

# 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.

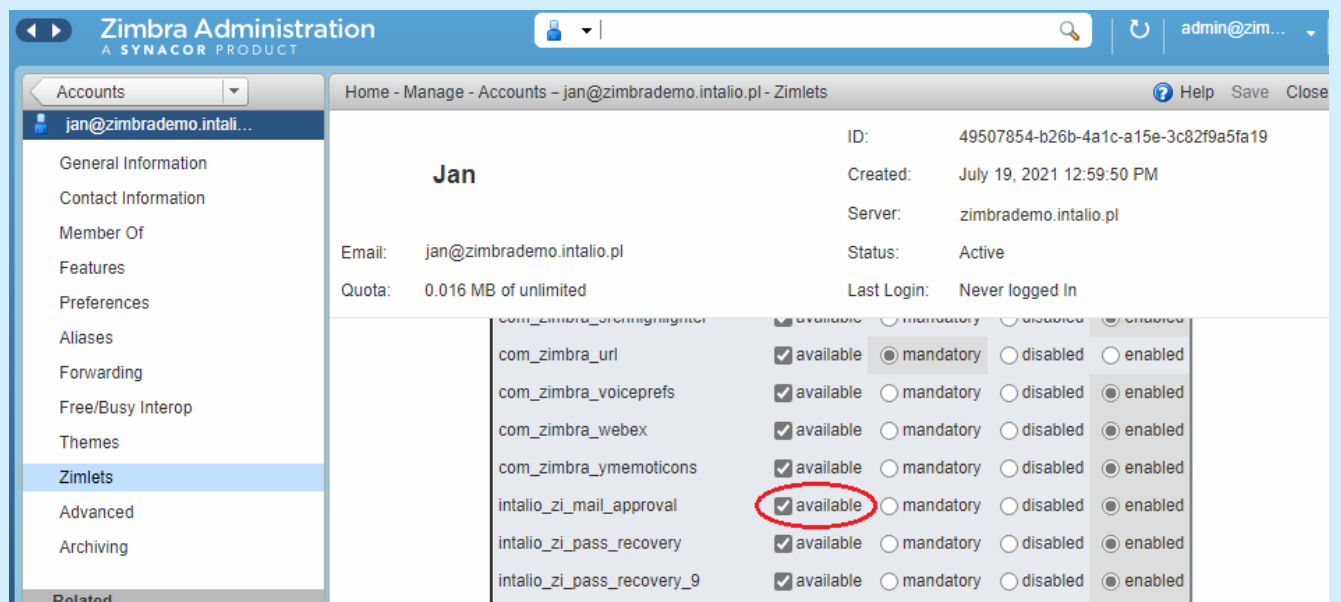
**IrresponsibleGroups** - Groups of accounts whose e-mails have to be accepted or declined.

**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
zmprov ms `zmhostname` zimbraCBPolicydAccessControlEnabled TRUE
zmmactl restart
zmcbpolicydctl 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 navigation 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. Below the form is a 'Prześlij' (Submit) button. A 'Back to groups' link is located at the top left of the main content area.

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

The screenshot shows the 'PolicyD Web Administration' interface. The sidebar is the same as in the previous screenshot. The main content area is titled 'Policy Groups'. It features a table with columns for 'Name', 'Action', and 'Disabled'. The 'Action' column has a dropdown menu open, showing options: 'Add', 'Change', 'Delete', and 'Members'. The table lists three groups: 'GrupaZiIntalioMailApproval' (selected with a radio button), 'internal\_domains', and 'internal\_ips'. The 'Disabled' column has a 'no' value for each group. A 'Back to groups' link is at the top left of the main content area.

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 'PolicyD Web Administration' interface. The sidebar is the same. The main content area is titled 'Add Policy Group Member'. It contains a form with a 'Member' field filled with 'test@zimbrademo.intalio.pl' and an empty 'Comment' text area. Below the form is a 'Prześlij' (Submit) button. At the top of the main content area, there are two links: 'Back to groups' and 'Back to members'.

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

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

Home

Policies
 > Main
 > Groups

Access Control
 > Configure

HELO/EHLO Checks
 > Configure
 > Blacklist
 > Whitelist

SPF Checks
 > Configure

Update Policy Group Member

|          | Old Value                  | New Value            |
|----------|----------------------------|----------------------|
| Member   | test@zimbrademo.intalio.pl | <input type="text"/> |
| Comment  |                            | <div></div>          |
| Disabled | no                         | -- ▾                 |

-- ▾

No

Yes

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

PolicyD Web Administration

[Back to groups](#)

Home

Policies
 > Main
 > Groups

Access Control
 > Configure

HELO/EHLO Checks
 > Configure
 > Blacklist
 > Whitelist

Update Policy Group

|          | Old Value                  | New Value            |
|----------|----------------------------|----------------------|
| Name     | GrupaZiIntalioMailApproval | <input type="text"/> |
| Disabled | no                         | -- ▾                 |

Prześlij

-- ▾

No

Yes

- The *GrupaZiIntalioMailApproval* group is now enabled.

## Policy

- Go to **Policies -> Main**.
- Click on **Action** dropdown -> Add.
- 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*.

## PolicyD Web Administration

[Back to access cntrl](#)

Home

Policies

- > Main
- > Groups

Access Control

- > Configure

HELO/EHLO Checks

- > Configure
- > Blacklist
- > Whitelist

SPF Checks

- > Configure

Greylisting

- > Configure
- > Whitelist

Add Access Control

Name

ControlZiIntalioMailApproval

Link to policy

ZiIntalioMailApproval ▼

Verdict ?

Hold ▼

Data ?

Mail hold

Comment

Prześlij

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**

Revision #10

Created Wed, Sep 1, 2021 12:12 PM by [Admin](#)

Updated Thu, Sep 2, 2021 10:12 AM by [Admin](#)