



OX Cloud Plugins  
**Release Notes for Release 1.9.1**  
2019-10-16

## Copyright notice

---

©2019 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

<b>1</b>	<b>General Information</b>	<b>3</b>
1.1	Warnings	3
1.2	Delivery Comment	3
1.3	Install Package Repository	3
1.4	Build Dependencies	4
1.5	Notice	4
<b>2</b>	<b>Shipped Product and Version</b>	<b>4</b>
2.1	Package open-xchange-cloudplugins	4
2.1.1	General Functionality	4
2.1.2	Admin Plugins	5
2.1.2.1	SOAP API	5
2.1.2.2	Admin REST API	5
2.1.3	Authentication Plugin	5
2.1.4	Masterauth Servlet	5
2.1.5	Cassandra	6
2.1.6	Dovecot	6
2.1.7	Mailmapping	6
2.1.8	LDAP Management	6
2.1.8.1	LDAP structure	7
2.1.9	Nginx Servlet	7
2.1.10	Cloud Report	7
2.1.10.1	Requirements	7
2.1.10.2	Report Types	7
2.1.10.3	Usage	8
2.1.10.4	Data Format and Storage	8
2.1.10.5	TKG112 Data Description	10
2.1.10.6	Metrics Data Description	10
2.1.11	Unified Quota	12
2.1.12	Passwordchange	12
2.1.13	Installation	12
2.1.14	Configuration	12
2.2	Package open-xchange-cloudplugins-blackwhitelist-ldap	12
2.2.1	Installation	12
2.2.2	Configuration	13
2.3	Package open-xchange-cloudplugins-forwards-ws	13
2.3.1	General Functionality	13
2.3.2	Installation	13
2.3.3	Configuration	13
2.4	Package open-xchange-cloudplugins-keycloak	14
2.4.1	General Functionality	14
2.4.2	Installation	14
2.4.3	Configuration	14
2.5	Package open-xchange-cloudplugins-mailfilter	14
2.5.1	General Functionality	15
2.5.2	Installation	15
2.5.3	Configuration	15
2.6	Package open-xchange-cloudplugins-oidc	15
2.6.1	General Functionality	16
2.6.2	Installation	16
2.6.3	Configuration	16
2.7	Package open-xchange-cloudplugins-saml	16
2.7.1	General Functionality	16
2.7.2	Installation	16
2.7.3	Configuration	16
2.8	Package open-xchange-oxaas-alias	17

2.8.1	General Functionality . . . . .	17
2.8.2	Installation . . . . .	17
2.8.3	Configuration . . . . .	17
2.9	Package open-xchange-oxaas-mail-notify-ws . . . . .	17
2.9.1	General Functionality . . . . .	18
2.9.2	REST API . . . . .	18
2.9.3	Installation . . . . .	18
2.9.4	Configuration . . . . .	18
2.9.5	Templates . . . . .	19
2.10	Package open-xchange-oxaas-mail-unread-ws . . . . .	19
2.10.1	General Functionality . . . . .	19
2.10.2	Installation . . . . .	19
2.10.3	Configuration . . . . .	19
2.11	Package open-xchange-oxaas-mail-ws . . . . .	20
2.11.1	General Functionality . . . . .	20
2.11.2	Installation . . . . .	20
2.11.3	Configuration . . . . .	20
<b>3</b>	<b>Changes relevant for Operators</b>	<b>20</b>
3.1	Changes of Configuration Files . . . . .	20
3.2	Changes of Behavior . . . . .	21
<b>4</b>	<b>Tests</b>	<b>22</b>
4.1	Test Report . . . . .	22
<b>A</b>	<b>Configuration Files</b>	<b>24</b>

## 1 General Information

### 1.1 Warnings

#### Warning

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

#### Warning

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

#### 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:

```
Second RC of 1.9.1
```

### 1.3 Install Package Repository

This delivery is part of a public software repository:

```
https://software.open-xchange.com/components/cloud-plugins/stable/1.9.1/DebianJessie
https://software.open-xchange.com/components/cloud-plugins/stable/1.9.1/DebianStretch
https://software.open-xchange.com/components/cloud-plugins/stable/1.9.1/RHEL6
https://software.open-xchange.com/components/cloud-plugins/stable/1.9.1/RHEL7
```

Licensed customers should also configure a restricted software updates repositories by using their credentials:

```
https://software.open-xchange.com/components/cloud-plugins/updates/1.9.1/DebianJessie
https://software.open-xchange.com/components/cloud-plugins/updates/1.9.1/DebianStretch
https://software.open-xchange.com/components/cloud-plugins/updates/1.9.1/RHEL6
https://software.open-xchange.com/components/cloud-plugins/updates/1.9.1/RHEL7
```

## 1.4 Build Dependencies

This delivery was build and tested with following dependencies:

```
plugins-1.4.4-rev7,frontend-7.10.0-rev29
```

## 1.5 Notice



### Info

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

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

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

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

## 2 Shipped Product and Version

### 2.1 Package open-xchange-cloudplugins

The Open-Xchange cloud plugin bundles

Version: 1.9.1-2

Type: OX Middleware Plugin

Depends on:

```
open-xchange-admin-reseller (<<7.10.3)
open-xchange-admin-soap-reseller (>=7.10.0)
open-xchange-cassandra (<<7.10.3)
open-xchange-cassandra (>=7.10.0)
open-xchange-mailfilter (<<7.10.3)
open-xchange-mailfilter (>=7.10.0)
open-xchange-rest (<<7.10.3)
open-xchange-rest (>=7.10.0)
```

Conflicts with:

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

#### 2.1.1 General Functionality

The package open-xchange-cloudplugins contains a set of bundles to manage an integrated platform consisting of OX App Suite components and dovecot. It uses some additional software components in order to do that.

- openldap to store information for mail routing used by dovecot and postfix and to act as authentication source
- postfix as mail server
- nginx to act as a proxy for http, imap, pop3 and smtp
- cassandra to store data that often changes like last login attempts, etc.

The package itself contains some OSGi bundles explained in the following sections and the file cloudplugins.properties contain configurations shared among each other.

## 2.1.2 Admin Plugins

Those plugins extend the OX provisioning capabilities. They maintain the data required into the openldap server to do mail routing and authentication using the [2.1.8 LDAP Management](#) functionality. Whenever a context or user is created, deleted or changed, the corresponding data in the ldap server is also updated.

```
com.openexchange.admin.cloudplugins
com.openexchange.admin.cloudplugins.console
```

### 2.1.2.1 SOAP API

Also in these bundles, there's another SOAP API providing cloud-plugins specific methods. Please see for further details the [OXaaS SOAP API Documentation](#).

### 2.1.2.2 Admin REST API

Starting with release 1.6.3, there's now also a REST API, check <https://documentation.open-xchange.com> for a link.



#### Info

Note that in order for this API to be accessible, you need to add an entry like ProxyPass /oxaas balancer://oxcluster/oxaas to your proxy\_http.conf.

## 2.1.3 Authentication Plugin

This plugin authenticates against the ldap server. To determine the user it needs to know the brand the user is belonging to. This is done using a configurable HTTP host header. This host header is added by the nginx proxy which sits in front of the ox middleware. Please see corresponding file cloudplugins-authentication.properties for configuration details.

```
com.openexchange.authentication.cloudplugins
```

## 2.1.4 Masterauth Servlet

This servlet allows to create an ox http session on behalf of a configurable master login and password without knowing the individual users login and password.

```
com.openexchange.cloudplugins.api.masterauth
```

This servlet provides the following API call which returns a valid OX session.

```
GET /api/oxaas/masterauth/brand/<brand>/context/<contextid>/user/<userid>
```

The following entry must be added to the apache proxy configuration:

```
ProxyPass /api/oxaas balancer://oxcluster/api/oxaas
```

The request has to provide a X-AUTHENTICATION header containing the value of

```
Base64( HMAC-SHA1( brand-auth-Key, UTF-8-Encoding-Of( StringToSign ) ) );
```

```
StringToSign = brand " " +
contextid + " " +
userid;
```

*brand-auth-key* is the value of the ldap nginxAuthKey Attribute of the brand entry. In addition to that, the requestor has to implement HTTP Basic auth using a configured master login and password. How to generate the X-AUTHENTICATION header with perl:

```
perl -MMIME::Base64 -MDigest::HMAC_SHA1=hmac_sha1
-e 'print encode_base64(hmac_sha1("example.com 24 3","secret"))." ;"'
```

How to test with wget:

```
wget -dv --user=admin --password=secret
--header='X-AUTHENTICATION: 6cmrSTcWCcyOV7mzkSgHdbrk8RI='
http://example.com/api/oxaas/masterauth/brand/example.com/context/24/user/3 -O -
```

The `cloudplugins-master-auth-servlet.properties` configuration file belongs to this servlet.

### 2.1.5 Cassandra

This bundle utilizes the `cassandra` bundle from the `ox` middleware to read and write data from/to a `cassandra` cluster.

```
com.openexchange.cloudplugins.cassandra
```

As of now, the following data structures have to be created in order to use this bundle.

```
1 $ cqlsh
2
3 create keyspace ox WITH REPLICATION = { 'class' : 'SimpleStrategy', 'replication_factor' :
4     1 };
5 use ox;
6 CREATE TYPE login_info ( login_time timestamp, ip_address text);
7 CREATE TABLE logins (ox_id text PRIMARY KEY, brand text, logins map<text, frozen<
8     login_info>> );
9 CREATE TABLE failure_logins (ox_id text PRIMARY KEY, brand text, login_errors map<text,
10    int>);
11 CREATE TABLE alias_log ( alias text PRIMARY KEY, brand text, creation_date timestamp,
12    deletion_date timestamp, ox_id text );
13 CREATE TABLE quota_usage ( ox_id text, type text, usage bigint, count bigint, primary key
14    ((ox_id), type));
```



The complete bundle can be turned off and some functionality must be configured per brand. See corresponding configuration file `cloudplugins-cassandra.properties`.

### 2.1.6 Dovecot

This is an interface to the `doveadm` REST API of `dovecot`. Right now it only implements querying the mail quota usage of users.

```
com.openexchange.cloudplugins.dovecot
```

The `doveadm-config.properties` configuration file belongs to this interface.

### 2.1.7 Mailmapping

The mail mapping is required to integrate with `OX Guard`. It resolves an email address into a context and userid.

```
com.openexchange.cloudplugins.mailmapping
```

### 2.1.8 LDAP Management

This provides methods to maintain data in the `LDAP` server.



```
com.openexchange.cloudplugins.management
```

### 2.1.8.1 LDAP structure

The ldap schema used with these bundles can be found in the `ldap` folder within this git repository. The ldap tree consists of three main branches:

- 1. The brand tree contains the brand accounts with all users belonging to each brand below.
- 2. The configuration tree containing configuration entries like mailstores, mailservers, etc.
- 3. The context tree containing all contexts of all brands in the entire system.

A brand is the same as a subadmin in the ox reseller bundle. This reseller bundle is a requirement to run the cloud-plugins environment. Due to the fact that all users within a brand are in the tree below a brand, user logins must not be unique within contexts as it is usually in an open-xchange environment, they must be unique within each brand. For details about the reseller bundle please see the [Reseller Bundle Documentation](#).

### 2.1.9 Nginx Servlet

This provides a servlet used by Nginx to authenticate external IMAP, POP and SMTP users against the ox cloud-plugins scheme.

```
com.openexchange.cloudplugins.nginx.auth.servlet
```

Where users directly using OX webmail are authenticated using the [2.1.3 Authentication Plugin](#), external IMAP, POP and SMTP logins must also be mapped from the internal `uid@contextid` representation to a login string the corresponding brand prefers. This might be an email address, a phone number, or whatever else. Nginx acts as a IMAP, POP and SMTP proxy in front of dovecot and uses the nginx auth servlet as an authentication and transformation source to provide dovecot with the internal login id after it successfully authenticated the user. See corresponding configuration file `nginx-auth-servlet.properties`.

### 2.1.10 Cloud Report

This is a central tool to get service usage informations on user level. Therefore the administrator has different options to generate this report, which are explained later. The report procession is designed to be highly efficient in regard of memory and cpu usage. If not configured otherwise, the used resources should never interfere with the processes of the operating system. While in procession, parts of the report are stored on hdd, merged into the resulting report and deleted, when the report is done. The report is processing each relevant schema in its own thread and all schemas in parallel for maximum speed. See corresponding configuration file `cloudplugins_report.properties`.

```
com.openexchange.cloudplugins.report
```

#### 2.1.10.1 Requirements

The report loads data from OX-DB as well as cassandra and LDAP storage. If no cassandra or OX-DB connection can be established, the report will not start. Without a valid LDAP connection, errors will be logged inside the report.

#### 2.1.10.2 Report Types

Currently, there are two report types.

- Metrics - The original cloud-plugins report which provides user usage information in JSON.
- TKG112 - Provides user alias information in CSV.

These report types are described further below.

### 2.1.10.3 Usage

In general, there can be only one report processed at a time. A second report will be denied and the ID of the current report will be displayed. This report can be aborted with the corresponding option and all stored data will be deleted. During procession, the current status can be requested and the user will be provided with all finished contexts compared to totals.

#### Warning

The processed contexts will only be updated when the schema is completely processed to evade potential bottlenecks because of Object locks.

```

1 Usage: createreport
2 -h,--help                Prints a help text
3   --environment          Show info about commandline environment
4   --nonl                 Remove all newlines (\n) from output
5   --responsetimeout <responsetimeout>
6                           response timeout in seconds for reading
7                           response from the backend (default 0s; infinite)
8 -A,--adminuser <adminuser> * master admin user name
9 -P,--adminpass <adminpass> * master admin password
10 -s,--timeframe-start <timeframe-start>
11                          Set the starting date of the desired
12                          timeframe in which the user logins are considered, format: dd.mm.yyyy.
13 -e,--timeframe-end <timeframe-end>
14                          Set the ending date of the desired
15                          timeframe in which the user logins are considered, in format: dd.mm.yyyy.
16 -a,--ignore-admin
17                          Ignore admins and dont show users of
18                          that category in the report.
19 -d,--show-drive-metrics  Add drive metrics for every user.
20 -m,--show-mail-metrics  Add mail metrics for every user.
21 -b,--single-brand <single-brand>
22                          Create a report for the selected brand
23                          only. Identified by the brand admins sid.
24 -t,--terminate-report
25                          Terminates the currently processed
26                          report uuid.
27 -p,--pending-reports
28                          Get the status of the pending report.
29
30 Entries marked with an asterisk (*) are mandatory.
31 Entries marked with an question mark (?) are mandatory depending on your
32 configuration.
33 Entries marked with a pipe (|) are mandatory for one another which means that
34 at least one of them must be set.

```



```

1 Usage: createtkg112report
2 -h,--help                Prints a help text
3   --environment          Show info about commandline environment
4   --nonl                 Remove all newlines (\n) from output
5   --responsetimeout <responsetimeout>
6                           response timeout in seconds for reading
7                           response from the backend (default 0s; infinite)
8 -A,--adminuser <adminuser> * master admin user name
9 -P,--adminpass <adminpass> * master admin password
10 -b,--single-brand <single-brand>
11                          * Brand to create report for. Identified
12                          by the brand admins sid.
13 -t,--terminate-report
14                          Terminates the currently processed
15                          report uuid.
16 -p,--pending-reports
17                          Get the status of the pending report.
18
19 Entries marked with an asterisk (*) are mandatory.
20 Entries marked with an question mark (?) are mandatory depending on your
21 configuration.
22 Entries marked with a pipe (|) are mandatory for one another which means that
23 at least one of them must be set.

```



### 2.1.10.4 Data Format and Storage

The Metrics Report data is stored in JSON format and looks like the example below.

```

1  {
2  "uuid":"28b3573af6734877a448ab614698d115",
3  "reportType":"OXaaS-report",
4  "timestamps":{
5      "start":1498477236283,
6      "stop":1498477276490
7  },
8  "version":{
9      "buildDate":"01.01.2017",
10     "version":"7.8.3"
11 },
12 "configs":{
13     "options":{
14         "show-drive-metrics":false,
15         "timeframe-start":1466941236283,
16         "show-mail-metrics":false,
17         "single-brand":0,
18         "ignore-admin":true,
19         "timeframe-end":1498477236283
20     }
21 },
22 "errors":{
23     "Exception-ID":"ERROR-ID Categories=ERROR Message='Message' exceptionID=Exception-ID
24     "
25 },
26 "oxaas":{
27     "capabilitySets":{
28         "283724704":"autologin,blacklist,...",...
29     },
30     "brandname":{
31         "totals":{
32             "quota" : 2621440000,
33             "quotaUsage" : 2522466,
34             "mailQuota" : 45365,
35             "mailQuotaUsage" : 0
36         },
37         "1":{
38             "3":{
39                 "capabilitySet":"283724704",
40                 "drive" : {
41                     "mime-types" : {
42                         "text/plain" : 5,
43                         "application/zip" : 2
44                     },
45                     "file-count-all-versions" : 7,
46                     "quota" : 104857600,
47                     "used-quota" : 2511077,
48                     "file-size-min" : 5,
49                     "file-count-latest-version" : 7,
50                     "file-size-avg" : 358725,
51                     "file-size-max" : 1255526
52                 },
53                 "mail" : {
54                     "mail-quota" : 2048,
55                     "mail-quota-usage" : 0
56                 },
57                 "imap-login":"301",
58                 "login-info":"adam@brandname",
59                 "email":"adam@brandname",
60                 "user-logins":{
61                     "HTTP" : 1497364334092,
62                     "open-xchange-appsuite" : 1497364334090
63                 },
64                 "unified-quota-enabled":true,
65                 "unified-quota-limit":104859648,
66                 "unified-quota":2511533
67             }
68         }
69     }
70 }

```



The TKG112 Report data is stored in CSV format and looks like the example below. It will output an additional file with \_info appended that contains configuration information as well as errors.

```

1 Email_nameID, Email_Displayname, Email_Begin, Email_Address, Email_Create, Email_Remove,
  Email_isactive
2 ID1, TestUser1, 2016-12-06 14:11:00 +0000, testuser@brand.com, 2016-12-06 14:11:00 +0000,
  , true
3 ID2, TestUser2, 2016-12-06 14:11:00 +0000, testuser2@brand.com, 2016-12-06 14:11:00 +0000,
  2016-12-06 14:11:00 +0000, false

```



### 2.1.10.5 TKG112 Data Description

#### All

- Email\_nameID - Varchar (256) - OX "userName"
- Email\_Displayname - Varchar (320) - Displayname used when sending emails
- Email\_Begin - Date (YYYY-MM-DD hh:mm:ss TIME\_ZONE) - Date of the registration in the OX system
- Email\_Address - Varchar (256) - email address including the domain name
- Email\_Create - Date (YYYY-MM-DD hh:mm:ss TIME\_ZONE) - Date when the email address was created
- Email\_Remove - Date (YYYY-MM-DD hh:mm:ss TIME\_ZONE) - Date when the email address was removed (optional)
- Email\_isactive - Boolean true/false - Flag if the email account is active or not. Will be always true when Email\_Remove is empty.

### 2.1.10.6 Metrics Data Description

#### General

- uuid - The report identifier
- reportType - Type of this report, so far only "OXaaS-report" possible
- timestamps - The start and end time of the report in milliseconds
- version - The builddate and version of the processing server
- errors - Map of all errors occurred during procession. Key is the exception Id and value is further information like message, category and Error-Id

#### Configs

- show-drive-metrics - true or false
- timeframe-start - The used timeframe start, if not set by the user, one year in the past is used
- show-mail-metrics - true or false
- single-brand - The sid of the brand admin or 0 if not set
- ignore-admin - true or false
- timeframe-end - The used timeframe end, if not set, the starting time of the report is used

**OXaaS**

- capabilitySets - All capability sets determined by the report. Key is the hashed value of all capabilities in a list
- brandname - The brandname with all userdata for the brand

**Per Brand**

- totals - Drive and mail quota information for the whole brand, comulated values of all users.
- contexts - All context informations for this brand

**Per User**

- capabilitySet - The hash value of the capability-set this user has
- drive - All drive data for this user (only present if drive option is true)
- mail - All mail data for this user (only present if mail option is true)
- imap-login - Imap login address
- login-info - Login info, gather from LDAP
- email - users email address
- user-logins - A list of all protocols, the user used to login with the latest timestamp as milliseconds
- unified-quota-enabled - true or false
- unified-quota-limit - This users unified quota limit (only present if unified quota is enabled for this user)
- unified-quota - This users unified quota (only present if unified quota is enabled for this user)

**Drive Data**

- mime-types - Map of all mimetypes and their amount
- file-count-all-versions - Number of all files and versions for this user
- quota - Quota limit
- used-quota - Used quota
- file-size-min - Smallest file size in this storage
- file-count-latest-version - Number of files, respecting only the latest version
- file-size-avg - Average filesize
- file-size-max - Maximum filesize

**Quota Data Sources** With unified quota enabled

- drive limit - From LDAP
- drive quota - From Cassandra
- mail limit - From LDAP
- mail quota - From Cassandra

**Without Unified Quota**

- drive limit - From filestore
- drive quota - From filestore
- mail limit - From LDAP
- mail quota - From Cassandra

### 2.1.11 Unified Quota

This implements the unified quota feature for cloud-plugins. It requires cassandra to be running and initialized with the `quota_usage` table, see [2.1.5 Cassandra](#) section. All file quota usage is updated into and read from cassandra.

```
com.openexchange.cloudplugins.unifiedquota
```

Please see for information about how to use this bundle the [Unifiedquota Documentaion](#)

### 2.1.12 Passwordchange

This implements the ox password change callback API in order to be able to change passwords in LDAP.

```
com.openexchange.passwordchange.cloudplugins
```

### 2.1.13 Installation

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

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

### 2.1.14 Configuration

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

`/opt/open-xchange/etc/plugin/mailstore-cloudplugins.properties` (page [24](#))

`/opt/open-xchange/etc/cloudplugins-authentication.properties` (page [25](#))

`/opt/open-xchange/etc/cloudplugins-master-auth-servlet.properties` (page [25](#))

`/opt/open-xchange/etc/cloudplugins-cassandra.properties` (page [26](#))

`/opt/open-xchange/etc/cloudplugins.properties` (page [27](#))

`/opt/open-xchange/etc/doveadm-config.properties` (page [28](#))

`/opt/open-xchange/etc/nginx-auth-servlet.properties` (page [28](#))

`/opt/open-xchange/etc/cloudquotaservice.properties` (page [29](#))

`/opt/open-xchange/etc/cloudquotaservice-cassandra.properties` (page [30](#))

`/opt/open-xchange/etc/cloudplugins_report.properties` (page [30](#))

## 2.2 Package open-xchange-cloudplugins-blackwhitelist-ldap

Implementation of blacklist whitelist for cloudplugins within LDAP

Version: 1.9.1-2

Type: OX Middleware Plugin

Depends on:

```
open-xchange-cloudplugins (<<1.9.2)
open-xchange-cloudplugins (>=1.9.1)
open-xchange-core (<<7.10.3)
open-xchange-core (>=7.10.0)
open-xchange-plugins-blackwhitelist (<<1.5.0)
open-xchange-plugins-blackwhitelist (>=1.4.1)
```

### 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 [31](#))

## 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: 1.9.1-2

Type: OX Middleware Plugin

Depends on:

```
open-xchange-cloudplugins (<<1.9.2)
open-xchange-cloudplugins (>=1.9.1)
open-xchange-core (<<7.10.3)
open-xchange-core (>=7.10.0)
```

### 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 [31](#))

## 2.4 Package open-xchange-cloudplugins-keycloak

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

Version: 1.9.1-2

Type: OX Middleware Plugin

Depends on:

```
open-xchange-cloudplugins (<<1.9.2)
open-xchange-cloudplugins (>=1.9.1)
open-xchange-oidc (<<7.10.3)
open-xchange-oidc (>=7.10.0)
```

### 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 configurable 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 [32](#))

## 2.5 Package open-xchange-cloudplugins-mailfilter

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

Version: 1.9.1-2

Type: OX Middleware Plugin

Depends on:



```
open-xchange-cloudplugins (<<1.9.2)
open-xchange-cloudplugins (>=1.9.1)
open-xchange-mailfilter (<<7.10.3)
open-xchange-mailfilter (>=7.10.0)
open-xchange-rest (<<7.10.3)
open-xchange-rest (>=7.10.0)
```

### 2.5.1 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.

### 2.5.2 Installation

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

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

### 2.5.3 Configuration

For details, please see appendix [A](#)  
/opt/open-xchange/etc/mailfilter-interceptor-drivers.properties (page [33](#))

## 2.6 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: 1.9.1-2

Type: OX Middleware Plugin

Depends on:

```
open-xchange-cloudplugins (<<1.9.2)
open-xchange-cloudplugins (>=1.9.1)
open-xchange-oidc (<<7.10.3)
open-xchange-oidc (>=7.10.0)
```

### 2.6.1 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

### 2.6.2 Installation

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

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

### 2.6.3 Configuration

For details, please see appendix [A](#)  
`/opt/open-xchange/etc/cloudplugins-oidc.properties` (page [35](#))

## 2.7 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: 1.9.1-2

Type: OX Middleware Plugin

Depends on:

```
open-xchange-cloudplugins (<<1.9.2)
open-xchange-cloudplugins (>=1.9.1)
open-xchange-saml-core (<<7.10.3)
open-xchange-saml-core (>=7.10.0)
```

### 2.7.1 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

### 2.7.2 Installation

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

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

### 2.7.3 Configuration

For details, please see appendix [A](#)  
`/opt/open-xchange/etc/cloudplugins-saml.properties` (page [39](#))

## 2.8 Package open-xchange-oxaas-alias

OXaaS alias bundle This package implements OXaaS alias handling.

Version: 1.9.1-2

Type: OX Middleware Plugin

Depends on:

```
open-xchange-admin (<<7.10.3)
open-xchange-admin (>=7.10.0)
open-xchange-core (<<7.10.3)
open-xchange-core (>=7.10.0)
```

### 2.8.1 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.

### 2.8.2 Installation

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

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

### 2.8.3 Configuration

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

`/opt/open-xchange/etc/oxaas-alias.properties` (page [40](#))

## 2.9 Package open-xchange-oxaas-mail-notify-ws

OXaaS notification mail servlet bundle

Version: 1.9.1-2

Type: OX Middleware Plugin

Depends on:

```
open-xchange-cloudplugins (<<1.9.2)
open-xchange-cloudplugins (>=1.9.1)
open-xchange-core (<<7.10.3)
open-xchange-core (>=7.10.0)
open-xchange-ldap (<<7.10.3)
open-xchange-ldap (>=7.10.0)
open-xchange-smtp (<<7.10.3)
open-xchange-smtp (>=7.10.0)
```

### 2.9.1 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

### 2.9.2 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}/

```



### 2.9.3 Installation

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

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

### 2.9.4 Configuration

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

`/opt/open-xchange/etc/oxaas-mail-notification-templates.properties` (page [40](#))

`/opt/open-xchange/etc/oxaas-drive-quota-notification.properties` (page [40](#))

## 2.9.5 Templates

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

## 2.10 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: 1.9.1-2

Type: OX Middleware Plugin

Depends on:

```
open-xchange-cloudplugins (<<1.9.2)
open-xchange-cloudplugins (>=1.9.1)
open-xchange-core (<<7.10.3)
open-xchange-core (>=7.10.0)
open-xchange-imap (<<7.10.3)
open-xchange-imap (>=7.10.0)
```

### 2.10.1 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`

### 2.10.2 Installation

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

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

### 2.10.3 Configuration

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

`/opt/open-xchange/etc/oxaas-mail-unread.properties` (page [41](#))

## 2.11 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: 1.9.1-2

Type: OX Middleware Plugin

Depends on:

```
open-xchange-cloudplugins (<<1.9.2)
open-xchange-cloudplugins (>=1.9.1)
open-xchange-core (<<7.10.3)
open-xchange-core (>=7.10.0)
open-xchange-imap (<<7.10.3)
open-xchange-imap (>=7.10.0)
```

### 2.11.1 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

### 2.11.2 Installation

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

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

### 2.11.3 Configuration

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

/opt/open-xchange/etc/oxaas-mail.properties (page [41](#))

Find more information about product versions and releases at [http://oxpedia.org/wiki/index.php?title=AppSuite:Versioning\\_and\\_Numbering](http://oxpedia.org/wiki/index.php?title=AppSuite:Versioning_and_Numbering) and <http://documentation.open-xchange.com/>.

## 3 Changes relevant for Operators

### 3.1 Changes of Configuration Files

#### Change #1 /opt/open-xchange/etc/cloudplugins-oidc.properties

```
+com.openexchange.oidc.enabled=true
+com.openexchange.cloudplugins.oidc.user.regex=[0-9a-zA-Z.@]*
+com.openexchange.cloudplugins.oidc.enabled=false
+com.openexchange.cloudplugins.oidc.id=
+com.openexchange.cloudplugins.oidc.ldapLookup=
```

```
+com.openexchange.cloudplugins.oidc.brand=
+com.openexchange.cloudplugins.oidc.tokenAuth=
+com.openexchange.cloudplugins.oidc.backendPath=
+com.openexchange.cloudplugins.oidc.hosts=
```

Package: open-xchange-cloudplugins-oidc

## Change #2 /opt/open-xchange/etc/cloudplugins-saml.properties

```
-com.openexchange.cloudplugins.saml.disableOtherAuthentication=false
-com.openexchange.cloudplugins.saml.id="default_id"
-com.openexchange.cloudplugins.saml.logout.redirect.url="https://www.google.com"
-com.openexchange.cloudplugins.saml.domain=
+com.openexchange.cloudplugins.saml.id=
+com.openexchange.cloudplugins.saml.ldapLookup=
+com.openexchange.cloudplugins.saml.logout.redirect.url=
+com.openexchange.cloudplugins.saml.brand=
+com.openexchange.cloudplugins.saml.logout.failure.redirect=
+com.openexchange.cloudplugins.saml.samlPath=
+com.openexchange.cloudplugins.saml.staticRedirect=
+com.openexchange.cloudplugins.saml.enableMetadataService=false
+com.openexchange.cloudplugins.saml.enableSingleLogout=false
+com.openexchange.cloudplugins.saml.entityID=
+com.openexchange.cloudplugins.saml.providerName=
+com.openexchange.cloudplugins.saml.acsURL=
+com.openexchange.cloudplugins.saml.slsURL=
+com.openexchange.cloudplugins.saml.logoutResponseBinding=http-redirect
+com.openexchange.cloudplugins.saml.logoutResponseTemplate=saml.logout.response.html
+com.openexchange.cloudplugins.saml.idpEntityID=
+com.openexchange.cloudplugins.saml.idpAuthnURL=
+com.openexchange.cloudplugins.saml.idpLogoutURL=
+com.openexchange.cloudplugins.saml.enableAutoLogin=false
+com.openexchange.cloudplugins.saml.allowUnsolicitedResponses=true
+com.openexchange.cloudplugins.saml.enableSessionIndexAutoLogin=false
+com.openexchange.cloudplugins.saml.hosts=
```

Package: open-xchange-cloudplugins-saml

## 3.2 Changes of Behavior

### Change #CP-188 Restructured mail domain handling

#### Warning

This release contains LDAP schema changes. After the update, the schema must be adapted before starting and using this release. Shared domains must now be created within sub-trees for each brand. This does not happen automatically. Shared domains stored as multi-value attribute in brand entries are not taken into account anymore.

#### Info

Please see also new REST APIs.

Status: Done

Resolution: Fixed

### Change #CP-190 Make the cloud-plugins SAML implementation highly configurable and multi SAML aware

Status: Done

Resolution: Fixed

Affected Packages: open-xchange-cloudplugins  
open-xchange-cloudplugins-oidc  
open-xchange-cloudplugins-saml

**Change #CP-191 Don't use LDAP read connection in any administrative API**

Status: Done

Resolution: Done

Affected Packages: open-xchange-cloudplugins  
open-xchange-cloudplugins-forwards-ws

**Change #CP-193 General multi tenant aware OIDC backend support in cloud-plugins**

Status: Done

Resolution: Fixed

Affected Packages: open-xchange-cloudplugins-oidc

## 4 Tests

To avoid side effects, the shipped packages have gone through automated regression test on both, a Continuous Integration System and a dedicated server set-up for system and integration testing. All changes have been checked for potential side-effects and effect on behavior. Unless explicitly stated within this document, we do not expect any side-effects.

### 4.1 Test Report

**Test T1550148 Restrict mail access (cloud-plugins-1.9.1-rev2)**

Status: Passed

If a user has access-webmail off, this must be written into LDAP

**Test T1550149 Installation setup of Cassandra (cloud-plugins-1.9.1-rev2)**

Status: Passed

**Test T1550150 Login table creation in Cassandra (cloud-plugins-1.9.1-rev2)**

Status: Passed

**Test T1550151 Record logging of Http protocol with valid credentials (cloud-plugins-1.9.1-rev2)**

Status: Passed

[Jira CP-4](#)

**Test T1550152 Record logging of Http protocol with invalid credentials (cloud-plugins-1.9.1-rev2)**

Status: Passed

[Jira CP-5](#)

**Test T1550153 Record logging of Smtplib protocol with valid credentials (cloud-plugins-1.9.1-rev2)**

Status: Passed

[Jira CP-4](#)

**Test T1550154 Record logging of Smtplib protocol with invalid credentials (cloud-plugins-1.9.1-rev2)**

Status: Passed

[Jira CP-5](#)



- Test T1550155 Record logging of IMAP protocol with valid credentials (cloud-plugins-1.9.1-rev2)**  
Status: Passed  
[Jira CP-4](#)
- Test T1550156 Record logging of IMAP protocol with invalid credentials (cloud-plugins-1.9.1-rev2)**  
Status: Passed  
[Jira CP-5](#)
- Test T1550157 Record reset counter for IMAP protocol on successful login (cloud-plugins-1.9.1-rev2)**  
Status: Passed  
[Jira CP-5](#)
- Test T1550158 Record reset counter for SMTP protocol on successful login (cloud-plugins-1.9.1-rev2)**  
Status: Passed  
[Jira CP-5](#)
- Test T1550159 Record reset counter for Http protocol on successful login (cloud-plugins-1.9.1-rev2)**  
Status: Passed  
[Jira CP-5](#)
- Test T1550160 Logging the Upgrade time of Drive (cloud-plugins-1.9.1-rev2)**  
Status: Passed
- Test T1550161 Logging the Downgrade time of Drive (cloud-plugins-1.9.1-rev2)**  
Status: Passed
- Test T1550162 Record the creation time of Email Alias (cloud-plugins-1.9.1-rev2)**  
Status: Passed  
[Jira CP-14](#)
- Test T1550163 Record the deletion time of Email Alias (cloud-plugins-1.9.1-rev2)**  
Status: Passed  
[Jira CP-14](#)
- Test T1550164 User authentication without ldap binding (cloud-plugins-1.9.1-rev2)**  
Status: Passed  
[Jira CP-34\(CP-34\)](#)
- Test T1550165 Record the quota information in Quota Usage table in Cassandra (cloud-plugins-1.9.1-rev2)**  
Status: Passed  
Verify the quota logging in database  
[Jira MW-442](#)
- Test T1550166 User master authentication (cloud-plugins-1.9.1-rev2)**  
Status: Passed  
[Jira CP-1](#)
- Test T1550167 Get user with option attributes (cloud-plugins-1.9.1-rev2)**  
Status: Passed

[Link](#)

**Test T1550168 Restful API function to Create/update oxMSISDN and oxCustomId attributes (cloud-plugins-1.9.1-rev2)**

Status: Passed

[Link](#)

**Test T1550169 Delete optional attributes from Ldap Schema (cloud-plugins-1.9.1-rev2)**

Status: Passed

[Link](#)

**Test T1550170 Record creation and deletion of AutoForward sieve filter in Cassandra table (cloud-plugins-1.9.1-rev2)**

Status: Passed

[Jira CP-110](#)

**Test T1550171 Get User configuration (cloud-plugins-1.9.1-rev2)**

Status: Passed

[Jira CP-93](#)

**Test T1550172 Configuration (cloud-plugins-1.9.1-rev2)**

Status: Passed

**Test T1550173 Auto forward (cloud-plugins-1.9.1-rev2)**

Status: Passed

**Test T1550174 Use Nginx Auth with Alias (cloud-plugins-1.9.1-rev2)**

Status: Passed

## A Configuration Files

**File 1 /opt/open-xchange/etc/plugin/mailstore-cloudplugins.properties**

```
1 MAILSTORE_CLOUD_STORAGE=com.openexchange.admin.cloudplugins.storage.mysqlStorage.  
MailstoreCloudMySQLStorage
```

**File 2 /opt/open-xchange/etc/cloudplugins-authentication.properties**

```
1 # Regex to validate host HTTP Header value  
2 com.openexchange.authentication.cloudplugins.host.regex= [0-9a-zA-Z.]*  
3  
4 #Regex to validate user name  
5 com.openexchange.authentication.cloudplugins.user.regex= [0-9a-zA-Z.@]*  
6  
7 # Setting to control the start of the own authenticationService which would be used as a  
8 fallback in the Tracker if started  
9 # Default: true  
9 com.openexchange.authentication.cloudplugins.enableauthentication=true  
10  
11 # Comma seperated blacklist of hostnames that should not be handled by the default  
authenticationService
```

```

12 # Default: <empty>
13 com.openexchange.authentication.cloudplugins.authentication.blacklist=
14
15 # Setting to control the start of the CloudAuthenticationDriverTracker
16 # Default: true
17 com.openexchange.authentication.cloudplugins.enable.authentication.tracker=true
18
19 # Configure the LDAP lookup method to find users using their logins.
20 # It is the method that is used by default when there is no brand specifi
21 # configuration setting).
22 #
23 # Optional, defaults to "uid".
24 #
25 # Possible values:
26 # uid
27 #   attempts to find users by matching their login against the uid attribute.
28 # email
29 #   attempts to find users by matching their login against the alias attribute.
30 # auto
31 #   when the login contains a "@", the "email" method is used and when not,
32 #   the "uid" method is used
33 # uid-or-email
34 #   attempts to find users by matching their login against the uid and the alias
35 #   attributes (either may match)
36 #
37 # Note that this only applies to the default authentication driver. If there
38 # is a custom implementation that is used for a given brand, its behavior is
39 # not influenced by this properties.
40 #
41 # Example:
42 # com.openexchange.authentication.cloudplugins.authentication.uid.mode=auto
43
44 # One may define any number of such settings per brand by setting properties
45 # with the following format for their name:
46 #
47 # com.openexchange.authentication.cloudplugins.authentication.uid.mode.<brand>=<uid|email|
48 #   auto|uid-or-email>
49 #
50 # For the list of possible values, please consult the documentation for
51 # com.openexchange.authentication.cloudplugins.authentication.uid.mode
52 #
53 # Optional, defaults to falling back to the method configured in
54 # com.openexchange.authentication.cloudplugins.authentication.uid.mode
55 #
56 # Note that this only applies to the default authentication service driver.
57 # If there is a custom implementation that is used for a given brand, its
58 # behavior is not influenced by these properties.
59 #
60 # Example:
61 # com.openexchange.authentication.cloudplugins.authentication.uid.mode.brand1=auto
62 # com.openexchange.authentication.cloudplugins.authentication.uid.mode.brand2=uid

```

### File 3 /opt/open-xchange/etc/cloudplugins-master-auth-servlet.properties

```

1 #
2 # login name of httpauth user to access the master auth api
3 #
4 com.openexchange.cloudplugins.master.auth.httpauth.login=
5
6 #
7 # password of httpauth user
8 #
9 com.openexchange.cloudplugins.master.auth.httpauth.password=

```

**File 4 /opt/open-xchange/etc/cloudplugins-cassandra.properties**

```
1 # turn on/off cassandra integration
2 # possible values: true/false
3 com.openexchange.cloudplugins.useCassandra = false
4
5 # keyspace to use in cassandra
6 com.openexchange.cloudplugins.cassandraKeyspace = ox
7
8 # comma separated list of brands which logins should be recorded to cassandra
9 com.openexchange.cloudplugins.cassandra.loginrecorder.remoteipfor.brands=
10
11 # comma separated list of brands where alias creation and deletion time should be recorded
    to cassandra
12 com.openexchange.cloudplugins.cassandra.loginrecorder.createdeletealias.brands=
13
14 # comma separated list of brands where mail autoforward active flag should be set
15 com.openexchange.cloudplugins.cassandra.autoforward.record.brands=
```

**File 5 /opt/open-xchange/etc/cloudplugins.properties**

```
1
2 # ldap url for read access
3 com.openexchange.cloudplugins.read.ldapurl=ldap://localhost:389
4
5 # admin dn for read access
6 com.openexchange.cloudplugins.read.binddn=cn=oxadmin,o=oxcs
7
8 # admin dn password for read access
9 com.openexchange.cloudplugins.read.bindpassword=
10
11 # ldap url for write access
12 com.openexchange.cloudplugins.write.ldapurl=ldap://localhost:389
13
14 # admin dn for write
15 com.openexchange.cloudplugins.write.binddn=cn=oxadmin,o=oxcs
16
17 # admin dn password for write access
18 com.openexchange.cloudplugins.write.bindpassword=
19
20 # tree for brands
21 com.openexchange.cloudplugins.branddn=ou=brands,o=oxcs
22
23 # tree for other stuff like mailstores
24 com.openexchange.cloudplugins.configdn=ou=config,o=oxcs
25
26 # tree for contexts
27 com.openexchange.cloudplugins.contextdn=ou=contexts,o=oxcs
28
29 # password for doveadm service
30 com.openexchange.cloudplugins.doveadmPassword=
31
32 # This timeout only works since Java 6 SE to time out waiting for a response.
33 com.openexchange.cloudplugins.read.timeout=10000
34
35 # Specifies the connect timeout (in milliseconds) when establishing a connection to the
    LDAP end-point
36 #
37 # Default is 5000 (5 seconds)
38 com.openexchange.cloudplugins.connect.timeout=5000
39
40 # Algorithm to use to encrypt passwords
41 # valid values are: SSHA and SSHA-384
42 com.openexchange.cloudplugins.password.algorithm=SSHA
43
44 # how long should the random salts be
45 com.openexchange.cloudplugins.password.algorithm.saltlength=64
```

```

46
47 # HTTP Header from which the brand name is fetched
48 com.openexchange.cloudplugins.header=host
49
50 # can a user change the password without providing the old one?
51 # default is false
52 com.openexchange.capability.password_change_without_old_password=false
53
54 # use ldapbind as password verification (true) or retrieve password digest from
55 # ldap using provided read credentials and do the check locally (false)
56 # NOTE: local password check only works when setting
57 # com.openexchange.cloudplugins.password.algorithm to SSHA or SSHA384
58 # and all existing users must have the userPassword encoded with any of those mechanisms.
59 com.openexchange.cloudplugins.passwordcheck.ldapbind=true
60
61 # Comma separated list of brands that where aliases should be moved into deleted tree
62 com.openexchange.cloudplugins.store.deleted.alias.brands=
63
64 # jndi ldap pool configuration
65 # see http://docs.oracle.com/javase/jndi/tutorial/ldap/connect/config.html for more
  information
66 com.openexchange.cloudplugins.pool=true
67 com.openexchange.cloudplugins.pool.initsize=1
68 com.openexchange.cloudplugins.pool.maxsize=20
69 com.openexchange.cloudplugins.pool.prefsiz=10
70 com.openexchange.cloudplugins.pool.timeout=300000
71 com.openexchange.cloudplugins.pool.protocol=plain
72
73 # Allowed encryption methods for LDAP userPassword
74 # internal default: MD5,SHA,CRYPT,SSHA,SSHA384
75 com.openexchange.cloudplugins.setPasswordHash.allowedMethods=MD5,SHA,CRYPT,SSHA,SSHA384
76
77 # Comma separated list of brands that should be able to explicitly add maildomains to
  contexts
78 # This parameter is reloadable
79 com.openexchange.cloudplugins.explicitMailDomains.brands=

```

## File 6 /opt/open-xchange/etc/doveadm-config.properties

```

1 # Api secret
2 com.openexchange.cloudplugins.dovecot.apiSecret=
3
4 # Dovecot port
5 com.openexchange.cloudplugins.dovecot.port=8080
6
7 # Protocol to use
8 com.openexchange.cloudplugins.dovecot.protocol=http://
9
10 # Dovecot host
11 com.openexchange.cloudplugins.dovecot.host=localhost
12
13 # Path to dovecot commands
14 com.openexchange.cloudplugins.dovecot.path=/doveadm/v1
15
16 # How many contexts per request should be transmitted
17 com.openexchange.cloudplugins.dovecot.contextChunks=100
18
19 # Max number of http connections
20 com.openexchange.cloudplugins.dovecot.maxConnections=100
21
22 # Max number of http connections per host
23 com.openexchange.cloudplugins.dovecot.maxConnectionsPerHost=100
24
25 # The connection timeout in milliseconds
26 com.openexchange.cloudplugins.dovecot.connectionTimeout=5000
27
28 # The socket read timeout in milliseconds
29 com.openexchange.cloudplugins.dovecot.socketReadTimeout=15000

```

**File 7 /opt/open-xchange/etc/nginx-auth-servlet.properties**

```

1 # Regex to validate brandName value
2 com.openexchange.cloudplugins.nginx.auth.servlet.brandName.regex= [0-9a-zA-Z.]*
3
4 # Regex to validate user name
5 com.openexchange.cloudplugins.nginx.auth.servlet.uid.regex= [0-9a-zA-Z.@]*
6
7 # Configure the LDAP lookup method to find users using their logins.
8 # It is the method that is used by default when there is no brand specific
9 # configuration setting).
10 #
11 # Optional, defaults to "uid".
12 #
13 # Possible values:
14 # uid
15 #   attempts to find users by matching their login against the uid attribute.
16 # email
17 #   attempts to find users by matching their login against the alias attribute.
18 # auto
19 #   when the login contains a "@", the "email" method is used and when not,
20 #   the "uid" method is used
21 # uid-or-email
22 #   attempts to find users by matching their login against the uid and the alias
23 #   attributes (either may match)
24 #
25 # Note that this only applies to the default authentication driver. If there
26 # is a custom implementation that is used for a given brand, its behavior is
27 # not influenced by this properties.
28 #
29 # Example:
30 # com.openexchange.cloudplugins.nginx.auth.servlet.uid.mode=auto
31
32 # One may define any number of such settings per brand by setting properties
33 # with the following format for their name:
34 #
35 # com.openexchange.cloudplugins.nginx.auth.servlet.uid.mode.<brand>=<uid|email|auto|uid-or
36 #   -email>
37 #
38 # For the list of possible values, please consult the documentation for
39 # com.openexchange.cloudplugins.nginx.auth.servlet.uid.mode
40 #
41 # Optional, defaults to falling back to the method configured in
42 # com.openexchange.cloudplugins.nginx.auth.servlet.uid.mode
43 #
44 # Note that this only applies to the default authentication driver. If there
45 # is a custom implementation that is used for a given brand, its behavior is
46 # not influenced by these properties.
47 #
48 # Example:
49 # com.openexchange.cloudplugins.nginx.auth.servlet.uid.mode.brand1=auto
50 # com.openexchange.cloudplugins.nginx.auth.servlet.uid.mode.brand2=uid

```

**File 8 /opt/open-xchange/etc/cloudquotaservice.properties**

```

1 # Identifier of the default quota driver to use when not
2 # superseded by a per-brand configuration setting (see below).
3 #
4 # This configuration property is optional.
5 # When it is not set, it will attempt to use the "dovecot"
6 # driver, if available (installed).

```

```

7 # If the "dovecot" driver is not installed, it will use the
8 # highest ranked driver that is installed.
9 #
10 # For a deterministic approach, it is recommended to set
11 # a value for this configuration setting.
12 #
13 # Example:
14 # com.openexchange.cloudplugins.quota.default.driver=cassandra
15 com.openexchange.cloudplugins.quota.default.driver=
16
17 # Override the quota driver per brand.
18 #
19 # Use property names that start with
20 # "com.openexchange.cloudplugins.quota.driver."
21 # followed by the brand name (not the complete DN
22 # but just the brand name).
23 #
24 # These are optional and, if not defined, will always fall
25 # back to the driver configured in the property
26 # com.openexchange.cloudplugins.quota.default.driver
27 #
28 # Example:
29 # com.openexchange.cloudplugins.quota.driver.brand1=cassandra
30 # com.openexchange.cloudplugins.quota.driver.otherbrand=cassandra
31 #

```

#### File 9 /opt/open-xchange/etc/cloudquotaservice-cassandra.properties

```

1 # Use the legacy "type" value for lookups in the Cassandra
2 # quota table.
3 # In recent deployments, the "type" parameter is "dovecot_mail",
4 # but in previous installments, the "type" used to be null.
5 # Setting this property to true will use null for the "type"
6 # query parameter.
7 #
8 # This property is optional and when not set, defaults to false.
9 #
10 # Example:
11 # com.openexchange.cloudplugins.quota.use.legacy.type=true
12 #
13
14 com.openexchange.cloudplugins.quota.use.legacy.type=false
15
16 # Unified quota performance optimizations.
17 #
18 # The default behavior is to check whether every single user
19 # who's usage quota is retrieved has unified quota enabled or not,
20 # and return data accordingly.
21 #
22 # In most use cases, if not all, unified quota will be enabled or
23 # disabled uniformly
24 # - globally for a platform,
25 # - or globally for a brand,
26 # - or for a whole context,
27 # in which case the implementation can avoid or minimize the amount
28 # of queries it needs to perform in order to determine how to
29 # calculate the quota usage, depending on whether unified quota
30 # is enabled or disabled for a user.
31 #
32 # Two configuration settings govern this behavior:
33 # - the default behavior which is used for every brand on a platform
34 # (com.openexchange.cloudplugins.quota.unified.quota)
35 # - per-brand behaviors which take precedence over the default
36 # (com.openexchange.cloudplugins.quota.unified.quota.<brand name>)
37 #
38 # Each of those settings can have one of the following values:
39 #
40 # always

```

```
41 # the implementation will assume that unified quota is enabled for
42 # all contexts within the brand, or for all contexts within all
43 # brands if applied to the default setting
44 #
45 # never
46 # the implementation will assume that unified quota is disabled for
47 # all contexts within the brand, or for all contexts within all
48 # brands if applied to the default setting
49 #
50 # context
51 # the implementation will only check whether unified quota has
52 # been enabled for the context the user(s) are in, and not for
53 # each individual user, assuming that all users within the same
54 # context are always configured uniformly regarding unified quota,
55 # be it enabled or disabled
56 #
57 # user
58 # the implementation will make no assumptions and check whether
59 # unified quota is enabled or not for every individual user -- this
60 # is the safest setting, which is why it is the default, but also
61 # the slowest and should be avoided if possible
62 #
63 # The default setting can be configured using the property
64 # com.openexchange.cloudplugins.quota.unified.quota=...
65 #
66 # It is optional and defaults to "user" (as explained above) if
67 # omitted, commented out or left empty.
68 #
69 # Example:
70 # com.openexchange.cloudplugins.quota.unified.quota=never
71 com.openexchange.cloudplugins.quota.unified.quota=
72
73 # Per-brand settings can be configured using the following
74 # prefix, followed by the name of the brand:
75 # com.openexchange.cloudplugins.quota.unified.quota.<brand name>=...
76 #
77 # Example:
78 # com.openexchange.cloudplugins.quota.unified.quota.my_brand=always
79 # com.openexchange.cloudplugins.quota.unified.quota.my_other_brand=context
80 #
81 # Those are obviously optional and default to using the default
82 # setting above (which, in turn, when omitted, defaults to "user").
83 #
```

#### File 10 /opt/open-xchange/etc/cloudplugins\_report.properties

```
1 # Where the report and its parts should be stored
2 com.openexchange.cloudplugins.report.storagePath=/tmp
3
4 # How many contexts can be stored in memory before writing them on hdd
5 com.openexchange.cloudplugins.report.maxChunkSize=200
6
7 # How many parallel threads can work on the report
8 com.openexchange.cloudplugins.report.maxThreadPoolSize=20
9
10 # Report thread priority
11 com.openexchange.cloudplugins.report.threadPriority=1
12
13 # Max number of entities that will be included in an ldap search
14 com.openexchange.cloudplugins.report.maxLdapChunks=20000
```

#### File 11 /opt/open-xchange/etc/cloudplugins-blackwhitelist-ldap.properties



```

1 # Identifier of this blackwhitelist connector: cloudplugins_blackwhitelist_ldap
2 # ldap uri
3 com.openexchange.cloudplugins.blackwhitelist.connector.ldap.uri=remote.url.for.ldap
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 base, can be empty
15 com.openexchange.cloudplugins.blackwhitelist.connector.ldap.base=ou=lists,o=oxcs
16
17 # ldap search filter
18 # possible template values {{usercontext}}
19 # usercontext is build as 'userid + "@" + contextid'
20 com.openexchange.cloudplugins.blackwhitelist.connector.ldap.searchFilter=
    oxLocalMailrecipient={{usercontext}}
21
22 # ldap DN to create when an entry is missing
23 # possible template values {{usercontext}}, {{brand}}
24 # usercontext is build as 'userid + "@" + contextid'
25 # brand is searched from default LDAP
26 com.openexchange.cloudplugins.blackwhitelist.connector.ldap.user.dn=oxLocalMailrecipient
    ={{usercontext}},bn={{brand}},ou=lists,o=oxcs
27
28 # ldap maximum pool size
29 com.openexchange.cloudplugins.blackwhitelist.connector.ldap.pool.size=10
30
31 # ldap max requests before connection is closed
32 # can be set to -1 to be disabled
33 com.openexchange.cloudplugins.blackwhitelist.connector.ldap.pool.max.requests=2000
34
35 # ldap max lifetime in seconds for each connection in the pool
36 com.openexchange.cloudplugins.blackwhitelist.connector.ldap.pool.max.lifetime=120
37
38 # config to enable LDAP SSL connection over ldaps
39 com.openexchange.cloudplugins.blackwhitelist.connector.ldap.useSSL=false
40
41 # Setting to check if memory backed test mock should be started
42 # This connector is identified by cloudplugins_blwl_test
43 # Default: false
44 com.openexchange.cloudplugins.blackwhitelist.connector.ldap.test=false

```

### File 12 /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 13 /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://
  localhost:8080/auth/realms/demo/protocol/openid-connect/token
7 com.openexchange.cloudplugins.keycloak.oauth.[client].tokenEndpoint=
8
9 # The clientId, if left empty, no clientId will be used
10 #
11 # Optional, default value: ""
12 #
13 # Example:
14 # com.openexchange.cloudplugins.keycloak.oauth.exampleClient.clientId=customerClient
15 com.openexchange.cloudplugins.keycloak.oauth.[client].clientId=
16
17 # The client secret. Must be provided if clientId is set.
18 #
19 # Optional, default value: ""
20 #
21 # Example:
22 # com.openexchange.cloudplugins.keycloak.oauth.exampleClient.clientSecret=123123
23 com.openexchange.cloudplugins.keycloak.oauth.[client].clientSecret=
24
25 # Max connections
26 #
27 # Optional, default value: 100
28 com.openexchange.cloudplugins.keycloak.oauth.maxConnections=
29
30 # Max connections per host
31 #
32 # Optional, default value: 100
33 com.openexchange.cloudplugins.keycloak.oauth.maxConnectionsPerHost=
34
35 # Connection timeout in ms
36 #
37 # Optional, default value in ms: 3000
38 com.openexchange.cloudplugins.keycloak.oauth.connectionTimeout=
39
40 # Socket read timeout in ms
41 #
42 # Optional, default value in ms: 6000
43 com.openexchange.cloudplugins.keycloak.oauth.socketReadTimeout=
44
45 # Refresh time in ms before expiry date
46 #
47 # Optional, default value is ms: 60000
48 com.openexchange.cloudplugins.keycloak.oauth.refreshTime=

```

#### File 14 /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 # 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 constructs: 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 autofoward rules which are defined by having the "
    autofoward" 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.
    autofoward.only=true
53 #
54 ### End Redirect Blacklist Driver ###
55
56 ##### End Driver Specific configurations #####

```

### File 15 /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 OIDCBackends 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 OIDCBackends by configuration
32 #
33 # com.openexchange.cloudplugins.oidc.enabled is also valid and will be used as an empty
34 # identifier
35 # An empty identifier will use all properties set in this config file.
36 # com.openexchange.cloudplugins.oidc.enabled.<identifier>=true
37 com.openexchange.cloudplugins.oidc.enabled=false
38
39 ### OIDC Specific configuration
40 #####
41 # All properties mentioned at https://documentation.open-xchange.com/components/middleware
42 # /config/7.10.2/#mode=features&feature=OpenID
43 # can be assigned to each OIDCbackend.
44 #
45 # !! NOTE !!
46 # The default prefix is not 'com.openexchange.oidc'
47 # 'com.openexchange.cloudplugins.oidc'
48 # is used instead meaning that there is an additional
49 # 'cloudplugins' in between to differentiate from the general oidc configuration.
50 #
51 # Example:
52 # com.openexchange.oidc.clientId will not be evaluated
53 # com.openexchange.oidc.cloudplugins.clientId is the correct default key
54 #
55 # The id inside the jwt token response which holds the userinformation
56 #
57 # The search for the id is done in the attributeStatement if nothing is configured
58 # possible configuration values are:
59 # <not_set> // the subject is used
60 # claim:key // a claim with the identifier <key> is used
61 # key // a claim with the identifier <key> is used
62 #
63 # In any case, the id must match the uid used to provision the user
64 # com.openexchange.cloudplugins.oidc.<identifier>.id=
65 com.openexchange.cloudplugins.oidc.id=
66
67 # The ldap lookup used by this OIDCBackend
68 #
69 # Configure the LDAP lookup method to find users using their identifiers.
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=

```

### File 16 /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 ### Key-store/certificate settings
12 #####
13 # All properties below can also be assigned to an identifier by configuring them as
14 # com.openexchange.cloudplugins.saml.<identifier>.key
15 #
16 # If a property is not set for an identifier, the key without the identifier is used as a
17 # default
18 # !!Note !!
19 # If a property is marked as optional, the default value for the optional case is used
20 # and not the general
21 # optional value if that is set
22 #
23 # Example:
24 # com.openexchange.cloudplugins.saml.example.id=someValue
25 # com.openexchange.cloudplugins.saml.keyStore=testStore
26 # com.openexchange.cloudplugins.saml.example.keyStore=
27 # example keyStore => testStore
28 #
29 # Example2:
30 # com.openexchange.cloudplugins.saml.example.id=someValue

```

```

29 # com.openexchange.cloudplugins.saml.brand=defaultBrand
30 # com.openexchange.cloudplugins.saml.example.brand=
31 # example brand (for ldap selection) => <empty>, will use the domainName of the request
32 #
33 # !! Note !!
34 # The list of possible SAMLBackends is identified by the property
35 # com.openexchange.cloudplugins.saml.<identifier>.id
36 # If there is no property for the id(s) set, no SAMLBackend will be started.
37 # com.openexchange.cloudplugins.saml.id is also valid and will be used as an empty
   # identifier
38 # An empty identifier will use all properties set in this config file.
39 #
40 # The full path to a Java keystore containing the IdPs certificate.
41 #
42 # Default: <empty>
43 com.openexchange.cloudplugins.saml.keyStore=
44
45 # Password to open the keystore.
46 #
47 # Default: <empty>
48 com.openexchange.cloudplugins.saml.keyStorePass=
49
50 # The aliases of the IdP certificate entry within the above specified
51 # keystore. Split by ','. Multiple certs can be used in a rolling upgrade
52 # case at the customers location without the need to coordinate an upgrade.
53 #
54 # The support for multiple certs is only enabled on 7.10.1+ systems.
55 # A 7.10.0 system will only use the first certAlias
56 #
57 # Default: <empty>
58 com.openexchange.cloudplugins.saml.certAlias=
59
60 # The alias of the signingKey entry within the above specified
61 # keystore.
62 #
63 # Default: <empty>
64 com.openexchange.cloudplugins.saml.signingKeyAlias=
65
66 # The password of the signingKey entry within the above specified
67 # keystore.
68 #
69 # Default: <empty>
70 com.openexchange.cloudplugins.saml.signingKeyPassword=
71
72 # The alias of the decryptionKey entry within the above specified
73 # keystore.
74 #
75 # Default: <empty>
76 com.openexchange.cloudplugins.saml.decryptionKeyAlias=
77
78 # The password of the decryptionKey entry within the above specified
79 # keystore.
80 #
81 # Default: <empty>
82 com.openexchange.cloudplugins.saml.decryptionKeyPassword=
83
84 ### SAML Specific configuration
85 #####
86 # The id inside the saml response which holds the userinformation
87 #
88 # The search for the id is done in the attributeStatement if nothing is configured
89 # possible configuration values are:
90 # key // search is done in the attributeStatement with the key
91 # attribute:key // search is done in the attributeStatement with the key
92 # subject:nameID // the subject:NameID is used
93 #
94 # In any case, the id must match the uid used to provision the user
95 com.openexchange.cloudplugins.saml.id=
96
97 # The ldap lookup used by this SAMLBackend
98 #

```

```
99 # Configure the LDAP lookup method to find users using their identifiers.
100 #
101 #
102 # Possible values:
103 # uid
104 # attempts to find users by matching their login against the uid attribute.
105 # email
106 # attempts to find users by matching their login against the alias attribute.
107 # auto
108 # when the login contains a "@", the "email" method is used and when not,
109 # the "uid" method is used
110 # uid-or-email
111 # attempts to find users by matching their login against the uid and the alias
112 # attributes (either may match)
113 #
114 # This property is optional.
115 # Default: uid
116 com.openexchange.cloudplugins.saml.ldaplookup=
117
118 # URL of where the users are redirected after logout if single_logout is active
119 # Must only be set if enableSingleLogout is enabled
120 #
121 # Default: <empty>
122 com.openexchange.cloudplugins.saml.logout.redirect.url=
123
124 # The brand to use for OXaaS LDAP authentication operations.
125 # Uses the host name when empty or not set.
126 #
127 # This property is optional.
128 # Default: <empty>
129 com.openexchange.cloudplugins.saml.brand=
130
131 # The URL to redirect to in case the SAML back-end fails to look up the authenticated user
132 # When left empty or not set, an HTTP 500 error page is sent instead.
133 #
134 # This property is optional.
135 # Default: <empty>
136 com.openexchange.cloudplugins.saml.failure.redirect=
137
138 # The URL to redirect to in case the SAML back-end has an error, when the user logs out
139 # When left empty or not set, the value of com.openexchange.cloudplugins.saml.failure.
    redirect is used.
140 #
141 # Default: <empty>
142 com.openexchange.cloudplugins.saml.logout.failure.redirect=
143
144 # The samlPath value required for the servlet alias
145 # registered with '{prefix}/saml/{samlPath}/..' as servlet alias.
146 #
147 # This property is optional.
148 # Default: <empty>
149 com.openexchange.cloudplugins.saml.samlPath=
150
151 # Static redirect upon login or relogin
152 #
153 # This property is optional.
154 # Default: <empty>
155 com.openexchange.cloudplugins.saml.staticRedirect=
156
157 # Whether the SPs metadata XML shall be made available via HTTP. The according
158 # servlet will then be available under 'http(s)://{hostname}/{prefix}/saml/metadata'.
159 #
160 # Default: false
161 com.openexchange.cloudplugins.saml.enableMetadataService=false
162
163 # Whether the single logout profile is enabled.
164 #
165 # Default: false
166 com.openexchange.cloudplugins.saml.enableSingleLogout=false
167
168 # Sets the entity ID of the service provider.
```

```
169 #
170 # This property is mandatory.
171 # Default: <empty>
172 com.openexchange.cloudplugins.saml.entityID=
173
174 # Sets the human-readable name of the service provider.
175 #
176 # This property is mandatory.
177 # Default: <empty>
178 com.openexchange.cloudplugins.saml.providerName=
179
180 # Sets the URL of the local assertion consumer service (ACS). This value is used within
181 # authentication requests, compared against Destination attributes in IdP responses
182 # and will be contained in the service providers metadata XML. The according endpoint
183 # is always registered with '{prefix}/saml/{samlPath}/acs' as servlet alias.
184 #
185 # This property is mandatory.
186 # Default: <empty>
187 # Example: https://appsuite.example.com/appsuite/api/saml/{samlPath}/acs
188 com.openexchange.cloudplugins.saml.acsURL=
189
190 # Sets the URL of the local single logout service. This value is compared against
191 # Destination
192 # attributes in IdP responses and will be contained in the service providers metadata XML.
193 # The according endpoint is always registered with '{prefix}/saml/{samlPath}/sls' as
194 # servlet alias.
195 #
196 # This property is mandatory if 'com.openexchange.cloudplugins.saml.enableSingleLogout' is
197 # 'true'.
198 # Default: <empty>
199 # Example: https://appsuite.example.com/appsuite/api/saml/{samlPath}/sls
200 com.openexchange.cloudplugins.saml.slsURL=
201
202 # The binding via which logout responses shall be sent to the IdP on IdP-initiated single
203 # logout flows. Must be 'http-redirect' or 'http-post'.
204 #
205 # This property is mandatory if 'com.openexchange.cloudplugins.saml.enableSingleLogout' is
206 # 'true'.
207 # Default: http-redirect
208 com.openexchange.cloudplugins.saml.logoutResponseBinding=http-redirect
209
210 # The HTML template to use when logout responses are sent to the IdP via HTTP POST.
211 # The template must be located in '/opt/open-xchange/templates'.
212 #
213 # This property is mandatory if 'com.openexchange.cloudplugins.saml.enableSingleLogout' is
214 # '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
220 # responses.
221 #
222 # This property is mandatory.
223 # Default: <empty>
224 com.openexchange.cloudplugins.saml.idpEntityID=
225
226 # The URL of the IdP endpoint where authentication requests are to be sent to.
227 #
228 # This property is mandatory.
229 # Default: <empty>
230 com.openexchange.cloudplugins.saml.idpAuthnURL=
231
232 # The URL of the IdP endpoint where logout requests are to be sent to.
233 #
234 # This property is mandatory if 'com.openexchange.cloudplugins.saml.enableSingleLogout' is
235 # 'true'.
236 # Default: <empty>
237 com.openexchange.cloudplugins.saml.idpLogoutURL=
238
239 # It is possible to enable a special kind of auto login mechanism that allows user agents
240 # to
```



```

233 # re-use an existing OX session if it was created during the same browser session. If
      enabled,
234 # a special cookie will be set, which is linked to the OX session and bound to the browser
      sessions
235 # life time. The advantage of this mechanism is, that sessions are simply re-entered if
      the user
236 # refreshes his browser window. He is then also able to open more than one tab of OX App
      Suite
237 # at the same time. This mechanism can only re-use sticky sessions, i.e. it is mandatory
      that the
238 # requests are always routed to the same backend for a certain session.
239 #
240 # --- SECURITY WARNING ---
241 # Enabling this setting is not compliant to the SAML specification as it bypasses the IdP
      in
242 # certain cases. Additionally in scenarios where a public device is used, a foreign user
      might
243 # take over a formerly authenticated users session if that user forgets to log out and
      doesn't
244 # close his web browser (even if he closes the App Suite tab). As no login screen is
      displayed
245 # by OX in SAML environments, the user is even not able to decide, whether the application
      shall
246 # remember him or not.
247 #
248 # Default: false
249 com.openexchange.cloudplugins.saml.enableAutoLogin=false
250
251 # Whether unsolicited responses will be accepted or not.
252 #
253 # Default: true
254 com.openexchange.cloudplugins.saml.allowUnsolicitedResponses=true
255
256 # Whether SAML-specific auto-login is enabled, that uses the SessionIndex of the
      AuthnResponse
257 #
258 # Default: false
259 com.openexchange.cloudplugins.saml.enableSessionIndexAutoLogin=false
260
261 # List of hosts where that this SAMLBackend is responsible for
262 # if all is present, this SAMLBackend responsible for all hosts
263 #
264 # It is possible to control the samlPath with this property.
265 # Another way would be to set the samlPath within the as-config.yml.
266 # Default: <empty>
267 com.openexchange.cloudplugins.saml.hosts=

```

### File 17 /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 18 /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 19 /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
  the filestore is context-wide
5 com.openexchange.oxaas.mail.quota.drive.updateAdmin=false
6
7 # Config-cascade aware setting to control how often a mail should be sent
8 # Default is 86400 (1 day)
9 # Set to 0 to ignore that and always send a new mail
10 com.openexchange.oxaas.mail.quota.drive.mail.seconds=86400

```

#### File 20 /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=

```

```
    internalBrandForhosterone
8  #com.openexchange.oxaas.mail.unread.ws.basic.[username].brand=
9
10 # Setting to control basic auth password
11 # example would be com.openexchange.oxaas.mail.unread.ws.basic.hosterone.password=
    verySecretPassword
12 #com.openexchange.oxaas.mail.unread.ws.basic.[username].password=
```

## File 21 /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=
    internalBrandForhosterone
18 #com.openexchange.oxaas.mail.ws.basic.[username].brand=
```