OX App Suite Univention Plugins Technical Documentation for 7.10.6

2021-12-15

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:

Univention 7.10.6 Maintenance Delivery

1.3 Install Package Repository

This delivery is part of a restricted software repository:

https://software.open-xchange.com/components/univention/stable/7.10.6/DebianBuster
https://software.open-xchange.com/components/univention/stable/7.10.6/DebianStretch
https://software.open-xchange.com/components/univention/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-rev3,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 Univention OpenID Connect handler

Package(s)	`open-xchange-authentication-ucs`, `open-xchange-authentication-ucs-common`
Required capabilities	none, please see **Configuration** section for further information
Available since	`6.20.4`

The Authentication Service for Univention uses the default ldap backend to to the user lookups.

2.1 Configuration

The auth handling has been extracted to a custom package named `open-xchange-authentication-ucs-common` which takes care of the actual LDAP lookup. The same connector is also used inside the SAML and OIDC component.

Properties inside `authplugin.properties`:

```
# Switch to enable or disable the UCSAuthenticaitonService
#   Might be required when OIDC is active and
#   com.openexchange.oidc.enablePasswordGrant = true
#   is configured
#
# Default: true
com.openexchange.authentication.ucs.auth.enabled=true

# use ldap pooling
com.openexchange.authentication.ucs.useLdapPool=false

# basedn of ldap directory
com.openexchange.authentication.ucs.baseDn=dc=example,dc=org

# ldap url; use ldaps:// for ssl
com.openexchange.authentication.ucs.ldapUrl=ldap://localhost

# specify attribute containing email address from which domain part will be used to
# identify context
com.openexchange.authentication.ucs.mailAttribute=mailPrimaryAddress

# ldap attribute containing the OX Login name
com.openexchange.authentication.ucs.loginAttribute=uid

# specify name of attribute containing contextId in order to lookup context
# this is optional; if not specified, context lookup will be done using domain name as
    found
# in com.openexchange.authentication.ucs.mailAttribute
com.openexchange.authentication.ucs.contextIdAttribute=

# search query to find the user within ldap
# %s will be replaced by the login as entered in the ox login mask
com.openexchange.authentication.ucs.searchFilter=(&(objectClass=oxUserObject)(|(uid=%s)(
    mailPrimaryAddress=%s)))

# where to redirect users that need to change their password when it is expired
com.openexchange.authentication.ucs.passwordChangeURL=

# optionally specify dn to be used to bind to ldap server instead of doing anonymous
    access
com.openexchange.authentication.ucs.bindDn=

# password for specified binddn
com.openexchange.authentication.ucs.bindPassword=
```

3 Univention OpenID Connect handler

Package(s)	`open-xchange-oidc-ucs`
Required capabilities	none, please see **Configuration** section for further information
Available since	`7.10.4`

The OpenID Connect handler for Univention uses the default ldap backend to to the user lookups. In addition the connector is able to perform a userinfo lookup instead of relying on the IdToken.

3.1 Configuration

The OpenID Connect handler uses the core framework which is also explained on documentation.open-xchange.com - middleware - OpenID in detail. Available config options are also explained on documentation.open-xchange.com - middleware configuration - OpenID.

In addition to the default config options, the following additional options are available:

Property	Default Value	Option
`com.openexchange.oidc.ucs.enabled`	false	enables the oidc backend for univention
`com.openexchange.oidc.ucs.userInfoEndpoint`	""	if configured, uses the userInfoEndpoint instead of relying on the IdToken claims

When the `com.openexchange.oidc.ucs.userInfoEndpoint` is configured, the userLookupClaim will search inside the response from the userInfoEndpoint instead of the IdToken.

3.2 OAUTH access for mail

When OIDC is running, it is also possible to enable `oauthbearer` for imap access. By default OIDC is only relevant for the UI. To mitigate this problem there is a switch to enable an AuthenticationService via `com.openexchange.oidc.enablePasswordGrant = true`. This additional AuthenticationService can cause issues with the AuthenticationService provided by `open-xchange-authentication-ucs`. As a workaround, an additional property is present to disable the start of the `open-xchange-authentication-ucs` with `com.openexchange.authentication.ucs.auth.enabled=false`.

When the package `open-xchange-authentication-ucs` is not installed, the following property is not required:

```
1 com.openexchange.authentication.ucs.auth.enabled=false
```

4 Univention SAML handler

Package(s)	`open-xchange-oidc-saml`
Required capabilities	none, please see **Configuration** section for further information
Available since	`7.10.1`

The SAML handler for Univention uses the default ldap backend to to the user lookups.

4.1 Configuration

The SAML handler uses the core framework which is explained in following documentation: documentation.open-xchange.com - middleware - SAML 2.0 SSO

Available config options are also explained on documentation.open-xchange.com - middleware configuration - SAML.

In addition to the default config options, the following additional options are available:

Property	Default Value	Option
`com.openexchange.saml.ucs.enabled`	false	If UCS SAML should be enabled or disabled

Property	Default Value	Option
com.openexchange.saml.ucs.id	""	The id inside the saml authnResponse which holds the userinformation
com.openexchange.saml.ucs.logoutRedirectUrl	""	URL of where the users are redirected after logout
com.openexchange.saml.ucs.failureRedirect	""	The URL to redirect to in case the SAML back-end fails to look up the authenticated user. When left empty or not set, an HTTP 500 error page is sent instead.
com.openexchange.saml.ucs.logoutFailureRedirect	""	The URL to redirect to in case the SAML back-end has an error, when the user logs out. When left empty or not set, the value of com.openexchange.saml.ucs.failure.redirect is used.
com.openexchange.saml.ucs.keyStore	""	The full path to a Java keyStore containing the IdPs certificate.
com.openexchange.saml.ucs.keyStorePass	""	Password to open the keyStore.
com.openexchange.saml.ucs.certAlias	""	The alias of the IdP certificate entry within the keyStore.
com.openexchange.saml.ucs.signingKeyAlias	""	The alias of the signingKey entry within the keyStore.
com.openexchange.saml.ucs.signingKeyPassword	""	The password of the signingKey entry within the keyStore.
com.openexchange.saml.ucs.decryptionKeyAlias	""	The alias of the decryptionKey entry within the keyStore.
com.openexchange.saml.ucs.decryptionKeyPassword	""	The password of the decryptionKey entry within the keystore.

5 Shipped Packages and Version

5.1 Package open-xchange-authentication-ucs

Module for authenticating users on a Univention Corporate Server installation This package installs the OSGi bundle implementing the OSGi AuthenticationService for the backend. The implementation uses Univention Corporate Server to authenticate login requests. This authentication module is mutually exclusive with any other authentication module. Only one authentication module can be installed on the backend.
Version: 7.10.6-2
Type: OX Middleware Plugin
Depends on:

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

Conflicts with:

```
open-xchange-authentication-database
open-xchange-authentication-imap
open-xchange-authentication-ldap
```

5.1.1 Installation

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

```
<package installer> install open-xchange-authentication-ucs
```

5.2 Package open-xchange-authentication-ucs-common

Common Module for authenticating users on a Univention Corporate Server installation This package installs the OSGi bundle implementing the common helper service that uses Univention Corporate Server to authenticate login requests.
Version: 7.10.6-2
Type: OX Middleware Plugin
Depends on:

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

5.2.1 Installation

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

```
<package installer> install open-xchange-authentication-ucs-common
```

5.2.2 Configuration

For details, please see appendix A
/opt/open-xchange/etc/authplugin.properties (page 8)

5.3 Package open-xchange-oidc-ucs

Module for authenticating users on a Univention Corporate Server installation via OIDC This package installs the OSGi bundle implementing the OSGi OIDCBackend for the backend. The implementation uses Univention Corporate Server to authenticate login requests.
Version: 7.10.6-2
Type: OX Middleware Plugin
Depends on:

```
open-xchange-authentication-ucs-common (<<7.10.7)
open-xchange-authentication-ucs-common (>=7.10.6)
open-xchange-core (<<7.10.7)
open-xchange-core (>=7.10.6)
open-xchange-oidc (<<7.10.7)
open-xchange-oidc (>=7.10.6)
```

5.3.1 Installation

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

```
<package installer> install open-xchange-oidc-ucs
```

5.4 Package open-xchange-saml-ucs

Module for authenticating users on a Univention Corporate Server installation via SAML This package installs the OSGi bundle implementing the OSGi SamlBackend for the backend. The implementation uses Univention Corporate Server to authenticate login requests.
Version: 7.10.6-2
Type: OX Middleware Plugin
Depends on:

```
open-xchange-authentication-ucs-common (<<7.10.7)
open-xchange-authentication-ucs-common (>=7.10.6)
open-xchange-core (<<7.10.7)
open-xchange-core (>=7.10.6)
open-xchange-saml-core (<<7.10.7)
open-xchange-saml-core (>=7.10.6)
```

5.4.1 Installation

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

```
<package installer> install open-xchange-saml-ucs
```

A Configuration Files

File 1 /opt/open-xchange/etc/authplugin.properties

```
# Switch to enable or disable the UCSAuthenticaitonService
#   Might be required when OIDC is active and
#   com.openexchange.oidc.enablePasswordGrant = true
#   is configured
#
# Default: true
com.openexchange.authentication.ucs.auth.enabled=true

# use ldap pooling
com.openexchange.authentication.ucs.useLdapPool=false

# basedn of ldap directory
com.openexchange.authentication.ucs.baseDn=dc=example,dc=org

# ldap url; use ldaps:// for ssl
com.openexchange.authentication.ucs.ldapUrl=ldap://localhost

# specify attribute containing email address from which domain part will be used to
# identify context
com.openexchange.authentication.ucs.mailAttribute=mailPrimaryAddress

# ldap attribute containing the OX Login name
com.openexchange.authentication.ucs.loginAttribute=uid

# specify name of attribute containing contextId in order to lookup context
# this is optional; if not specified, context lookup will be done using domain name as
    found
# in com.openexchange.authentication.ucs.mailAttribute
com.openexchange.authentication.ucs.contextIdAttribute=

# search query to find the user within ldap
# %s will be replaced by the login as entered in the ox login mask
com.openexchange.authentication.ucs.searchFilter=(&(objectClass=oxUserObject)(|(uid=%s)(
    mailPrimaryAddress=%s)))

# where to redirect users that need to change their password when it is expired
com.openexchange.authentication.ucs.passwordChangeURL=

# optionally specify dn to be used to bind to ldap server instead of doing anonymous
    access
```

```
38  com.openexchange.authentication.ucs.bindDn=
39
40  # password for specified binddn
41  com.openexchange.authentication.ucs.bindPassword=
```