

# ZI-ACCESS - Installation and Administration Guide

- [Installation or update](#)
- [Zimlet configuration](#)
- [Necessary Zimbra configuration](#)
- [Release Notes](#)
  - [ZI-Access 2.5](#)

# Installation or update

**It is necessary to have ZI-LicenseSystem already installed in the system prior to any other ZI-\* zimlet installation.** Check here: [ZI-LicenseSystem - Installation or update](#)

To update zimlet to the newer version just follow the installation steps and when the installer asks you if you want to update answer: Y

Download the latest version of the zimlet package from <https://www.intalio.pl/en/zi-access-downloads> and unpack it in /tmp (as root) for exmaple:

```
cd /tmp
wget https://www.intalio.pl/sites/default/files/modules-files/zi-access-1.9-zimbra9.tar__0.gz
tar xvzf zi-access-1.9-zimbra9.tar_.gz
```

Be sure to download zimlet designed for your Zimbra release eg. 8.8.15 or 9.0.0

Run installation script (as root):

```
cd ./ZI-Access-1.9-Zimbra9/
perl ./ZI-Installer --install-deps
```

At the beginning required perl packages will be installed if they are not available in the system already:

```

o JSON.....ok (v2.94)
o String::Random.....ok (v0.30)
o Text::ASCIITable.....ok (v0.22)
o File::Copy::Recursive.....ok (v0.44)
o Archive::Zip.....ok (v1.64)
o Archive::Zip::MemberRead.....ok (v1.64)
o File::chmod.....ok (v0.42)
o File::chmod::Recursive.....ok (v1.0.3)
o JSON.....ok (v2.94)
o String::Random.....ok (v0.30)
o Text::ASCIITable.....ok (v0.22)
o LWP::Authen::Basic.....ok (v6.26)
o LWP::Authen::Digest.....ok (v6.26)
o LWP::Protocol::cpan.....FAILED! Not all prerequisites for this module correctly installed.
o LWP::Protocol::data.....FAILED! Not all prerequisites for this module correctly installed.
o LWP::Protocol::file.....FAILED! Not all prerequisites for this module correctly installed.
o LWP::Protocol::ftp.....FAILED! Not all prerequisites for this module correctly installed.
o LWP::Protocol::gopher.....FAILED! Not all prerequisites for this module correctly installed.
o LWP::Protocol::http.....FAILED! Not all prerequisites for this module correctly installed.
o LWP::Protocol::https.....FAILED! Not all prerequisites for this module correctly installed.
o LWP::Protocol::ldap.....Not installed! Use: 'apt-get install -y libnet-ldap-perl' (required - Provide LDAP support for LWP::UserAgent)
o LWP::Protocol::ldaps.....Not installed! Use: 'apt-get install -y libnet-ldap-perl' (required - Provide LDAP support for LWP::UserAgent)
o LWP::Protocol::loopback.....FAILED! Not all prerequisites for this module correctly installed.
o LWP::Protocol::nntp.....FAILED! Not all prerequisites for this module correctly installed.
o LWP::Protocol::nogo.....FAILED! Not all prerequisites for this module correctly installed.
o LWP::UserAgent.....FAILED! Not all prerequisites for this module correctly installed.
o Term::ReadKey.....Not installed! Use: 'apt-get install -y libterm-readkey-perl' (required - A perl module for simple terminal control)
o URI::URL.....ok (v5.04)
o URI::http.....ok (v1.71)
o File::Copy::Recursive.....ok (v0.44)
o Try::Tiny.....Not installed! Use: 'apt-get install -y libtry-tiny-perl' (required - Try::Tiny - Minimal try/catch with proper preservation of $@)
o Archive::Zip.....ok (v1.64)
o Archive::Zip::MemberRead.....ok (v1.64)
o JSON.....ok (v2.94)
o String::Random.....ok (v0.30)
o Text::ASCIITable.....ok (v0.22)
o File::Copy::Recursive.....ok (v0.44)
o Archive::Zip.....ok (v1.64)
o Archive::Zip::MemberRead.....ok (v1.64)
o File::chmod.....ok (v0.42)
o File::chmod::Recursive.....ok (v1.0.3)

```

The script has the appropriate root privileges.

Install the missing modules? (Y/n or exit):

Answer: Y and wait until the package manager finishes its work:

System check dependencies....

- o JSON.....ok (v2.94)
- o String::Random.....ok (v0.30)
- o Text::ASCIITable.....ok (v0.22)
- o File::Copy::Recursive.....ok (v0.44)
- o Archive::Zip.....ok (v1.64)
- o Archive::Zip::MemberRead.....ok (v1.64)
- o File::chmod.....ok (v0.42)
- o File::chmod::Recursive.....ok (v1.0.3)
- o JSON.....ok (v2.94)
- o String::Random.....ok (v0.30)
- o Text::ASCIITable.....ok (v0.22)
- o LWP::Authen::Basic.....ok (v6.26)
- o LWP::Authen::Digest.....ok (v6.26)
- o LWP::Protocol::cpan.....ok (v6.26)
- o LWP::Protocol::data.....ok (v6.26)
- o LWP::Protocol::file.....ok (v6.26)
- o LWP::Protocol::ftp.....ok (v6.26)
- o LWP::Protocol::gopher.....ok (v6.26)
- o LWP::Protocol::http.....ok (v6.26)
- o LWP::Protocol::https.....ok (v6.06)
- o LWP::Protocol::ldap.....ok (v1.25)
- o LWP::Protocol::ldaps.....ok (undef)
- o LWP::Protocol::loopback.....ok (v6.26)
- o LWP::Protocol::nntp.....ok (v6.26)
- o LWP::Protocol::nogo.....ok (v6.26)
- o LWP::UserAgent.....ok (v6.26)
- o Term::ReadKey.....ok (v2.37)
- o URI::URL.....ok (v5.04)
- o URI::http.....ok (v1.71)
- o File::Copy::Recursive.....ok (v0.44)
- o Try::Tiny.....ok (v0.30)
- o Archive::Zip.....ok (v1.64)
- o Archive::Zip::MemberRead.....ok (v1.64)
- o JSON.....ok (v2.94)
- o String::Random.....ok (v0.30)
- o Text::ASCIITable.....ok (v0.22)
- o File::Copy::Recursive.....ok (v0.44)
- o Archive::Zip.....ok (v1.64)
- o Archive::Zip::MemberRead.....ok (v1.64)
- o File::chmod.....ok (v0.42)
- o File::chmod::Recursive.....ok (v1.0.3)

```

mysqlNewUser
ZimletDirName
mysqlNewPassword
NoAsk
installConfigPath
RestartZimbra
NoActivate
zimbraPath
InstallDeps
mysqlNewDatabaseName
DatabaseConfigLocation
mysqlHost
mysqlPort
SqlFile
NoDatabase
PostinstallCommand
DatabaseConfigFormat
version
ZI-Installer: "mysqlNewPassword" is not specified, use 3QPIYEsDjQ91fKm6uDjn081Ww3AXtwh9 password instead
ZI-Installer: "mysqlHost" is not specified, use 127.0.0.1 host instead
ZI-Installer: "mysqlPort" is not specified, use 7306 port instead

-----CONFIG-----
DatabaseConfigFormat      --> CS
DatabaseConfigLocation    --> ./Extensions/db.properties
installConfigPath         --> zi-install-conf.json
InstallDeps               -->
mysqlHost                 --> 127.0.0.1
mysqlNewDatabaseName      --> intalioAuth
mysqlNewPassword          --> 3QPIYEsDjQ91fKm6uDjn081Ww3AXtwh9
mysqlNewUser              --> user_intalioauth
mysqlPort                 --> 7306
NoActivate                -->
NoAsk                     -->
NoDatabase                -->
PostinstallCommand        -->
RestartZimbra             -->
SqlFile                   -->
Update                    --> 0
version                   -->
zimbraPath                --> /opt/zimbra
ZimletDirName             --> IntalioZiAccess
-----

Mailboxd service won't be restarted automatically.
Proceed? (Y/n or exit): y

```

Type: Y and press Enter

```

SqlFile          -->
Update           --> 0
version          -->
zimbraPath       --> /opt/zimbra
ZimletDirName    --> IntalioZiAccess
-----

Mailboxd service won't be restarted automatically.
Proceed? (Y/n or exit): y
Installation starting.....
Creating database...
Creating connection string file....
Creating zimlet directory...
Removing earlier version...
Earlier versions not found...
Copying Extensions...
Copying helpers...
Copying files:
helpers/config.json -> /opt/zimbra/lib/ext/IntalioZiAccess/config.json
Copying script libs...
Setting permissions...
Looking for zip files in Zimlets directory...
Found 2 files
Starting deploy....
2022-09-06 10:25:25,589 [main] INFO : Deploying Zimlet intalio_zi_access in LDAP.
2022-09-06 10:25:25,782 [main] INFO : Installing Zimlet intalio_zi_access on this host.
2022-09-06 10:25:25,818 [main] INFO : Upgrading Zimlet intalio_zi_access to 1.9.124
2022-09-06 10:25:25,876 [main] INFO : Enabling Zimlet intalio_zi_access
2022-09-06 10:25:32,519 [main] INFO : Deploying Zimlet intalio_zi_access_9 in LDAP.
2022-09-06 10:25:32,674 [main] INFO : Installing Zimlet intalio_zi_access_9 on this host.
2022-09-06 10:25:32,725 [main] INFO : Upgrading Zimlet intalio_zi_access_9 to 1.9.0
2022-09-06 10:25:32,793 [main] INFO : Adding Zimlet intalio_zi_access_9 to COS default
2022-09-06 10:25:32,842 [main] INFO : Enabling Zimlet intalio_zi_access_9

```

When the deployment process is done you will be asked to provide the login and password that you can find in the license documents you received from us:

```

Please enter your login/email: zimbrademo
Enter your password:

```

Choose the license number (usually you will see only one option), press Enter, verify that the details are correct and proceed by answering Y

Licenses		
Nr	license_number	description
1	np [REDACTED]	ZI-License for Intalio ZimbraDemo
2	81 [REDACTED]	ZI-License for Intalio ZimbraDemo (for Trial testing)

```
Please choose from 1-2 option or type exit
```

Your option: 1

Extensions in license number: n[REDACTED]							
Nr	name	extension_number	start_date	end_date	version	support	user_limit
1	ZI-Piler	E[REDACTED]	2019-03-21	2099-12-31	2.x	2050-12-31	1000
2	ZI-Knock	E[REDACTED]	2020-04-30	2023-04-29	1.x	2050-12-31	500
3	ZI-Access	J[REDACTED]	2019-06-03	2099-12-31	1.x	2050-12-31	9999
4	ZI-MailApproval	C[REDACTED]	2019-06-04	2099-12-31	1.x	2050-12-31	9999
5	ZI-ADPassword	C[REDACTED]	2019-01-01	2099-03-03	1.x	2022-03-03	2000
6	ZI-Chat	E[REDACTED]	2019-06-04	2099-12-31	2.x	2050-12-31	9999
7	ZI-PolicyD	T[REDACTED]	2020-09-08	2099-12-31	2.x.x	2050-12-31	0
8	ZI-PassRecovery	C[REDACTED]	2021-07-08	2099-12-31	1.x	2022-07-07	9999
9	ZI-SecurityIncident	L[REDACTED]	2020-09-11	2099-09-29	1.x	2099-09-11	100000

```
Proceed? (Y/n or exit):
```

Your license will be downloaded and activated. In the last step you will be asked to restart the mailbox service. **You can skip it (answer: N) and restart the mailboxd service manually later but until that zimlet will not work properly.**

If you are going to install another zimlet right after this one it's not necessary to restart the mailbox at this point and you can do it only once after installing the last one.

```
Proceed? (Y/n or exit): y
Downloading license...
Saving license.....
Saving complete!
Activating Main License - version 1.0.15.3...
New zimbra version
Starting activation process.
Message from the activation server: Main license has been activated!
You have the right to activate the license.
New activation - ok
Reponse is 0
Activate ZI-Access - version 1.9.1....
New zimbra version
Starting activation process.
Message from the activation server: Extension was activated!
You have the right to activate the license.
New activation - ok

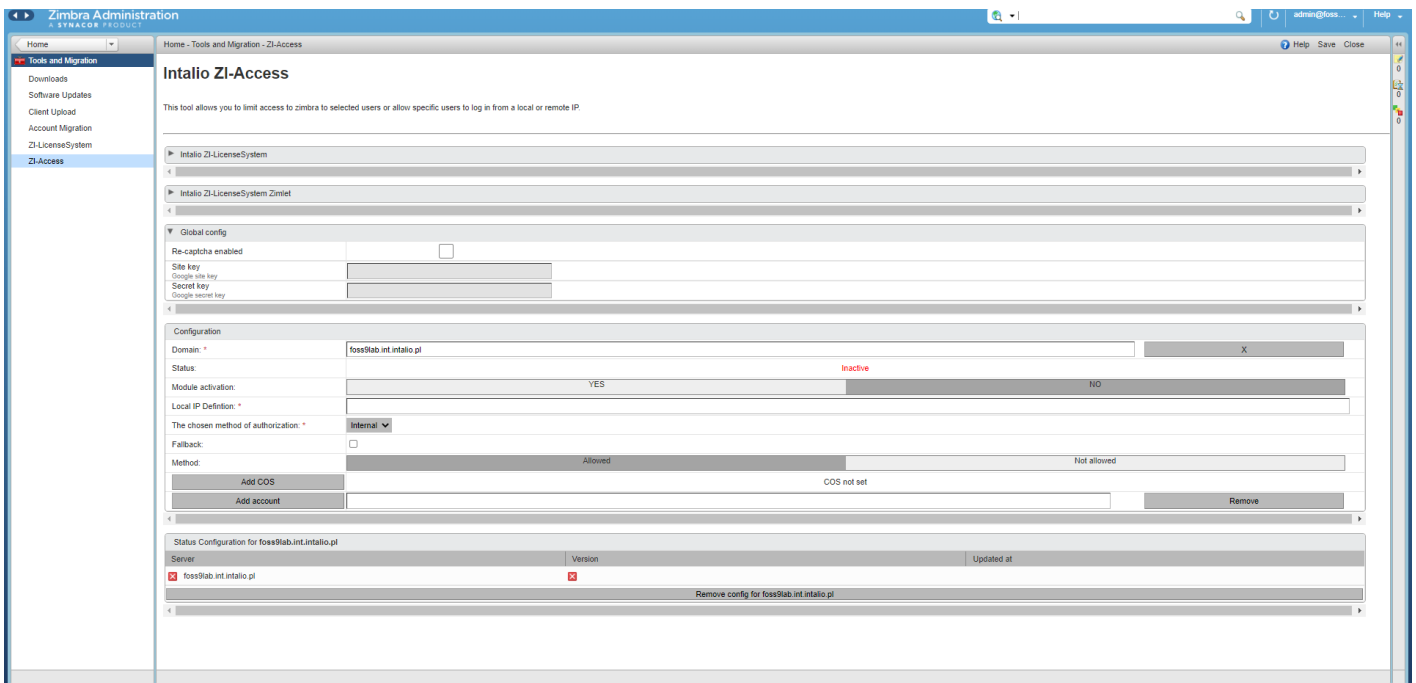
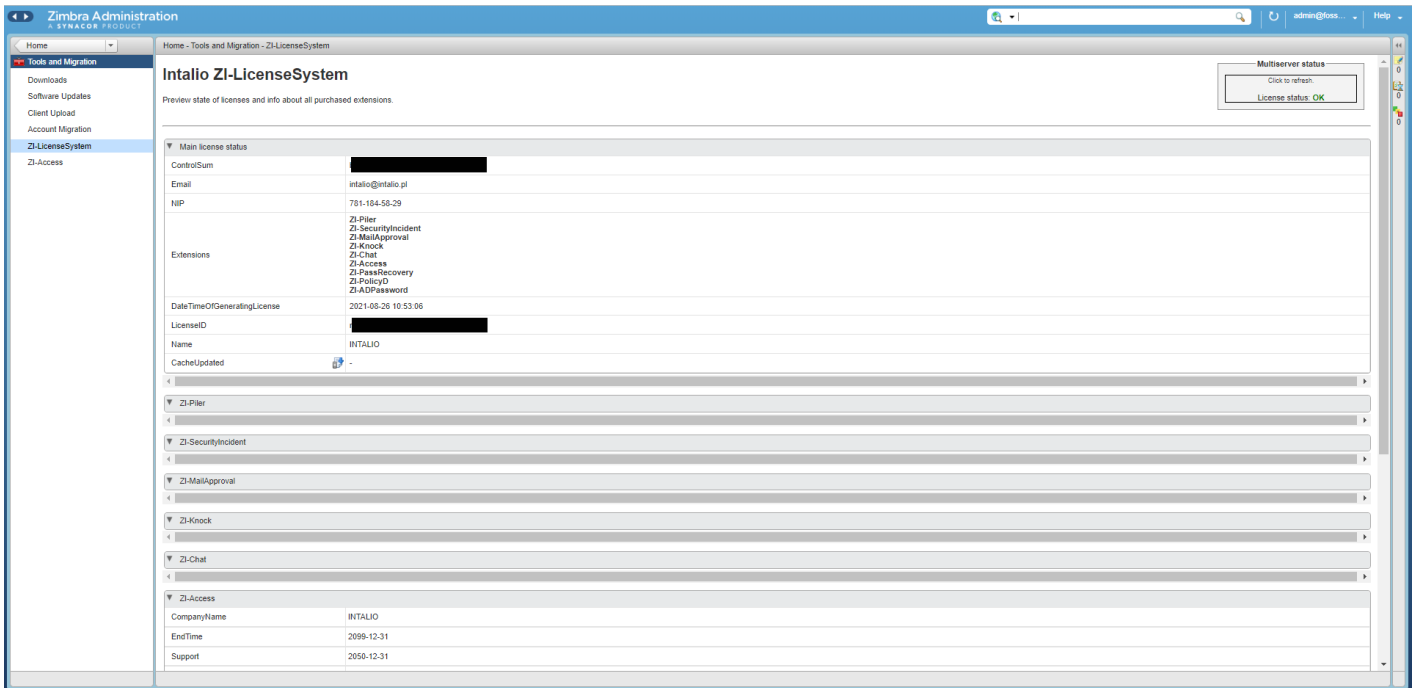
Thanks for activation!
Deleting cache...
Cache deleted

##### INFO #####
After license reactivation there's no need to restart zimbra
##### INFO #####

Restart zimbra? (Y/n or exit):
```

After the mailboxd restart, zimlet should be installed. To check it, log in to the Administration Console of your ZCS Server and navigate to Tools and Migration > ZI-LicenseSystem where you can find details about granted licenses or Tools and Migration > ZI-Access where you can configure your zimlet.





## reCAPTCHA (only in v2.x)

To be able to use the reCaptcha feature you have to **manually copy** the whole content of the helpers/reCaptcha\_patch.html file to the /opt/zimbra/jetty/webapps/zimbra/public/login.jsp file **right before** the

```
</body>
</html>
```

tags at the end of it.

After any Zimbra patch installation or Zimbra upgrade it is possible that the `/opt/zimbra/jetty/webapps/zimbra/public/login.jsp` may be overwritten so you have to check that proper reCaptcha script is in there after you finish updating your Zimbra.

# Zimlet configuration

## Overview

To configure the ZI-Access zimlet, please open the Administration Console > Tools and migration > ZI-Access

Home - Tools and Migration - ZI-Access Help Save Close

### Intalio ZI-Access

This tool allows you to limit access to zimbra to selected users or allow specific users to log in from a local or remote IP.

▶ Intalio ZI-LicenseSystem

◀ ▶

▶ Intalio ZI-LicenseSystem Zimlet

◀ ▶

▼ Global config

Re-captcha enabled	<input type="checkbox"/>
Site key <small>Google site key</small>	<input type="text"/>
Secret key <small>Google secret key</small>	<input type="text"/>

◀ ▶

Configuration

Domain: *	<input type="text"/>	X
Status:		
Module activation:	<div>YESNO</div>	
Local IP Defintion: *	<input type="text"/>	
The chosen method of authorization: *	Internal ▼	
Fallback:	<input type="checkbox"/>	
Method:	<div>AllowedNot allowed</div>	
<div>Add COS</div>	Domain not set	
<div>Add account</div>	Domain not set	

◀ ▶

Status

Server	Version	Updated at
--------	---------	------------

◀ ▶

ZI-Access consists of the following display panes:

- Intalio ZI-LicenseSystem - displays license informations

- Intalio ZI-LicenseSystem Zimlet - displays information about licensed zimlets
- Global config - a configuration that is applied for all of the domains for which the ZI-Access module is activated (**Module activation: YES**)
- Configuration - main panel of the zimlet where you set per domain configuration
- Status - here you will see configuration version number (and when it was saved) for the selected domain on each mailbox server (it has to be the same version on all of them for the zimlet to work properly)

# Configuration

The fields on the Configuration Panel have the following meaning:

- **Domain** - type in a domain name that you want ZI-Access to be configured for
- **Status** - indicates wherever ZI-Access is enabled for the domain
- **Modul activation** - choose YES or NO to enable or disable ZI-Access for the selected domain
- **Local IP Definition** - it's a list of IPs in regex form that determine which IPs are considered "local"

For example list: `(10.193.\d{1,3}.\d{1,3})|(10.194.\d{1,3}.\d{1,3})`

means that 10.193.\*.\* **or** 10.194.\*.\* IP addresses will be treated as "local" IPs

Depending on the choosen Method "local" IP addresses from this list will be allowed or not allowed to access

If you only want to use the reCAPTCHA functionality then fill this box with `.*`

- **The chosen method of authorization** - choose method of authorization configured in the domain (*Internal*, *AD* or *LDAP*)
- **Fallback** - enable this option if you have AD or LDAP external authorization and you want to use Fallback to Local
- **Method** - If you select *Allowed* then COSes or accounts that meet the regular expression declared above will be able to log in. If you select *Not allowed* then those specific COSes or accounts meeting the regular expression will not be able to log in.
- **Add COS** - type in a COS name you want to grant access (if Method set to *Allowed*) or block access (if Method set to *Not Allowed*)
- **Add account** - account name you want to grant access (if Method set to *Allowed*) or block access (if Method set to *Not Allowed*)

After filling out the form switch Module activation to YES and then click Save (in the top right corner).

If you use External Authentication (LDAP or Active Directory) you have to **turn off Fallback to Local** on your domains

```
zmprov md contoso.com zimbraAuthFallbackToLocal FALSE
```

and use the **Fallback** checkbox in the ZI-Access settings if you want to.

## reCAPTCHA

Soon

# Necessary Zimbra configuration

## Originating IP

In a multi-server environment, or any environment running a proxy, a mailbox server may only log the IP of the connecting proxy instead of the real client IP.

For example:

```
2022-09-06 15:21:29,972 INFO [qtp192881625-932: //localhost:8080/service/soap/BatchRequest]
[name=admin@foss9lab.int.intalio.pl;oip=172.17.0.147;ua=zclient/9.0.0_GA_4373;soapId=7e375894;]
account - Authentication successful for user: admin@foss9lab.int.intalio.pl
```

**In such case ZI-Access will not work.**

To solve this you have to define the Trusted IPs of your internal nginx proxies, so that the mailstores will instead capture the data on the originating IP from the HTTP traffic. By default, the `zimbraMailTrustedIP` is empty:

```
zmpov gcf zimbraMailTrustedIP
```

By adding your nginx proxy addresses (as seen by the mailstores) to this attribute, it should then log appropriately. For example, if there are two nginx proxies 10.11.12.1 and 10.11.12.2:

```
zmpov mcf +zimbraMailTrustedIP 10.11.12.1 +zimbraMailTrustedIP 10.11.12.2
```

Please note here too, if you are running Nginx on the same node as the mailstore, you will need to add both 127.0.0.1 and the real address of that node:

```
zmpov mcf +zimbraMailTrustedIP 127.0.0.1 +zimbraMailTrustedIP 10.11.12.13
```

Then restart mailboxd

```
zmmailboxdctl restart
```

And check /opt/zimbra/log/mailbox.log to find out that now "oip=" presents the real client IP address

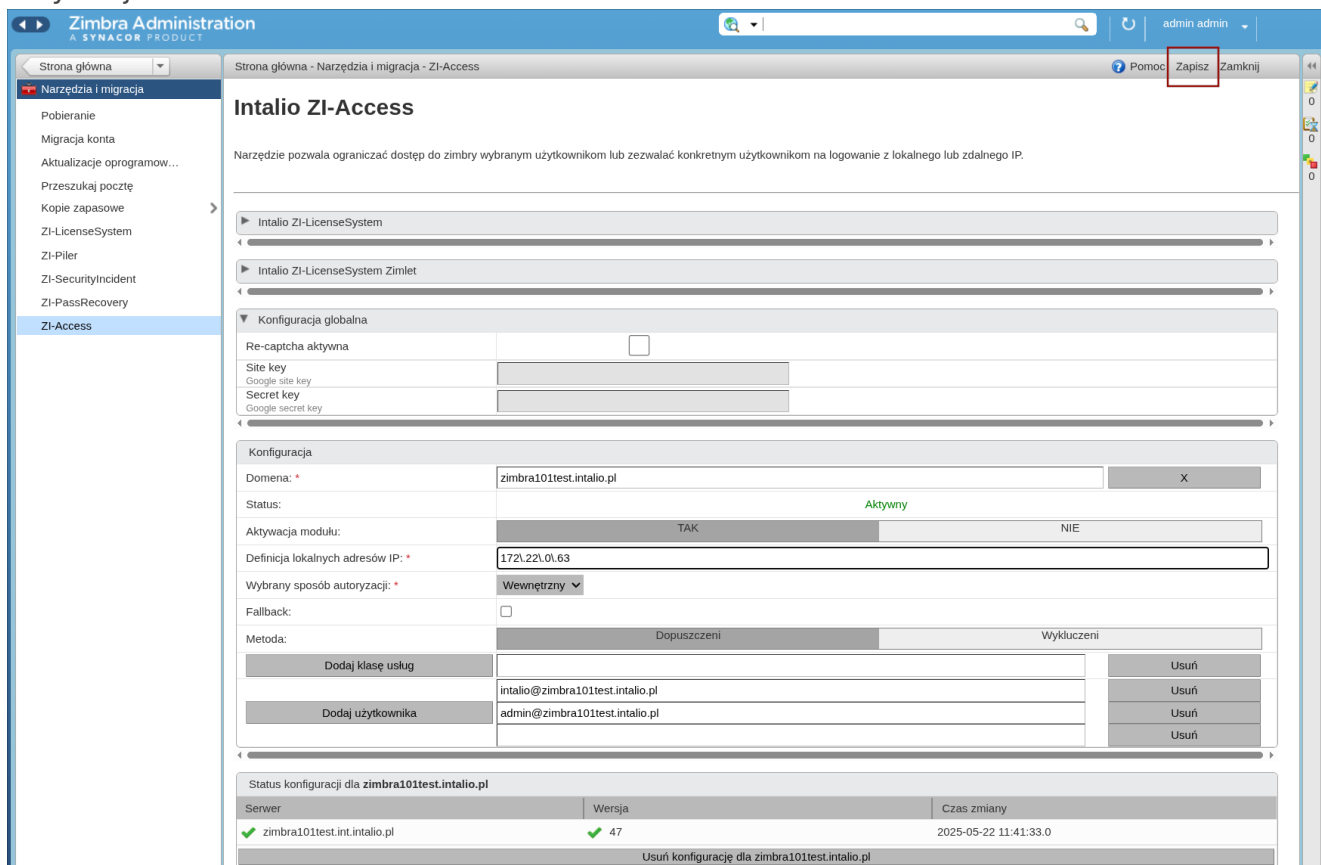
```
2022-09-06 15:56:50,653 INFO [qtp192881625-128: //localhost: 8080/service/soap/BatchRequest]
[name=admin@foss9lab.int.intalio.pl; oip=172.17.0.140; ua=zclient/9.0.0_GA_4373; soapId=6fbb7960; ]
account - Authentication successful for user: admin@foss9lab.int.intalio.pl
```

# Release Notes



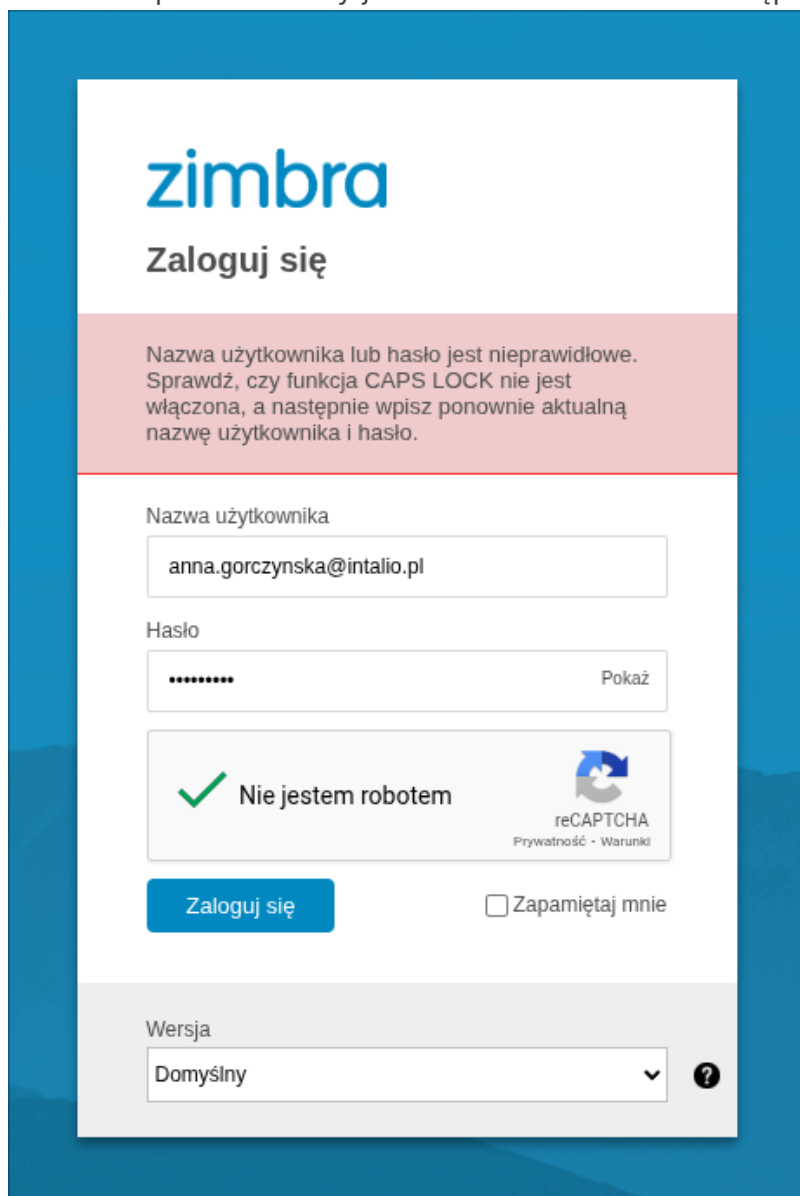
# ZI-Access 2.5

- **Zmieniono sposobu zapisu wprowadzonych zmian.** Od teraz trzeba każdorazowo kliknąć "Zapisz" w prawym górnym rogu. Nie wystarczy jak wcześniej kliknąć "TAK" przy aktywacji zimletu.



- **Zmieniono kolejność mechanizmów autentykacji** w przypadku aktywnego modułu. Od teraz proces autentykacji **rozpoczyna się od weryfikacji, czy adres IP inicjujący logowanie znajduje się na liście dozwolonych** jako lokalne. W przypadku adresu niedozwolonego dalsza weryfikacja nie jest wykonywana, co zapobiega zablokowaniu konta w wyniku wielokrotnych prób logowania z nieprawidłowym hasłem. Autentykacja zostaje

przerwane, a użytkownikowi prezentowany jest komunikat o braku dostępu.



The image shows a Zimbra login interface. At the top, the 'zimbra' logo is displayed in blue. Below it, the heading 'Zaloguj się' (Login) is shown. A red error message box contains the text: 'Nazwa użytkownika lub hasło jest nieprawidłowe. Sprawdź, czy funkcja CAPS LOCK nie jest włączona, a następnie wpisz ponownie aktualną nazwę użytkownika i hasło.' (Username or password is incorrect. Check if the CAPS LOCK function is enabled, and then re-enter the current username and password). Below the error message, there are two input fields: 'Nazwa użytkownika' (Username) with the value 'anna.gorczyńska@intalio.pl' and 'Hasło' (Password) with masked characters '.....'. To the right of the password field is a 'Pokaż' (Show) button. Below the inputs is a reCAPTCHA widget showing a green checkmark and the text 'Nie jestem robotem' (I am not a robot). To the right of the widget is the reCAPTCHA logo and the text 'reCAPTCHA Prywatność - Warunki' (Privacy - Terms). Below the widget is a blue 'Zaloguj się' (Login) button and a checkbox labeled 'Zapamiętaj mnie' (Remember me). At the bottom, there is a 'Wersja' (Version) dropdown menu set to 'Domyślny' (Default) and a help icon (question mark).

- **Dodatkowo poprawiono mechanizm blokowania konta** w przypadku jednoczesnego **aktywowania funkcji reCaptcha** - blokada lub zwiększenie licznika nieudanych logowań następuje wyłącznie po podaniu błędnego hasła wraz z kluczem zdefiniowanym w `whitelist_recaptcha_keys`. Zapobiega to blokowaniu kont przez atakujących, którzy nie

posiadają poprawnego klucza.

The image shows the Zimbra login interface. At the top, the Zimbra logo is displayed. Below it, the text "Zaloguj się" (Log in) is shown. A red error message box contains the text: "Nazwa użytkownika lub hasło jest nieprawidłowe. Sprawdź, czy funkcja CAPS LOCK nie jest włączona, a następnie wpisz ponownie aktualną nazwę użytkownika i hasło." (Username or password is incorrect. Check if the CAPS LOCK function is enabled, and then re-enter the current username and password). Below the error message, there are two input fields: "Nazwa użytkownika" (Username) with the value "anna.gorczyńska@intalio.pl" and "Hasło" (Password) with masked characters. To the right of the password field is a "Pokaż" (Show) link. Below the input fields is a reCAPTCHA widget with the text "Nie jestem robotem" (I am not a robot) and a green checkmark. To the right of the reCAPTCHA widget is a "Zaloguj się" (Log in) button. Below the button is a checkbox labeled "Zapamiętaj mnie" (Remember me). At the bottom, there is a "Wersja" (Version) dropdown menu with the value "Domyślny" (Default) and a help icon.

- **Zaktualizowano angielskie tłumaczenia** komunikatów wyświetlanych w okienkach dialogowych

- **Poprawiono literówkę** w komunikacie o błędzie autentykacji.

- Usunięto problem powodujący błąd "URI too long" po zaakceptowaniu reCaptcha i kliknięciu "Zaloguj" przy jednoczesnym podaniu nieprawidłowego hasła??