Release notes

ForgeRock® Autonomous Identity is an entitlements and roles analytics system that lets you fully manage your company's access to your data.

These release notes are written for anyone using the Autonomous Identity 2022.11.3 release. Read these notes before you install Autonomous Identity software, especially for production deployments.

What's New

Discover new features.

Before You Install

Check prerequisites.

Known Issues

Check known issues.

Documentation

Track doc changes.

Interface Stability

Learn about the Release Levels, upgrades, and stability levels.

Getting Support

Get support and training.

What's New in 2022.11.3

Autonomous Identity 2022.11.3 is a patch release containing a collection of bug and security fixes released as part of our commitment to our customers.

For general information on ForgeRock's maintenance and patch releases, see Maintenance and Patch availability policy.

You can deploy Autonomous Identity 2022.11.3 as an initial deployment or upgrade it from an existing 2022.11.0, 2022.11.1, or 2022.11.2 deployment.

Improvements/Changes in Configuration

- **New property to use MongoDB with LDAP**. Autonomous Identity has a new `vars.yml` property, `mongo_ldap=false`, which when set to `true`, lets Autonomous Identity authenticate with MongoDB, configured with LDAP.
- **New assignments endpoint**. Autonomous Identity now provides an endpoint to support the extraction of assignments. Refer to Assignments.

Known issue

ForgeRock discovered a known issue in 2022.11.3: Refer to Known issues in 2022.11.3.

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.

Before you start

Autonomous Identity server software requires the following hardware, storage, and operating system requirements to run in your production environment. Autonomous

Identity's flexible architecture runs in a variety of network environments: on-prem, cloud, multi-cloud, and hybrid.

IMPORTANT

All production systems differ in many ways. Please discuss with your ForgeRock Professional Services, installers, or partner representatives about your environment specifics.

ForgeRock Google Cloud registry key

You deploy Autonomous Identity using a Docker image that pulls other dependent images from the ForgeRock Google Cloud Registry repository and installs the components on a target node.

For specific instructions on obtaining the registry key, refer to How To Configure Service Credentials (Push Auth, Docker) in Backstage.

Hardware and memory requirements

Autonomous Identity has a number of components that include application, data, and analytics servers, which are all included in the Docker images. The minimum hardware and memory requirements for a single-node target and a separate deployer machine are as follows:

Hardware and memory requirements

Vendor	Versions
Deployer Node	32 GB RAM, 8 CPU
Analytics (Target) Node	64 GB RAM, 16 CPU

Storage requirements

Autonomous Identity has a number of components that include application, data, and analytics servers, which are included in the Docker images. The minimum storage requirements for a single-node deployment are as follows:

Autonomous Identity requires the following minimum storage requirements:

Storage requirements

Type	Size
Data Storage	500 GB (minimum), 1 TB (production)

Operating systems requirements

Autonomous Identity is supported on the following operating system:

Operating System Requirements

Vendor	Versions[1]
CentOS Stream	8.0
Redhat Enterprise Linux	8.0

Cloud services requirements

Autonomous Identity has been successfully deployed on the following cloud services:

Cloud Services Requirements

Vendor	Versions
Google Cloud Platform (GCP)	Latest
Amazon Web Services (AWS) standard Elastic File System (EFS) shared drive	Latest

Java requirements

Autonomous Identity software supports the following Java version:

Java requirements

Vendor	Versions
OpenJDK	11.0.16

Third-party software

Autonomous Identity uses the following third-party software in the deployment.

IMPORTANT:

> If your existing deployment uses the deployer-pro installer (2022.11.0 and later), you can upgrade these third-party dependencies to these versions.
>
> If your existing deployment uses the deployer installer (pre-2022.11.0 or earlier), you do not need to pre-install or upgrade these components in your environment.

The Autonomous Identity deployer installs or upgrades these dependencies.

Third-party software

Component	Version	Usage
Python	3.8.13	Scripts
Docker CE	20.10.17	Container cluster management
Apache Cassandra	4.0.8	Database for all Autonomous Identity services
MongoDB	4.4.19	Database for all Autonomous Identity services. If using MongoDB with LDAP, set the `mongo_ldap` property to `true` in the `vars.yml` file.
Apache Spark	3.3.2 with Hadoop 3	Cluster to run Autonomous Identity analytics
Apache Livy	Updated to work with Spark 3.3.2	REST interface to Spark master to run Autonomous Identity analytics
OpenSearch/OpenSearch Dashboards	1.3.9	Distributed, open source search engine and visualization tool for all data types.

Supported browsers

Autonomous Identity supports the following browsers:

Supported browsers

Vendor	Versions
Google Chrome	version 85.0.4183.121 and higher

Vendor	Versions
Mozilla Firefox	version 86.0.1 and higher

Autonomous Identity ports

Autonomous Identity uses the following ports:

Autonomous Identity ports

Port	Protocol	Machine	Source	Description
2377	TCP	Docker managers	Docker managers and nodes	Communication between the nodes of a Docker swarm cluster
7946	TCP/UDP	Docker managers and workers	Docker managers and workers	Communication among nodes for container network discovery
4789	UDP	Docker managers and workers	Docker managers and workers	Overlay network traffic
7001	TCP	Cassandra	Cassandra nodes	Internode communication
9042	TCP	Cassandra	Cassandra nodes, Docker managers and nodes	CQL native transport
27017	TCP	MongoDB	MongoDB nodes, Docker managers and nodes	Default ports for mongod and mongos instances
9200	TCP	Open Distro for Elasticsearch	Docker managers and nodes	Elasticsearch REST API endpoint
7077	TCP	Spark master	Spark workers	Spark master internode communication port
40040-40045	TCP	Spark Master	Spark Workers	Spark driver ports for Spark workers to callback

Port	Protocol	Machine	Source	Description
443	TCP	Docker managers	User's browsers/API clients	Port to access the dashboard and API
10081	TCP	Docker managers	User's browsers/API clients	Port for the JAS service.

Key Fixes

Key Fixes in 2022.11.3

The following bug was fixed in this release as well as other security fixes:

- AUTOID-3174: Need an assignments API
- AUTOID-3362: Allow customer to change timeout for API container when run opensearch query

Key Fixes in 2022.11.2

The following bugs were fixed in this release:

- AUTOID-3329: Misspelled http header for kibana conf
- AUTOID-3331: Elasticsearch keystore and truststore password

Key Fixes in 2022.11.1

This release contains a collection of important security fixes.

Key Fixes in 2022.11.0

This release contains a collection of security and bug fixes. The following issues were fixed:

- AUTOID-2766: Analytics results show inconsistent results
- AUTOID-2864: Not able to delete data sources in AutoID
- AUTOID-2894: Support for updating all certificates in AutoID
- AUTOID-3130: Upgrade Spark to 3.3

- AUTOID-3135: Upgrade Open Distro to OpenSearch
- AUTOID-3145: Upgrade Python to 3.8
- AUTOID-3160: Upgrade OpenJDK to 11

Known Issues

Known Issues in 2022.11.3

- **Discovered regression**

  Autonomous Identity 2022.11.3 was originally released on 04-11-2023.

  We discovered a regression where Apache Livy has log4j1 binaries included with the deployer. If you installed 2022.11.3 *before* 04/13/2023, run the steps below to upgrade log4j1 to log4j2.

  If you installed 2022.11.3 *after* 04/13/2023, the binaries are updated, and you do not need to upgrade log4j1 binaries.

  > ***Update log4j1 to log4j2***
  >
  > 1. Stop the Apache Livy server:
  >
  >    ```
  >    ~/livy/bin/livy-server stop
  >    ```
  >
  > 2. Back up your old log4j and related jar files:
  >
  >    ```
  >    cd ~/livy/jars
  >    mv log4j-1.2.16.jar ~/log4j-1.2.16.jar.bkp
  >    mv slf4j-log4j12-1.6.1.jar ~/slf4j-log4j12-
  >    1.6.1.jar.bkp
  >    mv slf4j-reload4j-1.7.36.jar ~/slf4j-reload4j-
  >    1.7.36.jar.bkp
  >    mv slf4j-api-1.7.25.jar ~/slf4j-api-1.7.25.jar.bkp
  >    ```
  >
  > 3. Replace with log4j2 jar and its bridge jars:
  >
  >    ```
  >    cd ~/livy/jars
  >    wget
  >    https://repo1.maven.org/maven2/org/apache/logging/log4j
  >    /log4j-1.2-api/2.18.0/log4j-1.2-api-2.18.0.jar
  >    wget
  >    https://repo1.maven.org/maven2/org/apache/logging/log4j
  >    ```

```
/log4j-core/2.18.0/log4j-core-2.18.0.jar
wget
https://repo1.maven.org/maven2/org/apache/logging/log4j
/log4j-slf4j-impl/2.18.0/log4j-slf4j-impl-2.18.0.jar
wget
https://repo1.maven.org/maven2/org/apache/logging/log4j
/log4j-api/2.18.0/log4j-api-2.18.0.jar
wget https://repo1.maven.org/maven2/org/slf4j/slf4j-
api/1.7.36/slf4j-api-1.7.36.jar
```

4. Under the `conf` folder, create a `log4j2.properties` file:

```
cd ~/livy/conf
vi log4j2.properties
```

5. In your `log4j2.properties` file, adjust the log level and related configuration suited for your requirements:

```
status = info
name= RollingFileLogConfigDemo
# Log files location
property.basePath = ./logs
# RollingFileAppender name, pattern, path and rollover
policy
appender.rolling.type = RollingFile
appender.rolling.name = fileLogger
appender.rolling.fileName= ${basePath}/autoid.log
appender.rolling.filePattern=
${basePath}/autoid_%d{yyyyMMdd}.log.gz
appender.rolling.layout.type = PatternLayout
appender.rolling.layout.pattern = %d{yyyy-MM-dd
HH:mm:ss.SSS} %level [%t] [%l] - %msg%n
appender.rolling.policies.type = Policies
# RollingFileAppender rotation policy
appender.rolling.policies.size.type =
SizeBasedTriggeringPolicy
appender.rolling.policies.size.size = 10MB
appender.rolling.policies.time.type =
TimeBasedTriggeringPolicy
appender.rolling.policies.time.interval = 1
appender.rolling.policies.time.modulate = true
appender.rolling.strategy.type =
DefaultRolloverStrategy
appender.rolling.strategy.delete.type = Delete
appender.rolling.strategy.delete.basePath = ${basePath}
```

```
appender.rolling.strategy.delete.maxDepth = 10
appender.rolling.strategy.delete.ifLastModified.type =
IfLastModified
# Delete all files older than 30 days
appender.rolling.strategy.delete.ifLastModified.age =
30d
# Configure root logger
rootLogger.level = info
rootLogger.appenderRef.rolling.ref = fileLogger
log4j1.compatibility = true
```

6. Restart Apache Livy:

```
cd ~/livy/
./bin/livy-server start
```

7. Check that Apache Livy is up and running. You can access a log on an analytics jobs. Specific Autonomous Identity logs are at `~/livy/logs/autoid.log`.

Known Issues in 2022.11.2

There are no known issues in this release.

Known Issues in 2022.11.1

There are no known issues in this release.

Known Issues in 2022.11.0

There is a known issue with RHEL8/CentOS Stream 8 when Docker swarm overlay network configuration breaks when the outside network maximum transmission unit (mtu) is smaller than the default value. The `mtu` is the maximum size of the packet that can be transmitted from a network interface.

Refer to https://github.com/moby/libnetwork/issues/2661 and https://github.com/moby/moby/pull/43197.

When deploying a multinode configuration on RHEL 8/CentOS Stream 8, run the following steps:

1. Check mtu for docker0 and eth0 using `ifconfig | grep mtu`.
2. Set the docker0 mtu value to be equal to `eth0` using `sudo ifconfig eth0 mtu 1500`. Make sure to set the command on all nodes and also after each virtual

machine reboot.

Deprecated

Deprecated in 2022.11.3

- No functionality has been deprecated in this release.

Deprecated in 2022.11.2

- No functionality has been deprecated in this release.

Deprecated in 2022.11.1

- No functionality has been deprecated in this release.

Deprecated in 2022.11.0

- No functionality has been deprecated in this release.

Removed

Removed in 2022.11.3

- No functionality has been removed in this release.

Removed in 2022.11.2

- No functionality has been removed in this release.

Removed in 2022.11.1

- No functionality has been removed in this release.

Removed in 2022.11.0

- No functionality has been removed in this release.

Documentation updates

The following table tracks changes to the documentation following the release of Autonomous Identity 2022.11.3:

Documentation Change Log

Date	Description
2023-08-15	Added a line that you need to update your third-party software packages to the supported versions prior to upgrading Autonomous Identity. Refer to Upgrade from Autonomous Identity 2022.11.x to 2022.11.3 using deployer pro.
2023-04-13	Added a known issue. Refer to Known issues in 2022.11.3.
2023-04-12	Added a section on updating the domain and namespace in existing deployments. Refer to admin-guide:chap-deployment-tasks.adoc#customize-domain-existing.
2023-04-11	• Initial release of Autonomous Identity 2022.11.3. • Added a section to change the default timeout (30 ms) for the API's Elasticsearch client request timeout. Refer to Change the API's Elasticsearch client request timeout. • Added the Assignments endpoint to the API. Refer to Assignments.
2023-02-24	Initial release of Autonomous Identity 2022.11.2.
2023-01-09	Initial release of Autonomous Identity 2022.11.1.
2022-12-08	• Removed the refresh-company-view command as it is no longer required in the Analytics pipeline process. • Updated the steps to install the Python egg file. Refer to Install Autonomous Identity. • Removed sections pertaining to third-party component backup-restore and import-export data in the Server Maintenance.
2022-11-28	Added a section to change the MongoDB password post-deployment. Refer to Change the MongoDB password post-deployment.
2022-11-15	Initial release of Autonomous Identity 2022.11.0.

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.

IMPORTANT

Autonomous Identity uses a different version numbering system from other ForgeRock products. The version number use the following format: `Major.Minor.Patch`, where *Major* is the year of the release, *Minor* is the month of the release, *Patch* is the number beginning with 0, and increases for each patch release.

Thus, for this release of Autonomous Identity, the version number is **2022.11.3**.

Release Level Definitions

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 year of the release, for example, `2021`
Minor	Version: x.y[.0]	• Bring minor features, and bug fixes • Can include backwards-compatibile changes to Stable interfaces in the same Major release, and incompatible changes to Evolving interfaces • Minor indicates the month of the release, for example, `8` for August
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

Upgrade and Patching

ForgeRock plans to introduce quarterly upgrades and patches for Autonomous Identity as a service to our customers. Autonomous Identity's architecture supports seamless rolling upgrades to simplify the process.

The following are some general points about upgrades and patches:

- Upgrades and patches are implemented using a simple swap of the underlying container. The operation is zero down-time as long as the cluster has a redundant instance of the microservice.
- Patching does not require schema changes.

  Autonomous Identity schema changes are additive and backward-compatible. This means that during a zero-downtime upgrade, older versions of the container can still write to the new version of the schema. Also, newer versions of the container may alter the tables in a way that preserves the semantics of the previous columns.
- If an upgrade requires a downgrade due to some issue, the downgrade will not restore the previous schema.

More information about upgrading, refer to Upgrade Autonomous Identity.

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.

Stability Label	Definition
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.

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, refer to 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.

1. For Autonomous Identity 2022.8.x systems that use CentOS/Redhat Enterprise Linux 7.0 and upgrade to Autonomous Identity 2022.11.x, Autonomous Identity continues to run on CentOS/Redhat Enterprise Linux 7.0. For new Autonomous Identity 2022.11.x installations, use CentOS/Redhat Enterprise Linux 8.0.