Release Notes

/ ForgeRock Identity Management 7

Latest update: 7.0.1

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

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 release. Read these notes before you install or upgrade ForgeRock Identity Management software.

Quick Start

 What's New Discover new features and improvements in this version.	 Prepare for Deployment Learn about the requirements for running IDM software in production.	 Check Compatibility Review key implementation changes and compatibility with previous deployments.
 Review Fixes Review bug fixes, limitations, and open issues.	 Check Doc Updates Track important changes to the documentation.	 Get Support 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 on ForgeRock's maintenance and patch releases, see Maintenance and Patch Availability Policy.

- IDM 7.0.1 is the latest release targeted for IDM 7.0 deployments and can be downloaded from the *ForgeRock Backstage* website.

  The release can be deployed as an initial deployment or updated from an existing 7.0.0 deployment. For information on updating from 7.0.0, see "*Update to a Maintenance Release*" in the *Upgrade Guide*.

  Note

  ForgeRock strongly recommends that you update your IDM 7.0 deployment to IDM 7.0.1.

New Features

The release of ForgeRock Identity Management 7.0.0 software includes the following new features:

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

  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*.

+ *Access Configuration Over REST*

You can now configure access rules over REST, at the endpoint `openidm/config/access`. 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. For more information, see "*Protect REST Endpoints With Authorization and Access Control*" in the *Security Guide*.

+ *Configurable HTTP I/O Request Buffer*

You can now configure the temporary storage file size in the *Setup Guide* for HTTP I/O requests.

+ *Filter Expanded Relationships*

You can use `_queryFilter` to directly filter expanded relationships from a collection, such as `authzRoles`. For more information, see "Filter Expanded Relationships" in the *Object Modeling Guide*.

+ *Deterministic ECDSA signatures for JWT*

By default, JWTs are now signed with deterministic Elliptic Curve Digital Signature Algorithm (ECDSA). In order to use this more secure signing method, you must install Bouncy Castle. If Bouncy Castle is unavailable or the key is incompatible, IDM falls back to normal ECDSA.

Note

If you need to turn off the use of deterministic ECDSA, add the following line to `conf/system.properties`:

```
org.forgerock.secrets.preferDeterministicEcdsa=false
```

+ *Debugging Information for Groovy Scripts*

In previous releases, setting `javascript.exception.debug.info=true` in the `boot.properties` file enabled additional debug information including line numbers and file names for JavaScript exceptions. In this release, setting `groovy.exception.debug.info=true` enables you to gather comparable debug information for Groovy scripts.

+ *REST API Versioning*

IDM now supports the ability to specify the REST API version in HTTP calls and scripts. For more information, see "*REST API Versioning*" in the *REST API Reference*.

The following APIs have been updated in this release:

`openidm/scheduler`

Version 2 of this endpoint adds a `previousRunDate` property to the output of REST calls on specific scheduled tasks.

Version 2 also lets you trigger a scheduled task manually and pause and resume a scheduled task.

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

+ *Support for AM Bearer Tokens*

IDM now supports using AM bearer tokens for authentication, with the `rsFilter` authentication module. Going forward, this is the only supported method for integrating AM and IDM. For more information, see "rsFilter" in the *Security Guide*.

+ *Notification Property Now Configurable*

Notifications of changes to managed objects are injected into a property in that object type. Previously, the name of this property was always `_notifications`. In this IDM release, you can customize the name of the notifications property. For more information, see "Configure Notifications" in the *Audit Guide*.

+ *Reconciliation Association Information*

The new `recon/assoc` endpoint can be used to gather detailed information about the associations created between a source and a target object during a reconciliation. This endpoint requires the following tables and views to be added to your repository: `reconassoc`, `reconassocentry`, and `reconassocentryview`. For instructions on updating your existing repositories to enable this feature, see "Upgrade an Existing Repository" in the *Upgrade Guide*. For more information about recon association, see "Viewing Reconciliation Association Details" in the *Synchronization Guide*.

+ *Profile Completeness Endpoint*

A new endpoint has been added to self-service, which lets you get a percentage value of how complete a specified user's profile is. For more information, see "Viewing Profile Completeness" in the *Self-Service Reference*.

+ *Audit Logging Safelist*

By default, IDM now safelists fields that are safe to log. For more information, including the complete safelist, see "Use Policies to Filter Audit Data" in the *Audit Guide*.

+ *'IN' Clause for Queries*

The `in` expression clause provides limited support for queries on singleton string properties. For more information, see "`In` Expression Clause" in the *Object Modeling Guide*.

+ *Disposal of Idle Poolable Connector Instances (ICF)*

In version 1.5.17.1 of the ICF framework, the framework disposes of idle connector instances in the connection pool (for poolable connectors such as the LDAP connector and the Database Table connector).

A connection pool cleaner thread now runs every minute and removes connections whose `lastUsed` time is larger than the `minEvictableIdleTimeMillis`.

This behavior is an improvement on previous releases, where a connection that had been used then returned to the connection pool remained there until the next connector operation. The previous behavior could result in several idle connections in the pool, still connected to the target resource. The next time the connector was used, ICF would attempt to use the existing connection in the pool. The pool manager would check the `lastUsed` time of the connection, which would be expired, and would then close that connection before creating a new one.

+ *Separate Mapping Configuration Files*

This release lets you configure mappings in separate mapping files, instead of, or in addition to one `sync.json` file. You cannot manage separate mapping configurations through the Admin UI. For more information, see "*Mapping Data Between Resources*" in the *Synchronization Guide*.

+ *Queued Sync Retry*

This release provides the ability to configure an infinite number of queued synchronization retries. For more information, see "Configure Queued Synchronization" in the *Synchronization Guide*.

+ *Material Design Icon Added to Managed Object Configuration*

`mat-icon` has been added to the `schema` property of the managed object configuration. For more information, see "Managed Object Configuration" in the *Object Modeling 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.

+ *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/opendj/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 software is supported on the following operating systems:

- Red Hat Enterprise Linux (and CentOS Linux) 7.0 and 8.0
- Ubuntu Linux 16.04, and 18.04
- Windows Server 2012 R2, 2016, and 2019

+ *Java Requirements*

Identity Management software supports the following Java environments:

Supported Java Versions

Vendor	Versions
OpenJDK, including OpenJDK-based distributions: • AdoptOpenJDK/Eclipse Adoptium • Amazon Corretto • Azul Zulu • Red Hat OpenJDK ForgeRock tests most extensively with AdoptOpenJDK/Eclipse Adoptium.	11
Oracle Java	11

Important

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

+ *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.

Note

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 5.6.4, 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 Releases 1 (12.1) and 2 (12.2), 19c.
- PostgreSQL 9.6, 10.1, 11.6, 12.1, and 12.5.
- IBM DB2 10.1, 10.5, and 11.

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 Client Applications*

The following table summarizes supported clients and their minimum required versions:

Supported Clients

Client Platform	Native Apps [a]	Chrome 62+	Internet Explorer 11+	Edge 25+	Firefox 57+	Safari 11+	Mobile Safari
Windows 8 or later	✔	✔	✔	✔[b]	✔		
Mac OS X 10.11 or later	✔	✔			✔	✔	

Client Platform	Native Apps [a]	Chrome 62+	Internet Explorer 11+	Edge 25+	Firefox 57+	Safari 11+	Mobile Safari
Ubuntu 14.04 LTS or later	✔	✔			✔		
iOS 9 or later	✔	✔					✔
Android 6 or later	✔	✔					

[a] *Native Apps* is a placeholder to indicate the platform is not limited to browser-based technologies. An example of a native app would be something written to use our REST APIs.
[b]Windows 10 only.

+ *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

  The Kerberos connector that is bundled with IDM 7 is *not* backward-compatible with IDM 6.x. IDM 7 uses Groovy version 3.0. IDM 6.5 uses version 2.5, and IDM 6 uses version 2.4. The bundled Kerberos connector requires Groovy version 3.0.
- 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
- MongoDB Connector
- Salesforce Connector

- SCIM Connector
- Scripted REST Connector

  The scripted REST connector that is bundled with IDM 7 is *not* backward-compatible with IDM 6.x. IDM 7 uses Groovy version 3.0. IDM 6.5 uses version 2.5, and IDM 6 uses version 2.4. The bundled scripted REST connector requires Groovy version 3.0.
- Scripted SQL Connector

  The scripted SQL connector that is bundled with IDM 7 is *not* backward-compatible with IDM 6.x. IDM 7 uses Groovy version 3.0. IDM 6.5 uses version 2.5, and IDM 6 uses version 2.4. The bundled scripted SQL connector requires Groovy version 3.0.
- ServiceNow Connector
- Scripted SSH Connector

  The scripted SSH connector that is bundled with IDM 7 is *not* backward-compatible with IDM 6.x. IDM 7 uses Groovy version 3.0. IDM 6.5 uses version 2.5, and IDM 6 uses version 2.4. The bundled scripted SSH connector requires Groovy version 3.0.

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 CREST, 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 CREST, 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 CREST, 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	7.0.1, supported with DS 7.0.x and IDM 7.0.x 6.5.0, supported with DS 6.5.x and IDM 6.5.x 6.0, supported with DS 6.0.x and IDM 6.0.x 5.5.0, supported with DS 5.5.x and IDM 5.5.x 5.0, supported with DS 5.0.x and IDM 5.0.x 3.5, supported with OpenDJ 3.5 and OpenIDM 4.x DS Password Sync plugins are not supported with DS OEM

Plugin	Supported Version
Active Directory Password Synchronization Plugin	1.4.0, 1.3.0, 1.2.0 and 1.1.0 supported on Windows Server versions 2012 R2, 2016, and 2019

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 7.0.x from a version prior to IDM 7.0.0, the following changes may impact existing deployments. Adjust existing scripts, files, and clients, as necessary:

+ *New Workflow Engine*

The Activiti workflow engine has been replaced with Flowable. Current workflow definitions will continue to work with the new engine in compatibility mode, but all new workflow definitions must be written for Flowable. For more information, see "Workflow Definition Comparison" in the *Workflow Guide*.

If you are using MySQL for the workflow database, the following apply:

- You must use MySQL version 5.6.4 or later. If you are using an older version, perform the MySQL upgrade before upgrading to IDM 7 or later. For additional information, see the *Flowable Note for MySQL users*.
- Flowable automatically upgrades the database schema, and can encounter non-recoverable errors related to date settings. Before you start IDM 7 or later for the first time, remove the `SQL_MODE` settings `NO_ZERO_IN_DATE` and `NO_ZERO_DATE`. Example SQL command:

```
mysql -uroot -ppassword

set GLOBAL SQL_MODE='';

use openidm;
set SQL_MODE='';
```

After you complete the upgrade process, you can restart MySQL, and your original settings should be restored.

+ *Changes to boot.properties*

Prometheus Monitoring

Monitoring using Prometheus is no longer achieved with a specific access role. The `openidm/metrics/prometheus` endpoint is now protected by a basic authentication filter, using credentials set in the `resolver/boot.properties` file. For more information, see "Monitoring With the Prometheus Endpoint" in the *Monitoring Guide*.

Debugging Information for Groovy Scripts

In previous releases, setting `javascript.exception.debug.info=true` in `resolver/boot.properties` enabled additional debug information, including line numbers and file names for JavaScript exceptions. In this release, setting `groovy.exception.debug.info=true` lets you gather comparable debug information for Groovy scripts.

Added Properties

These properties have been added to `resolver/boot.properties`:

- `openidm.servlet.upload.alias=/upload`, `openidm.servlet.export.alias=/export`: Sets the REST endpoints for the bulk import feature.
- `openidm.admin.password=openidm-admin`: Lets you change the password of the administrative user before startup.

Removed Properties

These properties have been removed from `resolver/boot.properties`:

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

+ *Changes to logging.properties*

The default log message formatter has changed from `ThreadIdLogFormatter` to `SanitizedThreadIdLogFormatter`. The new default encodes control characters (such as newline characters) using URL-encoding, to protect against log forgery. Control characters in stack traces are not encoded. For more information, see Set the Log Message Format in the *Monitoring Guide*.

+ *Change to How Authorization Roles are Assigned*

In previous IDM releases, managed users were granted the `openidm-authorized` role as a relationship during user creation, as part of the `onCreateUser.js` script. In IDM 7, users are granted the `openidm-authorized` role statically, when they authenticate. For more information, see "Authentication and Roles" in the *Security Guide*.

Note

This way of granting internal authentication roles is considered a best practice and is recommended for performance reasons. However, if your deployment relies on the old way of granting the `openidm-authorized`

role, that configuration is still supported, and you can use your existing `onCreateUser.js` script to grant the role on creation.

+ *Schema Change to authzRoles*

The default relationship model for `authzRoles` and `authzMembers` has changed in this release. In the default configuration, a user's `authzRoles` now references only the `internal/role` resource collection, and not the `managed/role`. Conversely, an internal role's `authzMembers` property now references only the `managed/user` resource collection.

The default schema configuration files have been amended to support this change. The `managed/role` collection has been removed from the `authzRoles` property on a managed user object, and the `internal/user` collection has been removed from the `authzMembers` property on an internal role object.

Multiple resource collections for a single relationship field are not currently supported with a DS repository. Multiple resource collections will still work with a JDBC repository, for legacy reasons.

+ *Change to the INTERNAL_USER Authentication Module*

The `INTERNAL_USER` authentication module is no longer provided in the default authentication configuration.

This change means that any scripts you used previously to update internal user passwords in the IDM repository will need to be modified.

+ *Change to Prometheus Monitoring*

Monitoring using Prometheus is no longer achieved with a specific access role. The `openidm/metrics/prometheus` endpoint is now protected by a basic authentication filter, using credentials set in the `resolver/boot.properties` file. For more information, see "Monitoring With the Prometheus Endpoint" in the *Monitoring Guide*.

+ *Change in how Boolean Values are Assessed*

Properties stored in the repository with boolean (`true/false`) values are processed differently from this release. A property value is now considered `false` if its value is `false` or `null`. The value is considered `true` only if it is `true`, not if it is `null`. If you are migrating from a previous IDM release, you might need to adjust your scripts to take this change into account.

+ *Queued Sync Changes*

Processing order of queued synchronization mappings

In previous IDM releases, mappings for which queued synchronization was enabled were processed first. The synchronization engine would then process the non-queued mappings in order. In IDM 7, all mappings are processed in the order in which they are listed, regardless of whether queued synchronization is enabled.

If you want to retain the pre-7.0 behavior, place your queued synchronization mappings first in your list of mappings.

Removal of `remainingRetries` from queued synchronization

This release lets you configure an infinite number of queued synchronization retries. As part of this change, the `remainingRetries` property has been removed from the queued synchronization object.

For more information about the queued synchronization configuration, see "Configure Queued Synchronization" in the *Synchronization Guide*.

+ *Virtual Property calculation for effectiveRoles and effectiveAssignments*

`effectiveRoles` and `effectiveAssignments` are now calculated in IDM by default, using the new `queryConfig` property. The old method of using `onRetrieve` scripts will still work. The new `queryConfig` property is also available for use with other virtual properties. For more information about effective roles and assignments, see "Effective Roles and Effective Assignments" in the *Object Modeling Guide*. For more information about `queryConfig` and virtual properties, see "Virtual Properties" in the *Object Modeling Guide*.

+ *Gzip Compression for HTTP Responses*

You can now configure Gzip compression for HTTP responses in `conf/jetty.xml`. In previous IDM releases, compression was configured in `conf/servletfilter-gzip.json`. This file has been removed.

+ *Configurable Hashing*

IDM 7 supports configurable hashing algorithms.

+ *Temporal Constraint Enforcement on Roles*

Enforcing temporal constraints on roles is now achieved through Java, rather than through the `onSync-roles.js` and `postOperation-roles.js` scripts. These scripts are still provided in `openidm/bin/defaults/script/roles` for backward-compatibility.

To use the new Java-based functionality in existing deployments, change the `role` object in your managed object schema (`conf/managed.json`), by adding `"isTemporalConstraint" : true` to the `"temporalConstraints"` object. For example:

```
"temporalConstraints" : {
    "description" : "An array of temporal constraints for a role",
    "title" : "Temporal Constraints",
    "viewable" : false,
    "returnByDefault" : true,
    "isTemporalConstraint" : true,
    "type" : "array",
    ...
}
```

For information about setting temporal constraints on roles, see "Use Temporal Constraints to Restrict Effective Roles" in the *Object Modeling Guide*.

+ *Change to JMS Audit Handler*

The `batch` configuration for the JMS common audit handler for access logs has changed to support reconnection if the broker becomes unavailable.

This change adds a `batch.writeInterval` setting. It removes the following settings:

- `batch.batchEnabled`
- `batch.insertTimeoutSec`
- `batch.pollTimeoutSec`
- `batch.shutdownTimeoutSec`
- `batch.threadCount`

For details on the JMS handler configuration, see "Configure the JMS Audit Event Handler" in the *Audit Guide*.

+ *Change to Default Audit Configuration*

The default configuration for audit has been changed to no longer have the `recon` audit topic included by default. It can be enabled by adding the `recon` audit topic to the `topics` list in `conf/audit.json`, for the event handlers you choose.

This change does not affect how auditing reconciliations works, just what the default configuration includes. No action is necessary unless you wish to have auditing on reconciliations enabled on a new installation. For more information, see Query the Reconciliation Audit Log in the *Audit Guide*.

+ *Datatype of userPassword Property in Provisioner Files*

As a security precaution, the `nativeType` for `userPassword` properties has been changed to `JAVA_TYPE_GUARDEDSTRING` in all sample provisioner files for the LDAP Connector. If you have customized provisioner files, you should change this property. For example, change:

```
"userPassword" : {
    "type" : "string",
    "nativeName" : "userPassword",
    "nativeType" : "string",
    ...
```

to

```
"userPassword" : {
    "type" : "string",
    "nativeName" : "__PASSWORD__",
    "nativeType" : "JAVA_TYPE_GUARDEDSTRING",
    ...
```

+ *Removal of the Global Consent Setting*

Previous IDM versions included a global consent setting, in `conf/consent.json`. This file included a single configuration property, `enabled`, which determined whether IDM should check any mappings for which consent was enabled and prompt end users for consent.

This global consent setting, and the corresponding `consent.json` file, have been removed. If you have an existing `consent.json` file in your configuration, it will simply be ignored.

Consent is now assessed only on a per-mapping, per-object basis. For more information, see "Configure Privacy and Consent" in the *Self-Service Reference*.

+ *Support for MySQL Connector/J version 8.0*

IDM 7 adds support for the latest version of MySQL Connector/J has been added. If you are using version 8.0 or later, make sure your `datasource.jdbc-default.json` file includes a setting for the time zone in your `jdbcUrl` property:

```
"jdbcUrl" : "jdbc:mysql://&{openidm.repo.host}:&{openidm.repo.port}/openidm?
allowMultiQueries=true&characterEncoding=utf8&serverTimezone=UTC",
```

Also, note the `driverClass` changed in version 8.0, from `com.mysql.jdbc.Driver` to `com.mysql.cj.jdbc.Driver`. The previous `driverClass` name will still work for now, but should be updated to avoid it displaying a warning when starting up IDM.

+ *Default Security Protocols for Inbound Connections*

The default security protocols for inbound connections to IDM are `TLSv1.2` and `TLSv1.3`. For information on enabling additional protocols, see "Enable and Disable Secure Protocols and Cipher Suites" in the *Installation Guide*.

Support for the `TLSv1.1` protocol has been removed by default.

+ *Removal of 'address2' from the managed object schema*

The `address2` attribute has been removed from the managed object schema (`conf/managed.json`).

+ *ICF and Connector Changes*

The following ICF and connector changes will have an impact on existing IDM deployments that use those connectors:

Workday connector

The Workday connector is no longer bundled with IDM. Download the connector and its dependencies from the ForgeRock BackStage download site.

Database Table connector

The configuration requirements for the Database Table connector have changed:

- The `jdbcDriver` and `jdbcUrlTemplate` properties have been removed. Use `driverClassName` and `url` instead.
- The `database` property has been removed. The database should now be specified in the JDBC address in `url`.
- Additional (optional) configuration properties are now available. For a full list, see "Database Table Connector" in the *Connectors Guide*.

Additionally, the Database Table connector example configurations have changed:

`samples/example-configurations/provisioners/provisioner.openicf-contractordb.json`

- Removed `required : true` from the `_NAME_` property.
- Added `required : true` to the `EMAIL` property.
- Removed `"keyColumn" : "UNIQUE_ID"`.

`samples/example-configurations/provisioners/provisioner.openicf-contractordb.sql`

Set `EMAIL` as the `PRIMARY KEY`.

Chapter 4

Deprecation

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

+ *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 "*Protect REST Endpoints With Authorization and Access Control*" in the *Security 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 has been removed for interactions with social identity providers, as discussed in "*Discontinued*".

Default versions of relevant configuration files no longer include `oauthReturn` in the `redirectUri` setting. However, for IDM 7, 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
    }
}
```

Chapter 5
Discontinued

Support for the following functionality has been removed in IDM 7.0.0:

+ *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.iplanet.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 "*Managing 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 7.0.1

IDM 7.0.1 introduces important security fixes for current IDM 7.0.0 deployments.

IDM 7.0.0

The following important bugs were fixed in the IDM 7.0.0 release. For details and information on other issues, see the IDM issue tracker:

- OPENIDM-14771: Managed user property that is userEditable and nullable isn't visible on Enduser UI.
- OPENIDM-14379: non-unique id: W3C uncompliant coding in Admin UI for multiple linked system
- OPENIDM-15150: IE11 script error in End-User UI
- OPENIDM-12131: UI javascript errors when a property does not have a nativeType attribute in a provisioner config file
- OPENIDM-14082: Admin UI Single Record Reconciliation Find Source Record could result in 400 error
- OPENIDM-14114: Syslog audit event handler host and port are not automatically populated when editing an existing syslog audit event handler in the admin ui
- OPENIDM-14046: Duplicates of the same workflow process show within the end user UI
- OPENIDM-14907: Admin UI displays "ERROR WITH SCRIPT" for any property mapping with transform script
- OPENIDM-13064: End User admin link broken when Self-Service relative URL is not "/"
- OPENIDM-12796: jsonstorage "local" self-service with "uuid" option fails in multi-node cluster scenario
- OPENIDM-14851: Duplicate links may be created with external DS repository
- OPENIDM-12105: Delegated Admin UI Should Only Display Supported Fields in grid

- OPENIDM-12170: Delete on managed or internal object does not return the included relationship fields that were included in the request
- OPENIDM-12109: Able to add managed object property with illegal character via Admin UI
- OPENIDM-14326: IDM unnecessarily writes to keystore and trustore
- OPENIDM-13129: PATCH remove a field could result in 500 error: Can not add or remove a 'null' value
- OPENIDM-13870: Queued sync breaks implicit synchronization
- OPENIDM-14421: queryFilter boolean handling is inconsistent between JDBC and DS repositories
- OPENIDM-13096: ConcurrentModificationException when invoking test action on system endpoint
- OPENIDM-13971: Assigning tasks in enduser UI does not work
- OPENIDM-13457: UI broken for social auth registration
- OPENIDM-12698: Custom GitHub end-user UI not working with proxy
- OPENIDM-13772: End User UI Delegated Administrator search doesn't encode '+' sign properly
- OPENIDM-13119: UI does not correctly display validation for Password History
- OPENIDM-12318: Unable to create new contacts because reCaptcha load failure
- OPENIDM-12613: Missing Admin in the user profile drop down menu for managed object user
- OPENIDM-13229: 'Sign in' in the registration interface has a broken link due to trailing "/"
- OPENIDM-13075: Security questions set upon registration are not displayed properly in End User UI profile page
- OPENIDM-14538: Exception 412 thrown when multiple updates occur on a single managed/user
- OPENIDM-14554: Missing _NAME_ attribute in a provisioner objectTypes properties throws NPE on create
- OPENIDM-14324: We need to be able to run Jetty.xml from a Project directory
- OPENIDM-14519: Generic object properties within map not searchable
- OPENIDM-14253: Admin UI: Tab key to move to next textbox does nothing after selecting Japanese input
- OPENIDM-14424: ScriptedREST sample: Update on system endpoint proceeds though Search has no results
- OPENIDM-11050: Mutual SSL authentication failure with external REST

- OPENIDM-15000: Rhino: Handlebars.js is not multithreaded
- OPENIDM-14237: Admin UI: Japanese input not saved when creating new managed object
- OPENIDM-14184: Self-Service password reset gives no warning/explanation for passwords failing CANNOT_CONTAIN_OTHERS policy
- OPENIDM-14528: Relationship signal propagation not working for patch operations against singleton relationships
- OPENIDM-14900: Virtual properties are calculated incorrectly in ManagedObjectSet#handleSignalVertexUpdateFromEdge
- OPENIDM-14349: Relationship properties not in source object when returnByDefault is true
- OPENIDM-12964: 'Try resetting your password again' link is not working after entering KBA incorrectly.
- OPENIDM-13265: reconById fails with sourceQueryFullEntry true on an external source
- OPENIDM-12695: Slow response time when querying a large dataset
- OPENIDM-12692: DelegatedAdminFilter does not dissallow relationship attributes
- OPENIDM-13375: REST2LDAP: Null source on query-all-ids
- OPENIDM-12513: Two different connector parameters mixed when clicking both in succession in UI
- OPENIDM-12775: Clustered recon fails if external resource page cookie is non-unique
- OPENIDM-12550: Workflow forms do not load in Internet Explorer 11
- OPENIDM-13764: Type Boolean property viewable when creating a new user
- OPENIDM-13465: Error message on Firefox when validating pattern or min length
- OPENIDM-12335: Queued sync tasks stuck in PENDING using DS repo, search results cannot be sorted
- OPENIDM-13314: CLIENT_CERT doesn't concat authzRoles to defaultUserRoles
- OPENIDM-11838: Foreign language passwords don't work if they are hashed in IDM.
- OPENIDM-12669: Admin UI Registration Page overwrites customizations in selfservice-registration.json made outside the UI
- OPENIDM-14314: Performance degradation when using query _fields param and returnByDefault is enabled
- OPENIDM-14489: PKCS12 keystore in IDM

- OPENIDM-12379: /openidm/recon endpoint fails on an upgraded repository
- OPENIDM-12259: New assignment is not reflected in onSync script hook when a new role with its members and assignments is created in one REST call
- OPENIDM-13241: Sample password history policy results in 500 error when used with SelfService registration/reset
- OPENIDM-13261: Fix exception in PendingLinkAction.getPendingActionContext
- OPENIDM-12190: Router authz fails in multiple-passwords sample
- OPENIDM-13763: Admin UI: Japanese input not working for managed user and role
- OPENIDM-12309: "require" javascript changes are not picked up by IDM 6.5
- OPENIDM-12359: Changing "Identity Email Field" in "User Query Form" from "mail" to another managed object property throws an error
- OPENIDM-12897: Large integers not handled correctly in JavaScript
- OPENIDM-12517: Adding the triggerSyncProperties in sync.json stops pushing a newly created managed object implicitly to the end resource
- OPENIDM-13882: Admin UI sends multiple REST requests with opposite values in the payload when disabling a connector
- OPENIDM-12804: uuid token expiry doesn't work with jdbc repo
- OPENIDM-12498: UI: Schedule Task Scanner with empty Object Property Field gets unexpected value added
- OPENIDM-12755: Editing of task in admin console throws validatorErrors in handlebars-4.0.5.js
- OPENIDM-12904: Sending mail with null "to" field causes IDM to hang
- OPENIDM-12865: jwt token fails in multi-node cluster scenario
- OPENIDM-12254: IDM UI doesn't render linked view for SAP R3
- OPENIDM-12941: Samples: scripted-sql-with-mysql has a syntax error in provisioner
- OPENIDM-13721: NULL not set correctly when adding users. It is set to string of 'null'
- OPENIDM-13740: Explicit repo table: validate mapping before CREATE
- OPENIDM-12969: Assignment of workflow to candidate user/group fails
- OPENIDM-12680: Reconciliation stuck in ACTIVE_QUERY_ENTRIES (or other ACTIVE_ state) and cannot be cancelled

- OPENIDM-12376: Error retrieving scheduler jobs and firing triggers after upgrading to 6.5
- OPENIDM-14398: end-user ui delegated admin loading could degrade with increasing number of entries in managed objects
- OPENIDM-12206: Invalid filter in Privilege can be created and cannot be fix in UI
- OPENIDM-12192: Modifying virtual property corrupts managed.json
- OPENIDM-14290: Internal Server Error reported when entering double quotes into username field
- OPENIDM-12786: Improve consent service to remove duplicate fields, include fields sourced through transform script
- OPENIDM-14417: "ActivitiContext class cannot be found" error during queued sync
- OPENIDM-13993: Access to the old password in a mapping condition should require decrypt()
- OPENIDM-14535: IDM does not support IBM's PKCS11 provider
- OPENIDM-12591: authzMembers can have duplicate entries when added using openidm.create() in scripts
- OPENIDM-12814: Setting returnByDefault for a relationship property to true could cause reconciliation exception with DJ repo explicit mapping managed user
- OPENIDM-14287: cli.sh keytool export and import causes IDM startup failure with 'Invalid AES key length' error
- OPENIDM-14099: Queued sync doesn't work for mappings with names longer than 38 characters in JDBC repo
- OPENIDM-13821: Queued sync event getting stuck in state PENDING
- OPENIDM-13213: Editing the members property of the managed role object schema breaks conditional provisioning role members
- OPENIDM-12827: Setting returnByDefault to true on relationship properties in managed objects DJ repo could cause missing attributes in sync.json script hooks
- OPENIDM-14039: Exception caught marshalling a SynchronizationEvent due to missing serialization in SelfServiceContext
- OPENIDM-14066: Recon status report showed extra recon was done
- OPENIDM-14837: When a user has a large number of assignments, every additional assignment added takes an increasing length of time to process
- OPENIDM-13589: Memory visibility issues dictating persisted sync-token state in the context of live-sync failures

- OPENIDM-14654: Database creation on Azure Database for PostgreSQL fails with - ERROR: must be member of role "openidm"
- OPENIDM-10660: User metadata is logged in the audit log when an object is changed
- OPENIDM-11879: Workflow time zone handling is not consistent and leads to unexpected results
- OPENIDM-14205: Exception caught marshalling a SynchronizationEvent for requests made with CLIENT_CERT authentication
- OPENIDM-13983: Unable to delete attribute when it has "scope": "private"
- OPENIDM-14322: Unable to delete private properties via openidm.update()
- OPENIDM-12312: UNIQUE policy on properties other than userName not validated during self-registration
- OPENIDM-14505: ManagedObjectSet handling of patch removal of singleton relationship field will prevent successful calculation of virtual properties based on this field
- OPENIDM-11921: Errors logged when password-reset email URL is expired and clicked
- OPENIDM-14501: Reset selfservice stage is checking mail attribute and not identityEmailField
- OPENIDM-12778: Schedules to execute a file-based script are generated incorrectly via the Admin UI
- OPENIDM-13787: Workflow filtered-query on task instance with param taskId does not work
- OPENIDM-12681: Admin GUI: Role condition with attribute type boolean are treated as string
- OPENIDM-14400: Deletion of roles ignores the userId
- OPENIDM-12372: A managed object is not capable of handling simultaneous requests from an edge
- OPENIDM-12304: IDM doesn't add suffix to CAUD transactionId propagated to external DS user store
- OPENIDM-12332: Unable to register using a managed object other then managed/user
- OPENIDM-12408: Object properties when set to propertiesToCheck in notification configuration don't work
- OPENIDM-12330: Notification create date no longer stored by default
- OPENIDM-12367: Queued sync event processing ignores discard result, possibly discards twice
- OPENIDM-12465: Managed Object UI forms do not persist all changed fields
- OPENIDM-12319: Audit Event Handler Port only displays first number in UI

- OPENIDM-12186: Sample AD LDS Provisioner schema should not include SAMAccountName and is missing uid
- OPENIDM-12188: Repo init service fails in multiple-password sample
- OPENIDM-12208: Clustered reconciliation fails due to paging cookie from ldap AD
- OPENIDM-13633: Enabling password history causes error for existing users when they log into the enduser UI and edit their profile
- OPENIDM-12017: IDM CAUD syslog product name (APP-NAME) is null
- OPENIDM-14060: Bug in the at-least-X-capitals policy regex
- OPENIDM-14548: External REST: Calling endpoints which return a JSON array throws error
- OPENIDM-13854: REST - Deleting user with a non existent relationship object returns 404
- OPENIDM-13023: Include an out of the box Oracle specific bnd file in db/oracle/scripts
- OPENIDM-13130: Viewing roles on a user with empty temporalConstraint array fails
- OPENIDM-12833: Removing the preferences property causes admin UI mapping/association to stop responding properly
- OPENIDM-13411: identityServer.getProperty() returns null pointer if property isn't set rather than being handled gracefully
- OPENIDM-13160: PATCH may succeed although If-Match does not match _rev
- OPENIDM-13497: /openidm/health/recon data inaccurate
- OPENIDM-12632: queryFilter on recon audit fails using MSSQL as repo
- OPENIDM-12383: API descriptor not available after setting relationship-type property to nullable
- OPENIDM-12200: Uncaught TypeError in JavaScript console when saving reverse relationship
- OPENIDM-12080: External Email connects to SMTP servers with TLSv1
- OPENIDM-14520: Admin UI: IDM Recon result failure summary "View Entries" does not display entries
- OPENIDM-14462: Trailing spaces stripped from input after " in Admin UI
- OPENIDM-12334: UI: IDM Recon result failure summary doesn't respond to click on "View Entries"
- OPENIDM-12709: Workflow Processes Completed have "Not Found Error" for managed/user
- OPENIDM-14193: deletePersistedTargetIds could result in SQL exception: valid column name 'reconId'

- OPENIDM-13966: Modifying the Display Properties of a relationship within the admin UI causes the notify attribute to be lost
- OPENIDM-13940: Query workflow via REST with non-string parameter
- OPENIDM-14432: Restarting IDM cluster generates error message on first node: Scheduled service "scheduler-service-group.liveSync" invocation reported failure:
- OPENIDM-12691: Scheduler performance in IDM 6.x
- OPENIDM-7198: Apostrophe (and likely other special HTML characters) do not render properly in the UI in some spots
- OPENIDM-12877: Exception caught signalling deletion of edge when removing a relationship
- OPENIDM-12354: Admin UI "Change Source to Target Association" button doesn't respond to click
- OPENIDM-12425: Uncaught TypeError in Javascript console when editing managed role in admin UI

Chapter 7
Limitations

ForgeRock Identity Management 7.0.0 has the following known limitations:

+ *Workflow limitations*

  - Workflows are not supported with a DS repository. You must install a JDBC repository to use workflows.
  - For native email workflow tasks in the *Workflow Guide*, the mail server must be configured to use the secure port `465`. Why?
  - 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*

- The scripted REST, scripted SQL, and SSH connectors that are bundled with IDM 7 are *not* backward-compatible with IDM 6.x. IDM 7 uses Groovy version 3, while IDM 6.x uses Groovy version 2.5.7. The bundled scripted Groovy connectors requires Groovy version 3.
- 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 the IDM 7.0.0 release. For details and information on other issues, see the IDM issue tracker:

- OPENIDM-14828: updateLastSync sets returnByDefault relationship to empty array
- OPENIDM-15220: Temporal constraints on internal role grants with privileges are not reflected in the end-user UI
- OPENIDM-11765: Warnings on startup with Java 11
- OPENIDM-12177: Notifications service does not work with relationship fields
- OPENIDM-14666: SCIM connector cannot be configured through the UI
- OPENIDM-12187: Creating a new Marketo connector in UI fails
- OPENIDM-14645: Saving privacy & encryption or script tab on relationship edit screen doesn't save
- OPENIDM-15119: Admin UI should not enforce uniqueness on array properties
- OPENIDM-14494: Admin UI: Email Settings handling of property substitution
- OPENIDM-15086: Using POST "_action=patch&_queryId=for-userName" succeeds despite read-only flag
- OPENIDM-15145: UI: Audit Filter Policies only save to "excludeIf"
- OPENIDM-9692: Usernames for workflow are case sensitive
- OPENIDM-12805: Allow target-vertex field filtering on edge-vertex relationship query with embedded DJ
- OPENIDM-14832: triggerSyncProperties does not work when using an encrypted password
- OPENIDM-15019: End-user UI displays user name without accents (umlaut etc)
- OPENIDM-14601: "View Resource" button in linked systems links to invalid URL

Chapter 9
Documentation

Date	Description
TBD	• Updated DS configuration in "*Synchronize Passwords With ForgeRock Directory Services (DS)*" in the *Password Synchronization Plugin Guide*. • Added notes about MySQL to the samples "*Direct Audit Information To MySQL*" in the *Samples Guide* and "*Connect to a MySQL Database With ScriptedSQL*" in the *Samples Guide*. • Updated the default `datasource.jdbc-default.json` file configuration for workflow in the *Workflow Guide*. • Updated the description of the INTERNAL_USER authentication module in the *Security Guide* to indicate that this is no longer enabled by default.
2021-03-11	• Release notes for ICF updated to include version 1.5.19.6. • Documentation for using Apple as a social identity provider in the *Self-Service Reference* added. • `integer` is a supported managed object type. • Updated Oracle DB repository in the *Installation Guide* instructions to reference an updated version of the `bnd` utility. • Updated the list of supported OS and repository versions. • Added a note about some configurations not using property substitution in the *Setup Guide*. • Updated the install procedure when using a PostgreSQL Repository in the *Installation Guide*. • Added details on value substitution order of precedence in the *Setup Guide*. • Added a restriction warning on the production use of the embedded workflow H2 database in the *Workflow Guide*. • Corrected the documentation on avoiding URL-hijacking in the *Security Guide*.
2021-02-04	Corrected the documentation on the impact of Daylight Savings Time on schedules in the *Schedules Guide*.
2021-02-03	Added instructions on configuring two external DS repositories in an active/passive deployment in the *Installation Guide*.

Date	Description

2021-01-20	• The new "MS Graph API Java Connector" in the *Connectors Guide* is supported with IDM 7.0.1.
	• The latest version of the Active Directory Password Synchronization Plugin (1.4.0) 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*.
	  • The use of AM bearer tokens as an authentication method. For more information, see "Installing the Active Directory Password Synchronization Plugin" in the *Password Synchronization Plugin Guide*.
	• Added documentation for the new feature Material Design Icon Added to Managed Object Configuration.

2020-12-10	• The latest DS password synchronization plugin (version 7.0.1) supports 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*. • Added a warning not to edit downloaded CSV files in the *Object Modeling Guide* with Microsoft Excel. • Removed the restriction on support for the SSH connector in the *Connectors Guide*. This connector is fully supported.
2020-11-04	• Added a supported upgrades matrix in the *Upgrade Guide* with information on upgrading from earlier IDM versions. • Updated the procedure for using Microsoft SQL as the IDM repository. in the *Installation Guide*. • Revised procedure for creating admin users in the *Security Guide*. • Additional email configuration properties for workflow.json in the *Workflow Guide*. • Fixed a documentation bug related to the storage location of metadata in the *Object Modeling Guide*. • Added information about validating properties of unknown resources in the *Object Modeling Guide*.
2020-10-16	• Updated the path to the custom self-service stage sample project in the *Self-Service Reference*. • Fixed the procedure on changing the default REST context in the *Setup Guide*. • Fixed the procedure on "Using CA-Signed Certificates" in the *Security Guide*. • Added examples for `$list` and `$array` to the explanation of property type coercion in the *Setup Guide*.

Date	Description
2020-10-07	• Updated the instructions on Installing IDM With an External DS Repository in the *Installation Guide* to indicate that the `am-identity-store` profile is required for explicit mappings. • Clarified that scripted connectors cannot be configured through the UI in the *Connectors Guide*.
2020-09-15	• Updated the list of remote connector server configuration properties in the *Connectors Guide*. • Noted the limitation on backward compatibility with the scripted Groovy connectors. • Added note regarding user DELETE requests for Salesforce connector in the *Connectors Guide*. • Removed extraneous install requirements in the *Getting Started*.
2020-09-10	• Added instructions for updating to a maintenance release in the *Upgrade Guide*. • Fixed typo in curl command for uploading bulk CSV entries into the repository in the *Object Modeling Guide*.
2020-09-08	• Release of Identity Management 7.0.1. • Fixed Javadoc search box. • Added a note about log forgery protection to the Security Guide in the *Security Guide*.
2020-08-10	Initial release of Identity Management 7 software. In addition to the changes described elsewhere in these notes, the following important changes were made to the documentation: **Reorganized Documentation** The *Integrator's Guide* of previous versions has been removed and replaced with a number of smaller, more focused guides.

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)	• Bring major new features, minor features, and bug fixes • Can include changes even to Stable interfaces • Can remove previously Deprecated functionality, and in rare cases remove Evolving functionality that has not been explicitly Deprecated • Include changes present in previous Minor and Maintenance releases
Minor	Version: x.y[.0] (trailing 0s are optional)	• Bring minor features, and bug fixes • Can include backwards-compatible changes to Stable interfaces in the same Major release, and incompatible changes to Evolving interfaces • Can remove previously Deprecated functionality

Release Label	Version Numbers	Characteristics
		• Include changes present in previous Minor and Maintenance releases
Maintenance, Patch	Version: x.y.z[.p] The optional `.p` reflects a Patch version.	• Bring bug fixes • Are intended to be fully compatible with previous versions from the same Minor release

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	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. 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.
Legacy	This feature or interface has been replaced with an improved version, and is no longer receiving development effort from ForgeRock. You should migrate to the newer version, however the existing functionality will remain. Legacy features or interfaces will be marked as *Deprecated* if they are scheduled to be removed from the product.
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	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. DO NOT DEPLOY A TECHNOLOGY PREVIEW INTO A PRODUCTION ENVIRONMENT. 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. 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.
Internal/Undocumented	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 info@forgerock.com to discuss your needs.

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.