Release Notes

ForgeRock Identity Management 5

Mark Craig
Lana Frost
Mike Jang
Andi Egloff

ForgeRock AS
201 Mission St., Suite 2900
San Francisco, CA 94105, USA
+1 415-599-1100 (US)
www.forgerock.com

Abstract

Notes covering ForgeRock® Identity Management software requirements, fixes, and known issues. This software offers flexible services for automating management of the identity life cycle.

Table of Contents

About ForgeRock Identity Management Software

ForgeRock Identity Platform™ is the only offering for access management, identity management, user-managed access, directory services, and an identity gateway, designed and built as a single, unified platform.

The platform includes the following components that extend what is available in open source projects to provide fully featured, enterprise-ready software:

- ForgeRock Access Management (AM)
- ForgeRock Identity Management (IDM)
- ForgeRock Directory Services (DS)
- ForgeRock Identity Gateway (IG)

ForgeRock Identity Management software provides centralized, simple management and synchronization of identities for users, devices and things.

ForgeRock Identity Management software is highly flexible and therefore able to fit almost any use case and workflow.

These release notes are written for anyone using the ForgeRock Identity Management 5 release. Read these notes before you install or upgrade ForgeRock Identity Management software.

These release notes cover the following topics:

- A list of the major new features and functionality provided with this release
- Hardware and software prerequisites for installing and upgrading ForgeRock Identity Management software
- Compatibility with previous releases
- Potential upcoming deprecation and removals that affect scripts and applications
- Issues fixed since the previous release
- Known issues open at the time of release

See the Installation Guide after you read these *Release Notes*. The *Installation Guide* covers installation and upgrade for ForgeRock Identity Management software.

Chapter 1
What's New

This chapter covers new capabilities in ForgeRock Identity Management 5.

1.1. New Features

This release includes the following new features:

Registration With Social Identities

Users can now register new accounts using information from social identity providers, including Google, Facebook, and LinkedIn. If you configure access through more than one social identity provider, users can select and manage the providers they use.

For more information, see Chapter 10, "*Configuring Social ID Providers*" in the *Integrator's Guide*.

Integration Between Products Across the Platform

It is now much easier to use ForgeRock Access Management as the default authentication provider. This enhanced functionality is demonstrated in the new Full Stack Sample. For more information, see Chapter 11, "*Integrating IDM With the ForgeRock Identity Platform*" in the *Samples Guide*, which works with OpenIDM 5 and OpenAM 5.

The old Full Stack sample is still available in the *OpenIDM 4.5 Samples Guide*

Scripted JMS Message Handler

A new scripted JMS Message Handler enables you to perform CRUDPAQ operations by subscribing to an ActiveMQ message queue.

For more information, see Chapter 7, "*Scripted JMS Sample*" in the *Samples Guide*.

Enhanced Update Process

The update process from OpenIDM 4.5 to OpenIDM 5 is simpler than in previous versions. For more information, see Section 4.3, "Updating to IDM 5" in the *Installation Guide*.

New Audit Event Handlers

The following new audit event handlers are supported:

- JSON audit event handler, that logs audit data to a set of JSON files.

Important

This is the new default file-based audit event handler, and replaces the default CSV audit configuration. Auditing to CSV is still supported but must be configured on an OpenIDM 5 system.

For more information, see Section 21.2.1, "JSON Audit Event Handler" in the *Integrator's Guide*.

- Splunk audit event handler, that supports logging to a Splunk system. For more information, see Section 21.2.8, "Splunk Audit Event Handler" in the *Integrator's Guide*.
- Syslog audit event handler, based on RFC 5424, *The Syslog Protocol*. For more information, see Section 21.2.7, "Syslog Audit Event Handler" in the *Integrator's Guide*.

New Authentication Modules

OpenIDM 5 includes support for OpenID Connect and OAuth 2.0 authentication. For more information, see Section 18.1.2, "Supported Authentication and Session Modules" in the *Integrator's Guide*

A new `SOCIAL_PROVIDERS` authentication module allows you to configure additional OAuth 2.0 or OpenID Connect social identity providers. These providers must be *entirely* compliant with the OAuth 2.0 and OpenID Connect 1.0 standards. For more information, see Chapter 10, "*Configuring Social ID Providers*" in the *Integrator's Guide*.

Improved Cluster Service and Scheduled Job Management

OpenIDM 5 provides simpler configuration and management of a clustered deployment, including improvements to how scheduled jobs across a cluster are managed. Support has been added for the following:

- Removal of the keystore from the repository.

  The OpenIDM keystore is no longer persisted in the repository. In a clustered environment, you must copy the initialized keystore to each instance in the cluster, or point to a single, centralized keystore. For more information, see Section 22.1, "Configuring an IDM Instance as Part of a Cluster" in the *Integrator's Guide*.

- Changes to the cluster configuration.

  It is no longer necessary to specify the `openidm.instance.type` of nodes in a cluster. This configuration property does not exist in OpenIDM 5 and all nodes are assumed to be of the same *type*. If you leave this property in your `boot.properties` file after an upgrade, it is simply ignored. For more information, see Section 22.1, "Configuring an IDM Instance as Part of a Cluster" in the *Integrator's Guide*.

- Basic cluster monitoring in the Admin UI.

  For more information, see Section 22.4, "Managing Nodes Through the Admin UI" in the *Integrator's Guide*.

Support for Hardware Security Module (HSM) Devices

OpenIDM 5 supports the configuration of an external PKCS #11 (HSM) device to manage the keys used to secure OpenIDM transactions. For more information, see Section 19.3, "Configuring a Hardware Security Module (HSM) Device" in the *Integrator's Guide*.

Changes to Supported Connectors and Connector Servers

- New Marketo Connector

  Part of the Social Registration feature, the Marketo Connector is an example of how OpenIDM can be used to manage customer data. For more information, see Chapter 12, "*Marketo Connector*" in the *Connectors Guide*.

- Upgraded Remote Connector Servers

  OpenIDM 5 supports version 1.5.2.0 of the .NET and Java connector servers. The updated connector servers provide full support for the `websocket` protocol communication protocol and fix a number of issues. For more information, see Section 13.2, "Accessing Remote Connectors" in the *Integrator's Guide*.

- Updated LDAP Connector

  OpenIDM 5 bundles version 1.4.3.0 of the LDAP connector. The updated connector provides a number of enhancements, including:

  - A `resetSyncToken` flag to address possible inconsistencies between the `syncToken` value and the `lastChangeNumber` in the changelog (see OPENICF-601).
  - Better exception logging for failed updates (see OPENICF-593).
  - Detection of the Red Hat Directory Server server type and subsequent selection of the correct sync strategy (see OPENICF-539).
  - More efficient search filters (see OPENICF-505).

- Updated Groovy Connector Toolkit

  OpenIDM 5 bundles version 1.4.3.0 of the Groovy connector toolkit.

- SAP Connector Now Supports SNC

  Version 1.4.1.0 of the SAP connector supports an SNC (Secure Network Connection) configuration. For more information, see Section 7.5, "Configuring the SAP Connector For SNC" in the *Connectors Guide*.

Password Reset Capability for Administrators

Administrators can now reset user passwords in a secure, configurable way, through the Admin UI. For more information, see Section 4.8, "Resetting User Passwords" in the *Integrator's Guide*.

API Explorer For Managed Objects

The OpenIDM 5 UI includes an API Explorer that allows you to list the supported methods and actions on managed object endpoints. For more information, see Section 4.11, "API Explorer" in the *Integrator's Guide*.

JSON Configuration File to Protect the Felix Web Console

OpenIDM 5 provides a new configuration file that enables you to protect access to the Felix Web Console, in the event that you cannot remove the console in production. For more information, see Section 19.2.10, "Remove or Protect Development & Debug Tools" in the *Integrator's Guide*.

For installation instructions, see Chapter 1, "*Preparing to Install and Run Servers*" in the *Installation Guide*.

Several samples are provided to familiarize you with the OpenIDM features. For more information, see Chapter 1, "*Overview of the Samples*" in the *Samples Guide*.

For an architectural overview and a high-level presentation of OpenIDM, see Chapter 1, "*Architectural Overview*" in the *Integrator's Guide*.

1.2. Security Advisories

ForgeRock issues security advisories in collaboration with our customers and the open source community to address any security vulnerabilities transparently and rapidly. ForgeRock's security advisory policy governs the process on how security issues are submitted, received, and evaluated as well as the timeline for the issuance of security advisories and patches.

For details of all the security advisories across ForgeRock products, see Security Advisories in the *Knowledge Base library*

Chapter 2

Before You Install

This chapter covers requirements to consider before you run ForgeRock Identity Management software, especially before you run the software in your production environment.

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

2.1. Supported Repositories

The following JDBC repositories are supported for use in production:

- MySQL version 5.5, 5.6, and 5.7 with MySQL JDBC Driver Connector/J 5.1.18 or later
- Microsoft SQL Server 2012 and 2014
- Oracle Database 11gR2 and 12c
- PostgreSQL 9.3.10 and 9.4.5
- IBM DB2, 10.1, 10.5

OrientDB is provided for evaluation only.

2.2. Containers

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

OpenIDM bundles Jetty version 9.2.

2.3. Connectors

OpenIDM bundles the following OpenICF connectors:

- CSV File Connector
- Database Table Connector

- Groovy Connector Toolkit

  This toolkit enables you to create scripted connectors to virtually any resource

- LDAP Connector
- XML File Connector
- Kerberos Connector
- Scripted SSH Connector

  Currently supported only as a prerequisite for the Kerberos Connector

- Google Apps Connector
- Salesforce Connector

A PowerShell Connector Toolkit is available for download from ForgeRock's BackStage site. This Toolkit enables you to create scripted connectors to address the requirements of your Microsoft Windows ecosystem.

Additional connectors are available from ForgeRock's BackStagesite.

Use of the LDAP connector to provision to Active Directory is supported with Active Directory Domain Controllers, Active Directory Global Catalogues, and Active Directory Lightweight Directory Services (LDS).

Windows 2012 R2 is supported as the remote system for connectors and password synchronization plugins.

The following table lists the supported connectors, connector servers, and password synchronization plugins for this OpenIDM release.

Table 2.1. Supported Connectors, Connector Servers, and Plugins

Connector/Plugin	Supported Version
CSV File Connector	1.5.1.4
Database Table Connector	1.1.0.2
Google Apps Connector	1.4.1.0
Groovy Connector Toolkit	1.4.3.0
Kerberos Connector	1.4.2.0
LDAP Connector	1.4.3.0
Powershell Connector Toolkit	1.4.3.0
RACF Connector	1.1.0.0
Salesforce Connector	2.0.29.4
SAP Connector	1.4.1.0

Connector/Plugin	Supported Version
XML Connector	1.1.0.3
Active Directory Connector	1.4.0.0
Java Connector Server	1.5.2.0, 1.5.1.0, 1.5.0.0, 1.4.1.0
.NET Connector Server	1.5.2.0, 1.5.1.0, 1.5.0.0, 1.4.1.0
DS Password Synchronization Plugin	3.5.0, supported with OpenDJ 3.5.0 5.0.0, supported with DS 5 DS Password Sync plugins are not supported with OpenDJ OEM
Active Directory Password Synchronization Plugin	1.1.0, supported on Windows 2008 R2 and Windows 2012 R2

OpenIDM 4.0 and upwards supports a revised version of the OpenICF Framework. You must use the supported versions of the .NET Connector Server, or the Java Connector Server. The 1.5.x Java Connector Server is backward compatible with the version 1.1.x connectors. The 1.5.x .NET Connector Server is compatible only with the 1.4.x and 1.5.x connectors.

The 1.5.2.0 .NET connector server requires the .NET framework (version 4.5 or later) and is supported on Windows Server 2008 R2 and 2012 R2.

Important

Although the scripted connector toolkits are supported, connectors that you build with these toolkits are not supported. You can find examples of how to build connectors with these toolkits in Chapter 4, "*Samples That Use the Groovy Connector Toolkit to Create Scripted Connectors*" in the *Samples Guide* and Chapter 5, "*Samples That Use the PowerShell Connector Toolkit to Create Scripted Connectors*" in the *Samples Guide*.

2.4. Browsers

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

- Chrome and Chromium, latest stable version
- Firefox, latest stable version
- Safari, latest stable version
- Internet Explorer 11 and later

2.5. Operating Systems

ForgeRock Identity Management software is supported on the following operating systems:

- Red Hat Enterprise Linux 6.x/7.x (CentOS Linux 6.x/7.x)
- Ubuntu Linux 16.04
- Windows 2008 R2, 2012 R2, 2016

2.6. Java Environment

OpenIDM requires Java 7 or Java 8, specifically at least the Java Standard Edition runtime environment. ForgeRock has performed most testing with Oracle Java Platform 8, Standard Edition.

ForgeRock recommends that you keep your Java installation up to date with the latest security fixes.

When using the Oracle JDK, you also need the Java Cryptography Extension (JCE) policy files.

On Windows systems, you must use at least Java SE JDK 7 update 6 to take advantage of the JVM fix relating to non-blocking sockets with the default Jetty configuration.

OpenJDK 1.7 and OpenJDK 1.8 are also supported.

2.7. Memory

You need 250 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 any internal and external repositories, as well as the size of the audit and service log files that OpenIDM creates.

Chapter 3

Fixes, Limitations, and Known Issues

This chapter covers the status of key issues and limitations for ForgeRock Identity Management 5. For details and information on other issues, see the OpenIDM issue tracker.

3.1. Key Fixes

This section covers key bug fixes in IDM 5 software.

3.1.1. Key Fixes in 5.0.0.1

The following important bugs were fixed in this release:

- OPENIDM-9707: Backport update related fixes from 5.5.0 to 5.0.x maintenance branch
- OPENIDM-9651: Backport OPENIDM-9107: NullPointerException in AbstractScheduler calling trigger.getFireTimeAfter
- OPENIDM-9631: Backport OPENIDM-8050: External IDM endpoint does not return response codes and errors
- OPENIDM-9630: Backport OPENIDM-9211: External REST service does not return error details from remote server
- OPENIDM-9629: Backport OPENIDM-7726: Unable to filter by '_id' attribute on Managed Objects in the UI
- OPENIDM-9628: Backport OPENIDM-9207: recon creates incorrect links when using linkQualifiers
- OPENIDM-9155: Backport OPENIDM-8527: Persistent schedules do not failover if recovery initiated by a node with execute.persistent.schedules=false
- OPENIDM-9154: Backport OPENIDM-8288: scheduler: getting resource NotFoundException
- OPENIDM-9153: Backport OPENIDM-8042: scheduler throws NullPointerException at startup
- OPENIDM-9152: Backport OPENIDM-7894: Clustered recon may fail
- OPENIDM-9151: Backport OPENIDM-8275: new managed user boolean property not getting saved via Admin UI

- OPENIDM-9150: Backport OPENIDM-8049: Self-signed cert not stored in truststore during initialization
- OPENIDM-9149: Backport OPENIDM-8043: Unable to initialize keystore and truststore when passwords are different
- OPENIDM-9148: Backport OPENIDM-8276: ReconContext should generate it's own Id and not inherit the RootContext Id
- OPENIDM-9146: Backport OPENIDM-8154: The splunk, elastic search, and jdbc audit config have sensitive fields that need to be encrypted in the audit json config
- OPENIDM-9143: Backport OPENIDM-7669: When defining an array type in configuration, the type specified for the items is ignored

3.1.2. Key Fixes in 5.0

The following important bugs were fixed in this release:

- OPENIDM-7349: LDAP Group assignment removal fails due to case mismatch
- OPENIDM-7286: GET on manager/user/user_id/reports/relation_id and managed/user/user_id/manager/relation_id are giving wrong results on user with a manager
- OPENIDM-7199: Policies not executed for multiple type attributes
- OPENIDM-7108: Password Reset Token issued by one process cannot be validated by a different process
- OPENIDM-7028: Audit schema missing db index
- OPENIDM-7025: Setting the authzRoles 's attribute Return by Default to true, triggers the error "Changes pending - Authorization Roles"
- OPENIDM-7014: SQLException thrown during GenericTableHandler.readForUpdate() is masked by failure to close the Statement associated with the ResultSet
- OPENIDM-6973: AD Powershell samples: __ENABLE__ used in README but not in provisioner and create script
- OPENIDM-6966: credential-query is inconsistent across repo config and needs to include status = 'active'
- OPENIDM-6954: NullPointerException thrown during LiveSync when connectivy to Remote Connector Server has been lost
- OPENIDM-6818: OpenIDM ICF Provisioner 'runAs' use-case is broken when integrating with OpenDJ
- OPENIDM-6783: Unable to set managed object attribute type within UI to multiple values

- OPENIDM-6742: ["relationship","null"] on 'manager' in managed.json causes tabs to disappear in the UI
- OPENIDM-6723: Policy failure during forgotten password reset causes redirect to Login Page and obscures the failure cause
- OPENIDM-6710: index and constraints on relationshipproperties table not properly configured in schemas
- OPENIDM-6700: Self Service Dashboard displays task names incorrectly
- OPENIDM-6641: cannot-contains-others policy is broken and does not correctly detect values which do not meet the policy requirements
- OPENIDM-6619: "After" object missing from activity log when removing an authzRole
- OPENIDM-6559: Patch ADD operation on system adds value to single-valued attribute
- OPENIDM-6508: CountPolicy does not work because -count queryIds are missing
- OPENIDM-6504: recon status may have incorrect data with recon after update
- OPENIDM-6481: OpenIDM creates redundant BoneCPDataSource
- OPENIDM-6457: CREATE request with _fields for relationships are not returned in the response
- OPENIDM-6385: sample2d 'group' entry in managed.json causes UI issue
- OPENIDM-6348: mapping properties page doesn't display completely if error occurs in script evaluation
- OPENIDM-6313: Editing managed user schema from admin-ui corrupts lastSync and kbaInfo property definitions
- OPENIDM-6291: '/_id: Expecting a value' warning when adding a Role with an On Assignment script
- OPENIDM-6230: IDM hangs in shutdown waiting on promise.PromiseImpl.await
- OPENIDM-6215: With non-local project, after update to 4.5.0 OpenIDM startup fails to activate crypto module
- OPENIDM-6207: Excessive DB lock contention resulting from readForUpdateQueryStr execution in GenericTableHandler
- OPENIDM-6200: conf/logging.properties not managed by update tool
- OPENIDM-6196: With a non-local project, update is not updating default OpenIDM project directory
- OPENIDM-6193: JobEntity was updated by another transaction concurrently

- OPENIDM-6192: Update CLI causes OpenIDM to restart when previewing repo updates
- OPENIDM-6170: Update process creates erroneous new keystore and truststore files that should be removed
- OPENIDM-6169: unAssignment script undetected by defaultMapping.js
- OPENIDM-6145: Admin UI incorrectly changes Managed User schema
- OPENIDM-6086: Deleting attributes in the LDAP Connector via the Admin UI creates empty strings
- OPENIDM-6083: Sample 2d -- Admin UI rendering of group recon is illegible in the UI
- OPENIDM-6071: OpenIDM changes port from 389 to 1389 when configuring LDAP connector through the UI
- OPENIDM-6068: Target reconciliation does not finish for large datasets
- OPENIDM-6067: When a mapping is deleted through the Admin UI, links associated with the mapping are not deleted
- OPENIDM-6051: Entire source object is returned when an attribute in sample data is null
- OPENIDM-6044: When boolean or number property is updated on managed user in Admin UI the Save button remains grayed out
- OPENIDM-6043: ScriptedREST and ScriptedCREST samples do not work with OpenDJ 3.5.0
- OPENIDM-6031: Some workflow use cases show the wrong property name (_body instead of body)
- OPENIDM-6025: "Filter Actions" message for "authentication" and "access" event is not correct
- OPENIDM-6015: Clicking the '-' button next to 'The Value for' Reconciliation Query Filters in the Admin UI throws JavaScript errors in the console
- OPENIDM-5997: Invalid "lastSync" JSON schema syntax in managed.json
- OPENIDM-5986: cli.sh configimport returns success when errors occur
- OPENIDM-5963: Connector schema data preview can fail depending on the order of automatically generated schema fields
- OPENIDM-5962: Managed User Edit page displays changes pending warning
- OPENIDM-5960: EmailClient requires username/password when auth is disabled
- OPENIDM-5906: PATCH request with null rev invoked twice at the same time causes infinite loop
- OPENIDM-5904: Incorrect "Missing source/target" text in Admin UI
- OPENIDM-5896: A single role can be assigned multiple times to the same user

- OPENIDM-5887: SyncResult always specifies default situation action and not the actual action determined during synchronization
- OPENIDM-5878: Newly added Object type doesn't appear in mappings
- OPENIDM-5851: Backgrid: Clicking on filter reset button sorts the column
- OPENIDM-5850: groupRoleMapping in passthrough authentication not working with LDAP
- OPENIDM-5796: Change Association Dialog not working for ambiguous values
- OPENIDM-5772: Identity Relationship graph in widget isn't responsive
- OPENIDM-5754: onUpdate trigger on managed user called twice with a patch operation
- OPENIDM-5731: In Usecase 2 date validation in the Admin UI does not reject an invalid date
- OPENIDM-5724: unAssignment event not executing inline script
- OPENIDM-5721: Admin UI does not respond after setting connector nativeType to array
- OPENIDM-5705: Removal of multiple elements of an array in a single patch set produces incorrect results
- OPENIDM-5697: Cluster state failure yields permanent persistent schedule failure in cluster when a cluster node is shutdown
- OPENIDM-5622: Update of bundle file on Windows fails with "Could not remove temporary directory" error
- OPENIDM-5579: Unable to download Update Report using Safari
- OPENIDM-5541: Configuring LDAP connector with incorrect DN and trying to view the data causes the UI to fail
- OPENIDM-5504: Unable to use cli.sh for administration over a secure port
- OPENIDM-5486: Via REST API it is possible to create an assignment with an invalid mappingName
- OPENIDM-5472: OpenAM fullStack sample: session timeout option not available
- OPENIDM-5459: targetIdsCaseSensitive not honored when "links" set in mapping
- OPENIDM-5454: User profile page does not support boolean attributes on managed objects
- OPENIDM-5416: PUT REST call to AD with LDAP adapter is interpreted as create instead of update
- OPENIDM-5361: Mapping source property cannot be empty
- OPENIDM-5345: Connector names need to be validated as alpha-numeric
- OPENIDM-5297: Property substitution is lost when saving from REST

- OPENIDM-5235: Sample configuration for explicit mapping for managed user table is missing description
- OPENIDM-5107: PUT with no "If-Match" header fails to update an object with the Google Apps Connector
- OPENIDM-5091: CORS servlet filter should read https port from boot.properties
- OPENIDM-5086: Illegal State Exception REST with invalid credentials and Accept header
- OPENIDM-5038: Creating connector with underscore in its name fails with exception
- OPENIDM-5033: No validation is done when using the Admin UI to configure an LDAP connector
- OPENIDM-4918: Attempt by openidm-admin to add Security Questions leads to Problem During Profile Update error
- OPENIDM-4905: Querying info/ping returns 503 UnavailableException: Servlet not initialized
- OPENIDM-4829: Admin UI, Audit, CSV Handler configuration, fails without proper signatureInterval entry
- OPENIDM-4777: Support PATCH cluster event on ConfigObjectService
- OPENIDM-4693: Creating a Managed Object with a semicolon leads to an error
- OPENIDM-4692: ALL_GONE situation for deleted entries leads to NPE in JS
- OPENIDM-4521: Custom attributes submitted in request to store in jdbc repo are not stored but the request returns them.
- OPENIDM-4185: Command-line hashing of JSON objects provided interactively returns an exception
- OPENIDM-4076: TaskScanner dates not using ISO 8601 standard
- OPENIDM-3187: Custom authentication headers cannot handle Unicode characters
- OPENIDM-3039: Mapping page not displaying if connector with mapping is removed
- OPENIDM-2722: several samples are not working properly with sample configuration for MySQL explicit mapping
- OPENIDM-2718: Creating a user in DJ via LDAP connector with different ID in URL and payload leads to 500 but user is created anyway

3.2. Limitations

ForgeRock Identity Management 5 has the following known limitations:

- The automated update process is not currently supported on Windows platforms.
- When you add or edit a connector through the Admin UI, the list of required `Base Connector Details` is not necessarily accurate for your deployment. Some of these details might be required for specific deployment scenarios only. If you need a connector configuration where not all the Base Connector Details are required, you must create your connector configuration file over REST (see Section 13.6, "Creating Default Connector Configurations" in the *Integrator's Guide*) or edit the connector configuration file (`conf/provisioner.openicf-connector-type.json`) directly.
- For OracleDB repositories, queries that use the `queryFilter` syntax do not work on CLOB columns in explicit tables.
- 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.
- If you're using the `OPENAM_SESSION` module to help IDM work with ForgeRock Access Management software, modify the `JWT_SESSION` module to limit token lifetime to *5 seconds*. For more information, see information on the *OPENAM_SESSION Module* in the *Integrator's Guide* and Section 18.1.2.1, "Supported Session Module" in the *Integrator's Guide*.

3.3. Known Issues

The following important issues remained open at the time of this release:

- OPENIDM-7984: Unable to edit ForgeRock Identity Provider in Admin UI
- OPENIDM-7982: Backport OPENIDM-7803: Audit activity occurs for update even when before/after show no differences
- OPENIDM-7978: Full Stack sample: unable to log in as a regular user after logging out as an admin
- OPENIDM-7968: amAdmin doesn't work with fullStack (or full-stack) sample
- OPENIDM-7803: Audit activity occurs for update even when before/after show no differences
- OPENIDM-7700: Core attributes can specify returnByDefault even though not applicable
- OPENIDM-7665: Admin UI mapping view returns HTTP 400 error
- OPENIDM-7659: Updating the CSV audit event handler using the Admin UI may disable the handler
- OPENIDM-7644: Admin UI should create schedule config instead of direct scheduler entries
- OPENIDM-7422: Apostrophe character is not displaying properly in the Provisioning Roles

- OPENIDM-7284: Create manager/reports relationship with POST or PUT work on managed/user/id/reports but fails on managed/user/id/manager
- OPENIDM-7223: Recon always detects manager field as modified
- OPENIDM-7054: Samples declare wrong type for ds-pwp-account-disabled in provisioner conf
- OPENIDM-6179: UI doesn't display error when Relationship Validation fails
- OPENIDM-6072: Multiple answers to the same security question are possible
- OPENIDM-5923: ScriptedSSH sample - group members create/update is not working
- OPENIDM-5914: Role is still showing as assigned in effectiveRoles attribute on query-all output if role is unassigned via the admin UI
- OPENIDM-5909: ScriptedSSH incorrect sample provisioner group members nativeName
- OPENIDM-5907: ScriptedSSH search script unsupported filter cause timeout exception
- OPENIDM-5905: Removing a workflow definition file from the filesystem does not delete it in the config
- OPENIDM-5900: ScriptedSSH ErrorCodes.groovy is not loaded
- OPENIDM-5893: Recon on AD LDAPS mapping (tap association) gives 500 Server Error
- OPENIDM-5791: JNDI Config for JMS Audit Handler not rendered correctly.
- OPENIDM-5465: Performance Issue updating conditional role memberships
- OPENIDM-5450: When Buffering is not enabled, related options should not be available
- OPENIDM-5399: Spaces in CSV field names result in an exception when creating a CSV connector
- OPENIDM-5166: Changing CSV audit event handler formatting fields causes an exception

  Workaround: Do not use the UI to change any of the CSV Output Formatting parameters. If you need to change these parameters, change them directly in your project's `conf/audit.json` file.
- OPENIDM-4797: Connector info provider needs to be updated to connect to .NET server
- OPENIDM-4462: Delete request with HTTP "If-Match *" header does not work on repo endpoints
- OPENIDM-4227: Use value of managed object prior to save for sync events to use hashed values
- OPENIDM-4149: availableConnectors are not updated after remote ICF shut down
- OPENIDM-4127: Endpoint system/os returns cpu usage above available
- OPENIDM-3857: Cannot pass along custom context when making router requests from script

- OPENIDM-3199: When a mailtask can't be completed in an Activiti workflow, an exception is thrown
- OPENIDM-3197: '%' character in object id of openidm.read calls has to be encoded
- OPENIDM-3149: Custom Endpoint Example: object request.patchOperations is wrong for Groovy scripts
- OPENIDM-2016: Sync on unsupported object class with remote java connector returns 500 instead of 400
- OPENIDM-1898: Representation of request-object differs between code and json-representation
- OPENIDM-1488: XDate locales could not be initialized correctly
- OPENIDM-1445: Provisioner service does not decrypt encrypted attributes before passing them to OpenICF framework
- OPENIDM-1269: some issues with Case Sensitivity options for Sync
- OPENIDM-1165: EXCEPTION action when doing liveSync stops the synctoken processing
- 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
Compatibility

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

4.1. Important Changes to Existing Functionality

Take the following changes into account when updating to ForgeRock Identity Management 5. These changes will have an impact on existing deployments. Adjust existing scripts and clients accordingly:

Hikari is the default connection pool library

In ForgeRock Identity Management 5, the default connection pool library is Hikari, and not BoneCP. If you use the update mechanism to move from a previous release, your existing JDBC connection configuration will not be changed to use the new default. To use the Hikari connection pool library in an updated deployment, change your `datasource.jdbc-default.json` file, as described in Section 6.1.1, "Understanding the JDBC Connection Configuration File" in the *Integrator's Guide*.

JSON is the default file-based audit event handler

In ForgeRock Identity Management 5, the default file-based audit event handler is JSON, and not CSV. If you use the update mechanism to move from a previous release, your existing audit configuration will not be changed to use the new default. To use the JSON audit event handler in an updated deployment, enable it, as described in Section 21.2.1, "JSON Audit Event Handler" in the *Integrator's Guide*.

Changes in database schema

The database schema of the supported JDBC repositories has changed slightly in ForgeRock Identity Management 5. When you update, the repository update scripts located in the `/path/to/openidm/db/repo/script/update` directory will implement the changes for your database. To understand what has changed, you can review the update scripts for your specific repository.

Changes to how the search filter is constructed with the LDAP connector

The LDAP connector version 1.4.3.0 constructs the LDAP search filter in a different way to previous versions. Previously, the filter was built as follows:

```
(& (object class filter) (native filter) (user filter) )
```

Now the filter is built as follows:

```
(& (native filter) (user filter) (object class filter) )
```

The user filter and object class filter are now mutually exclusive. The user filter takes precedence and the object class filter is used *only* if a user filter is not defined. Consider the following excerpt of a connector configuration:

```
"configurationProperties" : {
    ...
    "accountSearchFilter" : "(uid = bjensen)",
    "accountObjectClasses" : [
        "top",
        "person",
        "organizationalPerson",
        "inetOrgPerson"
        ]
...
```

With connector versions prior to 1.4.3.0, the LDAP filter would be constructed as follows:

```
"(&(&(objectClass=top)(objectClass=person)(objectClass=organizationalPerson)
(objectClass=inetOrgPerson))(uid=bjensen))"
```

With connector versions from 1.4.3.0 onwards, the LDAP filter would be constructed as follows:

```
"(uid=bjensen)"
```

If your existing connector configuration defines a filter using either the `accountSearchFilter` or `groupSearchFilter` properties, you *must* update that filter to include *all* requirements, including any object class requirements that would otherwise have been pulled in from the `accountObjectClasses` property.

For example:

```
"accountSearchFilter" : "(&(!(userAccountControl:1.2.840.113556.1.4.803:=2))(!
(objectClass=Computer)))",
```

must be changed to:

```
"accountSearchFilter" : "(&(!(userAccountControl:1.2.840.113556.1.4.803:=2))(objectClass=User))",
```

For more information, see Section 2.4, "Constructing the LDAP Search Filter" in the *Connectors Guide*.

4.2. Deprecated Functionality

The following functionality is deprecated in ForgeRock Identity Management 5 and is likely to be removed in a future release.

- Support for Java 7 is deprecated and will be removed in the next 5.5 release.

  When upgrading to the current release, also move to Java 8 in order to be prepared for pending removal of support for Java 7.

- When configuring connectors, (see Section 13.3, "Configuring Connectors" in the *Integrator's Guide*), you can set up `nativeType` property level extensions. The `JAVA_TYPE_DATE` extension is deprecated.

- Support for a POST request with `?_action=patch` is deprecated, when patching a specific resource. Support for a POST request with `?_action=patch` is retained, when patching by query on a collection.

  Clients that do not support the regular PATCH verb should use the `X-HTTP-Method-Override` header instead.

  For example, the following POST request uses the `X-HTTP-Method-Override` header to patch user jdoe's entry:

  ```
  $ curl \
   --header "X-OpenIDM-Username: openidm-admin" \
   --header "X-OpenIDM-Password: openidm-admin" \
   --header "Content-Type: application/json" \
   --request POST \
   --header "X-HTTP-Method-Override: PATCH" \
   --data '[
      {
      "operation":"replace",
      "field":"/description",
      "value":"The new description for Jdoe"
      }
    ]' \
    "http://localhost:8080/openidm/managed/user/jdoe"
  ```

- The XML file connector is deprecated and support for its use in OpenIDM will be removed in a future release. This connector is really useful only in a demonstration context and should not be used in the general provisioning of XML data stores. In real deployments, if you need to connect to a custom XML data file, you should create your own scripted connector by using the Groovy connector toolkit.

No additional functionality is deprecated at this time.

4.3. Removed Functionality

Support for creating system objects with a client-assigned ID

The ability to specify the ID of an object when it is created is not supported across all system resources. Because the OpenICF framework cannot assess whether the resource supports a client-assigned ID, this functionality is generally no longer supported for any system object.

Ability to retrieve private keys over REST

The ability to read a private key from the `/security/keystore/privatekey` endpoint has been removed. A read on that endpoint now returns a "not supported" exception. The ability to obtain a private key when generating a certificate, or a certificate signing request has also been removed.

4.4. Functionality That Will Change in the Future

The Active Directory (AD) .NET Connector will be deprecated in a future OpenICF release, and, ultimately, support for its use with OpenIDM will be discontinued.

For simple Active Directory (and Active Directory LDS) deployments, the Generic LDAP Connector works better than the Active Directory connector, in most circumstances. For more information, see Chapter 2, "*Generic LDAP Connector*" in the *Connectors Guide*.

For more complex Active Directory deployments, use the PowerShell Connector Toolkit, as described in Chapter 5, "*PowerShell Connector Toolkit*" in the *Connectors Guide*.

Note that deprecating the AD Connector has no impact on the PowerShell connector, or on the .NET Connector Server.

Chapter 5
Documentation Updates

Table 5.1, "Documentation Change Log" tracks important changes to the documentation:

Table 5.1. Documentation Change Log

Date	Description
2017-12-xx	Updated list of fixed issues for 5.0.0.1 release (see Section 3.1.1, "Key Fixes in 5.0.0.1"). Updated the section on external rest for new configuration options (OPENIDM-9664). See (Section 24.4, "Configuring the External REST Service" in the *Integrator's Guide*).
2017-11-10	Added a workaround for the problem related to Quartz schedules and daylight savings time (Section 16.3, "Schedules and Daylight Savings Time" in the *Integrator's Guide*).
2017-10-10	Refreshed formatting.
2017-04-20	Added a note to Section 14.1, "Types of Synchronization" in the *Integrator's Guide* to indicate the required permissions for the LDAP user when configuring liveSync with DS.
2017-03-29	Initial release of ForgeRock Identity Management 5.

Chapter 6
Getting Support

This chapter offers information and resources about ForgeRock Identity Management and ForgeRock support.

6.1. Accessing Documentation Online

ForgeRock publishes comprehensive documentation online:

- The ForgeRock Knowledge Base offers a large and increasing number of up-to-date, practical articles that help you deploy and manage ForgeRock software.

  While many articles are visible to community members, ForgeRock customers have access to much more, including advanced information for customers using ForgeRock software in a mission-critical capacity.

- ForgeRock product documentation, such as this document, aims to be technically accurate and complete with respect to the software documented. It is visible to everyone and covers all product features and examples of how to use them.

6.2. Using the ForgeRock.org Site

The ForgeRock.org site has links to source code for ForgeRock open source software, as well as links to the ForgeRock forums and technical blogs.

If you are a *ForgeRock customer*, raise a support ticket instead of using the forums. ForgeRock support professionals will get in touch to help you.

6.3. Getting Support and Contacting ForgeRock

ForgeRock provides support services, professional services, classes through ForgeRock University, and partner services to assist you in setting up and maintaining your deployments. For a general overview of these services, see https://www.forgerock.com.

ForgeRock has staff members around the globe who support our international customers and partners. For details, visit https://www.forgerock.com, or send an email to ForgeRock at info@forgerock.com.