OpenIDM 2.1.0 Release Notes

Mark Craig
Lana Frost
Andi Egloff

Software release date: February 20, 2013

Publication date: December 10, 2013

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.

Table of Contents

Chapter 1. What's New in OpenIDM 2.1.0

OpenIDM 2.1.0 provides many new features, including the following:

- Browser-based user interface

  Includes self service capabilities, a generic platform to expose and invoke workflows, and a notification service for tasks.

  For more information, see *OpenIDM User Interface* in the *Integrator's Guide*.

- BPMN 2.0 workflow engine, embedded as an OSGi bundle and accessible over REST.

  For more information, see *Integrating Business Processes and Workflows* in the *Integrator's Guide*.

- Configurable task scheduling service, including support for clustered schedules and scanning tasks.

  For more information, see *Scheduling Tasks and Events* in the *Integrator's Guide*.

- Configurable policy service.

  For more information, see *Using Policies to Validate Data* in the *Integrator's Guide*.

- Ability to perform batch scans to execute tasks

  For more information, see *Scanning Data to Trigger Tasks* in the *Integrator's Guide*.

- Ability to create custom RESTful endpoints.

  For more information, see *Adding Custom Endpoints* in the *Integrator's Guide*.

- Support for MS SQL JDBC as an internal repository.

  For more information, see *To Set Up OpenIDM With MS SQL* in the *Installation Guide*.

- Enhanced, multi-threaded reconciliation service, accessible over REST.

  For more information, see *Configuring Synchronization* in the *Integrator's Guide*.

- Support for Powershell scripts on the Active Directory connector.

For more information, see *Using PowerShell Scripts With the Active Directory Connector* in the *Integrator's Guide*.

- Reusable server configuration and property value substitution in the configuration.

  For more information, see *Using Property Value Substitution in the Configuration* in the *Integrator's Guide*.

- Support for calling LiveSync operations over REST, or using the resource API.

  For more information, see *Triggering LiveSync Over REST* in the *Integrator's Guide*.

For installation instructions and several samples to familiarize you 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*.

Chapter 2. Before You Install OpenIDM Software

This chapter covers prerequisites for installing and running OpenIDM software.

For OpenIDM 2.1.0, 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

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 2.1.0 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.

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 130 MB disk space and 256 MB memory for a minimal 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

Note

The current list of fixes and issues reflects OpenIDM 2.1.0 in progress as of February 15, 2013.

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

3.1. Fixes and Improvements

OpenIDM 2.1.0 includes the following major fixes and improvements.

- OPENIDM-1122: Populate the X-Requested-With header in the requests
- OPENIDM-1118: Enforce origin by default, CORS whitelist with default to disable CORS
- OPENIDM-1081: Move to OrientDB 1.3.0 release version
- OPENIDM-1060: JSON Resource should decode URI (normalize)
- OPENIDM-1055: Add base type check to OpenIDMELResolver to resolve only openidm router operations
- OPENIDM-1023: Potential NPE in JsonResourceObjectSet
- OPENIDM-1008: Add not null check to openidm calls in ScopeFactoryService to avoid NPE when handling the result
- OPENIDM-1007: Update the MS SQL JDBC Repository support in 2.1.0
- OPENIDM-988: OpenDJ Password Synchronization Plugin raising error on password change in OpenDJ
- OPENIDM-987: Remove old startprocessinstance syntax from workflow integration
- OPENIDM-970: OpenIDM Livesync: entry deleted on source leads to UNQUALIFIED situation. Should be SOURCE_MISSING
- OPENIDM-965: Encrypted password in boot.properties example does not authenticate
- OPENIDM-961: Must have an easy way to integrate servlet filter based access managers

- OPENIDM-956: OpenIDM assembly depends on ScriptedSQL conn. 1.1.0.0. Should be 1.1.0.1
- OPENIDM-940: onValidate not triggering during recon via rest
- OPENIDM-930: Align provisioner parameters with the new naming convention
- OPENIDM-921: Provisioner fail coerce from String to some primitive types
- OPENIDM-914: CLI.SH configimport not working when using replaceAll option
- OPENIDM-913: CLI.SH configimport not working when importing all set of files
- OPENIDM-911: OpenIDM LiveSync failed to sync user changes from OpenDJ source.
- OPENIDM-885: Convert all samples to be self contained, i.e. start-able via -p option
- OPENIDM-883: Align API with CREST 2.0 for compatibility
- OPENIDM-827: Parallel execution support of reconciliation tasks
- OPENIDM-818: Customizable OpenIDM info service
- OPENIDM-802: Recon: Source reconciliation gives NP exception in certain UNQUALIFIED situation and default DELETE action.
- OPENIDM-797: Sample 3 - MySQL script is not correct on Windows + workaround
- OPENIDM-756: Authentication module needs to be able to propagate user id, not just user name
- OPENIDM-741: Back-end pasword policy support
- OPENIDM-730: Add legacy java lib drop folder to allow non OSGi jars add to Connector classloader
- OPENIDM-729: Remote Shell script password and username parameters requires special care
- OPENIDM-727: UTC date representation in openidm should show UTC time zone with "Z" post-fix as specified by ISO 8601
- OPENIDM-715: OpenIDM freezes on reconciliation

- OPENIDM-695: MS SQL Server JDBC repository
- OPENIDM-686: Include remote Activiti integration artifacts with the default OpenIDM package
- OPENIDM-685: Upgrade to Activiti 5.10
- OPENIDM-682: REST API: Failed to delete a system object w/ condition in openDJ
- OPENIDM-679: Productize script execution on system objects
- OPENIDM-674: Lazy loading of source or target objects during reconciliation
- OPENIDM-670: Scheduler General Configuration
- OPENIDM-669: Scheduler JSON Resource API
- OPENIDM-661: Special characters are not saved properly in MySQL Database with the default sample configuration.
- OPENIDM-659: Provide more helpful log messages to locate the configuration or usage problems.
- OPENIDM-652: Simple way/flag to restrict authorized URL access in the authorization script
- OPENIDM-638: Performance optimization
- OPENIDM-637: Allow to specify history level of the embedded Activiti ProcessEngine
- OPENIDM-635: Use single ConnectorFacade per service
- OPENIDM-631: Remove the reconId from links
- OPENIDM-630: Enable connection pool by default
- OPENIDM-629: Repository needs to ensure selects do not start implicit transactions
- OPENIDM-613: Allow authentication module to configure which properti(es) constitute password or role
- OPENIDM-612: Support authentication query with user roles
- OPENIDM-602: Authentication bug in backend which makes impossible authentication with encrypted password

- OPENIDM-600: Audit log flag to mark password change/reset
- OPENIDM-598: nullpointer exception when reading from activedirectory group, crash when writing to active drirectory group
- OPENIDM-593: The Json Resource Restlet 1.2.2 fails with the http://localhost:8080/openidm/managed/user?_action=create request
- OPENIDM-564: OpenIDM and the Connector Server, under some conditions, fails to esatablish a connection with each other
- OPENIDM-549: onValidate hook should only be invoked before managed object accepts changes to store, not upon retrieval
- OPENIDM-546: Create audit log records with timestamp
- OPENIDM-540: Ability to easily maintain multiple scenario set-ups and to switch between them
- OPENIDM-527: All connectors must distinguish between successful empty results, and failures to obtain results
- OPENIDM-492: Align sample UI with new Authentication mechanisms

3.2. 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 2.1.0 has the following known issues.

- OPENIDM-1176: Disabled schedules via dynamic scheduler API disappear
- OPENIDM-1170: Linux startup script generator is not working correctly

- OPENIDM-1162: With OrientDB, for a MISSING/CREATE situation/action, reconciliation creates a new link instead of using an existing link
- 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-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-803: For reconciliation, the default DELETE action does not delete target objects when targets are ambiguous, including UNQUALIFIED situations, if there is more than one target

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

The following changes will have an impact on existing deployments. Read these changes carefully and adjust existing scripts and clients accordingly.

Changes to the scheduler configuration

The way in which scheduled tasks is configured has changed, as described in *Scheduling Tasks and Events*.

Schedules are now defined in files named `openidm/conf/schedule-*.json`. If you use the previous naming convention (scheduler-*.json), the schedules will not be launched.

Reconciliation now on `recon` service

In previous releases, reconciliation was called on the `sync` service. This API has been deprecated and reconciliation is now called on the `recon` service. For example, a reconciliation operation that previously targeted the following URL:

```
"http://localhost:8080/openidm/recon?_action=sync&mapping=systemLdapAccounts_managedUser"
```

would now use the following URL:

```
"http://localhost:8080/openidm/recon?_action=recon&mapping=systemLdapAccounts_managedUser"
```

Audit log changes

Timestamps now have milliseconds and are in UTC timezone.

The access log now has an additional field, `userid`, which is the OpenIDM ID for a managed or internal user who is logged in. For authentication via SSL mutual auth only, the `userid` is currently `null` because there is no direct associated user in OpenIDM.

Database schema changes

The `reconID` column has been removed from the `links` table.

The size of the `linkType` column in the `links` table has been reduced to 255 characters. This is because MySQL can only create unique indexes on that size for UTF-8 encoding.

The `links` table indexes have been changed to unique indexes to prevent duplication.

The `auditactivity` table contains two new columns - `changedfields` and `passwordchanged`, for additional auditing functionality.

Tables have been added for the scheduler configuration and for User Interface notifications.

The `openidm` user is created with all the required privileges to update the `openidm` database by default.

Changes to token definitions in OrientDB query definitions

Existing `repo.orientdb.json` query definitions with tokens like `${mytoken}` must be reviewed and adjusted to match the new definition which aligns declarations for regular and prepared statement uses.

Existing `${token}` tokens are now suitable for quoted strings by default. Prefixes such as `unquoted:` and `dotnotation:` allow you to use queries in contexts where the unquoted value or the JSON pointer converted to OrientDB dot notation should be inserted.

New queries in `repo.*.json` definitions

query-by-linkType

Security context changes

The request context now includes the security context of the user that is associated with the call.

The `"user"` property has been renamed `"username"`, the name used to log in (for example, to authenticate against an access manager).

Name change for the `query-id` parameter

The `query-id` parameter has been renamed `queryID` for consistency across the API.

4.2. Minor Changes to Existing Functionality

The following changes should not have an impact on existing deployment configurations.

Connection pooling is on by default

For existing configurations, keep this setting off unless you explicitly require it to be changed.

Explicit definition of username, password, and role

The authentication configuration now explicitly defines which properties from the query represent the username, password, and role. Existing configurations rely on the logic of the query order to determine which property is which.

Prefetching of links during reconciliation operations

All links are now queried at the start of a correlation and the results of that query are used.

For more information, see *Prefetching Links* in the *Integrator's Guide*.

4.3. Deprecated Functionality

The following functionality is deprecated in OpenIDM 2.1.0.

- Reconciliation is no longer called on the `sync` service. For more information, see the list of changes to existing functionality.

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

4.4. Removed Functionality

No functionality has been removed in OpenIDM 2.1.0.

No functionality is planned to be removed at this time.

4.5. Functionality That Will Change in the Future

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 2.1.0, 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/.