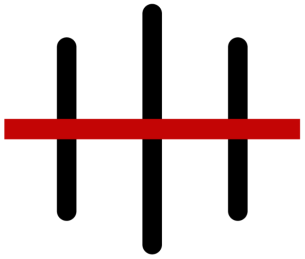

Cage Undefined

Mail Server Manual

Welcome to the mail server of Cage Undefined, a private and secure way to receive and send mail for your organisation. This document outlines how to configure your setup to work with our mail server.

We offer our mail service to animal rights aligned organisations completely for free. If you appreciate this service, please donate to our Patreon so we are able to keep providing services like these for free to those that can't afford it. Patreon.com/CageUndefined

Contents

Contents
Terms of service
  Bulk mail
  Access control
DNS
  Mail server
  Sender Policy Framework
  Domain Keys Identified Mail
  DMARC
  Automatic mail configuration discovery
  Finally
Webmail
  Roundcube
  CU Cloud
Other mail clients
  Protocols
    IMAP
    POP3
    SMTP
  Popular clients
    Gmail
Domain management
  Postfix Admin
Privacy & Security
  Our Security Measures
    Encryption
  Your Security Measures
    Password
    VPN
    POP3
    PGP
      PGP on Roundcube
    Mind other services

Terms of service

In order to be able to freely provide our mail server to other organisations at no cost, we require everyone to play nice and follow a few rules. Failure to abide by these may result in having your access to our mail server temporarily or permanently revoked.

Bulk mail

In order to keep our mail server's reputation in good standing and prevent our outgoing mail from being flagged as spam as much as possible, we prohibit the use of our mail server to send out bulk mail. This includes mail sent out through automation and mail sent out with an excessive amount of recipients. If you wish to send out mail through automation, we recommend Mailgun and Sendgrid. For newsletters, we recommend Beehiiv and Mailchimp.

Access control

Both user and admin accounts are permitted to be shared with other individuals at your own discretion, as long as it happens in a controlled fashion. For the sake of our security, we require you to at all times be aware of exactly which individuals have access to the domain administrator accounts managed by your organisation.

DNS

> ➢ If your domain is managed by Cage Undefined or a Cage Undefined partner (e.g. Vegan Hacktivists), then you can skip this section. We will take care of all necessary DNS adjustments for you.

To properly send and receive mail using our mail server, you will need to make a few adjustments to your DNS records. These changes are all outlined and explained below. For your convenience, all mentioned DNS records are also available as a text file in the BIND format at https://cumail.org/dns.txt, which can be imported by most providers for quick configuration.

If your provider does not allow you to fill in `@` for the name, fill in your own domain name instead.

Mail server

Type	Name	Content	Priority
MX	@	mail.cageundefined.org	10

The MX record specifies the mail server responsible for handling your incoming mail. This allows us to start receiving your mail. Make sure that no other MX records are configured for your domain.

Sender Policy Framework

Type	Name	Content
TXT	@	v=spf1 mx ~all

This TXT record configures the Sender Policy Framework (SPF) for your domain to allow our mail server to send mail as your domain. Without this record, your mail is likely to be filtered as spam. If you already have an SPF record configured for your main domain that you'd like to keep in order to also send mail using other services, simply prefix the current ruleset with "mx". For example:
`v=spf1 include:_spf.google.com include:mailgun.org ~all`
becomes
`v=spf1 mx include:_spf.google.com include:mailgun.org ~all`.

Domain Keys Identified Mail

Type	Name	Content
TXT	cu21._domainkey	v=DKIM1; h=sha256; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuBLLxsCNt1sv+TyHYWbU3nWleNepiqCwCb4aE0ece0pzHQ17A2cpZr5laN06XWd4pCqnqlw5vSdElb6wNTYtc7PIIoHAqPcyiODho85I61m0gBVHwdooh+aE+X4R1XAacwXcTXNQtToA/76APkSbUM7gAFzX4XcRte4ViFABbrMIMtcCq/NVbQ7HbMIjfcIxB9RMRUMwZUPp5cACcK8F4e/S8qLQfQ7XA9HlpBOjPxM1R1KAmFn1Wlfl2WUpjFcCN7wJieH6eIhCL/lPqPIKtZMlziO3pqBXaH0RnTESl50rvOLANwnen5YyTyniU+Suh4xQUkVtzxJJpsPgFslgIQIDAQAB

This TXT record configures DKIM to authorise our digital signature to be used for your domain. Without this record, we will have to sign your mail with our own domain and the recipient will see “Signed by: mail.cageundefined.org” instead when they receive your mail.

DMARC

Type	Name	Content
TXT	_dmarc	v=DMARC1; p=quarantine;

This TXT record configures DMARC for your domain, instructing other mail providers to authenticate your mail using the SPF and DKIM policies that are configured for your domain. If you already have a DMARC record set, you do not have to adjust it. Without this record, mail providers may still flag your mail as spam.

Automatic mail configuration discovery

Type	Name	Target
CNAME	autoconfig	autoconfig.mail.cageundefined.org
CNAME	autodiscover	autodiscover.mail.cageundefined.org
CNAME	maildiscovery	maildiscovery.mail.cageundefined.org

These records point modern email clients to our configuration server, using only the user's email address. This allows them to automatically look up the proper configuration to use with our mail server and lets your users login with just their email and password, without any technical knowledge.

Finally

With everything configured properly, we should now be able to receive and send mail for you using our mail server. Lastly, double check to make sure that you have no other MX records and only a single SPF and DMARC record set for your domain.

Webmail

If you're familiar with email services like Gmail and ProtonMail, then you're used to having an online web interface (webmail) to access your email. We also provide such an interface using Roundcube at cumail.org. To login, simply visit this URL and enter the login credentials that we've provided you with.

Roundcube

We use Roundcube to provide our webmail, which can be drastically different from the interface you're familiar with. If you have any feature requests or questions, please let us know and we'll try to address any concerns that you may have. If you do not wish to use our Roundcube web interface, but prefer your own mail client instead (such as your native mail app, Thunderbird or even Gmail), please check out the Other clients section. Keep in mind that if your mail client is managed by a third party, you may be giving up the privacy over your email.

CU Cloud

With your mailbox, you are also able to access our cloud services at cloud.cageundefined.org. This includes a webmail client that will at some point replace Roundcube, but also file storage and sharing, contacts and calendar. If your website is managed by us, you will also be able to access its files through here.

Other mail clients

While we provide a webmail interface for your email, you can also use your email on other clients through IMAP, POP3 and SMTP. To do so, find the “connect”, “add account” or similar option in your mail client and follow the steps you’re given. Whenever you’re asked for a username and password, use your full email address as the username, and enter your password as usual.

If your mail client has an automatic configuration option, you should be able to complete the configuration through that with just your email and password. If this is not possible, then note down the protocol that your client is using to connect and follow the advice for the protocol in the protocols subsection below. Whenever you’re asked for a server to connect to, enter `mail.cageundefined.org`.

Protocols

IMAP

IMAP is used to synchronise mail between your mail client and the mail server. This allows multiple clients or users to connect to the mail server at the same time and manage the same mailbox. To connect using IMAP, use port `993` when prompted and opt to connect using a secure connection (SSL/TLS). We do not support insecure connections over IMAP.

POP3

POP3 is used to retrieve mail from a mail server, and either delete it after or leave it untouched. This is not recommended when you want to use multiple clients or users to directly manage the mail on our mailserver. To connect using POP3, use port `995` when prompted and opt to connect using a secure connection (SSL/TLS). We do not support insecure connections over POP3.

SMTP

SMTP is used to send mail using a mail server and is used in conjunction with either IMAP or POP3 to make full use of your mail account. To connect using SMTP, use port `465` when prompted and opt to connect using a secure connection (SSL/TLS). Port `578` can also be

used which, although unrecommended, also supports insecure connections. We also offer insecure connections over port `25` for compatibility reasons, but using it is strongly discouraged.

Popular clients

Gmail

Despite Gmail users having their own mail account, you can import mail from other mail accounts on it as well. To do so, enter your settings and go to the tab “Accounts and Import”. Find the section “Check email from other accounts” and click on “Add an email account”, then follow the steps to add your account using POP3. Choose to also send mail using this account, then make sure you uncheck “treat as an alias”.

Domain management

If you require the ability to create and manage multiple mailboxes and aliases for your organisation's domains, then we can provide you with an account on our administration interface. We use Postfix Admin to provide this interface, which you can access at cumail.org/admin. Regular users can login there as well by navigating to the user section, in order to change their password and configure mail forwarding for their account.

Postfix Admin

Postfix Admin is the tool we use to allow users to manage the email settings on our mail server for their domains through a web interface. Through this you can freely create additional mailboxes for different departments in your organisation. Additionally, you'll also be able to create aliases for your mailboxes (e.g. to have hello@yourdomain function like admin@yourdomain) and create aliases for your domains (e.g. to have hello@otherdomain.com function as hello@yourdomain).

Privacy & Security

All Cage Undefined services, and especially our email, is designed with privacy and security in high regard. To that end, there are several measures that you might want to be aware of. Also remember that in the end, security is only as strong as the weakest link. So make sure that you are also taking appropriate measures to keep your data safe.

Our Security Measures

To safeguard your privacy, our servers are situated in a country with strong privacy laws and hosted by a privacy-conscious provider. Additionally, while all systems keep logs for diagnostic and security purposes, we securely wipe ours on a daily basis, shorter than it takes us to abide by a subpoena.

Encryption

While your mails are in safe hands on our server, domain administrators can opt for an additional layer of security by enabling encryption on any mailbox. This way, even with direct access to that mailbox, nobody without its password will be able to decipher its mails.
As mails can only be decrypted using the password for that mailbox, losing that password means that you will no longer have access to your encrypted mails. **We will not be able to restore this for you.**
To that end, while we recommend that organisational and personal mailboxes should be encrypted, business and administrative mailboxes should not be.
Your encryption setting will only apply to new mails. To encrypt/decrypt older mails, simply move them between folders to reprocess them under the new setting.

Your Security Measures

Password

Your privacy and security starts with your password. Make sure that you don't reuse your password for other services and ideally use a long, complicated password which you can store in a password

manager. If you don't know which password manager to use, you're free to apply for an account on ours.

VPN

Whenever you access outside systems like ours, traces of your IP address will be left behind. While we regularly erase these, you should always use Tor or an anonymous VPN such as Mullvad (paid by crypto) to maintain your privacy, especially when dealing with other systems. We do not recommend other VPNs that tie your account to your name, as they can easily be subpoenaed to pass on your activity. If you do not have the capability to obtain a crypto-paid Mullvad account, feel free to contact us. We will provide one for you at cost price.

POP3

If you trust your own system to be fully secure, then the safest way to use our mail is using POP3, while opting to delete the copy on our server once it's retrieved. This means that your and only your system has access to your mail, once it's retrieved.

PGP

Using PGP allows you to send and receive encrypted mails that nobody but the holders of the encryption keys can read, regardless of the mail server and who has access to your mail. We provide support for PGP on our own webmail (Roundcube), but you can also use PGP anywhere else using Mailvelope.

PGP on Roundcube

To use PGP on our webmail, create a PGP key in your settings (lock it behind a password), then share your public key with others by enabling 'Attach my public key'. People can now use your public key to send you encrypted mails that only you can read using your private key. To send encrypted mails to others, ask them for their public key and add it to your account when you receive it. Then simply enable 'Encrypt this message' when sending them a mail.

Mind other services

While your mails are safe with us, they might not be with your recipients and senders. Make sure that whoever you exchange emails

with is using privacy-focused services like ProtonMail or avoid the issue altogether by always using PGP with sensitive emails. Make sure that contacts that use PGP use it on a trustworthy email client that performs the encryption locally, instead of on the server.