OX App Suite Public Sector Plugins Technical Documentation for
7.10.6-rev2

2022-07-14

Copyright notice

Contents

1 General Information

1.1 Warnings

⚠️ **Warning**
It is mandatory to restart the **open-xchange** service on all middleware nodes after performing the update.

⚠️ **Warning**
When updating only custom packages, it may be necessary to invalidate the browser cache to make the changes visible. An invalidation of the cache will be done automatically when updating OX core UI packages at the same time, but not if you are updating only custom UI plug-ins. In the latter case, please call the following command on all Apache nodes with the same value for <timestamp> :

```
/opt/open-xchange/sbin/touch-appsuite --timestamp=<timestamp>
```

⚠️ **Warning**
UI packages with themes need to generate CSS after installation. This will be done automatically when the service is restarted but if you wish to not perform a service restart, you must call the following command on each node:

```
/opt/open-xchange/appsuite/share/update-themes.sh
```

⚠️ **Warning**
Custom configuration or template files are potentially not updated automatically. After the update, please always check for files with a **.dpkg-new** or **.rpmnew** suffix and merge the changes manually. Configuration file changes are listed in their own respective section below but don't include changes to template files. For details about all the configuration files and templates shipped as part of this delivery, please read the relevant section of each package.

1.2 Delivery Comment

This delivery was requested with following comment:

Public Sector 7.10.6 Feature Delivery

1.3 Install Package Repository

This delivery is part of a restricted software repository:

https://software.open-xchange.com/components/public-sector/stable/7.10.6/DebianBuster
https://software.open-xchange.com/components/public-sector/stable/7.10.6/DebianStretch
https://software.open-xchange.com/components/public-sector/stable/7.10.6/DebianBullseye
https://software.open-xchange.com/components/public-sector/stable/7.10.6/RHEL7

1.4 Build Dependencies

This delivery was build and tested with following dependencies:

```
AppSuite:node-10,frontend-7.10.6-rev12,backend-7.10.6-rev16
```

1.5 Notice

ℹ️ **Info**
Some configurations can be changed without restarting the service, please call following command for getting a list of supported settings.

```
/opt/open-xchange/sbin/listreloadables
```

Please use following command to enable capable and changed configurations on a running system.

```
/opt/open-xchange/sbin/reloadconfiguration
```

2   Token Exchange Mailauth Provider for secondary/functional accounts

Bundle Identifier	`com.openexchange.mailauth.impersonate`
Package(s)	`open-xchange-mailauth-impersonate`
Required capabilities	`none`, enabled by configuration
Available since	7.10.6-rev1

The token Exchange Mailauth allows secondary accounts to use `access_tokens` for access. Those `access_tokens` are exchanged using a so called `token_exchange` that is currently a loose implementation only supported by keycloak#token_exchange.

The plugin is able to request either an `access_token` or an `access_token` and `refresh_token`. As this is only a request, the keycloak server can decide to only return an `access_token`, even though both are requested.

Logouts are supported with the keycloak#post-logout handling. Only enabled, when following setting is configured:

```
1   com.openexchange.mailauth.impersonate.tokenLogoutEndpoint
```

It will only work for `refresh_tokens`, as `access_tokens` are not supported by keycloak for logout.

If no user `access_tokens` are present or the users should not be allowed to impersonate, an admin can be configured which will be kept active in a dedicated cache. This admin will use its `access_tokens` to call the `token_exchange` for the requested users.

2.1   Configuration

`/opt/open-xchange/etc/mailauth-impersonator.properties`

```
1    # Enable or disable the functional mail account handling via token_exchange impersonation
2    # Default: false
3    com.openexchange.mailauth.impersonate.enabled=false
4
5    # The clientId to access the token endpoint to get the impersonation token via
         token_exchange
6    # Must be configured if feature is enabled
7    #com.openexchange.mailauth.impersonate.clientId=
8
9    # The clientSecret to access the token endpoint to get the impersonation token via
         token_exchange
10   # Must be configured if feature is enabled
11   #com.openexchange.mailauth.impersonate.clientSecret=
12
13   # Supported authTypes:
14   #    login
15   #    xoauth2
16   #    oauthbearer
17   #
18   # Default: oauthbearer
19   #com.openexchange.mailauth.impersonate.authType=
20
21   # The token type to request for the token_exchange
```

```
22  # Allowed values are
23  #   access_token - will request an access token
24  #   refresh_token - will request an access and refresh_token
25  #   ignore - will not add the requested_token_type and let the server decide
26  #
27  # Default: refresh_token
28  #com.openexchange.mailauth.impersonate.tokenType=
29
30  # In case the login to imap should be changed, this setting will search in the provided
        accessToken for a given claim
31  # If not set or empty, the configured login value for the account login or transportLogin
        will be used
32  # Will also be ignored in case the claim set does not contain the configured claim.
33  #
34  # Default: <not-set>
35  #com.openexchange.mailauth.impersonate.accessTokenLoginClaim=
36
37  # In case the access token from the user is not allowed to impersonate other users, it is
        possible to enable an admin auth
38  #
39  # Default: false
40  #com.openexchange.mailauth.impersonate.admin.enabled=
41
42  # Admin user name if admin.enabled is configured
43  #com.openexchange.mailauth.impersonate.admin.username=
44
45  # Admin password if admin.enabled is configured
46  #com.openexchange.mailauth.impersonate.admin.password=
47
48  # The tokenEndpoint to request new access tokens for the token_exchange as well as refresh
        and access tokens for the admin, if admin.enabled is configured
49  # Must be configured
50  #
51  # Default:<not-set>
52  #com.openexchange.mailauth.impersonate.tokenEndpoint=
53
54  # Optional logout endpoint in case the admin user should be logged out after the default
        timeout of 1 hour
55  # If empty or not set, the revocation will not occur
56  #com.openexchange.mailauth.impersonate.tokenLogoutEndpoint=
57
58  # Time to live for refresh tokens, also accounts for access_tokens that are provided in
        the same request
59  # All values are allowed, however a minimum of 1 hour should be configured as otherwise
        access_tokens may
60  # also timeout earlier than their configured minimum time
61  #
62  # Can contain units of measurement: D(=days) W(=weeks) H(=hours) M(=minutes), S(=seconds),
        MS(=milliseconds)
63  # If no identifier is given, MS is assumed
64  # Default: 1H
65  #com.openexchange.mailauth.impersonate.refreshTtl=1H
```

3   Shipped Version

3.1   Package open-xchange-appsuite-public-sector

UI customizations for the public sector
Version: 7.10.6-2
Type: OX Frontend Plugin with Themes
Depends on:

```
open-xchange-appsuite (<<7.10.7)
open-xchange-appsuite (>=7.10.6)
open-xchange-appsuite-manifest (<<7.10.7)
open-xchange-appsuite-manifest (>=7.10.6)
```

3.1.1 Installation

Install on OX middleware nodes with package installer **apt-get** or **yum**:

```
<package installer> install open-xchange-appsuite-public-sector
```

Install on Apache nodes with package installer **apt-get** or **yum**:

```
<package installer> install open-xchange-appsuite-public-sector-static
```

3.1.2 Configuration

For details, please see appendix A
/opt/open-xchange/etc/settings/public-sector.properties (page 6)

3.2 Package open-xchange-mailauth-impersonate

This package provides a MailAuthenticator for secondary Mailboxes which uses token_exchange to get tokens
Version: 7.10.6-2
Type: OX Middleware Plugin
Depends on:

```
open-xchange-core (<<7.10.7)
open-xchange-core (>=7.10.6)
```

3.2.1 Installation

Install on OX middleware nodes with package installer **apt-get** or **yum**:

```
<package installer> install open-xchange-mailauth-impersonate
```

3.2.2 Configuration

For details, please see appendix A
/opt/open-xchange/etc/mailauth-impersonator.properties (page 7)

3.3 Package open-xchange-matrixproxy

Open-Xchange Matrix Bot Proxy
Version: 7.10.6-2
Type: OX Middleware Plugin
Depends on:

```
open-xchange-core (<<7.10.7)
open-xchange-core (>=7.10.6)
```

3.3.1 Installation

Install on OX middleware nodes with package installer **apt-get** or **yum**:

```
<package installer> install open-xchange-matrixproxy
```

3.3.2 Configuration

For details, please see appendix A
/opt/open-xchange/etc/matrix-proxy-servlet.properties (page 7)

A   Configuration Files

File 1   /opt/open-xchange/etc/settings/public-sector.properties

```
1   # Category identifier for OX App Suite
2   io.ox.public-sector//navigation/oxtabname=tab_groupware
3
4   # URL of the InterCom Service.
5   # Defaults to the same host as the OX App Suite UI.
6   io.ox.public-sector//ics/url=
7
8   # Remove quick launchers
9   io.ox/core//apps/quickLaunchCount=0
10
11  # Set Phoenix theme
12  io.ox/core//theme=phoenix
```

File 2   /opt/open-xchange/etc/mailauth-impersonator.properties

```
1   # Enable or disable the functional mail account handling via token_exchange impersonation
2   # Default: false
3   com.openexchange.mailauth.impersonate.enabled=false
4
5   # The clientId to access the token endpoint to get the impersonation token via
        token_exchange
6   # Must be configured if feature is enabled
7   #com.openexchange.mailauth.impersonate.clientId=
8
9   # The clientSecret to access the token endpoint to get the impersonation token via
        token_exchange
10  # Must be configured if feature is enabled
11  #com.openexchange.mailauth.impersonate.clientSecret=
12
13  # Supported authTypes:
14  #   login
15  #   xoauth2
16  #   oauthbearer
17  #
18  # Default: oauthbearer
19  #com.openexchange.mailauth.impersonate.authType=
20
21  # The token type to request for the token_exchange
22  # Allowed values are
23  #   access_token - will request an access token
24  #   refresh_token - will request an access and refresh_token
25  #   ignore - will not add the requested_token_type and let the server decide
26  #
27  # Default: refresh_token
28  #com.openexchange.mailauth.impersonate.tokenType=
29
30  # In case the login to imap should be changed, this setting will search in the provided
        accessToken for a given claim
31  # If not set or empty, the configured login value for the account login or transportLogin
        will be used
32  # Will also be ignored in case the claim set does not contain the configured claim.
33  #
34  # Default: <not-set>
35  #com.openexchange.mailauth.impersonate.accessTokenLoginClaim=
36
37  # In case the access token from the user is not allowed to impersonate other users, it is
        possible to enable an admin auth
38  #
39  # Default: false
40  #com.openexchange.mailauth.impersonate.admin.enabled=
41
42  # Admin user name if admin.enabled is configured
43  #com.openexchange.mailauth.impersonate.admin.username=
```

```
44
45    # Admin password if admin.enabled is configured
46    #com.openexchange.mailauth.impersonate.admin.password=
47
48    # The tokenEndpoint to request new access tokens for the token_exchange as well as refresh
           and access tokens for the admin, if admin.enabled is configured
49    # Must be configured
50    #
51    # Default:<not-set>
52    #com.openexchange.mailauth.impersonate.tokenEndpoint=
53
54    # Optional logout endpoint in case the admin user should be logged out after the default
           timeout of 1 hour
55    # If empty or not set, the revocation will not occur
56    #com.openexchange.mailauth.impersonate.tokenLogoutEndpoint=
57
58    # Time to live for refresh tokens, also accounts for access_tokens that are provided in
           the same request
59    # All values are allowed, however a minimum of 1 hour should be configured as otherwise
           access_tokens may
60    # also timeout earlier than their configured minimum time
61    #
62    # Can contain units of measurement: D(=days) W(=weeks) H(=hours) M(=minutes), S(=seconds),
           MS(=milliseconds)
63    # If no identifier is given, MS is assumed
64    # Default: 1H
65    #com.openexchange.mailauth.impersonate.refreshTtl=1H
```

File 3 /opt/open-xchange/etc/matrix-proxy-servlet.properties

```
1     # URL of the Matrix server
2     #
3     com.openexchange.matrixproxy.servlet.serverUrl=https://matrix.dpx-wp7a.at-univention.de
4
5     # URL of the Bot Server
6     #
7     com.openexchange.matrixproxy.servlet.botURL=https://meetings-widget-api.dpx-wp7a.at-
           univention.de
8
9     # Application Service Token to login to Matrix server
10    #
11    com.openexchange.matrixproxy.servlet.asToken=
12
13    # Comma separated list of path to pass-through to the Bot server
14    # Every path that doesn't start with any of them listed here will be
15    # rejected.
16    com.openexchange.matrixproxy.servlet.apiWhitelist=/v1/meeting,/v1/health
```