

ZI-MailApproval - Installation and Administration Guide

- [Installation](#)
- [Configuration](#)
- [Release Notes](#)
 - [ZI-MailApproval 1.0](#)

Installation

Unpack installer archive file *.tar.gz in /tmp/ (as root):

```
tar xvzf ZI-MailApproval-1.6.tar.gz  
cd ZI-MailApproval-1.6/  
perl ZI-Installer
```

At the beginning required perl packages will be checked and installed if necessary:

```
root@zimbralab-krzysztof:/tmp/ZI-MailApproval-1.6# perl ZI-Installer
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)
ZI-Installer: "installationType" is not specified, use local installation instead
ZI-Installer: "NoDatabase" was set. Database configuration will be ignored
```

Then script will display configuration summary:

```
-----CONFIG-----
DatabaseConfigFormat      -->
DatabaseConfigLocation    -->
help                      -->
installationType          --> local
installConfigPath         -->
InstallDeps               -->
mysqlHost                 -->
mysqlNewDatabaseName      -->
mysqlNewPassword          -->
mysqlNewUser              -->
mysqlPort                 -->
NoActivate                --> 0
NoAsk                     -->
NoDatabase                --> 1
PostinstallCommand        -->
RestartZimbra             -->
SqlFile                   -->
Update                    --> 0
version                   -->
zimbraPath                --> /opt/zimbra
ZimletDirName             --> IntalioZiMailApproval
-----

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

Answer: Y

```
Installation starting.....
Creating zimlet directory...
Removing earlier version....
Earlier versions not found...
Copying Extensions...
Copying language properties...
Copying script libs...
Setting permissions...
Looking for zip files in Zimlets directory...
Found 1 files
Starting deploy....
[] INFO: Deploying Zimlet intalio_zi_mail_approval in LDAP.
[] INFO: Installing Zimlet intalio_zi_mail_approval on this host.
[] INFO: Upgrading Zimlet intalio_zi_mail_approval to 1.6.27
[] INFO: Adding Zimlet intalio_zi_mail_approval to COS default
[] INFO: Enabling Zimlet intalio_zi_mail_approval
Deploy complete
System check dependencies...
  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 (v2.33)
  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)
ZI-LicenseManager - version 1.02
Please enter your login/email: zimbrademo
Enter your password:
```

Enter login and password received with the license.

```
|-----|
|                               | Licenses                               |
|-----+-----+-----+-----+
| Nr | license_number | description |
|-----+-----+-----+-----+
| 1 | 8[REDACTED] | ZI-License for Intalio [REDACTED] |
| 2 | n[REDACTED] | ZI-License for Intalio [REDACTED] |
|-----+-----+-----+-----+
Please choose from 1-2 option or type exit
Your option: 2
```

Choose your license.

```
|-----+-----+-----+-----+-----+-----+-----+-----+
|                               | Extensions in license number: [REDACTED] |
|-----+-----+-----+-----+-----+-----+-----+-----+
| Nr | name | extension_number | start_date | end_date | version | support | user_limit |
|-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | ZI-Access | [REDACTED] | 2019-06-03 | 2099-12-31 | 1.x | 2050-12-31 | 9999 |
| 2 | ZI-MailApproval | [REDACTED] | 2019-06-04 | 2099-12-31 | 1.x | 2050-12-31 | 9999 |
| 3 | ZI-Knock | [REDACTED] | 2020-04-30 | 2023-04-29 | 1.x | 2050-12-31 | 500 |
| 4 | ZI-Chat | [REDACTED] | 2019-06-04 | 2099-12-31 | 2.x | 2050-12-31 | 9999 |
| 5 | ZI-ADPassword | [REDACTED] | 2019-01-01 | 2099-03-03 | 1.x | 2022-03-03 | 2000 |
| 6 | ZI-Piler | [REDACTED] | 2019-03-21 | 2099-12-31 | 2.x | 2050-12-31 | 1000 |
| 7 | ZI-PolicyD | [REDACTED] | 2020-09-08 | 2099-12-31 | 2.x.x | 2050-12-31 | 0 |
| 8 | ZI-SecurityIncident | [REDACTED] | 2020-09-11 | 2099-09-29 | 1.x | 2099-09-11 | 100000 |
| 9 | ZI-PassRecovery | [REDACTED] | 2021-07-08 | 2099-12-31 | 1.x | 2022-07-07 | 9999 |
|-----+-----+-----+-----+-----+-----+-----+-----+
Proceed?
(Y/n or exit): y
```

Choose: Y

```
Downloading license...
Saving license.....
Saving complete!
Activating Main License - version 1.0.11.10...
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
Activate ZI-Piler - version 2.9.1....
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
Activate ZI-MailApproval - version 1.6.1....
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
Activate ZI-PassRecovery - version 1.5.1....
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): y
```

Choose: Y

If You answer Y, the zimbra mailbox will be restarted

```
Stopping mailboxd...done.
Starting mailboxd...done.
Done

Clear temporary files...
```

After the mailbox restart, zimlet should be installed. To check it, login into the Panel Admin in Your ZCS Server and see Panel Administrator > Migration and tool > ZI-License. There should be

information about granted licenses.

In case of the **multi server** instalation, zimlet must be installed on **each mailbox**.

Remeber to restart all mailboxes (as zimbra):

```
zmmailboxdctl restart
```


Configuration

Zimlet configuration

Main configuration is done through the config file available under

```
/opt/zimbra/lib/ext/IntalioZiMailApproval/approvalMap.json
```

ResponsibleGroups - Groups of accounts accepting or declining e-mails.

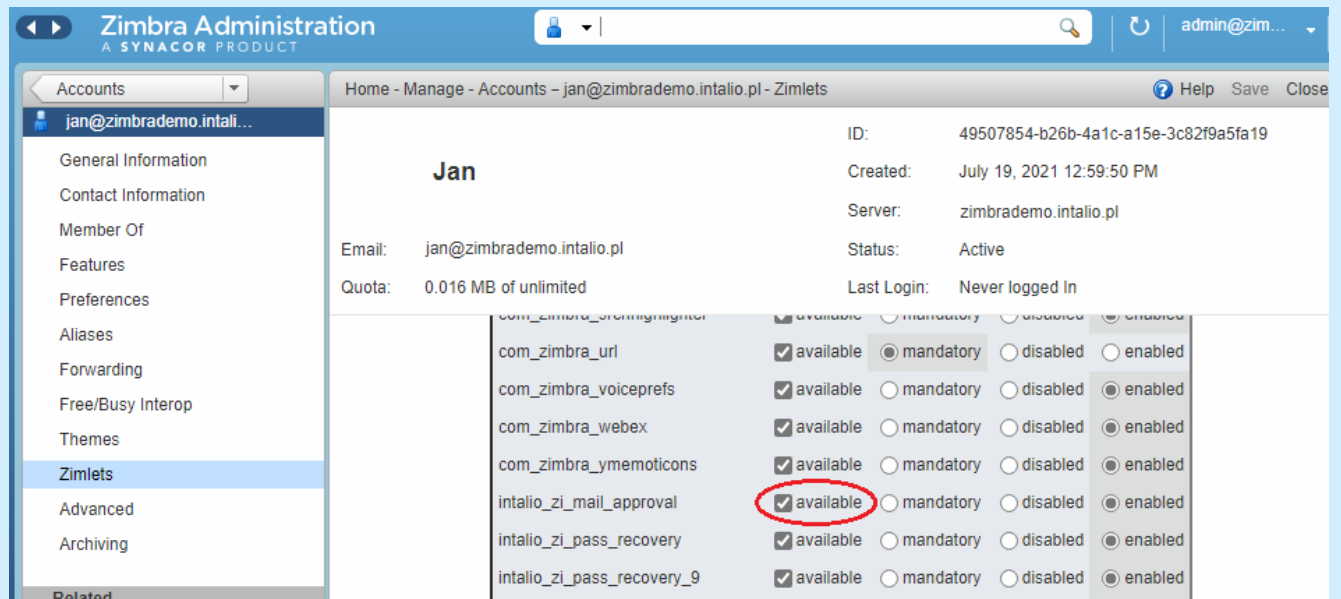
IrresponsibleGroups - Groups of accounts whose e-mails have to be accepted or declined.

Map - Defines who can accept whose e-mails.

In the following example `jan@zimbrademo.intalio.pl` can review `robert@zimbrademo.intalio.pl` mails when he doesn't have an influence on `test@zimbrademo.intalio.pl` account's mails.

```
{  
  "ResponsibleGroups": {  
    "Admins1": [  
      "jan@zimbrademo.intalio.pl"  
    ],  
    "Admins2": [  
      "admin@zimbrademo.intalio.pl"  
    ]  
  },  
  "IrresponsibleGroups": {  
    "RegularEmployees": [  
      "robert@zimbrademo.intalio.pl"  
    ],  
    "Trainees": [  
      "test@zimbrademo.intalio.pl",  
      "test2@zimbrademo.intalio.pl"  
    ]  
  },  
  "Map": {  
    "Admins1": [  
      "RegularEmployees"  
    ],  
    "Admins2": [  
      "Trainees"  
    ]  
  }  
}
```

Mail reviewers have to have also zimlet availability set on in the Zimbra Administration Console.



CBPolicyd configuration

ZI-MailApproval requires installed, enabled and configured CBPolicyd service.

Pre-requisites

Enable the Access Control attribute in Zimbra and restart services.

```
su - zimbra
zmpov ms `zmhostname` zimbraCBPolicydAccessControlEnabled TRUE
zmmactl restart
zmcbspolicyctl start
```

Group

1. In PolicyD Web interface, Go to **Policies -> Groups**.
2. Click on **Action** dropdown -> Add.

3. Specify Name for example *GrupaZiIntalioMailApproval*. Click **Submit**.

GrupaZiIntalioMailApproval group should be created successfully.

The screenshot shows the 'PolicyD Web Administration' interface. On the left is a sidebar with links: Home, Policies (Main, Groups), Access Control (Configure), and HELO/EHLO Checks (Configure, Blacklist, Whitelist). The main content area is titled 'Add Policy Group'. It contains a form with a 'Name' field filled with 'GrupaZiIntalioMailApproval' and an empty 'Comment' text area. A 'Prześlij' (Submit) button is at the bottom left of the form. A 'Back to groups' link is at the top left of the main area.

4. Go to **Policies -> Groups** and select *GrupaZiIntalioMailApproval* and from Action dropdown select **Members**.

The screenshot shows the 'Policy Groups' section of the 'PolicyD Web Administration' interface. It features a table with columns: Name, Action, and Disabled. The 'GrupaZiIntalioMailApproval' group is selected with a radio button. An 'Action' dropdown menu is open, showing options: Add, Change, Delete, and Members. The 'Disabled' column shows 'no' for all groups.

Name	Action	Disabled
<input checked="" type="radio"/> GrupaZiIntalioMailApproval	select action	no
<input type="radio"/> internal_domains	select action	no
<input type="radio"/> internal_ips	select action	no

5. On the page, from Action dropdown select **Add**
6. In *Member* textbox, specify one of the users you want to assign to ZI-MailApproval functionality. Here *test@zimbrademo.intalio.pl* was used as an example. Then click **Submit**.

The screenshot shows the 'Add Policy Group Member' form in the 'PolicyD Web Administration' interface. The sidebar is the same as in previous screenshots. The main content area has a title 'Add Policy Group Member'. It contains a form with a 'Member' field (with a user icon) filled with 'test@zimbrademo.intalio.pl' and an empty 'Comment' text area. A 'Prześlij' (Submit) button is at the bottom left. 'Back to groups' and 'Back to members' links are at the top left of the main area.

7. At the top of the page, click on **Back to members**. Select the above created member *test@zimbrademo.intalio.pl*. From Action dropdown select **Change**.
8. For **Disabled**, select **No** from the dropdown. Click **Submit**.

PolicyD Web Administration

Home

Policies

- > Main
- > Groups

Access Control

- > Configure

HELO/EHLO Checks

- > Configure
- > Blacklist
- > Whitelist

SPF Checks

- > Configure

[Back to groups](#) [Back to members](#)

Update Policy Group Member

	Old Value	New Value
Member	test@zimbrademo.intalio.pl	<input type="text"/>
Comment	<div style="height: 40px;"></div>	<div style="height: 40px;"></div>
Disabled	no	<div style="border: 1px solid black; padding: 2px; display: inline-block;"> -- </div> <div style="border: 1px solid black; padding: 2px; display: inline-block; margin-top: 2px;"> P No Yes </div>

9. Go to **Policies -> Groups** and select *GrupaZiIntalioMailApproval*. From Action dropdown select **Change**.
10. For **Disabled**, select **No** from the dropdown. Click **Submit**

PolicyD Web Administration

Home

Policies

- > Main
- > Groups

Access Control

- > Configure

HELO/EHLO Checks

- > Configure
- > Blacklist
- > Whitelist

[Back to groups](#)

Update Policy Group

	Old Value	New Value
Name	GrupaZiIntalioMailApproval	<input type="text"/>
Disabled	no	<div style="border: 1px solid black; padding: 2px; display: inline-block;"> -- </div> <div style="border: 1px solid black; padding: 2px; display: inline-block; margin-top: 2px;"> -- No Yes </div>

11. The *GrupaZiIntalioMailApproval* group is now enabled.

Policy

1. Go to **Policies -> Main**.
2. Click on **Action** dropdown -> Add.
3. Specify Name for example *ZiIntalioMailApproval*, Priority 10 and Description *ZiIntalioMailApproval*. Click **Submit**. The policy should be created successfully.

PolicyD Web Administration

[Back to policies](#)

- Home
- Policies**
 - > Main
 - > Groups
- Access Control**
 - > Configure
- HELO/EHLO Checks**
 - > Configure
 - > Blacklist
 - > Whitelist
- SPF Checks**
 - > Configure
- Greylisting**
 - > Configure
 - > Whitelist

Add Policy

Name

Priority

Description

4. Go to **Policies -> Main** and select *ZiIntalioMailApproval*. From Action dropdown select **Members**.
5. On the page, from Action dropdown select **Add**.
6. In **Source** textbox, specify *%GrupaZiIntalioMailApproval* and in **Destination** textbox, specify *any*. Click **Submit**.

PolicyD Web Administration

[Back to policies](#) [Back to members](#)

- Home
- Policies**
 - > Main
 - > Groups
- Access Control**
 - > Configure
- HELO/EHLO Checks**
 - > Configure
 - > Blacklist
 - > Whitelist
- SPF Checks**
 - > Configure
- Greylisting**
 - > Configure

Add Policy Member

Source

Destination

Comment

7. At the top of the page, click on **Back to members**. Select the above created member. From Action dropdown select **Change**.
8. For **Disabled**, select **No** from the dropdown. Click **Submit**.
9. Go to **Policies -> Main** and select *ZiIntalioMailApproval*. From Action dropdown select **Change**.
10. For **Disabled**, select **No** from the dropdown. Click **Submit**.
11. The *ZiIntalioMailApproval* policy is now enabled.

Access Control

1. Go to **Access Control -> Configure**.
2. Click on **Action** dropdown -> Add.
3. In **Name** textbox, specify *ControlZiIntalioMailApproval*.
4. In **Link to policy** dropdown, select policy *ZiIntalioMailApproval*
5. In **Verdict** dropdown, select *Hold*.

The screenshot displays the 'PolicyD Web Administration' interface. On the left is a navigation menu with the following items: Home, Policies (with sub-items Main and Groups), Access Control (with sub-item Configure), HELO/EHLO Checks (with sub-items Configure, Blacklist, and Whitelist), SPF Checks (with sub-item Configure), and Greylisting (with sub-items Configure and Whitelist). The main content area is titled 'Add Access Control' and contains a form with the following fields: 'Name' (text input with value 'ControlZiIntalioMailApproval'), 'Link to policy' (dropdown menu with value 'ZiIntalioMailApproval'), 'Verdict' (dropdown menu with value 'Hold'), 'Data' (text input with value 'Mail hold'), and 'Comment' (text area). A 'Prześlij' (Submit) button is located at the bottom left of the form. A 'Back to access cntrl' link is visible at the top left of the main content area.

6. Click **Submit**. The Access Control list should be created successfully.
7. Go to **Access Control -> Configure** and select *ZiIntalioMailApproval*
8. From Action dropdown select **Change**.
9. For **Disabled**, select **No** from the dropdown. Click **Submit**

Release Notes

ZI-MailApproval 1.0

[29.09.2023] Wersja 1.8

Nowości

- Dodano możliwość zmiany hasła lokalnego. Jeżeli autoryzacja ma włączony fallback - po nieudanej zmianie hasła w AD, system zmieni hasło lokalne (funkcja działa zarówno z panelu użytkownika, `zmprov setPassword` oraz panelu admina).
-

[22.08.2023] Wersja 1.7

Nowości

- Przygotowanie modułu pod Z10.
-

[16.08.2022] Wersja 1.7

Nowości

- Przygotowanie modułu pod JRE 17.
-

[09.03.2021] Wersja 1.6

Nowości

- Wydanie wersji dla Zimbry 9 - kompatybilnej z Zimbrą 8
-

[03.06.2020] Wersja 1.5

Nowości

- Dodanie nowego CI.
-

[02.04.2020] Wersja 1.5

Nowości

- Dodanie weryfikacji portu SSL podczas sprawdzania licencji.
-

[31.03.2020] Wersja 1.5

Nowości

- Dodanie obsługi nowej wersji serwera licencji ($\geq 1.0.6$), zmiana sposobu odpytywania o licencje (mniejsze zużycie zasobów).
-

[03.03.2020] Wersja 1.4

Nowości

- Dodanie katalogu głównego do instalatorów.
-

[03.03.2020] Wersja 1.4

Nowości

- Dodanie obfuskacji kodu.
-

[07.01.2020] Wersja 1.3

Nowości

- Aktualizacja flagi wymagania zmiany hasła po poprawnym zalogowaniu (jeżeli użytkownik spróbował zalogować się do systemu, ale AD zwróciło potrzebę zmiany hasła to flaga wymaganej zmiany hasła pozostawała niezmieniona)
-

[02.01.2020] Wersja 1.3

Nowości

- Dostosowanie kodu do java13 + Zimbry 8.8.15, porzucenie wsparcia dla Javy starszej niż 13
-

[24.04.2019] Wersja 1.2

Nowości

- Dodanie zamykania sesji po autoryzacji (W przypadku samby)
-

[15.04.2019] Wersja 1.1

Nowości

- LicenseSystem - dodanie kompatybilnej weryfikacji licencji dla Zimbry > 8.8.11
-

[15.04.2019] Wersja 1.1

Nowości

- Ustawienie poprawnego scope.