Release notes

These release notes are intended to provide information to administrators and evaluators of the ForgeRock Identity Governance. All information is accurate at the time of publication and updates will be provided by ForgeRock with subsequent software releases.

ForgeRock supports and maintains versions according to the ForgeRock Product Support Lifecycle Policy | AM, DS, IDM, and IGA.

What's new?

Learn about what's new in this version of IGA.

Before you start

Learn about the requirements for running Identity Governance software in production.

Fixes, limitations, and known issues

Learn about the fixes, limitations, and known issues in this release.

Compatibility

Learn about major and minor changes to

Check doc updates

Track important changes to the documentation.

existing, deprecated, and removed functionality.

Get support

Find out where to get professional support and training.

What's new

IGA 7.1.1

IGA 7.1.1 introduces the following new features and functionality:

- **Reassign tasks in access review**: In previous versions of IGA, only administrator users were able to reassign campaign events from one certifier to another. In patch release 7.1.1, end users can run reassignments on their own if the system settings are configured to allow them.

  Configure as an administrator to view this access as a certifier.
- **Enhanced certification filtering**: Users can now filter on multiple columns at once in their access review line-items.

IGA 7.1

IGA 7.1 introduces the following new features and functionality:

- **Unified user interface**: Both Identity Governance and Access Request components now exist within the same UI context at `/governance`.
- **Custom request form fields**: Administrators can define custom request fields using multiple input types and assign them to requestable objects to dynamically create custom request forms.
- **Custom request workflow support**: In addition to the standard request process, administrators can assign custom BPMN workflows or Javascript scripts to requestable objects to control the request process for individual items.

- **Requests for removal of access**: End users can now create requests for the removal of a given requestable item.
- **Expanded requestable item options**: In addition to IDM managed objects, administrators can now set generic IDM attributes as well as disconnected system entitlements to be requestable by users.
- **Add consults to tasks**: Approvers can reach out to another user or group to ask them for additional insight or information to help make their approval decision.
- **Manual provisioning tasks**: For any requestable item that requires manual provisioning steps, such as disconnected system entitlements, a manual provisioner can be assigned as a final step of the process to complete provisioning of any item.
- **File attachments**: End users have the ability to attach file uploads to an existing request, either as a requirement to create the request or as supplemental information from the requester, requestee, approver, or consult.
- **End user task reassignment**: When enabled, approvers can reassign a given approval task to another end user or group of their choosing. Additionally, approval tasks now follow the same delegation pattern introduced in Identity Governance 3.0 when configured by administrators.
- **Pre-request and provisioning script hooks**: Administrators can define automated scripts to run any pre-processing logic on a request for access, as well as to automate any additional logic or steps to the provisioning process.
- **Policy validations against requests**: When enabled, an access request that violates an existing policy cannot be submitted even if approved. End users are informed of the policy violation that would occur if given access, as well as a description of the policy. This allows the end user to adjust their request.
- **Autonomous Identity integration**: Administrators can configure system settings to allow Identity Governance to work in conjunction with ForgeRock Autonomous Identity to provide additional insights to certifiers and approvers within certifications and requests. Items that have recommendations available from AutoID will be marked with a recommendation to approve/certify or reject/revoke, as well as a confidence score for that suggestion.
- **Scripted certification and policy remediation**: Administrators now have the option to use a scripted remediation process, in addition to using the IDM BPMN workflow functionality, to remediate revoked access or policy violations.

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.

Before you start

Identity Governance server software requires the following hardware and software requirements to run in your production environment.

ForgeRock Identity Management

ForgeRock Identity Governance is designed to work with Identity Management. Identity Governance requires the following Docker image for installation.

Table 1: Identity Management Requirements

ForgeRock® Identity Management	7.0, 7.1, 7.2, 7.3

Operating systems

Identity Governance is supported on the following operating system:

Table 2: Operating System Requirements

Vendor	Versions
Red Hat Enterprise Linux/CentOS	6.6, 6.7, 7.0, and 8.0
Ubuntu Linux	16.04, 18.04
Windows Server	2012 R2, 2016, 2019

Java requirements

Identity Governance software supports the following Java environments:

Table 3: Java Requirements

Vendor	Versions

Vendor	Versions
OpenJDK, including OpenJDK-based distributions: * AdoptOpenJDK/Eclipse Adoptium • Amazon Corretto • Azul Zulu • Red Hat OpenJDK	8, 11
Oracle Java	8, 11 (specifically at least the Java Standard Edition runtime environment)

System requirements

ForgeRock Identity Governance requires at least 100MB disk space and 4GB memory for non-production implementations. Production sizing depends on user population, audit requirements and expected request volume.

Fixes, limitations, and known issues

This section covers key issues in Identity Governance software, both past, and present.

New fixes in 7.1.1

- IGA-276 - Group (role) drop-down list not functioning if AM OAuth is used
- IGA-501 - False error message 'Access Denied' is shown on logon with Access Review
- IGA-518 - Reviewer unable to sign-off on the access review task
- IGA-882 - Clicking the Submit button twice in 'Approve Access-Request' causes failure
- IGA-887 - Removal approvers list incorrectly referenced when defined without approvers
- IGA-888 - AR Admin check will reference both role types if configured that way
- IGA-891 - User with only AR Admin role blocked from certain access
- IGA-1221 - Notifications not sending on certain second stage certification tasks
- IGA-1223 - Scheduled object cert failing validation
- IGA-1306 - Internal role filters returning only 1 entry
- IGA-1349 - Event Details modal stage stepper not loading in other stage’s information

- IGA-1355 - Nested attribute specific filters only matching first condition
- IGA-1430 - Access denied error when logging out from certain screens
- IGA-1455 - Campaigns auto sign-off when using DS as IDM repository
- IGA-1628 - Cert generation calls outdated config endpoint
- IGA-1837 - Policy scan query for active eq true

New fixes in 7.1

- FOR-1967 - Multi Stage certification with completely empty first stage not advancing
- FOR-1969 - Events view off when one of the other stage's events is empty
- FOR-1975 - Expiration certification failing to fully close certification
- FOR-1977 - Add displayName to defaults for glossary
- FOR-1980 - Reassigning events in bulk sends a notification for every single event
- HAR-217 - Create request API allowing duplicates
- HAR-252 - Manager approver not failing gracefully when can't calculate
- HAR-323 - Ensure all reserved keywords in the glossary are properly type casted
- HAR-331 - Header alignment
- HAR-332 - No-events-generated translation
- HAR-336 - Reserved glossary keys not respecting default values
- IGA-262 - Request for self not self-selecting
- IGA-258 - New glossary item creation is slow
- IGA-155 - Access Review not allowing us to delete scheduled script
- IGA-85 - OOTB example remediate does not remove assignments

Limitations

Identity Governance does not officially support internationalization or multi-language support of any kind.

Known issues

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

- There is a vulnerability in the most recent available release of the JavaScript library lodash (version 4.17.15, the most recent version upon this release) that is used by Identity Governance and was detected during routine security scans of the Identity Governance source. We are aware of this issue, have looked into it, and have

determined that the vulnerable functionality is not used or exposed within the application.

- In certain cases, the included example remediation workflow throws an exception in the IDM logs on installation due to an issue with image loading.

Compatibility

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

Important changes to existing functionality

IGA 7.1.1

- If you are using IDM 7.2 or above with Identity Governance, in order for all the functionality within the IGA User Summary UI to work correctly, IDM must have `linkedView` endpoint enabled. In prior versions of IDM, this existed by default.
  - To enable this endpoint copy the contents shown below into a **newly created** file at `openidm/conf/endpoint-linkedView.json`:

```
{
"context" : "endpoint/linkedView/*",
"type" : "text/javascript",
"source" :
"require('linkedView').fetch(request.resourcePath);"
}
```

IGA 7.1

- Access Request 1.0 used a single custom BPMN workflow definition to drive the request lifecycle that is no longer used with this release. Request and approval objects are now stored within the IDM repository and are no longer driven by workflow process instances. For existing implementations of Access Request 1.0 that are upgrading to this version, conversion scripts must be run after installation to maintain existing request history.
- Access Request 1.0 supported Start and End Dates as advanced field options for all requests. Since requests for access now support multiple different types of access, and no longer only roles, these temporal constraints are no longer included by default in request forms. However, any requestable role can still be requested with

temporal constraints by using custom request fields and a provisioning script as detailed within the Admin Guide.

Deprecated functionality

No functionality is deprecated at this time.

Removed functionality

- Validation on the `userProvisionProperty` key for requestable glossary objects has been removed. Glossary administrators can use any existing relationship property on a managed user for this key value in order to request custom objects in their schema.

Documentation updates

The following table tracks changes to the documentation set following the release of Identity Governance 7.1:

Documentation Change Log

Date	Description
2023-05-18	Release of Identity Governance patch version 7.1.1.
2021-05-18	Initial release of Identity Governance 7.1.

Appendix A: Release levels and interface stability

ForgeRock defines Major, Minor, 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

Release Label	Version Numbers	Characteristics
Major	Version: x[.0.0]	• Bring major new features, minor features, and bug fixes • Can include changes even to Stable interfaces • Major indicates the version, for example, `7`.
Minor	Version: x.y[.0]	• 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 • Minor indicates the version, for example, `1`.
Patch	Version: x.y.z	• Bring bug fixes • Are intended to be fully compatible with previous versions from the same Minor release • Patch starts with `0` and increases for each bug fix 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

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.

Stability Label	Definition
Removed	This feature or interface was deprecated in a previous release and has now been removed from the product.
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.