



OpenIDM Release Notes

Version 2.1.2

Mark Craig
Lana Frost
Andi Egloff

ForgeRock AS
33 New Montgomery St.,
Suite 1500
San Francisco, CA 94105, USA
+1 415-599-1100 (US)
www.forgerock.com

Copyright © 2011-2015 ForgeRock AS

Abstract

Notes covering OpenIDM software requirements, fixes, compatibility issues, and known issues. The OpenIDM project offers flexible, open source services for automating management of the identity life cycle.



This work is licensed under the [Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License](http://creativecommons.org/licenses/by-nc-nd/3.0/).

To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

ForgeRock™ is the trademark of ForgeRock Inc. or its subsidiaries in the U.S. and in other countries. Trademarks are the property of their respective owners.

UNLESS OTHERWISE MUTUALLY AGREED BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

DejaVu Fonts

Bitstream Vera Fonts Copyright

Copyright (c) 2003 by Bitstream, Inc. All Rights Reserved. Bitstream Vera is a trademark of Bitstream, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of the fonts accompanying this license ("Fonts") and associated documentation files (the "Font Software"), to reproduce and distribute the Font Software, including without limitation the rights to use, copy, merge, publish, distribute, and/or sell copies of the Font Software, and to permit persons to whom the Font Software is furnished to do so, subject to the following conditions:

The above copyright and trademark notices and this permission notice shall be included in all copies of one or more of the Font Software typefaces.

The Font Software may be modified, altered, or added to, and in particular the designs of glyphs or characters in the Fonts may be modified and additional glyphs or characters may be added to the Fonts, only if the fonts are renamed to names not containing either the words "Bitstream" or the word "Vera".

This License becomes null and void to the extent applicable to Fonts or Font Software that has been modified and is distributed under the "Bitstream Vera" names.

The Font Software may be sold as part of a larger software package but no copy of one or more of the Font Software typefaces may be sold by itself.

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL BITSTREAM OR THE GNOME FOUNDATION BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

Except as contained in this notice, the names of Gnome, the Gnome Foundation, and Bitstream Inc., shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Font Software without prior written authorization from the Gnome Foundation or Bitstream Inc., respectively. For further information, contact: fonts at gnome dot org.

Arev Fonts Copyright

Copyright (c) 2006 by Tavmjong Bah. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of the fonts accompanying this license ("Fonts") and associated documentation files (the "Font Software"), to reproduce and distribute the modifications to the Bitstream Vera Font Software, including without limitation the rights to use, copy, merge, publish, distribute, and/or sell copies of the Font Software, and to permit persons to whom the Font Software is furnished to do so, subject to the following conditions:

The above copyright and trademark notices and this permission notice shall be included in all copies of one or more of the Font Software typefaces.

The Font Software may be modified, altered, or added to, and in particular the designs of glyphs or characters in the Fonts may be modified and additional glyphs or characters may be added to the Fonts, only if the fonts are renamed to names not containing either the words "Tavmjong Bah" or the word "Arev".

This License becomes null and void to the extent applicable to Fonts or Font Software that has been modified and is distributed under the "Tavmjong Bah Arev" names.

The Font Software may be sold as part of a larger software package but no copy of one or more of the Font Software typefaces may be sold by itself.

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL TAVMJONG BAH BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

Except as contained in this notice, the name of Tavmjong Bah shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Font Software without prior written authorization from Tavmjong Bah. For further information, contact: tavmjong @ free . fr.

Table of Contents

| | |
|---|----|
| 1. What's New in OpenIDM 2.1.2 | 1 |
| 1.1. New Features | 1 |
| 1.2. OpenIDM Documentation | 2 |
| 2. Before You Install OpenIDM Software | 3 |
| 3. OpenIDM Fixes, Limitations, & Known Issues | 5 |
| 3.1. Fixes and Improvements | 5 |
| 3.2. Limitations | 7 |
| 3.3. Known Issues | 7 |
| 4. OpenIDM Compatibility | 13 |
| 4.1. Major Changes to Existing Functionality | 13 |
| 4.2. Minor Changes to Existing Functionality | 13 |
| 4.3. Deprecated Functionality | 14 |
| 4.4. Removed Functionality | 14 |
| 5. How to Report Problems & Provide Feedback | 15 |
| 6. Support | 17 |

Chapter 1

What's New in OpenIDM 2.1.2

OpenIDM 2.1.2 is a maintenance release that resolves a number of issues, including security issues in OpenIDM. It is strongly recommended that you update to this release to make your deployment more secure, and to take advantage of important functional fixes. ForgeRock customers can contact support for help and further information.

Before you install OpenIDM or update your existing OpenIDM installation, read these release notes. Then update or install OpenIDM.

For installation instructions and several samples to familiarize you with the features, see the [OpenIDM 2.1.0 Installation Guide](#).

For an architectural overview and high-level presentation of OpenIDM, see the [Architectural Overview](#) chapter in the *OpenIDM 2.1.0 Integrator's Guide*.

1.1 New Features

Compared to the OpenIDM 2.1.1 release, OpenIDM 2.1.2 fixes a number of issues and provides the following new features:

- [OPENIDM-957](#): Ability to launch startup.sh and cli.sh from any directory
- [OPENIDM-1764](#): New launcher.bat override, including install-service.bat

1.2 OpenIDM Documentation

You can read the following additional [product documentation](#) for OpenIDM 2.1.0 online at <http://docs.forgerock.org>.

- [OpenIDM 2.1.0 Release Notes](#)
- [OpenIDM 2.1.0 Installation Guide](#)
- [OpenIDM 2.1.0 Integrator's Guide](#)

Chapter 2

Before You Install OpenIDM Software

This chapter covers prerequisites for installing and running OpenIDM software.

For OpenIDM 2.1.2, the following configurations are supported for use in production.

Repository

The following JDBC repositories are supported for use in production:

- MySQL 5.1 or 5.5 with Connector/J 5.1.18 or later
- Microsoft SQL Server 2008 Express
- Oracle Database 11g Enterprise Edition

OrientDB is provided for evaluation only.

Stand-alone installation

You must install OpenIDM as a stand-alone service, using Apache Felix and Jetty as provided. Alternate containers are not supported.

This OpenIDM release bundles Jetty version 7.6.2.v20120308.

Connectors

OpenIDM 2.1.2 comes packaged with these OpenICF connectors:

- CSV File
- LDAP

-
- Scripted SQL
 - XML File
 - Database Table

ForgeRock provides additional connectors, as listed on the [OpenICF project connectors site](#).

If you have a special request to support a component or combination not listed here, contact ForgeRock at info@forgerock.com.

OpenIDM requires Java SE JDK 6 update 24 or later. When using the Oracle JDK, you also need Java Cryptography Extension (JCE) [policy files](#).

On Windows systems, use Java SE JDK 7 update 6 or later, to take advantage of a recent JVM fix relating to non-blocking sockets with the default Jetty configuration.

You need 150 MB disk space and 1 GB memory for an evaluation installation. For a production installation, disk space and memory requirements will depend on the size of the repository, and on size of the audit and service log files that OpenIDM writes.

Chapter 3

OpenIDM Fixes, Limitations, & Known Issues

OpenIDM issues are tracked at <https://bugster.forgerock.org/jira/browse/OPENIDM>.

3.1 Fixes and Improvements

OpenIDM 2.1.2 includes the following major fixes and improvements.

- [OPENIDM-2776](#): Install path with space not handled correctly in shutdown.sh
- [OPENIDM-2500](#): properties set as encrypted in managed.json written in plain text in activity audit when new and old values are the same
- [OPENIDM-2480](#): Enable READ_COMMITTED_SNAPSHOT isolation w/MSSQL
- [OPENIDM-2127](#): Switching existing schedule from persisted=false to persisted=true results in duplicate scheduled jobs.
- [OPENIDM-1915](#): Add ability to configure the HTTP session timeout for the OpenIDM UI
- [OPENIDM-1907](#): Recon failures as a result of policy violations do not indicate the cause of the violation in the recon audit log.
- [OPENIDM-1885](#): onUnlink trigger throws NPE if invoked for SOURCE_MISSING situation (action=UNLINK) during target reconciliation

- [OPENIDM-1755](#): Recon target phase is always single threaded regardless of the number of configured taskThreads
- [OPENIDM-1739](#): Changes made to target objects by onLink triggers should be persisted if the situation action is UPDATE
- [OPENIDM-1665](#): Startup failure when connectors directory contains arbitrary sub-directories
- [OPENIDM-1663](#): Deadlock within OpenIDM when updating managed users w/ MSSQL as the repository
- [OPENIDM-1658](#): Hard-coded reference to database schema and table name in jdbc config files
- [OPENIDM-1655](#): External Rest Service erroneously sets the remote auth ChallengeScheme to HTTP_COOKIE instead of HTTP_BASIC
- [OPENIDM-1652](#): Policy violation doesn't prevent managed objects creation
- [OPENIDM-1647](#): LiveSync fails when using Generic LDAP Connector if readSchema=false
- [OPENIDM-1629](#): Policy cannot-contain-others raises an exception when one of the fields to check against is absent
- [OPENIDM-1624](#): Linux rc script generated by create-openidm-rc.sh fails to shutdown OpenIDM when installed to a directory other than 'openidm'
- [OPENIDM-1584](#): java.lang.OutOfMemoryError exception
- [OPENIDM-1583](#): OpenIDM should not enforce the REAUTH_REQUIRED policy for openidm-cert role.
- [OPENIDM-1563](#): Task scanner creates a new thread pool for each execution resulting in a thread leak.
- [OPENIDM-1433](#): OpenIDM renames entry on update (OpenIDM ICF glue code sets __NAME__ to __UID__)
- [OPENIDM-1416](#): Default onCreate script of UI sets the accountStatus to 'active', overrides the value of the managed user attribute
- [OPENIDM-1281](#): Query for "get-by-field-value" is incorrect
- [OPENIDM-1256](#): additionalPolicies option in policy.json not working
- [OPENIDM-1236](#): ScriptableList: cannot put 0 (zero) index element
- [OPENIDM-1170](#): Linux startup script generator is not working correctly

- [OPENIDM-1147](#): Install path with space not handled correctly in startup.sh
- [OPENIDM-969](#): Console login fails and leaves OpenIDM in unusable state

3.2 Limitations

OpenIDM 2.1.2 has the following known limitations:

- A conditional GET request, with the If-None-Match request header, is not currently supported.
- The keystore password, the truststore password and the secret key passwords must all be set to the same value. If you use different passwords, OpenIDM is unable to read the required keys and certificates.
- Connectors generally use the global JVM settings for keystore and truststore, rather than the settings that are specified in the boot.properties file. You can work around this by specifying a path to the keystore or truststore in the conf/system.properties file. For example:

```
# Set the truststore
javax.net.ssl.trustStore=/path/to/openidm/security/truststore
```

3.3 Known Issues

OpenIDM 2.1.2 has the following known issues.

- [OPENIDM-2595](#): OpenIDM failed to start-up during installation
- [OPENIDM-2312](#): SmartEvent framework maintains a unbounded event name cache which consumes the entire heap
- [OPENIDM-2184](#): NPE thrown from within ObjectMapping \$SyncOperation.isValidSource() during reconciliation.
- [OPENIDM-2078](#): PermGen leak in "source" scripts
- [OPENIDM-2034](#): Support arbitrary [commons] auth modules via className
- [OPENIDM-1946](#): Working location flag (-w) not working as documented
- [OPENIDM-1912](#): Exception from OpenIDMResolverFactory if used in a parallel execution workflow task
- [OPENIDM-1878](#): DELETE situation-actions on managed objects in bidirectional mappings result in incorrect LINK_ONLY

- [OPENIDM-1860](#): Null pointer exception when setting target attribute during onUnlink
- [OPENIDM-1823](#): getScriptBindings function of ServiceScript (ScriptRegistryImpl.java) slows down extremely when accessed parallel from multiple threads
- [OPENIDM-1770](#): CLI tool needs the ability to authenticate as a user other than openidm-admin w/default password
- [OPENIDM-1664](#): Memory usage of AD connector continue to increase.
- [OPENIDM-1637](#): Problem in UI when the username contains a space char.
- [OPENIDM-1632](#): create-openidm-logrotate.sh is not properly defined
- [OPENIDM-1619](#): OperationOptions specified within the provisioner configuration are not passed to connectors by OpenIDM
- [OPENIDM-1600](#): Cluster with Oracle DB backend
- [OPENIDM-1574](#): AD sync service might crash after applying latest Windows updates
- [OPENIDM-1564](#): __NAME__ attribute incorrectly required as part of object definition for a create action
- [OPENIDM-1562](#): Route to endpoint service not found if there is a resourcename after the name of the endpoint
- [OPENIDM-1560](#): when starting OpenIDM with -p option logging.properties file is not taken in project location
- [OPENIDM-1535](#): incomplete handleQuery implementation in ScriptedRequestHandler
- [OPENIDM-1530](#): OpenIDM self-signed certificates in keystore and truststore does not match
- [OPENIDM-1513](#): Inconsistency in script context: request object has different representations
- [OPENIDM-1511](#): Policy.java overwrites the action parameter of async recon
- [OPENIDM-1509](#): false 'validSource' entries still being evaluated, and returned correlation records are unexpectedly DELETED
- [OPENIDM-1507](#): Logging level change to FINE causes NullPointerException in OrientDBRepoService

- [OPENIDM-1504](#): OpenICFProvisionerService handle method performs `logger.isDebugEnabled()` checks but logs at the error level
- [OPENIDM-1503](#): `InvalidCredentialException` thrown from OpenICFProvisionerService uses 500 HTTP error code
- [OPENIDM-1501](#): `sync?_action=performAction` with an `action=DELETE` results in a delete on the source rather than the target
- [OPENIDM-1489](#): Command line needs to allow supplying user/pwd
- [OPENIDM-1483](#): Pool size settings not effective for OrientDB repo
- [OPENIDM-1445](#): Provisioner service does not decrypt encrypted attributes before passing them to OpenICF framework
- [OPENIDM-1444](#): json schema package needs to specify export version and import version ranges
- [OPENIDM-1430](#): OpenIDM needs a restart after importing a new cert via REST API
- [OPENIDM-1417](#): Throwing 401 exception in augment security context javascript ends up being a 500 in the response
- [OPENIDM-1413](#): In async recon starter script (`workflow.js`) the query of the already running instances is executed before all it's parameters are set
- [OPENIDM-1412](#): Missing 'not undefined' check for `sourceId` and `targetId` in async recon workflow starter script (`workflow.js`)
- [OPENIDM-1411](#): Add not null check to async recon starter script (`workflow.js`) for `sourceId` query parameter, fill `businessKey` field of the workflow when starting a new workflow
- [OPENIDM-1390](#): Unable to parse boolean configuration values from custom OpenICF provisioner
- [OPENIDM-1380](#): `opendj-accountchange-handler` schema does not load schema provided after install
- [OPENIDM-1379](#): ADD operation failed for OpenDJ account notification handler
- [OPENIDM-1361](#): Exception from UI when a workflow started by scheduler has a user task in it
- [OPENIDM-1358](#): Connector test of LDAP fails
- [OPENIDM-1338](#): Validation for create without `objectId` is always true

- [OPENIDM-1329](#): OrientDB as repo does not initialize if there is no network connection
- [OPENIDM-1293](#): OpenIDMELResolver should use component.name to bind JavaDelegate implementations instead of component.id
- [OPENIDM-1269](#): some issues with Case Sensitivity options for Sync
- [OPENIDM-1267](#): Add Enum and DateFormType specific data to the taskdefinitions returned by Activiti
- [OPENIDM-1265](#): liveSync process should never get stuck because of exceptions with the synchronizationListener.
- [OPENIDM-1245](#): Align openidm and activiti contract on scripting(openidm.action() and openidm.patch() failed in a workflow on managed object.)
- [OPENIDM-1219](#): DB/Config bootstrapping should use IdentityServer support for getting properties, including boot prop
- [OPENIDM-1218](#): Audit filter on eventTypes for recon.csv does not work properly
- [OPENIDM-1210](#): Directly-assigned workflow tasks disappear when "Requeue" button is hit
- [OPENIDM-1190](#): Disable Quartz update check by default
- [OPENIDM-1186](#): PATCH with POST using MVCC are successful even if revision wrong
- [OPENIDM-1184](#): sample/sample3 and sample/provisioner use hardcoded path in provisioner configuration.
- [OPENIDM-1175](#): IE9 and below aggressively cache AJAX requests, causing the UI to behave strangely
- [OPENIDM-1174](#): Some UI Features are Indistinguishable From Plaintext
- [OPENIDM-1165](#): EXCEPTION action when doing liveSync stops the synctoken processing
- [OPENIDM-1162](#): With OrientDB, for a MISSING/CREATE situation/action, reconciliation creates a new link instead of using an existing link
- [OPENIDM-1142](#): Harmless error message may appear when starting OpenIDM
- [OPENIDM-1141](#): OrientDB config bootstrap repository does not use .json config file, only properties

- [OPENIDM-1133](#): Certain sample files contain unnecessary, unused entries
- [OPENIDM-1129](#): OpenIDM freezes when the connection to the repository is interrupted
- [OPENIDM-1117](#): Malformed content-type request header produces 500 error
- [OPENIDM-1115](#): When an LDAP user is created through the REST API, the `_id` that is returned is not normalized
- [OPENIDM-1098](#): `onDelete` script generates exception
- [OPENIDM-1096](#): A PUT command on a configuration object may return an incorrect value
- [OPENIDM-1094](#): Starting a second OpenIDM instance with a conflicting port causes the instance to freeze
- [OPENIDM-1093](#): A user's `accountStatus` (active or inactive) has no effect on the UI or the REST API
- [OPENIDM-1074](#): disabling automatic polling for changes of config file not possible on new install
- [OPENIDM-1021](#): Wrong starting arguments during start could throw an error or warning.
- [OPENIDM-964](#): An incorrect password in `boot.properties` causes OpenIDM to hang on startup
- [OPENIDM-848](#): Conflicting behavior might be observed between the default fields set by the `onCreate` script and policy enforcement
- [OPENIDM-470](#): OpenIDM cannot rename objects - if the identifier of the object changes, the associated link breaks

Chapter 4

OpenIDM Compatibility

This chapter covers both major changes to existing functionality, and also deprecated and removed functionality.

4.1 Major Changes to Existing Functionality

There are no major changes that will have an impact on existing deployments in this maintenance release.

4.2 Minor Changes to Existing Functionality

The following change will have a minor impact on existing deployments.

Change to additional policy specification

With the resolution of [OPENIDM-1256](#), the way in which additional policy files are referenced in the `policy.json` configuration file has changed.

In previous OpenIDM versions, the path to additional policy files was relative to the root of the OpenIDM installation directory. In OpenIDM 2.1.2, the path to additional files is relative to the *project* directory (if you start the server using the `-p` option).

For example, if you had started OpenIDM with the configuration for Sample 1 in a previous version, you would have specified an additional policy file as follows:

```
{
```

```
"type" : "text/javascript",
"file" : "bin/defaults/script/policy.js",
"additionalFiles" : [
  "samples/sample1/script/password-policy.js"
],
"resources" : [
...
}
```

In OpenIDM 2.1.2, you would specify the additional file as follows:

```
{
  "type" : "text/javascript",
  "file" : "bin/defaults/script/policy.js",
  "additionalFiles" : [
    "script/password-policy.js"
  ],
  "resources" : [
...
}
```

4.3 **Deprecated Functionality**

No additional functionality is planned to be deprecated at this time.

4.4 **Removed Functionality**

No functionality has been removed in OpenIDM 2.1.2.

Chapter 5

How to Report Problems & Provide Feedback

If you have questions regarding OpenIDM which are not answered by the documentation, there is a mailing list which can be found at <https://lists.forgerock.org/mailman/listinfo/openidm> where you are likely to find an answer.

If you have found issues or reproducible bugs within OpenIDM 2.1.2, report them in <https://bugster.forgerock.org>.

When requesting help with a problem, please include the following information:

- Description of the problem, including when the problem occurs and its impact on your operation
- Machine type, operating system version, Java version, and OpenIDM release version, including any patches or other software that might be affecting the problem
- Steps to reproduce the problem
- Any relevant access and error logs, stack traces, or core dumps

Chapter 6

Support

You can purchase OpenIDM support subscriptions and training courses from ForgeRock and from consulting partners around the world and in your area. To contact ForgeRock, send mail to info@forgerock.com. To find a partner in your area, see <http://forgerock.com/partners/find-a-partner/>.

