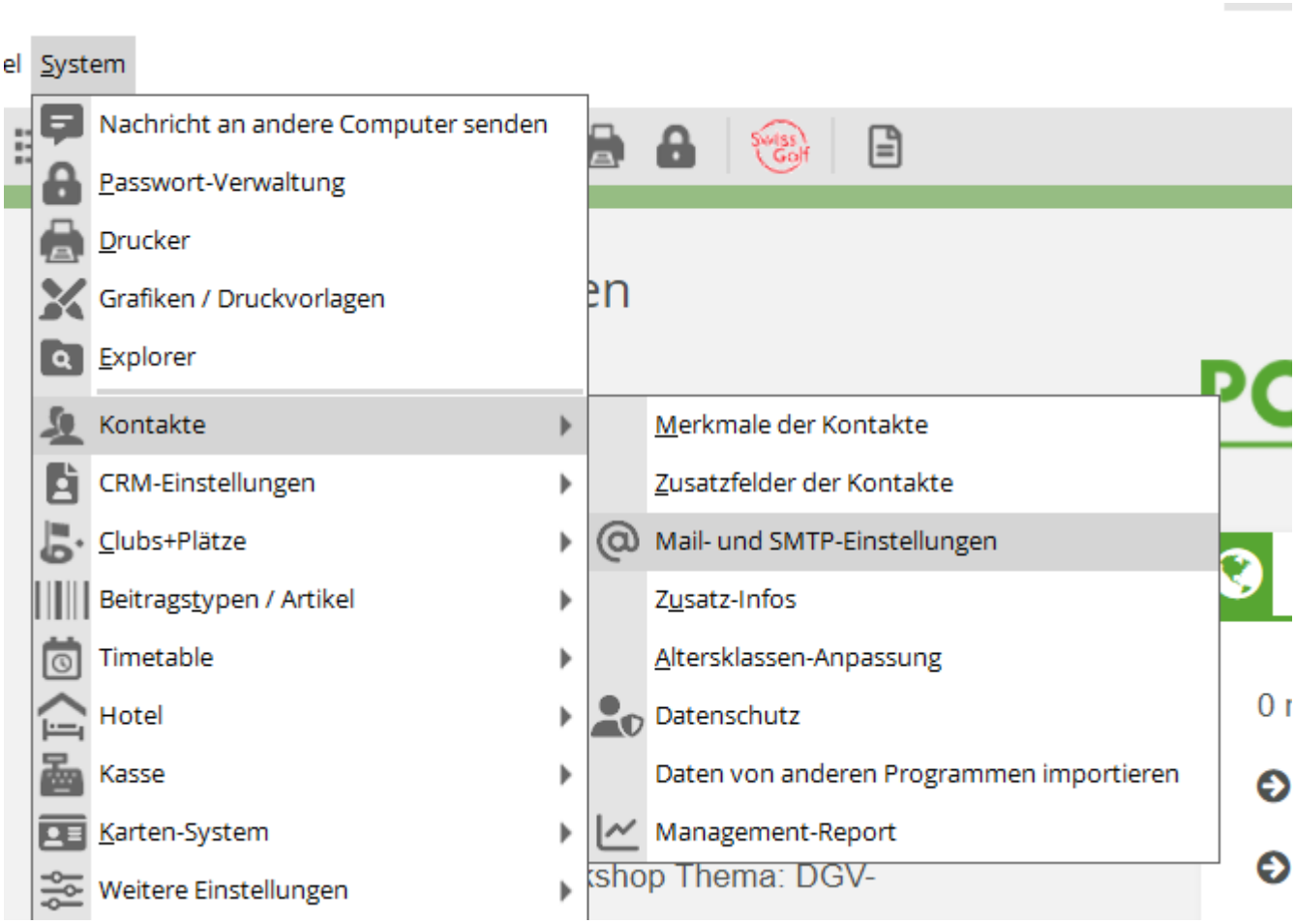
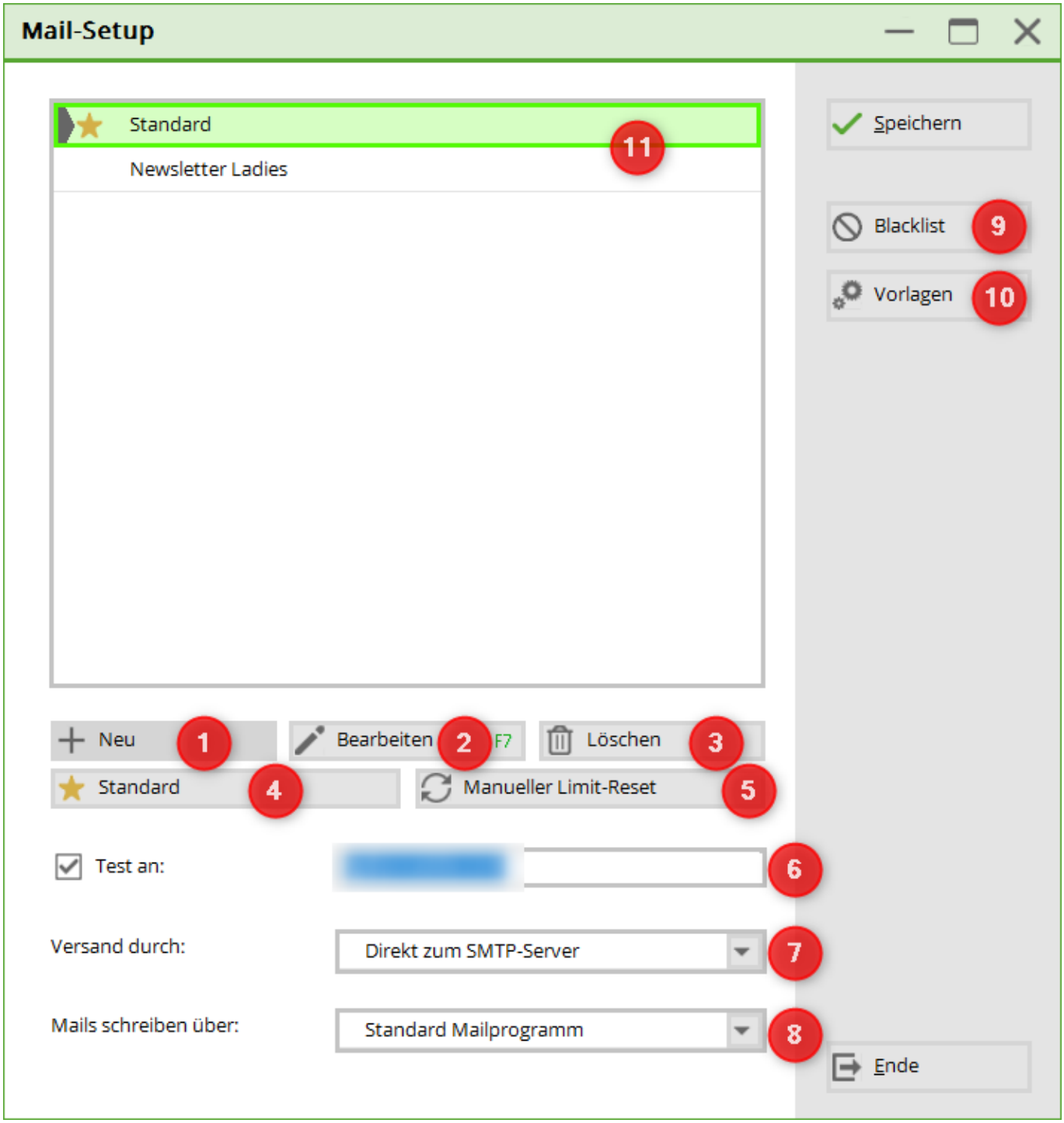
Mail and SMTP settings

You can access the settings via ***System***, ***Contacts***, ***Mail and SMTP settings***

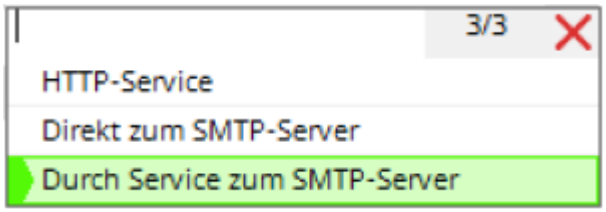


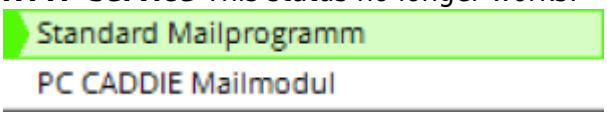
Mail setup



}}

1. Create a new SMTP server
2. Edit an existing SMTP server
3. Deleting an existing SMTP server
4. This allows one of the existing SMTP servers to be defined as the default. To do this, simply click on the desired line in the list and click on the Define as default button. The asterisk then marks the mail server defined as the default.
5. Manual limit reset
6. The tick activates the Test mode is activated. The mails are then not sent to the customer but only to the address entered.

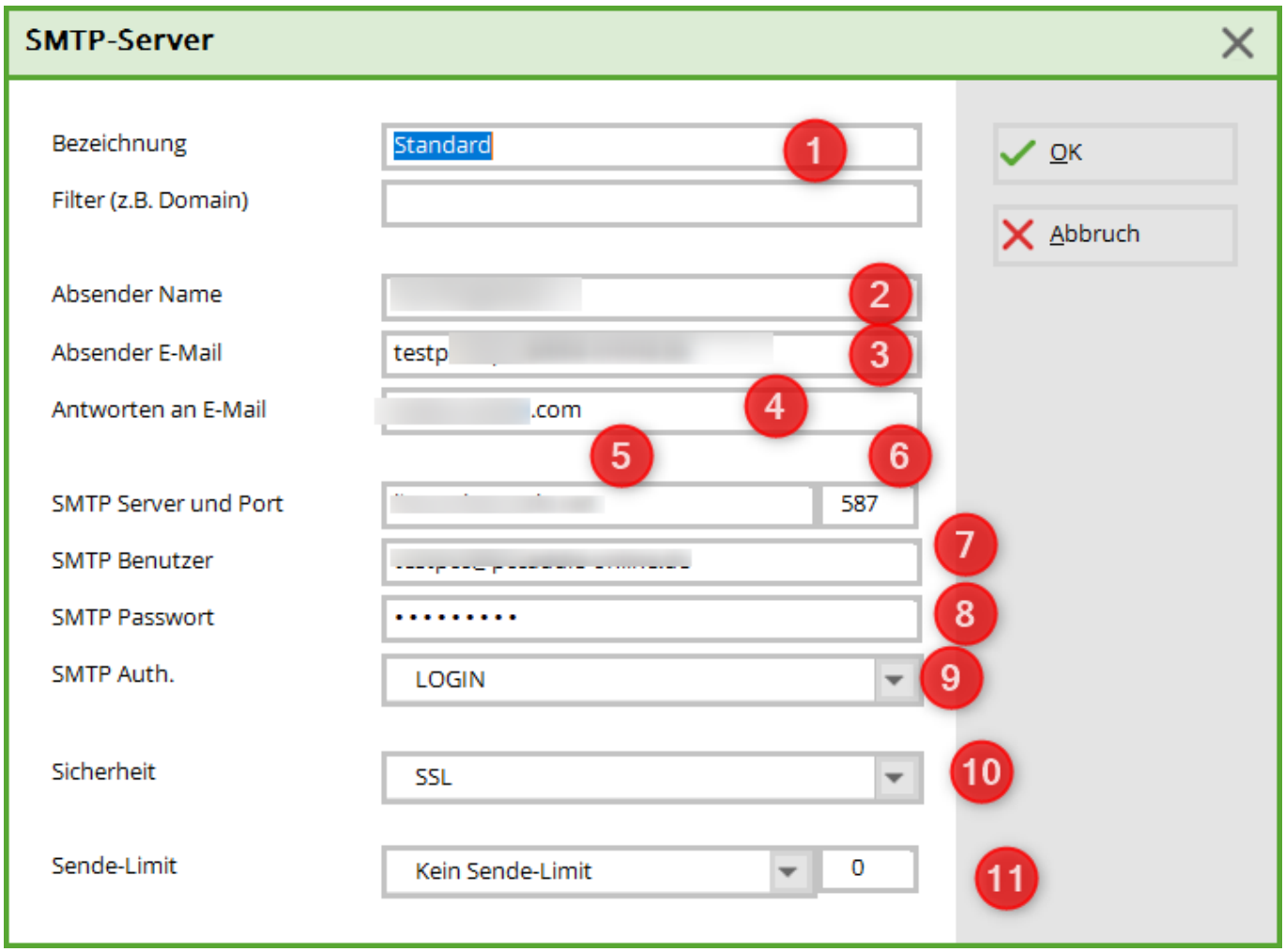
7. 

   Normally we set here that the dispatch ***sent by the service to the SMTP server*** is sent by the service. The mail service is installed by PC CADDIE Support for this purpose. The service is responsible in the background for ensuring that the data transfer is triggered again and again if the mail was not sent on the first attempt.
   Directly to the SMTP server sends the mails without the help of the service. With this option, you must check yourself whether all mails have been sent and, if necessary, manually retrigger those that have not been sent.
   HTTP service This status no longer works!
8. 

   This setting is also related to the CRM. Is ***Default mail programme*** is set, PC CADDIE sends the mails when you click on the letter next to the mail address in the person mask
   

   via your external mail programme Outlook, Tunderbird, etc.
   Set the setting to ***PC CADDIE mail module*** all mails are sent directly from PC CADDIE via this mail module and would also be saved directly in CRM.
9. Blacklist
10. Templates: This takes you to the editing window of the stored mail templates.
11. Which mail service should be used to send the mail?

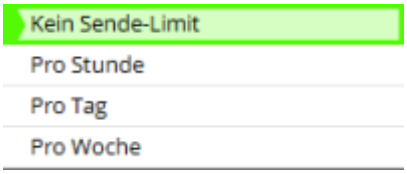
SMTP settings



Fill in the appropriate fields here:

1. Name - Name of the SMTP server
   Filter - this field is used to define if a server should only be used for a specific sender. In such cases, enter the domain or complete sender address here. If this is then also entered as the sender and reply address in the mail template, PC CADDIE knows that the mail must be sent via this server. In most cases, however, this field should remain empty!
2. Sender name - this is your sender name, this is how the sender is displayed to the recipients.
3. Sender email - which sender email address do you want to send from?
4. Reply to email - the replies to your emails from the recipients will be sent to this address.
5. SMTP server - enter the server name
6. Port - enter the port number
7. SMTP user - You will receive this user from your IT department.
8. SMTP Password - You will receive this from your IT department.
9. SMTP Auth. - Authentication

10. Security -

11. Send limit - 

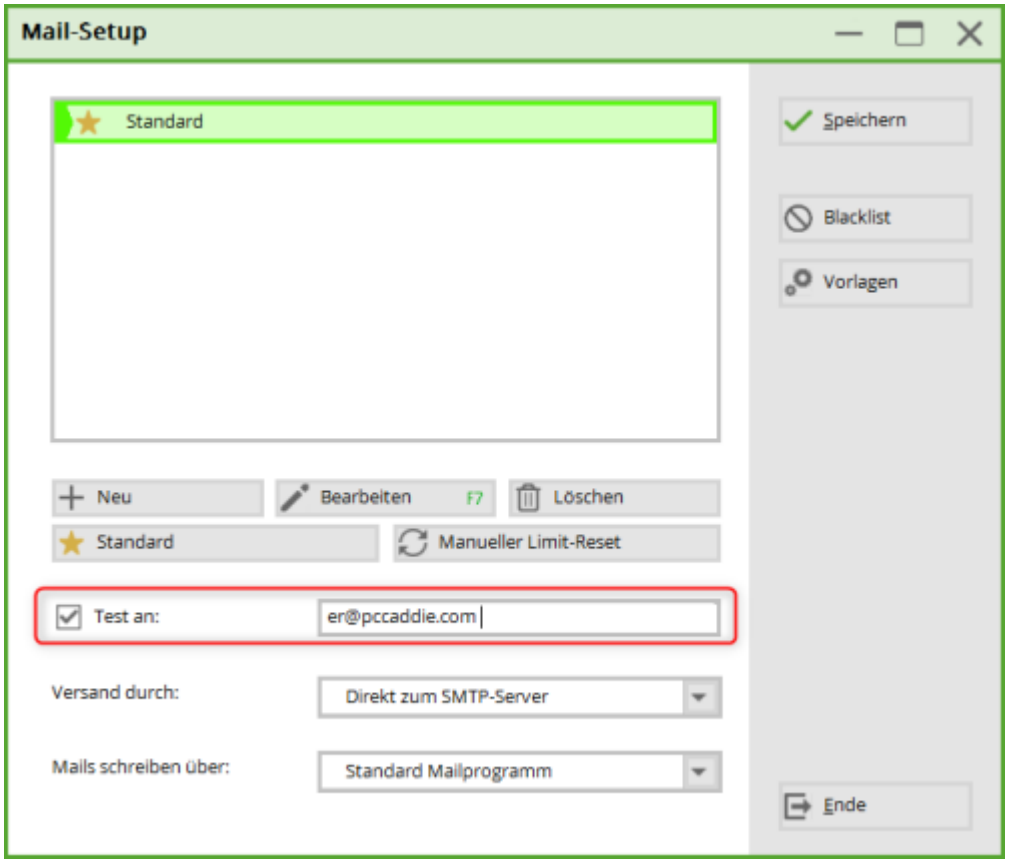
Selection of the SMTP server

The selection of the correct server for the sender stored in the mail is done in two steps:

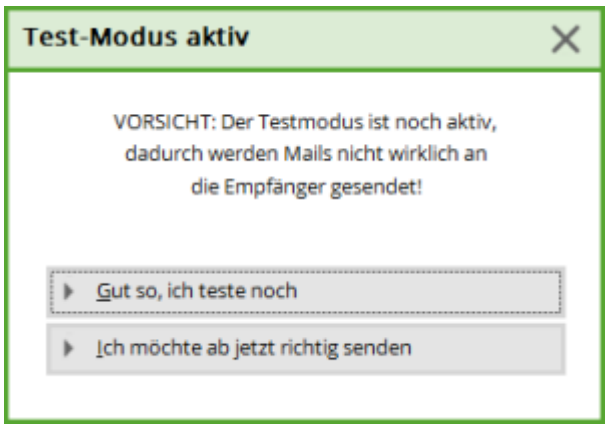
1. If a filter selected in the **Filter** field applies to the sender, the correct server is found
2. If 1 does not apply, the **server marked as the default** server is used to send the mail

Test of the E-MAIL dispatch

If you would like to test the module in detail first, you can set the configuration so that all emails are sent to a test address. As long as this box is ticked, all emails are sent to the test address and not to the final recipient.



As long as the tick for *Test on* you will be asked in the following dialogue whether you still want to test or whether the mail can definitely be sent:



Sending by:

- Directly to the SMTP server - this is the default setting!
- Through service to the SMPT server - this requires an installation on your server - if necessary, ask support@pccaddie.com
- Do NOT tick the box „send through PCCADDIE“!

Please confirm with ***OK*** if all fields are filled correctly.

This only works if dispatch is installed via a service in the Service Manager!

Office 365

Please note: The PC CADDIE Online Mailer service cannot be operated with Office 365 mail accounts. This is not possible due to Microsoft's volume limitation to prevent spam.

SMTP dispatch is only included in the Enterprise packages (E1, E3, E5) - otherwise a so-called smarthost must be created or a separate additional mail server must be operated. Further details can be found here

https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-limits?redirectedfrom=MSDN#RecipientLimits

We recommend the domain email hosting from PC CADDIE.

Blacklist

If an e-mail does not reach the end customer, please check whether the address is on the blacklist. Moving to the blacklist is often related to the person's data protection settings. Entries can be removed, edited or added manually.

Sending from different e-mail addresses

Prevent spoofing and spam with SPF Protect against spoofing and phishing and prevent messages from being marked as spam

SPF is a standard method of email authentication. It protects your domain from spoofing and prevents outgoing messages from being marked as spam by the receiving servers. It also defines the mail servers that are authorised to send emails for your domain. In incoming mail servers, incoming messages that appear to come from your domain are checked with SPF to ensure that they have actually been sent from servers that you have authorised.

Without SPF, there is a higher probability that messages sent from your organisation or domain will be marked as spam by inbound mail servers.

Important: From November 2022, new senders sending emails to private Gmail accounts will need to install either SPF or DKIM. Google will perform random checks on messages from new senders to private Gmail accounts to determine if they have been authenticated. Messages without at least one of these authentication methods will be rejected or marked as spam. This requirement does not apply to existing senders. However, we recommend that you always install SPF and DKIM to protect your organisation's emails and meet future authentication requirements.

Source: https://support.google.com/a/answer/33786?hl=de