AppSuite Engineering Services Plugins
Release Notes for Release 1.3.2

2017-11-17

Copyright notice

Contents

1 General Information

1.1 Warnings

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

Warning
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/1.3.2/DebianJessie
https://software.open-xchange.com/components/plugins/stable/1.3.2/RHEL6
https://software.open-xchange.com/components/plugins/stable/1.3.2/RHEL7
https://software.open-xchange.com/components/plugins/stable/1.3.2/SLE_12

1.3 Build Dependencies

This delivery was build and tested with following dependencies:

```
frontend-7.8.4-rev15
```

2 Shipped Product and Version

2.1 Package open-xchange-appsuite-blackwhitelist

Black/Whitelist plugin for App Suite
Version: 1.3.2-5
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/meta/blackwhitelist.yml (page 7)
/opt/open-xchange/etc/settings/blackwhitelist.properties (page 7)

2.2 Package open-xchange-appsuite-sieve-blacklist

Blacklist plugin for App Suite
Version: 1.3.2-5
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/meta/blacklist.yml (page 7)
/opt/open-xchange/etc/settings/blacklist.properties (page 8)

2.3 Package open-xchange-authentication-masterpassword

Authentication implementation that uses a global password for all users – DO NOT USE IN PRODUCTION 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: 1.3.2-5
Type: OX Middleware Plugin
Depends on:

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

Conficts 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 8)

2.4 Package open-xchange-ldap-client

This package provides an advanced LDAP client library that is used by other Open-Xchange bundles.
Version: 1.3.2-5
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 11)

2.5 Package open-xchange-plugins-blackwhitelist

Plugins abstraction layer for blacklist/whitelist connectors
Version: 1.3.2-5
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 12)

2.6 Package open-xchange-plugins-blackwhitelist-sieve

This package installs the OSGi bundles needed to access the blacklist for plugins within Sieve
Version: 1.3.2-5
Type: OX Middleware Plugin
Depends on:

```
open-xchange-core (>=7.8.4)
open-xchange-mailfilter (>=7.8.4)
open-xchange-plugins-blackwhitelist (>=1.3.2)
```

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 12)

2.7 Package open-xchange-sms-twilio

This package installs the OSGi bundles needed to send SMS messages via twilio
Version: 1.3.2-5
Type: OX Middleware Plugin
Depends on:

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

2.7.1 Installation

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

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

2.7.2 Configuration

For details, please see appendix A
/opt/open-xchange/etc/twilio.properties (page 12)

2.8 Package open-xchange-util-imap

This package is a library that provides various utilities for IMAP.
Version: 1.3.2-5
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-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 Bugs fixed with this Release

This section provides a summary of bug fixes and changes that have been applied subsequently to shipping Release 1.3.1. Some of the announced bug fixes may have already been fixed at the existing code-base via Patch Releases.

ES-231 ldap-client: connections are established at bundle startup
Status: Done
Affected Packages: open-xchange-ldap-client

4 Changes relevant for Operators

4.1 Changes of Behaviour

Change #ES-228 ldap-client: StartTLS support
Status: Done
Affected Packages: open-xchange-ldap-client

Change #ES-229 ldap-client: upgrade unboundid library to 4.0.1
Status: Done
Affected Packages: open-xchange-ldap-client

Change #ES-232 ldap-client: add pool id aliasing
Status: Done
Affected Packages: open-xchange-ldap-client

5 Tests

Not all defects that got resolved could be reproduced within the lab. Therefore, we advise guided and close monitoring of the reported defect when deploying to a staging or production environment. Defects which have not been fully verified, are marked as such.
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.

6 Fixed Bugs

ES-231,

A Configuration Files

File 1 /opt/open-xchange/etc/meta/blackwhitelist.yml

```
io.ox/mail//blackwhitelist/maxAddresses:
    protected: false
io.ox/mail//blackwhitelist/allowDuplicates:
    protected: false
io.ox/mail//blackwhitelist/validateAddresses:
    protected: false
io.ox/mail//blackwhitelist/editable:
    protected: false
io.ox/mail//blackwhitelist/showAddButton:
    protected: false
io.ox/mail//blackwhitelist/showEditButton:
    protected: false
io.ox/mail//blackwhitelist/showSaveButton:
    protected: false
io.ox/mail//blackwhitelist/searchable:
    protected: false
```

File 2 /opt/open-xchange/etc/settings/blackwhitelist.properties

```
##
# Blackwhitelist settings
#
# Max number of addressed on the list
io.ox/mail//blackwhitelist/maxAddresses = 250
# Allow users to add duplicates
io.ox/mail//blackwhitelist/allowDuplicates = false
# Validate if only valid mail addresses are on the list
io.ox/mail//blackwhitelist/validateAddresses = false
# Allow users to edit items on their list
io.ox/mail//blackwhitelist/editable = false
# Allow users to manually add addresses
io.ox/mail//blackwhitelist/showAddButton = false
# Show edit button next to entry
io.ox/mail//blackwhitelist/showEditButton = false
# Show save button next to entry when creating it
io.ox/mail//blackwhitelist/showSaveButton = false
# Show search box for blacklist
io.ox/mail//blackwhitelist/searchable = true
```

File 3 /opt/open-xchange/etc/meta/blacklist.yml

```
io.ox/mail//blacklist/ruleName:
    protected: false
io.ox/mail//blacklist/maxAddresses:
    protected: false
io.ox/mail//blacklist/allowDuplicates:
    protected: false
io.ox/mail//blacklist/validateAddresses:
    protected: false
io.ox/mail//blacklist/userEditable:
    protected: false
io.ox/mail//blacklist/showAddButton:
    protected: false
```

File 4 /opt/open-xchange/etc/settings/blacklist.properties

```
# Name of the rule used as blacklist
io.ox/mail//blacklist/ruleName = Blocklist
# Max number of addressed on the list
io.ox/mail//blacklist/maxAddresses = 250
# Allow users to add duplicates
io.ox/mail//blacklist/allowDuplicates = false
# Validate if only valid mail addresses are on the list
io.ox/mail//blacklist/validateAddresses = false
# Allow users to edit items on their list
io.ox/mail//blacklist/editable = false
# Allow users to manually add addresses
io.ox/mail//blacklist/showAddButton = false
# Show edit button next to entry
io.ox/mail//blacklist/showEditButton = false
# Show save button next to entry when creating it
io.ox/mail//blacklist/showSaveButton = false
# Show search box for blacklist
io.ox/mail//blacklist/searchable = true
```

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

```
# Configuration file for the master password authentication plugin
#
# DO NOT USE IN PRODUCTION !
#

# The clear text password to authenticate all users.
# Mandatory.
# Example:
# com.openexchange.authentication.masterpassword.password=supersecret
com.openexchange.authentication.masterpassword.password=

# The default value for the context when it is not specified.
# Optional and defaults to using the "defaultcontext" mapping.
#com.openexchange.authentication.masterpassword.default.context=

# Whether the username portion of the login should be lowercased
# before being looked up in the user database.
# Optional and defaults to false
#com.openexchange.authentication.masterpassword.lowercase=false

# Whether the context name portion of the login should be lowercased
# before being looked up in the context database.
# Optional and defaults to false
#com.openexchange.authentication.masterpassword.lowercase.context=false

# Whether to use the complete login string as the username,
# e.g. login "foo@bar.com" -> user name "foo@bar.com" and
# context name "bar.com"
# Optional and defaults to false
#com.openexchange.authentication.masterpassword.use.full.login.info=false

# Whether to use the complete login string for the context name,
# e.g. login "foo@bar.com" -> context name "foo@bar.com"
# Optional and defaults to false
#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

```
# The top-level key is the identifier of the pool, which can be
# any string of text and is being used by the bundles and applications
# to access that pool configuration.
```

```
# Typically, those are fixed or need to be configured in the bundles
# that use this library.
pool1:
  trust-store:
    # SSL: path to the JKS trust store file that contains the anchors
    file: /etc/trust.jks
    # SSL: indicates whether to reject certificates if the current time
    # is outside the validity window for the certificate
    validity: true
  key-store:
    # SSL: path to the JKS client key store file that contains the key
    file: /etc/private.jks
    # SSL: password to access the keystore and the key
    password: foobar
    # SSL: alias of the key to use
    alias: key
  # Configure a read/write pool with different settings for read operations
  # and for write operations (i.e. different pools of LDAP servers).
  # Here comes the part for the read operations:
  read:
    # Use a failover cluster of two nodes:
    failover:
      - ldap1.example.com
      - ldap2.example.com
    # Pool connection management
    # -------------------------
    # When creating a connection pool, you may specify an initial number of
    # connections (pool-min) and a maximum number of connections (pool-max).
    # The initial number of connections is the number of connections that should
    # be immediately established and available for use when the pool is created.
    # The maximum number of connections is the largest number of unused connections
    # that may be available in the pool at any time.
    # Whenever a connection is needed, whether by an attempt to check out a
    # connection or to use one of the pool's methods to process an operation,
    # the pool will first check to see if there is a connection that has already
    # been established but is not currently in use, and if so then that connection
    # will be used.
    # If there aren't any unused connections that are already established, then
    # the pool will determine if it has yet created the maximum number of
    # connections, and if not then it will immediately create a new connection
    # and use it.
    # If the pool has already created the maximum number of connections, then the
    # pool may wait for a period of time (as configured using 'maxWaitTimeMillis' below,
    # which has a default value of zero to indicate that it should not wait at all)
    # for an in-use connection to be released back to the pool.
    # If no connection is available after the specified wait time (or there should
    # not be any wait time), then the pool may automatically create a new connection
    # to use if 'createIfNecessary' is true (which is the default).
    # If it is able to successfully create a connection, then it will be used.
    # If it cannot create a connection, or if 'createIfNecessary' is set to false,
    # then an error will be thrown.
    # Note that the maximum number of connections specified when creating a pool
    # refers to the maximum number of connections that should be available for use
    # at any given time.
    # If 'createIfNecessary' is set to true, then there may temporarily be more
    # active connections than the configured maximum number of connections.
    # This can be useful during periods of heavy activity, because the pool will
    # keep those connections established until the number of unused connections
    # exceeds the configured maximum.
    # If you wish to enforce a hard limit on the maximum number of connections so
    # that there cannot be more than the configured maximum in use at any time,
    # then set 'createIfNecessary' to false to indicate that the pool should not
    # automatically create connections when one is needed but none are available,
    # and you may also want to set 'maxWaitTimeMillis' to a maximum wait time to allow
    # the pool to wait for a connection to become available rather than throwing
    # an exception if no connections are immediately available.
    pool-min: 10
    pool-max: 50
    maxConnectionAgeMillis: 30000
    maxWaitTimeMillis: 500
    createIfNecessary: true
    # 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

```
# Setting to control the used connector for a specific user
# This setting is config-cascade aware to support different implementations for each user.
# Default is <none> which means that the feature is disabled for a user
com.openexchange.plugins.blackwhitelist.connector=

# Setting to check if memory backed test System should be started
# This connector is identified by plugins_blwl_test
# Default: false
com.openexchange.plugins.blackwhitelist.test=false
```

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

```
# Identifier of this blackwhitelist connector: plugins_blackwhitelist_sieve
# Setting to control the rulename to be set and checked as a antispam value inside the sieve rules
# Default: Blacklist
# Config-cascade aware: true
# Lean: true
com.openexchange.plugins.blackwhitelist.connector.sieve.rulename=Blacklist

# Setting to control wether the blacklisted mails should be moved to SPAM or deleted directly
# If set to true, mails are moved to SPAM
# If set to false, mails are deleted
# Default: true
# Config-cascade aware: true
# Lean: true
com.openexchange.plugins.blackwhitelist.connector.sieve.moveToSpam=true

# Setting to check if memory backed test System should be started
# This connector is identified by plugins_blwl_test
# Default: false
com.openexchange.plugins.blackwhitelist.connector.sieve.test=false
```

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

```
# Twilio accountSID
com.openexchange.plugins.sms.twilio.accountSID=ACCOUNT_SID

# Twilio auth token
com.openexchange.plugins.sms.twilio.authtoken=AUTH_TOKEN

# Twilio Message Service SID
com.openexchange.plugins.sms.twilio.messageservicesid=SERVICE_SID

# Max message length. 1600 characters is Twilio's maximum
com.openexchange.plugins.sms.twilio.maxlength=1600
```