



# Release Notes

/ ForgeRock Identity Management 7.1

Latest update: 7.1.6

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

---

Copyright © 2011-2020 ForgeRock AS.

## 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.



This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License.

To view a copy of this license, visit <https://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.

© Copyright 2010-2020 ForgeRock, Inc. All rights reserved. ForgeRock is a registered trademark of ForgeRock, Inc. Other marks appearing herein may be trademarks of their respective owners.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, and distribution. No part of this product or document may be reproduced in any form by any means without prior written authorization of ForgeRock and its licensors, if any.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESSED OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

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](mailto: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](mailto:tavmjong @ free . fr).

FontAwesome Copyright

Copyright (c) 2017 by Dave Gandy, <https://fontawesome.com/>.

This Font Software is licensed under the SIL Open Font License, Version 1.1. See <https://opensource.org/licenses/OFL-1.1>.

# Table of Contents

Overview .....	iv
1. What's New .....	1
Maintenance Releases .....	1
New Features .....	1
2. Before You Install .....	5
Third-Party Software .....	10
3. Incompatible Changes .....	12
Changes between IDM 7.1.4 and 7.1.6 .....	12
Changes between IDM 7.1.2 and 7.1.4 .....	12
Changes between IDM 7.1.0 and 7.1.2 .....	12
4. Deprecation .....	17
5. Discontinued .....	21
6. Fixed Issues .....	24
IDM 7.1.6 .....	24
IDM 7.1.4 .....	24
IDM 7.1.2 .....	27
IDM 7.1.0 .....	28
7. Limitations .....	32
8. Known Issues .....	34
9. Documentation .....	36
A. Release Levels and Interface Stability .....	37
ForgeRock Product Release Levels .....	37
ForgeRock Product Stability Labels .....	38
B. Getting Support .....	40

# Overview

ForgeRock Identity Management (IDM) software provides centralized, simple management and synchronization of identities for users, devices, and things. IDM software is highly flexible and therefore able to fit almost any use case and workflow.

These release notes are written for anyone using the IDM 7.1 release. Read these notes before you install or upgrade ForgeRock Identity Management software.

## Quick Start

 <b>What's New</b> Discover new features and improvements in this version.	 <b>Prepare for Deployment</b> Learn about the requirements for running IDM software in production.	 <b>Check Compatibility</b> Review key implementation changes and compatibility with previous deployments.
 <b>Review Fixes</b> Review bug fixes, limitations, and open issues.	 <b>Check Doc Updates</b> Track important changes to the documentation.	 <b>Get Support</b> Find out where to get professional support and training.

ForgeRock Identity Platform™ serves as the basis for our simple and comprehensive Identity and Access Management solution. We help our customers deepen their relationships with their customers, and improve the productivity and connectivity of their employees and partners. For more information about ForgeRock and about the platform, see <https://www.forgerock.com>.

The ForgeRock Common REST API works across the platform to provide common ways to access web resources and collections of resources.

## Chapter 1

# What's New

## Maintenance Releases

ForgeRock maintenance releases contain a collection of fixes and minor RFEs that have been grouped together and released as part of our commitment to support our customers. For general information about ForgeRock's maintenance and patch releases, see [Maintenance and Patch Availability Policy](#).

- IDM 7.1.6 is the latest release targeted for IDM 7.1 deployments and can be downloaded from the [ForgeRock Download Center](#).

The release can be deployed as an initial deployment or updated from an existing 7.1 deployment. For information on updating from 7.1, see "[Update to a Maintenance Release](#)" in the *Upgrade Guide*.

## New Features

### IDM 7.1.6

This release of ForgeRock Identity Management software includes updates to ICF connectors, bug fixes, and the following new feature:

- The Salesforce connector template supports client\_credentials grant type. Refer to [Salesforce connector](#).

### IDM 7.1.4

This release of ForgeRock Identity Management software includes updates to ICF connectors, bug fixes, and the following new feature:

- Upgrading to DS 7.3 is now supported. Refer to [Supported Repositories](#).

### IDM 7.1.2

This release of ForgeRock Identity Management software includes updates to ICF connectors, updates to dependency libraries, and multiple bug fixes, including:

- The Flowable embedded workflow engine has been upgraded to version 6.6.0. This upgrade fixes the issue with native email tasks previously mentioned in the [Workflow Guide](#).

## IDM 7.1.0

This release of ForgeRock Identity Management software includes the following new features:

### + *Sample Showing Connection to Azure AD with the MS Graph API Connector*

The `sync-with-azuread` sample uses the MS Graph API connector to synchronize users between IDM and Azure AD.

### + *Password Sync Plugins*

#### + *Active Directory Password Synchronization Plugin UTC Timestamps*

The latest version of the Active Directory password synchronization plugin uses UTC timestamps for logs.

#### + *Active Directory Password Synchronization Plugin Infinite Loop Prevention*

The latest version of the Active Directory Password Synchronization Plugin supports a new registry key that helps prevent infinite password update loops. For more information, see the registry key, `pwdChangeInterval` in the *Password Synchronization Plugin Guide*.

#### + *Active Directory Password Synchronization Plugin Configurable Max Retries*

The latest version of the Active Directory Password Synchronization Plugin supports a new registry key to configure the maximum retry attempts for password changes. For more information, see the registry key, `maxFileRetry` in the *Password Synchronization Plugin Guide*.

#### + *Active Directory Password Synchronization Plugin Search Filter*

The latest version of the Active Directory Password Synchronization Plugin supports a new registry key to configure a search filter to omit users/groups from password syncing. For more information, see the registry key, `userSearchFilterStrict` in the *Password Synchronization Plugin Guide*.

#### + *Support for AM Bearer Tokens in the DS and Active Directory Password Synchronization Plugins*

The latest versions of the DS and Active Directory password synchronization plugins now support the use of AM bearer tokens as an authentication method. For more information, see:

- "Configure the Password Synchronization Plugin to Accept AM Bearer Tokens" in the *Password Synchronization Plugin Guide*.
- "Installing the Active Directory Password Synchronization Plugin" in the *Password Synchronization Plugin Guide*.

#### + Support for Alternative KBA Answer Hashing

Previously, KBA answers were always hashed as SHA-256 upon save, which is still the default setting; however, you can now specify an alternative hashing algorithm in the *Self-Service Reference*.

#### + Managed Object Default Values

You can now specify default values in the *Object Modeling Guide* for properties in the managed object configuration. For example, the default managed object configuration (You can edit the managed object configuration over REST at the `config/managed` endpoint, or directly in the `config/managed.json` file.) includes a default value that makes `accountStatus:active`, which effectively replaces the `onCreate` script that was previously used to achieve the same result.

##### Note

IDM assumes all default values are valid for the schema. Although IDM skips policy validation for objects with default values, you can force validation in the *Object Modeling Guide* on property values.

#### + Support for REST Queries on Array Properties (JDBC)

You can now perform REST queries on properly configured array fields.

For more information, see:

- "Queries on Object Array Properties (JDBC)" in the *Object Modeling Guide*
- "Configure Array Fields" in the *Installation Guide*
- "Convert an Explicit Mapped Object to a Generic Mapped Object (JDBC)" in the *Object Modeling Guide*

#### + 'waitForCompletion' Property Added to the 'config' Endpoint

The optional `waitForCompletion` parameter is now available to the `config` endpoint for create, update, and patch requests.

For more information, see:

- "Configure the Server Over REST" in the *Setup Guide*
- "Server Configuration" in the *REST API Reference*

#### + *API Endpoint Requires Admin Authentication*

To protect production servers from unauthorized API descriptor requests, IDM now requires admin authentication for the API endpoint. For more information, see "Securing the API Explorer" in the *Security Guide*.

#### + *Additional Query Types in JDBC Explicit Tables*

Queries on explicit tables in JDBC now support `bool:`, `num:`, and `long:` in addition the previously supported query parameters (strings, `list:`, and `int:`).

## 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](mailto:info@forgerock.com).

### + *Hardware and Memory Requirements*

Due to the underlying Java platform, IDM software runs well on a variety of processor architectures.

When you install IDM for evaluation with the embedded DS repository, you need 256 MB memory (32-bit) or 1 GB memory (64-bit) available.

You also need 10 GB free disk space for the software and for sample data.

#### **Important**

A DS repository (whether embedded or external) requires free disk space of 5% of the filesystem size, plus 1 GB by default. To change this requirement, set the `disk-full-threshold` in the DS configuration. For more information, see Disk Space Thresholds in the *DS Maintenance Guide*.

In the case of an embedded DS instance, you can manage the configuration using the `dsconfig` command in `/path/to/openidm/db/openidm/openssl/bin`.

In production, disk space and memory requirements will depend on the size of your external repository, as well as the size of the audit and service log files that IDM creates.

The amount of memory that IDM consumes is highly dependent on the data that it holds. Queries that return large data sets will have a significant impact on heap requirements, particularly if they are run in parallel with other large data requests. To avoid out-of-memory errors, analyze your data requirements, set the heap configuration appropriately, and modify access controls to restrict requests on large data sets.

### + *Operating System Requirements*

Identity Management 7.1 software is supported on the following operating systems:

- Red Hat Enterprise Linux (and CentOS Linux) 7.0 and 8.0

- Ubuntu Linux 16.04, 18.04, and 20.04
- Windows Server 2012 R2, 2016, and 2019

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

## + Java Requirements

Identity Management software supports the following Java environments:

### *Supported Java Versions*

Vendor	Versions
OpenJDK, including OpenJDK-based distributions: <ul style="list-style-type: none"> <li>• AdoptOpenJDK/Eclipse Adoptium</li> <li>• Amazon Corretto</li> <li>• Azul Zulu</li> <li>• Red Hat OpenJDK</li> </ul> ForgeRock tests most extensively with AdoptOpenJDK/Eclipse Adoptium. ForgeRock recommends using the HotSpot JVM.	11
Oracle Java	11

## + Supported Web Application Containers

You must install IDM as a stand-alone service, using the bundled Apache Felix framework and Jetty web application container. Alternate containers are not supported.

IDM bundles Jetty version 9.4.22.

## + Supported Repositories

The following repositories are supported for use in production:

- ForgeRock Directory Services (DS) 7.1 and 7.3.

By default, IDM uses an *embedded* DS instance for testing purposes. The embedded instance is not supported in production. If you want to use DS as a repository in production, you must set up an external instance.

- MySQL version 5.7 and 8.0 with MySQL JDBC Driver Connector/J (at least version 5.1.18).
- MariaDB version 10.2 and 10.3 with MySQL JDBC Driver Connector/J (at least version 5.1.18).
- Microsoft SQL Server 2014, 2016, and 2017.
- Oracle Database 12c, 12c Release 2 (12.2), and 19c.
- PostgreSQL 9.6, 10.13, 11.6, and 12.5.
- IBM DB2 11 and 11.1.

ForgeRock supports repositories in cloud-hosted environments, such as AWS and GKE Cloud, as long as the underlying repository is supported. In other words, the repositories listed above are supported, regardless of how they are hosted.

**Note**

These repositories might not be supported on all operating system platforms. See the specific repository documentation for more information.

Do not mix and match versions. For example, if you are running Oracle Database 19c, and want to take advantage of the support for Oracle UCP, download driver and companion JARs for Oracle version 19c.

### + *Supported Browsers*

The IDM UI has been tested with the latest, stable versions of the following browsers:

- Chrome and Chromium
- Edge
- Firefox
- Safari

### + *Supported Connectors*

IDM bundles the following connectors:

- Adobe CM Connector
- CSV File Connector
- Database Table Connector

- Google Apps Connector
- Groovy Connector Toolkit

This toolkit lets you create scripted connectors to virtually any resource.

- Kerberos Connector
- LDAP Connector

Using 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).

- Marketo Connector
- Microsoft Graph API Connector
- MongoDB Connector
- Salesforce Connector
- SCIM Connector
- Scripted REST Connector
- Scripted SQL Connector
- ServiceNow Connector
- Scripted SSH Connector

You can download a PowerShell Connector Toolkit from the [ForgeRock BackStage download site](#). This Toolkit lets you create scripted connectors to address the requirements of your Microsoft Windows ecosystem.

Additional connectors are available from the [ForgeRock BackStage download site](#).

Windows Server 2012 R2, and 2016 are supported as the remote systems for connectors and password synchronization plugins.

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. For more information, see "IDM / ICF Compatibility Matrix".

The Java connector server requires Java 11, and is supported on any platform on which Java runs.

The .NET connector server requires the .NET framework (version 4.5 or later) and is supported on Windows Server versions 2012 R2, and 2016.

### 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 the Samples Guide.

The following table lists the connector and connector server versions that are supported across IDM versions. For a list of connectors supported with this IDM release, see [Overview](#) in the *Connectors Guide*. For a list of connector releases associated with this version of IDM, see "[Connector Release Notes Overview](#)" in the *Connector Release Notes*

*IDM / ICF Compatibility Matrix*

IDM Version	Connector Server Version	Java Connectors	Scripted Groovy Connectors	.NET Connectors
4.x	1.4.x, 1.5.x	Java connectors version 1.1.x - 1.5.x	Scripted REST, Scripted SQL, SSH, Kerberos connectors up to version 1.5.1.0.	PowerShell Connector 1.4.x
5.x	1.4.x, 1.5.x	Java connectors version 1.1.x - 1.5.x	Scripted REST, Scripted SQL, SSH, Kerberos connectors up to version 1.5.1.0.	PowerShell Connector 1.4.x
6.x	1.4.x, 1.5.x	Java connectors version 1.1.x - 1.5.x	Scripted REST, Scripted SQL, SSH, Kerberos connectors up to version 1.5.1.0.	PowerShell Connector 1.4.x
7.x	1.4.x, 1.5.x	Java connectors version 1.1.x - 1.5.x	Scripted REST, Scripted SQL, SSH, Kerberos connectors version 1.5.x.	PowerShell Connector 1.4.x

### + Supported Password Synchronization Plugins

The following table lists the supported password synchronization plugins:

*Supported Password Synchronization Plugins*

Plugin	Supported Version
DS Password Synchronization Plugin	7.1.x, supported with DS 7.1.x and IDM 7.1.x 7.0.2, supported with DS 7.0.x, IDM 7.0.x, and IDM 7.1.x 6.5.6, supported with DS 6.5.x and IDM 6.5.x 6.0, supported with DS 6.0.x and IDM 6.0.x

Plugin	Supported Version
	<p>5.5.0, supported with DS 5.5.x and IDM 5.5.x</p> <p>5.0, supported with DS 5.0.x and IDM 5.0.x</p> <p>3.5, supported with OpenDJ 3.5 and OpenIDM 4.x</p> <p>DS Password Sync plugins are not supported with DS OEM</p>
Active Directory Password Synchronization Plugin	<p>1.7.0, 1.5.0, 1.4.0, 1.3.0, 1.2.0 and 1.1.0 supported on Windows Server versions 2012 R2, 2016, and 2019</p> <div> <p><b>Note</b></p> <p>Because version 1.4.0 can fail to make a secure connection with certain Windows versions, ForgeRock recommends using a later version.</p> </div>

## Third-Party Software

ForgeRock provides support for using the following third-party software when logging ForgeRock Common Audit events:

Software	Version
Java Message Service (JMS)	2.0 API
MySQL JDBC Driver Connector/J	8 (at least 8.0.19)
Splunk	8.0 (at least 8.0.2)

### Tip

Elasticsearch and Splunk have native or third-party tools to collect, transform, and route logs. Examples include Logstash and Fluentd.

ForgeRock recommends that you consider these alternatives. These tools have advanced, specialized features focused on getting log data into the target system. They decouple the solution from the ForgeRock Identity Platform systems and version, and provide inherent persistence and reliability. You can configure the tools to avoid losing audit messages if a ForgeRock Identity Platform service goes offline, or delivery issues occur.

These tools can work with ForgeRock Common Audit logging:

- Configure the server to log messages to standard output, and route from there.

- Configure the server to log to files, and use log collection and routing for the log files.

ForgeRock provides support for using the following third-party software when monitoring ForgeRock servers:

Software	Version
Grafana	5 (at least 5.0.2)
Graphite	1
Prometheus	2.0

For hardware security module (HSM) support, ForgeRock software requires a client library that conforms to the PKCS#11 standard v2.20 or later.

## Chapter 3

# Incompatible Changes

When you update to IDM 7.1.6, the following changes may impact existing deployments. Adjust existing scripts, files, and clients, as necessary:

## Changes between IDM 7.1.4 and 7.1.6

No additional incompatible changes were made between 7.1.4 and 7.1.6.

## Changes between IDM 7.1.2 and 7.1.4

No additional incompatible changes were made between 7.1.2 and 7.1.4.

## Changes between IDM 7.1.0 and 7.1.2

### + *Embedded Workflow Database*

Previously, you could use the Flowable workflow engine's embedded H2 database for demo and testing purposes. IDM no longer includes this database. Before you use workflow, you must install a JDBC repository in the *Installation Guide*.

For more information, see "*Enable Workflows*" in the *Workflow Guide*.

### + *Workflow Version Update*

Previously, workflows would break when upgrading from version 7.0.2 to 7.1.0 of IDM, due to out of sync versions of the Flowable workflow engine. This is fixed in version 7.1.2 of IDM. If you are upgrading IDM from version 7.0, please use IDM version 7.1.2 or higher.

## Changes between IDM 7.0.x and 7.1.0

### + *Data Format Change for External DS Repositories*



For external DS repositories, with explicitly mapped managed objects, the stored data format has changed for certain data types.

In IDM versions prior to 7.1, certain property values were always considered as strings, so the returned JSON format of a managed object would look something like this:

```
{
  "boolean": "true",
  "integer": "12345",
  "timestamp": "20210315010101Z",
  "json": "{\"key\":\"value\"}"
}
```

In IDM 7.1, these properties are returned with the correct data type, so a similar object in IDM 7.1 looks something like this:

```
{
  "boolean": true,
  "integer": 12345,
  "timestamp": "2021-03-15T01:01:01Z",
  "json": { "key": "value" }
}
```

New deployments are not impacted by this change. If you are upgrading an existing deployment with an external DS repository, with explicit object mappings, you should test this change and adapt your scripts and REST API calls, if necessary.

The data types affected by this change are as follows:

- Booleans: from string to JSON boolean

Affected OIDs: [1.3.6.1.4.1.1466.115.121.1.7](#) and [1.3.6.1.4.1.36733.2.1.3.3.7](#)

- Integers: from string to JSON integer

Affected OIDs: [1.3.6.1.4.1.1466.115.121.1.27](#) and [1.3.6.1.4.1.36733.2.1.3.3.27](#)

- Generalized time: from string in LDAP generalized time format, to string in ISO 8601 format

Affected OIDs: [1.3.6.1.4.1.1466.115.121.1.24](#) and [1.3.6.1.4.1.36733.2.1.3.3.24](#)

- JSON: from JSON embedded in a string to structured JSON

Affected OIDs: [1.3.6.1.4.1.36733.2.1.3.1](#)

#### Note

If you want to retain the legacy behavior, set the following property in `conf/system.properties`:

```
openidm.ds.rest2ldap.ignoreSchema.enabled=true
```

This is *not recommended* in a production deployment, and should be used only temporarily, as part of a plan to adapt to these changes.

### + Audit Handler Changes

The `JsonStdoutAuditEventHandler` is now pre-configured in the standard audit configuration, but is disabled by default.

Previously, to enable/disable audit handlers, you needed to modify `conf/audit.json` directly. Now, you can set the following properties in the `resolver/boot.properties` file to `true` or `false`:

- `openidm.audit.handler.json.enabled`
- `openidm.audit.handler.stdout.enabled`
- `openidm.audit.handler.repo.enabled`

For more information, see:

- "Choose Audit Event Handlers" in the *Audit Guide*
- "Property Value Substitution" in the *Setup Guide*

### + Parameterized HTTP and HTTPS Enablement

Previously, to enable/disable HTTP or HTTPS, you could modify `conf/config.properties` directly. Now, you can set the following properties in the `resolver/boot.properties` file to `true` or `false`:

- `openidm.https.enabled`
- `openidm.http.enabled`

For more information, see "Property Value Substitution" in the *Setup Guide*.

### + Parameterized Felix Web Console Credentials

Previously, to change the Felix web console credentials, you could modify the `conf/felix.webconsole.json` file directly. Now, you can set the following properties in the `resolver/boot.properties` file:

- `openidm.felix.webconsole.username`
- `openidm.felix.webconsole.password`

For more information, see:

- "Removing or Protecting Development and Debug Tools" in the *Security Guide*
- "Property Value Substitution" in the *Setup Guide*

#### + Notification Changes

Notifications are now disabled, by default. Previously, to enable/disable notifications, you could modify the applicable `conf/notificationType.json` file directly. Now, you can set the following properties in the `resolver/boot.properties` file to `true` or `false`:

- `openidm.notifications.passwordUpdate`
- `openidm.notifications.profileUpdate`
- `openidm.notifications`

For more information, see "Configure Notifications" in the *Audit Guide*.

#### + Moved Configuration Files

The following files have been moved from the `/path/to/openidm/conf/` directory:

- `auth.profile.json` in the *Self-Service Reference* moved to `/path/to/openidm/samples/example-configurations/self-service/`.
- `jsonstore.json` in the *Self-Service Reference* moved to `/path/to/openidm/samples/example-configurations/self-service/`.
- `identityProviders.json` in the *Self-Service Reference* moved to `/path/to/openidm/samples/example-configurations/self-service/`.

#### + Improved `validateProperty` Error Handling

Previously, API requests containing the `validateProperty` action to unknown resources or those with invalid POST body content could result in an invalid `true` response, or a generic 500 Internal Server Error. Both of these situations now return a 400 Bad Request Error with an explanation.

##### Error Comparison

- BEFORE:

```
{
  "code": 500,
  "reason": "Internal Server Error",
  "message": "TypeError: Cannot call method \"hasOwnProperty\" of null",
  "detail": {}
}
```

- AFTER:

```
{
  "code": 400,
  "reason": "Bad Request",
  "message": "object and properties were not provided in request content, and they are unable to be
retrieved.",
  "detail": {}
}
```

#### + *Changes to router.json*

The default `router.json` file no longer includes `system` in the matching pattern.

## Chapter 4

# Deprecation

The following features are deprecated and likely to be discontinued in a future release:

### + *Splunk and Elasticsearch Audit Handlers*

The Splunk and Elasticsearch audit event handlers are deprecated.

IDM 7.1 supports both file-based audit handlers and logging to standard output, which Elasticsearch and Splunk can consume.

### + *Access Configuration in access.js*

In previous releases, access rules were configured in the `access.js` script. This script has been replaced by an `access.json` configuration file, that performs the same function. Existing deployments that use customized `access.js` files are still supported for backward compatibility. However, support for access rules defined in `access.js` is deprecated, and will be removed in a future release. You should move these access rules to a `conf/access.json` file. For more information, see "Authorization and Access Control" in the *Authentication and Authorization Guide*.

### + *Actions on scheduler Endpoint*

The `action` parameter on the `scheduler` endpoint was deprecated in Version 1 of the endpoint and is not supported in Version 2.

To validate a cron expression, use the `validateQuartzCronExpression` action on the `scheduler/job` endpoint, as described in *Validate Cron Trigger Expressions in the Schedules Guide*.

### + *Health Endpoints*

The `health` endpoints, used to monitor system activity have been deprecated in this release, as their functionality was not considered to be of much use.

The information available on `health/recon` was node-specific. Instead, you can retrieve cluster-wide reconciliation details with a GET on the `recon` endpoint.

The information available on the `health/os` and `health/memory` endpoints can be retrieved by inspecting the JVM using third-party tools such as the Prometheus JMX Exporter.

### + Conditional Query Filters

The syntax of conditional query filters and scripts within notification filters has changed in this release. In previous IDM releases, request properties such as `content` in create and update requests or `patchOperations` in patch requests were referenced directly. For example, the `notification-newReport.json` configuration previously used the following query filter:

```
"condition" : "content/manager pr"
```

In IDM 7, query filters and scripts should reference the `request` object to obtain any request properties. Sample query filters have been changed accordingly. For example, the query filter in `notification-newReport.json` has been changed to the following:

```
"condition" : "request/content/manager pr",
```

This syntax is more verbose, but it lets script implementations use request visitors logic based on the request type, and is more consistent with generic router filters.

The old request syntax will still work in IDM 7.0, but is considered deprecated. Support for the old syntax will be removed in a future release. Note that this change is limited to notification filters. Filters such as those used with scripted endpoints have never supported direct access to request properties, and are therefore not changing. For more information on notification filters, see *"Configure Notifications"* in the *Audit Guide*.

### + Self-Service Stages

Self-Service Stages (described in *"Self-Service Stage Reference"* in the *Self-Service Reference*) are deprecated in this release and support for their use will be removed in a future release. From IDM 7 onwards, this functionality is replaced by AM Authentication Trees.

### + `oauthReturn` Endpoint

Support for `oauthReturn` as an endpoint for OAuth2 and OpenID Connect standards has been deprecated for interactions with AM and will be removed in a future release. Support for interactions with social identity providers was removed in IDM 6.5.0.

Default versions of relevant configuration files no longer include `oauthReturn` in the `redirectUri` setting. However, for IDM 7.1, these configuration files should still work both with and without `oauthReturn` in the endpoint.

### + `timeZone` in Schedules

In schedule configurations, setting a time zone using the `timeZone` field is deprecated. To specify a time zone for schedules, use the `startTime` and `endTime` fields.

#### + MD5 and SHA-1 Hash Algorithms

Support for the MD5 and SHA-1 hash algorithms is deprecated and will be removed in a future release. You should use more secure algorithms in a production environment. For a list of supported hash algorithms, see "Encoding Attribute Values by Using Salted Hash Algorithms" in the *Security Guide*.

#### + JAVA\_TYPE\_DATE Attribute Type

Support for the native attribute type, `JAVA_TYPE_DATE`, is deprecated and will be removed in a future release. This property-level extension is an alias for `string`. Any dates assigned to this extension should be formatted per ISO 8601.

#### + POST Request With `?_action=patch`

Support for a POST request with `?_action=patch` is deprecated, when patching a specific resource. You can still use `?_action=patch` 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 "Accept-API-Version: resource=1.0" \
--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"
```

#### + `minLength` property

The managed object property `minLength` is deprecated. When you need to specify a minimum length for a property, instead use the `minimum-length` policy:

```
{
  "policyId" : "minimum-length",
  "params" : {
    "minLength" : 8
  }
}
```

+ *OAUTH\_CLIENT authentication module*

The `OAUTH_CLIENT` authentication module is deprecated. Using OAuth2 for authentication is available through `rsFilter` authentication. For more information about `rsFilter`, see "Authenticate through AM" in the *Authentication and Authorization Guide*.



## Chapter 5

# Discontinued

Support for the following functionality has been removed in this release:

### + *Native queries using `queryExpression`*

Native query expressions using the `_queryExpression` keyword are no longer supported on managed objects. You must rewrite any custom queries that use `_queryExpression` as regular `filtered queries` or as `parameterized queries`. Native query expressions are still supported for system objects.

### + *`reloadScriptOnExecution` for Scripted Groovy connectors*

For scripted Groovy connectors, the `reloadScriptOnExecution` property has been removed from all sample provisioner files, as the property is not used by the connectors. For information on how scripts are loaded, see "Script Compilation and Caching" in the *Connectors Guide*.

Note that scripted PowerShell connectors still use the `ReloadScriptOnExecution` property to determine when a script is reloaded from disk.

### + *Properties from `boot.properties`*

The following properties have been removed from `resolver/boot.properties`:

- `openidm.script.javascript.debug`
- `openidm.script.javascript.sources`
- `openidm.ssl.host.aliases`
- `com.ipplanet.am.cookie.name`
- `com.sun.identity.auth.cookieName`

### + *Custom aliases for default keys*

You can no longer specify custom aliases for the default keys that IDM generates on startup. For more information about these keys, see ["Working With the Default Keystore"](#) in the *Security Guide*.

#### + *Communication protocol for connector servers*

In previous IDM releases, the `protocol` property of a connector server configuration specified the communication protocol to the remote connector server. This property existed purely for legacy purposes and was set to `websocket` by default. The property has now been removed, and connections to the remote connector server *always* use the `websocket` protocol.

#### + *Full Stack sample*

The "full stack sample" (*Integrating IDM With the ForgeRock Identity Platform*) has been removed in this release. The only supported method of authentication through AM is by using AM bearer tokens and the `rsFilter` authentication module. For information on configuring an integrated deployment, see the [Platform Setup Guide](#).

#### + *Obfuscating and encrypting property values*

The ability to generate obfuscated and encrypted property values by using the crypto bundle has been removed. This functionality is replaced by the *secrets* service. For more information, see ["Secret Stores, Certificates and Keys"](#) in the *Security Guide*.

#### + *Self-service registration with the legacy UI*

When configuring self-service registration, the `idmUserDetails` stage had previously used the `identityResourceUrl` property instead of `identityServiceUrl`. This stage now correctly uses the `identityServiceUrl` property. `identityResourceUrl` has been removed. For more information about self-service registration, see ["Self-Registration"](#) in the *Self-Service Reference*.

#### + *ScriptedCREST Connector and Sample*

The ScriptedCREST connector and the corresponding sample have been removed in this release. You should migrate any deployments use this connector to the ["Scripted REST Connector"](#).

#### + *Office 365 Connector*

Support for the Office 365 connector has been removed in this release.

Instead of the Office 365 connector, use the "MS Graph API Java Connector" in the *Connectors Guide*.

#### + *Active Directory Connector*

Support for the Active Directory (AD) .NET Connector has been removed.

For simple Active Directory (and Active Directory LDS) deployments, use the *Generic LDAP Connector*.

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

## Chapter 6

# Fixed Issues

### IDM 7.1.6

The following important bugs were fixed in this release:

- OPENIDM-16678: Clustered recon fails with "Schedule does not exist"
- OPENIDM-18743: IDM throws a NPE when `operationOptions{}` is defined in the provisioner
- OPENIDM-18875: Incorrect behaviour in handling variables in workflow subprocesses
- OPENIDM-19082: Support for upgrading DS with IDM 7.1.x
- OPENIDM-19141: `tablePrefix` and `tablePrefixIsSchema` is not honoured in IDM 7.1.2. In IDM 6.5.x this was the case.
- OPENIDM-19411: Recovery of queued sync events at startup does not use paged queries
- OPENIDM-19466: Queued sync not working
- OPENIDM-19590: IDM 7.1.x fails to load the log handler when running audit-jms sample
- OPENIDM-19639: Salesforce connector template update for `client_credentials` grant for OPENICF-2246

### IDM 7.1.4

The following important bugs were fixed in this release. For details and information on other issues, see the [IDM issue tracker](#):

- OPENIDM-15670: Workflow Invocation Does Not Work with Platform Enduser UI 7.0 in AM/IDM Integrated deployments
- OPENIDM-15622: Managed object roles `_refProperties` incomplete if `_sortKeys` included, when using DS repo
- OPENIDM-17856: Possible multiple X-Not-Modified headers appended to response
- OPENIDM-16607: If deletion of the previous recon data under `ou=assoc` fails the data is never cleaned up

- OPENIDM-17913: Workday connector fails to start
- OPENIDM-17988: Error being thrown editing a user with an organization relationship type field
- OPENIDM-17987: Generic Add Connector template incorrectly sets enabled boolean to string value
- OPENIDM-17985: From field not allowing saving email address with multiple "domains" after the @
- OPENIDM-17531: Conditional policy is not enforced for patch remove
- OPENIDM-16478: Environment Variables do not get parsed when added to managed.json
- OPENIDM-17532: Unable to access to audit data using auditdb connector
- OPENIDM-16866: Setting managed/user/roles schema to returnByDefault = true breaks password tab in user edit page
- OPENIDM-17605: 00-propertyindex.sql requires EOF character
- OPENIDM-17909: IDM admin UI: disallowedFields.map TypeError if password policies include cannot-contain-others and other policies
- OPENIDM-17664: Adding whitespace in BaseDN results in invalid configuration
- OPENIDM-16290: DA: Resulting privileges calculated incorrectly if object update modifies the qualifying attribute
- OPENIDM-17870: Attempting to write certain data to the audit logs on a SQL DB results in a retry-loop event.
- OPENIDM-17393: Data Association Management Tab Exception
- OPENIDM-17364: Some variables are undefined when triggering "Sample source preview" in mapping
- OPENIDM-17269: User creation with a blank telephoneNumber results in managed/user object with a telephoneNumber attribute value of ""
- OPENIDM-17773: Delete operations fail with DB2 repository
- OPENIDM-17743: With dynamic roles enabled, using social provider login results in a return to the login page
- OPENIDM-17652: UI: IDM Recon result failure summary display no data when clicking on "View Entries"
- OPENIDM-16449: End User UI allows DA to perform operations that are disallowed by Admin UI on "relationship" type attributes
- OPENIDM-17702: propertyObject is not defined

- OPENIDM-17567: audit data while using samples/audit-jdbc throws 500 Error
- OPENIDM-17591: NPE when creating object with null value for singleton relationship
- OPENIDM-17792: 7.1 doesn't start on M1 mac
- OPENIDM-18123: Correctly load scripts that use ISO 8859-1 encoding
- OPENIDM-17642: Document the usage of cancel action on openidm.action "recon"
- OPENIDM-16768: Workflow process form should submit formProperty id instead of name
- OPENIDM-16677: Cannot retrieve entries from /recon endpoint when using DS as a repo if reconprogressstate size exceeds index limits
- OPENIDM-16472: Relationship properties sent to repo as part of defaultPostMapping patch
- OPENIDM-18211: Unable to resolve org.forgerock.openidm.workflow-activiti
- OPENIDM-17876: Query filter editor incorrectly removes double quotes from all properties that aren't of type "string"
- OPENIDM-17924: Conditional policy, with required policyId, modifies the schema
- OPENIDM-17847: Relationship Properties label is invisible due to white font
- OPENIDM-17989: Tag not closed on Native UI for scripted rest connector "/button"
- OPENIDM-17984: In samples/audit-jdbc, the column for response\_detail is missing from the sample files.
- OPENIDM-17394: Two tabs for privileges when Internal roles created on UI
- OPENIDM-17980: Inconsistent Policy Validation message on Admin UI for some policyId's
- OPENIDM-17869: Inconsistent display with viewable option for managed object creation on Admin UI
- OPENIDM-17726: Inconsistent UI display for custom attribute creation
- OPENIDM-17687: Admin UI updates manager relationship using only the \_ref field
- OPENIDM-17472: Discrepancy table name in upgrade script for Oracle DB
- OPENIDM-16037: UI does not reflect the default sync failure handler if none is specified
- OPENIDM-17360: Subsequent logins with social provider throws 500 error
- OPENIDM-15050: Please add SchemaScript.groovy to audit-jdbc sample
- OPENIDM-17894: 404 page license is 3 years out of date

- OPENIDM-17498: LiveSync stops working with RCS
- OPENIDM-16906: Sample auditjdbc causes increasing flow of exceptions

## IDM 7.1.2

The following important bugs were fixed in this release. For details and information on other issues, see the [IDM issue tracker](#):

- OPENIDM-17053: Registration form is not loading
- OPENIDM-16944: ttf-dejavu font is deprecated. Review for removal from dockerfile
- OPENIDM-17195: Change password button disabled state is inverted
- OPENIDM-16216: Delegated Admin UI should not attempt to load first page of whole dataset
- OPENIDM-17138: JsonValueException thrown when using Social providers Authentication
- OPENIDM-16479: Privileges not displayed when user authenticates with certificate
- OPENIDM-16929: Values of relationship properties lost when updating another relationship property on the same object
- OPENIDM-16920: base contexts and base contexts to synchronize not properly compared
- OPENIDM-17133: JsonValueException thrown when using Passthrough Authentication
- OPENIDM-16732: Unable to generate API description for custom endpoints
- OPENIDM-16771: Updating managed/user property from the EndUserUI fails with policy validation error if there are Required relationships
- OPENIDM-16727: Admin UI displays object relationships incorrectly when uninitialised virtual property is present
- OPENIDM-16696: Failing to load a CA-signed certificate due to restrictive KeyUsage constraints in the certificates themselves
- OPENIDM-16640: Updated relationship properties are no longer available to property onRetrieve hooks after object onUpdate
- OPENIDM-16484: Error when accessing managed user object that has relationship to itself
- OPENIDM-16464: End User UI tries to create user with boolean in relationship field
- OPENIDM-16433: Policy Validation messages not displayed as field error message in the DA End user UI

- OPENIDM-16519: QueryFilters on reference properties do not work with ds as a repo
- OPENIDM-16444: Content-API-Version header does not appear in REST call in IDM 7.0.1
- OPENIDM-16267: Update sample provisioner files to use a non-specific bundleVersion range
- OPENIDM-15843: RouterAuditEventHandler groovy script throws an error when trying to write out Scheduler events to activity audit.
- OPENIDM-15696: Upgrade to Flowable 6.6.0
- OPENIDM-15792: Selfservice registration submits input as string for boolean attribute
- OPENIDM-13845: Sorting by default leads to extreme slowness in Admin UI
- OPENIDM-17204: Changed value of totalPagedResultsPolicy from ESTIMATE to EXACT causing negative impact on query performance
- OPENIDM-16969: Adding incorrect type to managed attribute expecting a map results in 500 error
- OPENIDM-17344: Update post\_request\_receiving\_204\_response test to use HTTPS requests to httpstat.us
- OPENIDM-17331: Investigate delegated admin role\_grants\_with\_temporal\_constraint test failures
- OPENIDM-16386: Inconsistent policy evaluation between replace and add no-op PATCH requests
- OPENIDM-16931: SynchronizationException caught on clustered recon node not propagated to other nodes
- OPENIDM-16379: Removing values from a multi-valued managed/user property fails with policy validation error if the property is set to Required
- OPENIDM-17306: Nullable boolean variables are set to false
- OPENIDM-17077: IDM becomes unresponsive when external postgres pod goes into read only mode.
- OPENIDM-17071: NullPointerException with augmentSecurityContext

## IDM 7.1.0

The following important bugs were fixed in this release. For details and information on other issues, see the [IDM issue tracker](#):

- OPENIDM-16095: Configure Reverse Relationship Error
- OPENIDM-15220: Temporal constraints on internal role grants with privileges are not reflected in the end-user UI



- OPENIDM-15578: Incorrect calculation of the lastSync attribute by defaultPostMapping.groovy
- OPENIDM-15562: Schedule will be invoked when changing schedule properties even if the schedule is "enabled" : false
- OPENIDM-15909: Unable to delete mapping if managed/resource -> managed/resource
- OPENIDM-15780: IDM should not transform queryId to queryFilters for external/migration
- OPENIDM-14494: Admin UI: Email Settings handling of property substitution
- OPENIDM-14645: Saving privacy & encryption or script tab on relationship edit screen doesn't save
- OPENIDM-14832: triggerSyncProperties does not work when using an encrypted password
- OPENIDM-12805: Allow target-vertex field filtering on edge-vertex relationship query with embedded DJ
- OPENIDM-15637: In the admin UI, trying to save a source query in a reconciliation query filter doesn't work
- OPENIDM-15372: ldapGroups cannot be used as the attribute with assignments
- OPENIDM-15320: Changing connectionTimeout in datasource.jdbc makes no difference in behavior
- OPENIDM-15584: Using Salesforce connector and changing the updated context URL is not picked up
- OPENIDM-15989: Updated relationship properties are no longer available to property onRetrieve hooks after object onUpdate
- OPENIDM-15576: Unable to save the 'Reconciliation Query Filters' under Mappings in the Admin UI.
- OPENIDM-16113: rsFilter is case sensitive, which triggers authentication errors
- OPENIDM-15792: Selfservice registration submits input as string for boolean attribute
- OPENIDM-15076: Updating connector config in a clustered env could inflate config rev number and incur deadlock at repo db level
- OPENIDM-15021: authenticationIdKey setting is not respected during registration/authentication with OpenIDConnectClient
- OPENIDM-14651: Edit and saving a managed object results in UI breaking
- OPENIDM-16207: CSV File Connector property Password Column input has "password" type in UI
- OPENIDM-16390: Bad definition of "roles" in SCIM provisioner sample.
- OPENIDM-15695: IDM Admin UI: shows Unauthorized message for Forbidden errors

- OPENIDM-15901: IDM gives no log feedback when it is shutting down
- OPENIDM-15122: validateProperty fails with conditionalPolicies
- OPENIDM-15546: Access token containing subject not found by rsFilter results in anonymous
- OPENIDM-15718: triggerSyncProperties does not work properly when using roles
- OPENIDM-15871: Policy validation fails for nested attributes in managed.json
- OPENIDM-15853: Unable to complete connection with Salesforce Connector when using an updated urlContextRoot
- OPENIDM-16191: New live sync schedule created from UI is missing invokeContext.source
- OPENIDM-15805: End User UI doesn't format page correctly within Delegated Admin's view of managed/users with very long details
- OPENIDM-15511: IDM Admin console - Paging controls in managed objects are disabled
- OPENIDM-15507: Paging controls in connector data tab are disabled and should not be
- OPENIDM-16394: IDM 6.5.0.3 end-user UI blank in IE11
- OPENIDM-16206: TaskScanner tries to read object after deletion
- OPENIDM-15782: Unable to edit KBA security questions in the Admin UI
- OPENIDM-15932: Blank Page shown for Admin UI Login-in Page in IE11
- OPENIDM-16134: /system?\_action=createFullConfig unexpectedly replaces variables
- OPENIDM-15016: OperationOptions specified within the provisioner configuration are not passed to connectors by OpenIDM
- OPENIDM-15796: User creation form in end-user-ui, unable to <tab> to boolean fields
- OPENIDM-15529: If ICF \_\_NAME\_\_ is null on Create, then Create will fail if trace enabled
- OPENIDM-14601: "View Resource" button in linked systems links to invalid URL
- OPENIDM-15449: IDM admin UI does not save boolean property (of an object attribute) based on role conditions
- OPENIDM-15846: Password that contain special characters do not work for internal users
- OPENIDM-15903: Grant Type not shown in the Grant Column for Assigned Roles
- OPENIDM-15266: Admin UI defaults number attributes to 0 when creating a managed resource
- OPENIDM-15331: UI always warns of 'Pending Changes' to time constraint when a role condition is defined

- OPENIDM-15011: validateObject fails if userName contains single parenthesis
- OPENIDM-15559: working-location option to startup.sh does not set felix-cache location
- OPENIDM-15481: Admin UI translation.json contains duplicate key "selectResource" with different value

## Chapter 7

# Limitations

ForgeRock Identity Management 7.1.6 has the following known limitations:

### + *Workflow limitations*

- Workflows are not supported with a DS repository. If you are using a DS repository for IDM data, you must configure a separate JDBC repository as the [workflow datasource](#) in the *Workflow Guide*.
- The embedded workflow and business process engine is based on Flowable and the Business Process and Notation (BPMN) 2.0 standard. As an embedded system, local integration is supported. Remote integration is not currently supported.

### + *Queries with a DS repository*

For DS repositories, relationships must be defined in the repository configuration ([repo.ds.json](#)). If you do not explicitly define relationships in the repository configuration, you will be able to query those relationships, but filtering and sorting on those queries will not work. For more information, see "Relationship Properties in a DS Repository" in the *Object Modeling Guide*.

### + *Queries with an OracleDB repository*

For OracleDB repositories, queries that use the [queryFilter](#) syntax do not work on CLOB columns in explicit tables.

### + *Queries with privileges*

When using privileges, relationships are not returned in queries. This means information that is handled as a relationship to another object (such as roles for a managed user) will not be available.

### + *Connector limitations*

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 or by editing the provisioner file. For more information, see "*Configure Connectors*" in the *Connectors Guide*.

#### + *If-Match requests*

A conditional GET request, with the **If-Match** request header, is not supported.

## Chapter 8

# Known Issues

The following important issues remained open at the time of this release. For details and information on other issues, see the [IDM issue tracker](#):

- OPENIDM-15322: Query on relationship endpoint with \*\_ref without paging takes much longer time to return with external DS as repo
- OPENIDM-15585: Admin UI doesn't display correct enable state for Audit Event Handlers
- OPENIDM-16441: Enduser UI can fail to load organizations when the managed organization schema is updated
- OPENIDM-16453: Enduser login fails if user\_id contains special characters
- OPENIDM-16465: Saved powershell connector config through admin UI is not valid
- OPENIDM-16487: The UI should allow the admin to select which linkQualifier the assignment belongs to
- OPENIDM-16516: Incoherent script hooks bindings when PATCH a relationship collection containing relationship properties
- OPENIDM-16528: Properties defined as "nullable" become required
- OPENIDM-16564: 404 Error when viewing recon events in System Monitoring Dashboard
- OPENIDM-16618: Admin UI sends encrypted data as string when an unrelated attribute is modified
- OPENIDM-16631: Cron-like Trigger for Weekly schedule shows incorrectly
- OPENIDM-16795: Inconsistent URLs when hovering on Admin UI home page OOTB widgets across IDM versions
- OPENIDM-16796: Error message: Only "replace" patch operation is supported on /kbaInfo when set to viewable
- OPENIDM-16804: Admin UI forgets mat-icon setting when object properties are re-ordered
- OPENIDM-16825: User updates needs to be submitted twice
- OPENIDM-16923: If all KBA info questions are deleted through UI, question index is corrupted
- OPENIDM-17255: The admin UI breaks the schema when editing it

- OPENIDM-17345: Changing default rest context to /svc/idm rather than /idm causes UI to misbehave
- OPENIDM-17516: Pattern policy ignored when doing operation replace with empty values
- OPENIDM-17631: Overriding the key “aliases” in conf/secrets.json using \$array and \$list coercion type to support multiple key aliases is not working
- OPENIDM-17813: File content incorrect on read

## Chapter 9

# Documentation

Date	Description
2023-12-15	Release of IDM 7.1.6.
2023-08-14	<ul style="list-style-type: none"> <li>Added a note regarding repository upgrade in the <i>Upgrade Guide</i>.</li> <li>Upgrading to DS 7.3 is now supported. Refer to Supported Repositories.</li> </ul>
2023-03-14	ICF-related guides now direct the reader to use updated documentation on Backstage instead. Use the new documentation for any future ICF updates going forward.
2023-01-06	Release of IDM 7.1.4.  Released connectors version 1.5.20.12.
2022-05-09	Released connectors version 1.5.20.6.
2022-04-30	Updated Epic connector documentation.
2022-02-28	Release of IDM 7.1.2.
2022-02-23	Released connectors version 1.5.20.5.
2021-12-10	Released connectors version 1.5.20.4.
2021-11-22	<ul style="list-style-type: none"> <li>Clarified note about the default Bouncy Castle installation.</li> <li>Updated the procedure for building custom self-service stages.</li> <li>Released connectors version 1.5.20.3.</li> </ul>
2021-07-30	Released connectors version 1.5.20.2.
2021-07-07	<ul style="list-style-type: none"> <li>Updated the list of mapping properties specific to data migration.</li> <li>Updated the supported data types in columns for explicit mappings.</li> <li>Fixed an error in the documentation on authenticating as a different user.</li> <li>Updated the instructions on adding a custom self-service stage.</li> </ul>
2021-05-11	Initial release of Identity Management 7.1 software.



# Appendix A. Release Levels and Interface Stability

## ForgeRock Product Release Levels

ForgeRock defines Major, Minor, Maintenance, and Patch product release levels. The release level is reflected in the version number. The release level tells you what sort of compatibility changes to expect.

### *Release Level Definitions*

Release Label	Version Numbers	Characteristics
Major	Version: x[.0.0] (trailing 0s are optional)	<ul style="list-style-type: none"><li>• Bring major new features, minor features, and bug fixes</li><li>• Can include changes even to Stable interfaces</li><li>• Can remove previously Deprecated functionality, and in rare cases remove Evolving functionality that has not been explicitly Deprecated</li><li>• Include changes present in previous Minor and Maintenance releases</li></ul>
Minor	Version: x.y[.0] (trailing 0s are optional)	<ul style="list-style-type: none"><li>• Bring minor features, and bug fixes</li><li>• Can include backwards-compatible changes to Stable interfaces in the same Major release, and incompatible changes to Evolving interfaces</li><li>• Can remove previously Deprecated functionality</li></ul>

Release Label	Version Numbers	Characteristics
		<ul style="list-style-type: none"><li>• Include changes present in previous Minor and Maintenance releases</li></ul>
Maintenance, Patch	Version: x.y.z[.p]  The optional <b>.p</b> reflects a Patch version.	<ul style="list-style-type: none"><li>• Bring bug fixes</li><li>• Are intended to be fully compatible with previous versions from the same Minor release</li></ul>

## ForgeRock Product Stability Labels

ForgeRock products support many features, protocols, APIs, GUIs, and command-line interfaces. Some of these are standard and very stable. Others offer new functionality that is continuing to evolve.

ForgeRock acknowledges that you invest in these features and interfaces, and therefore must know when and how ForgeRock expects them to change. For that reason, ForgeRock defines stability labels and uses these definitions in ForgeRock products.

### *ForgeRock Stability Label Definitions*

Stability Label	Definition
Stable	This documented feature or interface is expected to undergo backwards-compatible changes only for major releases. Changes may be announced at least one minor release before they take effect.
Evolving	<p>This documented feature or interface is continuing to evolve and so is expected to change, potentially in backwards-incompatible ways even in a minor release. Changes are documented at the time of product release.</p> <p>While new protocols and APIs are still in the process of standardization, they are Evolving. This applies for example to recent Internet-Draft implementations, and also to newly developed functionality.</p>
Legacy	<p>This feature or interface has been replaced with an improved version, and is no longer receiving development effort from ForgeRock.</p> <p>You should migrate to the newer version, however the existing functionality will remain.</p> <p>Legacy features or interfaces will be marked as <i>Deprecated</i> if they are scheduled to be removed from the product.</p>
Deprecated	This feature or interface is deprecated and likely to be removed in a future release. For previously stable features or interfaces, the change was likely announced in a previous release. Deprecated features or interfaces will be removed from ForgeRock products.
Removed	This feature or interface was deprecated in a previous release and has now been removed from the product.

Stability Label	Definition
Technology Preview	<p>Technology previews provide access to new features that are considered as new technology that is not yet supported. Technology preview features may be functionally incomplete and the function as implemented is subject to change without notice. <b>DO NOT DEPLOY A TECHNOLOGY PREVIEW INTO A PRODUCTION ENVIRONMENT.</b></p> <p>Customers are encouraged to test drive the technology preview features in a non-production environment and are welcome to make comments and suggestions about the features in the associated forums.</p> <p>ForgeRock does not guarantee that a technology preview feature will be present in future releases, the final complete version of the feature is liable to change between preview and the final version. Once a technology preview moves into the completed version, said feature will become part of the ForgeRock platform. Technology previews are provided on an “AS-IS” basis for evaluation purposes only and ForgeRock accepts no liability or obligations for the use thereof.</p>
Internal/Undocumented	<p>Internal and undocumented features or interfaces can change without notice. If you depend on one of these features or interfaces, contact ForgeRock support or email <a href="mailto:info@forgerock.com">info@forgerock.com</a> to discuss your needs.</p>

## Appendix B. Getting Support

ForgeRock provides support services, professional services, training 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 on ForgeRock's support offering, including support plans and service level agreements (SLAs), visit <https://www.forgerock.com/support>.

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.