Autoryzacja 2

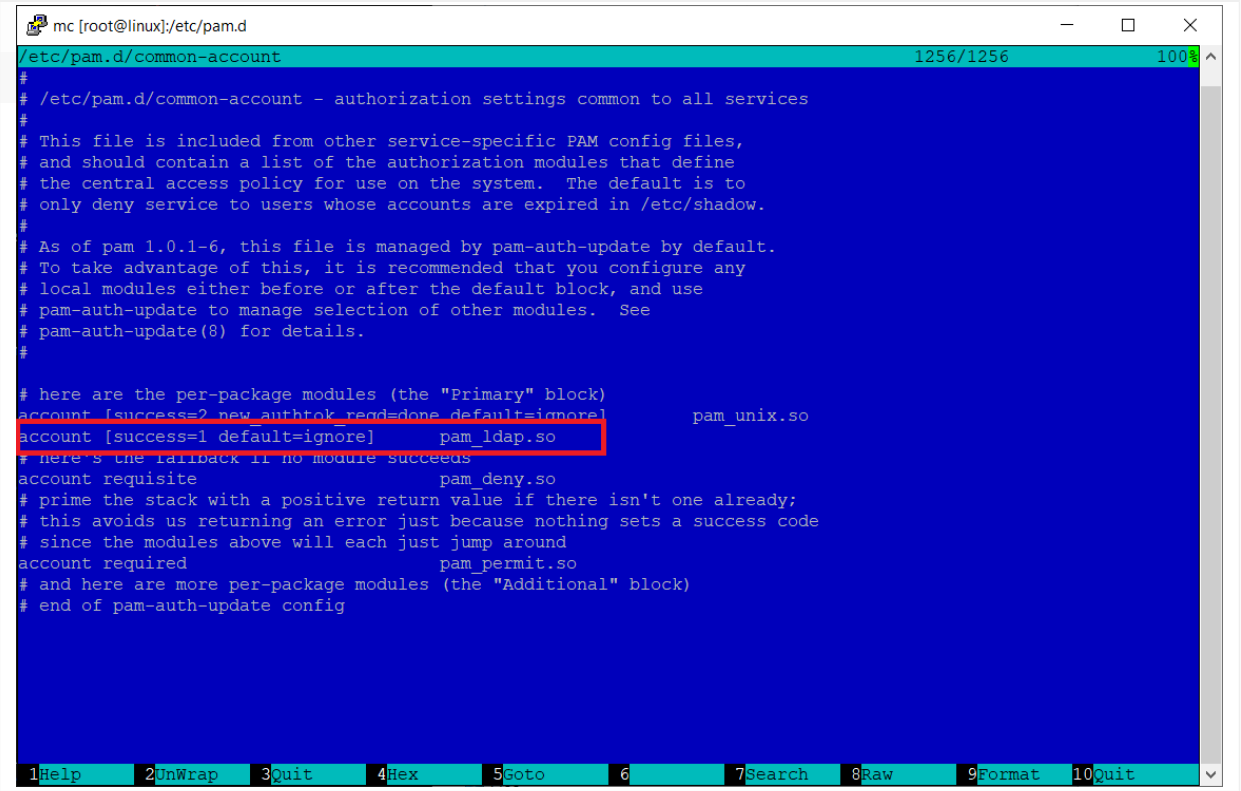
written by archi | 16 października 2019

vcenterlab.wi.zut.edu.pl

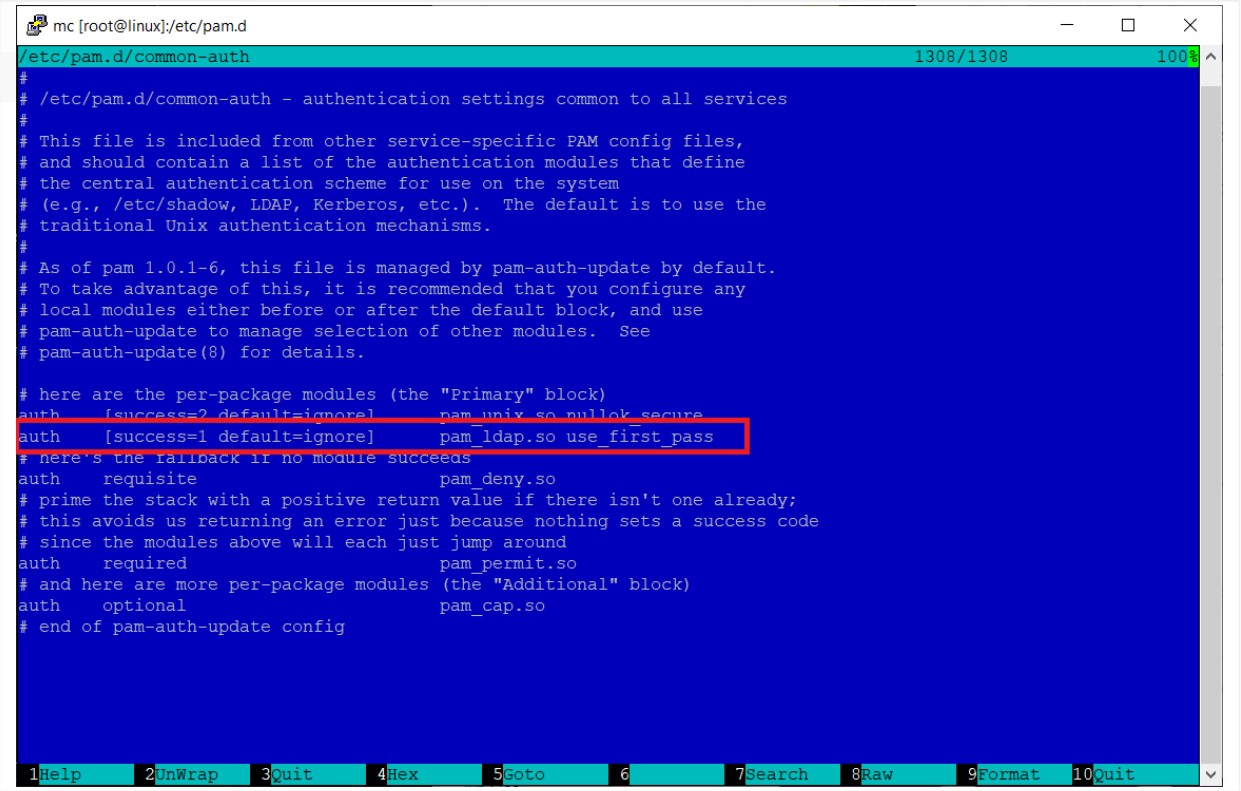
1. Zainstaluj pakiet „`libpam-ldap`„. Prawdopodobnie otrzymasz komunikat, że pakiet jest już zainstalowany. Został dołączony przy poprzednim laboratorium.
2. Następujące polecenia powinny być rozpoznawane prawidłowo w systemie:

```
id user1
cd ~user1    (tylko po ponownym zalogowaniu się do putty)
```

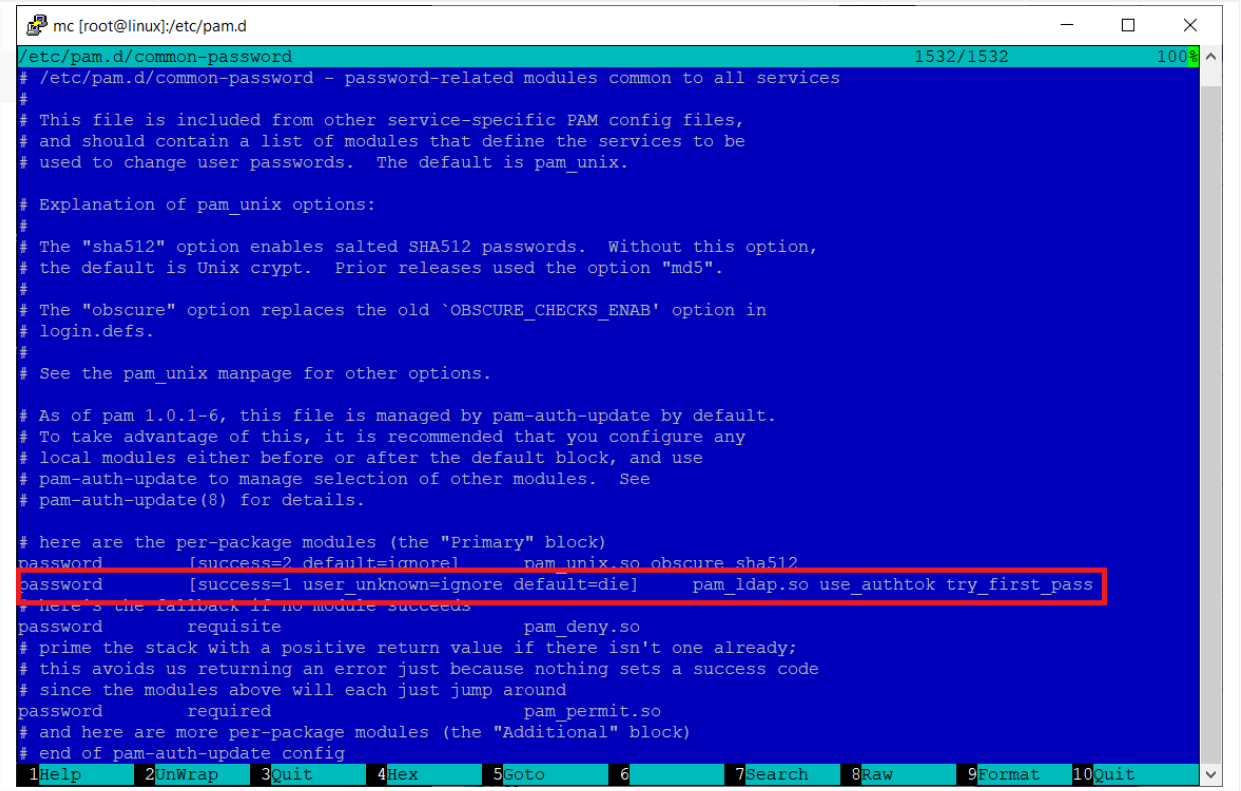
1. System PAM wykorzystuje ten sam plik konfiguracji („`/etc/ldap.conf`„) jak libnss-LDAP. System automatycznie również skonfiguruje dostęp w systemie PAM wewnątrz katalogu `/etc/pam.d` należy jedynie sprawdzić poprawność wpisów.
   NIE WOLNO NIC ZMIENIAĆ – tylko sprawdzić !!!!!!!!!!!! czy występują w każdym pliku pozycje na czerwono !!! Jeśli tak o wszystko OK.
2. Prawidłowa postać wszystkich wpisów:
   - common-account:



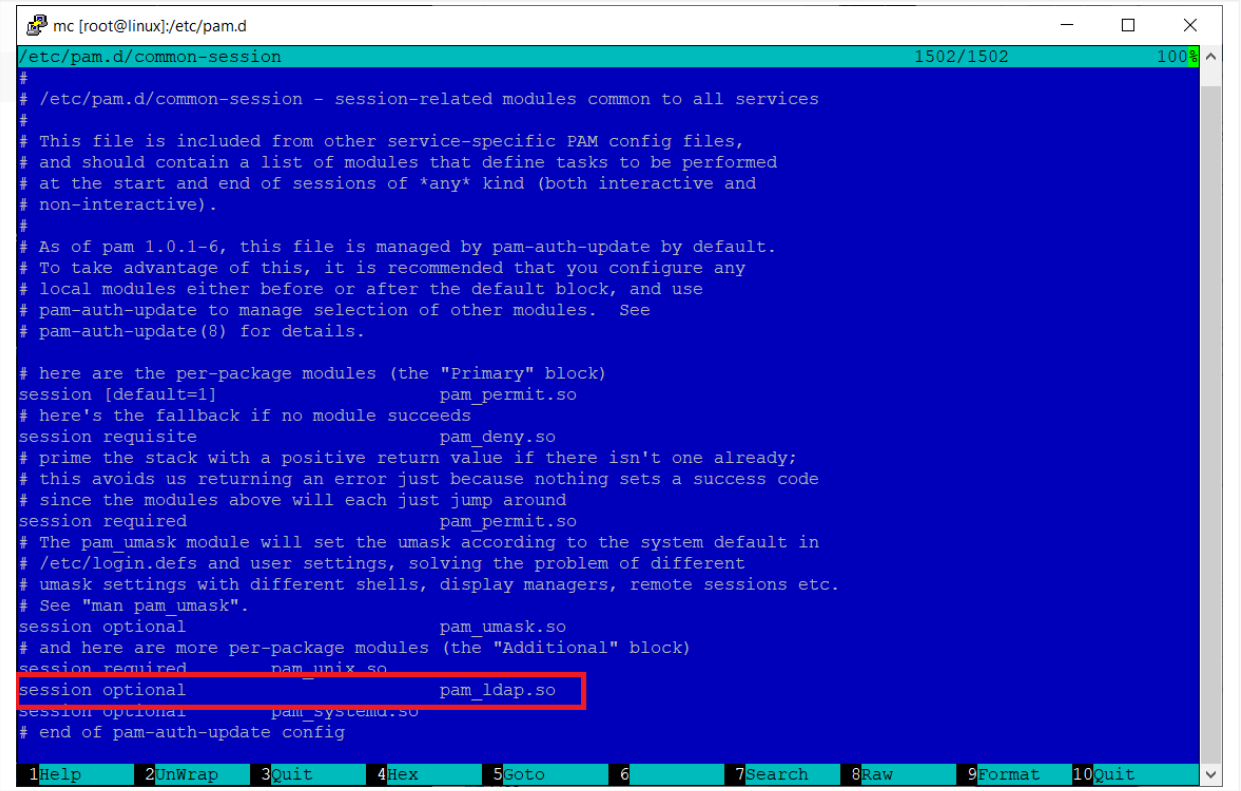
- common-auth:



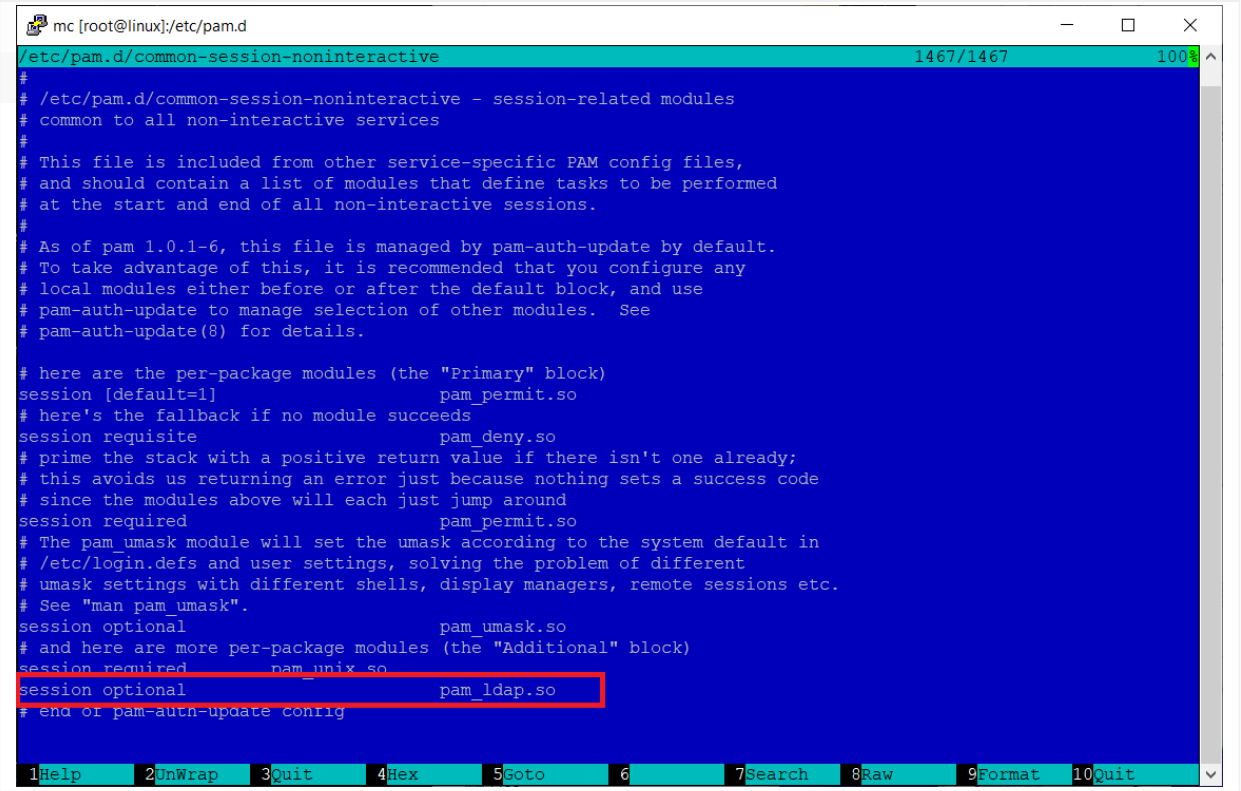
- common-password:



- common-session:



- common-session-noninteractive:



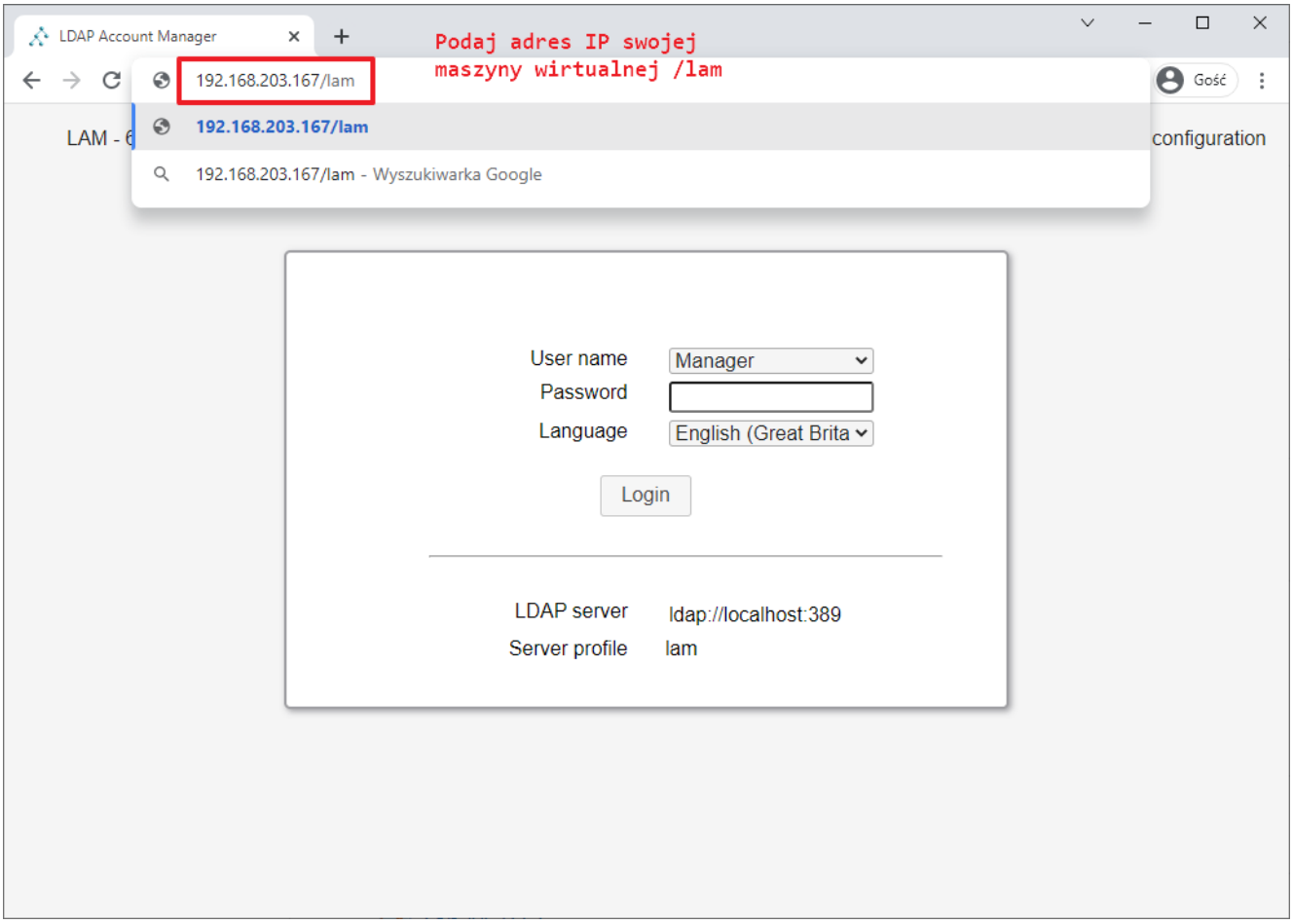
3. Prawidłowo wykonane wpisy po zrestartowaniu usługi SSH powinny pozwolić na zalogowanie się przy pomocy użytkownika z LDAP do systemu. restart: **`service ssh restart`**
4. Połączenie wykonujemy przez kolejną sesję SSH (nowa sesja) i logowaniu się użytkownikiem i hasłem z LDAP. Znak zachęty jest bez przypisanego shella. Dlatego też w dalszej części rozszerzymy schemat LDAPa, przy okazji konfigurując narzędzie graficzne LDAP Account Manager.
5. Poniżej zrzuty ekranu z konfiguracją

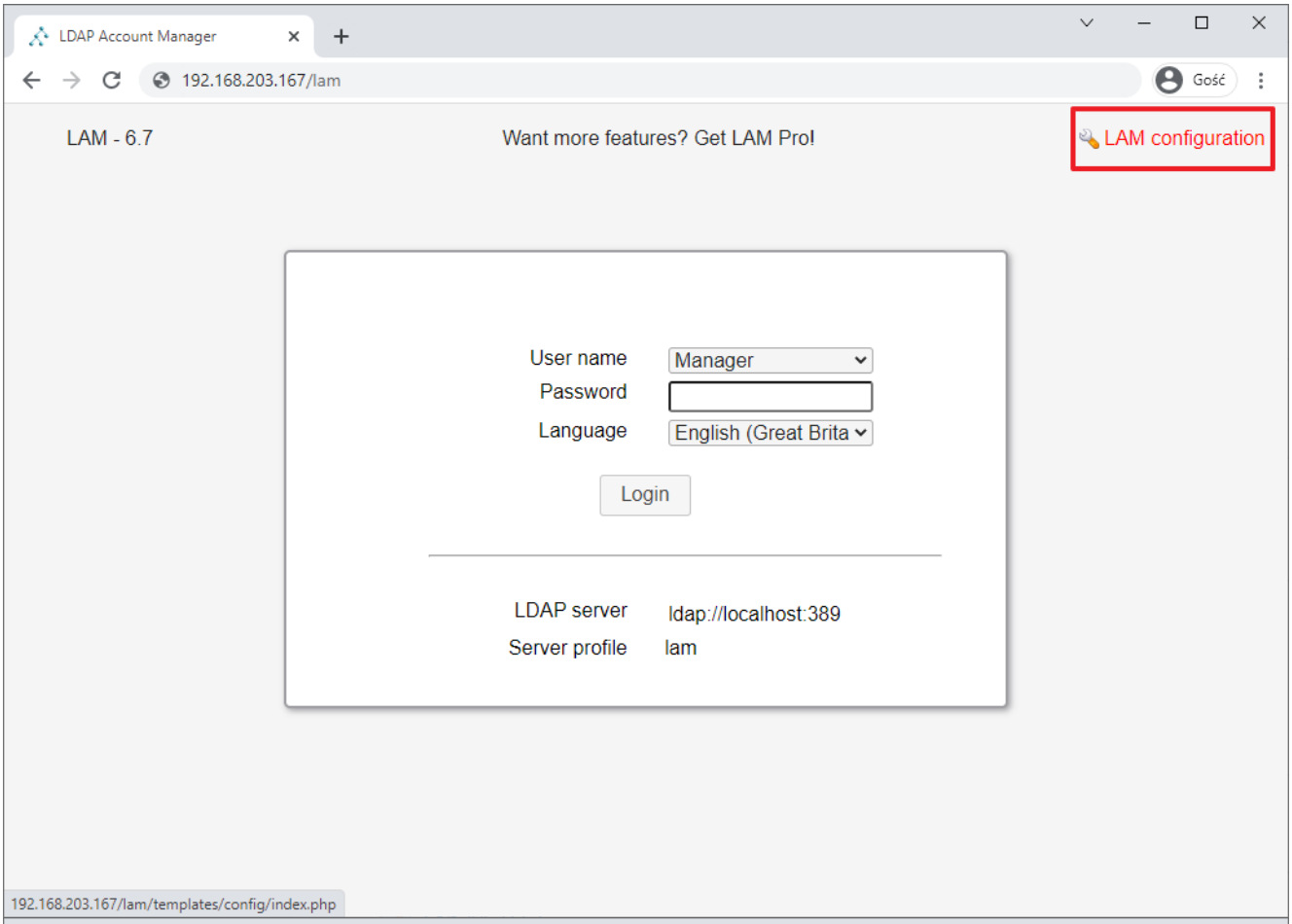
Pobierz za pośrednictwem wget pakiet aktualnej wersji LAM (https://gsliwinski.wi.zut.edu.pl/sieci/ldap-account-manager_7.7-1_all.deb)

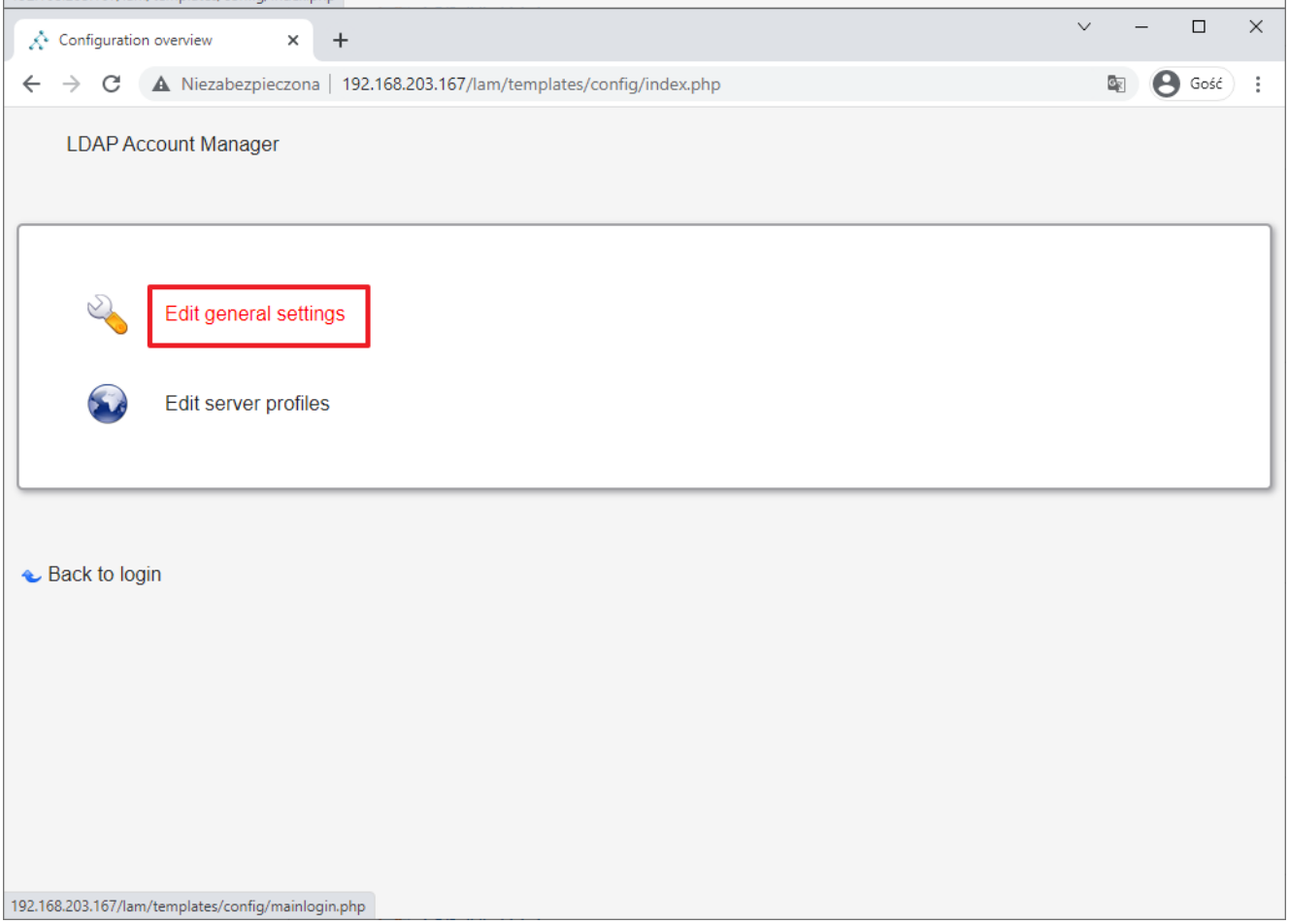
Z wykorzystaniem polecenia **`dpkg -i ldap-account-manager_7.7-1_all.deb`** rozpocznij proces instalacji – zakończy się błędem zależności

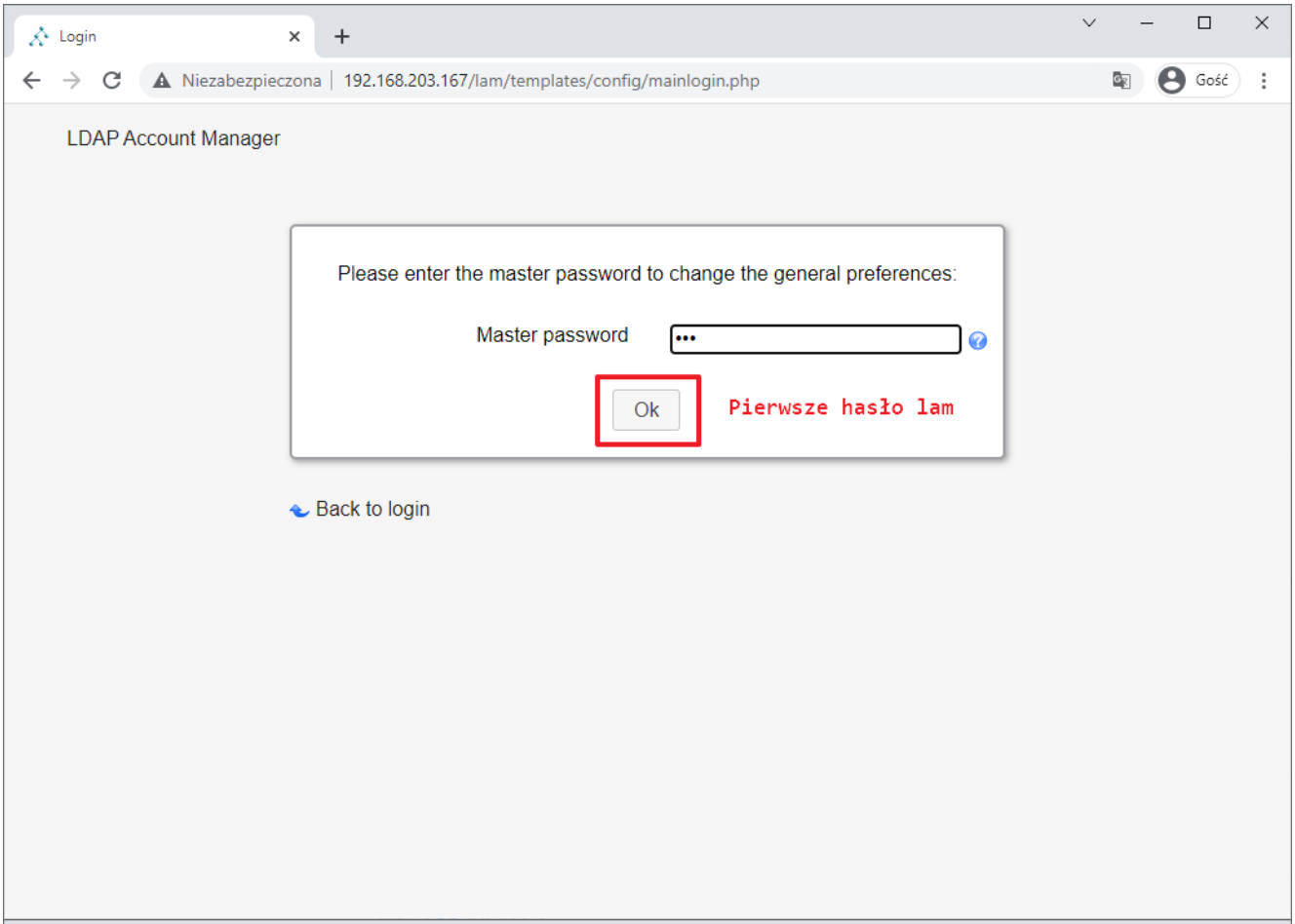
Napraw ten stan poleceniem **`apt install -f`**

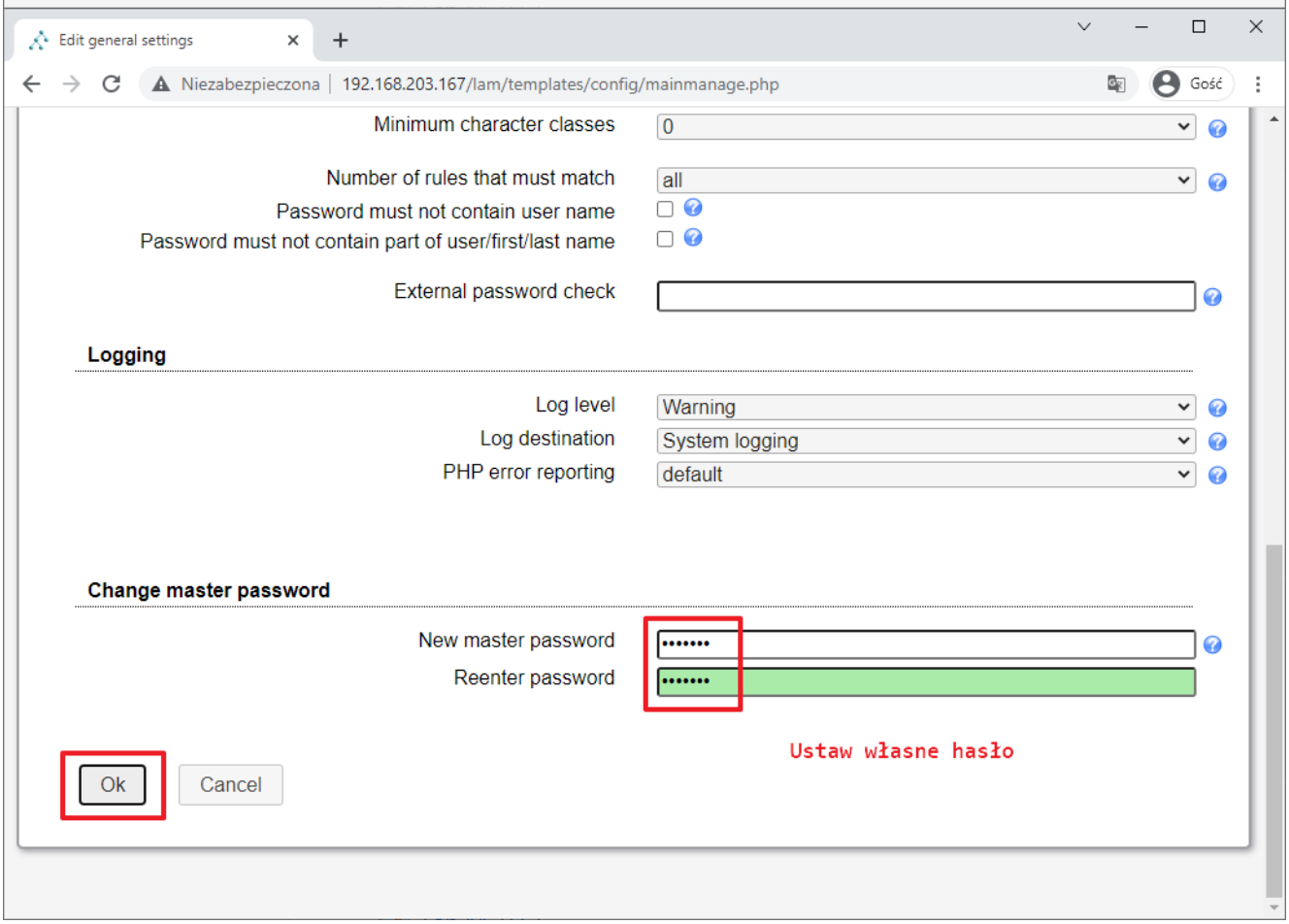
Otwórz w przeglądarce witrynę LAM poprzez swój adres IP maszyny VM dodając przyrostek /lam

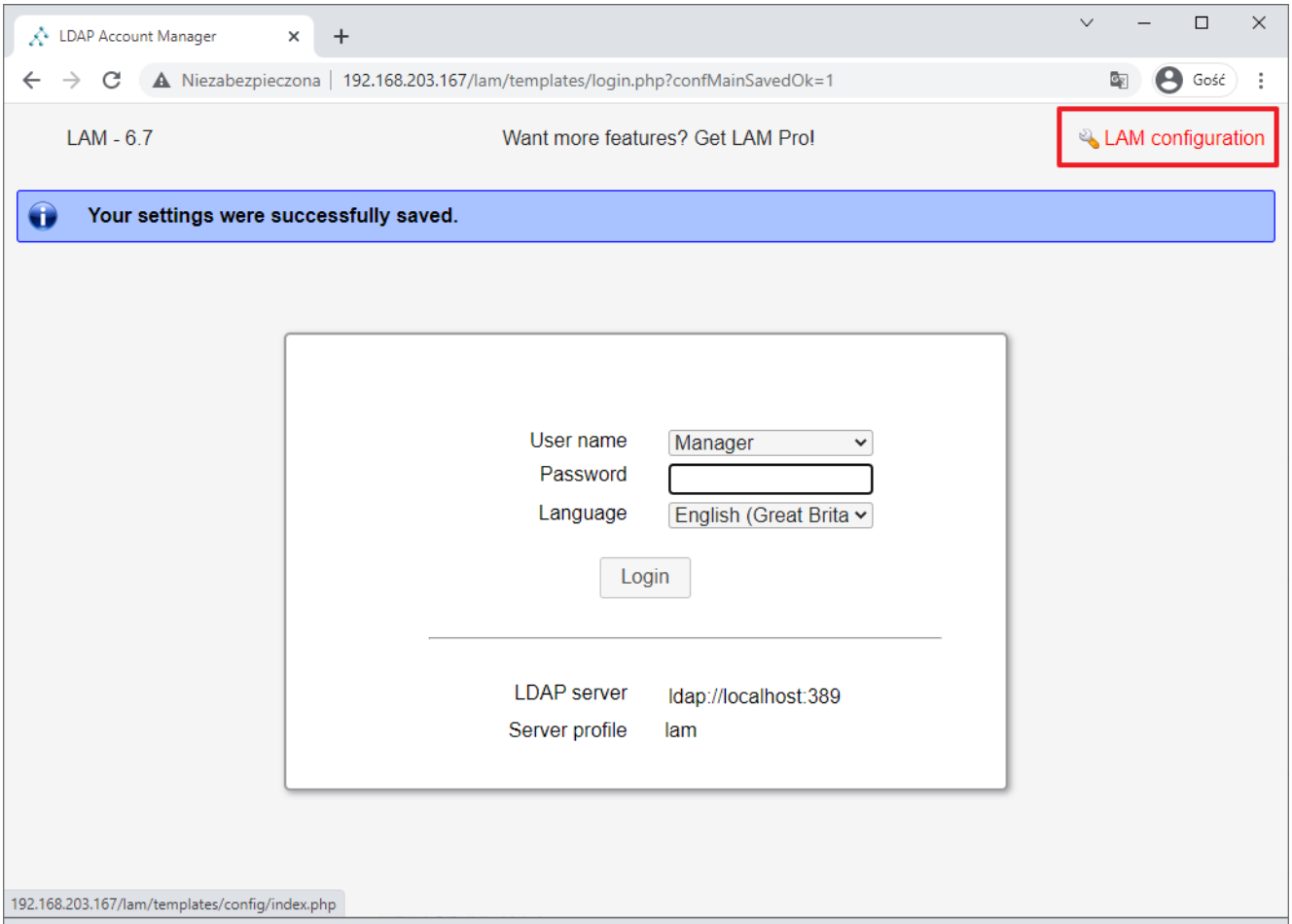


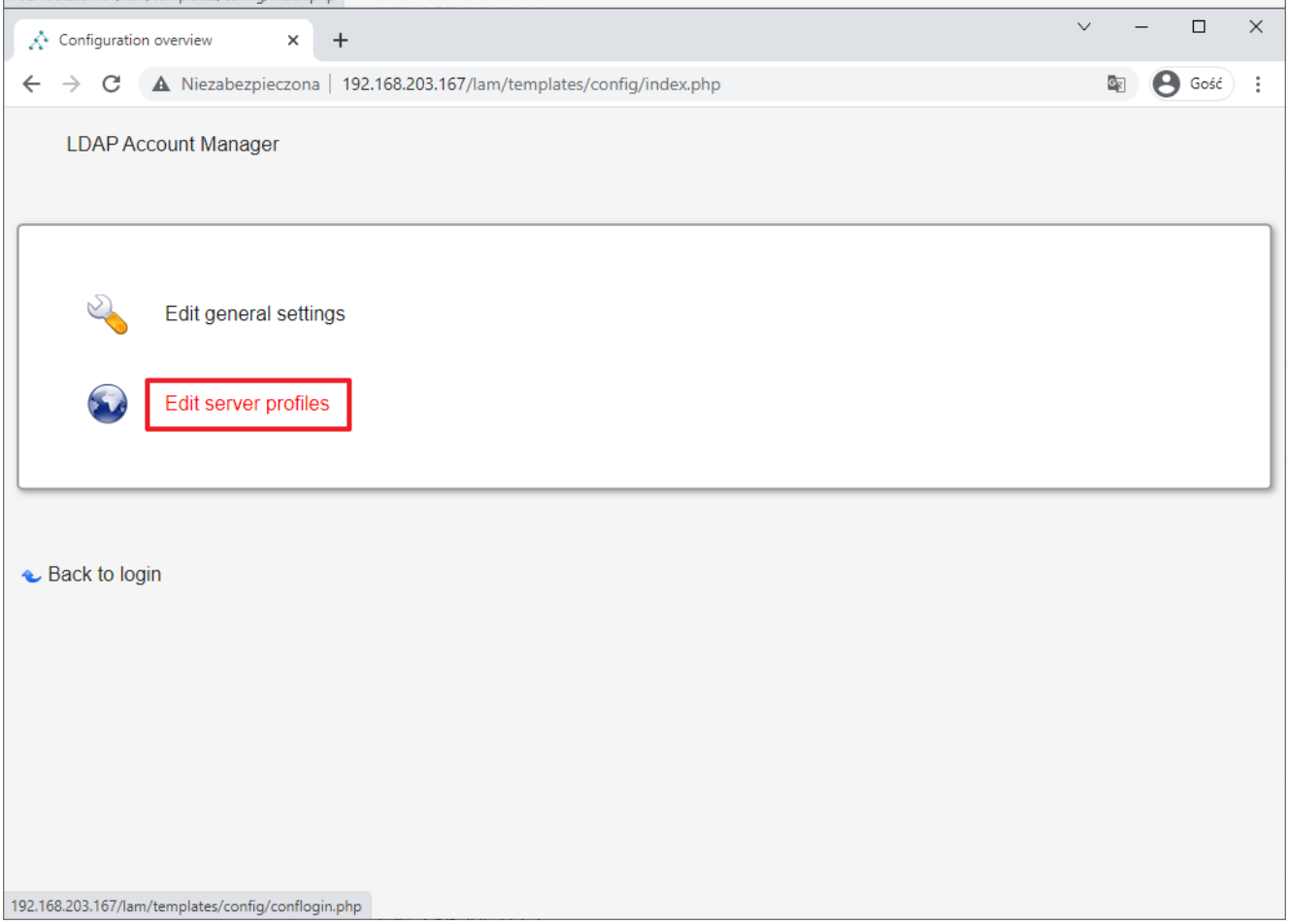

LDAP Account Manager
192.168.203.167/lam
Gość
LAM - 6.7
Want more features? Get LAM Pro!
LAM configuration
User name
Manager
Password
Language
English (Great Brita
Login
LDAP server
ldap://localhost:389
Server profile
lam
192.168.203.167/lam/templates/config/index.php

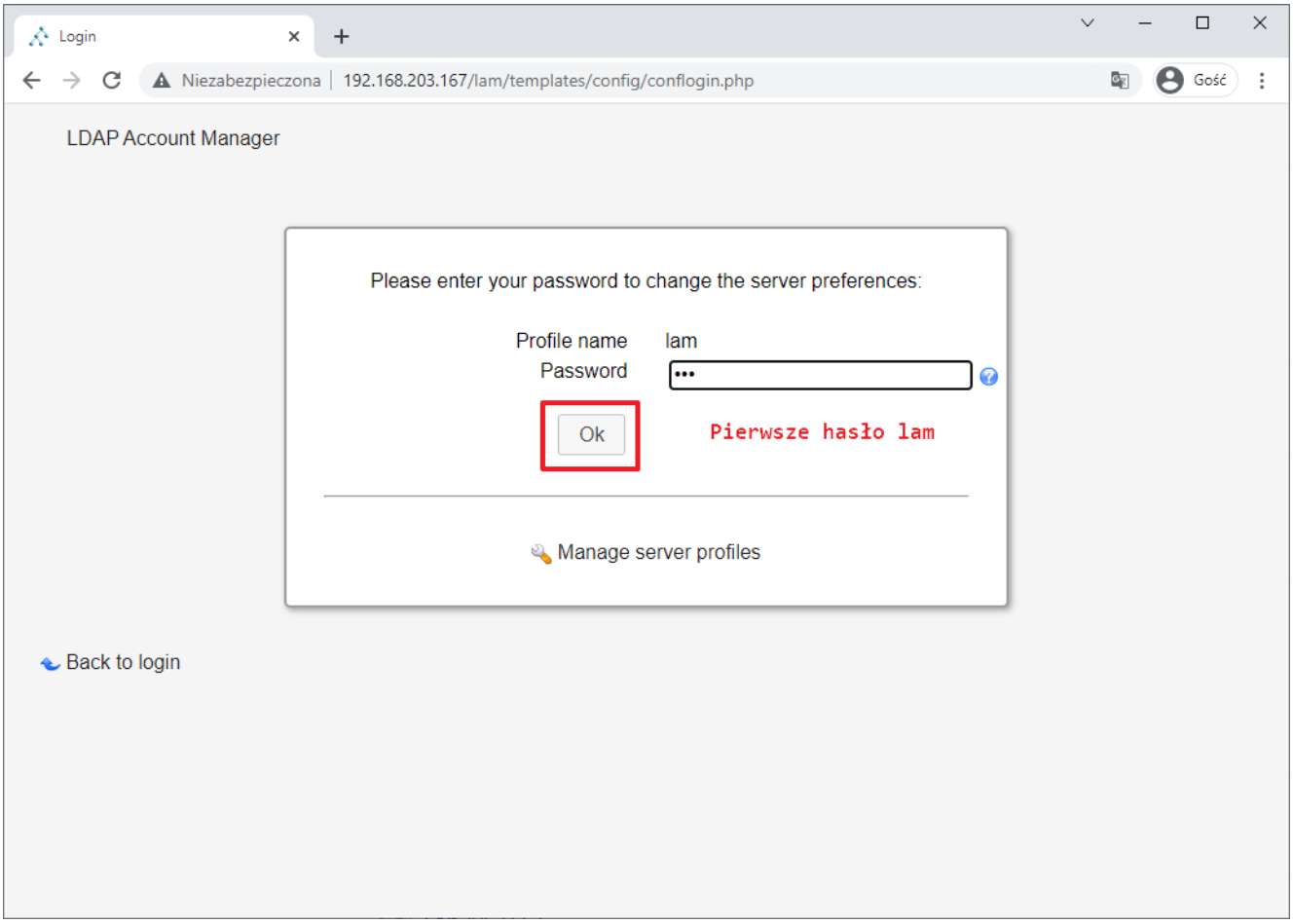

Configuration overview
Niezabezpieczona
192.168.203.167/lam/templates/config/index.php
Gość
LDAP Account Manager
Edit general settings
Edit server profiles
Back to login
192.168.203.167/lam/templates/config/mainlogin.php


Login
Niezabezpieczona | 192.168.203.167/lam/templates/config/mainlogin.php
Gość
LDAP Account Manager
Please enter the master password to change the general preferences:
Master password
Ok
Pierwsze hasło lam
Back to login

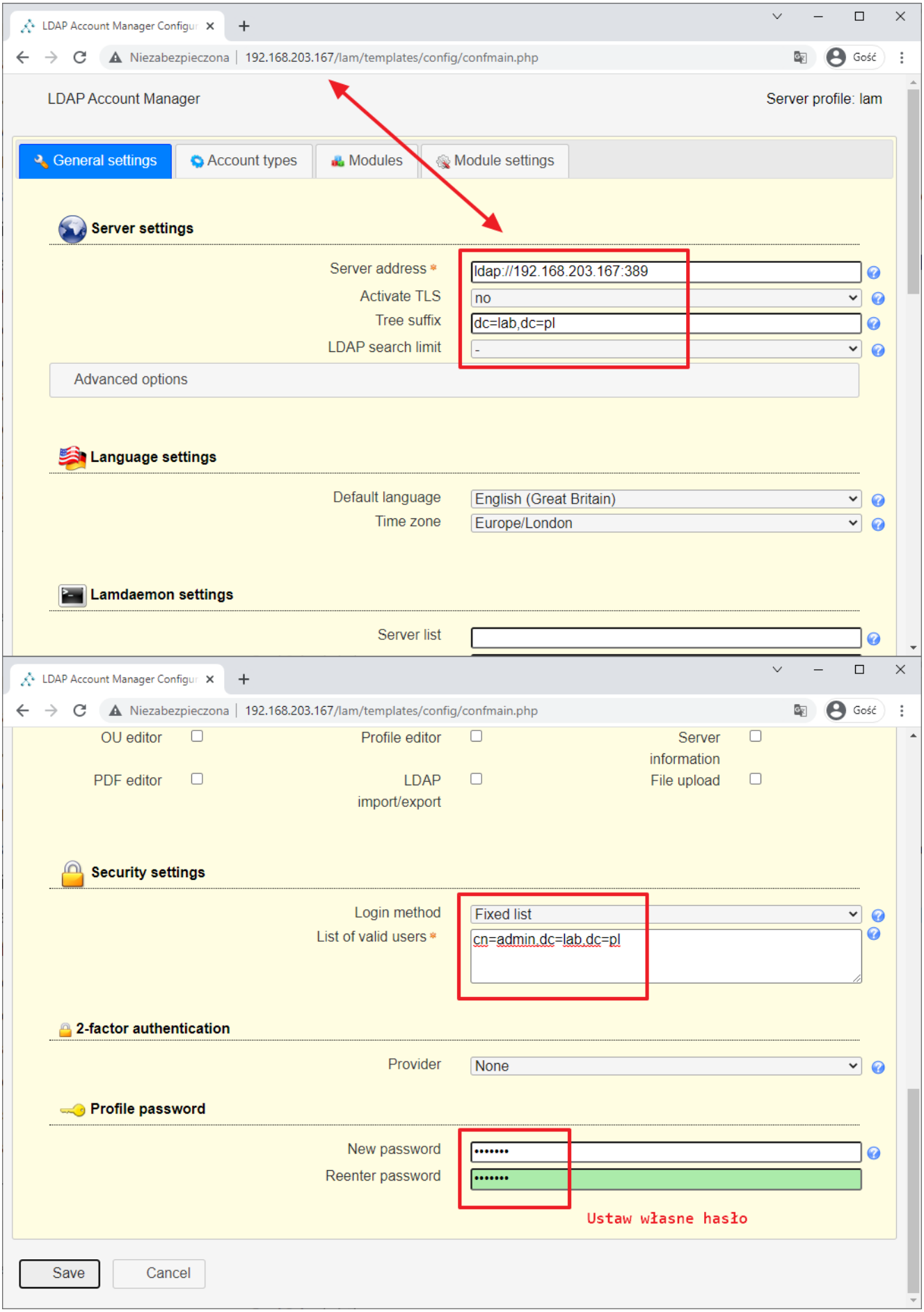

Edit general settings
Niezabezpieczona | 192.168.203.167/lam/templates/config/mainmanage.php
Gość
Minimum character classes
0
Number of rules that must match
all
Password must not contain user name
Password must not contain part of user/first/last name
External password check
Logging
Log level
Warning
Log destination
System logging
PHP error reporting
default
Change master password
New master password
Reenter password
Ustaw własne hasło
Ok
Cancel

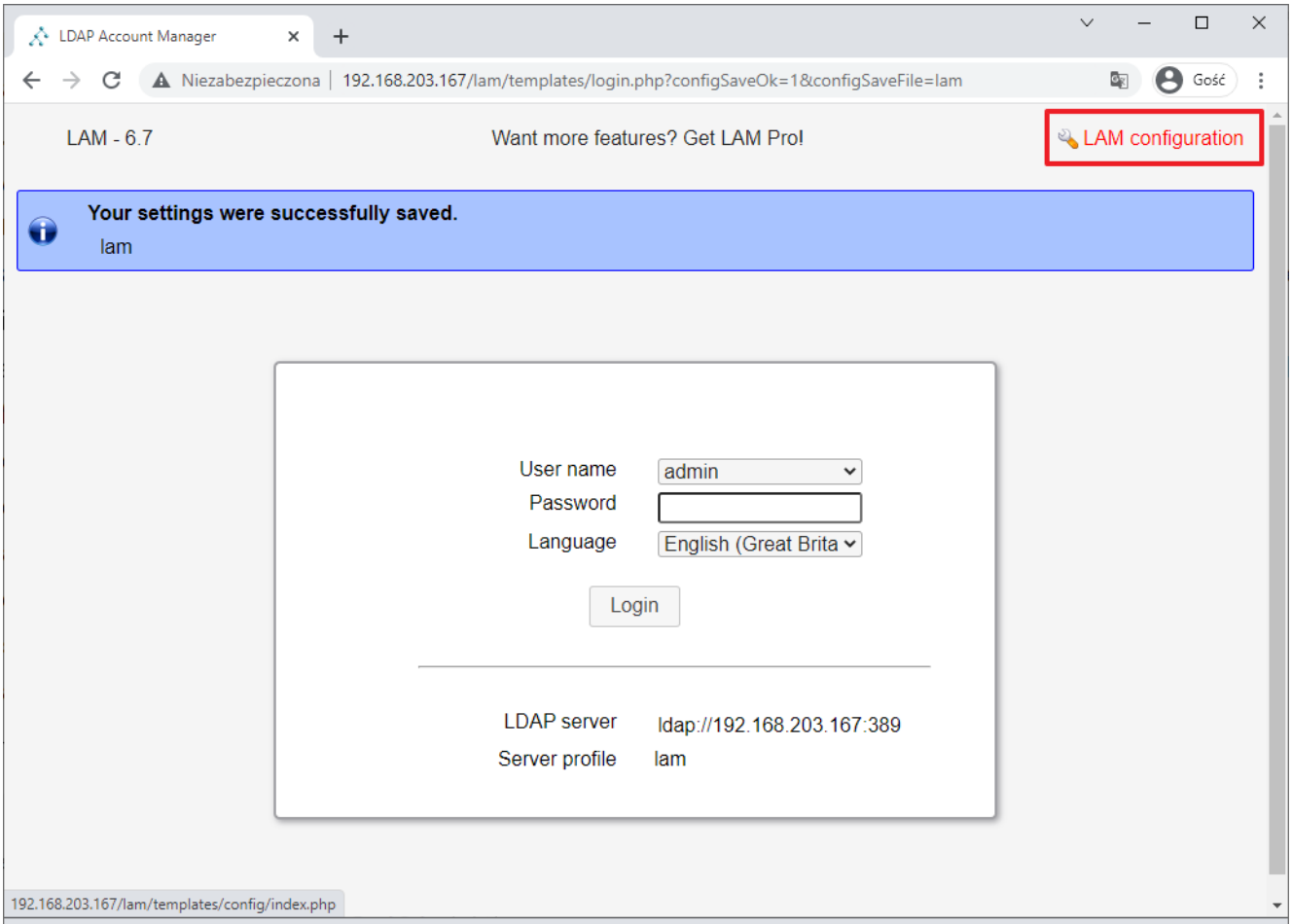

LDAP Account Manager
Niezabezpieczona | 192.168.203.167/lam/templates/login.php?confMainSavedOk=1
Gość
LAM - 6.7
Want more features? Get LAM Pro!
LAM configuration
Your settings were successfully saved.
User name
Manager
Password
Language
English (Great Brita
Login
LDAP server
ldap://localhost:389
Server profile
lam
192.168.203.167/lam/templates/config/index.php

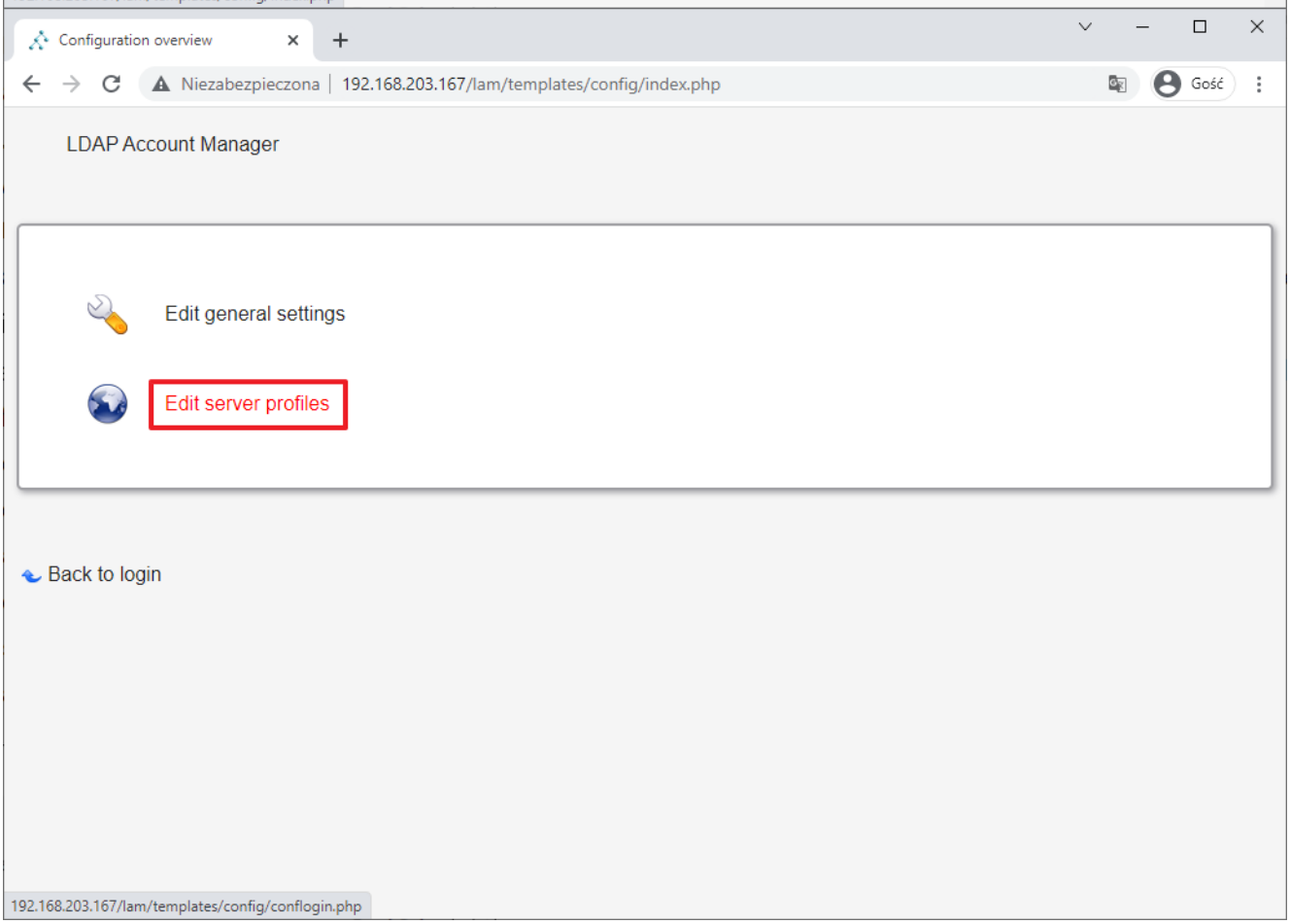

Configuration overview
Niezabezpieczona | 192.168.203.167/lam/templates/config/index.php
Gość
LDAP Account Manager
Edit general settings
Edit server profiles
Back to login
192.168.203.167/lam/templates/config/conflogin.php

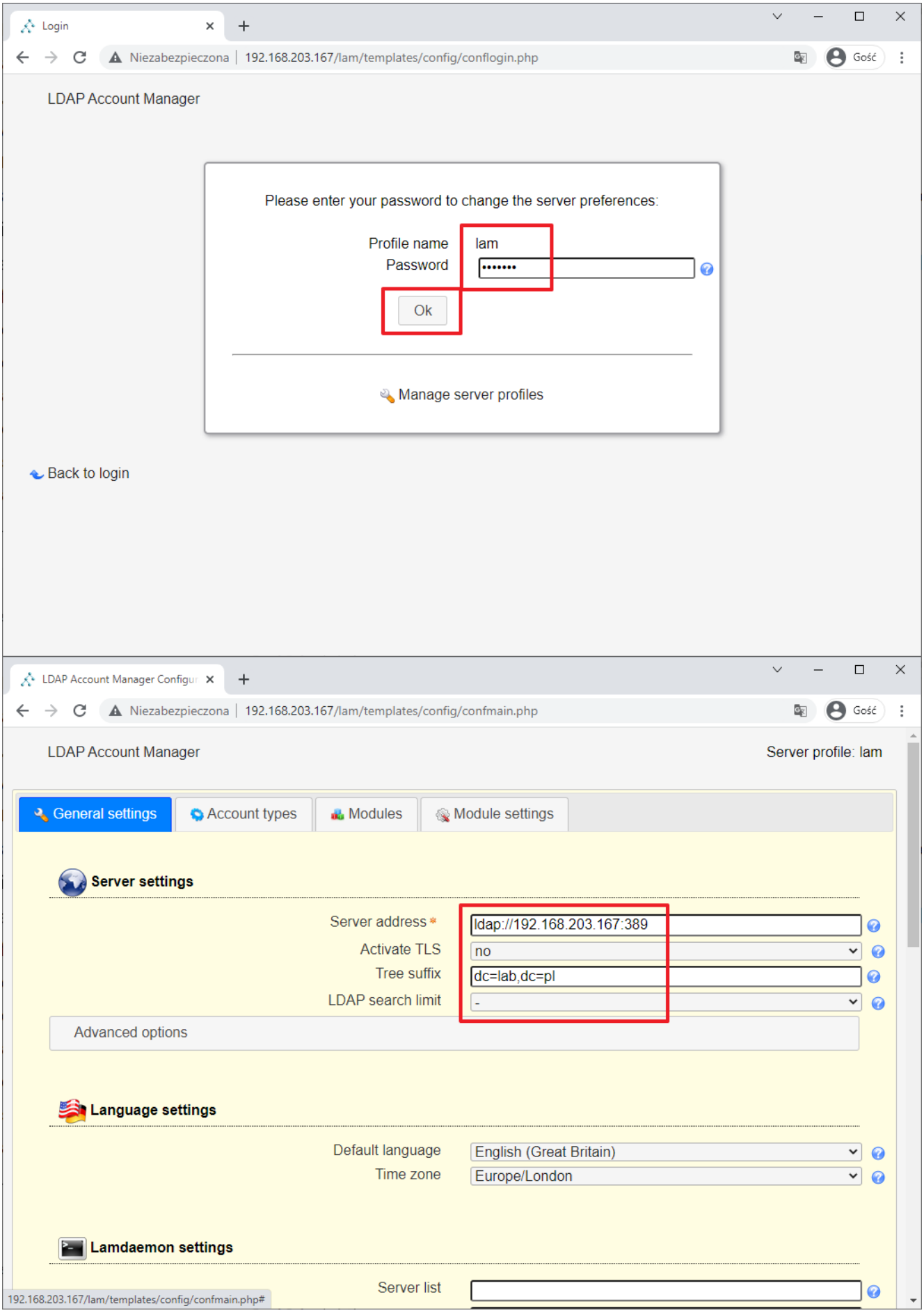


Tu możesz zostaw adres LOCALHOST zamiast adresu IP ldap://localhost:389 , „Tree suffix” jest trochę niżej w tym okienku.

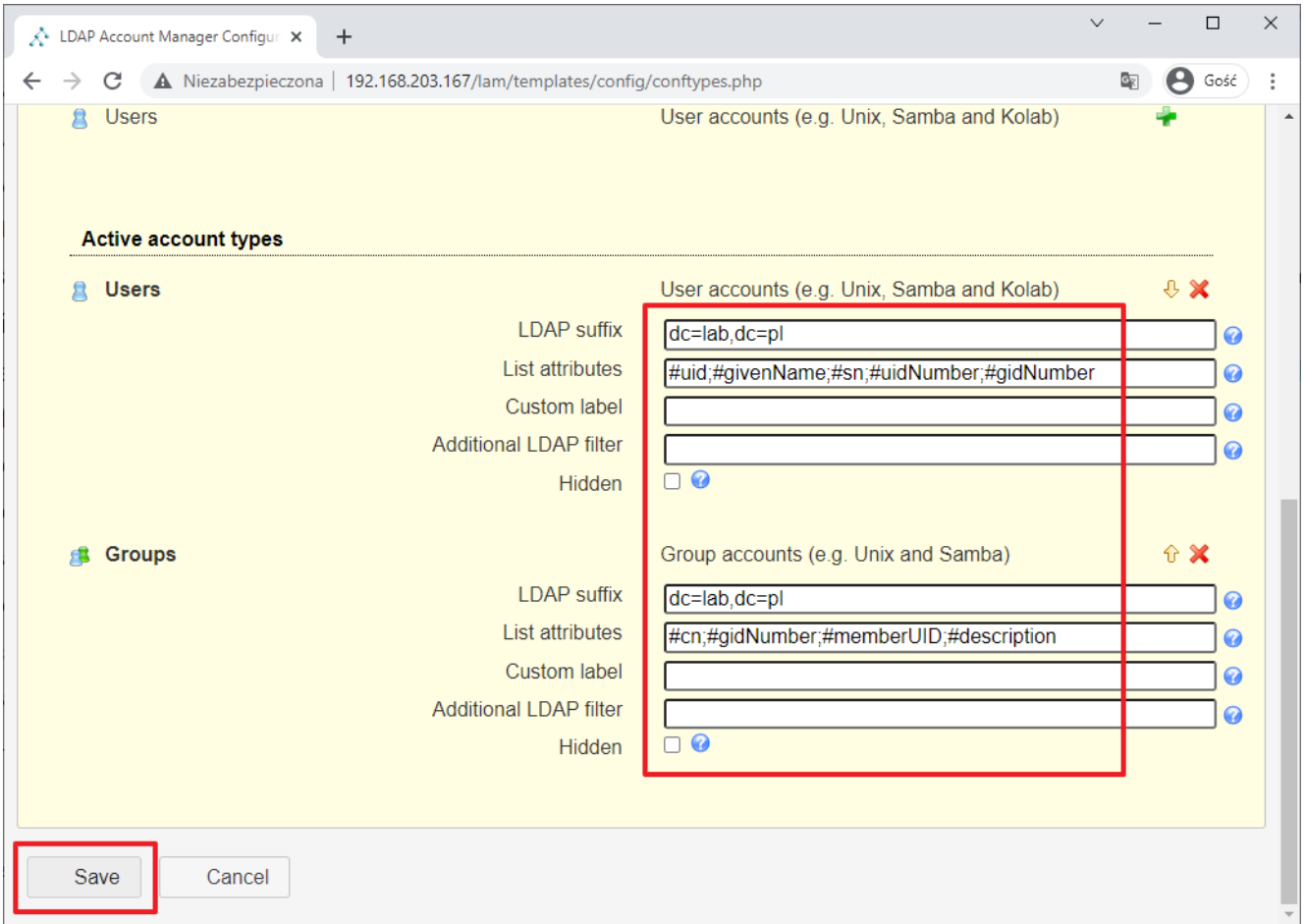

LDAP Account Manager Configu
Niezabezpieczona | 192.168.203.167/lam/templates/config/confmain.php
Gość
LDAP Account Manager
Server profile: lam
General settings
Account types
Modules
Module settings
Server settings
Server address *
ldap://192.168.203.167:389
Activate TLS
no
Tree suffix
dc=lab,dc=pl
LDAP search limit
-
Advanced options
Language settings
Default language
English (Great Britain)
Time zone
Europe/London
Lamdaemon settings
Server list
LDAP Account Manager Configu
Niezabezpieczona | 192.168.203.167/lam/templates/config/confmain.php
Gość
OU editor
Profile editor
Server information
PDF editor
LDAP import/export
File upload
Security settings
Login method
Fixed list
List of valid users *
cn=admin,dc=lab,dc=pl
2-factor authentication
Provider
None
Profile password
New password
Reenter password
Ustaw własne hasło
Save
Cancel

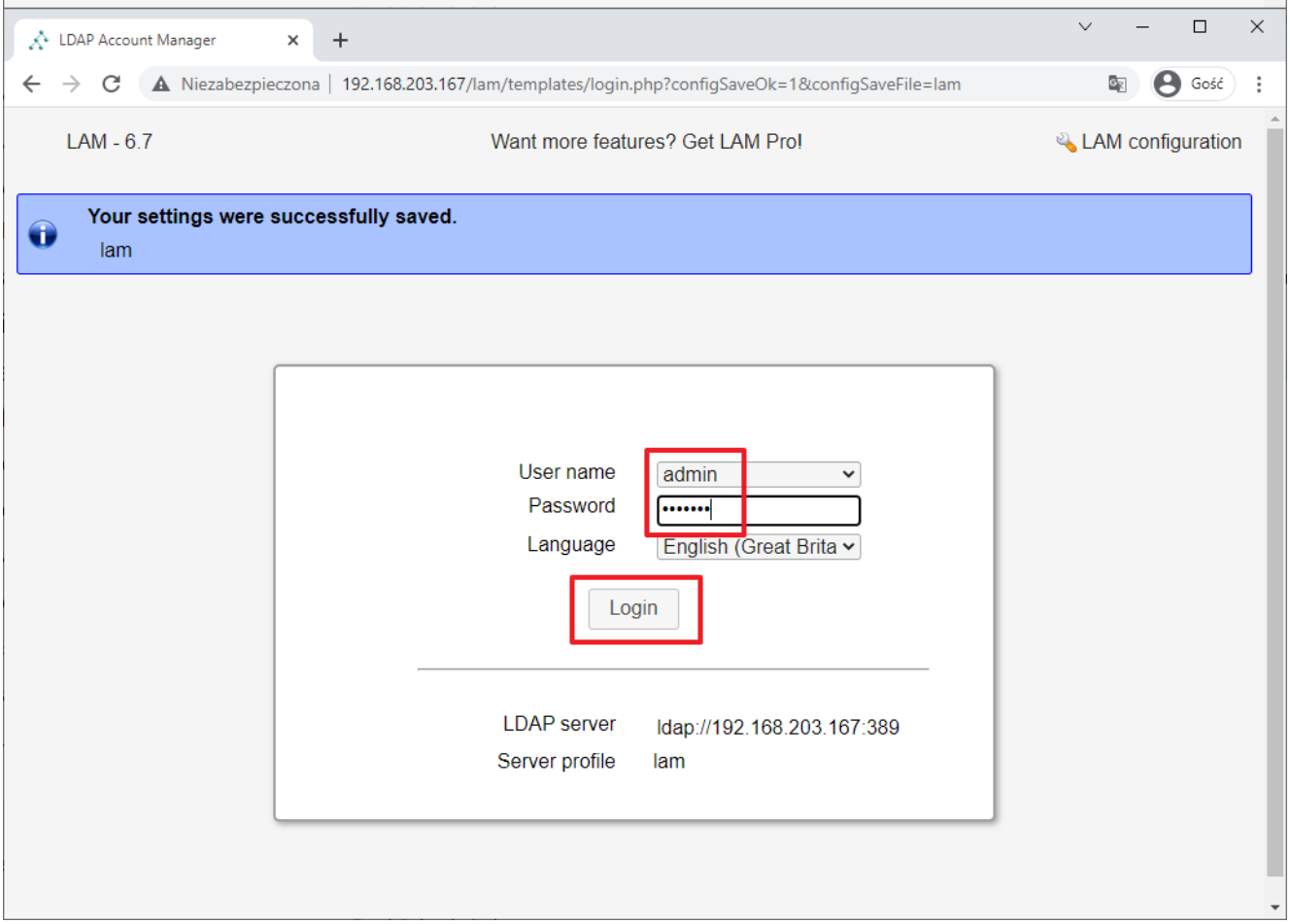

LDAP Account Manager
Niezabezpieczona | 192.168.203.167/lam/templates/login.php?configSaveOk=1&configSaveFile=lam
Gość
LAM - 6.7
Want more features? Get LAM Pro!
LAM configuration
Your settings were successfully saved.
lam
User name
admin
Password
Language
English (Great Brita
Login
LDAP server
ldap://192.168.203.167:389
Server profile
lam
192.168.203.167/lam/templates/config/index.php

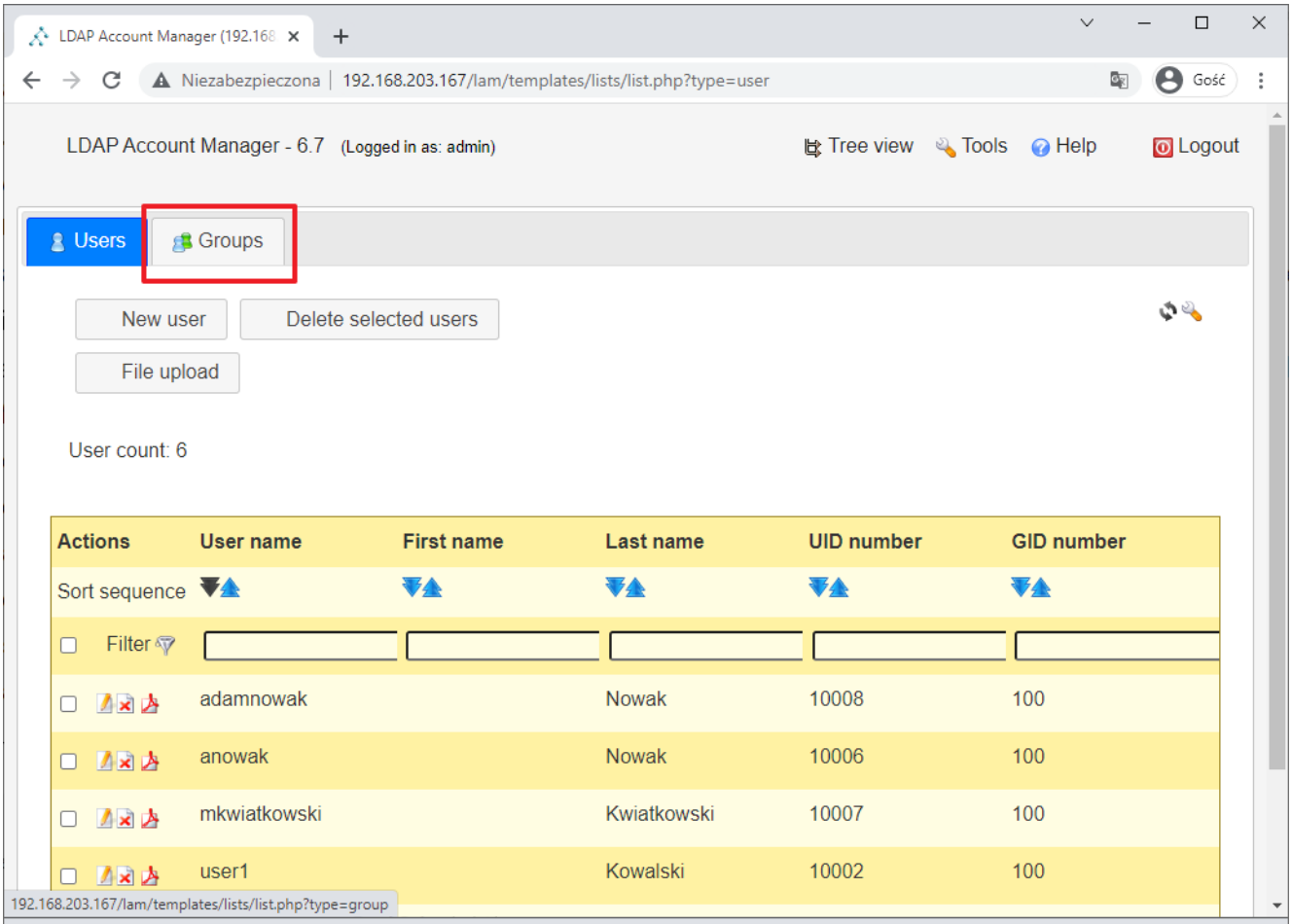

Configuration overview
Niezabezpieczona | 192.168.203.167/lam/templates/config/index.php
Gość
LDAP Account Manager
Edit general settings
Edit server profiles
Back to login
192.168.203.167/lam/templates/config/conflogin.php

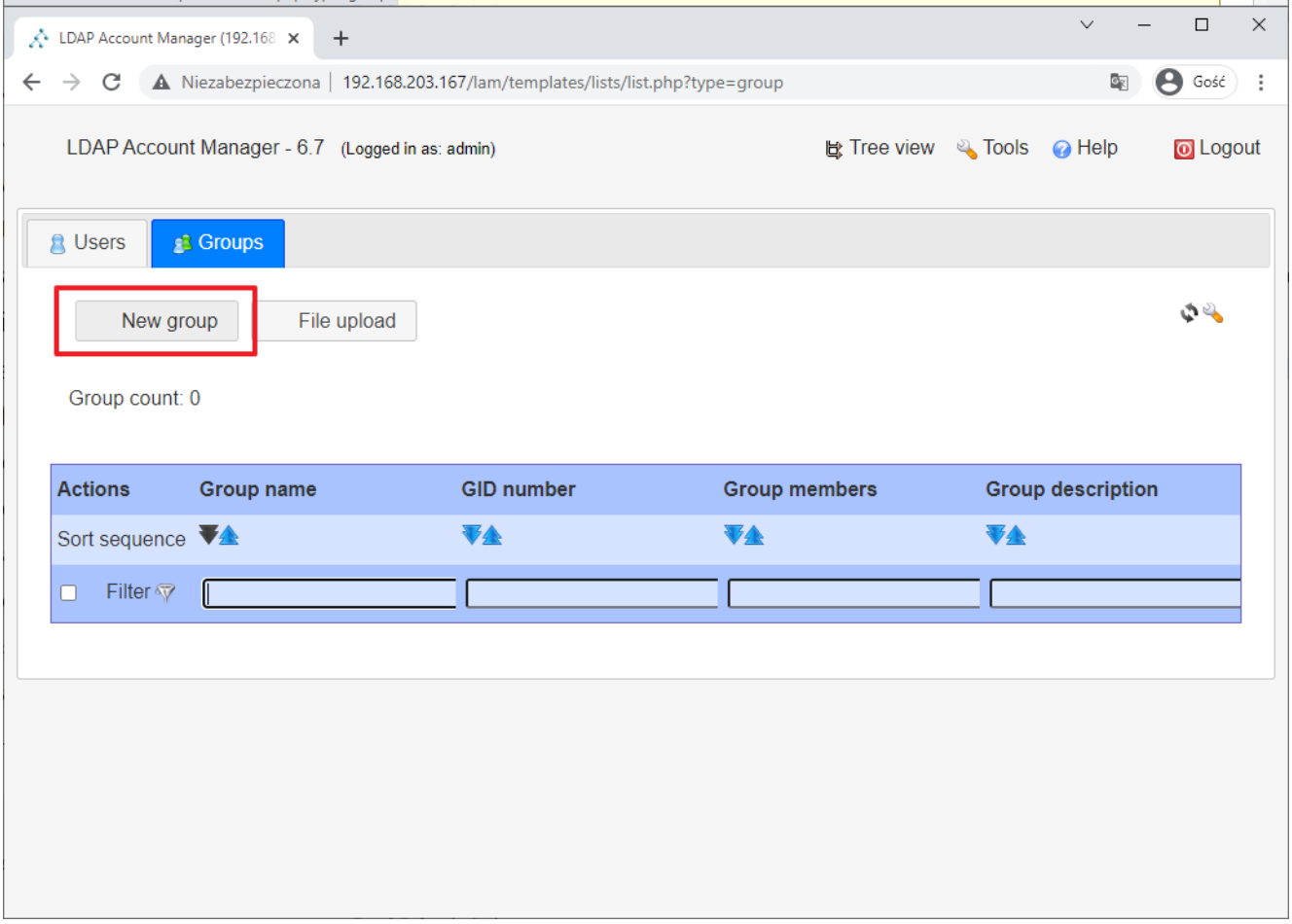


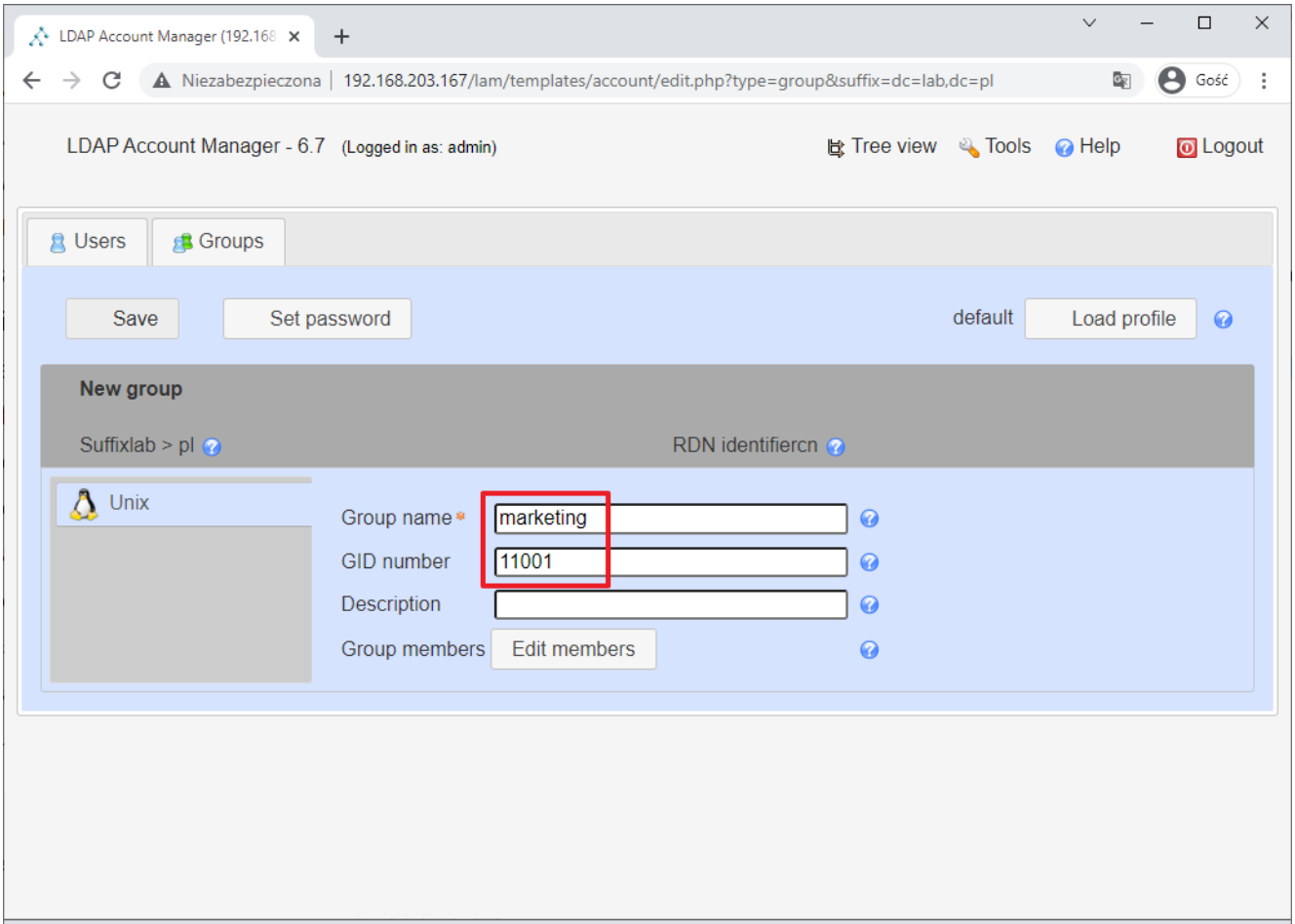
W zakładce „Account types” ustaw

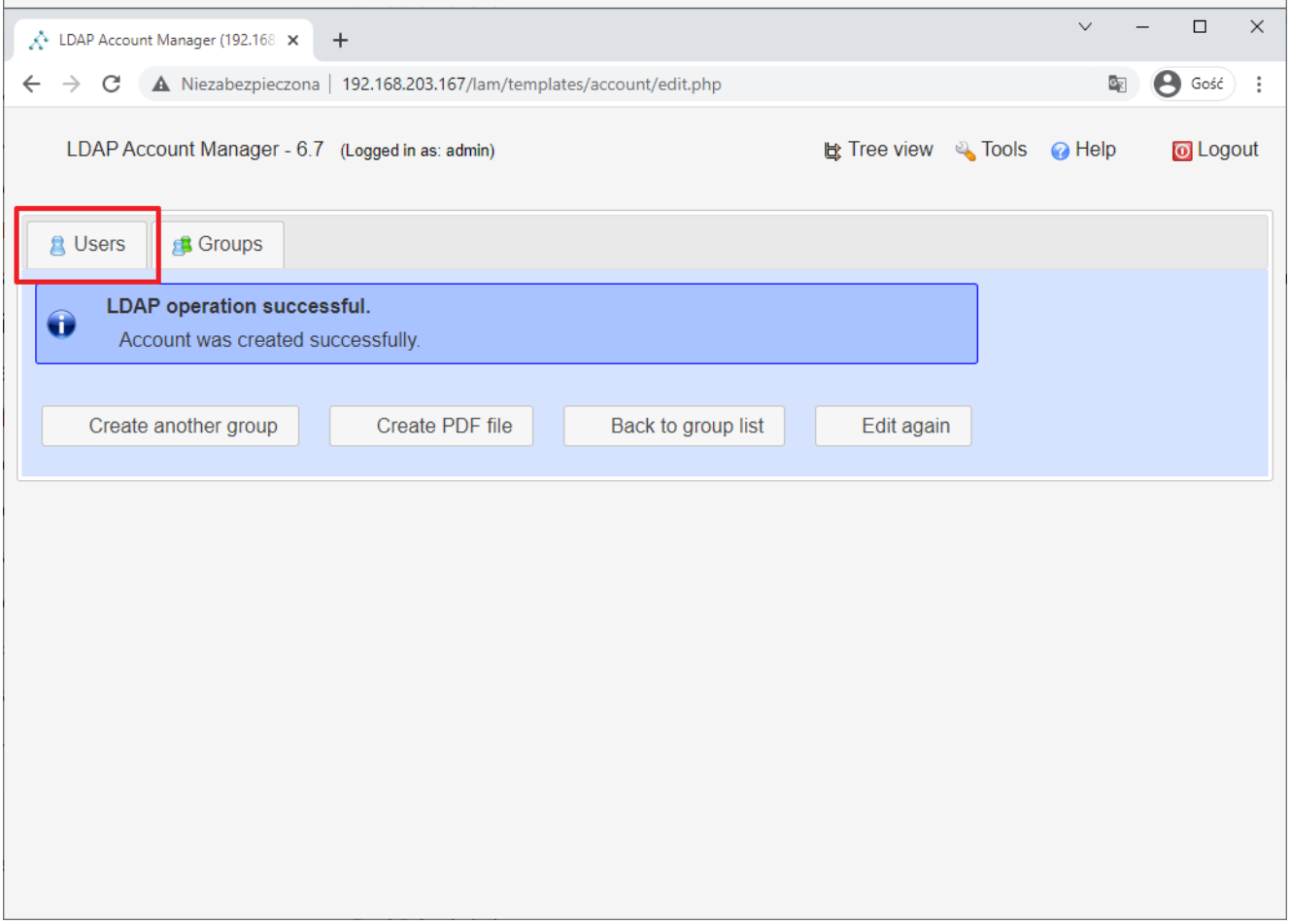

LDAP Account Manager Configu
Niezabezpieczona | 192.168.203.167/lam/templates/config/conftypes.php
Gość
Users
User accounts (e.g. Unix, Samba and Kolab)
Active account types
Users
User accounts (e.g. Unix, Samba and Kolab)
LDAP suffix
dc=lab,dc=pl
List attributes
#uid;#givenName;#sn;#uidNumber;#gidNumber
Custom label
Additional LDAP filter
Hidden
Groups
Group accounts (e.g. Unix and Samba)
LDAP suffix
dc=lab,dc=pl
List attributes
#cn;#gidNumber;#memberUID;#description
Custom label
Additional LDAP filter
Hidden
Save
Cancel

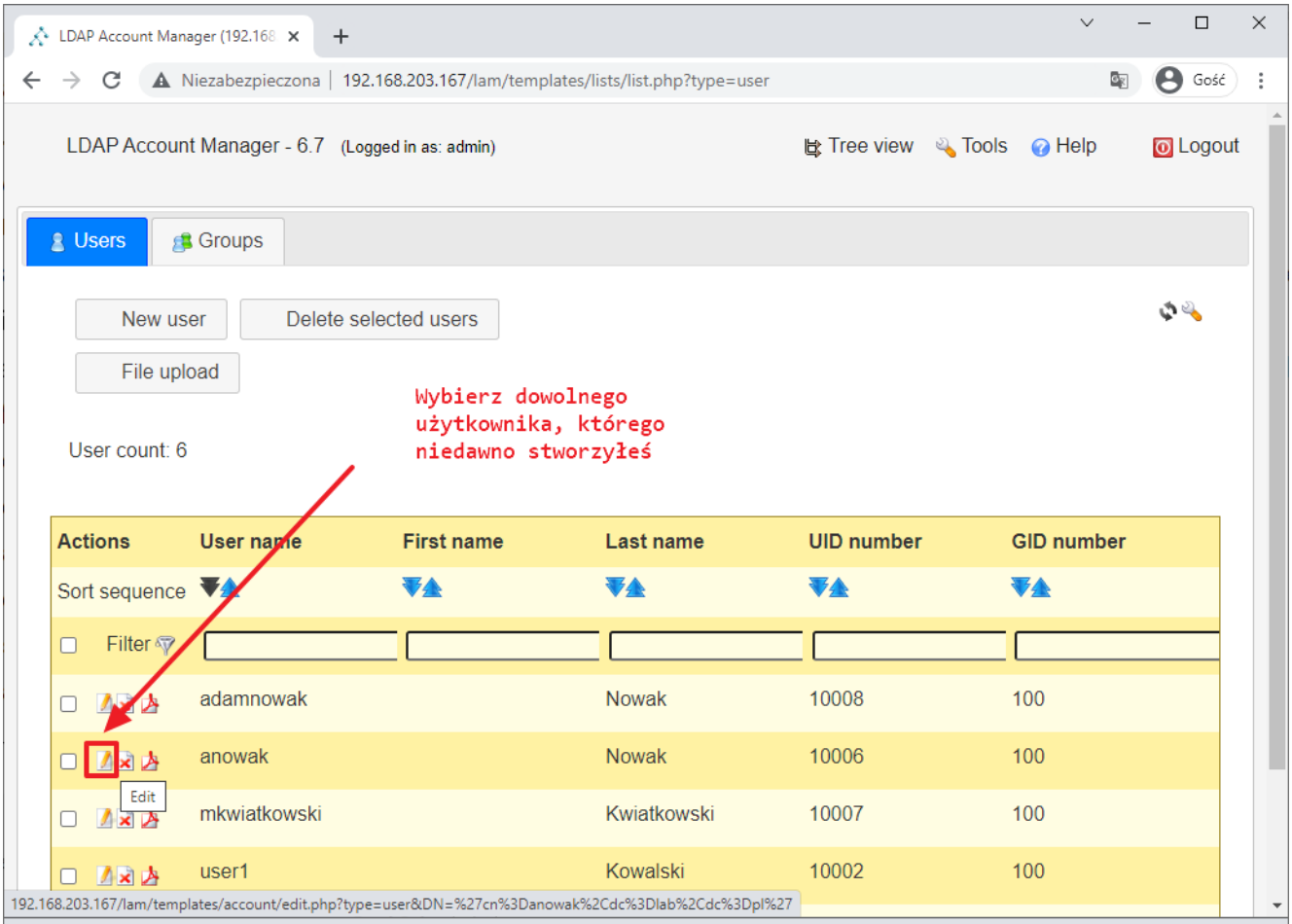

LDAP Account Manager
Niezabezpieczona | 192.168.203.167/lam/templates/login.php?configSaveOk=1&configSaveFile=lam
Gość
LAM - 6.7
Want more features? Get LAM Pro!
LAM configuration
Your settings were successfully saved.
lam
User name
admin
Password
Language
English (Great Brita
Login
LDAP server
ldap://192.168.203.167:389
Server profile
lam

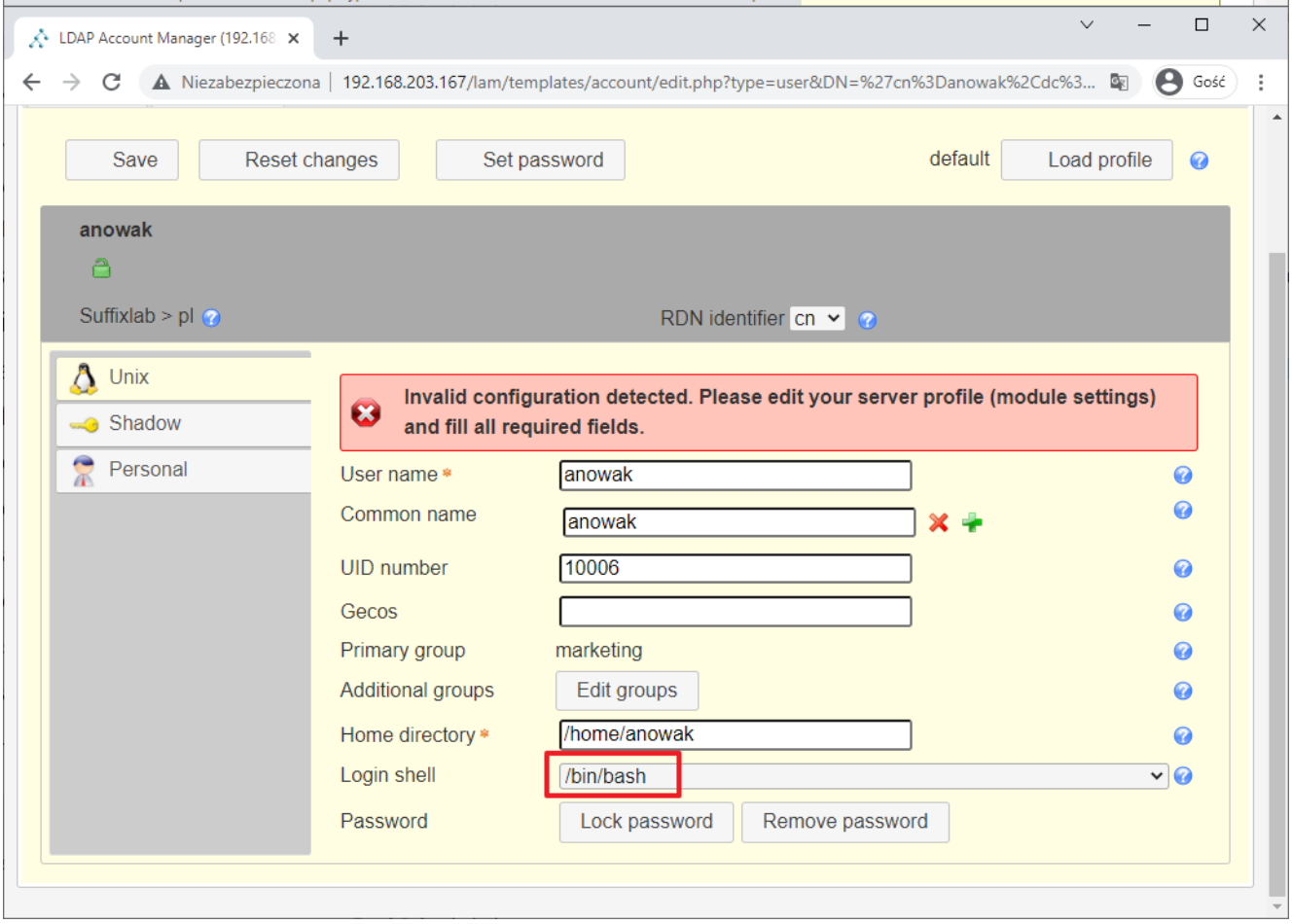

LDAP Account Manager (192.168
Niezabezpieczona | 192.168.203.167/lam/templates/lists/list.php?type=user
Gość
LDAP Account Manager - 6.7 (Logged in as: admin)
Tree view
Tools
Help
Logout
Users
Groups
New user
Delete selected users
File upload
User count: 6
Actions
User name
First name
Last name
UID number
GID number
Sort sequence
Filter
adamnowak
Nowak
10008
100
anowak
Nowak
10006
100
mkwiatkowski
Kwiatkowski
10007
100
user1
Kowalski
10002
100
192.168.203.167/lam/templates/lists/list.php?type=group

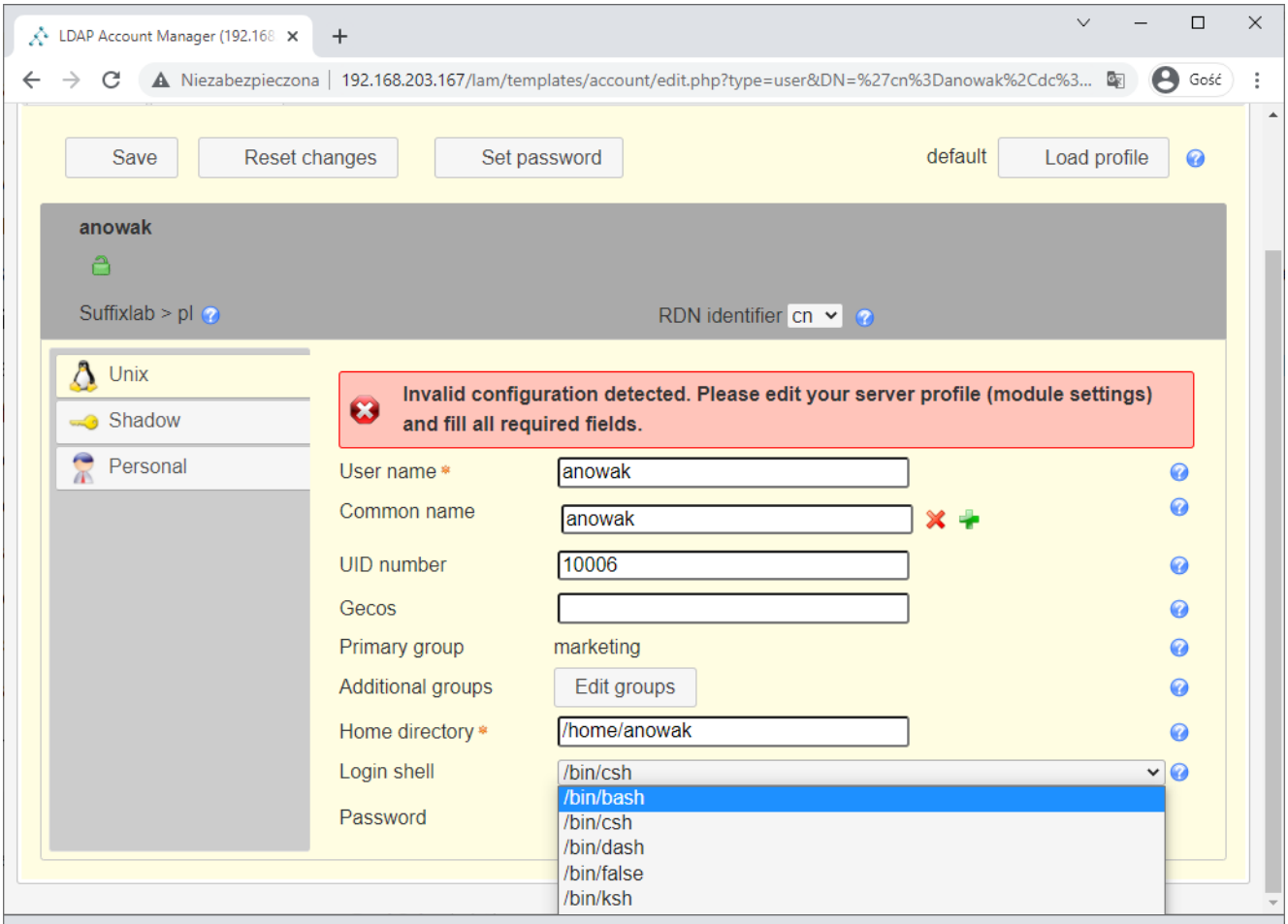

LDAP Account Manager (192.168
Niezabezpieczona | 192.168.203.167/lam/templates/lists/list.php?type=group
Gość
LDAP Account Manager - 6.7 (Logged in as: admin)
Tree view
Tools
Help
Logout
Users
Groups
New group
File upload
Group count: 0
Actions
Group name
GID number
Group members
Group description
Sort sequence
Filter

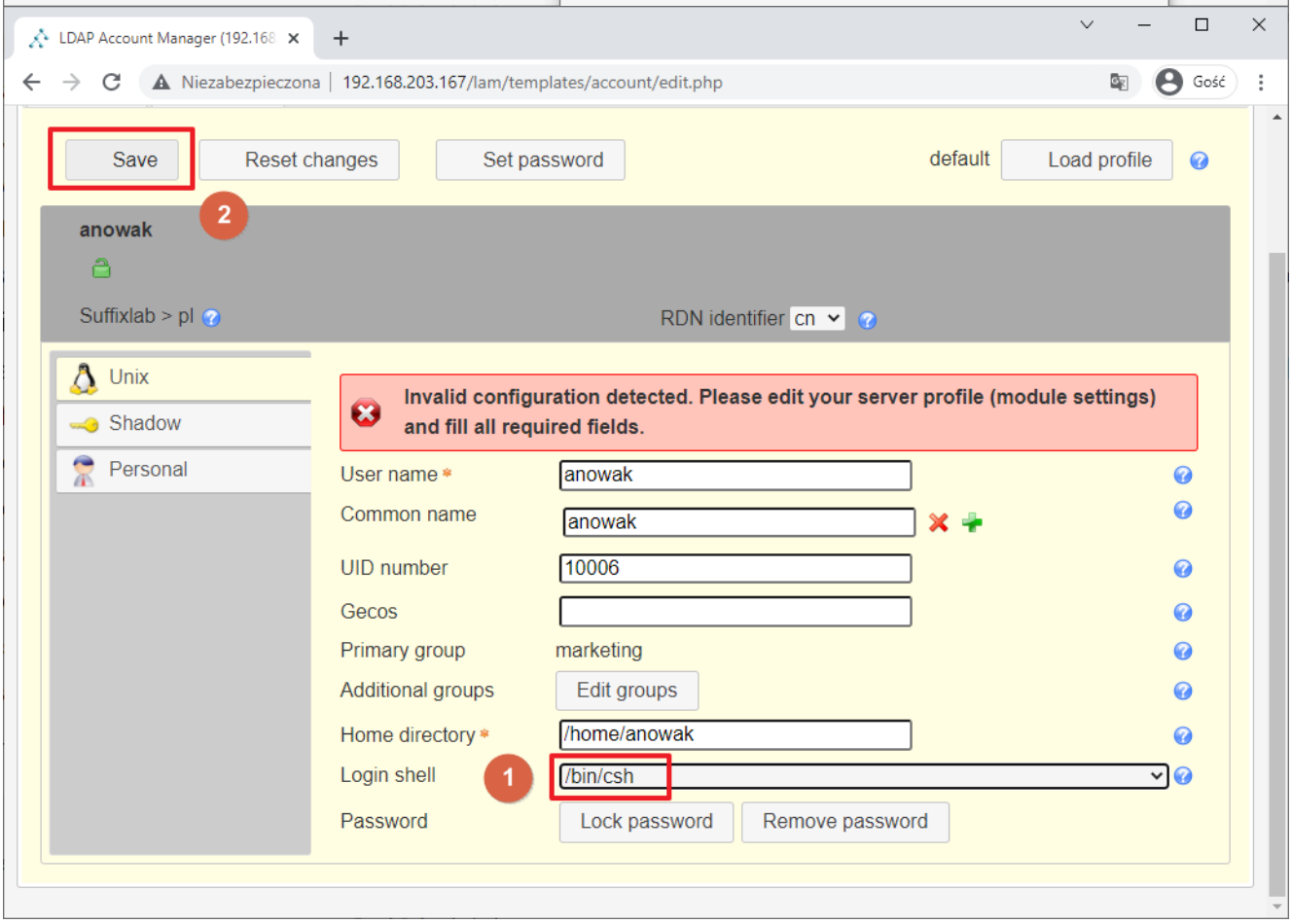

LDAP Account Manager (192.168
Niezabezpieczona | 192.168.203.167/lam/templates/account/edit.php?type=group&suffix=dc=lab,dc=pl
Gość
LDAP Account Manager - 6.7 (Logged in as: admin)
Tree view
Tools
Help
Logout
Users
Groups
Save
Set password
default
Load profile
New group
Suffixlab > pl
RDN identifiercn
Unix
Group name *
marketing
GID number
11001
Description
Group members
Edit members

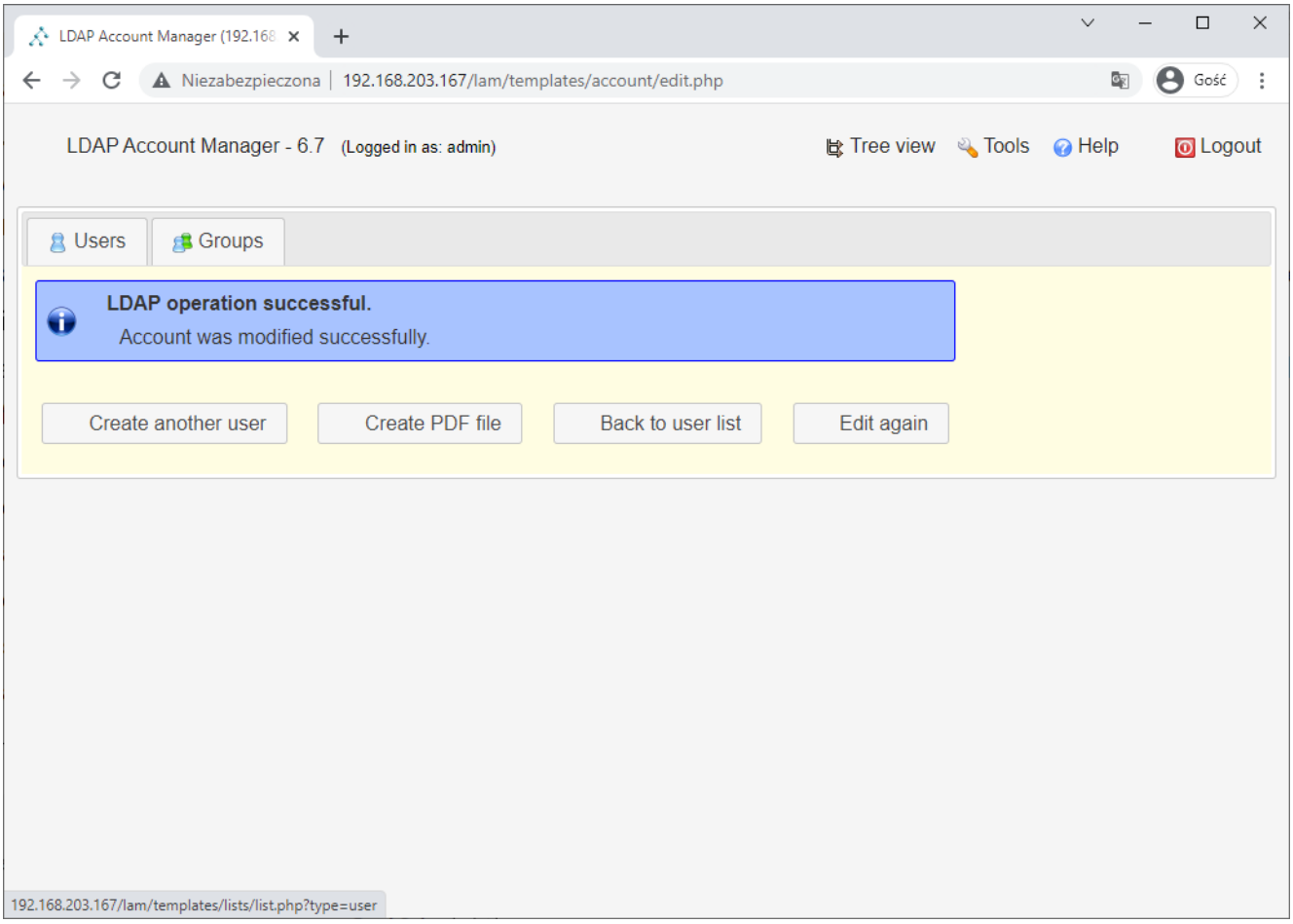

LDAP Account Manager (192.168
Niezabezpieczona | 192.168.203.167/lam/templates/account/edit.php
Gość
LDAP Account Manager - 6.7 (Logged in as: admin)
Tree view
Tools
Help
Logout
Users
Groups
LDAP operation successful.
Account was created successfully.
Create another group
Create PDF file
Back to group list
Edit again


LDAP Account Manager (192.168
Niezabezpieczona | 192.168.203.167/lam/templates/lists/list.php?type=user
Gość
LDAP Account Manager - 6.7 (Logged in as: admin)
Tree view
Tools
Help
Logout
Users
Groups
New user
Delete selected users
File upload
Wybierz dowolnego użytkownika, którego niedawno stworzyłeś
User count: 6
Actions
User name
First name
Last name
UID number
GID number
Sort sequence
Filter
adamnowak
Nowak
10008
100
anowak
Nowak
10006
100
Edit
mkwiatkowski
Kwiatkowski
10007
100
user1
Kowalski
10002
100
192.168.203.167/lam/templates/account/edit.php?type=user&DN=%27cn%3Danowak%2Cdc%3Dlab%2Cdc%3Dpl%27

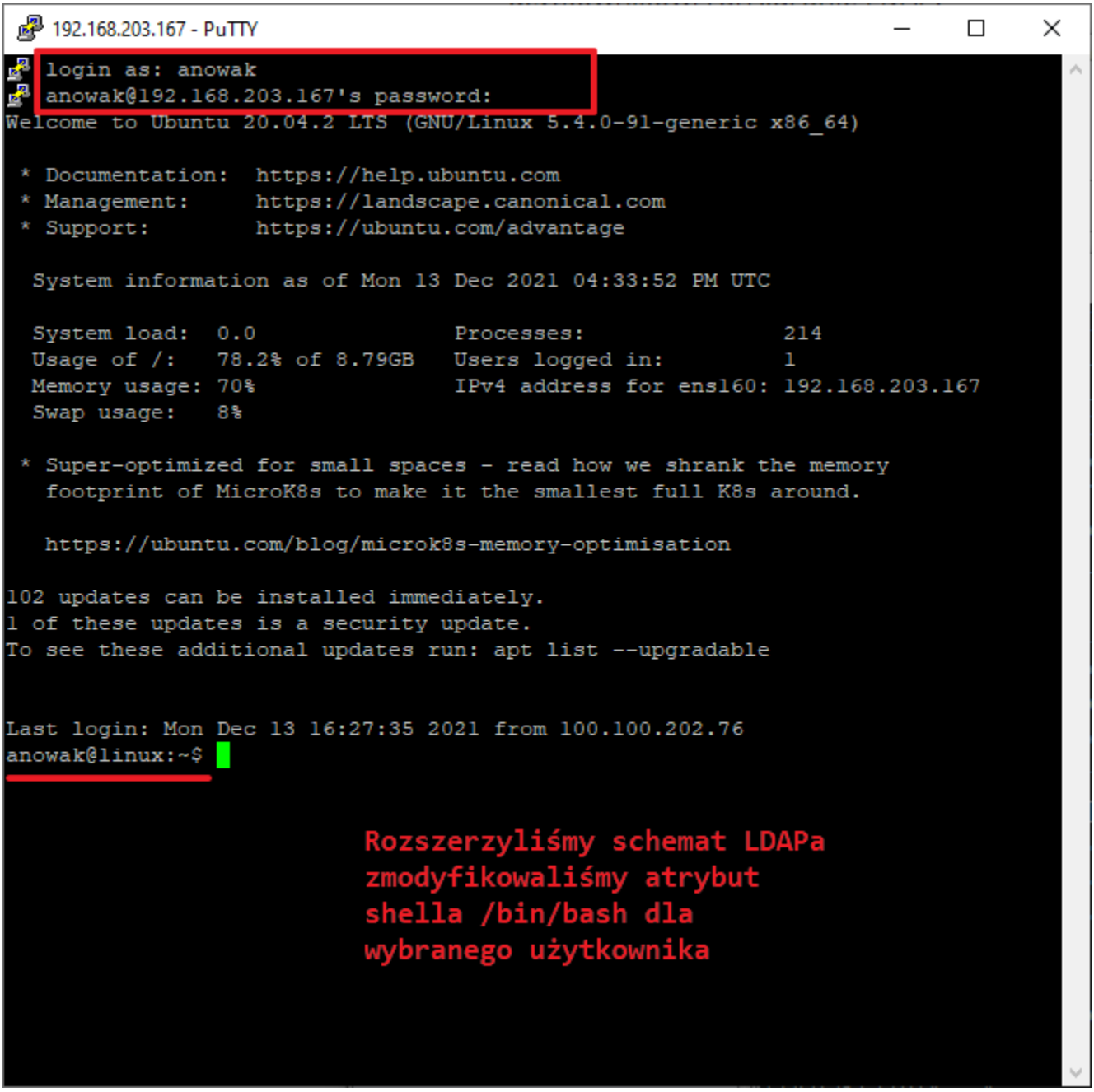

LDAP Account Manager (192.168
Niezabezpieczona | 192.168.203.167/lam/templates/account/edit.php?type=user&DN=%27cn%3Danowak%2Cdc%3...
Gość
Save
Reset changes
Set password
default
Load profile
anowak
Suffixlab > pl
RDN identifier cn
Unix
Shadow
Personal
Invalid configuration detected. Please edit your server profile (module settings) and fill all required fields.
User name *
anowak
Common name
anowak
UID number
10006
Gecos
Primary group
marketing
Additional groups
Edit groups
Home directory *
/home/anowak
Login shell
/bin/bash
Password
Lock password
Remove password


LDAP Account Manager (192.168
Niezabezpieczona | 192.168.203.167/lam/templates/account/edit.php?type=user&DN=%27cn%3Danowak%2Cdc%3...
Gość
Save
Reset changes
Set password
default
Load profile
anowak
Suffixlab > pl
RDN identifier cn
Unix
Shadow
Personal
Invalid configuration detected. Please edit your server profile (module settings) and fill all required fields.
User name *
anowak
Common name
anowak
UID number
10006
Gecos
Primary group
marketing
Additional groups
Edit groups
Home directory *
/home/anowak
Login shell
/bin/csh
/bin/bash
/bin/csh
/bin/dash
/bin/false
/bin/ksh
Password


LDAP Account Manager (192.168
Niezabezpieczona | 192.168.203.167/lam/templates/account/edit.php
Gość
Save
2
Reset changes
Set password
default
Load profile
anowak
Suffixlab > pl
RDN identifier cn
Unix
Shadow
Personal
Invalid configuration detected. Please edit your server profile (module settings) and fill all required fields.
User name *
anowak
Common name
anowak
UID number
10006
Gecos
Primary group
marketing
Additional groups
Edit groups
Home directory *
/home/anowak
Login shell
1
/bin/csh
Password
Lock password
Remove password



Sprawdź jeszcze raz Putty łączność za pomocą wybrane użytkownika z katalogu LDAP. Znak zachęty wskazuje na shella /bin/bash


192.168.203.167 - PuTTY
login as: anowak
anowak@192.168.203.167's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-91-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Mon 13 Dec 2021 04:33:52 PM UTC
System load: 0.0
Usage of /: 78.2% of 8.79GB
Memory usage: 70%
Swap usage: 8%
Processes: 214
Users logged in: 1
IPv4 address for ens160: 192.168.203.167
* Super-optimized for small spaces - read how we shrank the memory
footprint of MicroK8s to make it the smallest full K8s around.
https://ubuntu.com/blog/microk8s-memory-optimisation
102 updates can be installed immediately.
1 of these updates is a security update.
To see these additional updates run: apt list --upgradable
Last login: Mon Dec 13 16:27:35 2021 from 100.100.202.76
anowak@linux:~$
Rozszerzyliśmy schemat LDAPa
zmodyfikowaliśmy atrybut
shella /bin/bash dla
wybranego użytkownika