

# ZI-CHAT - Installation and Administration Guide

- [Configuration](#)
- [Installation](#)
- [Release Notes](#)
  - [New Page](#)

# Rocket.Chat configuration

From Administration -> Permissions -> "New role"

We create **zimbraintegrator** role , with following options:

- add-user-to-any-c-room
- view-user-administration
- view-room-administration
- view-privileged-setting
- view-full-other-user-info
- user-generate-access-token
- set-owner
- remove-user


- manage-assets
- join-without-join-code
- edit-other-user-password
- create-personal-access-tokens
- create-user - Stwórz użytkownika
- call-management
- api-bypass-rate-limit
- access-mailer




## Create user

From menu Administration -> User -> "New user"

×

Zdjęcie profilowe





Użyj adresu URL

Użyj adresu URL


Nazwa

ZiChatSync

Nazwa użytkownika


@ ZiChatSync

E-mail


 infoadm@extema.mos.gov.pl

☒ Zweryfikowany

Wiadomość status



Hasło


 [Losowy](#)

☐ Set random password and send by email

☐ Nakaz zmianę hasła

Roles

Wybierz rolę

 zimbraIntegrator

Anuluj

Zapisz

W powyższym oknie ustawiamy:

- Nazwa - dowolna nazwa wykorzystywana do integracji z ZI-Chat
- Nazwa użytkownika - to samo jak wyżej
- E-mail

W celu wprowadzenia hasła odznaczyć "Set random password and send by email"

- Hasło

## Configuration LDAP synchronization

LDAP służy do pobierania danych na temat użytkowników RocketChat. W celu skonfigurowania LDAP należy:

- ustawić dane serwera LDAP
- ustawić dane potrzebne do synchronizacji kont zimbry z kontami w RocketChat
- ustawić parametry wyszukiwania kont w LDAP

## LDAP

LDAP to hierarchiczna baza danych wykorzystywana przez wiele firm w celu udostępniania pojedynczej usługi autoryzacji użytkowników pomiędzy wieloma serwisami. Aby uzyskać dodatkowe informacje i przykłady konfiguracji, odwiedź nasze wiki: <https://rocket.chat/docs/administrator-guides/authentication/ldap/>.

### ☒ Włącz LDAP

Włącza LDAP podczas uwierzytelniania.

### ☒ Obniżenie liczby zgłoszeń

Jeżeli logowanie LDAP zakończy się niepowodzeniem, spróbuj zalogować lokalnie. Pomocne w przypadku gdy LDAP jest nieosiągalny.

### ☒ Znajdź użytkownika po zalogowaniu

Wykona wyszukiwanie DN użytkownika po wiązaniu, aby upewnić się, że powiązanie powiodło się, uniemożliwiając logowanie przy użyciu pustych haseł, o ile zezwala na to konfiguracja AD.

### Host

Gospodarz LDAP, np `ldap.example.com` lub `10.0.0.30`.

### Port LDAP

Port dla LDAP, np: `389` lub `636` dla LDAPS

### ☒ Podłącz

Spróbuj ponownie połączyć się automatycznie, gdy połączenie zostanie przerwane z jakiegokolwiek powodu podczas wykonywania operacji

### Szyfrowanie

Metoda szyfrowania wykorzystywany do zabezpieczenia komunikacji z serwerem LDAP. Przykłady obejmują `plain` (bez szyfrowania), `SSL / LDAPS` (zaszyfrowany od początku) i `StartTLS` (upgrade do szyfrowanej komunikacji po połączeniu).

## LDAP

LDAP

☒ Odrzuć nieautoryzowane

Wyłącz tę opcję, aby zezwolić na certyfikaty, których nie można zweryfikować. Zazwyczaj certyfikaty z własnym podpisem wymagają wyłączenia tej opcji

Base DN ✖

ou=people,dc=mos,dc=gov,dc=pl

W pełni kwalifikowana nazwa wyróżniająca (DN) w podrzewie LDAP chcesz wyszukać użytkowników i grup. Możesz dodać tyle, ile zechcesz; Jednakże, każda grupa musi być określona w ten sam bazie domeny jako użytkowników należących do niego. Jeśli podasz niewielkich grup użytkowników, tylko użytkownicy należący do tych grup będzie w zasięgu. Zaleca się, aby określić górny poziom drzewa katalogów LDAP jako baza domeny i użyć filtru wyszukiwania w celu kontroli dostępu.

Wewnętrzny poziom logowania ✖

Błąd ▼

Test połączenia

W powyższym oknie ustawić:

- Host - adres serwera ldap (najczęściej będzie to adres ldap zimborowego)
- Port ldap
- Szyfrowanie
- Base DN - ou=people,dc=intalios,dc=pl

Po skonfigurowaniu parametrów LDAP, wybranie przycisku "Test połączenia" powinniśmy nawiązać połączenie. Jeśli nie, należy sprawdzić port, rodzaj szyfrowania.

Sprawdzenie połączenia z ldap można sprawdzić w CLI z maszyny, na której zainstalowany jest RocketChat:

```
telnet wartość_poła_HOST 389
```

## LDAP

Test połączenia

Zresetuj ustawienia sekcji

### Uwierzytelnianie



Włącz

#### DN użytkownika

uid=zimbra,cn=admins,cn=zimbra

Użytkownik LDAP, który wykonuje wyszukiwań użytkowników do uwierzytelnienia innych użytkowników podczas logowania się.

Jest to zazwyczaj konto usługi stworzony specjalnie dla integracji osób trzecich. Użyj pełnej nazwy, takie jak `cn = Administrator, CN = Users, DC = example, dc = com`.

#### Hasło

.....

W celu uwierzytelniania, należy z serwera zimbra odczytać konfigurację (jako zimbra):

```
zmlocalconfig -s | grep ldap
```

poszukać DN użytkownika zimbra oraz jego hasło

Uzyskane dane wpisać w pola:

- DN użytkownika
- Hasło

## Synchronization/ import



## Synchronizacja / import



## Nazwa pola



Które pole będzie używany jako nazwa użytkownika. Dla nowych użytkowników. Zostaw puste, aby użyć nazwy użytkownika informować na stronie logowania.

Można używać znaczników szablonów też, podobnie jak `{givenName}.#{sn}`.

Domyślną wartością jest `sAMAccountName`.

## Unikalny Identyfikator Pole



To które będą stosowane do łączenia użytkownika LDAP i użytkownika Rocket.Chat. Możesz poinformować wiele wartości oddzielonych przecinkiem, aby postarać się o wartość z rejestru LDAP.

Domyślną wartością jest `objectGUID, IBM-entryUUID, GUID, dominoUNID, nsuniqueId, uidNumber`

## Domyślna domena

Jeśli zostanie podana, domyślna domena będzie używana do tworzenia unikatowych wiadomości e-mail dla użytkowników, których poczta e-mail nie została zaimportowana z LDAP. Wiadomość e-mail zostanie zamontowana jako "nazwa\_uzytkownika @ domyślna\_domena" lub "unikalny\_domyślny @ domyślna\_domena".

Przykład: `rocket.chat`

## LDAP

### ☒ Połącz istniejących użytkowników

**Uwaga!** Gdy importowanie użytkownika z serwera LDAP i użytkownika o tej samej nazwie już istnieje, informacje LDAP i hasło zostaną ustawione na istniejącego użytkownika.

### ☒ Synchronizuj dane

Utrzymuj dane (np: nazwa, email) w synchronizacji z serwerem podczas logowania

### Mapa pól użytkownika

```
{ "cn": "name", "zimbraMailDeliveryAddress": "email" }
```

Konfigurowanie sposobu w jaki pola kont (np. email) są uzupełniane z rekordów LDAP (gdy takowe zostaną znalezione).

Na przykład podając `{ "cn": "name", "mail": "email" }` system wybierze wyświetlaną nazwę użytkownika z pola cn i jego adres email z pola email.

Dostępne pola to: `name`, `email`.

### ☐ Synchronizuj grupy LDAP

### ☐ Auto Remove User Roles

**Attention:** Enabling this will automatically remove users from a role if they are not assigned in LDAP! This will only remove roles automatically that are set under the user data group map below.

## LDAP

corresponding LDAP group! Only enable this if you know what you're doing.

☒ Synchronizacja User Avatar

☐ Synchronizacja w tle

Interwał synchronizacji tła

Every 24 hours

Odstęp między synchronizacjami. Przykład "co 24 godziny" lub "pierwszego dnia tygodnia", więcej przykładów w [Cron Text Parser] (<http://bunkat.github.io/later/parsers.html#text>)

☒ Synchronizacja tła Importuj nowych użytkowników

Zaimportuje wszystkich użytkowników (w oparciu o kryteria filtru), które istnieją w LDAP i nie istnieją w Rocket.Chat

☒ Aktualizacja synchronizacji w tle Istniejących użytkowników

Zsynchronizuje avatar, pola, nazwę użytkownika itp. (W zależności od konfiguracji) wszystkich użytkowników już zaimportowanych z LDAP na każdy **Interwał synchronizacji**

Uruchom teraz synchronizację

Wykona teraz **Background Sync** zamiast czekać **Interwał synchronizacji** nawet jeśli **Synchronizacja tła** jest Fałsz.

Ta akcja jest asynchroniczna, proszę zobaczyć dzienniki, aby uzyskać więcej informacji na temat procesu

Pola do ustawienia:

- Nazwa pola
- Unikalny Identyfikator Pole
- Mapa pól użytkownika

## LDAP search configu

## Wyszukiwanie użytkowników

## Filtr

Jeśli określony, tylko użytkownicy pasujących ten filtr będzie mógł zalogować. Jeśli filtr nie jest określony, wszyscy użytkownicy w zakresie określonym bazie domeny będą mogli się zalogować.

Np Active Directory `memberOf = cn = ROCKET_CHAT, ou = Ogólne Groups`.

Np OpenLDAP (rozszerzalny wyszukiwania match) `ou: dn: = ROCKET_CHAT`.

## Zakres

## Pole wyszukiwania

W powyższym formularzu ustawić:

- Filtr  
(&(objectclass=zimbraAccount)(!(zimbraHideInGal=TRUE))(!(zimbraSystemResource=TRUE))(z
- Zakres - sub
- Pole wyszukiwania - uid

## ZI-Chat zimlet configuration

W pierwszej kolejności przenosimy pliki :

- loginPage.html,
- ZiChatConfig.json,

z *ZI-Chat-1.7-InstallerRC/helpers/* do */opt/zimbra/lib/ext/IntalioZiChat* .

Następnie edytujemy plik IntalioZiChat:

```
{
  "nazwa.domeny.pl": {
    "ZiChatUserLogin": "ZiChatSync",
    "ZiChatUserPassword": "haslojakwRC",
    "ZiChatUrl": "https://adres.serwera.rc",
    "ZiChatLoginPage": "/opt/zimbra/lib/ext/IntalioZiChat/loginPage.html"},
  "*": {
    "ZiChatUserLogin": "ZiChatSync",
    "ZiChatUserPassword": "haslojakwRC",
    "ZiChatUrl": "https://adres.serwera.rc",
    "ZiChatLoginPage": "/opt/zimbra/lib/ext/IntalioZiChat/loginPage.html"},
  "other": {
    "UseOnlyUID": true,
    "DelegatedAdminSecurity": false
  }
}
```

W powyższym pliku ważne jest aby **ZiChatUrl** miał tę samą wartość co **Environment=ROOT\_URL=** w `/lib/systemd/system/rocketchat.service` i `/lib/systemd/system/rocketchat@.service`.

Po dokonanych zmianach, zrestartować mailboxa (jako zimbra):

```
zmailboxdctl restart
```

# Installation

## Installation

Installation is performed by execution following:

```
perl ZI-Installer
```

In case of the **multi server** installation, zimlet must be installed on **every mailbox**.

Remember to restart all mailboxes (as root):

```
zmmailboxctl restart
```

# Release Notes

# New Page