



OX Cloud Plugins Technical Documentation for
1.11.3

2021-03-30

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	3
1.1	Warnings	3
1.2	Delivery Comment	3
1.3	Install Package Repository	3
1.4	Global Configuration	4
1.5	Build Dependencies	4
1.6	Notice	4
2	Shipped Packages and Version	4
2.1	Package open-xchange-cloudplugins-antiphishing-vadesecure-ldap	4
2.1.1	Installation	4
2.1.2	Configuration	4
2.2	Package open-xchange-cloudplugins-blackwhitelist-ldap	5
2.2.1	Installation	5
2.2.2	Configuration	5
2.3	Package open-xchange-cloudplugins-forwards-ws	5
2.3.1	General Functionality	5
2.3.2	Installation	6
2.3.3	Configuration	6
2.4	Package open-xchange-cloudplugins-keycloak	6
2.4.1	General Functionality	6
2.4.2	Installation	6
2.4.3	Configuration	7
2.5	Package open-xchange-cloudplugins-loginproxy-ui	7
2.5.1	Installation	7
2.6	Package open-xchange-cloudplugins-loginproxy-ws	7
2.6.1	General Functionality	7
2.6.2	Installation	7
2.6.3	Configuration	7
2.7	Package open-xchange-cloudplugins-mailfilter	8
2.7.1	General Functionality	8
2.7.2	Installation	8
2.7.3	Configuration	8
2.8	Package open-xchange-cloudplugins-oidc	8
2.8.1	General Functionality	9
2.8.2	Installation	9
2.8.3	Configuration	9
2.9	Package open-xchange-cloudplugins-saml	9
2.9.1	General Functionality	9
2.9.2	Installation	9
2.9.3	Configuration	9
2.10	Package open-xchange-oxaas-alias	10
2.10.1	General Functionality	10
2.10.2	Installation	10
2.10.3	Configuration	10
2.11	Package open-xchange-oxaas-mail-notify-ws	10
2.11.1	General Functionality	10
2.11.2	REST API	11
2.11.3	Installation	11
2.11.4	Configuration	11
2.11.5	Templates	11
2.12	Package open-xchange-oxaas-mail-unread-ws	12
2.12.1	General Functionality	12
2.12.2	Installation	12
2.12.3	Configuration	12
2.13	Package open-xchange-oxaas-mail-ws	12
2.13.1	General Functionality	13

2.13.2 Installation	13
2.13.3 Configuration	13
A Configuration Files	13

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:

```
First candidate for the 1.11.3 release
```

1.3 Install Package Repository

This delivery is part of a restricted software repository:

<https://software.open-xchange.com/components/cloud-plugins/stable/1.11.3/DebianBuster>
<https://software.open-xchange.com/components/cloud-plugins/stable/1.11.3/DebianStretch>
<https://software.open-xchange.com/components/cloud-plugins/stable/1.11.3/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 [27](#))

1.5 Build Dependencies

This delivery was build and tested with following dependencies:

```
AppSuite:node-10,plugins-1.6.3-rev2,frontend-7.10.5-rev7,
backend-7.10.5-rev7
```

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: 1.11.3-1

Type: OX Middleware Plugin

Depends on:

```
open-xchange-cloudplugins (<<1.11.4)
open-xchange-cloudplugins (>=1.11.3)
open-xchange-core (<<7.10.6)
open-xchange-core (>=7.10.4)
open-xchange-plugins-antiphishing (<<1.7.0)
open-xchange-plugins-antiphishing (>=1.6.2)
open-xchange-plugins-antiphishing-vadesecure (<<1.7.0)
open-xchange-plugins-antiphishing-vadesecure (>=1.6.2)
```

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 [13](#))

2.2 Package open-xchange-cloudplugins-blackwhitelist-ldap

Implementation of blacklist whitelist for cloudplugins within LDAP

Version: 1.11.3-1

Type: OX Middleware Plugin

Depends on:

```
open-xchange-cloudplugins (<<1.11.4)
open-xchange-cloudplugins (>=1.11.3)
open-xchange-core (<<7.10.6)
open-xchange-core (>=7.10.4)
open-xchange-plugins-blackwhitelist (<<1.7.0)
open-xchange-plugins-blackwhitelist (>=1.6.3)
```

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 [14](#))

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: 1.11.3-1

Type: OX Middleware Plugin

Depends on:

```
open-xchange-cloudplugins (<<1.11.4)
open-xchange-cloudplugins (>=1.11.3)
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 [14](#))

2.4 Package open-xchange-cloudplugins-keycloak

Keycloak connector This package contains a keycloak connection handler to retrieve access and refresh tokens.

Version: 1.11.3-1

Type: OX Middleware Plugin

Depends on:

```
open-xchange-cloudplugins (<<1.11.4)
open-xchange-cloudplugins (>=1.11.3)
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 [16](#))

2.5 Package open-xchange-cloudplugins-loginproxy-ui

Implements a 2-step login flow required during migrations

Version: 1.11.3-1

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: 1.11.3-1

Type: OX Middleware Plugin

Depends on:

```
open-xchange-cloudplugins (<<1.11.4)
open-xchange-cloudplugins (>=1.11.3)
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 [16](#))
 /opt/open-xchange/etc/cloudplugins-loginproxy-ws.properties (page [17](#))

2.7 Package open-xchange-cloudplugins-mailfilter

CloudPlugins MailFilter Utilities This package implements a mailfilter interceptor driver framework and provides some useful drivers.

Version: 1.11.3-1

Type: OX Middleware Plugin

Depends on:

```
open-xchange-cloudplugins (<<1.11.4)
open-xchange-cloudplugins (>=1.11.3)
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 Cloud-ManagementCassandraService the autoforward status and how many redirects exist.
 - RedirectBlacklistDriver - supports Config Cascade. Blocks users from creating only auto-forward 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 [18](#))

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: 1.11.3-1

Type: OX Middleware Plugin

Depends on:

```
open-xchange-cloudplugins (<<1.11.4)
open-xchange-cloudplugins (>=1.11.3)
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 [20](#))

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: 1.11.3-1

Type: OX Middleware Plugin

Depends on:

```
open-xchange-cloudplugins (<<1.11.4)
open-xchange-cloudplugins (>=1.11.3)
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-oxaas-alias

OXaaS alias bundle This package implements OXaaS alias handling.

Version: 1.11.3-1

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)
```

2.10.1 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.

2.10.2 Installation

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

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

2.10.3 Configuration

For details, please see appendix [A](#)

/opt/open-xchange/etc/oxaas-alias.properties (page [25](#))

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

OXaaS notification mail servlet bundle

Version: 1.11.3-1

Type: OX Middleware Plugin

Depends on:

```
open-xchange-cloudplugins (<<1.11.4)
open-xchange-cloudplugins (>=1.11.3)
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)
```

2.11.1 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

2.11.2 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}/

```



2.11.3 Installation

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

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

2.11.4 Configuration

For details, please see appendix [A](#)

`/opt/open-xchange/etc/oxaas-mail-notification-templates.properties` (page [25](#))

`/opt/open-xchange/etc/oxaas-drive-quota-notification.properties` (page [26](#))

2.11.5 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

```

2.12 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: 1.11.3-1

Type: OX Middleware Plugin

Depends on:

```
open-xchange-cloudplugins (<<1.11.4)
open-xchange-cloudplugins (>=1.11.3)
open-xchange-core (<<7.10.6)
open-xchange-core (>=7.10.4)
open-xchange-imap (<<7.10.6)
open-xchange-imap (>=7.10.4)
```

2.12.1 General Functionality

API to fetch 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`

2.12.2 Installation

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

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

2.12.3 Configuration

For details, please see appendix [A](#)

`/opt/open-xchange/etc/oxaas-mail-unread.properties` (page [26](#))

2.13 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: 1.11.3-1

Type: OX Middleware Plugin

Depends on:

```
open-xchange-cloudplugins (<<1.11.4)
open-xchange-cloudplugins (>=1.11.3)
open-xchange-core (<<7.10.6)
open-xchange-core (>=7.10.4)
open-xchange-imap (<<7.10.6)
open-xchange-imap (>=7.10.4)
```

2.13.1 General Functionality

This plugin provides a middleware restfull API to retrieve details of customer data. 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

2.13.2 Installation

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

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

2.13.3 Configuration

For details, please see appendix [A](#)

/opt/open-xchange/etc/oxaas-mail.properties (page [26](#))

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

```

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

```

1 # Defines whether the forward REST API should be enabled or not.
2 #
3 # This parameter is optional and defaults to "false" (disabled).
4 #
5 # Example:
6 # com.openexchange.cloudplugins.admin.forwards.ws.enabled=true
7 com.openexchange.cloudplugins.admin.forwards.ws.enabled=false

```

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

```

1 # The token endpoint identified by the client
2 #
3 # Must be set for each client, default value: ""
4 #
5 # Example:
6 # com.openexchange.cloudplugins.keycloak.oauth.exampleClient.tokenEndpoint=http://
7 # localhost:8080/auth/realms/demo/protocol/openid-connect/token
8 com.openexchange.cloudplugins.keycloak.oauth.[client].tokenEndpoint=
9
10 # The clientId, if left empty, no clientId will be used
11 #
12 # Optional, default value: ""
13 #
14 # Example:
15 # com.openexchange.cloudplugins.keycloak.oauth.exampleClient.clientId=customerClient
16 com.openexchange.cloudplugins.keycloak.oauth.[client].clientId=
17
18 # The default-client used for the CloudAuthenticationDriver
19 com.openexchange.cloudplugins.keycloak.oauth.default-client.clientId=
20
21 # The client secret. Must be provided if clientId is set.
22 #
23 # Optional, default value: ""
24 #
25 # Example:
26 # com.openexchange.cloudplugins.keycloak.oauth.exampleClient.clientSecret=123123
27 com.openexchange.cloudplugins.keycloak.oauth.[client].clientSecret=
28
29 # The default-client secret used for the CloudAuthenticationDriver
30 com.openexchange.cloudplugins.keycloak.oauth.default-client.clientSecret=
31
32 # Max connections
33 #
34 # Optional, default value: 100
35 com.openexchange.cloudplugins.keycloak.oauth.maxConnections=100
36
37 # Max connections per host

```



```

37 #
38 # Optional, default value: 100
39 com.openexchange.cloudplugins.keycloak.oauth.maxConnectionsPerHost=100
40
41 # Connection timeout in ms
42 #
43 # Optional, default value in ms: 3000
44 com.openexchange.cloudplugins.keycloak.oauth.connectionTimeout=3000
45
46 # Socket read timeout in ms
47 #
48 # Optional, default value in ms: 6000
49 com.openexchange.cloudplugins.keycloak.oauth.socketReadTimeout=6000
50
51 # Refresh time in ms before expiry date
52 #
53 # Optional, default value is ms: 60000
54 com.openexchange.cloudplugins.keycloak.oauth.refreshTime=60000
55
56 # Enables the keycloak cloud-plugins CloudAuthenticationDriver.
57 # If either of the following properties is set, it is not required to enable this property
58 #     com.openexchange.mail.authType=xoauth2 or oauthbearer
59 #     com.openexchange.mail.filter.preferredSaslMech=OAUTHBEARER or XOAUTH2
60 #
61 # Default: false
62 com.openexchange.cloudplugins.keycloak.oauth.authentication.enabled=false
63
64 # Comma separated blacklist of hostnames that should not be handled by the keycloak
65 #     CloudAuthenticationDriver
66 # Default: <empty>
67 com.openexchange.cloudplugins.keycloak.oauth.authentication.blocklist=
68
69 # Sets the client identifier for the CloudAuthenticationDriver
70 # Internally will use the value "default-client" as a fallback
71 #
72 # Default: ""
73 com.openexchange.cloudplugins.keycloak.oauth.authentication.client=default-client
74
75 # One may set different clients on a brand base
76 #
77 # com.openexchange.cloudplugins.keycloak.oauth.authentication.client.<brand>=<client>
78 # Example:
79 # com.openexchange.cloudplugins.keycloak.oauth.authentication.client.brand1=cloudplugins-
80 #     keycloak-custom-client
81 # com.openexchange.cloudplugins.keycloak.oauth.authentication.client.brand2=brand-specific
82 #     -client
83
84 # Sets the response identifier for the CloudAuthenticationDriver
85 #
86 # Special case: oxUserId@oxContextId enables lookup for the two keys oxUserId and
87 #     oxContextId
88 #     Afterwards they are again handled as oxUserId@oxContextId
89 #
90 # Default: "preferred_username"
91 com.openexchange.cloudplugins.keycloak.oauth.authentication.response.identifier=
92     preferred_username
93
94 # One may set different response identifiers on a brand base
95 #
96 # com.openexchange.cloudplugins.keycloak.oauth.authentication.response.identifier.<brand
97 #     >=<client>
98 # Example:
99 #
100 # com.openexchange.cloudplugins.keycloak.oauth.authentication.response.identifier.brand1=
101     email
102 # com.openexchange.cloudplugins.keycloak.oauth.authentication.response.identifier.brand2=
103     alias
104
105 # Configure the LDAP lookup method to find users using their logins.
106 # It is the method that is used by default when there is no brand specific
107 # configuration setting).

```

```

101 #
102 # Optional, defaults to "uid".
103 #
104 # Possible values:
105 # uid
106 # attempts to find users by matching their login against the uid attribute.
107 # email
108 # attempts to find users by matching their login against the alias attribute.
109 # auto
110 # when the login contains a "@", the "email" method is used and when not,
111 # 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|
127 # auto|uid-or-email|userid-contextid>
128 #
129 # For the list of possible values, please consult the documentation for
130 # com.openexchange.cloudplugins.keycloak.oauth.authentication.uid.mode
131 #
132 # Optional, defaults to falling back to the method configured in
133 # com.openexchange.cloudplugins.keycloak.oauth.authentication.uid.mode
134 #
135 # Note that this only applies to the default authentication service driver.
136 # If there is a custom implementation that is used for a given brand, its
137 # behavior is not influenced by these properties.
138 #
139 # Example:
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 #
13 # Optional, default value: 300000
14 #
15 # Example:
16 # com.openexchange.cloudplugins.login.proxy.maxRateTimeWindow=60000
17 com.openexchange.cloudplugins.login.proxy.maxRateTimeWindow=300000
18
19 # Strategy to use for reacting to the inability to access the API for a given source
20 # IP address due to surpassing the maxRequestsPerSecond rate.
21 #
22 # Format: it must be one of:
23 # * fail-fast
24 # * block
25 # * timeout:...
26 #
27 # fail-fast
28 #   if the rate limit is exceeded, the API will respond with a 403 Forbidden
29 # block
30 #   if the rate limit is exceeded, the API will block infinitely until the rate limit
31 #   allows for another request to be performed
32 # timeout:...
33 #   block until the specified timeout is reached, after which the API responds with a
34 #   403 Forbidden
35 #   The value after "timeout:" consists of a number followed by a time unit, examples:
36 #   - timeout:400s ---> 400 seconds
37 #   - timeout:1m -----> 1 minute
38 #   - timeout:2000ms -> 2000 milliseconds
39 #
40 # Optional, default value: timeout:5s
41 #
42 # Example:
43 # com.openexchange.cloudplugins.login.proxy.strategy=timeout:10s
44 com.openexchange.cloudplugins.login.proxy.strategy=timeout:5s
45
46 # The default URL to redirect to when the user is not marked as not migrated
47 # and the identifier of the user is not mapped in cloudplugins-loginproxy-forward.yaml
48 # and the brand does not have a default redirect in cloudplugins-loginproxy-forward.yaml
49 #
50 # Example:
51 # com.openexchange.cloudplugins.login.proxy.default.redirect=https://example.com/mail
52 # Default: not set
53 com.openexchange.cloudplugins.login.proxy.default.redirect=

```

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

```

1 # This is the CloudPlugins MailFilterInterceptorDriver configuration
2 #
3 # Enable drivers by adding at least one brand in the brands property for that driver
4 # on the server level configuration. If no brand exists, the driver will not be registered
5 #
6 # Some drivers may also have additional configurations
7 #
8
9 ##### Driver Brand Lists #####
10 # Comma delimited lists
11
12 # Brands that the RedirectStatusDriver should be enabled for
13 #

```

```

14 # Optional - default is no brands
15 com.openexchange.cloudplugins.mailfilter.intercept.drivers.redirect.status.driver.brands=
16
17 # Brands that the RedirectBlacklistDriver should be enabled for
18 #
19 # Optional - default is no brands
20 com.openexchange.cloudplugins.mailfilter.intercept.drivers.redirect.blacklist.driver.
    brands=
21
22 ##### End Driver Brand Lists #####
23
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 #
32 # This should be used to set different configurations per brand or an even lower level.
33 # This property is NOT config cascade aware as it is used to control use of it.
34 # Even the driver brand list property can be config cascade if this is enabled which would
    be useful
35 # to enable it for a brand, but disable it for some users
36 #
37 # Optional - default is false
38 com.openexchange.cloudplugins.mailfilter.intercept.drivers.redirect.blacklist.driver.
    configcascade.enable=false
39 #
40 # The comma+space delimited list of regular expressions that are blacklisted for mail
    filter redirects.
41 # Java regular expressions are supported here, so non regex characters must be escaped.
42 # Example: abuse@.*, spam@domain\.com <-- '.' has been escaped to match only '.' and not
    any char
43 # See for regex constructs: https://docs.oracle.com/javase/7/docs/api/java/util/regex/
    Pattern.html
44 # WARNING: You must use ", " (comma and a space) as the separator to separate the regexs
45 #
46 # Optional - default is empty which should only be left if this driver is not used
47 com.openexchange.cloudplugins.mailfilter.intercept.drivers.redirect.blacklist.driver.
    blacklist=
48 #
49 # Set to true to only blacklist true autoforward rules which are defined by having the "
    autoforward" flag.
50 # If set to false, then all redirect rules will be checked for the blacklist addresses
51 #
52 # Optional - default is true
53 com.openexchange.cloudplugins.mailfilter.intercept.drivers.redirect.blacklist.driver.
    autoforward.only=true
54 #
55 ### End Redirect Blacklist Driver ###
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 !!
23 #   The list of possible OI DCBackends is identified by the property
24 #   com.openexchange.cloudplugins.oidc.enabled.<identifier>
25 #
26 # Example:
27 #   com.openexchange.cloudplugins.oidc.enabled=true
28 #   com.openexchange.cloudplugins.oidc.enabled.myIdentifier=true
29 #   com.openexchange.cloudplugins.oidc.enabled.moreIdentifier=true
30 #
31 #   It is possible to disable certain OI DCBackends by configuration
32 #
33 #   com.openexchange.cloudplugins.oidc.enabled is also valid and will be used as an empty
    # identifier
34 #   An empty identifier will use all properties set in this config file.
35 #
36 # com.openexchange.cloudplugins.oidc.enabled.<identifier>=true
37 com.openexchange.cloudplugins.oidc.enabled=false
38
39 ### OI DC Specific configuration
40 #####
41 # All properties mentioned at https://documentation.open-xchange.com/components/middleware
    # /config/7.10.2/#mode=features&feature=OpenID
42 # can be assigned to each OI DCbackend.
43 #
44 # !! NOTE !!
45 #   The default prefix is not 'com.openexchange.oidc'
46 #   'com.openexchange.cloudplugins.oidc'
47 #   is used instead meaning that there is an additional
48 #   'cloudplugins' in between to differentiate from the general oidc configuration.
49 #
50 # Example:
51 #   com.openexchange.oidc.clientId will not be evaluated
52 #   com.openexchange.oidc.cloudplugins.clientId is the correct default key
53 #
54 # The id inside the jwt token response which holds the userinformation
55 #
56 # The search for the id is done in the attributeStatement if nothing is configured
57 # possible configuration values are:
58 #   <not_set>      // the subject is used
59 #   claim:key      // a claim with the identifier <key> is used
60 #   key            // a claim with the identifier <key> is used
61 #
62 # In any case, the id must match the uid used to provision the user
63 # com.openexchange.cloudplugins.oidc.<identifier>.id=
64 com.openexchange.cloudplugins.oidc.id=
65
66 # The ldap lookup used by this OI DCBackend
67 #
68 # Configure the LDAP lookup method to find users using their identifiers.
69 #
70 #
71 # Possible values:
72 # uid
73 #   attempts to find users by matching their login against the uid attribute.
74 # email
75 #   attempts to find users by matching their login against the alias attribute.
76 # auto
77 #   when the login contains a "@", the "email" method is used and when not,
78 #   the "uid" method is used
79 # uid-or-email
80 #   attempts to find users by matching their login against the uid and the alias
81 #   attributes (either may match)

```

```

82 #
83 # This property is optional.
84 # Default: uid
85 # com.openexchange.cloudplugins.oidc.<identifier>.ldapLookup=
86 com.openexchange.cloudplugins.oidc.ldapLookup=
87
88
89 # The brand to use for OXaaS LDAP authentication operations.
90 # Uses the host name when empty or not set.
91 #
92 # This property is mandatory.
93 # Default: <empty>
94 # com.openexchange.cloudplugins.oidc.<identifier>.brand=
95 com.openexchange.cloudplugins.oidc.brand=
96
97 # The authentication method used for the token endpoint.
98 # Can be a selection of:
99 #   basic
100 #   post
101 #
102 # This property is optional.
103 # Default: basic if not set
104 # com.openexchange.cloudplugins.oidc.<identifier>.tokenAuth=
105 com.openexchange.cloudplugins.oidc.tokenAuth=
106
107 # This backends servlet path, which is appended to the default /oidc/ path.
108 #
109 # This property is optional.
110 # Default: <empty>
111 # com.openexchange.cloudplugins.oidc.<identifier>.backendPath=
112 com.openexchange.cloudplugins.oidc.backendPath=
113
114 # List of hosts where that this OIDCBackend is responsible for
115 # if all is present, this is responsible for all hosts
116 #
117 # It is possible to control the backendPath with this property.
118 # Another way would be to set the backendPath within the as-config.yml.
119 # If set in as-config.yml, it must be set as oidcPath
120 # Default: <empty>
121 # com.openexchange.cloudplugins.oidc.<identifier>.hosts=
122 com.openexchange.cloudplugins.oidc.hosts=
123
124 # Set the redirect location for a failed authentication request if the request could not be
125 # identified or took too long
126 com.openexchange.cloudplugins.oidc.failureRedirect=
127
128 # Set the redirect location for all other authentication exceptions that may occur. This
129 # mainly targets issues with the token validation
130 com.openexchange.cloudplugins.oidc.authenticationFailedExceptionRedirect=
131
132 # Set the redirect location for logout exceptions.
133 com.openexchange.cloudplugins.oidc.logoutFailedExceptionRedirect=
134
135 # Set the redirect location for general exceptions in the middleware that could not be
136 # handled by either
137 # - failureRedirect
138 # - authenticationFailedExceptionRedirect
139 # - logoutFailedExceptionRedirect
140 # If only one endpoint should be defined for redirect, it is safe to only set
141 # responseExceptionRedirect
142 com.openexchange.cloudplugins.oidc.responseExceptionRedirect=

```

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

```

1 # The properties for cloud setup SAML bundle
2
3 ### General settings
4 #####

```

```

5 # Regex to validate host HTTP Header value
6 com.openexchange.cloudplugins.saml.host.regex=[0-9a-zA-Z.]*
7
8 # Regex to validate user name
9 com.openexchange.cloudplugins.saml.user.regex=[0-9a-zA-Z.@]*
10
11 # Base folder for the saml keystore files
12 # This property must be set if Java Security Manager is enabled
13 # It can't be set for individual identifiers
14 com.openexchange.cloudplugins.saml.keyStoreBasePath=
15
16 ### Key-store/certificate settings
17 #####
18 # All properties below can also be assigned to an identifier by configuring them as
19 # com.openexchange.cloudplugins.saml.<identifier>.key
20 #
21 # If a property is not set for an identifier, the key without the identifier is used as a
  default
22 # !!Note !!
23 #   If a property is marked as optional, the default value for the optional case is used
  and not the general
24 #   optional value if that is set
25 #
26 # Example:
27 #   com.openexchange.cloudplugins.saml.example.id=someValue
28 #   com.openexchange.cloudplugins.saml.keyStore=testStore
29 #   com.openexchange.cloudplugins.saml.example.keyStore=
30 #   example keyStore => testStore
31 #
32 # Example2:
33 #   com.openexchange.cloudplugins.saml.example.id=someValue
34 #   com.openexchange.cloudplugins.saml.brand=defaultBrand
35 #   com.openexchange.cloudplugins.saml.example.brand=
36 #   example brand (for ldap selection) => <empty>, will use the domainName of the request
37 #
38 # !! Note !!
39 #   The list of possible SAMLBackends is identified by the property
40 #   com.openexchange.cloudplugins.saml.<identifier>.id
41 #   If there is no property for the id(s) set, no SAMLBackend will be started.
42 #   com.openexchange.cloudplugins.saml.id is also valid and will be used as an empty
  identifier
43 #   An empty identifier will use all properties set in this config file.
44 #
45 # The full path to a Java keystore containing the IdPs certificate.
46 #
47 # Default: <empty>
48 com.openexchange.cloudplugins.saml.keyStore=
49
50 # Password to open the keystore.
51 #
52 # Default: <empty>
53 com.openexchange.cloudplugins.saml.keyStorePass=
54
55 # The aliases of the IdP certificate entry within the above specified
56 # keystore. Split by ','. Multiple certs can be used in a rolling upgrade
57 # case at the customers location without the need to coordinate an upgrade.
58 #
59 # The support for multiple certs is only enabled on 7.10.1+ systems.
60 # A 7.10.0 system will only use the first certAlias
61 #
62 # Default: <empty>
63 com.openexchange.cloudplugins.saml.certAlias=
64
65 # The alias of the signingKey entry within the above specified
66 # keystore.
67 #
68 # Default: <empty>
69 com.openexchange.cloudplugins.saml.signingKeyAlias=
70
71 # The password of the signingKey entry within the above specified
72 # keystore.

```

```

73 #
74 # Default: <empty>
75 com.openexchange.cloudplugins.saml.signingKeyPassword=
76
77 # The alias of the decryptionKey entry within the above specified
78 # keystore.
79 #
80 # Default: <empty>
81 com.openexchange.cloudplugins.saml.decryptionKeyAlias=
82
83 # The password of the decryptionKey entry within the above specified
84 # keystore.
85 #
86 # Default: <empty>
87 com.openexchange.cloudplugins.saml.decryptionKeyPassword=
88
89 ### SAML Specific configuration
90 #####
91 # The id inside the saml response which holds the userinformation
92 #
93 # The search for the id is done in the attributeStatement if nothing is configured
94 # possible configuration values are:
95 #   key           // search is done in the attributeStatement with the key
96 #   attribute:key // search is done in the attributeStatement with the key
97 #   subject:nameID // the subject:NameId is used
98 #
99 # In any case, the id must match the uid used to provision the user
100 com.openexchange.cloudplugins.saml.id=
101
102 # The ldap lookup used by this SAMLBackend
103 #
104 # Configure the LDAP lookup method to find users using their identifiers.
105 #
106 #
107 # Possible values:
108 # uid
109 #   attempts to find users by matching their login against the uid attribute.
110 # email
111 #   attempts to find users by matching their login against the alias attribute.
112 # auto
113 #   when the login contains a "@", the "email" method is used and when not,
114 #   the "uid" method is used
115 # uid-or-email
116 #   attempts to find users by matching their login against the uid and the alias
117 #   attributes (either may match)
118 #
119 # This property is optional.
120 # Default: uid
121 com.openexchange.cloudplugins.saml.ldapLookup=
122
123 # URL of where the users are redirected after logout if single_logout is active
124 # Must only be set if enableSingleLogout is enabled
125 #
126 # Default: <empty>
127 com.openexchange.cloudplugins.saml.logout.redirect.url=
128
129 # The brand to use for OXaaS LDAP authentication operations.
130 # Uses the host name when empty or not set.
131 #
132 # This property is optional.
133 # Default: <empty>
134 com.openexchange.cloudplugins.saml.brand=
135
136 # The URL to redirect to in case the SAML back-end fails to look up the authenticated user
137 # When left empty or not set, an HTTP 500 error page is sent instead.
138 #
139 # This property is optional.
140 # Default: <empty>
141 com.openexchange.cloudplugins.saml.failure.redirect=
142
143 # The URL to redirect to in case the SAML back-end has an error, when the user logs out

```



```
144 # When left empty or not set, the value of com.openexchange.cloudplugins.saml.failure.  
    # redirect is used.  
145 #  
146 # Default: <empty>  
147 com.openexchange.cloudplugins.saml.logout.failure.redirect=  
148  
149 # The samlPath value required for the servlet alias  
150 # registered with '{prefix}/saml/{samlPath}/..' as servlet alias.  
151 #  
152 # This property is optional.  
153 # Default: <empty>  
154 com.openexchange.cloudplugins.saml.samlPath=  
155  
156 # Static redirect upon login or relogin  
157 #  
158 # This property is optional.  
159 # Default: <empty>  
160 com.openexchange.cloudplugins.saml.staticRedirect=  
161  
162 # Whether the SPs metadata XML shall be made available via HTTP. The according  
163 # servlet will then be available under 'http(s)://{hostname}/{prefix}/saml/metadata'.  
164 #  
165 # Default: false  
166 com.openexchange.cloudplugins.saml.enableMetadataService=false  
167  
168 # Whether the single logout profile is enabled.  
169 #  
170 # Default: false  
171 com.openexchange.cloudplugins.saml.enableSingleLogout=false  
172  
173 # Sets the entity ID of the service provider.  
174 #  
175 # This property is mandatory.  
176 # Default: <empty>  
177 com.openexchange.cloudplugins.saml.entityID=  
178  
179 # Sets the human-readable name of the service provider.  
180 #  
181 # This property is mandatory.  
182 # Default: <empty>  
183 com.openexchange.cloudplugins.saml.providerName=  
184  
185 # Sets the URL of the local assertion consumer service (ACS). This value is used within  
186 # authentication requests, compared against Destination attributes in IdP responses  
187 # and will be contained in the service providers metadata XML. The according endpoint  
188 # is always registered with '{prefix}/saml/{samlPath}/acs' as servlet alias.  
189 #  
190 # This property is mandatory.  
191 # Default: <empty>  
192 # Example: https://appsuite.example.com/appsuite/api/saml/{samlPath}/acs  
193 com.openexchange.cloudplugins.saml.acsURL=  
194  
195 # Sets the URL of the local single logout service. This value is compared against  
    # Destination  
196 # attributes in IdP responses and will be contained in the service providers metadata XML.  
197 # The according endpoint is always registered with '{prefix}/saml/{samlPath}/sls' as  
    # servlet alias.  
198 #  
199 # This property is mandatory if 'com.openexchange.cloudplugins.saml.enableSingleLogout' is  
    # 'true'.  
200 # Default: <empty>  
201 # Example: https://appsuite.example.com/appsuite/api/saml/{samlPath}/sls  
202 com.openexchange.cloudplugins.saml.slsURL=  
203  
204 # The binding via which logout responses shall be sent to the IdP on IdP-initiated single  
205 # logout flows. Must be 'http-redirect' or 'http-post'.  
206 #  
207 # This property is mandatory if 'com.openexchange.cloudplugins.saml.enableSingleLogout' is  
    # 'true'.  
208 # Default: http-redirect  
209 com.openexchange.cloudplugins.saml.logoutResponseBinding=http-redirect  
210
```

```
211 # The HTML template to use when logout responses are sent to the IdP via HTTP POST.
212 # The template must be located in '/opt/open-xchange/templates'.
213 #
214 # This property is mandatory if 'com.openexchange.cloudplugins.saml.enableSingleLogout' is
    'true'
215 # and 'com.openexchange.cloudplugins.saml.logoutResponseBinding' is set to 'http-post'.
216 # Default: saml.logout.response.html.tpl
217 com.openexchange.cloudplugins.saml.logoutResponseTemplate=saml.logout.response.html.tpl
218
219 # The entity ID of the IdP. It will be used to validate the 'Issuer' elements of SAML
    responses.
220 #
221 # This property is mandatory.
222 # Default: <empty>
223 com.openexchange.cloudplugins.saml.idpEntityID=
224
225 # The URL of the IdP endpoint where authentication requests are to be sent to.
226 #
227 # This property is mandatory.
228 # Default: <empty>
229 com.openexchange.cloudplugins.saml.idpAuthnURL=
230
231 # The URL of the IdP endpoint where logout requests are to be sent to.
232 #
233 # This property is mandatory if 'com.openexchange.cloudplugins.saml.enableSingleLogout' is
    'true'.
234 # Default: <empty>
235 com.openexchange.cloudplugins.saml.idpLogoutURL=
236
237 # It is possible to enable a special kind of auto login mechanism that allows user agents
    to
238 # re-use an existing OX session if it was created during the same browser session. If
    enabled,
239 # a special cookie will be set, which is linked to the OX session and bound to the browser
    sessions
240 # life time. The advantage of this mechanism is, that sessions are simply re-entered if
    the user
241 # refreshes his browser window. He is then also able to open more than one tab of OX App
    Suite
242 # at the same time. This mechanism can only re-use sticky sessions, i.e. it is mandatory
    that the
243 # requests are always routed to the same backend for a certain session.
244 #
245 # --- SECURITY WARNING ---
246 # Enabling this setting is not compliant to the SAML specification as it bypasses the IdP
    in
247 # certain cases. Additionally in scenarios where a public device is used, a foreign user
    might
248 # take over a formerly authenticated users session if that user forgets to log out and
    doesn't
249 # close his web browser (even if he closes the App Suite tab). As no login screen is
    displayed
250 # by OX in SAML environments, the user is even not able to decide, whether the application
    shall
251 # remember him or not.
252 #
253 # Default: false
254 com.openexchange.cloudplugins.saml.enableAutoLogin=false
255
256 # Whether unsolicited responses will be accepted or not.
257 #
258 # Default: true
259 com.openexchange.cloudplugins.saml.allowUnsolicitedResponses=true
260
261 # Whether SAML-specific auto-login is enabled, that uses the SessionIndex of the
    AuthnResponse
262 #
263 # Default: false
264 com.openexchange.cloudplugins.saml.enableSessionIndexAutoLogin=false
265
266 # List of hosts where that this SAMLBackend is responsible for
267 # if all is present, this SAMLBackend responsible for all hosts
```

```

268 #
269 # It is possible to control the samlPath with this property.
270 # Another way would be to set the samlPath within the as-config.yml.
271 # Default: <empty>
272 com.openexchange.cloudplugins.saml.hosts=

```

File 10 /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 should 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 user
38 # Default: 15
39 com.openexchange.oxaas.aliasquota=15

```

File 11 /opt/open-xchange/etc/oxaas-mail-notification-templates.properties

```

1 # Config cascade-aware property to control the prefix of the users templates
2 # For each prefix and each user configured percentage
3 com.openexchange.oxaas.mail.quota.notify.prefix=notify.oxaas.over.quota
4
5 # Config cascade-aware property to control the prefix of the users templates
6 # For each prefix and each user configured percentage
7 com.openexchange.oxaas.mail.welcome.mail.notify.prefix=notify.oxaas.welcome.mail
8
9 # Config cascade-aware property to control the prefix of the users templates
10 # For each prefix and each user configured percentage
11 com.openexchange.oxaas.mail.removed.sent.spam.notify.prefix=notify.oxaas.disable.sent.spam

```

File 12 /opt/open-xchange/etc/oxaas-drive-quota-notification.properties

```
1 # Config-cascade aware setting to control the quotas that should be monitored
2 com.openexchange.oxaas.mail.quota.drive.quotas=90,100
3
4 # Config-cascade aware setting to control if the admin should also receive a mail, in case
5   the filestore is context-wide
6 com.openexchange.oxaas.mail.quota.drive.updateAdmin=false
7
8 # Config-cascade aware setting to control how often a mail should be sent
9 # Default is 86400 (1 day)
10 # Set to 0 to ignore that and always send a new mail
11 com.openexchange.oxaas.mail.quota.drive.mail.seconds=86400
```

File 13 /opt/open-xchange/etc/oxaas-mail-unread.properties

```
1 # Value holding the usernames for basic authentication
2 # must be the username for basic auth split by ,
3 # e.g hosterone,hostertwo
4 com.openexchange.oxaas.mail.unread.ws.basic.usernames=
5
6 # Setting to control basic auth username
7 # example would be com.openexchange.oxaas.mail.unread.ws.basic.hosterone.brand=
8   internalBrandForhosterone
9 #com.openexchange.oxaas.mail.unread.ws.basic.[username].brand=
10
11 # Setting to control basic auth password
12 # example would be com.openexchange.oxaas.mail.unread.ws.basic.hosterone.password=
13   verySecretPassword
14 #com.openexchange.oxaas.mail.unread.ws.basic.[username].password=
```

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

```
1 # Value holding the usernames for basic authentication
2 # must be the username for basic auth split by ,
3 # e.g hosterone,hostertwo
4 com.openexchange.oxaas.mail.ws.basic.usernames=
5
6 # Setting to optimize the fetching of recentMessages
7 # If set to true, the virtual/all folder will be queried
8 # If set to false, the calculation is done in the middleware
9 # config-cascade aware
10 com.openexchange.oxaas.mail.ws.recentMessagesFromVirtualAll=false
11
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=
18   internalBrandForhosterone
19 #com.openexchange.oxaas.mail.ws.basic.[username].brand=
```

File 15 /opt/open-xchange/etc/as-config.yml

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

```
4 loginProxy: true
```