



OpenIDM Release Notes

Version 3.0.0

Mark Craig
Lana Frost
Mike Jang
Andi Egloff

ForgeRock AS
33 New Montgomery St.,
Suite 1500
San Francisco, CA 94105, USA
+1 415-523-0772
www.forgerock.com

Copyright © 2011-2014 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](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 3.0.0	1
2. Before You Install OpenIDM Software	7
3. OpenIDM Fixes, Limitations, & Known Issues	9
3.1. Fixes and Improvements	9
3.2. Limitations	21
3.3. Known Issues	21
4. OpenIDM Compatibility	27
4.1. Major Changes to Existing Functionality	27
4.2. Minor Changes to Existing Functionality	33
4.3. Deprecated Functionality	33
4.4. Removed Functionality	34
4.5. Functionality That Will Change in the Future	34
5. How to Report Problems & Provide Feedback	35
6. Support	37

Chapter 1

What's New in OpenIDM 3.0.0

OpenIDM 3.0.0 provides many new features and product enhancements. The following list describes the main new features affecting an end user.

Commons REST

OpenIDM 3.0.0 is the first ForgeRock product to fully implement the ForgeRock Commons REST API. It is the ForgeRock-unique RESTful API with a set of easy-to-remember REST calls: create, read, update, delete, patch, action, and query (CRUDPAQ). For more information, see [Major Changes To Existing Functionality](#).

New OpenICF 1.4.0.0 Connectors

OpenICF connectors support interfaces between OpenIDM and a variety of external databases. For more information, see [Major Changes To Existing Functionality](#)

Role-based Provisioning

OpenIDM 3.0.0 provides the ability to create and manage roles that can be assigned to users. Roles provides an abstraction layer in the way entitlements and attributes are set on target resources. The roles functionality makes the assignment and removal of entitlements and resources more consistent and easier to manage.

Support for a new managed/role object allows easy assignment of roles to user objects, implicitly, via business logic, or explicitly, over the REST interface.

High Availability Support

OpenIDM 3.0.0 supports cluster configuration and high availability "out of the box".

Specific nodes can be configured to deal only with certain types of tasks, for example, reconciliations. Nodes can also be configured to share load and to act as a backup in the event of another node becoming unavailable.

For more information, see [Configuring OpenIDM to Work in a Cluster](#) in the *Integrator's Guide*.

Scripting Enhancements

OpenIDM 3.0.0 supports product-wide scripting in Groovy.

Previous releases supported only JavaScript, with the exception of Workflow definitions and certain generic scripted connectors. With product-wide Groovy scripting, the language can now be used throughout to define business logic and customizations.

PowerShell Capabilities

OpenIDM 3.0.0 supports PowerShell scripts.

The PowerShell connector is a generic scripted connector to address the Microsoft Windows ecosystem. You can use this connector to provision any Microsoft system, including, but not limited to, Active Directory, MS SQL, MS Exchange, Sharepoint, Office365, and Azure. Essentially, any task that can be performed with PowerShell can be executed through this connector.

Synchronization Delivery Guarantees

OpenIDM 3.0.0 provides a new onSync hook that enables clients to assess whether an overall synchronization operation was successful on all remote systems, with the ability to roll back synchronized changes in the event of one or more remote systems being unavailable.

For more information, see [How Automatic Sync works with onSync](#) in the *Integrator's Guide*.

User Interface Improvements

- Expanded folder structure

Previously, the static files making up the UI were packaged into a jar, which made customization of the UI difficult. In this version, UI files are expanded into the directory path/to/openidm/ui/default/enduser/public, and can be edited in this location. Changes made to files in this directory will take effect after a browser refresh.

- Project-specific UI customization

A new mechanism in the servlet that hosts the UI searches for installation-specific overrides for many of the default UI files. Customized files can be placed in the corresponding location in the path/to/openidm/ui/extension

directory. As long as the files placed here have the same name as the default UI files, the UI displays the customized files instead of the defaults. This facility allows you to customize the UI without having to make changes to any default files, which in turn makes upgrading easier.

For more information, see [Customizing the UI Theme](#) in the *Integrator's Guide*.

- Configuration-based customization

A new UI theme configuration file (`/path/to/openidm/conf/ui-themeconfig.json`) stores detailed color values, background image paths, and a number of other common styling options. Because the UI theme configuration file is part of the configuration store, it is shared by all nodes in a cluster. Changes made to this file do therefore not have to be replicated manually across nodes.

For more information, see [Customizing the UI Theme](#) in the *Integrator's Guide*.

- Sample OpenIDM configurations that work with the UI

All the documented sample configurations now work with the UI. For more information, see [OpenIDM Samples](#) in the *Installation Guide*.

- Pass-Through Authentication

In previous OpenIDM releases, the only way in which an end user could log into the UI for self-service requests was when a password had been set in the end user's managed/user record. This situation presented problems for organizations in which user records originated in an external resource (such as an LDAP directory). In this case, OpenIDM would generally be unable to read the clear text password from the system resource (because such passwords are usually stored in encrypted form).

OpenIDM 3.0.0 supports delegated authentication to most external data sources. This means that users are able to log into the UI based on, for example, their LDAP credentials. After they have logged in, they are able to perform the full range of end-user-oriented tasks.

The DELEGATED module can now authenticate against multiple targets, using either a named `queryId` or an `authenticate` action, as appropriate. These targets are described by the `queryOnResource` property.

Furthermore, to describe the authentication target, you may see `MANAGED_USER`, `INTERNAL_USER`, or `PASSTHROUGH` used as aliases for `DELEGATED`.

If `queryId` is not defined, the `DelegatedAuthModule` proceeds with an authentication action, requiring `username` and `password` parameters.

For more information, see [Using Delegated Authentication](#) in the *Integrator's Guide*.

- JWT Sessions

In previous releases, user sessions existed in the memory of the OpenIDM server that performed the initial authentication. This was acceptable in single-node environments, but in a clustered environment, this meant that the user had to remain on the node they first encountered. The solution provided no high-availability or failover.

In OpenIDM 3.0.0, user sessions are created as encrypted Java Web Token (JWT) cookies. All the details of the user are stored on the client, rather than on the server. Requests can therefore be sent to any node in a cluster, enabling high-availability and failover server configurations.

- Scalable managed/user administration

OpenIDM 3.0.0 supports server-side paging, searching and sorting for managed/user records. This improvement enables supports for the administration of millions of records in the managed/user table with little noticeable performance degradation, assuming correct database tuning.

- External website integration

In previous releases, it was particularly complex to use any of the end-user oriented REST endpoints provided by OpenIDM from another website within the organization.

OpenIDM 3.0.0 supports Cross Origin Resource Sharing (CORS), which allows a "white list" of domains to make REST calls to OpenIDM directly from within their own webpage context. Authenticated users are now able to interact with OpenIDM services (workflows, profile management, custom endpoints, and so forth) from within their existing applications.

Workflow improvements

- External Activiti workflow templates

In previous OpenIDM releases, if you needed to define a custom template for a workflow, you had to embed the HTML template within the workflow definition. This was often cumbersome and difficult to maintain.

In this release, you can define an external HTML template and refer to that template from within the workflow definition.

For more information, see [Using Custom Templates for Activiti Workflows](#) in the *Integrator's Guide*.

-
- Documented workflow use cases

OpenIDM 3.0.0 provides a number of sample workflows, that demonstrate typical use cases for OpenIDM. Each of these sample workflows is integrated with the default UI. For more information see [Workflow Use Cases](#) in the *Integrator's Guide*.

For installation instructions and several samples to familiarize you with the OpenIDM 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 3.0.0, 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
- Oracle Database 11g

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.

OpenIDM 3.0.0 bundles Jetty version 8.1.9.v20130131.

Connectors

OpenIDM 3.0.0 comes packaged with these OpenICF connectors:

- CSV File
- Database Table

-
- LDAP
 - Scripted Groovy
 - Scripted SQL
 - XML File

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

Browsers

ForgeRock has tested many browsers with the OpenIDM UI, including the following browsers.

- Chrome and Chromium 16 and later
- Firefox 3.6 and later
- Internet Explorer 8 and later
- Safari 5 and later

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 3.0.0 includes the following major fixes and improvements.

- [OPENIDM-2079](#): Cannot PATCH managed user when ID contains special characters.
- [OPENIDM-2067](#): For an MS SQL repository, queries in the repo config file containing concatenation functions do not work
- [OPENIDM-2063](#): Failed to start OpenIDM when MySQL was used as repo with SSL enabled
- [OPENIDM-2061](#): Recon Fails to create users from AD "REV" : invalid identifier [Oracle]
- [OPENIDM-2017](#): OpenIDM does not check availability of remote connectors.
- [OPENIDM-2009](#): External REST service does not pass custom headers
- [OPENIDM-1994](#): JAVA_TYPE_BYTE and JAVA_TYPE_PRIMITIVE_BYTE is not supported as native type with .NET

- [OPENIDM-1972](#): scheduler.json should be delivered with instanceId of &{openidm.node.id} instead of scheduler1234
- [OPENIDM-1967](#): Exceptions in connector when using remote java connector server are not wrapped properly
- [OPENIDM-1966](#): External REST calls without any authentication specified are now refused
- [OPENIDM-1961](#): Persistent scheduler jobs cannot be failed over
- [OPENIDM-1960](#): when password of internal user is encrypted in MySQL repo, we can not authenticate with this user
- [OPENIDM-1953](#): sample2 authentication should not be looking in managed/user
- [OPENIDM-1943](#): LiveSync of ObjectClass __ALL__ is broken
- [OPENIDM-1930](#): Attributes from role assignments are not in onAssignments/onUnassignments scripts
- [OPENIDM-1925](#): remove parameters that are not being applied in script.json config file
- [OPENIDM-1923](#): IWAModule hard-codes resource path
- [OPENIDM-1917](#): livesync create failed
- [OPENIDM-1916](#): [OracleDB] Resource 'user' not found
- [OPENIDM-1912](#): Exception from OpenIDMResolverFactory if used in a parallel execution workflow task
- [OPENIDM-1901](#): The effectiveAssignments had error and caused merge failure when multiple roles were assigned dynamically
- [OPENIDM-1900](#): User created through UI failed to login when no role was selected.
- [OPENIDM-1896](#): passthroughAuthnPopulateContext script is named too specifically; functionality is not specific to pass-through
- [OPENIDM-1893](#): ScriptedRequestHandler throws away detail from ScriptThrowException
- [OPENIDM-1892](#): External REST service returns a 500 InternalServerError on any error by the external call instead of what was returned
- [OPENIDM-1891](#): Failed to change password for openidm-admin on UI

- [OPENIDM-1890](#): Failed to update openidm-admin profile
- [OPENIDM-1884](#): Managed/role entries are not being rendered on the Admin user management form with the proper `_id`
- [OPENIDM-1883](#): Synchronization Situations / Actions: List "rational" options for each Synchronization Situation
- [OPENIDM-1877](#): Exception when updated an assigned role.
- [OPENIDM-1876](#): Various samples not syncing password properly
- [OPENIDM-1874](#): `_fields` ignores `NOT_READABLE` attribute flag
- [OPENIDM-1873](#): Recon audit on a successfully completed recon contains `ACTIVE` state instead of `SUCCESS`
- [OPENIDM-1872](#): `CLI.SH` - `configureconnector` cannot recognize available connectors
- [OPENIDM-1863](#): ICF's `UnsupportedOperationException` is wrapped into wrong OpenIDM exception
- [OPENIDM-1862](#): Null exception when both sunrise and sunset taskscanners were triggered at the same time.
- [OPENIDM-1861](#): `AoN` should be included as a sample
- [OPENIDM-1856](#): compensate mechanism issue on auditing `UPDATE`
- [OPENIDM-1854](#): Change role attribute didn't clean target value changed by the original role
- [OPENIDM-1853](#): roles didn't take effect when multiple roles were assigned to user
- [OPENIDM-1851](#): external/rest calls no longer supply headers to remote system
- [OPENIDM-1849](#): Default MySQL config refers to stored procedures which do not exist in default schema
- [OPENIDM-1848](#): Changes to the repo configuration while the system is running cause global system failure
- [OPENIDM-1847](#): `AND` and `OR` are not working anymore in queries built with `_queryFilter` and called from scripts
- [OPENIDM-1846](#): `JAVA_TYPE_BYTE_ARRAY` is not supported as native type
- [OPENIDM-1844](#): `triggerWorkflowFromSync.js` failed to generate task instance and `sample9` failed

- [OPENIDM-1842](#): onCreate-user-set-default-fields.js script does not update users on creation
- [OPENIDM-1839](#): self-registration page should display error messages about the non valid fields
- [OPENIDM-1824](#): Request command didn't return properly(proper value) when custom endpoint was used.
- [OPENIDM-1819](#): Failures from ICF connectors are not available from onFailure handler
- [OPENIDM-1813](#): reading a non existing workflow task via REST should return 404 instead of 500
- [OPENIDM-1812](#): invoking non existing workflow via REST should return 4XX instead of 500
- [OPENIDM-1810](#): OpenIDM requires all attributes which are defined in provisioner in update operation
- [OPENIDM-1809](#): OpenIDM ignores required attribute in provisioner file
- [OPENIDM-1806](#): DELETE managed object(user, role) returns 200+null on OrientDB (not ok)
- [OPENIDM-1795](#): Async Recon via REST using performAction with a non-existing action not returning proper error
- [OPENIDM-1794](#): GET with queries using _queryId with missing params on MySQL should return 400 instead of 200
- [OPENIDM-1792](#): PATCH by Query via POST not working anymore (getting error 400)
- [OPENIDM-1789](#): Role didn't take effect when replaceTarget operation was applied to a single value property
- [OPENIDM-1781](#): clean-up obsolete properties in authentication.json that are now defined in authModules map
- [OPENIDM-1773](#): Set up Working Custom Endpoint Samples / Query Requests on Groovy Endpoint
- [OPENIDM-1767](#): BadPaddingException while authenticating as openidm-admin on Windows with MSSQL
- [OPENIDM-1766](#): authenticated users can not PATCH their own data anymore
- [OPENIDM-1759](#): In ResourceFunctions of script-common the non-string parameters of openidm.action call are ignored without any warning

- [OPENIDM-1755](#): Recon target phase is always single threaded regardless of the number of configured taskThreads
- [OPENIDM-1749](#): Startup randomly fails on scheduler bundle when launching sample1 on Centos
- [OPENIDM-1748](#): Confusing policy validation display for passwords in the UI
- [OPENIDM-1746](#): Javascript needs access to external packages
- [OPENIDM-1739](#): Changes made to target objects by onLink triggers should be persisted if the situation action is UPDATE
- [OPENIDM-1732](#): onRetrieve scripts not executing for managed/ query results
- [OPENIDM-1708](#): reauthentication not functioning with alternate auth modules
- [OPENIDM-1705](#): Sync Exception actions are returned with 409/conflict instead of 500/exception
- [OPENIDM-1702](#): CLI.SH configimport not working on some configuration files
- [OPENIDM-1701](#): Creating "managed" objects from sync doesn't create link immediately, causing unnecessary correlation for other mappings
- [OPENIDM-1689](#): cleaning up the generic and explicit table mapping defaults for managed user
- [OPENIDM-1679](#): Activity audit file not created when performing CRUD on OpenDJ via connector
- [OPENIDM-1674](#): Slashes in _id break reconciliation
- [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-1655](#): External Rest Service erroneously sets the remote auth ChallengeScheme to HTTP_COOKIE instead of HTTP_BASIC
- [OPENIDM-1649](#): SSL client/mutual auth not working even though certificate is present
- [OPENIDM-1647](#): LiveSync fails when using Generic LDAP Connector if readSchema=false
- [OPENIDM-1637](#): Problem in UI when the username contains a space char.

- [OPENIDM-1631](#): OrientDB Studio not working correctly after upgrade to OrientDB 1.6.4
- [OPENIDM-1629](#): Policy cannot-contain-others raises an exception when one of the fields to check against is absent
- [OPENIDM-1626](#): Duplicated keys in Index in OrientDB returns error code 500 instead of 4XX
- [OPENIDM-1624](#): Linux rc script generated by create-openidm-rc.sh fails to shutdown OpenIDM when installed to a directory other than 'openidm'
- [OPENIDM-1616](#): Customization of the location of OrientDB db broken since upgrade to 1.6.4
- [OPENIDM-1608](#): create schedule via REST with a bad misfirepolicy fails with 500 status code instead of 400
- [OPENIDM-1597](#): openidm takes 100% CPU even in "idle" state on Windows
- [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-1537](#): Getting 500 error when loading the UI when an old invalid session-jwt cookie is present
- [OPENIDM-1535](#): incomplete handleQuery implementation in ScriptedRequestHandler
- [OPENIDM-1532](#): random issues with authentication on some startups leading to 401 on all requests
- [OPENIDM-1529](#): IDMUserAuthModule should be using IdentityServer to get property for "openidm.auth.clientauthonlyports"
- [OPENIDM-1526](#): Recon values fail to be reconstructed from the audit log when using a JDBC repo
- [OPENIDM-1524](#): Jetty floods OpenIDM log with error
- [OPENIDM-1515](#): MVCC is broken when using MSSQL as the OpenIDM repository.
- [OPENIDM-1514](#): Failed login or expired session following a successful login results in empty response body.

- [OPENIDM-1513](#): Inconsistency in script context: request object has different representations
- [OPENIDM-1511](#): Policy.java overwrites the action parameter of async recon
- [OPENIDM-1507](#): Logging level change to FINE causes NullPointerException in OrientDBRepoService
- [OPENIDM-1503](#): InvalidCredentialException thrown from OpenICFProvisionerService uses 500 HTTP error code
- [OPENIDM-1502](#): Audit log entries with same activitydate
- [OPENIDM-1490](#): missing comma in DN definition of certificate
- [OPENIDM-1489](#): Command line needs to allow supplying user/pwd
- [OPENIDM-1486](#): 'en-US' language is always used
- [OPENIDM-1479](#): Cannot delete from generic objects using PostgreSQL
- [OPENIDM-1478](#): Encrypt with Command Line (CLI) is broken
- [OPENIDM-1470](#): Set max heap size (Xmx) and min heap size (Xms) to the same value
- [OPENIDM-1467](#): Private key validation before importing into the keystore
- [OPENIDM-1457](#): Running OrientDB in memory results in failure and ACTIVE_NOT_READY state
- [OPENIDM-1456](#): Correlation query not working correctly: recon leads to absent +unassigned instead of found
- [OPENIDM-1450](#): Deleting record from Managed/user with mismatched version yields in 500 error [OrientDB]
- [OPENIDM-1444](#): json schema package needs to specify export version and import version ranges
- [OPENIDM-1433](#): OpenIDM renames entry on update (OpenIDM ICF glue code sets __NAME__ to __UID__)
- [OPENIDM-1432](#): Missing uinotification table within Oracle openidm.sql schema
- [OPENIDM-1431](#): authentication initialization messages should not appear in the log (INFO) for every request on the REST API
- [OPENIDM-1426](#): Openidmui/index.html hangs on browser refresh

- [OPENIDM-1424](#): gzip servlet filter no longer working
- [OPENIDM-1419](#): Can't logout of openidmui (Session not terminating)
- [OPENIDM-1417](#): Throwing 401 exception in augment security context javascript ends up being a 500 in the response
- [OPENIDM-1416](#): Default onCreate script of UI sets the accountStatus to 'active', overrides the value of the managed user attribute
- [OPENIDM-1415](#): Need to enable cascade delete on foreign keys within Oracle schema
- [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-1406](#): cluster.json should be using a property substitution, and take the setting from boot.properties
- [OPENIDM-1403](#): considerable start-up happening after OpenIDM reports ready
- [OPENIDM-1388](#): AD sync service does not work with SSL 8443
- [OPENIDM-1385](#): Error with REST call to "/openidm/audit/access"
- [OPENIDM-1381](#): Audit log does not correctly record the 'before' state of system objects when calling openidm.update().
- [OPENIDM-1368](#): AD password sync service throws critical error in SSL - mutual auth
- [OPENIDM-1365](#): Recon Audit Log Entries Should Contain "messageDetails" for ScriptExceptions During Reconciliation
- [OPENIDM-1361](#): Exception from UI when a workflow started by scheduler has a user task in it
- [OPENIDM-1354](#): Recon Log Entries Missing "messageDetail" From Errors During Recon
- [OPENIDM-1348](#): Get requests are not including the shutdown time for nodes that have shutdown normally

- [OPENIDM-1346](#): Disabling The Cluster Management Service Causes Startup Errors/Exceptions
- [OPENIDM-1341](#): Add support for the Cluster Management Service to MSSQL and Oracle repository configs and schemas
- [OPENIDM-1339](#): AD password sync plugin service causes critical error and restarts Windows
- [OPENIDM-1338](#): Validation for create without objectId is always true
- [OPENIDM-1337](#): Recon.csv and recon detail over REST are not aligned.
- [OPENIDM-1329](#): OrientDB as repo does not initialize if there is no network connection
- [OPENIDM-1321](#): OpenIDM Audit Logger Service - Fix Camel-Case Typo In Activity Log For "parentActionId" Parameter
- [OPENIDM-1309](#): On mysql 5.6 db init script raises a "Specified key was too long" on creation of index of auditactivity table
- [OPENIDM-1308](#): InternalServerErrorException CryptoService unavailable; regression from OPENIDM-1185
- [OPENIDM-1304](#): Custom queries for recon audit logs which return different columns do not get returned correctly
- [OPENIDM-1298](#): Reconciliation should re-use the executor, and explicitly shut it down at the end
- [OPENIDM-1293](#): OpenIDMELResolver should use component.name to bind JavaDelegate implementations instead of component.id
- [OPENIDM-1292](#): Obfuscate Bootstrap information does not work properly
- [OPENIDM-1287](#): Scheduler null pointer exception
- [OPENIDM-1285](#): Private Key not getting stored in keystore when certificate is generated and store.
- [OPENIDM-1283](#): External/rest requests to endpoints which return non-200 responses result in errors
- [OPENIDM-1281](#): Query for "get-by-field-value" is incorrect
- [OPENIDM-1268](#): Formatting in user registration page broken
- [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-1259](#): OrientDB config file in Samples does not have the new query for clusters
- [OPENIDM-1256](#): additionalPolicies option in policy.json not working
- [OPENIDM-1253](#): Password reset dialog behaving incorrectly
- [OPENIDM-1247](#): Policy Service property validation on a property with no configured policy results in a TypeError
- [OPENIDM-1245](#): Align openidm and activiti contract on scripting(openidm.action() and openidm.patch() failed in a workflow on managed object.)
- [OPENIDM-1236](#): ScriptableList: cannot put 0 (zero) index element
- [OPENIDM-1216](#): Cluster Management Service
- [OPENIDM-1210](#): Directly-assigned workflow tasks disappear when "Requeue" button is hit
- [OPENIDM-1208](#): UI is inoperable in IE8 due to lowercase request headers
- [OPENIDM-1190](#): Disable Quartz update check by default
- [OPENIDM-1187](#): Inconsistent "If-None-Match:" behavior between query and read actions
- [OPENIDM-1185](#): Internal Server error while patching an object's attribute with mysql as repository
- [OPENIDM-1184](#): sample/sample3 and sample/provisioner use hardcoded path in provisioner configuration.
- [OPENIDM-1179](#): Delete non-existing schedules via dynamic scheduler API triggers exception on openidm OSGI console
- [OPENIDM-1176](#): Disabled schedules via dynamic scheduler API disappear
- [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-1173](#): After stopping and restarting eg. the groovy bundle the necessary Activiti ScriptEngineResolver service is not added again to the OSGI services

- [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-1151](#): CLI.SH configExport not working on Linux Ubuntu
- [OPENIDM-1150](#): Additional policy files raises an error about addPolicy()
- [OPENIDM-1149](#): sample5 and sample9 broken due to javascript method method hasOwnProperty missing
- [OPENIDM-1148](#): Changes to static files within /ui/default/bundle-dir unloads the /openidm context, breaking system
- [OPENIDM-1147](#): Install path with space not handled correctly in startup.sh
- [OPENIDM-1141](#): OrientDB config bootstrap repository does not use .json config file, only properties
- [OPENIDM-1129](#): OpenIDM freezes when the connection to the repository is interrupted
- [OPENIDM-1126](#): Listing reconciliation tasks endpoint sends back a JSON with an extra "progress" level
- [OPENIDM-1123](#): Memory leak in directory/file processor
- [OPENIDM-1115](#): When an LDAP user is created through the REST API, the _id that is returned is not normalized
- [OPENIDM-1111](#): Empty OpenIDM response (HTTP 204) causes response parser to fail
- [OPENIDM-1110](#): Immediate dll password change request has wrong content-length value
- [OPENIDM-1109](#): Password needs to be valid JSON string after decryption
- [OPENIDM-1100](#): Site images need to be changeable/extensible without re-packaging the UI
- [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-1087](#): ObjectMapping's call-back action does not support sync-based use-cases

- [OPENIDM-1083](#): Update with PUT on managed user returns the qualified id rather than the local id only
- [OPENIDM-1070](#): RECON: link was not deleted when UNLINK or DELETE action was used for the TARGET IGNORED situation.
- [OPENIDM-1068](#): Typo on individual user's profile page
- [OPENIDM-1062](#): Issue with credential-query using Oracle
- [OPENIDM-1056](#): Policy on repo/internal/openidm-admin/userName causes validation 500 failures
- [OPENIDM-1021](#): Wrong starting arguments during start could throw an error or warning.
- [OPENIDM-969](#): Console login fails and leaves OpenIDM in unusable state
- [OPENIDM-964](#): An incorrect password in boot.properties causes OpenIDM to hang on startup
- [OPENIDM-910](#): Eliminate process bundle warning message on re-starts
- [OPENIDM-681](#): arbitrary query would return all ldap user account info
- [OPENIDM-615](#): More graceful failure when DB drivers are missing
- [OPENIDM-604](#): querying for "query-all-ids" with the repo.jdbc configuration set for explicit tables gives an exception
- [OPENIDM-595](#): Sample 3 provisioner.openicf-sciptedsql.json has hard-coded path to /opt/111/openidm
- [OPENIDM-594](#): Sample2c not showing ldapGroups
- [OPENIDM-589](#): OrientDB index naming convention needs to be unique
- [OPENIDM-577](#): System object audit logging
- [OPENIDM-576](#): Support writing to newly created audit log file after moving/deleting the existing
- [OPENIDM-556](#): NPE during patch action due to logger level
- [OPENIDM-554](#): Running OpenIDM from any directory
- [OPENIDM-553](#): Authorization re-configuration and re-registration issues
- [OPENIDM-551](#): onStore, onRetrieve at managed object level not initialized
- [OPENIDM-550](#): Using "*" condition on PUT to relax MVCC fails

- [OPENIDM-548](#): If-None-Match tries to read the object and fails
- [OPENIDM-547](#): NPE with the ETag header when not using quotes
- [OPENIDM-545](#): Command line help not working
- [OPENIDM-538](#): SSL Mutual auth should set openidm-cert role
- [OPENIDM-536](#): Missing "_from" request param and "from" default causes NPE
- [OPENIDM-532](#): Authentication rejected on first start-up (possible filter registration issue)
- [OPENIDM-530](#): OpenICF connectors and related should not have EA tag anymore
- [OPENIDM-467](#): Cannot save JSON object in repository if it contains a list
- [OPENIDM-456](#): Support of systems with case-sensitive and case-insensitive ids are unpredictable

3.2 Limitations

OpenIDM 3.0.0 has the following known limitations:

- A conditional GET request, with the If-Match request header, is not currently supported.
- OpenIDM provides an embedded workflow and business process engine based on Activiti and the Business Process Model and Notation (BPMN) 2.0 standard. As an embedded system, local integration is supported. Remote integration is not currently supported.
- The OpenIDM implementation of roles does not enforce referential integrity. In other words, you can set up users with a hypothetical role x, before you create that referential role x. Conversely, if you delete an existing referential role y, users with that role will retain that role.

When dynamically assigned roles are added, OpenIDM does not set up provisioning for previously existing users. Any updates to dynamically assigned roles will not update users assigned with those roles.

3.3 Known Issues

OpenIDM 3.0.0 has the following known issues.

- [OPENIDM-2089](#): Remove the need to store certificates in the default java keystore when doing ssl over jdbc.
- [OPENIDM-2078](#): PermGen leak in "source" scripts
- [OPENIDM-2074](#): When the workflow module is disabled, shutdown errors are displayed on the console
- [OPENIDM-2068](#): Audit service does not pass cREST paging parameters along with other query details
- [OPENIDM-2062](#): openidm/system/NAME?_action=test does not properly handle encrypted values causing the tests to fail.
- [OPENIDM-2058](#): Issues on status code and response content for REST API of Configuration with put and delete
- [OPENIDM-2057](#): Issues on status code and response content for REST API of System with post, and delete
- [OPENIDM-2056](#): Recon audit log entry formatting has issues (missing entries and extra entries)
- [OPENIDM-2055](#): Issues on status code and response content for REST API of Scheduler with query, put, and delete
- [OPENIDM-2054](#): Should not be able to create two provisioners with the same name
- [OPENIDM-2034](#): Support arbitrary [commons] auth modules via className
- [OPENIDM-2028](#): The .NET Connector Server Exception displays an incorrect connector error
- [OPENIDM-2021](#): If a query is made on an attribute that is not part of the object schema, OpenIDM returns an inaccurate message
- [OPENIDM-2016](#): sync on unsupported object class with remote java connector returns 500 instead of 400
- [OPENIDM-2005](#): OpenICF query filter does not support literal expressions
- [OPENIDM-2004](#): NPE in OpenICF Provisioner query w/o filter
- [OPENIDM-2002](#): Failed to Decrypt Jwt errors (badPaddingException)
- [OPENIDM-1998](#): Error 500/NPE during reconciliation (ObjectClassResourceProvider.queryCollection)
- [OPENIDM-1991](#): IDM blocked accessing Orientdb ReadWriteDiskCache

- [OPENIDM-1988](#): Scripted SQL 1.4 unable to find jdbc driver
- [OPENIDM-1981](#): Importing all config files with CLI configimport fails with Java 8
- [OPENIDM-1959](#): cli.bat fails to export configuration when we give an absolute path in argument
- [OPENIDM-1954](#): Enabling the OrientDB Studio UI doesn't take effect until the second restart of OpenIDM
- [OPENIDM-1949](#): Update managed user with patch by query in POST should return modified object instead of null
- [OPENIDM-1948](#): Creating manager user with PUT on managed/user// endpoint is accepted whereas it should be refused
- [OPENIDM-1945](#): Invalid workflow config results in the request being stuck in the queue
- [OPENIDM-1941](#): "pattern" property in access.js rules does not work when used on system endpoints
- [OPENIDM-1907](#): Recon failures as a result of policy violations do not indicate the cause of the violation in the recon audit log.
- [OPENIDM-1898](#): Representation of request-object differs between code and json-representation
- [OPENIDM-1889](#): UI failed to recover from password changing failure
- [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-1779](#): Recon action DELETE on situation UNASSIGNED does not delete the target object
- [OPENIDM-1771](#): Failed requests (updating user data) are not audited in the activity audit log
- [OPENIDM-1744](#): Canceling a completed recon changes its stage from COMPLETED_SUCCESS to ACTIVE_CANCELING
- [OPENIDM-1742](#): Launching a recon by ID on a non-existent ID is not handled correctly

- [OPENIDM-1721](#): postAction scripts are not triggered when the "action" is IGNORE or ASYNC
- [OPENIDM-1664](#): Memory usage of AD connector continue to increase.
- [OPENIDM-1654](#): No sync/ service is registered if a sync.json file is not present in the configuration
- [OPENIDM-1642](#): no more possible to change the default Encryption Keys
- [OPENIDM-1641](#): Obfuscation of bootstrap information for Keystore not working
- [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-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-1530](#): OpenIDM self-signed certificates in keystore and truststore does not match
- [OPENIDM-1523](#): Generated self-signed cert does not work with the OpenDJ pwd sync plugin
- [OPENIDM-1504](#): OpenICFProvisionerService handle method performs logger.isDebugEnabled() checks but logs at the error level
- [OPENIDM-1501](#): sync?_action=performAction with an action=DELETE results in a delete on the source rather than the target
- [OPENIDM-1488](#): XDate locales could not be initialized correctly
- [OPENIDM-1476](#): Internal patch retry process in managed objects fails
- [OPENIDM-1452](#): Incorrect bundleVersion in provisioner config yields confusing error
- [OPENIDM-1445](#): Provisioner service does not decrypt encrypted attributes before passing them to OpenICF framework

- [OPENIDM-1437](#): Policy service not called at the right time
- [OPENIDM-1430](#): OpenIDM needs a restart after importing a new cert via REST API
- [OPENIDM-1409](#): The query-all and get-users-of-direct-role queries are not consistent across different repos
- [OPENIDM-1399](#): Logging into the working directory (specified with the -w option) does not work
- [OPENIDM-1398](#): ad plugin using old conventions for calling openidm patch operation to set password
- [OPENIDM-1390](#): Unable to parse boolean configuration values from custom OpenICF provisioner
- [OPENIDM-1379](#): ADD operation failed for OpenDJ account notification handler
- [OPENIDM-1277](#): cli.bat configexport does not work on Windows
- [OPENIDM-1269](#): some issues with Case Sensitivity options for Sync
- [OPENIDM-1219](#): DB/Config bootstrapping should use IdentityServer support for getting properties, including boot prop
- [OPENIDM-1186](#): PATCH with POST using MVCC are successful even if revision wrong
- [OPENIDM-1165](#): EXCEPTION action when doing liveSync stops the synctoken processing
- [OPENIDM-1098](#): onDelete script generates exception
- [OPENIDM-1074](#): disabling automatic polling for changes of config file not possible on new install
- [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
- [OPENIDM-662](#): query-all-ids always returns the revision as 0, even after the object has been updated to a newer revision

Chapter 4

OpenIDM Compatibility

This chapter covers major and minor changes to existing functionality, as well as deprecated and removed functionality in this release of OpenIDM. You must read this chapter before commencing a migration from a previous OpenIDM release.

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.

Integration of OpenICF 1.4.0.0

OpenIDM 3.0.0 is not compatible with the previous version of the OpenICF framework. If your deployment uses remote connector servers (either .NET or Java) you must upgrade them to the new connector server versions (1.4.0.0). With the exception of the Active Directory connector, the new connector framework is compatible with the older connectors, however, so you can use the older connectors with an OpenIDM 3.0.0 deployment. Only version 1.4.0.0 of the Active Directory connector is supported with OpenIDM 3.0.0. The following compatibility matrix indicates the supported connector and OpenICF framework versions.

Table 4.1. OpenIDM 3.0.0 / OpenICF Compatibility Matrix

OpenIDM Version	OpenICF Framework	Supported Java Connectors	Supported .NET Connectors
2.1	1.1	1.1	1.1
3.0.0	1.4	Previously supported Java connectors (1.1) Groovy Connector (1.4)	Active Directory Connector (1.4) PowerShell Connector (1.4)

Changes to the REST Interface

A number of changes have been made to the REST API in this release. Major changes include the following:

- In OpenIDM 3.0.0, the request header "Content-type: application/json" is required for all REST calls that include a request body (POST, PUT, and PATCH). This header was optional in OpenIDM 2.1.
- For REST calls to the external/rest endpoint, an action name is now mandatory. In addition, there are no leading underscores in attribute names.

For example:

```
$ curl \
--cacert self-signed.crt \
--header "Content-Type: application/json" \
--header "X-OpenIDM-Password: openidm-admin" \
--header "X-OpenIDM-Username: openidm-admin" \
--data '{
    "url" : "http://example.com/",
    "method" : "GET",
    "content-type" : "application/xml"
}' \
--request POST \
"https://localhost:8443/openidm/external/rest
?_action=call"
```

- Creating system objects with a PUT request (specifying a client-assigned ID) is handled differently in OpenIDM 3.0.0, in that the resulting user_id is no longer URL-encoded. For example, consider the following request:

```
$ curl \
--cacert self-signed.crt \
--header "X-OpenIDM-Username: openidm-admin" \
```



```
--header "X-OpenIDM-Password: openidm-admin" \
--header "If-None-Match: *" \
--header "Content-Type: application/json" \
--request PUT \
--data '{"cn":"James Smith",
      "dn":"uid=jsmith, ou=people,dc=example,dc=com",
      "uid":"jsmith",
      "sn":"Smith",
      "givenName":"James",
      "mail":"jsmith@example.com",
      "description":"Created by OpenIDM REST."
    }' \
https://localhost:8443/openidm/system/ldap/account/uid=jsmith,ou=people,dc=example,dc=com
```

The resulting `_id` in OpenIDM 3.0.0 is:

```
"_id": "uid=jsmith,ou=people,dc=example,dc=com"
```

In OpenIDM 2.1, the resulting `_id` is:

```
"_id": "uid%3Djsmith%2Cou%3Dpeople%2Cdc%3Dexample%2Cdc%3Dcom"
```

When you create a system object with a PUT request (that is, specifying a client-assigned ID), you should specify the ID in the URL only and not in the JSON payload. If you specify a different ID in the URL and in the JSON payload, the request will fail, with an error similar to the following:

```
{
  "code": 500,
  "reason": "Internal Server Error",
  "message": "The uid attribute is not single value attribute."}
```

For details of the new interface, including examples, see the [REST API Reference](#) in the *Integrator's Guide*.

Changes to the authentication service

The authentication service now uses the ForgeRock commons authentication framework. Authentication modules are specified in `conf/authentication.json` and are applied in the order in which they are specified.

Change to patch action data syntax

In OpenIDM 2.1.0, the syntax to patch a data object was as follows:

```
--data '[
  {
    "replace": "/email",
    "value": "new-mail-address@example.com"
  }
]'
```

In OpenIDM 3.0.0, the syntax is as follows:

```
--data '[
  {
    "operation": "replace",
    "field": "/email",
    "value": "new-mail-address@example.com"
  }
]'
```

The value of the "operation" field now specifies the patch action (for example, "add", "replace", or "remove"). For more information, see [Patch Resource](#) in the *Integrators Guide*.

Changes to the logging service

- The name of the parentActionid column in the activity log has changed to parentId, for consistency across the product.

Scripting changes

- Managed object property scripts (onRetrieve and onStore) must now return the modified property values from the script, instead of changing the property member in the scope itself.

propertyName is now available in managed object property scripts.

- The format of script exceptions has changed, replacing openIdmCode with code. For example, in OpenIDM 2.1.0:

```
throw {
  "openIdmCode" : 403,
  "message" : "Access denied"
}
```

In OpenIDM 3.0.0:

```
throw {
  "code" : 403,
  "message" : "Access denied"
}
```

- Global script properties, as well as default and custom script file locations, are now defined in the file conf/script.json.

For more information, see [Default and Custom Configuration Directories](#) in the *Integrators Guide*.

- The method signature for `openidm.create` has changed. The ID provided in the create has been separated into two parts - a resource container name and an (optional) client-supplied resource ID.

This change makes it easier to determine whether the client is supplying an ID, or whether the server should generate an ID.

Scripts using this function must now use the following format if the client is providing the ID:

```
openidm.create('managed/user", "userName", user-object)
```

and the following format if the server should generate the ID:

```
openidm.create('managed/user", null, user-object)
```

- The way in which a request object is accessed has changed from `request.value` to `request.content`. For example, to obtain the ID of a process definition in 2.1.0, the script extract would have been:

```
var processDefinitionId = request.value._processDefinitionId;
```

In OpenIDM 3.0.0, the corresponding script would be:

```
var processDefinitionId = request.content._processDefinitionId;
```

In addition, parameters are now added to a request using `request.additionalParameters` instead of the 2.1.0 construct `request.params`.

For more information about request objects, see [Custom Endpoints and request Objects](#) in the *Integrators Guide*.

- The way in which the log level is set for JavaScripts has changed. Previously, the log level was set as follows:

```
org.forgerock.openidm.script.javascript.JavaScript.level=level
```

In OpenIDM 3.0.0, the log level is set as follows:

```
org.forgerock.script.javascript.JavaScript.level=level
```

Changes to query support

- Token substitution from user parameters is no longer supported for lists, and is only supported for strings.

- The way in which queries on system objects are constructed has changed. Queries that followed the OpenICF format are no longer supported and query filters must now be specified in common filter notation. This includes correlation queries on system objects.

For example, the following query in OpenIDM 3.0.0:

```
'query': { 'Equals': { 'field' : 'employeeType', 'values': ['Permanent'] } }
```

would be constructed as follows in OpenIDM 3.0.0:

```
"_queryFilter" : "employeeType eq \"Permanent\""
```

For information about the supported query format, see [Constructing Queries](#) in the *Integrators Guide*.

Security Module Changes

- The way in which the security context is addressed has changed from `request.parent.security` in OpenIDM 2.1.0 to `context.security` in OpenIDM 3.0.0.

A sample object showing the security context in OpenIDM 2.1.0 follows:

```
"parent": {  
  ...  
  "security": {  
    "username": "openidm-admin",  
    "openidm-roles": [  
      "openidm-admin",  
      "openidm-authorized"  
    ],  
    "userid": {  
      "id": "openidm-admin",  
      "component": "internal/user"  
    }  
  }  
}
```

A corresponding sample security context in OpenIDM 3.0.0 would be:

```
"security": {  
  "context": {  
    "authenticationId": "openidm-admin",  
    "class": "org.forgerock.json.resource.SecurityContext",  
    "parent": {  
      "class": "org.forgerock.json.resource.RootContext",  
      "parent": null,  
      "id": "0a8d43c2-1c54-487f-bec4-564b944fa835"  
    },  
    "authorizationId": {  
      "roles": [  
        "openidm-admin",  
        ...  
      ]  
    }  
  }  
}
```

```
        "openidm-authorized"
      ],
      "component": "repo/internal/user",
      "id": "openidm-admin"
    }
  }
```

Changes to the workflow module

The action used to start a workflow process instance has changed. In OpenIDM 2.1.0, you would start a process instance with a POST request to the following URL:

```
"https://localhost:8443/openidm/workflow/processinstance
?_action=createProcessInstance"
```

In OpenIDM 3.0.0, you would send a similar POST request to:

```
"https://localhost:8443/openidm/workflow/processinstance
?_action=create"
```

4.2 Minor Changes to Existing Functionality

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

Change to how roles are stored

In OpenIDM 2.1.0, roles were stored as a CSV list. For example:

```
"roles": "openidm-authorized,contractor",
```

In OpenIDM 3.0.0, roles are stored in an array. For example:

```
"roles": [
  "openidm-authorized", "contractor"
],
```

4.3 Deprecated Functionality

Apart from the support for OpenICF-style queries, noted previously, no functionality has been deprecated in OpenIDM 3.0.0.

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

4.4 Removed Functionality

No functionality has been removed in OpenIDM 3.0.0.

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 3.0.0, 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/>.

