OpenIDM 2.0.3 Release Notes

Mark Craig
Andi Egloff
March 30, 2012

Copyright © 2011-2012 ForgeRock AS

Abstract

Notes covering OpenIDM software requirements, fixes, 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[1].

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.

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, MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, 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 NONINFRINGEMENT 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 NONINFRINGEMENT 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.

[1] http://creativecommons.org/licenses/by-nc-nd/3.0/

Table of Contents

1. What's New in OpenIDM 2.0.3 1
2. Before You Install OpenIDM Software 3
3. OpenIDM Fixes, Limitations, & Known Issues 5
4. OpenIDM Compatibility 9
5. How to Report Problems & Provide Feedback 11
6. Support 13

Chapter 1. What's New in OpenIDM 2.0.3

OpenIDM 2.0.3 provides many new features, including the following:

- OSGi based runtime
- Embedded OrientDB as the out-of-the-box repository store
- Embedded Jetty Servlet container
- REST and Java interfaces for CRUD, queries, and actions
- Reconciliation and synchronization that can be scheduled, and also triggered programmatically or over the REST interface, including LiveSync for resources that expose change logs
- Embedded scheduler for running both reconciliation and synchronization, and also scripts
- Pluggable scripting facility with built-in support for JavaScript
- Outbound connectivity support, including REST and email out of the box
- Automatic encryption handling for sensitive configuration properties and for data
- Comprehensive customization capabilities, including built-in scripting hooks and request filter facilities
- Flexible authentication and authorization policy mechanism
- Integration with the Open Identity Connector Framework (OpenICF)[1]
- Password synchronization capabilities with plugins for OpenDJ and Active Directory
- Workflow and Business Process support for BPMN 2.0 (Experimental)

For installation instructions and a sample to get familiar with the features, see the *Installation Guide*.

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

[1] http://openicf.forgerock.org

Chapter 2. Before You Install OpenIDM Software

This chapter covers prerequisites for installing and running OpenIDM software.

For OpenIDM 2.0.3, the following configurations are supported for use in production.

Repository
: MySQL 5.1 or 5.5 with Connector/J 5.1.18 or later is supported for use as a JDBC repository in production.

  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.

Connectors
: OpenIDM 2.0.3 comes packaged with these OpenICF connectors:

  - CSV File
  - LDAP
  - Scripted SQL
  - XML File

  ForgeRock provides additional connectors, as listed on the OpenICF project connectors site[1].

If you have a special request to support a component or combination not listed here, contact ForgeRock at info@forgerock.com[2].

OpenIDM requires Java SE JDK 6 update 24 or later. When using the Oracle JDK, you also need Java Cryptography Extension (JCE) policy files[3].

You need 30 MB disk space for a minimal evaluation installation. For a production installation, disk space required depends on the size of the repository, and on size of the audit and service log files that OpenIDM writes.

[1] http://openicf.forgerock.org/connectors/
[2] mailto:info@forgerock.com
[3] http://www.oracle.com/technetwork/java/javase/downloads/index.html

Chapter 3. OpenIDM Fixes, Limitations, & Known Issues

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

3.1. Fixes & Improvements in 2.0.0, 2.0.1, 2.0.2 & 2.0.3

OpenIDM 2.0.3 resolves the following issues. This list also includes many fixes and improvements in 2.0.0, 2.0.1, and 2.0.2.

- OPENIDM-577: System object audit logging
- OPENIDM-576: Support writing to newly created audit log file after moving/deleting the existing
- OPENIDM-574: Document Router filter behavior and order of hook invocations more clearly
- OPENIDM-556: NPE during patch action due to logger level
- OPENIDM-549: onValidate hook should only be invoked before managed object accepts changes to store, not upon retrieval
- OPENIDM-542: ManagedObjectProperty#onStore does not put the encrypted value into JsonCrypto
- OPENIDM-541: Rest POST managed/user?_action=patch returning with no response the status should be 204
- OPENIDM-538: SSL Mutual auth should set openidm-cert role
- OPENIDM-537: Mail connector uses runtime exceptions instead of object/resource set exceptions
- OPENIDM-532: Authentication rejected on first start-up (possible filter registration issue)
- OPENIDM-518: Improve recon strategy to never go through evaluated targets twice
- OPENIDM-517: OrientDB service gets stuck in "activating" state at startup
- OPENIDM-515: Need to be able to match activity log entries to recon log entries, and tell who initiated the action
- OPENIDM-509: Implement the UNASSIGNED situation

- OPENIDM-508: Provide and log a situation (SOURCE_IGNORED) for source objects that are "not qualified" and with no link or target object
- OPENIDM-507: Disable OrientDB multi casting by default
- OPENIDM-506: CREATE support on back link / bi-directional link use
- OPENIDM-502: Password sync needs to work in the context of the enhanced authentication
- OPENIDM-501: JDBC repo explicit table mapping enhancements
- OPENIDM-499: Clean up default canonical model
- OPENIDM-496: onFailure triggers
- OPENIDM-495: Rename $OPENIDM/jscript to $OPENIDM/script to cater for more scripting languages
- OPENIDM-494: Add a default $OPENIDM/workflow directory
- OPENIDM-488: Warning appears when a managed user is updated or created and then reconciled into an external resource
- OPENIDM-487: JAAS authentication fails on some platforms
- OPENIDM-477: There is SQL locking issue when multiple thread try to create or update object.
- OPENIDM-467: Cannot save JSON object in repository if it contains a list
- OPENIDM-448: Reconciliation process is stopped when the first readObject throws SynchronizationException
- OPENIDM-446: Productize reconciliation status reports
- OPENIDM-445: Clean up default non-interactive start
- OPENIDM-440: Prevent Reconciliation from running until the system reports complete start-up
- OPENIDM-439: Setup default Jetty based authentication out of the box
- OPENIDM-438: Make embedded OrientDB server admin user details configurable
- OPENIDM-436: Cleanup of system properties file
- OPENIDM-435: Tool to validate basic validity of all .json configurations

- OPENIDM-434: Ability to attach javascript debugger
- OPENIDM-433: Cleanup and align windows start/stop scripts
- OPENIDM-432: Link inheritance, eliminate back-links
- OPENIDM-431: Single links table
- OPENIDM-429: Basic facility to disallow access to /system in production profile
- OPENIDM-428: REST inbound policy enforcement point and default policy
- OPENIDM-426: Default OrientDB dbURL generation on windows contains backslashes which OrientDB does not handle well

3.2. Limitations

OpenIDM 2.0.3 does not come packaged with a wrapper out of the box to run as a Windows service.

3.3. Known Issues

OpenIDM 2.0.3 has the following known issues.

- OPENIDM-583: Unable to set different passwords for keys in the key store
- OPENIDM-568: X-OpenIDM-NoSession=false header interpretation
- OPENIDM-565: Uploading provisioner configuration via REST stops reconciliation from working, restarting OpenIDM solves issue
- OPENIDM-564: OpenIDM and the Connector Server, under some conditions, fails to esatablish a connection with each other
- OPENIDM-558: Internal server errors and uncaught exceptions on erroneous REST invocation
- OPENIDM-554: Running OpenIDM from any directory
- OPENIDM-545: Command line help not working
- OPENIDM-536: Missing "_from" request param and "from" default causes NPE
- OPENIDM-527: All connectors must distinguish between successful empty results, and failures to obtain results
- OPENIDM-521: Spurious 4xx errors if HTTP service starts before others

- OPENIDM-519: OpenIDM logs "unbindHttpService: Failed unregistering Servlet" message on startup
- OPENIDM-514: Renamed object in OrientDB sometimes disappears until OpenIDM is restarted
- OPENIDM-491: Running recon with misconfigured or empty connector results in the error "Cowardly refusing to perform recon"
- OPENIDM-470: OpenIDM cannot rename objects. If the identifier of the object has been changed the link became broken.
- OPENIDM-469: The ObjectMapping can change the _id and then the OpenIDM can not find the original target object any more
- OPENIDM-467: Cannot save JSON object in OrientDB based repository if it contains a list
- OPENIDM-458: Add support of account types and distinguish them in the mappings
- OPENIDM-456: Support of systems with case-sensitive and case-insensitive ids are unpredictable
- OPENIDM-227: Updates to Resource not persisted via debug pages

Chapter 4. OpenIDM Compatibility

These capabilities are expected to change in upcoming releases:

- The way you generate connector configurations for access to external resources, described in *Creating Default Connector Configurations*

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 2.0.3, 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[1]. To find a partner in your area, see http://www.forgerock.com/partners.html.

[1] mailto:info@forgerock.com