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 2021.8.0 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

What's New in 2021.8.0

Autonomous Identity 2021.8.0 is a major release that contains a collection of fixes and RFEs. These fixes have been grouped together and released as part of our commitment to support our customers.

To view the list of fixes in this release, see Key Fixes in Autonomous Identity 2021.8.0. For general information on ForgeRock's maintenance and patch releases, see Maintenance and Patch availability policy.

You can deploy Autonomous Identity 2021.8.0 as an initial deployment, or upgrade it from an existing 2021.3.2 deployment.

New Features

Autonomous Identity 2021.8.0 introduces a number of new and exciting features in this release:

- **New Roles Workshop**. Autonomous Identity 2021.8.0 now provides a powerful role management system that lets you fully create and analyze all roles in your system. The *Roles Workshop* is the main dashboard for managing your roles. You can create *drafts* from discovered *candidates* in the latest role mining job, or create new roles from scratch. For more information, see Roles Management Tasks.
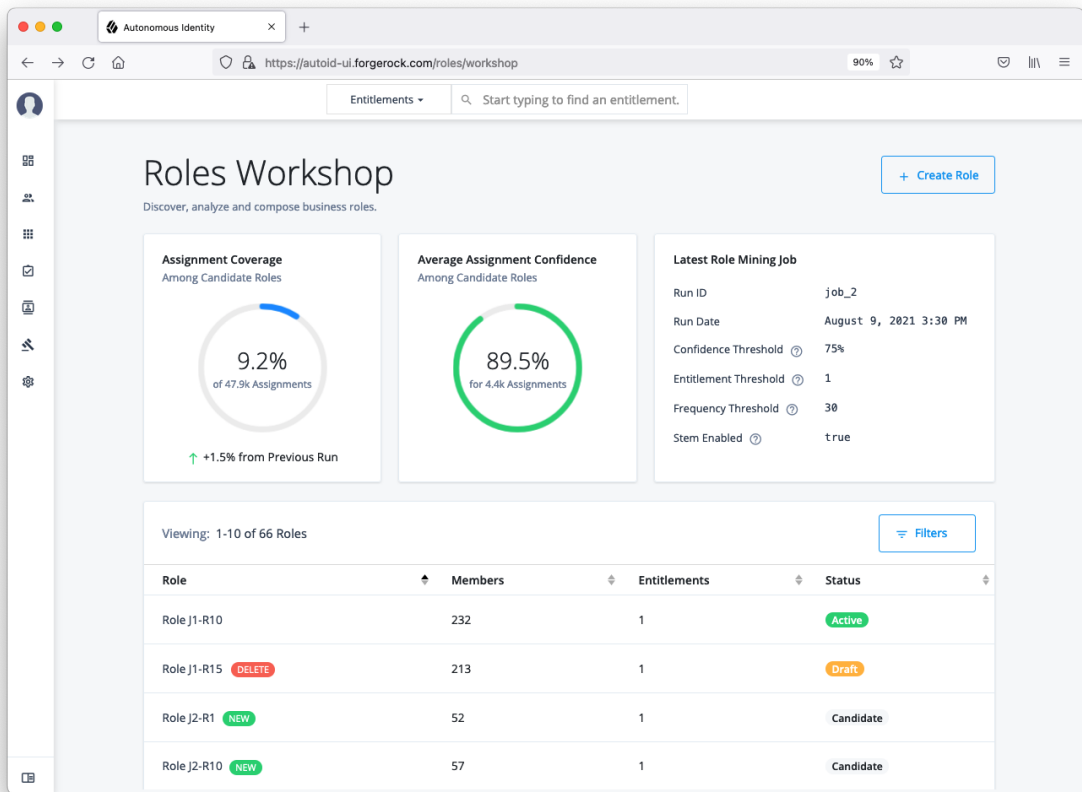
- **New Roles Catalog**. The Roles Catalog page lists your active roles in production, and lets you export some or all your roles to JSON.
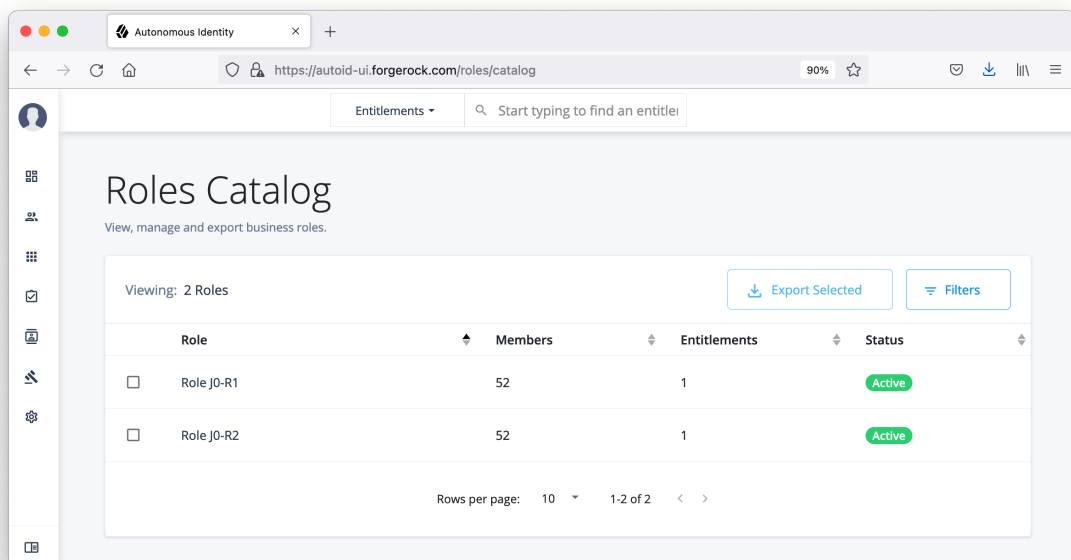

- **New Data Sources**. Autonomous Identity has a new and highly performant ingestion system to support new data source files types: CSV, JDBC, and Generic. Companies can import data with these different file sources without having to convert to a singular format. For more information, see Set Data Sources.
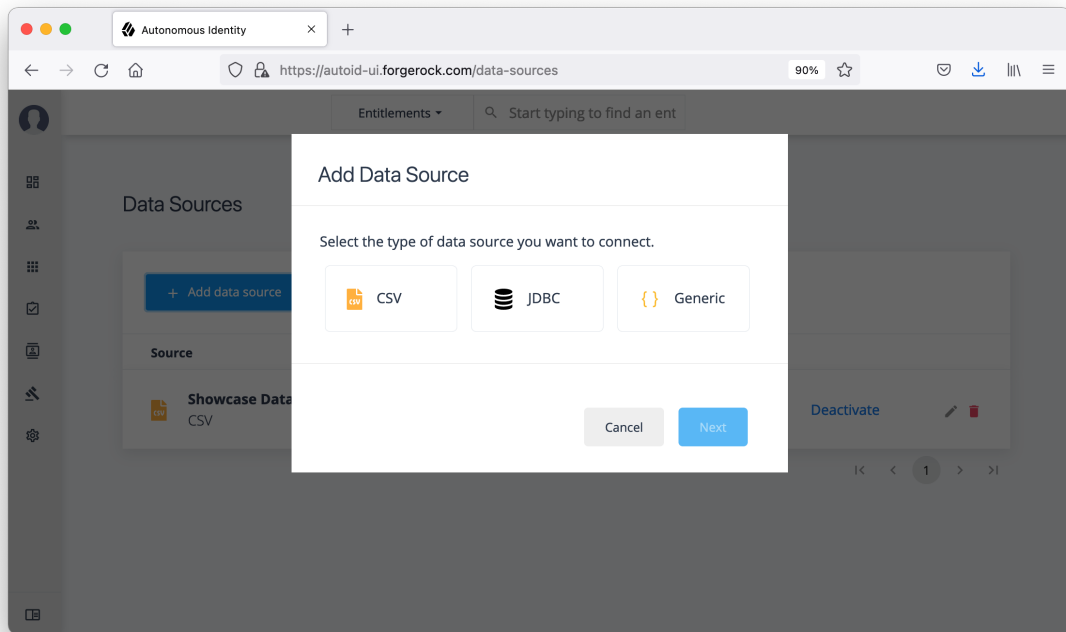
- **New Data Sources Sync Types**. The Data Sources page also provides synchronization types that lets you ingest data in different modes: full, incremental, enrichment, and delete. For more information, see Set Data Sources.
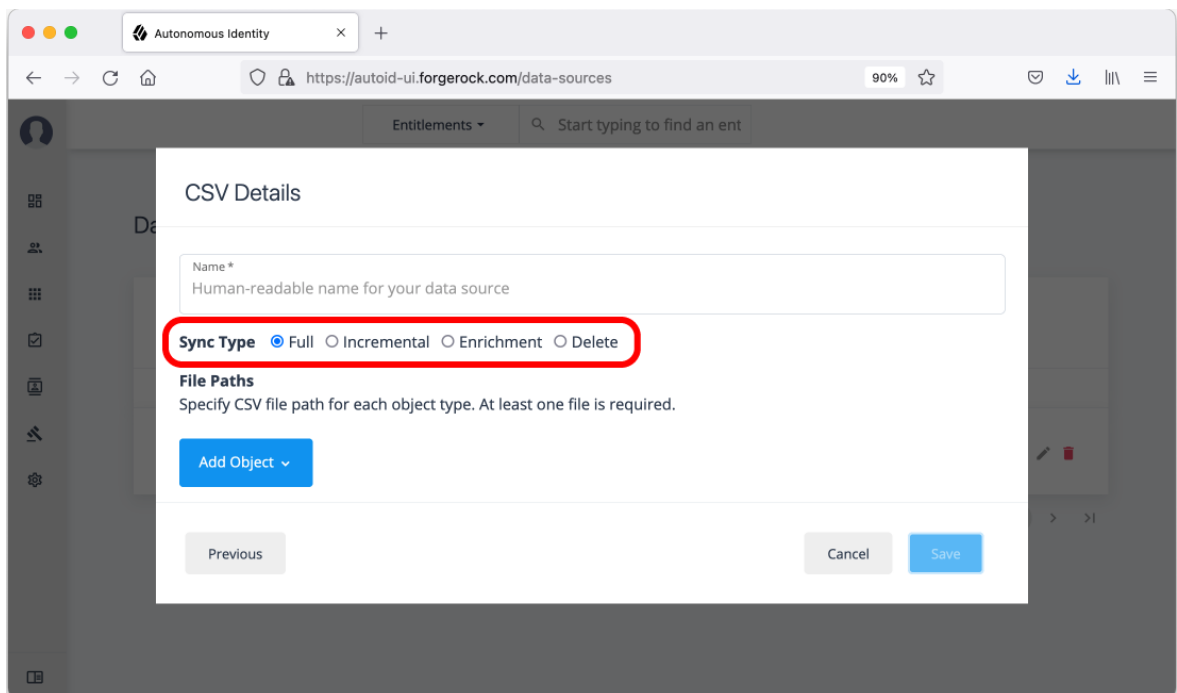
- **New Self Service Page**. The Self Service page lets administrators reset their personal account information and create time-based API keys for users. For more information, see Self Service.
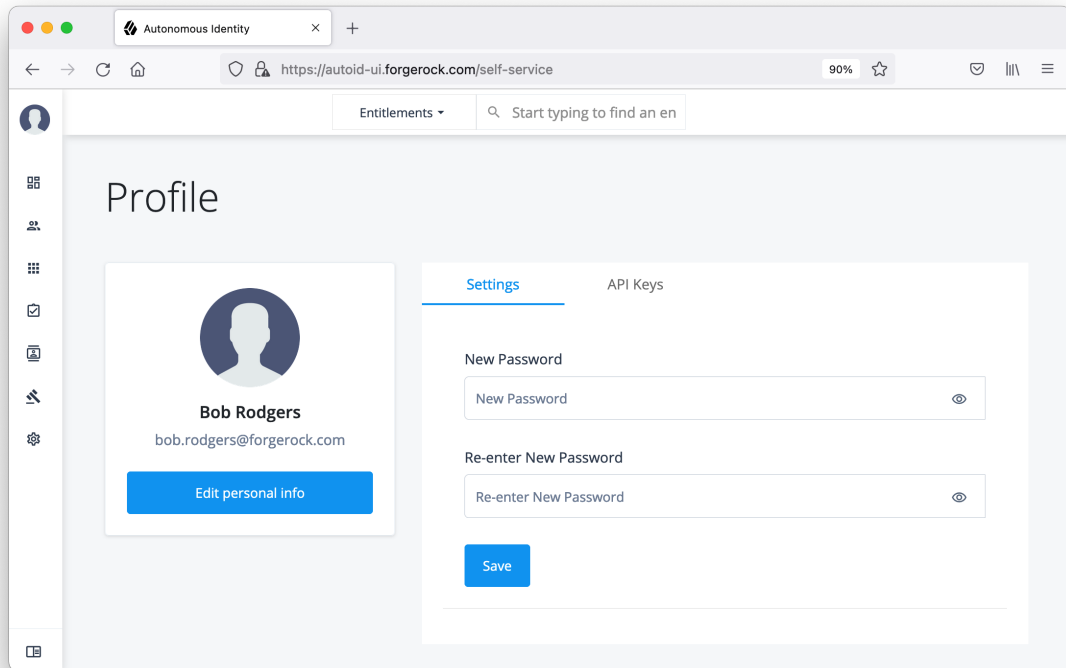
- **New Manage Identities Page**. The Manage Identities page lets administrators add, edit, or deactivate users in the system as well as assign specific roles. For more information, see Manage Identities.
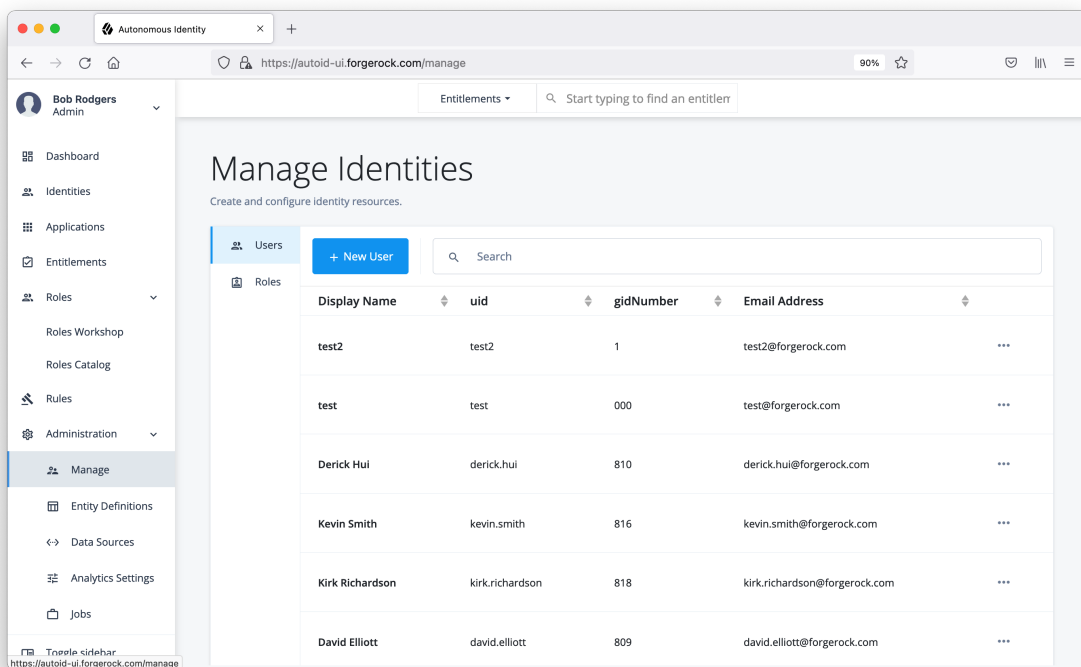
- **New Jobs Page**. The Jobs page lets administrators run the analytics pipeline steps using a UI interface. The previous analytics command-line steps can also be used to run the analytics pipeline. For more information, see Run Analytics.
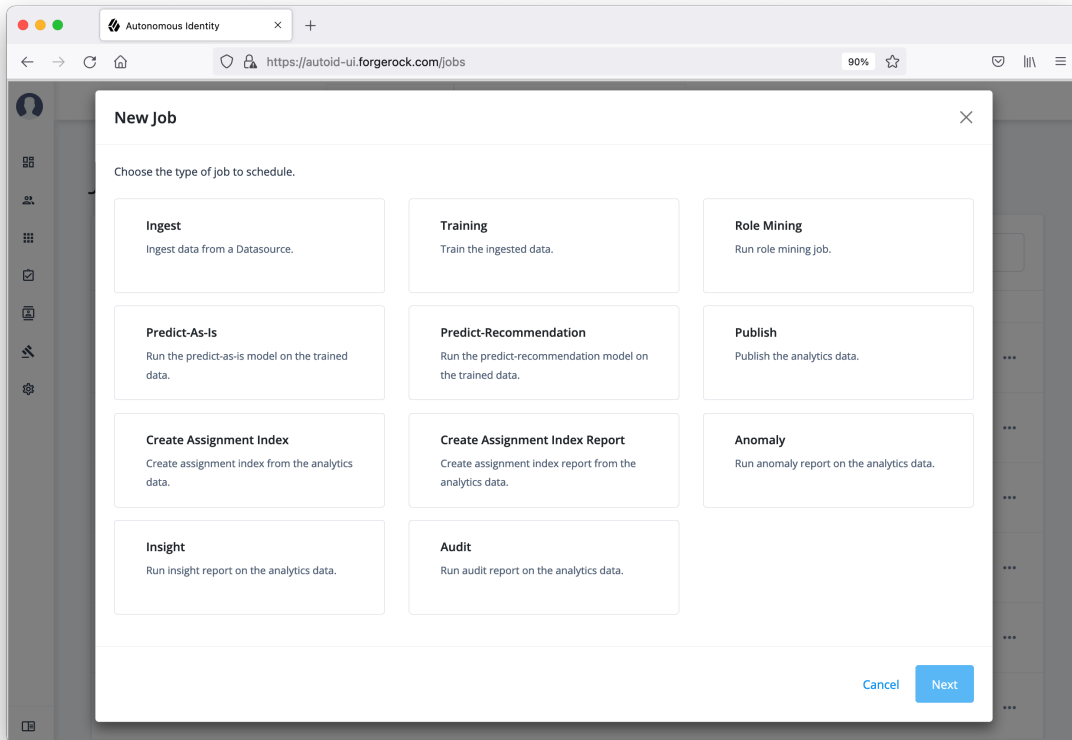
- **Updated Roles Entity Definitions**. The Entity Definitions page now lets you add new Roles attributes to the schema. For more information, see <u>Set Entity Definitions</u>.
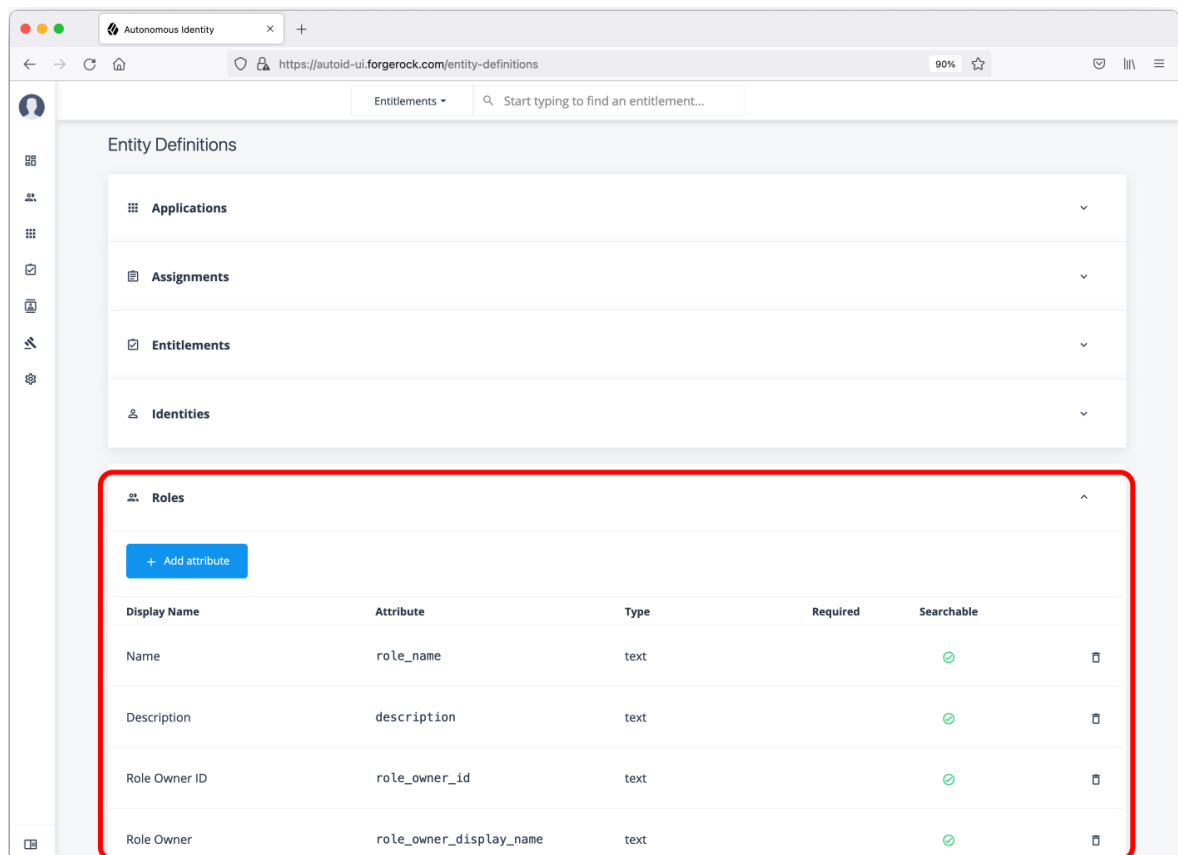
- **Updated Analytics Settings**. The Analytics Settings page has been expanded to include role discovery settings and analytics Spark job configuration. For more

information, see Set Analytics Thresholds.

- **Improvements/Changes in Configuration**.
  - **OpenLDAP Removal**. Autonomous Identity no longer bundles OpenLDAP as a default user repository and has removed it from the deployment. As a result, phpldapadmin 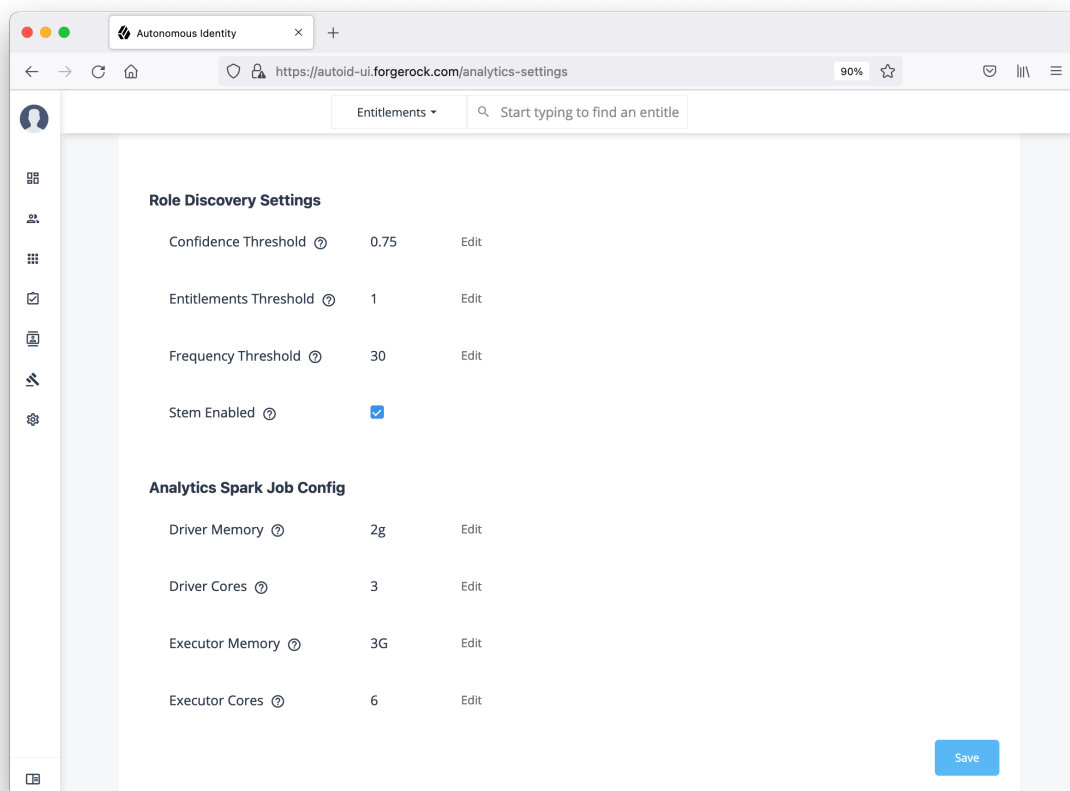is also no longer available. Autonomous Identity now supports the new self service and manage identities pages to let administrators manage Autonomous Identity users.
  - **Updated Vars.yml File Properties**. The following properties were updated or added to the `vars.yml`:
    - **authentication_option**. The `authentication_option` has changed the name of its values: `Local`, `SSO`, and `LocalAndSSO`. For more information, see Install a Single Node Deployment.
    - **local_auth_mode_password**. The `local_auth_mode_password` stores the local password for demo environments.
    - **role_owner_object_id, role_engineer_object_id**. New role user type objects were added to the SSO section in the `vars.yml` file.
  - **Updated Hosts file**. The `~/autoid-config/hosts` file no longer has the `[cassandra-workers]` as there is no longer a need to dedicate a node to the cassandra workers. All other properties still remain in the file.
  - **New API Endpoints**. Autonomous Identity introduces new API endpoints. For more information, see Autonomous Identity API.

- GET /api/authentication/verify
- GET /api/userDetails/distinct
- GET /api/entitlements/distinct
- GET /api/entitlements/recommendations
- POST /api/admin/updateUser
- POST /api/admin/updateSelf
- POST /api/admin/disableUser
- POST /api/admin/enableUser
- POST /api/admin/createUser
- POST /api/admin/createApiToken
- POST /api/admin/revokeApiToken
- GET /api/admin/verifyApiToken/{token}
- GET /api/admin/getTokens
- GET /api/admin/getUsers
- POST /api/roles
- POST /api/roles/delete
- POST /api/roles/export
- New property added to GET /api/rules

- **Processing Improvements**. Autonomous Identity has improved its backend infrastructure with new components that provide higher performance.

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.

> **IMPORTANT**
>
> ForgeRock has released a security advisory on Log4j. Refer to: Log4j Security Advisory #202111 for details.

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 (gcr.io) repository and installs the components on a target node.

For specific instructions on obtaining the registry key, see 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:

Table 2: 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 all 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:

Table 3: Storage requirements

Type	Size

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

Operating systems requirements

Autonomous Identity is supported on the following operating system:

Table 4: Operating System Requirements

Vendor	Versions
CentOS	7.0
Redhat Enterprise Linux	7.0

Cloud services requirements

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

Table 5: 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:

Table 6: Java requirements

Vendor	Versions
OpenJDK	8u262

Third-party software

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

You do not need to pre-install these components in your environment. The Autonomous Identity deployer installs these components.

Table 7: Third-party software

Component	Version	Usage
Python	3.6	Scripts
Docker CE	20.10.7	Container cluster management
Apache Cassandra	3.11.2	Database for all Autonomous Identity services
Apache Spark	3.1	Cluster to run Autonomous Identity analytics
Apache Livy	0.8.0-incubating	REST interface to Spark master to run Autonomous Identity analytics
Mongo DB	4.2	Database for all Autonomous Identity services
HashiCorp Consul	1.7	Service discovery and configuration server
nginx	1.18	Reverse proxy for routing HTTPS traffic
Open Distro for Elasticsearch	1.9	Distributed, open source search engine for all data types.

Supported browsers

Autonomous Identity supports the following browsers:

Table 8: Supported browsers

Vendor	Versions
Google Chrome	version 85.0.4183.121 and higher
Mozilla Firefox	version 86.0.1 and higher

Autonomous Identity ports

Autonomous Identity uses the following ports:

Table 9: 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
443	TCP	Docker managers	User's browsers/API clients	Port to access the dashboard and API

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

Key Fixes

The following epics were fixed in Autonomous Identity 2021.8.0:

- AUTOID-1129: Scheduling Jobs in AutoID
- AUTOID-1391: Role Composition in AutoID
- AUTOID-1392: AutoID Data Ingestion using JDBC
- AUTOID-2016: Support for JML Use Cases
- AUTOID-2057: Remove LDAP
- AUTOID-2456: API keys for partner integration

Known Issues

There are no known issues in this release.

Deprecated

No new functionality was deprecated in this release.

> **NOTE**
>
> In 2021.3.1: POST employees (/api/singleViewWithApp/employees) was deprecated and will be removed in a future release. For more information, see Single View with Application.

Removed

No functionality was removed in this release.

Documentation updates

The following table tracks changes to the documentation set following the release of Autonomous Identity 2021.8.0:

Documentation Change Log

Date	Description
2022-09-16	Updated the docker restart section to include a command to restart the JAS node. See Restart Docker.
2022-08-22	Added a note about the latest security on log4j. Refer to Security Advisories.
2022-07-26	Added a section on setting up SSO for existing deployments. Refer to Set up single sign-on (SSO) in existing deployments.
2022-07-18	Added a note about log4j version 1. Refer to Security Advisories.
2022-06-16	Added procedures to replace the self-signed certificates in various services. Refer to Custom certificates.
2022-06-14	Corrected the minimum storage requirements in the release notes. Refer to Storage requirements.
2022-01-12	Updated the upgrade section to streamline processes. Refer to Upgrade Autonomous Identity.
2022-01-05	Updated the graphic in the section Architecture in Brief.
2021-12-30	Updated the Set Up SSH on the Deployer section with additional explanations for some steps.
2021-12-17	Fixed a link in the Administration Guide.
2021-12-16	Removed a step to stop Spark master and workers in the 2021.8.1 → 2021.8.2 upgrade.

Date	Description
2021-12-15	Initial release of Autonomous Identity 2021.8.2. The following documentation updates were made: • Removed references to dark theme mode in the release notes and installation guide. Refer to <u>What's New</u>. • Added a section on updating certificates if your IDP changes their certificates. Refer to <u>Updating IDP Certificates</u>. • Added a note to not copy-n-paste a hosts file during a 2021.3.x to 2021.8.x upgrade. Refer to <u>Upgrade to Autonomous Identity 2021.8.2</u>. • Added a step (docker swarm leave) to the upgrade steps when upgrading multi-node deployments. Refer to <u>Upgrade to Autonomous Identity 2021.8.2</u>. • Added a new section on the ingest API endpoints. Refer to Ingest. • Added a known issue to no use "-" and "/" in application names. Refer to <u>Known Issues in 2021.8.2</u>. • Updated the multi-node steps for non-airgap and airgapped with new steps. Refer to <u>Install a Multi-Node Deployment</u> and <u>Install a Multi-Node Air-Gapped Deployment</u>. • Updated the upgrade section to include an important patch step. Refer to <u>Upgrading Autonomous Identity</u>.
2021-10-12	Initial release of Autonomous Identity 2021.8.1. The following documentation updates were made: • Updated the analytics instructions with a new step, **refresh-company-view**. Refer to <u>Refresh Company View</u>. • Updated the API guide with a new chapter on obtaining the API key. Refer to api-guide:chap-obtain-api-key.adoc. • Added a new section in the API Reference. Refer to Ingest API Endpoints.
2021-09-22	Updated the section on running the CLI analytics commands. Refer to <u>Run Analytics on the Command Line</u>.
2021-08-25	Added information on the Jobs API. Refer to <u>Jobs API Endpoints</u>.

Date	Description
2021-08-20	Initial release of Autonomous Identity 2021.8.0. The following documentation updates were made: - Updated the install instructions to indicate that the default shell for the `autoid` user is bash. Refer to Install a Single Node Deployment. - Added an upgrade procedure from 2021.3.2 to 2021.8.0. Refer to Upgrade Autonomous Identity. - Added the Roles section. Refer to Roles Management Tasks. - Added Self Service and Manage Identities sections. Refer to Self Service, Manage Identities. - Updated the Analytics Settings with expanded thresholds for roles and configuration. Refer to Set Analytics Thresholds. - Updated the API Guide with new endpoints. Refer to API Guide. - Updated the analytics pipeline section with the new Jobs page. Refer to Run Analytics. - Update the single node, single node air gap, multi-node, multi-node air gap instructions with updated properties. Refer to Installation. - Updated the Admin Guide with updated instructions for Set Entity Definitions, Set Data Sources, and Set Attribute Mappings. - Updated the SSO setup section. Refer to Set Up Single Sign-On. - Removed references to OpenLDAP and phpldapadmin as they are no longer bundled with Autonomous Identity. - Removed the Getting Started Guide.

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 **2021.8.0**.

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, see Upgrading 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.
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.

Stability Label	Definition
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.
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.

Was this helpful? 👍 👎