# Wikiprint Book

Title: Konfiguracja autentykacji LDAP / Active Directory

Subject: eDokumenty - elektroniczny system obiegu dokumentów, workflow i CRM - DeployerGuide/Others/LDAPAuthentication

Version: 38

Date: 07/25/25 22:20:42

# **Table of Contents**

Konfiguracja autentykacji LDAP / Active Directory	3
Aktualna dokumentacja od wersji 6.53.0 znajduje się pod poniższym linkiem	3
Menu	3
Wprowadzenie	3
Automatyczne tworzenie konta w eDokumenty po pierwszym logowaniu	3
Instalacja wymaganych bibliotek	3
Autentykacja przy pomocy LDAP	4
konfiguracja eDokumentów do autentykacji LDAP	4
Autentykacja przy pomocy Active Directory	4
Konfiguracja systemu eDokumenty do współpracy z Active Directory	5
Typowy sposób dołączania użytkownika do eDokumentów	6
Dodatkowe operacje	6

# Konfiguracja autentykacji LDAP / Active Directory

# Aktualna dokumentacja od wersji 6.53.0 znajduje się pod poniższym linkiem

### LDAP / Active Directory

#### Menu

- 1. <u>Wprowadzenie</u>
- 2. Instalacja wymaganych bibliotek
- 3. Autentykacja przy pomocy LDAP
- 3.1 konfiguracja eDokumentów do autentykacji LDAP
- 4. Autentykacja przy pomocy !Active Directory
  - 4.1 Konfiguracja systemu eDokumenty do współpracy z !Active Directory
  - 4.2 Typowy sposób dołączania użytkownika do eDokumentów

### Wprowadzenie

System eDokumenty umożliwia oprócz wbudowanego mechanizmu autentykcji, uwierzytelnianie użytkowników systemu w katalogu LDAP (w tym również ActiveDirectory).

Użytkownik po wejściu na stronę logowania podaje login i hasło które są zgodne z nazwą i hasłem w katalogu LDAP. System przekazuje dane do serwera LDAP który przeprowadza wyszukiwanie w swoim katalogu. W przypadku pomyślnego przebiegu procesu autentykacji następuje wejście do systemu oraz automatyczna aktualizacja podanego hasła w bazie eDokumenty.

### Automatyczne tworzenie konta w eDokumenty po pierwszym logowaniu

Jeżeli user jest w ActiveDirectory i zaloguje się pierwszy raz do systemu z użyciem poprawnego hasła wówczas system eDokumenty utworzy jego konto w bazie eDokumenty i doda tego użytkownika do tych **grup** do których jest przypisany w LDAP i które również obecne są w systemie eDokumenty. Niestety takie konto nie będzie jeszcze pozwalało na pracę w systemie gdyż wymagane jest przypisanie nowego użytkownika do stanowiska w strukturze organizacyjnej. Może to zrobić jedynie administrator w panelu *Pracownicy*.

Przejdź do Menu

### Instalacja wymaganych bibliotek

Do współpracy eDokumentów z LDAP oraz Active Directory wymagane jest zainstalowanie obsługi LDAP przez PHP. Obsługę taką zawiera pakiet php5-ldap (dla linuksa). Szczegóły są dostępne na stronie <a href="http://www.php.net/ldap">http://www.php.net/ldap</a>.

Jeżeli pakiet w Debianie nie jest zainstalowany, to należy wykonać następujące polecenia (z poziomu użytkownika root):

1. Odświeżenie repozytoriów

root@pc# apt-get update

1. Odświeżenie repozytoriów

root@pc# apt-get install php5-ldap

1. Po instalacji należy zrestartować serwer Apache'a

root@pc# /etc/init.d/apache2 restart

W systemie Windows w katalogu C:\Program Files\php\ext powinien znajdować się plik php-ldap.dll. Aby parser php mógł skorzystać z tej biblioteki nalezy w pliku php.ini odkomentować rozszerzenie: ;extension=php\_ldap.dll usuwając symbol średnika sprzed wyrażenia. Ostatnim krokiem jest zrestartowanie serwera Apache.

Przejdź do Menu

# Autentykacja przy pomocy LDAP

Ta część niniejszego artykułu dotyczyć będzie autentykacji przy pomocy protokołu LDAP. Zakłada się tutaj, iż mamy w systemie Windows bądź Linux zainstalowany serwer LDAP - przykładowo: OpenLDAP [http://www.openIdap.org/ (linux) oraz [http://www.userbooster.de/en/download/openIdap-for-windows.aspx (windows).

#### Przejdź do Menu

#### konfiguracja eDokumentów do autentykacji LDAP

Po zdefiniowaniu użytkowników na serwerze LDAP, należy przejść do eDokumentów, i zdefiniować sposób autentykacji. Wykonuje się to w menu *Ustawienia > Panel Sterowania > Autentykacja*. Otwiera się okienko, gdzie wybieramy *Typ: LDAP*. Pojawiają się nam pola, gdzie wprowadzamy:

- Dane serwera, w tym:
  - Host adres IP lub nazwę serwera LDAP
  - Port port serwera LDAP, domyślnie 389.
  - BaseDN: adres bazy danych, w której będą wyszukiwaniu użytkownicy LDAP. Należy sprawdzić w konfiguracji LDAP. Przykład: OU=users,DC=edokumenty,DC=ldap.
- Dodatkowe dane:
  - LDAP admin dane użytkownika, który posiada uprawnienia do przeszukiwania zasobów LDAP, np. CN=amdinistrator, DC=edokumenty, DC=ldap
  - Hasło hasło dla powyższego użytkownika.

Dodatkowo warto przetestować połączenie wprowadzając dane użytkownika, dla którego zostanie przeprowadzona testowa autentykacja.

🔀 Ustawienia a	utentykacji 🔤 🗶	
Тур:	LDAP	
Sprawdź testowe	e dane	
Login: <sup>0</sup>	Administrator	
Hasło:	•••••	
Dane serwera		
Host: <sup>0</sup>	192.168.0.120	
Port: <sup>0</sup>	389	
Base DN: <sup>0</sup>	ou=users,dc=edokumenty,dc=ldap	
Dodatkowe dane LDAP admin: <sup>®</sup> cn=amdinistrator,dc=edokumenty,dc=lda		
Hasło:®		
	Zapisz Zamknij	

### (Rys.1)

Dane z powyższego formularza są wprowadzone do pliku config.inc, którego fragment dotyczący autentykacji został przedstawiony w dalszej części artykułu.

Po ustawieniu i przetestowaniu połączenia do eDokumentów będzie się mógł zalogować tylko ten użytkownik, który posiada konto na serwerze LDAP.

Przejdź do Menu

# Autentykacja przy pomocy Active Directory

W niniejszej części artykułu zajmiemy się autentykacją przy pomocy Active Directory. System eDokumenty może być zainstalowany albo na serwerze Microsoft Windows lub też na serwerze Linuksowym np. Debian.

# Konfiguracja systemu eDokumenty do współpracy z Active Directory

Aby móc skorzystać z dobrodziejstw uwierzytelniania poprzez LDAP (Active Directory na Windows) należy skonfigurować podstawowe dane przy użyciu formularza umieszczonego w *Panelu Sterowania > Autentykacja*.

🔀 Ustawienia a	utentykacji 📃 🗾
Тур:®	Active Directory
Sprawdź testowe	e dane
Login:®	
Hasło:	
Dane serwera	
Host: <sup>0</sup>	192.168.0.1
Port:0	389
Base DN:0	DC=edokumenty,DC=domena
Dodatkowe dane	
Domena:®	@edokumenty.domena
	Zapisz Zamknij

#### (Rys.2)

W formularzu wybieramy rodzaj autoryzacji, następnie wpisujemy adres hosta - komputera, który jest kontrolerem domeny. Base DN - jest wyjaśnione w dalszej części artykułu. Ważne jest, aby w polu Domena wpisać pełny adres domeny poprzedzony znakiem @ np. @edokumenty.firma.

Aby przetestować wpisy, należy wprowadzić użytkownika z prawami administratora domeny i jego hasło.

Powyższy formularz uzupełnia poniższe stałe zawarte w pliku config.inc w katalogu głównym apps\edokumenty. W przypadku jeśli którejś z tych stałych nie ma należy dodać ją ręcznie korzystając z edytora teksu (zalecany Notepad++, VIM).

```
define('AUTHENTICATION_METHOD', 'PG');
// znacznik określający sposób autentykacji opcje: PG, LDAP, AD
define('LDAP_HOST', ''); // adres IP serwera
define('LDAP_PORT', 389); // port najczęściej 389
// ścieżka do wyszukania danych usera który ma prawo do
// przeglądania zasobów ldap włącznie z hasłami np.: cn=root,ou=BetaSoft,ou=Users,dc=firma,dc=local
define('LDAP_AUTH_USER', '');
define('LDAP_AUTH_USER', '');
define('LDAP_AUTH_PASS', ''); // haslo dla usera powyzej
define('LDAP_BASE_DN', ''); // ścieżka wyszukiwanie np ou=BetaSoft,ou=Users,dc=firma,dc=local
define('LDAP_USE_TLS', FALSE);
// specyficzne wartości dla Active Directory
define('ACTIVE_DIRECTORY_ACCOUNT_SUFFIX', '@firma.local'); // nazwa domeny poprzedzona @
```

W przypadku korzystania z TLS a gdy w AD mamy certyfikat podpisany przez nas samych w konfigruacji LDAP na serwerze eDokumentów należy edytować plik

/etc/ldap/ldap.conf

od dodać następujący wpis

```
TLS_REQCERT never
```

Odnośnie LDAP\_BASE\_DN najczęściej jest to ciąg postaci DC=firma,DC=local - każdy kolejny DC określa człon domeny np. edokumenty.firma.local będzie wyglądać DC=edokumenty,DC=firma,DC=local. Co do OU=betasoft jest to oznaczenie symboliczne oraz nazwa korzenia w którym nastąpi wyszukiwanie użytkowników.

Wyśmienitym narzędziem do pobrania tych danych jest Softerra LDAP Browser (Windows), phpLDAPadmin (PHP).

Po wprowadzeniu danych do powyższego formularza/pliku config.inc należy przetestować połączenie i zapisać ustawienia:

eDokum	enty 3.8.66
2	Proces autentykacji przebiegł pomyślnie. Czy na pewno chcesz zapisać wybrany sposób autentykacji oraz wpisane parametry
	Tak Nie

(Rys.3)

Przejdź do Menu

# Typowy sposób dołączania użytkownika do eDokumentów

Dodawanie użytkownika do eDokumentów, w przypadku autentykacji AD wymaga dodatkowej pracy związanej z założeniem użytkownika w AD. Dopiero po założeniu użytkownika na kontrolerze AD oraz w eDokumentach pozwoli użytkownikowi uruchomić system eDokumenty na swoim stanowisku.

# Przejdź do <u>Menu</u>

#### Dodatkowe operacje

W plikach /var/tpl/ad\_column\_map.ini oraz /var/tpl/ldap\_column\_map.ini można zadeklarować mapowanie pozostałych pól z LDAP/AD na pola z systemu eDokumenty (domyślnie ustawienia są gotowe po instalacji systemu eDokumenty).

```
; Mapa kolumn
;
; Kolumny firnam i lasnam zawsze musza byc
; Nalezy dopilnowac aby w ldapie kolumny
; mapowane na firnam i lasnam nie byly puste
[map]
samaccountname = usrnam
mail = e_mail
telephonenumber = phone_
givenname = firnam
sn = lasnam
initials = initls
description = commen
```

Przejdź do <u>Menu</u>