Users Guide

/ Autonomous Identity 2020.10.2

Latest update: 2020.10.2

, , ,

Abstract

This guide provides an understanding on the ForgeRock Autonomous Identity UI, confidence scores and actionable items.

Table of Contents

Overview

This guide provides background information to understand how to read the Autonomous Identity UI, confidence scores, and different page views.

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

An entitlement refers to the rights or privileges assigned to a user or thing for access to specific resources. A company can have millions of entitlements without a clear picture of what they are, what they do, and who they are assigned to. Autonomous Identity solves this problem by using advanced artificial intelligence (AI) and automation technology to determine the full entitlements landscape for your company. The system also detects potential risks arising from incorrect or over-provisioned entitlements that lead to policy violations. Autonomous Identity eliminates the manual re-certification of entitlements and provides a centralized, transparent, and contextual view of all access points within your company.

Quick Start

Features Learn about the Autonomous Identity features.	The Autonomous Identity UI Get an overview of the Autonomous Identity's powerful UI.	Admin User Tasks Learn about the Company Overview page and the Admin tasks.
Supervisor Tasks Learn about the Employee Overview page and Supervisor tasks.	Application Owner Tasks Learn about the Applications page and application owner tasks.	Entitlement Owner Tasks Learn about the Entitlement Owner page and tasks.

Chapter 1
Features

Autonomous Identity provides the following features:

- **Broad Support for Major Identity Governance and Administration (IGA) Providers**. Autonomous Identity supports a wide variety of Identity as a Service (IDaaS) and Identity Management (IDM) data including but not limited to comma-separated values (CSV), Lightweight Directory Access Protocol (LDAP), human resources (HR), database, and IGA solutions.
- **Highly-Scalable Architecture**. Autonomous Identity deploys using a microservices architecture, either on-prem, cloud, or hybrid-cloud environments. Autonomous Identity's architecture scales linearly as the load increases.
- **Powerful UI dashboard**. Autonomous Identity displays your company's entitlements graphically on its UI console. You can immediately investigate those entitlement outliers as possible security risks. The UI also lets you quickly identify those entitlements that are good candidates for automated low-risk approvals or re-certifications. Users can also view a trend-line indicating how well they are managing their entitlements. The UI also provides an application-centric view and a single-page rules view for a different look at your entitlements.
- **Automated Workflows**. Autonomous Identity reduces the burden on managers who must manually approve new entitlements, for example, assigning access for new hires, by auto-approving high confidence, low-risk access requests and automate the re-certification of entitlements. Predictive recommendations lends itself well to automation, which saves time and cost.
- **Powerful Analytics Engine**. Autonomous Identity's analytics engine is capable of processing millions of access points within a short period of time. Autonomous Identity lets you configure the machine learning process and prune less productive rules. Customers can run analyses, predictions, and recommendations frequently to improve the machine learning process.
- **Powerful Explainable AI Algorithms**. The Analytics Engine provides transparent and explainable results that lets business users get insight into why the end-user has the access they have, or what access they should have.
- **Broad Database Support**. Autonomous Identity supports both Apache Cassandra and MongoDB databases. Both are highly distributed databases with wide usage throughout the industry.
- **Improved Search Support**. Autonomous Identity now incorporates Open Distro for Elasticsearch, a distributed, open-source search engine based on Lucene, to improve database search results and performance.

Chapter 2

Autonomous Identity User Types

Autonomous Identity recognizes six different user types, or personas, within its system. Each user type has access to certain pages on the Autonomous Identity console.

- **Admin**. An *Admin* user is similar to the notion of a system administration *superuser* within Autonomous Identity. Admins have access to every Autonomous Identity page view within the console. The Admin user can view the list of critical entitlements, approve or revoke access, and run other tasks.
- **Executive**. An *Executive* user is a senior manager within a company. Executives have access to the Autonomous Identity company overview page, critical entitlements, employee page, user entitlements page, but cannot approve or revoke access, or certify entitlements to users.
- **Supervisor**. A *Supervisor* user is one who has responsibility of other users or things and grants access to resources for these users. Supervisors can only see the entitlements of those users who report to them. They cannot view the entitlement assignments of users who report to another supervisor. Supervisors can certify entitlements assigned to users, entitlements to unscored users, and approve or revoke access.
- **Application Owner**. An *application owner* is any person or thing that owns an application and every entitlement within that application. A single entitlement can have an entitlement owner and an application owner. The application owner can have the permissions to approve, auto-certify entitlement assignments, and approve or revoke rule justifications.
- **Entitlement Owner**. An *Entitlement Owner* is one who has the ability to grant access to entitlements that they manage to other users. Entitlement owners can only view the entitlements that they created. Entitlement owners can certify the entitlements that they manage, users to these entitlements, and approve or revoke access to these entitlements.
- **User**. A *user* is any person or thing that has access to a resource. General users cannot access the system.

Table: Summary of Autonomous Identity Users and Accessible Views

User Type/View	Dashboard	Identities	Applications	Entitlements	Rules
Admin	✔	✔	✔	✔	✔
Executive	✔				
Supervisor		✔		✔	
Application Owner			✔	✔	✔

User Type/View	Dashboard	Identities	Applications	Entitlements	Rules
Entitlement Owner				✔	✔

Chapter 3

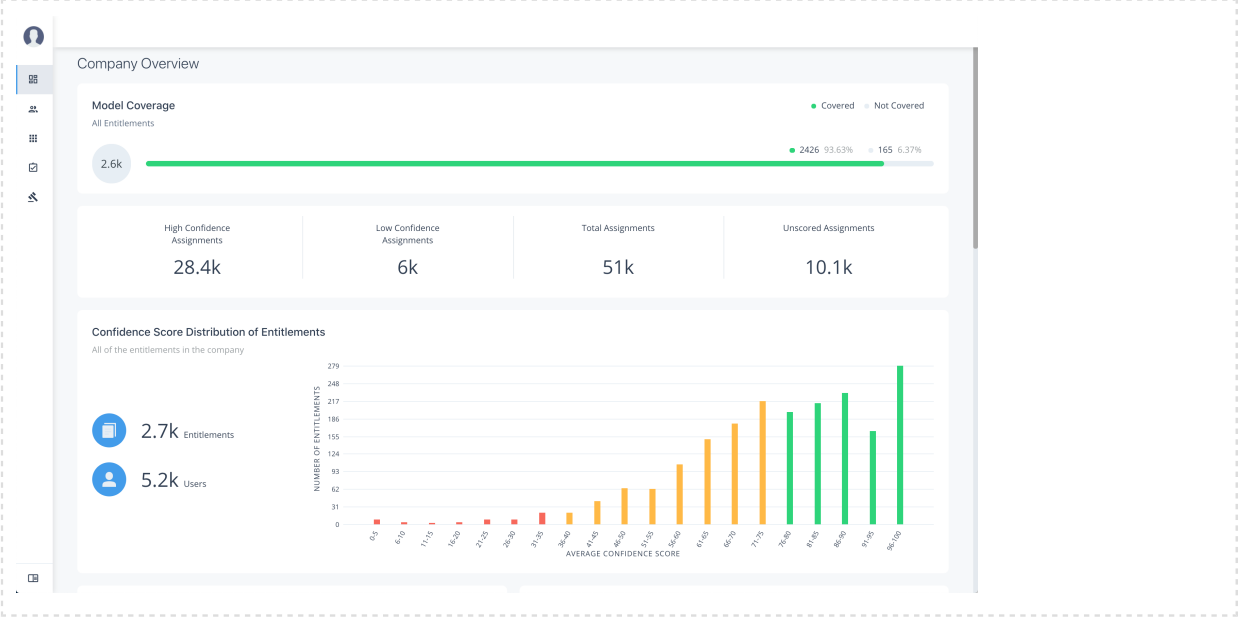
The Autonomous Identity UI

Autonomous Identity provides a powerful UI dashboard, displaying all of your entitlements, attributes, and confidence scores across your company. The UI provides different filtered levels of information depending on the user's access rights. For example, admin users can view all of the Autonomous Identity UI pages.

Dashboard

The Dashboard, also known as the Company View, provides a complete summary of your company's entitlements, confidences scores, and entitlement assignments. The page also shows the trend lines of your confidence score history over time. The navigation has a left-hand menu to go through each page. Only admin users and executives can view this page.

+ *Figure: Autonomous Identity Dashboard*



The Dashboard is partitioned into several modules as you scroll down:

- **Model Coverage**. Displays data on model coverage and confidence scoring of the assigned entitlements. The section summarizes the total number of entitlements processed by Autonomous Identity, and the number and percentage of those entitlements that were covered and not covered by the system. The section also displays a summary of entitlement *assignments*, specifically the number of High Confidence Assignments (90% and above), Low Confidence Assignments (20% and below), total assignments, and number of unscored entitlements. "Unscored" indicates that Autonomous Identity could not learn any patterns for a specific entitlement to properly assign a confidence score to it.

- **Confidence Score Distribution of Entitlements**. Displays a histogram of the distribution of confidence scores across your entitlements landscape. The chart provides a good summary of the current state of your entitlements landscape. In general, you want to set up your high confidence-scoring entitlements as candidates for automated approval and certification. You also want to move a good percentage of your middle level confidence scores to high confidence entitlements.

- **User Type**. Displays a summary of users versus non-users covered by the system.

- **Most Critical Entitlements**. Displays the list of the most critical entitlements with the low average confidence scores and the number of employees with the entitlement. You can drill down to view each entitlement, where you can approve or remove access to the entitlement for that user.

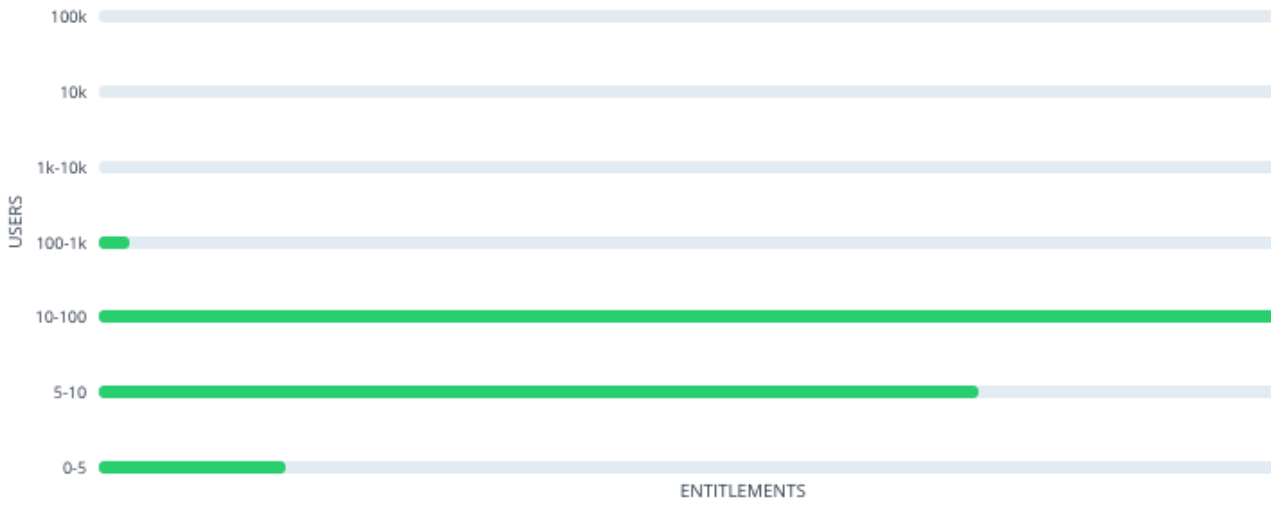
- **All Entitlements Distribution**. Displays the number of one-to-one matching and the highly assigned entitlements to distinct users.

  - **One-to-one matching** indicates the number of entitlement assigned to one user only.

  - **Highly Assigned** indicates the number of entitlements assigned to users. These highly-assigned entitlements are good candidates for automated access approval or certification using policies or roles.

  - **Graph of All Entitlements Distribution** displays a chart of the number of entitlements versus the number of users. The number range on the left (e.g., 0-5) indicate the number of entitlements assigned. The number on the right indicates the actual number of users. Thus, in the image below, there are 207 users who have 0-5 assigned entitlements. In the second row from the bottom, there are 979 users who have between 5-10 assigned entitlements. In the third row from the bottom, there are 1451 users who have between 10-100 assigned entitlements. In the fourth row from the bottom, there are 33 users who have betwen 100-1000 assigned entitlements.

An Example of the All Entitlements Distribution Graph



- **Entitlements Without Owners**. Displays the number of entitlements without an owner. This indicates that no user is managing this entitlement.
- **Users Without Supervisors**. Displays the number of users without a supervisor. This could indicate that a user was not properly set up or deprovisioned on your system.
- **History of Assignment Confidence Scores**. Displays a history of assigned confidence scores (high, medium, and low) over the past year versus the number of assignments. This graph shows the confidence score trends over time and indicates how well you are managing your entitlements. In general, you want rising high and mid confidence scores and decreasing low score trends.

Identities

The Identities page, formerly known as the Employee Overview/Supervisor view, displays a supervisor-based view of all user reporting to a specific supervisor and their entitlements. Admin users can see all supervisors and their users, while supervisors can only view their direct reports.

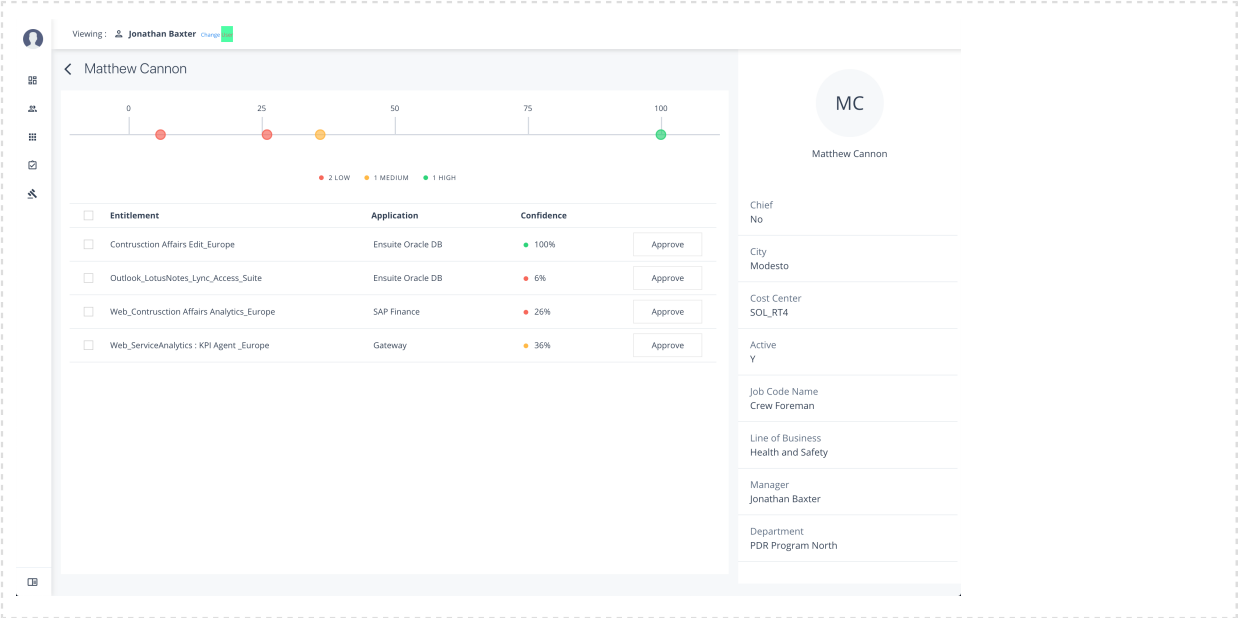
+ *The Autonomous Identity Identities Page.*

The Identities page is partitioned into several modules:

- **Total Number of Entitlements**. Displays the total number of entitlements assigned to users who report to the supervisor.
- **Total Number of Users**. Displays the total number of users that are assigned the entitlements.
- **Graph of Average Confidence Scores**. Displays a chart of the Average Confidence Scores versus the Number of Entitlements. You can hover over each circle to see the user's name, average confidence score, and number of entitlements assigned. If you double-click a circle, you can see the user's in the list on the right.
- **Filters**. Enable any of the application filters to display only those entitlements for the application. Enable the `Remove High Scores from Averages` filter to view only the mid and low confidence scores. Click the **Add Filters** button to filter the display based on User attributes, such as `city`.
- **List**. Displays a full list of users who have the assigned entitlements and their confidence scores. You can drill down and see each user's entitlements details by clicking on the user's name. To search for a specific user in the list, enter their name in the Search box above.

From the Identities page, you can view the user's detail by clicking a name in the right-hand menu. The User Detail is partitioned into several areas that display the following:

+ *The Autonomous Identity User Entitlements Detail Page.*



- **Not Scored**. Click the button to see any entitlements that were not scored by the system. Click Approve to approve or revoke the entitlement for the user.
- **Recommended**. Click the button to see any entitlements that were not assigned to the user but are a good candidate for the entitlement based on their attributes.

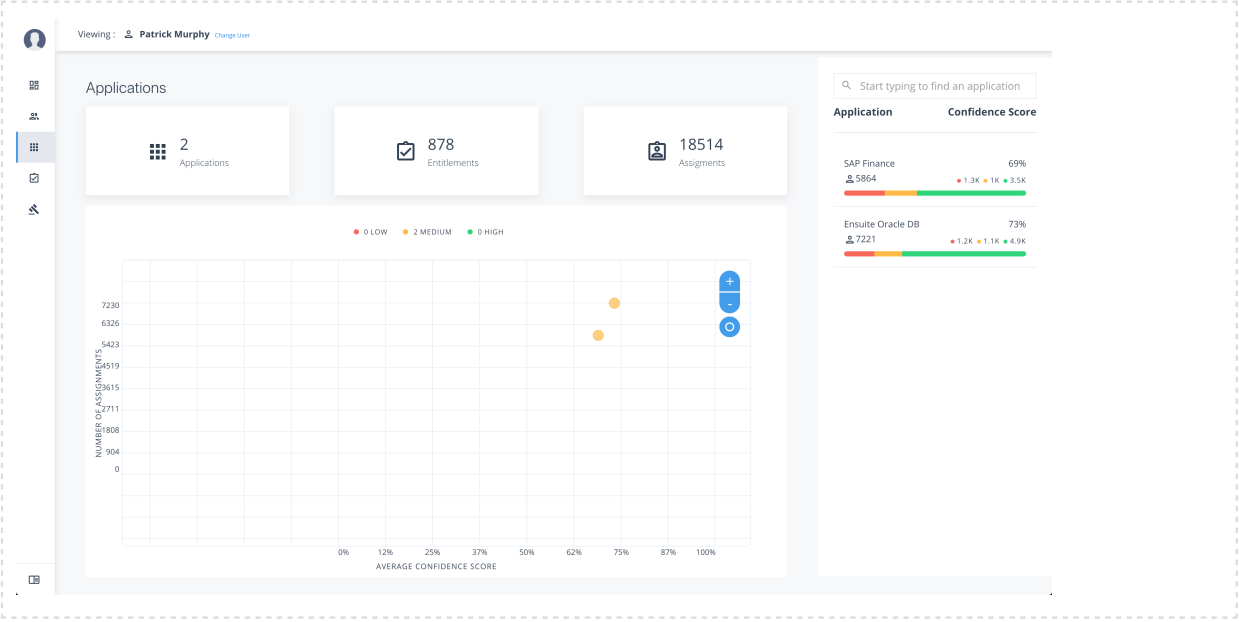
  Click the down arrow to review entitlement details that helps you

  - **Justifications**. Displays the attributes that lead to the confidence score.
  - **Driving Factor Comparison**. Displays a comparison of attributes and the driving factors that lead to a high confidence scored compared to the user's attribute values.
  - **Employees associated with the entitlement**. Displays the users, justifications, and confidence scores of users who also have the recommended entitlement.
- **Range of Confidence Scores**. Displays the low, medium, and high confidence scores for the assigned entitlements to the user. Click a circle to highlight the entitlement in the list below the graph.
- **Entitlements**. Displays the list of user's assigned entitlements, the application, and confidence score associated with the entitlement. Admins and supervisors can approve or revoke one or more entitlements for the user.
- **User Detail**. Displays the user's attributes as ingested from the company's HR database.

Applications

The Applications page provides an app-centric view for application owners and admin users to view the entitlements and assignments for an application. Admin users must enter the application owner to view the entitlement information on an application.

+ *The Autonomous Identity Applications Page*

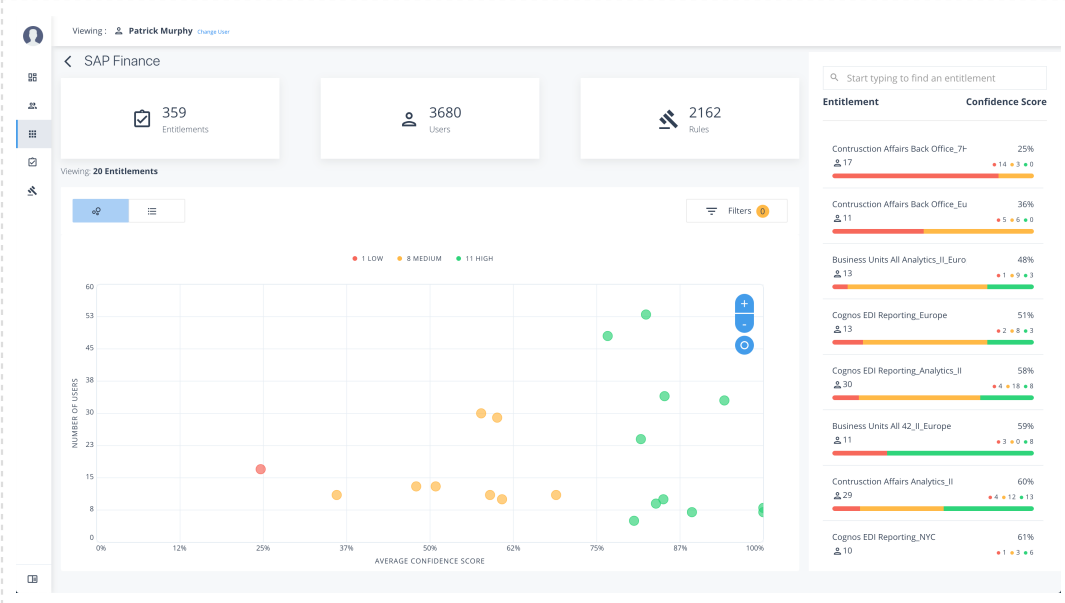


The Applications page is partitioned into several modules:

- **Total Number of Applications**. Displays the total number of applications for the application owner.
- **Total Number of Entitlements**. Displays the total number of entitlements that are associated with the applications.
- **Total Number of Assignments**. Displays the total number of entitlement assignments that are associated with the applications.
- **Graph of Average Confidence Scores**. Displays the Average Confidence Scores versus the Number of Assignments. You can hover over each circle to see the application's name, average confidence score, and number of users assigned to the application. If you double-click a circle, you can highlight an application on the right-hand list the list.
- **List of Application and Confidence Scores**. Displays the list of applications and confidence scores. If you click an application, you can drill down to the Application Detail page to see more information. To search through your list, enter an application name to access it.

Application Details page is partitioned into several modules:

+ *The Autonomous Identity Application Detail Page*



- **Total Number of Entitlements**. Displays the total number of entitlements associated with the application.
- **Total Number of Users**. Displays the total number of users who have access to the application.
- **Total Number of Rules**. Displays the total number of rules that are associated with the application.
- **Filters**. Displays options to filter the data based on entitlement attributes and user attributes.

  + *Click here to see a description of the filters*

  The Application filters let you filter the viewable entitlements based on the following attributes:

  - **Owner**. Filters the entitlements based on entitlement owner.
  - **Risk Level**. Filters the entitlements based on risk level: low, medium, and high.
  - **Criticality**. Filters the entitlements based on criticality of the entitlement: Essential or Non-Essential.

  You can also filter based on driving factor attributes:

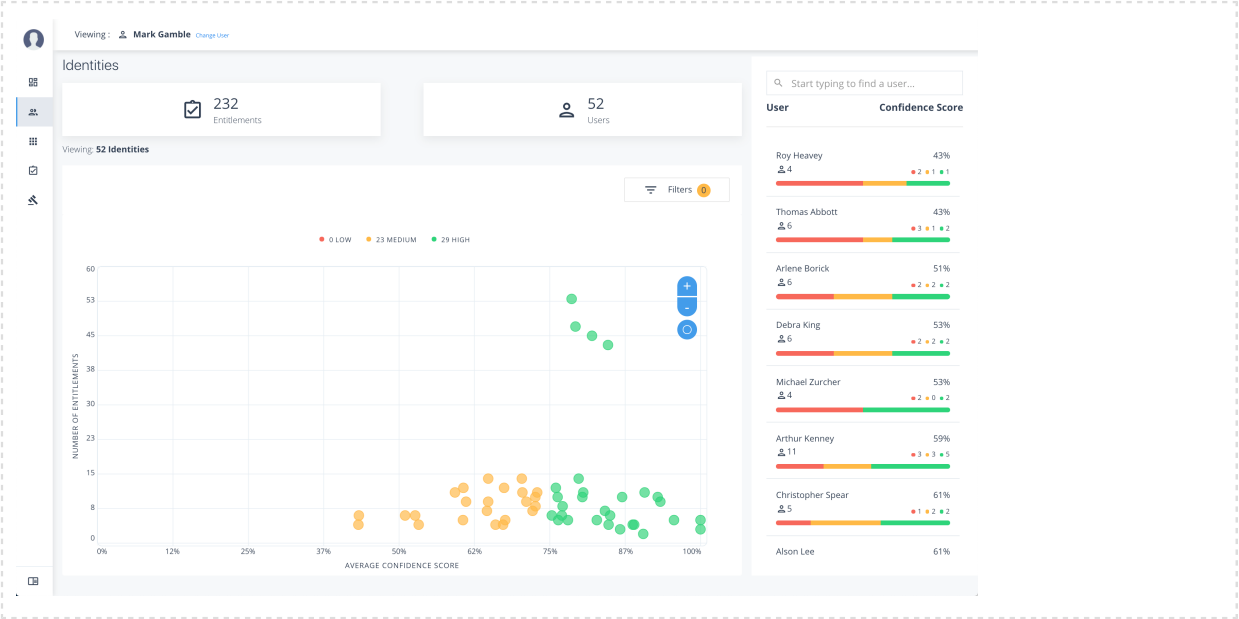
- **Manager Name**. Filters based on the manager's name. The menu displays the managers associated with the users who are assigned entitlements for the application.
- **Chief**. Filters based on if the user is a manager or not.
- **User Department Name**. Filters based on the department name. The menu displays the departments associated with the users who are assigned entitlements for the application.
- **Line of Business Subgroup**. Filters based on the Line of Business Subgroup. The menu displays the subgroups associatedwith the users who are assigned entitlements for the application.
- **Line of Business**. Filters based on the Line of Business. The menu displays the line of businesses associated with the users who are assigned entitlements for the application.
- **Cost Center**. Filters based on the cost center. The menu displays the cost centers associated with the users who are assigned entitlements for the application.
- **Job Code Name**. Filters based on the job code name. The menu displays the job code names associated with the users who are assigned entitlements for the application.
- **City** Filters based on the city. The menu displays the cities associated with the users who are assigned entitlements for the application.
- **User Employee Type**. Filters on user employee type, either `Employee` and `Non-Employee`.

- **Graph of Average Confidence Scores**. Displays the Average Confidence Scores versus the Number of Users. You have the option to view bubbles or a list view. You can hover over each circle to see the application's name to highlight it on the right-hand list. If you click list view, you can see the entitlement, user, confidence scores and an option to re-certify the entitlement for the user to access the application.
- **List of Entitlements and Confidence Scores**. Displays the list of entitlements and confidence scores for the application. If you click an entitlement, you can drill down to the Entitlement Detail page to see more information. To search for a specific entitlement, enter its name in the Search box.

Entitlements

The Entitlements page provides an entitlement-centric view of an owner's entitlements. Entitlement owners cannot see the entitlements of other owners. Admin users can access this page and must enter an entitlement owner to view a specific entitlement.

+ *The Autonomous Identity Entitlements Page*



The Entitlements page is partitioned into several modules as you scroll down:

- **Total Number of Entitlements**. Displays the total number of entitlements that the entitlement owner has responsibility for.
- **Total Number of Users**. Displays the total number of users that are assigned to the entitlements.
- **Graph of Average Confidence Scores**. Displays the Average Confidence Scores versus the Number of Users. You can hover over each circle to see the entitlement's name, average confidence score, and number of users with the assigned entitlement. If you double-click a circle, you can see the entitlement on the list on the right.
- **Filters**. Enable the `Remove High Scores from Averages` filter to view only the mid and low confidence scores. You can also filter based on one or more applications. Click Add Filters to further filter based on a user attribute, such as `city`.
- **List of Entitlements**. Displays a full list of entitlements and its average confidence score. You can drill down to see the details by clicking on the entitlement's name. To search for an entitlement, enter it in the Search box.

When you drill down to view a specific entitlement, the entitlement detail page is displayed with the following sections:

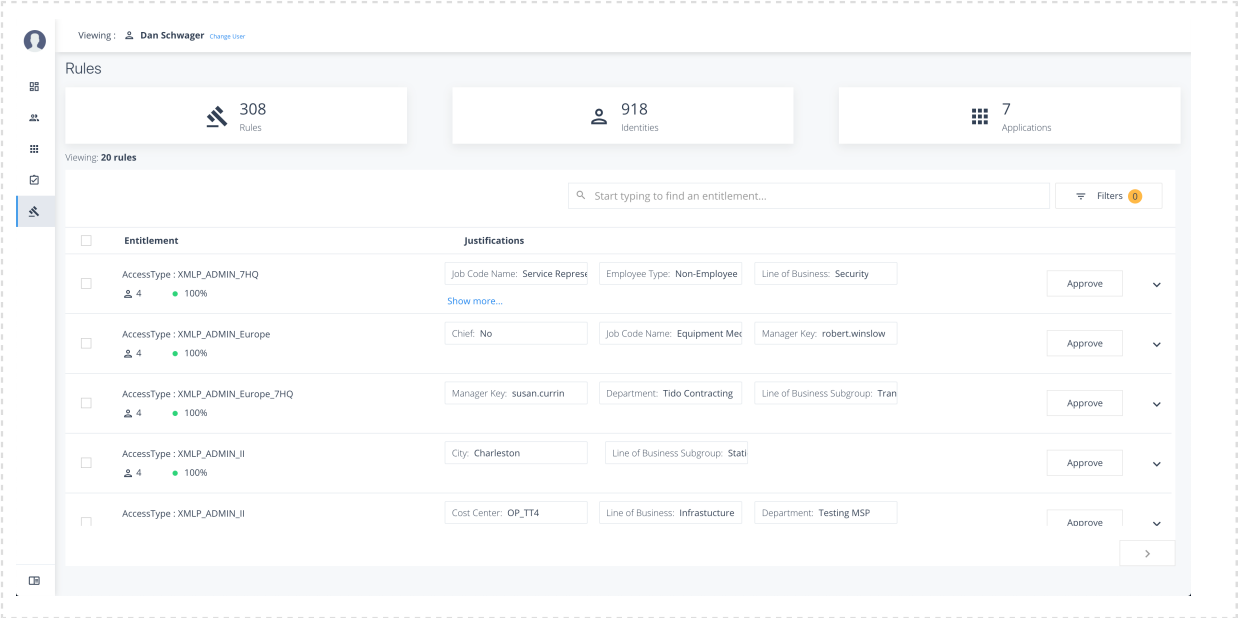
+ *The Autonomous Identity Entitlements Detail Page*

- **Average Confidence Score**. Displays the average confidence score for the entitlement.
- **Distribution of Users**. Displays the total number of users with the entitlements and the breakdown of low, medium, and high confidence scores.
- **Driving Factors**. Displays the driving factors, the attributes that lead to the confidence score. You can click the down arrow to see more information.
- **Graph of Average Confidence Score**. Displays a graph of the average confidence score versus the number of users with the confidence score. You can click one of the bars to highlight the justifications on the right-hand list.
- **List of Justifications**. Displays a list of justifications with the number of users and average confidence scores. You can click the right arrow to see the users with this entitlement and justifications. The checkbox next to each justification set lets you approve it. If you click a user's name, you can drill down to see the User Entitlements Detail page, which provides more detailed information from the user perspective.

Rules

The Rules page displays a rules-centric view of the entitlements for application and entitlement owners. Admin users must search for an application or entitlement owner to view a rule.

+ *The Autonomous Identity Rules Page*



The Rules page is partitioned into several modules as you scroll down:

- **Total Number of Rules**. Displays the total number of rules that the entitlement owner has responsibility for.
- **Total Number of Identities**. Displays the total number of identities that are assigned the entitlements.
- **Total Number of Applications**. Displays the total number of applications that are associated with the rules.
- **Filters**. Click Filters to view a segment of the total list. You can hide already reviewed auto-certified or auto-approved rules, low, medium, and high confidence scores, and by applications.
- **List of Entitlements and Justifications**. Displays the list of entitlements and their justifications. Entitlements with more than three justification attributes displays a `Show more` link. Application and entitlement owners can approve the entitlement based on the information displayed.

  Click the down arrow on the right to view the user attributes, driving factors, and values for a specific identity. If more than one users exists for that rule, you can change the user under the Identity drop-down list. The icons on the right indicate if a justification is appropriate for the entitlement or not. You can drill down to see the user's details by clicking the View <identity>.

Chapter 4

Admin User Tasks

The Admin user functionality is similar to that of a system administration *superuser*. Admin users have the access rights to company-wide entitlement data on the Autonomous Identity console. Admin users can approve or revoke a user's entitlement.

Performing Admin Tasks

+ *Investigate Most Critical Entitlements*

One important task that an administrator must perform is to examine all critical entitlements. Critical entitlements are assigned entitlements that have are highly-assigned but have a low confidence score associated with it. The Autonomous Identity console provides a means to examine these entitlements.

Follow these steps to evaluate the most critical entitlements list:

1. On the Dashboard, scroll down to the Most Critical Entitlements section. This section displays the entitlements that have low confidence scores and a high number of employees who have this entitlement.
2. Click an entitlement to view its details.
3. On the Entitlements detail page, review the key metrics.
4. Click the right arrow in one of the category ranges to view the users, and then click one of the users in the list.
5. On the User's Entitlements page, scroll down to review the Confidence Score Comparison table to see the differences between the user's attribute and the driving factor attributes.
6. Click Employees associated with this entitlement to review other uses who have this entitlement.
7. Click Actions, and then click Approve or Revoke for this entitlement. You can also bulk approve more than one entitlement. You can only revoke one entitlement at a time.

+ *Approve or Revoke Access an Entitlement for a User*

Follow these steps to investigate a confidence score and approve or revoke access an entitlement assigned to a specific user:

1. On Autonomous Identity console, click Identities, and enter a name of a supervisor. The only way to access a user's entitlements is through the Most Critical Entitlements section or the Identities page.
2. On the Identities page, click a circle, and then click the user in the list on the right.
3. On the User Entitlement page, click a confidence circle on the graph to highlight the entitlement below.
4. For the selected entitlement, click the down arrow on the right to view the Driving Factor Comparison.
5. Click Employees associated with this entitlement to view the justifications for those users with high confidence scores with this entitlement.
6. Click Actions, and then click **Approve Access** or **Revoke access**. If you have more than one entitlement that you want to approve, select them all and do a bulk Approval. You can only do one Revoke Access at a time.

+ *Check Non-Scored Users*

Follow these steps to check Not Scored entitlements. Not scored indicates that it does not have a justification associated with the entitlement:

1. On Autonomous Identity console, click Identities, and enter a name of a supervisor. The only way to access a user's entitlements is through the Most Critical Entitlements section or the Identities page.
2. On the Identities page, click a circle, and then click the user in the list on the right.
3. On the User Entitlement page, click Not Scored.
4. On the Not Scored Entitlements page, click the down arrow to view the driving factors comparison.
5. Click Employees associated with this entitlement to view the justifications for those users with high confidence scores with this entitlement.
6. Click Actions, and then click**Approve Access** or **Revoke access**. At a later date, you can re-click the Approve or Revoke button to cancel the operation.

+ *Apply Filters*

Follow these steps to apply filters to your confidence score graphs on the Identities and Entitlements pages:

Note

The Filters for the Identities and Entitlements are similar. The filters for the Applications and Rules pages offer different options to filter your searches.

1. On the Identities or Entitlements page, view the average confidence score graph.
2. On the right, click Filters.
3. Under filters, do one or all of the following:
    a. Click **Remove High Scores from Average** or enable any filter in the Application Filters section.
    b. Under Applications, click one or more applications to see the identities or entitlements asssociated with the selected application.
    c. Click Add Filters to further see only those identities or entitlements based on a user attribute, such as `city`. When ready, click Apply Filters.
4. Click Clear Filters to remove your filters.

Chapter 5
Supervisor Tasks

A Supervisor user is one who has responsibility of other users and grants or revoke access to resources for these users. A supervisor has access to the Employee Overview, User Detail, and User Entitlement Detail pages. Supervisors can only view their reports' information and cannot view the data of other supervisor's users.

Performing Supervisor Tasks

+ *Check Not Scored Users*

Follow these steps to check Not Scored entitlements. *Not scored* indicates that there are no justifications associated with the entitlement:

1. Log in to the Autonomous Identity console.
2. On the Identities page, click a circle, and then click the user in the list on the right.
3. On the User Entitlement page, click Not Scored.
4. On the Not Scored Entitlements page, click the down arrow to view the driving factors comparison table.
5. Click Employees associated with this entitlement to view the justifications for those users with this entitlement.
6. Click Actions, and then click **Approve Access** or **Revoke access**. At a later date, you can re-click the Approve or Revoke button to cancel the operation.

+ *View Recommended Entitlements*

Follow these steps to check Recommended entitlements.

The analytics engine determines if any entitlement, not currently assigned to a user, should be assigned to the user based on their attributes. Autonomous Identity generates a list of these *recommended* entitlements.

1. Log in to the Autonomous Identity console.

2. On the Identities page, click a circle, and then click the user in the list on the right.
3. On the User Entitlement page, click Recommended.
4. Review the recommended entitlement that Autonomous Identity determined was a good candidate for assignment to the user. Note that this page has no actions available since the entitlement is not assigned to the user. The page only presents information on the recommended entitlement.
5. Click the down arrow to view more information. View the Justifications that lead to the confidence score. Review the Driving Factor Comparison table. Click Employees associated with this entitlement to compare users with this entitlement.

+ *Approve or Revoke Access*

Follow these steps to investigate a confidence score and approve or revoke access an entitlement assigned to a specific user:

1. Log in to the Autonomous Identity console.
2. On the Identities page, click a circle, and then click the user in the list on the right.
3. On the User Entitlement page, click a confidence circle on the graph to highlight the entitlement below.
4. For the selected entitlement, click the down arrow on the right to view the Driving Factor Comparison.
5. Click Employees associated with this entitlement to view the justifications for those users with this entitlement.
6. Click Actions, and then click **Approve Access** or **Revoke access**.

+ *Apply Filters*

Follow these steps to apply filters to your confidence score graphs on the Identities page:

1. On the Identities page, view the average confidence score graph.
2. On the right, click Filters.
3. Under filters, do one or all of the following:
    a. Click **Remove High Scores from Average** or enable any filter in the Application Filters section.

b. Under Applications, click one or more applications to see the identities or entitlements asssociated with the selected application.

c. Click Add Filters to further see only those identities or entitlements based on a user attribute, such as `city`. When ready, click Apply Filters.

4. Click Clear Filters to remove your filters.

Chapter 6

Application Owner Tasks

The Applications lets an application owner view their applications and all associated entitlements.

Performing Application Owner Tasks

+ *View Applications*

Follow these steps to view applications:

1. As an Application Owner, log in to the Autonomous Identity console.
2. On the Applications page, click a circle in the graph or an application in the Applications list on the right.
3. On the Applications Detail page, review the information on the page: the number of entitlements associated with the application, the number of users, the number of rules, and a graph of the average confidence score versus number of users.
4. To view the list of entitlements for the application ordered by confidence score, click the list icon on the top left. From there, click Re-certify to approve the entitlement assignment for the application.

+ *Apply Filters*

Follow these steps to apply filters to your confidence score graphs:

1. Log in to the Autonomous Identity console.
2. On the Applications page, click **Filters**.
3. Under Entitlement Attributes, do one or all of the following:
    a. Click Owner to filter on the entitlement owner. You can make more than one selection.
    b. Click Risk Level to filter on low, high, and middle risk entitlements. You can make more than one selection.
    c. Click Criticality to filter on Essential or Non-Essential entitlements.

4. Under User Attributes, do one or all of the following:
   a. Click Manager to filter on a manager. You can make more than one selection.
   b. Click Chief to filter if the entitlement is manager or not.
   c. Click Department to filter on a specific department. You can make more than one selection.
   d. Click LOB Sub Group to filter on a line of business subgroup. You can make more than one selection.
   e. Click LOB to filter on the line of business for the division. You can make more than one selection.
   f. Click Cost Center to filter on a cost center. You can make more than one selection.
   g. Click Job Code Name to filter on a job code. You can make more than one selection.
   h. Click City to filter on the city of the operations. You can make more than one selection.
   i. Click Employee Type to filter Employee or Non-Employee.
5. Click Apply Filters to see the results on the graph. You can cancel your filters by click the `clear filters` link.

+ *Re-certify Entitlement Assignments*

Follow these steps to re-certify an entitlement assignment:

1. Log in to the Autonomous Identity console as an Application Owner.
2. On the Applications page, select an application to view by clicking a circle in the graph or the application on the right-hand menu.
3. Click list view.
4. Click Re-Certify, and then click Re-Certify again to confirm the assignment.

   You can also select all or multiple entitlements for bulk re-certify.

+ *Approve Rule Justifications*

Follow these steps to apply rule justifications for an entitlement:

1. Log in to the Autonomous Identity console.

2. Click Rules.
3. On the Rules page, select an entitlement to view, and then click the down arrow to see the driving factors for the entitlement.
4. Under Identity, change to see another user's attributes and driving factors. If you want to see the user's entitlements page, click View <User>.
5. After researching the entitlement, click Approve. Click Auto Certify or Auto Request or both, and enter a reason for the approval. Click Submit Approval when ready.

   You can also select all or multiple entitlements to do a bulk approve. Autonomous Identity only allows a single revoke action at a time.

   Note

   Auto Certify indicates that any user who has this justification is automatically approved for this entitlement. *Auto Request* indicates that anyone who matches these set of criteria and may not already have access, automatically gets provisioned for this entitlement.

Chapter 7

Entitlement Owner Tasks

An *Entitlement Owner* is one who has responsibility for a given access to a resource, but may not be a supervisor. Entitlement owners can only carry out tasks on those entitlements they are responsible for.

Performing Entitlement Owner Tasks

+ *Auto-Certify and Auto-Request an Entitlement*

Follow these steps to auto-certify and auto-request an entitlement:

1. Log in to the Autonomous Identity console as an Entitlement Owner.
2. On the graph, click a circle or click an entitlement in the right-hand list.
3. Review the details of the entitlement, especially the Driving Factors list.
4. Click the right arrow to view the users associated with the entitlement and confidence score. You can click a user to drill down to the Users Entitlements page.
5. Click the checkbox, and then Approve Justification to allow automated certifications and/or requests. Enter a reason for the approval and then click Submit Approval. You can cancel this auto certify or auto request transaction at any time.

Note

Auto Certify indicates that any user who has this justification is automatically approved for this entitlement. *Auto Request* indicates that anyone who matches these set of criteria and may not already have access, automatically gets provisioned for this entitlement.

+ *Apply Filters*

Follow these steps to apply filters to your confidence score graphs:

1. On the Entitlements page, view the average confidence score graph.

2. On the right, click **Filters**.
3. Do one or all of the following:
    a. Click Remove high scores from Averages.
    b. Click an application to filter the results.
    c. Click Add Filters to further filter on a user attribute.

+ *Approve or Revoke Access to an Assigned Entitlement*

Follow these steps to investigate a confidence score and approve or revoke access to an entitlement assigned to a specific user:

1. Log in to the Autonomous Identity console.
2. On the Entitlements page, click an entitlement to investigate on the list on the right. You can also type a specific entitlement in the Search box.
3. Click the down arrow under Driving Factor to review the key attributes that leads to the average confidence score.
4. Under Justification, click the right arrow to review the users who have the assigned attribute. Click a user to drill down to the User Entitlements page.
5. On the User Entitlements page, click one or more entitlements, and then click Actions to approve or revoke the entitlement or group of entitlements. You can select more than one entitlement for a bulk approve, or you can only revoke one entitlement as a time.

+ *Approve Rule Justifications*

Follow these steps to apply rule justifications for an entitlement:

1. Log in to the Autonomous Identity console.
2. Click Rules.
3. On the Rules page, select an entitlement to view, and then click the down arrow to see the driving factors for the entitlement.
4. Under Identity, change to see another user's attributes and driving factors. If you want to see the user's entitlements page, click View <User>.
5. After researching the entitlement, click Approve. Click Auto Certify or Auto Request or both, and enter a reason for the approval. Click Submit Approval when ready.

You can also select all or multiple entitlements to do a bulk approve. Autonomous Identity only allows a single revoke action at a time.

Note

Auto Certify indicates that any user who has this justification is automatically approved for this entitlement. *Auto Request* indicates that anyone who matches these set of criteria and may not already have access, automatically gets provisioned for this entitlement.

Glossary

anomaly report	A report that identifies potential anomalous assignments.
as-is predictions	A process where confidence scores are assigned to the entitlements that users have.
auto-certify	An action that an entitlement owner can do to approve a justification. Auto-certify indicates that anyone who has the justification is automatically approved for the entitlement.
auto-request	An action that an entitlement owner can do to approve a justification. Auto-request indicates that anyone who matches these justification attributes but may not already have access should automatically get provisioned for this entitlement.
confidence score	A score from a scale from 0 to 100% that indicates the strength of correlation between an assigned entitlement and a user's data profile.
data audit	A pre-analytics process that audits the seven data files to ensure data validity with the client.
data ingestion	A pre-analytics process that pushes the seven .csv files into the Cassandra database. This allows the entire training process to be performed from the database.
data sparsity	A reference to data that has null values. Autonomous Identity requires dense, high quality data with very few null values in the user attributes to get accurate analysis scores.
data validation	A pre-analytics process that tests the data to ensure that the content is correct and complete prior to the training process.

driving factor	An association rule that is a key factor in a high entitlement confidence score. Any rule that exceeds a confidence threshold level (e.g., 75%) is considered a driving factor.
entitlement	An entitlement is a specialized type of `assignment`. A user or device with an entitlement gets access rights to specified resources.
insight report	A report that provides metrics on the rules and predictions generated in the analytics run.
recommendation	A process run after the as-is predictions that assigns confidence scores to all entitlements and recommends entitlements that users do not currently have. If the confidence score meets a threshold, set by the `conf_thresh` property in the configuration file, the entitlement will be recommended to the user in the UI console.
resource	An external system, database, directory server, or other source of identity data to be managed and audited by an identity management system.
REST	Representational State Transfer. A software architecture style for exposing resources, using the technologies and protocols of the World Wide Web. REST describes how distributed data objects, or resources, can be defined and addressed.
stemming	A process that occurs after training that removes similar association rules that exist in a parent-child relationship. If the child meets three criteria, then it will be removed by the system. The criteria are: 1) the child must match the parent; 2) the child (e.g., [San Jose, Finance]) is a superset of the parent rule. (e.g., [Finance]); 3) the child and parent's confidence scores are within a +/- range of each other. The range is set in the configuration file.
training	A multi-step process that generates the association rules with confidence scores for each entitlement. First, Autonomous Identity models the frequent itemsets that appear in the user attributes for each user. Next, Autonomous Identity merges the user attributes with the entitlements that were assigned to the user. It then applies association rules to model the sets of user attributes that result in an entitlement access and calculates confidence scores, based on their frequency of appearances in the dataset.