







Release notes

ForgeRock® Autonomous Identity is an entitlements 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 2021.3.0 release. Read these notes before you install Autonomous Identity software, especially for production deployments.

Quick Start

 <u>What's New</u> Learn about what's new in this version.	 <u>Before You Start</u> Learn about the requirements for running Autonomous Identity software in production.	 <u>Known Issues</u> Learn about the known issues in this release.
 <u>Check Doc Updates</u> Track important changes to the documentation.	 <u>Release Levels</u> Learn about the Release Levels, upgrades, and stability levels.	 <u>Get Support</u> Find out where to get professional support and training.

What's New in 2021.3.0

What's New in 2021.3.0

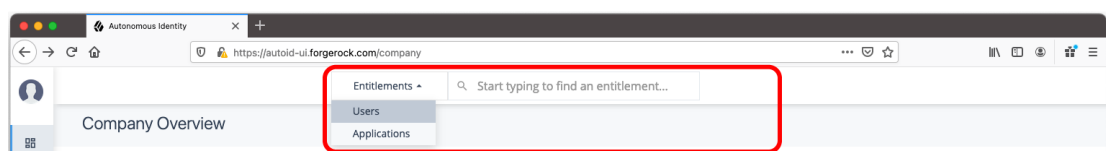
Autonomous Identity 2021.3.0 is a major release that introduces new features and functionality.

The following major improvements are introduced in this release:

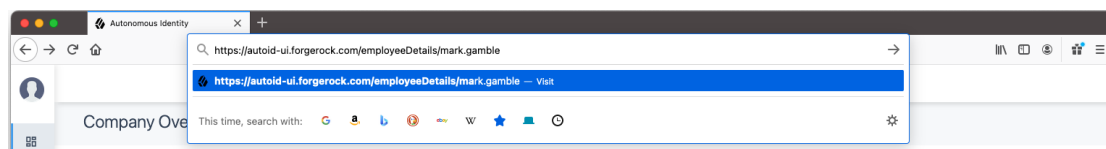
- **Schema Extension.** Autonomous Identity now provides UI-driven schema discovery and extension functionality. These features let you add new schema elements, letting

you fully manage the schema using the Autonomous Identity UI. For more information, see Set Entity Definitions.

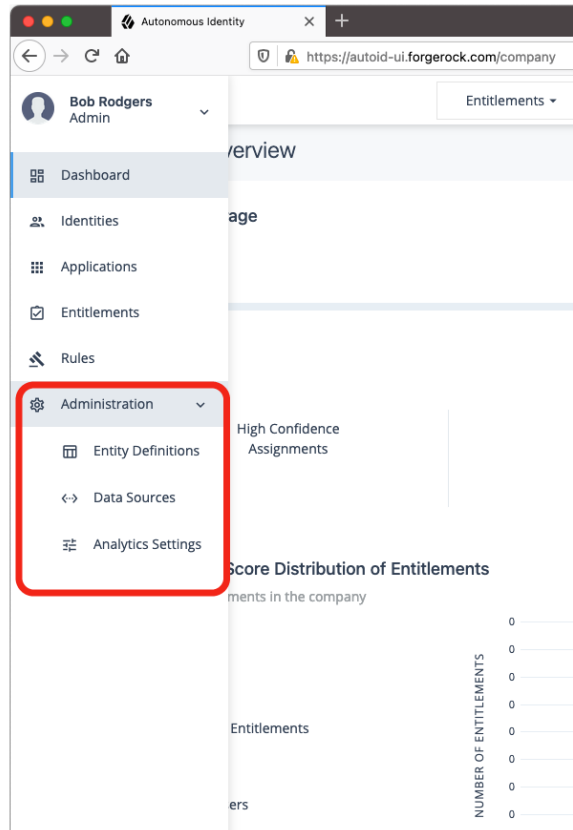
- **UI-Driven Data Source and Attribute Mapping.** Autonomous Identity now provides UI-driven data ingestion tools to define your CSV flat files. This feature eliminates the need to create nine CSV source files from your existing datasets for ingestion into Autonomous Identity. Instead, you can set up your source files, schema extensions, and attribute mappings to input application, assignment, entitlement, and identity data into the system. For more information, see Set Data Sources.
- **UI-Driven Analytics Configuration.** Autonomous Identity now provides UI-driven analytics settings feature that removes the need to edit a yaml file. For more information, see Set Analytics Thresholds.
- **Improved Infrastructure.** Autonomous Identity 2021.3.0 now supports:
 - **Spark 3.1.** Autonomous Identity 2021.3.0 now uses Spark 3.1 for enhanced performance and security.
 - **Improved Architecture.** Autonomous Identity 2021.3.0 has a new and updated architecture to allow scalable reads and writes, and improved performance.
 - **Updated API.** Autonomous Identity 2021.3.0 has restructured and updated its REST endpoints.
- **Improvements to the UI.** Autonomous Identity 2021.3.0 has made various UI fixes for improved user experience.
 - **Improved Search Menu.** The Autonomous Identity UI now provides a search function for administrators to find entitlements, users, or applications. For more information, see [The Autonomous Identity UI](#).



- **Access through the URL.** Administrators can also access a specific entitlement, user detail, or application page using the URL. For more information, see [The Autonomous Identity UI](#).



- **New Administrator Icon.** Administrators can add new attributes to the schema, set data sources and mappings, and configure the analytics settings on the UI. For more information, see [The Autonomous Identity UI](#).



- **Functionality Changes.** Autonomous Identity 2021.3.0 has made changes to the following items:
 - **Streamlined Analytics Steps.** To streamline the analytics process, the following commands have been removed: `create-template`, `apply-template`, `validate`, `audit`, `create-ui-config`, `apply-ui-config`, and `run-pipeline`. For more information, see [Run Analytics](#).
 - **New Offline Mode Parameter.** The `vars.yml` file now has a `offline_mode` parameter that you must set to `true` for single node or multinode air-gapped deployments. For more information, see [Install a Single Node Air-Gapped](#), or [Install a Multinode Air-gapped](#).
 - **Updated Hosts File.** In this release, analytics are no longer run from a Docker container as was done in previous releases but are directly run from the Spark master over a REST interface, facilitated by Apache Livy. As a result, the `autoid-config/hosts` file, no longer includes a `[analytics]` entry. For more information, see [Install Autonomous Identity](#).
 - **Expanded API Section in Vars.yml File.** The `vars.yml` file now has additional settings for `jwt_audience` and `oidc_jwks_url`. For more information, see [Install a Single Node](#).
 - **Additional SSO Parameters in Vars.yml File.** The `vars.yml` file now has additional entries for `application_owner_object_id`, `oidc_end_session_endpoint`, and `oidc_logout_redirect_url`. For more information, see [Set Up SSO](#).

- **Java API Service Support in Vars.yml File.** The `vars.yml` file provide Java API Service settings: `auth_enabled`, `max_memory`, `mapping_entity_type`, and `datasoure_entity_type`. For more information, see [Install Autonomous Identity](#).
- **Expanded API Section in Vars.yml File.** The `vars.yml` file now has additional settings for `jwt_audience` and `oidc_jwks_url`. For more information, see [Install a Single Node Deployment](#).
- **Additional SSO Parameters in Vars.yml File.** The `vars.yml` file now has additional entries for `application_owner_object_id`, `oidc_end_session_endpoint`, and `oidc_logout_redirect_url`. For more information, see [Set Up Single Sign-On](#).
- **Java API Service Support in Vars.yml File.** The `vars.yml` file provide Java API Service settings: `auth_enabled`, `max_memory`, `mapping_entity_type`, and `datasoure_entity_type`. For more information, see [Install Autonomous Identity](#).
- **New Upgrade Process.** The upgrade procedure has been enhanced to update 2020.10.x to 2021.3.0 deployments. For more information, see [Upgrade Autonomous Identity](#).

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.

A note about log4j version 1

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

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
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	18.09.1	Container cluster management

Component	Version	Usage
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.
OpenLDAP	2.4.50 and higher	An LDAP server backend.

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

Key Fixes

The following issues were fixed in Autonomous Identity 2021.3.0:

- [AUTOID-1975](#): Fix recommend runtime
- [AUTOID-1976](#): Re-work session management
- [AUTOID-1977](#): Add user permissions to other groups
- [AUTOID-1979](#): Application filters not working on Identities, Entitlements pages
- [AUTOID-1981](#): AutoID installation is trying to pull Access Notebook image
- [AUTOID-1993](#): Delete datasource not working for SSO
- [AUTOID-1994](#): Combo roles rails when approving entitlement (supervisor/entitlement owner)
- [AUTOID-1997](#): Api-configuration step in Deployer fails when public IP is used for target VMs
- [AUTOID-1999](#): JAS issue: after machine restarts, all UIHRData is not coming up
- [AUTOID-2004](#): Entitlements/unscored endpoint not working due to collision with entitlements/:id endpoint
- [AUTOID-2010](#): Bulk approval not working for entitlements - Application view
- [AUTOID-2011](#): Elastic search and filters not showing complete data (supervisor/entitlement owner)
- [AUTOID-2014](#): Bulk approval not working for entitlements - Employee details page
- [AUTOID-2015](#): Anomaly report is failing
- [AUTOID-2021](#): Dashboard - User type bug
- [AUTOID-2023](#): In Entity Definitions UI add Assignments section
- [AUTOID-2027](#): Enable additional attributes in assignments
- [AUTOID-2028](#): Assignments attributes marked as searchable should be saved to API config
- [AUTOID-2029](#): Change isinternal flag for usr_manager_id
- [AUTOID-2030](#): Modify UI behavior so that usr_manager_id can be changed
- [AUTOID-2032](#): Old colors user in dashboard → Most Critical Entitlements
- [AUTOID-2040](#): Remove reference to last_usage and is_assigned in autoid_es.json file
- [AUTOID-2046](#): Modify API to send assignment attributes with userDetails endpoint
- [AUTOID-2047](#): Modify employeeDetails page to enable optional attributes on assignment table
- [AUTOID-2064](#): Cassandra schema seeding fails if admin and user passwords are different
- [AUTOID-2065](#): Remove 'become:yes' from image-import.yml playbook
- [AUTOID-2068](#): Make firewall configuration in deployer optional
- [AUTOID-2077](#): Modify employeeDetails 'Not Scored' table to enable optional attributes

- [AUTOID-2094](#): API: Re-add singleViewWithApp/employees endpoint
- [AUTOID-2187](#): Overlapping text on user detail page

Known Issues

The following is a known issue in this release:

- [AUTOID-2209](#): Known issues: vault.yml passwords cannot contain special chars & or \$

Deprecated

Autonomous Identity 2021.3.0

- No functionality was deprecated in this release.

Removed

Autonomous Identity 2021.3.0

The following endpoints were removed in release 2021.3.0:

Companyview (/api/companyview)

- GET entitlementAvgGroupDetails Start End
- GET Assignments High Threshold
- GET Entitlements Without Owner
- GET Users without manager
- GET coverage
- GET companyViewEntitlements
- GET companyViewEmployeeTypes

Singleview with App (/api/singleViewWithApp)

- GET entitlements/:entitlementId

Roleowner with App (/api/roleOwnerWithAppOriented)

- All endpoints

Manager with App (/api/managers/WithAppOriented)

- All endpoints

Entitlements (/api/entitlements)

- GET Filters by Supervisor
- GET Filters by Entt Owners

Applications (/api/applications)

- GET filters

For more information, see [Autonomous Identity API Guide](#).

Documentation Updates

The following table tracks changes to the documentation set following the release of Autonomous Identity 2021.3.0:

Documentation Change Log

Date	Description
2022-08-22	Added a note about the latest security on log4j. Refer to Security Advisories .
2022-07-18	Added a note about log4j version 1. Refer to Security Advisories .
2022-06-14	Corrected the minimum storage requirements in the release notes: refer to Storage requirements .
2022-05-12	Made small changes to the Before you start section.
2022-02-09	Added a step to rename two files prior to upgrade, which will be overwritten in a later process. Refer to Upgrade Autonomous Identity .
2022-01-13	Updated the upgrade section to streamline processes. Refer to Upgrade Autonomous Identity .

Date	Description
2021-07-15	Updated the install instructions to indicate that the default shell for the <code>autoid</code> user is <code>bash</code> . Refer to Install a Single Node Deployment .
2021-07-13	The following doc changes were made:
2021-07-13	Changed a line in the air-gap setup instructions to set the <code>offline_mode</code> property in the <code>vars.yml</code> when setting up the tar file. Refer to Install a Single Node Air-Gapped Deployment or Install a Multi-Node Air-Gapped Deployment .

Date	Description
2021-06-28	<p data-bbox="379 203 1042 237">Initial release of Autonomous Identity 2021.3.1.</p> <p data-bbox="379 356 1078 389">The following documentation updates were made:</p> <ul data-bbox="411 434 1401 1733" style="list-style-type: none"> <li data-bbox="411 434 1305 517">• Updated the Admin Guide with updated instructions for Entity Definitions, Set Data Sources, and Set Attribute Mappings. <li data-bbox="411 539 1350 622">• Added a section on the default user permissions for Autonomous Identity. Refer to Appendix A: Default User Permissions. <li data-bbox="411 645 1358 678">• Fixed an air-gapped installation step. Refer to Prepare the Tar File. <li data-bbox="411 701 1401 784">• Added a prerequisite about Docker cluster IP addresses ranges. Refer to Install a Multi-Node Deployment. <li data-bbox="411 806 1358 889">• Removed the Lightweight deployment steps in the Getting Started Guide. <li data-bbox="411 911 1401 1039">• Removed Python 3.6 as an installation prerequisite. The Autonomous Identity deployer.sh uses Python 3.6 during installation and does not require that it exists on the target machine. <li data-bbox="411 1061 963 1095">• Made small changes to the API Guide. <li data-bbox="411 1120 1401 1202">• Added a prerequisite about enabling IPv4 forwarding in high-security environments. Refer to Install a Single Node Target. <li data-bbox="411 1225 1382 1308">• Added a new overview section on the Autonomous Identity security controls in the Deployment Planning Guide. <li data-bbox="411 1330 1286 1413">• Updated the Autonomous Identity port descriptions. Refer to Autonomous Identity Ports. <li data-bbox="411 1435 1358 1518">• Added sections on checking Cassandra, MongoDB and Spark after install. Refer to Install a Single Node Target. <li data-bbox="411 1541 1374 1624">• Added a known issue about vault passwords not containing special characters, & and \$. Refer to Known Issues. <li data-bbox="411 1646 1401 1729">• Added upgrade procedures to update Autonomous Identity 2021.3.0 to 2021.3.1.
2021-03-30	<p data-bbox="379 1794 1401 1877">Re-added the Data Preparation chapter to the Admin Guide. Refer to Data Preparation.</p>

Date	Description
2021-03-25	<p>Initial release of Autonomous Identity 2021.3.0.</p> <p>The following documentation updates were made:</p> <ul style="list-style-type: none"> • Updated the installation instructions for Autonomous Identity. For example, refer to Install a Single Node Deployment. • Updated the analytics procedures for Autonomous Identity. For more information, refer to Run Analytics. • Updated the upgrade procedure for Autonomous Identity. For more information, refer to Upgrade Autonomous Identity. • All guides have been updated to reflect the changes made in Autonomous Identity 2021.3.0.

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 **2021.3.0**.

Release Level Definitions

Release Label	Version Numbers	Characteristics
Major	Version: x[.0.0]	<ul style="list-style-type: none"> • 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

Release Label	Version Numbers	Characteristics
Minor	Version: x.y[.0]	<ul style="list-style-type: none"> • 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 month of the release, for example, 3 for March
Patch	Version: x.y.z	<ul style="list-style-type: none"> • 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.
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 <i>Deprecated</i> 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	<p>Technology previews provide access to new features that are considered as new technology that is not yet supported. Technology preview features may be functionally incomplete and the function as implemented is subject to change without notice. DO NOT DEPLOY A TECHNOLOGY PREVIEW INTO A PRODUCTION ENVIRONMENT.</p> <p>Customers are encouraged to test drive the technology preview features in a non-production environment and are welcome to make comments and suggestions about the features in the associated forums.</p> <p>ForgeRock does not guarantee that a technology preview feature will be present in future releases, the final complete version of the feature is liable to change between preview and the final version. Once a technology preview moves into the completed version, said feature will become part of the ForgeRock platform. Technology previews are provided on an “AS-IS” basis for evaluation purposes only and ForgeRock accepts no liability or obligations for the use thereof.</p>
Internal/Undocumented	<p>Internal and undocumented features or interfaces can change without notice. If you depend on one of these features or interfaces, contact ForgeRock support or email info@forgerock.com to discuss your needs.</p>

Appendix B: Getting Support

ForgeRock provides support services, professional services, training through ForgeRock University, and partner services to assist you in setting up and maintaining your deployments. For a general overview of these services, see <https://www.forgerock.com>.

ForgeRock has staff members around the globe who support our international customers and partners. For details on ForgeRock’s support offering, including support plans and service level agreements (SLAs), visit <https://www.forgerock.com/support>.

ForgeRock publishes comprehensive documentation online:

- The ForgeRock [Knowledge Base](#) offers a large and increasing number of up-to-date, practical articles that help you deploy and manage ForgeRock software.

While many articles are visible to community members, ForgeRock customers have access to much more, including advanced information for customers using

ForgeRock software in a mission-critical capacity.

- ForgeRock product documentation, such as this document, aims to be technically accurate and complete with respect to the software documented. It is visible to everyone and covers all product features and examples of how to use them.

Was this helpful?  

Copyright © 2010-2022 ForgeRock, all rights reserved.