OX App Suite Public Sector Plugins Technical Documentation for 7.10.6

2021-12-10

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
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/RHEL7

1.4 Build Dependencies

This delivery was build and tested with following dependencies:

```
backend-7.10.6-rev4
```

1.5 Notice

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:

```
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

```
# Enable or disable the functional mail account handling via token_exchange impersonation
# Default: false
com.openexchange.mailauth.impersonate.enabled=false

# The clientId to access the token endpoint to get the impersonation token via token_exchange
# Must be configured if feature is enabled
#com.openexchange.mailauth.impersonate.clientId=

# The clientSecret to access the token endpoint to get the impersonation token via token_exchange
# Must be configured if feature is enabled
#com.openexchange.mailauth.impersonate.clientSecret=

# Supported authTypes:
#   login
#   xoauth2
#   oauthbearer
#
# Default: oauthbearer
#com.openexchange.mailauth.impersonate.authType=

# The token type to request for the token_exchange
# Allowed values are
#   access_token - will request an access token
#   refresh_token - will request an access and refresh_token
#   ignore - will not add the requested_token_type and let the server decide
#
# Default: refresh_token
#com.openexchange.mailauth.impersonate.tokenType=

# In case the login to imap should be changed, this setting will search in the provided accessToken for a given claim
# If not set or empty, the configured login value for the account login or transportLogin will be used
# Will also be ignored in case the claim set does not contain the configured claim.
#
# Default: <not-set>
#com.openexchange.mailauth.impersonate.accessTokenLoginClaim=

# In case the access token from the user is not allowed to impersonate other users, it is possible to enable an admin auth
#
# Default: false
```

```
#com.openexchange.mailauth.impersonate.admin.enabled=

# Admin user name if admin.enabled is configured
#com.openexchange.mailauth.impersonate.admin.username=

# Admin password if admin.enabled is configured
#com.openexchange.mailauth.impersonate.admin.password=

# 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
# Must be configured
#
# Default:<not-set>
#com.openexchange.mailauth.impersonate.tokenEndpoint=

# Optional logout endpoint in case the admin user should be logged out after the default
    timeout of 1 hour
# If empty or not set, the revocation will not occur
#com.openexchange.mailauth.impersonate.tokenLogoutEndpoint=

# Time to live for refresh tokens, also accounts for access_tokens that are provided in
    the same request
# All values are allowed, however a minimum of 1 hour should be configured as otherwise
    access_tokens may
# also timeout earlier than their configured minimum time
#
# Can contain units of measurement: D(=days) W(=weeks) H(=hours) M(=minutes), S(=seconds),
     MS(=milliseconds)
# If no identifier is given, MS is assumed
# Default: 1H
#com.openexchange.mailauth.impersonate.refreshTtl=1H
```

3 Shipped Packages and Version

3.1 Package open-xchange-mailauth-impersonate

This package provides a MailAuthenticator for secondary Mailboxes which uses token_exchange to get tokens
Version: 7.10.6-1
Type: OX Middleware Plugin
Depends on:

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

3.1.1 Installation

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

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

3.1.2 Configuration

For details, please see appendix A
/opt/open-xchange/etc/mailauth-impersonator.properties (page 6)

A Configuration Files

File 1 /opt/open-xchange/etc/mailauth-impersonator.properties

```
# Enable or disable the functional mail account handling via token_exchange impersonation
```

```
# Default: false
com.openexchange.mailauth.impersonate.enabled=false

# The clientId to access the token endpoint to get the impersonation token via token_exchange
# Must be configured if feature is enabled
#com.openexchange.mailauth.impersonate.clientId=

# The clientSecret to access the token endpoint to get the impersonation token via token_exchange
# Must be configured if feature is enabled
#com.openexchange.mailauth.impersonate.clientSecret=

# Supported authTypes:
#   login
#   xoauth2
#   oauthbearer
#
# Default: oauthbearer
#com.openexchange.mailauth.impersonate.authType=

# The token type to request for the token_exchange
# Allowed values are
#   access_token - will request an access token
#   refresh_token - will request an access and refresh_token
#   ignore - will not add the requested_token_type and let the server decide
#
# Default: refresh_token
#com.openexchange.mailauth.impersonate.tokenType=

# In case the login to imap should be changed, this setting will search in the provided accessToken for a given claim
# If not set or empty, the configured login value for the account login or transportLogin will be used
# Will also be ignored in case the claim set does not contain the configured claim.
#
# Default: <not-set>
#com.openexchange.mailauth.impersonate.accessTokenLoginClaim=

# In case the access token from the user is not allowed to impersonate other users, it is possible to enable an admin auth
#
# Default: false
#com.openexchange.mailauth.impersonate.admin.enabled=

# Admin user name if admin.enabled is configured
#com.openexchange.mailauth.impersonate.admin.username=

# Admin password if admin.enabled is configured
#com.openexchange.mailauth.impersonate.admin.password=

# 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
# Must be configured
#
# Default:<not-set>
#com.openexchange.mailauth.impersonate.tokenEndpoint=

# Optional logout endpoint in case the admin user should be logged out after the default timeout of 1 hour
# If empty or not set, the revocation will not occur
#com.openexchange.mailauth.impersonate.tokenLogoutEndpoint=

# Time to live for refresh tokens, also accounts for access_tokens that are provided in the same request
# All values are allowed, however a minimum of 1 hour should be configured as otherwise access_tokens may
# also timeout earlier than their configured minimum time
#
# Can contain units of measurement: D(=days) W(=weeks) H(=hours) M(=minutes), S(=seconds), MS(=milliseconds)
# If no identifier is given, MS is assumed
```

```
64  # Default: 1H
65  #com.openexchange.mailauth.impersonate.refreshTtl=1H
```