

# LDAP für zentrale Authentifizierung

Es gibt einen SSO Service via LDAP, der über warpsrvint läuft.

Für die Speicherung und die Bereitstellung der zentralen Anmeldungen wird ein OpenLDAP Server verwendet.

Es möglich, Dienste hierüber zu authentifizieren - mit dem Vorteil, dass es nur einen zentralen Ort gibt um User anlegen, löschen und bearbeiten zu können.

## Produktivumgebung

Aktuell existiert nur eine LDAP Server auf dem WebServer. Zukünftig soll der Server auf den internen Server warpsrvint repliziert werden.

Für Dienste ist der LDAP Server unter <ldap://10.0.20.2> erreichbar.

Das Benutzerinterface für die Verwaltung wird von [keycloak](https://keycloak.warpzone.ms) (ehemals [Warplnfra](#)) bereitgestellt und ist unter <https://keycloak.warpzone.ms> erreichbar.

Für die direkte Verwaltung des LDAPs für Administratoren ist unter <https://ldap.warpzone.ms> verfügbar.

## Testumgebung

FIXE

## Struktur des LDAP

Generell sind die LDAPs der Prod- und Testumgebung identisch aufgebaut. Lediglich in den Basisdaten gibt es Abweichungen um versehentliche Zugriffe auf die falsche Umgebung zu unterbinden.

Prod-Umgebung:

- Organisation: Warpzone
- Domain: warpzone.ms
- Base DN: dc=warpzone,dc=ms
- Admin DN: cn=admin,dc=warpzone,dc=ms
- Readonly DN: cn=readonly,dc=warpzone,dc=ms

Testumgebung:

- Organisation: Warpzone TEST
- Domain: warpzone-test.ms

- Base DN: dc=warpzone-test,dc=ms
- Admin DN: cn=admin,dc=warpzone-test,dc=ms
- Readonly DN: cn=readonly,dc=warpzone-test,dc=ms

### **ou=groups,dc=warpzone,dc=ms**

In dieser OU sind Gruppen für die allgemeine Verwendung angelegt.

### **cn=active,ou=groups,dc=warpzone,dc=ms**

Benutzer müssen Mitglied dieser Gruppe sein um sich überhaupt an einem bestimmten Dienst anmelden zu können. Diese Gruppe wird bei der Erstellung eines Accounts nach der Validierung der E-Mail Adresse automatisch zugewiesen.

### **cn=member,ou=groups,dc=warpzone,dc=ms**

Diese Gruppe erhalten alle Accounts von Warpzone Mitgliedern.

### **cn=vorstand,ou=groups,dc=warpzone,dc=ms**

Diese Gruppe wird den Vorstandsmitgliedern der Warpzone zugewiesen.

### **ou=infrastructure,dc=warpzone,dc=ms**

In dieser OU werden die Gruppen für Infrastruktur-spezifische Dienste angelegt.

### **cn=3dprint-admin,ou=infrastructure,dc=warpzone,dc=ms**

Benutzer mit dieser Rolle sind berechtigt die 3D-Drucker Nutzungsberechtigung zu erteilen.

### **cn=3dprint-user,ou=infrastructure,dc=warpzone,dc=ms**

Benutzer mit dieser Rolle sind berechtigt die 3D-Drucker zu nutzen.

### **cn=grafana-admin,ou=infrastructure,dc=warpzone,dc=ms**

Benutzer mit dieser Rolle haben administrative Berechtigungen im [grafana](#)

**cn=warpauth-admin,ou=infrastructure,dc=warpzone,dc=ms**

Benutzer mit dieser Gruppe haben administrative Berechtigungen in [WarpInfra](#)

**ou=users,dc=warpzone,dc=ms**

In Dieser OU werden die Benutzerkonten angelegt.

**uid=franziska,ou=users,dc=warpzone,dc=ms**

Beispiel für einen Benutzer.

## Verwendete Objektklassen

### Benutzer

Für Benutzer wird generell die *objectClass* „inetOrgPerson“ verwendet.

**Attribut: uid (required, identifizierend)** Benutzername des Benutzers. Dieses Attribut wird zur Identifizierung des Benutzers verwendet und ist Teil des CN. Beispiel für den CN (Benutzer Franziska):  
uid=franziska,ou=users,dc=warpzone,dc=ms

**Attribut: cn (required)** Name des Benutzers (Vorname und Nachname).

**Attribut: givenName** Vorname des Benutzers

**Attribut: sn** Nachname des Benutzers

**Attribut: mail** E-Mail Adresse der Person

**Attribut: userPassword** Passwort des Benutzers

**Attribut: employeeNumber** In diesem Attribut ist die ID der RFID Karte gespeichert.

**Attribut: carLicense** In diesem Attribut ist (verschlüsselt) der Pin Code für den Warptag gespeichert.

### Gruppen

Für Gruppen wird generell die *objectClass* „groupOfUniqueNames“ verwendet.

**Attribut: uniqueMember**

Dieses Attribut kann mehrere Werte enthalten. Als Wert ist jeweils die UID der Benutzerobjekte hinterlegt.

# Verwendete Abfragefilter

## Gitlab

- Filter:  
((&(objectClass=inetOrgPerson)(memberof=CN=active,OU=groups,DC=warpzone,DC=ms))
- Attribute für Aneldennamen: uid, cn

## HackMD

- Filter:  
(&(uid=[BENUTZERNAME])(objectClass=inetOrgPerson)(memberof=CN=active,OU=groups,DC=warpzone,DC=ms))

## aktuell via LDAP angebundene Dienste

- CodiMD <https://md.warpzone.ms>
- Gitlab <https://gitlab.warpzone.ms>
- Matrix <https://matrix.warpzone.ms>
- Verwaltung Gitea <https://verwaltung-git.warpzone.ms>
- Verwaltung Nextcloud <https://verwaltung.warpzone.ms>

## Dienste, die zukünftig angebunden werden sollen

- (Doku)Wiki <https://wiki.warpzone.ms>
- Wordpress ([www.warpzone.ms](https://www.warpzone.ms)) <https://www.warpzone.ms>
- Jabber ([jabber.warpzone.ms](https://jabber.warpzone.ms))

From:  
<http://wiki.warpzone.ms/> - **warpzone**

Permanent link:  
<http://wiki.warpzone.ms/infrastruktur:ldap>

Last update: **04.05.2021**

