


Mailcow

- [LDAP Authentication](#)
- [Split Delivery with Google Workspace](#)

LDAP Authentication

1. Sign in to your Mailserver

Anmeldung als Administrator 🌙 🇩🇪

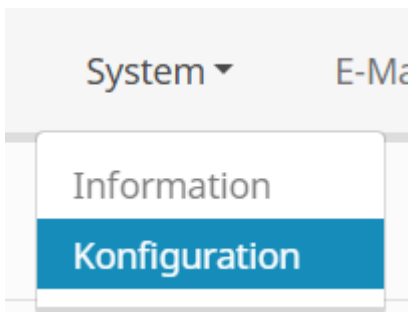


Anmelden

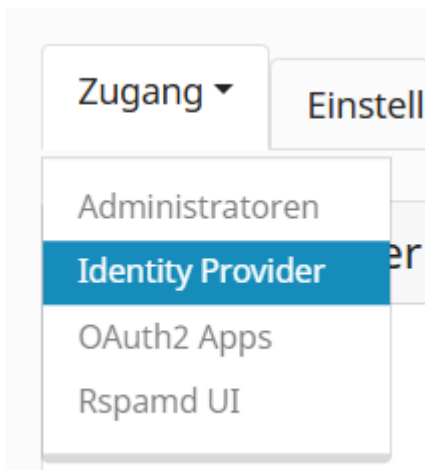
oder anmelden mit

FIDO2/WebAuthn Login

2. Go to *System - Configuration*



3. Access - Identity Provider



4. Setup LDAP Configuration

Identity Provider

Konfiguriere einen externen Identity Provider für die Authentifizierung
Die Mailboxen der Benutzer werden bei ihrer ersten Anmeldung automatisch erst

Identity Provider: **LDAP**

Server Settings

Host: 10.0.0.10

Port: 389

Encryption

Benutze SSL

Benutze StartTLS

Ignoriere SSL Fehler

Attributes

Base DN: dc=karger,dc=lan

Username Feld: mail

Filter:

Attribut Feld: objectclass

Bind Settings

Bind DN: CN=Ldap Bind,OU=Service Accounts,DC=karger,DC=lan

Bind Passwort:

Attribut Mapping: Attribut

Vorlage

Standardvorlage

Default

-- Vorlage --

Benutzer beim Login erstellen

Vollsynchronisation

Importiere Benutzer

Synchronization

Sync / Import interval (min) 5

Verbindung Testen

Änderungen speichern

• Server Settings

- Input either Hostname or IP (Recommended: *IP in case DNS f's up*)
- Port **389** for LDAP, **636** for LDAPS

• Encryption

- For LDAPS, use *StartTLS* not *SSL*
- For LDAP, disable *SSL/StartTLS* and Enable *Ignore SSL Errors*

• Attributes

- Base DN is usually your AD Domain (`dc=example,dc=local`)
- Username Field is the LDAP User Attribute that will be mapped to the appropriate Mailbox. If this is empty, nothing will be done.
- Attribute Field would be used for Attribute Mapping. With this a Mailbox Template can be assigned.

- **Bind Settings**

- Use a User that is not used for interactive Login and has limited Permission (*Read is enough*)

- **Synchronization**

- Enable User Creation so, on first login, the user is automatically created
- Enable Import to import and sync existing Users

Split Delivery with Google Workspace

What is "Split Delivery"?

Split Delivery is a common technique used when two separate Mailservers handle one singular E-Mail Domain.

Example: Mailserv 1 handles `user@domain.com` and Mailserv 2 handles `servicemail@domain.com`

What is required

- Two separate Mailservers (Google Workspace / G-Suite and Mailcow in this Case)
- Access and Understanding to DNS Records
- Understanding of DKIM/SPF
- Understanding of Mail Routing Policies
- Administrator Access to Mailcow
- Administrator Access to Google Workspace Admin / Google Admin Console

1. Mailcow Configuration

1. Open Mailcow Admin UI
2. Go to *System - Configuraiton*
3. Go to *Options - Forwarding Hosts*
4. Add public Mailserv IP's from Google here
 - `108.177.16.0/24`
 - `108.177.17.0/24`
 - `142.250.220.0/24`
 - `142.250.221.0/24`
 - `2600:1901:101::0/126`
 - `2600:1901:101::4/126`
 - `2600:1901:101::8/126`
 - `2600:1901:101::c/126`
 - `2600:1901:101::10/126`
 - `2600:1901:101::14/126`
 - `209.85.128.0/17`

- 74.125.0.0/16
- 66.249.80.0/20
- 173.194.0.0/16
- 64.233.160.0/19
- 172.217.0.0/16

2. Google Configuration

This Part is in German, English Names might be slightly different

2.1 Configure Mailcow Forwarding Host

1. Open Google Admin Console
2. Go to *Apps - Google-Workspace - Gmail*
3. Click *Hosts*
4. Click *Route hinzufügen*
 - Set *Name*, *Hostname* and *Port* of your second Mailserver to which E-Mails will be forwarded to
 - Enable TLS requirements and Host check. While not necessary, it is recommended

2.2 Configure Mail List

This Step creates a fixed List of Mail Addresses that will be forwarded. Will this is not strictly necessary, its a absolute way to make sure they're being forwarded

1. Open Google Admin Console
2. Go to *Apps - Google-Workspace - Gmail*
3. Click *Routing*
4. Click *Adresslisten verwalten*
5. Click *Adressliste hinzufügen*
 - Add all your Mail-Addresses
 - Uncheck *Authentifizierung erforderlich*

2.3 Add Route to Google

1. Open Google Admin Console
2. Go to *Apps - Google-Workspace - Gmail*
3. Click *Routing*
4. Click *Routing-Regel hinzufügen*
 1. Set Name
 2. Select *Eingehend* and *Intern - Empfangen*
 3. (Optional) Enable *Benutzerdefinierten Betreff voranstellen* and add [G-SUITE-RELAY]

4. Enable *Route ändern* and select your Mailserver Host created in 2.1
5. Click *Optionen einblenden*
6. Select *Unbekannte/Catchall Konten*

3. DNS Configuration

3.1 Add Google Mailserver' MX-Records

Based on Hetzner DNS

| Record Type | Domain | Value | Priority |
|-------------|--------|--------------------------|----------|
| MX | @ | aspmx.l.google.com. | 1 |
| MX | @ | alt1.aspmx.l.google.com. | 5 |
| MX | @ | alt2.aspmx.l.google.com. | 5 |
| MX | @ | alt4.aspmx.l.google.com. | 10 |
| MX | @ | alt3.aspmx.l.google.com. | 10 |

3.2 Add SPF/DKIM Records

3.2.1 DKIM

1. Open Google Admin Console
2. Go to *Apps - Google-Workspace - Gmail*
3. Click *E-Mail authentifizieren*
4. Select your Mail Domain

| Record Type | Domain | Value from Google |
|-------------|-------------------|---------------------|
| TXT | google._domainkey | v=DKIM1; k=rsa;.... |

3.2.2 SPF

You should edit your existing SPF Record from Mailcow, do not create a new one!

```
v=spf1 include:_spf.google.com ip4:<mailserver-ip> -all
```

`include:_spf.google.com` is the important part here. You simply include the SPF Configuration from Google