

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.

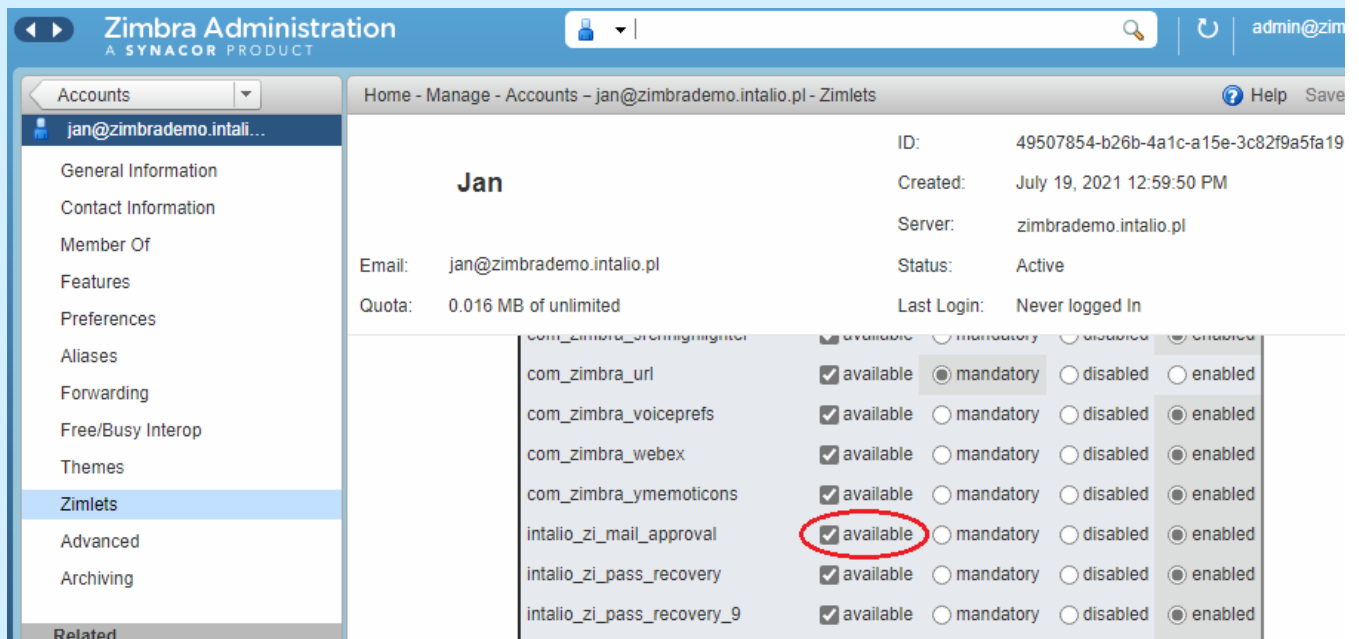
IrresponsibleGroups - Groups of accounts whose e-mails have to be accepted or declined.

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.



The screenshot shows the Zimbra Administration Console interface. On the left is a sidebar with a menu including 'Accounts', 'General Information', 'Contact Information', 'Member Of', 'Features', 'Preferences', 'Aliases', 'Forwarding', 'Free/Busy Interop', 'Themes', 'Zimlets' (highlighted), 'Advanced', and 'Archiving'. The main content area is titled 'Home - Manage - Accounts - jan@zimbrademo.intalio.pl - Zimlets'. It displays account details for 'Jan': ID: 49507854-b26b-4a1c-a15e-3c82f9a5fa19, Created: July 19, 2021 12:59:50 PM, Server: zimbrademo.intalio.pl, Status: Active, Last Login: Never logged in, Email: jan@zimbrademo.intalio.pl, and Quota: 0.016 MB of unlimited. Below this is a table of zimlets with columns for the zimlet name and its status (available, mandatory, disabled, enabled). The 'intalio_zi_mail_approval' row has its 'available' checkbox checked and circled in red.

Zimlet Name	available	mandatory	disabled	enabled
com_zimbra_oremhighlighter	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
com_zimbra_url	<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
com_zimbra_voiceprefs	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
com_zimbra_webex	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
com_zimbra_ymemoticons	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
intalio_zi_mail_approval	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
intalio_zi_pass_recovery	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
intalio_zi_pass_recovery_9	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

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
zmcbspolicydctl 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.

PolicyD Web Administration

[Back to groups](#)

Add Policy Group

Name:

Comment:

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

PolicyD Web Administration

Policy Groups

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

Action:

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**.

PolicyD Web Administration

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

Add Policy Group Member

Member:

Comment:

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="background-color: #eee; height: 40px;"></div>	<div style="border: 1px solid #ccc; height: 40px;"></div>
Disabled	no	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;"> -- </div> <div style="border: 1px solid #ccc; padding: 2px; display: inline-block; margin-top: 2px;"> -- 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 #ccc; padding: 2px; display: inline-block;"> -- </div> <div style="border: 1px solid #ccc; 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

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

[Back to policies](#)

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

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

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

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

Home

Policies

- > Main
- > Groups

Access Control

- > Configure

HELO/EHLO Checks

- > Configure
- > Blacklist
- > Whitelist

SPF Checks

- > Configure

Greylisting

- > Configure
- > Whitelist

[Back to access cntrl](#)

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 1 September 2021 12:12:11 by Admin

Updated 2 September 2021 10:12:19 by Admin