2 - User Panel - Advanced Setup for Your Mailbox

The User Control Panel is located at http://cp.emailarray.com and can also be accessed via Webmail, from the "Control Panel" link.

It lets users manage several aspects, such as change their password, setup autoresponder, manage spam quarantine, forwarders, track deliveries, create delivery rules, manage white and blacklist and much more.

- Change your mailbox password
- 2FA - Two-factor authentication for your mailbox
- Forward Messages
- Set Vacation Message
- Share E-mail Folders
- Manage Extensions
- Set Spam filter preferences and manage spams
- Whitelist or Blacklist an e-mail address
- Retrain Messages
- Track Remote Deliveries
- Configure Incoming E-mail Rules
- Disabling local delivery to an account
- How to avoid forged e-mails?
- CalDAV Synchronizer Setup
- ownCloud - free file storage and sharing on the cloud

Change your mailbox password

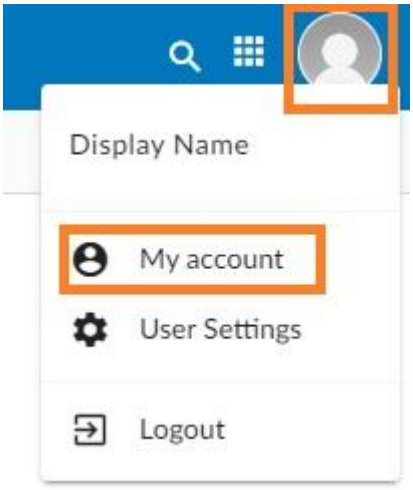
> Your mailbox password is the one you use when you log in to the Webmail or e-mail client, such as Apple Mail, Outlook, or the mail app on your phone.
> If you have set up the e-mail address on other devices, once you update the e-mail password, you should update the settings of all your e-mail clients to use this new password for IMAP and SMTP logins.

> Your password must contain at least 8 characters, and at least one UPPERCASE letter, one lowercase, one number, and one special character (,./!@#$%^&*, etc.)

1. Change your mailbox password from the Webmail

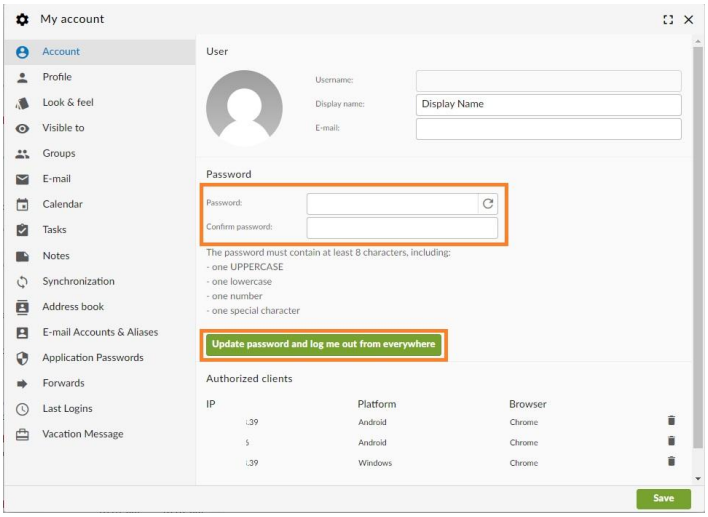
To change the password for your e-mail address, log in to the **GroupOffice Webmail** using your current password:

- Log into the **Webmail** using your full **e-mail address** and your **current e-mail password**
- Click on the **User** icon from the top right to activate the menu. Then click on **My account**



- In the **Account** tab, in the **Password** section, you can fill in the new password.
- Fill in and confirm the new password. Please note the password must meet all the requirements.
- You can also generate a strong password by clicking on the **Refresh arrow** icon at the right of the **Password** field.
- Click on the **Update password and log me out from everywhere** button. This will log you out of every device or email client.

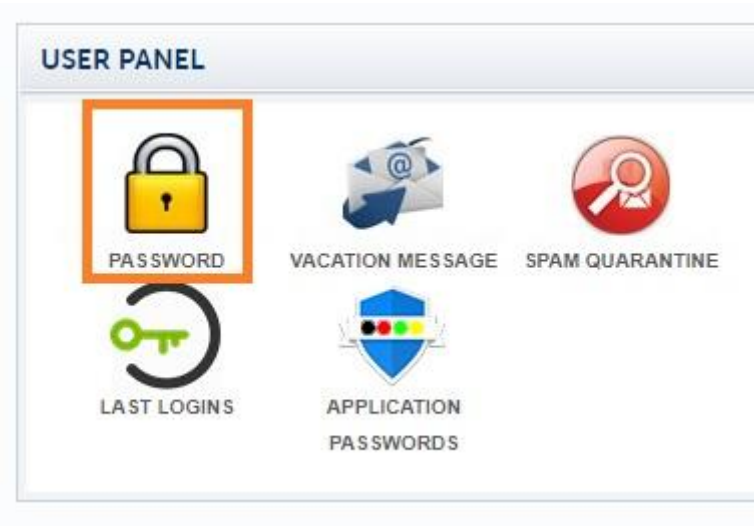
- Your password was updated, and you can now use it to log back in.



2. Change your mailbox password from the User Panel

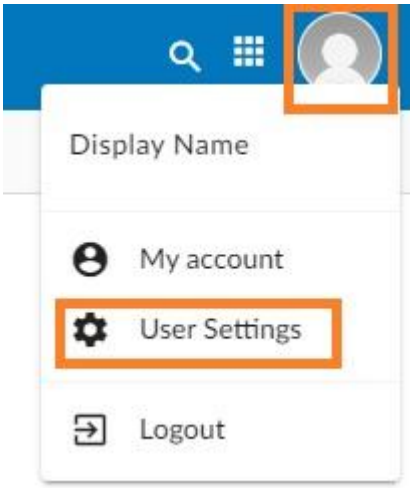
To change your password for your e-mail address:

- Go to the **User Panel**
- Log in using your **full e-mail address** (user@domain.com) and your current e-mail **password**.
- Click on the **Password** icon from the menu
- Enter your new password, confirm it and click on the **Change** button



You can also access the control panel directly from within Webmail:

- From the Group Office Webmail , click on the **User** icon to show the menu, and then go to **User Settings**. You will be automatically logged into your User Panel.



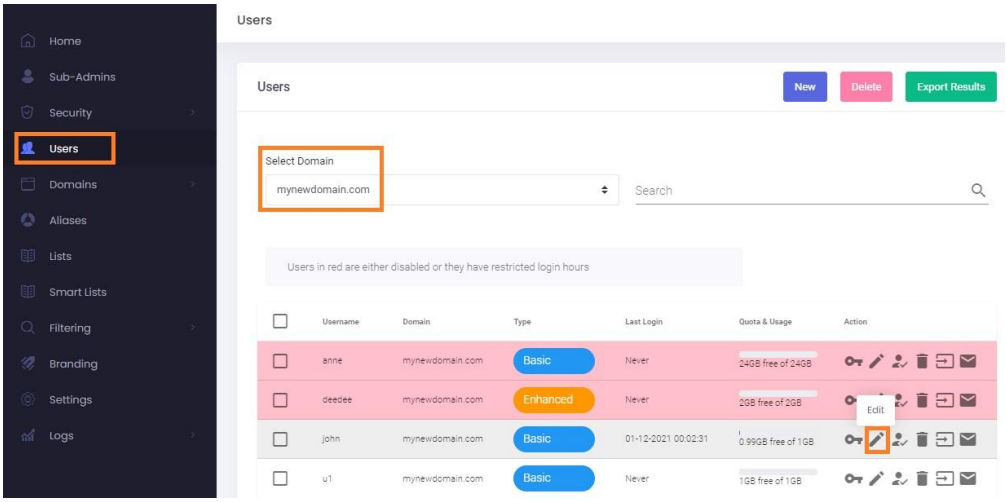
3. Change the mailbox password from the Admin Panel

If you have administration permissions, you can update the password of a mailbox without knowing the current one.

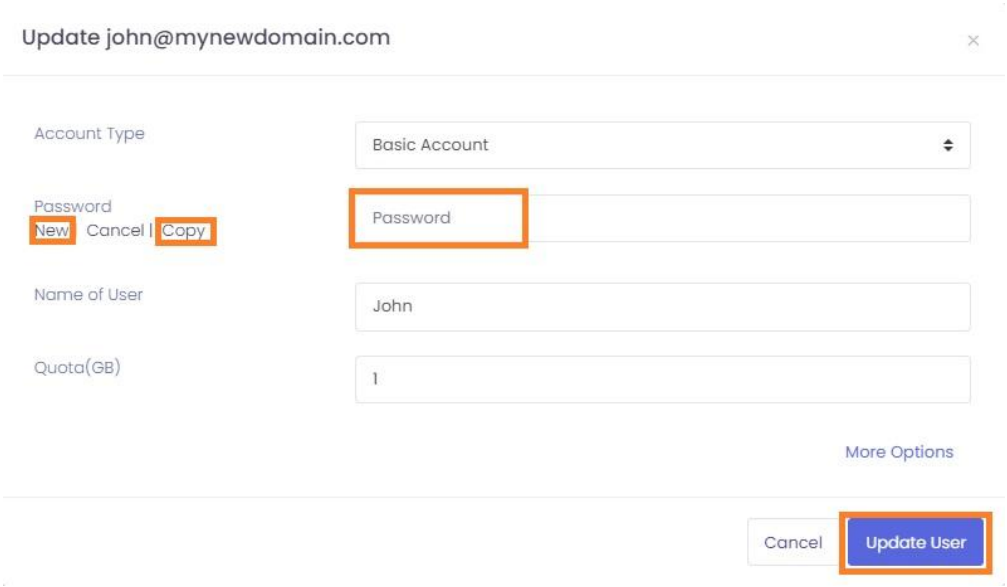
To update the password:

- Go to the **Admin Panel**
- Log in using your **Admin username** and **password**
- Go to the **Users** tab from the menu

- From the **Select Domain** dropdown, select the desired domain name
- Click on the **Edit (pencil)** icon to update the desired mailbox



- In the new pop-up window, you can fill in the new **Password** for the e-mail address.
- You can also use the **New** button to generate a complex password and copy it to clipboard using the **Copy** button.
- Click on the **Update User** button to save the changes.

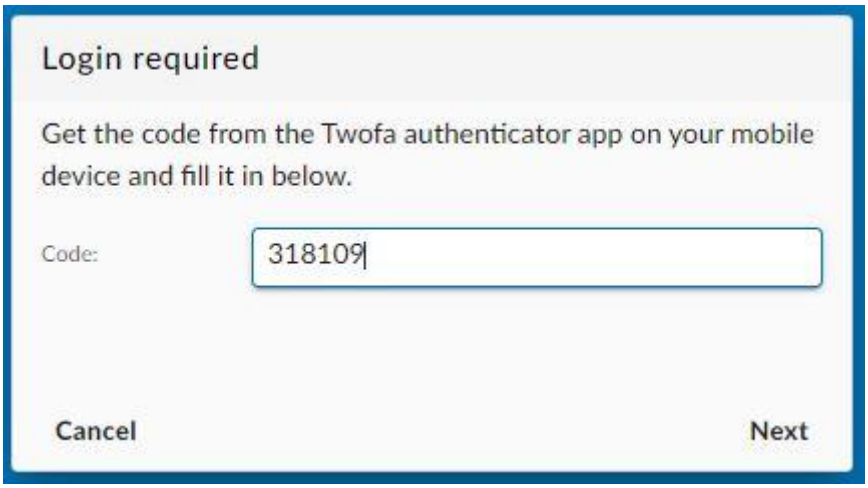


2FA - Two-factor authentication for your mailbox

Two-factor authentication, or **2FA** as it's commonly abbreviated, adds an extra step to your basic login procedure. Without 2FA, the password is your single factor of authentication: you enter your username and password, then you're done.

With 2FA, you log in to the Webmail by entering your username and password and the six-digit code provided by an app installed on your smartphone.

> In the Webmail, you will be prompted to enter the 2FA code in a new pop-up window.



> When logging into the User Panel, if you have 2FA enabled for your mailbox, you must add at the end of the password the 6-digit code provided by the app on your phone. For example, if your password is **T9D3K!px** and the 6-digit code is **189 145**, you must enter **T9D3K!px189145** in the login form of the User Panel.

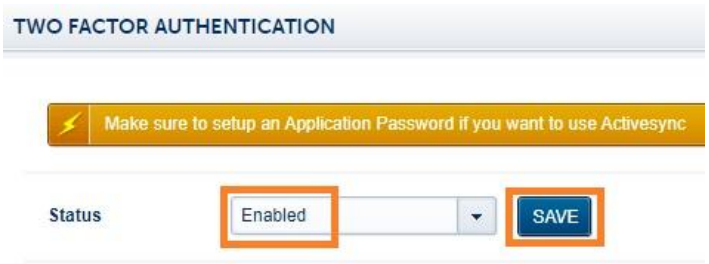
1. How to enable 2FA for your mailbox

First, you need a smartphone with a two-factor authenticator App installed (OTP / 2-Step Verification / 2-Factor Authentication), such as Authy or Google Authenticator.

To enable 2FA for your e-mail address:

- Log in to the **User Panel**
- From the menu, go to **2-Factor Auth**

- Update the dropdown **Status** to **Enabled**. Click on the **Save** button.



- Recheck the requirements: have a 2FA App installed on your phone, such as Authy or Google Authenticator
- When ready, click on the **Next** button

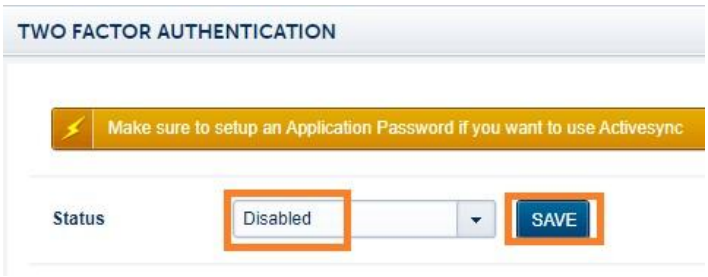
- Scan the QR code with the installed 2FA App and fill in the generated six-digit code in the **Challenge** input field.
- **Click on the Save button before your token expires. It is always better to wait for the app to generate a fresh token, so you have enough time before it expires.**
- You have enabled 2FA, and you will be prompted to fill in the token every time you log in using Webmail.

2. Disable 2FA for your mailbox

To disable 2FA for your e-mail address:

- Log in to the **User Panel**
- From the menu, go to **2-Factor Auth**

- Update the dropdown **Status** to **Disabled**. Click on the **Save** button.



- Insert the token from your 2FA App (such as Authy or Google Authenticator) in the **Challenge** input field.
- **Click on the Save button before the token expires. It is always better to wait for the app to generate a fresh token, so you have enough time before it expires.**
- After you see the confirmation message that the 2FA was disabled, you can delete the entry from your 2FA app.

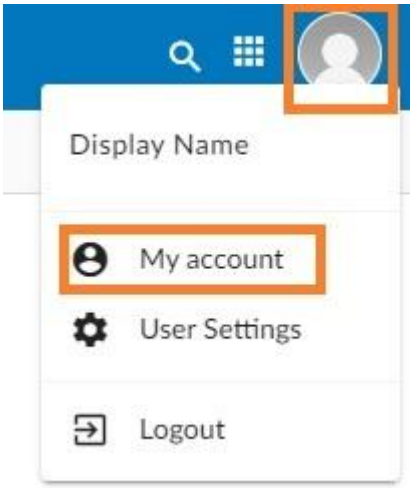
Forward Messages

Incoming e-mail messages to your account can automatically be forwarded to other accounts while also delivering a copy locally. E-mails detected by our server as spam are not forwarded.

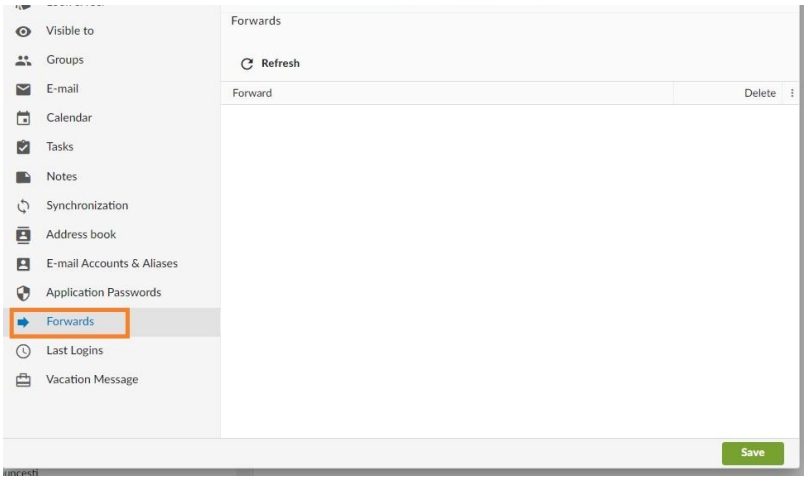
Add a Forward

Option 1: from the Webmail

- Go to the **Webmail**
- Log in using your full **e-mail address** and your **current e-mail password**
- Click on the **User** icon from the top right to activate the menu. Then click on **My account**



- In the **Forwards** tab, fill in the **Email address field** with the destination e-mail address and click on the **Add forward** button.



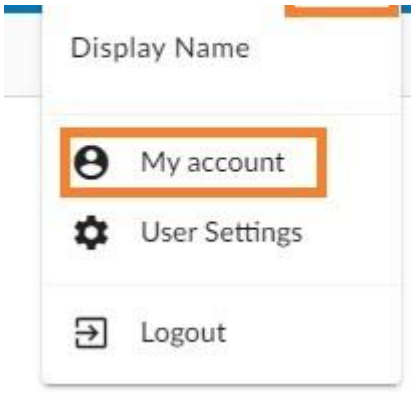
Option 2: from the User Panel

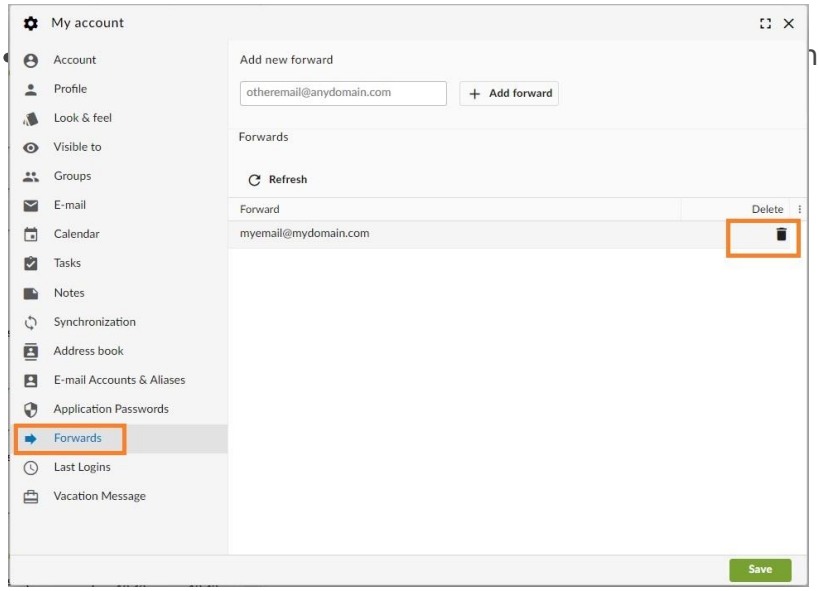
- Visit the User Control Panel (https://cp.emailarray.com)
- Log in using your full e-mail address (user@domain.com) and current password.
- Click on **Forwards** icon (envelope with arrow)
- Enter the e-mail address where you wish to forward incoming messages
- Click on the **Add Forward** button

Remove a Forward

Option 1: from the Webmail

- Go to the **Webmail**
- Log in using your full **e-mail address** and your **current e-mail password**
- Click on the **User** icon from the top right to activate the menu. Then click on **My account**





nd click on the **Delete** icon.

Option 2: from the User Panel

- Visit [User Control Panel (https://cp.emailarray.com)]
- Log in using your full e-mail address (user@domain.com) and current password.
- Click on **Forwards** icon (envelope with arrow)
- Click on the "**-**" icon (minus sign) next to the forward you wish to remove

Set Vacation Message

Vacation Message

A vacation message can let people know that you are not available by sending an automatic reply to their messages. Autoresponders are sent once every hour to each sender that sends you an email, to avoid technical issues.

Enabling the Vacation Message

- Go to
  Unknown macro: {link-window}

  https://cp.emailarray.com

- Log in using your full e-mail address (user@domain.com) and current password.
- Click on **Vacation Message** icon (opened envelope with arrow)
- Make sure Status is set to **Enabled**
- You can set a **From** and **To date** for the autoresponder to work. The default, is to send autoresponder emails until you disable the feature (from today until "never").
- Choose **Reply type**, either plain text (default) or HTML (permits graphical formatting of the vacation message)
- Enter your message in the **Vacation Message** text box
- Click on the **Update** button

Disabling the Vacation Message

- Go to
  Unknown macro: {link-window}

  https://cp.emailarray.com

- Log in using your full e-mail address (user@domain.com) and current password.
- Click on **Vacation Message** icon (opened envelope with arrow)
- Select **Disabled** in the Status pull down menu
- Click on the **Update** button

Share E-mail Folders

By Sharing E-mail Folders you allow your colleagues access to your e-mail folders, either for viewing or for modifying.

- Go to
  Unknown macro: {link-window}

  https://cp.emailarray.com
- Log in using your full e-mail address (user@domain.com) and current password.
- Click on the **Folders** icon
- Click on **Edit** icon (pencil) next to the folder you wish to share
- Click on the New Share button
- Select the user you wish to give permission to and the permissions users will have
- Click on the **Share button**

By default, your own account has full permissions on the folder you are editing. Make sure not to erase your own permissions or you will lose access to that folder

Removing permission on a folder

- Go to
  Unknown macro: {link-window}

  https://cp.emailarray.com
- Log in using your full e-mail address (user@domain.com) and current password.
- Click on the **Folders** icon
- Click on the **Edit** icon (pencil) next to the folder you wish to edit shares
- Click on the "**-**" icon (minus sign) next to the user you wish to remove the permissions for

Manage Extensions

User Extensions allows you to uniquely extend your e-mail address in order to create disposable addresses.

They can be of the form: **user-sales@domain.com** In this case '**sales**' is the extension for '**username**'. You can also have wildcard extensions that let you effectively create unique, disposable e-mail addresses.

Add a static extension

This example will create a static extension called 'sales' which will accept messages sent only to the address: user-sales@domain.com

- Visit
  Unknown macro: {link-window}

  https://cp.emailarray.com
- Log in using your full e-mail address (user@domain.com) and current password.
- Click on **Extensions** icon (image of a plus sign)
- Click on the **Add extension** button
- Enter **sales** as the extension name
- Enter your e-mail address as the **Deliver to** address
- Click on **Add extension**

Add a dynamic(wildcard) extension

This example will create a dynamic extension called 'sales' which will accept messages sent to any address of the form: user-sales-anything@domain.com
Valid addresses can be: user-sales-john@domain.com , user-sales-amy@domain.com, etc

- Visit
  Unknown macro: {link-window}

  https://cp.emailarray.com
- Log in using your full e-mail address (user@domain.com) and current password.
- Click on **Extensions** icon (image of a plus sign)
- Click on the **Add extension** button
- Enter **sales-default** as the extension name
- Enter your e-mail address as the **Deliver to** address
- Click on **Add extension**

To forward the extension to another address, simply enter another address in the **Deliver to** field

Remove an extension

- Visit
  Unknown macro: {link-window}

  https://cp.emailarray.com
- Log in using your full e-mail address (user@domain.com) and current password.
- Click on **Extensions** icon (image of a plus sign)
- Click on the "**-**" icon (minus sign), next to the extension you want to remove

Set Spam filter preferences and manage spams

Set Spam filter preferences

You can login to the user control panel inside WebMail. On the top right, click on **Control panel** link followed by the **Access Control Panel** button. You will be logged in automatically to your user control panel, just be sure your browser doesn't block any pop ups and permit them if that happens. For Enhanced accounts, there is a **Control Panel** link inside WebMail, also on the top right.

You can also access the user control panel directly:

- Go to https://cp.emailarray.com
- Log in using your full e-mail address (user@domain.com) and current password.

Notice you can also set spam filter preferences on the domain level, to define settings for users that don't have custom preferences saved, however, our goal in this FAQ is to detail the user level preferences and management.

After logging in and click on **Filtering**, on the top bar, the options are:

Accept e-mail from:

- **Everyone, Whitelist & Address book:** This is the default option and lets all messages reach you. Further down, we mention the option that controls if you want to send spams to your spam box, but it depends on this option being set.
- **Whitelist & Address book:** This option only allows messages present in the Whitelist & Address book to reach the Inbox, the rest will be sent to your spam folder.

System default is to accept emails from everyone, but the option to accept only from whitelisted senders and contacts in your address book is a nice alternate way of receiving practically no spams in your inbox, at the cost of having to check your spam folder or spam reports, from time to time.

Blacklisted Messages: What to do with messages whose senders are in user's or domain's blacklist. The default is to delete them, but you can have them moved to your spam folder.

Enable autowhitelist: All e-mails sent by this e-mail account have the recipient's address of each e-mail added to the domain's auto-whitelist. Can be dangerous if a user account is compromised,

sends spams and automatically all recipients of such spams are added to the domain level auto-whitelist (accessible in Filtering > Auto-Whitelist, in the admin panel), which would require cleaning up the auto-whitelist. This option is enabled by default.

Send spam to: this controls what happens to messages which are identified as Spam.

- **Spam folder:** Places the Spam messages in the Spam folder
- **Deliver to Inbox:** Delivers the Spam messages to the Inbox, basically same as disabling anti-spam for this user
- **Delete:** Deletes the Spam messages

Filter sensitivity: The filtering system can be adjusted on a scale from 1 to 10, with 10 being the most restrictive while 1 is the most permissive. We find that the default setting of Regular Sensitivity is just right for most users.

Keep Spam for: How many days to keep the Spam messages in your Spam folder.

Send Spam E-mail Report every: This defines how often you wish to receive in your Inbox the summary of Spam messages trapped over the past few hours (default is every 12 hours), or if you want it disabled. Using the report received via e-mail, you can easily click on the item in the Via column, which opens up the user panel and lets you deliver & whitelist an email/sender, just deliver the email (deliver only) or delete it. In the From column, click on the sender to preview the e-mail in the browser.

Spam E-mail Report Format: Lets you choose the format of the Spam Report message. Default is HTML and TEXT.

Detect Forged From: Creates a rule for user which checks if SMTP authentication has not occurred when the sender's e-mail address of a received e-mail is the same as the recipient account's address. Such messages are moved to user's spam folder. Click here for our wiki page about this topic.

After making any changes, click on the **Update Settings** button.

Managing spams

Note that e-mail accounts have a folder entitled "Spam", where messages detected by the system as spam are moved to. Such folder can be viewed via WebMail or using an email client with your account setup as IMAP, which may require right clicking the account root in your email program and subscribing to the Spam folder. If you use POP (not recommended), you should use the spam reports (described below), to release messages incorrectly detected as being spam (false positives) and you can also log o WebMail and view the Spam Folder, moving any false positive to your inbox.

Spam reports lead you to the user's control panel Spam quarantine and it is the best way to release false positives, as you can automatically deliver the email and at the same time, add the sender to your whitelist.

If you want to help us with undetected spam emails or emails incorrectly identified as spam, please contact our support. Consider also creating an account at SpamCop in order to use the system they provide to report spam.

Spam reports and Spam Quarantine

The system sends an email to your inbox, by default every 12 hours, detailing the emails caught in your spam folder, so you don't have to constantly check your spam box. The feature is extremely useful for those who use POP accounts with an e-mail client, since in that case, you cannot view the spam folder, except via WebMail.

Spam reports are sent from the sender "Spam Monitor" and let you click on the **Via** column of each e-mail listed, which opens your account's control panel. Login with your email address and password and you will be directed to the **Spam Quarantine** section. Click on the **Display** button to view the list of spams in your spam folder, being able to change the visualization criteria, such as view by **Date** (All or a specific date) or **filter by** text in the From, Subject or Unique ID fields.

Click on the **From** or **Subject** column on any of the listed e-mails to preview their content.

When you view the list of spams in your Spam quarantine/box, notice there's a checkbox next to each e-mail, which lets you select several e-mails at once and take some action, such as "**Deliver & Whitelist**", which delivers a message incorrectly detected as spam to your inbox and allocates the sender on your whitelist. Other options include "**Blacklist & Delete**", which can be useful to minimize the amount of spams received, as you can first deliver & whitelist the legit e-mails and then, possibly blacklist & delete from spam folder all the rest. Just be careful as, if there's some spam with a forged FROM address, you might end up blocking a legit sender. To check each senders FROM address, roll over the From field of each e-mail listed.

Other options include "**Delivery only**", which only delivers a spam to your inbox but does not whitelist the sender, useful if you're unsure if the email is legit or not and just want to deliver the e-mail to your inbox and **"Delete"**, to simply delete the selected e-mails(s), which is the same as deleting them directly from your spam folder.

Remember you can always view all your blacklist and whitelist entries, as well as add new entries manually, as per our respective FAQ.

Tips

The Anti-Spam tips below are also very important to have better results.

- If you receive too much spam in your account, consider creating a new email address and preserve it. Use an alternate email address created on a free email service such as Hotmail, to be

used when filling out forms in web sites, especially those that can expose your data, such as your domain's registries Whois.

Consider having an alternate address to promote socially, and maintain your own address domain restricted for work.

- When you create a new e-mail account, avoid common words before the @ sign, as John. Prefer to use, for example, johndoe@yourdomain.com.

- Use forms on your site, without publishing your email address explicitly. Forms allow you to be contacted without having to display your e-mail address, since spammers often track web pages looking for email addresses.

- If you want to publish your email address on web page, consider encoding it.

- Never reply to spam e-mails, since it is often a confirmation of the existence of your e-mail, as well as a trigger for auto-whitelisting, which adds all addresses to whom you send e-mail in your domain's auto-whitelist, feature which can be disabled in the Filtering section of your control panel.

- One interesting idea is to create aliases for your account and use them when informing your e-mail addresses in certain places, where you believe it could be exposed and spammed to. This way you can easily remove such alias, to stop receiving such emails. Another option is to create disposable addresses, such as a Dynamic (wildcard) extension.

Whitelist or Blacklist an e-mail address

Whitelist / Blacklist an e-mail address

Our system automatically whitelists e-mail addresses that you communicate with, for your entire domain. For example, within your domain hosted with us, you have two users: joe@domain.com and amy@domain.com. If joe e-mails mary@hotmail.com , mary@hotmail.com will become whitelisted for both joe and amy. If mary@hotmail.com decides to write to amy@domain.com or joe@domain.com, her e-mail will get through without being filtered. For more details on this, please see our page about whitelist / blacklist on domain level.

You can also manually add an e-mail address to the whitelist or blacklist, as described below. Notice that the best way to add whitelist records is using the Spam reports, as it automatically delivers the e-mail and adds sender to your whitelist. Our system uses the Sender instead of the From in the e-mail header, both for blacklist and whitelist, which is automatically done if you authorize e-mails through spam reports. If you enter an e-mail address manually to your black or whitelist and notice it doesn't work, check the e-mail header and look for the **X-EmailArray-EnvFrom:** field, which should be used. Yet another possibility is that the sender might change each time you receive a certain e-mail. In this case, you can use Rules to delete undesired messages, based on part of the From header address or subject.

Add an e-mail address to the whitelist

- Go to https://cp.emailarray.com
- Log in using your full e-mail address (user@domain.com) and current password.
- Pass your mouse over the **Filtering** menu and choose Blacklist
- Make sure you have the correct domain selected in the pull down menu on the left side
- Click on the **New Whitelist** button
- In the text field next to **Address**, enter the e-mail address you wish to whitelist
- Select whether you still wish to check for viruses (Recommended!)
- Click on the **Add Whitelist** button

Add an e-mail address to the blacklist

- Go to https://cp.emailarray.com
- Log in using your full e-mail address (user@domain.com) and current password.
- Pass you mouse over the **Filtering** menu and choose Blacklist
- Make sure you have the correct domain selected in the pull down menu on the left side
- Click on the **New Blacklist** button

- In the text field next to **Address**, enter the e-mail address you wish to blacklist
- Click on the **Add Blacklist** button

Remove an e-mail address from the whitelist or blacklist

- Go to https://cp.emailarray.com
- Log in using your full e-mail address (user@domain.com) and current password.
- Pass you mouse over the **Filtering** menu and choose either **Blacklist** or **Whitelist**
- Make sure you have the correct domain selected in the pull down menu on the left side
- Click on "**-**" icon (minus sign) next to the e-mail address you wish to remove

Retrain Messages

Sometimes it happens that messages are classified incorrectly by the filtering system.

A **false positive** refers to a message that was incorrectly classified as being Spam.

A **false negative** refers to a message that was incorrectly classified as NOT being Spam.

In other words, **false positive** messages end up in the Spam folder instead of the Inbox, while **false negative** messages end up in the Inbox instead of the Spam folder.

We have several methods to help retrain our system so that it doesn't make the same mistake again:

- In your configured IMAP account or in Webmail, simply drag the message from the Inbox to the Spam folder or vice-versa and keep it there at least overnight
- Retrain using the **Spam Quarantine** feature of the User Control Panel:
- Go to
  Unknown macro: {link-window}

  https://cp.emailarray.com
- Log in using your full e-mail address (user@domain.com) and current password.
- Click on the **Spam Quarantine** icon
- Search for the Spam message by selecting the appropriate date, optionally defining a search term and clicking on the **Display** button
- Mark the checkbox next to desired email and click on one following buttons: **deliver and whitelist** the sender, **deliver only** or **delete**
- Forward the offending message to the specific retraining address as defined by your Administrator. Usually they are of the form: spam@domain.com & notspam@domain.com

Track Remote Deliveries

You can easily determine if the messages you send out reach your recipients or not. While this is no guarantee that your recipient read the message, you can at least find out if their e-mail services provider properly received the message and warn them in case of problems.

- Go to the User Panel: https://cp.emailarray.com
- Log in using your full e-mail address (user@domain.com) and current password.
- Click on the **Track Deliveries** button

By default, after clicking on the **Search** button, you will see the list of e-mails that you sent during the current day and which were delivered. You need to click on the arrow next to each delivery's date/subject to view details.

You can alter your search criteria and filter out by: **Temporarily Rejected Messages** (for example, user is over quota), **Permanently Rejected Messages** (invalid mailbox, blacklisted, etc.) or **All Messages**. You can also specify the range of dates to search for while also specifying the e-mail address where you sent it.

Optionally, you can mark the checkbox next to **Send me a monthly PDF report**, to receive such reports via e-mail.

> You can review Remote Delivery data for up to 60 days in the past

Here's an example of a successful delivery:

2014-10-27 15:24:35 - test
Sent From: tests@emailarray.com
Sent To: "testsemailarray@gmail.com"
Recipient delivery status: Message accepted
Message delivery status: 74.125.193.26 accepted message.Remote host said: 250 2.0.0 OK 1414437875 x11si18095722icx.68 - gsmtp

In this case, email was delivered to the remote server who answered with some SMTP codes initiated by the number 2, indicating that such e-mail is in the queue to be delivered to the recipient. It does not mean the recipient received or read the email, but usually that should occur, since the remote server did receive it and queued it to be delivered, unless recipient's mail server has some technical problem.

If our server is unable to connect to the recipient server, it will try to send your e-mail for 7 days, after which it will bounce back an error message indicating that the email could not be sent. In these cases, a temporary rejection error is presented, such as the example below:

From and To: may show as "null", since our server did not even connect to the recipient server
Message delivery status:Sorry, I wasn't able to establish an SMTP connection. (#4.4.1)

There isn't an always guaranteed way to know that the recipient read an e-mail. Some email clients, such as Thunderbird, Windows Live Mail and our WebMail are able to send a delivery receipt, which can be granted if the recipient decides to do so. On the other hand, some clients such as Thunderbird and Outlook are able to send a delivery receipt, to verify if an e-mail was received by a recipient server, however, many servers don't grant such confirmation.

Still, some services do offer a way to track if a user opened an email, such as the free WhoReadMe or ReadNotify (paid), sometimes criticized since they do track if an email was opened through an image/link embedded in it. Such services depend on adding their domain at the end of the recipient's e-mail address, so your e-mail passes through their server, which sends to the destination and tries to verify delivery.

Configure Incoming E-mail Rules

Incoming E-mail Rules

You can specify several rules that will apply to **Clean** messages only, before they reach your Inbox.

This will allow you to deliver certain messages to special folders or redirect them to other e-mail addresses.

> Rules will apply in the order they are created

Add a new rule

- Go to the User Panel
- Log in using your full e-mail address (user@domain.com) and current password.
- Click on **Delivery Rules** icon
- Click on the **New Rule** button
- Enter a unique rule name (without spaces in the name) and click on **Add Rule** button
- Click on the **Edit** icon (pencil) next to the newly created rule

Rules are composed of two sections. **Conditions** and **Delivery rules** once a match is found

You can add multiple Conditions and multiple Delivery rules within one rule.

After you click on the Edit rule icon, you will see buttons to create Conditions and Delivery rules.

Within the **Condition** you can match a message on the **From, To, CC, To or CC, Subject, List-ID** fields, or according to **Message size**.

Let's setup up a condition for our new rule. Click on one the two buttons: **NEW 'AND' CONDITION** or **NEW 'OR CONDITION'**.

Define your conditioning. Below is an example of a condition that will check for a certain text in the e-mail's subject.

Match Field: Subject
Condition: Contains
Negate match: No
Term: test subject

After the new conditions has been defined, click on the button **Add Condition** button.

You will see that your rule is now partially created, with a condition, but missing a delivery rule (action). **Delivery Rules** can be used to either deliver the message to a specific folder, send it to another e-mail address or delete it.

So now, let's choose our desired action. We will click on the **Deliver to e-mail button**, and inform a certain e-mail address, as we want to forward emails that have a subject "test subject" to this address. After that, click on the **Deliver** button.

Let's add yet one more rule, as we want the original account to also receive such emails. So let's click on **Deliver to Folder** an choose the original account's **Inbox**.

Now, check the Status of the rule, on the top. It will probably show as **DISABLED**. Click on top of **DISABLED** so it becomes **ENABLED** and, finally, click on the **Save Rule** button.

> A new rule won't take effect until the **Activate** button is clicked after you finished building your rule. After each modification to the Clauses or Delivery rules, the **Activate** button must be clicked.

Remove a rule

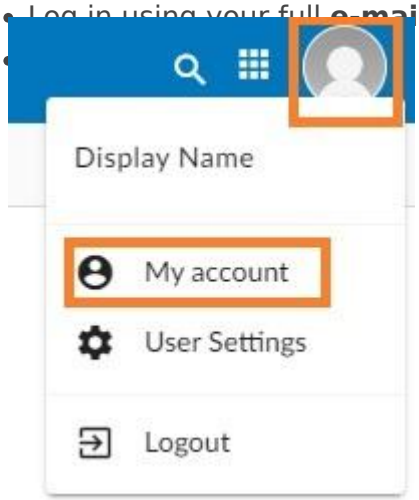
- Go to the User Panel
- Log in using your full e-mail address (user@domain.com) and current password.
- Click on the **Delivery Rules** icon
- Click on the "-" icon (minus sign) next to the rule you want to remove

Disabling local delivery to an account

Note that the procedure below is unusual. It may be useful, for example, if you want an account do not store received emails (to prevent the account from reaching its storage limit), but forward incoming emails to another account (case in which you'd have to setup a forwarder). Use with caution and note that you lose the backup functionality of incoming mail for the source account.

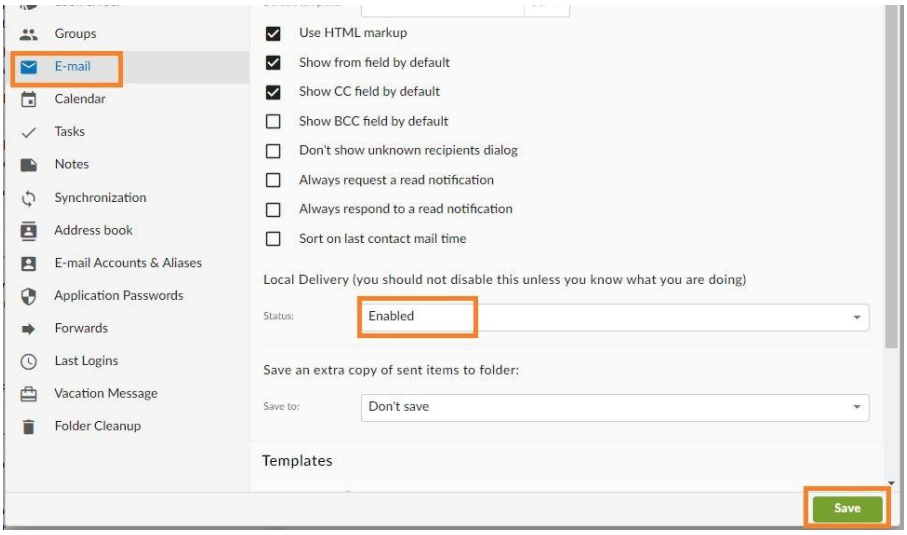
See below how to disable local delivery to an account (incoming emails are NOT stored in the e-mail account).

Option 1: from the Webmail

- Go to the **Webmail**
- Log in using your full **e-mail address** and your **current e-mail password**
- 

the top right to activate the menu. Then click on **My account**

- In the **E-mail** tab, find the Local Delivery section.



- Change the status to **Disabled**
- Click on the **Save** button

Option 2: from the User Panel

- Visit the [User Control Panel (https://cp.emailarray.com)]
- Log in using your full e-mail address (user@domain.com) and current password.
- Click on the **Local Delivery** icon
- Change the Status to **Disabled**
- Click on the **Update** button

How to avoid forged e-mails?

The From header of an e-mail, which you view in the header of e-mails can be anything, it doesn't even need to be a valid e-mail address and it can be different from the actual sender of the message.

For that reason, it's possible that you will receive forged e-mails as if they were sent from/to your account or from some other account in your domain to you. Usually, such emails, many times hoaxes or phishing attempts, are correctly caught as spam.

Let's start off enabling a rule that tries to catch e-mails sent from and to your account. So for example, From test@emailarray.com and To test@emailarray.com.

- Go to https://cp.emailarray.com
- Log in using your full e-mail address (user@domain.com) and current password.

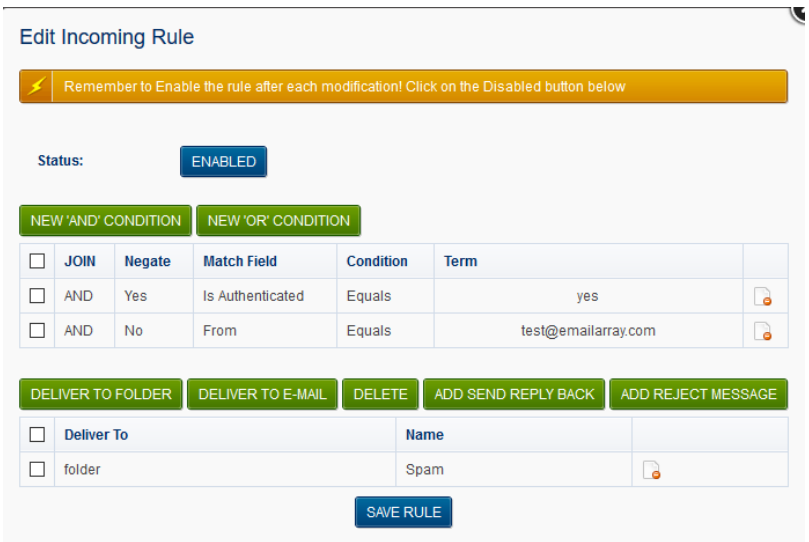
Alternatively, you can login to the user control panel using the respective link while logged to Webmail.

After logging in and click on **Filtering**, on the top bar.

Change the **Detect Forged From** pull-down menu to **Yes** and click on **Update settings**.

Afterwords, click on **Home** in the top bar, followed by the **Delivery Rules** icon.

You will notice a new rule entitled "DetectForgedFrom". Click on the **pencil icon** next to it, to edit it. This is what it looks like:



What the rule does is check if the user did NOT authenticate using our SMTP (notice that the Negate column for the first condition is set to Yes) and uses your address as a FROM address and in

such cases, it moves such e-mails to your spam folder.

This rule can currently be created only on the user level, however, if you decide to implement it for all your users, contact us, and we will enable it automatically for everyone.

One possibility is to change the folder where such e-mails are sent to. This will let you tweak the rule in an easier way. First of all, create a folder in WebMail or an e-mail client using IMAP, such as "Forged". Then, simply click on the **minus sign icon** next to the Spam folder action (shown above), click on **Deliver to folder** button and choose your "Forged" folder.

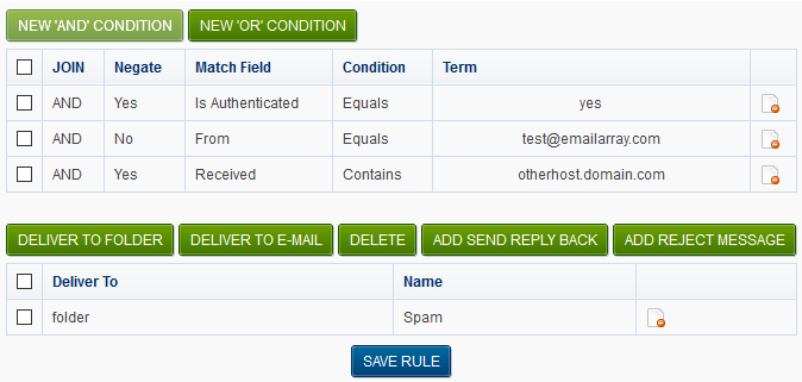
Notice that there's another rule entiled "SpamDelivery", responsible for moving spams to your spam folder and it comes before the Forged From rule. For that reason, forged e-mails detected as spam will be moved to your spam folder. If you decide to create a separate folder, such as the suggested "Forged folder", consider clicking on the **up arrow** next to the Forged From rule and moving this rule above the SpamDelivery rule. This way, all forged e-mails will be sent to your "Forged" folder, avoiding clutter in your spam folder.

Besides catching forged e-mails, this rule may catch legitimate messages that were send as being you, from some other SMTP server. For example, some website form or application that sends emails using your e-mail address in the From header.

You can tweak the rule by denying such cases, so the filter does not catch such cases.

For example, let's say you receive legitimate e-mails that come From your email and to your e-mail address, sent from a remote server called otherhost.domain.com, which is the hostname of the system that sends our server the e-mail, shown in the e-mail header. What we do is click on **New And Condition**. This new condition should have the **Match field** menu set to **Received** and **Negate Match** set to **Yes**. In the **term** field, type in otherhost.domain.com and click on **Add Condition**. Notice that rule is not set to Disabled. Click on the **Disabled** button to enable the rule and click on **Save rule**. What we did, is inform the system to NOT run the rule for e-mails that come from otherhost.domain.com.

This is how the rule now looks:



Let's consider one last scenario. Consider that you want to avoid forged e-mails coming from ANY account of your domain, not just your own account.

In such case, click on the **minus sign icon** next to the FROM condition and add a **New And Condition** of the **type FROM** and for **Term**, type in **your domain**, in this case "emailarray.com" (without quotes).

It might give you a bit of work to fine tune the rule so that it is near perfect, but many customers and companies consider it a good idea.

CalDAV Synchronizer Setup

> **Enhanced mailbox only.**
> Enhanced mailboxes allow you to sync calendars (CalDAV) and contacts (CardDAV) across multiple devices with applications that support the CardDAV/CalDAV protocols.

In Outlook you can sync via CalDAV / CardDAV by installing the caldavsynchronizer - an Open Source plugin that you can install on your computer and use with your Outlook. This plugin supports Outlook 2007 to Outlook 2016 and is Free and Open-Source Software (FOSS), licensed under AGPL 3 and developed by Alexander Nimmervoll and Gerhard Zehetbauer. You can find the project on Github and SourceForge.

This is a step-by-step guide to installing and setting up the caldavsynchronizer plugin.

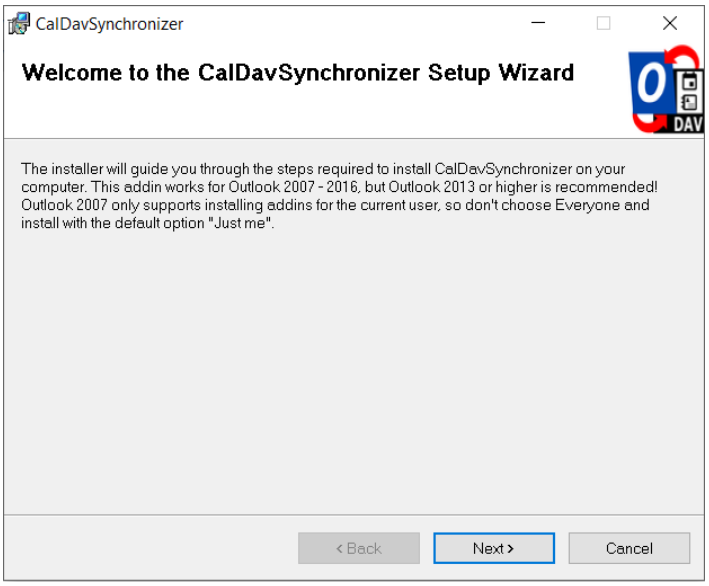
1. Download the caldavsynchronizer

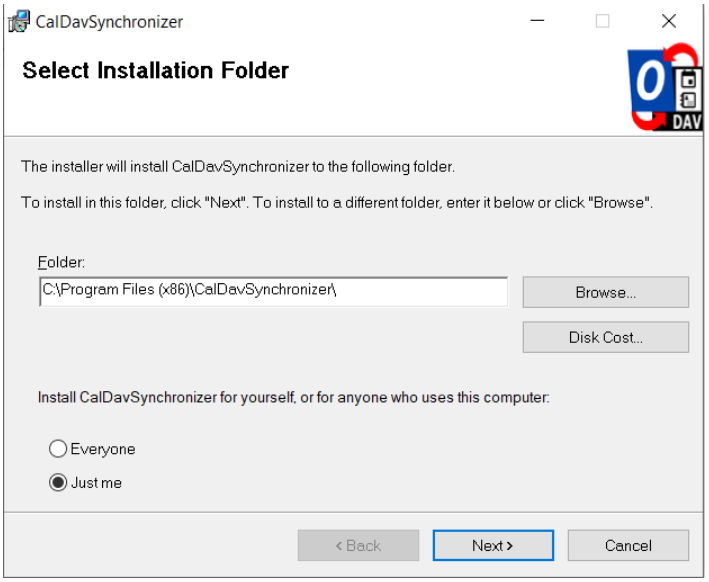
You can download the caldavsynchronizer plugin from the project's website:

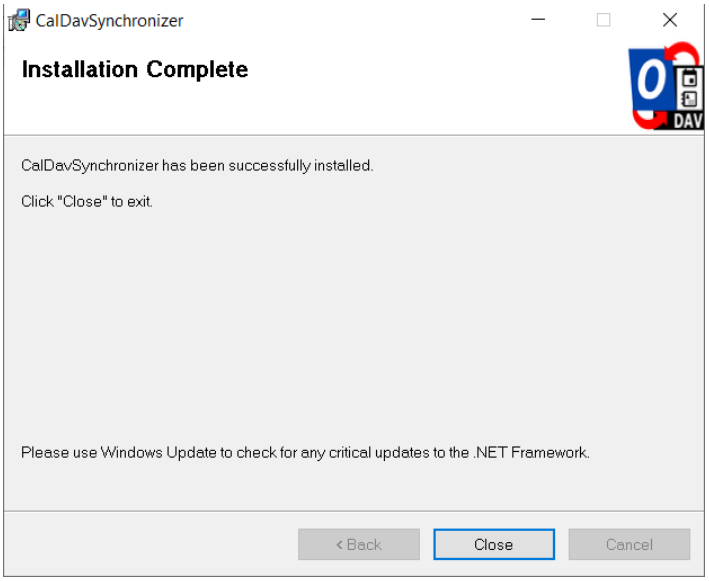
https://caldavsynchronizer.org/.

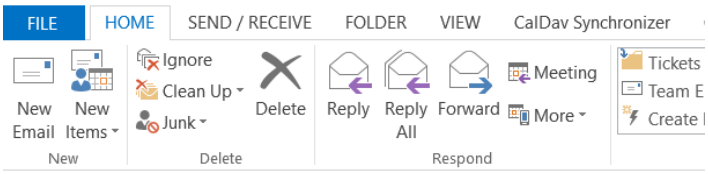
2. Install the caldavsynchronizer

Extract the downloaded .zip file and start the installation. Once the installation is complete, you will see a new ribbon called "CalDav Synchronizer" in your Outlook.


CalDavSynchronizer
Welcome to the CalDavSynchronizer Setup Wizard
The installer will guide you through the steps required to install CalDavSynchronizer on your computer. This addin works for Outlook 2007 - 2016, but Outlook 2013 or higher is recommended! Outlook 2007 only supports installing addins for the current user, so don't choose Everyone and install with the default option "Just me".
< Back
Next >
Cancel


CalDavSynchronizer
Select Installation Folder
The installer will install CalDavSynchronizer to the following folder.
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".
Folder:
C:\Program Files (x86)\CalDavSynchronizer\
Browse...
Disk Cost...
Install CalDavSynchronizer for yourself, or for anyone who uses this computer:
Everyone
Just me
< Back
Next >
Cancel

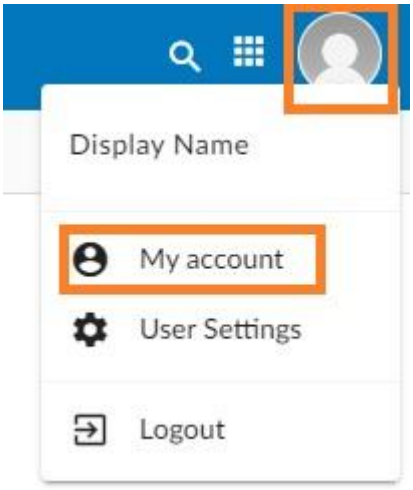

CalDavSynchronizer
Installation Complete
CalDavSynchronizer has been successfully installed.
Click "Close" to exit.
Please use Windows Update to check for any critical updates to the .NET Framework.
< Back
Close
Cancel



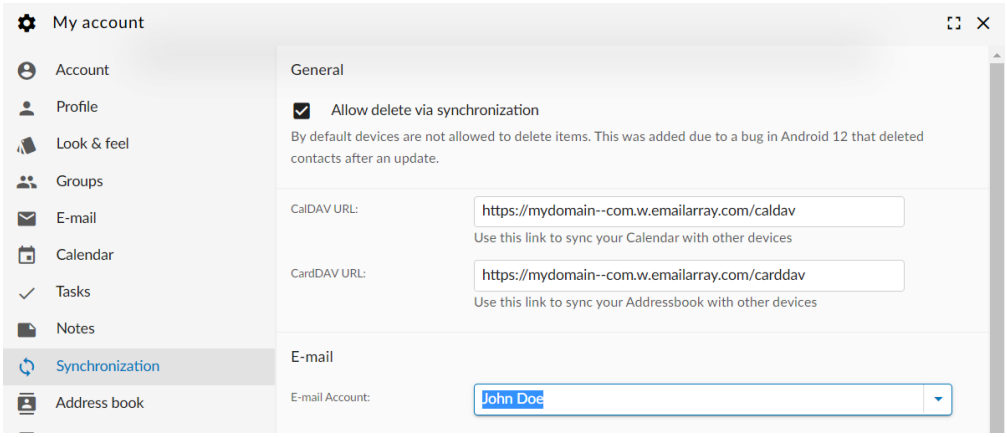
3. Get your CalDAV / CardDAV URLs

First, you need to obtain your CalDAV / CardDAV URLs. CalDAV is for Calendar synchronization, and CardDAV is for Contacts.

- Log into the Webmail using your full **e-mail address** and your **current e-mail password**
- Click on the **User** icon from the top right to activate the menu. Then click on **My account**

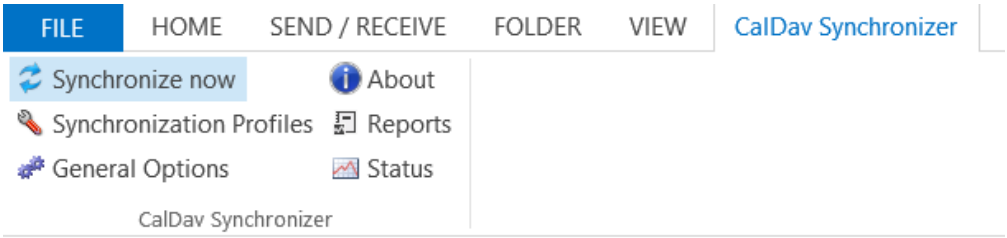


- In the **Synchronization** tab, find the CalDAV / CardDAV URL. You will need to copy and use these URLs with the caldavsynchronizer.

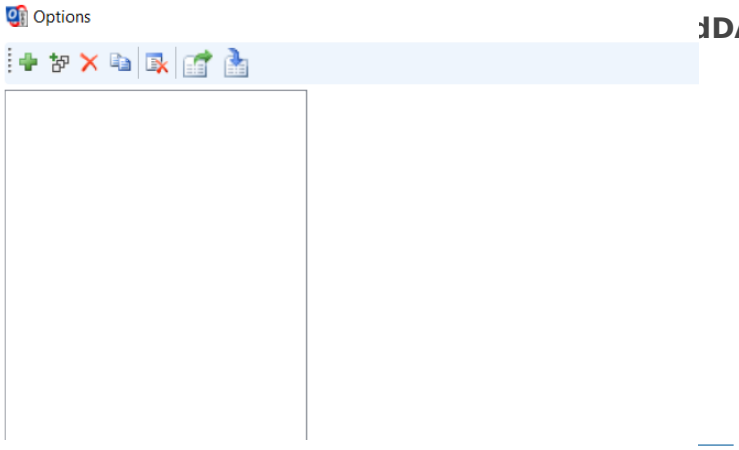


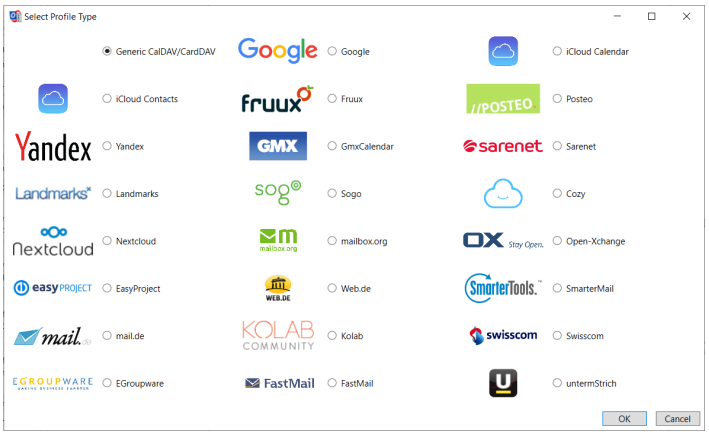
4. Set up the caldavsynchronizer

- Open **Outlook** on your computer.
- Go to the **CalDav Synchronizer** ribbon. Click on the **Synchronization Profiles** option.



- Click on the **Add** button (plus sign) to set up a new Calendar or Addressbook to sync. **DAV**.

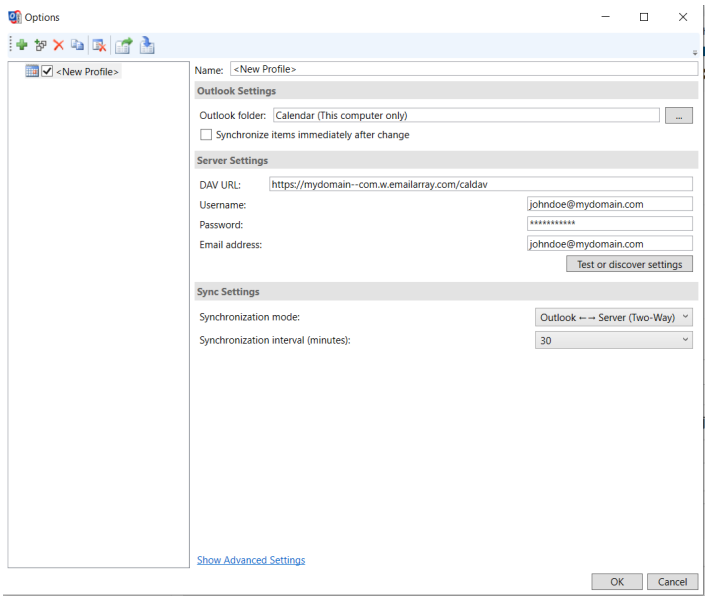




- A new profile window will show. Fill in the following details:
  - Name: give a name to this profile. For example, Calendar - personal, or Calendar - work.
  - Outlook folder: create a new folder in the **Calendar Items** or **Contact Items** category. You can also choose an existing Calendar or Contact folder.
  - Server Settings: these are your CalDAV / CardDAV details:
    - **DAV URL**: if you're adding a **Calendar**, use the **CalDAV** URL obtained from the Webmail at step 3. This URL should be in the form of https://mydomain–com.w.emailarray.com/caldav - be sure to replace mydomain--com with your own domain name. If you're adding a **Contact** list, use the **CardDAV** URL.
    - **Username**: your full email address

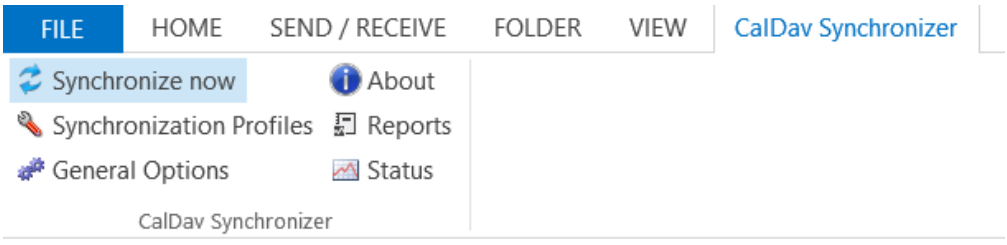
- **Password**: your email password
- **Email address**: your full email address
- Click on the **Test or discover settings** button. If you have multiple Calendars (or Contact lists) you can choose which one of them to sync with this Profile.

- Sync Settings: choose how and how often to synchronize the Profile. **We recommend the Outlook ↔ Server (Two-Way) synchronization mode**.
- After you finish the setup, you can choose to synchronize items immediately after change by ticking the option in the Outlook Settings. Please note you can only activate this option after you have finished the above setup and clicked on the Test or discover settings.
- Click on the **OK** button to finish setup and save changes.



5. Synchronize your new Profile

If the synchronization didn't start automatically, you could manually sync by going to the CalDAV Synchronization ribbon in Outlook and clicking the **Synchronize now** option.



> You can now set up a new Calendar or Contact list by adding a new Profile (step 4).

ownCloud - free file storage and sharing on the cloud

With ownCloud, we provide fully-featured file sync and sharing solution, with access to your data through a web interface, sync clients or WebDAV, while providing a platform to view, sync and share files across your devices easily all under your control.

This is an extremely useful feature, as it lets you synchronize your most important files to our cloud storage, keeping them safely backed up for up to 30 days. Besides that, it lets you install the ownCloud app on your mobile devices, such as smartphones and tablets, so that your files are easily accessible from wherever you are. There's more... You can also view and edit your files with an easy to use, visually clear and fast interface and share files with external users, using safe links generated by ownCloud, protect them my password and even set an expiration date for them.

You can even edit PDF, text and Office files using the web interface (https://files.emailarray.com), complete with revisions available for each copy you edited, with the option to roll back to a previous version of the file (up to 30 days).

Enhanced accounts have the advantage of being able to share files between users, including revision control, which details changes made to a file which is accessed by several users. You can even work at one same file at the same time as a colleague and, in real time, owncloud shows you who is editing what (text) with a differentiated color. If you have an existing Enhanced account, please open a ticket so that we can enable Owncloud in your account.

We are offering 5 gigabytes of space on ownCloud FREE to each basic e-mail account and 15 GB for enhanced accounts.

You can easily setup ownCloud to sync files from your local computer/devices (smartphones/tablets) to our ownCloud storage.

Logging in the web interface and downloading the sync client

Our goal with this FAQ is to get your started with the sync client. First of all, access https://files.emailarray.com and login with your e-mail address and respective password.

Authentication credentials are the same as your e-mail account, thanks to our single sign-on technology.

After you first login, ownCloud offers you the desktop client (Windows, OSX or Linux) and apps for both Android and iOS.

We'll focus on the desktop client. You can download the apps for mobile devices later, accessing from them.

When you click to download the desktop client, you are taken to https://owncloud.org/sync-clients/

In the Sync section (step 2), click on Desktop Clients and choose the version you desire, Windows, Mac or Linux.

Before installing the setup file you downloaded, feel free to take a look around ownCloud's web interface, create a new text file, edit it online, share the example files with external users (link), etc.

Regarding sharing, you can share files with other users of your domain, by clicking on the "Share" link next to each file and typing in your colleague's e-mail address. The system will find the address and you must click on it. The file will be shown on the side in "Shared with others" and for the user you shared it with, in "Shared with you". You can also click on the Share link and then mark the check box "Share Link", which is a very useful feature that lets you provide a secure link for anyone to be able to download the file, with options such as password protection and expiration of the link.

Regarding deleted files, you can restore them in the "Deleted files" link, on the bottom left. Then, pass your mouse over the file you want to restore and click on the "Restore" link.

Consider watching this short introduction video (5:14 min.):

https://www.youtube.com/watch?v=RrAhClhrRAc

Let's proceed to installing the Sync client on your computer.

Installing sync client on your desktop computer

Install the setup file, choose the Standard installation, click on **Next** twice and then click on **Install** .

At the end of the installation, ownCloud will offer the option to load it (checkbox enabled by default).

After it loads, you are requested for the server address. Type in: https://files.emailarray.com and click on **Next**.

In the **username** field, type in your full e-mail address, its respective **password** and click on **Next**.

ownCloud will now offer to sync all files on the server. If you haven't used our service before, then you don't have any of your files stored by us yet, rather just a few test files that ownCloud adds itself to every new account, approximately 3 MB. So you can safely keep the default to sync all files from Cloud to your computer, which is useful even so you can start to understand how it works.

The default directory used by ownCloud is the owncloud folder under your Users folder, on your local computer. You can easily change such location, if needed.

Click on **Connect** and then two options will be shown.

- **Open ownCloud in browser** - same as accessing https://files.emailarray.com from your browser. Lets you see all files stored on your cloud storage, even being able to view, create, edit and share files.

- **Open local folder** - opens your local computer folder which is synced to your cloud storage. If you click here, you will probably notice that the example files added by ownCloud to your account have already been synced to your local ownCloud folder.

Click on **Finish**.

Sync client settings

Let's now open ownCloud program, recently installed on your computer again. Below, a few tips on the main sections of the desktop client interface:

- The first tab, which mentions your account, shows you how much space you're using on cloud storage and lets you add folders for synchronization.

The **Add folder to Synchronize** button will be dimmed out. If you want to change your local sync directory, you will need to click on the ... icon next to current folder used for sync (probably ownCloud folder, as explained before) and click to remove it. Now you will be able to change your local sync directory.

When you add a new directory for sync, you first choose the local directory and, in the next step, where in the remote cloud storage you want to sync that directory with, if the root "owncloud" and all subfolder or only some subfolder(s).

If you choose to sync a local folder to "owncloud root", you are unable to add more directories to sync, as seen initially. If you set to sync local directories to certain folders in your cloud storage, then you're able to add several folders for synchronization.

Perhaps the easiest, is the default, of syncing your users ownCloud local folder with the remote owncloud root and store all files you want to sync, in your local owncloud directory, even moving existing directories to here.

If there are files/folders you don't want to sync, you have to specify them in the **General tab**, under **Edit ignored files**. For example, in your local owncloud folder you don't want to sync files in the subfolder **games**. Simply add a new file to ignore and type in **games**. You will see, in the **Activity Manager** tab, that it will be bypassed.

Edit ignored files is also useful if there are folders/files in ownCloud that you don't want to sync back to your local computer, all you have to do is specify their names.

- Under **Activity**, ownCloud shows you status of files synced to/from your cloud storage.

- In the **General** tab, you might want to mark the checkbox to **Launch on System Startup**, so that ownCloud will always be enabled on your computer, sycing files from/to your cloud storage.

Apps for mobile devices

In the case of Android, ownCloud's app has a small cost of US$ 0,99. An alternative is a free app called ocloud for owncloud, which has been tested by us and works fine.

For iOS, the paid official app costs also US$ 0,99. The only free alternatives we found for iOS are developed by universties that use ownCloud, such as South Oregon University's app (search for "SOU owncloud" in the app store), which does work if you specify our host * https://files.emailarray.com*.

We do recommend, however, the paid official app and can't be responsable for the apps provided by third party.