OX®

AppSuite Engineering Services Plugins
Release Notes for Release 1.3.3

2018-01-15

Contents

1 General Information

1.1 Warnings

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

⚠️ **Warning**
When updating only custom packages, it may be necessary to invalidate the browser cache to make the changes visible. An invalidation of the cache will be done automatically when updating OX core UI packages at the same time, but not if you are updating only custom UI plug-ins. In the latter case, please call the following command on all Apache nodes with the same value for <timestamp> :

```
/opt/open-xchange/sbin/touch-appsuite --timestamp=<timestamp>
```

⚠️ **Warning**
UI packages with themes need to generate CSS after installtion. This will be done automatically when the service is restarted but if you wish to not perform a service restart, you must call the following command on each node:

```
/opt/open-xchange/appsuite/share/update-themes.sh
```

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

1.2 Install Package Repository

This delivery is part of a restricted software repository:

https://software.open-xchange.com/components/plugins/stable/1.3.3/DebianJessie
https://software.open-xchange.com/components/plugins/stable/1.3.3/RHEL6
https://software.open-xchange.com/components/plugins/stable/1.3.3/RHEL7
https://software.open-xchange.com/components/plugins/stable/1.3.3/SLE_12

1.3 Build Dependencies

This delivery was build and tested with following dependencies:

```
frontend-7.8.4-rev18
```

1.4 Notice

ℹ️ **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-appsuite-blackwhitelist

Black/Whitelist plugin for App Suite
Version: 1.3.3-1
Type: OX Frontend Plugin with Themes
Depends on:

```
open-xchange-appsuite-manifest (>=7.8.4)
```

2.1.1 Installation

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

```
<package installer> install open-xchange-appsuite-blackwhitelist
```

2.1.2 Configuration

For details, please see appendix A
/opt/open-xchange/etc/settings/blackwhitelist.properties (page 9)
/opt/open-xchange/etc/meta/blackwhitelist.yml (page 10)

2.2 Package open-xchange-appsuite-sieve-blacklist

Blacklist plugin for App Suite
Version: 1.3.3-1
Type: OX Frontend Plugin with Themes
Depends on:

```
open-xchange-appsuite-manifest (>=7.8.4)
```

2.2.1 Installation

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

```
<package installer> install open-xchange-appsuite-sieve-blacklist
```

2.2.2 Configuration

For details, please see appendix A
/opt/open-xchange/etc/settings/blacklist.properties (page 10)
/opt/open-xchange/etc/meta/blacklist.yml (page 10)

2.3 Package open-xchange-authentication-masterpassword

Authentication implementation that uses a global password for all users – DO NOT USE IN PRO-
DUCTION This package provides an authentication implementation that verifies user passwords
against a globally configured password. DO NOT USE THIS IN PRODUCTION ! This implementation
is only meant for testing and migration scenarios.
Version: 1.3.3-1
Type: OX Middleware Plugin
Depends on:

```
open-xchange-core (>=7.8.4)
```

Conflcts with:

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

2.3.1 Installation

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

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

2.3.2 Configuration

For details, please see appendix A
/opt/open-xchange/etc/masterpassword-authentication.properties (page 11)

2.4 Package open-xchange-ldap-client

This package provides an advanced LDAP client library that is used by other Open-Xchange bundles.
Version: 1.3.3-1
Type: OX Middleware Plugin
Depends on:

```
open-xchange-core (>=7.8.4)
```

2.4.1 Installation

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

```
<package installer> install open-xchange-ldap-client
```

2.4.2 Configuration

For details, please see appendix A
/opt/open-xchange/etc/ldap-client.d/ldap-client-pools.yaml.example (page 14)

2.5 Package open-xchange-plugins-blackwhitelist

Plugins abstraction layer for blacklist/whitelist connectors
Version: 1.3.3-1
Type: OX Middleware Plugin
Depends on:

```
open-xchange-core (>=7.8.4)
```

2.5.1 Installation

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

```
<package installer> install open-xchange-plugins-blackwhitelist
```

2.5.2   Configuration

For details, please see appendix A
/opt/open-xchange/etc/plugins-blackwhitelist.properties (page 14)

2.6   Package open-xchange-plugins-blackwhitelist-sieve

This package installs the OSGi bundles needed to access the blacklist for plugins within Sieve
Version: 1.3.3-1
Type: OX Middleware Plugin
Depends on:

```
open-xchange-core (>=7.8.4)
open-xchange-mailfilter (>=7.8.4)
open-xchange-plugins-blackwhitelist (>=1.3.3)
```

2.6.1   Installation

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

```
<package installer> install open-xchange-plugins-blackwhitelist-sieve
```

2.6.2   Configuration

For details, please see appendix A
/opt/open-xchange/etc/plugins-blacklist-sieve.properties (page 14)

2.7   Package open-xchange-plugins-onboarding-maillogin

Plugin that enables the overriding of the login information that is shown to users during onboarding.
Version: 1.3.3-1
Type: OX Middleware Plugin
Depends on:

```
open-xchange-client-onboarding (>=7.8.4)
open-xchange-core (>=7.8.4)
```

2.7.1   General Functionality

Login information that is displayed to users in the onboarding configuration screens can be customized with these plugins. It requires enabling the `CustomLoginSource` in the first place, by setting the following properties to `true`, applicable to:

- CalDAV: `com.openexchange.client.onboarding.caldav.login.customsource`

- CardDAV: `com.openexchange.client.onboarding.carddav.login.customsource`

- IMAP: `com.openexchange.client.onboarding.imap.login.customsource`

- SMTP: `com.openexchange.client.onboarding.smtp.login.customsource`

 This bundle applies the login name display customization to all of the options above, and which mechanism is to be used is configurable through config cascade. The following (config cascade aware) property selects which plugin to use:

```
com.openexchange.plugins.onboarding.login
```

by setting it to one of the following built-in values:

- `email`: uses the default sender address

- `attr:{name}`: uses a user attribute with name `{name}`

- `login_name`: uses the user's login name

- `login`: uses the user's login (which is also the fallback and default, and the same as if the corresponding `com.openexchange.client.onboarding.*.login.customsource` property was not set to `true`

2.7.2 Installation

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

```
<package installer> install open-xchange-plugins-onboarding-maillogin
```

2.8   Package open-xchange-sms-twilio

This package installs the OSGi bundles needed to send SMS messages via twilio
Version: 1.3.3-1
Type: OX Middleware Plugin
Depends on:

```
open-xchange-core (>=7.8.4)
```

2.8.1 Installation

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

```
<package installer> install open-xchange-sms-twilio
```

2.8.2 Configuration

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

2.9   Package open-xchange-util-imap

This package is a library that provides various utilities for IMAP.
Version: 1.3.3-1
Type: OX Middleware Plugin
Depends on:

```
open-xchange-core (>=7.8.4)
```

2.9.1 Installation

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

```
<package installer> install open-xchange-util-imap
```

Find more information about product versions and releases at 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 Behaviour

Change #ES-237 **Generic bundle for changing the login displayed in onboarding to the user's email**
Status: Done
Affected Packages: open-xchange-plugins-onboarding-maillogin

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 behaviour. Unless explicitly stated within this document, we do not expect any side-effects.

4.1 Test Report

Test T203751 **Installation and Configuration (1.3.1-rev1)**
Status: Passed

Test T203752 **Reject own address (1.3.1-rev1)**
Status: Passed
Jira ES-20
Jira ES-25

Test T203753 **Add/remove address (1.3.1-rev1)**
Status: Passed
Jira ES-19
Jira ES-21
Jira ES-23
Jira ES-24
Jira ES-26
Jira ES-28
Jira ES-29

Test T203754 **Custom rule name (1.3.1-rev1)**
Status: Passed
Jira ES-18
Jira ES-22

Test T203755 **Edit entry (1.3.1-rev1)**
Status: Passed
Jira ES-27
Jira ES-80

Test T203756 **Installation (1.3.1-rev1)**
Status: Passed
Jira OXQA-229

Test T203757 **Configuration Option 1 (1.3.1-rev1)**
Status: Passed
Jira OXQA-229

Test T203758   Configuration Option 2 (1.3.1-rev1)
Status: Passed
Jira OXQA-229

Test T203759   Configuration Option 3 (1.3.1-rev1)
Status: Passed
Jira OXQA-229

Test T203760   Configuration Option 4 (1.3.1-rev1)
Status: Passed
Jira ES-60

Test T203761   Setup a default/test configuration for SMS(Twilio) integration with OX (1.3.1-rev1)
Status: Blocked
For user story
Jira ES-93 Setup test configuration for SMS(Twilio) integration with OX

Test T203762   OX SMS (Twilio) sending functionality to cell phone for Device Setup (1.3.1-rev1)
Status: Blocked
Jira ES-93 OX sms sending functionality to cell phone for device Setup

Test T203763   Installation and Configuration (1.3.1-rev1)
Status: Passed

Test T203764   Reject own address (1.3.1-rev1)
Status: Passed
Jira ES-20
Jira ES-25

Test T203765   Add/remove address (1.3.1-rev1)
Status: Passed
Jira ES-19
Jira ES-21
Jira ES-23
Jira ES-24
Jira ES-26
Jira ES-28
Jira ES-29

Test T203766   Edit entry (1.3.1-rev1)
Status: Passed
Jira ES-27
Jira ES-80

Test T212650   Installation and Configuration (1.3.1-rev1)
Status: Passed

Test T212651   Reject own address (1.3.1-rev1)
Status: Passed
Jira ES-20
Jira ES-25

Test T212652   Add/remove address (1.3.1-rev1)
Status: Passed

Jira ES-19
Jira ES-21
Jira ES-23
Jira ES-24
Jira ES-26
Jira ES-28
Jira ES-29

Test T212653   Custom rule name (1.3.1-rev1)
Status: Passed
Jira ES-18
Jira ES-22

Test T212654   Edit entry (1.3.1-rev1)
Status: Passed
Jira ES-27
Jira ES-80

Test T212660   Change mail spam handling (1.3.1-rev1)
Status: Passed
Jira ES-132

A   Configuration Files

File 1   /opt/open-xchange/etc/settings/blackwhitelist.properties

```
1   ##
2   # Blackwhitelist settings
3   #
4   # Max number of addressed on the list
5   io.ox/mail//blackwhitelist/maxAddresses = 250
6   # Allow users to add duplicates
7   io.ox/mail//blackwhitelist/allowDuplicates = false
8   # Validate if only valid mail addresses are on the list
9   io.ox/mail//blackwhitelist/validateAddresses = false
10  # Allow users to edit items on their list
11  io.ox/mail//blackwhitelist/editable = false
12  # Allow users to manually add addresses
13  io.ox/mail//blackwhitelist/showAddButton = false
14  # Show edit button next to entry
15  io.ox/mail//blackwhitelist/showEditButton = false
16  # Show save button next to entry when creating it
17  io.ox/mail//blackwhitelist/showSaveButton = false
18  # Show search box for blacklist
19  io.ox/mail//blackwhitelist/searchable = true
```

File 2   /opt/open-xchange/etc/meta/blackwhitelist.yml

```
1   io.ox/mail//blackwhitelist/maxAddresses:
2       protected: false
3   io.ox/mail//blackwhitelist/allowDuplicates:
4       protected: false
5   io.ox/mail//blackwhitelist/validateAddresses:
6       protected: false
7   io.ox/mail//blackwhitelist/editable:
8       protected: false
9   io.ox/mail//blackwhitelist/showAddButton:
```

```
10       protected: false
11   io.ox/mail//blackwhitelist/showEditButton:
12       protected: false
13   io.ox/mail//blackwhitelist/showSaveButton:
14       protected: false
15   io.ox/mail//blackwhitelist/searchable:
16       protected: false
```

File 3   /opt/open-xchange/etc/settings/blacklist.properties

```
1   # Name of the rule used as blacklist
2   io.ox/mail//blacklist/ruleName = Blocklist
3   # Max number of addressed on the list
4   io.ox/mail//blacklist/maxAddresses = 250
5   # Allow users to add duplicates
6   io.ox/mail//blacklist/allowDuplicates = false
7   # Validate if only valid mail addresses are on the list
8   io.ox/mail//blacklist/validateAddresses = false
9   # Allow users to edit items on their list
10  io.ox/mail//blacklist/editable = false
11  # Allow users to manually add addresses
12  io.ox/mail//blacklist/showAddButton = false
13  # Show edit button next to entry
14  io.ox/mail//blacklist/showEditButton = false
15  # Show save button next to entry when creating it
16  io.ox/mail//blacklist/showSaveButton = false
17  # Show search box for blacklist
18  io.ox/mail//blacklist/searchable = true
```

File 4   /opt/open-xchange/etc/meta/blacklist.yml

```
1   io.ox/mail//blacklist/ruleName:
2       protected: false
3   io.ox/mail//blacklist/maxAddresses:
4       protected: false
5   io.ox/mail//blacklist/allowDuplicates:
6       protected: false
7   io.ox/mail//blacklist/validateAddresses:
8       protected: false
9   io.ox/mail//blacklist/userEditable:
10      protected: false
11  io.ox/mail//blacklist/showAddButton:
12      protected: false
```

File 5   /opt/open-xchange/etc/masterpassword-authentication.properties

```
1   # Configuration file for the master password authentication plugin
2   #
3   # DO NOT USE IN PRODUCTION !
4   #
5
6   # The clear text password to authenticate all users.
7   # Mandatory.
8   # Example:
9   # com.openexchange.authentication.masterpassword.password=supersecret
10  com.openexchange.authentication.masterpassword.password=
11
12  # The default value for the context when it is not specified.
13  # Optional and defaults to using the "defaultcontext" mapping.
```

```
14  #com.openexchange.authentication.masterpassword.default.context=
15
16  # Whether the username portion of the login should be lowercased
17  # before being looked up in the user database.
18  # Optional and defaults to false
19  #com.openexchange.authentication.masterpassword.lowercase=false
20
21  # Whether the context name portion of the login should be lowercased
22  # before being looked up in the context database.
23  # Optional and defaults to false
24  #com.openexchange.authentication.masterpassword.lowercase.context=false
25
26  # Whether to use the complete login string as the username,
27  # e.g. login "foo@bar.com" -> user name "foo@bar.com" and
28  # context name "bar.com"
29  # Optional and defaults to false
30  #com.openexchange.authentication.masterpassword.use.full.login.info=false
31
32  # Whether to use the complete login string for the context name,
33  # e.g. login "foo@bar.com" -> context name "foo@bar.com"
34  # Optional and defaults to false
35  #com.openexchange.authentication.masterpassword.use.full.login.info.for.context=false
```

File 6 /opt/open-xchange/etc/ldap-client.d/ldap-client-pools.yaml.example

```
1   # The top-level key is the identifier of the pool, which can be
2   # any string of text and is being used by the bundles and applications
3   # to access that pool configuration.
4   # Typically, those are fixed or need to be configured in the bundles
5   # that use this library.
6   pool1:
7     trust-store:
8       # SSL: path to the JKS trust store file that contains the anchors
9       file: /etc/trust.jks
10      # SSL: indicates whether to reject certificates if the current time
11      # is outside the validity window for the certificate
12      validity: true
13    key-store:
14      # SSL: path to the JKS client key store file that contains the key
15      file: /etc/private.jks
16      # SSL: password to access the keystore and the key
17      password: foobar
18      # SSL: alias of the key to use
19      alias: key
20    # Configure a read/write pool with different settings for read operations
21    # and for write operations (i.e. different pools of LDAP servers).
22    # Here comes the part for the read operations:
23    read:
24      # Use a failover cluster of two nodes:
25      failover:
26        - ldap1.example.com
27        - ldap2.example.com
28      # Pool connection management
29      # ------------------------
30      # When creating a connection pool, you may specify an initial number of
31      # connections (pool-min) and a maximum number of connections (pool-max).
32      # The initial number of connections is the number of connections that should
33      # be immediately established and available for use when the pool is created.
34      # The maximum number of connections is the largest number of unused connections
35      # that may be available in the pool at any time.
36      # Whenever a connection is needed, whether by an attempt to check out a
37      # connection or to use one of the pool's methods to process an operation,
38      # the pool will first check to see if there is a connection that has already
39      # been established but is not currently in use, and if so then that connection
40      # will be used.
41      # If there aren't any unused connections that are already established, then
42      # the pool will determine if it has yet created the maximum number of
43      # connections, and if not then it will immediately create a new connection
```

```
 44      # and use it.
 45      # If the pool has already created the maximum number of connections, then the
 46      # pool may wait for a period of time (as configured using 'maxWaitTimeMillis' below,
 47      # which has a default value of zero to indicate that it should not wait at all)
 48      # for an in-use connection to be released back to the pool.
 49      # If no connection is available after the specified wait time (or there should
 50      # not be any wait time), then the pool may automatically create a new connection
 51      # to use if 'createIfNecessary' is true (which is the default).
 52      # If it is able to successfully create a connection, then it will be used.
 53      # If it cannot create a connection, or if 'createIfNecessary' is set to false,
 54      # then an error will be thrown.
 55      # Note that the maximum number of connections specified when creating a pool
 56      # refers to the maximum number of connections that should be available for use
 57      # at any given time.
 58      # If 'createIfNecessary' is set to true, then there may temporarily be more
 59      # active connections than the configured maximum number of connections.
 60      # This can be useful during periods of heavy activity, because the pool will
 61      # keep those connections established until the number of unused connections
 62      # exceeds the configured maximum.
 63      # If you wish to enforce a hard limit on the maximum number of connections so
 64      # that there cannot be more than the configured maximum in use at any time,
 65      # then set 'createIfNecessary' to false to indicate that the pool should not
 66      # automatically create connections when one is needed but none are available,
 67      # and you may also want to set 'maxWaitTimeMillis' to a maximum wait time to allow
 68      # the pool to wait for a connection to become available rather than throwing
 69      # an exception if no connections are immediately available.
 70      pool-min: 10
 71      pool-max: 50
 72      maxConnectionAgeMillis: 30000
 73      maxWaitTimeMillis: 500
 74      createIfNecessary: true
 75      # Specifies whether certain operations that should be retried on a newly-created
 76      # connection if the initial attempt fails in a manner that indicates that the
 77      # connection used to process the request may no longer be valid.
 78      # Only a single retry will be attempted for any operation.
 79      retryFailedOperations: true
 80    # Here comes the part for the write operations:
 81    write:
 82      host: ldap0.example.com
 83      pool-min: 1
 84      pool-max: 10
 85      maxConnectionAgeMillis: 60000
 86      maxWaitTimeMillis: 1000
 87      createIfNecessary: false
 88      retryFailedOperations: false
 89    # Specifies whether the pool should attempt to abandon any request for which
 90    # no response is received in the maximum response timeout period:
 91    abandonOnTimeout: true
 92    # Specifies the maximum length of time in milliseconds that a connection attempt
 93    # should be allowed to continue before giving up.
 94    # A value of zero (default) indicates that there should be no connect timeout.
 95    connectionTimeoutMillis: 3000
 96    # Specifies the maximum length of time in milliseconds that an operation should
 97    # be allowed to block while waiting for a response from the server.
 98    # A value of zero indicates that there should be no timeout.
 99    responseTimeoutMillis: 5000
100    # Specifies whether to use the SO_KEEPALIVE option for the underlying sockets
101    # used by associated connections.
102    keepAlive: true
103    # Specifies whether to use the TCP_NODELAY option for the underlying sockets.
104    tcpNoDelay: true
105    # Specifies whether to operate in synchronous mode, in which at most one
106    # operation may be in progress at any time on a given connection.
107    # When using asynchronous mode, a background thread takes care of multiplexing
108    # and dispatching all the operations on connections that are shared for
109    # multiple operations.
110    synchronousMode: true
111    # Specifies the length of time in milliseconds between periodic background
112    # health checks against the available connections in this pool.
113    healthCheckIntervalMillis: 120000
114    # Specifies whether associated connections should attempt to follow any
115    # referrals that they encounter.
```

```
116     followReferrals: true
117     # Specifies the maximum number of hops that a connection should take when
118     # trying to follow a referral, must be greater than zero when 'followReferrals'
119     # is true.
120     referralHopLimit: 1
121     # Specifies the maximum size in bytes for an LDAP message that a connection
122     # will attempt to read from the directory server.
123     # If it encounters an LDAP message that is larger than this size, then the
124     # connection will be terminated.
125     # Disabled when not specified or set to 0.
126     maxMessageSize: 1024
127
128 pool2:
129     # A failover pool that uses the same set of servers for read and for
130     # write operations.
131     failover:
132       - ldap0.example.com
133       - ldap1.example.com
134     pool-min: 5
135     pool-max: 20
136     trust-store:
137       file: /etc/trust.jks
138     key-store:
139       file: /etc/private.jks
140
141 pool3:
142     # A simple single-host setup
143     host: ldap.example.com
144     pool-min: 5
145     pool-max: 20
146
147 pool4:
148     # A load-balancing setup that will use a round-robin algorithm to
149     # select the server to which the connection should be established.
150     # Any number of servers may be included, and each request will
151     # attempt to retrieve a connection to the next server in the list,
152     # circling back to the beginning of the list as necessary.
153     # If a server is unavailable when an attempt is made to establish
154     # a connection to it, then the connection will be established to
155     # the next available server in the set.
156     round-robin:
157       - host: ldap1.example.com
158         port: 10389
159         responseTimeoutMillis: 5000
160       - host: ldap2.example.com
161         port: 10389
162         responseTimeoutMillis: 12000
163     pool-min: 10
164     pool-max: 50
165
166 pool5:
167     # A DNS RR setup handles the case in which a given hostname may
168     # resolve to multiplee IP addresses.
169     # Note that while a setup like this is typically referred to as
170     # "round-robin DNS", this option does not strictly require DNS (as names
171     # may be resolved through alternate mechanisms like a hosts file or an
172     # alternate name service), and it does not strictly require round-robin
173     # use of those addresses (as alternate ordering mechanisms like
174     # 'random' or 'failover' may be used).
175     dns-round-robin:
176       host: ldap.example.com
177       # The selection mode that should be used if the hostname resolves
178       # to multiple addresses.
179       # Possible values:
180       # - random: the order of addresses will be randomized for each attempt
181       # - failover: addresses will be consistently attempted in the order
182       #          they are retrieved from the name service.
183       # - round-robin: connection attempts will be made in a round-robin order
184       selection-mode: random
185       # Only use DNS if set to 'true'.
186       # If set to 'false' then the operating system's hostname resolution
187       # service will be used, which may include a hosts file.
```

```
188       only-dns: false
189       # The maximum length of time in milliseconds to cache addresses resolved
190       # from the provided hostname.
191       # Caching resolved addresses can result in better performance and can
192       # reduce the number of requests to the name service.
193       # A value that is less than or equal to zero indicates that no caching
194       # should be used.
195       cache-timeout: 1440000
196     pool-min: 5
197     pool-max: 20
198
199   pool6:
200     # A failover pool that uses the same set of servers for read and for
201     # write operations, as well as StartTLS
202     failover:
203       - ldap0.example.com
204       - ldap1.example.com
205     pool-min: 5
206     pool-max: 20
207     starttls: true
208     trust-store:
209       file: /etc/trust.jks
210     key-store:
211       file: /etc/private.jks
```

File 7　/opt/open-xchange/etc/plugins-blackwhitelist.properties

```
1  # Setting to control the used connector for a specific user
2  # This setting is config-cascade aware to support different implementations for each user.
3  # Default is <none> which means that the feature is disabled for a user
4  com.openexchange.plugins.blackwhitelist.connector=
5
6  # Setting to check if memory backed test System should be started
7  # This connector is identified by plugins_blwl_test
8  # Default: false
9  com.openexchange.plugins.blackwhitelist.test=false
```

File 8　/opt/open-xchange/etc/plugins-blacklist-sieve.properties

```
1  # Identifier of this blackwhitelist connector: plugins_blackwhitelist_sieve
2  # Setting to control the rulename to be set and checked as a antispam value inside the
       sieve rules
3  # Default: Blacklist
4  # Config-cascade aware: true
5  # Lean: true
6  com.openexchange.plugins.blackwhitelist.connector.sieve.rulename=Blacklist
7
8  # Setting to control wether the blacklisted mails should be moved to SPAM or deleted
       directly
9  # If set to true, mails are moved to SPAM
10 # If set to false, mails are deleted
11 # Default: true
12 # Config-cascade aware: true
13 # Lean: true
14 com.openexchange.plugins.blackwhitelist.connector.sieve.moveToSpam=true
15
16 # Setting to check if memory backed test System should be started
17 # This connector is identified by plugins_blwl_test
18 # Default: false
19 com.openexchange.plugins.blackwhitelist.connector.sieve.test=false
```

File 9 /opt/open-xchange/etc/twilio.properties

```
1   # Twilio accountSID
2   com.openexchange.plugins.sms.twilio.accountSID=ACCOUNT_SID
3
4   # Twilio auth token
5   com.openexchange.plugins.sms.twilio.authtoken=AUTH_TOKEN
6
7   # Twilio Message Service SID
8   com.openexchange.plugins.sms.twilio.messageservicesid=SERVICE_SID
9
10  # Max message length. 1600 characters is Twilio's maximum
11  com.openexchange.plugins.sms.twilio.maxlength=1600
```