

Users' Tasks

This chapter provides background information to understand how to read the Autonomous Identity UI, confidence scores, and different page views for non-administrators.



Features

Learn about the Autonomous Identity features.



User Types

Learn about Autonomous Identity user types.



The UI

See an overview of Autonomous Identity's UI.



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.

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 supports scalable reads and writes for efficient processing.
- **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.
- **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.
- **UI-Driven Schema Extension.** Autonomous Identity lets administrators discover and extend the schema, and set up attribute mappings using the UI.
- **UI-Driven Data Ingestion and Mappings.** Autonomous Identity provides improved data ingestion tools to define multiple csv input files needed for analysis and their attribute mappings to the schema using the UI.
- **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.

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 have created. Entitlement owners can certify the entitlements that they manage, users to these entitlements, and approve or revoke access to these entitlements.
- **Role Engineer.** A *Role Engineer*
- **Role Owner.** A *Role Owner*
- **Role Auditor.** A *Role Auditor*
- **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	Roles	Rules
Admin	✓	✓	✓	✓	✓	✓
Executive	✓					
Supervisor		✓		✓	❓[1]	
Application Owner			✓	✓	❓[1]	✓
Entitlement Owner				✓	❓[1]	✓

[1] If assigned a Roles user type: Roles Engineer, Roles Owner, or Roles Auditor

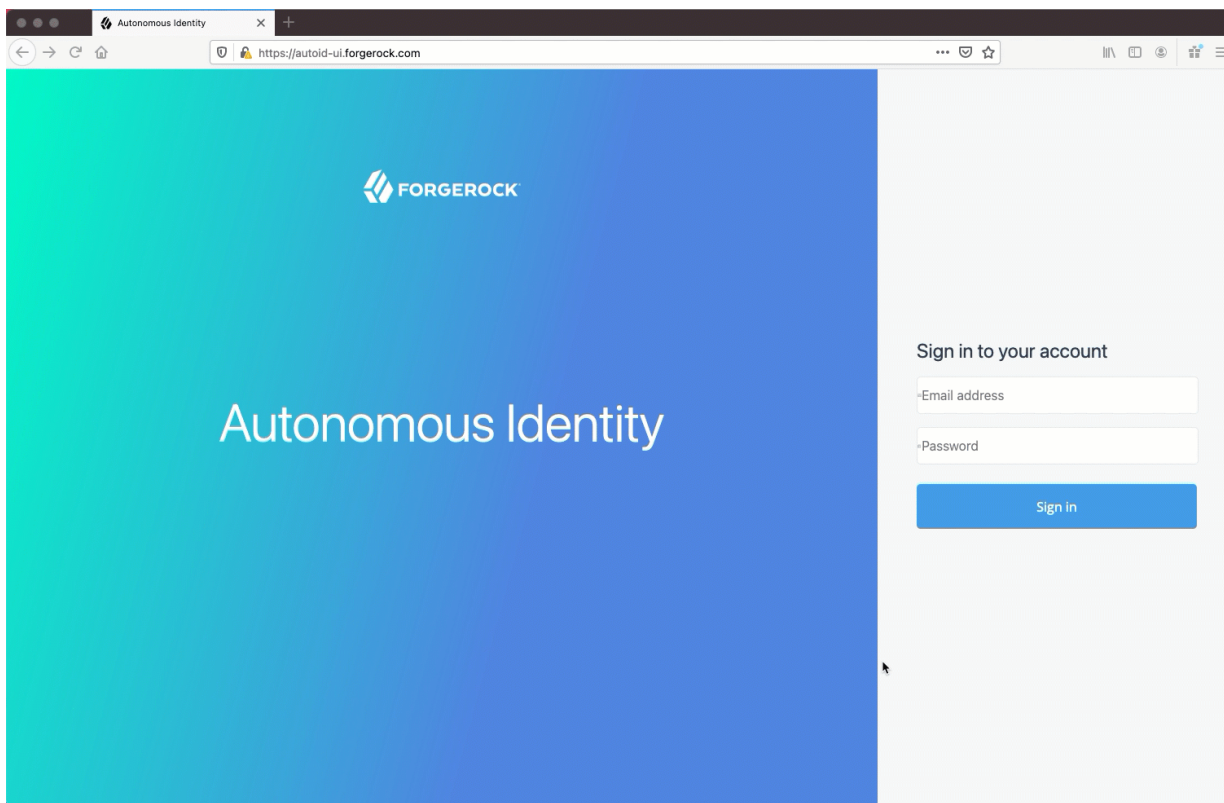
The Autonomous Identity UI

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.

Dashboard

The Dashboard, also known as the *Company Overview*, provides a complete summary of your organizations's entitlements, confidences scores, and entitlement assignments. Only admin users and executives can view this page. The page also shows the trend lines of your confidence score history over time plus a list of the Most Critical Entitlements.

▼ [See a tour of the 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 assigned 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 a number of distinct users listed below. 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 between 100-1000 assigned entitlements.



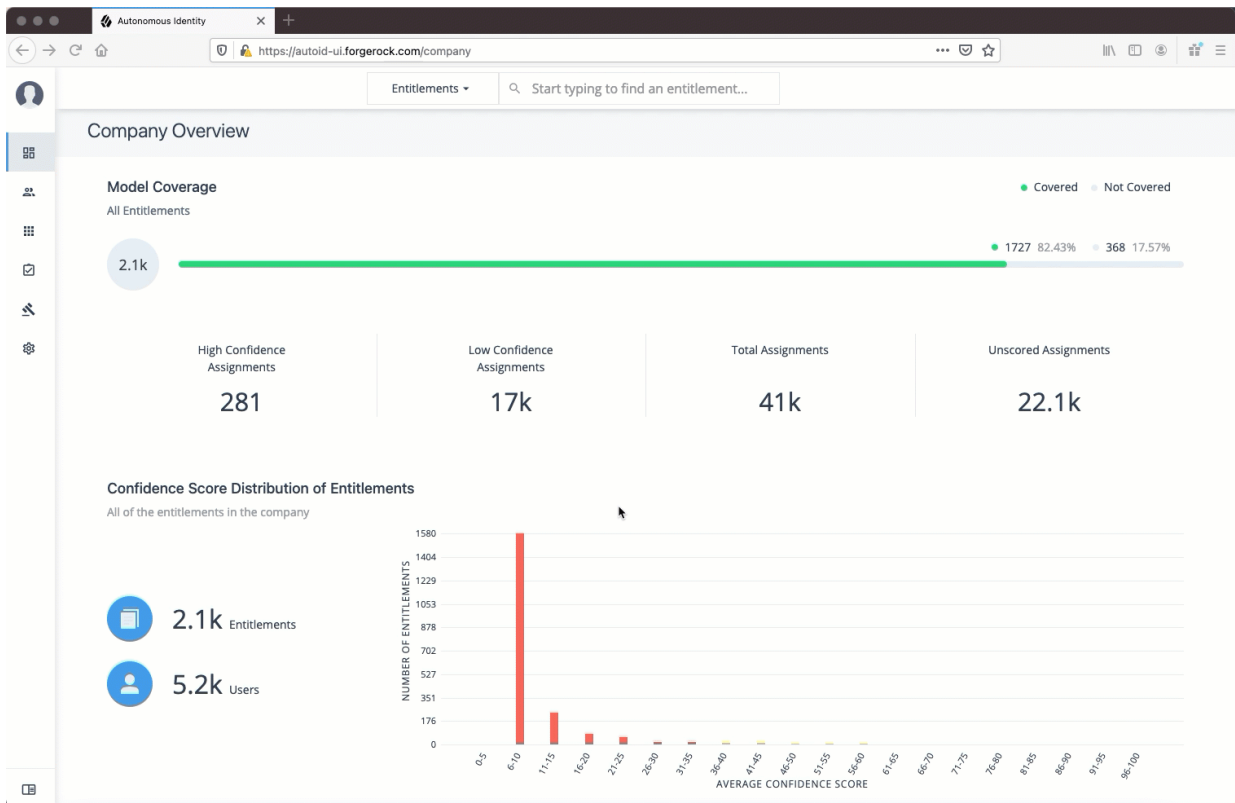
Figure 1. An Example of the All Entitlements Distribution Graph

- **History of Assignment Confidence Scores.** Displays a history of assigned confidence scores (high, medium, and low) over the past year (in months) versus the number of assignments. The time range on the x-axis shows the month and year for a specific range 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 displays a supervisor-based view of all users 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.

▼ [See a tour of the Autonomous Identity Identities Page](#)

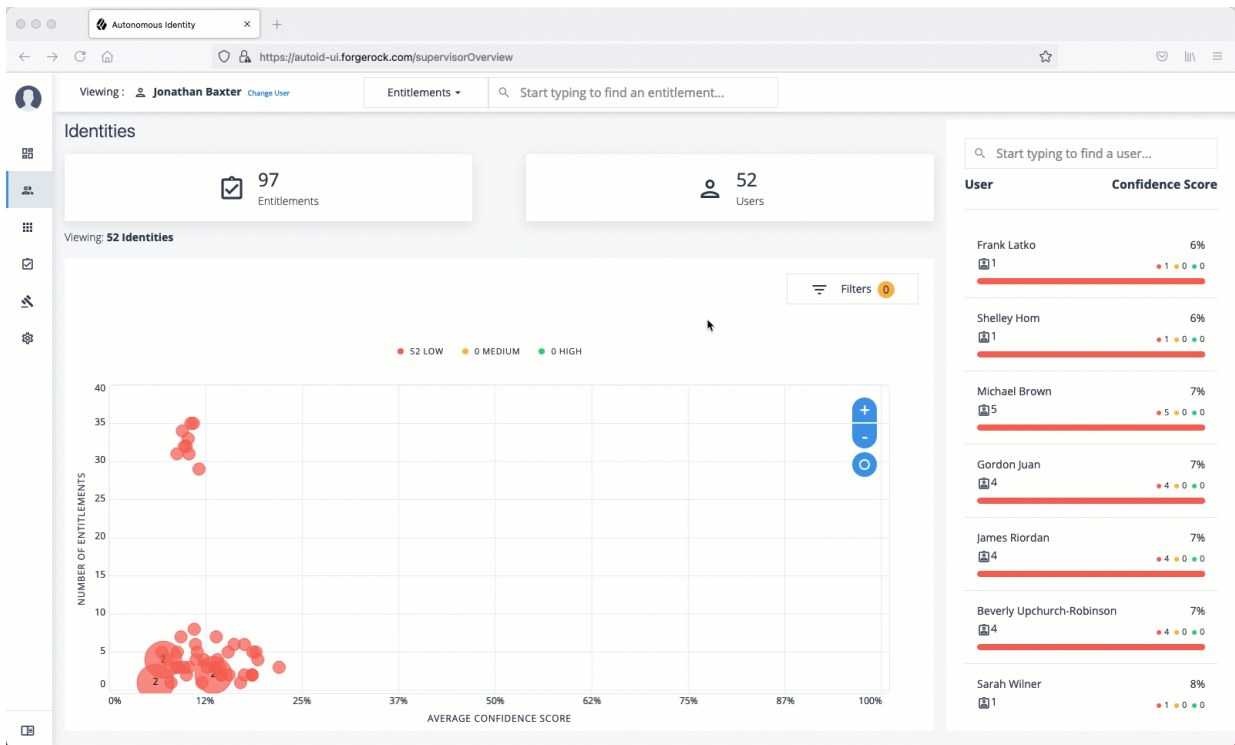


The Identities page is partitioned into several modules:

- **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 select the user in the list on the right.
- **Filters.** Enable any of the application filters to display only those entitlements for a specific application. Enable the **Remove High Scores from Averages** filter to view only the mid and low confidence scores.
- **List of Users.** 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 Details page by clicking a name in the right-hand menu, or by clicking the drop-down search at the top, select **User**, and enter the user's name.

▼ [See a tour of the Autonomous Identity User Details Page](#)



The User Detail is partitioned into several areas that display the following:

- **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 good candidates to assign to the user.
- **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.
- **Display Filter.** Displays a filter that matches any features set in the Assignments entity definition. This filter is also present on the Not Scored and Recommended pages.
- **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.

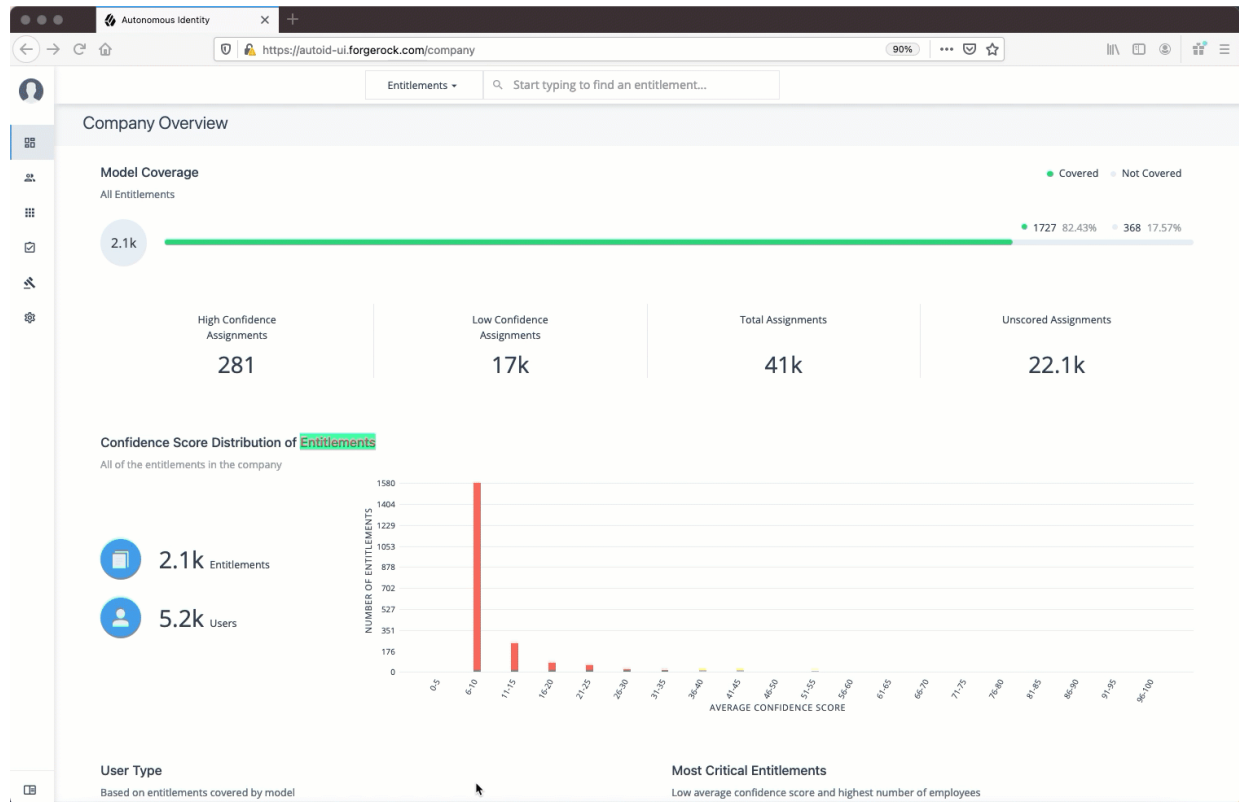
Click the down arrow to review entitlement details that helps you run the following:

- **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.
- **User Detail.** On the right, the page displays 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.

▼ [See a tour of the Autonomous Identity User Entitlements Detail Page](#)

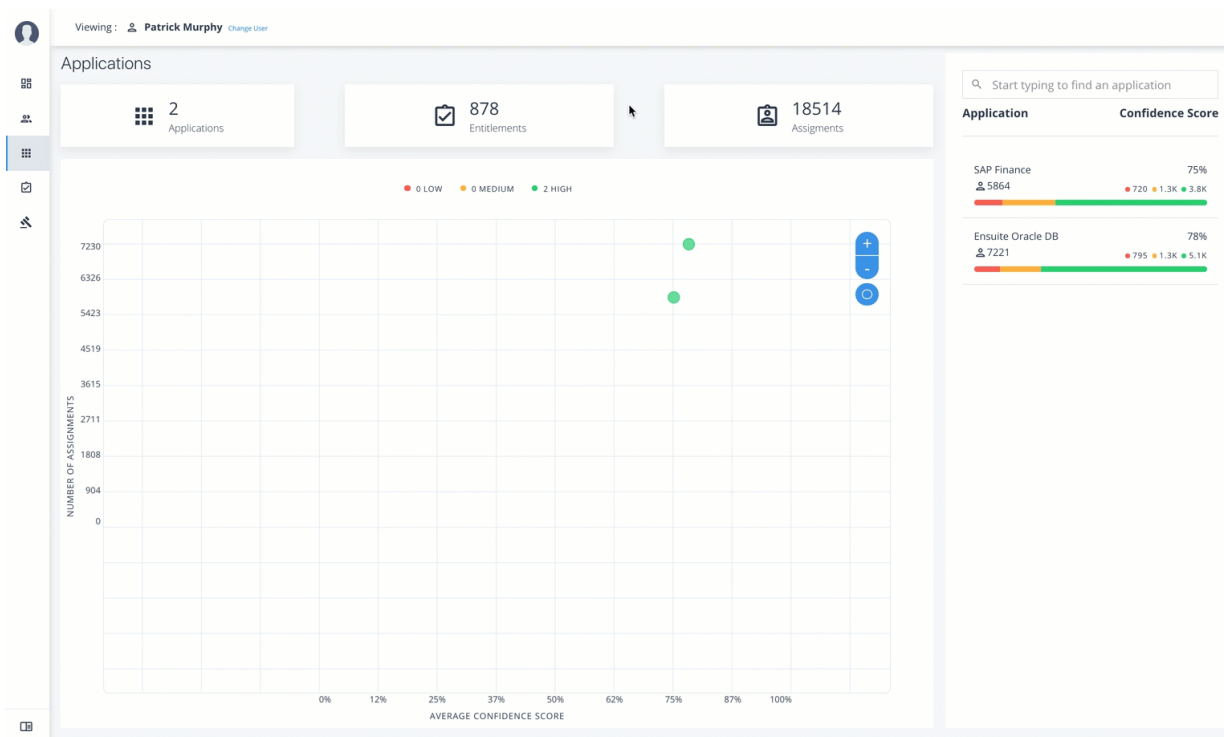


The Applications page is partitioned into several modules:

- **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 Details 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:

▼ [See a tour of 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:

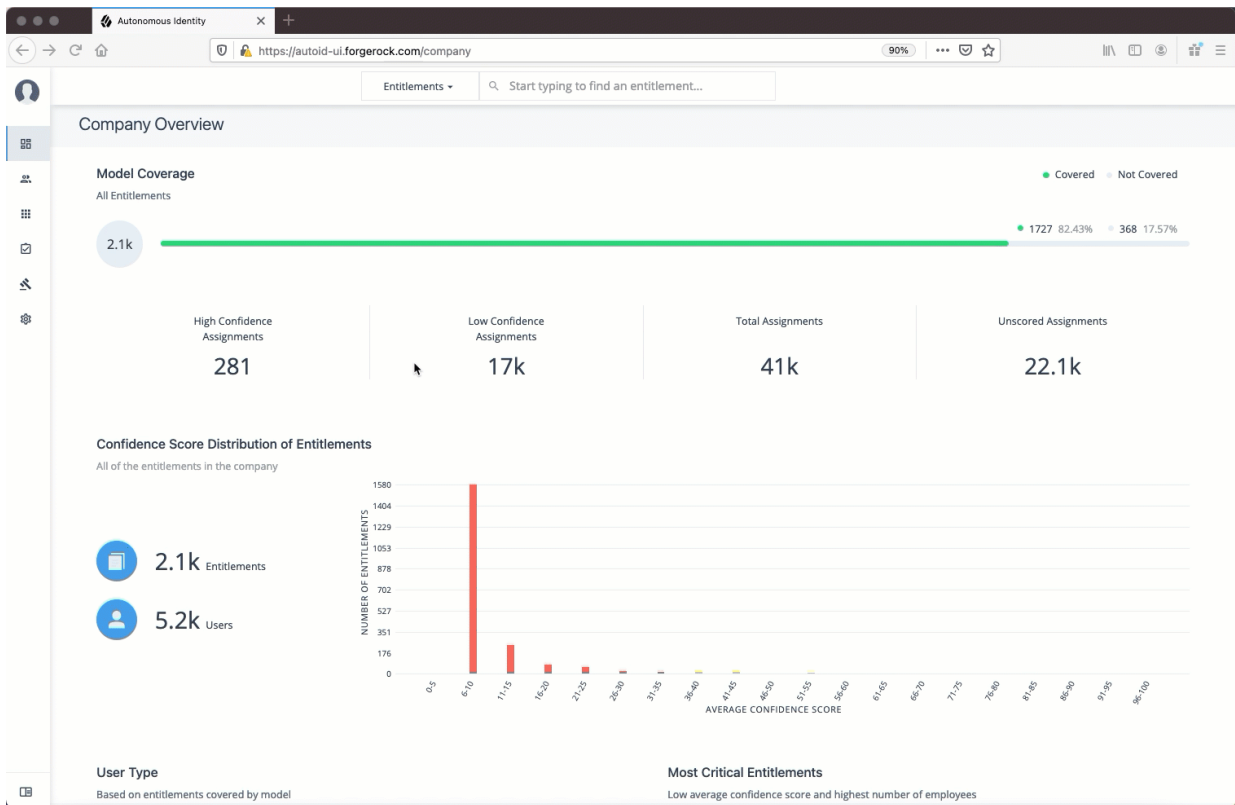
- **Manager Name.** Filters based on the manager's name. The menu displays the managers associated with the users who are assigned entitlements for the application.

- **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 associated with 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 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.

▼ [See a tour of the Autonomous Identity Entitlements Page](#)

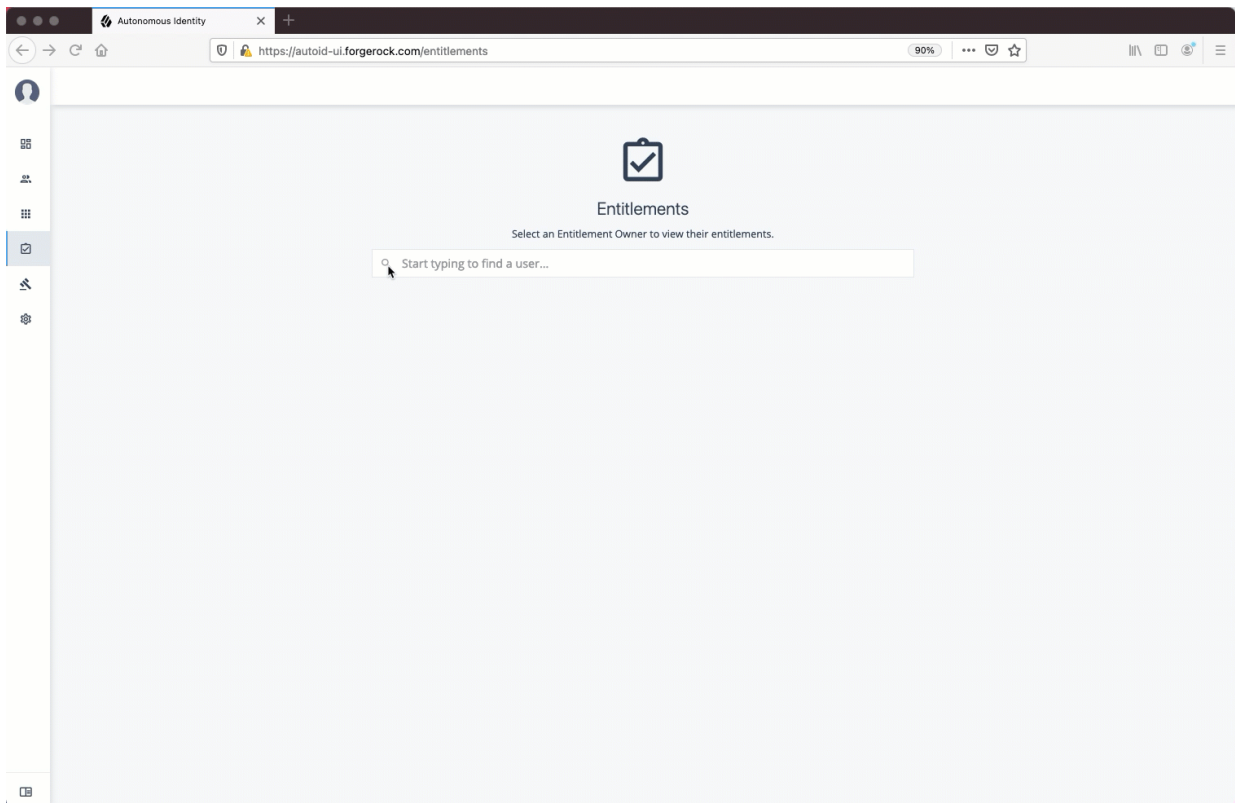


The Entitlements page is partitioned into several modules as you scroll down:

- **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 Entitlement Details page 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 Details page is displayed with the following sections:

▼ [See a tour of the Autonomously Identity Entitlement Details 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.

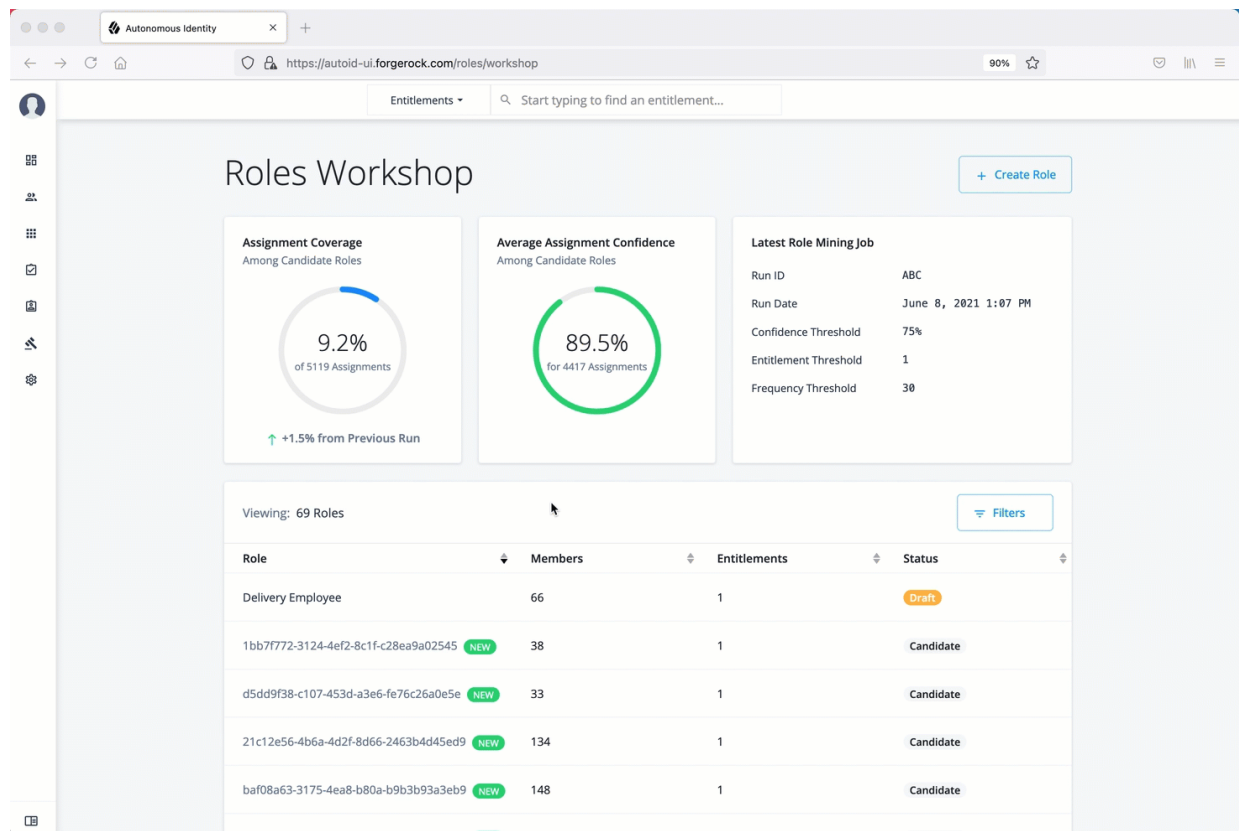
Roles

Autonomous Identity introduces new UI pages, Roles Workshop and Roles Catalog pages for authorized users to work on new and current roles assignments.

The Roles Workshop provides a UI where authorized users can view, create, or edit any roles based on Autonomous Identity's latest role mining job. The page provides a what-if scenario with confidence scores based on the addition or removal of justifications. The Roles Workshop also displays a list of recommended roles that were discovered in

the most recent role mining job.

▼ [See a tour of the Roles Workshop](#)



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

- **Assignment Coverage.** Displays data on average coverage percentage of the candidate roles to the total number of roles assigned. The model also displays any increase or decrease from the previous mining run.
- **Average Assignment Confidence.** Displays the average assignment confidence score to total assignment among the candidate roles.
- **Latest Role Mining Job.** Displays a timestamp for the latest role mining job along with confidence, entitlement, and frequency thresholds.
- **Table of Candidate Roles.** Displays a table of candidate roles discovered in the latest role mining job. The table displays the role, number of members associated with the role, number of entitlements in the role, and the status. The status displays the different workflow stages for the role.
 - **Candidate.** Indicates the recommended role discovered in the role mining run. Role engineers or role owners can review the candidate and approve the role to a draft status.
 - **Draft.** Indicates that the recommended role is in a draft state and requires review by an approver.
 - **Active.** Indicates that the role is ready for production use.

The Roles Catalog page displays a history of your roles include the role name, number of members, number of entitlements, and current status. You can filter your list of roles based on name, application, role owner, or origin.

▼ [See a tour of the Roles Catalog](#)

The screenshot shows the 'Roles Workshop' page. At the top, there are three summary cards:

- Assignment Coverage:** 9.2% of 5119 Assignments. A note indicates a +1.5% increase from the previous run.
- Average Assignment Confidence:** 89.5% for 4417 Assignments.
- Latest Role Mining Job:** Run ID: ABC, Run Date: June 8, 2021 1:07 PM, Confidence Threshold: 75%, Entitlement Threshold: 1, Frequency Threshold: 30.

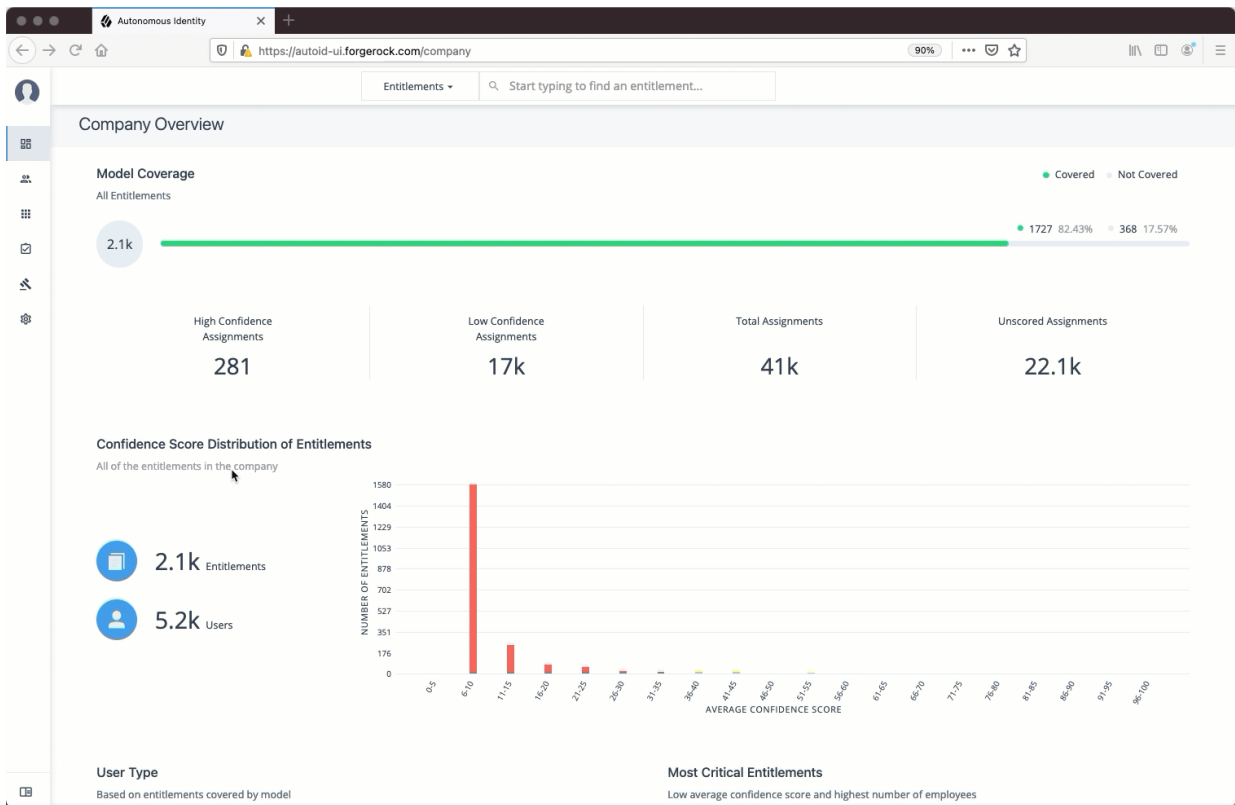
Below the cards is a table showing a list of roles. The table has columns for Role, Members, Entitlements, and Status. The first row is 'Delivery Employee' with 66 members and 1 entitlement, in a 'Draft' status. The following four rows are marked as 'NEW' and have 'Candidate' status.

Role	Members	Entitlements	Status
Delivery Employee	66	1	Draft
1bb7f772-3124-4ef2-8c1f-c28ea9a02545 NEW	38	1	Candidate
d5dd9f38-c107-453d-a3e6-fe76c26a0e5e NEW	33	1	Candidate
21c12e56-4b6a-4d2f-8d66-2463b4d45ed9 NEW	134	1	Candidate
baf08a63-3175-4ea8-b80a-b9b3b93a3eb9 NEW	148	1	Candidate

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.

▼ [See a tour of 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 <user identity>.

Supervisor Tasks

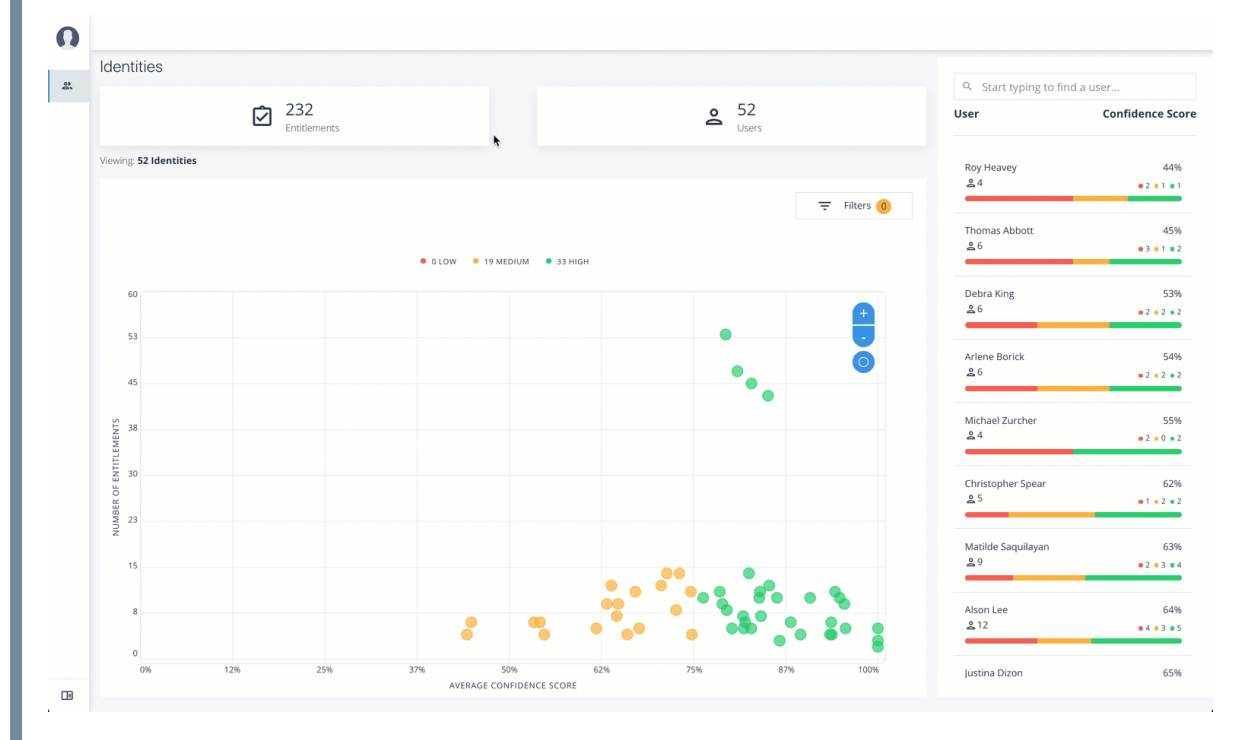
A Supervisor user is one who has responsibility of other users and grants or revoke access to resources for these users. A supervisor has access to the Employee Overview, User Detail, and User Entitlement Detail pages. Supervisors can only view their reports' information and cannot view the data of other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

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.

▼ [See it in action](#)



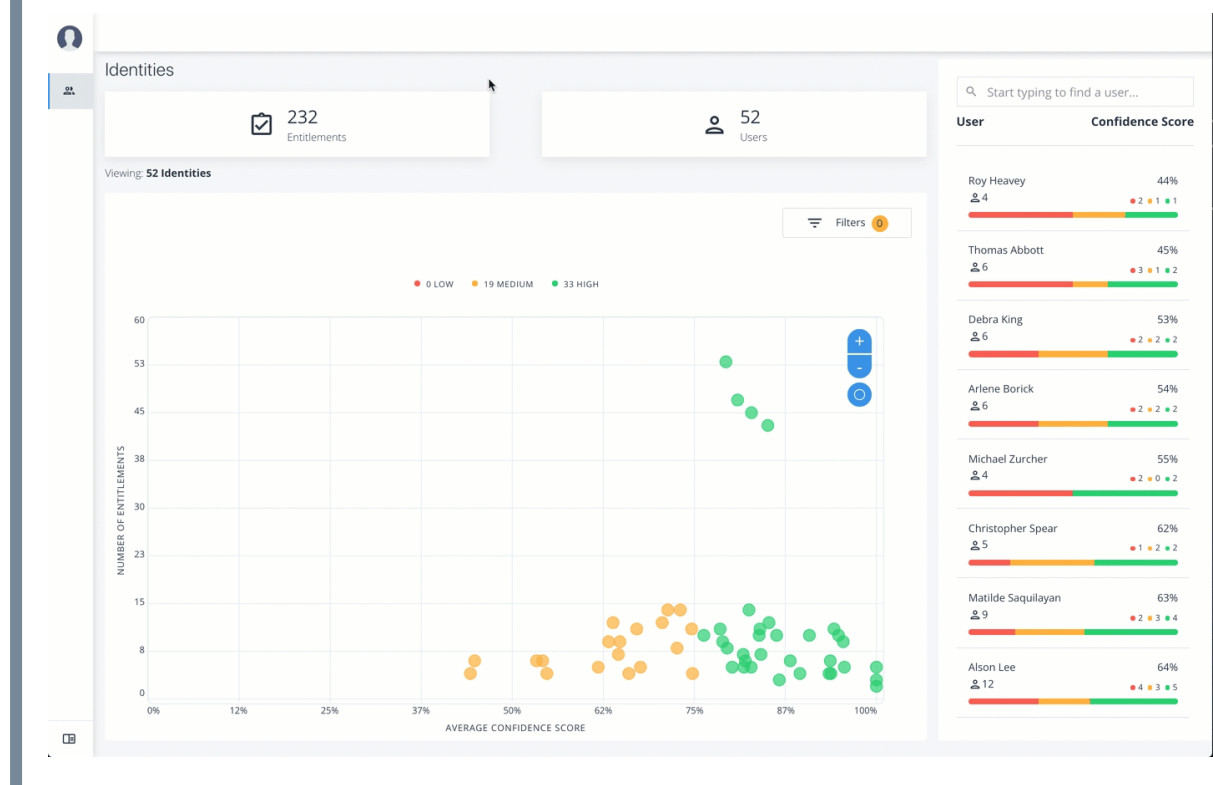
View Recommended Entitlements

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.

▼ [See it in action](#)

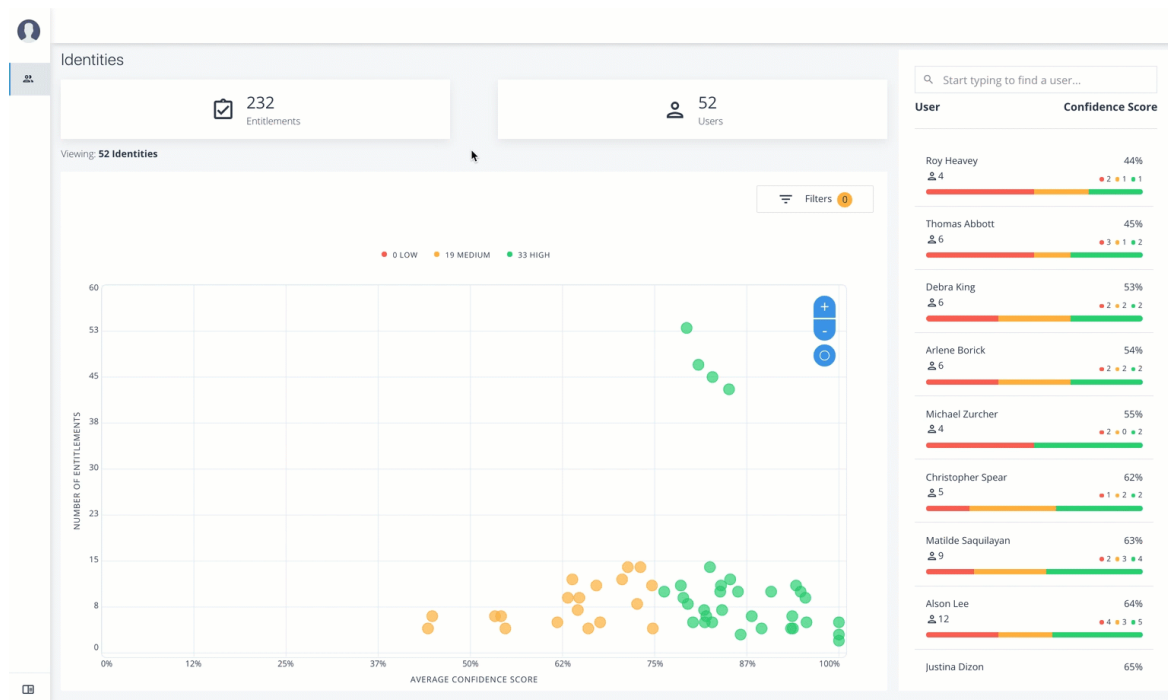


Approve or Revoke Access

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**.

▼ [See it in action](#)



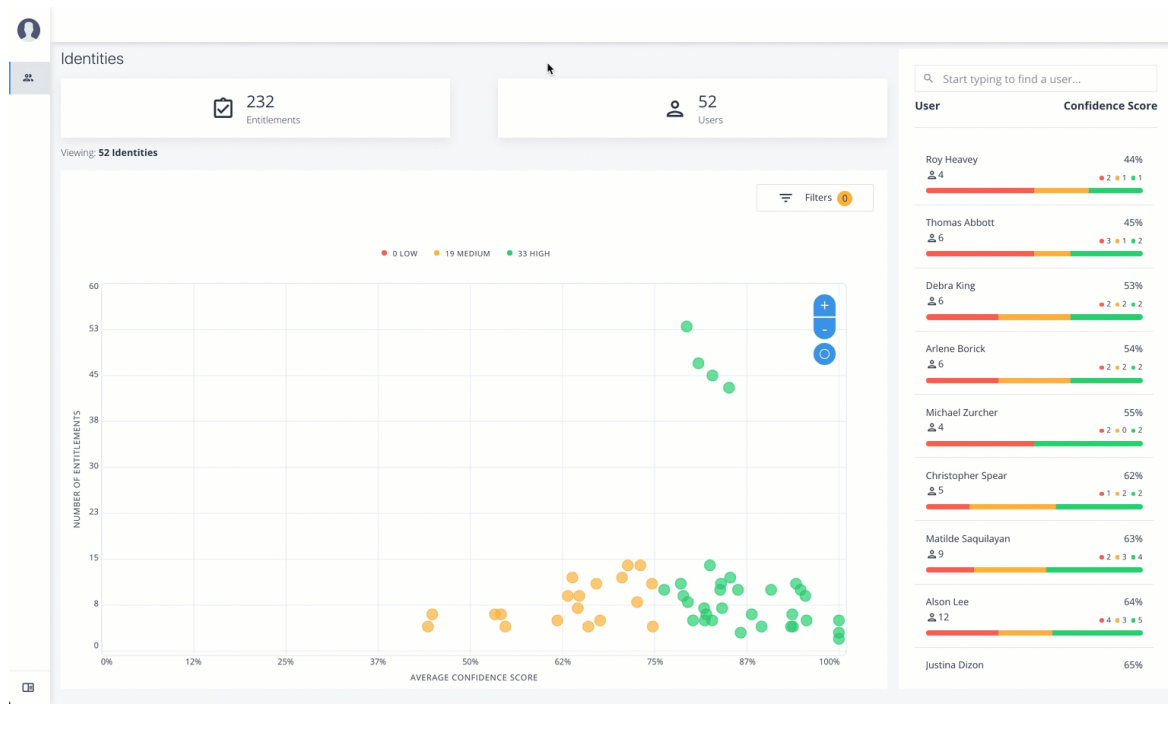
Apply Filters

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:
 - Click **Remove High Scores from Average** or enable any filter in the Application Filters section.

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

▼ [See it in action](#)



Application Owner Tasks

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

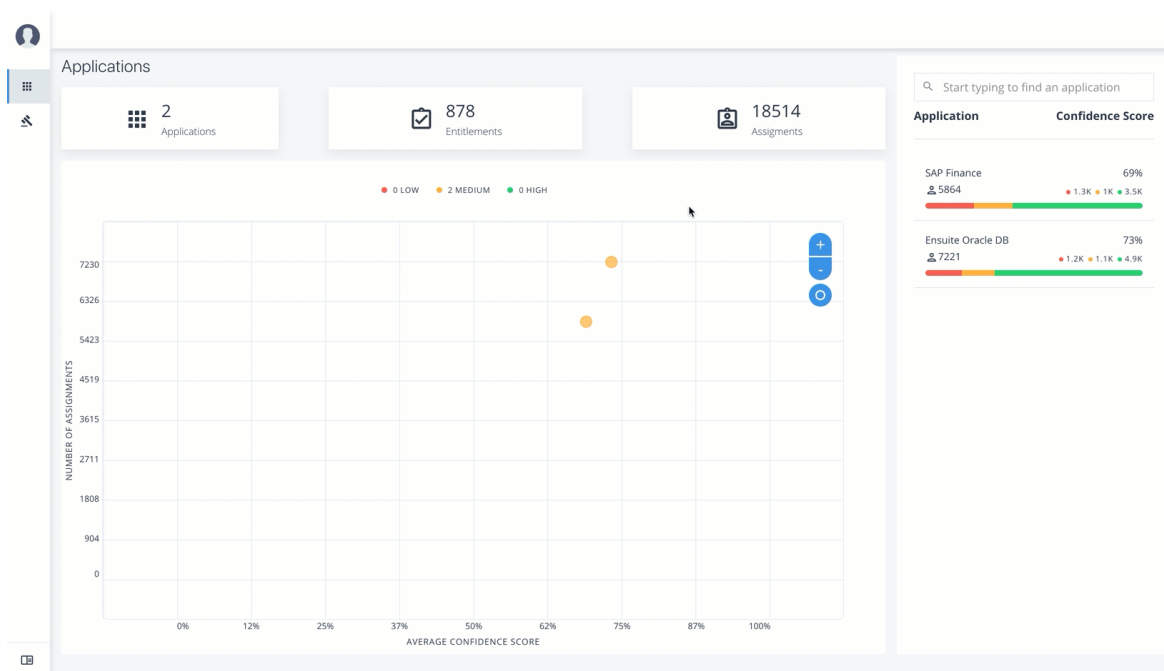
View Applications

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.

▼ [See it in action](#)



Apply Filters

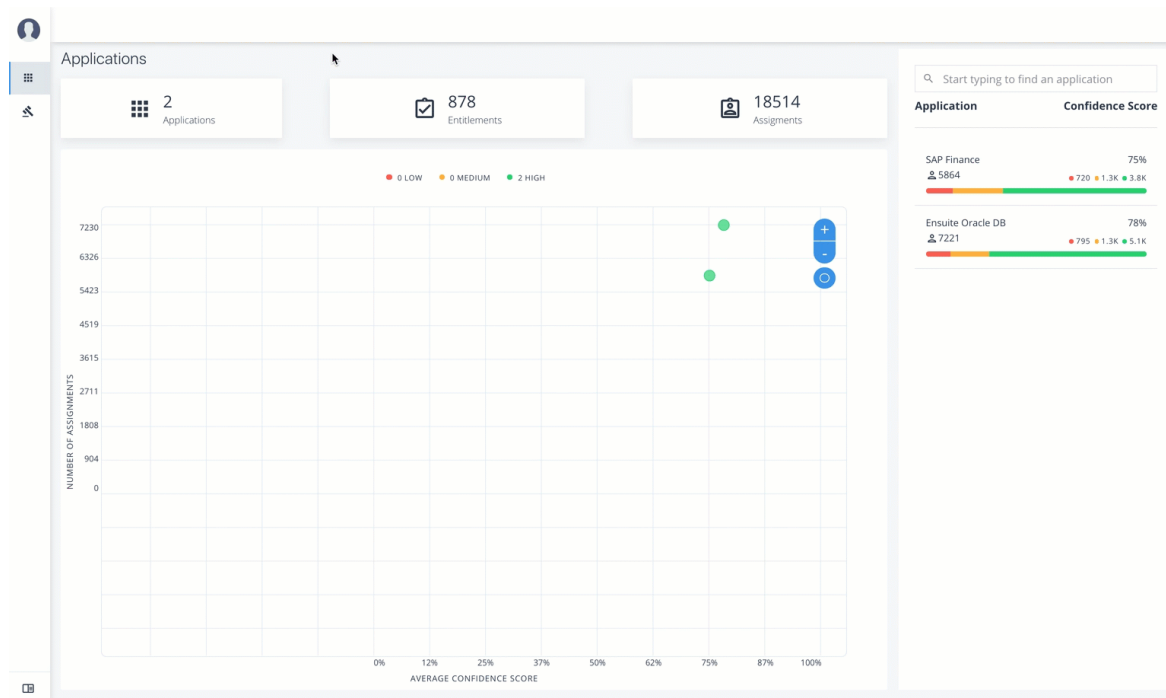
Follow these steps to apply filters to your confidence score graphs:

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:
 - Click Owner to filter on the entitlement owner. You can make more than one selection.
 - Click Risk Level to filter on low, high, and middle risk entitlements. You can make more than one selection.
 - Click Criticality to filter on Essential or Non-Essential entitlements.
4. Under User Attributes, do one or all of the following:
 - Click Manager to filter on a manager. You can make more than one selection.
 - Click Chief to filter if the entitlement is manager or not.
 - Click Department to filter on a specific department. You can make more than one selection.

- Click LOB Sub Group to filter on a line of business subgroup. You can make more than one selection.
- Click LOB to filter on the line of business for the division. You can make more than one selection.
- Click Cost Center to filter on a cost center. You can make more than one selection.
- Click Job Code Name to filter on a job code. You can make more than one selection.
- Click City to filter on the city of the operations. You can make more than one selection.
- 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.

▼ [See it in action](#)



Re-certify Entitlement Assignments

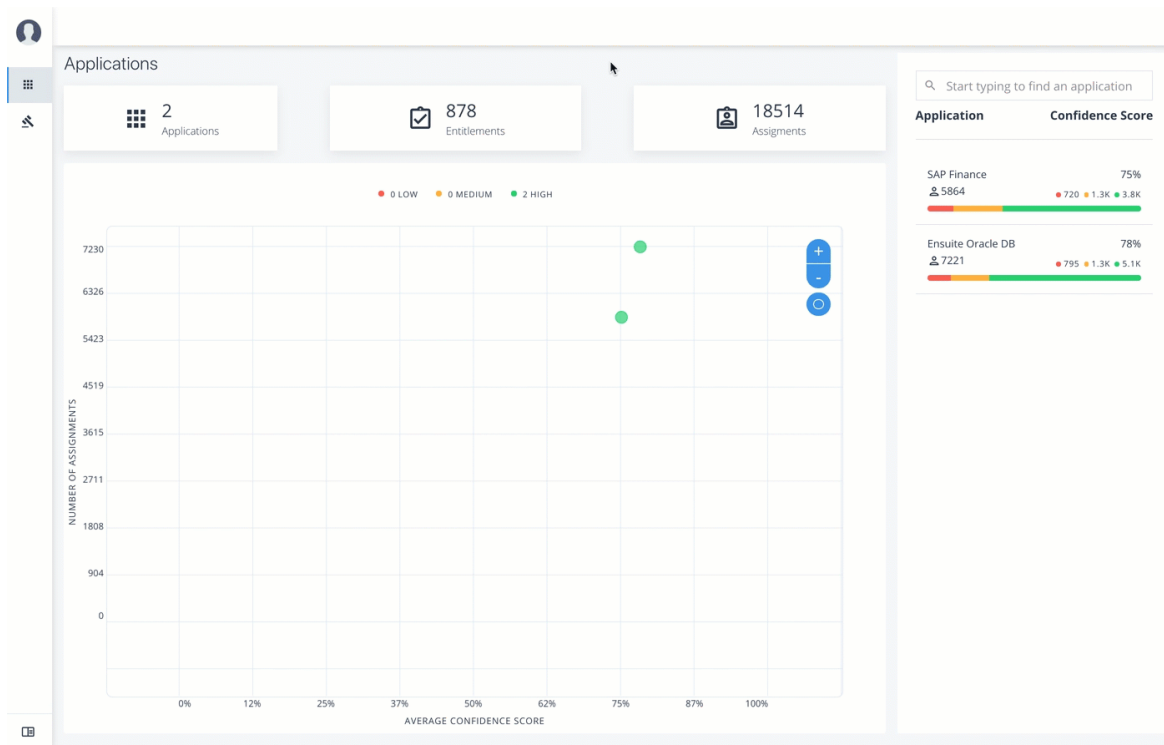
Follow these steps to re-certify an entitlement assignment:

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.

▼ [See it in action](#)



Approve Rule Justifications

Follow these steps to apply rule justifications for an entitlement:

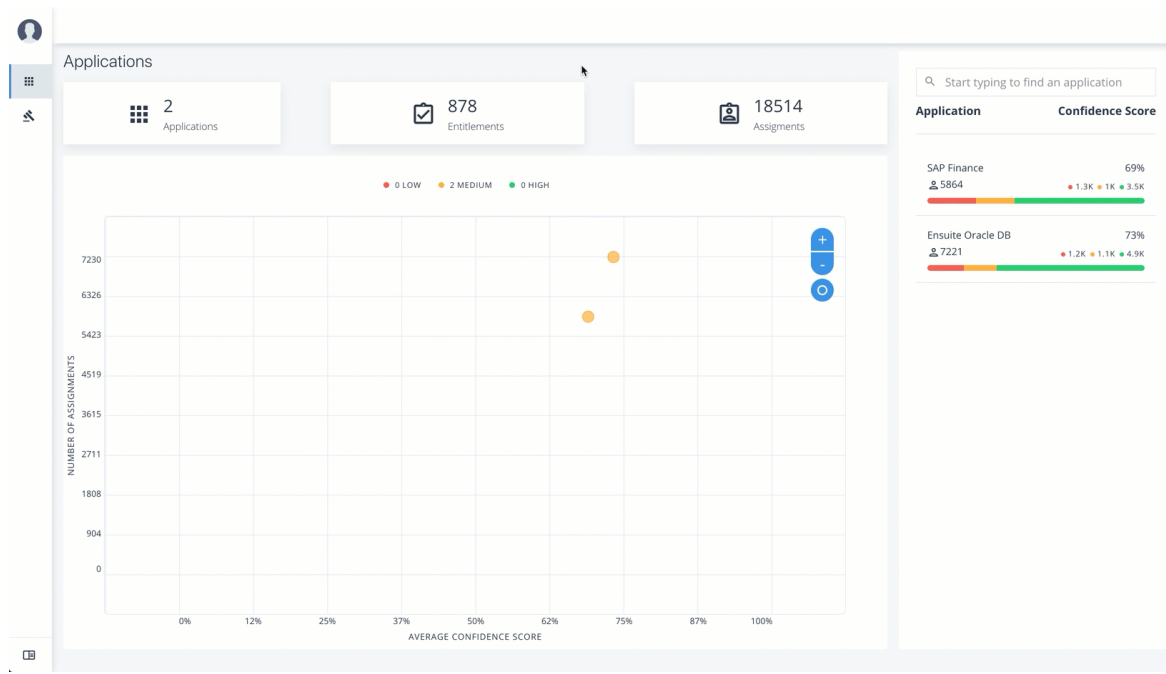
1. Log in to the Autonomous Identity console.
2. Click Rules.
3. On the Rules page, select an entitlement to view, and then click the down arrow to see the driving factors for the entitlement.
4. Under Identity, change to see another user's attributes and driving factors. If you want to see the user's 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.

▼ [See it in action](#)



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.

Auto-Certify and Auto-Request an Entitlement

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

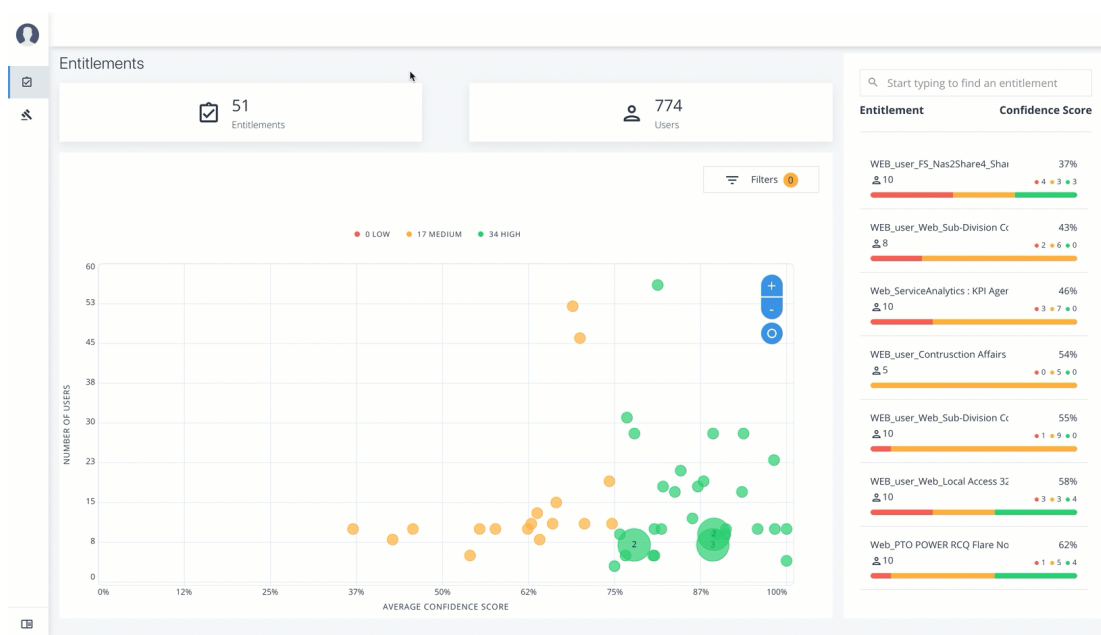
1. Log in to the Autonomous Identity console as an Entitlement Owner.
2. On the graph, click a circle or click an entitlement in the right-hand list.
3. Review the details of the entitlement, especially the Driving Factors list.
4. Click the right arrow to view the users associated with the entitlement and confidence score. You can click a user to drill down to the Users Entitlements page.

- 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.

▼ [See it in action](#)

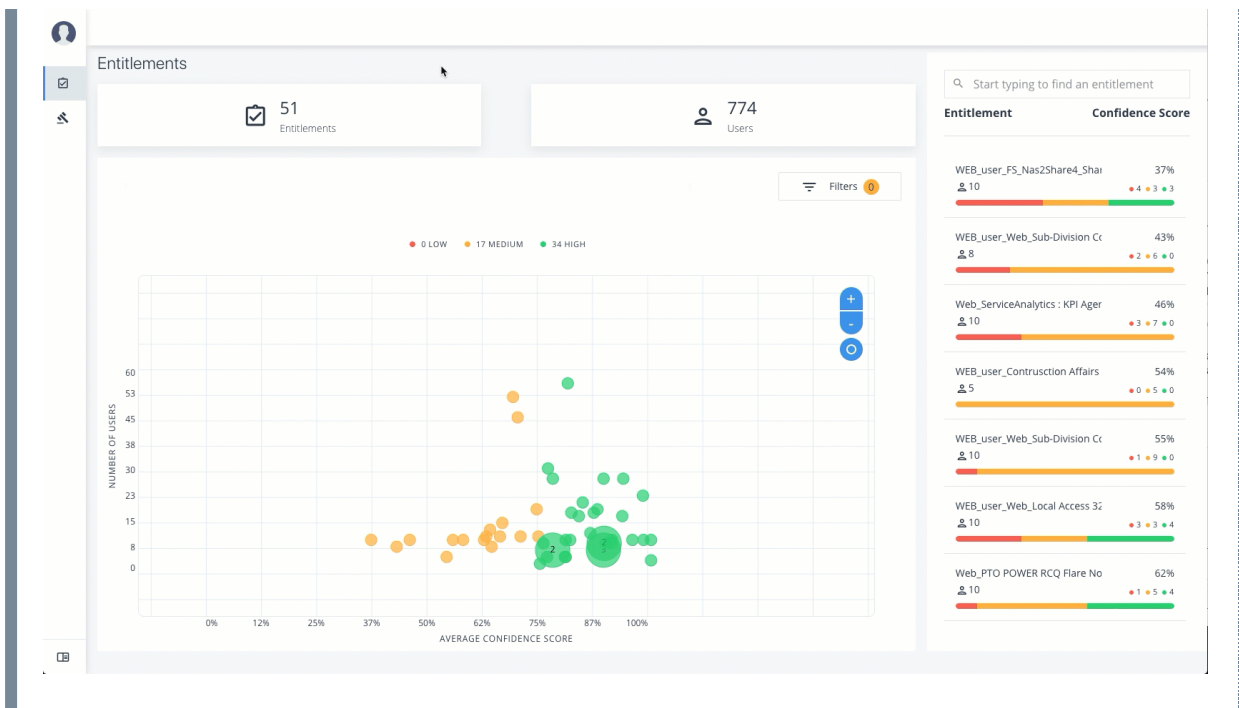


Apply Filters

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

- On the Entitlements page, view the average confidence score graph.
- On the right, click **Filters**.
- Do one or all of the following:
 - Click Remove high scores from Averages.
 - Click an application to filter the results.
 - Click Add Filters to further filter on a user attribute.

▼ [See it in action](#)

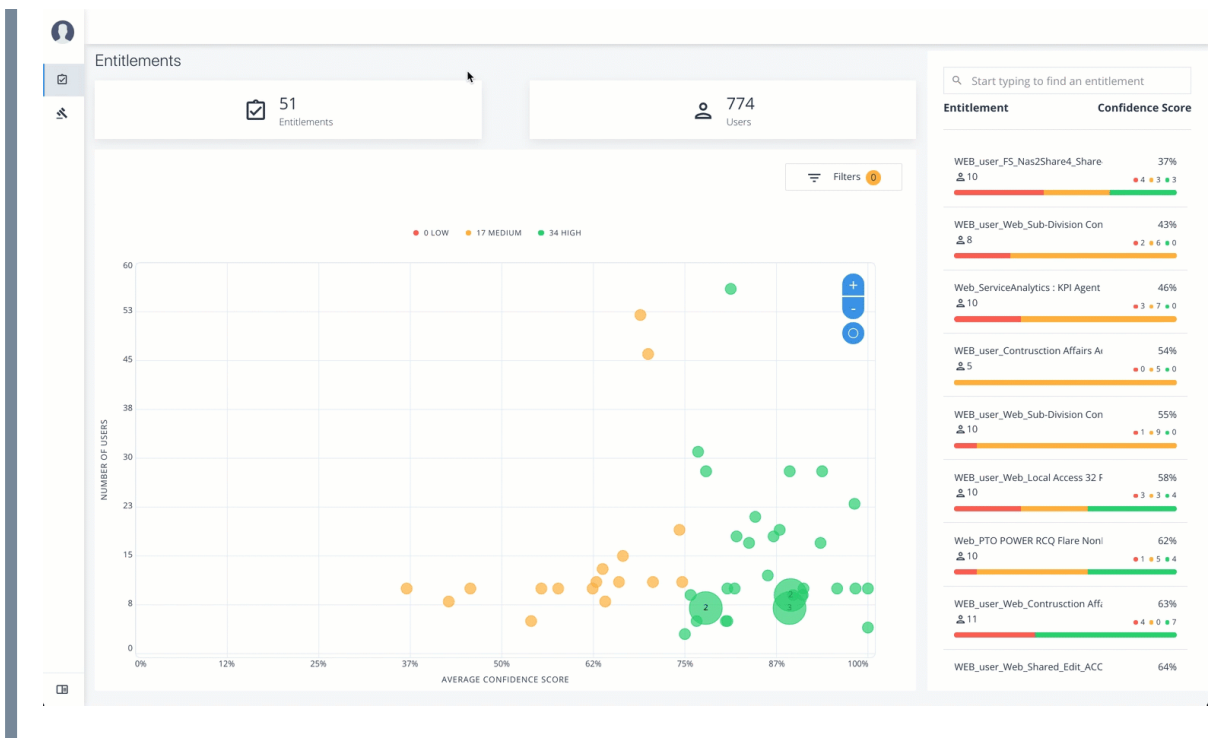


Approve or Revoke Access to an Assigned Entitlement

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.

▼ [See it in action](#)



Approve Rule Justifications

Follow these steps to apply rule justifications for an entitlement:

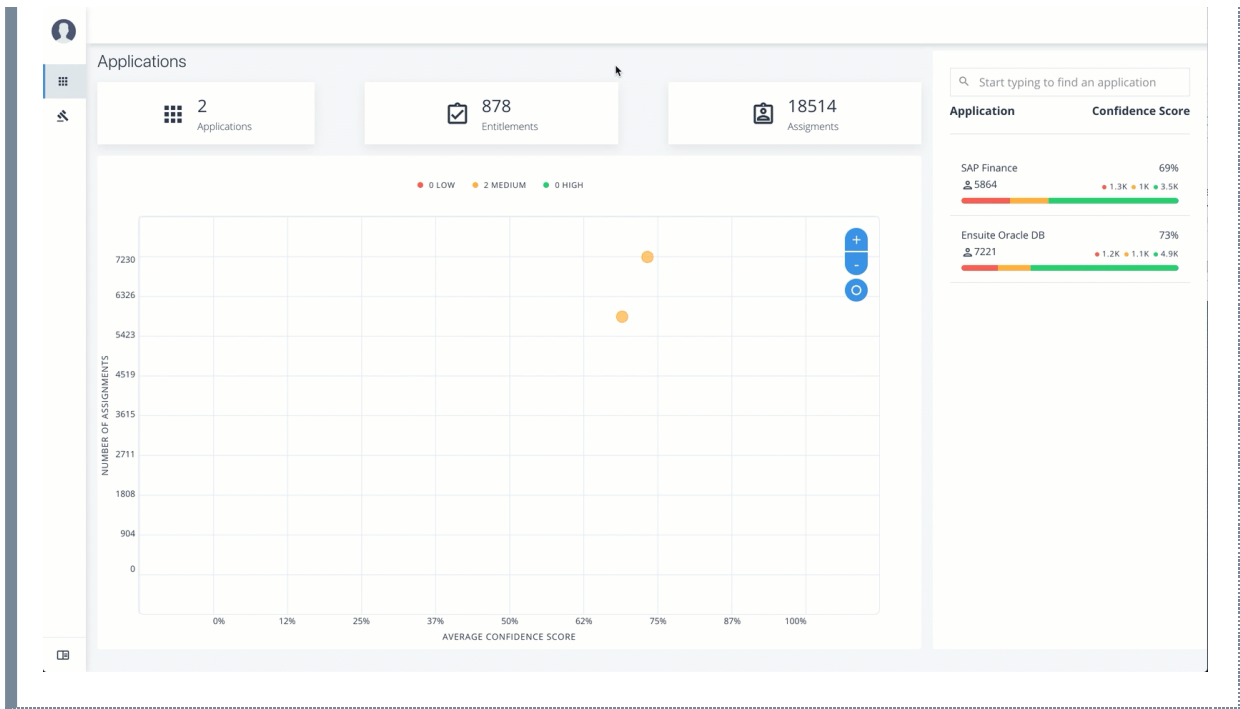
1. Log in to the Autonomous Identity console.
2. Click Rules.
3. On the Rules page, select an entitlement to view, and then click the down arrow to see the driving factors for the entitlement.
4. Under Identity, change to see another user's attributes and driving factors. If you want to see the user's 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.

▼ [See it in action](#)



Was this helpful?

Copyright © 2010-2022 ForgeRock, all rights reserved.