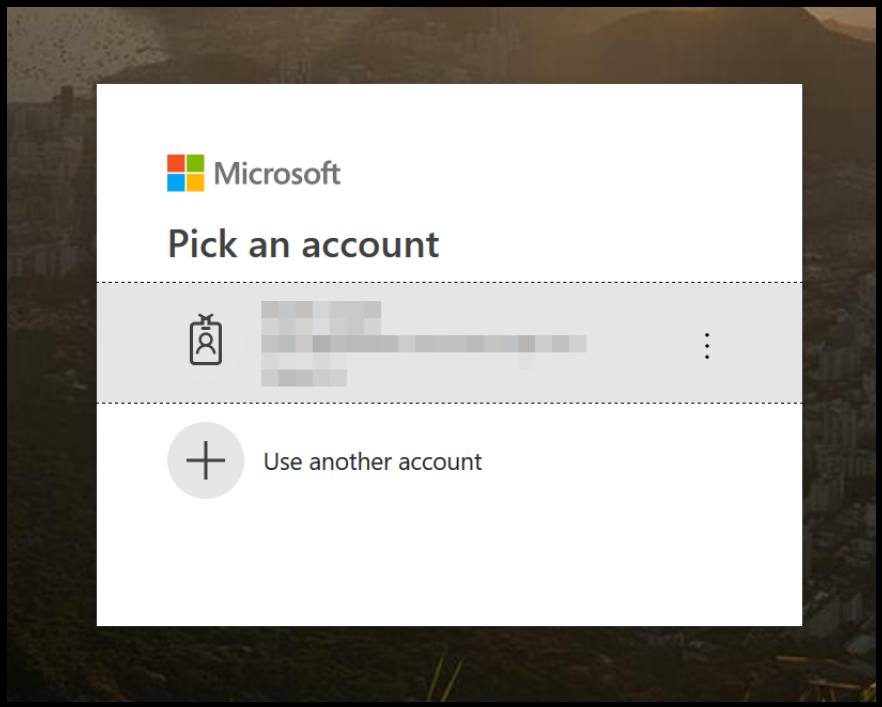


Figure 110: Microsoft login

7. Enter your password.
8. Click on **Accept** to accept the permissions.

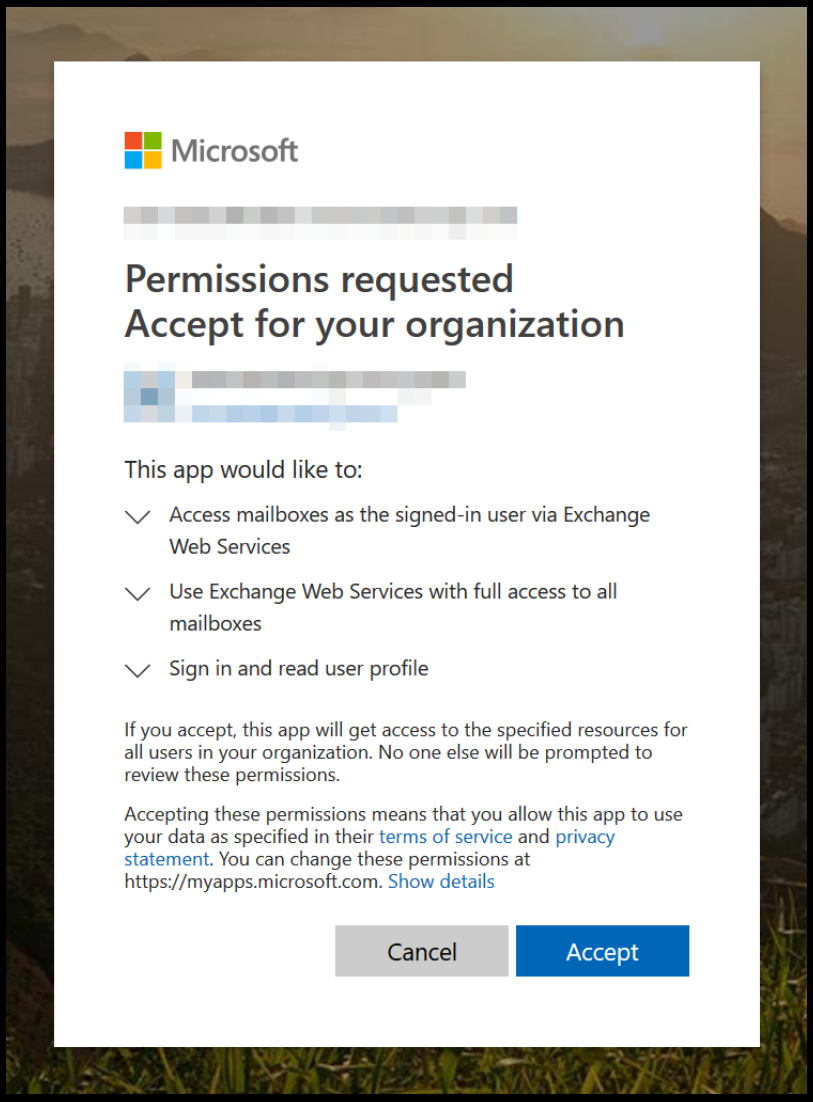


Figure 111: Accept permissions

365 Total Encryption has been activated for the selected domain.

Filtering mailboxes by status

You have the possibility to filter the created mailboxes according to their status.

You have activated 365 Total Encryption.

1. Log in to the Control Panel with your administrative credentials.
2. Navigate to **365 Total Protection → 365 Total Encryption**.

3. Click on **Status**.

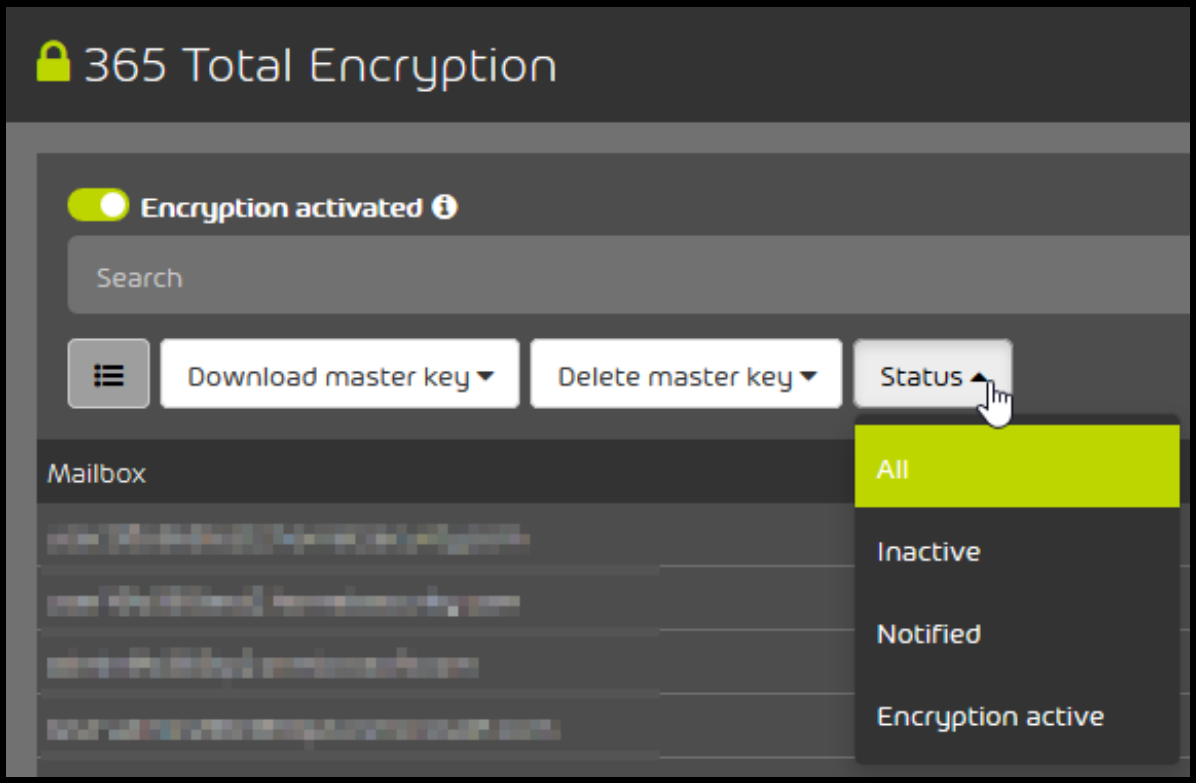


Figure 112: Select a status

4. From the drop-down menu, select the status by which you want to filter the mailboxes.
   Only the mailboxes with the selected status are displayed in the list below.

Activating the Mailbox Encryption

You can activate the mailbox encryption.

You have activated 365 Total Encryption.

1. Log in to the Control Panel with your administrative credentials.
2. Click on the menu button .

Figure 113: Select menu button

3. Select the mailboxes which you want to encrypt.
   - In order to encrypt all mailboxes under the domain, click on **Encrypt all mailboxes**.

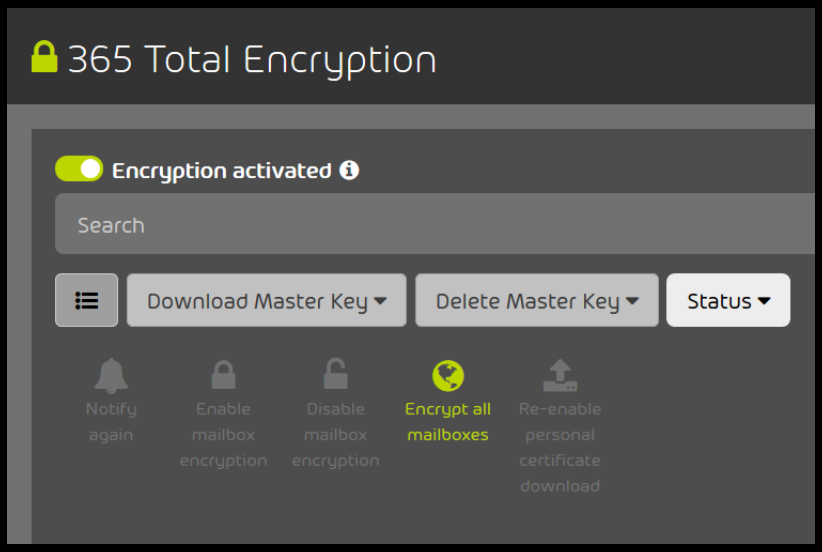


Figure 114: Activate encryption for all mailboxes

   - In order to encrypt individual mailboxes, mark the checkboxes in front of the desired mailboxes in the list below and click on **Enable mailbox encryption**.

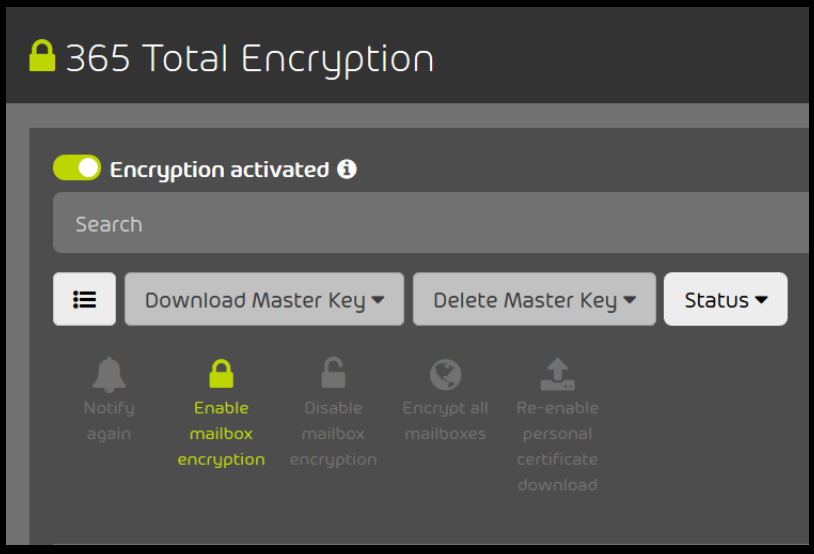


Figure 115: Activate encryption for all mailboxes

The mailbox encryption has been activated and the users receive emails with instructions for the configuration. The status of the mailboxes changes from **Inactive** to **Notified**. Once the users have successfully finished the configuration, the status of the mailboxes changes to **Active**.

Notifying users again

If the status of a mailbox for which encryption has been enabled, is still **Notified** after a long period of time, you can notify the user again.

You have activated 365 Total Encryption. You have activated the mailbox encryption for a mailbox. The status of the mailbox is **Notified**.

1. Log in to the Control Panel with your administrative credentials.
2. Navigate to **365 Total Protection → 365 Total Encryption**.
3. Click on the menu button .
4. In the list below, mark the checkbox next to the mailbox whose user you want to notify again.
5. Click on **Notify Again**.

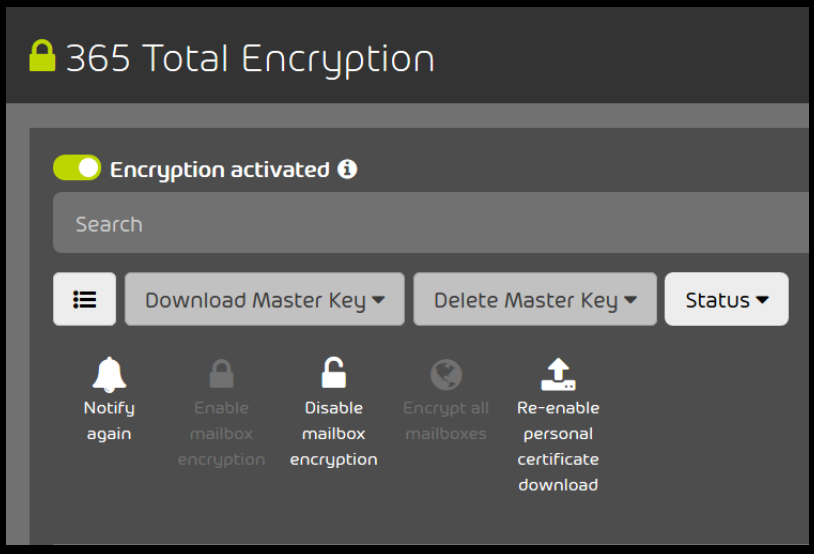


Figure 116: Notifying users again

The user receives a new email with configuration instructions.

Deactivating the Mailbox Encryption

You can deactivate the mailbox encryption.

You have activated 365 Total Encryption. You have activated the mailbox encryption.

1. Log in to the Control Panel with your administrative credentials.
2. Navigate to **365 Total Protection → 365 Total Encryption**.
3. Click on the menu button .
4. In the list below, activate the checkbox in front of the mailbox for which you want to deactivate the encryption.
5. Click on **Disable mailbox encryption**.

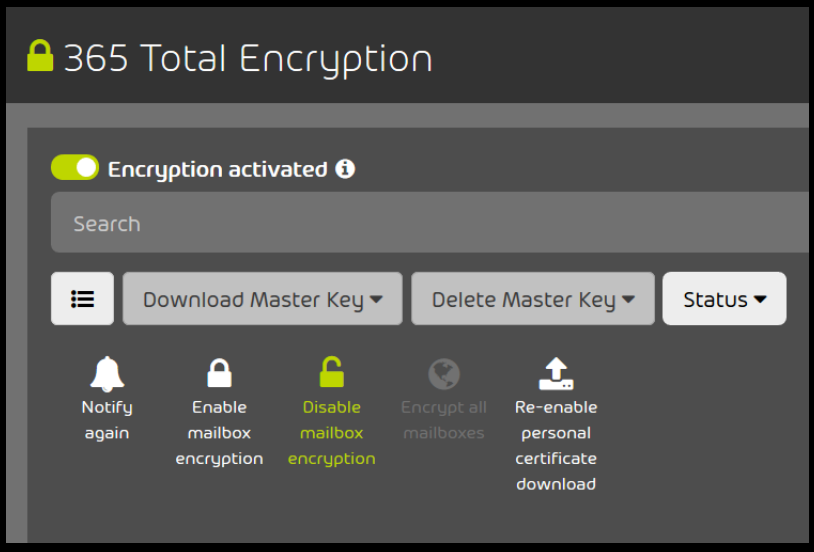


Figure 117: Deactivating the mailbox encryption

The mailbox encryption is deactivated for future sent and received emails.

Important:

Already received or sent emails remain encrypted.

Configuration as User

Installing the Personal Certificate

Download your personal certificate to obtain access to the encrypted emails in your mailbox.

Your administrator has activated 365 Total Encryption, and you have been informed by email.

1. Log in to the Control Panel with your user data.
2. Navigate to **365 Total Protection**#→**Personal Certificate Download**.
3. Select whether you want to receive your one-time password by email or SMS.

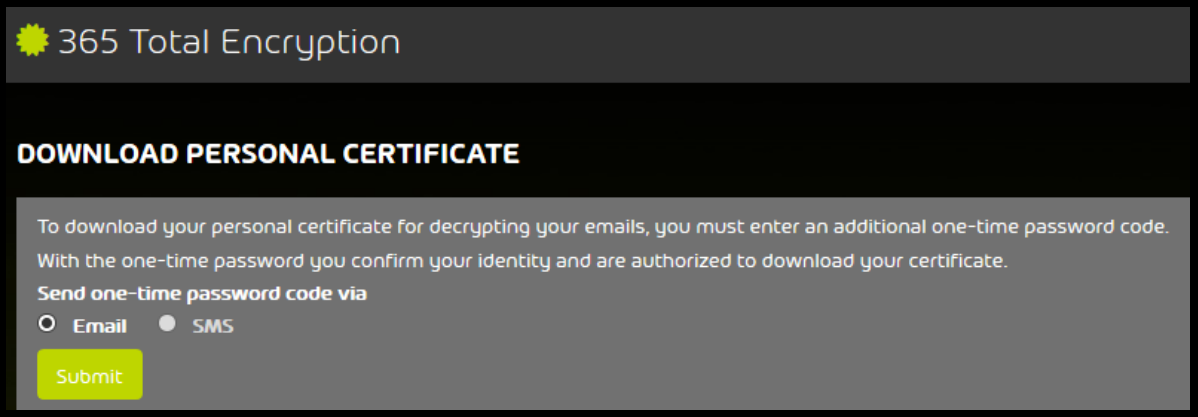


Figure 118: Select the delivery option

4. Define a passphrase for your personal certificate and repeat it.

> **Notice:**
>
> The passphrase is needed to install the downloaded certificate on your computer.

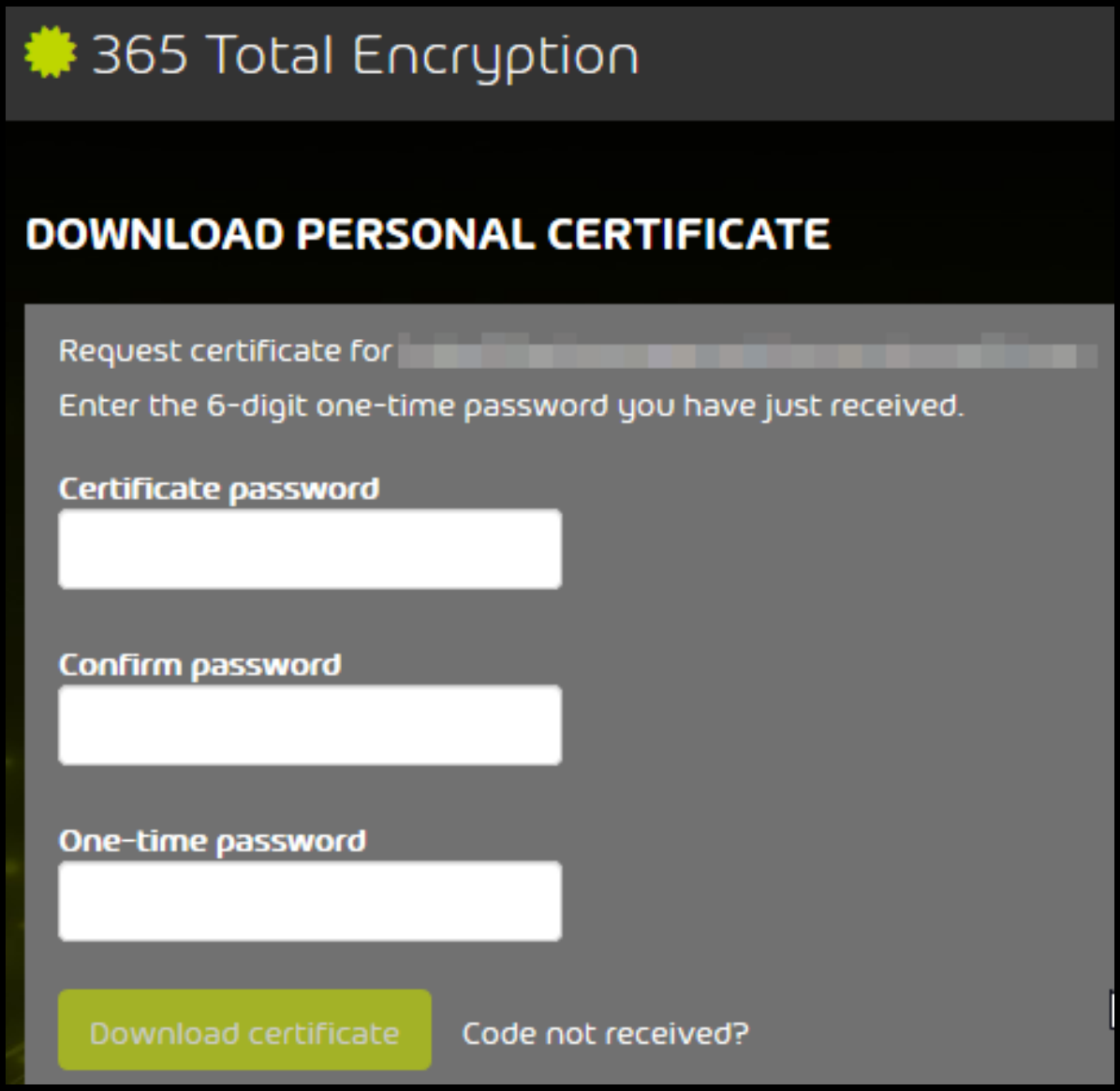


Figure 119: Enter the passphrase

5. Enter the one-time password which you have received by email or SMS in the **One-time password** field.
6. Click on **Download certificate**.

Your personal certificate is downloaded in .p12 format.

Install your personal certificate (see Installation of the Personal Certificate on page 113).

Installation of the Personal Certificate

After the download, install your personal certificate on your devices.

> **Important:**
>
> Install your personal certificate on all devices before activating the encryption for your mailbox.

- If you use Windows as your operating system, please follow the instructions under Importing the Certificate in Windows on page 113.
- If you use MacOS as your operating system, please follow the instructions under Importing a Certificate in MacOS on page 119.
- If you use Android as your operating system and Outlook as your email client, please follow the instructions under Opening Encrypted Emails with CipherMail on page 129
- If you use Android as your operating system, you can also use the Nine app. Please follow the instructions under Binding the certificate on Android with Nine on page 131 to set up the Nine app for 365 Total Encryption.
- If you use Android as your operating system and Outlook as your email client, please follow the instructions under Binding the Certificate on iOS with Outlook on page 142.

Importing the Certificate in Windows

1. Double-click on the downloaded certificate under **Downloads** in your browser or in your file system.
2. Under **Store Location**, select **Current user**.

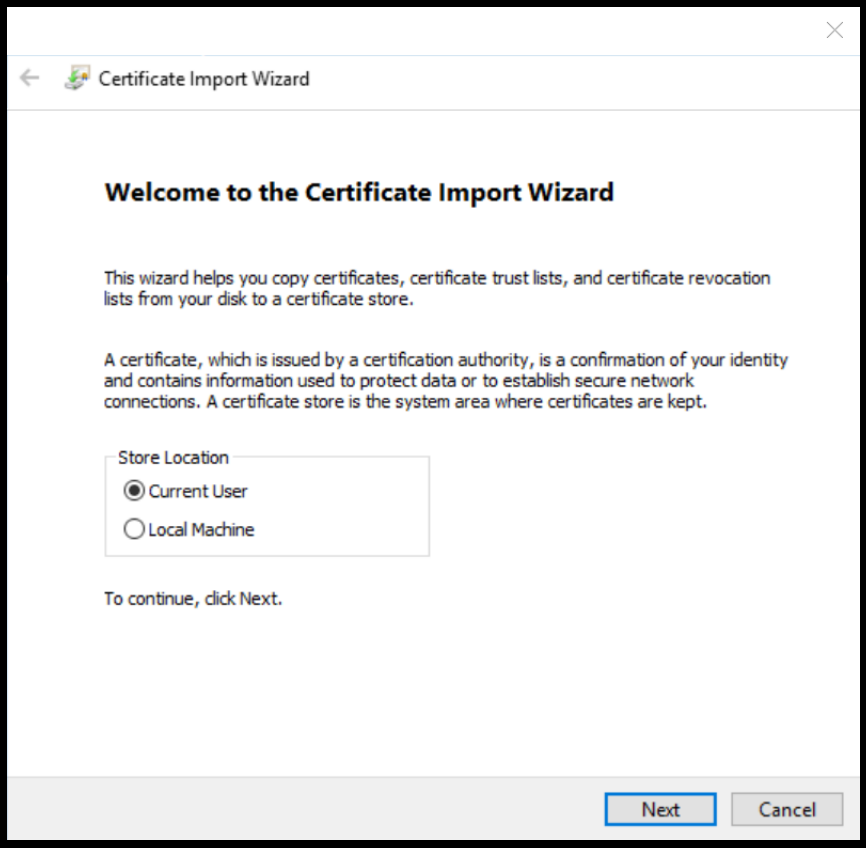


Figure 120: Select store location

3. Click on **Next**.
4. Select the downloaded certificate under **File name**.

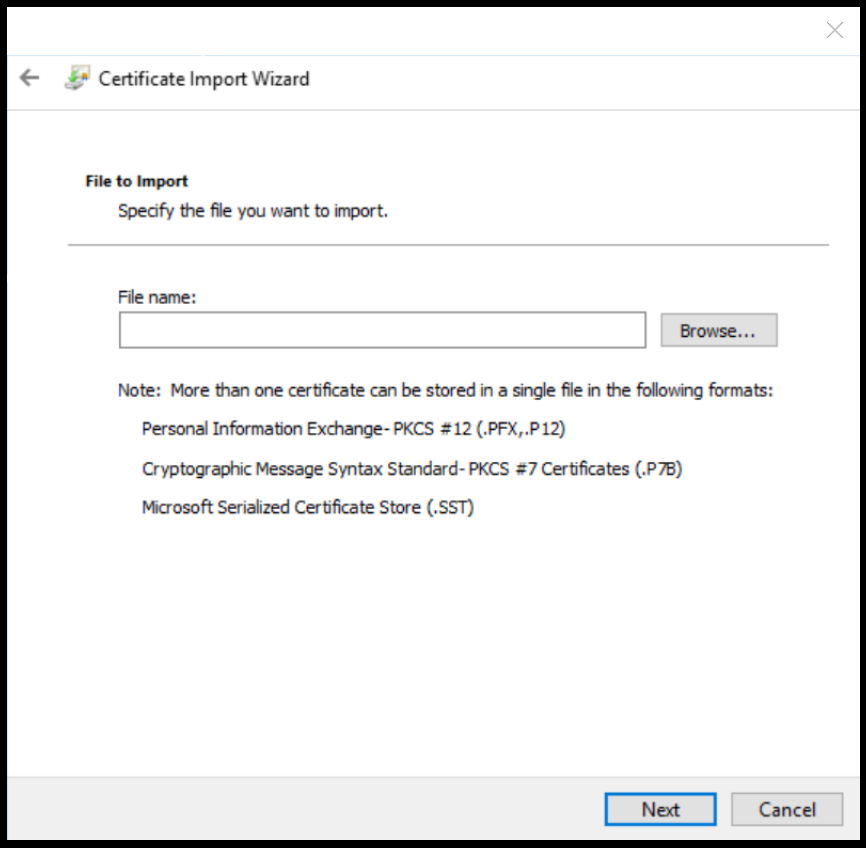


Figure 121: Select downloaded certificate

5. Click on **Next**.
6. In the field **Password**, enter the personal certificate passphrase which you defined in the previous section.
7. Do not change the settings under **Import options**.

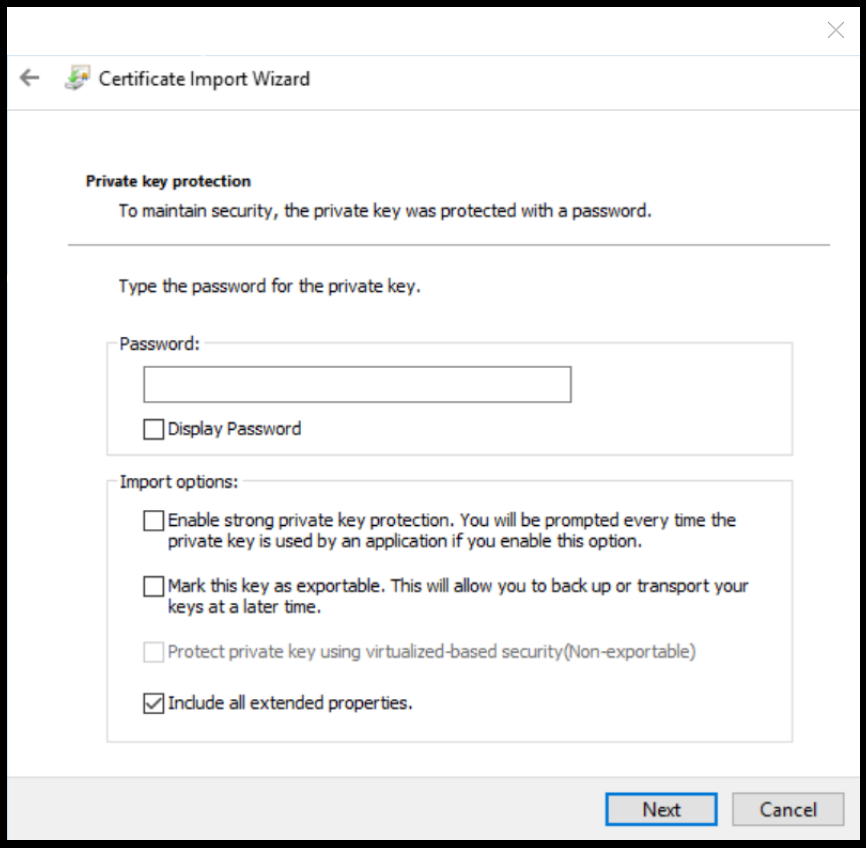


Figure 122: Enter passphrase and select import options

8. Click on **Next**.
9. Select where the certificate should be stored. We recommend the settings shown in the screenshot.

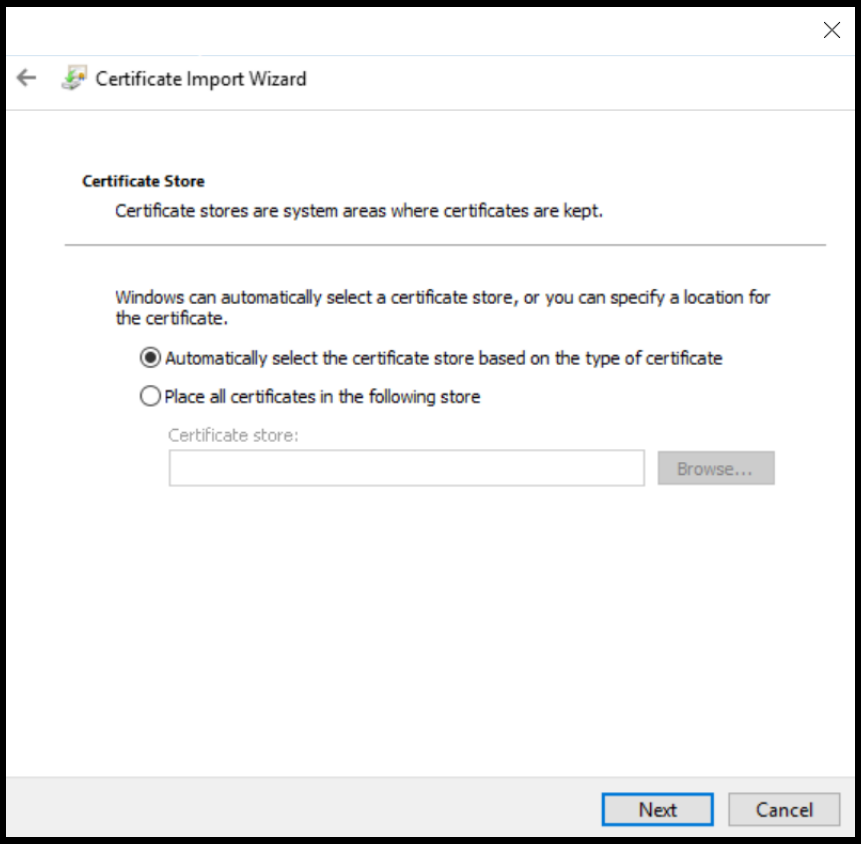


Figure 123: Select certificate store

10. Click on **Next**.

    A window with an overview of the settings appears.

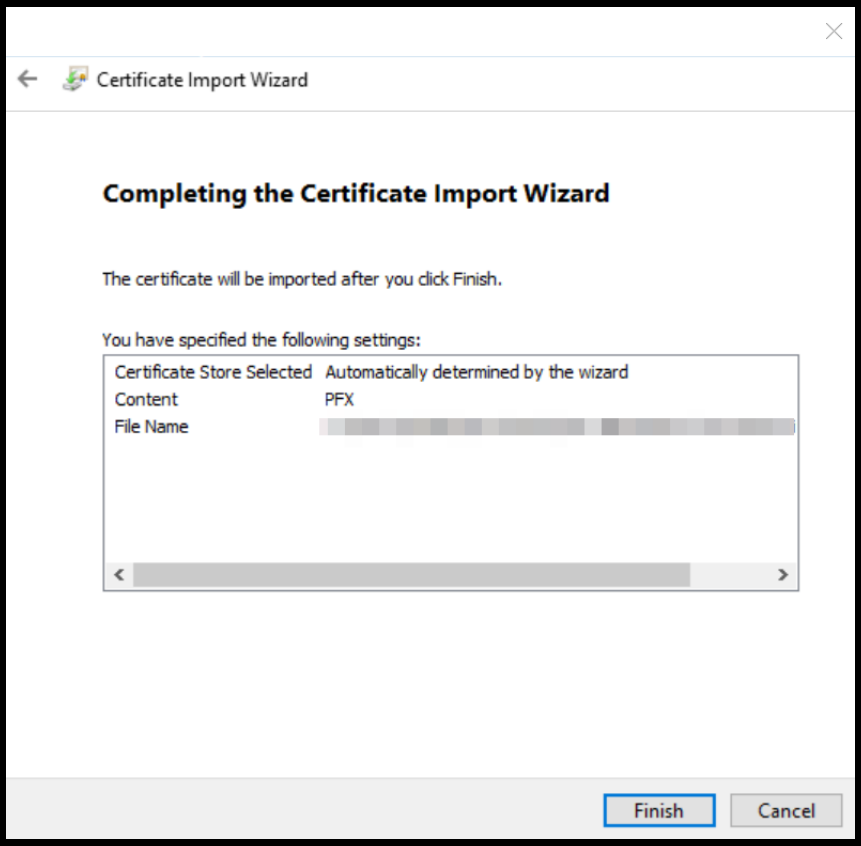


Figure 124: Settings overview

11. Click on **Finish**.

    Your personal certificate is installed on your computer.

> **Important:** The certificate is imported automatically only by the default Windows email client. If you are using another email client, please import the certificate manually according to the instructions of your email client.

> **Important:** In order to be able to read your e-mails on all your devices, you must install your personal certificate on every one of them. The supported operating systems and associated installation options can be found under Installation of the Personal Certificate on page 113.

Once you have installed your personal certificate on all your devices, follow the steps in Opening the Encrypted Email on page 146.

Importing a Certificate in MacOS

1. Click on the downloaded certificate under **Downloads** in your browser or in your file system.
2. Click on **Add** in the next window.

Figure 125: Adding a certificate

3. In the field **Password**, enter the passphrase to your personal certificate, which you created in Installing the Personal Certificate on page 110.

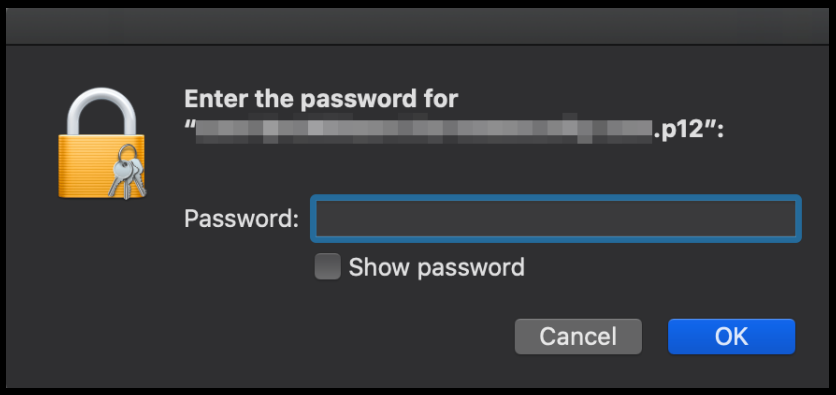


Figure 126: Enter the passphrase

4. Click on **OK**.

   Your personal certificate is stored under **Keychains**, in the category **Certificates**.

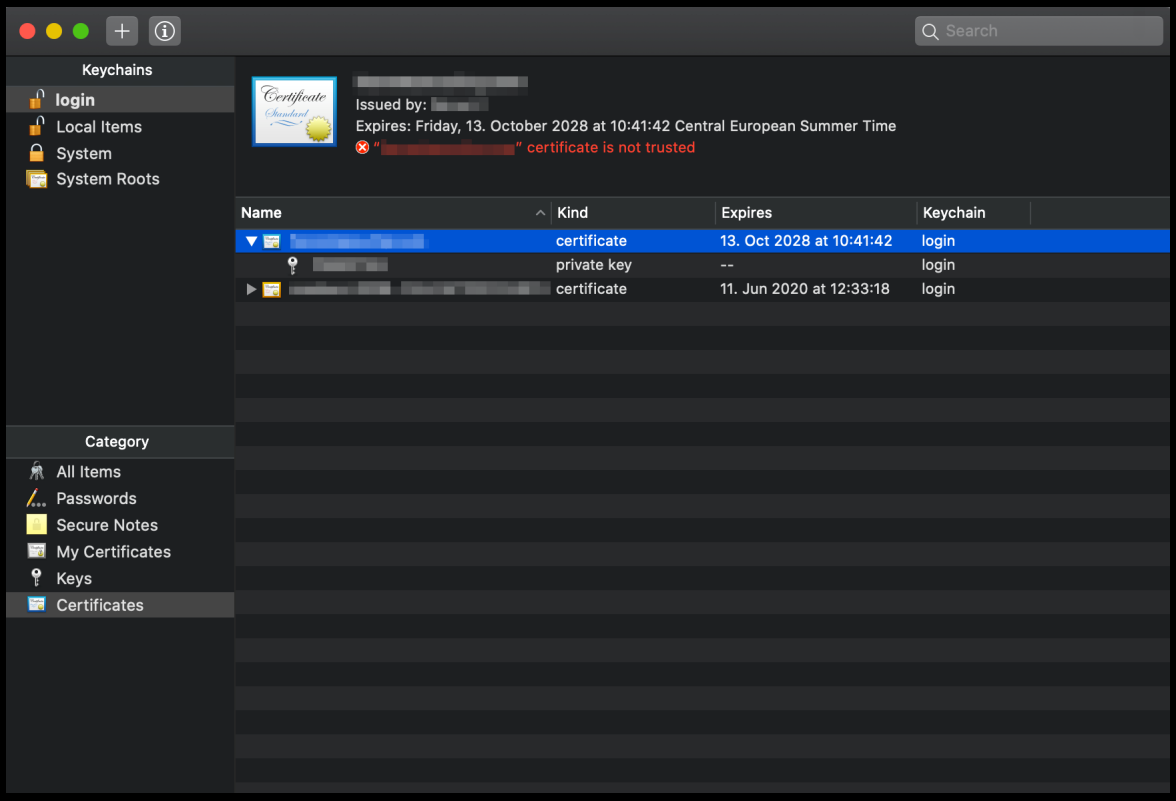


Figure 127: Certificate under Keychains

Notice:

All certificates which are not provided by Apple are not trusted by default.

5. Double-click on the certificate.
6. Open the tab **Trust** and select the option **Always trust** under **When using this certificate**.

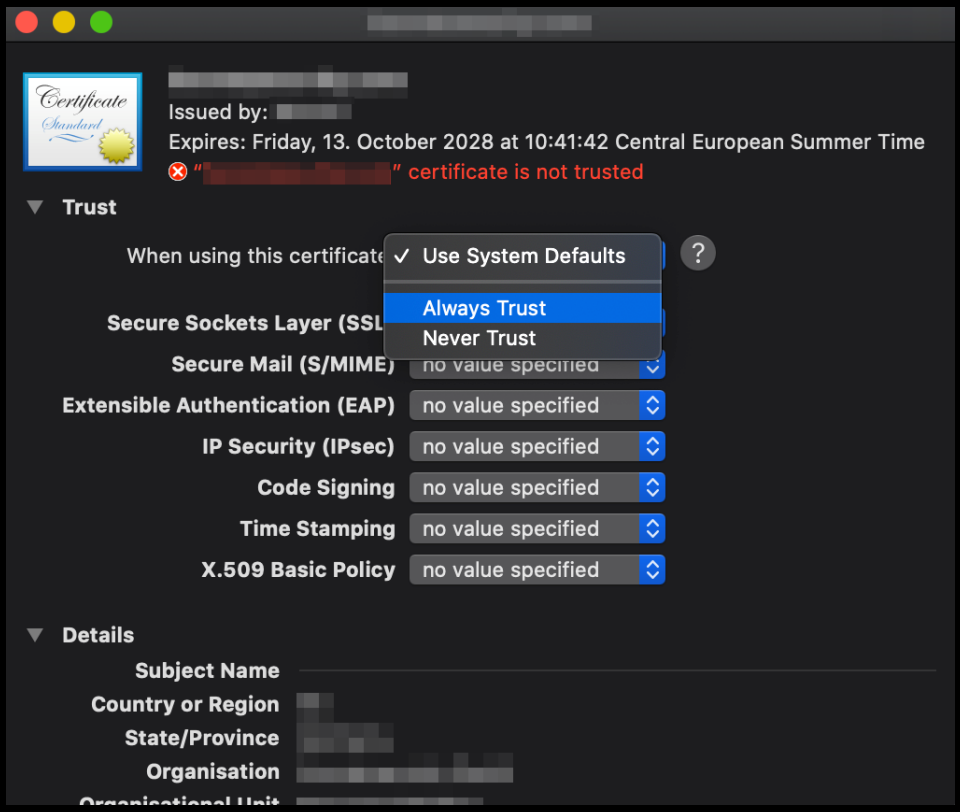


Figure 128: Always trust certificate

7. Enter your administrative password and click on **Update settings**.

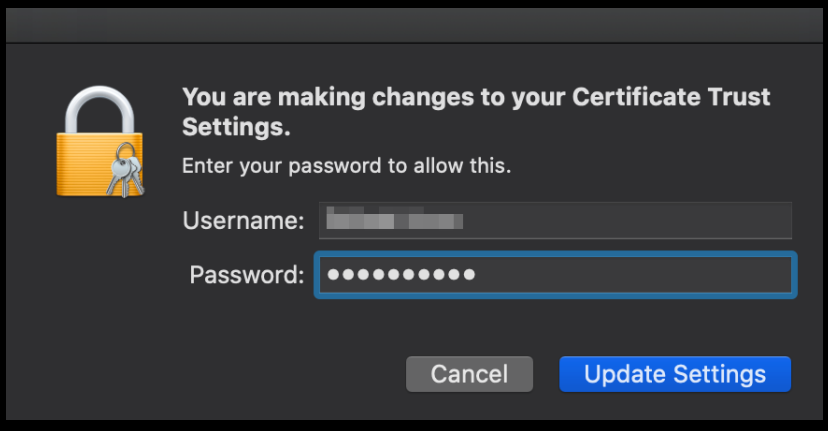


Figure 129: Enter administrative password

The certificate is marked as trustworthy.

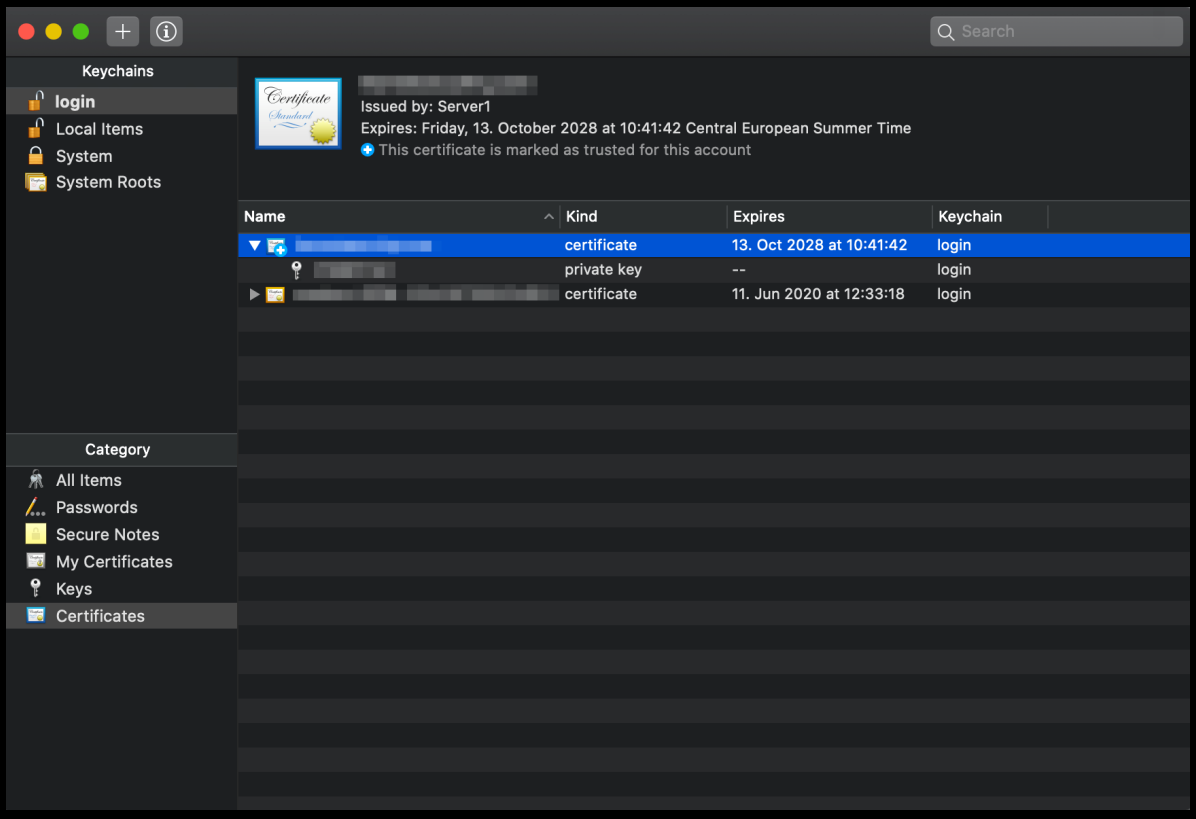


Figure 130: Trusted certificate

Important:

Your personal certificate is imported automatically only by the default iOS mail client. If you are using another email client, please import the certificate manually according to the instructions of your email client.

Important: In order to be able to read your e-mails on all your devices, you must install your personal certificate on every one of them. The supported operating systems and associated installation options can be found under Installation of the Personal Certificate on page 113.

Once you have installed your personal certificate on all your devices, follow the steps in Opening the Encrypted Email on page 146.

Binding the certificate on Android with CipherMail

With the additional add CipherMail, you can open and read emails encrypted with 365 Total Encryption from Outlook.

Important:

Under Android, it is not possible to bind your personal certificate directly to Outlook. Therefore, you need to use CipherMail.

Notice:

The following description refers to the English-language user interface of CipherMail 2.1.8. The actual contents of your app may differ.

1. Download the CipherMail app.
2. Start CipherMail.
3. Tap on the return button to abort the installation wizard.

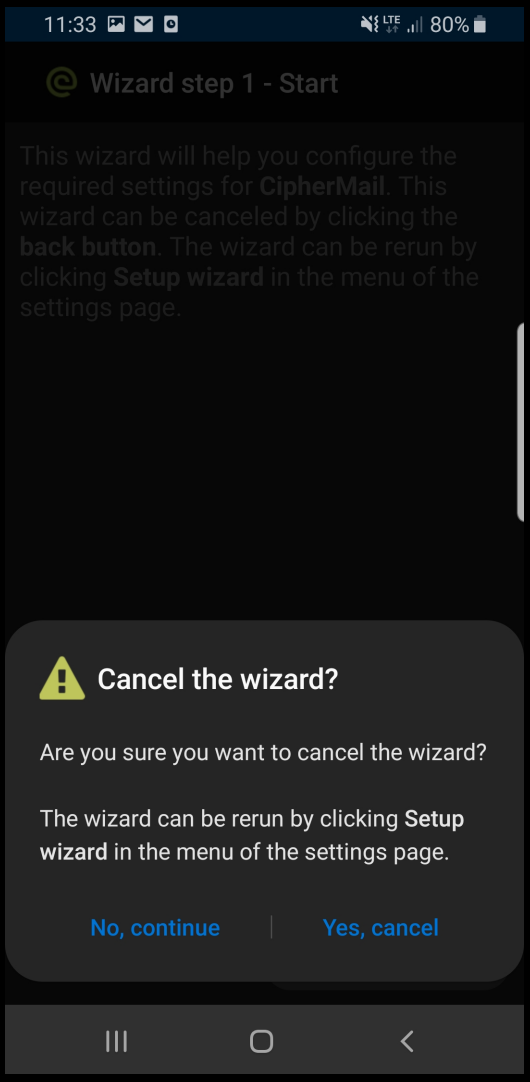


Figure 131: Aborting the installation wizard

4. Tap on **Certificates and Keys**.
5. Tap on the three points on the upper right corner.
6. Tap on **Import keys**.

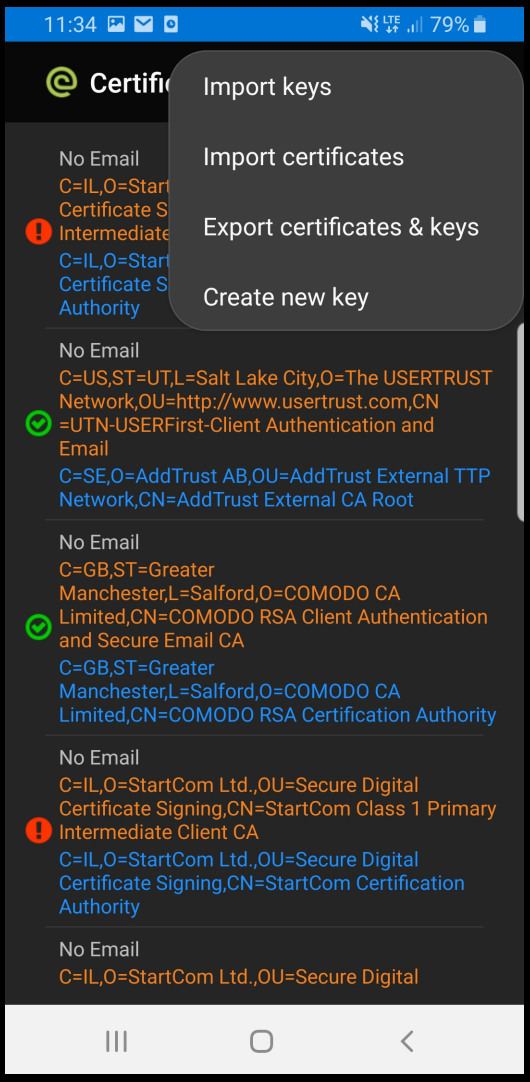


Figure 132: Importing a certificate

7. Tap on **Browse** to select your personal certificate.

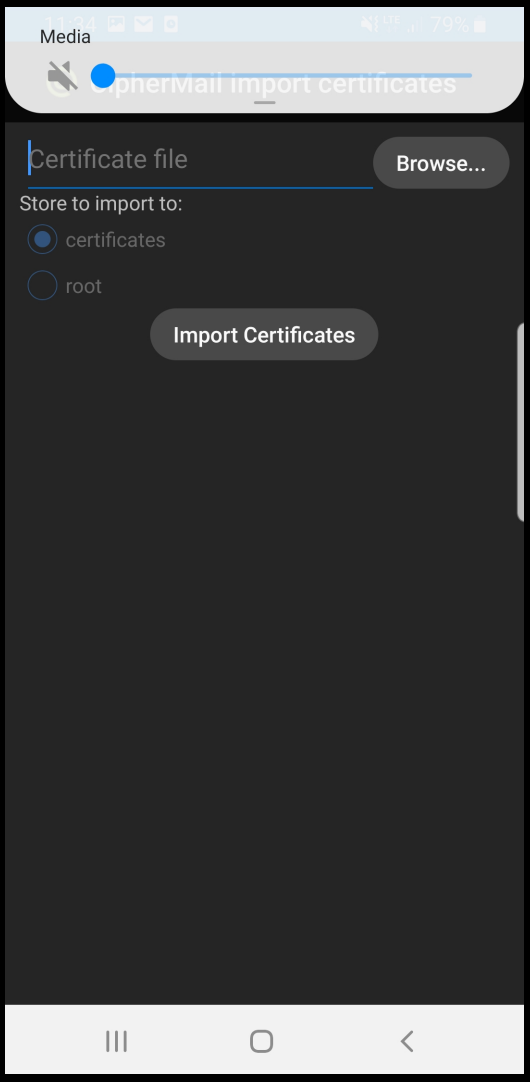


Figure 133: Selecting the certificate

8. After that, tap on **Import Certificates**.
9. Enter the password for your personal certificate in the **Password** field.

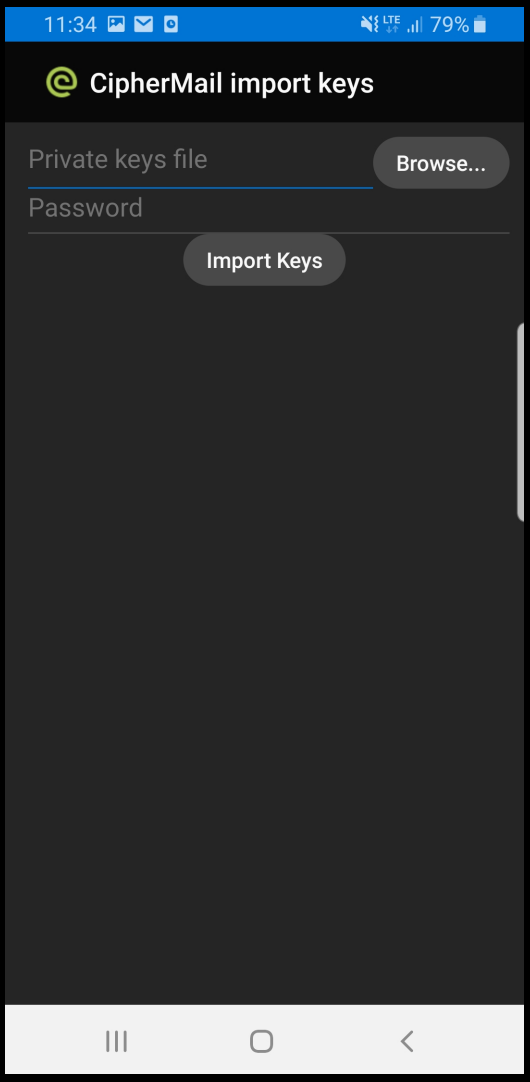


Figure 134: Entering the password

10. Tap on **Import Keys**.

    A request to create a **Key store** will be displayed.

11. Enter your password to the **Key store** in the **New password** field and confirm it in **Password repeat**. Afterwards, tap on **OK**.

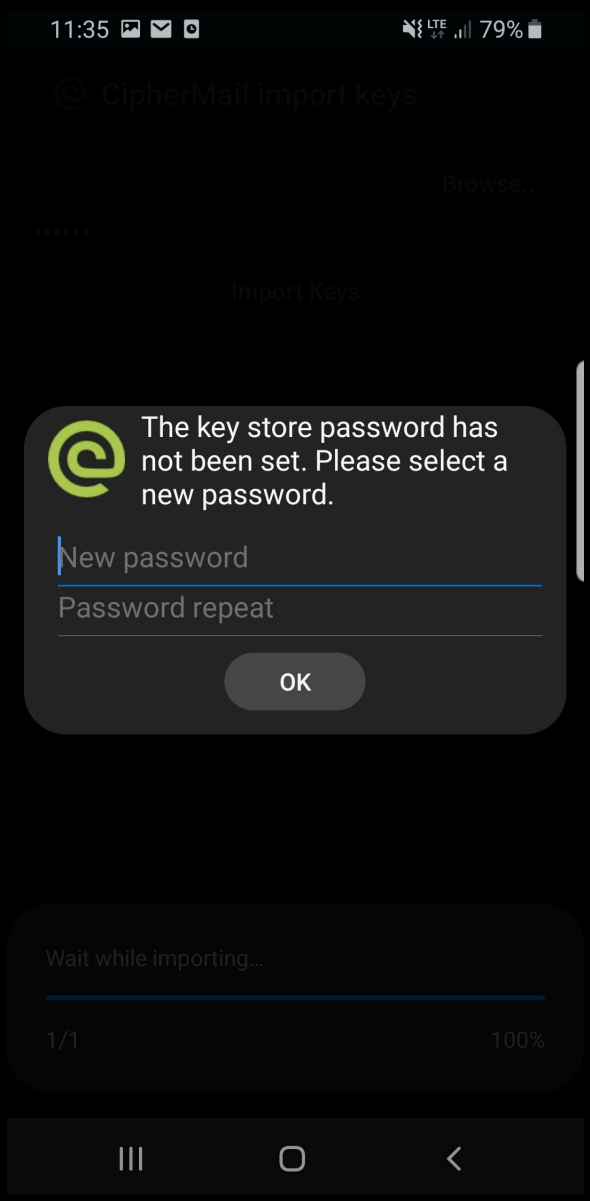


Figure 135: Defining a password for the key store

A notification on the successful installation of your personal certificate will be displayed.

You have stored your personal certificate in CipherMail.

After that, you can open encrypted emails in Outlook with CipherMail to read them.

Opening Encrypted Emails with CipherMail

Decrypt emails with CipherMail from Outlook.

In order to open encrypted emails with CipherMail, you must have stored your personal certificate in CipherMail.

1. **Notice:** The following description refers to the English-language user interfaces of CipherMail 2.1.8 and Outlook 4.0.23. The actual contents of your apps may differ.

   Open the Outlook app.
2. Open an email and tap on **smime.p7m**.

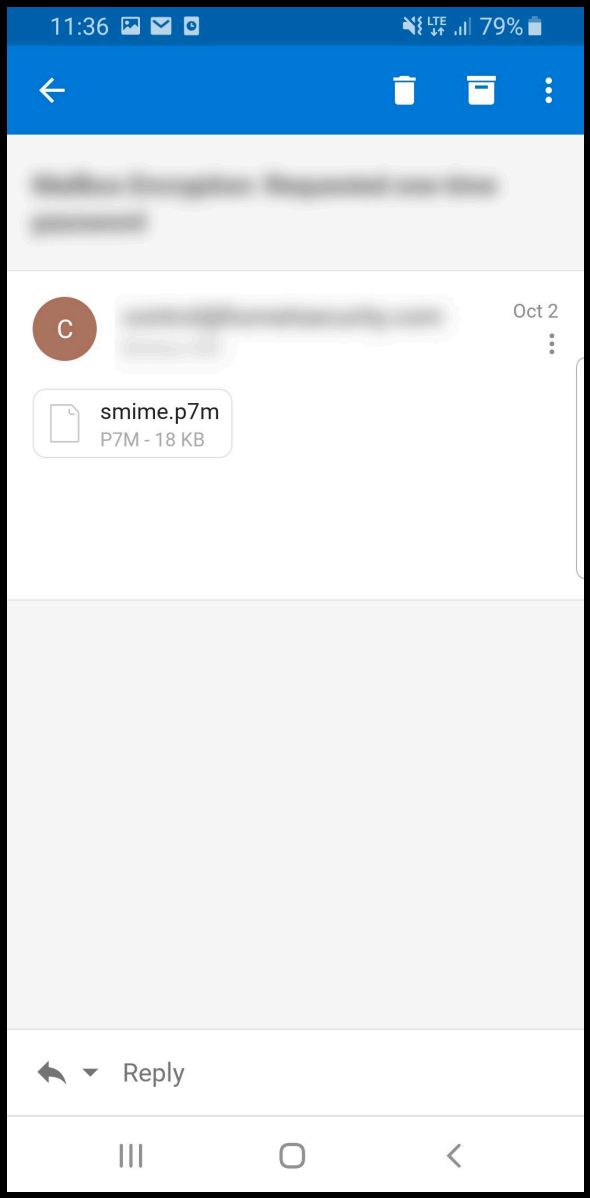


Figure 136: Open encrypted email

3. Afterwards, tap on **Open with CipherMail**.
4. Enter the password to your key store.

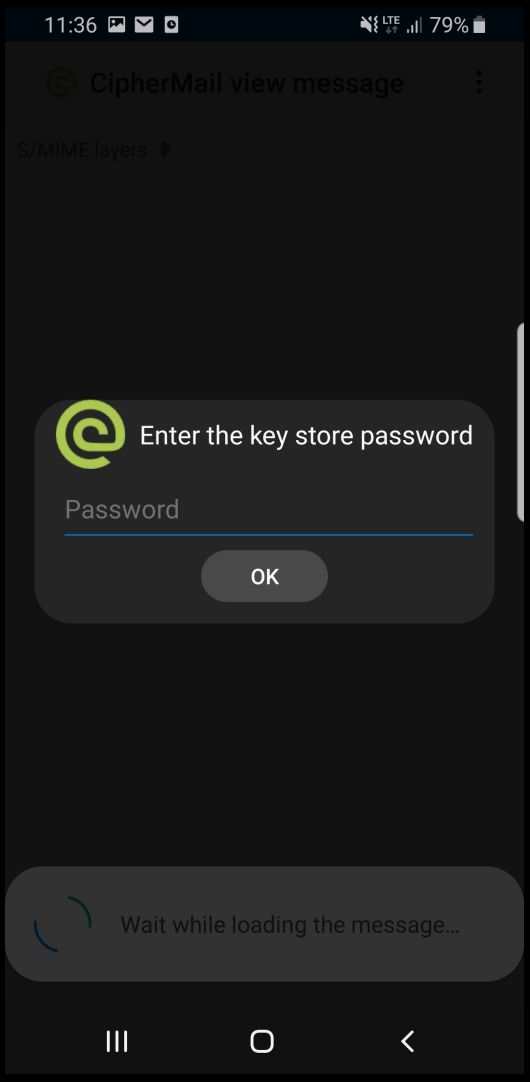


Figure 137: Encrypted email in CipherMail

The decrypted email is now displayed.

Binding the certificate on Android with Nine

With the email client Nine, you can bind your personal certificate to Android and read emails which were encrypted with 365 Total Encryption.

You have downloaded your personal certificate to decrypt your emails and have installed Nine on your Android terminal.

Notice: The following description refers to the English-language user interface of Nine 4.5.9a. The actual contents of your app may differ.

With Nine, you can set up your Microsoft 365 account and store the certificate to decrypt your emails.

1. Start the Nine app.
2. Tap on **Get started**.

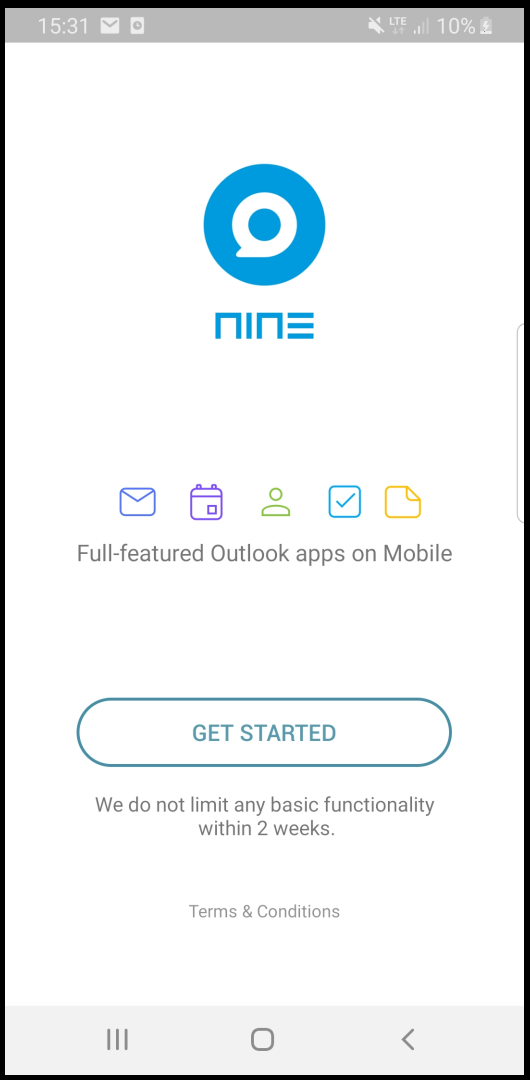


Figure 138: Starting the setup

3. Tap on **Manual setup**.

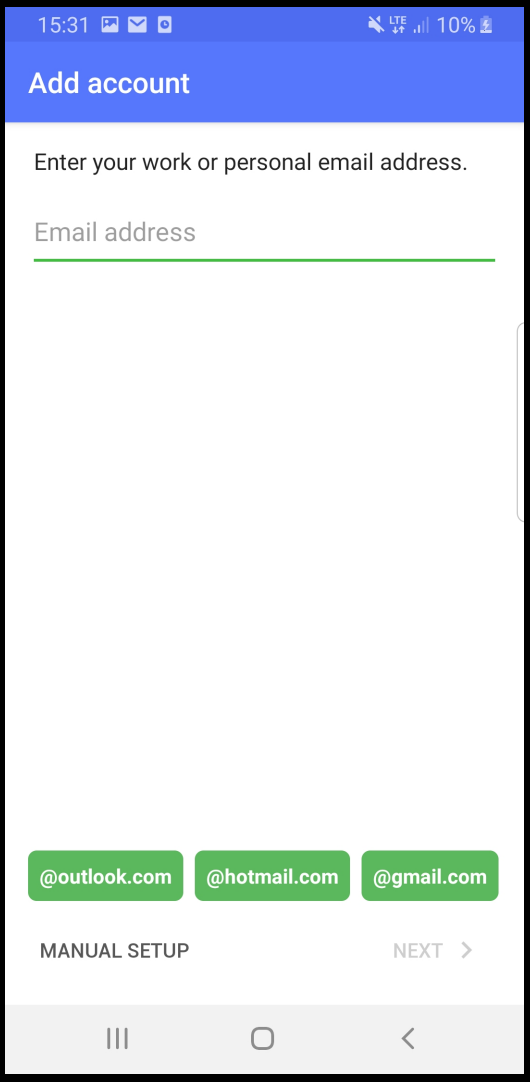


Figure 139: Select manual setup

4. Select **Microsoft 365**.

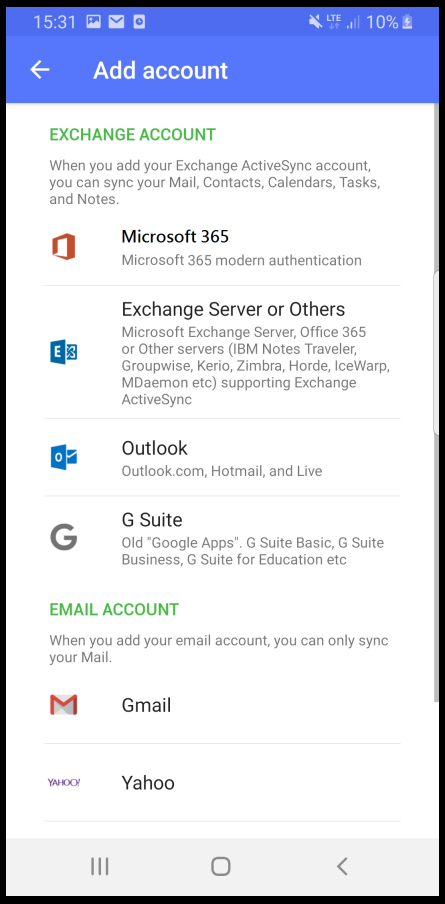


Figure 140: Select Microsoft 365

5. Enter your email address and tap on **Next**.

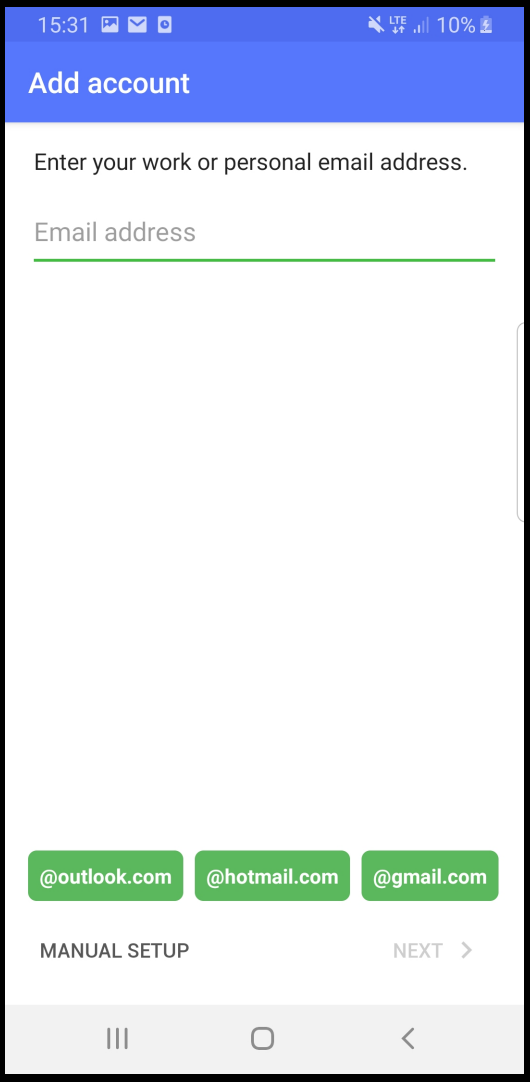
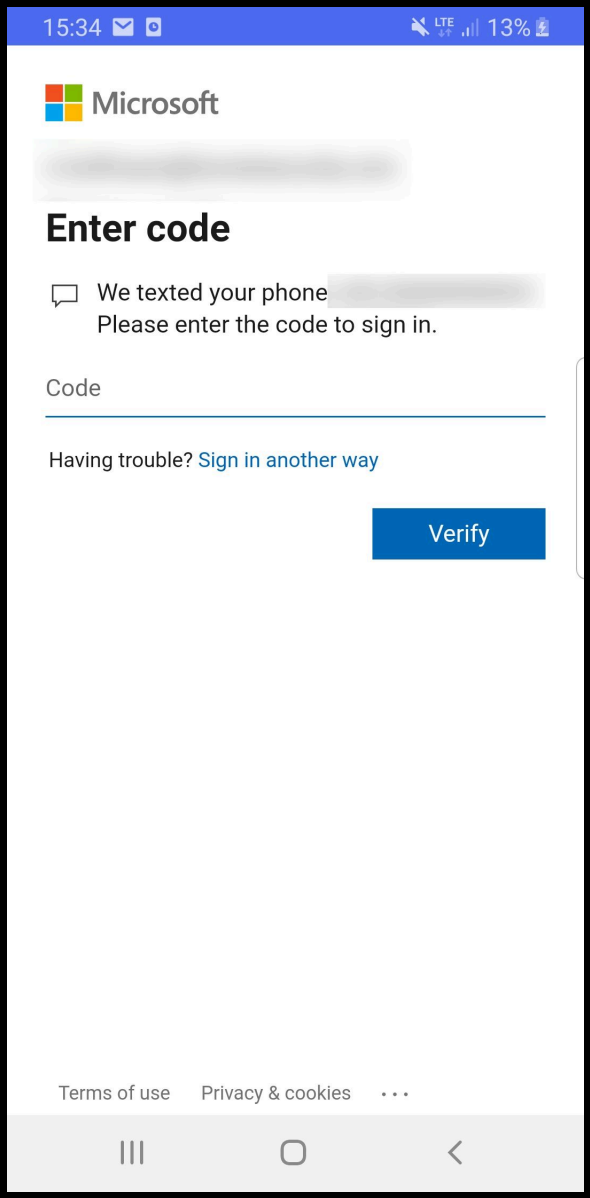


Figure 141: Microsoft Login

6. Enter the password to your email account and tap on **Sign in**.
7. Enter the 2FA code and tap on **Verify**.

2-Factor-Authentication



Your account is added.

8. Keep the settings on the **Content to sync** window and tap on **Next**.

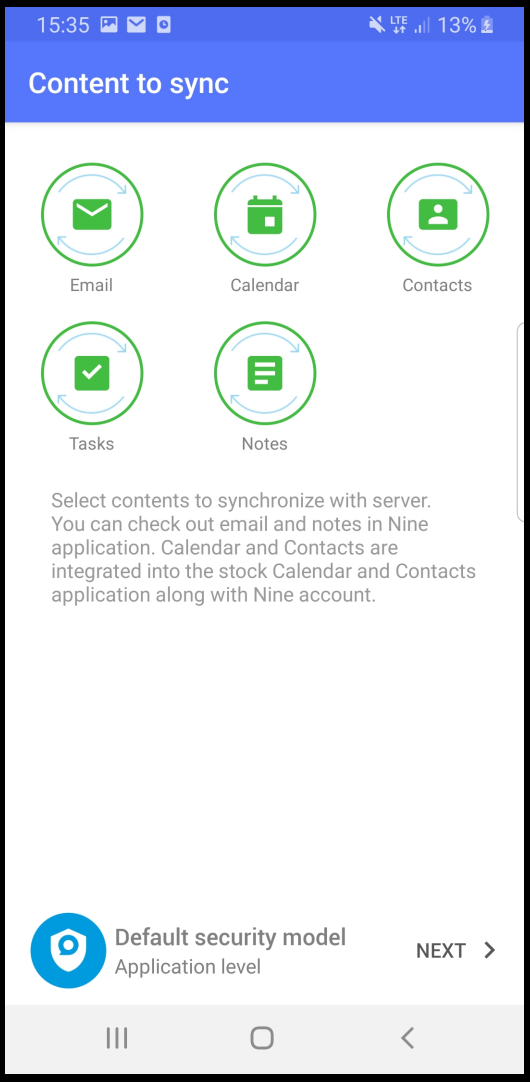


Figure 142: Contents to synchronize

9. On the **Account added** window, tap on **Next**.

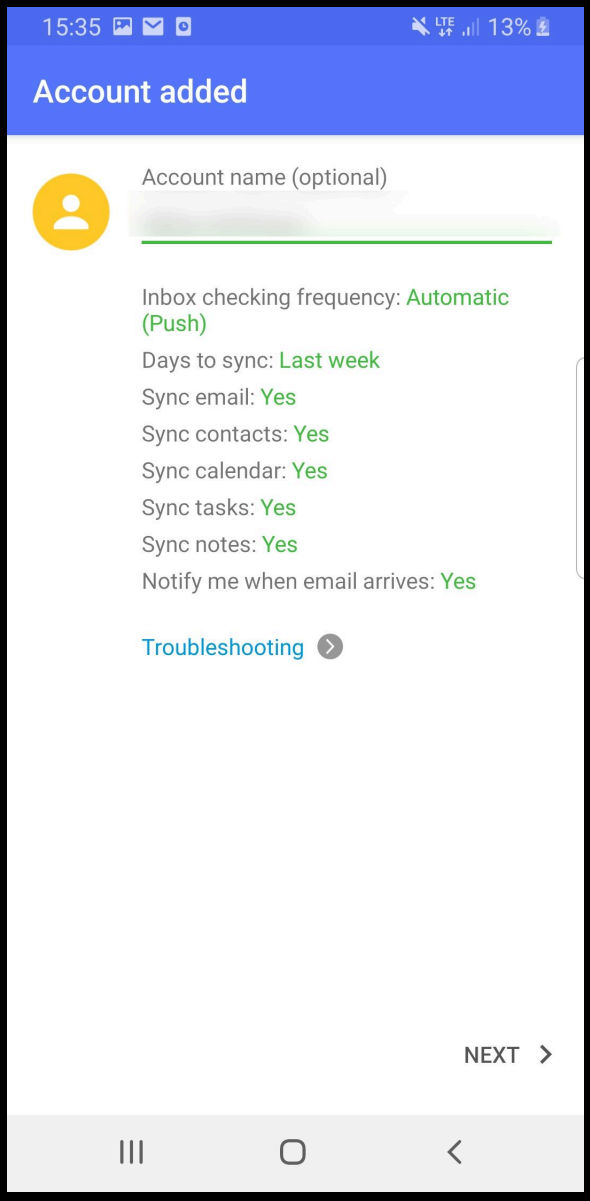


Figure 143: Checking the account

Your mailbox is displayed.

10. On the upper left corner, tap on the menu icon and select the gear wheel icon on the lower right corner.
11. Tap on the newly-added account.

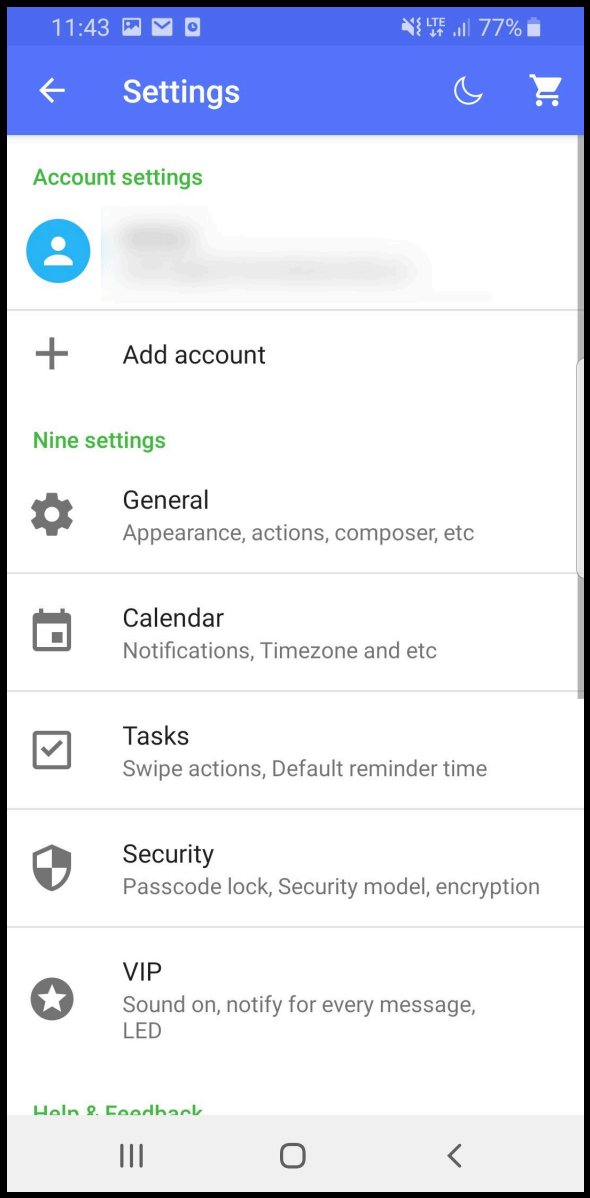


Figure 144: Opening the account settings

12. Tap on **Security**.
13. Tap on the **+** icon next to **Encryption certificate**.

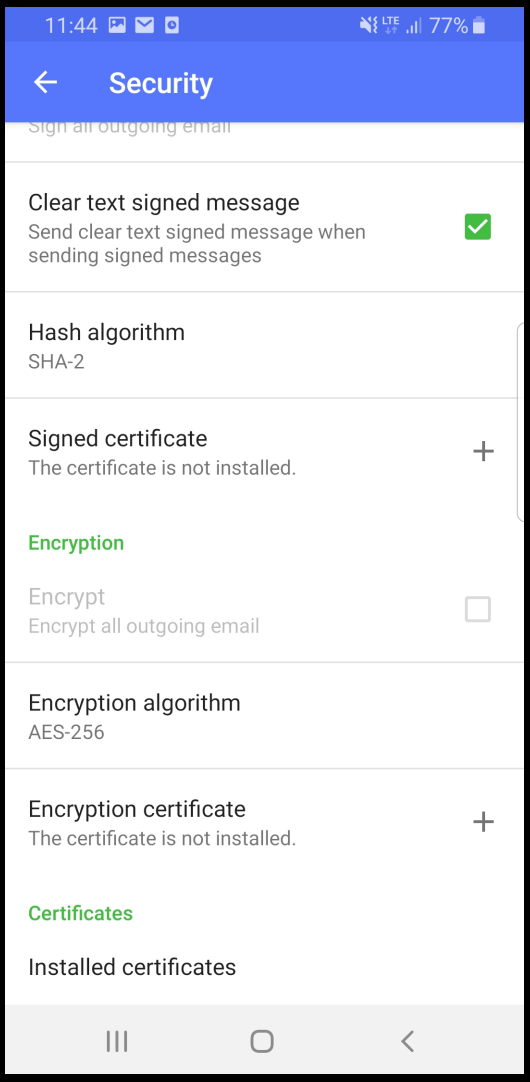


Figure 145: Adding a certificate

➔ If no certificate has been stored yet, a pop-up window will appear.

14. On the pop-up window, tap on **Install** to store your personal certificate.
15. Search for your personal certificate on your file browser and select it.
16. Enter the key password for your personal certificate in the pop-up window and tap on **OK**.
17. Optional: Assign a name to your personal certificate.
18. Tap on **OK**.

    ➔ The installed certificate is selected.
19. Tap on **Allow**.

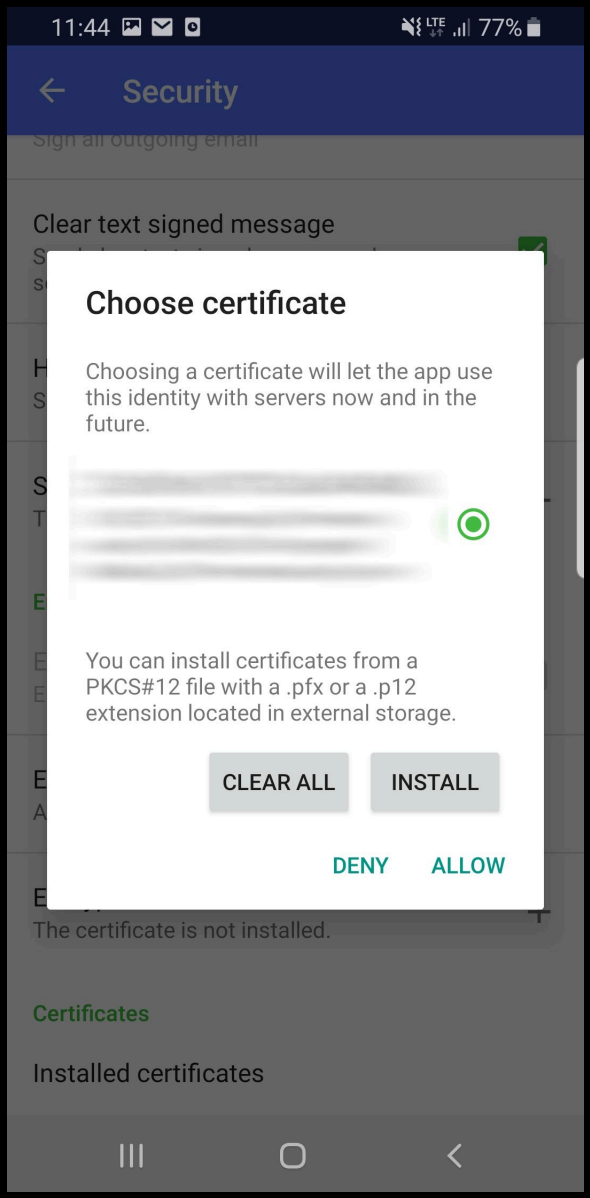


Figure 146: Allowing a certificate

Afterwards, all your emails are decrypted.

Binding the Certificate on iOS with Outlook

If you use iOS and Outlook as your client, you must add the personal certificate to Outlook manually.

Note:

If you have activated 365 Total Encryption before downloading your personal certificate to your mobile device, the emails in your mailbox will already be encrypted and can no longer be read. In this case, follow these instructions: Troubleshooting: Installing the Certificate in Outlook on a Mobile Device with iOS with an Already Encrypted Mailbox on page 147. If your mailbox is not yet encrypted, follow these instructions.

1. Send the certificate which you downloaded in Installing the Personal Certificate on page 110 via email to your own email address.
2. In Outlook on your iOS device, click on the certificate in the email.
3. Click on **Install certificate**.

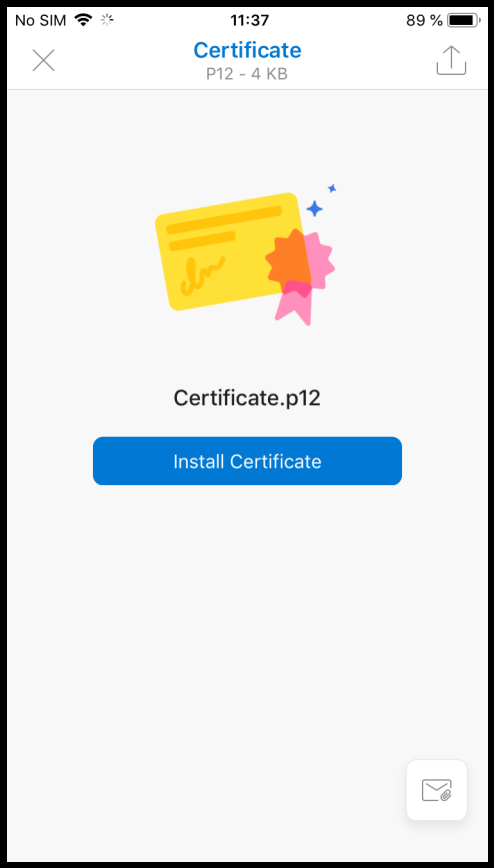


Figure 147: Install certificate

4. Enter the passphrase to your personal certificate and click on **Install**.

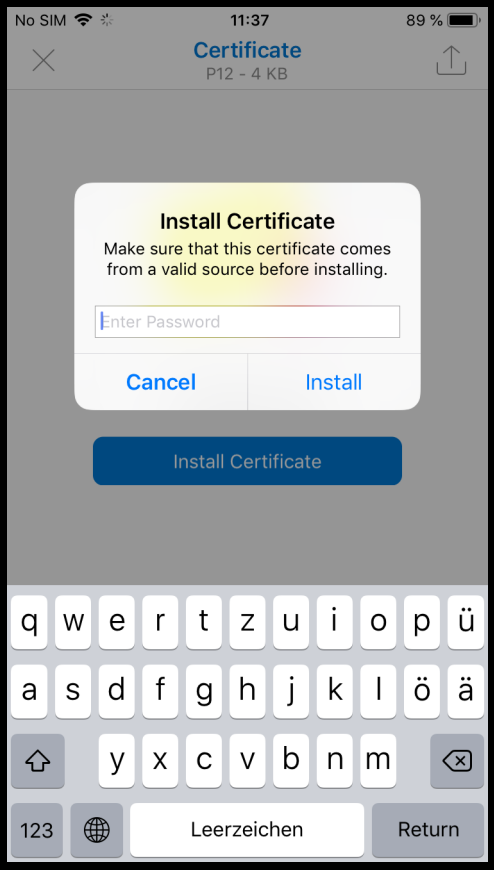


Figure 148: Enter the passphrase

The certificate has been installed.

5. In the next window, click on **Settings**.

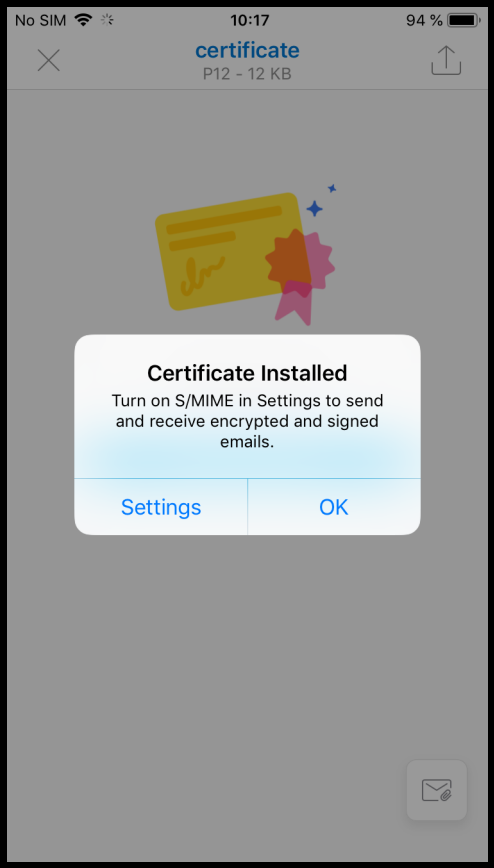


Figure 149: Select Settings

6. Activate S/MIME and click on **OK**.

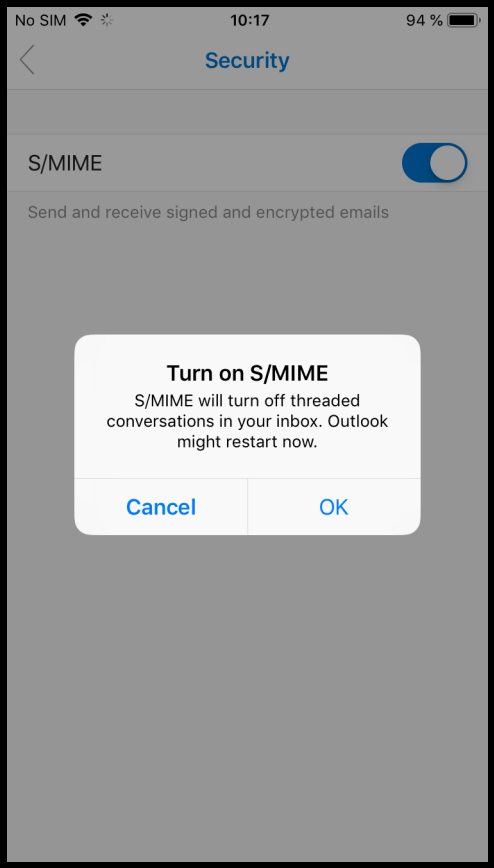


Figure 150: Activate S/MIME

You have installed your personal certificate in Outlook on iOS.

Follow the steps in Opening the Encrypted Email on page 146 to activate the encryption.

Opening the Encrypted Email

Open the encrypted email which you have received and activate 365 Total Encryption for your mailbox.

- You have installed your personal certificate.
- You have received the encrypted email to activate 365 Total Encryption.

1. Open the email with the header **Mailbox Encryption: Activation.**

> **Important:**
>
> You can only read this email if you have installed your personal certificate correctly. If you cannot read the email, this can have several reasons:
>
> - Your email client has not imported your personal certificate automatically. Please import the certificate manually into your email client according to the instructions of the client provider.
> - Your personal certificate has not been properly installed on your operating system. Please reinstall the certificate.
> - The email remains encrypted despite all suggested solutions. Please contact the support.

2. > **Important:** Only click on the activation link after you have installed the certificate for all clients on all devices on which the mailbox is registered.

   Click on the activation link in the email.
3. Restart the email client to activate the encryption of your mailbox.

The activation of 365 Total Encryption for your mailbox has been finished correctly: All already existing and future sent and received email messages are stored encrypted in the Microsoft Cloud. From now on, the emails can only be read with the private certificate.

Troubleshooting: Installing the Certificate in Outlook on a Mobile Device with iOS with an Already Encrypted Mailbox

Issue

You cannot open the email with the attached certificate, and therefore cannot install the your personal certificate on a mobile device with iOS.

Reason

You have already encrypted your mailbox with 365 Total Encryption and cannot read the encrypted emails on your mobile device with iOS.

Solution

1. Open Outlook on the device on which you installed the certificate.

2. On the **Calendar** section, click on **New Appointment**.

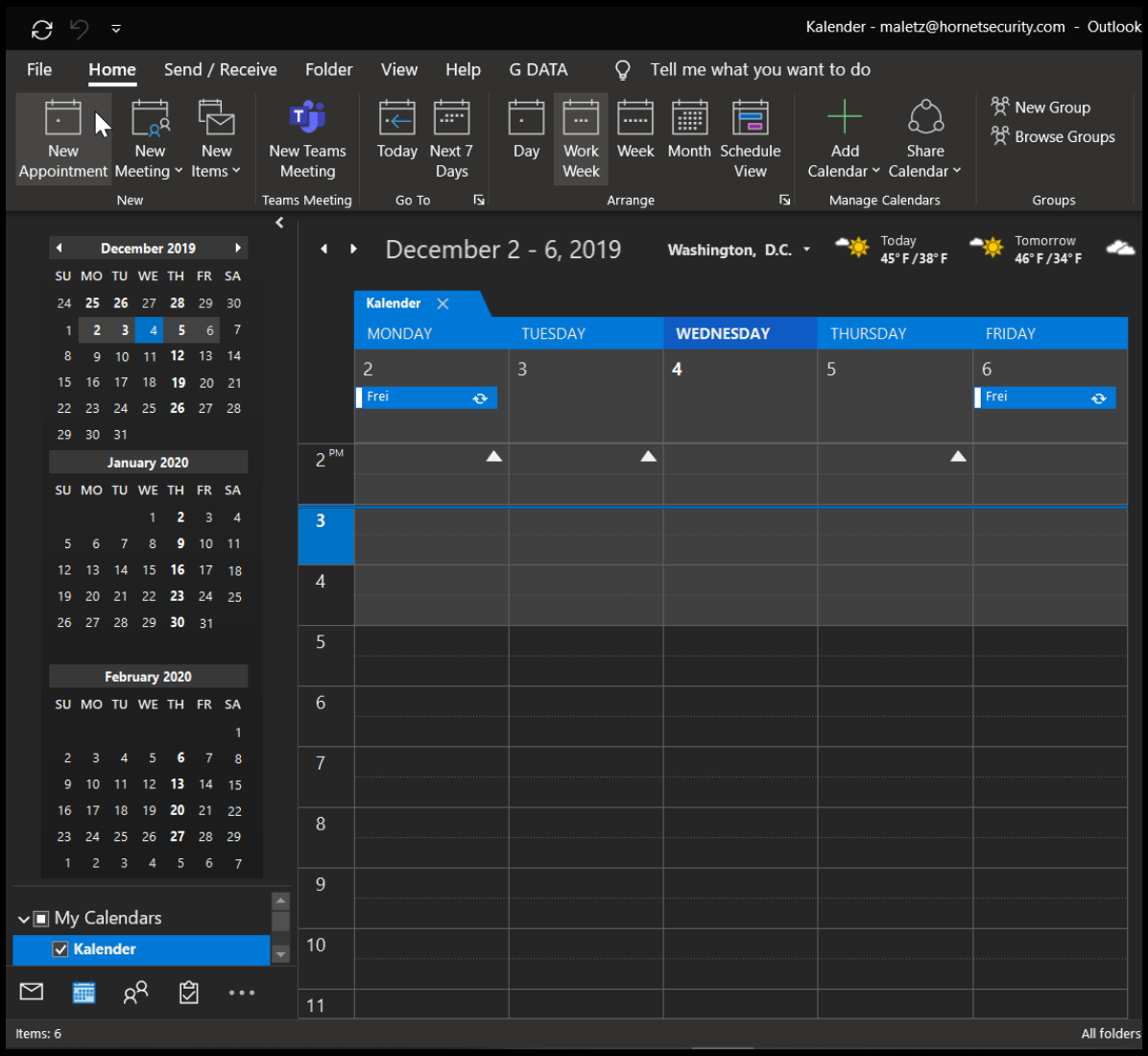


Figure 151: Create New Appointment

3. Enter a title for the appointment in the field **Title**.
4. Click on the tab **Insert**.
5. Click on **Attach File** and select the downloaded certificate.

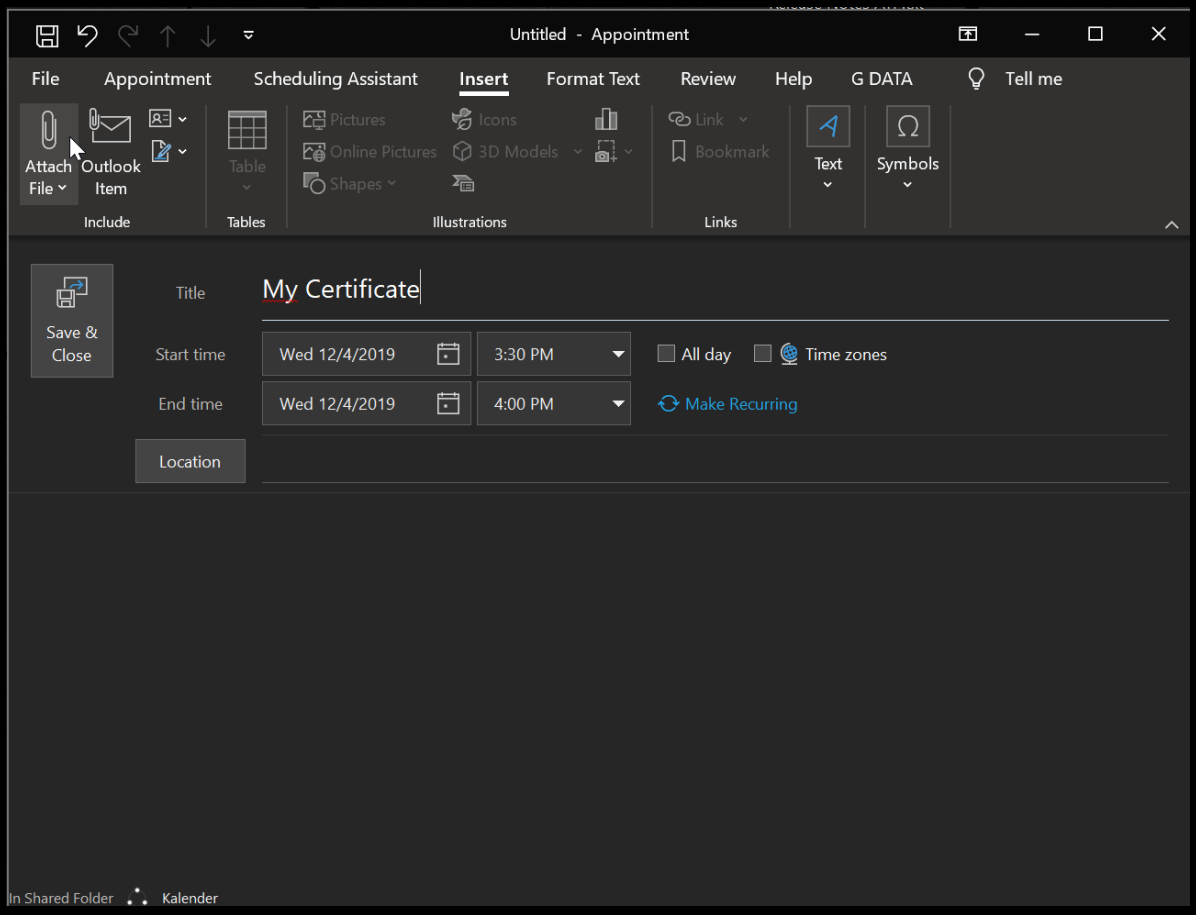


Figure 152: Attach Certificate to Appointment

6. Click on **Save & Close**.

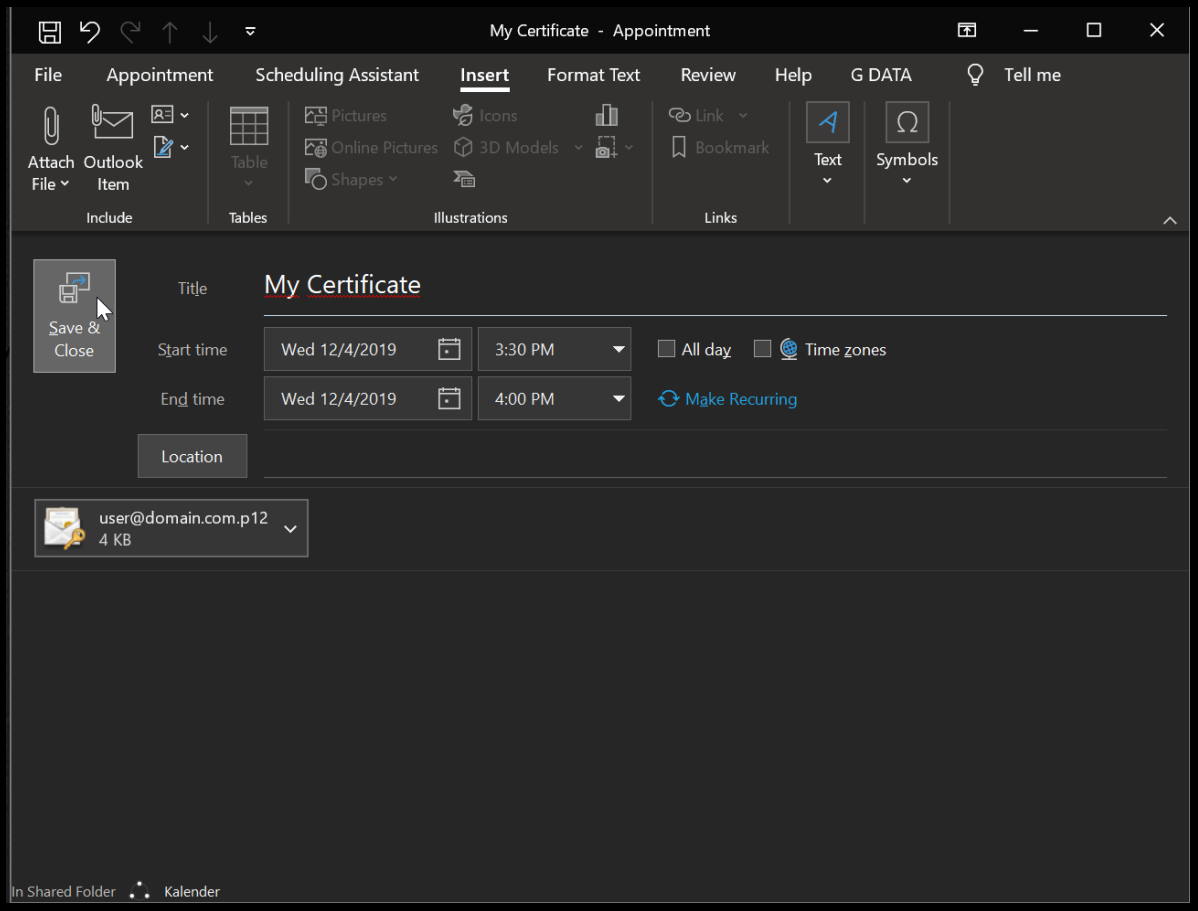
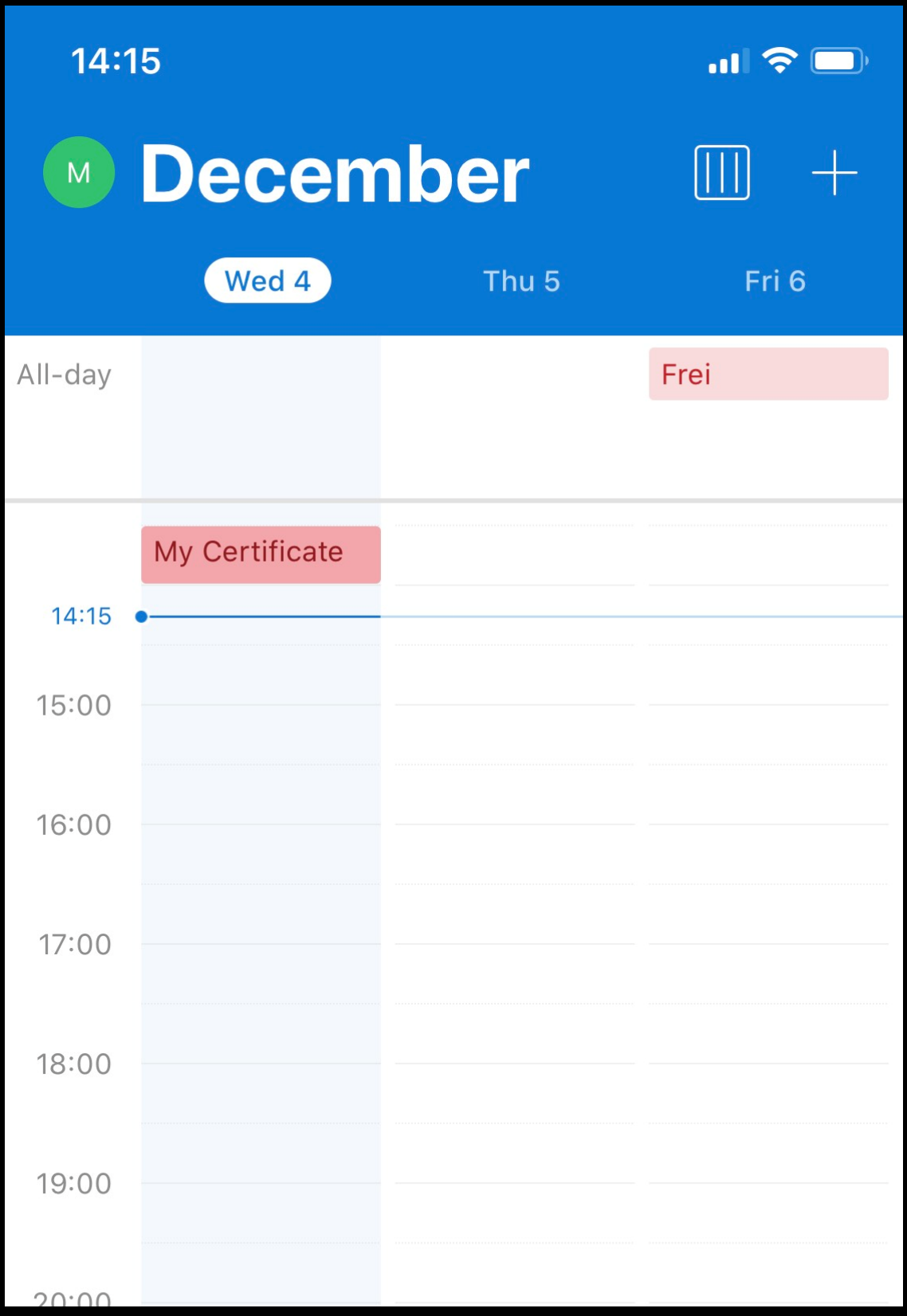


Figure 153: Save the Appointment

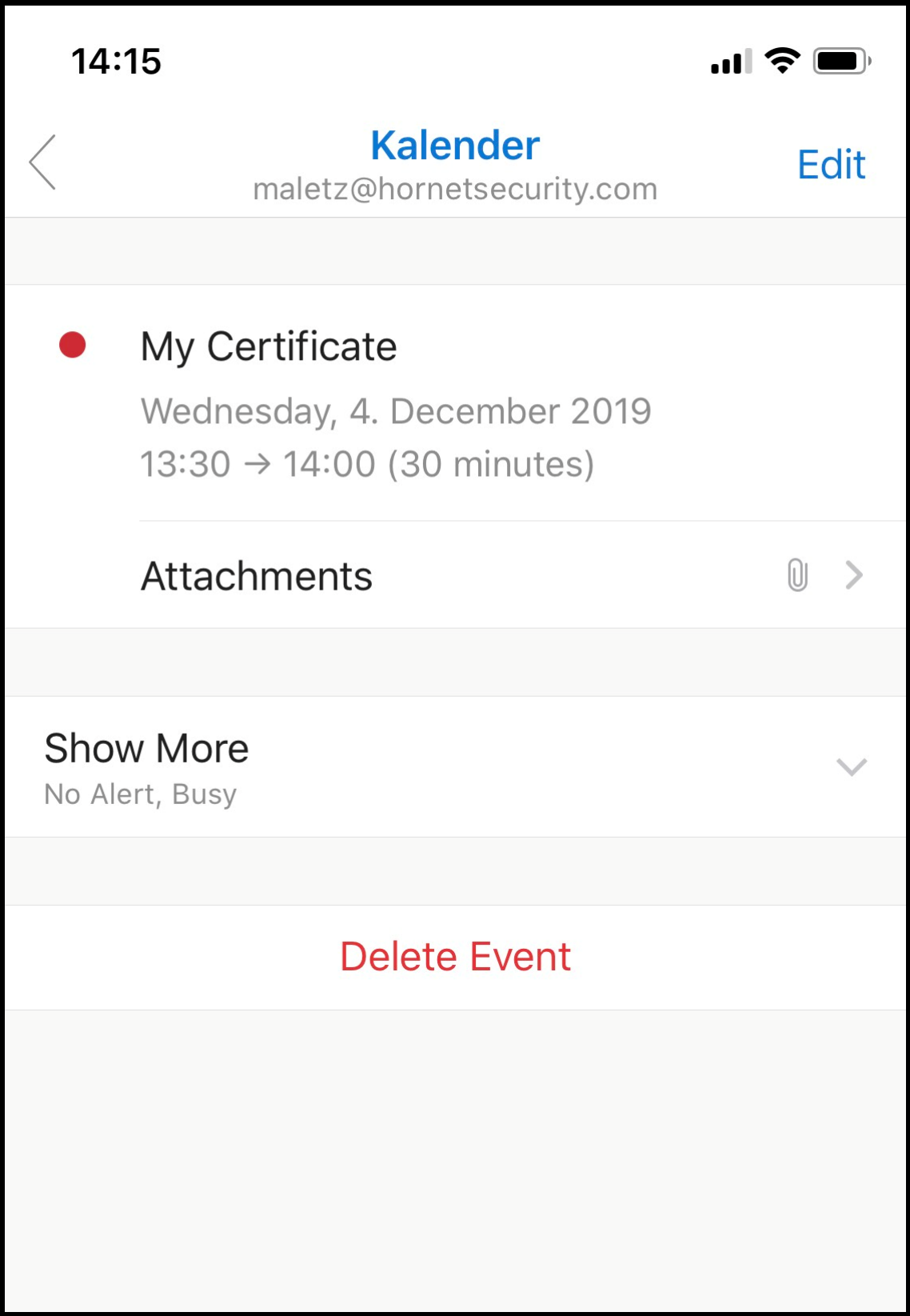
7. Open Outlook on your mobile device.
8. Select the calendar.

   The calendar opens.


14:15
M
December
Wed 4
Thu 5
Fri 6
All-day
Frei
My Certificate
14:15
15:00
16:00
17:00
18:00
19:00
20:00

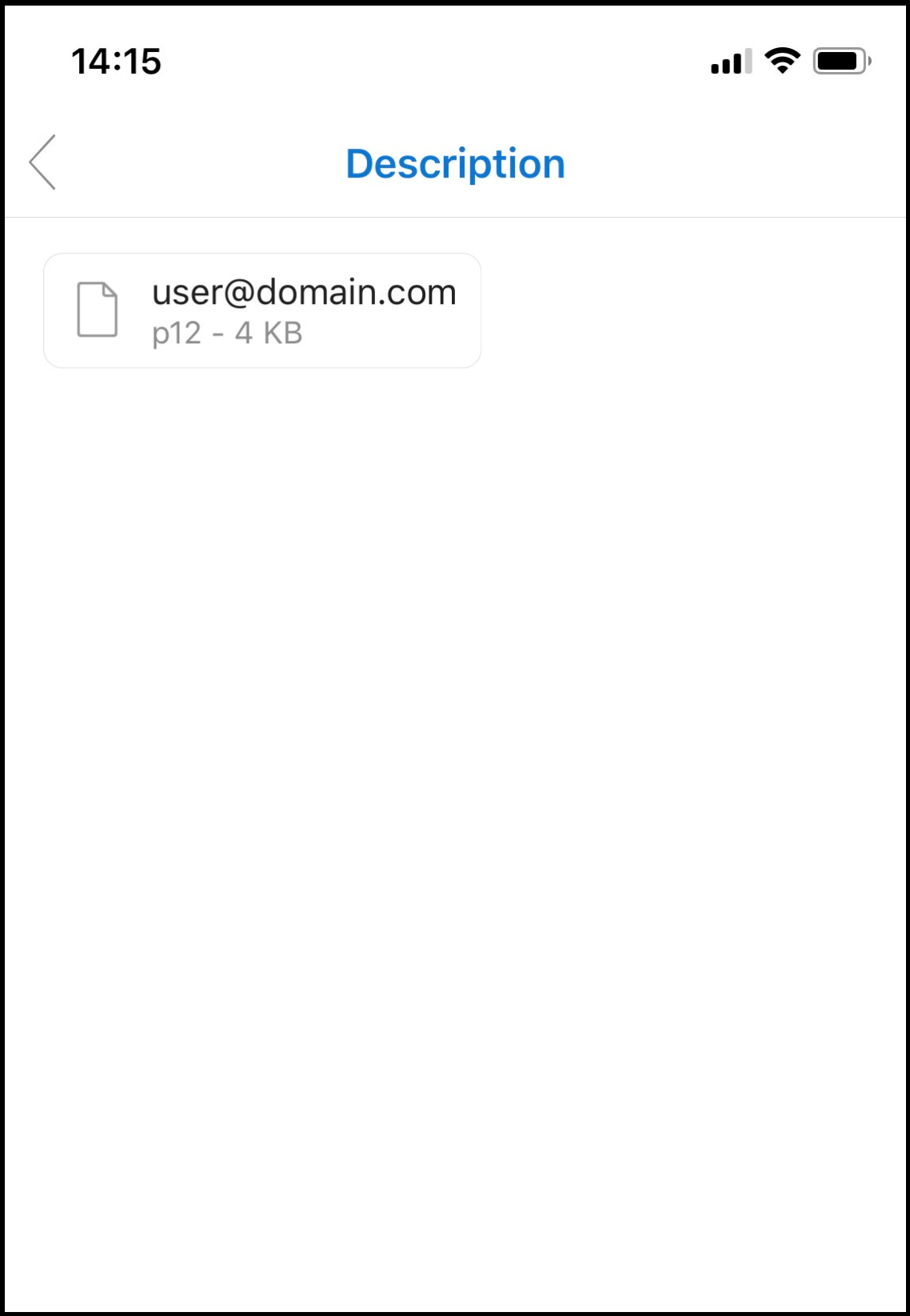
9. Open the appointment you have just created.

You see the details of your appointment.


14:15
Kalender
maletz@hornetsecurity.com
Edit
My Certificate
Wednesday, 4. December 2019
13:30 → 14:00 (30 minutes)
Attachments
Show More
No Alert, Busy
Delete Event

10. Tap on **Attachments**.

Your personal certificate is displayed as a file.


14:15
Description
user@domain.com
p12 - 4 KB

11. Tap on the displayed certificate.
12. Click on **Install certificate**.

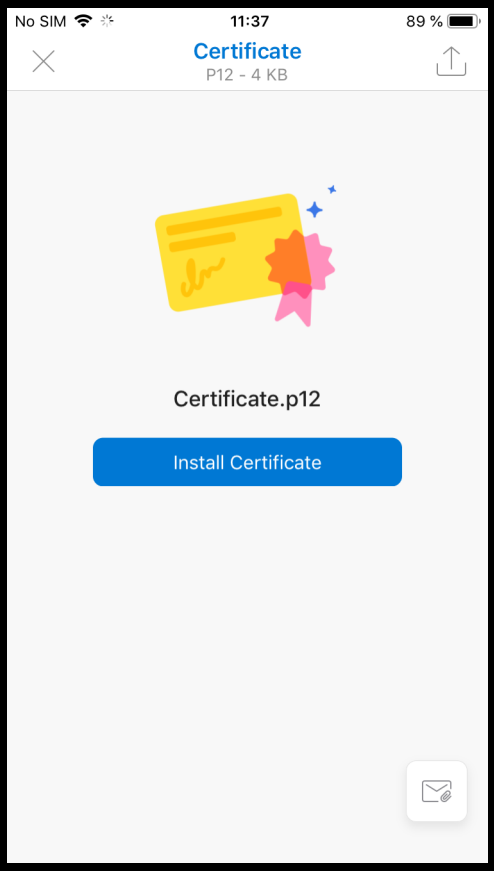


Figure 157: Install certificate

13. Enter the passphrase to your personal certificate and click on **Install**.

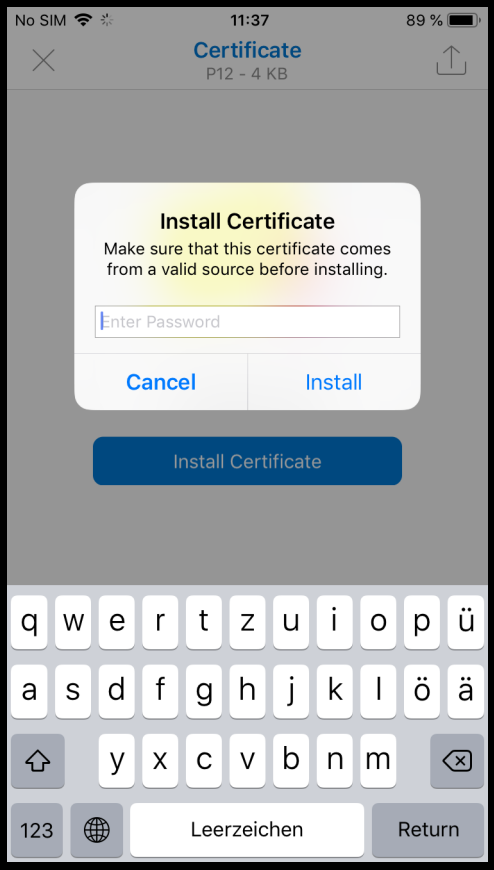


Figure 158: Enter the passphrase

➔ The certificate has been installed.

14. In the next window, click on **Settings**.

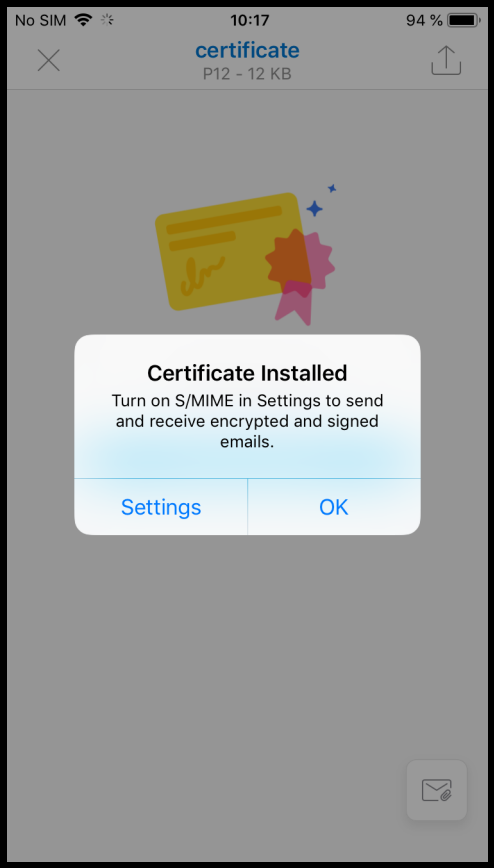


Figure 159: Select Settings

15. Activate S/MIME and click on **OK**.

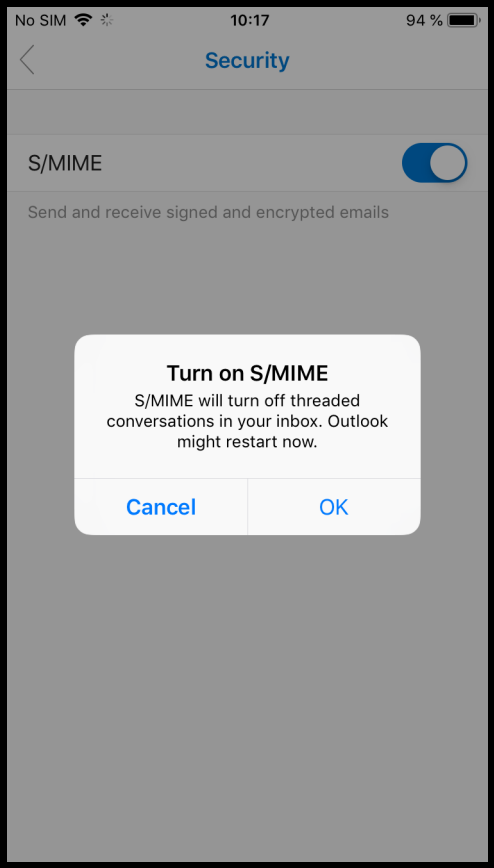


Figure 160: Activate S/MIME

- You have installed your personal certificate in Outlook on iOS.

Master Key

The Master Key is a key pair with which the personal certificates of the mailbox users can be centrally encrypted. Thus, the Master Key enhances security.

The Master Key encrypts the personal certificates of the mailbox users. Without the Master Key, the encrypted personal certificates do not grant access to the encrypted mailboxes. This prevents unauthorized persons from gaining access to the encrypted mailboxes if they obtain the encrypted personal certificates.

The Master Key consists of a public and a private key. With the public key, the personal certificates can be encrypted, but not decrypted. For decryption, the private key is required.

We store the personal certificates created for the users so that the users can download them as many times as needed (e. g., to bind them to new devices). Once a personal certificate has been

created, we encrypt it. We store the encrypted version for an unlimited time. But we only store the non-encrypted version for 14 days. If a user downloads his personal certificate and the non-encrypted version is no longer available, the encrypted one is decrypted with the Master Key and then made available.

As an additional security measure, you can download the whole Master Key (see Downloading the Master Key on page 160) and then remove its private part from our database (see Deleting the Master Key on page 162). In this case, we no longer have access to the non-encrypted personal certificates of the users once the non-encrypted version has been deleted after the 14 days have passed.

If a user needs his certificate after these 14 days and we no have the private key of the Master Key, you can provide us with the private key for a short period at any time so that we can decrypt the personal certificate of the corresponding user and make it available to him for another 14 days (see Re-enabling Personal Certificate Download on page 164).

Downloading the Master Key

You have the possibility to download the Master Key.

You have activated 365 Total Encryption.

The Master Key is used to encrypt and decrypt the personal certificates of the users' mailboxes. If you intend to have the private part of the Master Key removed from our database (see: Deleting the Master Key on page 162), you must **always** make a local copy first by downloading the Master Key.

1. **Notice:**

   Only administrators of Microsoft 365 accounts can download the Master Key.

   Log in to the Control Panel with your administrative credentials.
2. Navigate to **365 Total Protection** #→**365 Total Encryption**.
3. Click on **Download Master Key**.

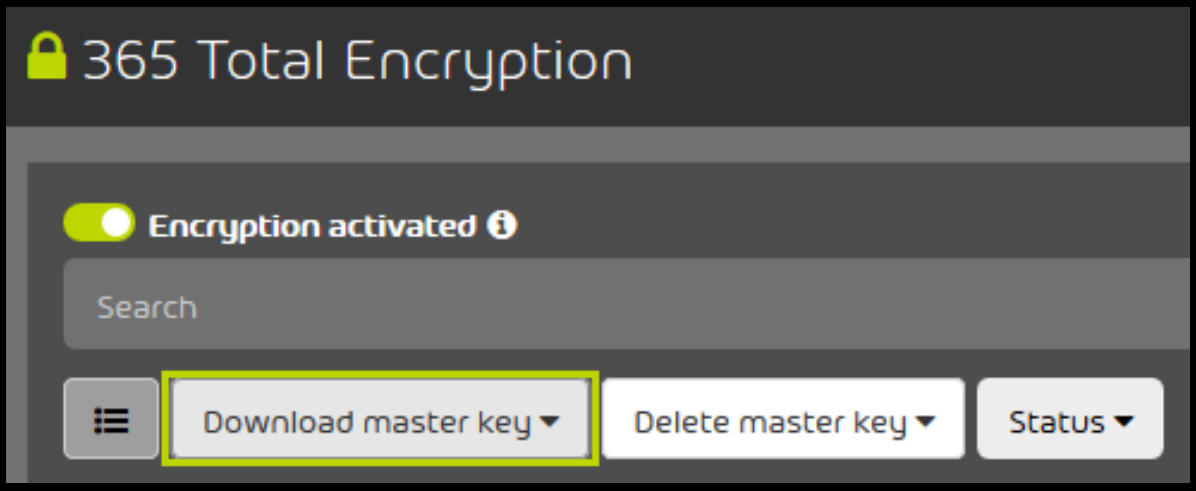


Figure 161: Downloading the Master Key

4. Select whether you want to receive the one-time password for downloading the Master Key by email or SMS.
5. Define a passphrase for the Master Key and repeat it.

> **Notice:**
>
> The passphrase is needed to install the downloaded Master Key securely on your computer.

6. Enter the one-time password which you have received by email or SMS in the **One-time password** field.
7. Click on **Download Master Key**.

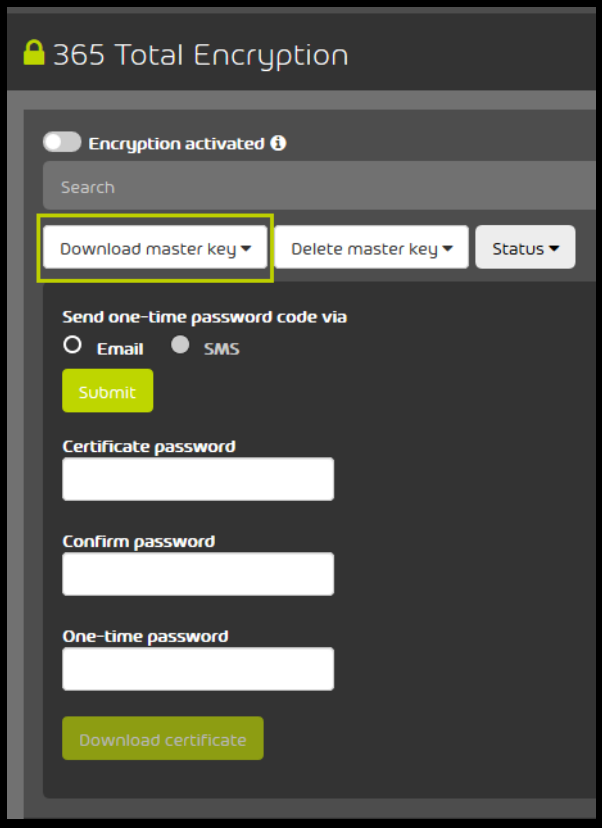


Figure 162: Certificate download

The Master Key is downloaded in .p12 format. Store the Master Key safely.

Deleting the Master Key

You have the possibility to permanently delete the private part of the Master Key from our database.

You have downloaded the Master Key (see Downloading the Master Key on page 160) and stored it safely.

The private part of the Master Key is needed to decrypt the personal certificates of the mailboxes.

DANGER:

Without the Master Key, it is not possible to decrypt the personal certificates. Be sure to download the Master Key and store it safely before deleting its private part from our database.

1. **Notice:**

   Only administrators of Microsoft 365 accounts can delete the Master Key.

   Log in to the Control Panel with your administrative credentials.
2. Navigate to **365 Total Protection** #→**365 Total Encryption**.
3. Click on **Delete Master Key**.
4. Select whether you want to receive the one-time password for deleting the Master Key by email or by SMS.

   The one-time password is sent.
5. Enter the one-time password that you received by email or SMS in the **One-time password** field.
6. Click on the button **Delete Master Key** to permanently delete the private part of the Master Key from our database.

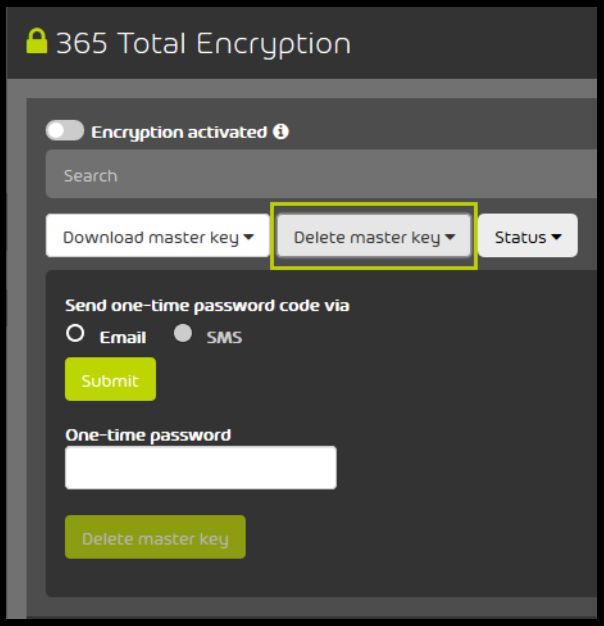


Figure 163: Select store location

The private part of the Master Key has been permanently deleted from our database.

Re-enabling Personal Certificate Download

You have the possibility to re-enable the download of personal certificates.

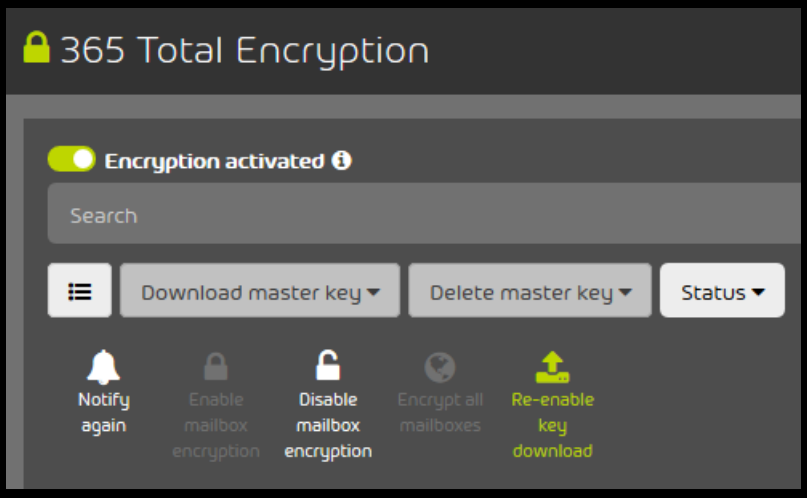
You have activated 365 Total Encryption and deleted the Master Key.

Once the Master Key has been deleted from the Control Panel, the private keys of user mailboxes can no longer be decrypted. It is not possible to download the master key again. To re-enable the download of personal certificates, the Master Key must be uploaded to the Control Panel again.

1. **Notice:**

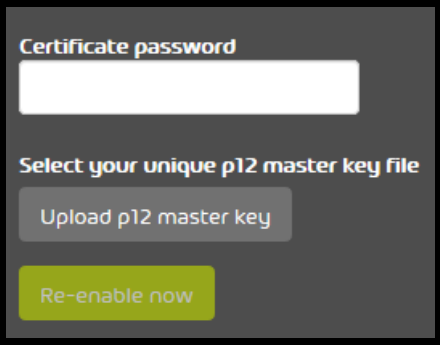
   Only administrators of 365 Office accounts can re-enable the download of certificates.

   Log in to the Control Panel with your administrative credentials.
2. Navigate to **365 Total Protection** #→**365 Total Encryption**.
3. Click on the menu button .
4. In the list below, mark the checkboxes next to the mailboxes for which you want to re-enable the certificate download.
5. Click on **Re-enable Certificate download**.



6. Enter the passphrase that was previously assigned to the Master Key.

Figure 164: Enter the passphrase



7. Upload the previously saved Master Key in the **Upload .p12 Master Key** field.
8. Click on **Re-enable now**.

The download of personal certificates has been re-enabled. If the certificate download could not be re-enabled for all selected mailboxes, a message appears indicating how many mailboxes the download has been re-enabled for.

Reporting & Compliance

The menu item Reports & Compliance bundles all statistics as well as the overview of the audit logs.

Email Statistics

The email statistics show the email traffic of the selected domain.

This section is intended for the administration of a domain. Select a domain in the scope selection of the Control Panel to make this area visible.

Filtering Diagrams and Statistics

The statistics and diagrams can be filtered by period and the direction of the email traffic.

1. To filter the emails for a certain period, click on the date button 01.03.2019 - 31.03.2019.

> **Important:**
>
> You can display emails from the last three months maximally.

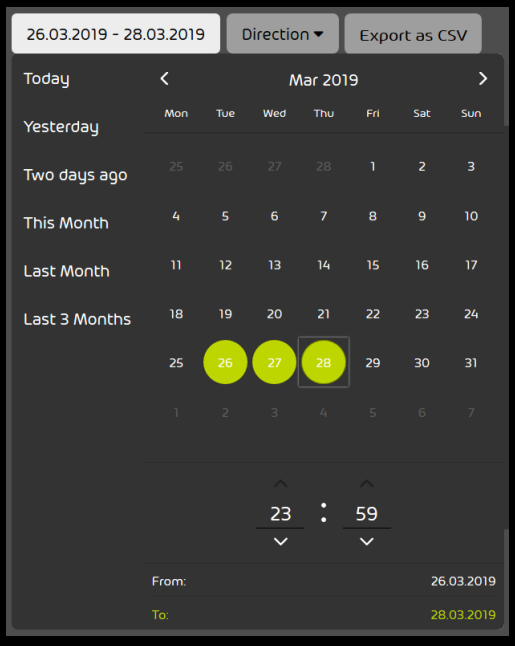


Figure 165: Select period

2. Optional: In the drop-down menu **Direction** select the direction of the displayed email traffic:
   - Both (incoming and outgoing)
   - Incoming
   - Outgoing

Figure 166: Select direction

Emails by Type

The diagram **Emails by type** shows an overview of emails per category.

The diagram shows how many emails of the domain were sent and/or received in the selected period displayed in absolute and relative numbers.

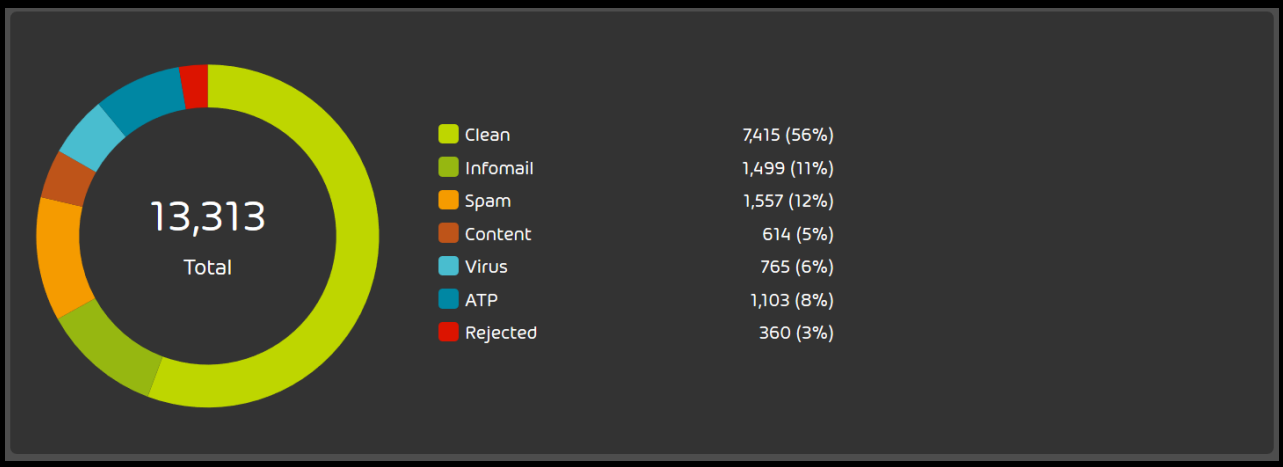


Figure 167: Emails by type

Emails by Time

The statistic shows emails according to the receiving or sending time.

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

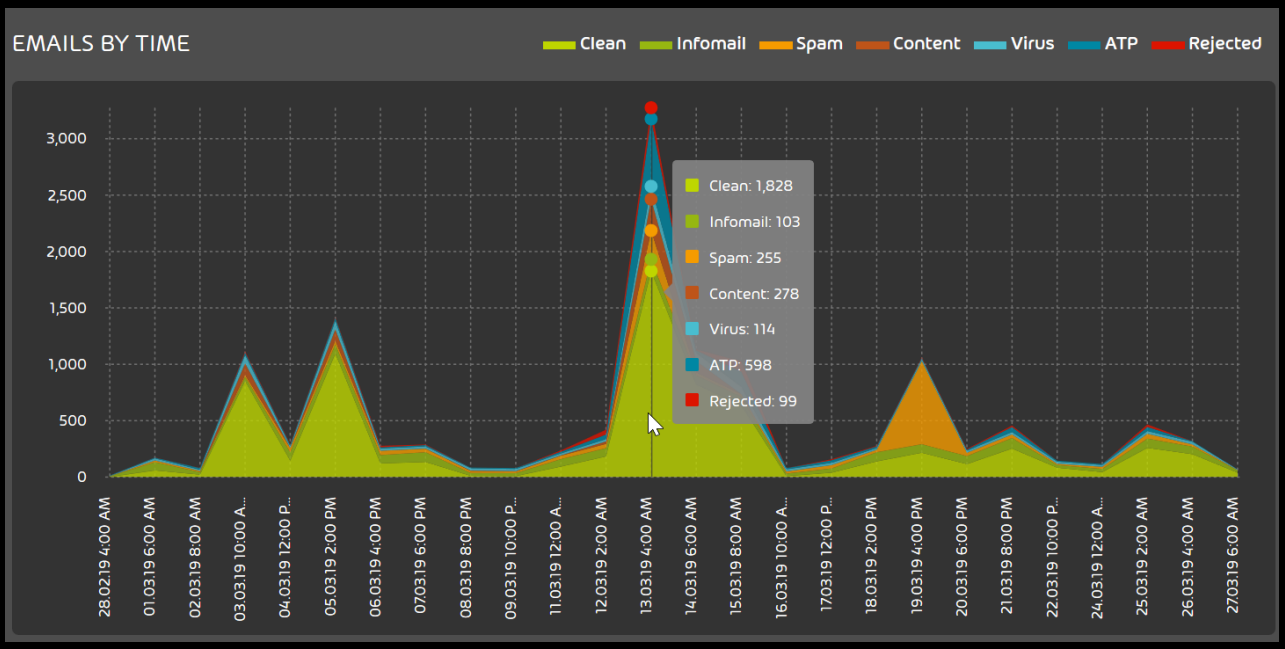


Figure 168: Emails by time

Emails by User

The statistic shows the amount of emails per user.

In the statistics, users of the domain are sequentially listed according to their total amount of emails in one week. Furthermore, the statistics show how many emails are sent and/or received per category in the selected period.

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

Postfach	Gültig	Info...	Spam	Cont...	Virus	ATP	Abge...	Gesamt
[redacted]	185	1,303	95	0	380	253	6	2,222
[redacted]	1,248	0	0	3	0	0	9	1,260
[redacted]	733	0	0	301	168	30	9	1,241
[redacted]	238	35	729	0	7	63	22	1,094
[redacted]	456	0	0	0	47	97	92	692
[redacted]	84	0	453	0	54	2	0	593
[redacted]	450	0	0	0	0	0	0	450
[redacted]	448	0	0	0	0	0	0	448
[redacted]	448	0	0	0	0	0	0	448
[redacted]	398	0	0	0	0	0	0	398
[redacted]	243	0	0	0	0	2	0	245
[redacted]	236	1	4	0	0	2	0	243
[redacted]	236	1	4	0	0	2	0	243
[redacted]	236	1	4	0	0	2	0	243
[redacted]	232	0	0	0	0	2	0	234
[redacted]	92	75	0	0	0	2	0	169
[redacted]	101	0	1	0	0	2	0	104
[redacted]	87	0	3	0	0	0	0	90

Figure 169: Emails by user

Threat Live Report

About Threat Live Report

In the module Threat Live Report different statistics for a domain are displayed.

> **Important:**
>
> The **Threat Live Report** is only available for **Advanced Threat Protection (ATP)** customers.

You can find the texts used here in the module in the Control Panel. Move over the ⓘ behind the respective statistics or diagram.

Displaying Global Data

When displaying global data, you can choose between the data of all customers and the data of the customer selected in the scope selection.

Important:

This function is only available for partners.

With the global button you can switch the LIVE ATTACK OVERVIEW and diagrams and statistics under ATTEMPTED ATTACKS and THREAT STATISTICS to the available data of all Hornetsecurity customers.

If **global** is activated, you can see attacks and threats which have been occurred to all customers of Hornetsecurity in the chosen period. If **global** is deactivated, you can only see those attacks and threats for the customer chosen in the scope selection.

Figure 170: Global button

Selecting the Period

Select the period for the displayed statistics.

Notice:

The selection of the period affects the diagrams and statistics under ATTEMPTED ATTACKS, THREAT STATISTICS and URL REWRITING STATISTICS.

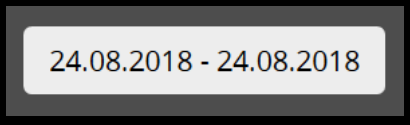


Figure 171: Select period

Statistic Descriptions

Live Attack Overview

The LIVE ATTACK OVERVIEW shows all attacks with their source and destination caught by Hornetsecurity worldwide at this moment. Furthermore, the attack type is shown.

You can find a description under Description of Attack Types on page 177.

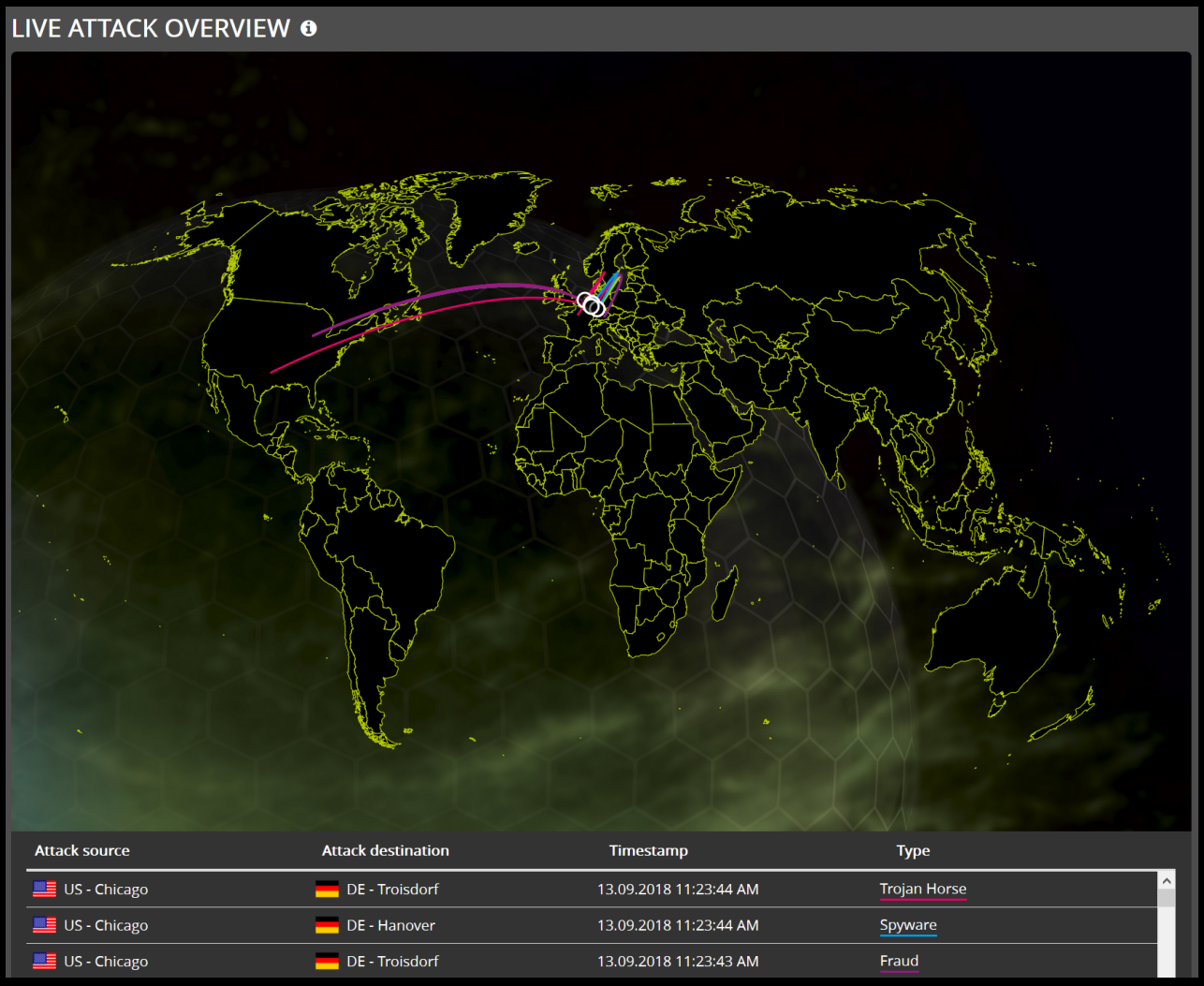


Figure 172: Live attack overview

Attempted Attacks – Attack Type by Date

The statistics show how many attacks per attack type took place at a certain time in the chosen period.

Move the mouse over the vertical lines to display the absolute numbers of the attacks per attack type for a certain time. Move over the points of each attack type to display the respective diagram and information about the number of attacks.

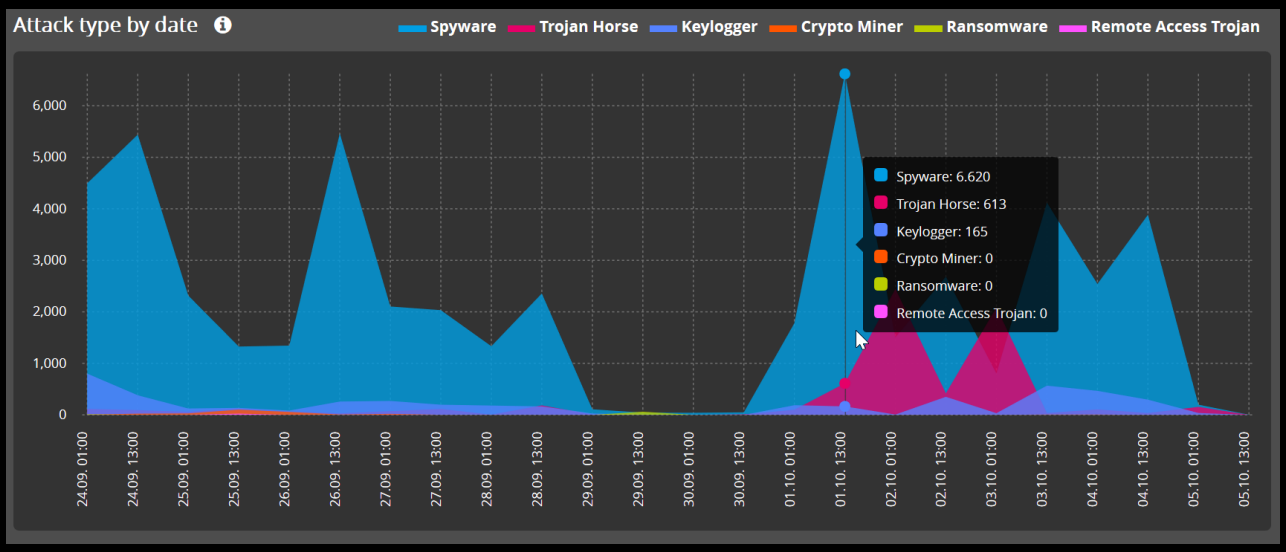


Figure 173: Attempted attacks - Attack type by date

Threat Statistic – by Attack Type

The diagram shows the proportions of attack types in relation to the total number of attacks in the selected period. The total number of attacks that took place is shown in the middle. It refers to the selected period.

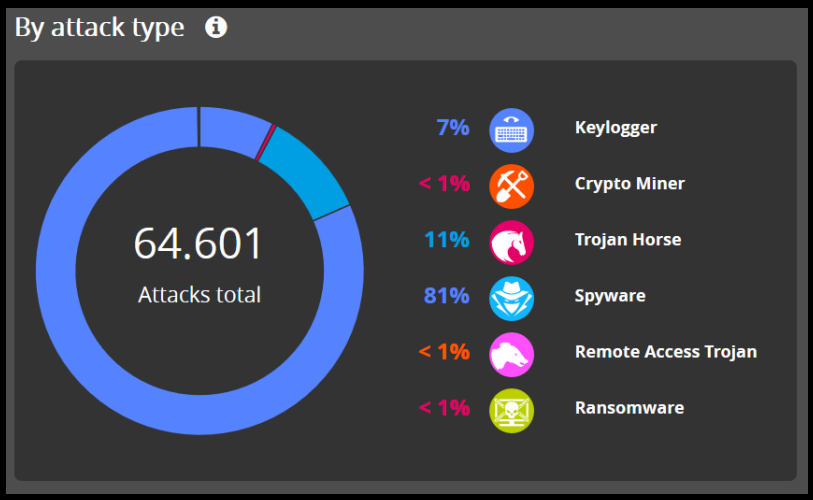


Figure 174: Threat statistics - By attack type

Threat Statistic - by Attack Vector

The diagram shows the proportions of attack vectors in relation to the total number of attacks in this period. The total number of attacks that took place is shown in the middle. It refers to the selected period.

You can find a description under Description of Attack Vectors on page 179.

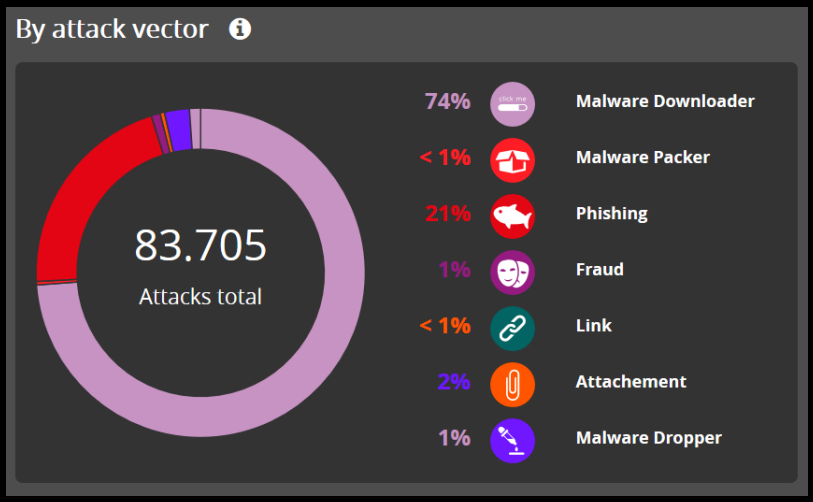


Figure 175: Threat statistics - By attack vector

Attempted Attacks - Attack Vectors by Date

The statistics show how many attacks per attack vector took place at a certain time in the chosen period.

Move the mouse over the vertical lines to display the absolute numbers of the attacks per attack vector for a certain time. Move over the points of each attack vector to display the respective diagram and information about the number of attacks.

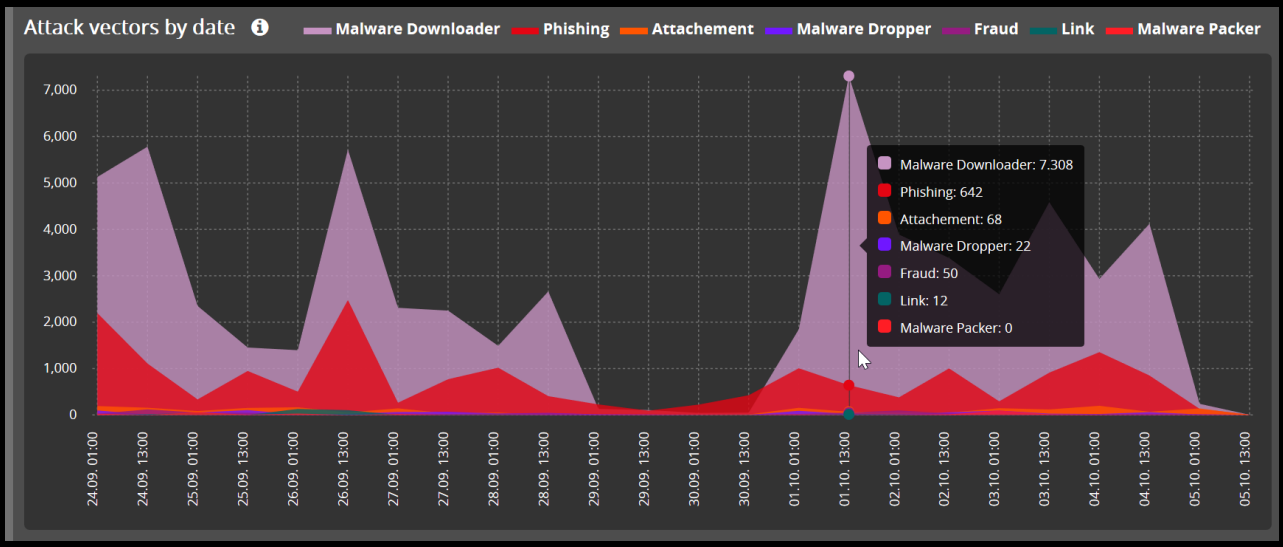


Figure 176: Threat statistics - Attack vectors by date

URL Rewriting Statistics

The statistics and charts under URL REWRITING STATISTICS each represent the number of clicked links in emails rewritten by the URL rewriting engine in the selected time period.

Clicks by Time of Day

The statistics Clicks by time of day shows the percentage of clicks on a link at a certain time.

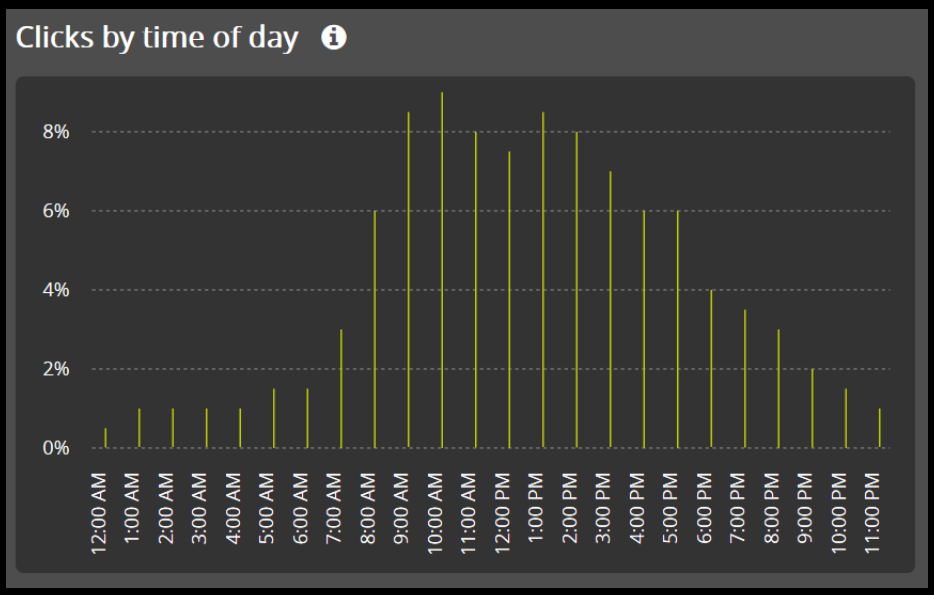


Figure 177: Clicks by time of day

Clicks by Device

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

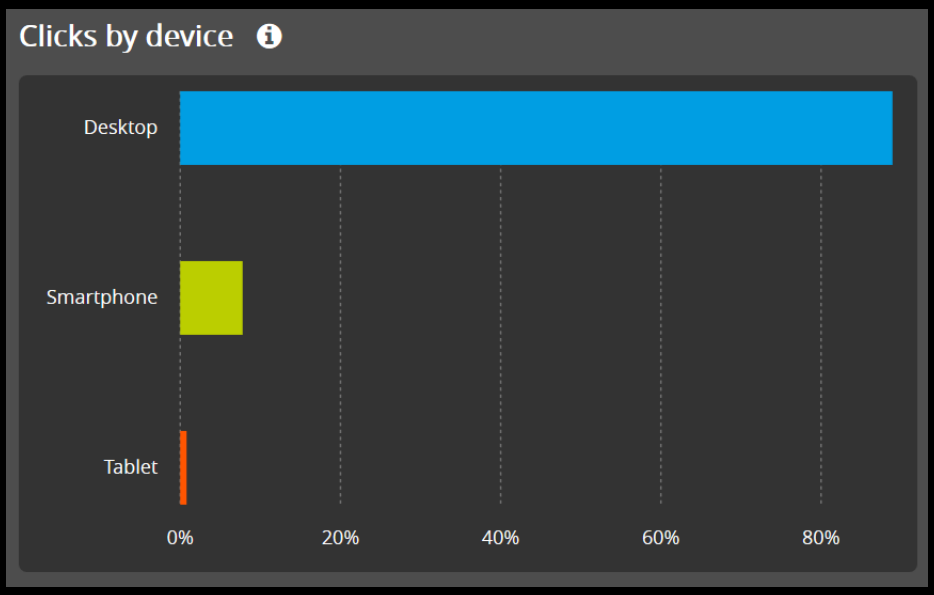


Figure 178: Clicks by device

Clicks by Operating System (OS)

The diagram Clicks by operating sytem (OS) shows the distribution of clicks per operating system in percent.

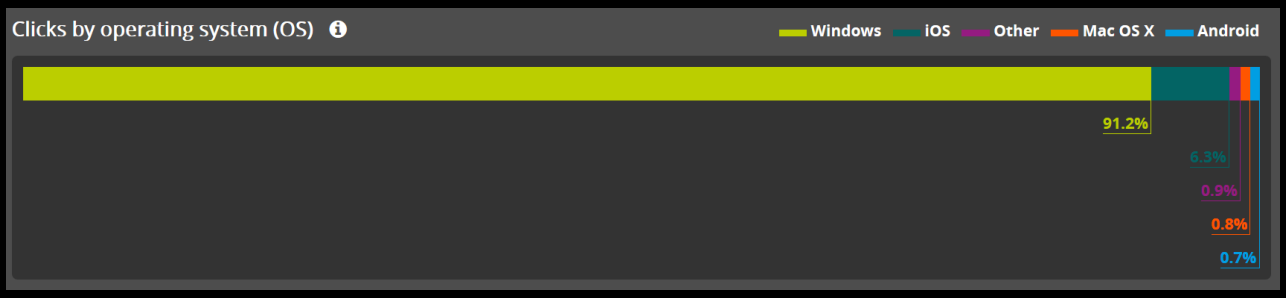


Figure 179: Clicks by operating system (OS)

Description of Attack Types

The attacks are divided into different types that are shown with different colors and symbols in the Threat Live Report.

Table 6: Attack Types

Name of the attack type	Description
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 Trojans	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.
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 perfidious thing is that the owners of the computers do not notice the "membership" in a botnet until it already executes the 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.

Name of the attack type	Description
Point-of-Sale Trojans	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.
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

The attacks are divided into different vectors that are shown with different colors and symbols in the Threat Live Report.

Table 7: Attack Vectors

Name of the attack vector	Description
Attachment	An attachment of an email is a file which 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.
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 the 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.

Name of the attack vector	Description
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.

Auditing 2.0

About this manual

This manual explains how the Control Panel module **Auditing** works. The options for filtering events and executable actions are explained.

Auditing

With **Auditing** you can track the activities of users in the Control Panel. As an administrator, you can find out who is responsible for creating, editing or deleting data sets and when the event occurred. This enables you to undo the actions if required.

Description of Categories

Every event is divided into different categories and is displayed in the audit log. These categories are explained in the table listed below.

Figure 180: Categories

Property	explanation
Timestamp	Shows at which time the action was performed.
users	Shows which user has performed the action.

Property	explanation
Target	Shows the user for whom the action was performed.
Action	Explains if an event has created, updated or deleted something. Success or failure indicate if a login was successful or not.
Event	Shows if the action is a modification of the user setting, the black- or whitelist, the credentials or the login.
Target path	Shows under which domain the user is created for whom the action is executed.
App ID	Shows the identification numbers of the applications which use the API. Applications can communicate with the Hornetsecurity Services via the API.
App version	Shows the version of the application which communicates with the API.
IP	Shows the IP address of the user who performed the action.
URL	Shows the path to the API endpoint which is used.

The categories **Timestamp**, **User**, **Target**, **Action** and **Event type** are displayed per default. Furthermore, you can activate **Target path**, **App ID**, **App version**, **IP** and **URL**. To do that, go to the chapter Selecting Displayed Categories on page 181.

Filtering Events

Selecting Displayed Categories

1. Click on the button on the right side.

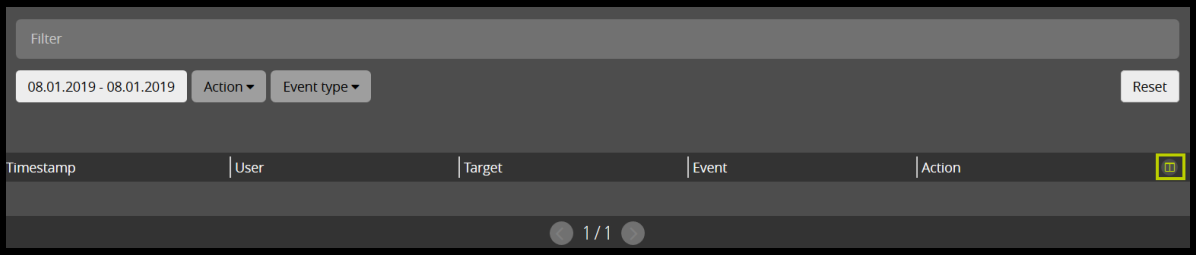


Figure 181: Button for selecting categories

2. Select the category which you would like to display.

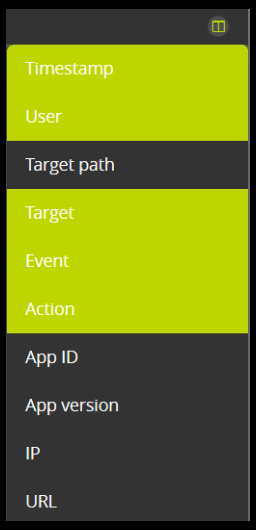


Figure 182: Drop-down menu of categories

Notice:

A multi-selection is possible.

Displayed categories have been selected.

Searching for Events

You can search for specific events in the search bar.

Select a category in the search bar and enter a term to search the events listed.

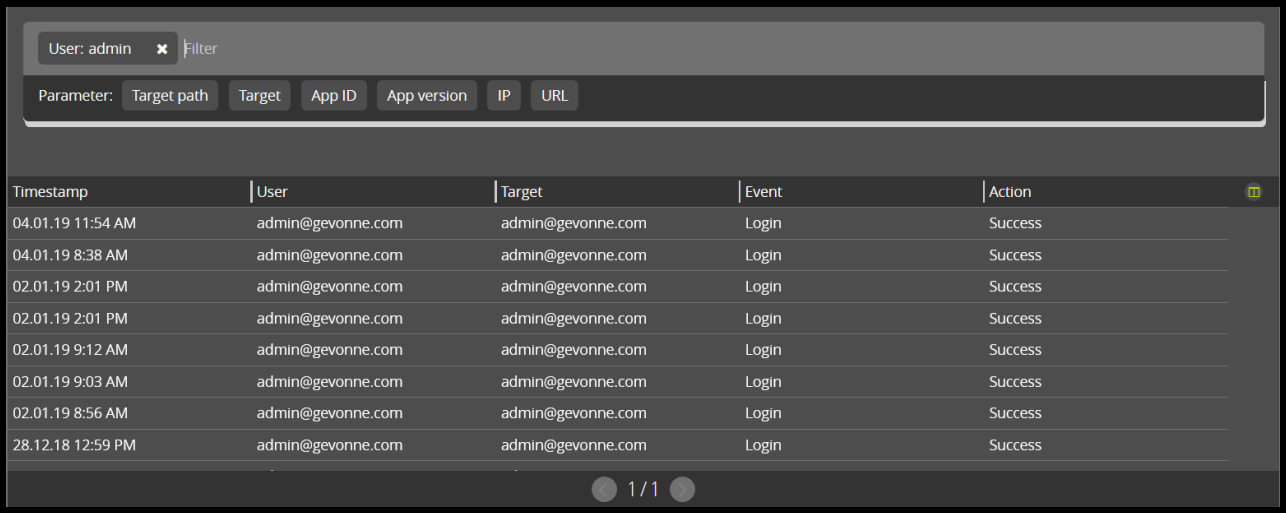


Figure 183: Searching for Events

You can find a description of all categories in the chapter Description of Categories on page 180.

Filtering by Actions

You can filter the displayed events by actions in the appropriate drop-down menu. After the selection only results of the chosen action are displayed. You can only filter by one action at a time.

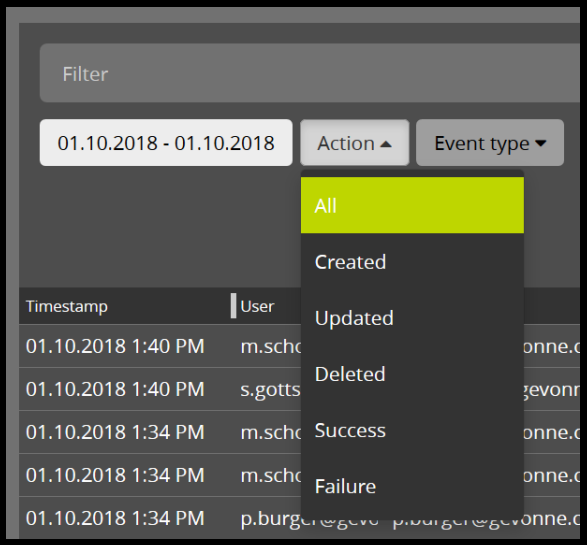


Figure 184: Filtering by actions

The following table lists the actions by which you can filter.

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

Filtering by Event Type

filtering

You can filter the displayed action by the event type in the appropriate drop-down menu. Depending on the filtering you can show or hide certain modules. You can only filter by one event type at a time.

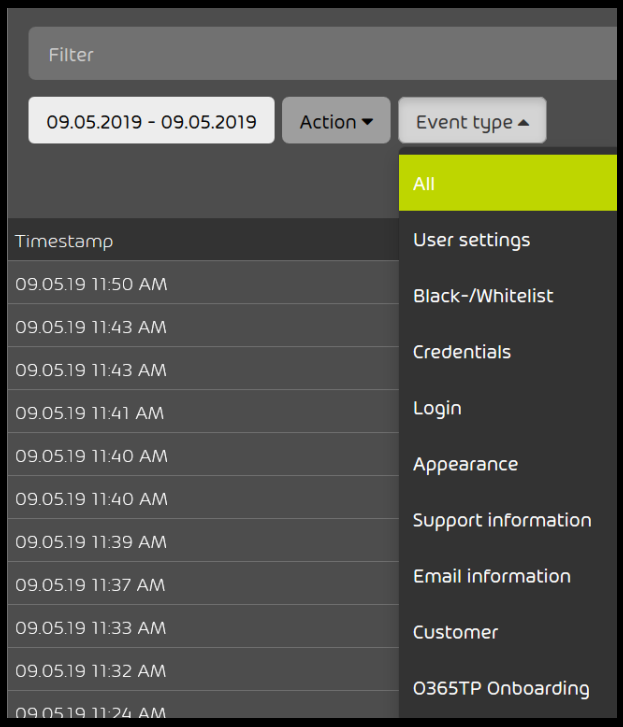


Figure 185: Filtering by Event Type

In the following table event types are listed by which you can filter.

Event	explanation
All	Shows all types of events.
User settings	Filters for all events that modified the user settings.
Black-/Whitelist	Filters for all events that modified the black or white lists.
Credentials	Filters for all events that modified user credentials.
Login	Filters for all login events.
Appearance	Filters for all events that modified the appearance in the Whitelabeling module.
Support information	Filters for all events that modified the support information in the Whitelabeling module.
email information	Filters for all events that modified the email information in the Whitelabeling module.
Customer	Filters by events that have led to changes in customer settings.
365TP onboarding	Filters by events related to customer onboarding for 365 Total Protection.
role assignment	Filters by events that led to the creation, update, or deletion of role assignments.
Password Policy & IPs	Filters for events that have led to changes in password policies and IPs.
Spam Report	Filters for events that have led to changes in the spam report settings.

Additional Events

The following table lists event types by which you cannot filter, but which are still displayed in the audit log.

ATP configuration	Contains information on changes to ATP settings.
API token	Contains information about changes on API tokens.
Domain	Contains information about changes on domain settings.
Group	Contains information about changes on group settings.

Selecting a Period

1. Click on the date selection.

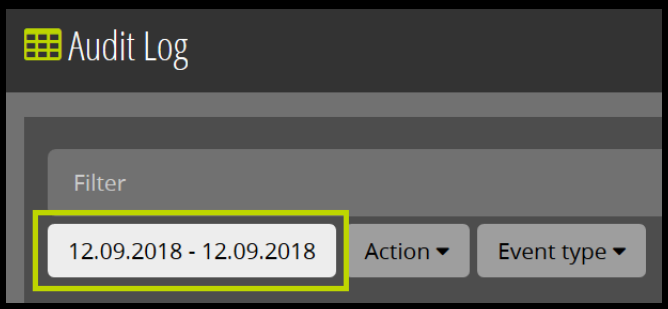


Figure 186: Select period

2. Select the period for which logged events should be displayed.

The display period has been selected.

Resetting Settings

Click on **Reset** to set all filter values on default.

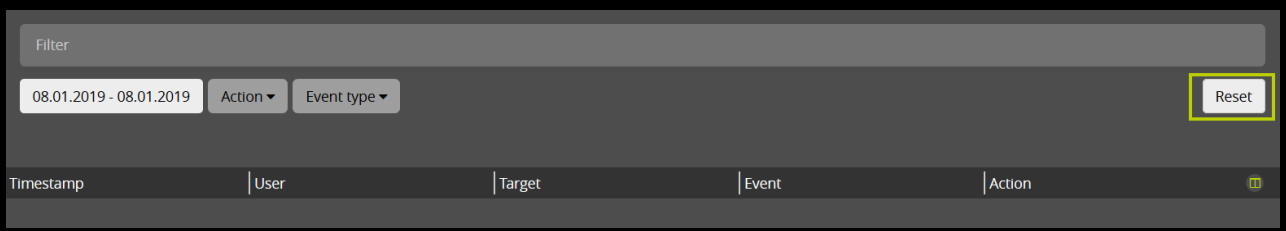


Figure 187: Reset settings

The settings were reset.

Auditing

In this module you will find the audit log for changes in the following modules:

- Management
- **Security Settings#→Hornetdrive**
- All changes in the old Control Panel

Web Filter

Editing Settings in the Web Filter Module

In the Web Filter module all release requests, blocked and allowed websites are displayed.

Basically, websites can be filtered by different categories whereby you can only change the displayed period of time for **Blocked websites** and **Valid websites**.

If desired, you can add the categories **User**, **Group** and **IP address** to the Web Filter display range. Only the domain administrator can add these categories for all users of the domain. There are different editing functions for the websites marked on the left column:

- Release Requests can be rejected or added to the white list on a user, group or global level.
- Blocked websites can be added to the white list on a user, group or global level.
- Valid websites can be added to the black list on a user, group or global level.

Release Requests

In this area all release requests are displayed.

The automatic sorting of the release requests is done according to the actuality. The latest release request is ranked first. If you want to see the oldest release request at the top of the table, click on **Date**. Additionally, you can sort the requests by **Status** and **Reason**.

You can reject release requests or put them on the appropriate white list and thus release the requests.

The administrator also receives every release request with related information via email. These release requests can be rejected or released directly in the email. The user asking for a release subsequently receives an appropriate message automatically.

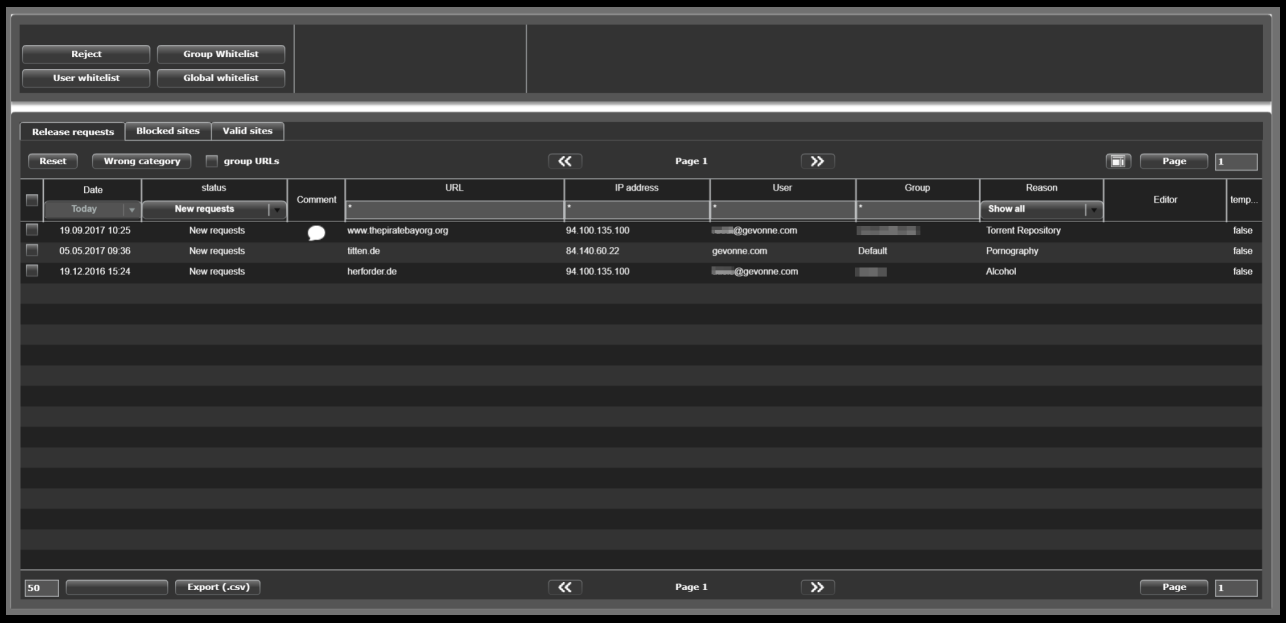


Figure 188: Release requests

Blocked Sites

In this area all blocked websites are displayed.

The automatic sorting of the blocked websites is done according to the actuality. The latest blocked website thus is ranked first. If you would like to see the oldest blocked website at the top of the table, click on **Date**. Click on the drop-down menu in the first column **Date** to select the period for which you would like to display blocked websites. Additionally, you can sort by **Reason**.

Figure 189: Blocked sites

Valid Sites

In this area all allowed websites are displayed.

The automatic sorting of the released websites is done according to the the actuality. The latest valid site is ranked first. If you would like to see the oldest valid site at the top of the table, click on **Date**. Click on the drop-down menu in the first column **Date** to select a period. Additionally, you can sort the websites by **Reason**.

Figure 190: Valid sites

Reporting an Incorrectly Categorized Website

You can report websites that are assigned to an incorrect category. The category of the website is then checked and if necessary reclassified.

1. Under **Web Filter#→#→Workspace#→Release requests, Blocked sites or Valid sites** in the Control Panel select the websites with the wrong category.

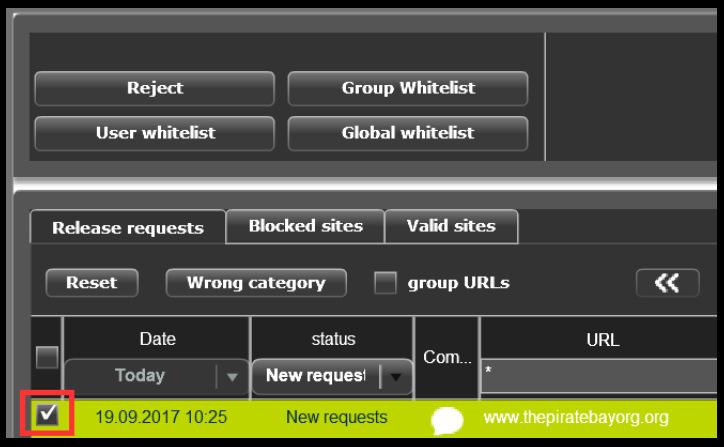


Figure 191: Select website

2. Click on **Wrong category** to have the category of the website checked.

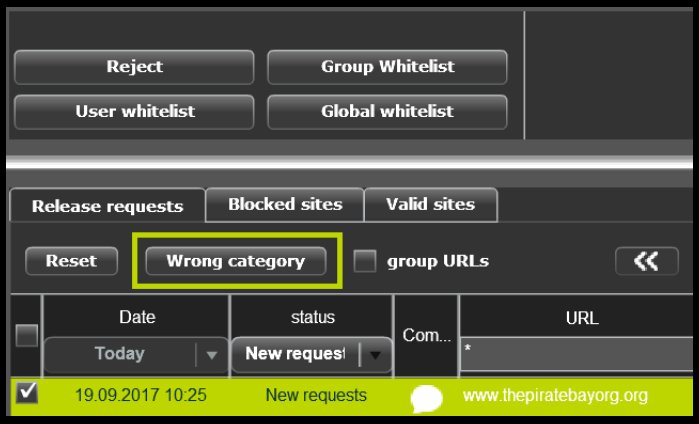


Figure 192: Report a wrong category

The incorrectly categorized website has been reported.

Grouping of URLs

With the function **group URL** websites, which are opened several times, are summarized and only displayed once.

As soon as you activate the function, the Control Panel summarizes all URLs that are opened multiple times. The appropriate URL is only displayed once.

You can find the appropriate function under **Web Filter#→Workspace#→Release requests, Blocked sites and Vaild sites**.

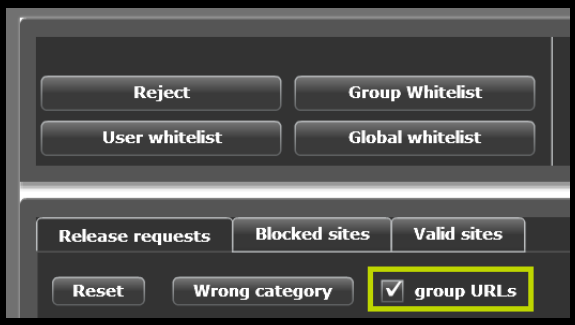


Figure 193: Activate group URLs

Example: Group URLs

If a user visits the website www.searchengine.com several times per day, the Web Filter module shows the URL only once. The date shows the time when the website was visited for the first time.

Black & White Lists

Blocking or Releasing Domains via Black or White List

1. Open the Control Panel.
2. Select the desired customer from the scope selection.
3. Go to **Web Filter#→Black- & Whitelist**.

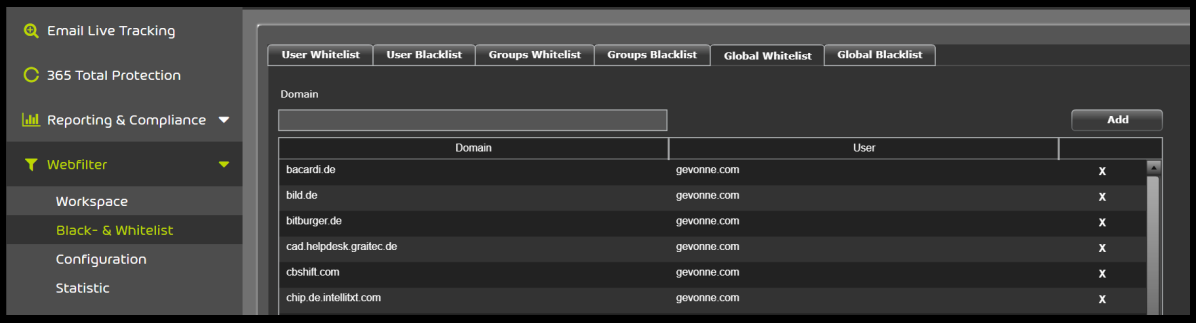


Figure 194: Web Filter Black- & Whitelist

4. Select the desired list:
   - User Whitelist
   - User Blacklist
   - Groups Whitelist
   - Groups Blacklist
   - Global Whitelist
   - Global Blacklist
5. Enter the domain to be released or blocked in the field **Domain**.

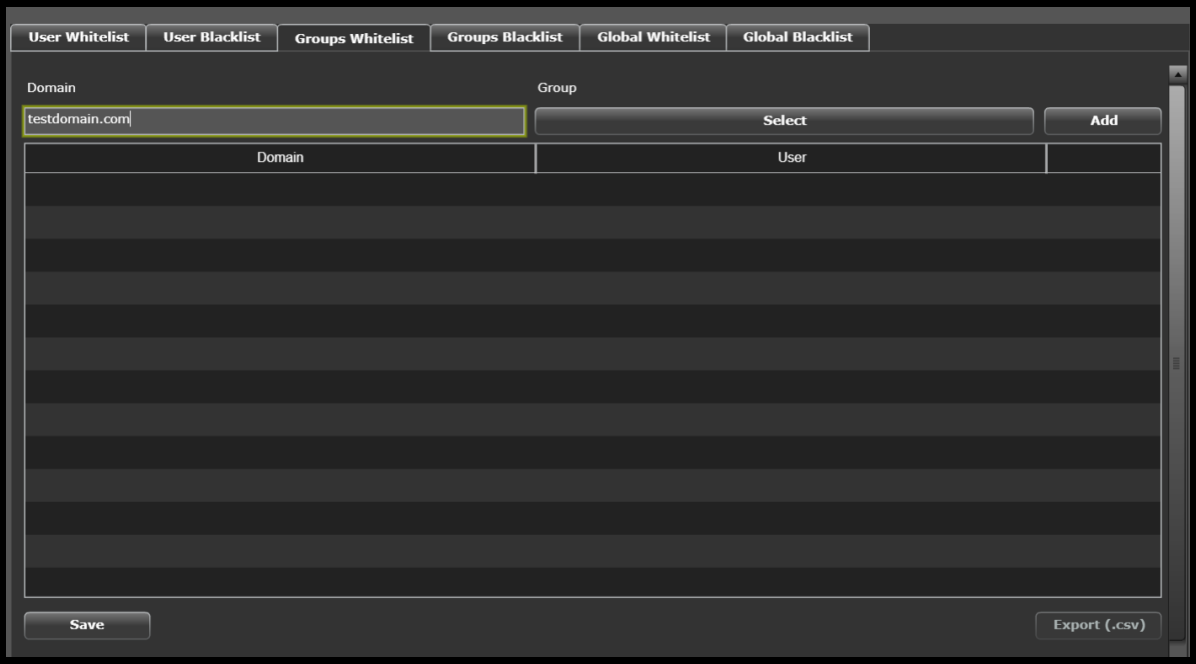


Figure 195: Enter domain

6. Select the appropriate user or group.

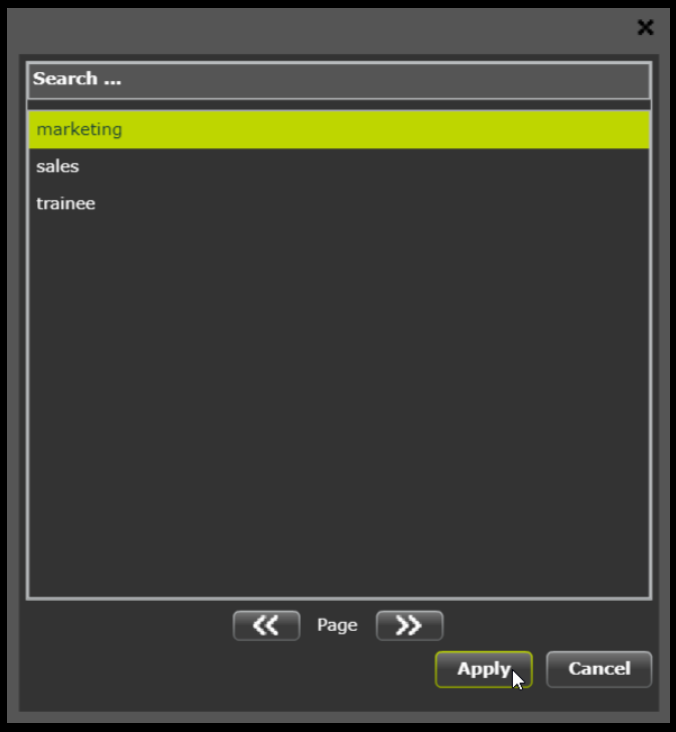


Figure 196: Select user or group

7. Click on **Add**, to add the domain.

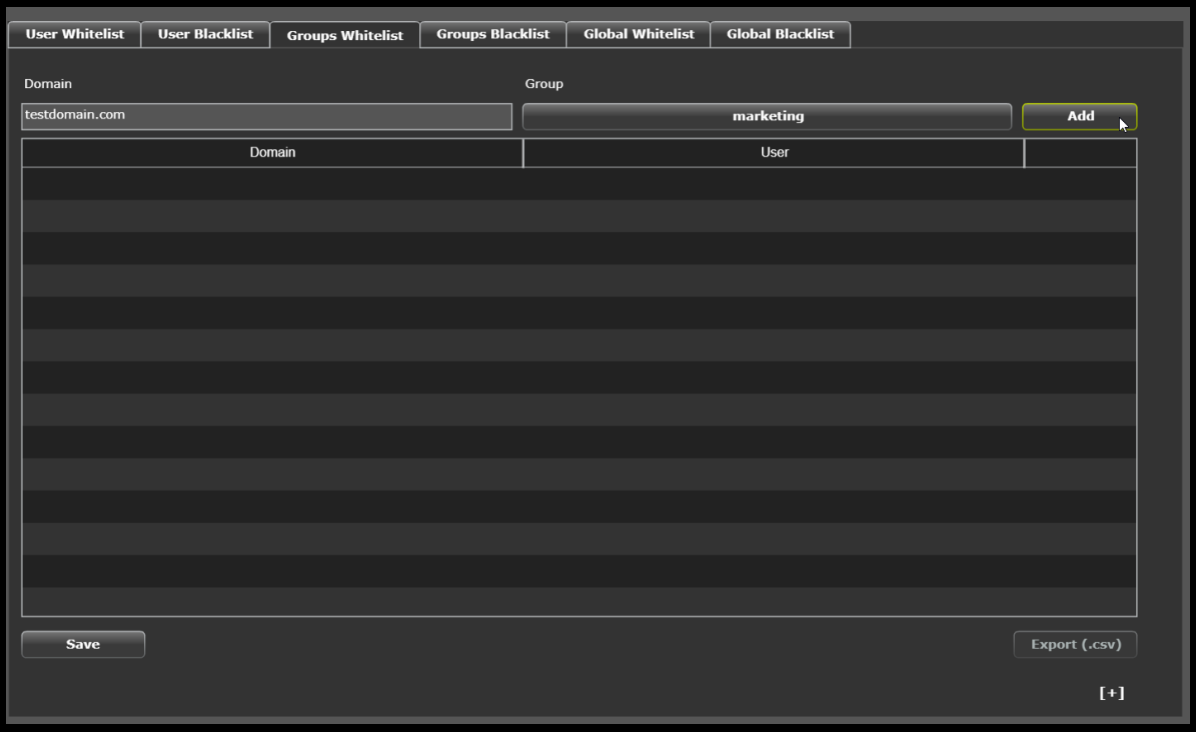


Figure 197: Add domain

8. Confirm with **Save**.

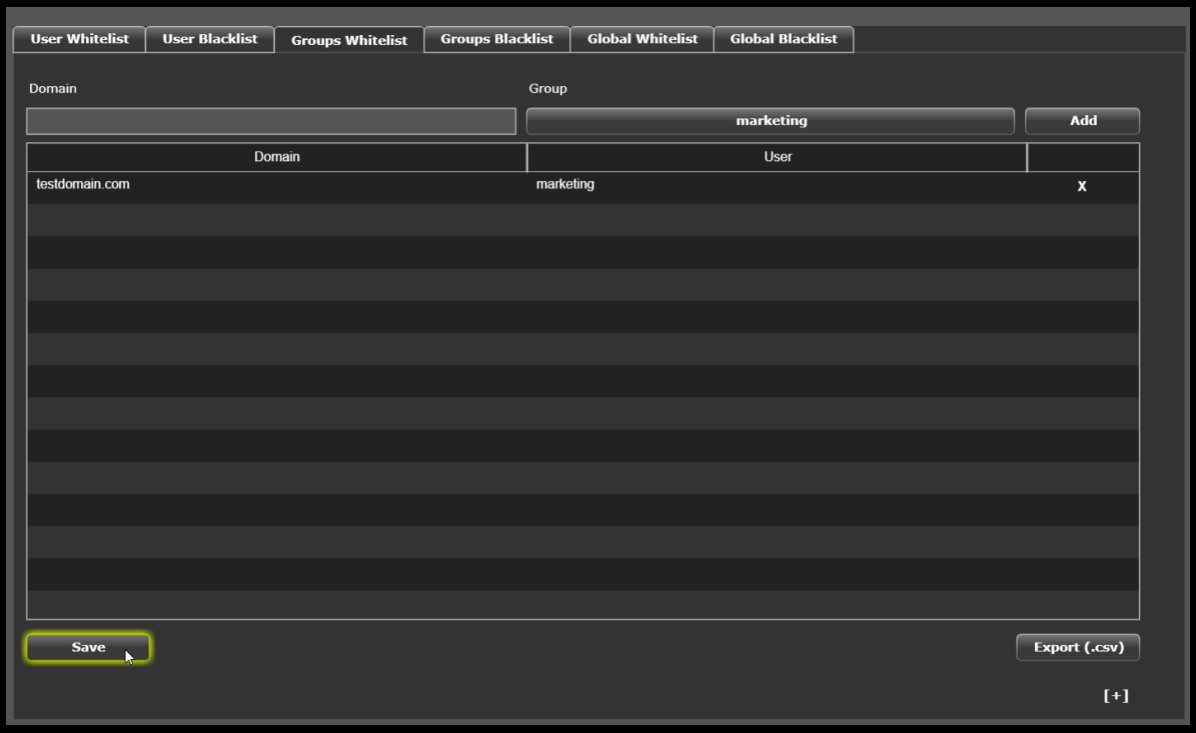


Figure 198: Save entry

The domains were blocked or released by black or white lists.

Releasing a Website Specifically

Do the following if you would like to block the whole category but release certain websites of the same category for your users:

1. Block the relevant category (e.g. Social media) as shown in Defining Web Filter Categories for a Group on page 207.
2. Put the desired website (e.g. XING) on the whitelist of the Web Filter (see Blocking or Releasing Domains via Black or White List on page 193).

The website has been released specifically.

Locking Websites Specifically

Do the following if you would to release the whole category but block certain websites of the same category for your users:

1. Unlock the appropriate category (e.g. Social media) as shown in Define Webfilter Categories for a Group.
2. Put the prohibited websites on the blacklist of the Webfilter as shown in Black- and Whitelist of the Webfilter.

The websites have been locked specifically.

Configuration

Activating Web Filter for an Individual Domain

1. Navigate to your primary domain in the Control Panel.

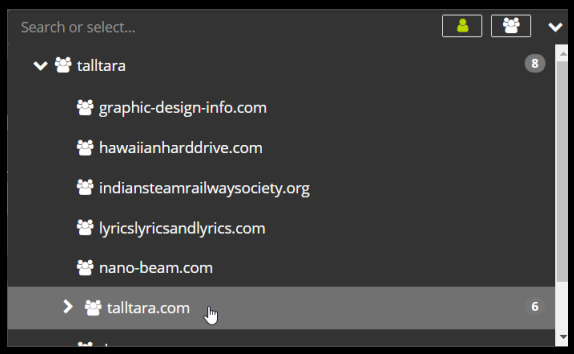


Figure 199: Select primary domain

2. Select **Web Filter#→Configuration**.
3. Check the box **Activate Web filter**.

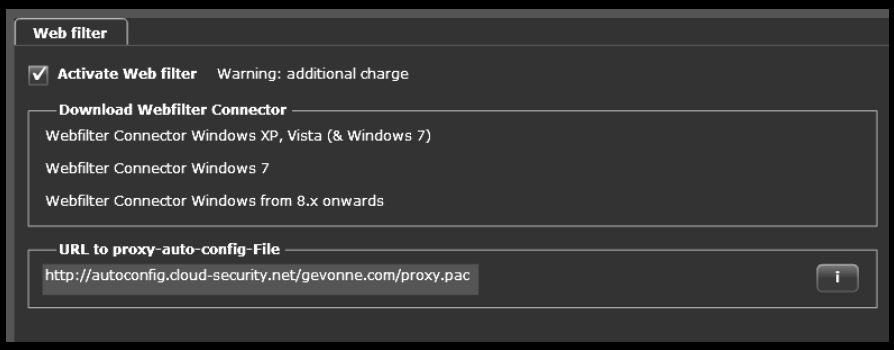


Figure 200: Activate Web Filter

4. Enter the email address, which gets Web Filter requests (e.g. requests for releases), in the field **Administrator Email**.

Notice:

If you check the box **Email on release requests**, requests for releases and corrections from users are sent to the entered administrator's email address.

5. Select the desired method for authentication:

   A multiple selection is possible.

   - If you activate the checkbox **user-based access**, you activate the authentication by the Web Filter Connector or by entering the user address and the password manually.
   - If you activate the checkbox **IP address-based access**, you allow access to the Web Filter Service for a certain IP address. If an access is made by an authorized IP address, no user authentication is necessary. However, the Web Filter rules of the group "Default" are applied. Further adjustment of the rights management is not possible in this case.

     Notice:

     You can enter IP addresses with slash notation (0.0.0.0/24) or you can separate IPs with a semicolon.

   - If you activate the checkbox **LDAP authentication**, users are authenticated by a directory service (e.g. Active Directory).

     Notice:

     Note that this configuration needs to be adjusted to the installation of a LDAP comparison by the support.

6. Optional: Activate the checkbox **Check HTTPS data** to be able to check and filter encrypted website calls by the Web Filter.

   Important:

   In addition to the activation in the Control Panel, you have to install the SSL certificate on all client computers. This is described in the chapter Installing the HTTPS Certificate on Windows.

   The field **Download HTTPS - Certificate** appears in the menu.

Figure 201: Download link for HTTPs certificate

7. Optional: Activate the checkbox **Select individual email recipient for release request** to add a person who can also get release requests besides an administrator. Enter this person in the area **Group**.
8. Confirm the booking of the Web Filter with **Save**.

The Web Filter has been activated for an individual domain.

Example: Activate Web Filter Services for the domain talltara.com

In this screenshot the previous steps are marked.

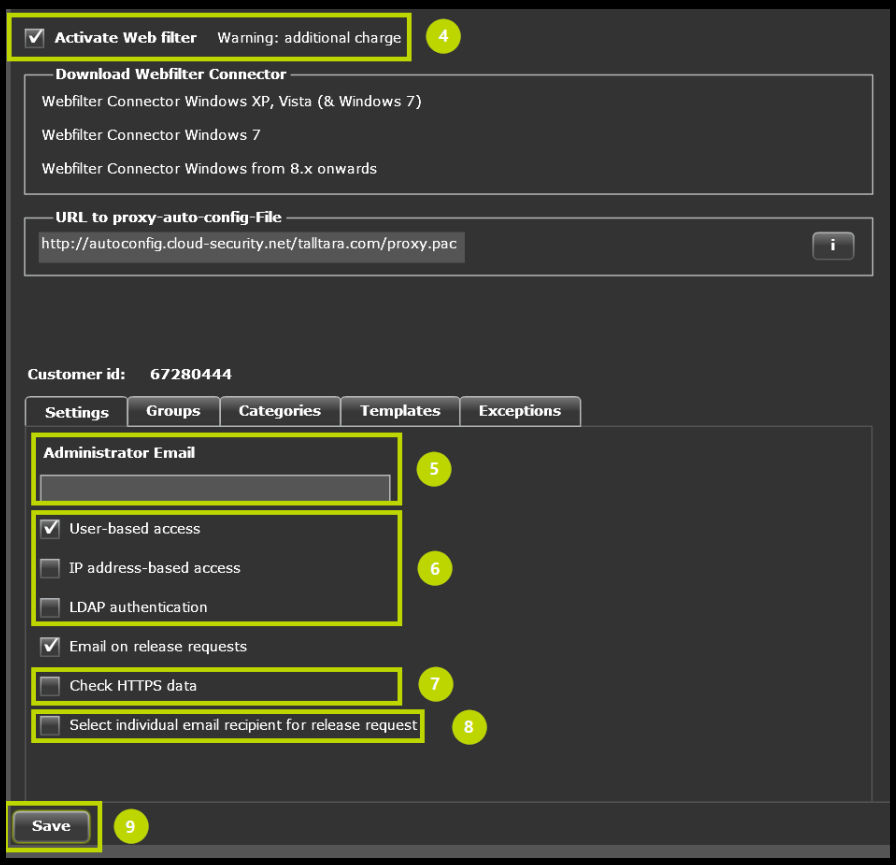


Figure 202: Activate web filter

Gruppeneinstellungen

Description of Group Settings

In the Control Panel you can configure group specific rules for the internet usage under **Web Filter#→Configuration#→Groups#→Settings**.

You can set different rules for the Web Filter for each group. It is possible to define a group leader for each group who can reject or confirm release requests for websites.

- **Activate group**: Check this box to activate or block the internet usage for the appropriate group generally.
- **Allow user to request a release**: Check this box to allow users to request releases for blocked websites.
- **Email group leader**: Enter the email address of a person who belongs to the group. This person decides upon release requests within a group.
- **Enable advertising filter**: Check this box to specify that advertising banners are to be blocked.
- **Block uncategorized URLs**: Check this box to define how the Web Filter should behave in case of unknown websites.
- **Enable virus protection:** The virus protection is always active and cannot be deactivated.
- **Block hacked server**: Check this box to specify if the access to manipulated websites should be blocked.
- **Enable ftp connections:** Activate this option to allow FTP connections.

  Notice:

  This option is obsolete because FTP is supported in general.

- **Allow temporary release**: Check this box to allow users to unlock blocked websites for a certain period of time (15 minutes). There are three differences:
  - If you check the box **Off**, it is not possible to unlock blocked websites temporary.
  - If you check the box **All**, all users are able to unlock all blocked websites.
  - If you select a **Group leader**, all categories that have a red lock in the categories are excluded from the release option. See Web Filter Categories on page 206 for more information.

> **Notice:**
>
> It is important for this function that the administrator can view all temporary releases in the Web Filter Display (see Editing Settings in the Web Filter Module on page 188).

- **Forbidden file extensions**: To block the download of certain file extensions, enter the file extensions here and click on **Add** to create a list of file extensions that should be blocked.

> **Important:**
>
> Always enter file extensions with a dot before the letters (**.exe**).

If you would like to reset the settings to default, click on **Default** in the upper right corner.

Defining Break Times

You can define break times, which deactivate the Web Filter for certain groups in this time, under **Web Filter**#→**Configuration**#→**Groups**#→**Break times**.

1. Select the tab **Break times** under the tab **Groups**.
2. Select the appropriate group.

   a) Click on **Select**.

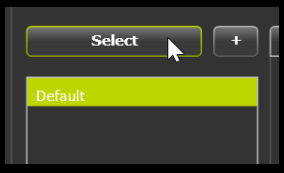


Figure 203: Open selection menu

   b) Select a group from the list.

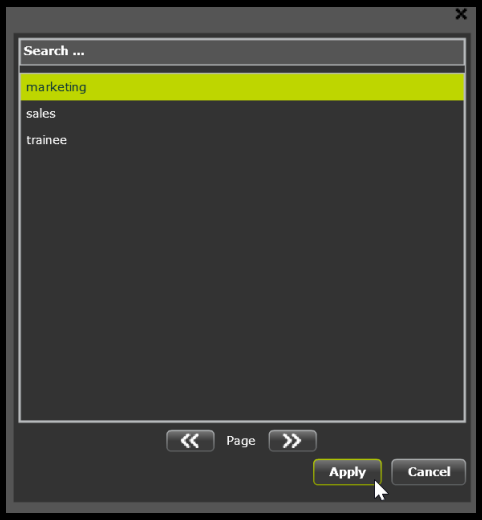


Figure 204: Select group

c) Click on **Apply**.

d) Click on **+** to add the group.

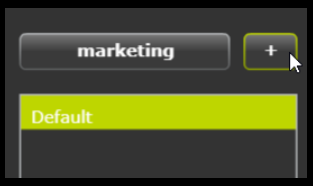


Figure 205: Add group

You have added the group.

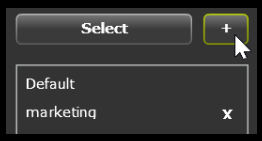


Figure 206: Added group

3. Click on **Add break times**.
4. Adjust the regulators on the timeline so that the desired break time appears in the window underneath.
5. Select the days for which this break time should apply.

> **Notice:**
>
> Repeat steps 3 to 5 to add further break times.

6. Click on **Save** to apply the defined break times.

The break times have been defined.

Define break times for a certain group

Figure 207: Define break times

Controlling Applications

You can block, release or temporarily release the access to the internet for certain applications (e. g., Skype, MSN, ICQ) with the **Application control** under **Web Filter#→Configuration#→Groups#→ Application Control**.

> **Important:**
>
> You can only use this function when the Web Filter Connector is installed (see Web Filter Connector).

1. Select the tab **Application control** under **Groups**.
2. Select the appropriate group.

   a) Click on **Select**.

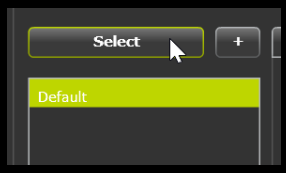


Figure 208: Open selection menu

   b) Select a group from the list.

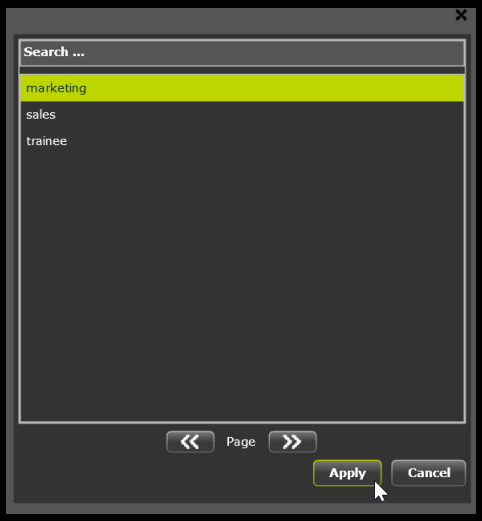


Figure 209: Select group

   c) Click on **Apply**.

   d) Click on **+** to add the group.

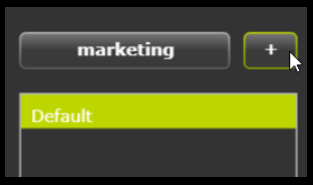


Figure 210: Add group

You have added the group.

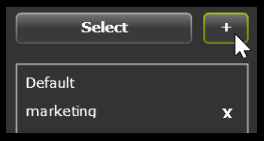


Figure 211: Added group

3. In the right area of the window you can select if the predefined programs should be **Allowed**, **Blocked** or just be **Break times** for the selected group.
4. Click on **Save** to confirm.

The applications for a certain group have been controlled.

Control applications for a certain group

In this screenshot the application **Skype** is changed for the group **marketing** from the Setting **Like default** to **Allowed**.

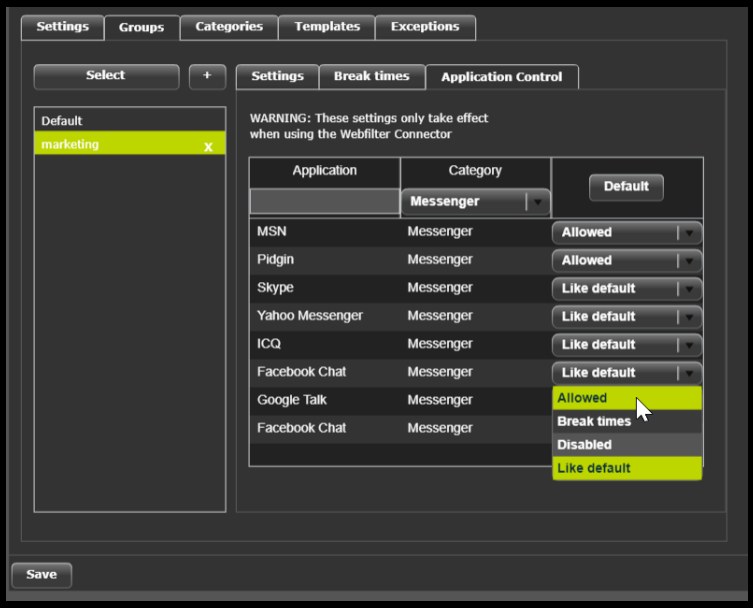


Figure 212: Application Control

Web Filter Categories

The setting for allowed and blocked website categories is made group-specific. The categories are separated in root and subcategories. For example, under the category **Internet** is the subcategory **Chat**. For each category you can select if it is **Allowed**, **Disabled** or **Break times**.

After the activation of the Web Filter all categories are disabled. To have a basis for your group settings, you can set rules for the group **Default**. This group applies to all users if you have not set further rules yet.

Click on **Default** to select a group setting.

Figure 213: Basic configuration for the group Default

Furthermore, you can define which categories can be temporarily unlocked by a group leader after a release request.

If a category is blocked, the lock turns green. If you click on the green lock, it turns red and is blocked for temporary releases by the group leader.

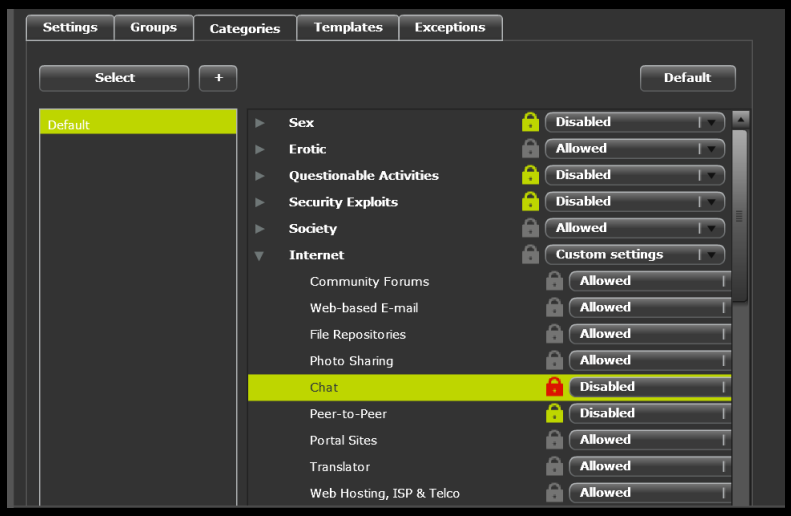


Figure 214: Lock temporary release

Defining Web Filter Categories for a Group

Starting from the basic settings for the **Default** group, you define group-specific settings for the Web Filter.

1. Select the tab **Categories** in the Web Filter settings.
2. Select the appropriate group.

   a) Click on **Select**.

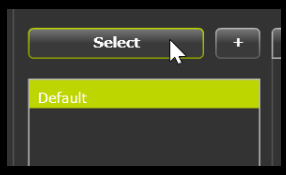


Figure 215: Open selection menu

   b) Select a group from the list.

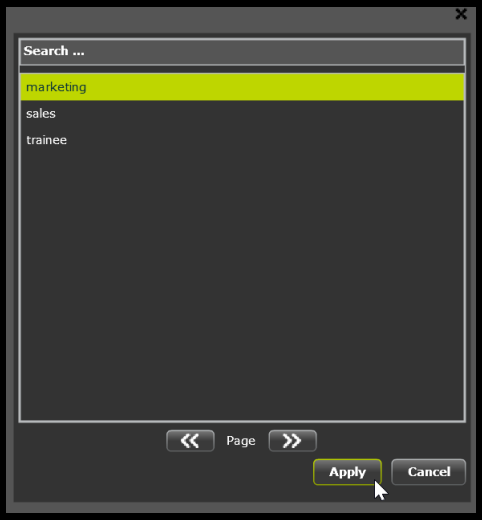


Figure 216: Select group

c) Click on **Apply**.

d) Click on **+** to add the group.

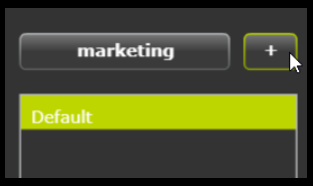


Figure 217: Add group

You have added the group.

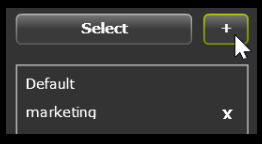


Figure 218: Added group

3. Select a category for which you would like to specify a setting differing from the default setting.
4. To open a subcategory, click on the **arrow** to the left of the category.

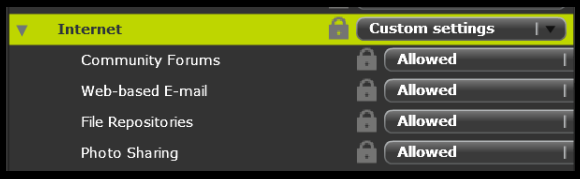


Figure 219: Click on arrow

5. Select an action from the drop-down menu on the right side of the selected category.

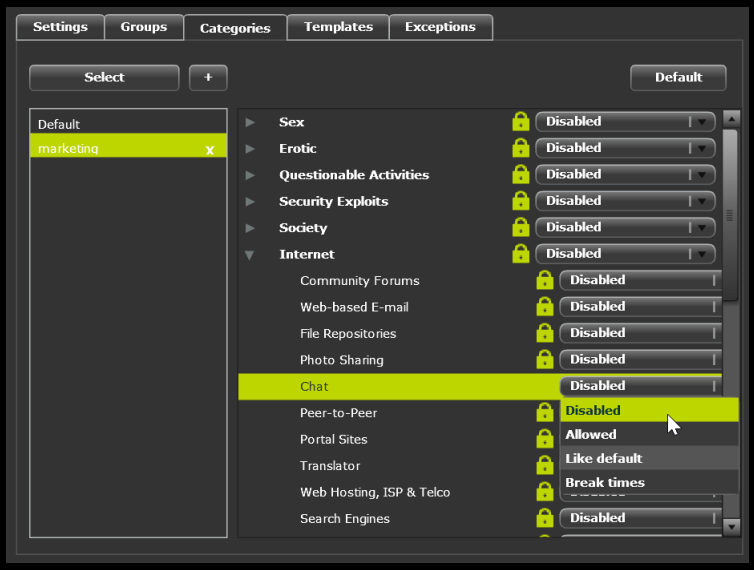


Figure 220: Allow chat in subcategory

6. Click on **Save** to confirm your changes.

The Web Filter categories for a group have been defined.

Web Filter Templates

In the tab **Templates** you can choose between different templates, which appear, e.g., when surfing on a blocked website. You also have the option of setting the languages of the various web filter templates.

Notice:

No new templates can be created in the HTML-CP!

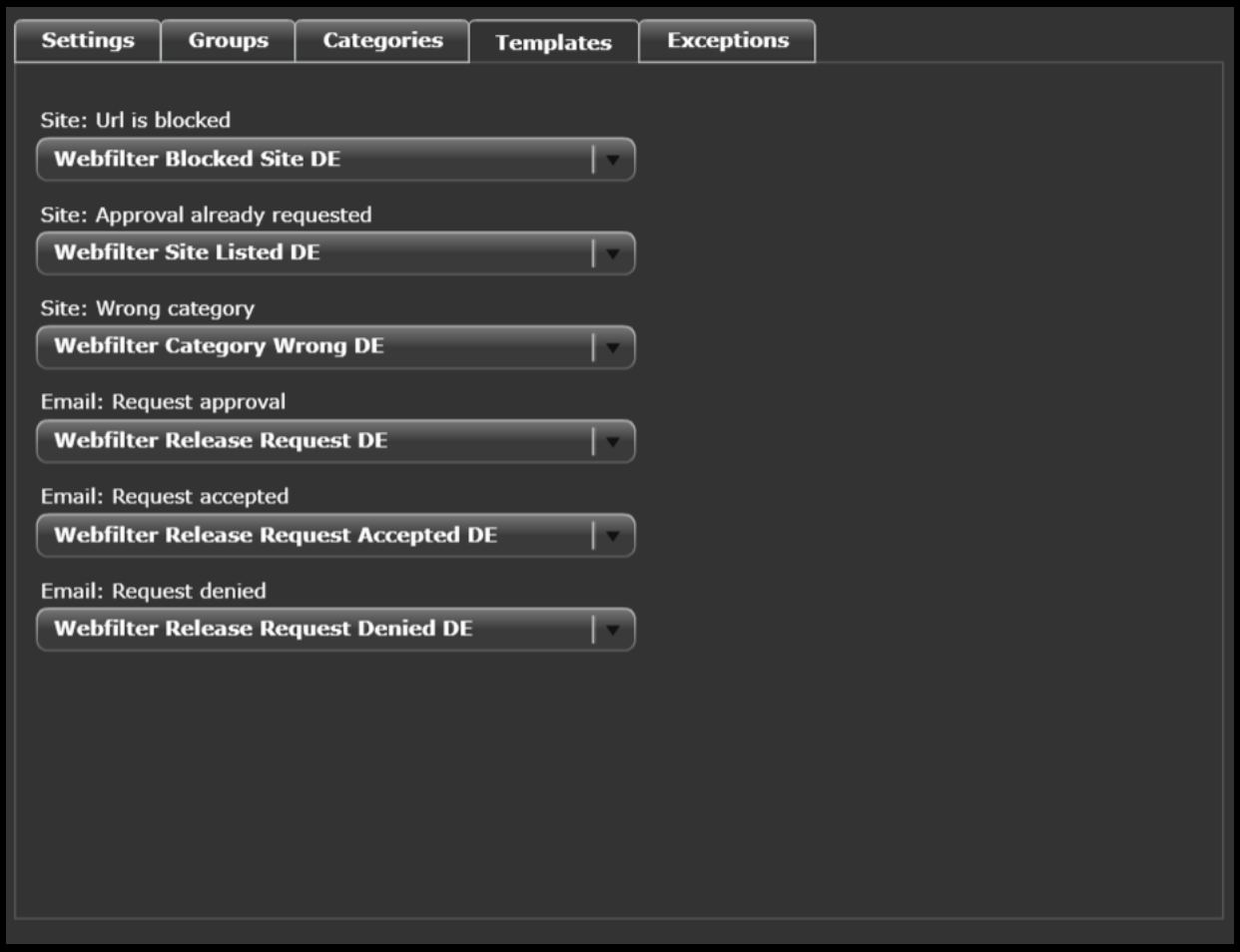


Figure 221: Templates

Exceptions

You can define website requests that are not be regulated by the Web Filter, in the area **Exceptions**.

> **Important:**
>
> The divergent settings are only active in connection with the Proxy Pac (see Setting Proxy Settings).

If you do not want to regulate the traffic for certain web servers (e.g. internal web servers which are directly addressed by the IP address) by the Web Filter, you can add web server addresses to the exception list.

The IP address access to websites is also possible by dynamical IP addresses.

Notice:

You can enter keywords with regular expressions. If these can be found in an URL, these pages will not be filtered either.

Defining Exceptions

1. Select the tab **Exceptions** in the Web Filter settings.
2. Enter the exceptions.
   Use a **;** (semicolon) as a separator between the exceptions.

Figure 222: Exceptions

3. Click on **Save** to confirm your settings.

Exceptions have been defined.

Statistics

Web Filter Statistics

The Web Filter statistics enable a comprehensive evaluation of the email traffic.

In the Control Panel you can display comprehensive statistics of the email traffic under **Web Filter#→Statistics**. The period can be the current day, the preceding three days or the preceding months. When a day is selected, all blocked and allowed domains as well as the most frequently blocked and allowed domains per hour are displayed.

When a month is selected, the distribution per day is shown. Additionally, you have the possibility to show the hourly distribution of the respective day if you click on a day of the month. If you select a month, the distribution per day is displayed. The information of the percentage distribution are independent from the period. They show the current distribution of blocked and allowed domains of the current hour, the current day or the month.

In addition to the total value, the distribution per topic is displayed.

Customer Settings

Under Customer Settings, you can view and manage the basic settings for mailboxes, groups, domains, and password policies.

Note: To adjust settings for a customer, switch to the scope of the corresponding customer (domain) in the scope selection.

As an administrator, you can view settings for mailboxes, groups, domains, and password policies and change them as follows:

- Managing basic user data
- Adding/removing alias addresses,
- Defining a deputy
- Setting delivery times for filters & reports
- Managing group members
- Changing group names
- Adjusting group descriptions
- Deleting groups
- Deleting domains
- Adding new mailboxes / forward mailboxes / groups / domains
- Exporting existing mailboxes / groups / domains as a CSV file
- Importing existing CSV files with mailboxes / / domains
- Defining password policies
- Assigning IP addresses

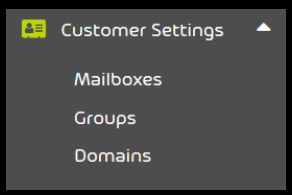


Figure 223: Customer settings in the Control Panel

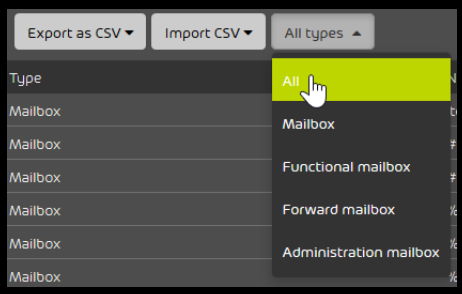
Mailboxes

Under **Mailboxes**, all mailboxes registered under your domain are displayed.

Mailboxes are the license basis for all services. In addition to a primary mailbox, several associated alias addresses can be created free of charge (see Adding an Alias Address on page 224).

The available mailboxes can be sorted by their type:

- Mailbox
- Functional mailbox
- Forward mailbox
- Administration mailbox



The stored data can be exported as a CSV file and imported again at suitable locations Importing Mailboxes from a CSV File on page 215.

You can use the following functions to manage and edit mailboxes:

Table 8: Manage mailboxes

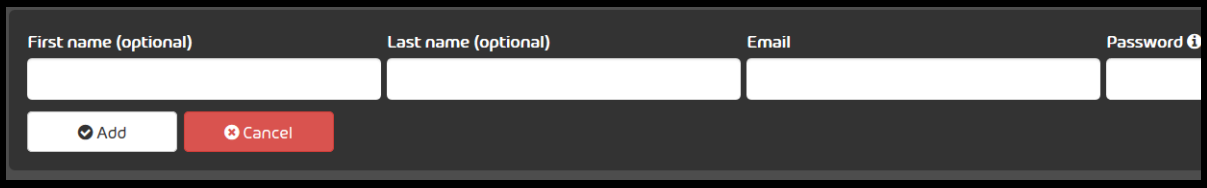
Symbol	Name	Description
	Basic data	Customize user data
	Change password	Change the password
	Active/Inactive	Activate or deactivate the mailbox
	Aliases	Add alias addresses to a primary mailbox
	Delegate	Enter a delegate for the mailbox

Symbol	Name	Description
	Spam Report	Configure the Spam Report
	Delete	Delete the mailbox

Adding a Mailbox

You have the possibility to add more mailboxes.

1. Navigate to **Customer Settings#→Mailboxes**.
2. Click on Add mailbox.
   A drop-down menu opens.



3. Fill in the fields.

> **Notice:**
> Enter a valid email address and assign a password that complies with the password guidelines.

4. Click on **Add** to add the mailbox.

You have added a mailbox.

Importing Mailboxes from a CSV File

Import primary mailboxes and their associated alias mailboxes from a CSV file.

Instead of entering mailboxes manually, you can import mailboxes from a CSV list. You can import mailboxes from a CSV list both initially, when no data has been entered yet, as well as anytime later. You can either update or remove the entries that already exist in the Control Panel.

1. Navigate to **Customer Settings#→Mailboxes**.
2. Click on **Import CSV**.

A new menu opens.

Figure 224: Import list from CSV file with mailboxes

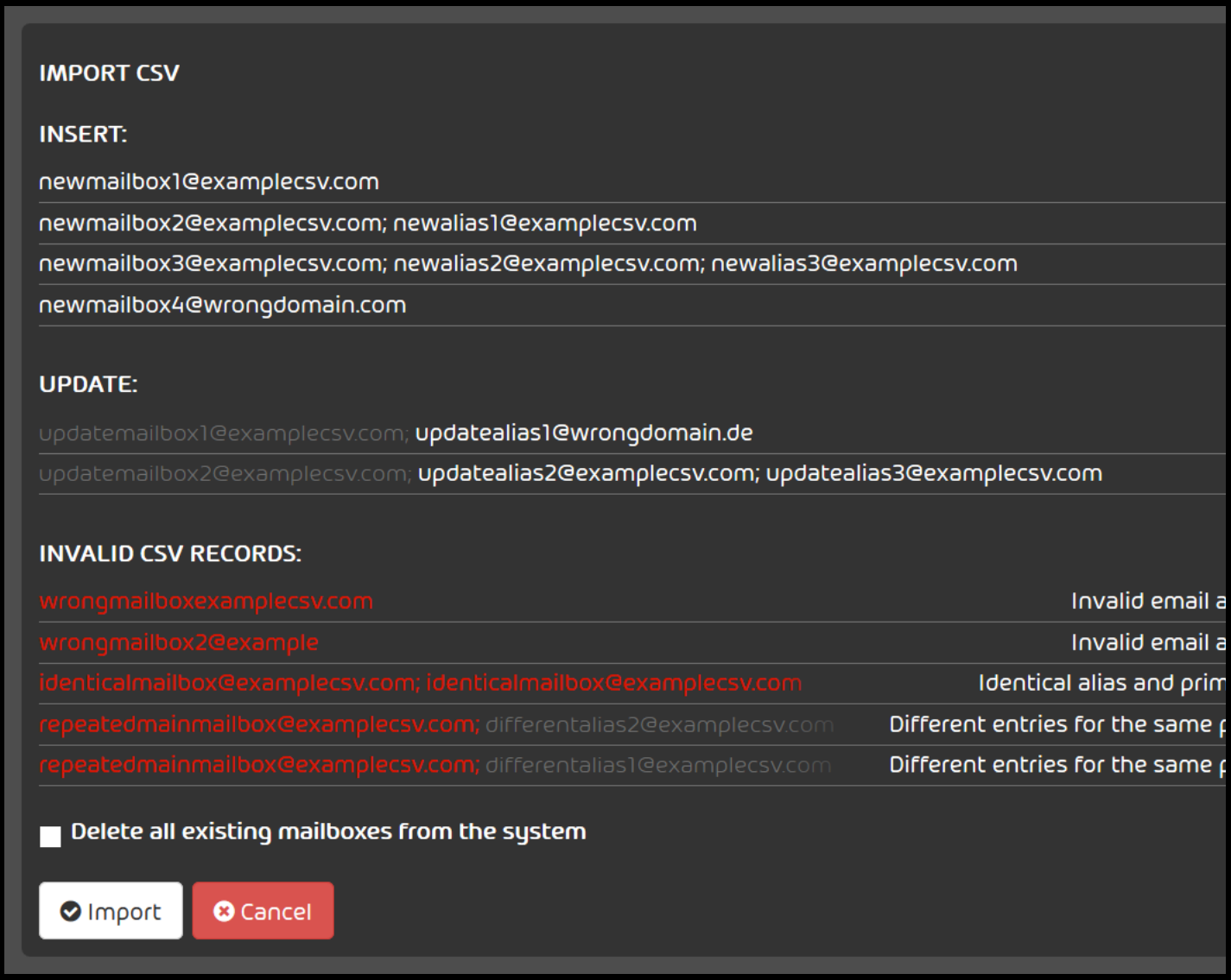
3. Click on **Upload file**.

   A file selection window opens.

4. 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 on page 228).

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.



Notice:

For more information about the errors listed here, see Mailbox Import Errors on page 220.

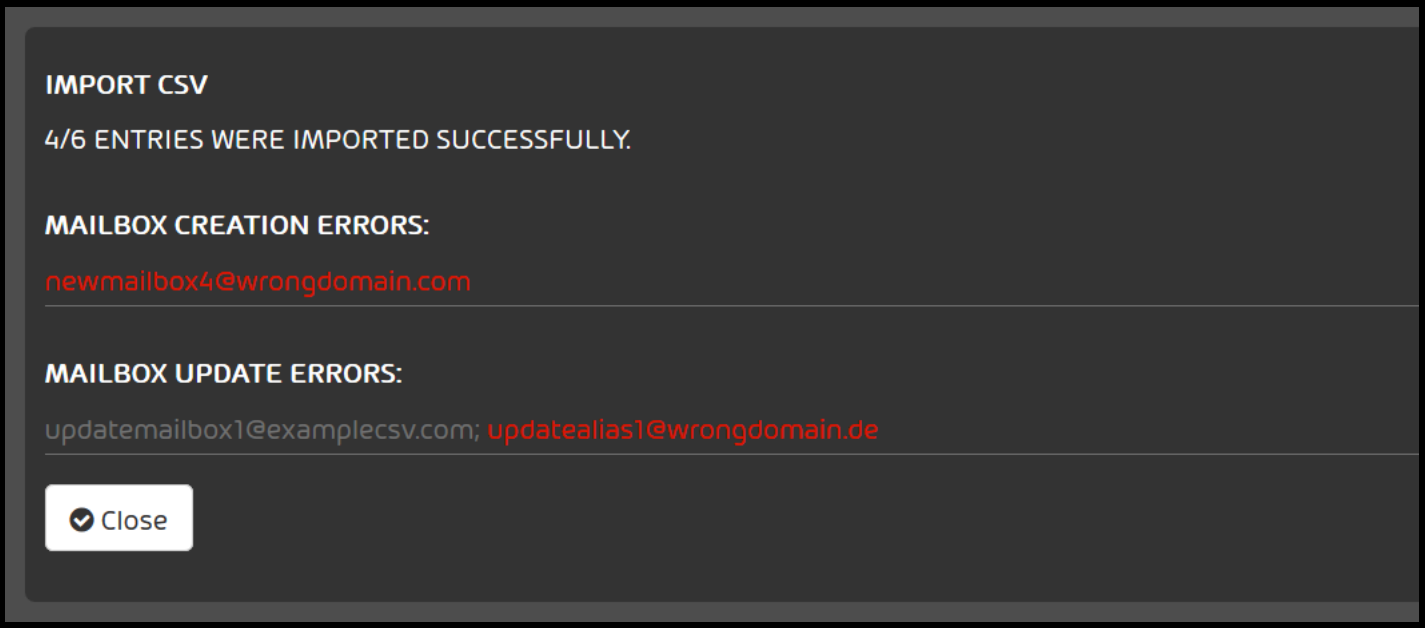
5. Optional: To delete all existing mailboxes in the system before importing new mailboxes, activate the **Delete all existing mailboxes from the system** checkbox.

CAUTION:

To avoid data loss, it is recommended to export the existing mailboxes before the import is performed with the **Delete all existing mailboxes from the system** checkbox selected.

6. Click on **Import**.

   The mailboxes listed in the summary are added or updated. The results of the import are then displayed.



Notice:

For more information about the errors listed here, see Mailbox Import Errors on page 220.

You have imported mailboxes from a CSV file.

CSV Files for Mailbox Import

CSV files for mailbox import must meet special requirements.

To ensure that an external CSV file with mailbox information can be imported into the Control Panel without errors, special rules regarding the file extension and content structure must be observed.

Rules for file extensions and columns

- The extension of the import file is **.csv**. Other file extensions, such as .txt or .docx, are not allowed and will not be accepted.
- The CSV file contains two columns separated by a comma.

  > **Important:**
  >
  > The second column is mandatory. Add a second column even if you do not want to add any alias mailboxes. In the first two rows, add a comma between the columns (see Rules for commas between the columns).

- The first row contains the column names, which can be freely defined.

Column names: **main,alias**

Formatting rules for mailbox addresses

- The addresses of the mailboxes must be correctly formatted (according to the pattern "local-part@hostname.top-level-domain").

  > **Important:**
  >
  > Incorrectly formatted addresses are not considered during the import.

- From the second row on, an address of a primary mailbox must be entered in the left column of each row.
- From the second row on, the addresses of alias mailboxes defined for the primary mailboxes listed on the left column can be entered in the right column.

Primary mailbox with an alias mailbox:
primarymailbox@example.com,aliasmailbox@example.com

Rule for several alias addresses

- If a cell of the right column is to contain several alias addresses, the content of this cell must be in quotation marks. The addresses must be separated from each other by commas.

Primary mailbox with several alias mailboxes:
primarymailbox@example.com,"alias1@example.com,alias2@example.com"

Rules for commas between the columns

- The left column must not be empty in any row.
- If the right column is empty, you can omit the comma between the columns from the third row onwards.

Valid rows without alias mailboxes: **primarymailbox@only.com,**, **primarymailbox@only.com**.

Rules for duplicated entries

- Duplicated entries do not affect the processing of the 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 right column.

Rows with the same primary mailbox and different alias mailboxes:

primarymailbox@example.com,"alias1@example.com,alias2@example.com"
primarymailbox@example.com,alias3@example.com

Error in case of identical primary mailbox addresses

Important:

Rows with a primary mailbox are not imported if the file contains another row with the same primary mailbox but different alias mailboxes.

Mailbox Import Errors

Various errors can occur when importing mailboxes.

When importing mailboxes, 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. This check checks for correctly-formatted addresses and repetitions. The following errors are possible and are listed in the subsequent summary under **Invalid CSV records**:

1. **Invalid email address format**: The listed addresses contain format errors (see valid format under CSV Files for Mailbox Import on page 219).

   > **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. **Identical alias and primary addresses**: In the affected record, the same address was specified as the main mailbox and as the alias mailbox.

3. **Different entries for the same primary address**: For a primary mailbox, the CSV file contains several records with different alias mailboxes. None of these records are imported into the Control Panel.

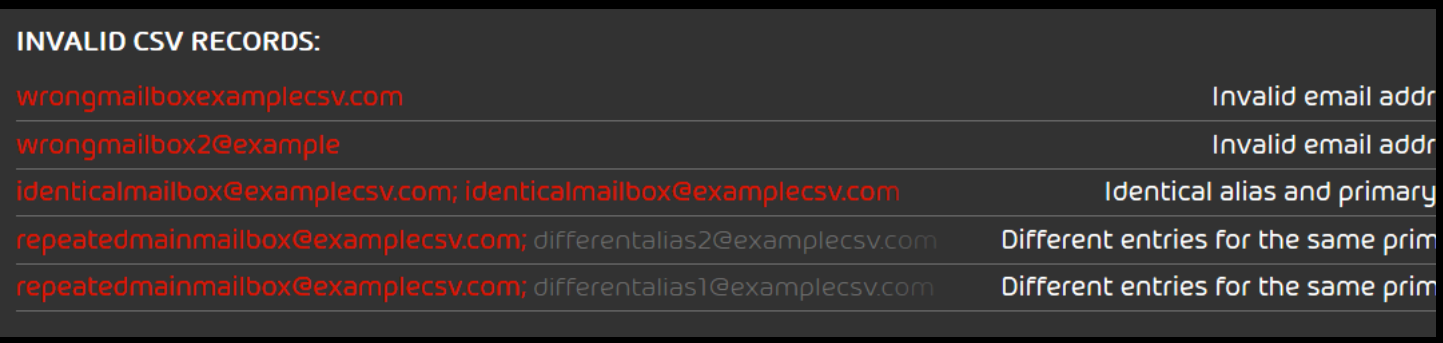


Figure 225: Error display after CSV file selection

The second check takes place after the user 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**, an import error occurs. In the following view of the import results these errors are listed sorted: either under **Mailbox creation errors** or under **Mailbox update errors**.

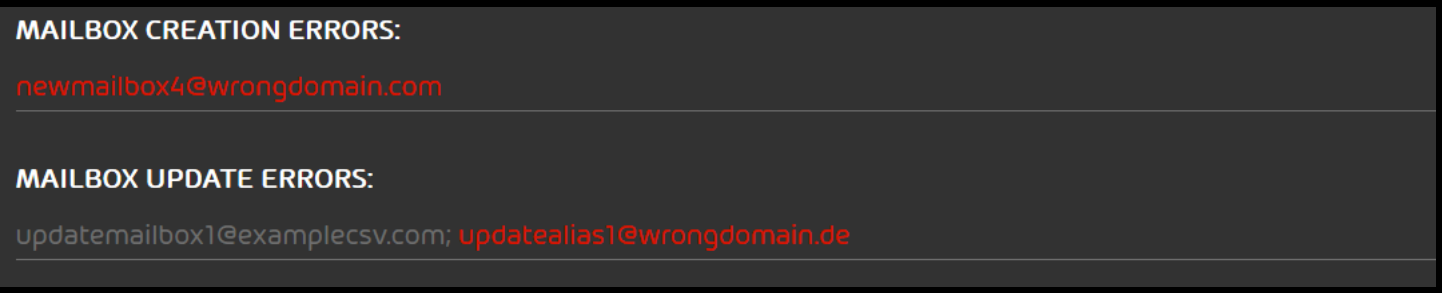


Figure 226: Error display after mailbox import from a CSV file

Notice: If these errors occur, the error-free contents of the affected CSV entries are imported.

Adding a forward mailbox

You can define forward mailboxes for existing mailboxes. These forward mailboxes can be set up to forward the email traffic to up to 100 internal or external mailboxes.

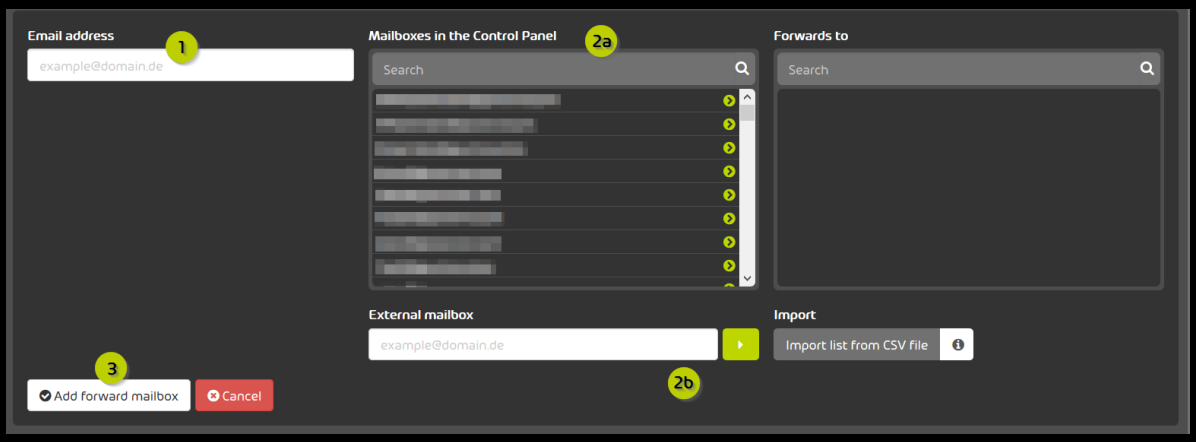
Your mailboxes are managed manually and not via LDAP.

Important: The maximum size for forwarding emails through forwarding mailboxes is limited and depends on the number of recipients. The following table shows the allowed size for forwarded emails according to the number of recipients.

Number of recipients	Max. allowed email size (MB)
1	100
2-9	50
10-24	25
25-49	15
50-100	10

1. Navigate to **Customer Settings#→Mailboxes**.
2. Click on Add forward mailbox.

A drop-down menu opens.



3. Under **Email address**, enter the mailbox for which you want to set up the forwarding. (1)
4. 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 click on to confirm.

> **Notice:** Repeat this step to add more forward mailboxes.

The mailboxes appear in the list **Forwards to**.

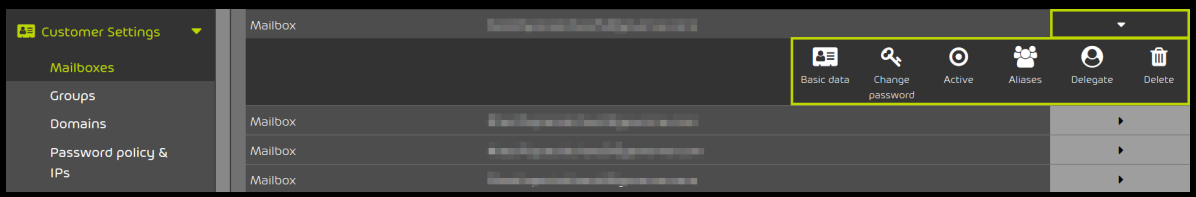
5. Click on **Add forward mailbox** (3) to set up the forwarding.

You have added a new forward mailbox.

Activating or Deactivating a Mailbox

You can activate or deactivate a mailbox.

1. Navigate to **Customer Settings#→Mailboxes** and click on the menu arrow of the corresponding mailbox.



2. Click on the button **Active** or **Inactive** to activate or deactivate a mailbox.

A drop-down menu opens.

3. Click on **Activate** or **Deactivate**.
   Depending on the activation status, the symbol is displayed in white (activated) or red (deactivated).

You have successfully activated or deactivated a mailbox.

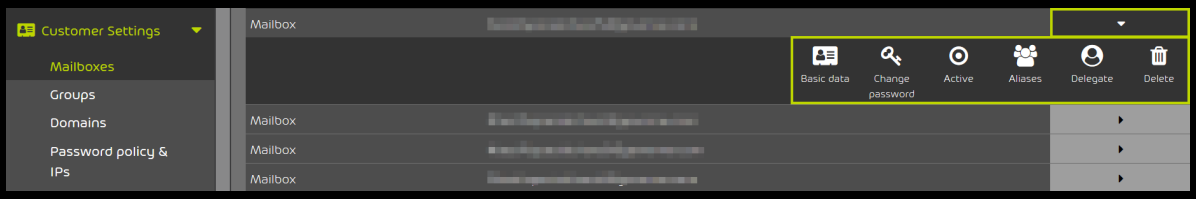
Adding an Alias Address

In addition to a primary mailbox, several associated alias addresses can be created, for which no fees are incurred.

Notice:

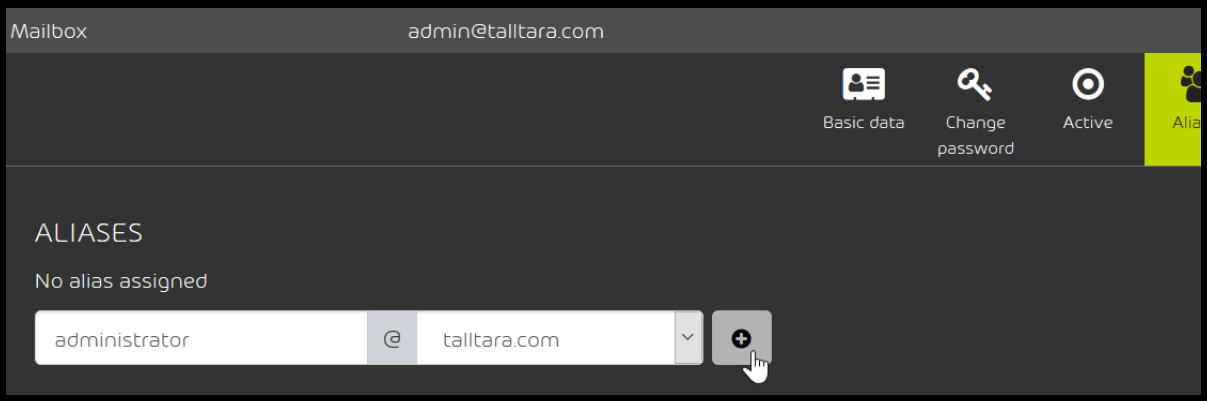
If alias addresses are assigned to a primary mailbox, the owner of the primary mailbox also sees the emails of the alias addresses under **Email Live Tracking**.

1. Navigate to **Customer Settings#→Mailboxes**.
2. Click on the menu arrow next to the desired mailbox.

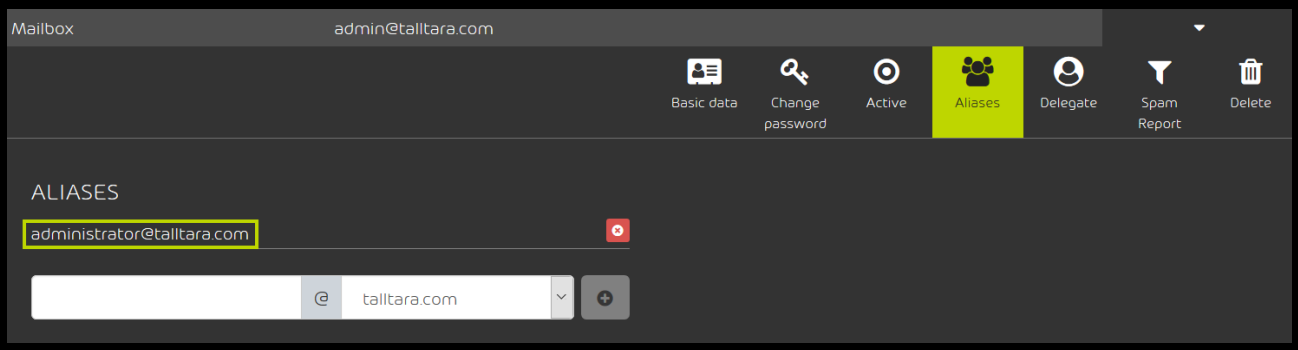


3. Click on **Aliases**.
   A drop-down menu opens.

4. Enter the desired alias under **ALIASES**, followed by the corresponding domain, and click on



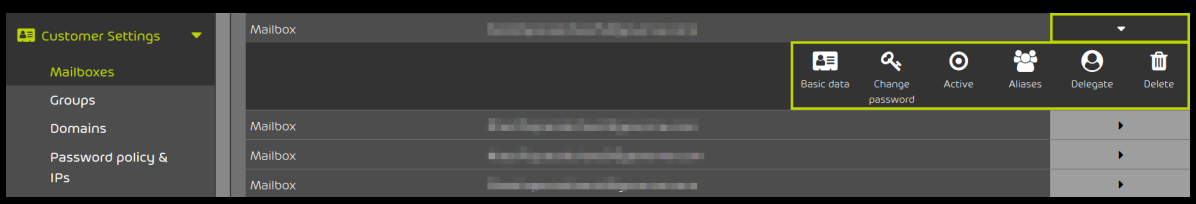
The alias address has been entered.



Entering a Delegate

You can enter a delegate for an existing primary mailbox.

1. Navigate to **Customer Settings**#→**Mailboxes**.
2. Click on the menu arrow next to the desired mailbox.

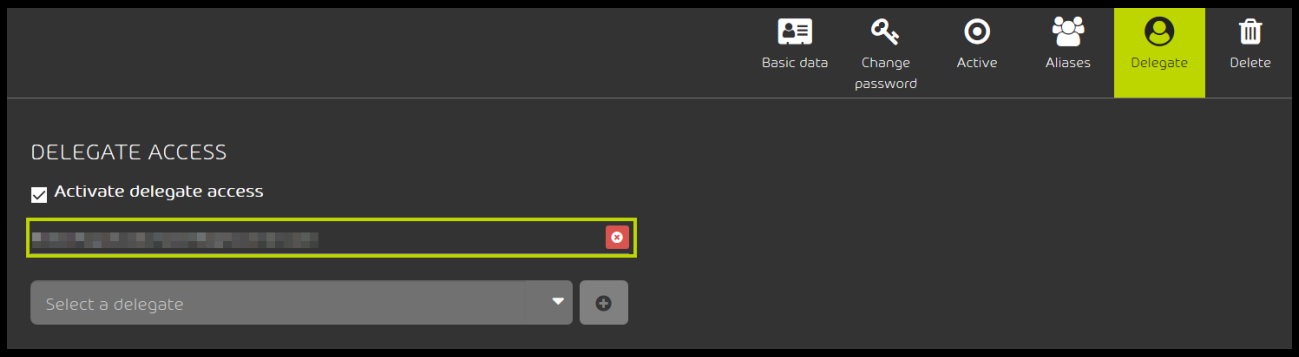


3. Click on **Delegate**.

   A drop-down menu opens.

4. Activate the checkbox **Activate delegate access**.
   A list of the registered users appears.
5. Select a delegate from the list and click on .

You have entered a delegate for the mailbox.



Importing Recipients for Forward Mailboxes from a CSV File

Import recipients for forward mailboxes from a CSV file.

Your mailboxes are managed manually and not via LDAP.

Instead of entering recipients for forward mailboxes manually, you can import them from a CSV list. This can be done both initially, when no data has been entered yet, and additionally during operation.

1. Navigate to **Customer Settings#→Mailboxes**.
2. Click on **Add forward mailbox**.
   A new form is displayed.

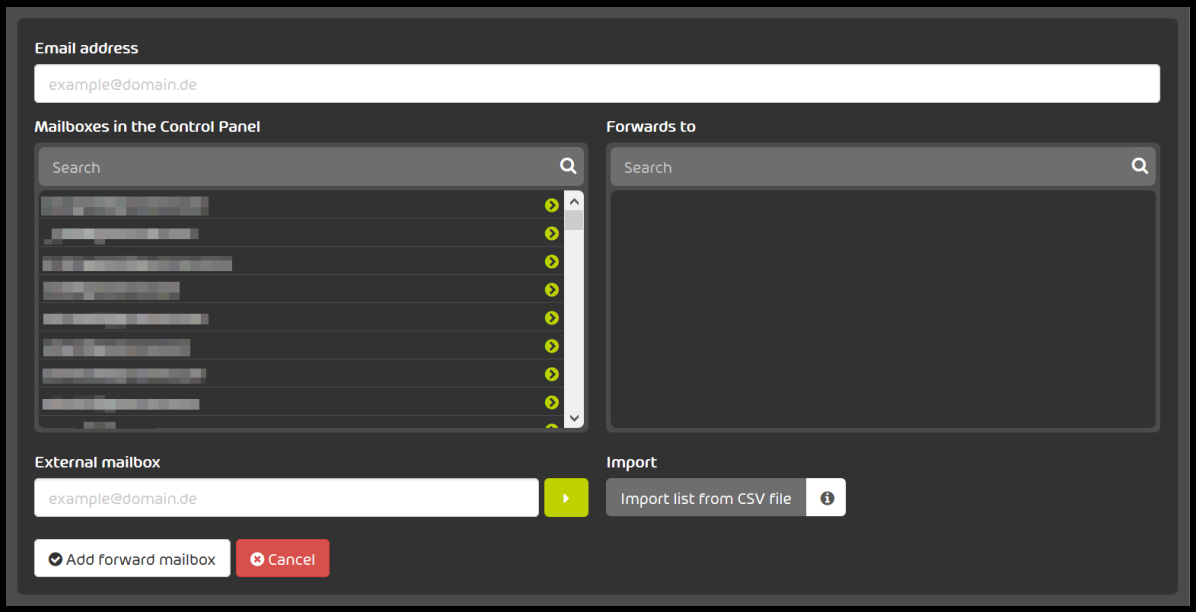


Figure 227: Import recipients for a forward mailbox from a CSV file

3. Enter the email address of the forward mailbox under **Email address**.
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 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 on page 228).

6. Click on **Import list from CSV file**.
   The recipients 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 which are already displayed under **Forwarded to** are not deleted.
- Only entries from the CSV file which 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.

7. Click on **Add forward mailbox**.

You have imported recipients for forward mailboxes from a CSV file.

CSV Files for the Import of Recipients

CSV files for the import of recipients for forward mailboxes must meet special requirements.

To ensure that an external CSV file with recipients can be imported into the Control Panel without errors, special rules regarding 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 contains always the column name and can be named individually.
- The addresses must be correctly formatted (according to the pattern "local-part@hostname.top-level-domain").

Important: Incorrectly-formatted addresses are not considered during import.

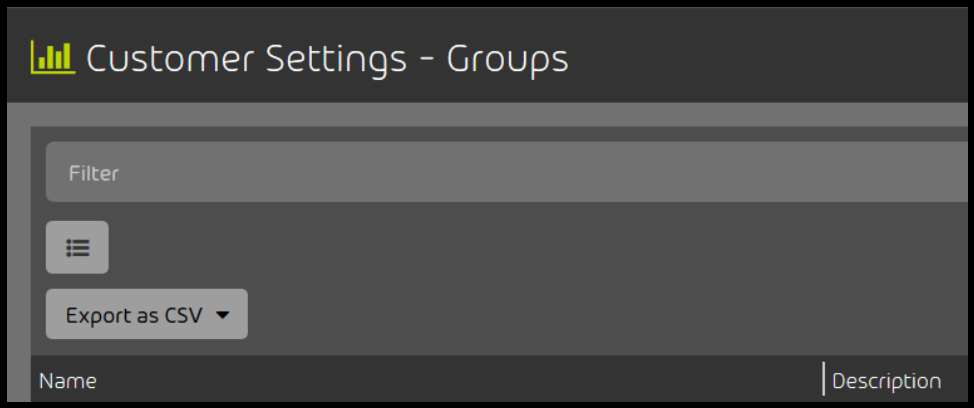
- Each row may contain only one address.

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

Groups

Under **Groups**, you can create, change or delete groups.

Under **Groups**, you can create new groups, combine several mailboxes into one group and manage the existing groups. Lists of group members of a group can be exported as CSV files.



The following options are available for managing groups:

Table 9: Manage groups

Symbol	Name	Description
	Details	Detailed information about the group
	Manage members	Add/delete members
	Rename	Changing the group name
	Customize description	Customizing the group description
	Delete	Delete a group

Adding a group

Create a new group from existing mailboxes.

1. Navigate to **Customer Settings#→Groups**.
2. Click on Add group
   A drop-down menu opens.

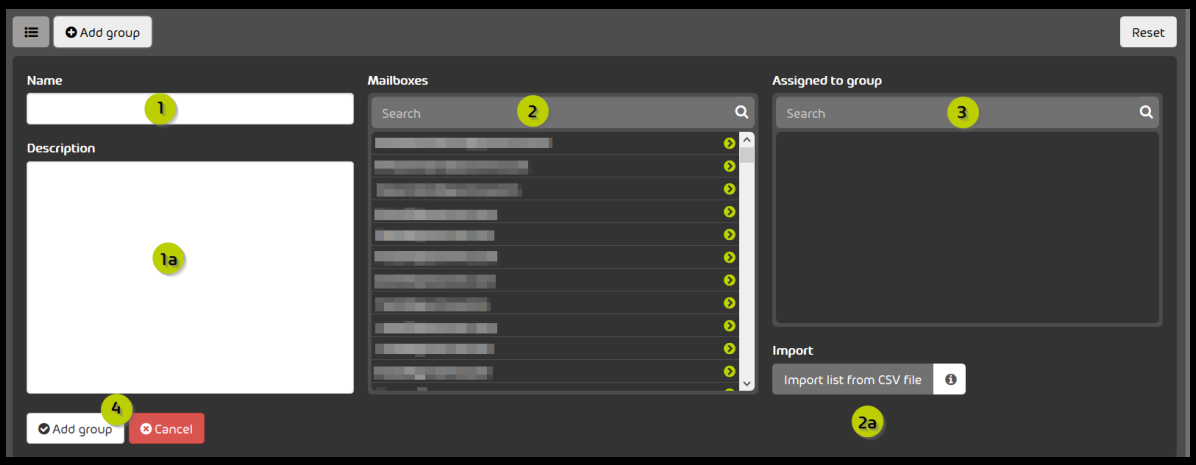


Figure 228: Add a new group

3. Assign a group name under **Name** (1). You can optionally add a description to the group in the field **Description** (1a).
4. Under **Mailboxes** (2), select at least one mailbox to add to the group.

> **Notice:**
>
> Previous member lists can be imported here from a CSV file (see Importing Group Members from a CSV File on page 230) (2a).

   The selected mailbox is displayed in the window **Assigned to group** (3).
5. Click on **Add Group** to combine the selected mailboxes into one group (4).

You have created a group from selected mailboxes.

Importing Group Members from a CSV File

Import group members from a CSV file.

Instead of adding users to a group manually, you can import users from a CSV list and assign them to a group. With a CSV list, you can assign users to both newly-created and existing groups.

1. Navigate to **Customer Settings#→Groups**.
2. You have two options:

a) Click on **Add group**.

➔ A new form is displayed.

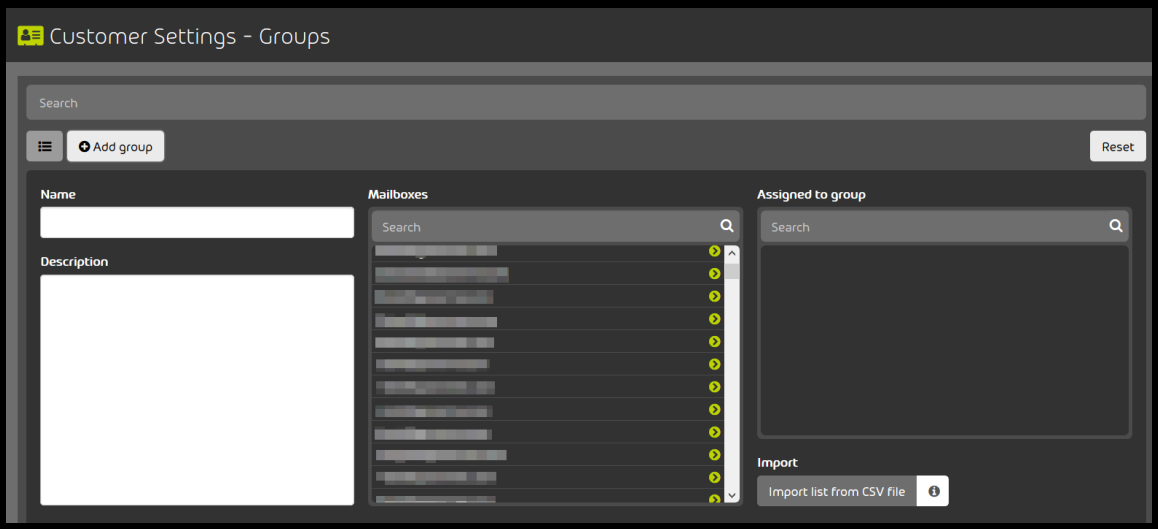


Figure 229: Import user name list from CSV file into a new group

b) Select an existing group at the bottom of the page and click **Manage Members**.

➔ A new form is displayed.

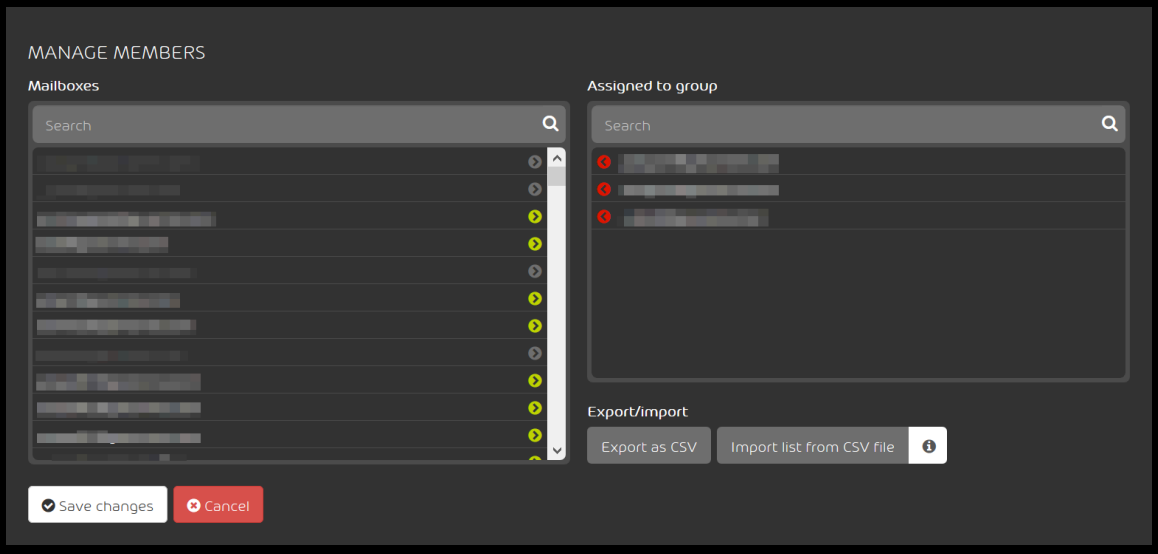


Figure 230: Import user name list from CSV file into an existing group

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

➔ A file selection window opens.

4. 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 232).

The users from the list who were not yet assigned to the group are displayed in the section **Assigned to group**.

Notice: The following rules apply to the import of group members:

- Group members which are already displayed under **Assigned to group** are not deleted.
- Only entries from the CSV file which are not already displayed under **Assigned to group** 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 appears informing about invalid entries.
- If the CSV file does not contain any valid addresses which are not already listed in the **Assigned to group** section, an error message appears and no addresses are imported.

5. Click on **Add group** or **Save changes** to save your changes.

You have imported users from a CSV file into a group.

CSV Files for Group Member Import

CSV files for group member import must meet special requirements.

To ensure that an external CSV file with information about group members can be imported into the Control Panel without errors, special rules regarding 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 contains always 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 import.

- Each row may contain only one address.
- Duplicated entries do not affect the processing of the file, but should be avoided.

Manage members

Manage the members of an existing group.

1. Navigate to **Customer Settings#→Groups** and click on the arrow for the desired group.

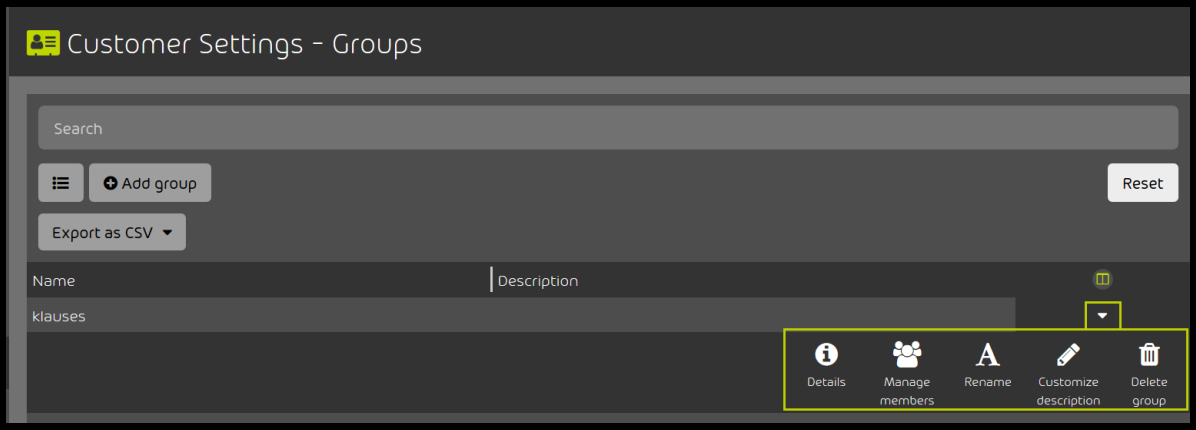


Figure 231: Open groups menu

2. Click on **Manage members**.

   A drop-down menu with two windows will open, showing all registered mailboxes (left) and all mailboxes assigned to the group (right).

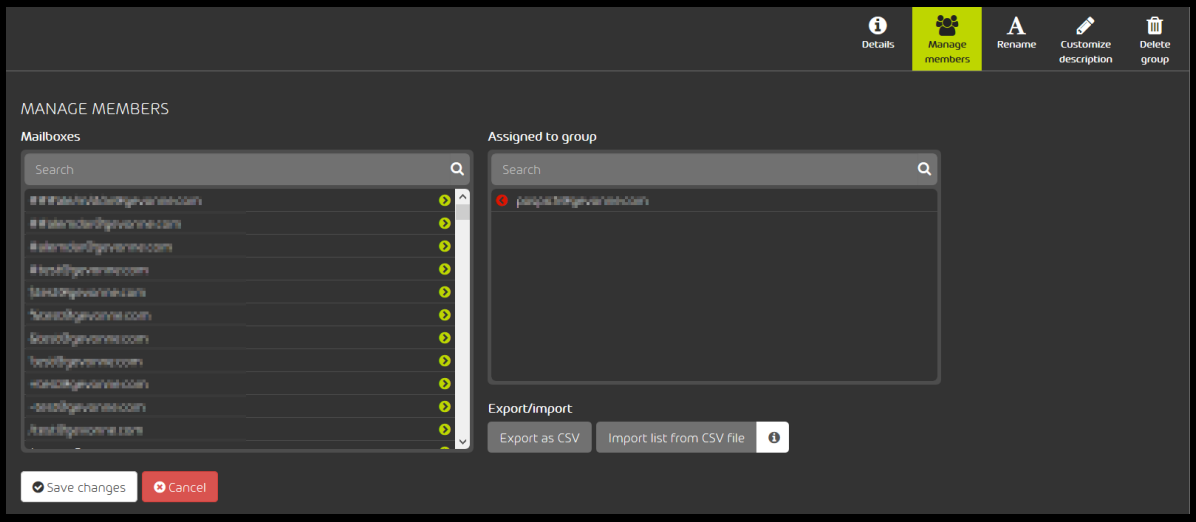


Figure 232: Manage group members

3. Manage the members of a group:

   - If you want to add more members to the group, click on the members to be added in the **Mailboxes** (left) window. You can also import existing group lists as a CSV file (see Importing Group Members from a CSV File on page 230).
   - If you want to remove already existing members from the group, click within the window **Assigned to Group** (right) on the group members to be removed.

   You have assigned or removed members from the selected group.

4. Click **Save Changes** to save the updated group.

You have successfully managed the group.

Renaming a Group

Rename a group.

1. Navigate to **Customer Settings#→Groups** and click on the arrow for the desired group.

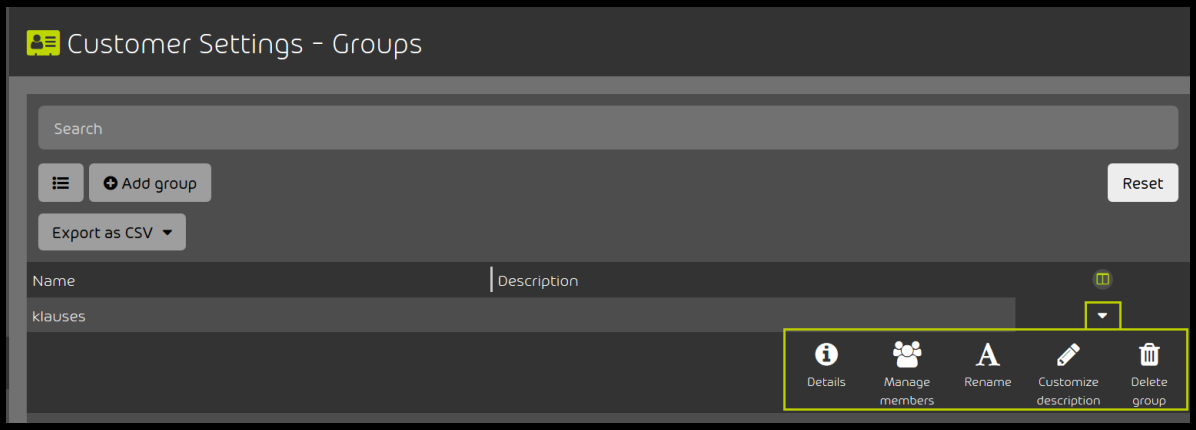
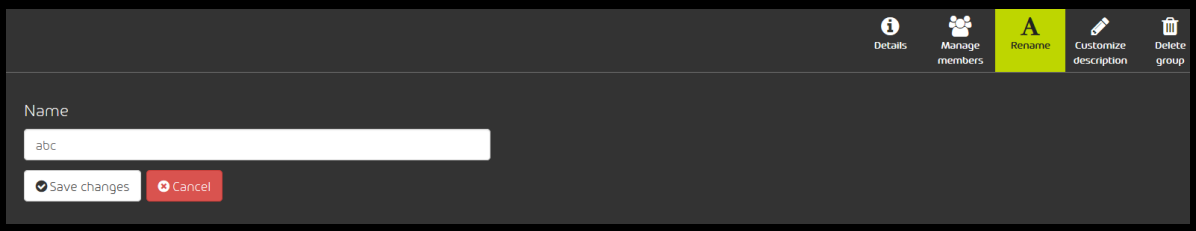


Abbildung 233: Open groups menu

2. Click on **Rename**.

   A drop-down menu opens.



3. Enter the desired name for the group and click **Save changes**.

You have successfully renamed a group.

Customizing a Description

Customize group description

1. Navigate to **Customer Settings#→Groups** and click on the arrow for the desired group.

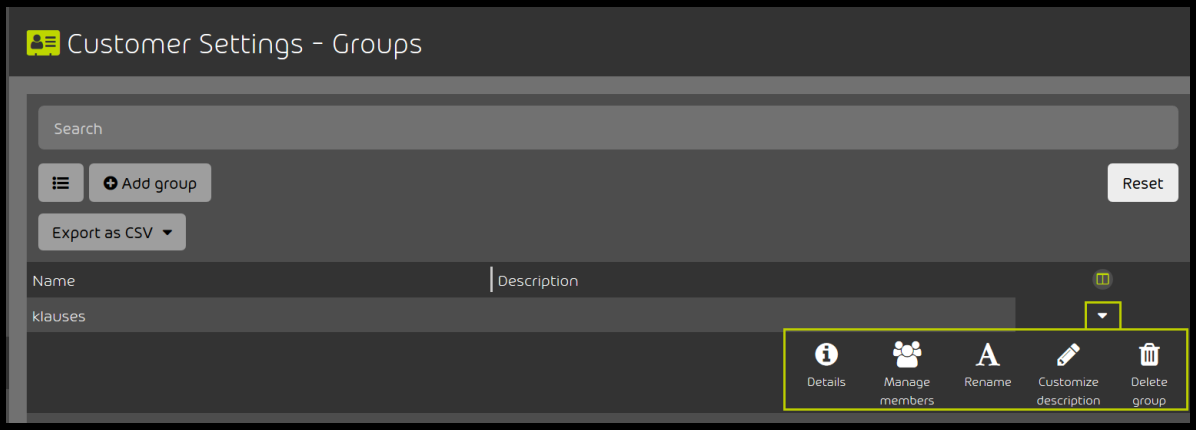
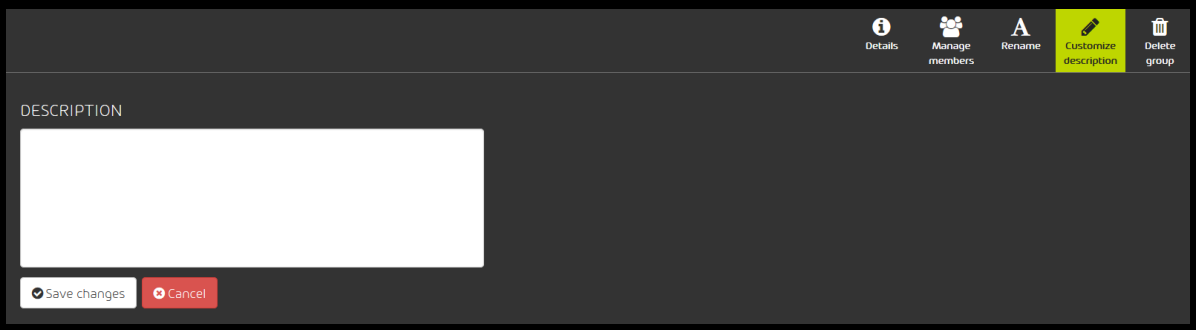


Figure 234: Open groups menu

2. Click on **Customize description**.
   A drop-down menu opens.



3. Enter the desired description for the group and click on **Save changes**.

You have successfully added the group description.

Deleting a Group

Delete an existing group.

1. Navigate to **Customer Settings#→Groups** and click on the arrow for the desired group.

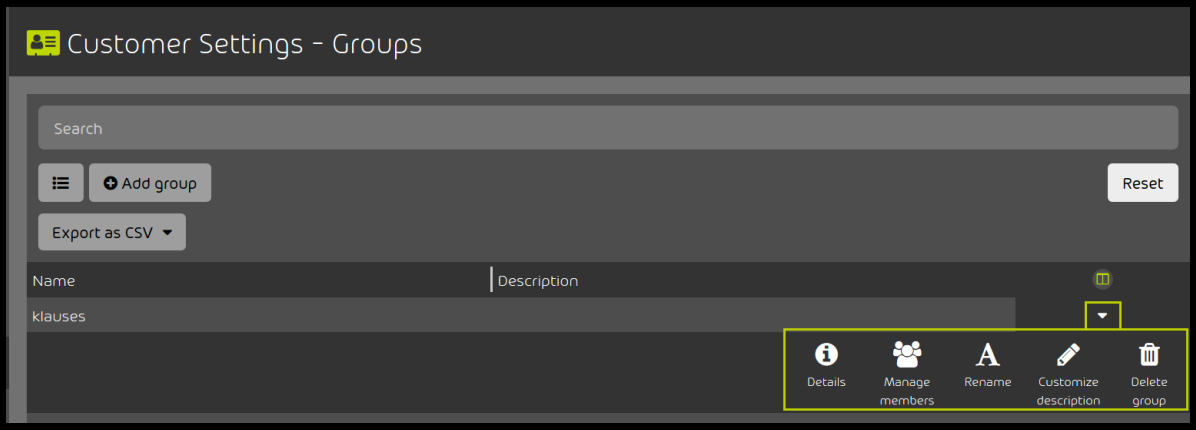


Figure 235: Open groups menu

2. Click **Delete**.

CAUTION:

When the group is deleted, all settings and group members are irrevocably deleted.

A warning message is displayed.

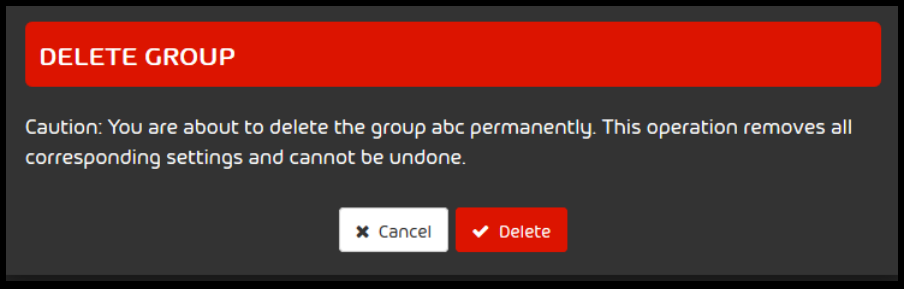


Figure 236: Delete group

3. Confirm the warning message by clicking **Delete**.

You have deleted the group.

Domains

Under **Domains**, you will find an overview of all existing domains and alias domains.

You can create new domains and delete existing ones. You can also export the displayed domains in CSV format and re-import them at the designated location (see Importing Domains from a CSV File on page 239).

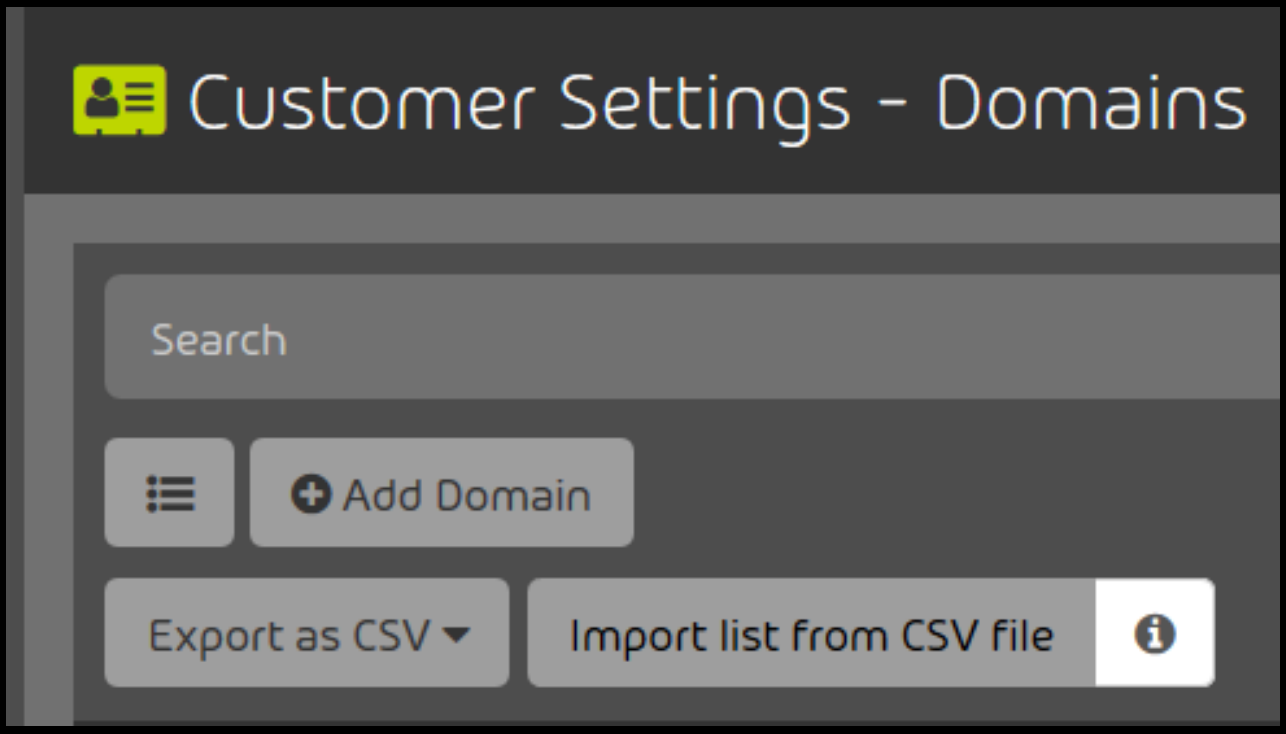
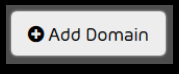


Figure 237: Domains

Adding a Domain

Add new domains.

1. Navigate to **Customer Settings#→Domains**.
2. Click on 

   A drop-down menu opens.

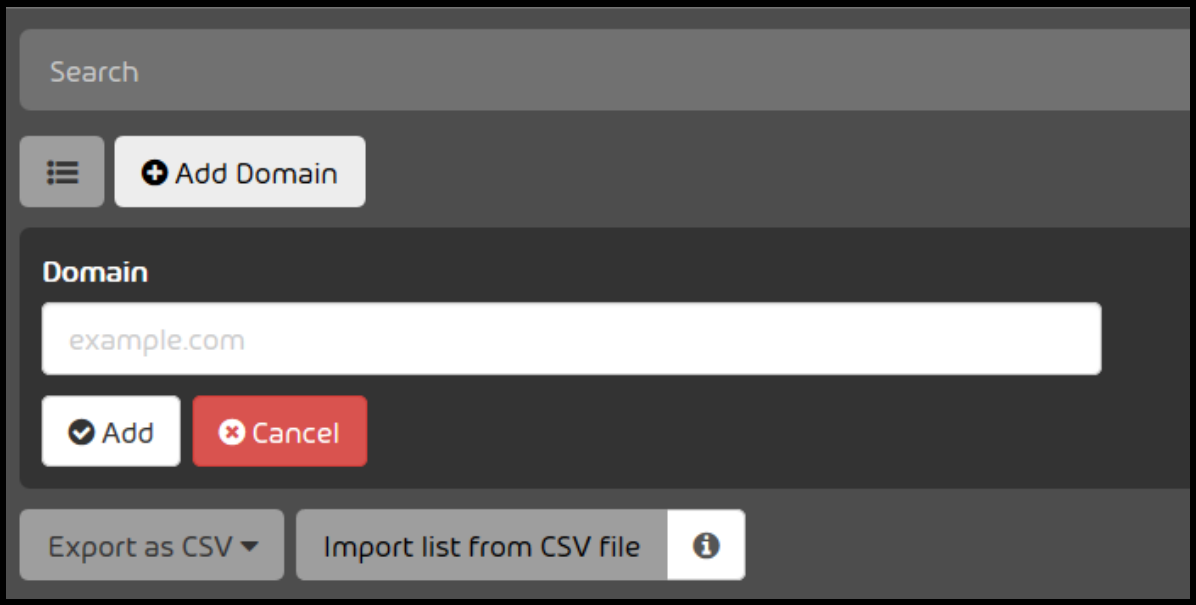


Figure 238: Add domain

3. Enter a valid domain under **Domain**.

> **Notice:**
>
> Existing domain lists can be imported here from a CSV file (see Importing Domains from a CSV File on page 239).

4. Click on **Add** to add the domain.

You have added new domains successfully.

Importing Domains from a CSV File

Import domains from a CSV file.

Instead of creating domains manually, you can import domains from a CSV list. You can import domains from a CSV list both initially, when no data has been entered yet, as well as anytime later.

1. Navigate to **Customer Settings#→Domains**.
2. Click on **Import list from CSV file**.
   A file selection window opens.
3. Select the desired CSV file.

> **Important:**
>
> To ensure that an external CSV file with 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 Domain Import on page 240).

If the CSV file contains new domains that are not yet available in the Control Panel, they will be added.

You have imported domains from a CSV file.

CSV Files for Domain Import

CSV files for domain import must meet special requirements.

To ensure that an external CSV file with domain names can be imported into the Control Panel without errors, special rules regarding file extension and content structure must be observed.

Rules for creating a CSV file for domain 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 contains always 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.
- Duplicated entries must not be present.

> **Important:** Duplicated entries lead to an immediate termination of the import. Correct entries will not be imported if the import is aborted.

Deleting Domains

Delete an existing domain.

1. Navigate to **Customer Settings#→Domains** and click on the menu arrow of the desired domain.

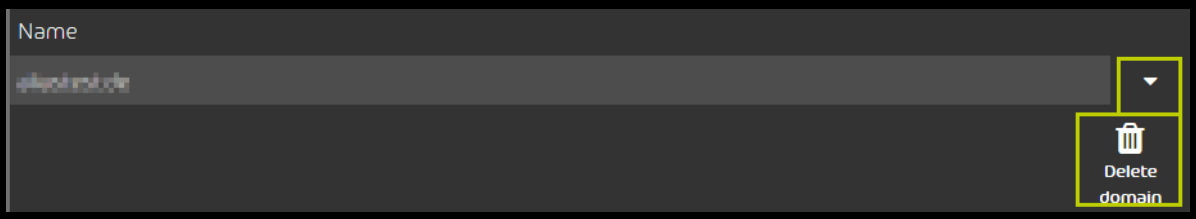


Figure 239: Drop-down menu for domains

> **CAUTION:**
>
> Deleting the domain irrevocably deletes all settings!

2. Click **Delete**.

   A warning message appears.

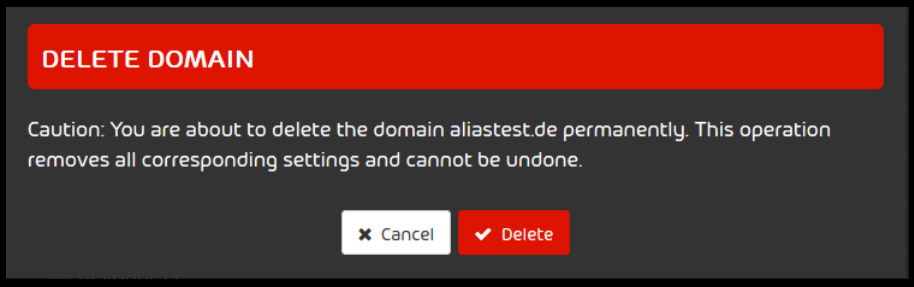


Figure 240: Delete domain

3. Confirm warning message by clicking **Delete**.

You have successfully deleted the domain.

Password Policy & IPs

Under **Password Policy & IPs**, you can define individual password policies and IP addresses for the Control Panel login.

Important:

The password policies are inherited to all subordinate 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.

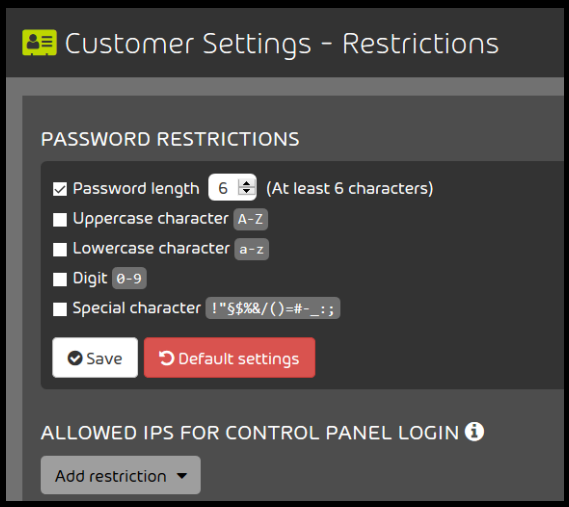


Figure 241: Password and IP Assignment policies

Assign Password Policies

Set your own password policy.

1. Navigate to **Customer Settings**#→**Password Policy & IPs**.

   Important:

   The password policies are inherited from the superordinate partners to the subordinate 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.

2. Activate the desired password policies.
3. Click **Save** to apply the settings.

You have successfully assigned the password policies.

Resetting Password Policies

Reset the password policies to default settings.

You have the option of resetting the assigned password policies to default settings. Default settings are settings that have been specified by parent administrators.

1. Navigate to **Customer Settings#→Password Policy & IPs**.
2. Click on **Default settings** to reset the policies to default settings.

   Notice:
   The password policies are also changed for all subordinate customers.
3. Click **Save** to apply the settings.

You have reset the password policies to default settings.

Assigning an IP Address

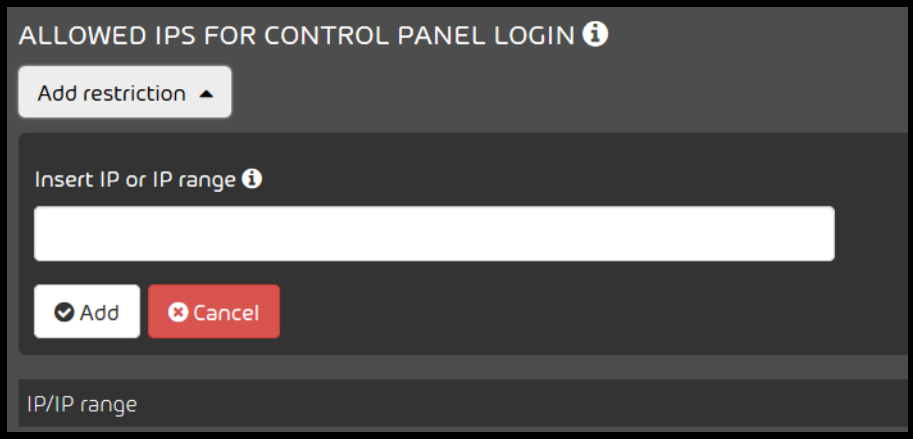
Assign your own IP addresses for the Control Panel login.

You can specify whether only selected IP addresses or IP address ranges are allowed when logging in to the Control Panel.

Notice:
If no IP addresses are assigned, all IP addresses are allowed for the Control Panel login.

1. Navigate to **Customer Settings#→Password Policy & IPs**.
2. Click on **Add IP**.
3. Enter a valid IP address or range of IP addresses and click **Add**.

You have assigned an IP address.



Deleting an IP Restriction

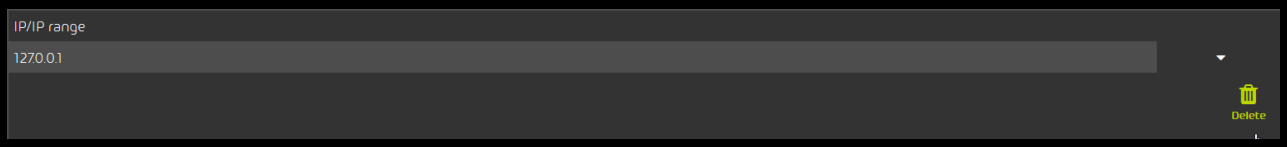
Delete a specified IP restriction.

Notice:

If no IP restrictions are assigned, all IP addresses are permitted for the Control Panel login.

1. Navigate to **Customer Settings#→Password Policy & IPs**.
2. Click on the menu arrow on the right in the line of the inserted IP restriction.
3. Click **Delete** to delete the IP address or IP address range.

You have deleted an IP restriction.



Black & White Lists

About Black & White Lists

In the Black & White Lists module you can define that emails from specific senders or domains are always quarantined (black list) or delivered (white list).

Creating Black and White List Entries

Adding entries to the blacklist or whitelist.

1. In the **scope search**, select the scope for which you want to create a blacklist or whitelist entry.

> **Notice:**
>
> It is no longer possible to create black and white list entries at partner level or for groups.

> **Notice:**
>
> If you have not selected a scope from the selection, the user you logged in with is selected.

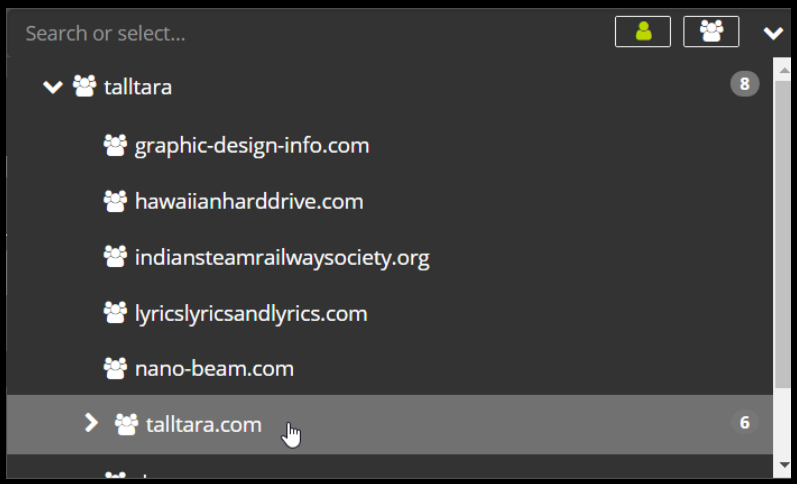


Figure 242: Select the scope

Depending on the selected scope, you can create entries that are valid globally for the domain or for specific users.

2. Go to the module **Black & White Lists**.

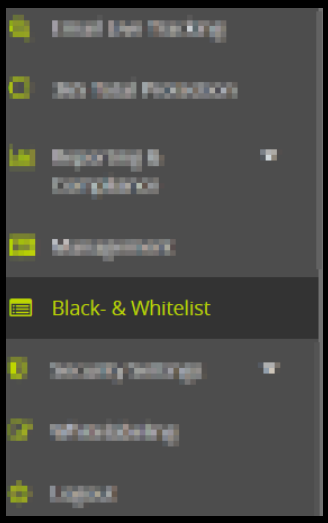


Figure 243: Black & White Lists module

3. Select the tab with the corresponding list:
   - Blacklist
   - Whitelist
4. Click on **Insert**.

   An input field opens.
5. Enter an email address, domain or IP in the input field.

> **Notice:**
>
> If entering a domain name, use the following syntax: **domainname.tld**

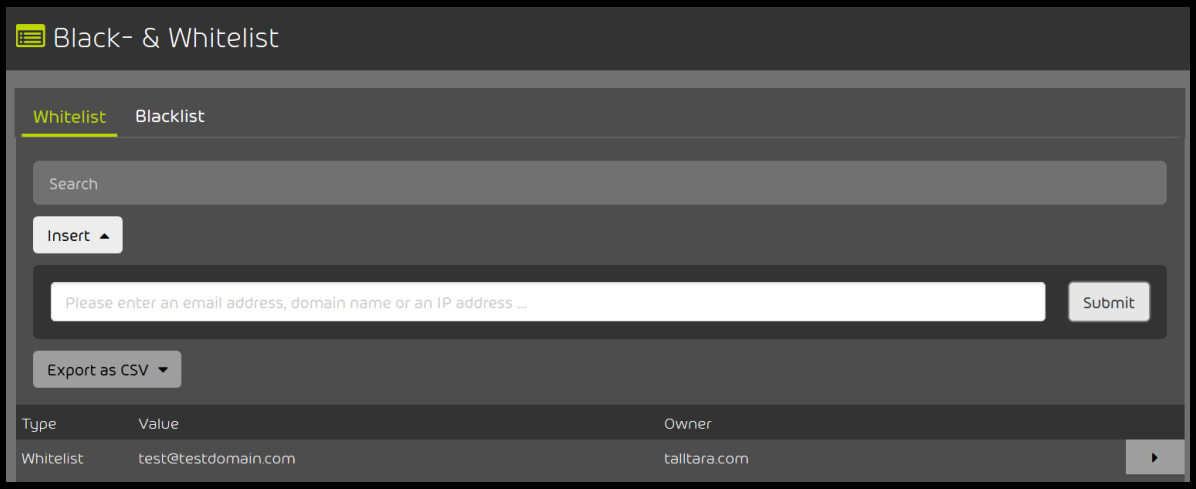


Figure 244: Domain blacklist entry

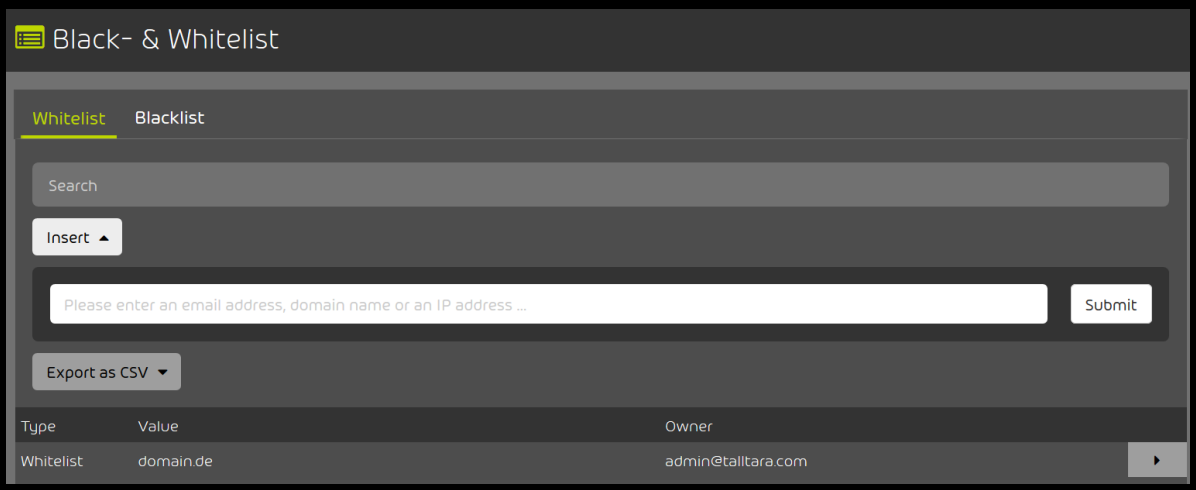


Figure 245: Black list entry for a user

6. Click on **Submit**.

   The entry is displayed in the list in the lower part of the module.

Deleting Black or White List Entries

1. Open the Black & White Lists module in the Control Panel.
2. Select the tab with the desired list.
3. Click on the arrow symbol on the right side of the entry you would like to delete.
4. Click on **Delete**.

You will receive a notification after successfully deleting the entry.

Example: Deleting entries from black- or whitelists

Following, the blacklist entry **test@testdomain** is deleted.

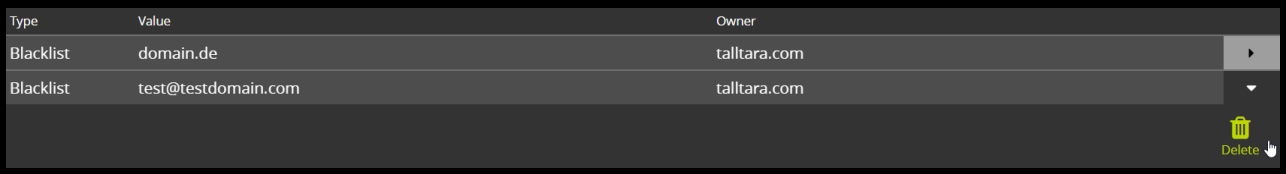


Figure 246: Delete entry

Searching for Black and White List entries

The search functionality of black and white list entries is similar to the search functionality of Email Live Tracking (see "Filtering Emails").

Enter search terms in the search bar. The entries are filtered dynamically.

Example: Search entries in the blacklist and whitelist module

The black list of the user admin@talltara.com is searched for the term **test**. Only results starting with test are shown.

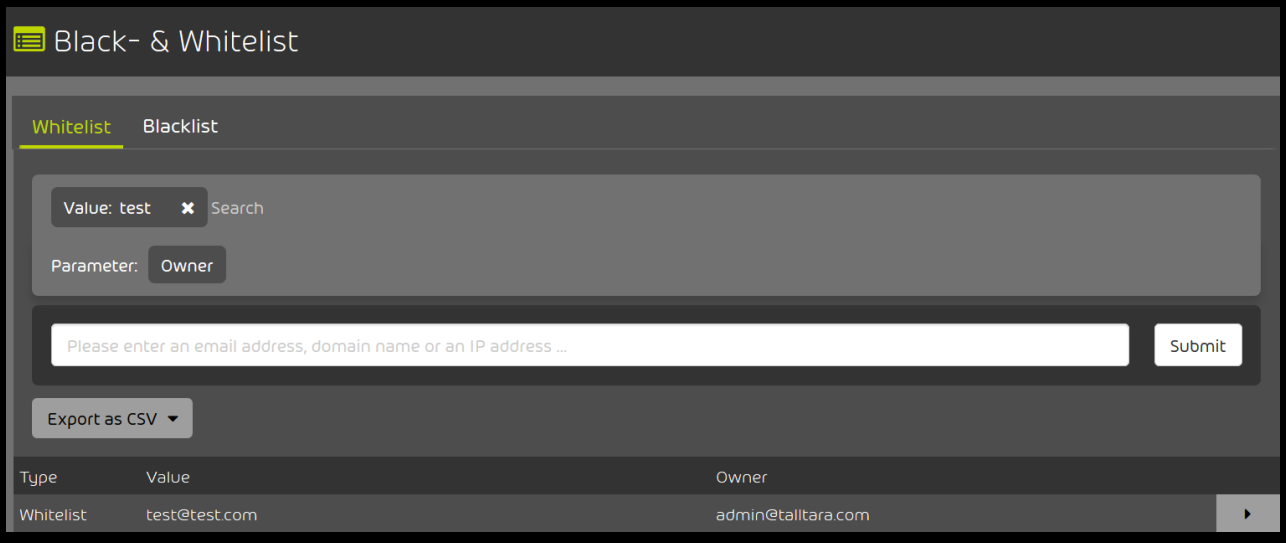


Figure 247: Search the black list

Processing hierarchy of black list and white list entries

The blacklist and whitelist entries are processed in the following order from the highest to the lowest priority:

- User white list
- User black list
- Domain and group whitelist
- Domain and group blacklist

If the system finds a fitting entry on either list, the execution is stopped and the remaining entries are not checked.

Example: Processing hierarchy of blacklist and whitelist entries

An admin adds the sender address example@example.com to the domain black list. A user adds this sender address to his white list. The emails from that account will be delivered to the user, but not to any other user who has not whitelisted that account.

Security Settings

Security Settings

Security Settings

In the security settings you will find configuration options for the services.

This section is intended for the administration of a domain. Select a domain in the scope selection of the Control Panel to make this area visible.

- Advanced Threat Protection
- Spam Report
- Spam and Malware Protection
- Content Control
- Compliance Filter
- Advanced Routing
- Signature & Disclaimer
- Archiving Audit Access Management
- Archiving
- Continuity Service
- Email Encryption
- Hornetdrive

Advanced Threat Protection (ATP)

Advanced Threat Protection functionality

Hornetsecurity Advanced Threat Protection (ATP) protects your company against targeted, individual attacks. Innovative forensic analysis engines ensure that attacks are prevented immediately. At the same time, the solution also provides your company with detailed information about the attacks.

ATP consists of the following analysis engines:

- Sandbox Engine
- URL Rewriting
- URL Scanning
- Freezing

- Targeted Fraud Forensics

Emails intercepted by ATP are categorized as **ATP** and placed in quarantine. Typically, they can be delivered manually by users with administrative rights.

ATP notifies the security officers of your company about security-related events at two different points in time:

- Immediately after the arrival of triggering emails with Real-Time Alerts (see Real time alert on page 253).
- Immediately after the detection of new threats in already delivered emails with the Ex Post Alerts (see Ex Post Alerts on page 255).

In addition to the automatic analysis of emails, both upon their arrival and subsequently with Ex Post Alerts, ATP offers the possibility of performing manual analyses of emails with executable attachments. With the so-called ATP scans (see ATP scan on page 263), 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 40).

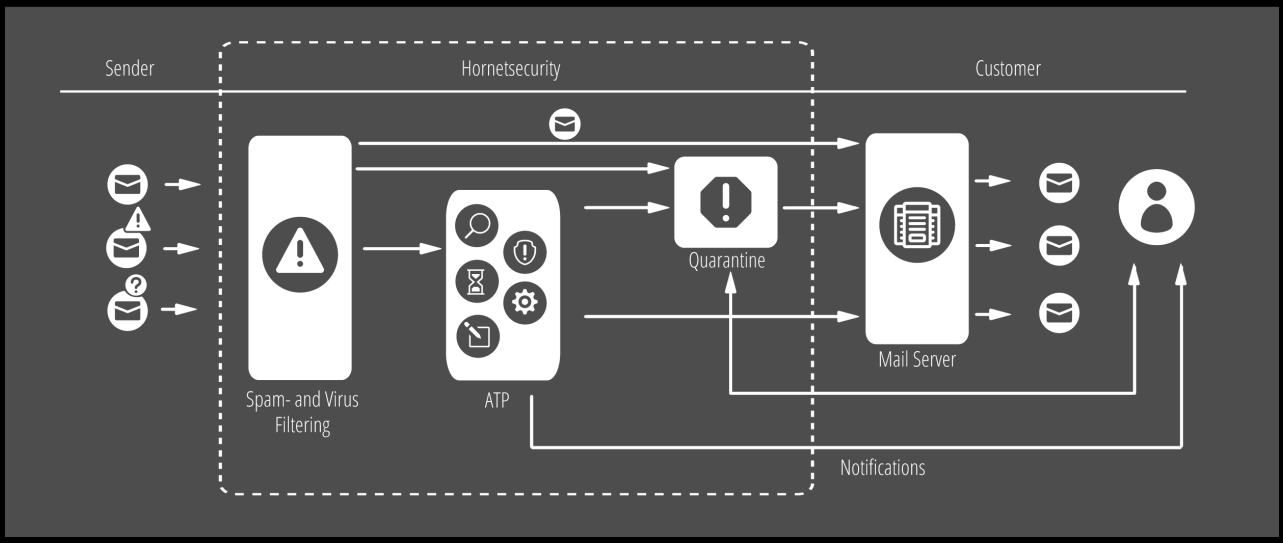


Figure 248: Workflow of Spam and Malware Protection with Hornetsecurity ATP

Description of the ATP Engines

ATP uses a number of engines to detect and fend off attacks.

Table 10: ATP engines

Hornetsecurity ATP Engines	Functionality 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	The URL Rewriting engine replaces all links in an email with our own links. As soon as the user clicks on one of those links, he is rerouted to the target website through the Web Filter service (see the chapter **Web Filter** in the Control Panel manual).
URL Scanning	A document (such as PDF, Microsoft Office) attached to an email may contain links. However, the links cannot be replaced as this would damage the integrity of the document. The Hornetsecurity URL Scanning engine leaves the document in its original form and only checks the target of such links.
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.

Hornetsecurity ATP Engines	Functionality 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.

Real time alert

Real-Time Alert informs you why emails have been intercepted.

Real-Time Alert is a notification function of ATP.

As soon as Hornetsecurity ATP detects an attack, Real-Time Alert sends a notification about a possible threat to your 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.

Under **Security Settings#→Advanced Threat Protection**, the recipients of alerts can be added to (see Adding a Recipient of Alerts on page 257) or removed from (see Removing Recipients of Alerts on page 258) the recipient list.

Notice:

Alerts are sent in the following cases:

- Malicious code has been found in the sandbox.
- URL Scanning has found a malicious URL.
- URL Rewriting has blocked a website or a download.

HORNETSECURITY®

Hornetsecurity Advanced Threat Protection - Real Time Alert

The Hornetsecurity Advanced Threat Protection Service has just detected the following email attack:

Classification:	Hornet-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 249: Real-time alert from Hornetsecurity

Figure 250: Real-time alert

Emails that have been classified as potentially dangerous by Hornetsecurity ATP are shown in the Control Panel under the category ATP, tagged in dark blue.

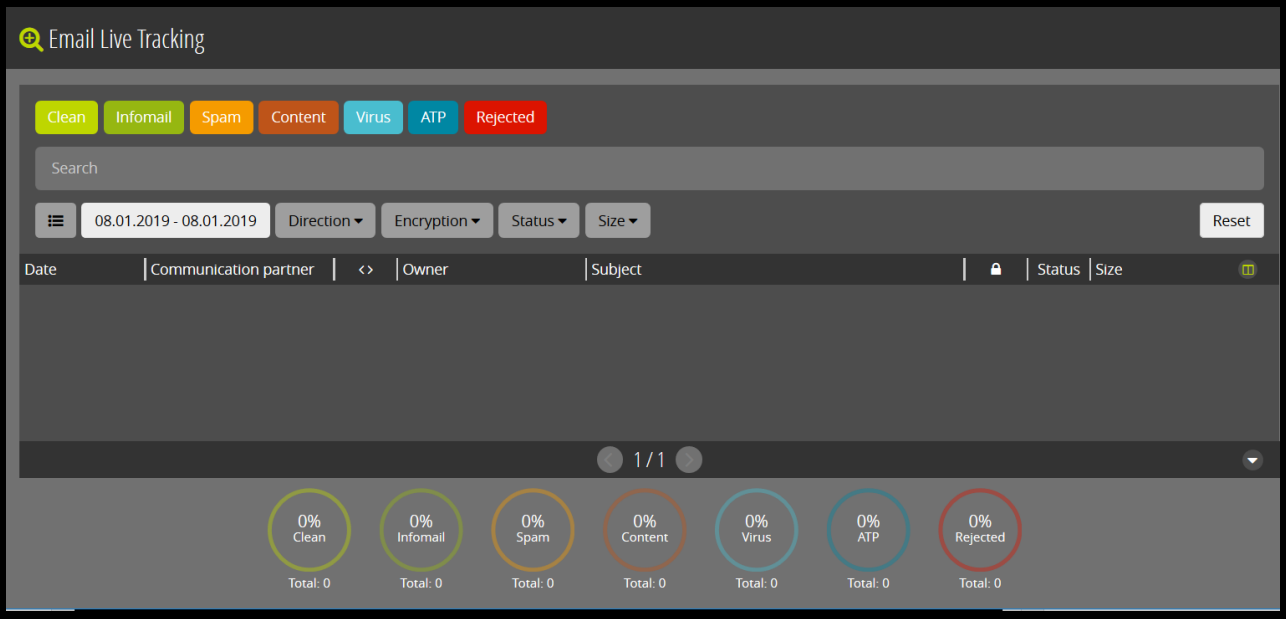


Figure 251: Category ATP

Ex Post Alerts

If it turns out that an already delivered email must be considered as potentially harmful after all, the IT security team of your company is notified about the extent and possible countermeasures as soon as this is known. This enables the threat to be contained quickly.

With Ex Post Alerts, your IT security team receives an automatic notification if an already delivered email is classified as malicious at a later point. You will receive a detailed evaluation of the attack so that you can immediately initiate actions such as checking the systems or sensitizing your own employees.

Under **Security Settings#→Advanced Threat Protection**, the recipients of alerts can be added to (see Adding a Recipient of Alerts on page 257) or removed from (see Removing Recipients of Alerts on page 258) the recipient list.

Notice:

As soon as ATP is activated, Ex Post Alerts is activated for all customer mailboxes.

Basic Settings

Activating ATP

Activate ATP in the Control Panel.

1. Navigate to **Security Settings#→Advanced Threat Protection**.
2. Click on the **Advanced Threat Protection** slider.

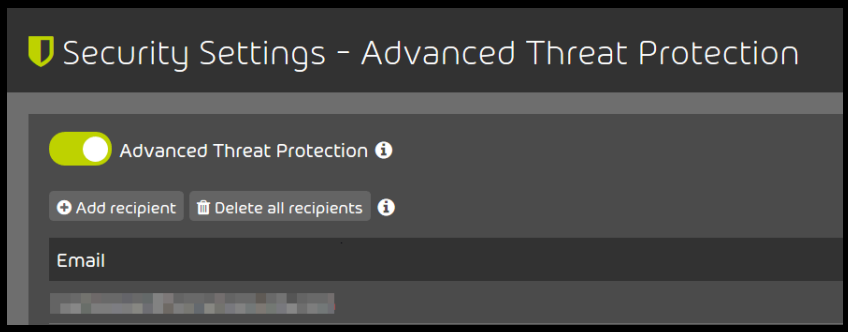


Figure 252: Activate ATP

A confirmation window with information on fees pops up.

3. Confirm the activation with **Confirm**.

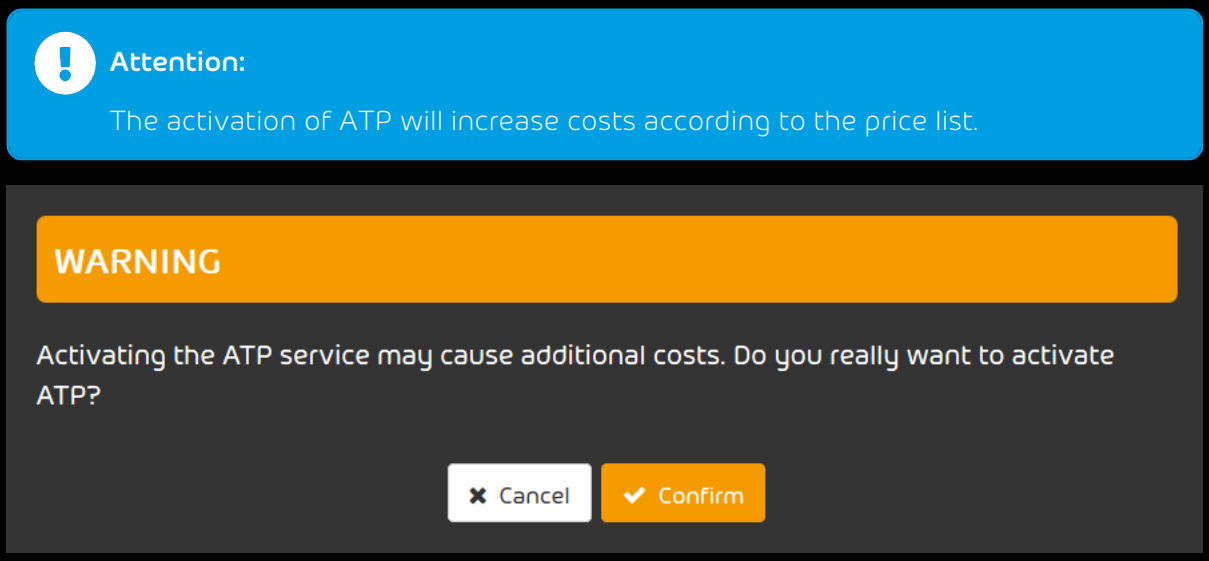


Figure 253: Activating ATP will cause additional charges

You have activated ATP.

Important:

By activating ATP, you activate all ATP engines (see Description of the ATP Engines on page 252) except URL Rewriting and the Targeted Fraud Forensics Filter for the selected scope. URL Rewriting and the Targeted Fraud Forensics Filter must be activated separately (see Activating URL Rewriting on page 260 or Activating the Targeted Fraud Forensics Filter on page 261).

Adding a Recipient of Alerts

Enter the email addresses of the users who should receive real-time alerts and Ex Post alerts.

Advanced Threat Protection is enabled.

1. Navigate to **Security Settings#→Advanced Threat Protection**.
2. Click on **Add recipient**.

Notice:

It is strongly recommended that you register your company's security officers as recipients.

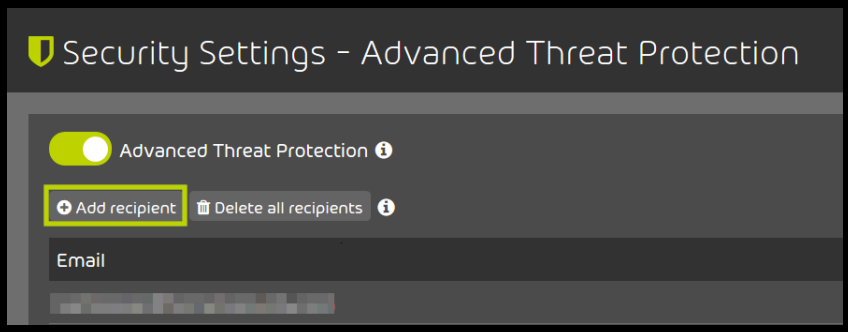


Figure 254: Activate ATP

A new input field appears below the button.

3. Enter the desired email address in the input field.

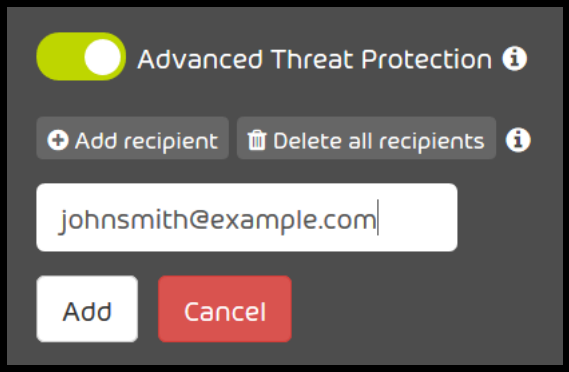


Figure 255: Enter an email address

4. Click on **Add**.
   The email address you entered appears in the **Email** section at the bottom of the page.

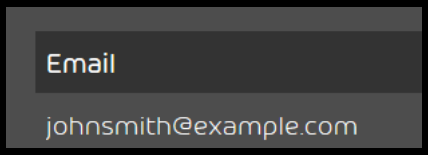


Figure 256: Entered email address

You have entered an email address for the reception of alerts.

Removing Recipients of Alerts

Remove one or all email addresses from the list of recipients of alerts.

Advanced Threat Protection is enabled and recipients of alerts are registered.

1. Navigate to **Security Settings#→Advanced Threat Protection**.
2. To delete a single email address, follow these steps:

   a) At the bottom of the page, you will find the registered email addresses under **Email**.

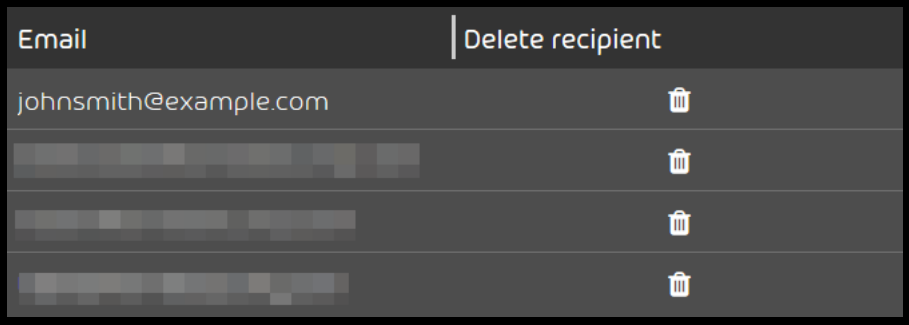


Figure 257: Recipient list

b) Click on the icon on the right side of the row of the desired e-mail address.

The desired e-mail address is removed from the recipient list.

3. To delete all recipients at once, follow these steps:

a) Click **Delete all recipients**.

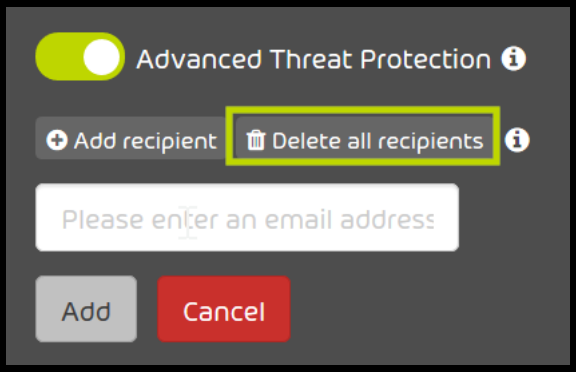


Figure 258: Delete all recipients

A confirmation window opens.

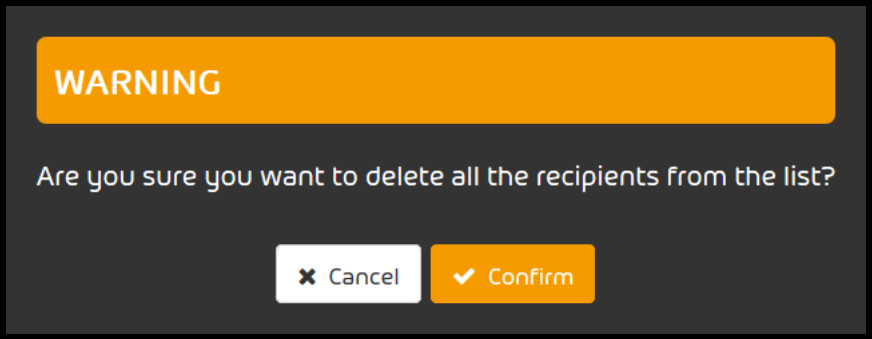


Figure 259: Confirm deletion of the recipients

b) Confirm with **Confirm**.

➔ All email addresses have been deleted from the recipient list.

You have removed some or all email addresses from the recipient list for alerts.

Activating URL Rewriting

Activate URL Rewriting in the Control Panel.

You have activated ATP.

In the module **Advanced Threat Protection**, you can activate the URL Rewriting ATP engine (see Description of the ATP Engines on page 252). This ATP engine is activated by default for all users of your domain and alias domains.

1. In the Control Panel, navigate to **Security Settings#→Advanced Threat Protection**.
2. Toggle the switch **Activated** under **URL REWRITING**.

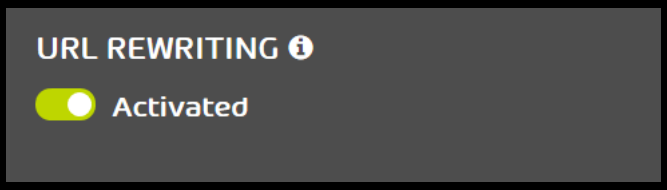


Figure 260: Toggle the Activated switch

➔ The button turns green and a confirmation window opens.

Notice:

URL Rewriting is activated by default for all mailboxes of your domain and alias domains. If you do not want to activate URL Rewriting for all domains, please contact the support before the activation and let them know which domains you want to exclude from the activation.

3. Click on **Confirm**.

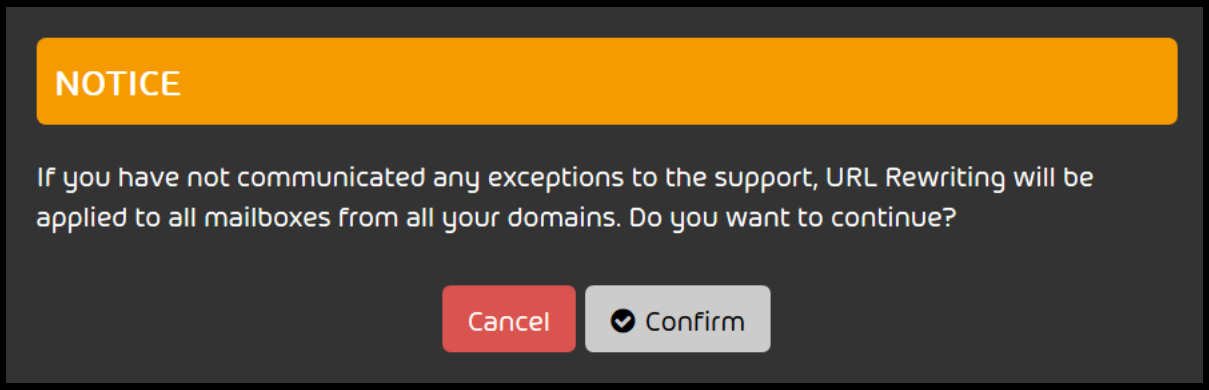


Figure 261: Confirm

URL Rewriting has been activated for all mailboxes under your domain and alias domains which were not defined as exceptions.

Activating the Targeted Fraud Forensics Filter

Activate the Targeted Fraud Forensics Filter for the desired user groups.

You have activated ATP and created user groups.

1. In the Control Panel, navigate to **Security Settings#→Advanced Threat Protection**.
2. Toggle the switch **Activated** under **TARGETED FRAUD FORENSICS FILTER**.

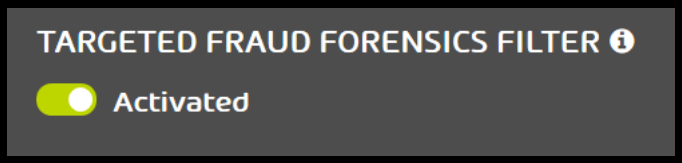


Figure 262: Toggle the Activated switch

The switch is highlighted in green. The Targeted Fraud Forensics Filter is activated, but it is not yet applied to any mailbox. The button **Add group** is enabled.

3. Add the desired user groups to the group list (see Adding a User Group to the TFFF Group List on page 262).

You have activated the Targeted Fraud Forensics Filter. The Targeted Fraud Forensics Filter is applied to all added user groups.

Adding a User Group to the TFFF Group List

Add a user group to the group list of the Targeted Fraud Forensics Filter.

You have activated the Targeted Fraud Forensics Filter and created user groups or synchronized them with LDAP.

The Targeted Fraud Forensics Filter is applied not 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. In the Control Panel, navigate to **Security Settings#→Advanced Threat Protection**.
2. In the section **TARGETED FRAUD FORENSICS FILTER**, click on **Add group**.

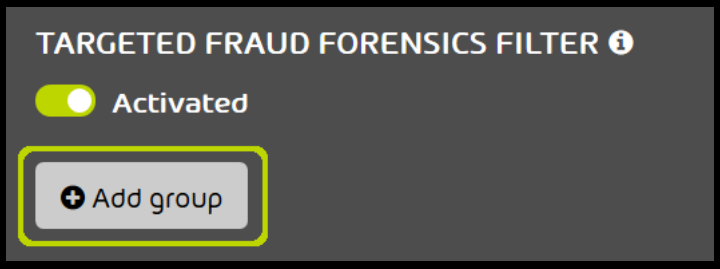


Figure 263: Add a group

→ A search field with additional buttons is displayed.

3. Enter the name of the desired group in the search field.
   → A drop-down menu with the search results opens.
4. Select the user group.
5. Click on **Confirm**.

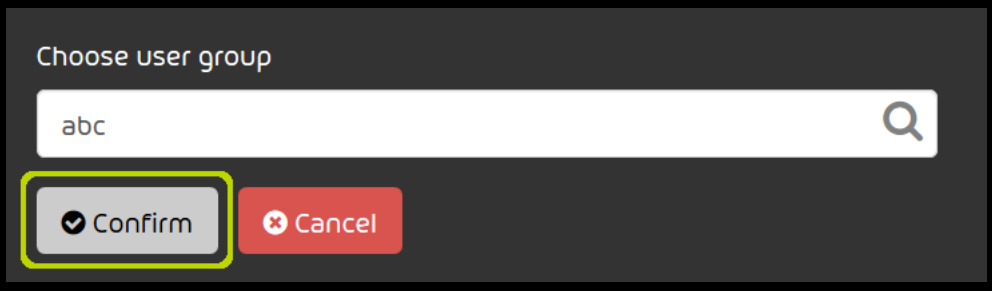


Figure 264: Confirm

→ The group is added to the group list.

You have added a user group to the group list of the Targeted Fraud Forensics Filter. The Targeted Fraud Forensics Filter is now applied to all mailboxes of this group.

Removing a User Group from the TFFF Group List

Remove a user group from the group list of the Targeted Fraud Forensics Filter.

You have activated the Targeted Fraud Forensics Filter and added user groups to its group list.

The Targeted Fraud Forensics Filter is applied not to domains, but 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. Navigate to **Security Settings**#→**Advanced Threat Protection**.
2. Select the desired user group from the group list in the section **TARGETED FRAUD FORENSICS FILTER**.
3. Click on the icon ✖ on the right side of the row of the group.

Figure 265: Remove a group

The group is removed from the group list.

You have removed a user group from the group list of the Targeted Fraud Forensics Filter. The Targeted Fraud Forensics Filter is no longer applied to the mailboxes of this group.

ATP scan

With the ATP Scan, you can perform an additional analysis on emails with executable attachments.

The ATP Scan is triggered manually and it 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 40).

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, for ATP customers, the ATP scan is mainly an additional security measure (for example, before manual delivery of emails categorized as **ATP**). On top of that, ATP customers receive additional information with the ATP report.

To learn how to perform an ATP scan, see Initiating an ATP Scan Manually on page 38.

Initiating an ATP Scan Manually

Analyze emails with executable attachments (e. g., .Exe files) manually with the ATP Scan.

With the ATP Scan, you can perform an analysis on emails with executable attachments.

Notice:

The ATP scan is only available for emails with executable attachments (e.g. .exe file). Furthermore, clean emails that have already been delivered can only be scanned when the products Archiving or the Hornetsecurity Continuity Service are active.

Attention:

If you have not booked Advanced Threat Protection, you can perform two ATP scans per month. You can only perform further ATP scans, if you have booked ATP.

1. Navigate to **Email Live Tracking** in the Control Panel.
2. Click on the arrow symbol right to the desired email.

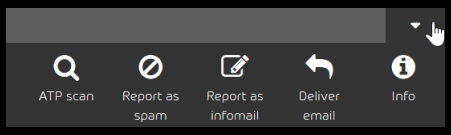


Figure 266: ATP scan in the Email Live Tracking module

➔ The detail view opens.

3. Click on **ATP**, to start the scan.

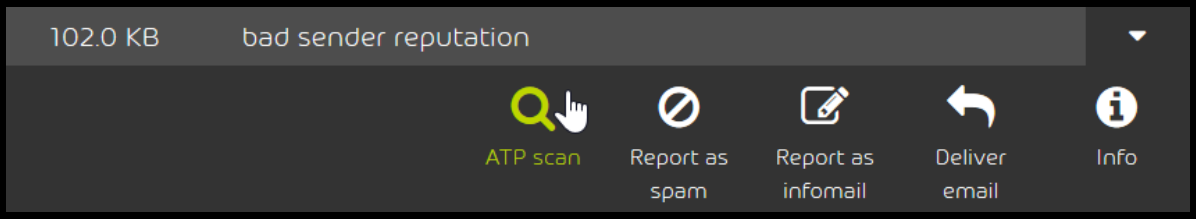


Figure 267: Initiating an ATP Scan Manually

You have started the ATP scan for the email.

Once the ATP scan is complete, you can view the ATP report in the detail view of the email under **Info**.

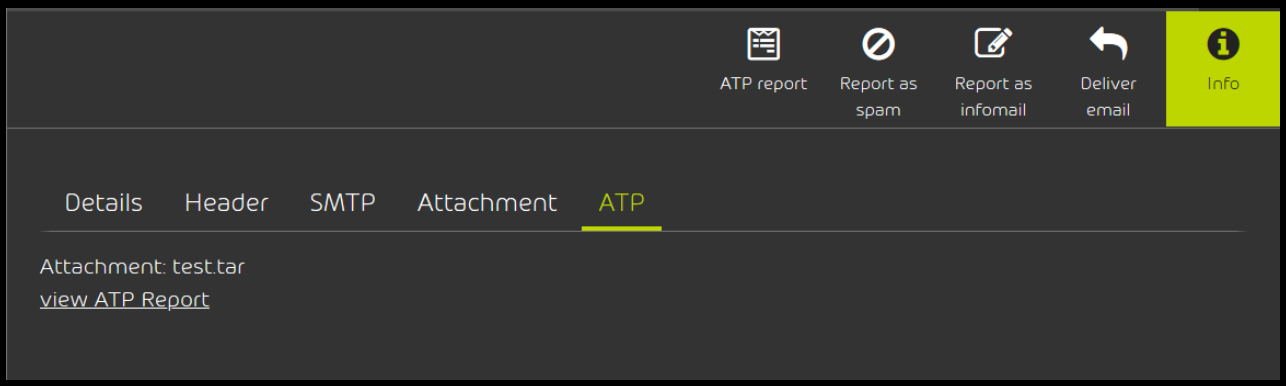


Figure 268: Open ATP report

ATP Report

The ATP report is a detailed report on the files analyzed with the ATP Scan.

The ATP report is a detailed report which is created as soon as an email has been analyzed with the ATP Scan (see ATP scan on page 263). The ATP report provides information about the analyzed email.

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.

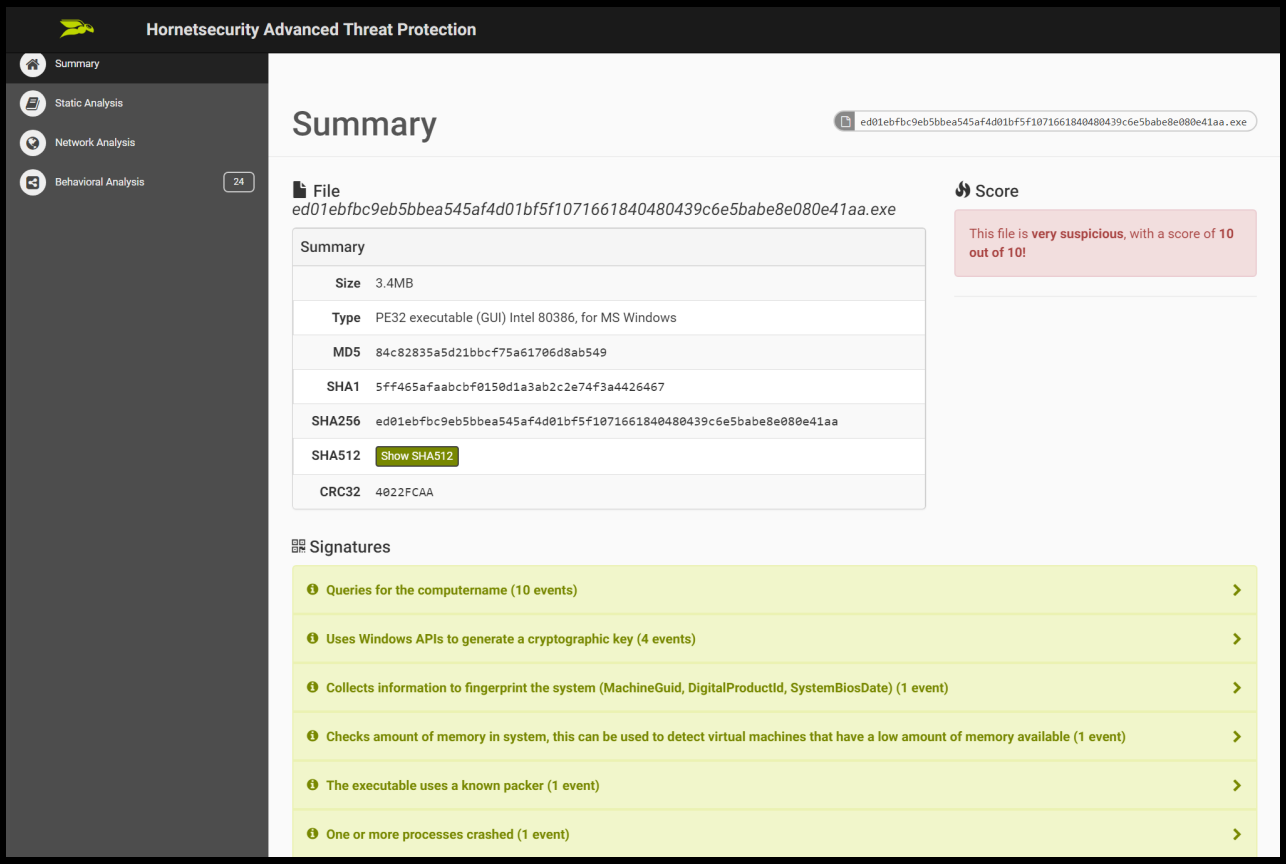


Figure 269: ATP Report Overview

Static Analysis

The static analysis is divided into three subcategories:

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

Network Analysis

In the network analysis, all network traffic is analyzed and listed according to protocols (e.g. HTTP, TCP, UDP).

Behavioral Analysis

The behavior analysis analyzes the behavior of the file at runtime.

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.
- If you select a process from the Process Tree, the executed API queries are displayed here in chronological order.

Spam Report

About the Spam Report

The Spam Report informs about quarantined emails.

The Spam Report is a report which is either created individually for a user or for the whole domain and is delivered to the recipient by email.

The Spam Report lists all emails which have not been delivered to the user but have been stored in quarantine. If the recipient of the Spam Report has the required authorization, they can later prompt the delivery of these emails if desired.

You can activate (see Activating the Spam Report for a Domain on page 267) and configure (see Configuring the Spam Report for a Domain on page 268) the Spam Report for a domain. Furthermore, you can configure the Spam Report differently for an individual mailbox (see Configuring the Spam Report for a Mailbox on page 270). If desired, you can also deactivate the Spam Report for a domain (see Deactivating the Spam Report for a Domain on page 272).

Activating the Spam Report for a Domain

Activate the Spam Report for a domain.

You have activated Spam and Malware Protection.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you want to activate the Spam Report.
3. Navigate to **Security Settings#→Spam Report**.

4. **Important:**

   If you want to whitelabel the Spam Reports, enter all required information into the module **Whitelabeling** before activating the Spam Report. The Spam Reports are automatically whitelabeled based on the information from this module. If you have not entered any information into the module, the Spam Reports will not be whitelabeled.

   Activate the switch **Activate Spam Report**.

Figure 270: Activate the Spam Report

You have activated the Spam Report for the domain.

Configure the Spam Report for the domain (see Configuring the Spam Report for a Domain on page 268).

Configuring the Spam Report for a Domain

Configure the Spam Report for a domain.

You have activated the Spam Report for the domain.

1. Log in to the Control Panel with your administrative credentials.
2. Navigate to **Security Settings**#→**Spam Report**.

3. **Notice:**

   By default, all users of the domain receive individual Spam Reports which are sent to their own email addresses. Alternatively, you can generate a Spam Report for the whole domain. If a Spam Report is generated for the whole domain, the users do not receive any Spam Reports.

   Optional: To generate a Spam Report for the whole domain, activate the switch **Generate a Spam Report for the whole domain**. Enter the email address to which the Spam Report will be delivered into the field **Recipient address for the Spam Report**.

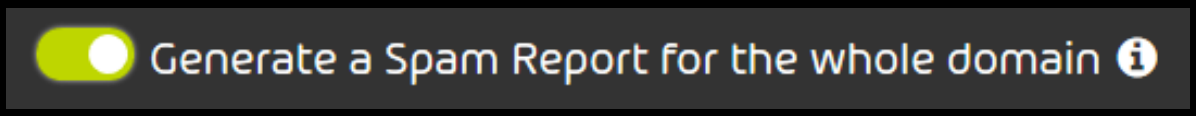


Figure 271: Generate a Spam Report for the whole domain

4. Under **Delivery times**, select the days on which the spam reports shall be delivered. Select at least one day.
   - To deliver the spam reports every day, activate the button **Daily**.
   - To deliver the spam reports every day from Monday to Friday, activate the button **Weekdays**.
   - Activate the checkboxes of the desired days.

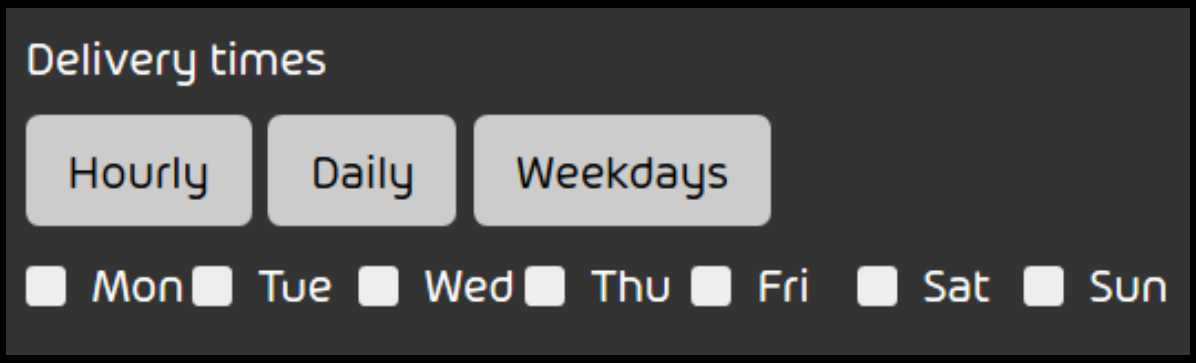


Figure 272: Select days

5. Under **Delivery times**, select the times at which the spam reports shall be delivered. Select at least one time.
   - To deliver the spam reports every hour, activate the button **Hourly**.
   - Activate the checkboxes of the desired times.

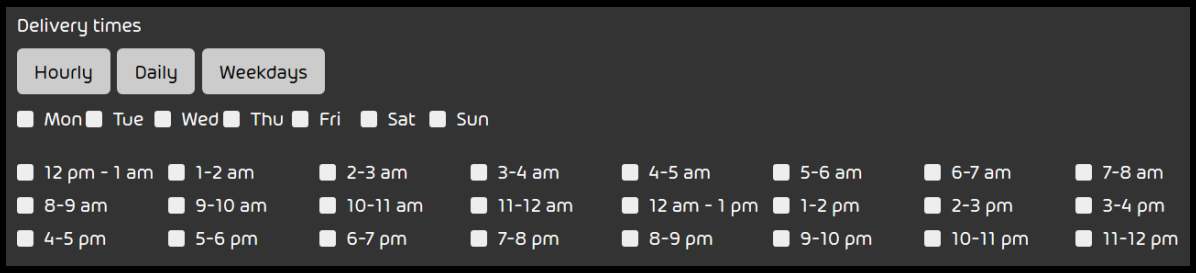


Figure 273: Select times

6. **Notice:**

   By default, the users of the domain receive the Spam Reports at the times set by the administrator. The users cannot change the delivery times of their Spam Reports by default.

   Optional: To allow the users of the domain to change the delivery times of their Spam Reports, activate the switch **Allow users to set the delivery times for their own Spam Reports**.

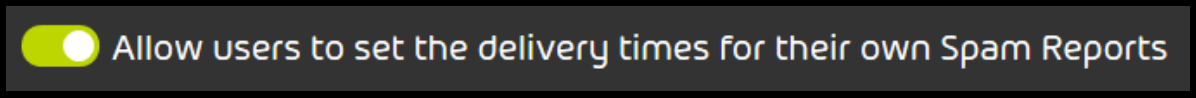


Figure 274: Allow users to change the delivery times

7. To apply the changes, click on **Save**.

You have configured the spam report for the domain.

You can configure the spam report differently for a mailbox of the domain (see Configuring the Spam Report for a Mailbox on page 270).

Configuring the Spam Report for a Mailbox

Configure the Spam Report individually for a mailbox.

You have activated the Spam Report for the domain.

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 Spam Report.
3. Navigate to **Customer Settings#→Mailboxes**.
4. Select the mailbox from the list and click on the arrow next to the mailbox .

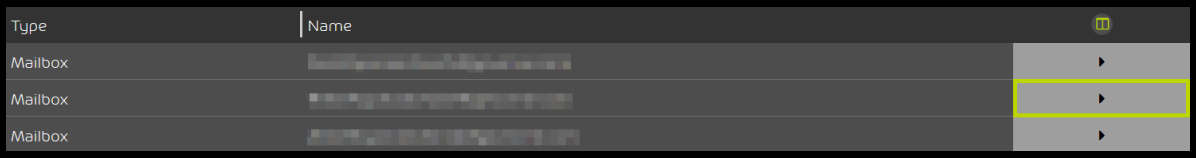


Figure 275: Display advanced settings

A menu opens.

5. In the menu, click on **Spam Report**.

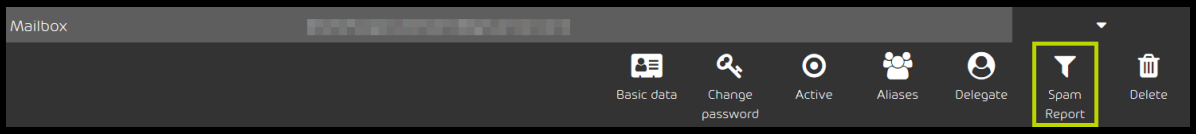


Figure 276: Menu

The Spam Report settings of the mailbox are displayed. If you have not yet configured the Spam Report for the mailbox, the settings of the domain are set by default.

6. To configure the Spam Report for the mailbox, activate the switch **Set your own delivery times**.

Figure 277: Set your own delivery times

You can deactivate the Spam Report for the mailbox or change the delivery times of the Spam Report.

7. If you would like to deactivate the Spam Report for the mailbox, activate the button **Deactivate**.

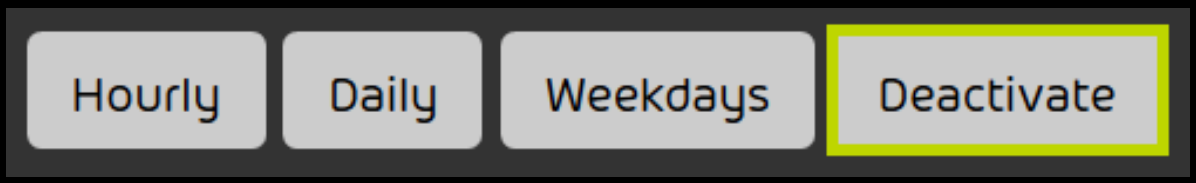


Figure 278: Deactivate the Spam Report

All delivery times and delivery days are deactivated for the mailbox. No spam reports are delivered to the mailbox. No further adjustments are required.

8. If the Spam Report remains activated for the mailbox, select on which days the spam reports shall be delivered. Select at least one day.
   - To deliver the spam reports every day, activate the button **Daily**.
   - To deliver the spam reports every day from Monday to Friday, activate the button **Weekdays**.
   - Activate the checkboxes of the desired days.

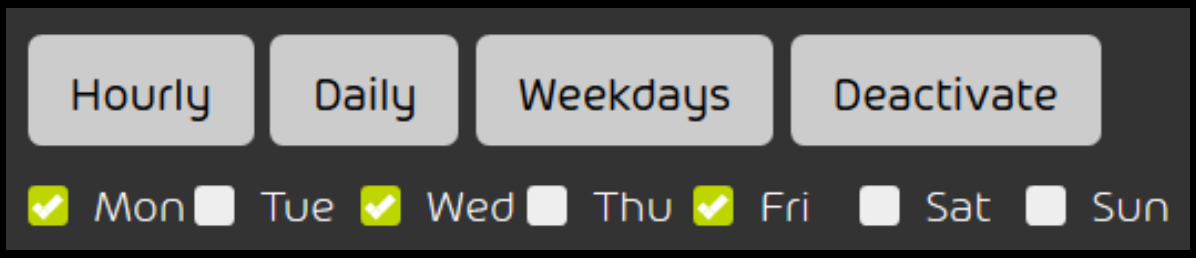


Figure 279: Select days

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

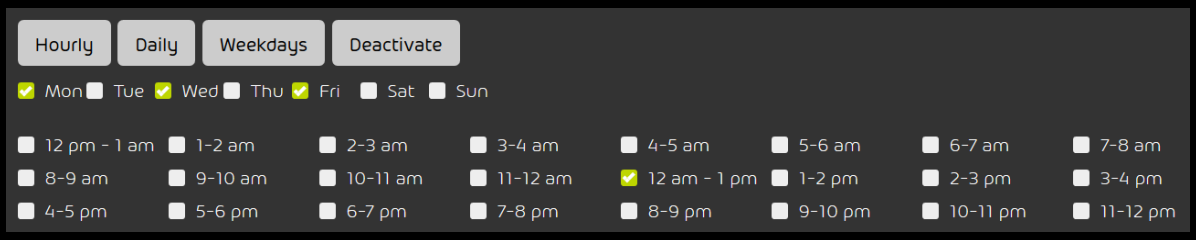


Figure 280: Select times

You have configured the Spam Report for the mailbox.

Deactivating the Spam Report for a Domain

You can deactivate the Spam Report for a domain.

You have activated the Spam Report for the 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**#→**Spam Report**.
4. Deactivate the switch **Activate Spam Report**.

Figure 281: Deactivate the Spam Report

You have deactivated the Spam Report for the domain.

Spam and Malware Protection

Spam and Malware Protection

Spam and Malware Protection is a service which blocks spam and emails containing viruses before they enter your mailboxes. Furthermore, infomail (e. g., newsletters), can be detected and rejected.

With the following features, Spam and Malware Protection offers protection against 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 which are sent in return to spam with fake sender addresses.

Spam and Malware Protection allows the user to determine how spam and infomail are dealt with. If emails have been classified incorrectly, the user can trigger the delivery of spam and infomail under **Email Live Tracking** (see Email Actions on page 45).

Furthermore, the services **Content Control** (see About Content Control on page 285) and **Compliance Filter** (see Compliance Filter on page 293) are part of Spam and Malware Protection and can be activated if desired.

Ruleset order

Spam and Malware Protection rules are processed according to a specific priority. If a rule with a high priority applies, processing is usually terminated. In some cases, this can lead to messages being blocked despite a whitelist entry for the sender's address, because the IP address of the sending server is on the RBL blacklist.

Rule order (from top to bottom in descending priority).

Incoming emails

1. RBL list (block)
2. Mass spam detection (block)
3. Compliance filter (deliver)
4. Virus check (quarantine)
5. Content Control, if activated (quarantine)
6. User-based whitelist string (deliver)
7. User-based blacklist string (quarantine)
8. Administrative whitelist (deliver)
9. Administrative blacklist (quarantine)
10. General whitelist (deliver)
11. General spam rules (quarantine)
12. Infomail filter (quarantine)

Notice: Due to this order, it is possible to create exceptions for Content Control with Compliance Filter rules which categorize emails as **Clean**. However, since user-based and administrative whitelisting and blacklisting are applied after the Content Control rules, they cannot be used to create exceptions for Content Control.

Outgoing emails

1. RBL list
2. Compliance Filter
3. Virus check
4. Content Control, if activated

Activating Spam and Malware Protection

Under **Security Settings#→Spam and Malware Protection**, you can activate the service Spam and Malware Protection.

You can activate Spam and Malware Protection yourself under **Spam and Malware Protection**. After the activation, you will have to make further settings.

> **Important:**
>
> The activation of Spam and Malware Protection will increase costs according to the price list.

> **Important:**
>
> After the activation, you will not be able deactivate Spam and Malware Protection yourself. For further assistance, contact the support.

1. Navigate to **Security Settings#→Spam and Malware Protection**.
2. Under **DOMAIN**, select the domain for which you want to activate Spam and Malware Protection.

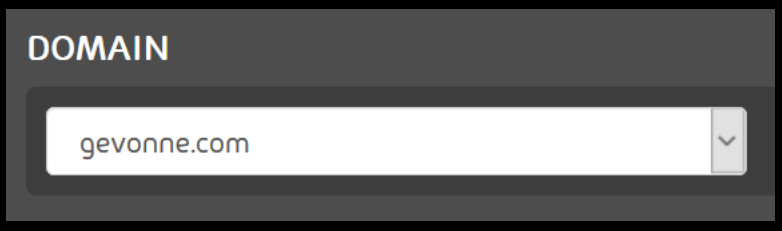


Figure 282: Select domain

3. Toggle the switch **Activate Spam and Malware Protection** under **ENVIRONMENT SETTINGS**.

Figure 283: Activate Spam and Malware Protection

➔ A notification about additional costs is displayed.

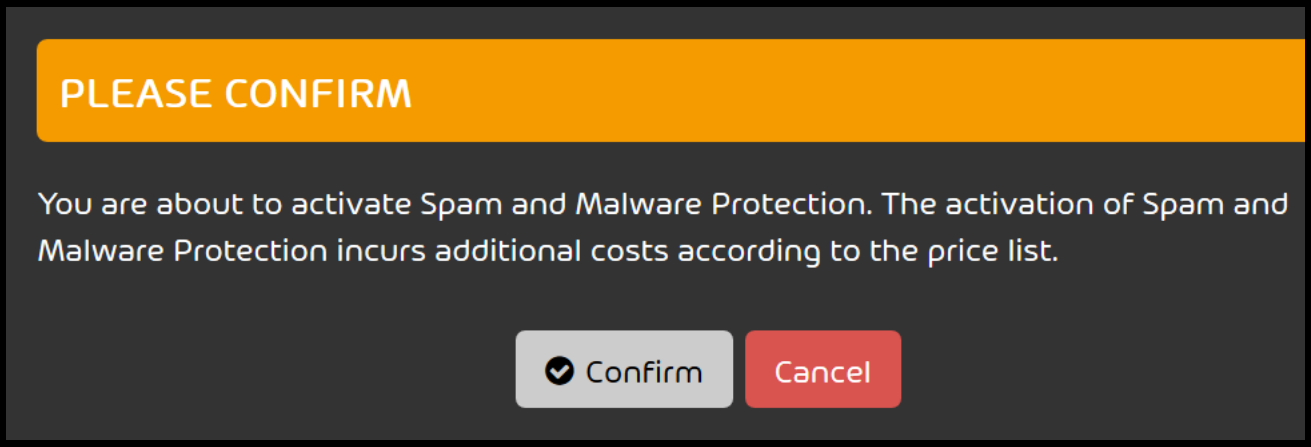


Figure 284: Confirm activation

4. Click on **Confirm** to confirm the activation.
   ➔ The switch turns green and additional control elements are unlocked under **ENVIRONMENT SETTINGS** and **EMAIL FILTER SETTINGS**.
5. Optional: If you want to adjust the environment settings and the email filter settings before Spam and Malware Protection is activated, adjust the settings now (see Adjusting the Environment Settings on page 278 and Email Filter Settings on page 280).
6. Click on **Apply changes**.

You have activated Spam and Malware Protection for the selected domain.

Environment Settings

Spam and Malware Protection requires several environment settings related to receiving and sending emails. Under **ENVIRONMENT SETTINGS**, you can set the destination of incoming emails,

specify IP addresses for other relay mail servers, activate the bounce management and configure the user check.

For more clarity, the available options are explained below: For more information about the configuration, please see chapter Adjusting the Environment Settings on page 278.

- **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 mail servers. Either the corresponding IP 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.
  - **Hornet.email**: If this option is selected, the email service Hornet.email is used. After selecting this option, select the size of the mailboxes. For Spam and Malware Protection, no other environment settings are required. All incoming and outgoing emails are checked. The user check is also configured automatically.
  - **POP3/IMAP**: This option should be selected if the customer's email provideris Hornetsecurity. If this option is selected, the size of the POP3/IMAP mailbox must be specified.
- Relay IP addresses for outgoing emails: If Spam and Malware Protection is activated, outgoing emails are filtered, too. Under **Relay IP addresses for outgoing emails**, you can specify the IP addresses of the customer's mail relay servers from which 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 relay IP addresses with suffixes not longer than /24, separated from each other by commas. 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 IP addresses specified here are also required for signing and encrypting emails with the services Signature and Disclaimer and Email Encryption. If no addresses are specified, none of both services will be able to process any emails. Even if you do not use these services, we recommend you to specify your relay IP addresses here. This does not apply to 365 Total Protection customers.
- **Bounce management:** Bounce management is a feature which checks incoming bounce messages to determine whether the emails which prompted them were actually sent via the domain's relay servers or via a fake sender address as the consequence 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 the mail servers of Hornetsecurity from accepting emails addressed to non-existing recipients under your domain, which could be exploited for DDoS attacks. The user check can be based on the users lists of the Control Panel or your directory service, or it can be carried out by directly sending an SMTP request to the mail servers of your domain which are specified under **Destination**.

Adjusting the Environment Settings

If Spam and Malware Protection is activated, you can adjust the settings for receiving and sending emails under **ENVIRONMENT SETTINGS**.

You have activated Spam and Malware Protection.

Spam and Malware Protection requires several environment settings related to receiving and sending emails. For more information about the functions, see chapter Environment Settings on page 276.

1. Navigate to **Security Settings#→Spam and Malware Protection**.
2. Under **DESTINATION**, set the destination of incoming emails. You have three options:
   - If you have your own mail server, mark the checkbox **IP/Hostname** and then enter the corresponding IP addresses or the corresponding hostname in the input field. Enter at least one IP or hostname. Optionally, you can also enter the port number and priority. Follow the input format **IP/Hostname:Port#Priority** and use a semicolon to separate several entries from each other.
   - If you use the email service Hornet.email, mark the checkbox **Hornet.email**. Select the size of the mailboxes. For Spam and Malware Protection, no other environment settings are required.
   - If Hornetsecurity is your email provider, mark the checkbox **POP3/IMAP**. Under **Mailbox Size**, enter the size of your POP3/IMAP mailbox (allowed values: 100-1024 MB).
3. **Notice:**

   Although this step is optional, we highly recommend it. The relay IP addresses specified under **Relay IP addresses for outgoing emails** are required for signing and encrypting emails with the services Signature and Disclaimer and Email Encryption. If no addresses are specified, none of both services will be able to process any emails.

Optional: If you want to enter the IP addresses of your mail relay servers manually, toggle the switch **Relay IP addresses for outgoing emails**.

An input field for IP addresses is displayed.

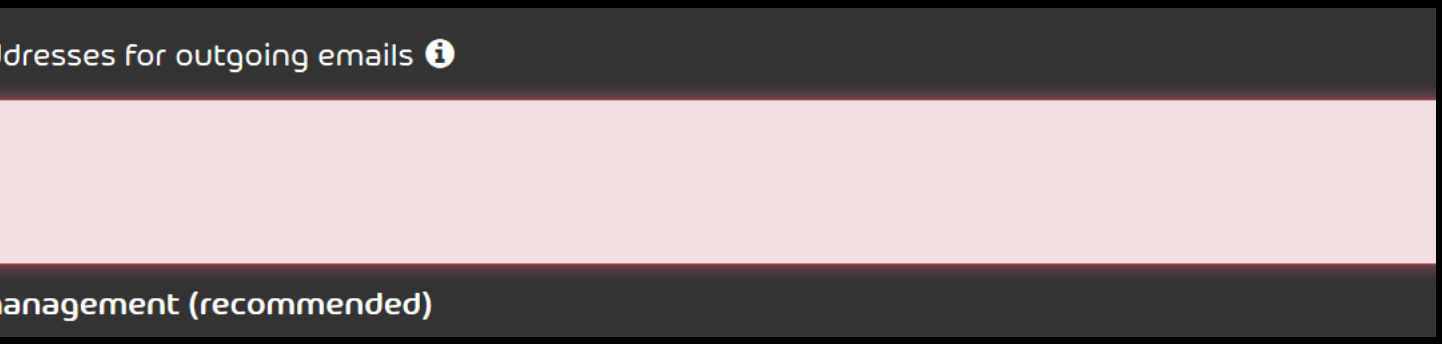


Figure 285: Define relay IP addresses for outgoing emails

4. Optional: Enter the IP addresses of your relay mail servers in the field under the switch **Relay IP addresses for outgoing emails**. If the switch is on, this field may not remain empty.
5. Optional: If you want to activate bounce management to prevent incorrect bounce messages, mark the checkbox **Bounce management (recommended)**.
6. Set up the user check under the section **USER CHECK**. You have four options:

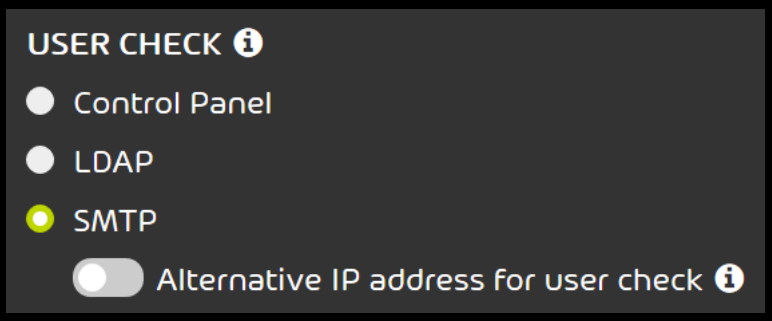


Figure 286: Set up user check

- **Control Panel**: If this checkbox is marked, Spam and Malware Protection checks whether the recipient address is listed in the user list of the Control Panel.
- **LDAP**: If you mark this checkbox, Spam and Malware Protection checks whether the recipient address is listed in your directory service.
- **SMTP**: If this checkbox is marked, 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 valid. Usually, the destination server is determined on the basis of the domain part. If you want to use

other destination servers for the user check with SMTP, toggle the switch **Alternative IP address for user check** and enter the IP address in the input field.

7. Click on **Apply changes**.

You have adjusted the environment settings of Spam and Malware Protection.

Email Filter Settings

In the section **Email Filter Settings** under the module **Spam and Malware Protection**, you can make several settings for the email filter.

Under **Security Settings#→Spam and Malware Protection#→Email Filter Settings**, you have the following options:

- Configuring the handling of spam (see Configuring the Handling of Spam on page 280).
- Activating the infomail filter (see Activating the Infomail Filter on page 281).
- Configuring the infomail filter (see Configuring the Infomail Filter on page 281).
- Configuring the handling of infomail (see Configuring the Handling of Infomail on page 283).

Configuring the Handling of Spam

Under **SPAM HANDLING**, you can decide how to handle spam messages which have been filtered out by the email filter.

You have activated **Spam and Malware Protection**.

1. Navigate to **Security Settings#→Spam and Malware Protection**.
2. Select the desired option for handling spam 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 spam messages with a personalized phrase, select **Tag**. Then the input field **Phrase for tag** is displayed. Enter the phrase with which spam messages shall be tagged in the field.

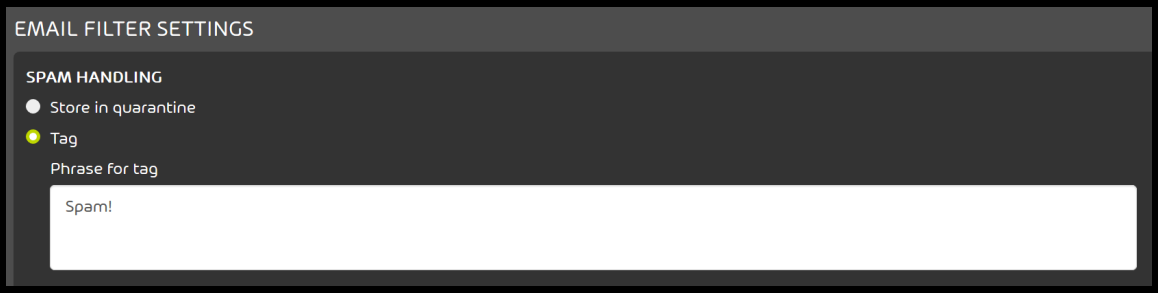


Figure 287: Tag spam

3. Click on **Apply changes**.

You have configured the handling of spam.

Activating the Infomail Filter

Under **INFOMAIL FILTER SETTINGS**, you can activate the infomail filter and make other settings.

You have activated **Spam and Malware Protection**.

The infomail filter detects infomail and carries out different actions depending on the settings. The infomail filter is one of the features of the email filter of **Spam and Malware Protection**. To use the infomail filter, you have to activate it first.

1. Navigate to **Security Settings#→Spam and Malware Protection**.
2. Toggle the switch **Activate infomail filter**.
   The switch turns green and a form containing more settings is displayed.
3. Click on **Apply changes**.

You have activated the infomail filter.

Set up the infomail filter (see Configuring the Infomail Filter on page 281).

Configuring the Infomail Filter

Configure the infomail filter to define its scope.

You have activated **Spam and Malware Protection** and the infomail filter.

The infomail filter can either be activated for all users of a domain or only for the users who want to use it.

1. Navigate to **Security Settings#→Spam and Malware Protection**.
2. If you want to activate the infomail filter by default for all users of the domain, mark the checkbox **Activate infomail filter for all users** under **EMAIL FILTER SETTINGS#→INFOMAIL FILTER SETTINGS**.
3. If you want to allow the users of the domain to turn the infomail filter on and off, mark the checkbox **Allow users to turn the infomail filter on/off**. If the checkbox is marked, the users can turn the infomail filter on and off under **Customer Settings#→Filter & Reports** By combining the two checkboxes, you have the following options:
   - **Activate infomail filter for all users** marked, **Allow users to turn the infomail filter on/off** unmarked: The infomail filter is activated for all users. The users cannot turn off the infomail filter.
   - **Activate infomail filter for all users** marked, **Allow users to turn the infomail filter on/off** marked: The infomail filter is activated for all users by default. The users can turn off the infomail filter.
   - **Activate infomail filter for all users** unmarked, **Allow users to turn the infomail filter on/off** marked: The infomail filter is deactivated for all users by default. The users can turn on the infomail filter.
   - **Activate infomail filter for all users** unmarked, **Allow users to turn the infomail filter on/off** unmarked: 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.

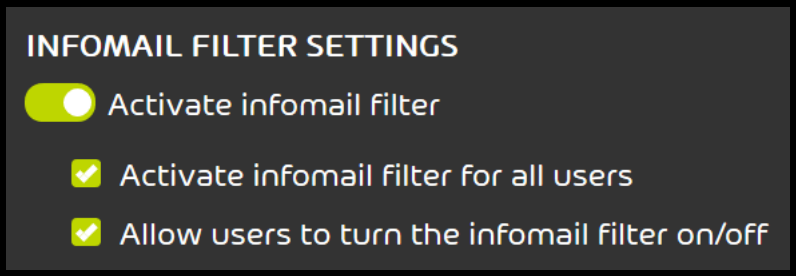


Figure 288: Configure the infomail filter

4. Click on **Apply changes**.

You have configured the infomail filter.

Configuring the Handling of Infomail

Under **INFOMAIL FILTER SETTINGS**, you can decide how to handle infomail which has been filtered out by the email filter.

You have activated **Spam and Malware Protection** and the infomail filter.

1. Navigate to **Security Settings#→Spam and Malware Protection**.
2. Select the desired option for handling infomail under **EMAIL FILTER SETTINGS#→INFOMAIL FILTER SETTINGS**. You have two options:
   - If you want to store infomail in quarantine, select **Store in quarantine**. For emails stored in quarantine, the module **Email Live Tracking** offers several actions.
   - If you want to tag infomail with a personalized phrase, select **Tag**. Then the input field **Phrase for tag** is displayed. Enter the phrase with which infomail shall be tagged in the field.

Figure 289: Tag infomail

3. Click on **Apply changes**.

You have configured the handling of infomail.

Allowing and Forbidding User Actions

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 and the Spam Reports, some actions are available to the users in order to deliver emails intercepted by Spam and Malware Protection. You can allow or forbid these actions.

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.

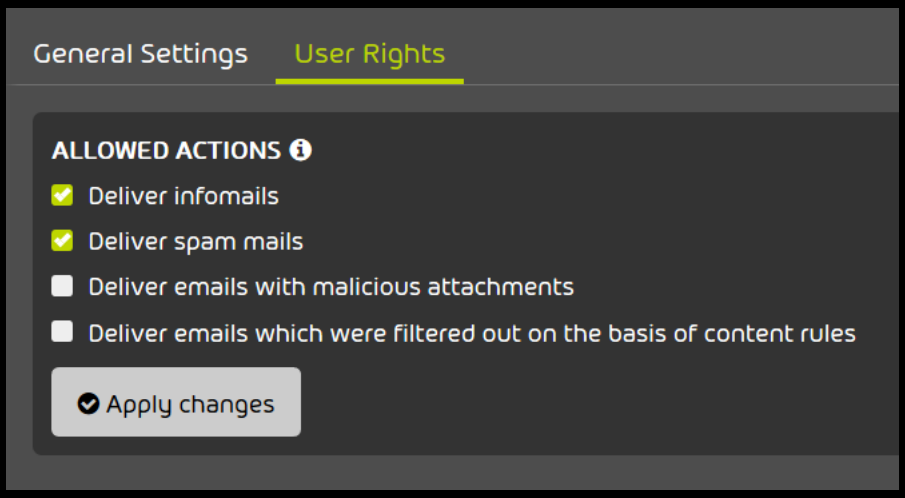


Figure 290: User rights

5. Under **ALLOWED ACTIONS**, mark the checkboxes of the actions you want to allow the users of the domain to perform. Uncheck 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 which were filtered out on the basis of content rules**.
6. Click on **Apply changes**.

You have allowed or forbidden user actions on emails intercepted by Spam and Malware Protection.

Content Control

About Content Control

Content Control offers domain administrators and partners the possibility to manage the handling of attachments of incoming and outgoing emails.

This section explains how to activate Content Control, add and delete groups, and configure Content Control. It also gives an overview of the categories of file types to be filtered out.

Activating Content Control

Activate Content Control to manage the handling of attachments of incoming and outgoing emails for the users of a domain.

Spam and Malware Protection has been activated.

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 291: Activating Content Control

Content Control has been enabled for the selected domain. Content Control default settings are applied to all users of the domain.

Set up Content Control (see Setting up Content Control on page 287).

Adding a group

To apply settings other than the default ones to a group, add the group to Content Control.

Content Control is activated. A group has been created under the domain (see Adding a group on page 94).

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 **Select a group**.

Figure 292: Selecting a group

➔ A drop-down menu with all groups created under the domain opens.

5. Select the group from the drop-down menu.
6. Click on .

➔ The group is listed under **Affected groups**.

The group is added to Content Control.

Set up Content Control for the group (see Setting up Content Control on page 287).

Deleting a Group

In order to assign the default settings to a Content Control group again, delete the group from Content Control.

You have added a group to Content Control.

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 next to the group.

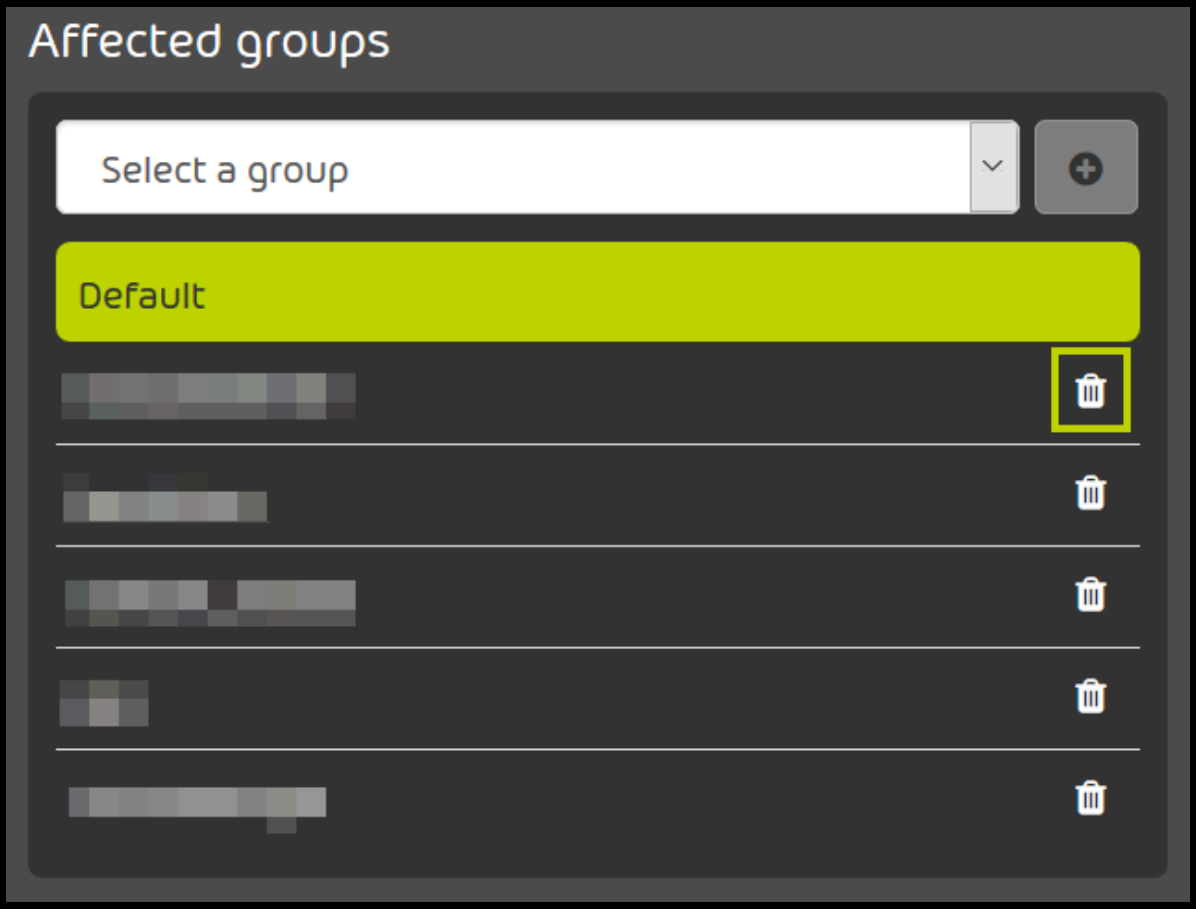


Figure 293: Deleting a group

A warning message appears.

5. Click on **Delete** to delete the group from Content Control.

The group is deleted from Content Control. The Content Control default settings are applied to the group members.

Setting up Content Control

Set up Content Control. You can modify the default settings for the domain as well as the settings for single groups.

Content Control is activated.

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.

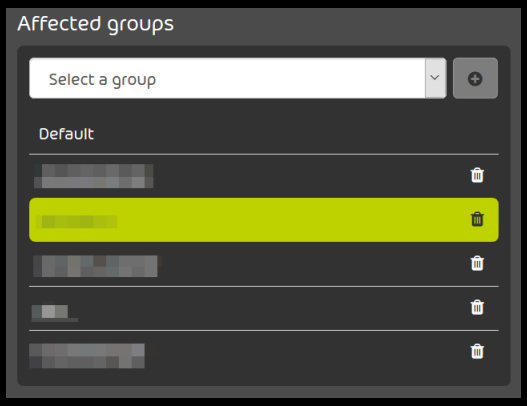


Figure 294: Selecting default or group settings

- To modify the settings for all users of the domain which 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 set up Content Control for incoming emails.
6. **Notice:**

   Select a maximum email size that does not exceed the size limit of your mail server.

   Under **Max. email size (MB)**, enter the maximum allowed email size in megabytes.

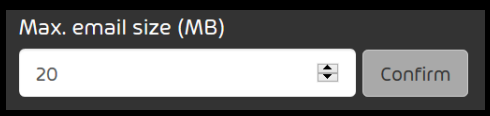


Figure 295: Entering the maximum email size

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.

Under **Handling of filtered out attachments**, select how to deal with emails with filtered out attachments.

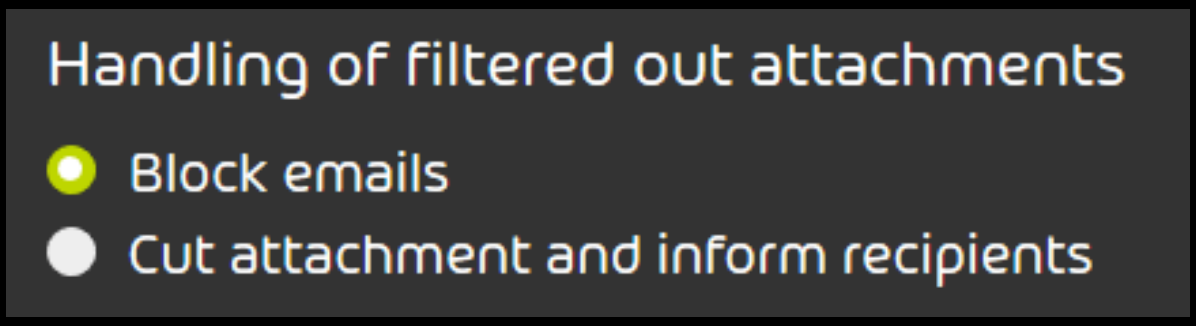


Figure 296: Select how to handle filtered out attachments

- To prevent emails with filtered out attachments from being delivered to the recipients, select **Block emails**.
- 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.

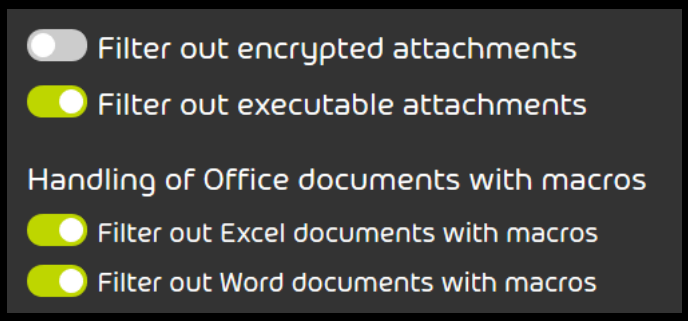


Figure 297: Filtering out attachments

- Select **Filter out encrypted attachments** to filter out encrypted attachments with the following file extensions:
  - .dot
  - .doc
  - .docx
  - .xls
  - .xlsx
  - .ppt

- .pptx
- .pdf
- .zip
- .rar
- .7z
- .gz

- Select **Filter out executable attachments** to filter out all file types from the category .executable (see Overview of Categories on page 291).
- Select **Filter out Excel documents with macros** to filter out all file types from the category .xlsmacro (see Overview of Categories on page 291).
- Select **Filter out Word documents with macros** to filter out all file types from the category .docmacro (see Overview of Categories on page 291).

10. **Notice:**

    You can use categories to filter out groups of file types (see Overview of Categories on page 291).

    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 298: 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")** and click on **Add**.

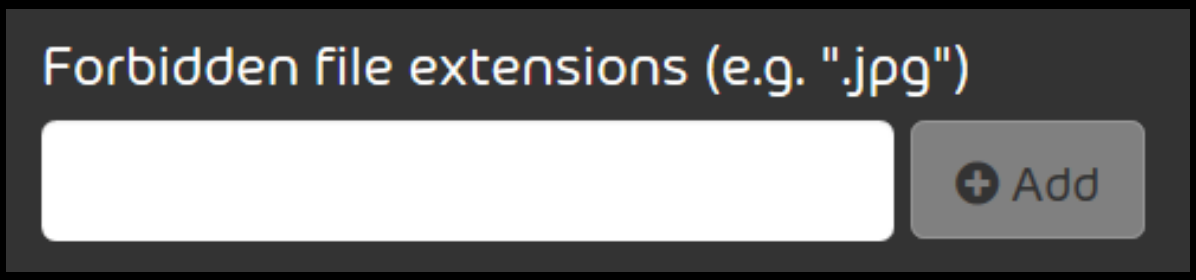


Figure 299: Filtering out file types

➔ 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 take over the file types listed above, under **Forbidden file extensions in archives (e.g. ".png")**, mark the **Inherit forbidden file extensions from above** checkbox.
    - To filter out files of a different file type, enter the file type in the field under **Forbidden file extensions in archives (e.g. ".png")** and click on **Add**.
12. Go to **Settings#→FOR OUTGOING EMAILS** to set up Content Control for outgoing emails.
13. Set up 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 make different settings for outgoing emails than for incoming emails, follow the same procedure as in the previous steps for incoming emails.

You have set up Content Control

Overview of Categories

The following table shows the categories by which groups of file types in attachments can be filtered out.

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

category	Filtered out file types
.docmacro	.doc files with macros. Email attachments in doc. format are searched for macro patterns with heuristic analysis. This filter does not cover all kinds of macros.
.xlsmacro	.xls files with macros. Email attachments in .xls format are searched for macro patterns with heuristic analysis. This filter does not cover all kinds of macros.

Deactivating Content Control

Deactivate Content Control for a domain.

Content Control is activated.

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 300: Deactivating Content Control

A warning message appears.

5. Click on **Delete** to permanently delete all Content Control settings for the domain.

Content Control is deactivated for the selected domain. All Content Control settings are permanently deleted for the domain.

Compliance Filter

Compliance Filter

Compliance Filter

With the Compliance Filter, custom filter rules are created to categorize incoming email as **Clean**, **Spam** or **Virus**. In addition, emails can be rejected, sent to another email server or the recipient can be changed.

CAUTION:

The use of incorrect filter rules has a considerable negative effect on email traffic. Filter rules can also be used to override email services. Compliance Filter is also not suitable for address rewriting.

Compliance Filter checks both incoming and outgoing email traffic. You can set up three different filter types:

- Advanced filter type to check the sender, recipient, IP, hostname and subject for search terms
- Filter for content in the email header
- Filter for content in the email body

In the email header and body, all you have to do is enter the search term in the input field. With the extended filter type, several criteria can be evaluated in parallel.

You can define an action for each individual filter that is automatically executed by the filter when an email matches the filter criteria. Different actions are possible for incoming and outgoing emails.

Setting up the Compliance Filter

Activate the Compliance Filter in the Control Panel.

1. Open the Control Panel and login.
2. **Notice:**

   Compliance Filter settings can only be configured via a partner account or as domain administrator.

   Select the domain for which you want to enable the Compliance Filter.

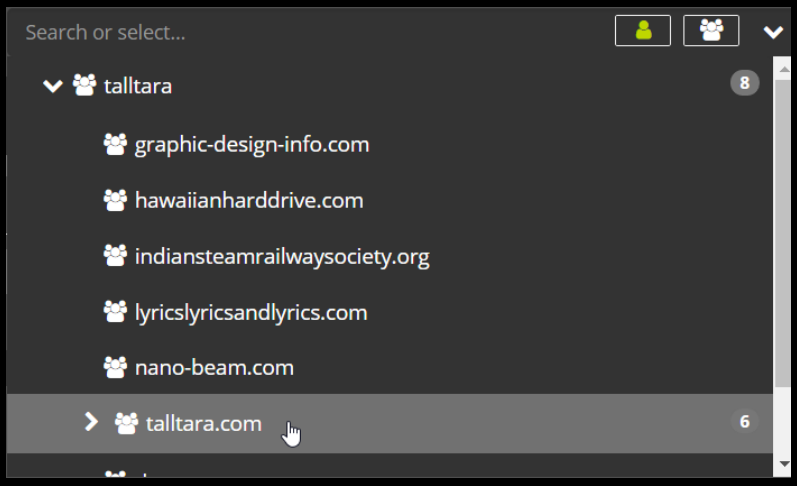


Figure 301: Domain selection

3. Navigate to **Security Settings#→Compliance Filter**.
4. Activate the checkbox **Activate Compliance Filter**.

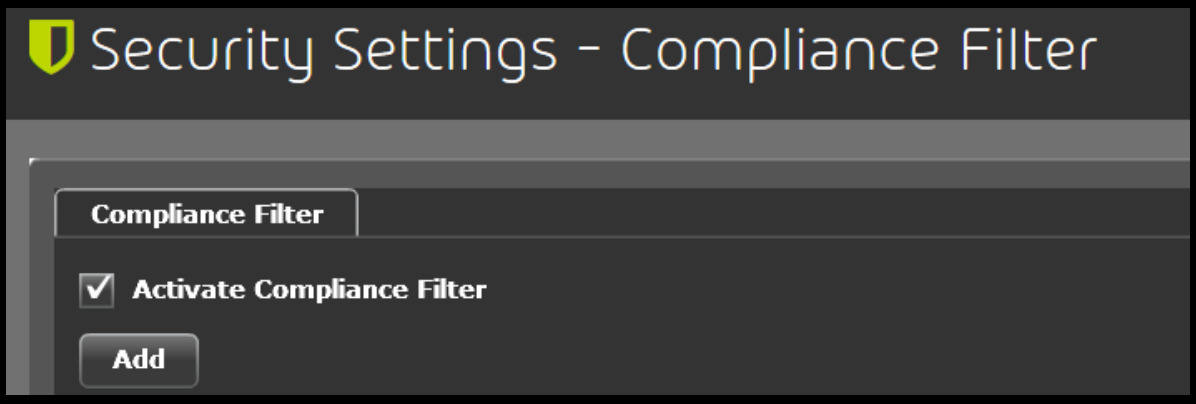


Figure 302: Activate Compliance Filter

5. Click on **Save** to confirm activation.

The Compliance Filter has been actived. You can now create filter rules.

Compliance Filter Rule Creation

The following chapters contain an explanation how filter rules are created and how actions are defined.

Adding a New Filter

Before defining a filter add a new filter.

1. Open the Compliance Filter module in the Control Panel and click on **Add**.
   A new window appears

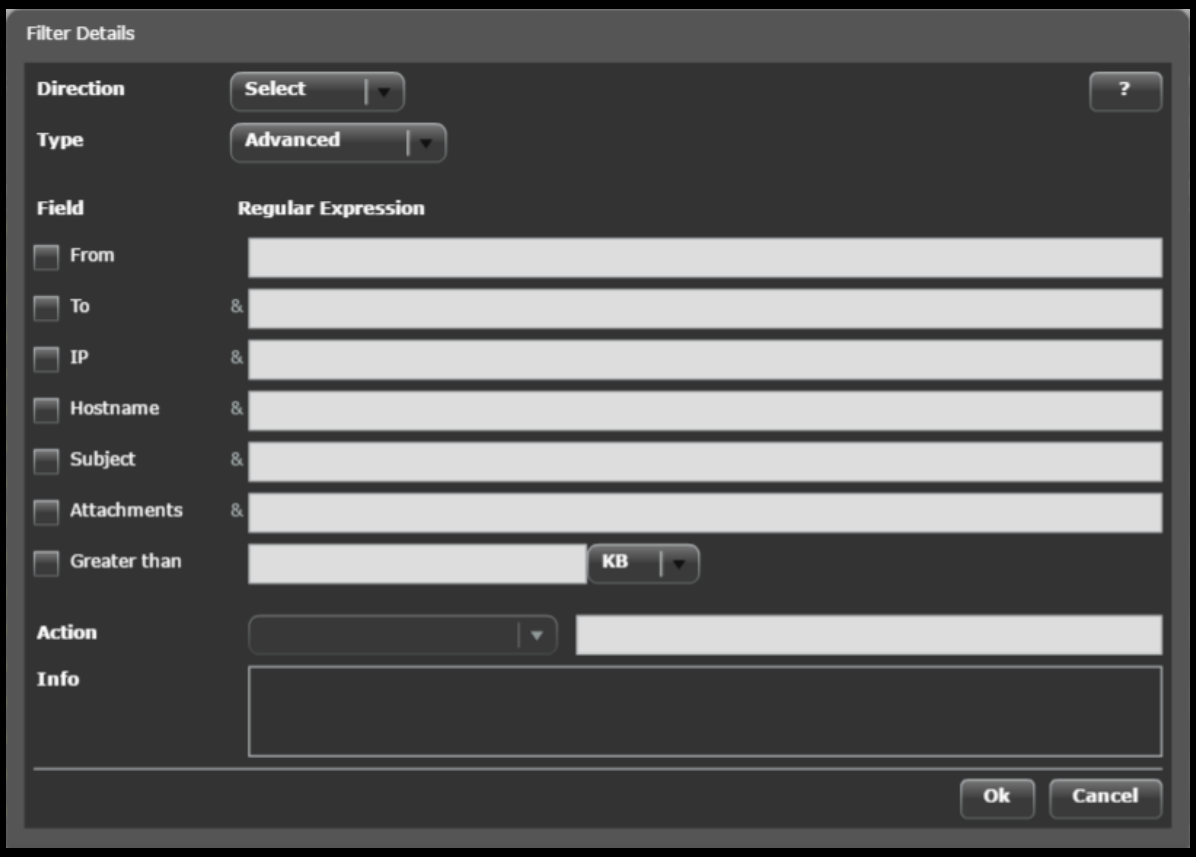


Figure 303: Compliance Filter: Extended View

Select the direction for emails handled by the filter rule from the dropdown menu:

2. In the field **Direction**, select an email direction for your filter.
3. Select the filter type from the dropdown menu:
   - Email Body: You can define a term that is searched for in the email body.
   - Email Header: You can define a term that is searched for in the email header.

- Advanced: You can define terms for different email fields and use them in combination.

4. Define the rules as shown in Defining Rules on page 296 and Defining Actions on page 298.
5. You can add a description to the filter rule in the **Info** field. The text entered has no effect on the filter rule.

Figure 304: Info field

6. Afterwards click on **Ok** to create the rule.
7. Confirm your input with **Save**.

A new filter has been added.

Defining Rules

The Compliance Filter searches emails for terms that are defined in the appropriate fields.

Following are simple examples for creating filter rules in the different filter types.

Notice:

To define filters in a more accurate and flexible way, you can also use regular expressions. For a description of the structure and functionality of regular expressions, see Regular Expressions on page 306.

Examples

Table 11: Filter definition examples

Feld	Brief description	Example
Email body	Searches the email body for the entered term.	Donate
Email header	Searches the email header for the entered term.	Make money
From	Filters for the envelope sender address.	user@gevonne.com

Feld	Brief description	Example
To	Filters for the envelope recipient address.	user.extern@yahoo.com
IP	Public IP address of the sending email server. **Notice:** Enter the IP address without subnetmask.	Right: 0.0.0.0 Wrong: 0.0.0.0/24
Hostname	PTR record (Hostname of the reverse lookup IP)	mailserver.hornetsecurity.com
Subject	Filters for the email subject.	Spam
Attachments	Filters for email attachments	.jpg
Greater than (KB/MB)	Maximum size of the email.	500

Attachments

You can filter for email attachments inside the filter type **Advanced**. Therefore, enter the file type (E.g. .exe or .jpg) inside the field **Attachments**.

Figure 305: Attachments

Notice:

You cannot use the collective terms for file types declared in the content filter for the compliance filter.

Defining Actions

An action is assigned to each filter rule. The action is executed if the rule matches.

Notice:

The Compliance Filter differs between actions for incoming and outgoing emails. The actions **Tag as Clean, Spam**, or **Virus** can only be performed on incoming emails. The action **Notify Sender** can only be performed on outgoing emails.

Table 12: Actions

Action	Description
Reject	**Attention:** The email will be blocked! The 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). The notification of the sender lies in responsibility of the email server.
Redirect	The email is redirected to one or more email addresses. You can enter as many email addresses as you want in the field. Separate the email addresses with spaces.
Reroute	The email is sent to another IP address or hostname. You can only enter one IP address or hostname into the field.

Action	Description
Add BCC	This action automatically adds one or more BCC Recipients. You can enter as many email addresses as you want in the field. Separate the email addresses with spaces.
Notify Sender	The Sender automatically receives an infomail, as soon as their email is accepted by the destination server.
Tag as Clean	Classifies the incoming email as clean.
Tag as Spam	Classifies the incoming email as spam.
Tag as Virus	Classifies the incoming email as Virus.

Filter Sequence and Classification

The order of the filter rules can be changed in the overview of the Compliance Filter.

Important:

You must observe the predefined sequence of filter rules (see Ruleset order on page 274. If a rule is fulfilled, the process is stopped and it is possible that some filter rules are not applied because another filter rule takes precedence.

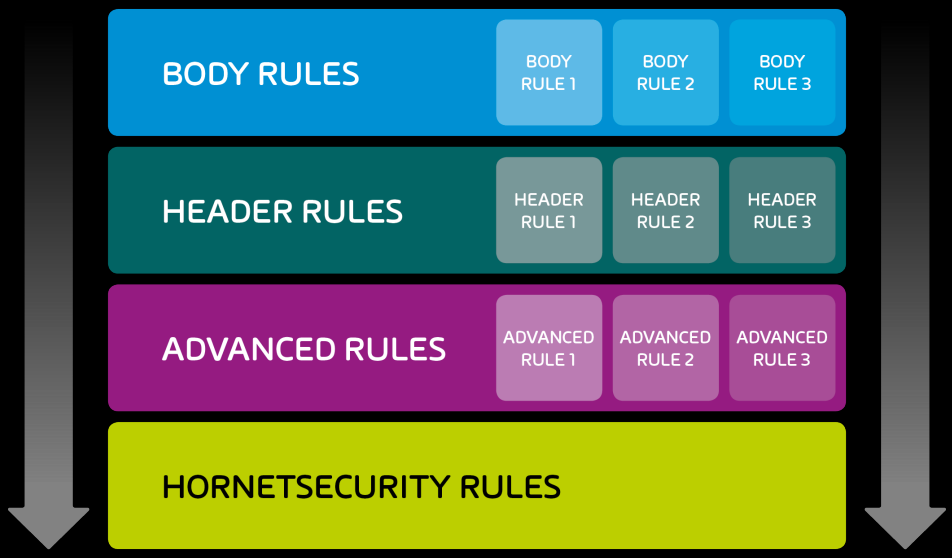


Figure 306: Sequence of filter rules

Notice:

The Compliance Filter cannot be used to create exceptions for the Content Control. In this case, Content Control takes precedence over the Compliance Filter and deviates from the regular rule sequence (see Ruleset order on page 274).

The following examples illustrate the sequence in which rules are processed.

Notice:

Dots and asterisks (.*) are automatically added to the fields before and after an expression.

Example: Simple filter application sequence

Initial situation:

The filter defined in figure above is the only rule. No other rules apply to that case.

Execution:

1. "invoice@anycompany.com" sends an email to any user of the domain "yourcompany.com".
2. The Compliance Filter first searches the body rules, then the header rules and finds a match in the advanced rules.

3. The rule is applied and the Compliance Filter does not search for other rules.

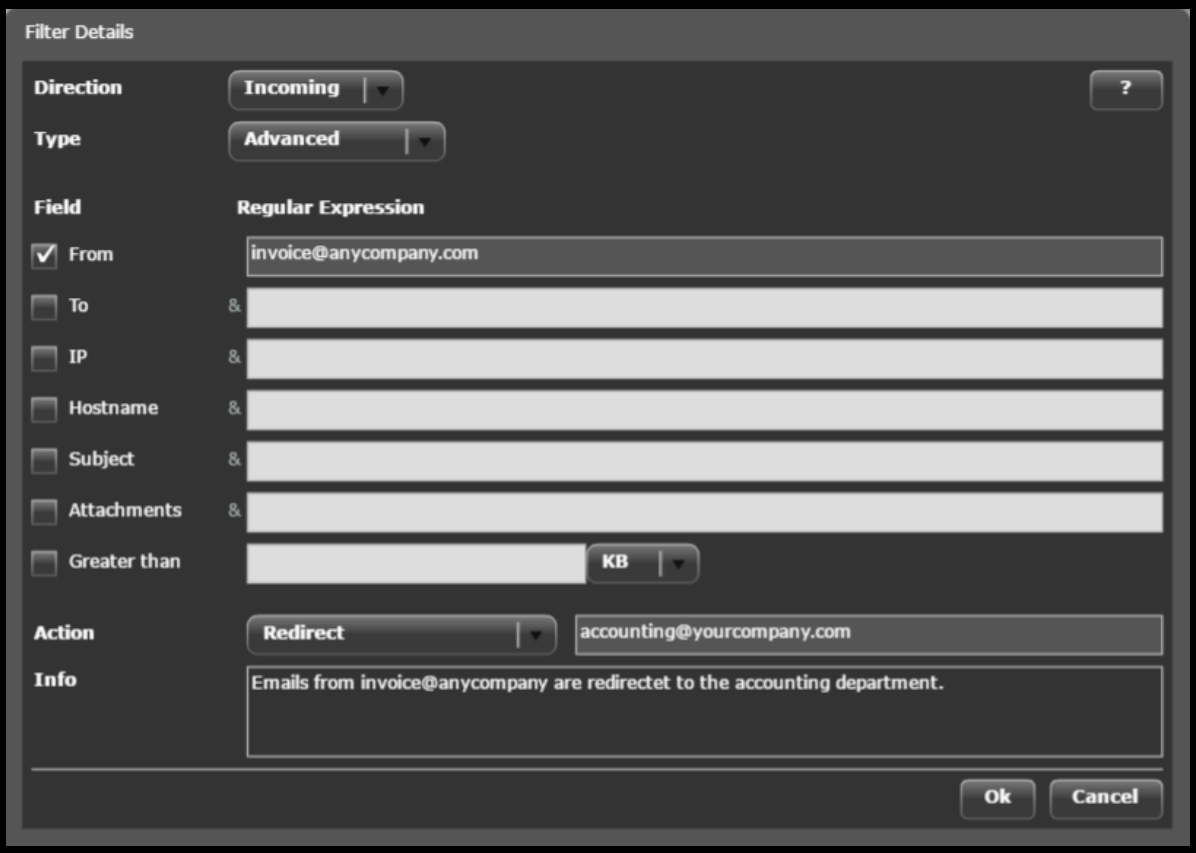


Figure 307: Filter rule: Redirect

Example: Conflict between two rules of one type

Initial situation:

Two different rules are defined for the case that an outgoing email is sent to "order@anycompany.com". In the rule overview, the rule 256083 (Purchase in BCC) stands before the rule 256063 (CEO in BCC). No other rules apply to that case.

Procedure:

1. Any user sends an email to "order@anycompany.com".
2. The Compliance Filter first searches the body rules, then the header rules and finds a match in the advanced rules.
3. The rule 256083 (purchase in BCC) is applied and the further procedure is stopped. The rule 256063 (CEO in BCC) is not applied.

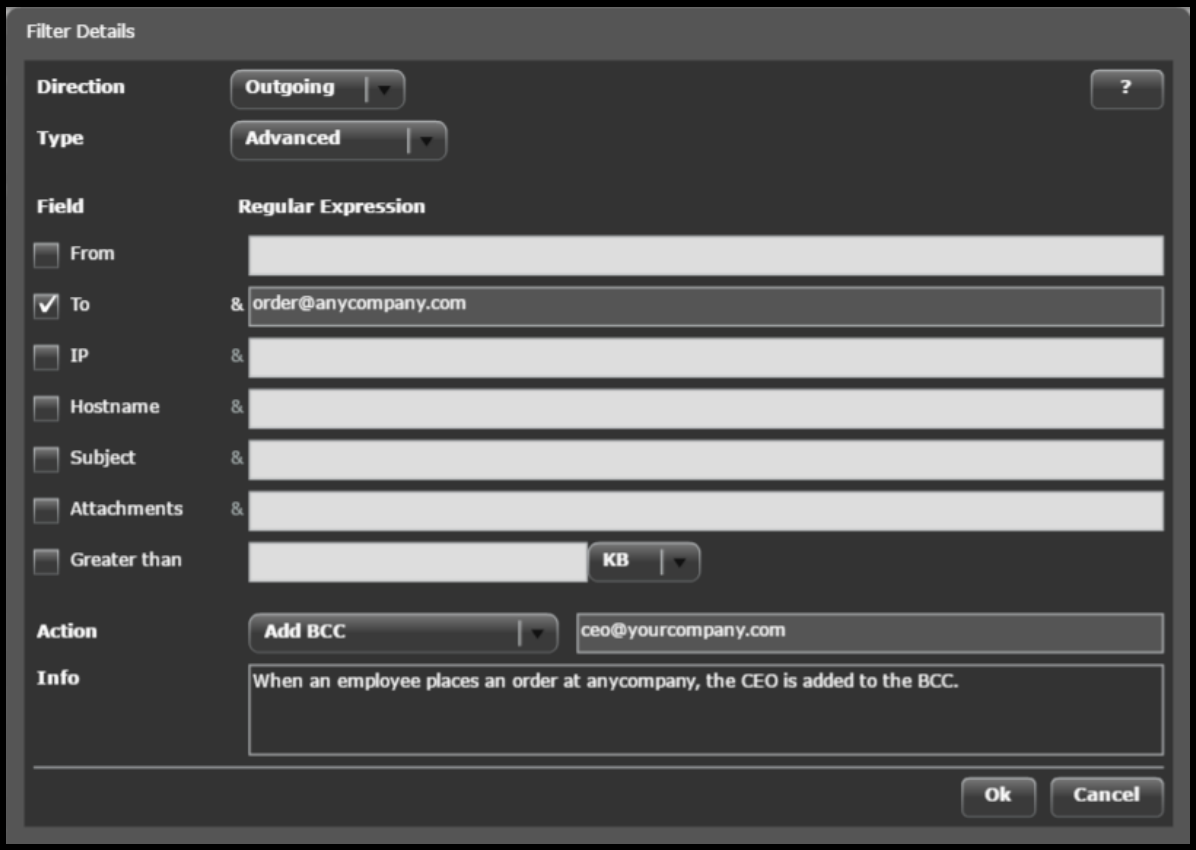


Figure 308: Filter rule: Add BCC to ceo@

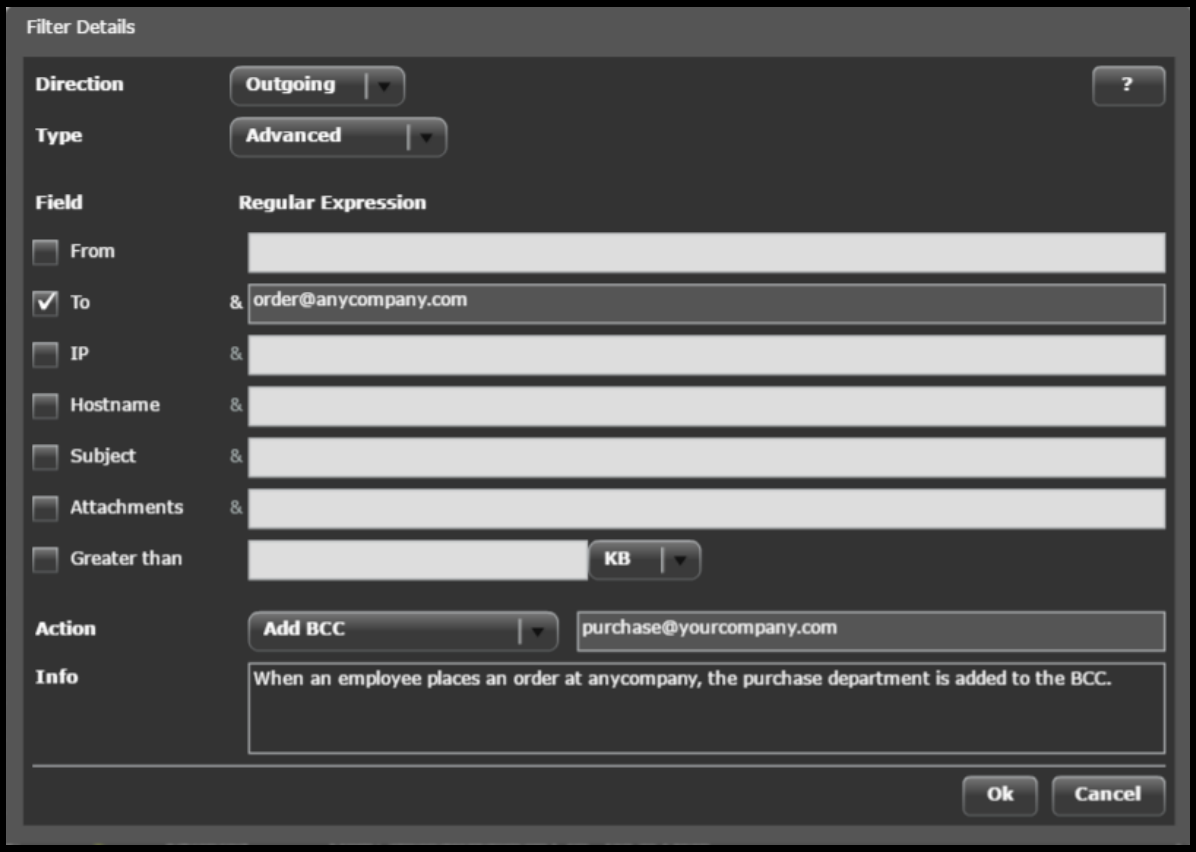


Figure 309: Filter rule: Add BCC to purchase@

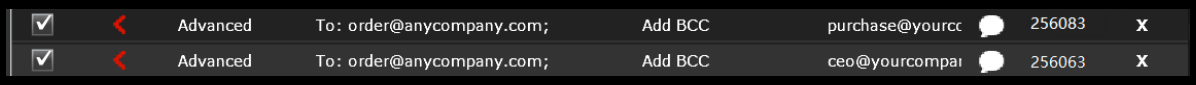


Figure 310: Order of the defined filters

Example: Conflict between multiple rules of different types

Initial situation:

Incoming emails that contain a link to Facebook are marked as spam. The marketing department is partly excluded from that rule, when receiving emails from Facebook directly, they are marked as clean. In the overview the rule (ID 259163) stands before the rule (ID 259143). No other rules apply to that case.

Execution:

1. A recipient from marketing receives an email from Facebook that contains a link.
2. The Compliance Filter searches the body rules and hits the rule (ID 259143).

3. The email is marked as spam and the execution stops.
4. The rule (ID 259163) is being ignored, although it is above the other rule in the overview as the body rules are applied first.

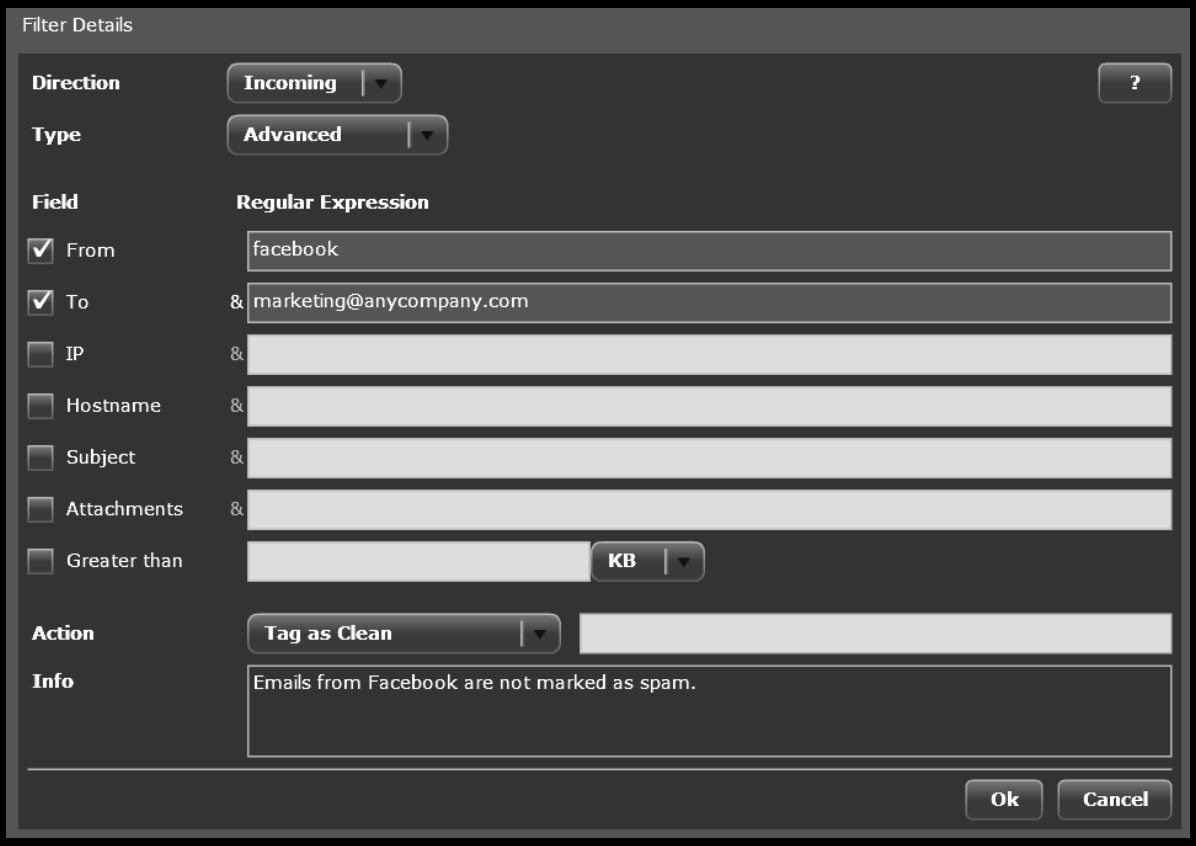


Figure 311: Filter rule: Tag as clean

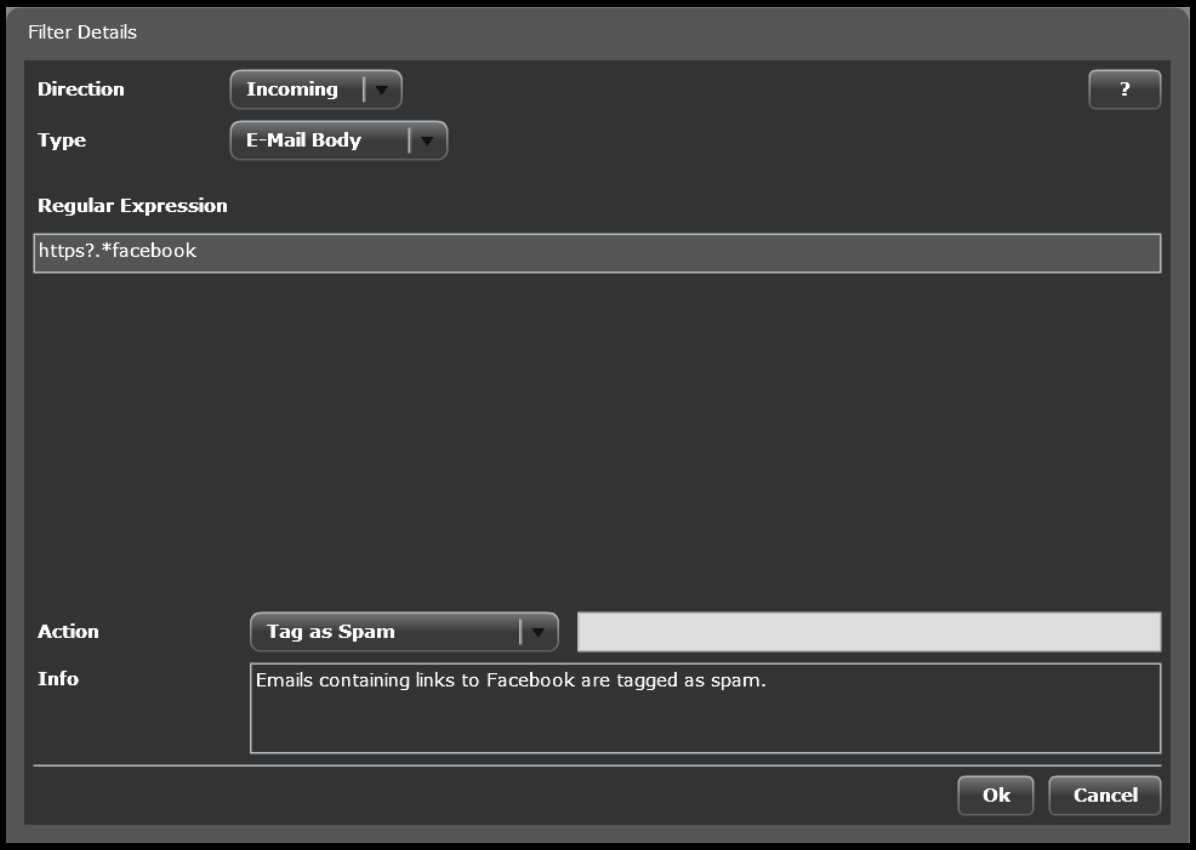


Figure 312: Filter rule: Tag as spam

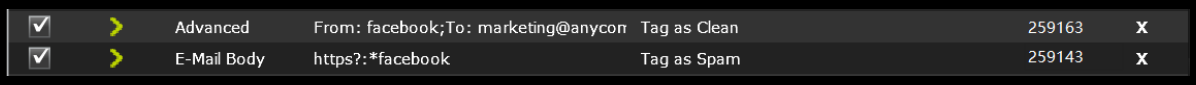


Figure 313: Order of the defined filters

Example: Conflict between a Compliance Filter rule and a Hornetsecurity filter

Initial situation:

Because of increased spam occurrence from an IP address, a rule is defined that the emails from that IP address are always marked as spam. No other Compliance Filter rule applies to that case.

Procedure:

1. A sender of the domain behind the IP address sends an email to any recipient.
2. The Compliance Filter first searches the body rules, then the header rules and matches a rule in the advanced rules.

3. The email is marked as spam and the execution stops.

4. Hornetsecurity has already defined precise filter rules for this domain. The increased spam volume could be narrowed down to the sender "info@"; other e-mail addresses do not send spam emails. However, since these filter rules are not applied, the specially defined rule applies with too large a validity scope. A clean email could therefore be marked as spam.

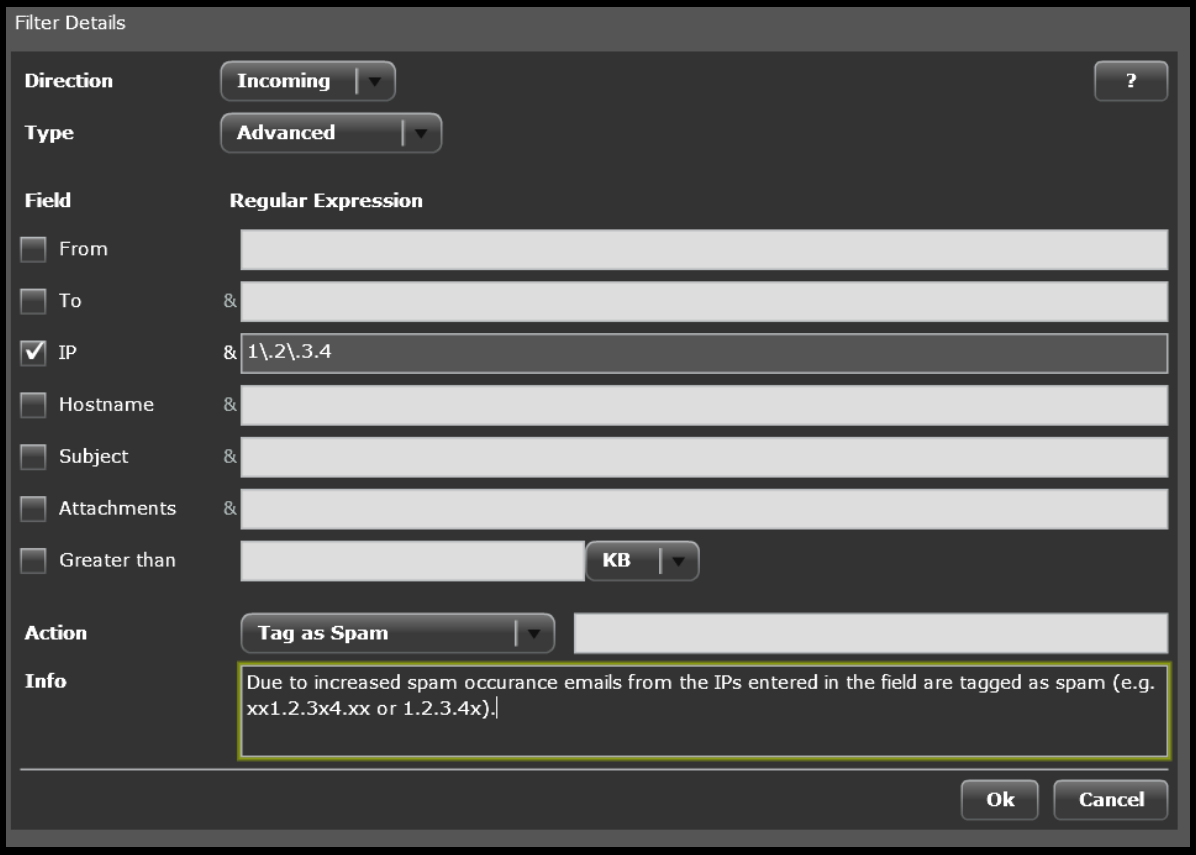


Figure 314: Filter rule: Tag emails from a certain IP address as spam

Regular Expressions

Regular expressions (RegEx) are used within the Compliance Filter to extract information from a string. Thus, it is possible to recognize and filter patterns in the subject or other components of an email.

The system automatically adds a ".*" to the beginning and the end of the subject as well as to the email body and header.

Important:

You can use Perl Compatible Regular Expressions. Other Libraries are not supported. (For more information, see: http://www.pcre.org/). In addition, there are special restrictions that are explained in the following.

Example: Using regular expressions in the Compliance Filter

Users often received emails with the subject "porn". An appropriate filter rule was set up to mark them as spam. Recently, an increased appearance of spam emails using leetspeak were observed to bypass the filter. For example, emails with the subject "p0rn" passed the filter rule. Therefore, the use of a regular expression is more effective:

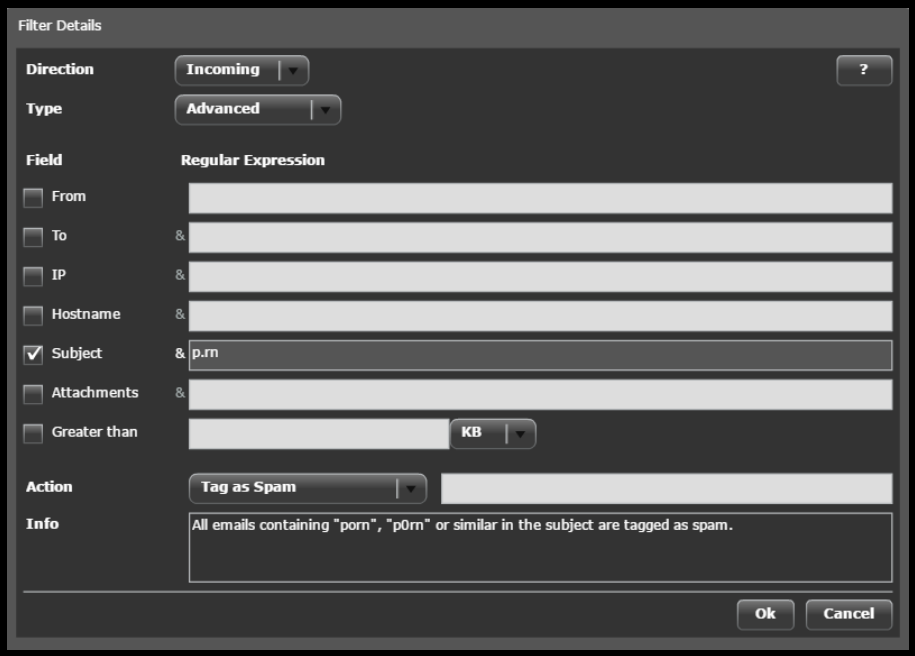


Figure 315: Using a regular expression in the Compliance Filter

Instead of the dot any character is interpreted as valid. Therefore, the filter is not determined to an "o", it reacts to any letter, digit and special character.

Creating Valid 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 captured by the regular expression.

Table 13: Match letters

Text	RegEx
abcdef	abc
abcde	
Abcd	

Enter letters to search for corresponding matches inside the text.

Table 14: Match 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, you can use the character class "\d" to match any digit.

Table 15: Match any character

Text	RegEx
bob.	...\.
tom.	
?!a.	
abc1	

The "." declares, that any character matches. If you want to match a dot, you must escape it with "\.".

Table 16: Match multiple characters

Text	RegEx
aaaaaaaaaa**b**	b+
aa**bbbbb**c	

Text	RegEx
acd	
aaaaaa**bb**e	

The trailing plus sign means that the sign may occur once or several times. If it does not occur, no match is made.

Table 17: Optional characters

Text	RegEx
3 users online	\d+ users? online
150 users online	
20 users online	
1 user online	
no user online	

Appending a "?", the leading character is declared as optional.

Table 18: Group regular expressions

Text	RegEx
dump025.csv	\w+\d+\.(\w+)
dump026.csv	

Parentheses group a series of pattern to a single element. In the example above, only the file extension after the dot is grouped.

> **Important:**
>
> You can only create one group per regular expression.

Table 19: Either/or match

Text	RegEx
data.csv	.*\.(exe|xlsx)
bild.jpg	

Text	RegEx
moving.gif	
document.pdf	
virus.exe	
locky.xlsx	

The "|" inside the round brackets describes, that any pattern separated by it is valid.

Table 20: Back reference

Text	RegEx
From: "local@domain.de" <local@domain.de>	From: "(.*@.*\.de)" \<\1\>
From: "local@domain.de" <hacker@hackeddomain.de>	

The back reference \1 takes the group definition (.*@.*\.de). A match is only made if the match of the group appears again at the referenced place.

The following syntax elements can be used to define regular expressions in the Compliance Filter:

Table 21: Syntax elements

Wildcard/Character class	Function
abc...	Letters
123...	Digits
\d	Any digit
.	Any character
\. \/ *	Escaping (The characters in bold)
\w	Any alphanumeric character
*	0 or more repetitions
+	1 or more repetitions
?	Optional character
\s	Any whitespace

Wildcard/Character class	Function
(...)	Group
(.*)	Match all
(abc|def)	Matches abc or def

Example for a Complex Regular Expression

Finally, we are facing the usage of a complex regular expression within the Compliance Filter:

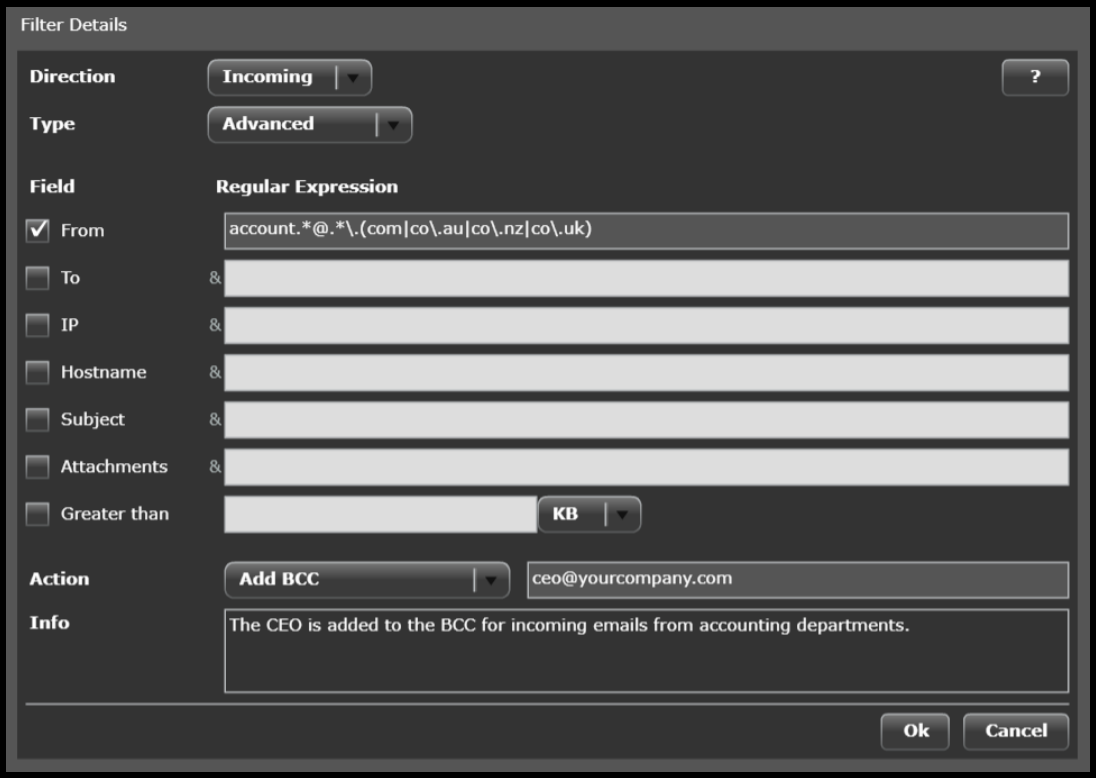


Figure 316: Complex regular expression

With this regular expression, you can, for example, match the following text segments:

- account@test.com
- accounting@testabc.co.au
- accountest@mytest.co.nz
- accountingtest@domain.co.uk

and many more combinations.

Exceptions to Regular Expressions for the Compliance Filter

The creation of regular expressions for the Compliance Filter differs from PCRE-compliant expressions because not all syntax elements can be used.

All syntax elements listed below cannot be used to create rules with regular expressions in the Compliance Filter:

- Square brackets "[]"
- Curly brackets "{}"
- Circumflex "^"
- Dollar sign "$"
- Only one group with parentheses "()" can be formed.

In addition, regular expressions are not case-sensitive.

Ruleset order

Spam and Malware Protection rules are processed according to a specific priority. If a rule with a high priority applies, processing is usually terminated. In some cases, this can lead to messages being blocked despite a whitelist entry for the sender's address, because the IP address of the sending server is on the RBL blacklist.

Rule order (from top to bottom in descending priority).

Incoming emails

1. RBL list (block)
2. Mass spam detection (block)
3. Compliance filter (deliver)
4. Virus check (quarantine)
5. Content Control, if activated (quarantine)
6. User-based whitelist string (deliver)
7. User-based blacklist string (quarantine)
8. Administrative whitelist (deliver)
9. Administrative blacklist (quarantine)

10. General whitelist (deliver)
11. General spam rules (quarantine)
12. Infomail filter (quarantine)

Notice: Due to this order, it is possible to create exceptions for Content Control with Compliance Filter rules which categorize emails as **Clean**. However, since user-based and administrative whitelisting and blacklisting are applied after the Content Control rules, they cannot be used to create exceptions for Content Control.

Outgoing emails

1. RBL list
2. Compliance Filter
3. Virus check
4. Content Control, if activated

Setting up Advanced Routing

You can use the function **Advanced Routing** to assign different mail servers to individual users or groups. Email traffic is then routed through these servers.

1. Navigate to **Security Settings**#→**Advanced Routing**.
2. Activate the checkbox **Activate Advanced Routing**.
   → **Further selection windows are activated.**
3. Select whether routing is to be performed for specific users or a user group.
4. Click **Select** to select a user or a group.
5. Enter the IP or host address that you want to use to route email traffic.
6. Click **Add**.
   → **The selected group is displayed in the list below.**
7. Confirm the changes with **Save**.

Advanced Routing is set up.

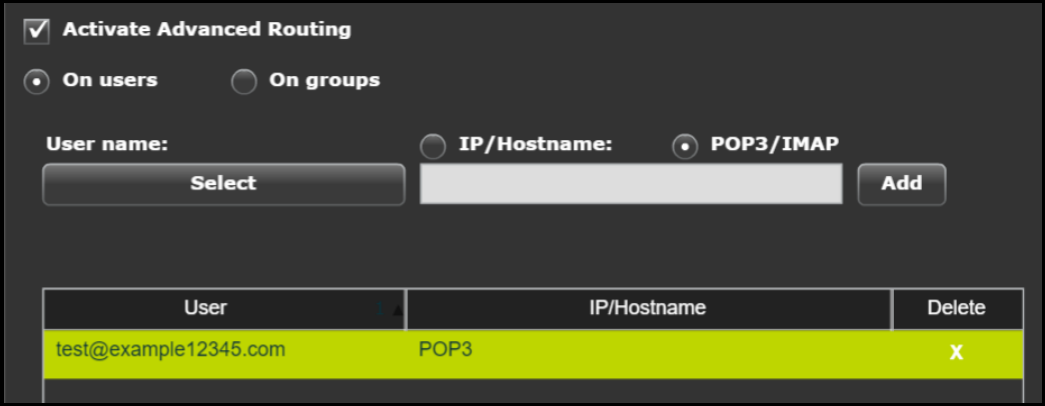


Figure 317: Setup Advanced Routing

Signature and Disclaimer

Introduction

Signature & Disclaimer controls the automated provision of email signatures and disclaimers on all Hornetsecurity gates. 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.

Notice:

There are two different variants of the **Signature & Disclaimer**. If you activated the checkbox at **Mail Footer** under **Management#→Email** in the old Control Panel, did not activate an LDAP connection and do not use Total Protection Enterprise or Business, you can use a static variant of the **Signature & Disclaimer**. However, you cannot use all functions. For more information see the documentation Signature & Disclaimer - Static Version .

Mobile Use of Signature & Disclaimer

With the activation of Signature & Disclaimer, the created signatures and disclaimers are also attached to emails sent from mobile devices.

Notice:

When using a mobile device with the Android, the installed Android version must still be supported so that the signature and the disclaimer are properly attached. Make sure that you are using a supported version so that your emails are displayed correctly.

Activating LDAP for Signature & Disclaimer

To use Signature & Disclaimer, activate it in the Control Panel. After the activation, optionally configure a different LDAP server for the synchronization and enter filters for the user synchronization.

Important:

Do not follow the steps in this chapter if you are an Microsoft 365 customer. You cannot use LDAP and the Microsoft 365 synchronization of attributes simultaneously. Follow the steps in the chapter Activating Signature & Disclaimer in the Web Interface on page 317

To use Signature & Disclaimer, you must activate it in the Control Panel.To use Signature & Disclaimer, activate it in the Control Panel. After the activation, optionally configure a different LDAP server for the synchronization and enter filters for the user synchronization.

1. Select **Service Dashboard#→LDAP connection#→Advanced Signature and Disclaimer** in the Control Panel.
2. Activate the checkbox **Activate Signature and Disclaimer**.

   Attention:

   Activating Signature & Disclaimer could be additionally charged depending on your license.

   a) Confirm the notification with **OK**.

3. **Notice:**

   Follow this step if you want to use a different directory service for the user synchronization with Signature and Disclaimer.

   Optional: Deactivate the checkbox **Use LDAP information for Signature and Disclaimer**.

   a) Define the logon information in the appearing fields.

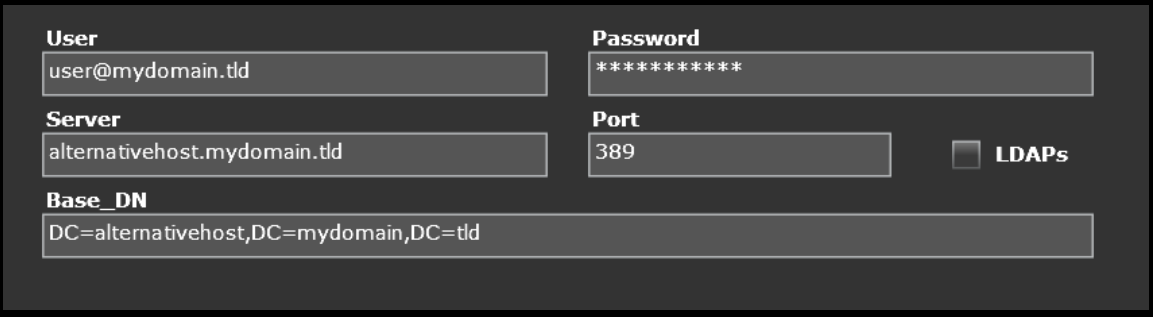


Figure 318: Selecting a different LDAP server

4. Optional: Enter the desired filter in the field **LDAP Filter**.

   Notice:

   The value **proxyaddresses=*** selects all users in an Active Directory. If your template does not comply with your directory structure, you can customize it here individually.

5. Click on **Save** in the lower left corner of the window.

You have activated LDAP for Signature & Disclaimer in the Control Panel.

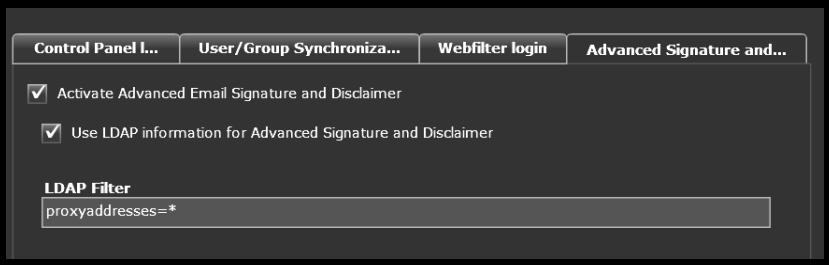


Figure 319: Activate Signature & Disclaimer

Now you can configure Signature & Disclaimer for users and groups of your directory service.

Activating Signature & Disclaimer in the Web Interface

To use Signature & Disclaimer, organize the users in an Active Directory and configure the LDAP synchronization for the corresponding domain in the Control Panel.

Notice:

Signature & Disclaimer can be used for for plain text messages as well.

You can access the Signature & Disclaimer web interface in the Control Panel under **Security Settings#→Signature & Disclaimer**.

1. From the scope selection, select the customer for which you want to activate the **Signature & Disclaimer**.
2. Activate the check box **Activate Signature and Disclaimer**.

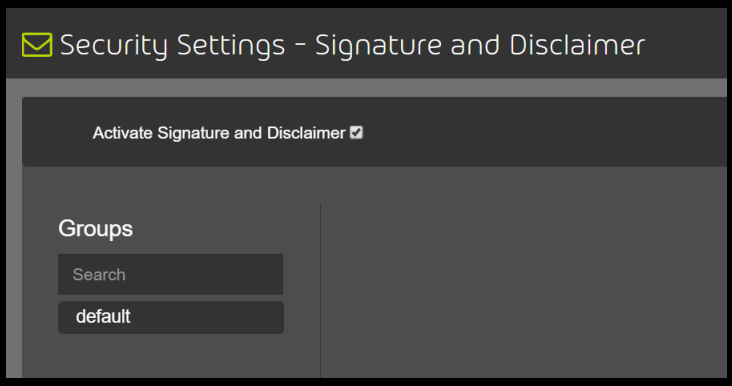


Figure 320: Activate Signature & Disclaimer

3. Click on **OK** to confirm the activation.

Signature & Disclaimer has been activated in the Web Interface.

Creating Signatures and Disclaimers

Create and activate group-based signatures and 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. 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.

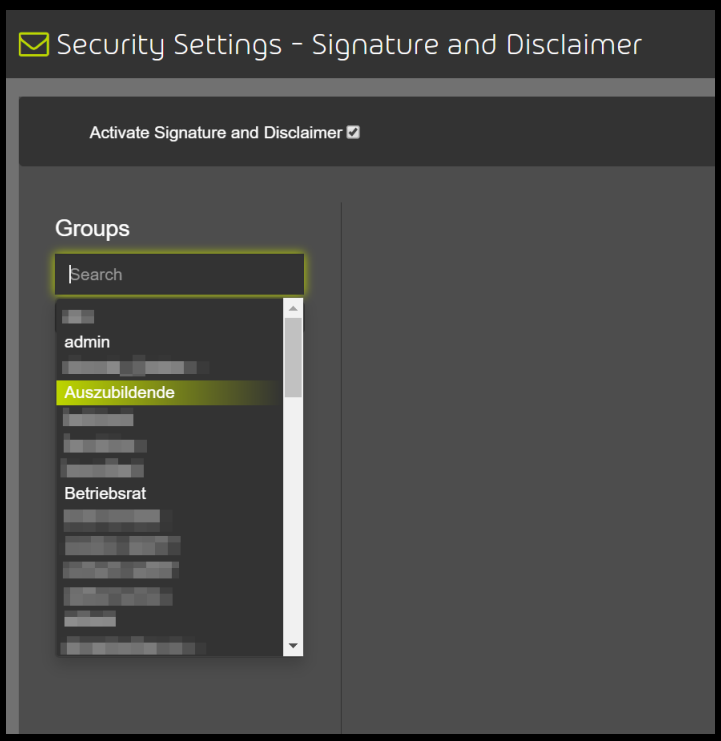


Figure 321: Add a group

2. Select the added group.

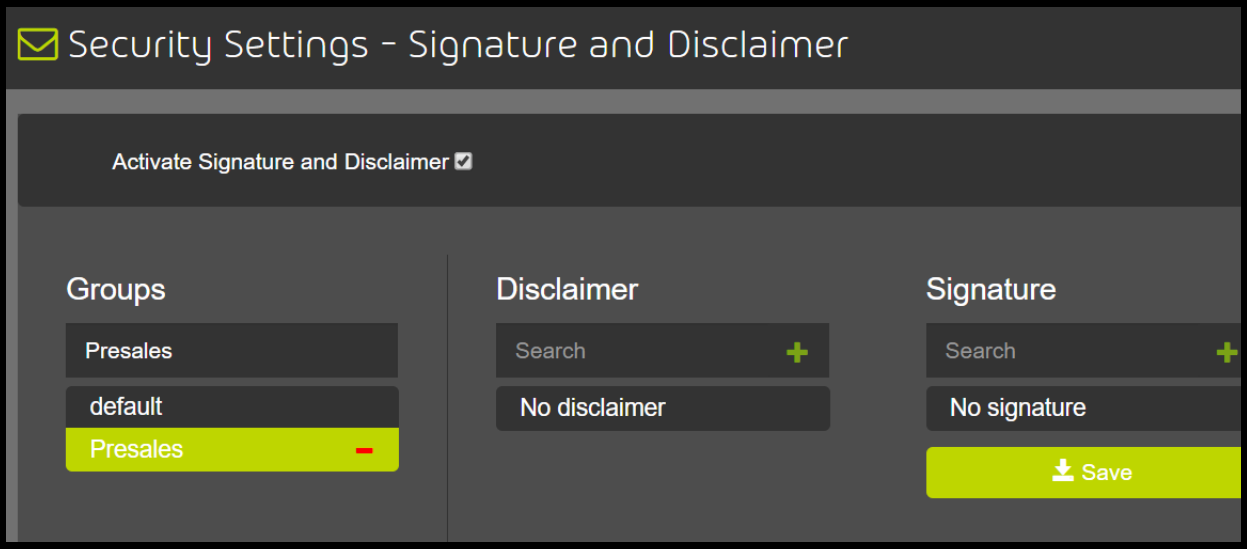


Figure 322: Select a group

On the right hand side of the main window, the selection of signatures and disclaimers appears.

3. On the right side under **Disclaimer** or **Signature**, click on **+** to create a new template.

Figure 323: Add a new template

4. Enter a name for the new template.

You can create templates for signatures or disclaimers for both HTML and plain emails at the same time. The templates are created separately.

5. Select the format for which you want to create the template:
   - HTML
   - Plain

Notice:

While editing, you can switch between the formats.

6. Define the template in the What You See Is What You Get editor (WYSIWYG editor): Using the WYSIWYG Editor on page 322

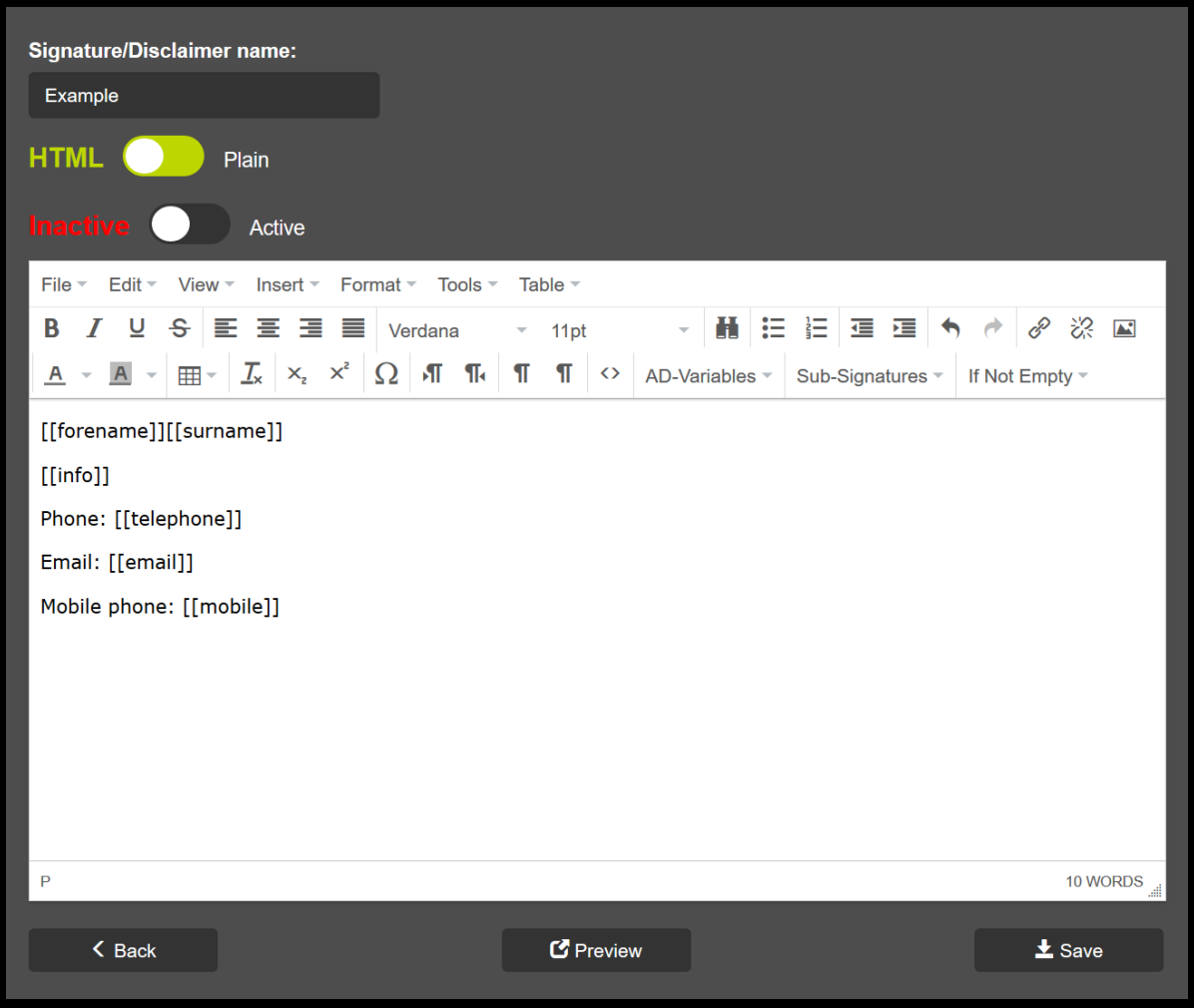


Figure 324: Define a template in the WYSIWYG editor

7. Save your template and select it in the main window.

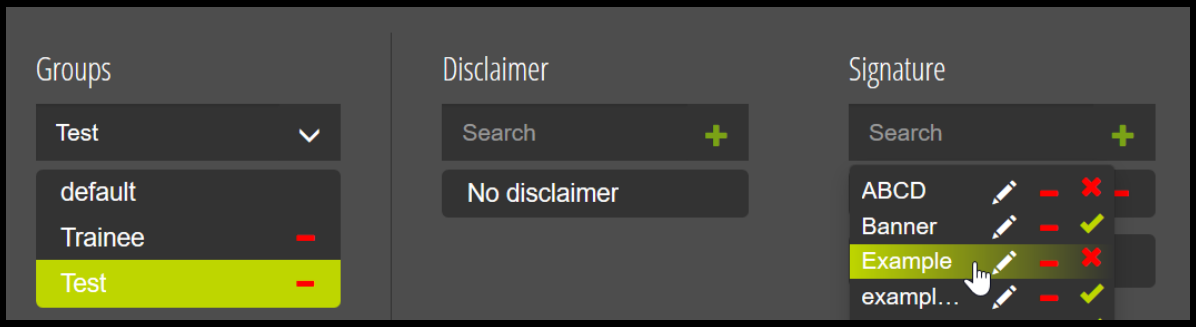


Figure 325: Select a signature in the main window

8. In the overview, click on **Save** to assign the previously selected template to the selected group.

You have created a signature and/or a disclaimer and assigned it to a group.

Notice:

Signatures and disclaimers are only added to emails which are sent via the relay IP addresses specified under Spam and Malware Protection (see Environment Settings on page 276).

Editing or Deleting Signature and Disclaimer Templates

1. Click on the field **Search** in the main window under **Signature** or **Disclaimer** and select the desired template.

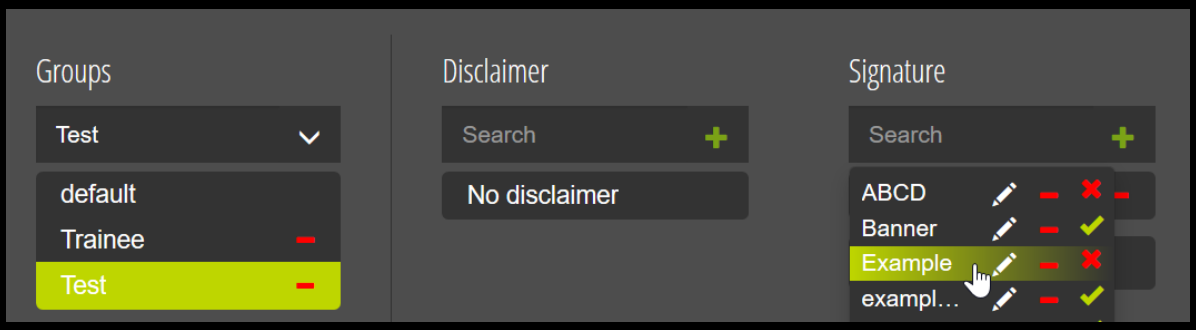


Figure 326: Select a signature in the main window

2. 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.

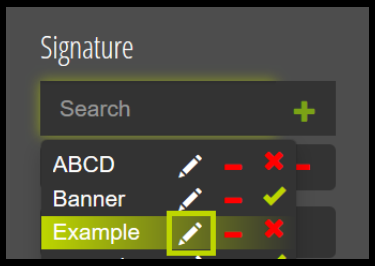


Figure 327: Edit a template

- To delete the selected template, click on the red **–** and confirm the deletion with **OK**.

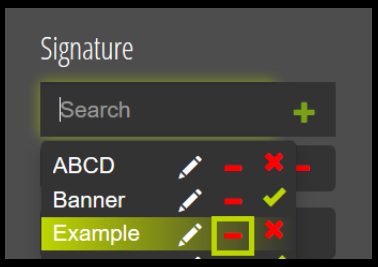


Figure 328: Delete a template

You have edited or deleted a signature or a disclaimer.

Using the WYSIWYG Editor

User attributes from the Active Directory can be entered into the WYSIWYG editor by selecting them from the drop-down menu **AD-Variables**.

You can easily create templates for signatures and disclaimers in the WYSIWYG editor.

The editor provides simple formatting options for example, paragraph alignment, font style and bulleting. Furthermore, you can use variables from the Active Directory to, for example, insert the first and last name of a user.

The following table provides all Active Directory attributes that you can select under **AD-Variables** in the editor.

Important:

You must have defined the variables in your Active Directory to use them in the editor.

Important:

When using the Azure Active Directory, not all attributes from the following table are synchronized. You can find a table with usable attributes under Synchronized Attributes from the Azure Active Directory on page 97.

AD-Variable	Description
cn	Common name
company	Company
countryCode	Country code
department	Department
description	Description
directReports	Employee
displayName	Complete name
facsimileTelephoneNumber	Facsimile Phone number
givenName	First name
homePhone	Private phone number
info	Jobtitle/Position **Notice:** The field Title is often used for other purposes. Therefore, the term Info is used here for the LDAP-attribute Title (Jobtitle/Position).
ipPhone	IP Phone
l (lower case L)	City
mail	Email address
manager	Manager
mobile	Mobile phone number
msExchIMAddress	IM address

AD-Variable	Description
pager	Pager number
physicalDeliveryOfficeName	Office
postalCode	Postal code
postOfficeBox	Post office box
samAccountName	User account name
sn	Surname
st	State
streetAddress	Street
telephoneNumber	Phone number
wwwHomepage	Website

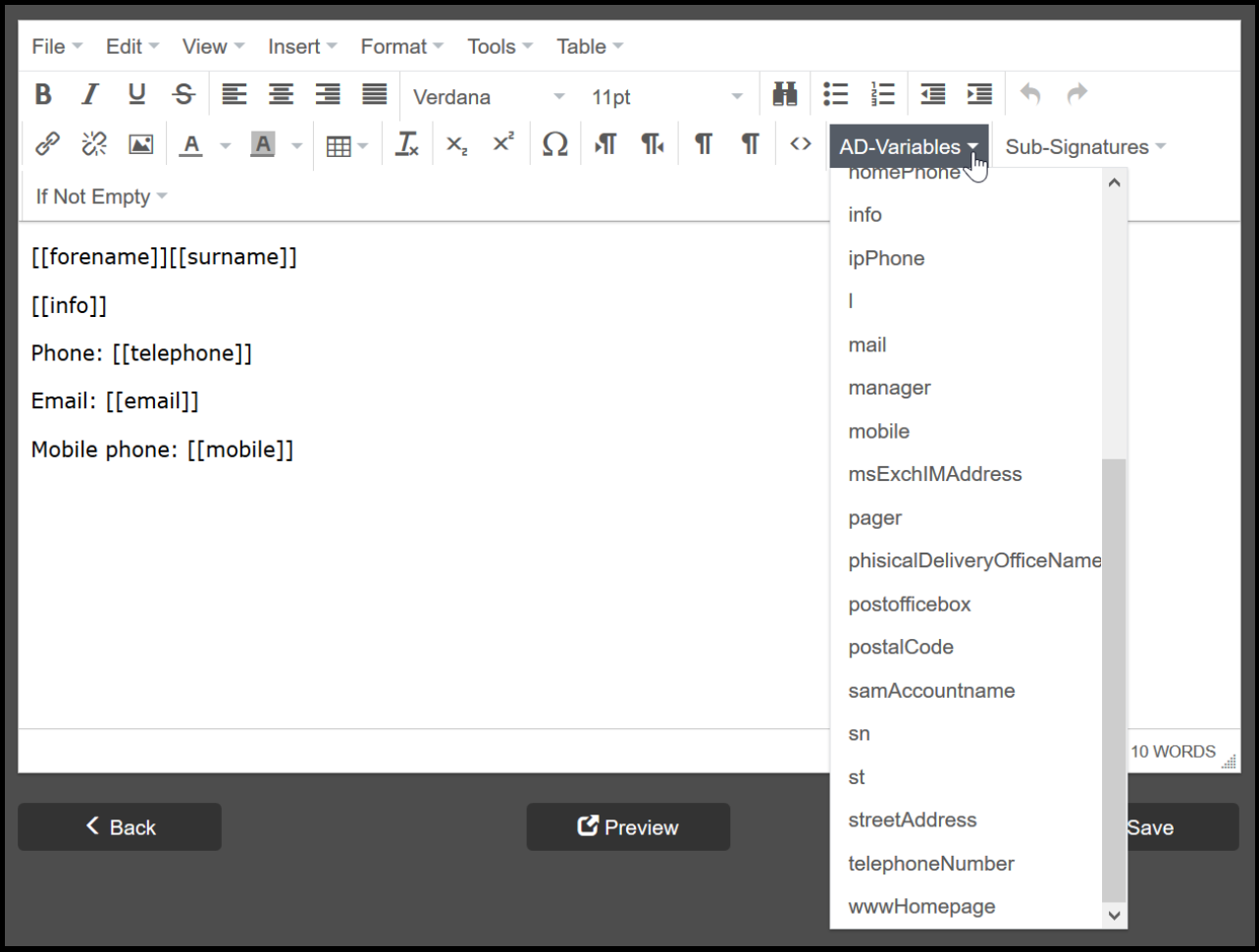


Figure 329: Active Directory attributes

Synchronized Attributes from the Azure Active Directory

With the Azure Active Directory of Microsoft only certain attributes are synchronized for Signature & Disclaimer.

> **Important:**
>
> It is not possible to use LDAP and attribute synchronization via Microsoft 365 at the same time. For Microsoft 365 customers, only the attributes in the table below are synchronized. The LDAP attributes are not synchronized.

The following attributes are synchronized and can be used to create signatures and disclaimers:

AD-Variable	Description
countryCode	Country code
department	Department
displayName	Complete name
givenName	First name
info	Jobtitle/Position **Notice:** The field Title is often used for other purposes. Therefore, the term Info is used here for the LDAP-attribute Title (Jobtitle/Position).
l (lower case L)	City
mail	Email address
mobile	Mobile phone number
postalCode	Postal code
sn	Surname
st	State
streetAddress	Street
telephoneNumber	Phone number

Hiding Empty Active Directory Elements

Use the **If Not Empty function** to hide content in signatures and disclaimers if certain AD variables are not filled for users.

1. Create a new signature or disclaimer or edit an existing one.
2. Select the line in the editor in which you want to insert the AD variable.
3. Click on **If Not Empty**.

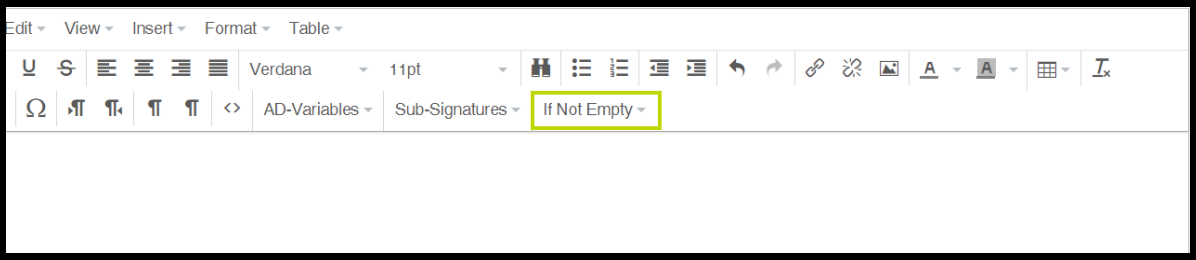


Figure 330: Open the selection

4. Select the desired AD variable from the field **Variable**.

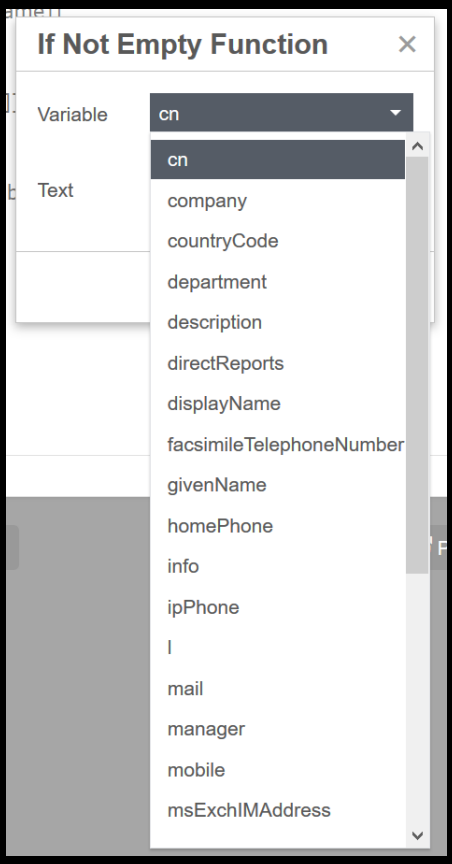


Figure 331: Select AD variable

5. Enter the text that you want to hide if the element is not filled for the user.
6. Confirm with **OK**.
7. 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.

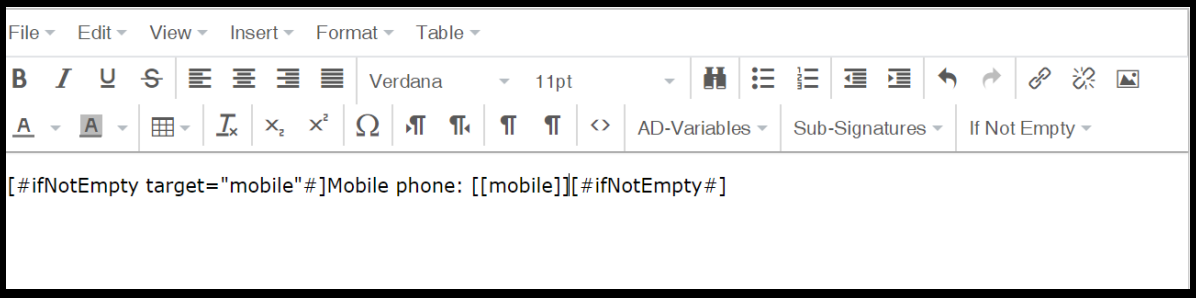


Figure 332: If Not Empty - Mobile phone

8. Click on **Save** to save the signature or disclaimer.

Empty Active Directory variables are hidden.

Example: Hiding non-existent AD variables

The following signature is created for all users:

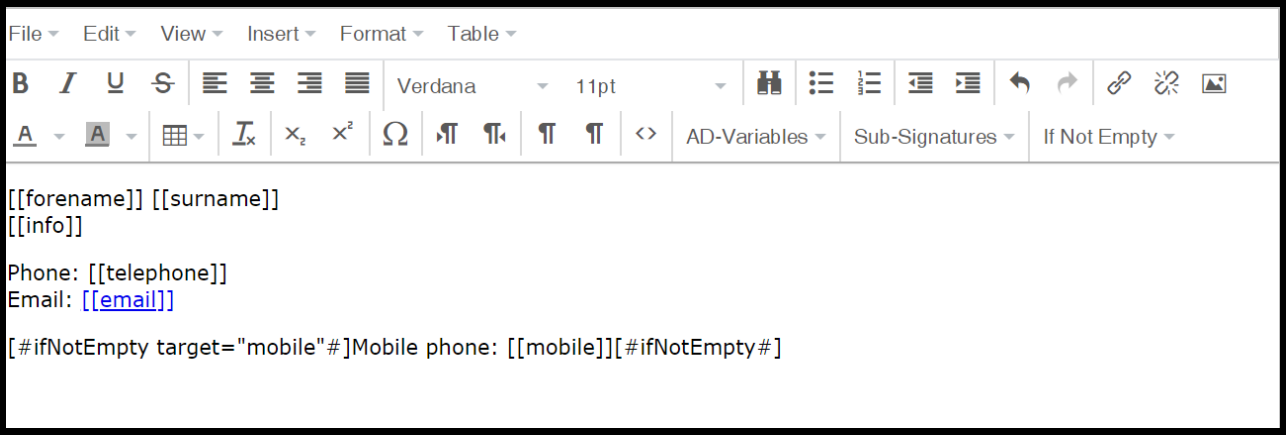


Figure 333: Signature in the editor

The following signature is displayed for users with a mobile phone number:

Figure 334: Signature mobile phone

The following signature is displayed for users without a mobile phone number:

Jane Doe
Product Management

Phone: +49 123456 789
Email: jadoe@domain.tld

Figure 335: Signature without mobile phone

Including Subsignatures

Use subsignatures to include previously created signatures in a signature.

Important:

Subsignatures can only be used in signatures. At least one signature must exist that you can include as a subsignature.

1. Create a new signature or edit an existing one.
2. Select the line in the editor, in which you want to insert the subsignature.
3. Click on **Sub-Signatures** and select the subsignature from the existing signatures.

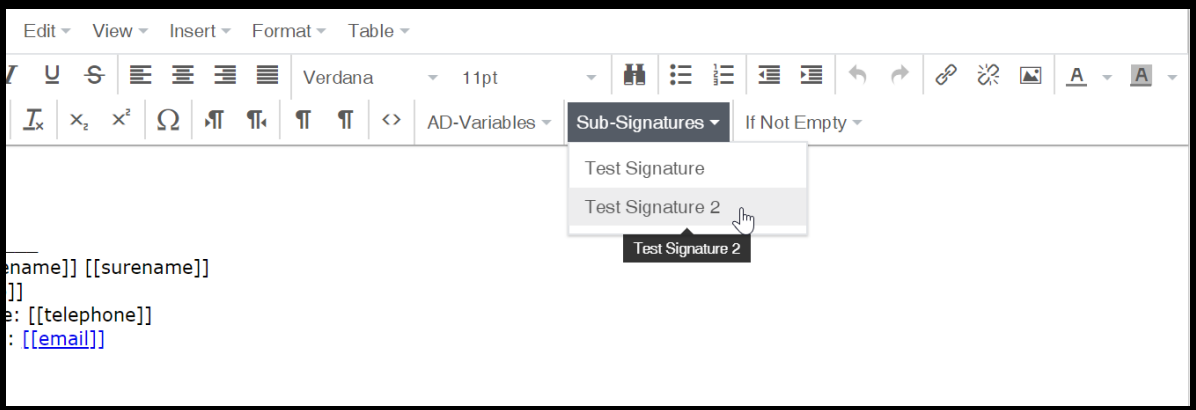


Figure 336: Select a subsignature

A placeholder is inserted for the subsignature.

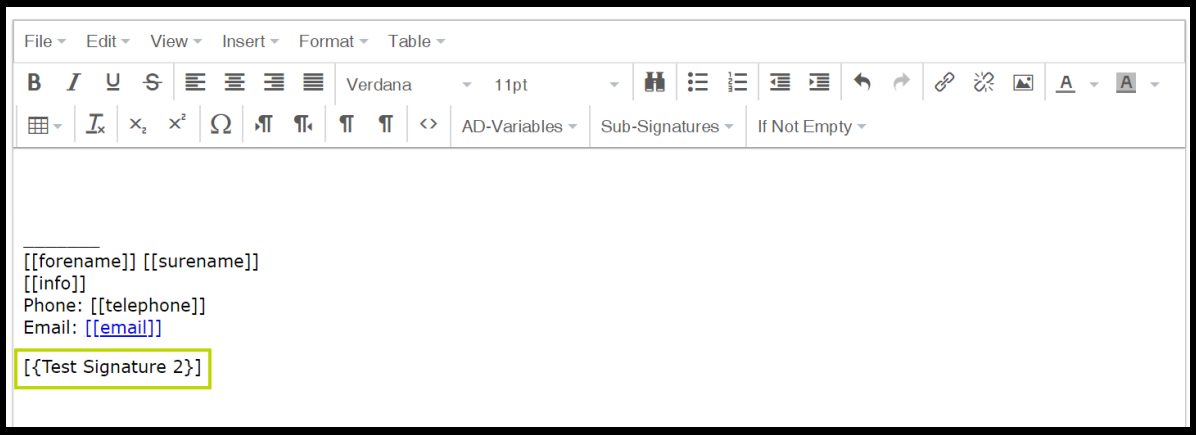


Figure 337: Subsignature placeholder

4. Click on **Save**.
5. **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) Set the toggle to **Active**.

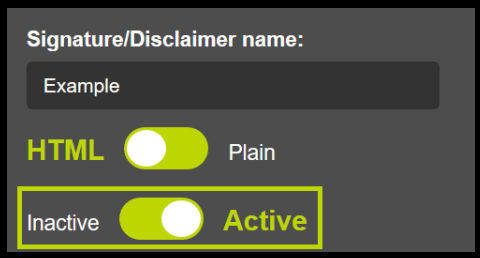


Figure 338: Activate subsignatures

➔ Activated and deactivated signatures are marked in the selection.

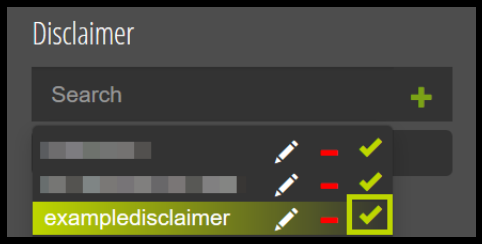


Figure 339: Active signature in the selection

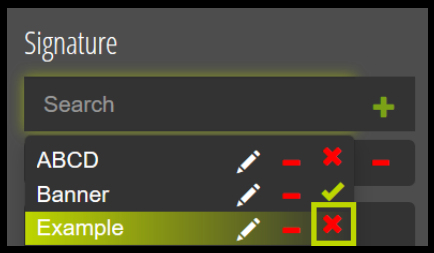


Figure 340: Inactive signature in the selection

Subsignatures have been included.

Inserting HTML Source Code

Use the editor to insert HTML source code.

1. In the WYSIWYG editor select the tab **Tools** and click on **Source Code**.

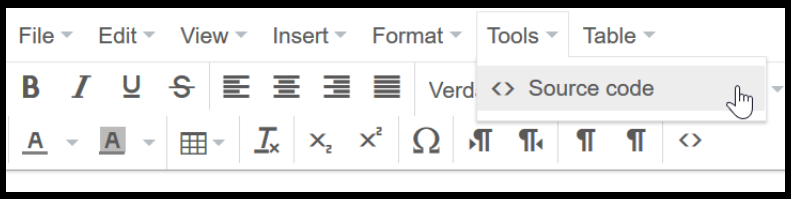


Figure 341: Open source code editor

A new window appears.

2. Enter the desired HTML source code and confirm with **OK**.

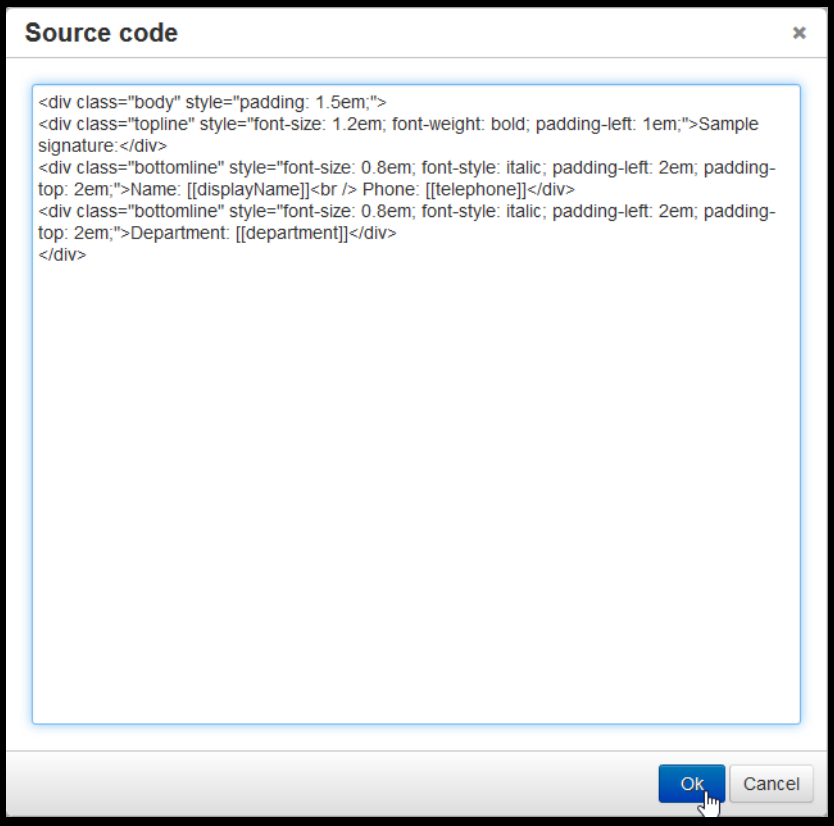


Figure 342: Insert source code

3. In the editor click on **Save** to save your changes.

You have inserted HTML source code to be used as a signature or a disclaimer.

Preview Signatures and Disclaimers

The preview shows a template for certain users of your Active Directory.

You can get a preview of the template you are creating or editing. Therefore, you can select any user in your Active Directory.

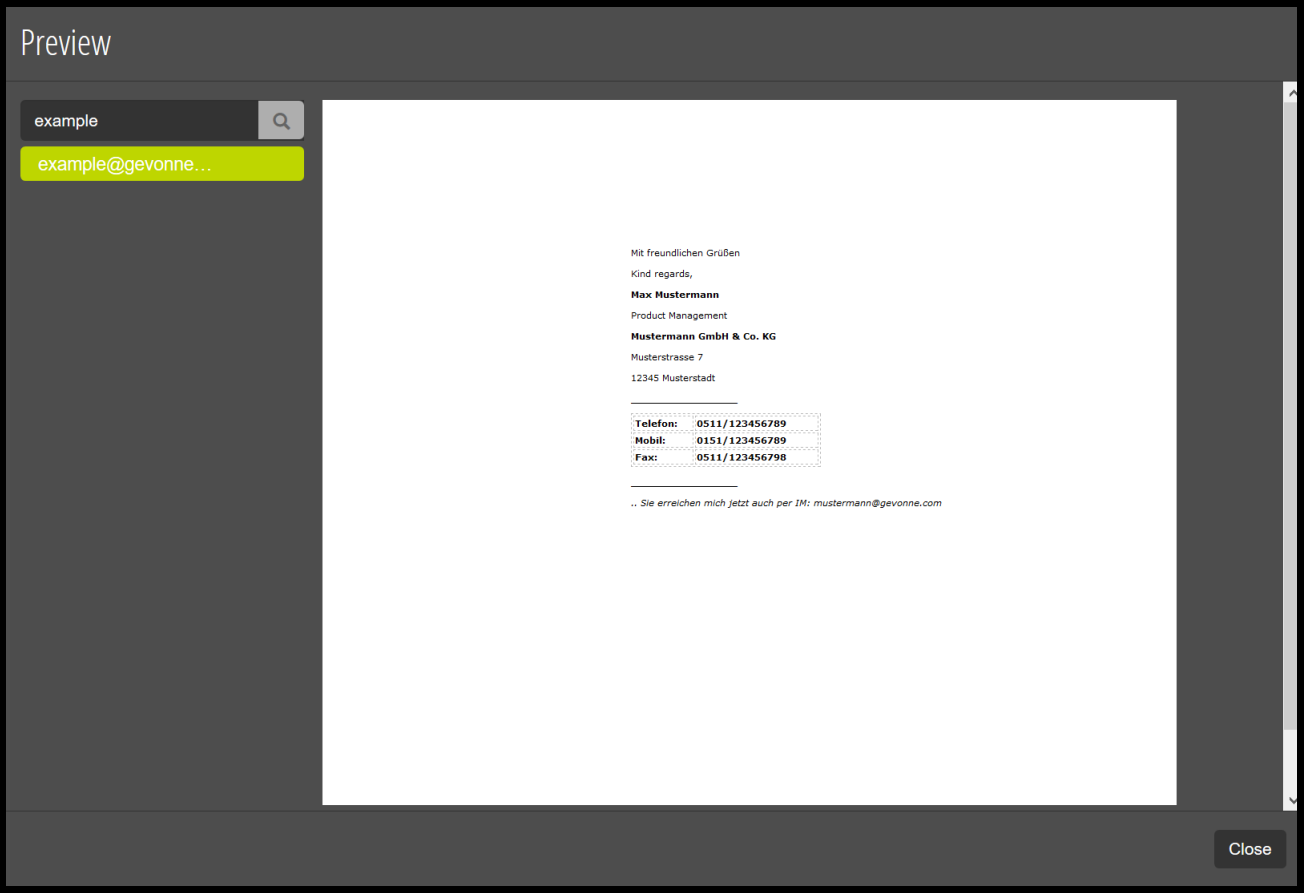


Figure 343: Preview your template

Embed Images in Signature & Disclaimer

The WYSIWYG editor allows you to add images to your signature or disclaimer.

After you have created your signature or disclaimer using the web interface (see Activating Signature & Disclaimer in the Web Interface on page 317) and/or via LDAP (see Activating LDAP for Signature & Disclaimer on page 64), you can Creating Signatures and Disclaimers on page 317 or Editing or Deleting Signature and Disclaimer Templates on page 321. Images can either be dragged and dropped directly into the WYSIWYG editor or embedded via URL.

Embedding Images Using a URL

1. When creating or editing a disclaimer or signature in the WYSIWYG editor, click the position where you intend to insert the image.
2. Within the editor navigate to **Insert#→Image**.

An input window with further parameters opens.

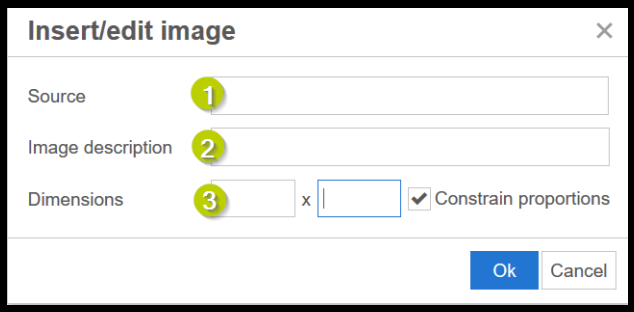


Figure 344: Input window for images

3. Under **Source** (1), enter the address of the image that is to be representative for your link. Search the internet for the desired image and copy the stored image location.

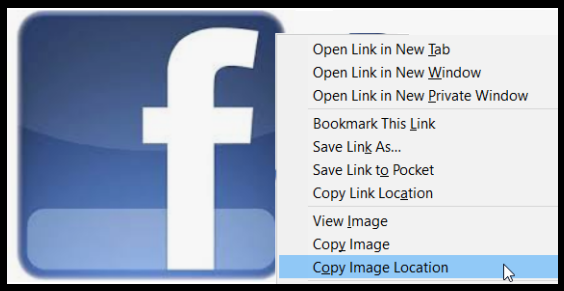


Figure 345: Copy the location of the representative image and paste under Source.

The location of the desired image is stored.

4. Alternatively, enter a description under **Image Description** (2).
5. If necessary, adjust the size of the image individually under **Dimensions** and save your input with **Ok**.

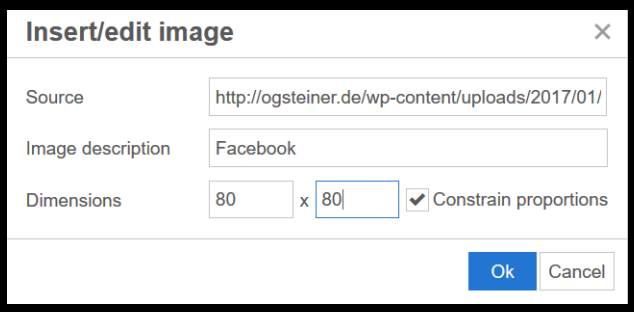


Figure 346: Resize the image

The parameters have been stored and the image is displayed in the editor.

6. Right-click on the image and select **Link** to enter a specific URL.

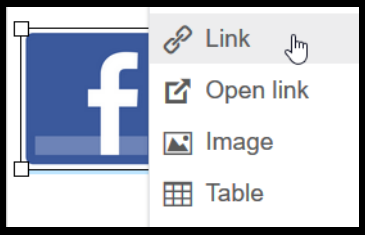


Figure 347: Link image

An input window with further parameters opens.

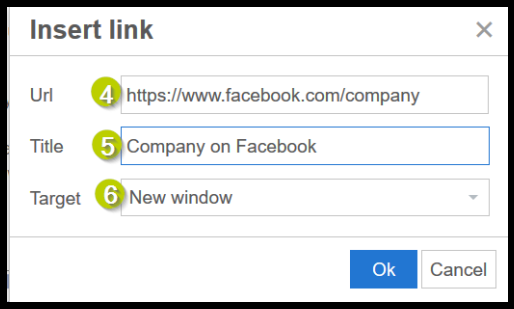


Figure 348: Enter URL

7. Enter the destination address of the desired website under **URL** (4).
8. Alternatively, enter a text under **Title** (5) which should be displayed over the image when the mouse hovers over it.
9. Under **Target** (6) select **New window** to open the linked website in a new tab to leave.
10. 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.

The image was embedded to your signature or disclaimer via an URL.

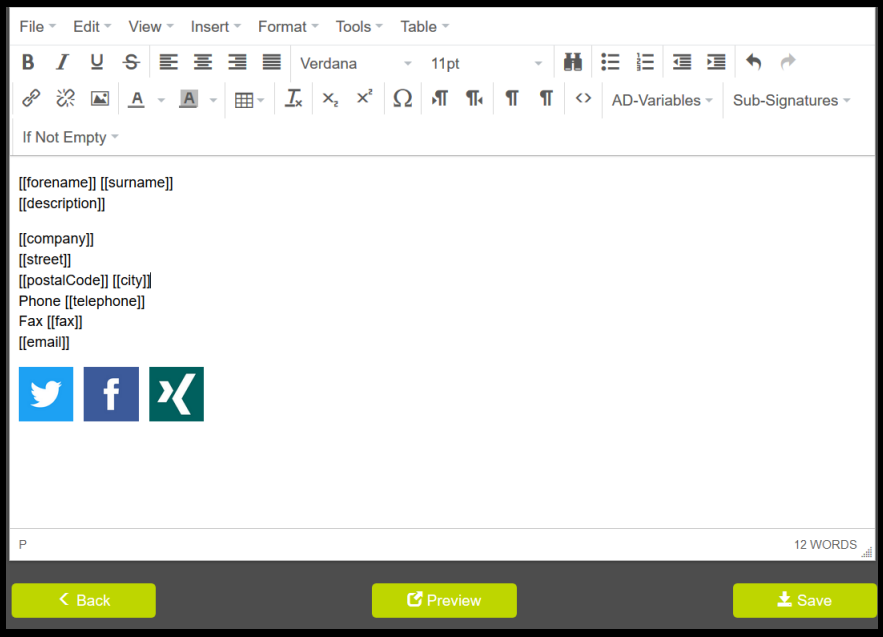


Figure 349: Assignment of AD-variables with linked images

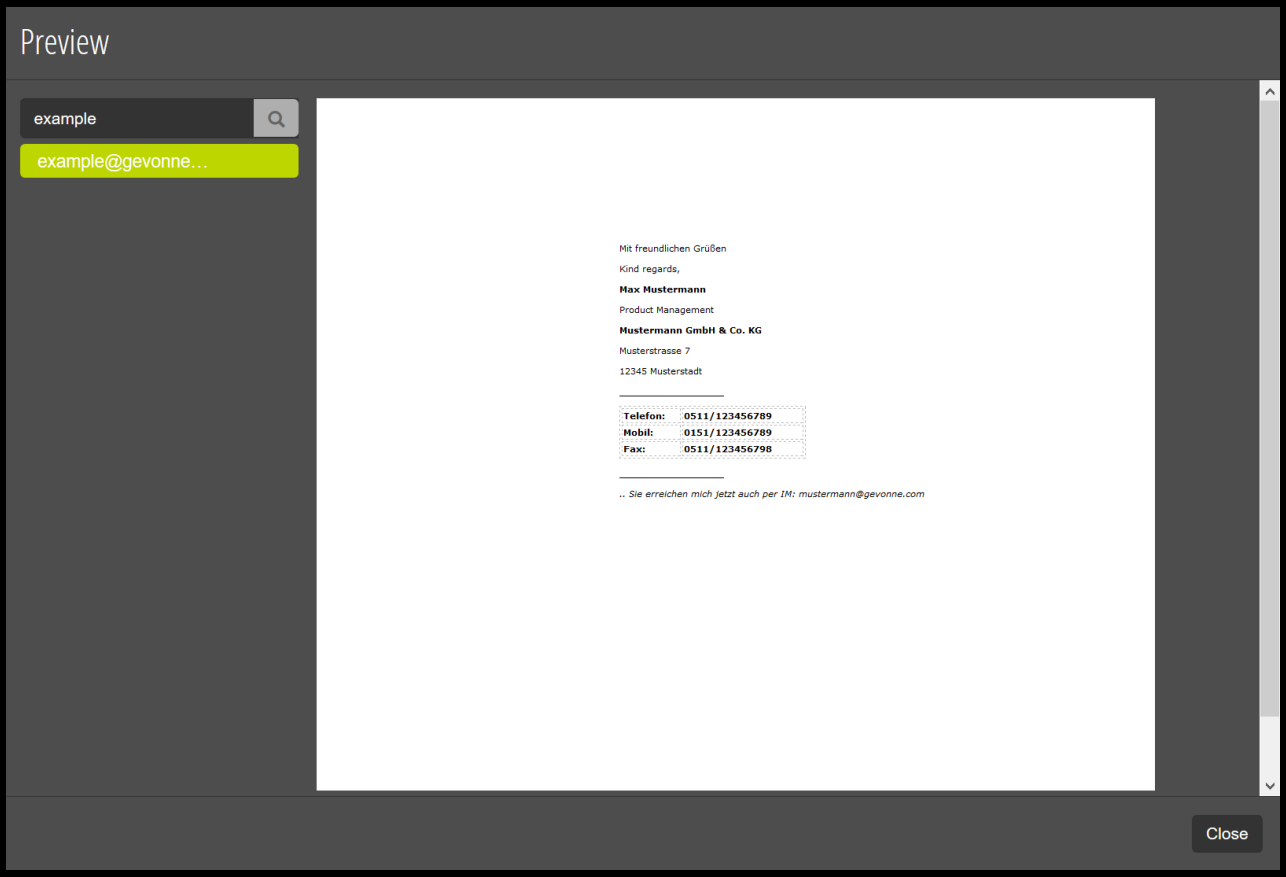


Figure 350: Preview of a signature with linked images

Inserting and Linking Images via Drag & Drop

1. When creating or editing a disclaimer or signature in the WYSIWYG editor, click the position where you intend to insert the image.
2. Drag the graphic to the desired position in your signature or disclaimer editor.
   The graphic was inserted at the desired position by drag & drop.
3. Right-click on the image and select **Link** to enter a specific URL.

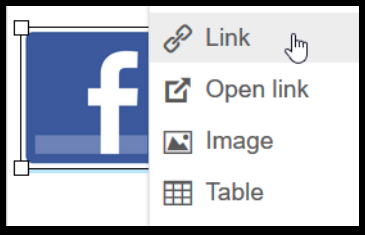


Figure 351: Link image

An input window with further parameters opens.

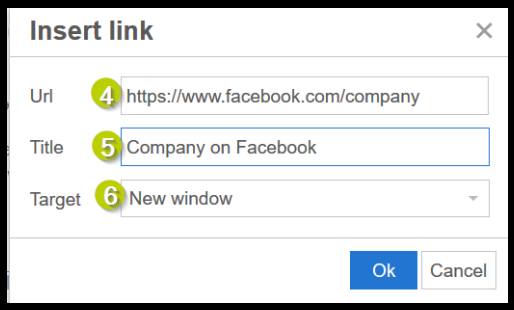


Figure 352: Enter URL

4. Enter the destination address of the desired website under **URL** (4).
5. Alternatively, enter a text under **Title** (5) which should be displayed over the image when the mouse hovers over it.
6. Under **Target** (6) select **New window** to open the linked website in a new tab to leave.
7. Click on **Ok** and then on **Save** to save all data.

   The image was linked.
8. Right-click on the added object and select **Image** to resize the image in the field **Dimensions** if necessary.
9. Click on **Ok** and then on **Save** to save all data.

> **Notice:**
>
> If necessary, repeat steps 1-9 if you want to insert several images.

You have added a graphic to your signature or disclaimer via drag & drop and linked it to a website.

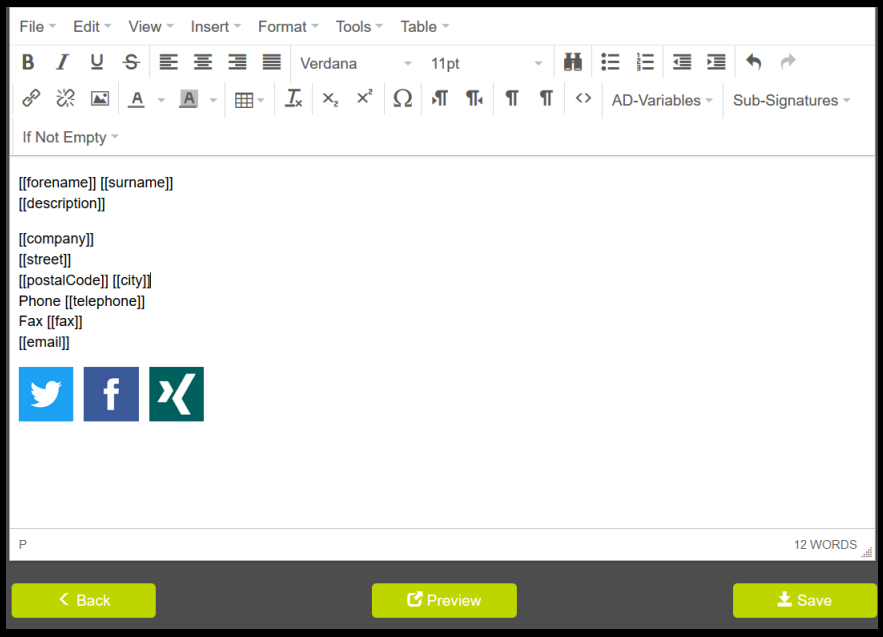


Figure 353: Assignment of AD-variables with linked images

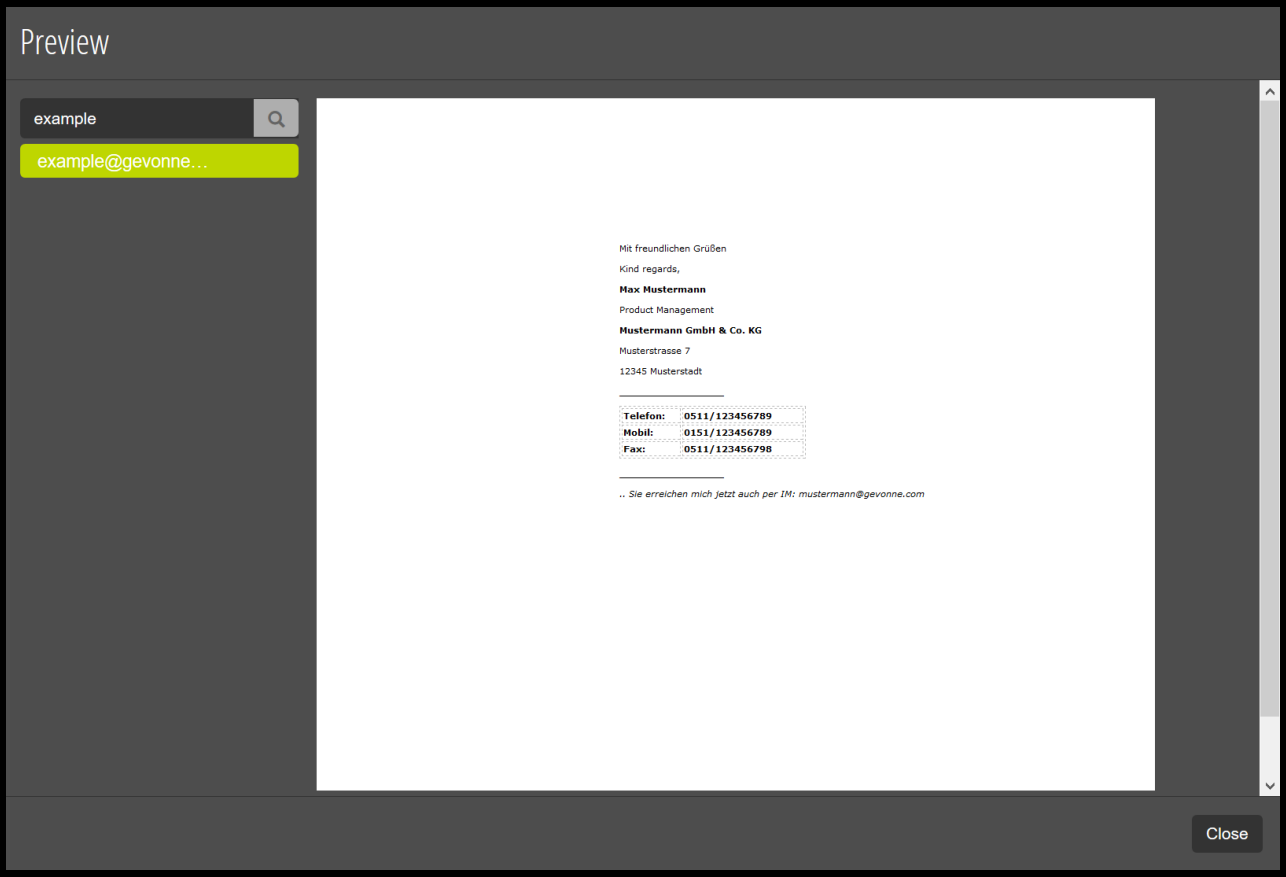


Figure 354: Preview of a signature with linked images

Data Synchronization via LDAP

Changes to the Active Directory cause a new synchronization.

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.

Notice:

If you perform a backup, the USNChangedNr is not increased but reset to an earlier value. The dataset is then also synchronized again.

Troubleshooting

When using **Signature & Disclaimer** errors may occur. In the following chapters the cause and the solution of frequent errors is explained.

Troubleshooting: Variables Are Not Referenced

Condition

You have inserted an AD variable or a subsignature and they are displayed incorrectly in the signature created.

Cause: AD Variable does not exist

The variable is not defined in the Active Directory.

Figure 355: 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.

Figure 356: Example for the integration of a non-existent signature

Remedy

Select the signature to be included again from the **Sub-Signatures** drop-down menu.

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.

Cause

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 & Disclaimer**.

Remedy for Mail (Apple) on MacOS

See Use 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 & Disclaimer** attaches the HTML signature.

Remedy for Thunderbird

- For single emails: Select **Write**#→**Options**#→**Delivery Format**#→**Rich Text (HTML) Only**.

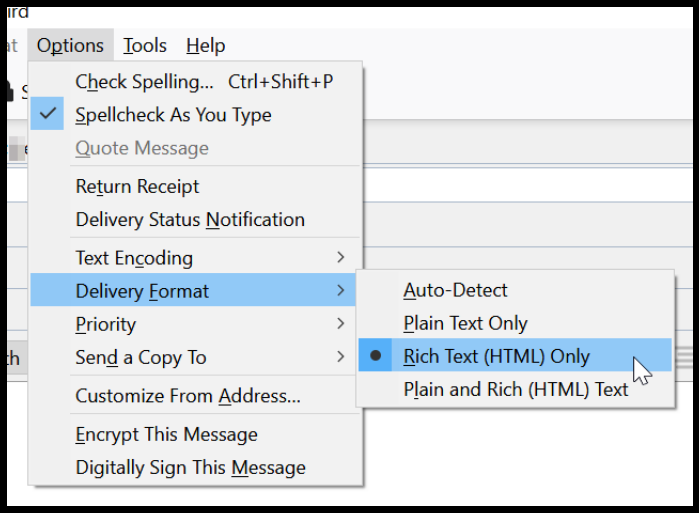


Figure 357: Options for a single email

- For all emails: Select **Write#→Tools#→Account Settings#→Composition & Addressing** and check the box **Compose messages in HTML format**.

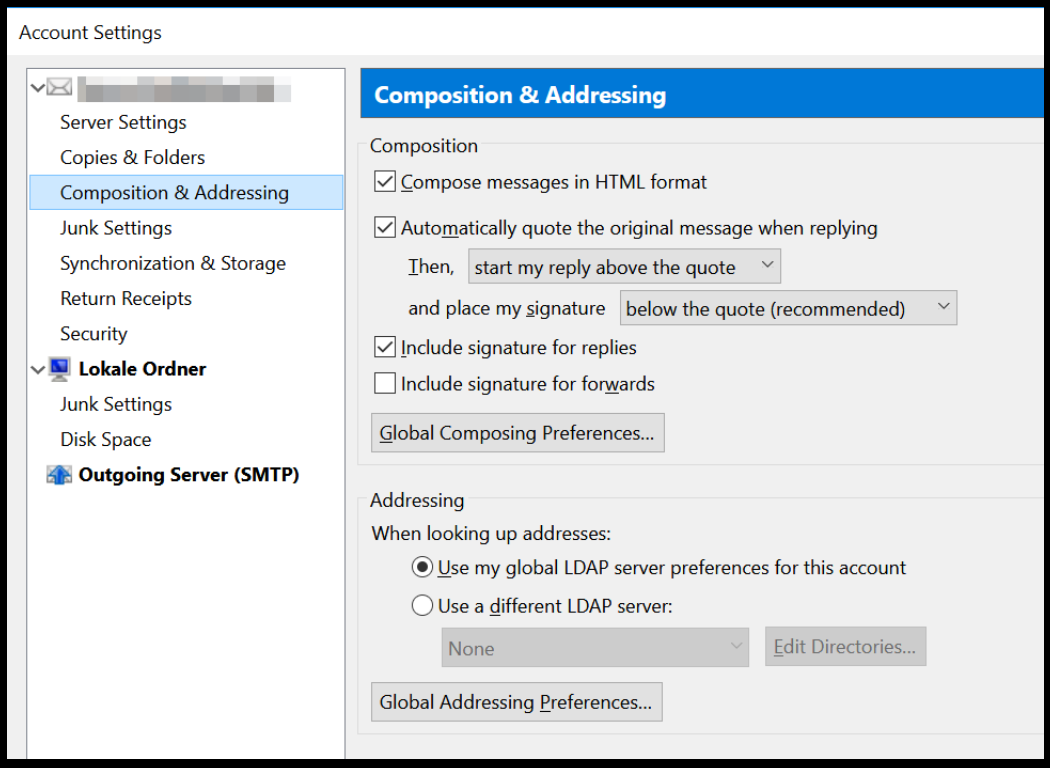


Figure 358: Settings for all emails

Archiving Audit Access Management

Archiving Audit Access Management

Archiving Audit Access Management

An audit access for authorized persons can be set up via the Archiving Audit Access Management.

With an audit access, authorized persons receive access to archived emails in certain mailboxes. The audit access is activated for a limited period of time. According to the two-man rule, two authorized auditors must be specified. The period of access granted and the audit-relevant archiving period can be defined individually. You can track audit activities with an audit log, when you have selected a domain in the scope selection.

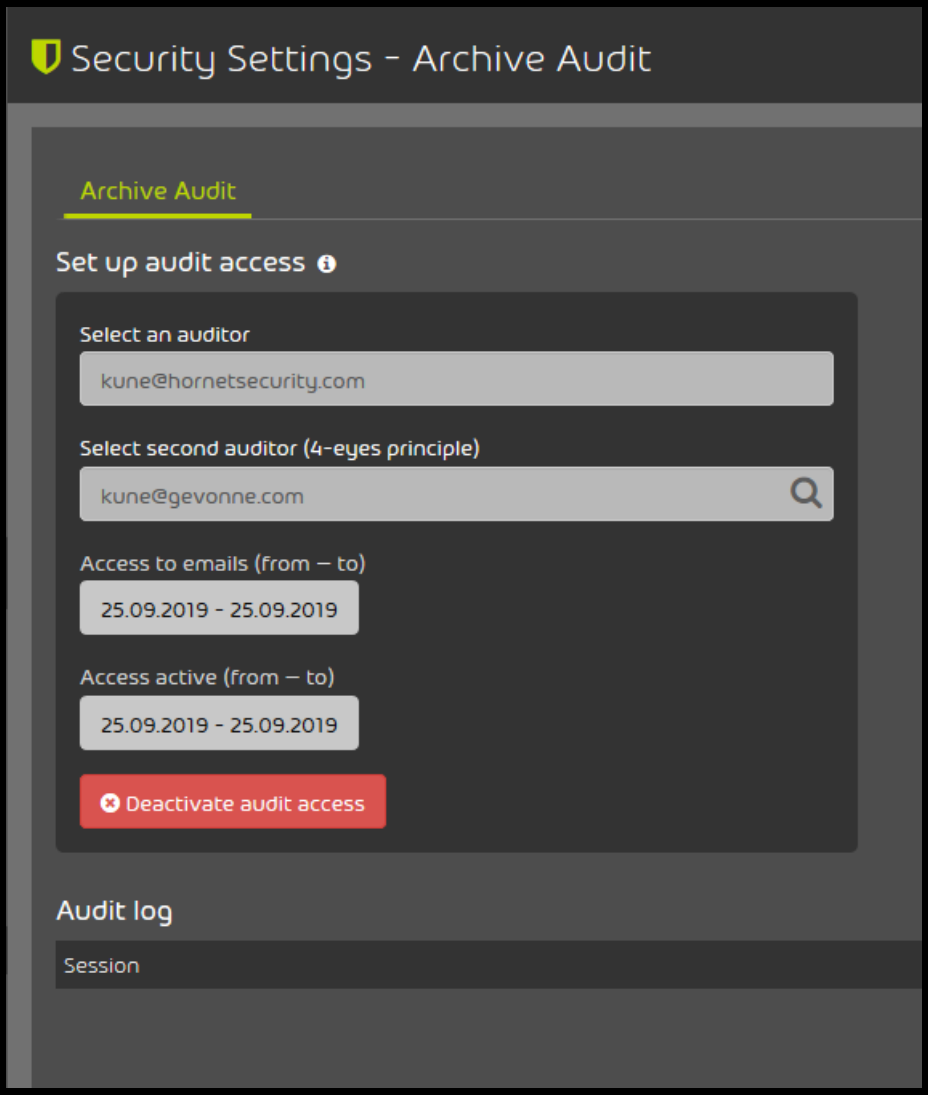


Figure 359: Setup of an audit access (domain selected)

Setting up and Activating Audit Accesses

Before you can use the Archiving Audit Access Management, it must be set up for the authorized persons.

1. Navigate to **Security Settings#→Archiving Audit Access Management**.
2. Enter the email address of the external auditor in the field **Select an auditor**.
3. Enter the email address of the internal auditor in the field **Select second auditor**.

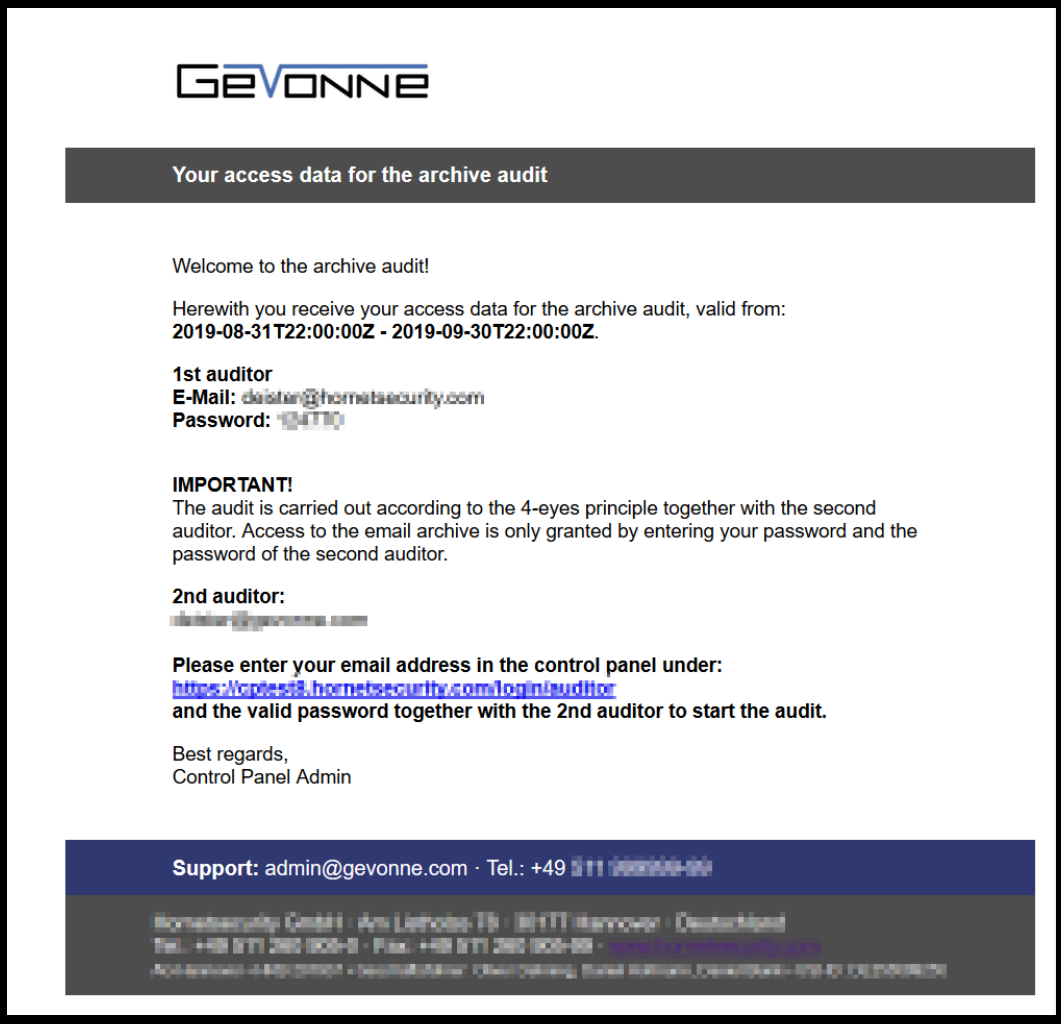
Notice: Together with the second auditor, a control function is performed according to the two-man rule.

4. Under **Access to emails (from - to)**, select the period for which archived emails are to be retrieved.
5. Under **Access active (from - to)**, select the period for which the access is to be activated.
6. Click **Activate audit access**.

The audit access has been set up and activated.

After the setup, both auditors receive an email with personalized login data as well as a login address for audit access.

Example:



GeVONNE

Your access data for the archive audit

Welcome to the archive audit!

Herewith you receive your access data for the archive audit, valid from:
2019-08-31T22:00:00Z - 2019-09-30T22:00:00Z.

1st auditor
E-Mail: [redacted]
Password: [redacted]

IMPORTANT!
The audit is carried out according to the 4-eyes principle together with the second auditor. Access to the email archive is only granted by entering your password and the password of the second auditor.

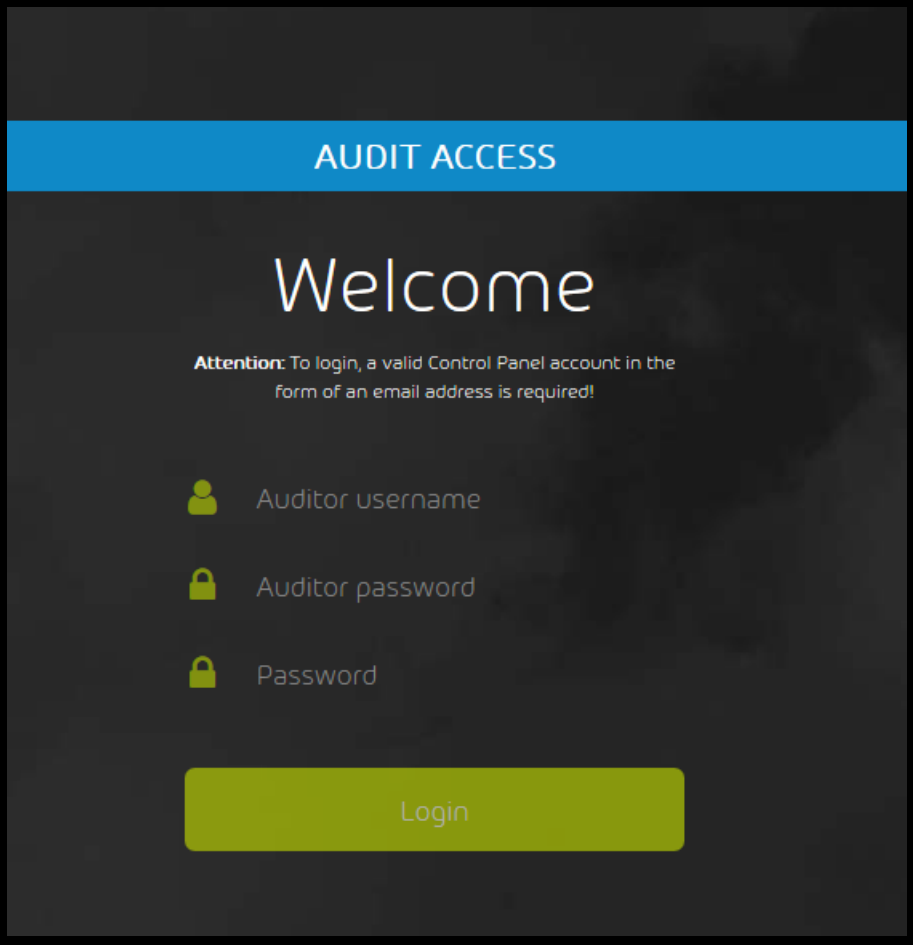
2nd auditor:
[redacted]

Please enter your email address in the control panel under:
https://cpdest8.hornetsecurity.com/login/auditor
and the valid password together with the 2nd auditor to start the audit.

Best regards,
Control Panel Admin

Support: admin@gevonne.com · Tel.: +49 [redacted]

[redacted]



Archiving

Important:

To use Archiving, you have to use Spam and Malware Protection (see Activating Spam and Malware Protection on page 275). Be aware that only external emails are archived at first. To also archive internal emails, you have to set up a forwarding to the archive.

In order to be archived, outgoing emails must be sent via the service Spam and Malware Protection of Hornetsecurity.

Internal emails can be archived in your email archive if a journaling mailbox is configured. For further instructions, please ask your provider, mail server provider or the Hornetsecurity support.

Setting up and Activating Archiving

1. Navigate to **Security Settings#→Archive**.
2. Select the domain to be archived under **Select**.
3. Insert the domain to be archived under **Add**.

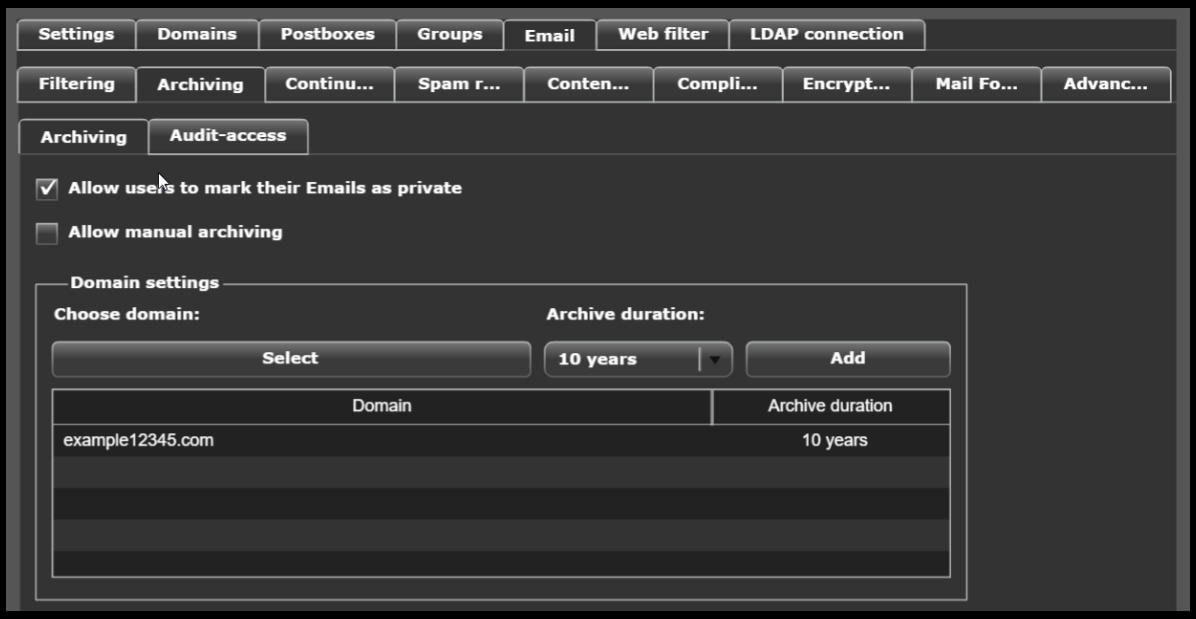


Figure 360: Navigation to archiving under Email

4. Confirm with **Apply** und then with **Save**.
   → Email archiving is activated.

Email archiving is set up.

Notice:

The archived emails are available for the set archiving period from the end of the year in which the respective archived email was sent or received. The archiving period for emails is the number of years that was set as the "archive duration" in the Control Panel for the domain or, alternatively, for the user. After the deadline, all emails are deleted from the archive.

Adding Exceptions

Groups / users that should be excluded for data protection reasons can be added to an exception list.

1. Select the tab **Email** → **Archiving**.
2. Select the domain concerned in the field **Exceptions** → **Select** and confirm with **Apply**.

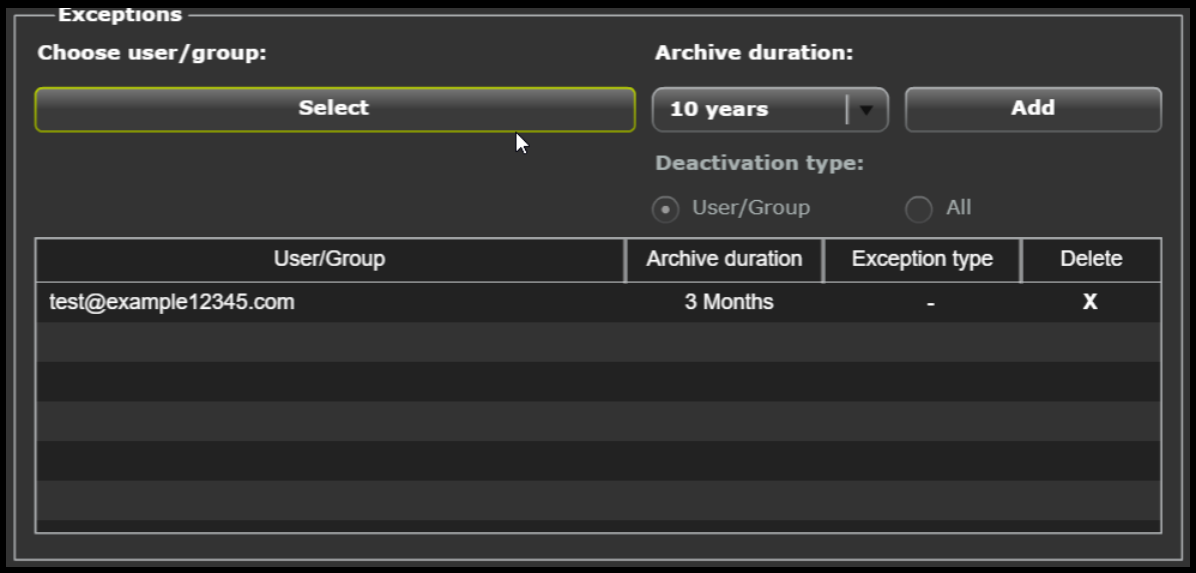


Figure 361: Add exceptions

Selected domain is displayed in the window **Select**.

3. Select the desired archiving duration from the drop-down menu **Archive duration**.
4. Click **Add** and comfirm the changes with **OK**.

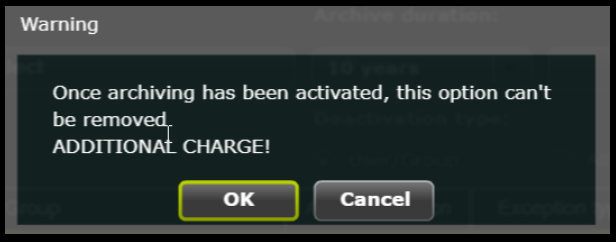


Figure 362: Confirm changes

5. Save your changes with **Save**.

Exceptions are added.

Deactivating Archiving

1. Select the tab **Email** → **Archiving**.
2. Select the domain concerned in the field **Exceptions** → **Select**.
3. Select **Deactivated** from the entry **Archive duration**.
4. Select the type of deactivation:
   a) **User/Group:** Emails for the user/group are not archived in the user's/group's own archive.
   b) **All:** All email traffic with the group/user is not archived.

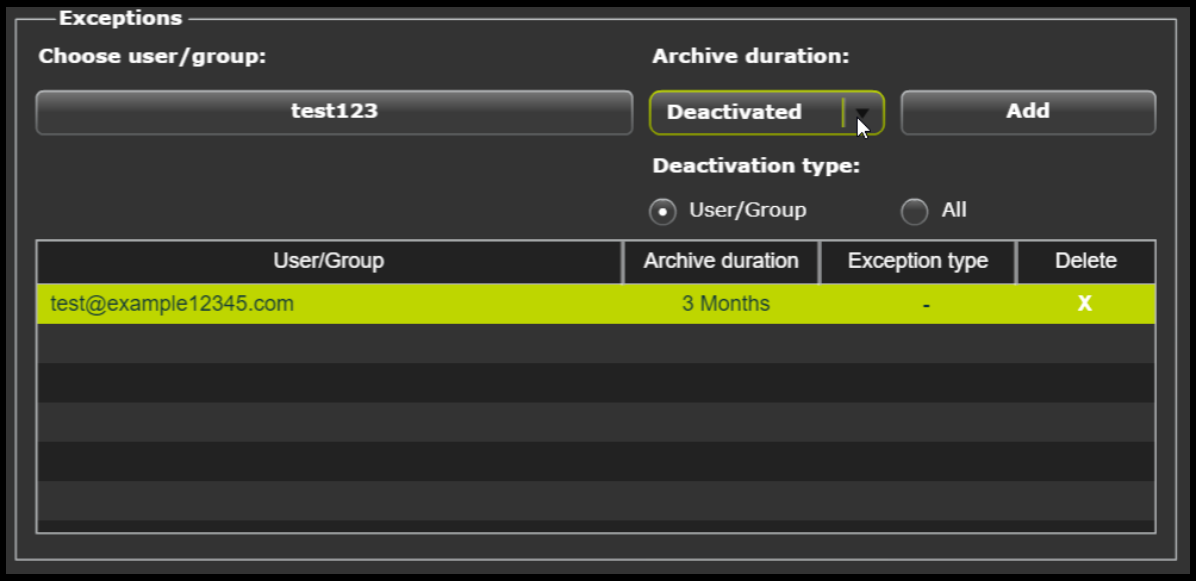


Figure 363: Deactivate Archiving

5. Confirm your changes with **Save**.

Email Archiving is deactivated.

Continuity Service

The Continuity Service is an additional email service that guarantees continuous email functionality in the event of an email service failure.

With the Continuity Service enabled, users can continue to receive and send email if their email server fails.

Attention:

This service is subject to a charge!

If the Continuity Service is set up for a domain or an individual user, automatic activation is set by default in the event of a mail server failure. In addition, the user can recognize in the email search which emails were delivered by the individual user via the Continuity Service.

Domains with the Continuity Service enabled can see their emails from the last three months in the archive.

Important:

The function "Send outgoing emails to own mail server during server failure" is deprecated, will be removed with future releases and should not be used.

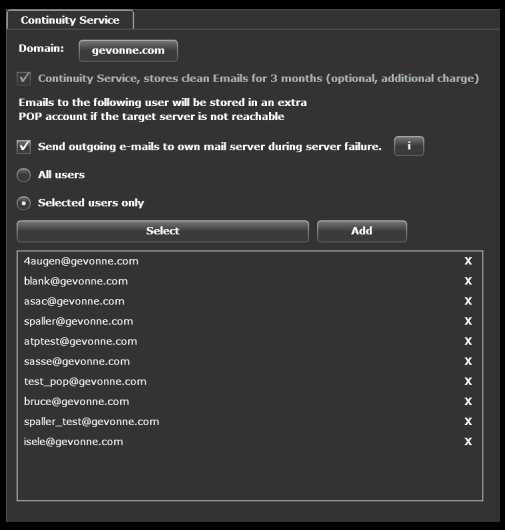


Figure 364: Continuity Service

Encryption

This guide explains how to configure and use the encryption service. Starting from the basic configuration, the encryption methods that can be used are explained and different rules are created using examples. In addition, the options for ordering and managing certificates are presented to you. The use of the Websafe for encrypted communication as well as the use of keywords within the email subject are also part of this manual.

Activating Email Encryption

Attention:

The activation of Email Encryption will increase costs according to the price list.

1. Navigate to **Security Settings#→Email Encryption**.
2. Mark the checkbox **Activate policy**.

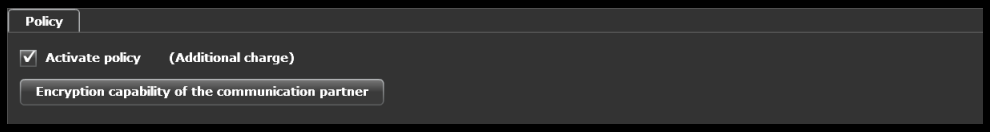


Figure 365: Activating Email Encryption

You have activated Email Encryption.

Notice:

Only emails which are sent from one of the relay IP addresses specified under Spam and Malware Encryption can be signed and encrypted with Email Encryption (see Environment Settings on page 276).

Checking the Encryption Capability

Check the encryption capability of communication partners before you proceed making further configurations on the Email Encryption.

1. Click on **Encryption capability of the communication partner** in the tab **Encryption**.
2. Enter the email addresses to be checked.

Figure 366: Enter communication partners

3. Click on **Check** to check the encryption capability of the entered email addresses.

Encryption Capability is displayed.

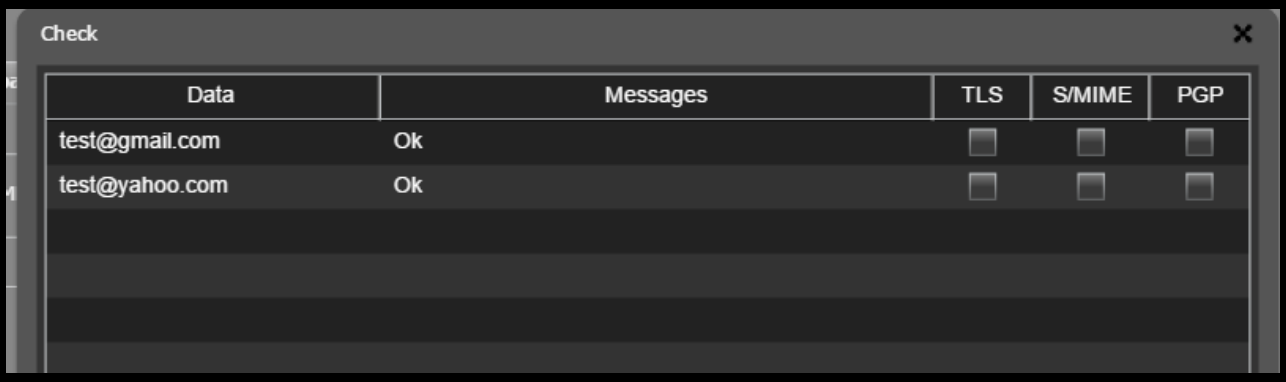


Figure 367: Encryption Capability

Encryption Methods

There are different encryption methods that can be used.

Activate the checkboxes to enable the encryption methods.

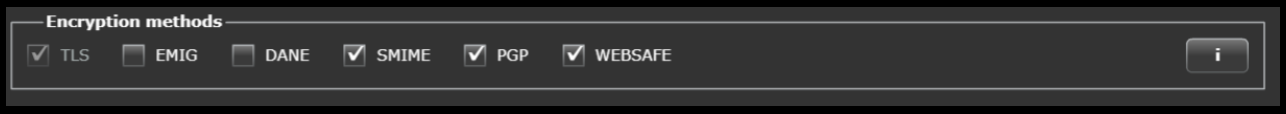


Figure 368: Activate encryption methods

Explanation of the encryption methods:

- **TLS**: Encrypts the email between the outgoing and incoming server. The checkbox is always activated as this encryption method is used in every communication.
- **EmiG**: Email transmission according to the EmiG (Email made in Germany) standard is a special form of TLS encryption with special requirements for the TÜV-certified communication partners, their server security and the certificates used for encryption. The procedure corresponds to a particularly secure TLS encryption in a closed network of certified email providers with increased security guidelines. A separate configuration in the Control Panel is not necessary.
- **DANE**: Is not yet supported but is currently in preparation for rollout. If you are interested, contact the support for a quick implementation.
- **S/MIME**: Is a standard for encrypting and signing MIME emails, using a hybrid encryption procedure. The certificate authority (CA) assures the validity of the email address and of the name of the sender.

- **WEBSAFE**: If the checkbox is activated, a rule for the exact use must still be specified. See Websafe on page 363 for more information.

Notice:

After the activation, you can use **PGP, S/MIME** and **Websafe** in order to define encryption policies. However, you should define explicitly who will communicate with whom with end-to-end encryption.

TLS and **EmiG** are used automatically if the communication partner supports these encryption methods.

Sequence of Encryption Methods

If you select various encryption methods, they are processed in a certain sequence.

S/MIME → PGP → EmiG → (DANE) → TLS → Websafe

Additionally, you can combine the different encryption methods. (see Combination of Encryption Methods on page 359

Subject Tagging for Encryption

For a simple handling of encrypted emails, tag them in the email subject. The tag content can be chosen freely.

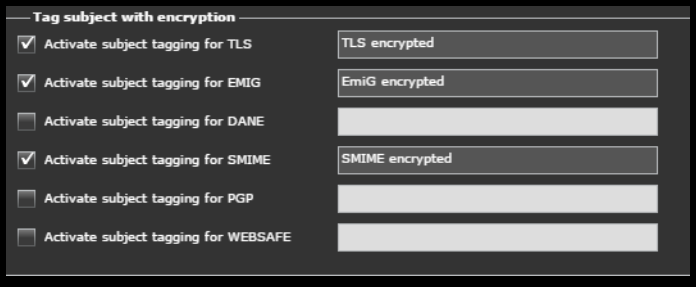


Figure 369: Subject tagging

Setting Deviating Encryption Policies

On the basis of the previously selected encryption methods, you can create rules for the encryption of specific emails.

Notice:

You can change the rule type for outgoing emails. The types **Advanced**, **Email Header** and **Email Body** are available. Furthermore, you can use regular expressions in the definition of rules. For more information about regular expressions and how to use them, see the Compliance Filter guide

1. Click on **Add** in the **Policy** section to create a new policy.
2. Select the direction: **Incoming** or **Outgoing**.
3. Enter the sender and/or receiver. You can enter domains, groups of users or individual email addresses.
4. Select the desired action. You can allow unencrypted emails (**Allow unencrypted**) or encrypt them always (**Encrypt always**). If you select the action **Encrypt always**, you must specify the encryption method. You can select **TLS** and **DANE** for incoming emails. You can use all previously selected encryption methods for outgoing emails.

The figure below shows a policy defined for incoming emails of the domain domain.com. All emails which are sent to @domain.com encrypted with TLS are rejected.

Notice:

All encryption policies with the direction "Incoming" refer to emails which are sent from an external server to your server.

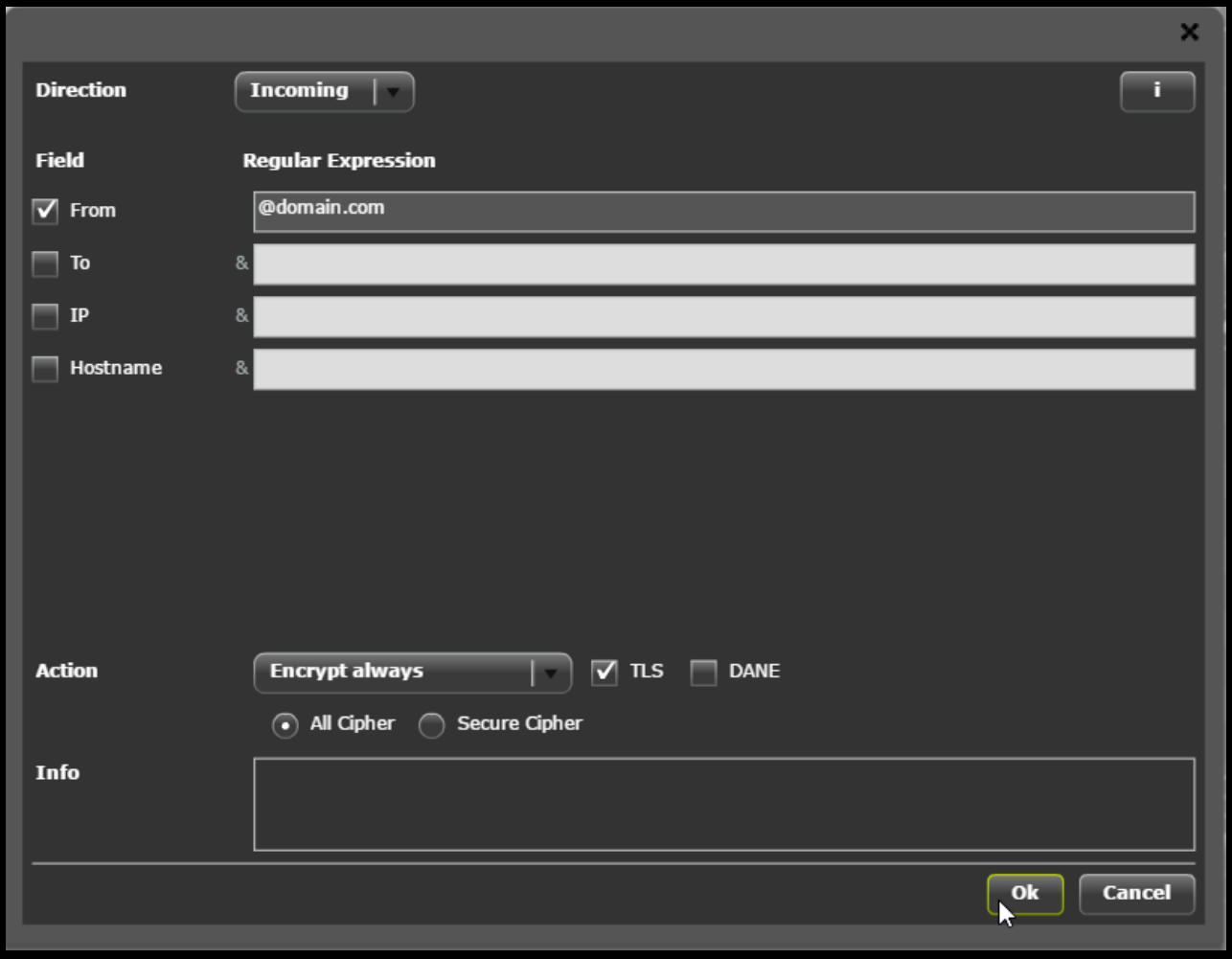


Figure 370: Create encryption policy for incoming emails

The figure below shows a policy defined for emails from secret@mycompany.com. The outgoing emails are sent TLS-encrypted and as a fallback Websafe is activated. Thus, all outgoing e-mails to this domain are sent encrypted.

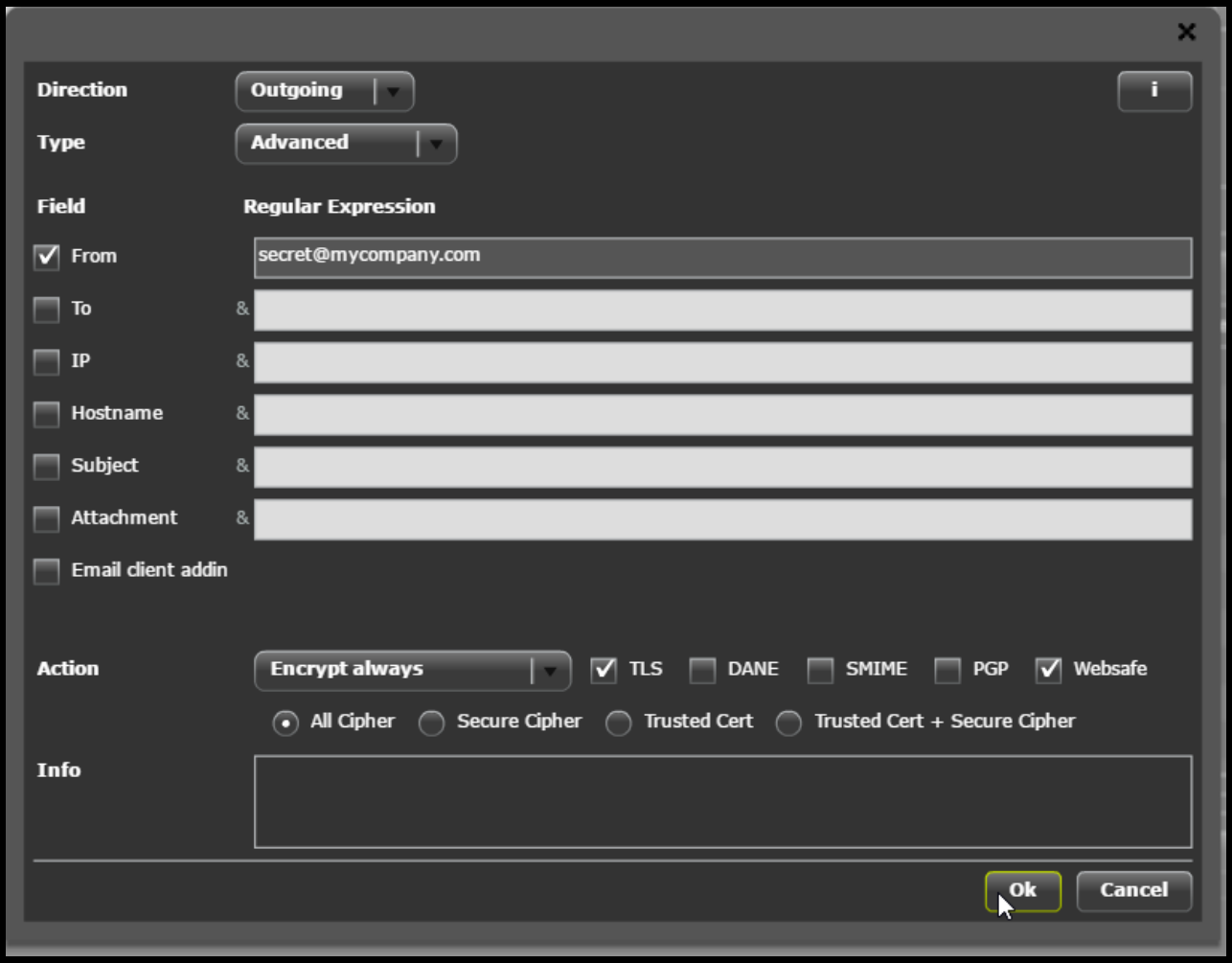


Figure 371: Create encryption policy for outgoing emails

The figure below shows a policy defined to search the email header of outgoing emails for the phrase "secret product name". If this phrase is found, the email is transmitted encrypted with TLS. If the communication partner cannot use TLS, the email will be transmitted to the Websafe This makes unencrypted transmission impossible.

Notice:

The expression is found even if it is surrounded by text. Therefore, "ABCsecret product nameDEF" will match as well.

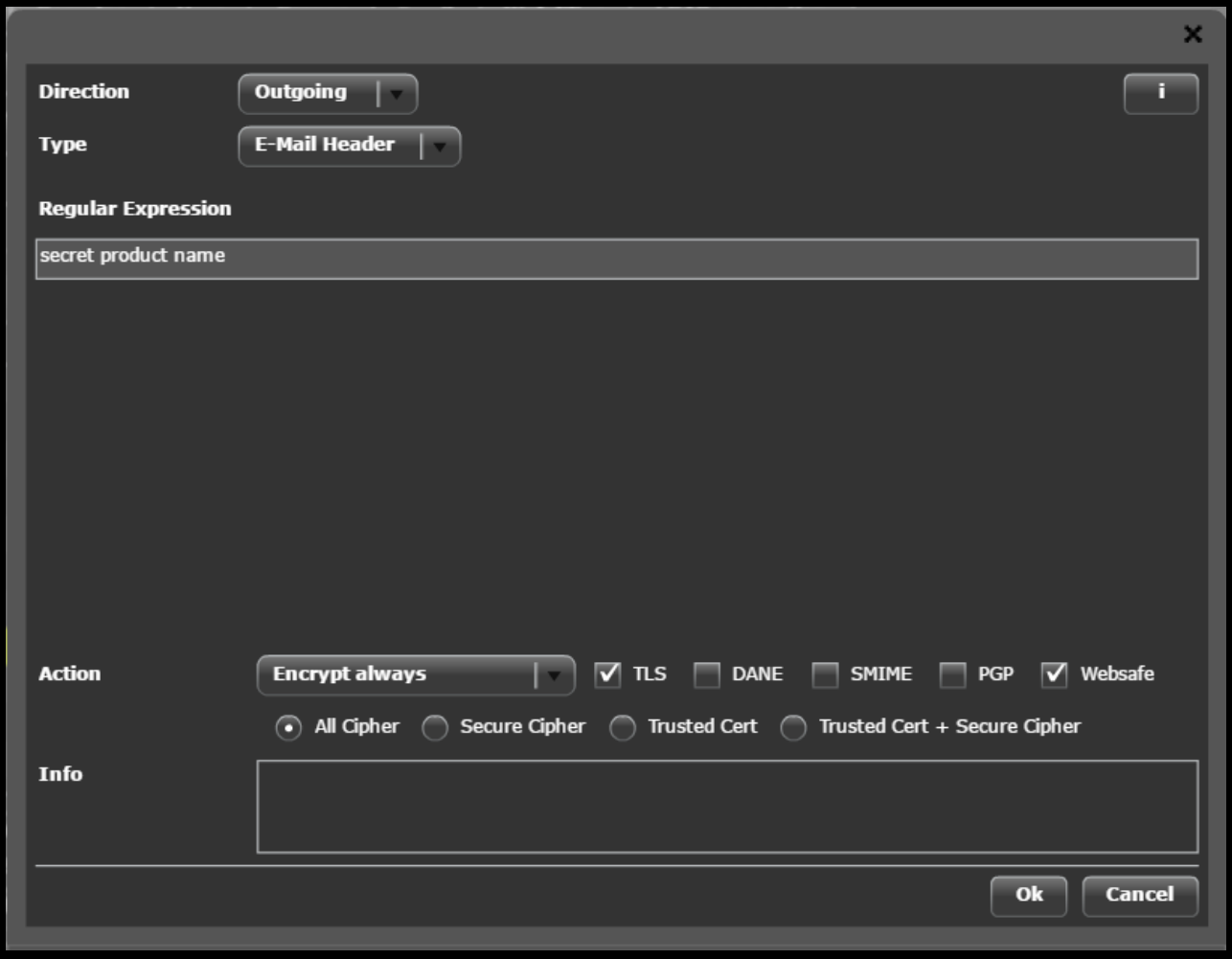


Figure 372: Encryption Policy for the email header or body of outgoing emails

All rules are collected in a list and processed from top to down. If you want to arrange the rules in a specific order, select a rule and click on the green arrows as shown in the figure below.

Notice:

If a policy matches, the execution stops and no other policy is applied.

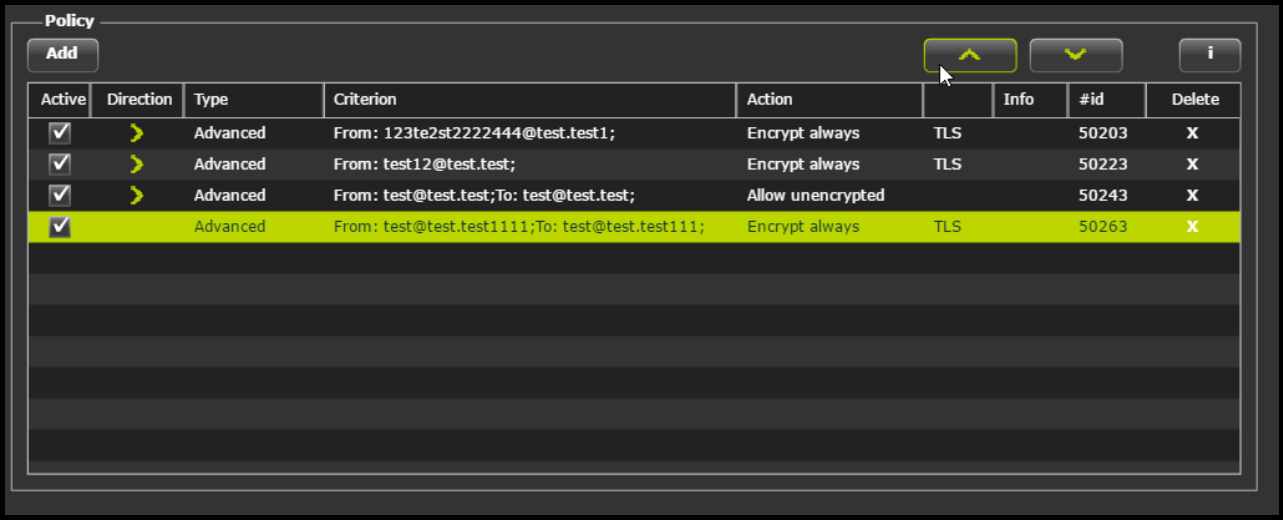


Figure 373: Policy order

Combination of Encryption Methods

It is possible to combine the different encryption methods. The following table provides the combination possibilities. An x indicates that the encryption methods are compatible with each other.

Table 22: Encryption combinations

Encryption	TLS	EmiG	S/MIME	PGP	DANE	WEBSAFE
TLS	-	-	x	x	x	-
EmiG	-	-	x	x	x	-
S/MIME	x	x	-	-	-	-
PGP	x	x	-	-	-	-
DANE	x	x	-	-	-	-
WEBSAFE	-	-	-	-	-	-

In addition, you can always activate the Websafe to have a fallback, if the communication partner does not support any other encryption method.

Example of combination of encryption methods:

The figure below shows a policy defined for outgoing emails from mydomain.com to communicationpartner.com. The action selected is "Encrypt always" with the encryption methods TLS and S/MIME. After the policy is applied, emails are sent encrypted, provided that the communication partner supports the encryption methods.

If your communication partner does not support any of the selected encryption methods, you can secure the encryption of your messages with the Websafe. (See:Websafe on page 363)

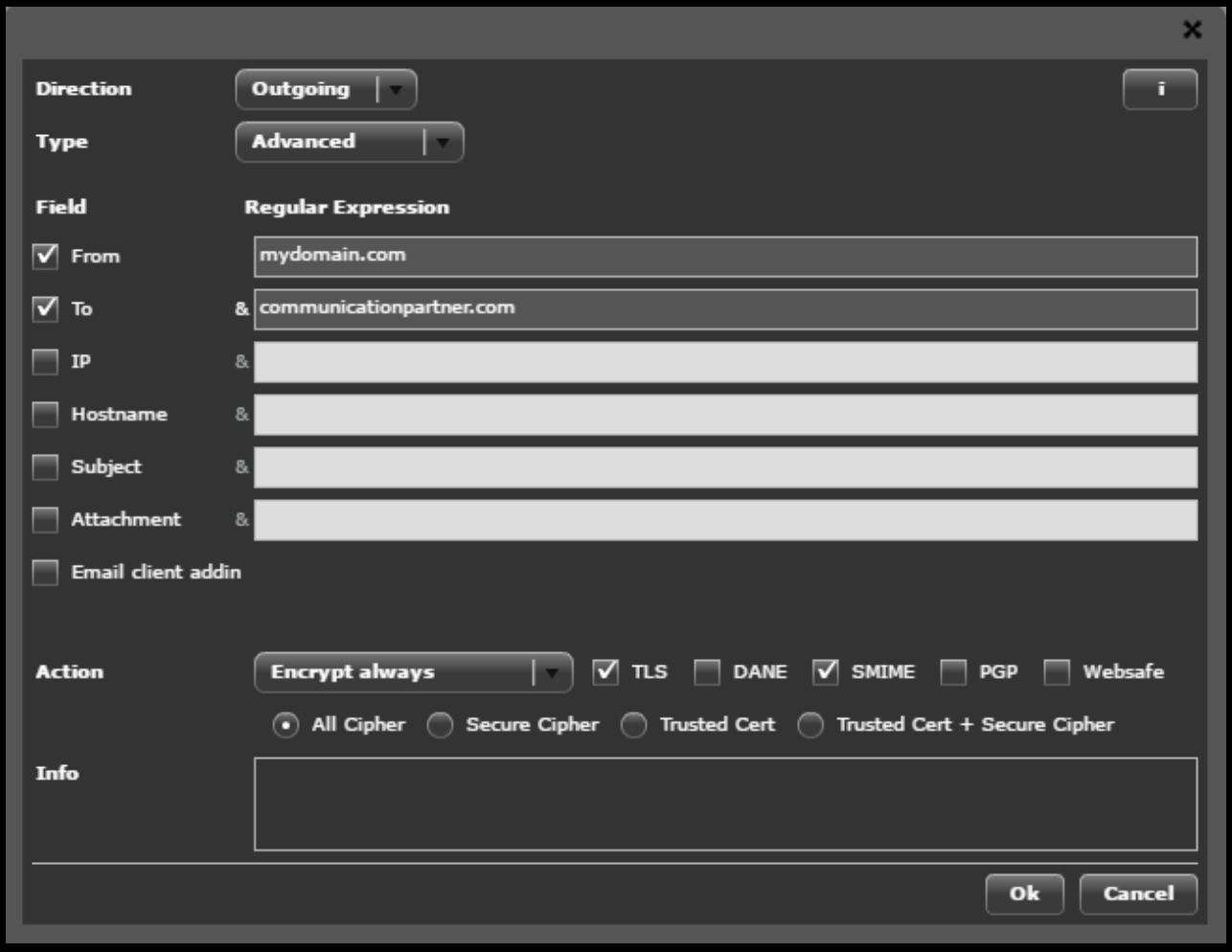


Figure 374: Combination of TLS and S/MIME

If you select all available encryption methods for a policy, the affected emails will be encrypted according to the sequence described in Sequence of Encryption Methods on page 354. All possible combinations are applied automatically.

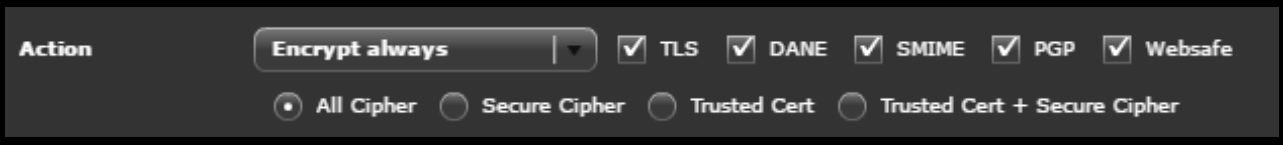


Figure 375: Selection of all encryption methods

Certificates

The administration of certificates is located under **Certificate**. Here S/MIME certificates for users of the selected domain are ordered and managed.

Ordering Certificates

1. Select the tab **Certificate**.
2. Select a user from the list.

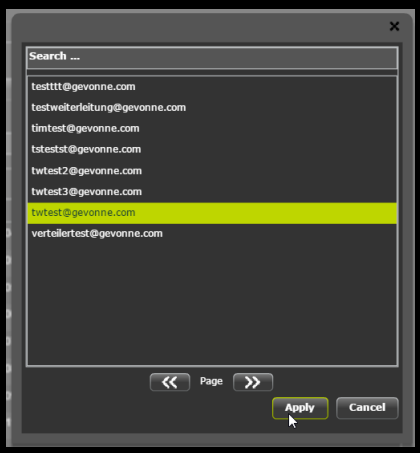


Figure 376: User selection for certificates

3. Enter the first and last name of the user

> **Important:**
>
> Be sure to enter the correct information before ordering the certificate. It is only valid as a signature if the entered name is valid.

4. Click on **Order** to complete.

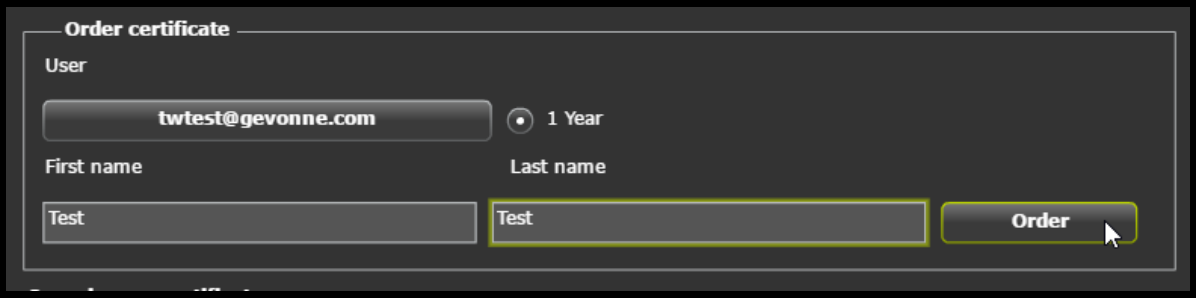


Figure 377: Order a certificate

Certificate is ordered.

Certificate Settings

In the certificate overview it can be defined for each certificate if it is used for the digital signature and/or for encryption. By default, signing and encrypting is enabled.

Furthermore, you can activate a subscription for the certificate. Certificates with an active subscription will automatically be renewed 29 days before expiration. The subscription is activated by default.

Notice:

If you do not want a subscription, deactivate it at least 30 days before renewal.

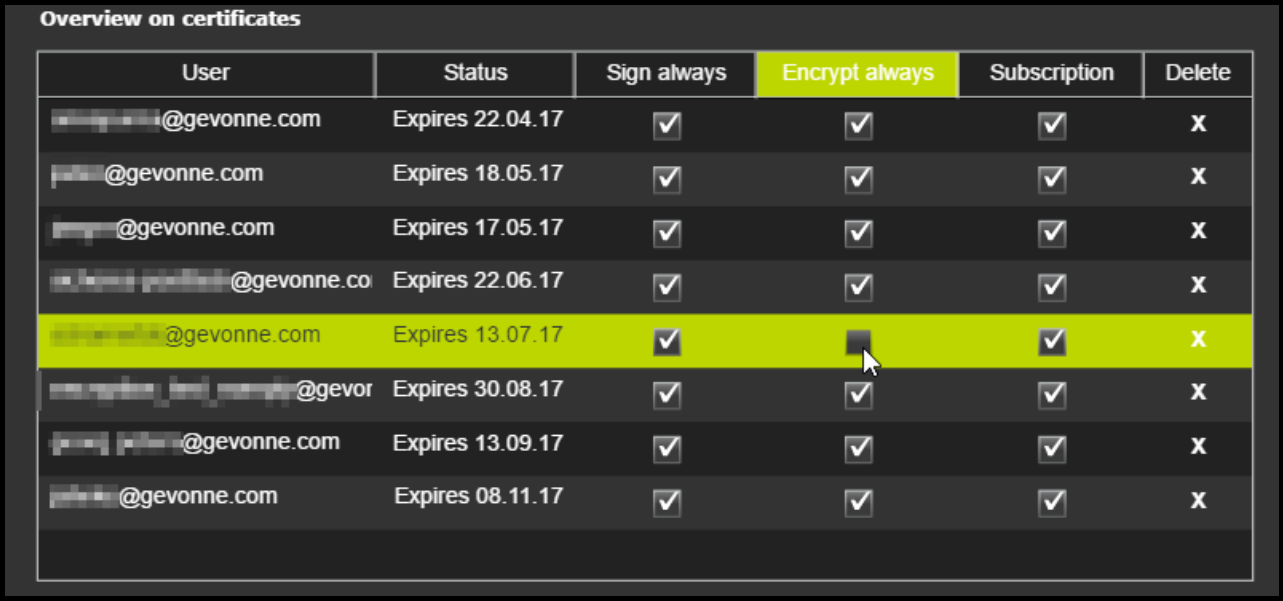


Figure 378: Certificate overview and options

Websafe

The Hornetsecurity Websafe is a method to encrypt the email communication with partners using no encryption technologies. The outgoing emails are sent to the Websafe and saved. After that, the communication partner receives an email with login credentials, but will need an additional PIN to unlock the personal Websafe. The email sender provides the PIN on a separate communication channel (phone, text message, fax). With the PIN and the login credentials, the user can access his personal Websafe.

Notice:

A Websafe account is automatically created and can be used for additional Websafe communication.

As soon as the communication partner opens a new email in the Websafe, the sender receives a confirmation message that the email has been read.

Messages remain stored in the Websafe for 12 months and are then automatically deleted.

Before configuring the Websafe, you must activate it in the encryption methods (see Encryption Methods on page 353).

Setting up Websafe

1. Click on **Add** in the tab **Encryption**.
2. Select **Outgoing** as direction.
3. Activate the checkbox **To** and insert the receiver into the field.
4. Select **Encrypt always** as action and activate the checkbox Websafe.
5. Save the entries with **Save**.

Websafe is set up. If no other encryption method can be used for the email communication, Websafe will be used.

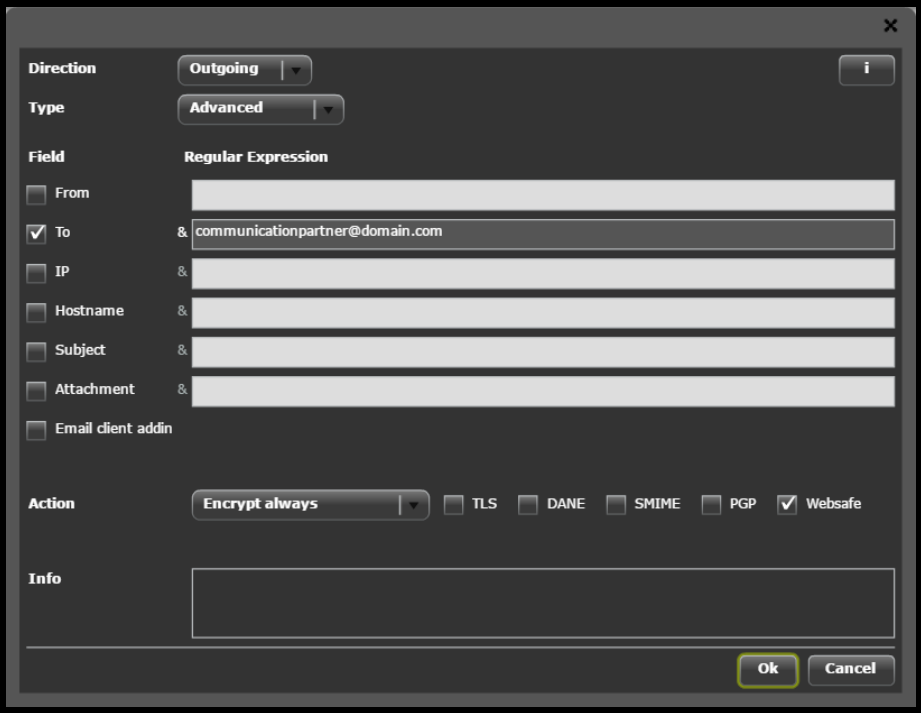


Figure 379: Activate websafe for a specific communication partner

Encrypting Emails with Websafe as Fallback

It is possible to use Websafe to always send encrypted emails even if no other encryption method is applied.

1. Click on **Add** in the tab **Encryption**.
2. Select Outgoing as direction.
3. Check the boxes **From** and **To**.

4. Insert **.*** in both fields.
5. Select **Encrypt always** as action and check the box **Websafe**.

Outgoing emails that are not encrypted by any other method, are sent to the Websafe.

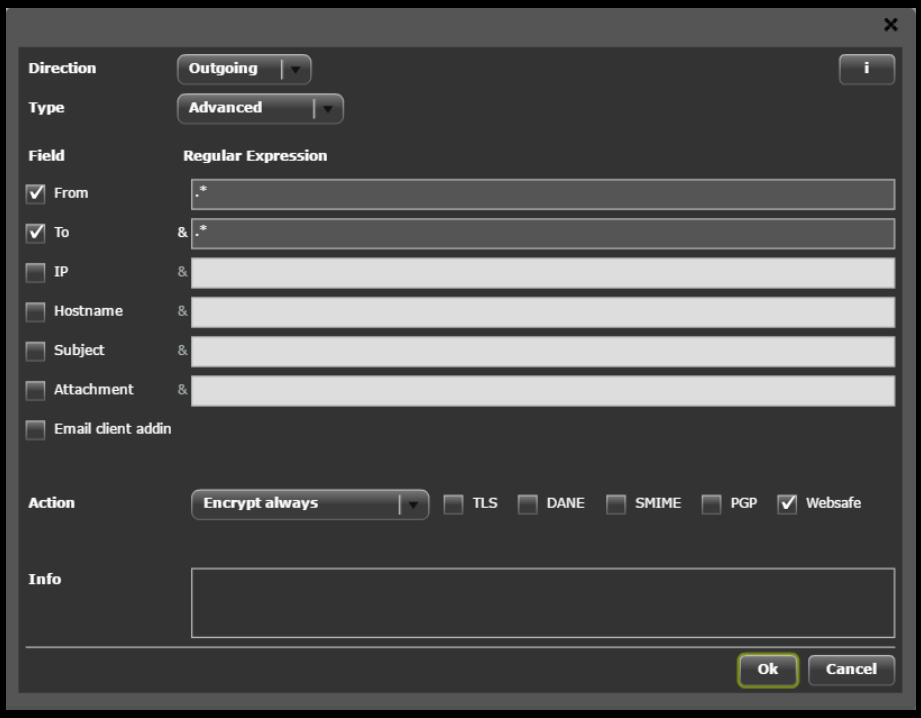


Figure 380: Websafe for all unencrypted emails

Encrypting Emails with Websafe through the Email Subject

Define a rule to encrypt emails by setting a keyword in an email's subject.

1. Click on **Add** in the tab **Encryption**.
2. Select **Outgoing** as direction.
3. Activate the checkbox **Subject**.
4. Enter the keyword **WEBSAFE** in the field.
5. Select **Encrypt always** as action and activate the checkbox **Websafe**.
6. Save the entries with **Save**.

If you enter the keyword **WEBSAFE** in the subject of an email, this email will be encrypted via the Websafe..

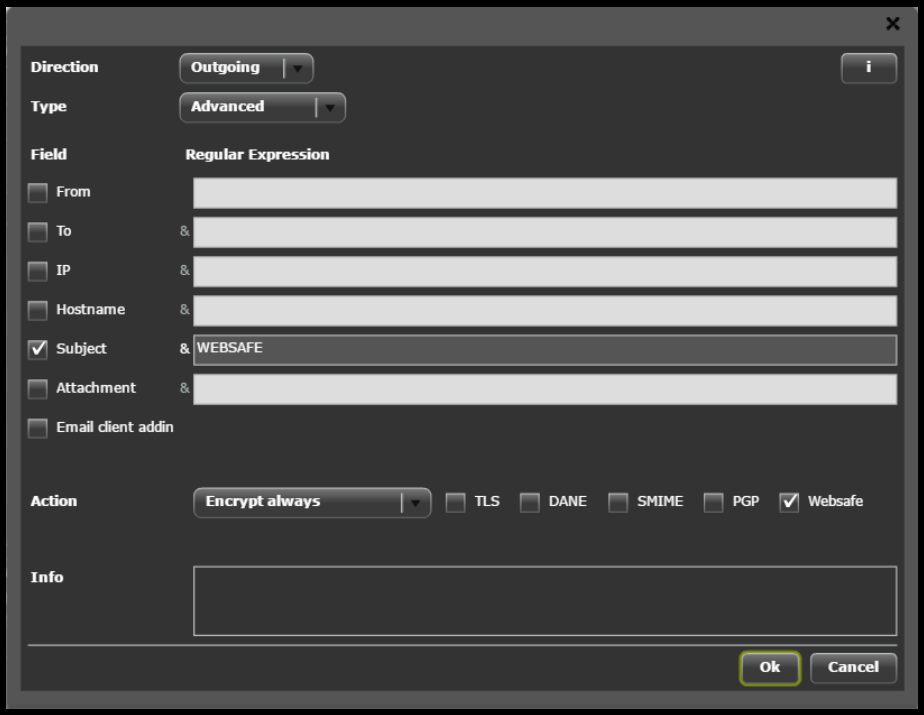


Figure 381: Websafe as subject keyword

Websafe Templates

It is possible to select templates for the sender notifications, the recipient notifications and the website of the Websafe activation.

Selecting Websafe Templates

1. Navigate to **Websafe Templates** under **Encryption**.
2. Select the desired templates from the drop-down menus.

Websafe templates have been selected.

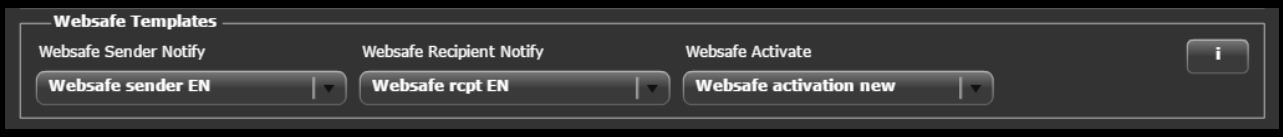


Figure 382: Selecting Templates

Using Keywords in the Email Subject

If you booked Email Encryption, use the following keywords in your email subject to trigger specific actions:

- CRYPT: The email is encrypted with the activated encryption methods in the defined order of encryption methods.

  > **Important:**
  >
  > The keyword **CRYPT** has no function.

- NOCRYPT: The email is sent unencrypted.
- SIGN: The email is sent signed.
- NOSIGN: The email is sent unsigned.
- WEBSAFE: The Websafe is used for the encrypted communication. (Only after setup in the Control Panel)

> **Important:**
>
> You must write the keywords in capitals.

Hornetdrive

About Hornetdrive

The main component of the window is the Hornetdrive administration, which sorts and displays the existing accounts according to the current search criteria.

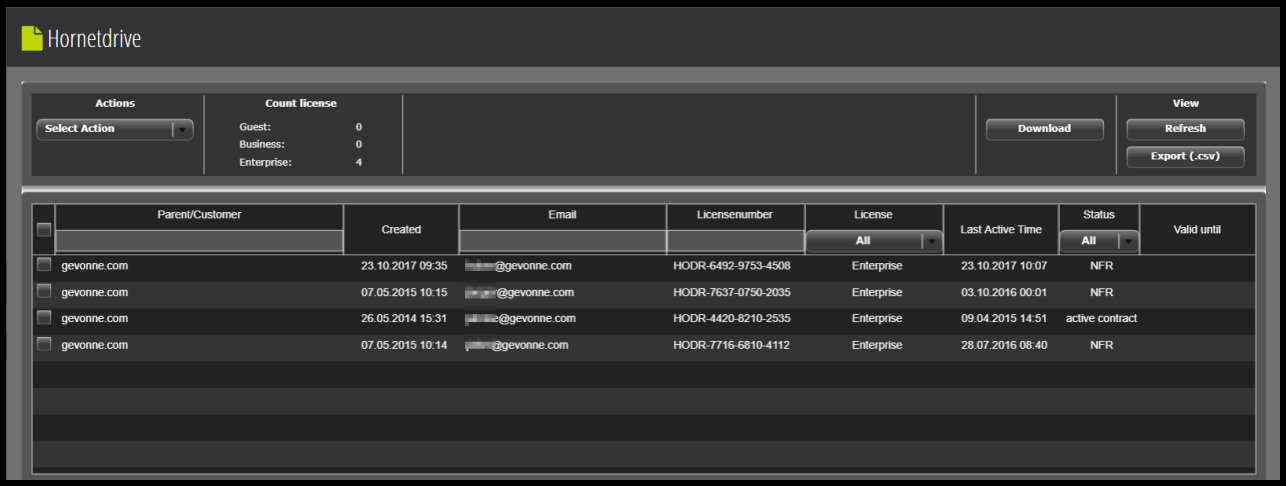


Figure 383: Hornetdrive-Management

In the **Actions** area in the upper left corner, you can trigger certain actions for the selected accounts. To the right is the area **Number of licenses**. The number of licenses assigned to customers and partners is displayed here. The **Help** and **View** areas are located on the right-hand side. The existing Hornetdrive accounts are displayed in the account area in the middle part of the window.

Performing Actions

In the **Actions** area in the upper left corner, you can trigger certain actions for the selected accounts.

1. Click on the drop-down menu.
2. Select the desired action.

Actions have been performed. A window appears with the respective setting options in the foreground.

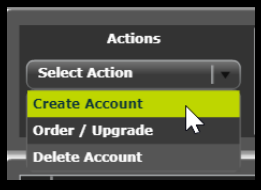


Figure 384: Actions

Creating an Account

1. In the **Actions** area, select the action **Create Account** from the drop-down menu

2. Enter the email address of the new account in the field **Email**.
3. Enter a password in the field **Password**.
4. Select the desired license from the drop-down menu **License**.
5. Select from drop-down menu **Language** in which emails are sent to the user.
6. Select from drop-down menu **Status** to select the status of the license.
   - active contract: an active contract license
   - NFR: a not-for-resale-lizenz
   - test customer: a trial license

   If you have selected test customer, you can then enter the expiration date of the test license.
7. Under Parent/Customer you can select the partner or the domain under which the new account should be created.
8. Read and confirm the License Agreement by clicking on the checkbox **Accept license agreements**.
9. Click on **Save**, to create the account and close the window.

> **Notice:**
>
> To create another account directly, click on **Save & Continue**.

Account has been created.

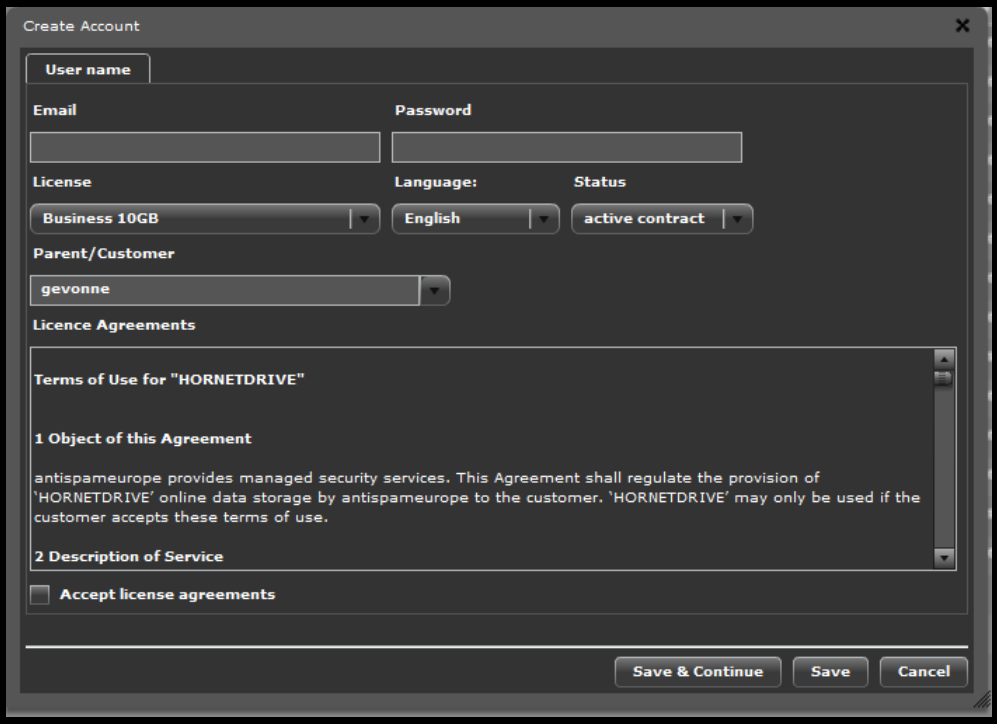


Figure 385: Create Account

Upgrading an Account

This function allows various upgrades or extensions of an existing account:

- Upgrade a test account into a contract account.
- Upgrade a guest account into a business or enterprise account.
- Upgrade business accounts in an enterprise account
- Increasing the volume of storage space and traffic contained in an enterprise account

1. Select one or more accounts in the account area of the Hornetdrive module.
2. In the **Actions** area, select the **Order/Upgrade** action from the drop-down menu.

   A new window opens.
3. Select the desired licenses for the previously selected accounts.
4. Read and confirm the license agreements with a click on the checkbox **Accept license agreements**.
5. Click on OK to complete the order.

Account has been upgraded/extended

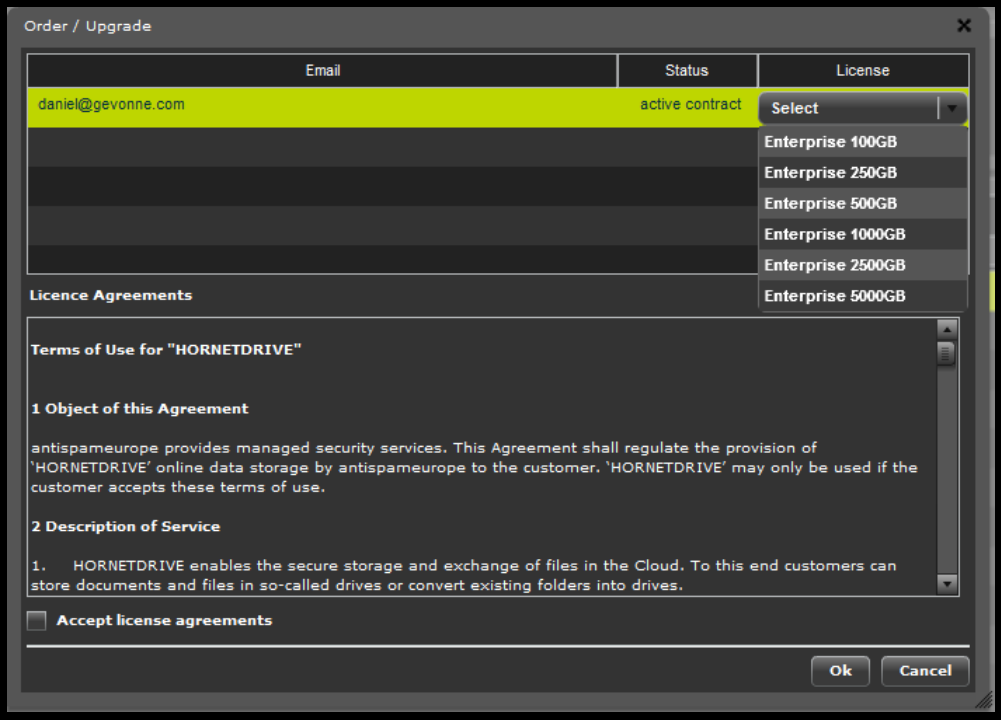


Figure 386: Upgrade accounts

Assigning Accounts to Other Partners or Customers

This action allows you to assign accounts to another partner or customer.

1. Select one or more accounts in the account area of the Hornetdrive module.
2. In the **Actions** area, select the **Assign Account** action from the drop-down menu.
   A new window opens.
3. Select the desired partner or customer from the drop-down menu.
4. Click on **OK** to make the assignment.

Account has been assigned to a Partner/Customer.

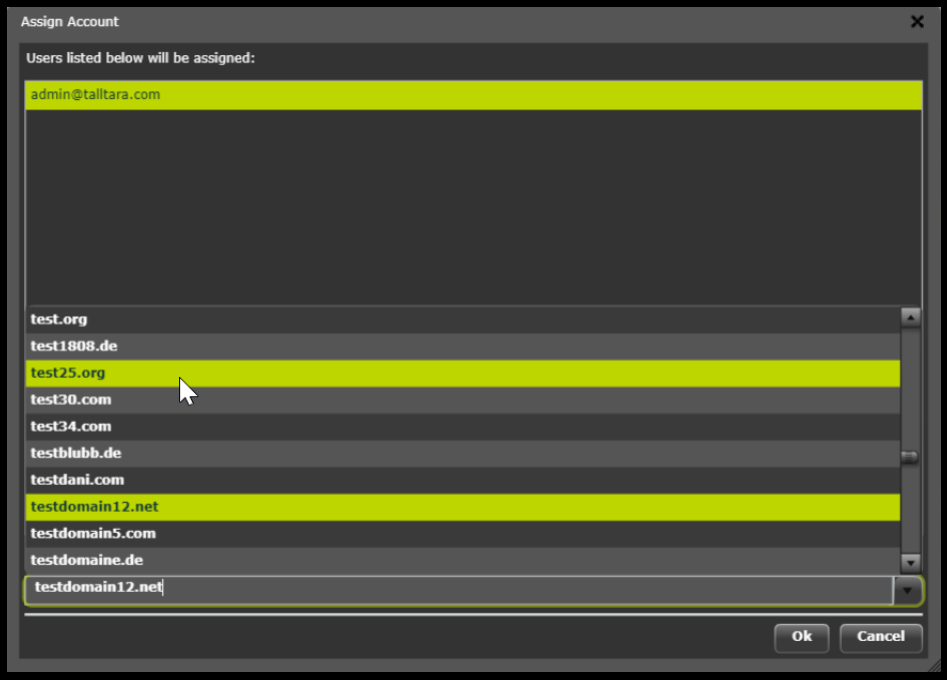


Figure 387: Assign accounts

Deleting Accounts

1. Select one or more accounts in the account area of the Hornetdrive module.
2. In the **Actions** area, select the **Delete Account** action from the drop-down menu.
   A new window opens in which all accounts to be deleted are listed.
3. Click on **OK** to delete the previously selected accounts.

Accounts have been deleted.

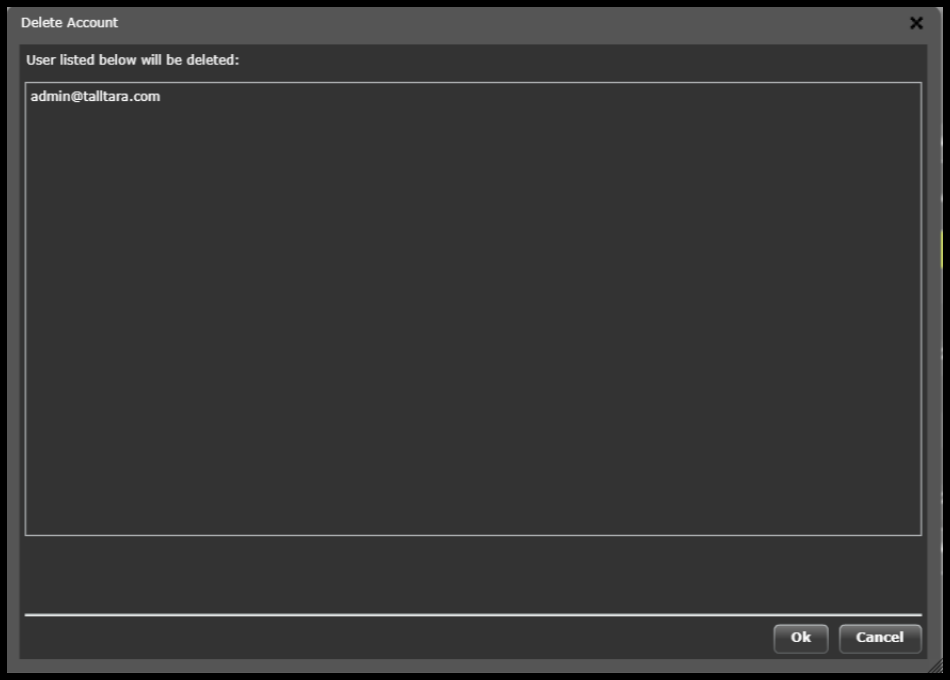


Figure 388: Delete accounts

Exporting Data as CSV

You can export a list of accounts as a CSV file. A window with the corresponding settings opens.

1. Select the columns you want to export in the upper area.

   The checkbox **All activate/deactivate** selects or deselects all columns in the upper area.
2. Activate the checkbox **Show column name in 1. row**, to export the column headers as well.
3. Activate the checkbox **Export only selected rows** to only export the previously selected rows.
4. Select the format of the export under **Export type**.
   - Display: Displays the data to be exported in a new window.
   - Download: Downloads the data as a CSV file,
   - Email to: Sends the data to the entered email address.
5. Click on **Export** to export the data.

Data has been exported as CSV.

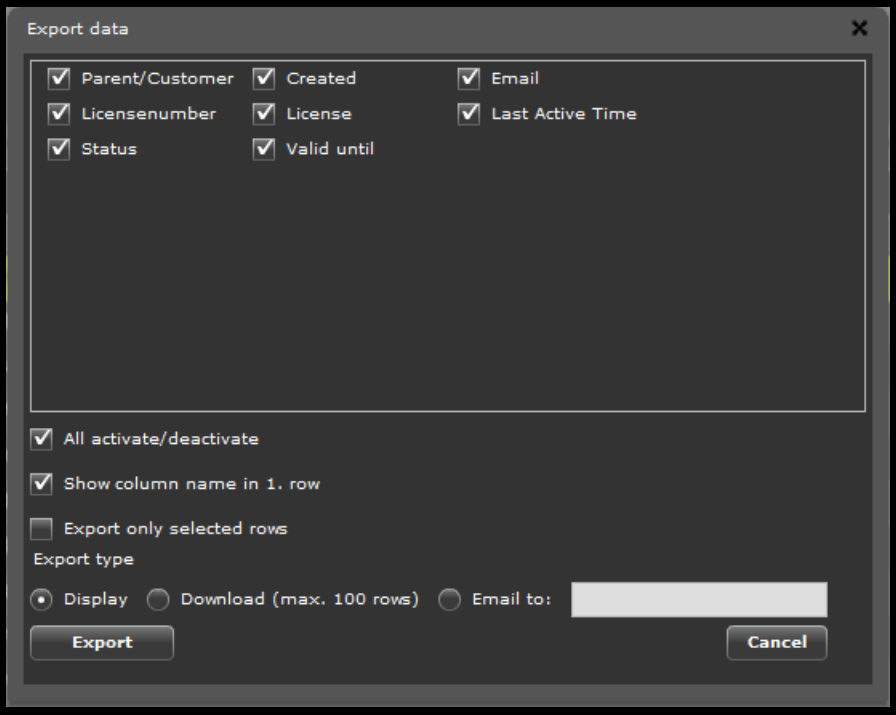


Figure 389: Export

Account Area

In this area you can view the data of all assigned users.

Search fields are located below the Partner/Customer, Email and License Number columns. These filter the data sets according to the value in the corresponding column. Selection menus are located under the licence and status column headings. These filter the data sets according to the value in the associated column.

The following columns are available:

- A selection box to select the data sets is located on the far left for each data set.
- The column **Partner/Customer** displays the superordinate customer or partner for the user.
- The column **Created on** displays the date on which the Hornetdrive account was created.
- The column **Email** displays the email address provided by the user. This is also the username.
- The column **Licence number** displays the user's licence number.
- The column **Licence** displays the type of user licence. A distinction is made between **Guest**, **Business** and **Enterprise**.
- The column **Last use** displays when the user last signed in to a client.

- The column **Status** displays whether the user is a contract customer, webshop customer or test customer. Test customers that have not purchased a full version within the test period are also listed as **Expired** for the period prior to the final cancellation of their account. Customers whose follow-up time has expired are no longer listed.
- The column **Valid until** displays the date on which the current licence expires. For test customers this refers to the end of the test period, while for contract customers this refers to the end of the paid-up licensing period.

Opening the Account Details

Double-click on an account row in the account area to open the detailed view for this account.

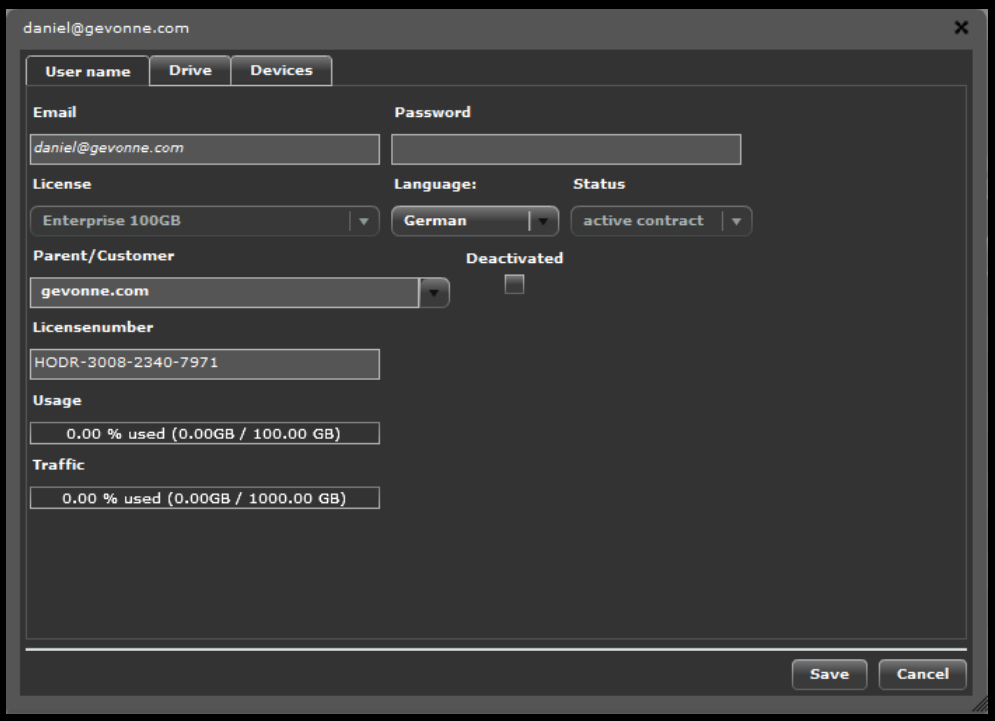


Figure 390: Account details

Account Details are displayed.

Account Details

Username Tab

- Username: Displays the user's email address, which is also the username.

- Password: A new password is accepted on re-entering the password and saving the change.
- License: This displays the user's license. The license cannot be changed here.
- Languages: Either German or English can be selected. This setting determines the language in which emails are sent to the user.
- Status: This allows a distinction to be made between contract customers and test customers. Another field appears for test customers for the end date of the test phase.
- Partner/Customer: This function allows the new user to be created / to be allocated to a partner or customer.
- License number: Displays the user's license number.
- Memory usage: Displays how much memory the user has used and how much is available in total.
- Traffic limit: This display provides information on how much traffic volume the user has used this month and how much is available for this month in total.

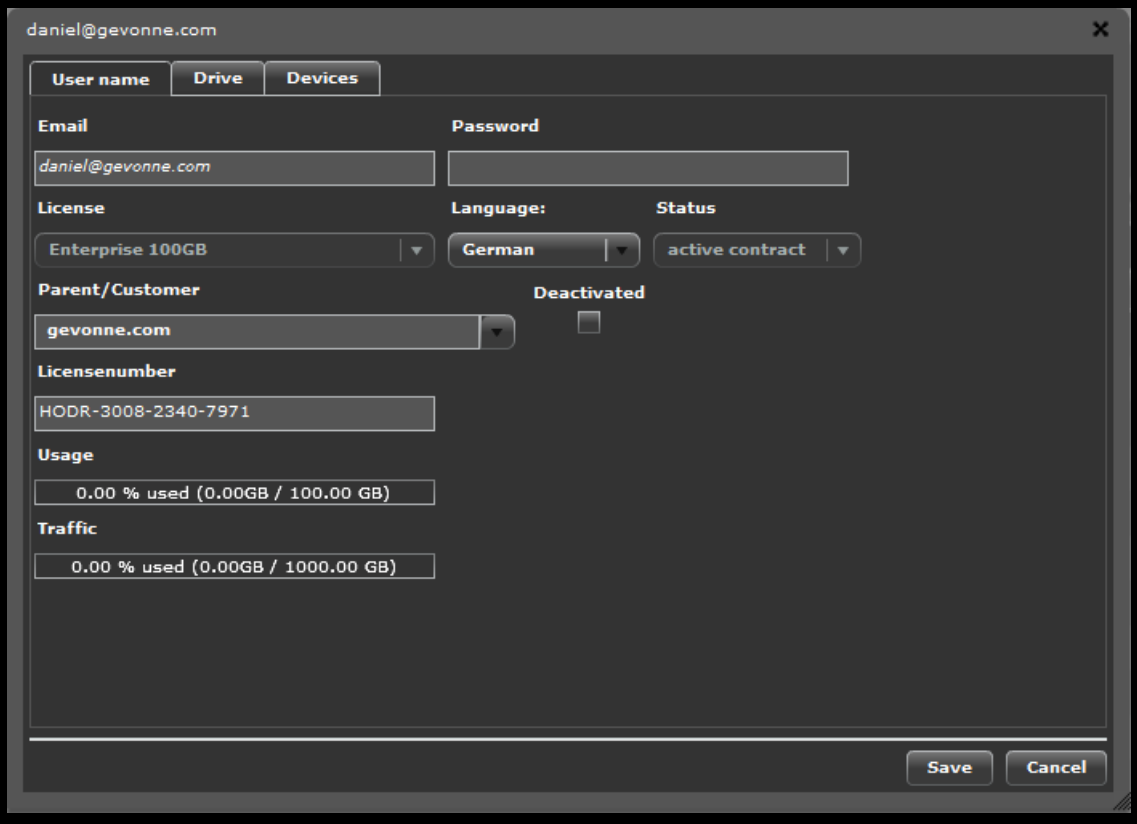


Figure 391: Account details - Username

Drive

This displays the drives created by the user. The following information is displayed:

- Name of the drive
- Date of creation
- Memory
- Currently used traffic
- Volume used this month.

The drive is deleted by clicking on the "Remove" cross in the corresponding row.

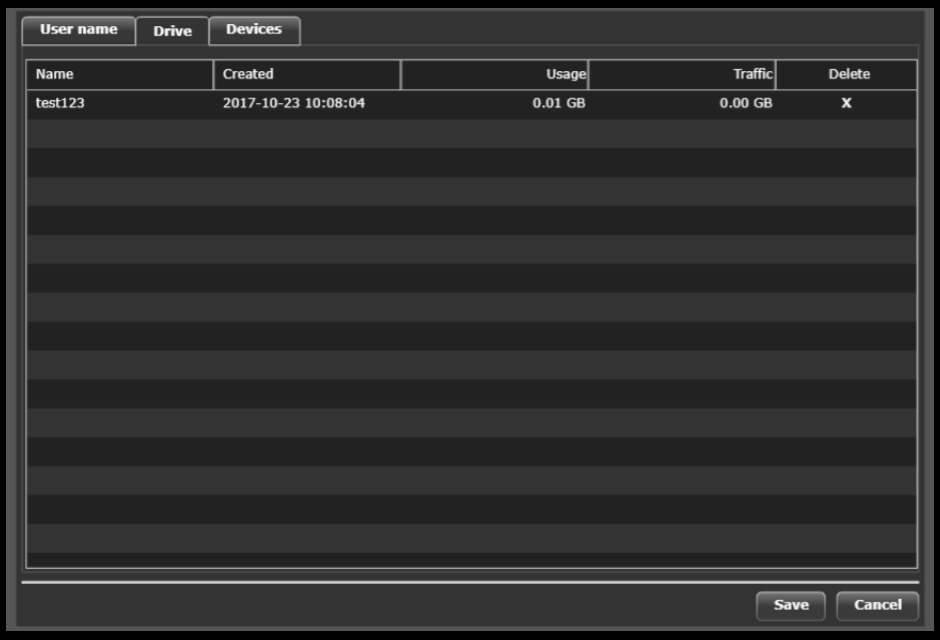


Figure 392: Account details - Drive

Devices

This displays all the devices on which the user has installed Hornetdrive.

The following information is displayed:

- Name of the device
- Date of creation
- Time of last use
- Last IP address used
- Version of the client installed on the device
- Operating system version

You can delete the device by clicking on the **x** under **Delete**.

Notice:

This device can then no longer be used to access the drives.

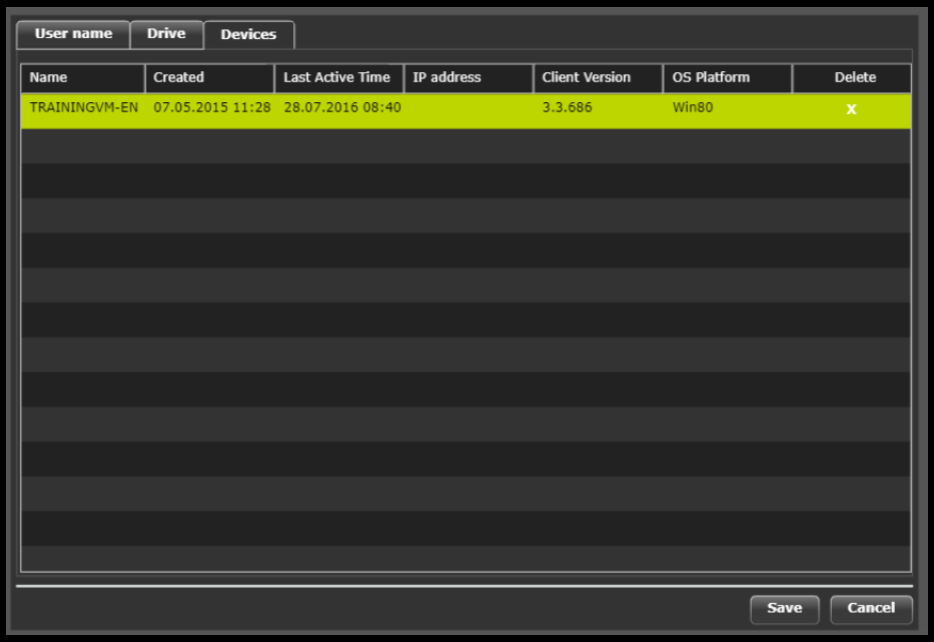


Figure 393: Account details - Devices

Whitelabeling

Control Panel Customization (Whitelabel)

You can customize the Control Panel to embed your company's color, logo and favicon.

Furthermore, you can select a theme for your Control Panel and add support and email information.

The customization is displayed to all users logging in to the domain you provide.

Attention:

The operation of a customized Control Panel will increase costs according to the price list.

Prerequisites to Customize the Control Panel

- You have an administrator role or a partner role.
- You have provided your domain's certificate to support@hornetsecurity.com.

  Important:

  The certificate must at least support SHA256 and use 2048 bit key length. Consider the note below about the automated generation of SSL/TLS certificates.
- Additionally, you must create a CNAME record for your domain. Otherwise, the URL of the Hornetsecurity Control Panel domain is shown in the browser.

Following a CNAME record is set for the domain **controlpanel.customerdomain.com**

controlpanel.customerdomain.com IN CNAME cp.hornetsecurity.com

Customizing the Control Panel

Customize the customer and logo to match your company's design.

1. Login to the Control Panel.

   Important:

   You need administration or partner authorization to customize the Control Panel.

2. From the scope selection, select the partner or customer for which you want to customize the Control Panel.

   You can only make changes in the scope with which you made the adjustments.

3. Select the section **Whitelabeling** on the left side.

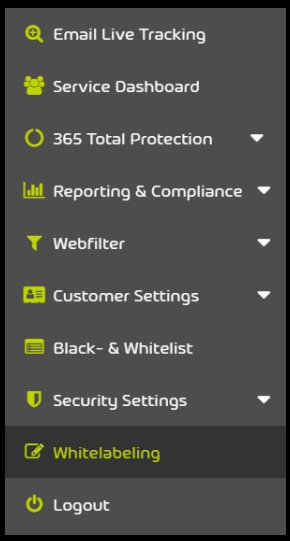


Figure 394: Select "Whitelabeling"

4. Select **Appearance**.

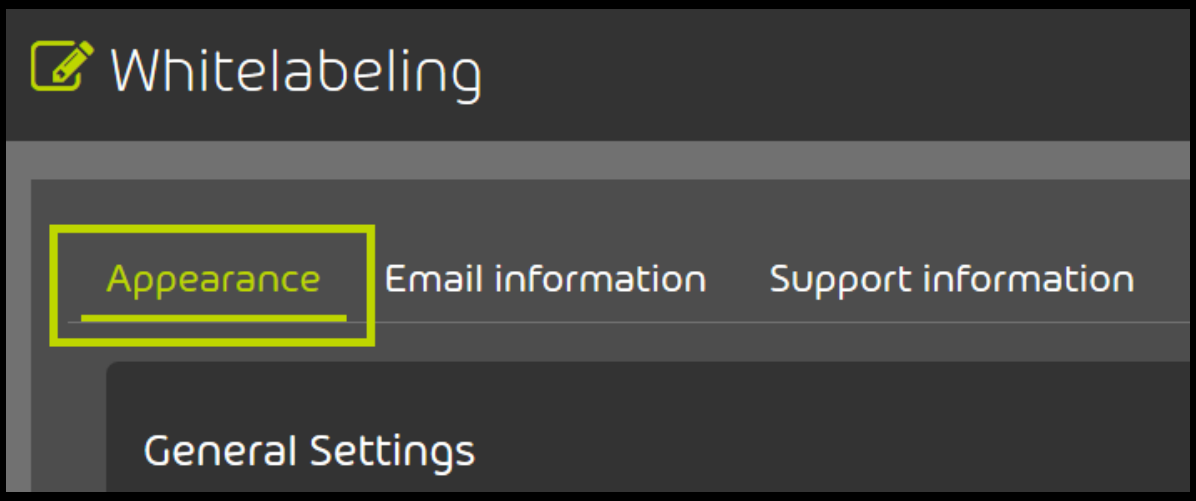


Figure 395: Select "Appearance"

5. Enter the URL of the domain for which you would like to customize the Control Panel.

   Enter the URL of your Control Panel website in the field **Url**:
   controlpanel.kundendomain.de

CAUTION:

If you change the URL subsequently, you must also update the CNAME record for your domain (see Prerequisites to Customize the Control Panel on page 379).

6. Select a primary color for your Control Panel.

Notice:

This allows you to include your corporate colors in the Control Panel. The primary color is responsible for the font color and other design elements.

a) Click in the field under **Primary color** to open a color selection.

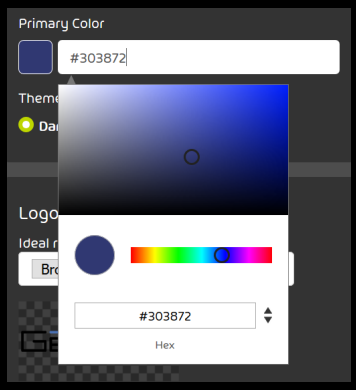


Figure 396: Color selection

b) Pick the desired color.

➔ **The selected color is represented in the field as HEX or sRGB.**

You can insert the color code directly into the field as well.

7. Select a theme for your Control Panel under **Theme**.

- Activate the radio button **Dark** to select a dark theme.

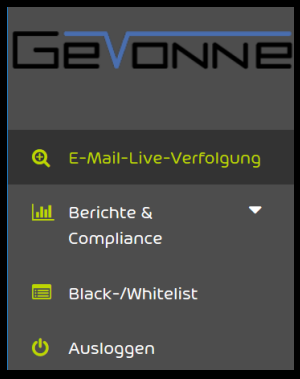


Figure 397: Dark theme preview

- Activate the radio button **Bright** to select a bright theme.

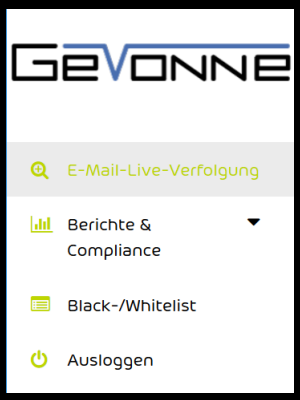


Figure 398: Bright theme preview

8. Click on **Browse...** under **Logo** to select your Logo.

> **Notice:**
>
> For the best result, upload a logo with a minimum resolution of 160 × 80 pixel.

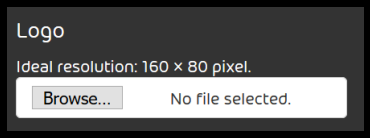


Figure 399: Logo

9. Click on **Browse...** under **Favicon** to select your favicon.

Notice:

The favicon must be uploaded in ICO file type (filename extension .ico). For the best result upload the favicon with a resolution of 128 × 128 pixel.

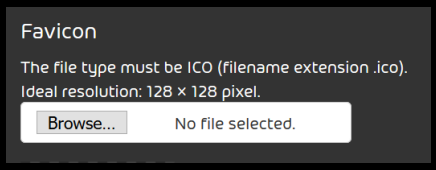


Figure 400: Favicon

10. Click on **Save** to confirm your customization.

Notice:

The deployment takes up to five minutes.

11. Refresh the Website to see your customized Control Panel.

    You must be logged in to your Control Panel domain to see the customization.

    Control Panel has been customized.

Customizing the Progressive Web App

Customize the app name and the app icon of the progressive web app to the design of your company.

1. Select **Whitelabeling#→Appearance**.
2. Enter the desired app name in the field **App Name**.

Figure 401: Enter app name

3. Upload a picture with the file type PNG under **App Icon**.

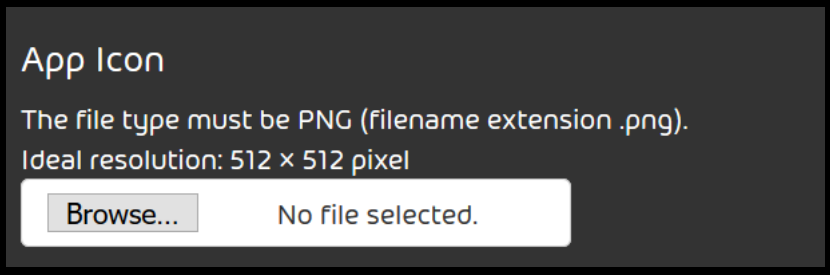


Figure 402: Upload app icon

Underneath the file selection for the App icon you can see a preview of the icon in various sizes. As well as you can see a preview of the splashscreen under **Splashscreen**. The splashscreen is displayed while loading the progressive web app and contains the file that was uploaded under **Logo**.

Figure 403: Preview of splashscreen

4. Save your settings.

The logo and the app name is displayed on the homescreen of mobile devices.

Example: Customizing the Control Panel

Below is an example for customizing the Control Panel which explains and visualizes what the customizations do.

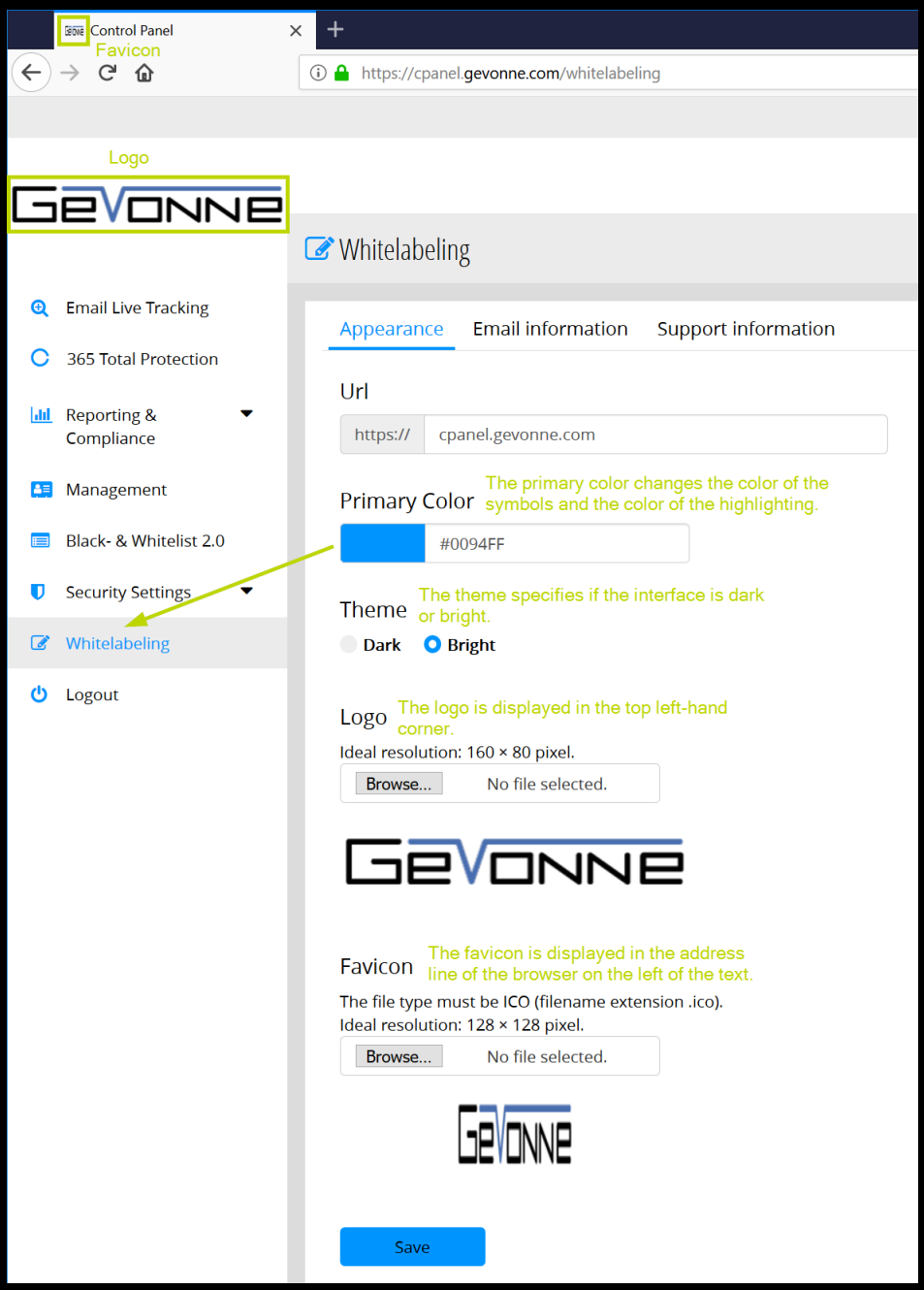


Figure 404: Example and explanations

Fallback Design

The fallback design ensures, that the Control Panel is shown without any company specific attributes, in case of misconfiguration.

In the case, that your domain has not been recorded at Hornetsecurity and your configuration cannot be set, an alternative design is selected.

Therefore, the Control Panel gets the dark theme, without any logo or favicon. For the primary color the default Hornetsecurity green will be used.

Displayed Email Information

The system automatically sends emails in various situations, for example when users reset their passwords. You can define a greeting formula, a contact person, the sender address and a disclaimer for these emails.

Adding Email Information

1. Select **Email information**.
2. Enter a salutation in the field **Salutation**.
3. Enter the name of the contact in the field **Contact**.
4. Enter the sender address for outgoing system emails in the field **Sender address for email templates**.
5. Optional: Enter the required information for a disclaimer in the field **Disclaimer**.

> **Important:**
>
> All data below is just an example. Inform yourself in your company which information is required for outgoing system emails.

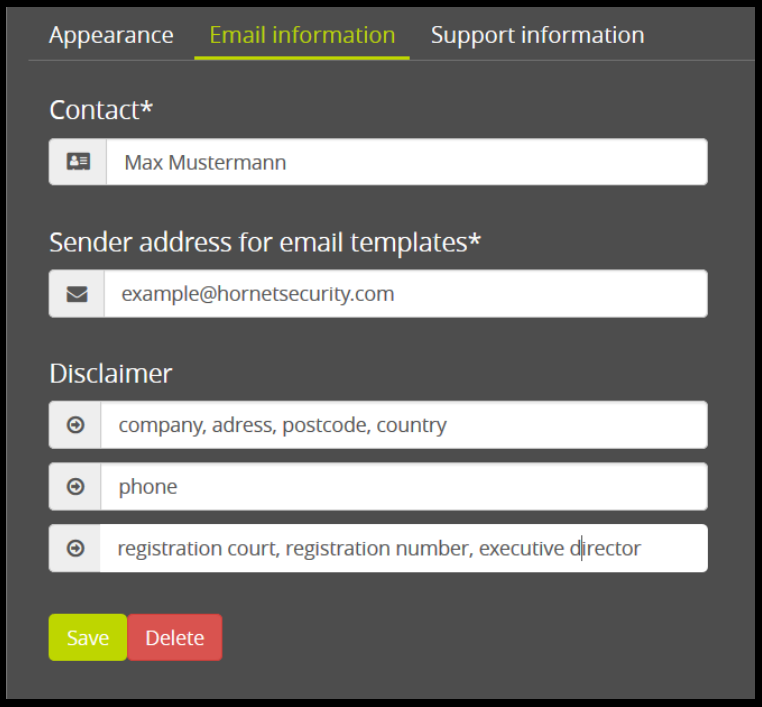


Figure 405: Select Email information

6. Click on **Save** to apply the settings.

Email information has been added.

Contact Data in the Control Panel

The contact data phone number and email address is shown in the Control Panel.

Figure 406: Contact data in the Control Panel

If you want to change the contact data, you must provide them under **Support information** (see Adding Support Information in the Control Panel on page 389).

Contact Data Processing

The contact data is processed hierarchically from bottom up.

Underneath a customer are several domains. That customer has provided his contact data on the top level. Thus, every user of the underlying domains gets the contact data of the customer.

If contact data for a underlying domain is provided, it will be shown to the users of that specific domain.

Adding Support Information in the Control Panel

1. Select **Support information**.
2. Enter the support phone number of your company in the field **Support phone number**.
3. Enter the support email address of your company in the field **Support email address**.

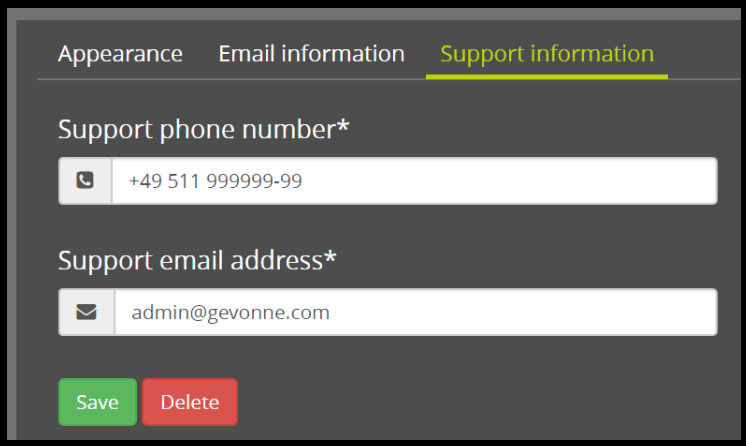


Figure 407: Add support information

4. Click on **Save**.

Support Information have been added in the Control Panel.

Email Categories

Your emails are classified into the following categories:

Email Category	Description
Clean	The category clean indicates that no threat was found.
Infomail	Infomails are promotional emails that can either be classified as clean or spam.
Spam	Emails classified as spam.
Content	Emails with illegal attachments. Defined by the partner or domain administrator.
Virus	Emails containing a virus.
ATP	Emails containing threats identified by Advanced Threat Protection.
Rejected	Rejected emails.

Classification Reasons

The following sections are structured in the different classification types for emails.

The tables list the reasons shown in the email display with their explanations.

> **Notice:**
>
> The classification reasons are incomplete and are extended in a later version of this manual.

Classifications ATP, Rejected, Virus

Classification	Reason	Definition
ATP	Business Email Compromise	Fraudulent email with a fake sender from your own company.
ATP, Rejected, Virus	Malicious Attachment	At least one attachment of the email is malicious.
ATP, Rejected, Virus	Malicious Email Content	The email contains malicious content.
ATP, Rejected, Virus	Malicious URL	The email contains links to malicious websites or documents.
ATP, Virus	Massive Attack Prevention	The email matches the pattern of a starting malware campaign.
ATP, Virus	Phishing	The email contains characteristics of a phishing attack.
ATP	Sandbox	At least one attachment of the email was dynamically analyzed in the ATP sandbox and rated as malicious.

Classification	Reason	Definition
ATP	Targeted Fraud	The email matches the pattern of a targeted fraud attack.
Rejected	Block by Compliance Filter Policy	The email was blocked by a compliance filter rule as a virus.
Rejected	RBL	The sending host of the email has a negative reputation.
Rejected	Envelope SPF Failure	The SPF check in the envelope of the email failed.

Classification Content

Classification	Reason	Definition
Content	Detached by Content Control Policy	At least one attachment is not permitted due to the settings in Content Control.
Content	Rejected by Content Control Policy	The email was rejected according to Content Control guidelines because it contains at least one forbidden attachment.

Classification Valid

Classification	Reason	Definition
Valid	Clean by Compliance Policy	The email was classified as valid by a compliance filter rule.
Valid	Good Sender Reputation	The sender or sending host of the email has a positive reputation.

Classification	Reason	Definition
Valid	Ham	Ham is the opposite of spam. Thus a desirable email that matches the pattern of a valid email.
Valid	Sender Whitelisted by Policy	The sender or sending host of the email is listed on the domain administrator's white list.
Valid	Statusmail	Automatically generated system notification, such as a spam report.
Valid	Whitelisted by User Policy	The sender or sending host of the email is listed on the recipient's white list.

Classification Spam

Classification	Reason	Definition
Spam	Bad Host Reputation	The sending host of the email has a negative reputation.
Spam	Bad IP Reputation	The IP address of the sending host of the email has a negative reputation.
Spam	Bad Sender Reputation	The sender of the email has a negative reputation.
Spam	Bad URL Reputation	The email contains at least one link to a web server with a negative reputation.
Spam	Blacklisted by User Policy	The sender or sending host of the email is listed on the recipient's blacklist.
Spam	DKIM Failure	The DKIM validation failed.

Classification	Reason	Definition
Spam	DMARC Failure	The DMARC validation failed.
Spam	Header SPF Failure	The SPF check failed.
Spam	Spam Content	The email contains content that is classified as spam.
Spam	Spam by Compliance Policy	The email was classified as spam by a compliance filter rule.

Deprecated Email Classification Reasons

Important:

The following classification reasons are deprecated, but are still used in the Flash Control Panel.

Classification ATP/Content/Virus

Reason	Definition
Virus-scan01	Found identical attributes of classified virus emails in metadata
Virus-scan01-XARG-V	Found known virus structure in multiple attributes of the email
Virus-scan02-Header-V	Found virus signature in email header
Virus-scan03-Link-Va	Linking of a compromised URL
Virus-scan04-Body-V	Found virus signature in email body
Virus-scan05-<VirusName>	Virus found – known, classified virus
Virus-scan06-<VirusName>	Virus scanner 2 found a virus
virus-scan07-doubleextension	Found a file with veiled or faked file type in an archive
Virus-scan07-archive-in.archive	Found nested archives in an archive

Reason	Definition
virus-scan07-heur-exploit	Found minimum one unknown and potentially dangerous file in an archive
Virus-scan07-fakeoffice2003	Found macro code of office 2007 in an office 2003 file
virus-scan07-potential-fake-archive	Found an archive with wrong declaration of content type (MIME-Content-Type)
Virus-scan08-executable	Found potentially dangerous file in attachment
Virus-scan09-asehtmlheuristics	Evidence of phishing and suspicious attachment found
Virus-scan09-ASEurl 0xHeuristics	Evidence of phishing and suspicious link found
Virus-scan09-ASEzipHeuristics	Evidence of phishing and suspicious attachment found
Virus-scan10-<VirusName>	Indistinct virus message through Heuristic intend analysis
Virus-scan12-AttachmentV	Found virus signature in attachment
Virus-scan13-ASE-PhishingHeuristics	Evidencce of phishing and suspicious email header found
Virus-scan14-Short-URL-obfuscation	Links are veiled through nested URL shortening
Virus-scan15-ASE-Phishing	Direct link to malware or phishing website
Virus-scan16-ASE-Phishing-heur	Evidence of phishing and inconsistent sender address
Virus-scan17-ASE-office-macro-exploit	Found evidence of malware and office file with macros, OLE-object or VBS code as attachment
Virus-scan17-office-webarchive-exploit-heur	Evidence of malware and attachment with suspicious content found
virus-scan17-office-rtf-exploit-heur	Evidence of malware and attachment with suspicious content found
virus-scan17-Macro	Evidence of malware and attachment with suspicious content found

Reason	Definition
Virus-scan18	Evidence of malware and the email was sent by different senders or email servers
Virus-scan21-<Virusname>	Virus message by optional virus scanner 3
Virus-scan22-<Virusname>	Virus message by optional virus scanner 4
Contentfilter	Customer defined forbidden attachment

Classification Rejected

Reason	Definition
450 4.1.1	rejection when relay check is enabled
450 4.1.8	sender address rejected : domain not found
450 4.5.5	early spam detection (temporarily blocked)
450 4.5.6	temporary failure in MTA - please retry
450 4.5.7	temporary failure in MTA - please retry
504 5.5.2	recipient address rejected : fully - qualified adress is needed
504 5.5.2	sender adress rejected: fully - qualified address is needed
550 5.1.1	unknown recipient (SMTP check)
550 5.2.2	explicit blocking of sender or recipient address
550 5.5.3	recipient address rejected: multi-recipient bounce
552 5.5.2	message size (Content Control)
554 5.5.3	email rejected due to Content Control Size Limit
554 5.5.4	IP sender address with a negative reputation
554 5.5.5	email rejection due to Spam
554 5.5.6	loop detection
554 5.5.7	email rejected due to content of attachment

Reason	Definition
554 5.6.1	signature of spam in mail header resp. subject
554 5.6.2	spam link signature detected
554 5.6.3	spam text signature detected
554 5.6.4	virus email blocked
554 5.6.5	TLS encryption required by customer rule
554 5.7.1	unknown domain or unknown recipient (LDAP check)

Classification Quarantined

Reason	Definition
admin-bl	black list controlled by admin
ase-bl	individual black list controlled by support dep.
ase-recap1	diffuse spam fingerprint
ase-recap4	diffuse spam fingerprint
ase-rep1	IP reputation list 1
ase-rep2	IP reputation list 2
ase-rep4	URL-/IP-Reputationsliste 4
asespf7-1	SPF filter variant 1
asespf7-2	SPF filter variant 2
bodytag	spam signature in mail text
customer-bl	black list controlled by the customer
dirtyip	reputation filter on IP basis
fingerprint	re - captured spam mail by hash
header	spam signature in mail header
link	ad link
rbl50	pre-stage to 554 5.5.4 but not blocking yet

Reason	Definition
sameip	signature recognition through spam engines
score	dynamic content evaluation
Score Tag	dynamic content evaluation
spam	reputation filter based on sender server
spamip-net	IP range of servers with poor reputation
spam-sum	spam fingerprint
subjecttag	spam signature in subject line
user-bl	black list controlled by the user
wc	spam pattern recognition
xarg	bounce attack or individual customer rule
zombie	botnet computer

Classification Valid

Grund	Definition
asespf1	familiar sender, type 1
asespf2	familiar sender, type 2
asespf3	familiar sender, type3
ase-wl	individual white list controlled by the support dep.
big2	email size increased email reputation in multi-criterial scoring function
bigmessage	email size increased email reputation in multi-criterial scoring function
body-wl	white list signature in mail text, type 1
body-wl2	white list signature in mail text, type 2
header-wl	White list signature in header, type 1
header-wl2	White list signature in header, type 2

Grund	Definition
knownsender	sender address with positive reputation, type 1
noreason	unevaluated email
qsender2	sender address with positive reputation, type 2
realbounce	sent via bounce management
score	dynamic contents evaluation
sender-ip	IP sender address with positive reputation
subject-wl	white list signature in subject line, type 1
subject-wl2	white list signature in subject line, type 2
user-wl	white list controlled by user
xarg-wl	bounce mail or individual customer rule

Numerics

365 Total Encryption
    Functions 102
365 Total Encryption, activating 103

A

account,
    assigning (Hornetdrive) 371
    creating (Hornetdrive) 368
    deleting (Hornetdrive) 372
    upgrading (Hornetdrive) 370
account details,
    explanation (Hornetdrive) 375
    opening (Hornetdrive) 375
actions
    defining (Compliance Filter) 298
    filtering (Auditing) 183
Activate Compliance Filter 293
activating
    365 Total Protection 103
    all mailboxes 106
    ATP 256
    Compliance Filter 293
    Content Control 285
    Continuity Service (Control Panel) 93
    email encryption (Email Encryption) 92, 352
    individual mailboxes 106
    LDAP connection 55
    Signature & Disclaimer 64, 315, 317
    Spam Report 267
    URL Rewriting 260
    Web Filter 197
    Websafe by keyword in subject 365
Activating Email Encryption (Email Encryption) 92, 352
Active Directory attributes
    explanation (Signature & Disclaimer) 322
Active Directory variables, *See* Active Directory attributes
adding
    CNAME record (365 Total Protection) 81
    contact data (Control Panel) 66
    contact information (Whitelabeling), *See* adding support information (Whitelabeling)
    email information (Whitelabeling) 387
    exceptions (Control Panel) 349
    filters (Compliance Filter) 295
    group to Content Control 285
    LDAP server, *See* activating LDAP connection
    MX record (365 Total Protection) 80
    recipient of alerts (ATP) 257
    support information (Whitelabeling) 389

adjusting
size of email field (Email Live Tracking) 32
Advanced Routing, configuring (Control Panel) 313
Advanced Threat Protection, *See* ATP
alert (Advanced Threat Protection) 253
all mailboxes
activating 106
allowed websites (Web Filter) 190
allowing
user actions 283
applications, managing 204
archiving
internal emails via Hornetsecurity (365 Total Protection) 82
archiving,
deactivating 350
setting up 348
Archiving
of internal emails via Hornetsecurity, configuring (365 Total Protection) 82
assigning
account (Hornetdrive) 371
role 53
ATP
activating 256
ATP engines
operating principle 252
ATP report
explanation (Advanced Threat Protection) 40, 265
ATP Report
viewing (Advanced Threat Protection) 38, 264
ATP scan
explanation (Advanced Threat Protection) 263
attachment
category 291
attack type
explanation (Threat Live Report) 177
attack vector
explanation (Threat Live Report) 179
attempted attacks
attack type by date (Threat Live Report) 172
attack vector by date (Threat Live Report) 174
Autodiscover, configuring (365 Total Protection) 81

B

blacklist entry
create (Black & White Lists) 245
deleting (Black & White Lists) 247
searching (Black & White Lists) 248
blocked website (Web Filter) 189
break times, configuring 201
browser (Control Panel), *See* System Requirements (Control Panel)

C

cancellation (365 Total Protection), *See* offboarding (365 Total Protection)

category
explanation (Auditing) 180
selecting (Auditing) 181
certificate, ordering 361
certificate settings 362
certificate, downloading 110
certificate, importing in MacOS 119
certificate, importing in Windows 113
changing
language (Control Panel) 18
location (Control Panel) 18
order of email fields (Email Live Tracking) 33
password (Control Panel) 17
checking
encryption capability 352
classfication
content (Control Panel) 392
classification
ATP, Rejected, Virus (Control Panel) 391
ATP/content/virus (Control Panel) 394
quarantined (Control Panel) 397
rejected (Control Panel) 396
spam (Control Panel) 393
valid (Control Panel) 392, 398
CNAME record, setting (365 Total Protection), *See* Autodiscover, configuring (365 Total Protection)
color of the Control Panel, customizing (Whitelabeling) 379
combination of encryption methods 359
combined search (Email Live Tracking), *See* search function (Email Live Tracking)
compatibility of encryption methods, *See* combination of encryption methods
configuring
Advanced Routing (Control Panel) 313
archiving internal emails via Hornetsecurity (365 Total Protection) 82
Autodiscover (365 Total Protection) 81
break times 201
Connector for journal reports (365 Total Protection) 88
Content Control 287
DNS settings (365 Total Protection) 80
LDAP settings 58
login 58
Spam Report 268, 270
SPF record (365 Total Protection) 79
Web Filter 197
Web Filter login via LDAP 62
Websafe for a specific communication partner 364
Websafe for outgoing emails 364
configuring DNS settings (365 Total Protection), *See* MX record, setting (365 Total Protection)
connector
configuring for journal reports (365 Total Protection) 88
deactivating (365 Total Protection) 99
deleting (365 Total Protection) 99
contact data, adding (Control Panel) 66
contact information, adding (Whitelabeling) , *See* support information, adding (Whitelabeling)
Content Control
activating 285
Content Control, configuring 287
Content Control, setting up 287

Continuity Service
    explanation 350
Continuity Service, activating (Control Panel) 93
Control Panel, accessing 12
create
    blacklist entry (Black & White Lists) 245
    whitelist entry (Black & White Lists) 245
creating
    account (Hornetdrive) 368
    customer (365 Total Protection) 71
    disclaimer 317
    encryption policy 355
    exception, *See* creating encryption policy
    journal rule (365 Total Protection) 87
    mail flow scenario (365 Total Protection), *See* configuring archiving internal emails via Hornetsecurity (365 Total Protection)
    onboarding link (365 Total Protection) 70
    signature 317
customer
    creating (365 Total Protection) 71
    onboarding, *See* customer creating (365 Total Protection)
customizing
    color of the Control Panel (Whitelabeling) 379
    favicon (Whitelabeling) 379
    logo (Whitelabeling) 379
    theme (Whitelabeling) 379
    URL (Whitelabeling) 379

D

DANE 353
data as CSV,
    exporting (Hornetdrive) 373
data overview (Hornetdrive) 374
deactivating
    archiving 350
    connector (365 Total Protection) 99
    email archiving, *See* deactivating archiving
    mailbox encryption 109
    Spam Report 272
Deactivating the Mailbox Encryption 109
defining
    actions (Compliance Filter) 298
    exceptions 211
    filter rule (Compliance Filter) 296
    Web Filter categories for a group 207
Delete role assignment 54
deleting
    account (Hornetdrive) 372
    blacklist entry (Black & White Lists) 247
    connector (365 Total Protection) 99
    Role assignment 54
    signature 321
    whitelist entry (Black & White Lists) 247
delimiter (Email Live Tracking), *See* search function (Email Live Tracking)

diagram,
emails by type (Email Statistics) 167
filtering (Email Statistics) 166
different LDAP server, entering 60
disclaimer
creating 317
disclaimer,
deleting 321
editing 321
displaying
encryption method in the subject, *See* subject tagging (Email Encryption)
downloading
certificate 110

E

editing
signature 321
email,
filtering by type (Email Live Tracking) 36
filtering per category (Email Live Tracking) 34
searching (Email Live Tracking) 34
selecting (Email Live Tracking) 44
email action
explanation (Email Live Tracking) 45
email archiving,
deactivating, *See* archiving, deactivating
setting up, *See* archiving, setting up
email categories
explanation (Control Panel) 390
email display,
explanation (Email Live Tracking) 29
opening (Email Live Tracking) 37
email field,
adjusting size (Email Live Tracking) 32
changing order (Email Live Tracking) 33
explanation (Email Live Tracking) 43
selecting (Email Live Tracking) 31
email information, adding (Whitelabeling) 387
EmiG 353
encryption capability, checking 352
encryption method in the subject, displaying, *See* subject tagging (Email Encryption)
encryption methods
explanation 353
encryption policy, creating 355
entering
different LDAP server 60
HTML source code (Signature & Disclaimer) 331
LDAP filter 62
LDAP server for Signature & Disclaimer 64, 315
entries, filtering 50
events, searching for (Auditing) 182
Ex Post Alerts (Advanced Threat Protection) 255
exception, creating, *See* encryption policy, creating
exceptions, adding (Control Panel) 349
exceptions, defining 211

exporting
    data as CSV (Hornetdrive) 373

F

fallback design (Whitelabeling) 387
favicon of the Control Panel, customizing (Whitelabeling) 379
field filter
    explanation (Email Live Tracking) 35
file type, *See* attachment
File type category 291
filling in
    onboarding form (365 Total Protection) 72
filter options
    explanation (Control Panel) 49
filter sequence (Compliance Filter) 299
filtering
    actions (Auditing) 183
    diagram (Email Statistics) 166
    email by type (Email Live Tracking) 36
    email per category (Email Live Tracking) 34
    event types (Auditing) 184
    statistics (Email Statistics) 166
filtering event types (Auditing) 184
filtering,
    entries 50
filters
    adding (Compliance Filter) 295
forbidding
    user actions 283

G

global data (Threat Live Report) 170
group
    adding to Content Control 285
group from TFFF group list
    removing 263
group settings
    explanation 200
grouping
    URLs (Web Filter) 192

H

hierarchy (Black & White Lists), *See* order (Black & White Lists)
HTML source code, entering (Signature & Disclaimer) 331

I

If Not Empty function, using (Signature & Disclaimer) 326
importing
    certificate in MacOS 119
    certificate in Windows 113

including
subsignature 329
individual mailboxes
activating 106
Initiating an ATP Scan Manually (Advanced Threat Protection) 38, 264
internal emails, archiving via Hornetsecurity (365 Total Protection) 82
internet access, limiting 204
IP address range, limiting 57

J

journal rule, creating (365 Total Protection) 87
journaling for archiving internal emails (365 Total Protection) 87

K

keywords in the subject, using 367

L

LDAP connection
activating 55
LDAP connection,
protecting 57
LDAP filter, entering 62
LDAP server, adding, *See* LDAP connection activating
LDAP server, entering for Signature & Disclaimer 64, 315
LDAP settings, configuring 58
limiting
internet access 204
IP address range 57
search (Email Live Tracking) 35
link, creating, *See* onboarding link, creating (365 Total Protection)
live attack overview (Threat Live Report) 171
location, changing (Control Panel) 18
location, location (Control Panel) 18
locking
website 196
login
Control Panel 12
login, configuring 58
logo of the Control Panel, customizing (Whitelabeling) 379

M

mail flow scenario, creating (365 Total Protection), *See* Archiving of internal emails via Hornetsecurity, configuring (365 Total Protection)
managing
applications 204
misconfiguration (Whitelabeling), *See* fallback design (Whitelabeling)
MX record, setting (365 Total Protection) 80

O

offboarding (365 Total Protection) 98

onboarding
customer (365 Total Protection), *See* creating customer (365 Total Protection)
onboarding form, filling in (365 Total Protection) 72
onboarding link, creating (365 Total Protection) 70
opening
account details (Hornetdrive) 375
email display (Email Live Tracking) 37
user settings (Control Panel) 17
Version Information (Control Panel) 11
order (Black & White Lists) 249
order of encryption methods 354
ordering
certificate 361

P

password,
changing (Control Panel) 17
resetting (Control Panel) 15
period
selecting (Auditing) 186
period,
selecting (Threat Live Report) 170
prerequisites (Whitelabeling) 379
preview (Signature & Disclaimer) 332
priority (Black & White Lists), *See* order (Black & White Lists)
processing hierarchy (Black & White Lists), *See* order (Black & White Lists)
processing of encryption methods, *See* order of encryption methods
protecting
LDAP connection 57

R

recipient of alerts (ATP)
adding 257
removing 258
regular expressions (Compliance Filter) 306
release request (Web Filter) 188
releasing
website 196
reminding
users 108
removing
group from TFFF group list 263
recipient of alerts (ATP) 258
reporting
website (Web Filter) 191
resetting
password (Control Panel) 15
Settings (Auditing) 186
role
selecting (Control Panel) 25
role assignment, adding 53
rules, defining (Compliance Filter) 296
Ruleset order (Spamfilter) 274, 312

S

S/MIME 353
search, limiting (Email Live Tracking) 35
search function (Email Live Tracking) 36
searching
    blacklist entry (Black & White Lists) 248
    email (Email Live Tracking) 34
    events (Auditing) 182
    whitelist entry (Black & White Lists) 248
searching field (Email Live Tracking) 34
selecting
    categories (Auditing) 181
    email (Email Live Tracking) 44
    email field (Email Live Tracking) 31
    period (Auditing) 186
    period (Threat Live Report) 170
    role (Control Panel) 25
    Websafe template 366
sequence of filtering (Compliance Filter), *See* filter sequence (Compliance Filter)
setting up
    archiving 348
    Content Control 287
    email archiving,, *See* setting up archiving
settings (Web Filter) 188
settings, resetting (Auditing) 186
signature
    creating 317
Signature & Disclaimer, activating 64, 315, 317
signature,
    deleting 321
    editing 321
Spam Report
    activating 267
    configuring 268, 270
    deactivating 272
    settings 267
SPF record, configuring (365 Total Protection) 79
starting
    ATP scan (Advanced Threat Protection) 38, 264
statistics,
    email by time (Email Statistics) 168
    email per user (Email Statistics) 168
    filtering (Email Statistics) 166
subject tagging (Email Encryption) 354
subsignature, including 329
support information, adding (Whitelabeling) 389
synchronizing
    users 60
System Requirements (Control Panel) 10

T

theme of the Control Panel, customizing (Whitelabeling) 379
threat statistics
    per attack type (Threat Live Report) 173

per attackvector (Threat Live Report) 173
TLS 353
troubleshooting (Signature & Disclaimer)
missing HTML signature 342
variables not referenced 341

U

upgrading
account (Hornetdrive) 370
URL,
grouping (Web Filter) 192
URL
of the Control Panel, customizing (Whitelabeling) 379
URL Rewriting
activating 260
URL rewriting statistics
per device (Threat Live Report) 176
per operating system (Threat Live Report) 176
per time (Threat Live Report) 175
user actions
allowing 283
forbidding 283
user settings,
opening (Control Panel) 17
users, reminding 108
users, synchronizing 60
using
If Not Empty function (Signature & Disclaimer) 326
keywords in the subject, using 367

V

version information (Control Panel) 10
version information, opening (Control Panel) 11
version number, *See* version information (Control Panel)
viewing
ATP Report (Advanced Threat Protection) 38, 264

W

Web Filter categories,
defining for a group 207
Web Filter login via LDAP, configuring 62
Web Filter statistics 211
Web Filter,
activating 197
configuring 197
Websafe 353
Websafe,
activating by keyword in subject 365
configuring for a specific communication partner 364
configuring for outgoing emails 364
explanation 363
Websafe template, selecting 366

website,
locking 196
releasing 196
reporting (Web Filter) 191
whitelist entry
create (Black & White Lists) 245
deleting (Black & White Lists) 247
searching (Black & White Lists) 248
WYSIWYG editor (Signature & Disclaimer) 322

Hornetsecurity GmbH
Am Listholze 78 | 30177 Hannover | Germany
Phone:+49 511 515 464-0 | info@hornetsecurity.com
www.hornetsecurity.com