Compliance Filter

Contents

Language and Icons Used in the Documentation

Gender Equality

For better readability, the generic masculine form is used in this documentation. Nevertheless, the information refers to members of all genders.

Used symbols

The following symbols are used to improve the recognizability of relevant steps within instructional chapters:

SYMBOL	DESCRIPTION	EXPLANATION
☑	Prerequisites	Condition that must be fulfilled before performing the next step
➜	Interim result	Result that is reached after executing a step
✓	Final result	Result that is reached after the described order of steps

Safety instructions and warnings

Warnings and safety instructions are used to inform the user about residual risks and dangers and how to avoid them with the recommended procedure. Following safety instructions and warnings are used in this documentation:

SYMBOL	DESCRIPTION	EXPLANATION
ℹ	NOTE	Further information within a given paragraph that is relevant for the execution of later steps.
ℹ	TIP	Note about configuration options.

SYMBOL	DESCRIPTION	EXPLANATION
!	IMPORTANT	Warning containing information about restrictions or important configuration options of a service.
⚠	ATTENTION	Warning about additional costs that may be incurred depending on the booked services.
❗	WARNING	Warning about a potential loss of data.
⚠	DANGER	Warning about a potential system infection with malware.

About the Compliance Filter

With the Compliance Filter, customer-level administrators can define their own filter rules, for example, to classify incoming emails as **Clean**, **Spam** or **Threat** (see "Email Categories" in the Control Panel manual). Furthermore, emails can be rejected, redirected through a different server or forwarded to other recipients. For the ranking of the filter rules of the Compliance Filter in the rule order of all our services, see Order of Rules Across All Services on page 8

CAUTION:

Incorrect filter rules have a negative impact on the email traffic and can override our services.

The Compliance Filter is not designed to rewrite addresses.

The Compliance Filter can check both incoming and outgoing emails. After the activation of the Compliance Filter (see Activating Compliance Filter on page 10), customer-level administrators can define filter rules of the following types:

- **Header**
- **Body**
- **Advanced**

Regular expressions can be used in the conditions of the filter rules (see Regular Expressions on page 60). Customer-level administrators assign an action to each filter rule. This action is automatically applied to the emails that match the filter rule. For more information on filter rules, see Filter Rules on page 11. In total, up to 1500 filter rules can be defined per customer.

Besides filter rules for individual expressions, more complex and precise filter rules can be created using dictionaries, each of which may contain up to 15000 literal expressions or up to 1000 regular expressions (see Dictionaries on page 51). Customer-level administrators can create and maintain up to 250 dictionaries for their primary domain. Dictionaries with regular expressions in particular significantly reduce the effort required to create and maintain filter rules.

In order to activate and configure the Compliance Filter for a domain, Spam and Malware Protection (see "Spam and Malware Protection" in the Control Panel manual) must be activated for the domain.Once Spam and Malware Protection is deactivated, the Compliance Filter is also deactivated and can no longer be configured.

Customer-level administrators can deactivate the Compliance Filter if they no longer want to use it (see Deactivating Compliance Filter on page 74).

Order of Rules Across All Services

The rules of Spam and Malware Protection (see "Spam and Malware Protection" in the Control Panel manual) are processed according to specific priorities. Once a rule with a higher priority applies, no rules with lower priorities are processed. This can lead to emails being blocked despite an allow list entry having been set for its sender's address because the IPv4 address of the sending server is on the RBL deny list.

Rule order (from top to bottom in descending priority):

Incoming emails

1. RBL list (block)
2. Mass spam detection (block)
3. Compliance Filter
4. Check for malicious content (quarantine)
5. Content Control if activated (quarantine)
6. User-based allow list (deliver)
7. User-based deny list (quarantine)
8. Administrative allow list (deliver)

    Notice:

    The administrative allow list is a special case among the rules. This is because administrators can select which filters will be bypassed by allow list entries at domain level (see "Creating a Deny List Entry for a Domain" in the Control Panel manual). While being processed, the affected emails thus skip the selected filters. This also applies to filters that are listed before the administrative allow list. The position where the administrative allow list is placed in the list refers to the default configuration of allow list entries at domain level. By default, the entries only bypass spam filtering.

9. Administrative deny list (quarantine)

10. General allow list (deliver)

11. General spam rules (quarantine)

12. Infomail filter (quarantine)

Notice:

The Compliance Filter (see About the Compliance Filter on page 6) is applied before Content Control (see About Content Control). This allows administrators to create exceptions for Content Control with filter rules of the Compliance Filter that categorize emails as **Clean**.

For Content Control, exceptions can neither be created using user-based allow and deny lists nor administrative deny lists because these rules are applied after Content Control. Only administrative allow lists can be used to bypass Content Control.

Outgoing emails

1. RBL list

2. Compliance Filter

3. Check for malicious content

4. Content Control if activated

Activating Compliance Filter

You have activated Spam and Malware Protection for the domain (see "Activating Spam and Malware Protection" in the Control Panel manual) for which you would like to activate the Compliance Filter.

In the **Security Settings** > **Compliance Filter** module, you can activate the Compliance Filter to create your own rules for filtering emails (see Filter Rules on page 11).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to activate the Compliance Filter.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Toggle the **Activate Compliance Filter** switch.

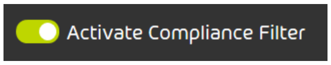


Figure 1: Activating Compliance Filter

The Compliance Filter is activated.

The Compliance Filter has been activated. Once filter rules have been created, the Compliance Filter can be used.

Next, you can create filter rules (see Filter Rules on page 11) and dictionaries (see Dictionaries on page 51) for the Compliance Filter.

Filter Rules

The Compliance Filter checks the emails of a domain. In the **Compliance Filter** module, customer-level administrators can manage filter rules for incoming and outgoing emails. Administrators can create filter rules for incoming (see Creating a Filter Rule for Incoming Emails on page 12) and outgoing emails (see Creating a Filter Rule for Outgoing Emails on page 18). The created filter rules are displayed in two tables (see Display of Filter Rules on page 25).

Notice:

Up to 1500 filter rules can be created for a primary domain.

Customer-level administrators can select an action (see Actions in Filter Rules on page 27) for each filter rule. The action is performed once an email matches the filter rule.

Customer-level administrators also select a type (see Types of Filter Rules on page 30) for each filter rule. The type of the filter rule determines to which emails the filter rule applies.

One of the possible conditions for filter rules regards the recipients to whom an email is sent. If an email is sent to multiple recipients and a filter rule applies to some of them, the action only affects the delivery of the email to the recipients to which the filter rule applies. Thus, different actions can be performed for different recipients of the same email.

Customer-level administrators can edit filter rules at a later stage (see Editing a Filter Rule on page 36). Furthermore, administrators can change the priorities of the filter rules (see Changing the Priority of a Filter Rule on page 38). The priority affects the order in which the filter rules of the Compliance Filter are processed. For more information on the order of the filter rules of the Compliance Filter, see Order of Filter Rules on page 40.

If a filter rule shall be temporarily suspended, customer-level administrators can deactivate it (see Deactivating a Filter Rule of the Compliance Filter on page 48). Deactivated filter rules can be reactivated later (see Activating a Filter Rule on page 47).

Once a filter rule is no longer required, customer-level administrators can delete the filter rule (see Deleting a Filter Rule of the Compliance Filter on page 49).

Creating a Filter Rule for Incoming Emails

✓ You have activated the Compliance Filter for the selected domain (see Activating Compliance Filter on page 10).

In the **Security Settings** > **Compliance Filter** module, you can create filter rules of the Compliance Filter (see About the Compliance Filter on page 6) for incoming emails.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to create the filter rule.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Select the **Rules** tab.
5. Click on **Add rule** under **Rules for incoming emails**.

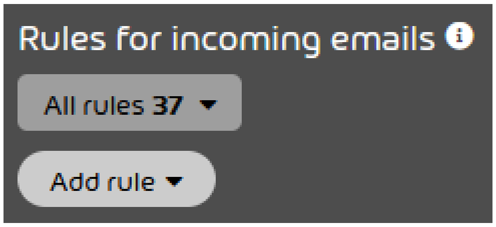


Figure 2: Add a rule

6. Under **Action**, select what shall happen to the emails that match the filter rule. You can choose from the following actions:

   - **Reject**
   - **Change recipient**
   - **Reroute**
   - **Add BCC**
   - **Tag as 'Clean'**
   - **Tag as 'Spam'**
   - **Tag as 'Threat'**

Notice:

For an overview of the actions, see Actions in Filter Rules on page 27.

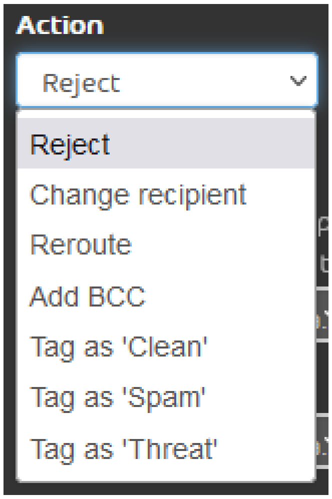


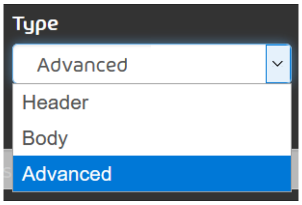
Figure 3: Select action

If the selected action requires additional information, an additional field appears under the drop-down menu. For more information about the additional fields of the actions, see Actions in Filter Rules on page 27.

7. Select the type of the filter rule under **Conditions**. You have the following options:

   - **Header**: The filter rule matches all emails with a header that contains a specified search term.
   - **Body**: The filter rule matches all emails with a body that contains a specified search term.
   - **Advanced**: You can specify the sender, the recipient, the IPv4 address and the hostname for the emails. You can also define search terms for the subject and attachment of the emails and a maximum email size. The filter rule matches all emails with the defined properties.

> **Notice:**
>
> The type of the filter rule determines to which emails the filter rule shall apply.



Type

Advanced

Figure 4: Select the type of the filter rule

Under the drop-down menu, fields for the configuration of the filter rule are displayed. The selected filter rule type determines which fields are displayed.

> **Notice:**
>
> Under Types of Filter Rules on page 30, you can find an overview and explanations of the fields that are available for each filter rule type.

8. If you have selected the **Advanced** type, follow the following steps:

   a) Under **Conditions**, select the logical operator between the conditions to which the filter rule shall apply. You have the following options:

   - **Match all conditions**: All selected conditions must match in order for the filter rule to be applied to an email. This relation corresponds to a logical AND operation.
   - **Match any condition** : It suffices that one of the selected conditions matches for the filter rule to be applied to an email. This relation corresponds to a logical OR operation.

   b) Tick the checkboxes of the conditions that shall apply to the filter rule.

   ➔

   The input fields of the selected conditions are enabled.

   c) If the input field of the selected condition contains a drop-down menu, select which type of data you would like to enter. You have the following options:

   - **Literal / regular expression**: The entered value is interpreted as a literal or a regular expression.
   - **Contained in dictionary**: The entered value is interpreted as the name of a dictionary (see Dictionaries on page 51) that is referenced in the condition. The condition is fulfilled if the corresponding value of the email matches an entry from the referenced dictionary.
   - **Not contained in dictionary**: The entered value is interpreted as the name of a dictionary (see Dictionaries on page 51) that is referenced in the condition. The

condition is fulfilled if the corresponding value of the email does not match any entry from the referenced dictionary.

d) If you have selected the conditions **Sender** or **Recipient**, select to which field of the email the entered value shall refer. You have the following options:

- **According to envelope**: The entered value must match the address that has been passed as the parameter of **MAIL FROM:** (sender address) or **RCPT TO:** (recipient address) during the email transfer.
- **According to header**: The entered value must match the address that has been passed in the field **From** (sender address) or **To** in the header of the email.
- **According to both**: The entered sender address must either be given as a parameter of **MAIL FROM:** or in the field **From** in the header of the email. The entered recipient address must either be given as a parameter of **RCPT TO:** or in the field **To** in the header of the email.

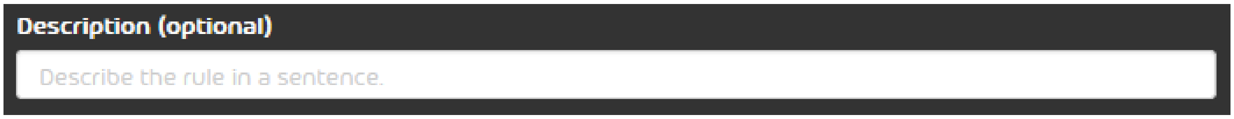
9. Depending on the input type, enter a search term, a value or the name of a directory in the input fields of the conditions

> **Notice:**
>
> A search term is found as a literal or a regular expression even if it is surrounded by text.

> **Notice:**
>
> To define more accurate and flexible rules, you can use regular expressions. For a description of the structure and functionality of regular expressions, see Regular Expressions on page 60 and Explanation of Regular Expressions on page 61. Under Exceptions to Regular Expressions on page 69, you will find an overview of unsupported characters.
>
> Regular expressions can only be used in rules of type **Advanced**.

> **Notice:**
>
> In the field **Larger than**, enter the maximum email size in megabytes.

10. Optional: Enter a description of the filter rule under **Description (optional)**.

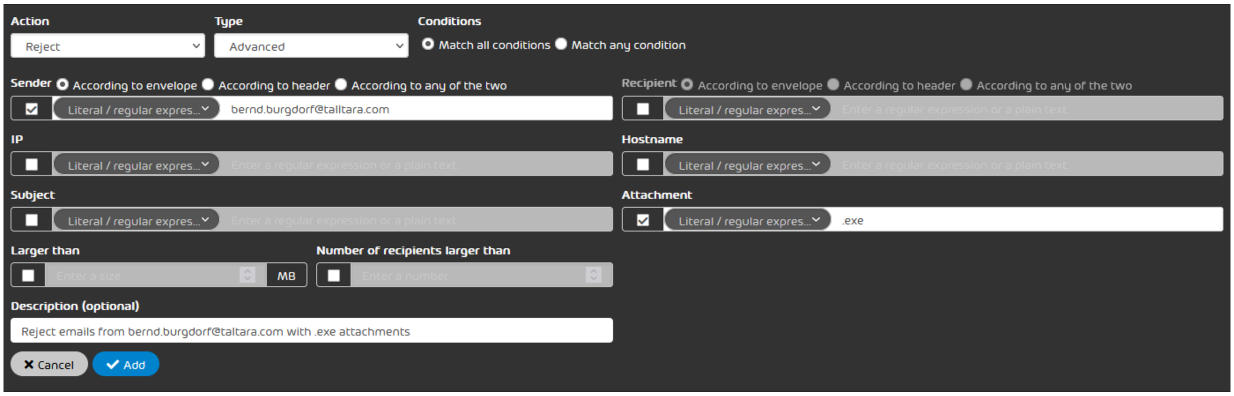


Description (optional)

Describe the rule in a sentence.

Figure 5: Describe filter rule

11. Click on **Add**.



Action: Reject

Type: Advanced

Conditions: ● Match all conditions ○ Match any condition

Sender ● According to envelope ○ According to header ○ According to any of the two

☑ Literal / regular expres... bernd.burgdorf@talltara.com

Recipient ● According to envelope ○ According to header ○ According to any of the two

□ Literal / regular expres... Enter a regular expression or a plain text.

IP

□ Literal / regular expres... Enter a regular expression or a plain text.

Hostname

□ Literal / regular expres... Enter a regular expression or a plain text.

Subject

□ Literal / regular expres... Enter a regular expression or a plain text.

Attachment

☑ Literal / regular expres... .exe

Larger than

□ Enter a size MB

Number of recipients larger than

□ Enter a number

Description (optional)

Reject emails from bernd.burgdorf@taltara.com with .exe attachments

Figure 6: Add filter rule

The filter rule is added to the table under **Rules for incoming emails** (see Display of Filter Rules on page 25). The filter rule is assigned the lowest priority of all existing filter rules and is placed at the end of the table. The filter rule is activated.

A filter rule for incoming emails has been created.

Next, you can edit the filter rule (see Editing a Filter Rule on page 36), change the priority of the filter rule (see Changing the Priority of a Filter Rule on page 38), temporarily deactivate the filter rule (see Deactivating a Filter Rule of the Compliance Filter on page 48) or delete it (see Deleting a Filter Rule of the Compliance Filter on page 49).

Creating a Filter Rule for Outgoing Emails

You have activated the Compliance Filter for the selected domain (see Activating Compliance Filter on page 10).

In the **Security Settings** > **Compliance Filter** module, you can create filter rules of the Compliance Filter (see About the Compliance Filter on page 6) for outgoing emails.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to create the filter rule.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Select the tab **Rules**.
5. Click on **Add rule** under **Rules for outgoing emails**.

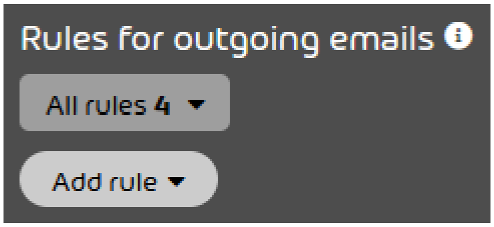


Figure 7: Add a rule

6. Under **Action**, select what shall happen to the emails that match the filter rule. You can choose from the following actions:

   - **Reject**
   - **Change recipient**
   - **Reroute**
   - **Add BCC**
   - **Notify sender**

Notice:

For an overview of the actions, see Actions in Filter Rules on page 27.

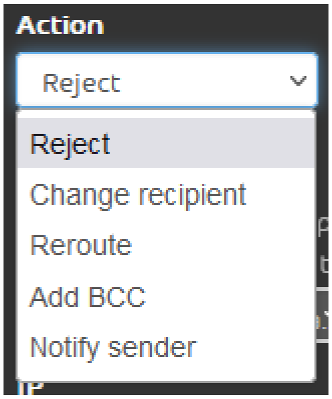


Figure 8: Select action

➔

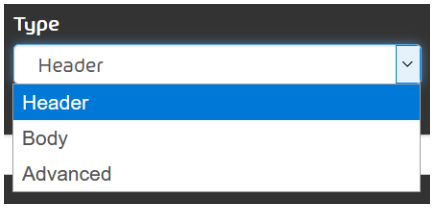
If the selected action requires additional information, an additional field appears under the drop-down menu. For more information about the additional fields of the actions, see Actions in Filter Rules on page 27.

7. Select the type of the filter rule under **Type**. It determines to which emails the filter rule shall apply. You have the following options:

   - **Header**: The filter rule matches all emails with a header that contains a specified search term.
   - **Body**: The filter rule matches all emails with a body that contains a specified search term.
   - **Advanced**: You can specify the sender, the recipient, the IPv4 address and the hostname for the emails. You can also define search terms for the subject and attachment of the emails and a maximum email size. The filter rule matches all emails with the defined properties.

Notice:

The type of the filter rule determines to which emails the filter rule shall apply.



Type

Figure 9: Select the type of the filter rule

➜

Under the drop-down menu, fields for the configuration of the filter rule are displayed. The selected filter rule type determines which fields are displayed.

Notice:

Under Types of Filter Rules on page 30, you can find an overview and explanations of the fields that are available for each filter rule type.

8. If you have selected the **Advanced** type, follow the following steps:

   a) Under **Conditions**, select the logical operator between the conditions to which the filter rule shall apply. You have the following options:

      - **Match all conditions**: All selected conditions must match in order for the filter rule to be applied to an email. This relation corresponds to a logical AND operation.
      - **Match any condition** : It suffices that one of the selected conditions matches for the filter rule to be applied to an email. This relation corresponds to a logical OR operation.

   b) Tick the checkboxes of the conditions that shall apply to the filter rule.

      ➔

      The input fields of the selected conditions are enabled.

   c) If the input field of the selected condition contains a drop-down menu, select which type of data you would like to enter. You have the following options:

      - **Literal / regular expression**: The entered value is interpreted as a literal or a regular expression.
      - **Contained in dictionary**: The entered value is interpreted as the name of a dictionary (see Dictionaries on page 51) that is referenced in the condition. The condition is fulfilled if the corresponding value of the email matches an entry from the referenced dictionary.
      - **Not contained in dictionary**: The entered value is interpreted as the name of a dictionary (see Dictionaries on page 51) that is referenced in the condition. The

condition is fulfilled if the corresponding value of the email does not match any entry from the referenced dictionary.

d) If you have selected the conditions **Sender** or **Recipient**, select to which field of the email the entered value shall refer. You have the following options:

- **According to envelope**: The entered value must match the address that has been passed as the parameter of **MAIL FROM:** (sender address) or **RCPT TO:** (recipient address) during the email transfer.
- **According to header**: The entered value must match the address that has been passed in the field **From** (sender address) or **To** in the header of the email.
- **According to both**: The entered sender address must either be given as a parameter of **MAIL FROM:** or in the field **From** in the header of the email. The entered recipient address must either be given as a parameter of **RCPT TO:** or in the field **To** in the header of the email.

9. Depending on the input type, enter a search term, a value or the name of a directory in the input fields of the conditions

Notice:

A search term is found as a literal or a regular expression even if it is surrounded by text.

Notice:

To define more accurate and flexible rules, you can use regular expressions. For a description of the structure and functionality of regular expressions, see Regular Expressions on page 60 and Explanation of Regular Expressions on page 61. Under Exceptions to Regular Expressions on page 69, you will find an overview of unsupported characters.

Regular expressions can only be used in rules of type **Advanced**.

Notice:

In the field **Larger than**, enter the maximum email size in megabytes.

10. Optional: Enter a description of the filter rule under **Description (optional)**.

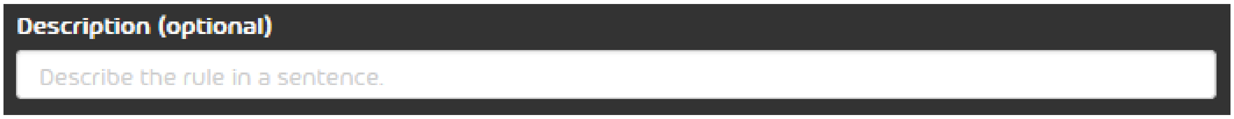
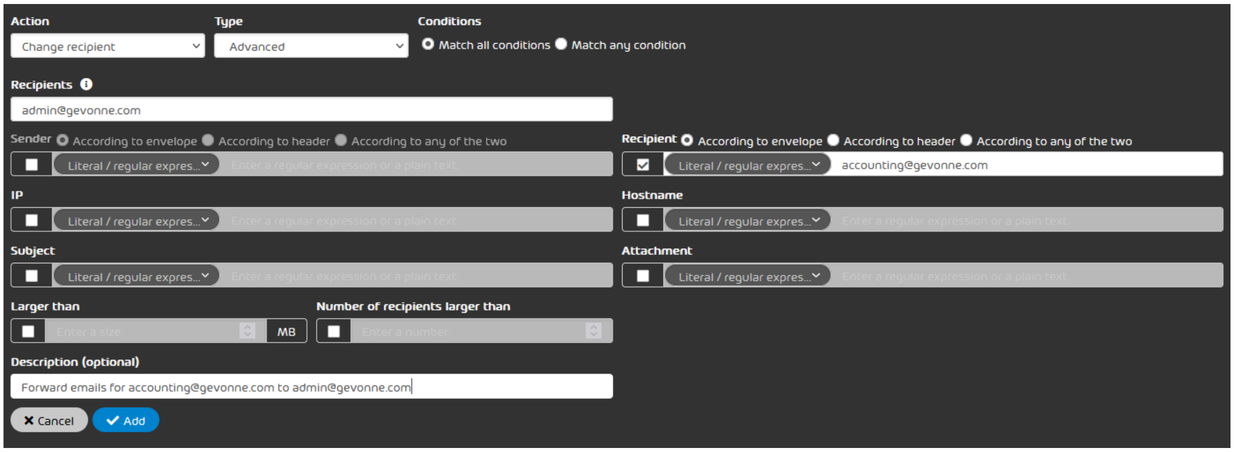


Figure 10: Describe filter rule

11. Click on **Add**.



Action: Change recipient

Type: Advanced

Conditions: ● Match all conditions ○ Match any condition

Recipients: admin@gevonne.com

Sender ● According to envelope ○ According to header ○ According to any of the two

□ Literal / regular expres...

Recipient ● According to envelope ○ According to header ○ According to any of the two

☑ Literal / regular expres... accounting@gevonne.com

IP □ Literal / regular expres...

Hostname □ Literal / regular expres...

Subject □ Literal / regular expres...

Attachment □ Literal / regular expres...

Larger than □ MB

Number of recipients larger than □

Description (optional): Forward emails for accounting@gevonne.com to admin@gevonne.com

Figure 11: Add filter rule

The filter rule is added to the table under **Rules for outgoing emails** (see Display of Filter Rules on page 25). The filter rule is assigned the lowest priority of all existing filter rules and is placed at the end of the table. The filter rule is activated.

A filter rule for outgoing emails has been created.

Next, you can edit the filter rule (see Editing a Filter Rule on page 36), change the priority of the filter rule (see Changing the Priority of a Filter Rule on page 38), temporarily deactivate the filter rule (see Deactivating a Filter Rule of the Compliance Filter on page 48) or delete it (see Deleting a Filter Rule of the Compliance Filter on page 49).

Display of Filter Rules

After filter rules for incoming and outgoing emails have been created, they will be displayed in the corresponding table in the sections **Rules for incoming emails** and **Rules for outgoing emails**.

Both tables contain the following columns:

- **Priority**: Application priority of the filter rule. A filter rule with a lower number in this field is applied before a filter rule with a higher number. The filter rules are sorted by their priority in descending order.
- **Active**: If the checkbox is ticked, this means that the filter rule is activated.
- **Action**: Here, the action is indicated that is performed by the filter rule.
  - Actions for incoming emails: **Change recipient**, **Reroute**, **Add BCC**, **Tag as 'Clean'**, **Tag as 'Spam'**, **Tag as 'Threat'**.
  - Actions for outgoing emails: **Reject**, **Change recipient**, **Reroute**, **Add BCC**, **Notify sender**.

Notice:

The available actions are described in chapter Actions in Filter Rules on page 27.

- **Type**: Here, the type of the filter rule is indicated.
- **Conditions**: Here, the filter conditions are indicated in the configured system language. If a dictionary is referenced in an advanced rule, this is indicated by the abbreviation **D**. In the following example, the rule takes into account senders from the dictionary **forbiddensenders**: **Sender: ?A=?D=forbiddensenders**. Furthermore, the entries of a dictionary can be negated. In the following example, the rule does not take into account senders from the dictionary **forbiddensenders**: **Sender: ?A=?D!=forbiddensenders**.

Note:

For the filter rules **Sender** and **Recipient**, the field or the fields to which the entered value refers is also indicated (**According to envelope**, **According to header** and **According to both** as described in chapter Types of Filter Rules on page 30). This is indicated by the abbreviations **E** (for **Envelope**), **H** (for **Header**) and **A** (for **Any**), regardless of the language.

For instance, **Sender:?E=miller@gevonne.com** would mean that a filter rule shall be applied to emails with the envelope sender **miller@gevonne.com**.

- **Description**: Description written by the creator of the filter rule.

- **ID**: Number that was automatically generated by the system to identify the filter rule.

Actions in Filter Rules

An action is assigned to each filter rule of the Compliance Filter (see About the Compliance Filter on page 6). Once an email matches the filter rule, this action is performed.

Different actions are available for incoming and outgoing emails.

The following actions are only available for incoming emails:

- **Tag as 'Clean'**
- **Tag as 'Spam'**
- **Tag as 'Threat'**

The action **Notify sender** is only available for outgoing emails.

The following table describes all actions for filter rules in the **Compliance Filter** module. If an action is selected that requires additional information in the **Compliance Filter** module, an additional field is displayed for the action. These fields are also described in the table.

Table 1: Actions for filter rules

ACTION	DESCRIPTION
Reject	**Attention:** The email is rejected. The sending email server is informed about the disconnection error with an error code and a text (**554 5.6.9 customer rule based reject by Compliance-Filter**). For more information, see "Classification reasons" in the Control Panel manual. The sending email server is in charge of notifying the sender.
Change recipient	The email is delivered to one or more other email addresses instead of the original recipient. If this action is selected, the **Send email to:** field is displayed. Customer-level administrators must enter all email addresses the email shall be forwarded to in this field. Administrators can enter as many email addresses as needed in the field. If multiple email addresses are entered, they must be separated from each other with semicolons.

ACTION	DESCRIPTION
Reroute	The email is redirected through another IPv4 address or hostname. If this action is selected, the **IP or hostname** field is displayed. Customer-level administrators must enter the IPv4 address or the hostname through which the email shall be redirected in this field. Administrators can only enter one IPv4 address or one hostname.
Add BCC	One or more BCC recipients are automatically added to the email. If this action is selected, the **Send email to:** field is displayed. Customer-level administrators must enter the email addresses to which blind copies of the email shall be sent in this field. Administrators can enter as many email addresses as needed in the field. If multiple email addresses are entered, they must be separated from each other with semicolons.
Notify sender	The sender of the email is automatically notified once the outgoing email has been accepted by the destination server.
Tag as 'Clean'	The incoming email is classified as **Clean**.
Tag as 'Spam'	The incoming email is classified as **Spam**.
Tag as 'Threat'	The incoming email is classified as **Threat**.

Types of Filter Rules

When creating filter rules in the **Compliance Filter** module (see About the Compliance Filter on page 6), customer-level administrators can select a type for the filter rule. With the type of the filter rule, administrators define the properties of the emails the rule should be applied to. In the **Compliance Filter** module, fields for different properties are displayed for each filter rule type.

The following tables give an overview of the fields that are available for each filter rule type. The tables contain descriptions of the properties and examples for possible input.

Notice:

To define more accurate and flexible rules, regular expressions can be used. For a description of the structure and functionality of regular expressions, see Regular Expressions on page 60 and Explanation of Regular Expressions on page 61. For an overview of all unsupported characters, see Exceptions to Regular Expressions on page 69.

Notice:

In order to manage conditions more easily, customer-level administrators can collect multiple expressions in dictionaries. Dictionaries can be referenced in the input fields of filter rule conditions. For more information on the functions, the creation and the management of dictionaries, see Dictionaries on page 51.

Table 2: Type Header

FIELD	DESCRIPTION	EXAMPLE FOR INPUT
Filter: header	The header of the email is searched for the entered search term.	Invoice

Table 3: Type Body

FIELD	DESCRIPTION	EXAMPLE FOR INPUT
Filter: body	The decoded body of the email is searched for the entered search term. **Notice:** Attachments are excluded from the search in the email body.	Payment order

Table 4: Type Advanced

FIELD	DESCRIPTION	EXAMPLE FOR INPUT
Sender	The sender address of the email is searched for the entered search term or for the entries in the referenced dictionary (see Dictionaries on page 51). **Notice:** Customer-level administrators have the following options to select which type of sender address is searched (see Creating a Filter Rule for Incoming Emails): • **According to envelope**: Sender address from the envelope (**MAIL FROM:**) • **According to header**: Sender address from the header (**To:**) • **According to both**: any of the two sender addresses	**user@gevonne.com**

FIELD	DESCRIPTION	EXAMPLE FOR INPUT
Recipient	The recipient addresses are searched for the entered search term or for the entries in the referenced dictionary. **Notice:** Customer-level administrators have the following options to select which type of recipient address is searched (see Creating a Filter Rule for Incoming Emails): • **According to envelope**: Recipient address from the envelope (**RCPT TO:**) • **According to header**: Recipient address from the header (**From:**) • **According to both**: any of the two recipient addresses **Notice:** If an email is sent to multiple recipients and a filter rule applies to some of them, the action only affects the	**user.extern@yahoo.com**

FIELD	DESCRIPTION	EXAMPLE FOR INPUT
IP	The public IPv4 address of the sending email server is searched for the entered search term or for the entries in the referenced dictionary. **Notice:** Enter the IPv4 address without the subnet mask as a search term.	Right: **0.0.0.0** Wrong: **0.0.0.0/24**
Hostname	The hostname (PTR record) obtained through a reverse lookup of the IPv4 address of the email server, is searched for the entered search term or for the entries in the referenced dictionary. Depending on whether the rule applies to incoming or outgoing emails, this is the hostname of the source server or the destination server,	**mailserver.domain.com**
Subject	The subject of the email is searched for the entered search term or for the entries in the referenced dictionary.	**Spam**

FIELD	DESCRIPTION	EXAMPLE FOR INPUT
Attachment	The file names and the file extensions of the email attachments are searched for the entered search term or for the entries in the referenced dictionary. ℹ **Notice:** It is possible to search for a file extension or for a part of the file name. To search for a file extension, the file extension must be entered as the search term. To search for a part of the file name, the part to be searched must be entered as the search term. ℹ **Notice:** The collective terms for attachments cannot be used for the Compliance Filter.	**.jpg** **express**

FIELD	DESCRIPTION	EXAMPLE FOR INPUT
Larger than	It is checked whether the email exceeds the entered size. **Notice:** The maximum email size is given in megabytes.	**500**
Number of recipients larger than	It is checked whether the number of recipients exceeds the entered size.	**10**

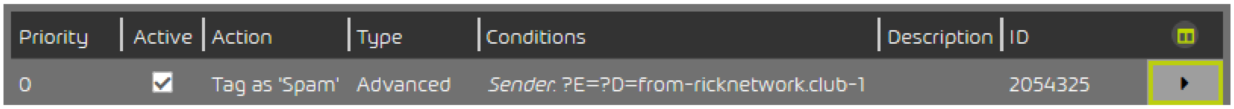
Editing a Filter Rule

You have activated the Compliance Filter for the selected domain (see Activating Compliance Filter on page 10) and have created filter rules for the Compliance Filter (see Creating a Filter Rule for Incoming Emails on page 12 or Creating a Filter Rule for Outgoing Emails on page 18)

In the **Security Settings** > **Compliance Filter** module, you can edit filter rules of the Compliance Filter (see About the Compliance Filter on page 6).

1. Log in to the Control Panel with your administrative credentials.
2. Select a domain from the scope selection.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Select the **Rules** tab.

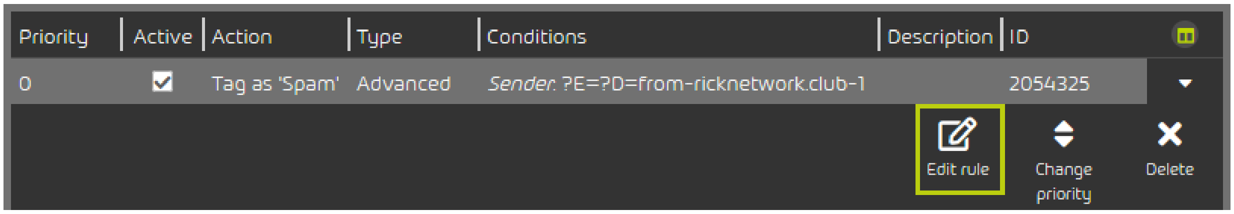
5. In the list of filter rules for incoming or outgoing emails, click on the menu arrow next to the filter rule you would like to edit.



Priority	Active	Action	Type	Conditions	Description	ID	
0	☑	Tag as 'Spam'	Advanced	*Sender:* ?E=?D=from-ricknetwork.club-1		2054325	▸

Figure 12: Open the menu

6. Click on **Edit rule**.



Priority	Active	Action	Type	Conditions	Description	ID	
0	☑	Tag as 'Spam'	Advanced	*Sender:* ?E=?D=from-ricknetwork.club-1		2054325	▾

Figure 13: Editing a Filter Rule

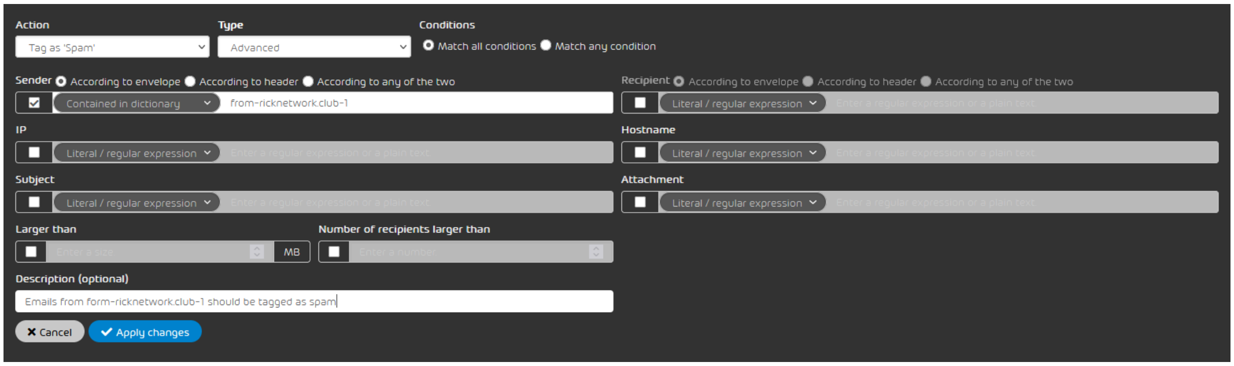
A menu with the current filter rule settings opens.

7. Edit the settings as desired.

Notice:

For more information, see Creating a Filter Rule for Incoming Emails on page 12 or Creating a Filter Rule for Outgoing Emails on page 18.

8. Click on **Apply changes**.



Action: Tag as 'Spam'

Type: Advanced

Conditions: ● Match all conditions ○ Match any condition

Sender ● According to envelope ○ According to header ○ According to any of the two

☑ Contained in dictionary: from-ricknetwork.club-1

Recipient ● According to envelope ○ According to header ○ According to any of the two

□ Literal / regular expression: Enter a regular expression or a plain text

IP

□ Literal / regular expression: Enter a regular expression or a plain text

Hostname

□ Literal / regular expression: Enter a regular expression or a plain text

Subject

□ Literal / regular expression: Enter a regular expression or a plain text

Attachment

□ Literal / regular expression: Enter a regular expression or a plain text

Larger than

□ Enter a size MB

Number of recipients larger than

□ Enter a number

Description (optional)

Emails from form-ricknetwork.club-1 should be tagged as spam

Figure 14: Apply changes

➜

The changes are applied.

✓

A filter rule has been edited.

Changing the Priority of a Filter Rule

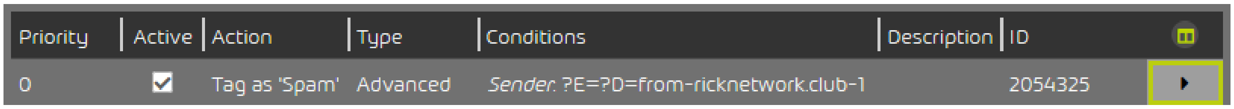
You have activated the Compliance Filter for the selected domain (see Activating Compliance Filter on page 10) and have created filter rules for the Compliance Filter (see Creating a Filter Rule for Incoming Emails on page 12 or Creating a Filter Rule for Outgoing Emails on page 18)

In the **Security Settings** > **Compliance Filter** module, you can change the order in which the filter rules of the Compliance Filter (see About the Compliance Filter on page 6) are processed. To change the order of the filter rules, change the priorities of the filter rules.

Important:

The order in which the filter rules of the Compliance Filter are processed depends not only on the priorities but also on the type of the filter rules (see Order of Filter Rules on page 40).

1. Log in to the Control Panel with your administrative credentials.
2. Select a domain from the scope selection.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Select the **Rules** tab.
5. In the list of filter rules for incoming or outgoing emails, click on the menu arrow next to the filter rule for which you would like to change the priority.

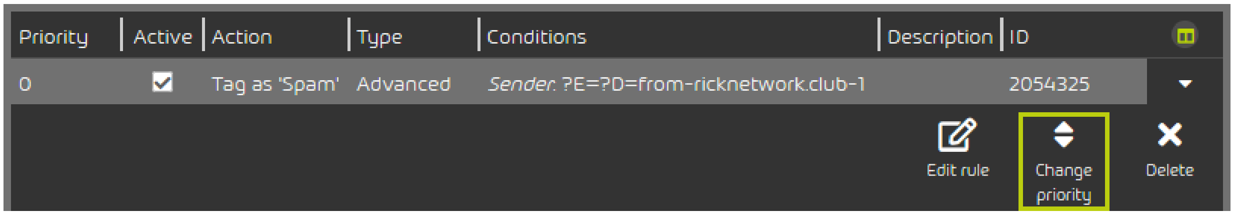


Priority	Active	Action	Type	Conditions	Description	ID
0	☑	Tag as 'Spam'	Advanced	*Sender:* ?E=?D=from-ricknetwork.club-1		2054325

Figure 15: Open the menu

A menu opens.

6. Click on **Change priority**.



Priority	Active	Action	Type	Conditions	Description	ID
0	☑	Tag as 'Spam'	Advanced	*Sender:* ?E=?D=from-ricknetwork.club-1		2054325

Figure 16: Change priority

A menu opens.

7. Enter the new priority of the filter rule under **Priority**.

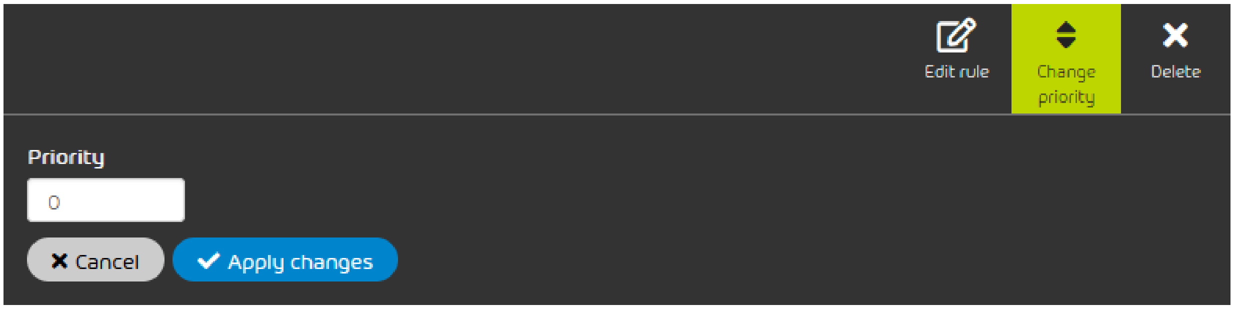


Figure 17: Enter priority

8. Click on **Apply changes**.

➜

The new priority is assigned to the filter rule. The filter rule will be moved to the position that complies with the new priority.

✓

The priority of a filter rule has been changed. Thus, the order in which the filter rules are processed has changed.

Order of Filter Rules

Important:

Please note how the Compliance Filter ranks in the order of our services (see Order of Rules Across All Services on page 8). Once a rule of one of the services matches an email, the processing of other rules is stopped. No other rules are applied to the email.

This order allows you to create exceptions for Content Control with filter rules of the Compliance Filter that categorize emails as **Clean**.

The filter rules of the Compliance Filter (see About the Compliance Filter on page 6) are processed according to their type (see Types of Filter Rules on page 30) in the following order:

1. Body
2. Header
3. Advanced

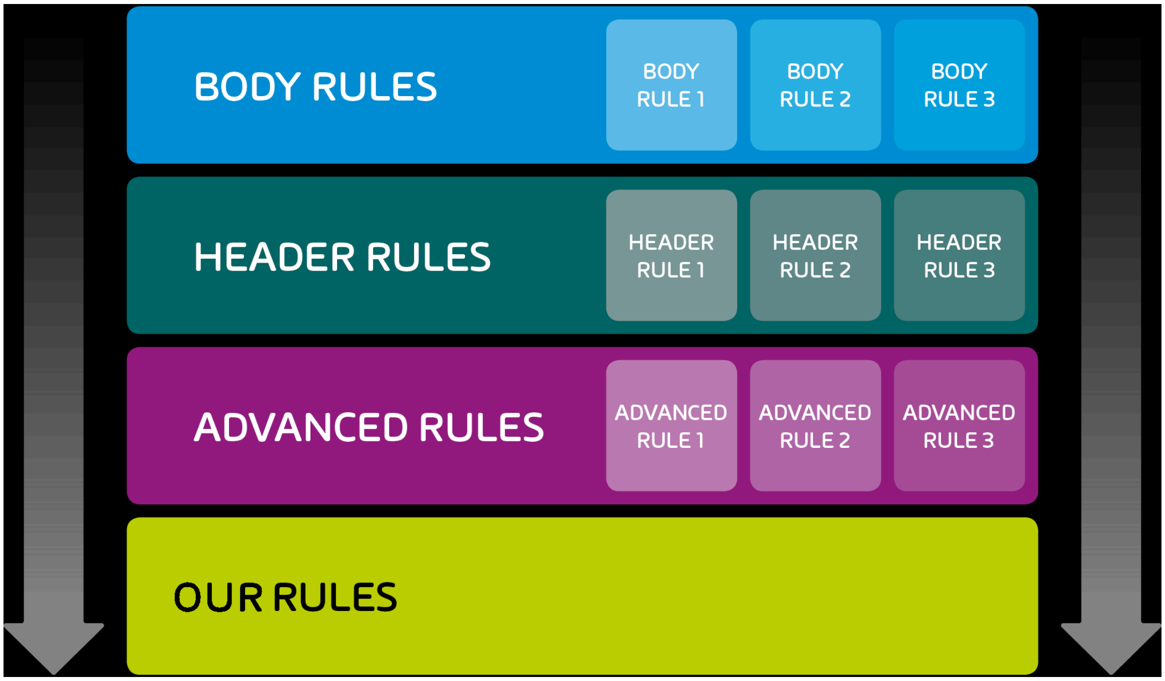


Figure 18: Order of filter rules by type

Filter rules of the same type are sorted according to their priority and processed in this order.

Notice:

The higher the number, the lower the priority of the filter rule.

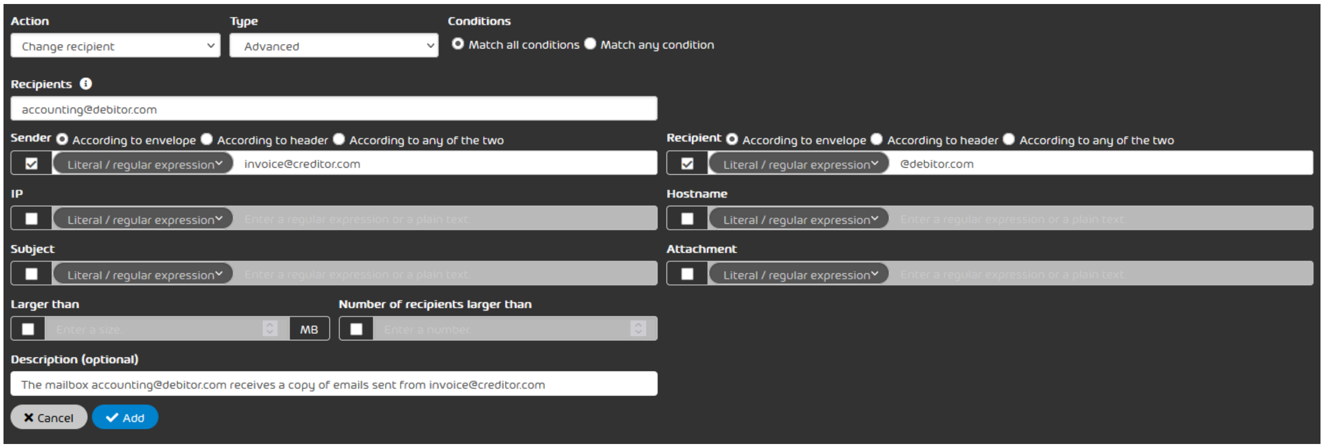
Customer-level administrators can change the priority of a filter rule (see Changing the Priority of a Filter Rule on page 38).

The following examples illustrate the order in which the rules are processed.

Simple processing of filter rules

Initial situation:

A customer-level administrator has defined filter rules for the Compliance Filter. No rules of other services apply to this case.



Action: Change recipient
Type: Advanced
Conditions: ○ Match all conditions ● Match any condition

Recipients: accounting@debitor.com

Sender ○ According to envelope ● According to header ● According to any of the two
☑ Literal / regular expression: invoice@creditor.com

Recipient ○ According to envelope ● According to header ● According to any of the two
☑ Literal / regular expression: @debitor.com

IP
□ Literal / regular expression: Enter a regular expression or a plain text

Hostname
□ Literal / regular expression: Enter a regular expression or a plain text

Subject
□ Literal / regular expression: Enter a regular expression or a plain text

Attachment
□ Literal / regular expression: Enter a regular expression or a plain text

Larger than
□ Enter a size MB

Number of recipients larger than
□ Enter a number

Description (optional): The mailbox accounting@debitor.com receives a copy of emails sent from invoice@creditor.com

Figure 19: Filter rule: Forward

Procedure:

1. An email from **invoice@creditor.com** is sent to any user of the domain debitor.com.

2. The Compliance Filter first searches the filter rules of the type **Body**, then the filter rules of the type **Header** and finds a match in the filter rules of the type **Advanced**.

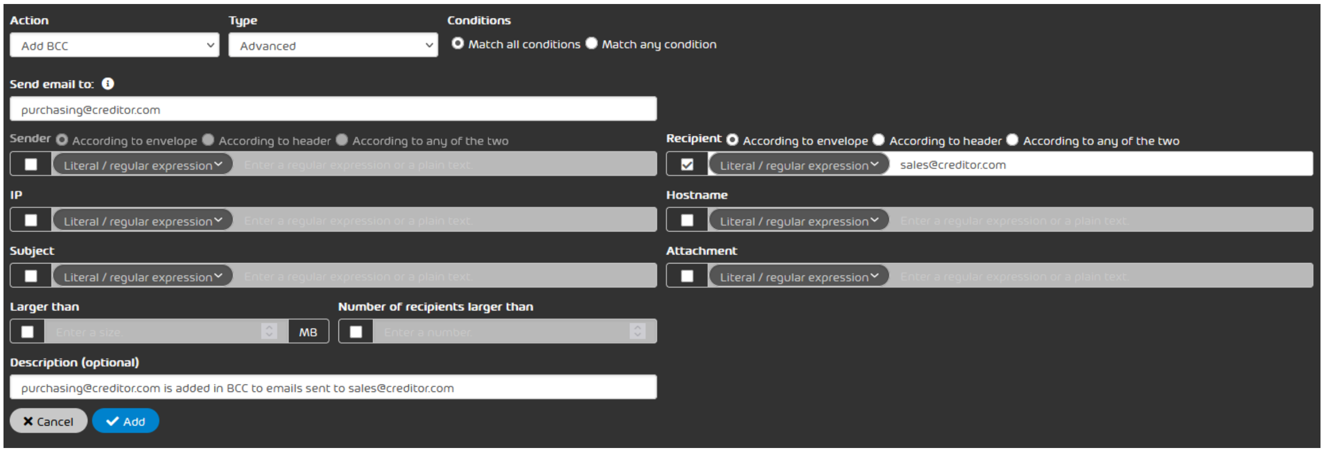
3. The filter rule is applied. The Compliance Filter does not search for any other matches in other filter rules.

Conflict between several filter rules of the same type

Initial situation:

A customer-level administrator has defined two different filter rules of the type **Advanced** for the Compliance Filter for the event that an outgoing email is sent to **sales@creditor.com**.

Both filter rules cause a BCC to be added to the email. For one filter rule the BCC recipient is **purchasing@creditor.com**, for the other one it is **ceo@creditor.com**. The filter rule with the BCC recipient **purchasing@creditor.com** has a higher priority than the filter rule with the BCC recipient **ceo@creditor.com**, and is listed above the other filter rule in the overview of filter rules. No other filter rules apply to this case.



Action: Add BCC
Type: Advanced
Conditions: ◉ Match all conditions ○ Match any condition

Send email to: purchasing@creditor.com

Sender ◉ According to envelope ○ According to header ○ According to any of the two
□ Literal / regular expression — Enter a regular expression or a plain text.

Recipient ◉ According to envelope ○ According to header ○ According to any of the two
☑ Literal / regular expression — sales@creditor.com

IP
□ Literal / regular expression — Enter a regular expression or a plain text.

Hostname
□ Literal / regular expression — Enter a regular expression or a plain text.

Subject
□ Literal / regular expression — Enter a regular expression or a plain text.

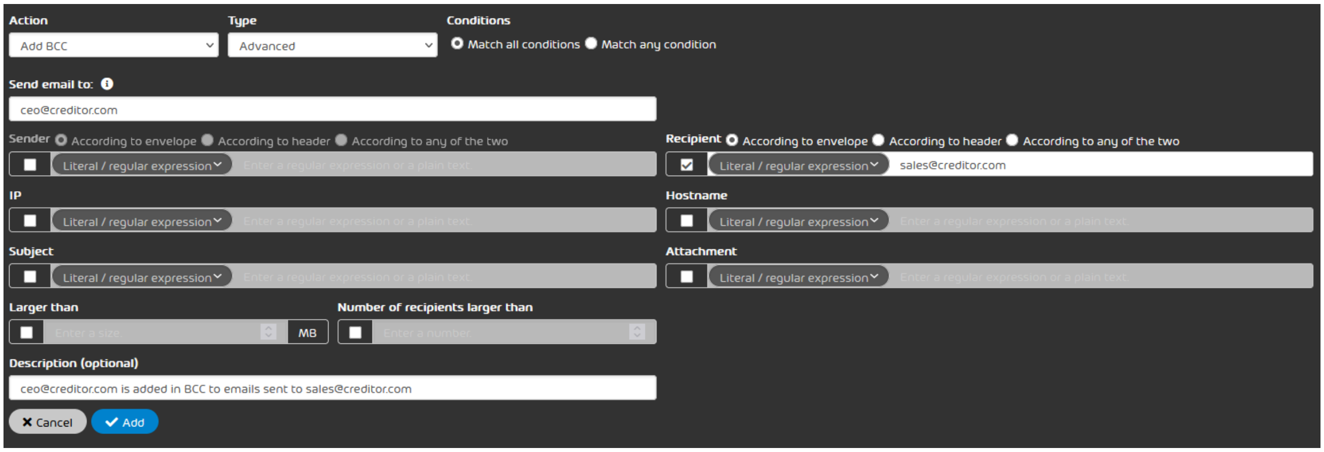
Attachment
□ Literal / regular expression — Enter a regular expression or a plain text.

Larger than
□ Enter a size MB

Number of recipients larger than
□ Enter a number

Description (optional)
purchasing@creditor.com is added in BCC to emails sent to sales@creditor.com

Figure 20: Filter rule: add purchasing@creditor.com as BCC recipient



Action: Add BCC
Type: Advanced
Conditions: ◉ Match all conditions ○ Match any condition

Send email to: ceo@creditor.com

Sender ◉ According to envelope ○ According to header ○ According to any of the two
□ Literal / regular expression — Enter a regular expression or a plain text.

Recipient ◉ According to envelope ○ According to header ○ According to any of the two
☑ Literal / regular expression — sales@creditor.com

IP
□ Literal / regular expression — Enter a regular expression or a plain text.

Hostname
□ Literal / regular expression — Enter a regular expression or a plain text.

Subject
□ Literal / regular expression — Enter a regular expression or a plain text.

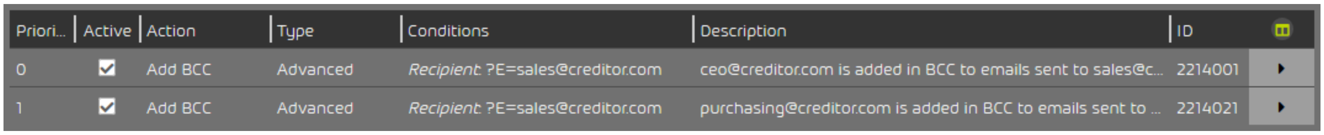
Attachment
□ Literal / regular expression — Enter a regular expression or a plain text.

Larger than
□ Enter a size MB

Number of recipients larger than
□ Enter a number

Description (optional)
ceo@creditor.com is added in BCC to emails sent to sales@creditor.com

Figure 21: Filter rule: add ceo@creditor.com as BCC recipient



Priori...	Active	Action	Type	Conditions	Description	ID	
0	☑	Add BCC	Advanced	*Recipient:* ?E=sales@creditor.com	ceo@creditor.com is added in BCC to emails sent to sales@c...	2214001	▸
1	☑	Add BCC	Advanced	*Recipient:* ?E=sales@creditor.com	purchasing@creditor.com is added in BCC to emails sent to ...	2214021	▸

Figure 22: Order of filter rules

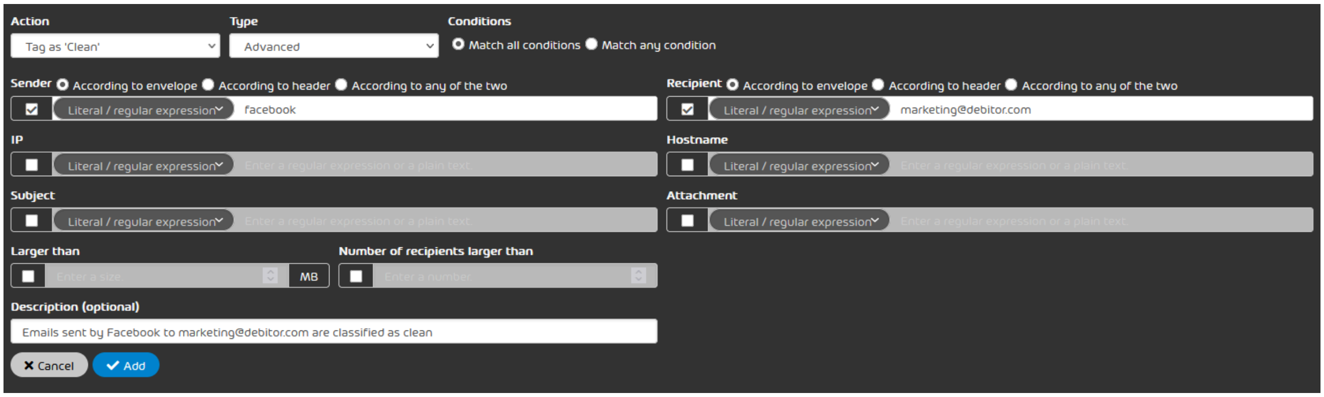
Procedure:

1. An email from any sender is sent to **sales@creditor.com**.
2. The Compliance Filter first searches the filter rules of the type **Body**, then the filter rules of the type **Header** and finds a match in the filter rules of the type **Advanced**.
3. The filter rule with the higher priority (BCC to **purchasing@creditor.com**) is applied. The Compliance Filter does not search for any other matches in other filter rules. The filter rule with the lower priority (BCC to **ceo@creditor.com**) is not applied.

Conflict between rules of different types

Initial situation:

A customer-level administrator has defined a filter rule establishing that incoming emails with a link to Facebook should be categorized as **Spam**. In another filter rule, the administrator had defined an exception for the recipient **marketing@debitor.com**. The exception defined by the administrator causes emails sent directly from Facebook to **marketing@debitor.com** to be categorized as **Clean**. The filter rule with the exception for **marketing@debitor.com** has a higher priority than the filter rule for emails with links to Facebook, and is listed above the other filter rule in the overview of filter rules. No other filter rules apply to this case.



Action: Tag as 'Clean'

Type: Advanced

Conditions: ◉ Match all conditions ○ Match any condition

Sender ◉ According to envelope ○ According to header ○ According to any of the two

☑ Literal / regular expression facebook

Recipient ◉ According to envelope ○ According to header ○ According to any of the two

☑ Literal / regular expression marketing@debitor.com

IP

☐ Literal / regular expression Enter a regular expression or a plain text.

Hostname

☐ Literal / regular expression Enter a regular expression or a plain text.

Subject

☐ Literal / regular expression Enter a regular expression or a plain text.

Attachment

☐ Literal / regular expression Enter a regular expression or a plain text.

Larger than

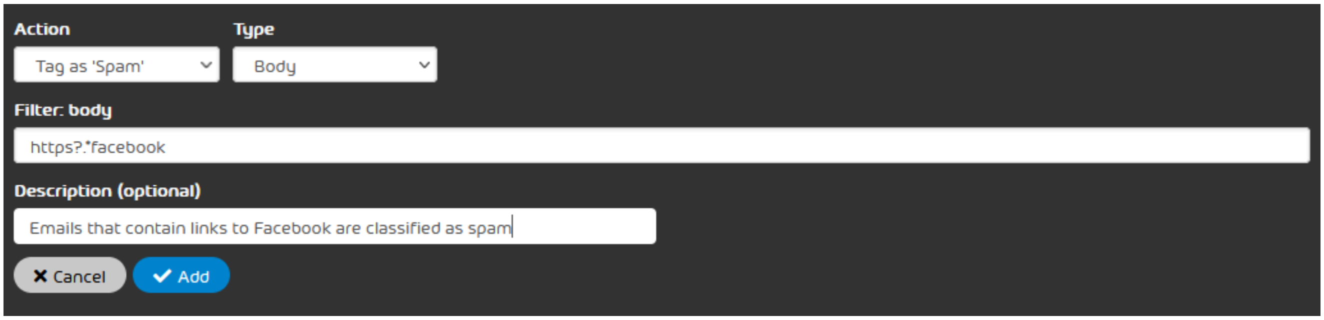
☐ Enter a size. MB

Number of recipients larger than

☐ Enter a number.

Description (optional): Emails sent by Facebook to marketing@debitor.com are classified as clean

Figure 23: Filter rule: Tag as clean



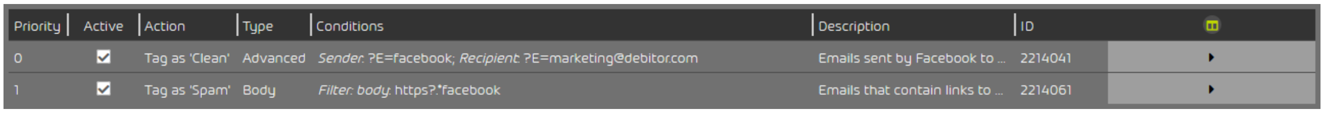
Action: Tag as 'Spam'

Type: Body

Filter: body: https?.*facebook

Description (optional): Emails that contain links to Facebook are classified as spam

Figure 24: Filter rule: Tag as spam



Priority	Active	Action	Type	Conditions	Description	ID	
0	☑	Tag as 'Clean'	Advanced	*Sender:* ?E=facebook; *Recipient:* ?E=marketing@debitor.com	Emails sent by Facebook to ...	2214041	▸
1	☑	Tag as 'Spam'	Body	*Filter: body:* https?.*facebook	Emails that contain links to ...	2214061	▸

Figure 25: Order of filter rules

Procedure:

1. Facebook sends an email with a link to **marketing@debitor.com**.

2. The Compliance Filter first searches the filter rules of the type **Body** and finds a match in the filter rule for emails that contain links to Facebook.

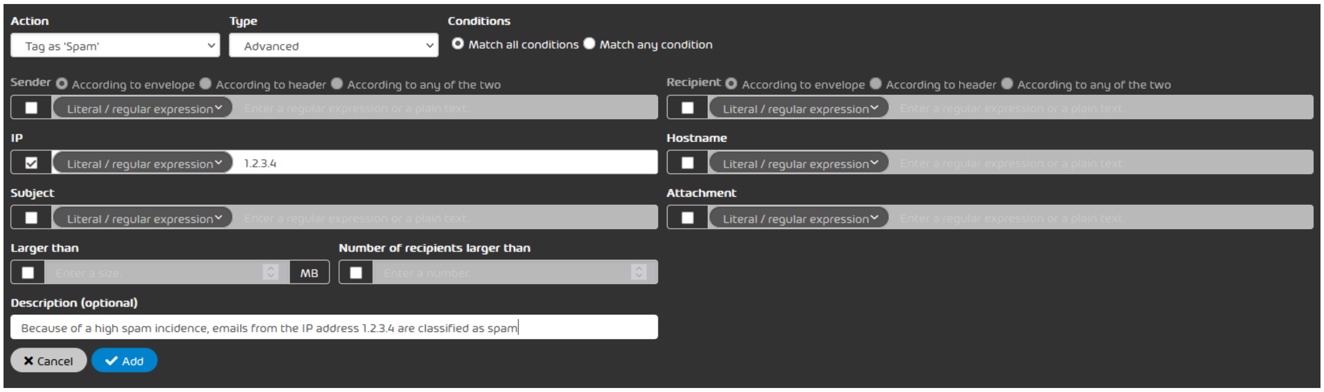
3. The filter rule is applied to the email and the email is categorized as **Spam**. The Compliance Filter does not search for any other matches in other filter rules. Despite its higher priority, the

filter rule with the exception for **marketing@debitor.com** is not applied because the filter rules of the type **Body** take precedence over the filter rules of other types.

Conflict between the Compliance Filter and our filter rules

Initial situation:

Due to a high spam volume from one IPv4 address, a customer-level administrator has defined a filter rule establishing that emails from this IP address should be tagged as spam. No other filter rules of the Compliance Filter apply to this case. In addition to the filter rule of the Compliance Filter, a filter rule defined by us applies to this case.



Action: Tag as 'Spam'

Type: Advanced

Conditions: ● Match all conditions ○ Match any condition

IP: ☑ Literal / regular expression 1.2.3.4

Description (optional): Because of a high spam incidence, emails from the IP address 1.2.3.4 are classified as spam

Sender ○ According to envelope ● According to header ● According to any of the two
□ Literal / regular expression
Enter a regular expression or a plain text.
Recipient ○ According to envelope ● According to header ● According to any of the two
Hostname
Subject
Attachment
Larger than
Enter a size.
MB
Number of recipients larger than
Enter a number.
✕ Cancel
✓ Add

Figure 26: Filter rule: Tag emails from an IPv4 address as spam

Procedure:

1. A sender from the domain behind the IPv4 address sends an email to any recipient.
2. The Compliance Filter first searches the filter rules of the type **Body**, then the filter rules of the type **Header** and finds a match in the filter rules of the type **Advanced**.
3. The filter rule is applied to the email and the email is categorized as **Spam**. The Compliance Filter does not search for any other matches in other filter rules.
4. We have already defined a more precise filter rule for this case. The high spam volume could be narrowed down to the sender **info@**. Other email addresses of the domain do not send any spam emails. Since our filter rules are not searched anymore, the filter rule defined by the

customer-level administrator, the scope of which is too extensive, is applied. A clean email could thus be tagged as spam.

Activating a Filter Rule

You have deactivated a filter rule of the Compliance Filter (see Deactivating a Filter Rule of the Compliance Filter on page 48).

If you would like to apply a deactivated rule of the Compliance Filter (see About the Compliance Filter on page 6) again, you can activate the filter rule in the **Security Settings** > **Compliance Filter** module.

1. Log in to the Control Panel with your administrative credentials.
2. Select a domain from the scope selection.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Select the **Rules** tab.
5. Select the desired filter rule from the list of filter rules for incoming or outgoing emails and activate the checkbox in the column **Active**.

Figure 27: Activate filter rule

The filter rule is activated. The filter rule is applied to the email traffic of the domain.

A filter rule of the Compliance Filter has been activated.

Deactivating a Filter Rule of the Compliance Filter

You have activated the Compliance Filter for the selected domain (see Activating Compliance Filter on page 10) and have created filter rules for the Compliance Filter (see Creating a Filter Rule for Incoming Emails on page 12 or Creating a Filter Rule for Outgoing Emails on page 18)

If you would like to temporarily suspend a filter rule of the Compliance Filter (see About the Compliance Filter on page 6), you can deactivate it in the **Security Settings** > **Compliance Filter** module.

1. Log in to the Control Panel with your administrative credentials.
2. Select a domain from the scope selection.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Select the **Rules** tab.
5. Select the desired rule from the list of filter rules for incoming or outgoing emails, and deactivate the checkbox in the column **Active**.

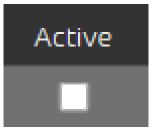


Figure 28: Deactivate the filter rule

The filter rule is deactivated. The filter rule is applied to the email traffic of the domain.

A filter rule of the Compliance Filter has been deactivated.

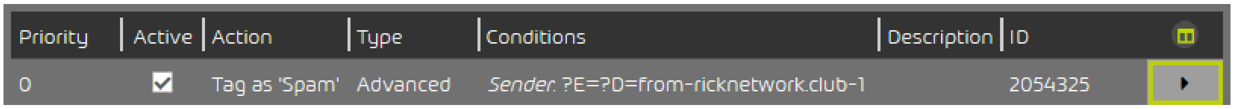
Next, you can reactivate the filter rule if it should be applied again (see Activating a Filter Rule on page 47).

Deleting a Filter Rule of the Compliance Filter

You have activated the Compliance Filter for the selected domain (see Activating Compliance Filter on page 10) and have created filter rules for the Compliance Filter (see Creating a Filter Rule for Incoming Emails on page 12 or Creating a Filter Rule for Outgoing Emails on page 18)

In the **Security Settings** > **Compliance Filter** module, you can delete filter rules of the Compliance Filter that you no longer need.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to delete a filter rule.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Select the **Rules** tab.
5. In the list of rules for incoming or outgoing emails, click on the menu arrow next to the filter rule you would like to delete.

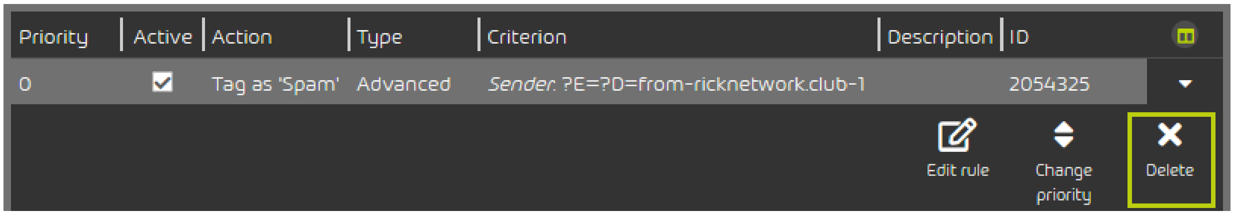


Priority	Active	Action	Type	Conditions	Description	ID	
0	☑	Tag as 'Spam'	Advanced	*Sender:* ?E=?D=from-ricknetwork.club-1		2054325	▸

Figure 29: Open the menu

A menu opens.

6. Click on **Delete**.

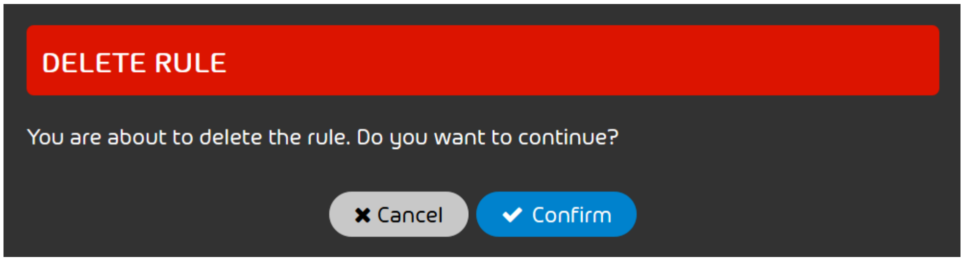


Priority	Active	Action	Type	Criterion	Description	ID
0	☑	Tag as 'Spam'	Advanced	*Sender*: ?E=?D=from-ricknetwork.club-1		2054325

Figure 30: Delete filter rule

A warning message is displayed.

7. Click on **Confirm**.



DELETE RULE

You are about to delete the rule. Do you want to continue?

Figure 31: Confirm deletion

The filter rule is deleted.

A filter rule of the Compliance Filter has been deleted.

Dictionaries

Dictionaries are sets of expressions that can be used to create filter rules in the **Security Settings** > **Compliance Filter** module (see About the Compliance Filter on page 6). The expressions of a dictionary can either all be interpreted as literal or as regular expressions. Regular expressions are more accurate and reduce the number of entries to be created and maintained.

Notice:

Up to 250 dictionaries can be created for a primary domain.

Dictionaries with regular expressions can contain up to 1000 entries whereas dictionaries with literal expressions can contain up to 15000 entries.

When creating filter rules of the type **Advanced** (see Creating a Filter Rule for Incoming Emails on page 12 or Creating a Filter Rule for Outgoing Emails on page 18), customer-level administrators can reference a dictionary in some conditions instead of entering a single expression. In order to reference an existing dictionary, administrators must enter the name of the dictionary in the input field of the condition and select from a drop-down menu how the expressions of the dictionary shall be interpreted by the filter rule. With the **Contained in dictionary** option, the filter rule applies if at least one expression from the dictionary matches an email. The expressions of the dictionary are thus logically linked with an OR within the condition. With the **Not contained in dictionary** option, the filter rule applies if no expression matches.

Dictionaries facilitate the creation of filter rules of the Compliance Filter because a single filter rule can apply to emails with different values for a condition. For instance, a single filter rule could mark emails from the senders **@facebook**, **@instagram** or **@tiktok** that are sent to email addresses from the marketing department as clean if a dictionary with these three terms is created and referenced in the condition **Sender** (see Types of Filter Rules on page 30). In order to have the same behavior of the Compliance Filter without referencing a dictionary, either three different filter rules containing one literal expression for a sender each or a single filter rule containing a regular expression with OR operators between the different senders would be required. The latter solution might be impractical for a high number of specified senders.

Another use case is to reject all incoming emails containing swear words. To do this, a customer-level administrator would create a dictionary of swear words and reference it in a filter rule for incoming emails. Creating and maintaining individual filter rules for each swear word instead would be much more time-consuming.

Customer-level administrators can create dictionaries (see Creating a Dictionary on page 52), edit existing dictionaries (see Editing a Dictionary on page 55) and delete them (see Deleting a Dictionary on page 57).

Creating a Dictionary

You have activated the Compliance Filter for the selected domain (see Activating Compliance Filter on page 10).

In the **Compliance Filter** > **Dictionaries** module, you can create dictionaries (see Dictionaries on page 51) for the Compliance Filter. Dictionaries allow you to easily create complex filter rules (see Creating a Filter Rule for Incoming Emails on page 12 and Creating a Filter Rule for Outgoing Emails on page 18).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to create a dictionary.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Select the tab **Dictionaries**.

5. Click on **Add**.

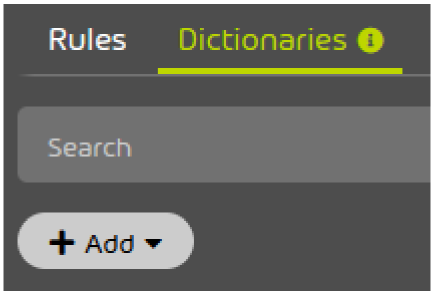


Figure 32: Add a dictionary

A form for creating a dictionary is displayed.

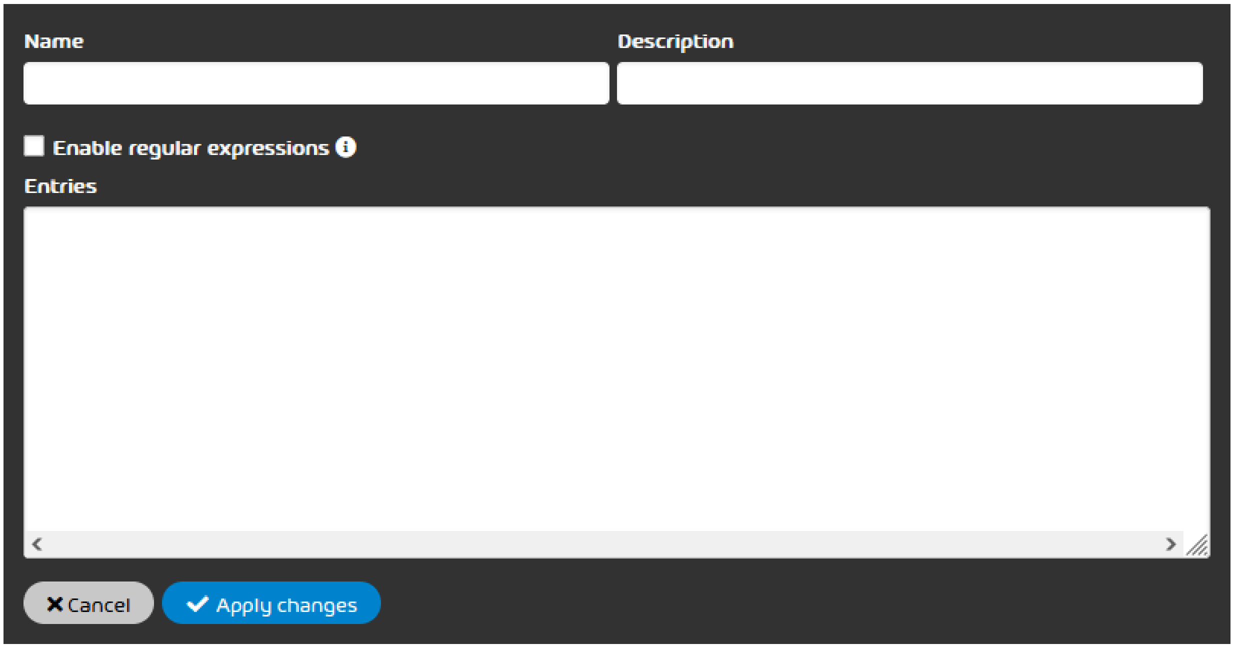


Figure 33: Form for a dictionary

6. Enter a name for the dictionary in the field **Name**.

> **Notice:**
>
> The name may only contain the following characters:
>
> - Latin lower case letters from a-z
> - digits from 0-9
> - Special characters **- _ . , =**
>
> Whitespaces and colons are not allowed.

7. Optional: Enter a description for the dictionary in the field **Description**.
8. Optional: If the entries of the dictionary are to be interpreted as regular expressions, tick the checkbox **Enable regular expressions**.

> **Notice:**
>
> If this option is selected, all entries of the dictionary must comply with the rules of regular expressions (see Explanation of Regular Expressions on page 61) and their exceptions (see Exceptions to Regular Expressions on page 69).

9. Enter the desired exceptions in the field **Entries**.

> **Notice:**
>
> Each line corresponds to an entry. The maximum line length is 1000 characters. The number of entries is limited to 15000 literal expressions and to 1000 regular expressions. Blank lines and duplicate entries are ignored and removed when the dictionary is saved.

10. Click on **Apply changes**.

    If the checkbox **Enable regular expressions** is ticked, we check whether the regular expressions are correct.

    The form is closed, the dictionary is saved and added to the table of dictionaries.

A dictionary has been created.

Next, you can edit (see Editing a Dictionary on page 55) or delete (see Deleting a Dictionary on page 57) the dictionary. You can reference the dictionary in filter rules of the Compliance Filter (see Creating a Filter Rule for Incoming Emails on page 12 and Creating a Filter Rule for Outgoing Emails on page 18).

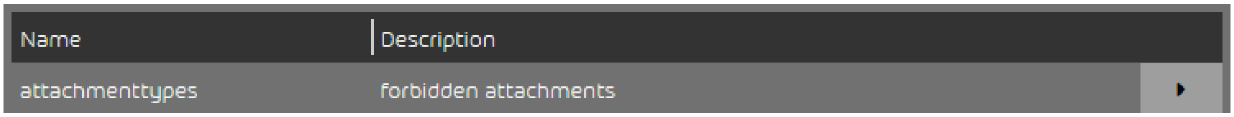
Editing a Dictionary

You have created a dictionary (see Creating a Dictionary on page 52).

In the **Security Settings** > **Compliance Filter** module, you can edit existing dictionaries (see Dictionaries on page 51) of the Compliance Filter (see About the Compliance Filter on page 6).

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to edit a dictionary.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Select the tab **Dictionaries**.

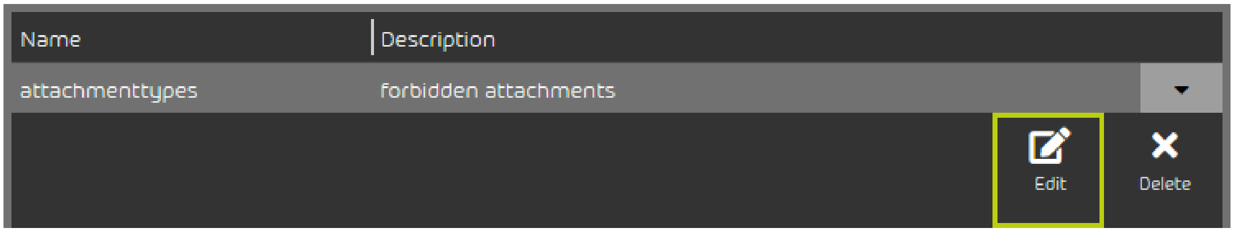
5. In the list of dictionaries, click on the menu arrow next to the dictionary that you would like to edit.



Name	Description
attachmenttypes	forbidden attachments

Figure 34: Open the menu

6. Click on **Edit**.



Name	Description
attachmenttypes	forbidden attachments

Figure 35: Edit the dictionary

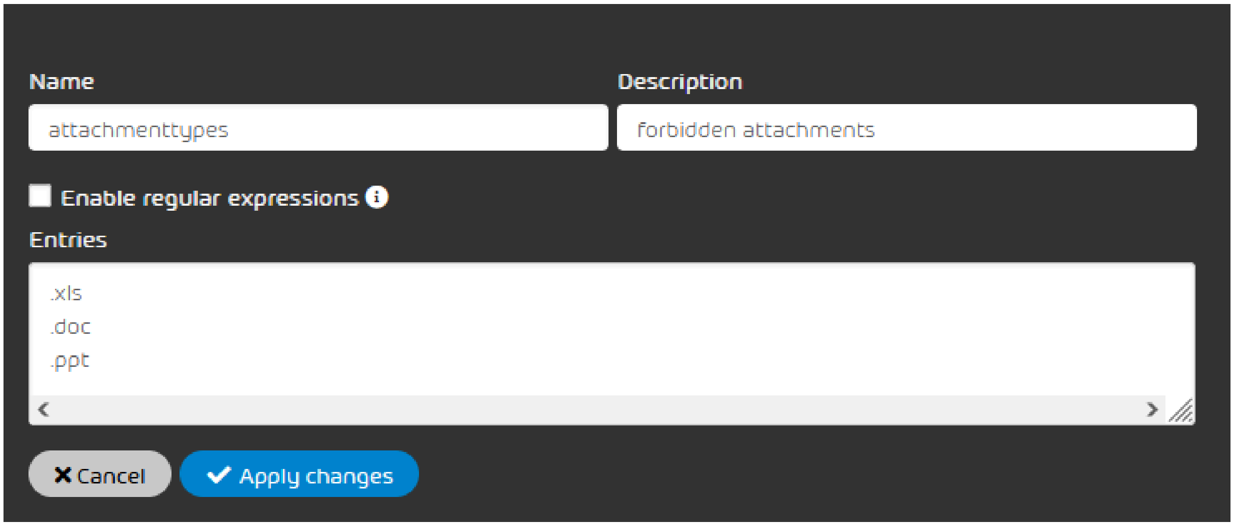
A form with the current settings of the dictionary opens.

7. Edit the settings as desired.

Notice:

For more information, see Creating a Dictionary on page 52.

8. Click on **Apply changes**.



Name: attachmenttypes

Description: forbidden attachments

☐ Enable regular expressions

Entries:

.xls
.doc
.ppt

Figure 36: Apply changes

The changes are applied.

Notice:

If the dictionary has been renamed and it is already referenced in filter rules, the name of the dictionary will also be updated in these filter rules.

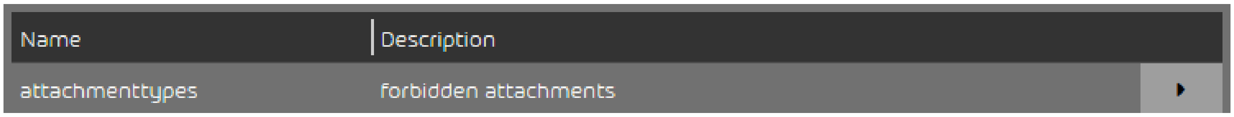
A dictionary has been edited.

Deleting a Dictionary

You have created a dictionary (see Creating a Dictionary on page 52). The dictionary is not referenced in any filter rule of the Compliance Filter.

If you no longer need an existing dictionary (see Dictionaries on page 51) of the Compliance Filter (see About the Compliance Filter on page 6), you can delete it in the **Security Settings** > **Compliance Filter** module.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to delete a dictionary.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Select the tab **Dictionaries**.
5. In the list of dictionaries, click on the menu arrow next to the dictionary that you would like to delete.



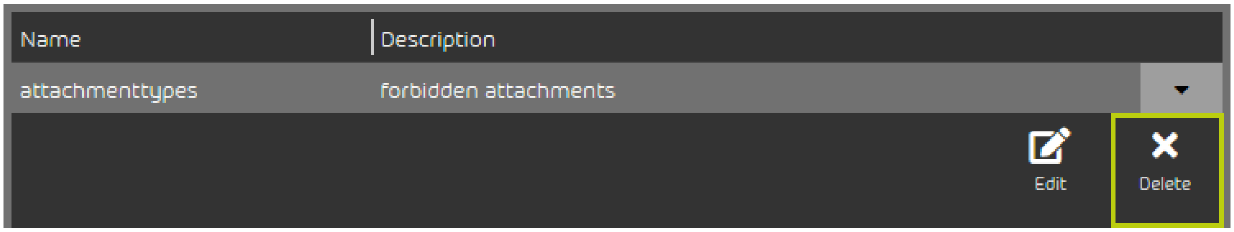
Name	Description
attachmenttypes	forbidden attachments

Figure 37: Open the menu

➔

A menu opens.

6. Click on **Delete**.



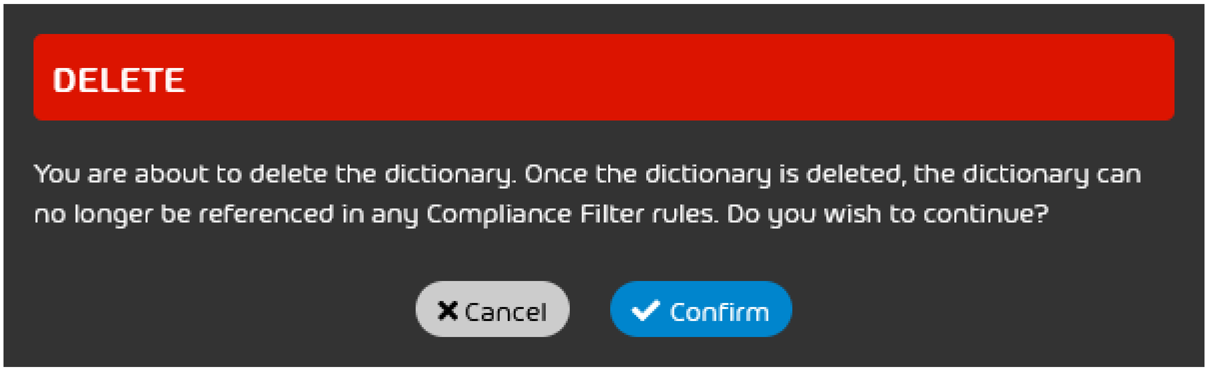
Name	Description
attachmenttypes	forbidden attachments

Figure 38: Delete the dictionary

➔

A warning message is displayed.

7. Click on **Confirm**.



DELETE

You are about to delete the dictionary. Once the dictionary is deleted, the dictionary can no longer be referenced in any Compliance Filter rules. Do you wish to continue?

Figure 39: Confirm deletion

➜

We check whether the dictionary is referenced in any filter rules of the Compliance Filter. If it is not referenced anywhere, the dictionary is deleted.

✓

A dictionary has been deleted.

Regular Expressions

In the filter rules of the Compliance Filter (see Filter Rules on page 11), regular expressions (RegEx for short) can be used to extract information from strings. This way, it is possible to recognize patterns in the subject or other components of an email, and to filter emails.

Notice:

The system automatically adds the sequence **.*** at the beginning and the end of regular expressions in the **Compliance Filter** module unless the regular expression starts with **^** or ends with **$**.

Notice:

By appending a question mark, the quantifiers **+** and ***** (see table Syntax elements and special characters in chapter Explanation of Regular Expressions on page 61) are automatically made lazy before the regular expressions are evaluated.

"Lazy" is the opposite of "greedy" and means that the search ends with the shortest possible match. For instance, the greedy regular expression **a.*b** would find the match **aabcaab** in the string **aabcaabcdf**. In contrast, the lazy expression **a.*?b** would find the match **aab** twice in the same string.

Important:

In the **Compliance Filter** module, regular expressions can only be used in filter rules of the type **Advanced** (see Types of Filter Rules on page 30) and in dictionaries (see Dictionaries on page 51).

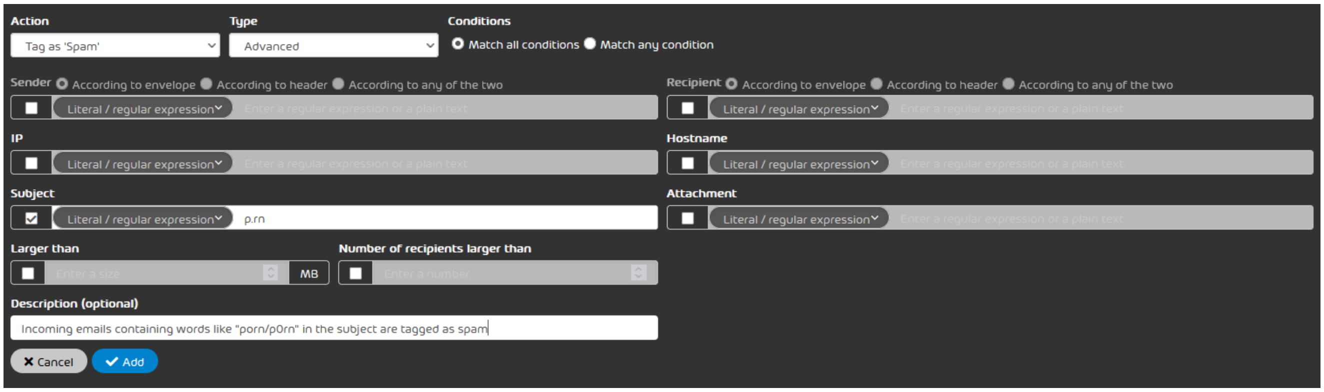
For an explanation and examples of regular expressions, see Explanation of Regular Expressions on page 61 and Examples for Complex Regular Expressions on page 71.

Within the Compliance Filter, regular expressions according to Perl Compatible Regular Expressions can be defined. Other libraries are not supported. For more information, see: http://www.pcre.org/.

In addition, there are special restrictions that are explained in Exceptions to Regular Expressions on page 69.

Example: Using regular expressions in the Compliance Filter

Users often received emails with the word "porn" in the subject. A filter rule was defined to mark them as spam. Recently, an increased volume of spam emails using leetspeak to bypass this filter was observed. For example, incoming emails with the subject "p0rn" were not tagged by the Compliance Filter. In this case, the use of a regular expression is more effective:



Action: Tag as 'Spam'

Type: Advanced

Conditions: ● Match all conditions ○ Match any condition

Sender ● According to envelope ○ According to header ○ According to any of the two

□ Literal / regular expression

Recipient ● According to envelope ○ According to header ○ According to any of the two

□ Literal / regular expression

IP

□ Literal / regular expression

Hostname

□ Literal / regular expression

Subject

☑ Literal / regular expression p.rn

Attachment

□ Literal / regular expression

Larger than

□ MB

Number of recipients larger than

□

Description (optional)

Incoming emails containing words like "porn/p0rn" in the subject are tagged as spam

Figure 40: Use of a regular expression in the Compliance Filter

The dot matches any character. The filter is not limited to an "o" in this place, but reacts to any letter, digit and special character.

Explanation of Regular Expressions

In the following examples for regular expressions, the text in the left column is validated against the regular expression in the right column. The text marked in bold is matched by the regular expression.

Individual characters

Table 5: Matching letters

TEXT	REGEX
abcdef	**abc**
abcde	
Abcd	

With letters, you can search anywhere inside a text for matches.

Table 6: Matching characters from a selection of characters

TEXT	REGEX
ac**bde**f	**[abc]de**
adefg	

A selection of characters searches individually for each of the characters that are bundled together by square brackets to form a selection.

Table 7: Matching characters from character ranges

TEXT	REGEX
1 Word	[1-5] [A-Z]
7 Words	
2 different words	

Square brackets can also be used to specify character ranges. The first and the last character of the range are separated by a hyphen. The character order is the same as in the ASCII table. Capital letters thus come before lower-case letters. Therefore, the regular expression **[A-z]** finds all ASCII characters from the capital letter A to the lower-case letter z. In contrast, the regular expression **[a-Z]** is invalid and does not find any matches.

Important:

The character range **[A-z]** contains only Latin letters. The following characters are excluded from the character range:

- umlauts (äöü)
- letters with accents (e.g., áéíóú)
- language-specific letters (e.g., ñ or ß)

Table 8: Matching digits

TEXT	REGEX
number = **123**	**123** or **\d\d\d**
var number = **123**	
ab**123**fg	

Digits have the same effect as letters. Instead of a specific digit, the character **\d** can be used to match any digit.

Table 9: Matching letters

TEXT	REGEX
a12**b**34**c**	**\w**

The expression **\w** matches any Latin letter from A to z (see above) without special characters or language-specific letters.

Table 10: Matching any character

TEXT	REGEX
bob.	**···\.**
tom.	
?!a.	
abc1	

A single "." matches any character. In order to match a dot, the dot must be escaped with "\.".

Table 11: Matching multiple characters

TEXT	REGEX
abcc	**ab*c**
a**abbbbbc**c	
bb**ac**cc	

Repetitions

The trailing asterisk means that the preceding character may occur any number of times. The character may thus occur not at all, once or multiple times.

Table 12: Matching at least one character

TEXT	REGEX
aaaaaaaaa**abc**	**ab+c**
a**abbbc**	
ac	

The trailing plus sign means that the character must occur at least once and may occur multiple times. If it does not occur, there is no match.

Table 13: Defining the number of character repetitions

TEXT	REGEX
12 **123 4544 1564**14	**\d{3,4}**

A given number or an interval for the number of repetitions of the preceding character can be specified in curly brackets. The example above searches for character sequences that contain only digits and consist of 3 to 4 characters. The following combinations are possible:

- {m}: The preceding character must occur exactly m times.
- {m,}: The preceding character must occur at least m times.
- {m,n}: The preceding character must occur at least m times and at most n times.

Table 14: Optional characters

TEXT	REGEX
3 users online	**\d+ users? online**
150 users online	
20 users online	

TEXT	REGEX
1 user online	
no user online	

By appending a "?", the leading character is declared as optional.

Groups

Table 15: Grouping regular expressions

TEXT	REGEX
dump025.csv	\w+\d+\.(\w+)
dump026.csv	

Parentheses around a part of the regular expression group the enclosed elements. In the example above, the file extension after the dot is a group. Several operators handle groups like individual characters. Therefore, trailing quantifiers such as ?, *, + or curly brackets have an effect on the group as a whole and not only on the last character. For instance, the whole group **(abc)?** would be optional. Besides, groups allow advanced operations such as backreferencing (see below). Another advantage is that groups make the expressions easier to read.

Table 16: Matching either/or

TEXT	REGEX
data.csv	.*\.(exe|xlsx)
bild.jpg	
moving.gif	

TEXT	REGEX
document.pdf	
virus.exe	
locky.xlsx	

A vertical bar **|** within parentheses separates character sequences from each other that are to be searched for alternatively.

Table 17: Backreferencing

TEXT	REGEX
From: "local@domain.com" <local@domain.com>	**From: "(*@.*\.com)" <\1>**
"local@domain.com" <hacker@hackeddomain.com>	

The backreference \1 stands for the group definition (.*@.*\.com). A match is only made if the match of the group appears again at the referenced place.

Syntax elements and special characters

The following syntax elements can be used to define regular expressions in the Compliance Filter:

Table 18: Syntax elements

WILDCARD/CHARACTER CLASS	FUNCTION
abc...	Letters
123...	Digits

WILDCARD/CHARACTER CLASS	FUNCTION
[abc]	Any of the characters a, b or c
[a-z]	Any ASCII character from the specified range
\d	Any digit
.	Any character
. **/** \ *	Escaping the characters in bold
\w	Any alphanumeric character
*	0 or more repetitions of the preceding expression
+	1 or more repetitions of the preceding expression
?	The preceding expression is optional
{m}	Exactly m repetitions of the preceding expression
{m,}	At least m repetitions of the preceding expression
{m, n}	m to n repetitions of the preceding expression
\s	Any whitespace
(...)	Extraction group
(.*)	All
(abc|def)	abc or def

WILDCARD/CHARACTER CLASS	FUNCTION
^	Beginning of the string
$	End of the string

The special characters from the table above are interpreted as part of a regular expression by default. However, it is also possible to search for these special characters literally. To do so, the functions of these special characters must be bypassed with a preceding backslash ****. For instance, the expression **a*** does not find any number of As but the literal character sequence **a***.

Exceptions to Regular Expressions

The creation of regular expressions for filter rules of the Compliance Filter (see About the Compliance Filter on page 6 and Filter Rules on page 11) differs from the creation of PCRE-compliant expressions because not all their syntax elements can be used in the Compliance Filter. Basically, characters from the extended ASCII table are allowed. When checking regular expressions, no distinction is made between upper and lower case.

Different restrictions apply to expressions that are entered directly in the input fields of filter rules in the **Compliance Filter** module and to those in dictionaries (see Dictionaries on page 51).

The following characters **cannot** be used in the input fields of filter rules in the **Compliance Filter** module whose values are interpreted as regular expressions:

- Semicolon ;
- Degree sign °
- Asterisk * at the beginning of an entry
- Slash / (unless it is escaped with \)

The following characters **cannot** be used in dictionaries of the **Compliance Filter** module whose entries are interpreted as regular expressions:

- Degree sign °
- Slash / (unless it is escaped with \)

Notice:

The vertical bar | (pipe) is both in input fields of filter rules and in dictionaries only allowed inside a group between parentheses. Furthermore, a single vertical bar | is used whenever it has the meaning OR. Two vertical bars || are interpreted as a wildcard and mean that all characters will be accepted.

Common Use Cases of Regular Expressions

In the following, sample regular expressions (see Explanation of Regular Expressions on page 61) of common use cases in the Compliance Filter (see About the Compliance Filter on page 6) are presented.

Different hostnames with the same ending

When creating filter rules for emails that are sent from or to the email servers of different subdomains of a specific domain, the condition **Hostname** in the **Security Settings** > **Compliance Filter** module can be used to search for strings with a certain ending.

The following regular expression can be used for this search:

String^

The circumflex means that the string that is searched for must be found at the end of the checked hostname. For instance, the regular expression **.*domain\.tld^** would find emails from or to the email servers of the domain **domain.tld** and all its subdomains (e.g., **marketing.domain.tld**, **sales.domain.tld**, **accounting.domain.tld**)

Numbered hostnames of email servers

Often, the only difference between the different email servers of a domain is their number. In order to process emails from and to these email servers using filter rules of the Compliance Filter, the condition **Hostname** can search for strings that only differ in their numbering.

The following regular expression can be used for this search:

(string before numbering)\d+(string after numbering)

Notice:

The brackets in this expression are optional and were used for clarity.

The sequence **\d+** stands for "at least one digit". For instance, the regular expression **mx\d+\.domain\.tld** would find emails from or to the following email servers: **mx3.domain.tld**, **mx30.domain.tld**, **mx100.domain.tld**.

Several specific email addresses of a domain

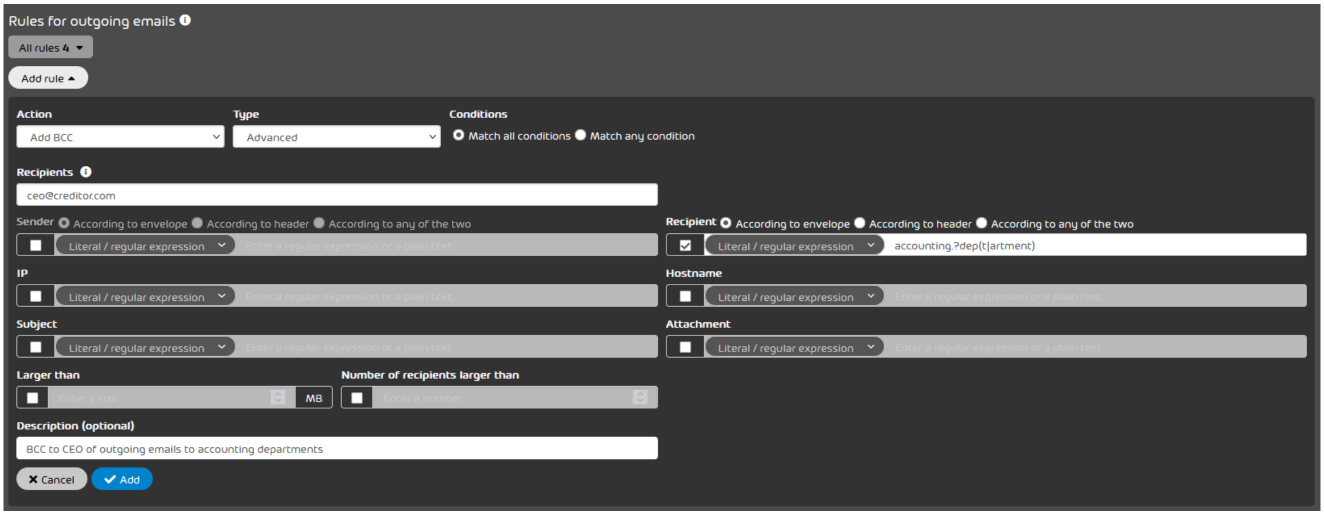
In order for a filter rule to be applied to a small number of email addresses of a domain, a regular expression with the following pattern can be used for the condition **Sender** or **Recipient**:

(user1|user2|user3)@domain

The symbol **|** separates several alternative strings from each other, one of which must be found. The alternative strings must be in brackets. For instance, the regular expression **(evan|peter|sandra)@domain.com** would find emails from and to the following email servers: **evan@domain.com**, **peter@domain.com**, **sandra@domain.com**.

Examples for Complex Regular Expressions

To conclude, we are taking a look at the usage of complex regular expressions (see Explanation of Regular Expressions on page 61) within filter rules of the Compliance Filter (see About the Compliance Filter on page 6).



Rules for outgoing emails

Action: Add BCC

Type: Advanced

Conditions: ◉ Match all conditions ○ Match any condition

Recipients: ceo@creditor.com

Sender ◉ According to envelope ○ According to header ○ According to any of the two

□ Literal / regular expression

Recipient ◉ According to envelope ○ According to header ○ According to any of the two

☑ Literal / regular expression: accounting.?dep(t|artment)

IP: □ Literal / regular expression

Hostname: □ Literal / regular expression

Subject: □ Literal / regular expression

Attachment: □ Literal / regular expression

Larger than: □ MB

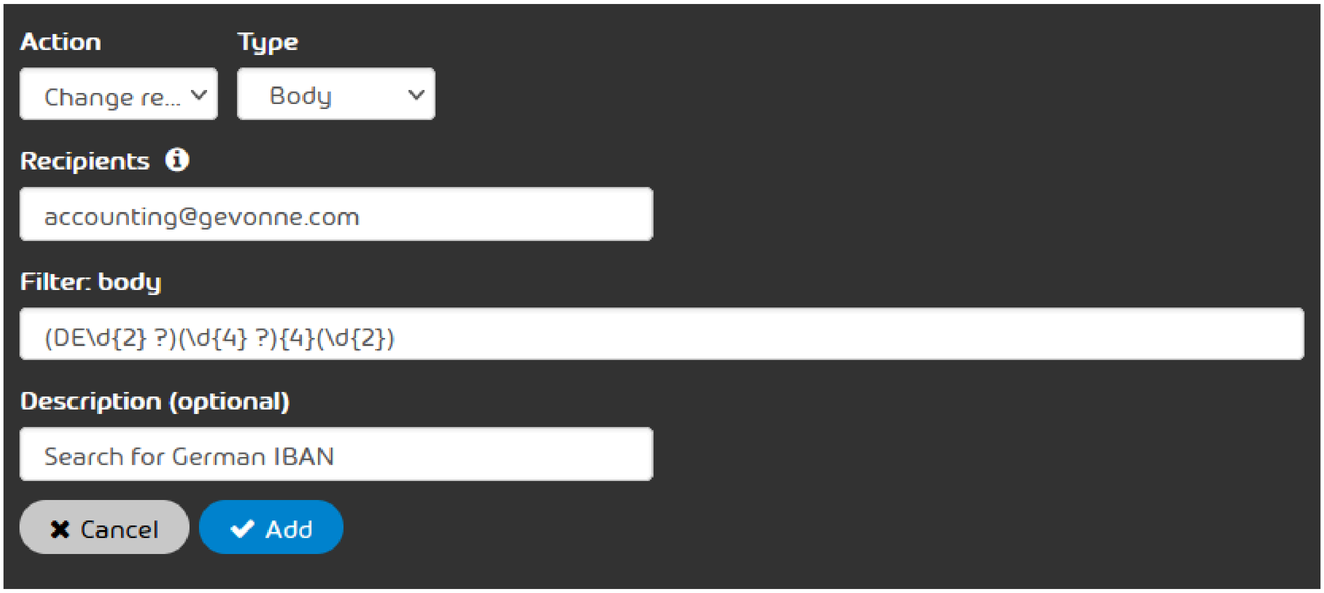
Number of recipients larger than: □

Description (optional): BCC to CEO of outgoing emails to accounting departments

Figure 41: Search for recipients

In this first example, a customer would like their CEO to receive blind copies of outgoing emails that are sent to the accounting departments of the company's customers. These email addresses follow a certain pattern. The regular expression **accounting.?dep(t|artmen)** finds the following text segments and many other combinations:

- **accountingdepartment@test.com**
- **accounting_department@test.com**
- **accounting_dept@test.com**
- **accounting.department@anothertest.com**



Action: Change re...

Type: Body

Recipients: accounting@gevonne.com

Filter: body: (DE\d{2} ?)(\d{4} ?){4}(\d{2})

Description (optional): Search for German IBAN

Figure 42: Search for IBAN in email body

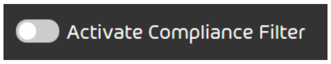
In this example, a customer would like to forward all incoming emails that contain German IBAN account numbers in the email body to their accounting department. The regular expression **(DE \d{2} ?)(\d{4} ?){4}(\d{2})** can be used to search for German IBAN numbers. This regular expression finds both German IBAN account numbers without whitespaces and German IBAN account numbers that are divided into 4-character blocks and a 2-character block at the end according the usual notation.

- **DE12345678901234567890**
- **DE12 3456 7890 1234 5678 90**

Deactivating Compliance Filter

If you no longer want to use the filter rules of the Compliance Filter (see About the Compliance Filter on page 6), you can deactivate the Compliance Filter in the **Security Settings** > **Compliance Filter** module. This action deletes all created rules.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to deactivate the Compliance Filter.
3. Navigate to **Security Settings** > **Compliance Filter**.
4. Toggle the switch **Activate Compliance Filter**.

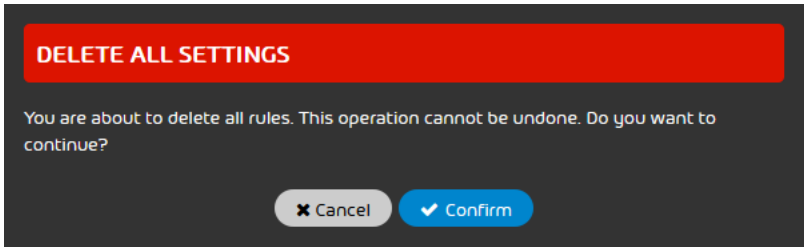


Activate Compliance Filter

Figure 43: Deactivate Compliance Filter

A confirmation window opens.

5. Click on **Confirm**.



DELETE ALL SETTINGS

You are about to delete all rules. This operation cannot be undone. Do you want to continue?

Figure 44: Confirm

The Compliance Filter is deactivated. All rules are deleted. The settings in the **Compliance Filter** module are disabled. No further input is possible.

The Compliance Filter has been deactivated.

Index

WatchGuard®

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com | pandasecurity.com