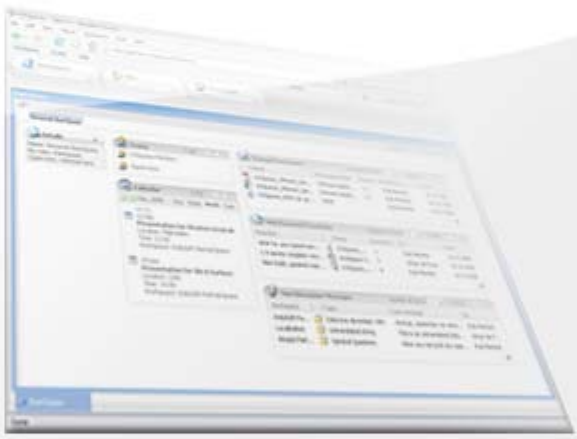
O3Spaces Zarafa plug-in Installation Readme

www.o3spaces.com
info@o3spaces.com



O3Spaces Zarafa plug-in

version 1.0

Installation Readme

Notice:

- **Before installing and using the O3Spaces Software read the '*O3Spaces Workplace End User License Agreement*', as enclosed in the Zarafa plug-in download carefully.**
- **By activating the O3Spaces Software you agree to the terms and conditions as contained in this agreement.**

Table of Contents

1. Technical prerequisites....4
1.1 Software prerequisites....4
1.2 Deployment prerequisites....4
2. Getting Started....5
2.1 Installing the Zarafa plug-in....5
2.1.1 Authentication strategy declaration....5
2.1.2 Workplace location declaration....7
2.2 Security - Trusted connection....7
2.2.1 Create a Workplace – Zarafa trust....7
2.3 First time configuration E-mail archiving....8
3. Contact O3Spaces....9
4. Disclaimer....9

1. Technical prerequisites

1.1 Software prerequisites

The O3Spaces Workplace Zarafa (version 1.0) integration requires the following software (versions) to be available:

- Zarafa Webaccess with plug-in system (6.30 or above)
- Enterprise Edition of O3Spaces Workplace 2.4.1 or newer
- PHP 5.X (Standard part of Ubuntu) and PEAR module HTTP_REQUEST

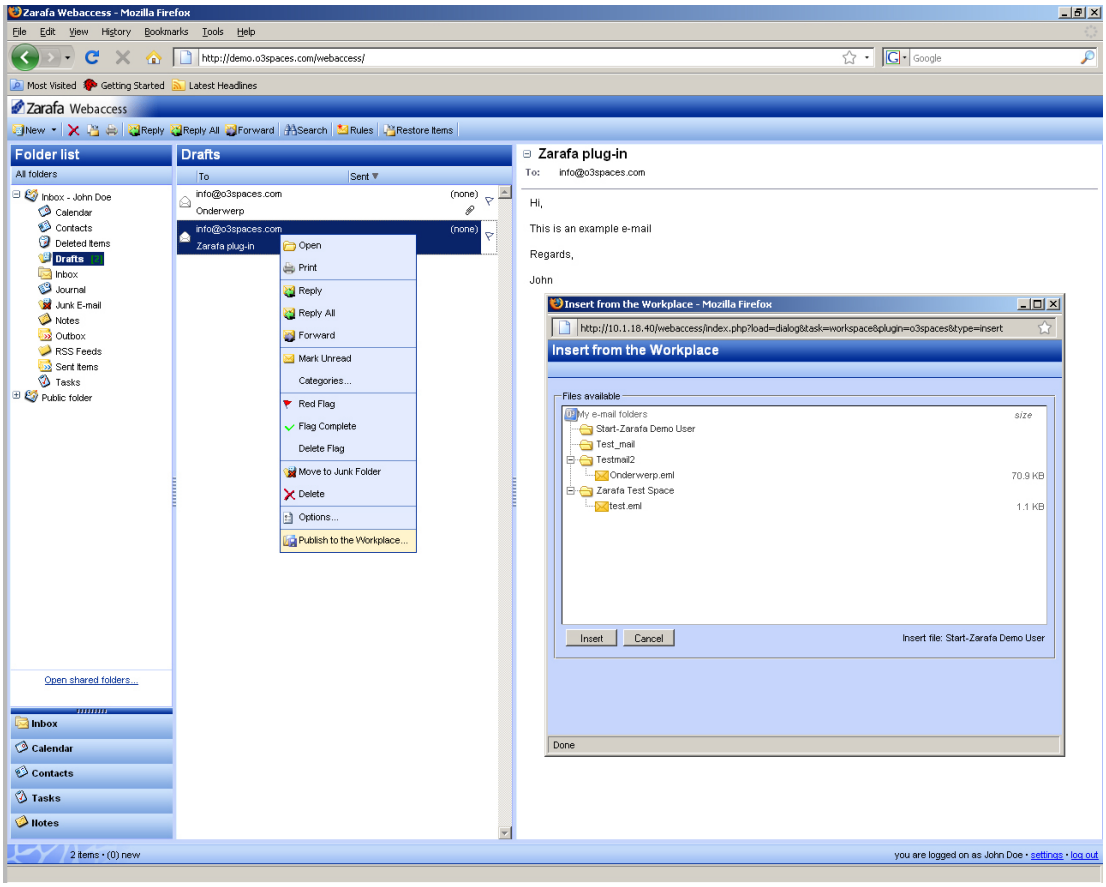


figure 1: The Zarafa plug-in

1.2 Deployment prerequisites

The O3Spaces Workplace Zarafa integration requires that both O3Spaces Workplace and Zarafa use a single user base. This implies that both solutions address the same LDAP-directory service.

2. Getting Started

The integration of O3Spaces Workplace is provided by a Zarafa plug-in. This Zarafa plug-in consists of a zip file of the plug-in folder containing all the documents needed for the plug-in. Install instructions for the plug-in are given in this section.

2.1 Installing the Zarafa plug-in

To start the installation unzip the zip file. Copy the unzipped folder, o3spaces, to the plug-in folder of your Zarafa installation (probably /var/www/webaccess/plugins/). Use for instance a SSH client and/or SCP client to copy the files. Afterwards the plug-in should be configured properly. This configuration can be done in the deployment.config.php file found in the o3spaces plug-in folder (probably /var/www/webaccess/plugins/o3spaces).

The configuration of the plug-in exists of two steps:

1. Declaration of the authentication strategy in the deployment.config.php. Trust-based authentication and basic authentication are the types of authentication that are available.
2. Declaration of the Workplace location in the deployment.config.php

More information about these steps is given in the next sections.

2.1.1 Authentication strategy declaration

Trust-based authentication

To use the trust-based authentication it is important to declare the right authentication strategy (**'auth.strategy'**) in the deployment.config.php. In case of the Trust-based authentication declare the 'TrustAuthStrategy' and 'remove' the 'BasicAuthStrategy'. An example is given in the box below.

```
    // Trust-based authentication strategy
    //
    "auth.strategy"   => "TrustAuthStrategy",
…….
 // Alternative authentication: based on username / password
    // In this case the current username/password is taken over from the webserver
    // The username and password will be automatically set by Zarafa after user login
    //
//"auth.strategy" => "BasicAuthStrategy",
```

To be able to declare the trust-based authentication in the deployment.config.php, a Workplace-Zarafa trust needs to be created. A description of the needed steps is given in section 2.2. The resulting Workplace-Zarafa trust can be used to change the deployment.config.php. The box below gives an example of the trust configuration section of the deployment file. In the example replace the **IP address zarafa webaccess}" => "{trust secret}"** part with the IP address of the zarafa webaccess and the trust 'secret' code obtained from the OSGI console of the Workplace (see section 2.2).

```
 * Section: Trust configuration
…...
$trusts = array(
        // Server IP-address
       "{IP address zarafa webaccess}" => "{trust secret}",
);
```

Basic authentication

Another option is to use basic authentication. Logically the Basic authentication requires a Basic authentication strategy declaration in the deployment file. The 'BasicAuthStrategy' should be declared and the TrustAuthStrategy' should be 'removed'. An example is given in the box below.

```
        // Trust-based authentication strategy
        //
    //"auth.strategy"    => "TrustAuthStrategy",
…....
  // Alternative authentication: based on username / password
        // In this case the current username/password is taken over from the webserver
        // The username and password will be automatically set by Zarafa after user login
        //
"auth.strategy" => "BasicAuthStrategy",
```

In case of Basic authentication the authentication is based on an username-password combination, requires that both O3Spaces Workplace and Zarafa use a single user base. With a shared user base declaration of the Basic authentication is sufficient if the zarafa settings are as shown in the box below:

```
    /*************************************************************
     * Section: Zarafa settings
     *************************************************************/
    "zarafa.override.user" => true, //always has to be set to true if you want to use the zarafa user
    "zarafa.override.pass" => true, // only has effect when BasicAuthStrategy is in place
```

2.1.2 Workplace location declaration

The workplace location is also declared in the deployment.config.php. In general only the location of the workplace is needed. SSL connections are also a possibility. Below an example is given of the workplace location declaration.

```
/*************************************************************
     * Section: Workplace General settings
     *************************************************************/

    // Location of the workplace, with ssl enabled or not
    "workplace.use_ssl" => false,
    "workplace.location" => "{workplaceIP}",

    "store.tmp_dir" => TMP_PATH . "/"
```

Note: After changing the deployment.config.php make sure that there are no 'Enters'on the last line.

2.2 Security - Trusted connection

A trusted connection must be configured to integrate external systems with Workplace. A specific set of IP-addresses is allowed to perform a Workplace user related actions.

A trusted network can be configured in the Workplace using the Studio OSGi Command Line Shell. A command named 'trust' is created for this purpose. Executing 'trust help' will show the usage of this command.

The available OSGi commands are:

- trust create x.x.x.x
  creates an IP-trust for the provided IP-address
- trust list
  lists all configured trusts (trusted IP-addresses)
- trust delete x.x.x.x
  deletes the IP-trust for the provided IP-address
- trust get x.x.x.x
  shows the trust ('secret') generated for a specific IP-address

2.2.1 Create a Workplace – Zarafa trust

In the Workplace Studio you'll find the Workplace OSGi console under: Tools > OSGi Command Line Shell

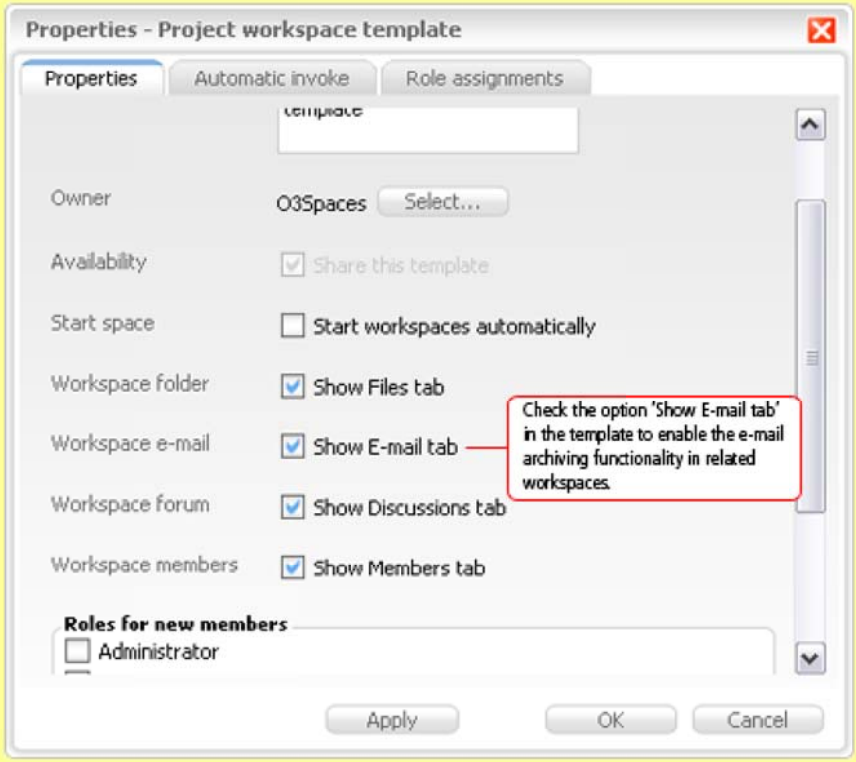
1. Create a Workplace server trust for the IP-address on which your Zarafa server is running, using the OSGi command: 'trust create x.x.x.x'
2. Retrieve the trust 'secret' for the trusted IP-address, using the OSGi command: 'trust get x.x.x.x'
3. In the plug-in deployment file enter the Workplace trust 'secret' you obtained in step 2.

2.3 First time configuration E-mail archiving

To use the (e-mail archiving features (E-mail tab, Zarafa plug-in, E-mail content search) some configuration is required in:

1. **The workspace template settings**
   To define which workspace(s) will have an e-mail tab.
2. **The e-mail tab properties of individual workspaces**
   To define which workspace-folder must be visible in the e-mail tab.

Tip: The visibility of the e-mail tab in workspaces will be defined by its related workspace-template.



In all existing and in all new workspace-templates the 'Show E-mail tab' option will not be checked by default.
To use the e-mail archiving features this option has to be checked in the workspace-template properties.

Tip: Before e-mail message can be displayed in a workspace e-mail tab, a specific workspace folder has to be defined first.

The workspace folder to be visible in the e-mail tab can be selected in the e-mail tab properties.
After defining a folder the available e-mail messages will be indexed. This can take some time.

2.4 Known issues

Zarafa Webaccess should be configured to handle plug-ins. To check this open the config.php file in the webaccess root folder and search for the part of the config file that is given below:

```
// Define the path to the plugin directory (No slash at the end)
define("PATH_PLUGIN_DIR", "{yourpluginsdir}");
// Define the path to the plugin directory
define("ENABLE_PLUGINS", true);
// Define list of disabled plugins separated by semicolon, o3spaces should not be listed here
define("DISABLED_PLUGINS_LIST", '');
```

Check for the following:

1. The plugin system has to be enables, this can be done in the 'ENABLE_PLUGINS' part.
2. The plug-in directory has to be set correctly in the 'PATH_PLUGIN_DIR' part.
3. The o3spaces plug-in should not be listed in the 'DISABLED_PLUGINS_LIST'.

If you are using Suse, it could be that the location of HTTP/Request.php is not set properly in the config.php of Zarafa.and you get the following error:

```
'msg' => 'require_once(HTTP/Request.php): failed to open stream: No such file or directory',
'file' => '/srv/www/htdocs/webaccess/plugins/o3spaces/include/O3Spaces/HTTP/WP_HTTP_Request.php:3',
```

In that case add the right path to the config/php, probably /usr/share/php5/PEAR.

3. Contact O3Spaces

O3Spaces B.V.
Hanzeweg 12d
2803 MC, Gouda
the Netherlands
+31 182 680 269
info@o3spaces.com
www.o3spaces.com

4. Disclaimer

All product names, logos, brands and any other trademarks contained in this documents and the associated software are the property of the respective owners.