OX Cloud Plugins Technical Documentation for 1.11.4

2021-05-19

Copyright notice

©2021 by OX Software GmbH. All rights reserved. Open-Xchange and the Open-Xchange logo are trademarks or registered trademarks of OX Software GmbH. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without 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
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.

Warning
Since Cloud Plugins 1.6.0, the Cassandra functionality has been moved to OX Middleware. This requires manual changes of configuration files because the following settings needs to be changed accordingly:

/opt/open-xchange/etc/cloudplugins-cassandra.properties:

```
com.openexchange.cloudplugins.cassandraHost (1)
com.openexchange.cloudplugins.cassandraPort (2)
```

to */opt/open-xchange/etc/cassandra.properties*:

```
com.openexchange.nosql.cassandra.clusterContactPoints (1)
com.openexchange.nosql.cassandra.port (2)
```

Please see OX Cassandra documentation for a full set of options.

Warning
Since Cloud Plugins 1.6.4, we removed the packaging epoch mechanism which will prevent an automatic update of open-xchange-oxaas packages from 1.6.3. If your environment contain 1.6.3 open-xchange-oxaas packages, please enforce the update to 1.6.4 or later manually.

1.2 Delivery Comment

This delivery was requested with following comment:

> *Cloud Plugins 1.11.4 Feature Delivery for Core 7.10.4 and 7.10.5*

1.3 Install Package Repository

This delivery is part of a restricted software repository:

https://software.open-xchange.com/components/cloud-plugins/stable/1.11.4/DebianBuster
https://software.open-xchange.com/components/cloud-plugins/stable/1.11.4/DebianStretch
https://software.open-xchange.com/components/cloud-plugins/stable/1.11.4/RHEL7

1.4 Global Configuration

The appendix A also contain recommended changes on global configurations which are shipped with OX products (core) and not part of this delivery.

/opt/open-xchange/etc/as-config.yml (page 29)

1.5 Build Dependencies

This delivery was build and tested with following dependencies:

```
AppSuite:node-10,plugins-1.6.4-rev3,frontend-7.10.5-rev10,
backend-7.10.5-rev10
```

1.6 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 Shipped Packages and Version

2.1 Package open-xchange-cloudplugins-antiphishing-vadesecure-ldap

Implementation of VadeSecure antiphishing for cloudplugins within LDAP
Version: 1.11.4-4
Type: OX Middleware Plugin
Depends on:

```
open-xchange-cloudplugins (<<1.11.5)
open-xchange-cloudplugins (>=1.11.4)
open-xchange-core (<<7.10.6)
open-xchange-core (>=7.10.4)
open-xchange-plugins-antiphishing (<<1.7.0)
open-xchange-plugins-antiphishing (>=1.6.4)
open-xchange-plugins-antiphishing-vadesecure (<<1.7.0)
open-xchange-plugins-antiphishing-vadesecure (>=1.6.4)
```

2.1.1 Installation

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

```
<package installer> install open-xchange-cloudplugins-antiphishing-vadesecure-ldap
```

2.1.2 Configuration

For details, please see appendix A
/opt/open-xchange/etc/cloudplugins-antiphishing-vadesecure-ldap.properties (page 14)

2.2 Package open-xchange-cloudplugins-blackwhitelist-ldap

Implementation of blacklist whitelist for cloudplugins within LDAP
Version: 1.11.4-4
Type: OX Middleware Plugin
Depends on:

```
open-xchange-cloudplugins (<<1.11.5)
open-xchange-cloudplugins (>=1.11.4)
open-xchange-core (<<7.10.6)
open-xchange-core (>=7.10.4)
open-xchange-plugins-blackwhitelist (<<1.7.0)
open-xchange-plugins-blackwhitelist (>=1.6.4)
```

2.2.1 Installation

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

```
<package installer> install open-xchange-cloudplugins-blackwhitelist-ldap
```

2.2.2 Configuration

For details, please see appendix A
/opt/open-xchange/etc/cloudplugins-blackwhitelist-ldap.properties (page 15)

2.3 Package open-xchange-cloudplugins-forwards-ws

Cloudplugins Admin forwards REST API This package provides a restful API to add/update/delete forwards saved in storage.
Version: 1.11.4-4
Type: OX Middleware Plugin
Depends on:

```
open-xchange-cloudplugins (<<1.11.5)
open-xchange-cloudplugins (>=1.11.4)
open-xchange-core (<<7.10.6)
open-xchange-core (>=7.10.4)
```

2.3.1 General Functionality

This plugin provides a middleware restfull API to set mail forwards in the user storage.
List of features implemented by this plugin:

- Main entry point is **/api/oxaas/v1/admin/forwards**
- secured by basic auth mapped to customer login data
- **POST /{contextId}/{alias}** Sets a forward alias
- **PUT /{contextId}/{alias}** Adds recipient to existing forward alias
- **DELETE /{contextId}** Deletes all forward aliases in context
- **DELETE /{contextId}/{alias}** Deletes an alias in a context
- **GET /{contextId}** Returns all forward aliases in a context
- **GET /{contextId}/{alias}** Returns an alias in a context
- **HEAD /{contextId}/{alias}** Checks if an alias in a context is present
- **HEAD /{contextId}/{alias}/{recipient}** Checks, if a recipient of an alias in a context is present

2.3.2 Installation

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

```
<package installer> install open-xchange-cloudplugins-forwards-ws
```

2.3.3 Configuration

For details, please see appendix A
/opt/open-xchange/etc/cloudplugins-forwards.properties (page 15)

2.4 Package open-xchange-cloudplugins-keycloak

Keycloak connector This package contains a keycloak connection handler to retrieve access and refresh tokens.
Version: 1.11.4-4
Type: OX Middleware Plugin
Depends on:

```
open-xchange-cloudplugins (<<1.11.5)
open-xchange-cloudplugins (>=1.11.4)
open-xchange-oidc (<<7.10.6)
open-xchange-oidc (>=7.10.4)
```

2.4.1 General Functionality

This plugin provides a connector interface to request access and refresh tokens from keycloak. List of features implemented by this plugin:

- Provides ICPKeycloakOAuthAccessTokenService to interact with configureable keycloak endpoints
  - Supports password grant with username and password
  - Supports refresh grant with refresh_token
- Provides additional services to interact with oauth mail handling
  - AuthenticationFailedHandler - will request a new access token, when the imap backend signals, that the current access token is not valid anymore. If that is not possible, the session is terminated
  - SessionInspectorService - will request a new access and refresh token, if the initial access_token provided an expires_in value before the token actually timed out. If that is not possible, the session will be logged out.
- Provides ICPJwtParserService
  - Supports parsing the body of a JWT to read additional provided values from the keycloak endpoint.

2.4.2 Installation

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

```
<package installer> install open-xchange-cloudplugins-keycloak
```

2.4.3 Configuration

For details, please see appendix A
/opt/open-xchange/etc/cloudplugins-keycloak.properties (page 17)

2.5 Package open-xchange-cloudplugins-loginproxy-ui

Implements a 2-step login flow required during migrations
Version: 1.11.4-4
Type: OX Frontend Plugin
Depends on:

```
open-xchange-appsuite-manifest (<<7.10.6)
open-xchange-appsuite-manifest (>=7.10.4)
```

2.5.1 Installation

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

```
<package installer> install open-xchange-cloudplugins-loginproxy-ui
```

2.6 Package open-xchange-cloudplugins-loginproxy-ws

Cloudplugins loginproxy REST API This package provides a restful API for the 2-step login.
Version: 1.11.4-4
Type: OX Middleware Plugin
Depends on:

```
open-xchange-cloudplugins (<<1.11.5)
open-xchange-cloudplugins (>=1.11.4)
open-xchange-core (<<7.10.6)
open-xchange-core (>=7.10.4)
```

2.6.1 General Functionality

This plugin provides a middleware restfull API to provide a 2-step login.
List of features implemented by this plugin:

- Main entry point is **/api/oxaas-public/v1/loginproxy**
- not secured, only by IP check rate limit
- **?login=loginValue** provide login pre-check

2.6.2 Installation

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

```
<package installer> install open-xchange-cloudplugins-loginproxy-ws
```

2.6.3 Configuration

For details, please see appendix A
/opt/open-xchange/etc/cloudplugins-loginproxy-forward.yaml (page 17)
/opt/open-xchange/etc/cloudplugins-loginproxy-ws.properties (page 18)

2.7 Package open-xchange-cloudplugins-mailfilter

CloudPlugins MailFilter Utilities This package implements a mailfilter interceptor driver framework and provides some useful drivers.
Version: 1.11.4-4
Type: OX Middleware Plugin
Depends on:

```
open-xchange-cloudplugins (<<1.11.5)
open-xchange-cloudplugins (>=1.11.4)
open-xchange-mailfilter (<<7.10.6)
open-xchange-mailfilter (>=7.10.4)
open-xchange-rest (<<7.10.6)
open-xchange-rest (>=7.10.4)
```

2.7.1 General Functionality

This plugin provides a mailfilter interceptor driver framework and some useful drivers. List of features implemented by this plugin:

- Registers a MailFilterInterceptor
  - Automatically starts a Driver Manager which tracks MailFilterInterceptor Drivers
  - When a user creates/updates/deletes a filter rule, the driver manager will run each driver that is supported for that user in order of their rank.
- Provides MailFilterInterceptor Drivers - configured via their enabled property
  - RedirectStatusDriver - supports any user in any of the configured brands and tells CloudManagementCassandraService the autoforward status and how many redirects exist.
  - RedirectBlacklistDriver - supports Config Cascade. Blocks users from creating only autoforward or all redirect mail filter rules that use a To Address that is blacklisted.

2.7.2 Installation

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

```
<package installer> install open-xchange-cloudplugins-mailfilter
```

2.7.3 Configuration

For details, please see appendix A
/opt/open-xchange/etc/mailfilter-interceptor-drivers.properties (page 19)

2.8 Package open-xchange-cloudplugins-oidc

OIDC backend for any default Identity Server This package contains multiple OIDC backends for any Identity Server, that fully supports the OIDC protocol.
Version: 1.11.4-4
Type: OX Middleware Plugin
Depends on:

```
open-xchange-cloudplugins (<<1.11.5)
open-xchange-cloudplugins (>=1.11.4)
open-xchange-oidc (<<7.10.6)
open-xchange-oidc (>=7.10.4)
```

2.8.1 General Functionality

The plugin provides the backend configuration for OIDC.
List of features implemented by this plugin:

- One or many OIDCBackends
- Supports reloadconfiguration clt without stopping unchanged OIDCBackends
- Can be started in addition to a normal AuthenticationService

2.8.2 Installation

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

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

2.8.3 Configuration

For details, please see appendix A
/opt/open-xchange/etc/cloudplugins-oidc.properties (page 21)

2.9 Package open-xchange-cloudplugins-saml

SAML backend for any default Identity Server This package contains an SAML backend for any Identity Server, that fully supports the SAML protocol.
Version: 1.11.4-4
Type: OX Middleware Plugin
Depends on:

```
open-xchange-cloudplugins (<<1.11.5)
open-xchange-cloudplugins (>=1.11.4)
open-xchange-saml-core (<<7.10.6)
open-xchange-saml-core (>=7.10.4)
```

2.9.1 General Functionality

The plugin provides the backend configuration for SAML.
List of features implemented by this plugin:

- One or many SAMLBackends
- Supports reloadconfiguration clt without stopping unchanged SAMLBackends
- Can be started in addition to a normal AuthenticationService

2.9.2 Installation

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

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

2.9.3 Configuration

For details, please see appendix A
/opt/open-xchange/etc/cloudplugins-saml.properties (page 25)

2.10 Package open-xchange-cloudplugins-trustedidentity-ldap

Cloud-Plugins Trusted Identity LDAP Support Support for storing Trusted Identity keys in LDAP using Cloud-Plugins.
Version: 1.11.4-4
Type: OX Middleware Plugin
Depends on:

```
open-xchange-cloudplugins (<<1.11.5)
open-xchange-cloudplugins (>=1.11.4)
open-xchange-core (<<7.10.6)
open-xchange-core (>=7.10.4)
open-xchange-plugins-trustedidentity (<<1.7.0)
open-xchange-plugins-trustedidentity (>=1.6.4)
```

2.10.1 General Functionality

This package provides a Trusted Identity key storage driver that looks up encrypted private keys from the OXaaS LDAP tree and decrypts them using on-disk storage keys.

2.10.2 Installation

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

```
<package installer> install open-xchange-cloudplugins-trustedidentity-ldap
```

2.10.3 Configuration

For details, please see appendix A
/opt/open-xchange/etc/trustedidentity-ldap.properties (page 27)

2.11 Package open-xchange-cloudplugins-trustedidentity-ldap-tools

CLI Tools for Cloud-Plugins Trusted Identity LDAP Support CLI Tools for support for storing Trusted Identity keys in LDAP using Cloud-Plugins.
Version: 1.11.4-4
Type: Other

2.11.1 General Functionality

This package provides a Trusted Identity key storage driver that looks up encrypted private keys from the OXaaS LDAP tree and decrypts them using on-disk storage keys.

2.11.2 Installation

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

```
<package installer> install open-xchange-cloudplugins-trustedidentity-ldap-tools
```

2.12 Package open-xchange-oxaas-alias

OXaaS alias bundle This package implements OXaaS alias handling.
Version: 1.11.4-4
Type: OX Middleware Plugin
Depends on:

```
open-xchange-admin (<<7.10.6)
open-xchange-admin (>=7.10.4)
open-xchange-core (<<7.10.6)
open-xchange-core (>=7.10.4)
```

2.12.1 General Functionality

The plugin is available to everyone on the installed system.
List of features implemented by this plugin:

- Alias are provided through internal and external APIs
- add and all requests are backed by a Tarent adapter
- del request is handled internally by using the internal provisioning interfaces
- max concurrent aliases are set by config-cascade aware setting com.openexchange.oxaas.aliasquota with default of 15.

2.12.2 Installation

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

```
<package installer> install open-xchange-oxaas-alias
```

2.12.3 Configuration

For details, please see appendix A
/opt/open-xchange/etc/oxaas-alias.properties (page 27)

2.13 Package open-xchange-oxaas-mail-notify-ws

OXaaS notification mail servlet bundle
Version: 1.11.4-4
Type: OX Middleware Plugin
Depends on:

```
open-xchange-cloudplugins (<<1.11.5)
open-xchange-cloudplugins (>=1.11.4)
open-xchange-core (<<7.10.6)
open-xchange-core (>=7.10.4)
open-xchange-imap (<<7.10.6)
open-xchange-imap (>=7.10.4)
open-xchange-smtp (<<7.10.6)
open-xchange-smtp (>=7.10.4)
```

2.13.1 General Functionality

The plugin is available to everyone that has correctly setup configuration.
List of features implemented by this plugin:

- Configuration for templates are done on a config-cascade base
- `com.openexchange.oxaas.mail.quota.notify.prefix` with default value `notify.oxaas.over.quota`
- `com.openexchange.oxaas.mail.welcomemail.notify.prefix` with default value `notify.oxaas.welcome.mail`

- com.openexchange.oxaas.mail.removed.sent.spam.notify.prefix
  with default value notify.oxaas.disable.sent.spam
- The above prefix is used for the templates where each template must have
  ${prefix}.${quotavalue}.[html|subject|text].tmpl files present, in the case of the over quota mails.For the others, it is
  ${prefix}.[html|subject|text].tmpl
- Default files are provided for 90% and 100% with the prefix notify.oxaas.over.quota.
- com.openexchange.noreply.address must be set via config-cascade, otherwise this feature won't work.
- com.openexchange.oxaas.mail.(quota|welcomemail|removed.sent.spam).ignoreFooterImage can be set via config-cascade to disable footerImage added as attachment to the mail, or by using com.openexchange.oxaas.mail.ignoreFooterImage that applies to all types

2.13.2 REST API

This package implements the OXaaS mail notification generation servlet which will return several mails via a REST API:

```
1 /api/oxaas/notification/mail/quota/{usercontext}/ (JSON body: {"quota_threshold":"..."})
2 /api/oxaas/notification/mail/welcomemail/{usercontext}/
3 /api/oxaas/notification/mail/disable_sent_spam_notification/{usercontext}/
```

2.13.3 Installation

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

```
<package installer> install open-xchange-oxaas-mail-notify-ws
```

2.13.4 Configuration

For details, please see appendix A
/opt/open-xchange/etc/oxaas-mail-notification-templates.properties (page 28)
/opt/open-xchange/etc/oxaas-drive-quota-notification.properties (page 28)

2.13.5 Templates

/opt/open-xchange/templates/notify.oxaas.over.quota.90.subject.tmpl
/opt/open-xchange/templates/notify.oxaas.over.quota.100.text.tmpl
/opt/open-xchange/templates/notify.oxaas.over.quota.90.text.tmpl
/opt/open-xchange/templates/notify.oxaas.over.quota.90.html.tmpl
/opt/open-xchange/templates/notify.oxaas.over.quota.100.subject.tmpl
/opt/open-xchange/templates/notify.oxaas.over.quota.100.html.tmpl

2.14 Package open-xchange-oxaas-mail-unread-ws

OXaaS mail custom mail servlet bundle This package implements OXaaS mail servlet to gather information via rest api.
Version: 1.11.4-4
Type: OX Middleware Plugin
Depends on:

```
open-xchange-cloudplugins (<<1.11.5)
open-xchange-cloudplugins (>=1.11.4)
open-xchange-core (<<7.10.6)
open-xchange-core (>=7.10.4)
open-xchange-imap (<<7.10.6)
open-xchange-imap (>=7.10.4)
```

2.14.1 General Functionality

API to featch the user related unread count for INBOX
List of features implemented by this plugin:

- API is reachable at `http://localhost:8009/preliminary/api/oxaas/mail/unread/<useridentifier>`
- API is secured by oxaas-mail-unread.properties where it is possible to add configuration for each brand that should have this feature enabled
- Set com.openexchange.oxaas.mail.unread.ws.basic.usernames=hosterone
- Set com.openexchange.oxaas.mail.unread.ws.basic.hosterone.brand=internalBrandForhosterone
- Set com.openexchange.oxaas.mail.unread.ws.basic.hosterone.password=verySecretPassword

2.14.2 Installation

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

```
<package installer> install open-xchange-oxaas-mail-unread-ws
```

2.14.3 Configuration

For details, please see appendix A
/opt/open-xchange/etc/oxaas-mail-unread.properties (page 28)

2.15 Package open-xchange-oxaas-mail-ws

OXaaS mail custom mail servlet bundle This package implements OXaaS mail servlet to gather information via rest api.
Version: 1.11.4-4
Type: OX Middleware Plugin
Depends on:

```
open-xchange-cloudplugins (<<1.11.5)
open-xchange-cloudplugins (>=1.11.4)
open-xchange-core (<<7.10.6)
open-xchange-core (>=7.10.4)
open-xchange-imap (<<7.10.6)
open-xchange-imap (>=7.10.4)
```

2.15.1 General Functionality

This plugin provides a middleware restfull API to retrieve details of customerdata.
List of features implemented by this plugin:

- Main entry point is **/api/oxaas/mail**
- secured by basic auth mapped to customer brand
- **/api/oxaas/mail/{uid}/recentmails** returns latest 5 mails in INBOX

- **/api/oxaas/mail/{uid}/quota** returns current mailbox quota
- **/api/oxaas/mail/{uid}/newmessages** returns the number of new mails since last login
- **/api/oxaas/mail/{uid}** all of the above combined

2.15.2 Installation

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

```
<package installer> install open-xchange-oxaas-mail-ws
```

2.15.3 Configuration

For details, please see appendix A
/opt/open-xchange/etc/oxaas-mail.properties (page 29)

A Configuration Files

File 1 /opt/open-xchange/etc/cloudplugins-antiphishing-vadesecure-ldap.properties

```
1
2  # Setting to change the VadeSecure connector identifier referenced in plugins-antiphishing
       .properties / com.openexchange.plugins.antiphishing.connector
3  # Default: "cloudplugins_antiphishing_vadesecure_ldap"
4  # Config-cascade aware: true
5  # Lean: true
6  com.openexchange.cloudplugins.antiphishing.vadesecure.ldap.identifier=
       cloudplugins_antiphishing_vadesecure_ldap
```

File 2 /opt/open-xchange/etc/cloudplugins-blackwhitelist-ldap.properties

```
1  # Identifier of this blackwhitelist connector: cloudplugins_blackwhitelist_ldap
2  # hostname of ldap server
3  com.openexchange.cloudplugins.blackwhitelist.connector.ldap.uri=ldap-fqhn.example.com
4
5  # ldap port
6  com.openexchange.cloudplugins.blackwhitelist.connector.ldap.port=389
7
8  # ldap user
9  com.openexchange.cloudplugins.blackwhitelist.connector.ldap.user=cn=oxadmin,o=oxcs
10
11 # ldap password
12 com.openexchange.cloudplugins.blackwhitelist.connector.ldap.passwd=
13
14 # ldap maximum pool size
15 com.openexchange.cloudplugins.blackwhitelist.connector.ldap.pool.size=10
16
17 # ldap max requests before connection is closed
18 # can be set to -1 to be disabled
19 com.openexchange.cloudplugins.blackwhitelist.connector.ldap.pool.max.requests=2000
20
21 # ldap max lifetime in seconds for each connection in the pool
22 com.openexchange.cloudplugins.blackwhitelist.connector.ldap.pool.max.lifetime=120
23
24 # config to enable LDAP SSL connection over ldaps
25 com.openexchange.cloudplugins.blackwhitelist.connector.ldap.useSSL=false
26
27 # Setting to check if memory backed test mock should be started
28 # This connector is identified by cloudplugins_blwl_test
```

```
# Default: false
com.openexchange.cloudplugins.blackwhitelist.connector.ldap.test=false
```

File 3 /opt/open-xchange/etc/cloudplugins-forwards.properties

```
# Defines whether the forward REST API should be enabled or not.
#
# This parameter is optional and defaults to "false" (disabled).
#
# Example:
# com.openexchange.cloudplugins.admin.forwards.ws.enabled=true
com.openexchange.cloudplugins.admin.forwards.ws.enabled=false
```

File 4 /opt/open-xchange/etc/cloudplugins-keycloak.properties

```
# The token endpoint identified by the client
#
# Must be set for each client, default value: ""
#
# Example:
# com.openexchange.cloudplugins.keycloak.oauth.exampleClient.tokenEndpoint=http://
    localhost:8080/auth/realms/demo/protocol/openid-connect/token
com.openexchange.cloudplugins.keycloak.oauth.[client].tokenEndpoint=

# The clientId, if left empty, no clientId will be used
#
# Optional, default value: ""
#
# Example:
# com.openexchange.cloudplugins.keycloak.oauth.exampleClient.clientId=customerClient
com.openexchange.cloudplugins.keycloak.oauth.[client].clientId=

# The default-client used for the CloudAuthenticationDriver
com.openexchange.cloudplugins.keycloak.oauth.default-client.clientId=

# The client secret. Must be provided if clientId is set.
#
# Optional, default value: ""
#
# Example:
# com.openexchange.cloudplugins.keycloak.oauth.exampleClient.clientSecret=123123
com.openexchange.cloudplugins.keycloak.oauth.[client].clientSecret=

# The default-client secret used for the CloudAuthenticationDriver
com.openexchange.cloudplugins.keycloak.oauth.default-client.clientSecret=

# Max connections
#
# Optional, default value: 100
com.openexchange.cloudplugins.keycloak.oauth.maxConnections=100

# Max connections per host
#
# Optional, default value: 100
com.openexchange.cloudplugins.keycloak.oauth.maxConnectionsPerHost=100

# Connection timeout in ms
#
# Optional, default value in ms: 3000
com.openexchange.cloudplugins.keycloak.oauth.connectionTimeout=3000

# Socket read timeout in ms
#
```

```
# Optional, default value in ms: 6000
com.openexchange.cloudplugins.keycloak.oauth.socketReadTimeout=6000

# Refresh time in ms before expiry date
#
# Optional, default value is ms: 60000
com.openexchange.cloudplugins.keycloak.oauth.refreshTime=60000

# Enables the keycloak cloud-plugins CloudAuthenticationDriver.
# If either of the following properties is set, it is not required to enable this property
#     com.openexchange.mail.authType=xoauth2 or oauthbearer
#     com.openexchange.mail.filter.preferredSaslMech=OAUTHBEARER or XOAUTH2
#
# Default: false
com.openexchange.cloudplugins.keycloak.oauth.authentication.enabled=false

# Comma seperated blocklist of hostnames that should not be handled by the keycloak
    CloudAuthenticationDriver
# Default: <empty>
com.openexchange.cloudplugins.keycloak.oauth.authentication.blocklist=

# Sets the client identifier for the CloudAuthenticationDriver
# Internally will use the value "default-client" as a fallback
#
# Default: ""
com.openexchange.cloudplugins.keycloak.oauth.authentication.client=default-client

# One may set different clients on a brand base
#
# com.openexchange.cloudplugins.keycloak.oauth.authentication.client.<brand>=<client>
# Example:
#
# com.openexchange.cloudplugins.keycloak.oauth.authentication.client.brand1=cloudplugins-
    keycloak-custom-client
# com.openexchange.cloudplugins.keycloak.oauth.authentication.client.brand2=brand-specific
    -client

# Sets the response identifier for the CloudAuthenticationDriver
#
# Special case: oxUserId@oxContextId enables lookup for the two keys oxUserId and
    oxContextId
#               Afterwards they are again handled as oxUserId@oxContextId
#
# Default: "preferred_username"
com.openexchange.cloudplugins.keycloak.oauth.authentication.response.identifier=
    preferred_username

# One may set different response identifiers on a brand base
#
# com.openexchange.cloudplugins.keycloak.oauth.authentication.response.identifier.<brand
    >=<client>
# Example:
#
# com.openexchange.cloudplugins.keycloak.oauth.authentication.response.identifier.brand1=
    email
# com.openexchange.cloudplugins.keycloak.oauth.authentication.response.identifier.brand2=
    alias

# Configure the LDAP lookup method to find users using their logins.
# It is the method that is used by default when there is no brand specific
# configuration setting).
#
# Optional, defaults to "uid".
#
# Possible values:
# uid
#   attempts to find users by matching their login against the uid attribute.
# email
#   attempts to find users by matching their login against the alias attribute.
# auto
#   when the login contains a "@", the "email" method is used and when not,
#   the "uid" method is used
```

```
112 # uid-or-email
113 #   attempts to find users by matching their login against the uid and the alias
114 #   attributes (either may match)
115 #
116 # Note that this only applies to the keycloak authentication driver. If there
117 # is a custom implementation that is used for a given brand, its behavior is
118 # not influenced by this properties.
119 #
120 # Example:
121 # com.openexchange.cloudplugins.keycloak.oauth.authentication.uid.mode=auto
122
123 # One may define any number of such settings per brand by setting properties
124 # with the following format for their name:
125 #
126 # com.openexchange.cloudplugins.keycloak.oauth.authentication.uid.mode.<brand>=<uid|email|
        auto|uid-or-email|userid-contextid>
127 #
128 # For the list of possible values, please consult the documentation for
129 # com.openexchange.cloudplugins.keycloak.oauth.authentication.uid.mode
130 #
131 # Optional, defaults to falling back to the method configured in
132 # com.openexchange.cloudplugins.keycloak.oauth.authentication.uid.mode
133 #
134 # Note that this only applies to the default authentication service driver.
135 # If there is a custom implementation that is used for a given brand, its
136 # behavior is not influenced by these properties.
137 #
138 # Example:
139 #
140 # com.openexchange.cloudplugins.keycloak.oauth.authentication.uid.mode.brand1=auto
141 # com.openexchange.cloudplugins.keycloak.oauth.authentication.uid.mode.brand2=uid
```

File 5 /opt/open-xchange/etc/cloudplugins-loginproxy-forward.yaml

```
1  # This file contains mappings of brand, identifiers and redirect urls.
2  # It must be a YAML mapping, where
3  # * the key is the brand
4  # * the value is a list of properties with key, value
5  ---
6  'brand1':
7  - identifier: https://loginpage1.example.com
8  - another_identifier: https://loginpage2.example.org
9  - default_redirect: https://default.example.com
10 'brand2':
11 - my_ident: https://loginpage1.example.com
12 - default_redirect: https://default.example.com
13 'brand3':
14 - some_other_identifier: https://loginpage1.example.com
```

File 6 /opt/open-xchange/etc/cloudplugins-loginproxy-ws.properties

```
1  # Maximum amount of login proxy lookup requests per second per source IP address.
2  # May be a decimal number.
3  #
4  # Optional, default value: 25.0
5  #
6  # Example:
7  # com.openexchange.cloudplugins.login.proxy.maxRequestsPerSecond=50.0
8  com.openexchange.cloudplugins.login.proxy.maxRequestsPerSecond=25.0
9
10 # Maximal time window, in milliseconds: after a given source IP address has not accessed
11 # the login proxy lookup API, its number of requests per second rate is reset.
12 #
```

```
# Optional, default value: 300000
#
# Example:
# com.openexchange.cloudplugins.login.proxy.maxRateTimeWindow=60000
com.openexchange.cloudplugins.login.proxy.maxRateTimeWindow=300000

# Strategy to use for reacting to the inability to access the API for a given source
# IP address due to surpassing the maxRequestsPerSecond rate.
#
# Format: it must be one of:
# * fail-fast
# * block
# * timeout:...
#
# fail-fast
#   if the rate limit is exceeded, the API will respond with a 403 Forbidden
# block
#   if the rate limit is exceeded, the API will block infinitely until the rate limit
#   allows for another request to be performed
# timeout:...
#   block until the specified timeout is reached, after which the API responds with a
#   403 Forbidden
#   The value after "timeout:" consists of a number followed by a time unit, examples:
#   - timeout:400s ---> 400 seconds
#   - timeout:1m ------>   1 minute
#   - timeout:2000ms -> 2000 milliseconds
#
# Optional, default value: timeout:5s
#
# Example:
# com.openexchange.cloudplugins.login.proxy.strategy=timeout:10s
com.openexchange.cloudplugins.login.proxy.strategy=timeout:5s

# The default URL to redirect to when the user is not marked as not migrated
# and the identifierof the user is not mapped in cloudplugins-loginproxy-forward.yaml
# and the brand does not have a default redirect in cloudplugins-loginproxy-forward.yaml
#
# Example:
# com.openexchange.cloudplugins.login.proxy.default.redirect=https://example.com/mail
# Default: not set
com.openexchange.cloudplugins.login.proxy.default.redirect=
```

File 7 /opt/open-xchange/etc/mailfilter-interceptor-drivers.properties

```
# This is the CloudPlugins MailFilterInterceptorDriver configuration
#
# Enable drivers by adding at least one brand in the brands property for that driver
# on the server level configuration. If no brand exists, the driver will not be registered
#
# Some drivers may also have additional configurations


##### Driver Brand Lists #####
# Comma delimited lists

# Brands that the RedirectStatusDriver should be enabled for
#
# Optional - default is no brands
com.openexchange.cloudplugins.mailfilter.intercept.drivers.redirect.status.driver.brands=

# Brands that the RedirectBlacklistDriver should be enabled for
#
# Optional - default is no brands
com.openexchange.cloudplugins.mailfilter.intercept.drivers.redirect.blacklist.driver.
    brands=

##### End Driver Brand Lists #####

```

```
24
25
26  ##### Driver Specific configurations #####
27
28  ### Redirect Blacklist Driver ###
29  #
30  # Set to true to enable config cascade for all properties of the Redirect Blacklist Driver
        .
31  # This should be used to set different configurations per brand or an even lower level.
32  # This property is NOT config cascade aware as it is used to control use of it.
33  # Even the driver brand list property can be config cascade if this is enabled which would
        be useful
34  # to enable it for a brand, but disable it for some users
35  #
36  # Optional - default is false
37  com.openexchange.cloudplugins.mailfilter.intercept.drivers.redirect.blacklist.driver.
        configcascade.enable=false
38  #
39  # The comma+space delimited list of regular expressions that are blacklisted for mail
        filter redirects.
40  # Java regular expressions are supported here, so non regex characters must be escaped.
41  # Example: abuse@.*, spam@domain\.com  <-- '.' has been escaped to match only '.' and not
        any char
42  # See for regex contructs: https://docs.oracle.com/javase/7/docs/api/java/util/regex/
        Pattern.html
43  # WARNING: You must use ", " (comma and a space) as the separator to separate the regexs
44  #
45  # Optional - default is empty which should only be left if this driver is not used
46  com.openexchange.cloudplugins.mailfilter.intercept.drivers.redirect.blacklist.driver.
        blacklist=
47  #
48  # Set to true to only blacklist true autoforward rules which are defined by having the "
        autoforward" flag.
49  # If set to false, then all redirect rules will be checked for the blacklist addresses
50  #
51  # Optional - default is true
52  com.openexchange.cloudplugins.mailfilter.intercept.drivers.redirect.blacklist.driver.
        autoforward.only=true
53  #
54  ### End Redirect Blacklist Driver ###
55
56  ##### End Driver Specific configurations #####
```

File 8 /opt/open-xchange/etc/cloudplugins-oidc.properties

```
1   # The properties for cloud setup OIDC bundle
2
3   # The general oidc property to enable or disable the core oidc registry
4   com.openexchange.oidc.enabled=true
5
6   ### General settings
7   ##########################################################################################
8   # Regex to validate user name
9   com.openexchange.cloudplugins.oidc.user.regex=[0-9a-zA-Z.@]*
10
11  # All properties below can also be assigned to an identifier by configuring them as
12  # com.openexchange.cloudplugins.oidc.<identifier>.key
13  #
14  # If a property is not set for an identifier, the key without the identifier is used as a
        default
15  #
16  # Example:
17  #    com.openexchange.cloudplugins.oidc.example.id=someValue
18  #    com.openexchange.cloudplugins.oidc.brand=someBrand
19  #    com.openexchange.cloudplugins.oidc.example.brand=
20  #    example brand => someBrand
21  #
22  # !! Note !!
```

```
#    The list of possible OIDCBackends is identified by the property
#    com.openexchange.cloudplugins.oidc.enabled.<identifier>
#
# Example:
#    com.openexchange.cloudplugins.oidc.enabled=true
#    com.openexchange.cloudplugins.oidc.enabled.myIdentifier=true
#    com.openexchange.cloudplugins.oidc.enabled.moreIdentifier=true
#
#    It is possible to disable certain OIDCBackends by configuration
#
#    com.openexchange.cloudplugins.oidc.enabled is also valid and will be used as an empty identifier
#    An empty identifier will use all properties set in this config file.
#
# com.openexchange.cloudplugins.oidc.enabled.<identifier>=true
com.openexchange.cloudplugins.oidc.enabled=false

### OIDC Specific configuration
################################################################################################
# All properties mentioned at https://documentation.open-xchange.com/components/middleware/config/7.10.2/#mode=features&feature=OpenID
# can be assigned to each OIDCbackend.
#
# !! NOTE !!
#     The default prefix is not 'com.openexchange.oidc'
#     'com.openexchange.cloudplugins.oidc'
#     is used instead meaning that there is an additional
#     'cloudplugins' in between to differentiate from the general oidc configuration.
#
# Example:
#    com.openexchange.oidc.clientId will not be evaluated
#    com.openexchange.oidc.cloudplugins.clientId is the correct default key
#
# The id inside the jwt token response which holds the userinformation
#
# The search for the id is done in the attributeStatement if nothing is configured
# possible configuration values are:
#    <not_set>      // the subject is used
#    claim:key      // a claim with the identifier <key> is used
#    key            // a claim with the identifier <key> is used
#
# In any case, the id must match the uid used to provision the user
# com.openexchange.cloudplugins.oidc.<identifier>.id=
com.openexchange.cloudplugins.oidc.id=

# The ldap lookup used by this OIDCBackend
#
# Configure the LDAP lookup method to find users using their identifiers.
#
#
# Possible values:
# uid
#   attempts to find users by matching their login against the uid attribute.
# email
#   attempts to find users by matching their login against the alias attribute.
# auto
#   when the login contains a "@", the "email" method is used and when not,
#   the "uid" method is used
# uid-or-email
#   attempts to find users by matching their login against the uid and the alias
#   attributes (either may match)
#
# This property is optional.
# Default: uid
# com.openexchange.cloudplugins.oidc.<identifier>.ldapLookup=
com.openexchange.cloudplugins.oidc.ldapLookup=


# The brand to use for OXaaS LDAP authentication operations.
# Uses the host name when empty or not set.
#
# This property is mandatory.
```

```
# Default: <empty>
# com.openexchange.cloudplugins.oidc.<identifier>.brand=
com.openexchange.cloudplugins.oidc.brand=

# The authentication method used for the token endpoint.
# Can be a selection of:
#    basic
#    post
#
# This property is optional.
# Default: basic if not set
# com.openexchange.cloudplugins.oidc.<identifier>.tokenAuth=
com.openexchange.cloudplugins.oidc.tokenAuth=

# This backends servlet path, which is appended to the default /oidc/ path.
#
# This property is optional.
# Default: <empty>
# com.openexchange.cloudplugins.oidc.<identifier>.backendPath=
com.openexchange.cloudplugins.oidc.backendPath=

# List of hosts where that this OIDCBackend is responsible for
# if all is present, this is responsible for all hosts
#
# It is possible to control the backendPath with this property.
# Another way would be to set the backendPath within the as-config.yml.
# If set in as-config.yml, it must be set as oidcPath
# Default: <empty>
# com.openexchange.cloudplugins.oidc.<identifier>.hosts=
com.openexchange.cloudplugins.oidc.hosts=

# Set the redirect location for a failed authentcation reuqest if the request could not be identified or took too long
com.openexchange.cloudplugins.oidc.failureRedirect=

# Set the redirect location for all other authentication exceptions that may occure. This mainly targets issues with the token validation
com.openexchange.cloudplugins.oidc.authenticationFailedExceptionRedirect=

# Set the redirect location for logout exceptions.
com.openexchange.cloudplugins.oidc.logoutFailedExceptionRedirect=

# Set the redirect location for general exceptions in the middleware that could not be handled by either
#  - failureRedirect
#  - authenticationFailedExceptionRedirect
#  - logoutFailedExceptionRedirect
# If only one endpoint should be defined for redirect, it is save to only set responseExceptionRedirect
com.openexchange.cloudplugins.oidc.responseExceptionRedirect=
```

File 9 /opt/open-xchange/etc/cloudplugins-saml.properties

```
# The properties for cloud setup SAML bundle

### General settings
##########################################################################################
# Regex to validate host HTTP Header value
com.openexchange.cloudplugins.saml.host.regex=[0-9a-zA-Z.]*

# Regex to validate user name
com.openexchange.cloudplugins.saml.user.regex=[0-9a-zA-Z.@]*

# Base folder for the saml keystore files
# This property must be set if Java Security Manager is enabled
# It can't be set for inidividual identifiers
com.openexchange.cloudplugins.saml.keyStoreBasePath=

```

```
### Key-store/certificate settings
################################################################################################
# All properties below can also be assigned to an identifier by configuring them as
# com.openexchange.cloudplugins.saml.<identifier>.key
#
# If a property is not set for an identifier, the key without the identifier is used as a
    default
# !!Note !!
#    If a property is marked as optional, the default value for the optional case is used
    and not the general
#    optional value if that is set
#
# Example:
#    com.openexchange.cloudplugins.saml.example.id=someValue
#    com.openexchange.cloudplugins.saml.keyStore=testStore
#    com.openexchange.cloudplugins.saml.example.keyStore=
#    example keyStore => testStore
#
# Example2:
#    com.openexchange.cloudplugins.saml.example.id=someValue
#    com.openexchange.cloudplugins.saml.brand=defaultBrand
#    com.openexchange.cloudplugins.saml.example.brand=
#    example brand (for ldap selection) => <empty>, will use the domainName of the request
    .
#
# !! Note !!
#    The list of possible SAMLBackends is identified by the property
#    com.openexchange.cloudplugins.saml.<identifier>.id
#    If there is no property for the id(s) set, no SAMLBackend will be started.
#    com.openexchange.cloudplugins.saml.id is also valid and will be used as an empty
    identifier
#    An empty identifier will use all properties set in this config file.
#
# The full path to a Java keystore containing the IdPs certificate.
#
# Default: <empty>
com.openexchange.cloudplugins.saml.keyStore=

# Password to open the keystore.
#
# Default: <empty>
com.openexchange.cloudplugins.saml.keyStorePass=

# The aliases of the IdP certificate entry within the above specified
# keystore. Split by ','. Multiple certs can be used in a rolling upgrade
# case at the customers location without the need to coordinate an upgrade.
#
# The support for multiple certs is only enabled on 7.10.1+ systems.
# A 7.10.0 system will only use the first certAlias
#
# Default: <empty>
com.openexchange.cloudplugins.saml.certAlias=

# The alias of the signingKey entry within the above specified
# keystore.
#
# Default: <empty>
com.openexchange.cloudplugins.saml.signingKeyAlias=

# The password of the signingKey entry within the above specified
# keystore.
#
# Default: <empty>
com.openexchange.cloudplugins.saml.signingKeyPassword=

# The alias of the decryptionKey entry within the above specified
# keystore.
#
# Default: <empty>
com.openexchange.cloudplugins.saml.decryptionKeyAlias=

# The password of the decryptionKey entry within the above specified
```

```
# keystore.
#
# Default: <empty>
com.openexchange.cloudplugins.saml.decryptionKeyPassword=

### SAML Specific configuration
##########################################################################################
# The id inside the saml response which holds the userinformation
#
# The search for the id is done in the attributeStatement if nothing is configured
# possible configuration values are:
#    key            // search is done in the attributeStatement with the key
#    attribute:key  // search is done in the attributeStatement with the key
#    subject:nameID // the subject:NameId is used
#
# In any case, the id must match the uid used to provision the user
com.openexchange.cloudplugins.saml.id=

# The ldap lookup used by this SAMLBackend
#
# Configure the LDAP lookup method to find users using their identifiers.
#
#
# Possible values:
# uid
#   attempts to find users by matching their login against the uid attribute.
# email
#   attempts to find users by matching their login against the alias attribute.
# auto
#   when the login contains a "@", the "email" method is used and when not,
#   the "uid" method is used
# uid-or-email
#   attempts to find users by matching their login against the uid and the alias
#   attributes (either may match)
#
# This property is optional.
# Default: uid
com.openexchange.cloudplugins.saml.ldapLookup=

# URL of where the users are redirected after logout if single_logout is active
# Must only be set if enableSingleLogout is enabled
#
# Default: <empty>
com.openexchange.cloudplugins.saml.logout.redirect.url=

# The brand to use for OXaaS LDAP authentication operations.
# Uses the host name when empty or not set.
#
# This property is optional.
# Default: <empty>
com.openexchange.cloudplugins.saml.brand=

# 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.
#
# This property is optional.
# Default: <empty>
com.openexchange.cloudplugins.saml.failure.redirect=

# 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.cloudplugins.saml.failure.redirect is used.
#
# Default: <empty>
com.openexchange.cloudplugins.saml.logout.failure.redirect=

# The samlPath value required for the servlet alias
# registered with '{prefix}/saml/{samlPath}/..' as servlet alias.
#
# This property is optional.
# Default: <empty>
```

```
com.openexchange.cloudplugins.saml.samlPath=

# Static redirect upon login or relogin
#
# Ths property is optional.
# Default: <empty>
com.openexchange.cloudplugins.saml.staticRedirect=

# Whether the SPs metadata XML shall be made available via HTTP. The according
# servlet will then be available under 'http(s)://{hostname}/{prefix}/saml/metadata'.
#
# Default: false
com.openexchange.cloudplugins.saml.enableMetadataService=false

# Whether the single logout profile is enabled.
#
# Default: false
com.openexchange.cloudplugins.saml.enableSingleLogout=false

# Sets the entity ID of the service provider.
#
# This property is mandatory.
# Default: <empty>
com.openexchange.cloudplugins.saml.entityID=

# Sets the human-readable name of the service provider.
#
# This property is mandatory.
# Default: <empty>
com.openexchange.cloudplugins.saml.providerName=

# Sets the URL of the local assertion consumer service (ACS). This value is used within
# authentication requests, compared against Destination attributes in IdP responses
# and will be contained in the service providers metadata XML. The according endpoint
# is always registered with '{prefix}/saml/{samlPath}/acs' as servlet alias.
#
# This property is mandatory.
# Default: <empty>
# Example: https://appsuite.example.com/appsuite/api/saml/{samlPath}/acs
com.openexchange.cloudplugins.saml.acsURL=

# Sets the URL of the local single logout service. This value is compared against
    Destination
# attributes in IdP responses and will be contained in the service providers metadata XML.
# The according endpoint is always registered with '{prefix}/saml/{samlPath}/sls' as
    servlet alias.
#
# This property is mandatory if 'com.openexchange.cloudplugins.saml.enableSingleLogout' is
     'true'.
# Default: <empty>
# Example: https://appsuite.example.com/appsuite/api/saml/{samlPath}/sls
com.openexchange.cloudplugins.saml.slsURL=

# The binding via which logout responses shall be sent to the IdP on IdP-initiated single
# logout flows. Must be 'http-redirect' or 'http-post'.
#
# This property is mandatory if 'com.openexchange.cloudplugins.saml.enableSingleLogout' is
     'true'.
# Default: http-redirect
com.openexchange.cloudplugins.saml.logoutResponseBinding=http-redirect

# The HTML template to use when logout responses are sent to the IdP via HTTP POST.
# The template must be located in '/opt/open-xchange/templates'.
#
# This property is mandatory if 'com.openexchange.cloudplugins.saml.enableSingleLogout' is
     'true'
# and 'com.openexchange.cloudplugins.saml.logoutResponseBinding' is set to 'http-post'.
# Default: saml.logout.response.html.tmpl
com.openexchange.cloudplugins.saml.logoutResponseTemplate=saml.logout.response.html.tmpl

# The entity ID of the IdP. It will be used to validate the 'Issuer' elements of SAML
    responses.
```

```
#
# This property is mandatory.
# Default: <empty>
com.openexchange.cloudplugins.saml.idpEntityID=

# The URL of the IdP endpoint where authentication requests are to be sent to.
#
# This property is mandatory.
# Default: <empty>
com.openexchange.cloudplugins.saml.idpAuthnURL=

# The URL of the IdP endpoint where logout requests are to be sent to.
#
# This property is mandatory if 'com.openexchange.cloudplugins.saml.enableSingleLogout' is 'true'.
# Default: <empty>
com.openexchange.cloudplugins.saml.idpLogoutURL=

# It is possible to enable a special kind of auto login mechanism that allows user agents to
# re-use an existing OX session if it was created during the same browser session. If enabled,
# a special cookie will be set, which is linked to the OX session and bound to the browser sessions
# life time. The advantage of this mechanism is, that sessions are simply re-entered if the user
# refreshes his browser window. He is then also able to open more than one tab of OX App Suite
# at the same time. This mechanism can only re-use sticky sessions, i.e. it is mandatory that the
# requests are always routed to the same backend for a certain session.
#
# --- SECURITY WARNING ---
# Enabling this setting is not compliant to the SAML specification as it bypasses the IdP in
# certain cases. Additionally in scenarios where a public device is used, a foreign user might
# take over a formerly authenticated users session if that user forgets to log out and doesn't
# close his web browser (even if he closes the App Suite tab). As no login screen is displayed
# by OX in SAML environments, the user is even not able to decide, whether the application shall
# remember him or not.
#
# Default: false
com.openexchange.cloudplugins.saml.enableAutoLogin=false

# Whether unsolicited responses will be accepted or not.
#
# Default: true
com.openexchange.cloudplugins.saml.allowUnsolicitedResponses=true

# Whether SAML-specific auto-login is enabled, that uses the SessionIndex of the AuthnResponse
#
# Default: false
com.openexchange.cloudplugins.saml.enableSessionIndexAutoLogin=false

# List of hosts where that this SAMLBackend is responsible for
# if all is present, this SAMLBackend responsible for all hosts
#
# It is possible to control the samlPath with this property.
# Another way would be to set the samlPath within the as-config.yml.
# Default: <empty>
com.openexchange.cloudplugins.saml.hosts=
```

File 10 /opt/open-xchange/etc/trustedidentity-ldap.properties

```
### Configuration for LDAP support for Trusted Identity.

# Storage Keys are used to decrypt private ECDSA keys that are stored in LDAP.
# LDAP oxCloudTrustedIdentityKeyPair entities contain optional (but
# strongly encouraged) references to storage keys by name.
# Storage keys are symmetric/secret keys (AES is recommended).
# Those storage keys are defined here by configuration, with multiple parameters,
# that are defined using different prefixes but the same storageKeyName part in
# each property name:
# com.openexchange.cloudplugins.trustedidentity.ldap.storageKey.file.{storageKeyName}=...
# com.openexchange.cloudplugins.trustedidentity.ldap.storageKey.keyType.{storageKeyName}=...
# com.openexchange.cloudplugins.trustedidentity.ldap.storageKey.cipher.{storageKeyName}=...
# com.openexchange.cloudplugins.trustedidentity.ldap.storageKey.alias.{storageKeyName}=...
# com.openexchange.cloudplugins.trustedidentity.ldap.storageKey.secret.{storageKeyName}=...
#
# For example, using "sk1" as the {storageKeyName}:
# com.openexchange.cloudplugins.trustedidentity.ldap.storageKey.file.sk1=keystore:/opt/open-xchange/etc/sk1.jks
# com.openexchange.cloudplugins.trustedidentity.ldap.storageKey.keyType.sk1=AES
# com.openexchange.cloudplugins.trustedidentity.ldap.storageKey.cipher.sk1=AES/GCM/NoPadding
# com.openexchange.cloudplugins.trustedidentity.ldap.storageKey.alias.sk1=storageKey
# com.openexchange.cloudplugins.trustedidentity.ldap.storageKey.secret.sk1=secret

# The storage key file location is a fully qualified path to either a plain
# file that contains the encoded bytes of the symmetric key, or a Java KeyStore
# file.
# When using a keystore file, one may also want to configure the key alias and secret
# (see next properties below.)
#
# Property format:
# com.openexchange.cloudplugins.trustedidentity.ldap.storageKey.file.{storageKeyName}=...
# When the file is a KeyStore file, it must be prepended with "keystore:":
# com.openexchange.cloudplugins.trustedidentity.ldap.storageKey.file.{storageKeyName}=keystore:...
#
# Example of a plain file:
# com.openexchange.cloudplugins.trustedidentity.ldap.storageKey.file.sk1=/opt/open-xchange/etc/sk1.key
#
# Example of a KeyStore file:
# com.openexchange.cloudplugins.trustedidentity.ldap.storageKey.file.sk1=keystore:/opt/open-xchange/etc/sk1.jks
#
# The value is mandatory and has no default.
#
# com.openexchange.cloudplugins.trustedidentity.ldap.storageKey.file.storageKeyName=

# KeyStore key alias: when using a KeyStore file, defines the alias of the key entry to use
# as the symmetric/secret key.
#
# Example:
# com.openexchange.cloudplugins.trustedidentity.ldap.storageKey.alias.sk1=storageKey
#
# The value is optional when the KeyStore file contains a single entry.
#
# com.openexchange.cloudplugins.trustedidentity.ldap.storageKey.alias.storageKeyName=

# KeyStore secret: when using a KeyStore file, defines the password to use to
# decrypt the KeyStore as well as the key inside of it.
#
# Example:
# com.openexchange.cloudplugins.trustedidentity.ldap.storageKey.secret.sk1=my_secret
#
# The value is optional and defaults to an empty string ("").
#
# com.openexchange.cloudplugins.trustedidentity.ldap.storageKey.secret.storageKeyName=
```

```
63
64  # The cipher algorithm defines which symmetric decryption algorithm to use when
65  # unwrapping the private key from LDAP, and must be the same as the cipher used
66  # when encrypting it in the first place.
67  #
68  # Example:
69  # com.openexchange.cloudplugins.trustedidentity.ldap.storageKey.cipher.sk1=AES/CBC/
        PKCS5Padding
70  #
71  # The value is optional and defaults to AES/GCM/NoPadding
72  #
73  # com.openexchange.cloudplugins.trustedidentity.ldap.storageKey.cipher.storageKeyName=
74
75  # Storage Key caching: keys that are looked up in LDAP are cached in memory for
        performance
76  # reasons.
77  # The following configuration property determines how long they are kept in cache
78  # before being fetched from LDAP again:
79  # Format: duration[d|h|m|s|ms]
80  #
81  # Example:
82  # com.openexchange.cloudplugins.trustedidentity.ldap.cache.ttl=4h
83  #
84  # Optional, the default value is 1h (one hour).
85  com.openexchange.cloudplugins.trustedidentity.ldap.cache.ttl=
```

File 11 /opt/open-xchange/etc/oxaas-alias.properties

```
1   # Setting to control the uri of the tarent adapter
2   com.openexchange.oxaas.alias.tarent.uri=http://localhost
3
4   # Setting to control allowed domains
5   com.openexchange.oxaas.alias.allowed.domains=
6
7   # Setting to control if alias adapter should be in test mode (this means a mock is used)
8   com.openexchange.oxaas.alias.test=false
9
10  # Loglevel for the internal OkHttp3 client
11  # Allowed values are: NONE, BASIC, HEADERS, BODY
12  com.openexchange.oxaas.alias.tarent.loglevel=NONE
13
14  # Setting to control if Unsecured Https should be allowed or not
15  # Default: false
16  com.openexchange.oxaas.alias.tarent.allowUnsecuredHttps=false
17
18  # Master user needed to delete alias
19  com.openexchange.oxaas.alias.master.user=
20
21  # Master user password needed to delete alias
22  com.openexchange.oxaas.alias.master.password=
23
24  # Setting to control if a client cert shoul be loaded, must be in PKCS 12 format
25  # Can be mixed with com.openexchange.oxaas.alias.tarent.allowUnsecuredHttps
26  # allowUnsecuredHttps=true and clientcert.path=set
27  #     a client cert is used but the hostname is not verified and all server certs are
        trusted
28  # allowUnsecuredHttps=false and clientcert.path=set
29  #     a client cert is used, but hostname is verified and server certs must be trustable
30  # Default: empty
31  com.openexchange.oxaas.alias.tarent.ssl.clientcert.path=
32
33  # Setting that holds the password for the PKCS 12 container
34  # Default: empty
35  com.openexchange.oxaas.alias.tarent.ssl.clientcert.password=
36
37  # Default number of aliases to be configured by each userr
38  # Default: 15
39  com.openexchange.oxaas.aliasquota=15
```

File 12 /opt/open-xchange/etc/oxaas-mail-notification-templates.properties

```
# Config cascade-aware property to control the prefix of the users templates
# For each prefix and each user configured percentage
com.openexchange.oxaas.mail.quota.notify.prefix=notify.oxaas.over.quota

# Config cascade-aware property to control the prefix of the users templates
# For each prefix and each user configured percentage
com.openexchange.oxaas.mail.welcome.mail.notify.prefix=notify.oxaas.welcome.mail

# Config cascade-aware property to control the prefix of the users templates
# For each prefix and each user configured percentage
com.openexchange.oxaas.mail.removed.sent.spam.notify.prefix=notify.oxaas.disable.sent.spam
```

File 13 /opt/open-xchange/etc/oxaas-drive-quota-notification.properties

```
# Config-cascade aware setting to control the quotas that should be monitored
com.openexchange.oxaas.mail.quota.drive.quotas=90,100

# Config-cascade aware setting to control if the admin should also receive a mail, in case the filestore is context-wide
com.openexchange.oxaas.mail.quota.drive.updateAdmin=false

# Config-cascade aware setting to control how often a mail should be sent
# Default is 86400 (1 day)
# Set to 0 to ignore that and always send a new mail
com.openexchange.oxaas.mail.quota.drive.mail.seconds=86400
```

File 14 /opt/open-xchange/etc/oxaas-mail-unread.properties

```
# Value holding the usernames for basic authentication
# must be the username for basic auth split by ,
# e.g hosterone,hostertwo
com.openexchange.oxaas.mail.unread.ws.basic.usernames=

# Setting to control basic auth username
# example would be com.openexchange.oxaas.mail.unread.ws.basic.hosterone.brand=internalBrandForhosterone
#com.openexchange.oxaas.mail.unread.ws.basic.[username].brand=

# Setting to control basic auth password
# example would be com.openexchange.oxaas.mail.unread.ws.basic.hosterone.password=verySecretPassword
#com.openexchange.oxaas.mail.unread.ws.basic.[username].password=
```

File 15 /opt/open-xchange/etc/oxaas-mail.properties

```
# Value holding the usernames for basic authentication
# must be the username for basic auth split by ,
# e.g hosterone,hostertwo
com.openexchange.oxaas.mail.ws.basic.usernames=

# Setting to optimize the fetching of recentMessages
# If set to true, the virtual/all folder will be quried
# If set to false, the calculation is done in the middleware
# config-cascade aware
com.openexchange.oxaas.mail.ws.recentMessagesFromVirtualAll=false

```

```
12  # Setting to control basic auth username
13  # example would be com.openexchange.oxaas.mail.basic.hosterone.password=verySecretPassword
14  #com.openexchange.oxaas.mail.ws.basic.[username].password=
15
16  # Setting to control basic auth password
17  # example would be com.openexchange.oxaas.mail.basic.hosterone.brand=
        internalBrandForhosterone
18  #com.openexchange.oxaas.mail.ws.basic.[username].brand=
```

File 16 /opt/open-xchange/etc/as-config.yml

```
1  default:
2    host: all
3    # To enable the two-step login for migrations
4    loginProxy: true
```