



# Users Guide

/ Autonomous Identity 2020.6.4

Latest update: 2020.6.4

---

Copyright © 2016-2020 ForgeRock AS.

## Abstract

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



This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License.

To view a copy of this license, visit <https://creativecommons.org/licenses/by-nc-nd/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

© Copyright 2010-2020 ForgeRock, Inc. All rights reserved. ForgeRock is a registered trademark of ForgeRock, Inc. Other marks appearing herein may be trademarks of their respective owners.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, and distribution. No part of this product or document may be reproduced in any form by any means without prior written authorization of ForgeRock and its licensors, if any.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESSED OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

DejaVu Fonts

Bitstream Vera Fonts Copyright

Copyright (c) 2003 by Bitstream, Inc. All Rights Reserved. Bitstream Vera is a trademark of Bitstream, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of the fonts accompanying this license ("Fonts") and associated documentation files (the "Font Software"), to reproduce and distribute the Font Software, including without limitation the rights to use, copy, merge, publish, distribute, and/or sell copies of the Font Software, and to permit persons to whom the Font Software is furnished to do so, subject to the following conditions:

The above copyright and trademark notices and this permission notice shall be included in all copies of one or more of the Font Software typefaces.

The Font Software may be modified, altered, or added to, and in particular the designs of glyphs or characters in the Fonts may be modified and additional glyphs or characters may be added to the Fonts, only if the fonts are renamed to names not containing either the words "Bitstream" or the word "Vera".

This License becomes null and void to the extent applicable to Fonts or Font Software that has been modified and is distributed under the "Bitstream Vera" names.

The Font Software may be sold as part of a larger software package but no copy of one or more of the Font Software typefaces may be sold by itself.

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL BITSTREAM OR THE GNOME FOUNDATION BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

Except as contained in this notice, the names of GNOME, the GNOME Foundation, and Bitstream Inc., shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Font Software without prior written authorization from the GNOME Foundation or Bitstream Inc., respectively. For further information, contact: [fonts@gnome.org](mailto:fonts@gnome.org).

Arev Fonts Copyright

Copyright (c) 2006 by Tavmjong Bah. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of the fonts accompanying this license ("Fonts") and associated documentation files (the "Font Software"), to reproduce and distribute the modifications to the Bitstream Vera Font Software, including without limitation the rights to use, copy, merge, publish, distribute, and/or sell copies of the Font Software, and to permit persons to whom the Font Software is furnished to do so, subject to the following conditions:

The above copyright and trademark notices and this permission notice shall be included in all copies of one or more of the Font Software typefaces.

The Font Software may be modified, altered, or added to, and in particular the designs of glyphs or characters in the Fonts may be modified and additional glyphs or characters may be added to the Fonts, only if the fonts are renamed to names not containing either the words "Tavmjong Bah" or the word "Arev".

This License becomes null and void to the extent applicable to Fonts or Font Software that has been modified and is distributed under the "Tavmjong Bah Arev" names.

The Font Software may be sold as part of a larger software package but no copy of one or more of the Font Software typefaces may be sold by itself.

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL TAVMJONG BAH BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

Except as contained in this notice, the name of Tavmjong Bah shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Font Software without prior written authorization from Tavmjong Bah. For further information, contact: [tavmjong@free.fr](mailto:tavmjong@free.fr).

FontAwesome Copyright

Copyright (c) 2017 by Dave Gandy, <https://fontawesome.com/>.

This Font Software is licensed under the SIL Open Font License, Version 1.1. See <https://opensource.org/licenses/OFL-1.1>.

---

# Table of Contents

Overview .....	iv
1. Features .....	1
2. Benefits of Autonomous Identity .....	2
3. Autonomous Identity User Types .....	4
4. The Autonomous Identity UI .....	5
5. Admin User Tasks .....	7
A Tour of the Company Overview Page .....	7
A Tour of the Entitlement Detail Page .....	9
Performing Admin Tasks .....	10
6. Supervisor Tasks .....	13
A Tour of the Employee Overview Page .....	13
A Tour of the User Entitlement Detail Page .....	14
Performing Supervisor Tasks .....	15
7. Entitlement Owner Tasks .....	17
A Tour of the Entitlement Overview Page .....	17
Performing Entitlement Owner Tasks .....	18
8. User Tasks .....	20
A Tour of the User Detail Page .....	20
Performing User Tasks .....	21
Glossary .....	22







# 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

 <p><b>Features</b></p> <p>Learn about the Autonomous Identity features.</p>	 <p><b>The Autonomous Identity UI</b></p> <p>Get an overview of the Autonomous Identity's powerful UI.</p>	 <p><b>Admin User Tasks</b></p> <p>Learn about the Company Overview page and the Admin tasks.</p>
 <p><b>Supervisor Tasks</b></p> <p>Learn about the Employee Overview page and Supervisor tasks.</p>	 <p><b>Entitlement Owner Tasks</b></p> <p>Learn about the Entitlement Owner page and tasks.</p>	 <p><b>User Tasks</b></p> <p>Learn about the User Detail page, and user tasks.</p>

## 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 that could potentially be a security risk. The UI also lets you quickly identify the 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.
- **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.

## Chapter 2

# Benefits of Autonomous Identity

Identity Governance and Administration (IGA) systems ensure that entitlement provisioning is compliant and consistent with company and regulatory standards. However, the entitlement landscape becomes less clear with the constant flux of employee movement and the high volume of entitlement provisioning to resources.

Nowadays, large global corporations have different and multiple hybrid environments for their applications and services; some on-prem, others in cloud, multi-cloud, and a combination of the three. Individual application dashboards are unable to provide a unified view of all entitlements across its network. Without this unified view, your company could be at risk for Segregation of Duties (SoD) violations, where multiple users approve an entitlement that could result in a security risk or possible internal fraud.

Many companies implement traditional role-based provisioning where roles are constantly added, removed, and edited as required. In fast-paced industries, administrators may carry-over many entitlements to new roles, while rubber-stamping additional privileges without clear assessment. When projects or employees change, roles become out-dated. Likewise, orphaned accounts or inactive entitlements are also pose as a risk. As a result, monitoring these role changes is a critical requirement for organizations.

Legal compliance regulations undergo strict yearly auditing. These audits require companies to know which entitlements exist within their organization, who has access to what resources, and how your company certifies these entitlements.

Autonomous Identity solves these problems and provides the following benefits:

- **Increased Security.** Autonomous Identity displays a centralized and unified view of the full entitlement landscape across a company's services and applications. This unified view alerts you to possible entitlement outliers that could pose a security risk to your system, which you can manually remove after investigation.
- **Automated Workflows.** Autonomous Identity calculates confidence scores for each entitlement, enabling you to automate many access functions that are currently run manually. These functions includes access request approval and certification. For example, when on-boarding new employees, Autonomous Identity can quickly automate basic access to resources specific to the user's job functions.
- **Near-Realtime Processing.** You can run Autonomous Identity on a weekly basis; thus, ensuring that entitlement assignments are up-to-date.
- **Full Compliance.** Autonomous Identity ensures that your IAM and IGA systems are fully compliant for regulatory standards and audits as it tracks all assigned entitlements.

- **Reduce Costs.** When you automate many manual provisioning processes based on the confidence scores, you save time and money by reducing service tickets. Autonomous Identity also eliminates the need for monthly, quarterly, and yearly re-certification reviews by supervisors.
- **Intelligent Entitlements Management and Intelligent Role Mining.** Autonomous Identity is well-suited for intelligent entitlements management and intelligent role mining.

## Chapter 3

# Autonomous Identity User Types

Autonomous Identity supports five different user types, or personas, within its system:

- **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 to users, users to entitlements, and approve or revoke access.
- **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. Users can view their entitlements, their own profile, and their certifications.



## Chapter 4

# 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.

Autonomous Identity provides multiple UI views depending on the user type:

- **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. Only admin users can view this page. You can add filters to limit what is displayed on the various graphics. For a description of the page, see "*Admin User Tasks*".
- **Employee Overview.** Also known as the *Supervisor View*. Displays a dashboard of all users and their entitlements reporting to the supervisor. The page also displays the number of entitlements assigned to a user and the average confidence score across these entitlements. The supervisor can investigate the entitlements for any user reporting to them, and approve or revoke access to a specific entitlement. For a description of the page, see "*Supervisor Tasks*".
- **Entitlement Owner Overview.** Displays a dashboard of all entitlement managed by the entitlement owner. An example of an entitlement owner is one who has access rights to a resource, such as a file or application, but may not be a supervisor of employees. For a description of the page, see "*Entitlement Owner Tasks*".
- **Entitlement Detail View.** Displays a detailed view of a specific entitlement including average confidence scores for this entitlement, the number of users assigned to the entitlement, and assignment justifications. For a description of the page, see "*Entitlement Owner Tasks*".
- **User Detail View.** Displays the user's profile and all entitlements assigned to that user. The page displays the average confidence scores for each entitlement. For a description of the page, see "*User Tasks*".
- **User's Entitlement Detail View.** Displays a detailed view of a specific entitlement including average confidence scores, the number of users assigned to the entitlement, and assignment justifications.

Table: Summary of Autonomous Identity Users and Accessible Views

User Type/View	Company View	Employee Overview	Entitlement Owner View	Entitlement Detail View	User Detail View	User's Entitlement Detail View	
Admin	✓	✓	✓	✓	✓	✓	

User Type/View	Company View	Employee Overview	Entitlement Owner View	Entitlement Detail View	User Detail View	User's Entitlement Detail View	
Executive	✓					✓	
Supervisor		✓			✓	✓	
Entitlement Owner			✓	✓			
User View					✓	✓	

## Chapter 5

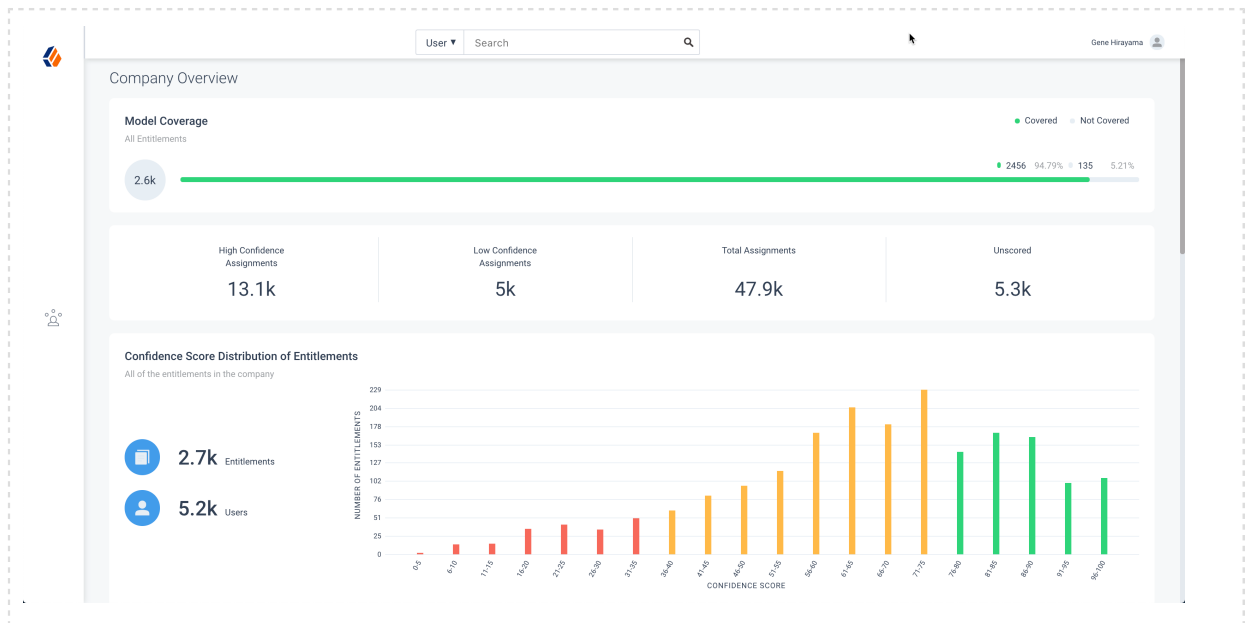
# Admin User Tasks

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.

## A Tour of the Company Overview Page

The Company Overview displays a dashboard with a complete summary of all entitlements, confidence scores, the most critical entitlements plus other useful data in your network. Only users with Admin User and Executive User access can view this page.

+ *Figure: Autonomous Identity Company Overview Page*



The Company Overview is partitioned into several modules as you scroll down:

- **Search function.** Provides a way to search on the Autonomous Identity system for any supervisor, entitlement owner, user, and entitlement within your company.

- **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 orphaned accounts, one-to-one matching, and the highly assigned entitlements to displayed number of users.
    - **Orphaned accounts** refer to those accounts that have existing access privileges without a valid owner.
    - **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 is one user who has 0-5 assigned entitlements. In the second row from the bottom, there are 1064 users who have between 5-10 assigned entitlements. In the third row from the bottom, there are 1549 users who have between 10-100 assigned entitlements.
- + *See an Example of the All Entitlements Distribution Graph*

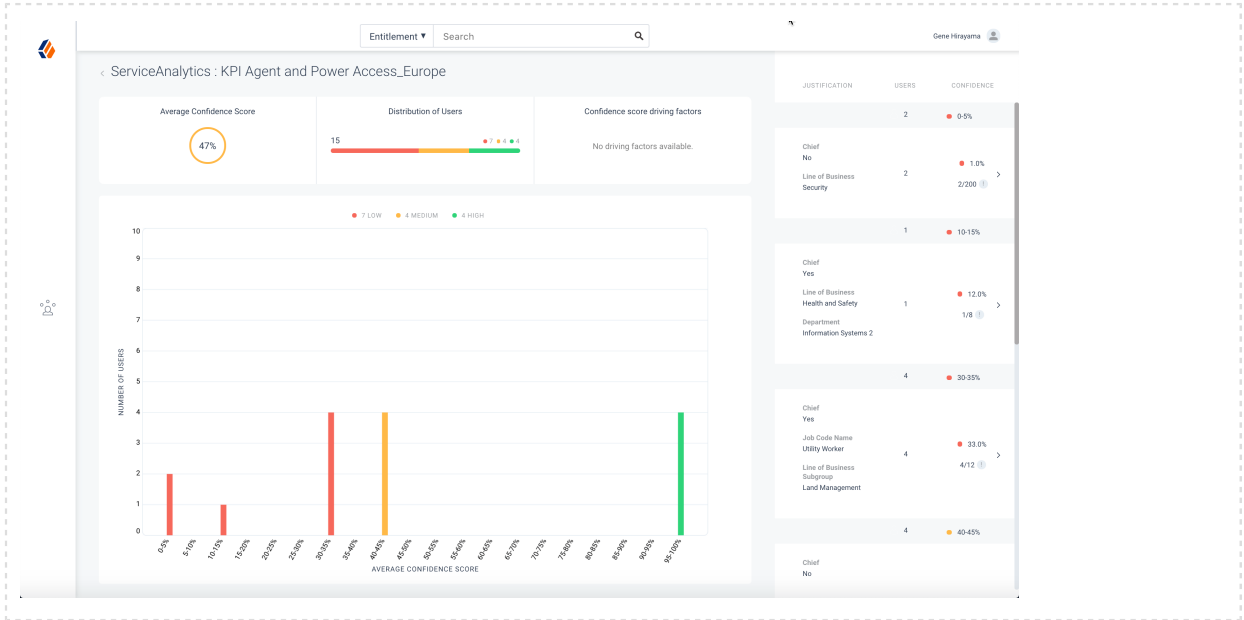


- **Entitlements Without Owners.** Displays the number of entitlements without an owner. This indicates that no user is managing this entitlement.
- **Users Without Supervisors.** Displays the number of users without a supervisor. This could indicate that a user was not properly set up or deprovisioned 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.

## A Tour of the Entitlement Detail Page

The Entitlement Detail displays the key information about a specific entitlement that lets approve the entitlement for automated certification or approval.

+ *The Autonomous Identity Entitlement Detail Page*



The Entitlement Detail is partitioned into different screen elements:

- **Search.** Search for any entitlement in the system.
- **Average Confidence Score, Distribution of Users, and Confidence Score Driving Factors.** Displays the average confidence score for the entitlement and the distribution of users who have the assigned entitlement. The confidence score driving factors are the key user attributes that lead to the confidence score.
- **Bar Chart of Average Confidence Scores.** Displays the average confidence scores broken down by percentages versus the number of users. Click the bar to select the entitlement's justification on the right. Click Approve Justification to select entitlement for automated certification or approval.
- **Justifications.** On the right, the page displays justifications for the percentage range of confidence scores in the graph. Click the right arrow to see the list of users who have the entitlement assigned to them.

## 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 Company Overview page, 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, and then look at the number next to the exclamation point. For example, you may see "3/43". This indicates that 3 out of 43 users that have the justification attributes have this entitlement, which may indicate an outlier.
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. On the User's Entitlements page, scroll down to review the Employees associated with this entitlement.
7. Click Approve Access or Revoke Access.

#### + *Check Non-Scored Users or Users with No Entitlements*

Follow these steps to check Non-Scored Users or Users with No Entitlements:

1. On the Search menu, select Supervisor, and enter a supervisor name.
2. On the Employee Overview page, click the exclamation point button with the associated number of unscored entitlements, and then click View All to view the list.
3. Click a user, and then view the Entitlement assigned to the user.
4. In the search menu, select Entitlement, and then enter the specific entitlement to view its details.

#### + *Approve or Revoke Access*

Follow these steps to investigate a confidence score and approve or revoke access:

1. On the Employee Overview page, view the average confidence score graph by hovering over a confidence score.

2. Click a circle, and then click the user in the list on the right.
3. On the User Detail page, click a confidence circle on the graph to highlight the entitlement below.
4. Click **Approve Access** or **Revoke access**. If you want to drill down for information on the specific entitlement, click the entitlement, and then click Approve Access or Revoke Access.

#### + *Apply Filters*

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

1. On the Employee Overview page, view the average confidence score graph.
2. On the right, enable **Remove High Scores from Average** or enable any filter in the Application Filters section.
3. To add a filter, click a category, and then click Add Filter.

#### + *Approve Justification*

Follow these steps to approve a confidence score justification:

1. On the Company Overview page or the Employee Overview page, select Entitlement on the drop-down menu, and then enter the name of the entitlement.
2. View the average confidence score and hover over the Confidence score driving factors for a quick review.
3. On the Average Confidence Score graph, click the green percentage range bar.
4. Click the right arrow to view the list of selected users who have the entitlement assigned to them. Click each user link to review the user's entitlements.
5. Click Approve Justification, and then select Auto Certify or Auto Request, and enter the reason for the justification. Click Yes to apply the justifications.



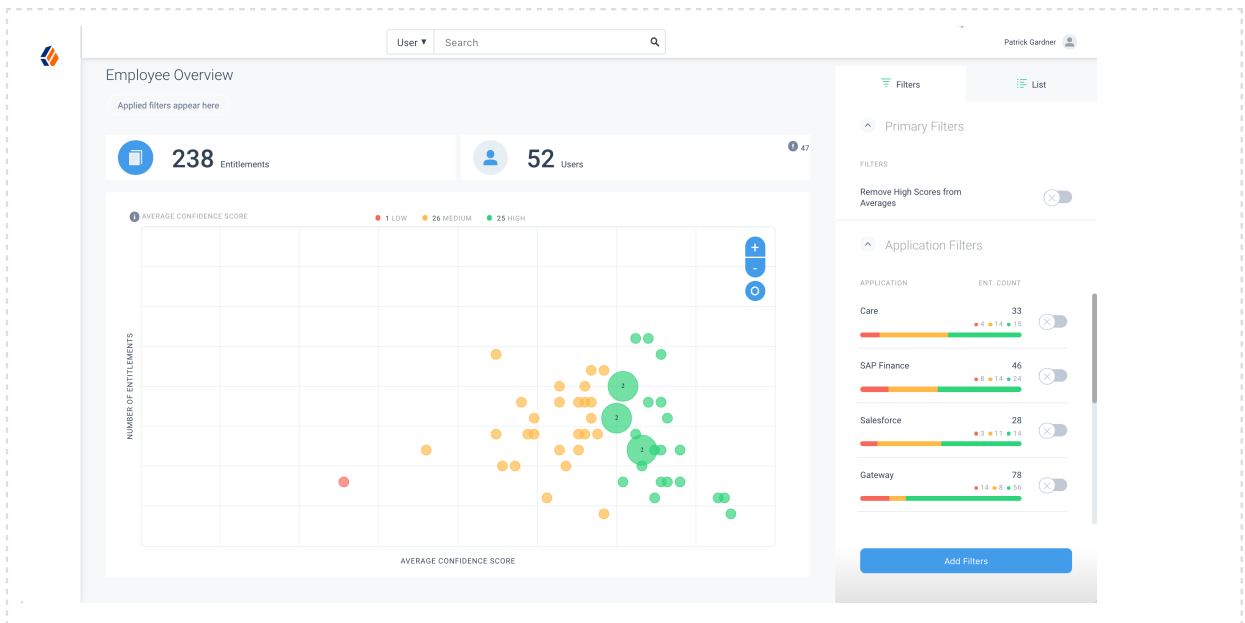
## Chapter 6 Supervisor Tasks

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.

### A Tour of the Employee Overview Page

The Employee Overview, or the Supervisor View, displays a dashboard of all users reporting to the supervisor and their entitlements.

+ *The Autonomous Identity Employee Overview Page.*



The Employee Overview is partitioned into several modules:

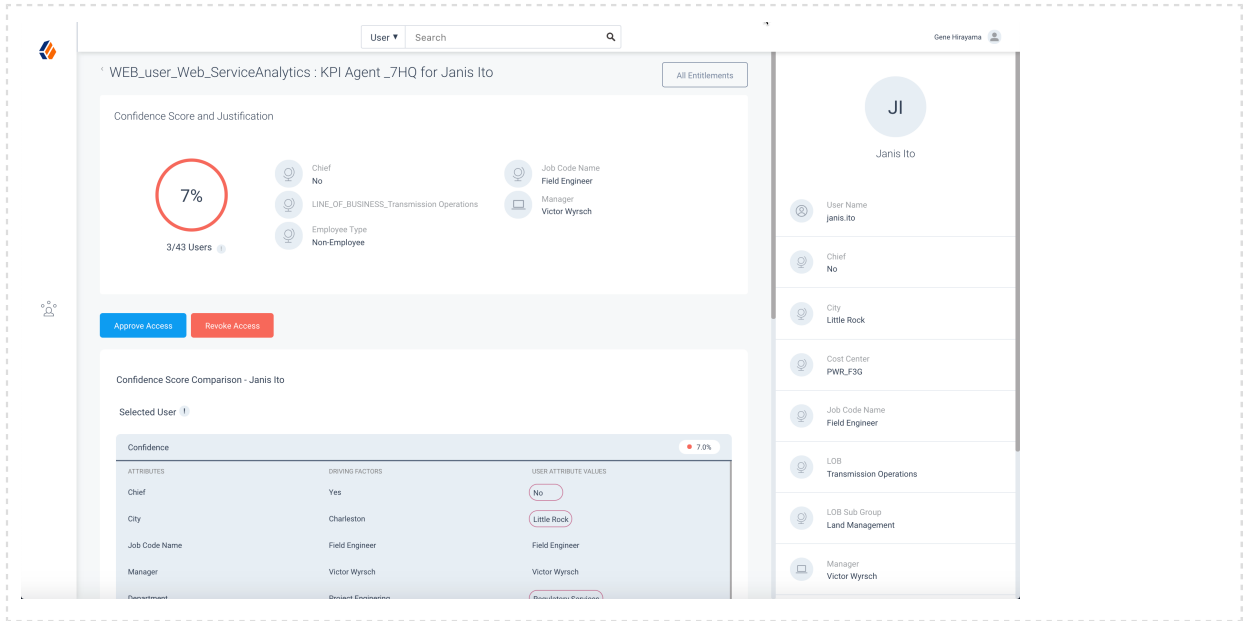
- **Total Number of Entitlements.** Displays the total number of entitlements assigned to users who report to the supervisor.

- **Total Number of Users.** Displays the total number of users that are assigned the entitlements.
- **Users with 'Not-scored Entitlements' & 'Users without Entitlements'.** Displays a list of unscored assignments that were not assigned a confidence score. These unscored entitlements stem from entitlements that have too few assigned users to determine access patterns for scoring calculations.
- **Average Confidence Score.** Displays the number of confidence scores for high, mid, and low.
- **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.
- **Primary Filters.** Enable the **Remove High Scores from Averages** filter to view only the mid and low confidence scores.
- **Application Filters.** Enable any of the application filters to determine the type of entitlement in this dataset. Click the **Add Filters** button to add more filters.
- **List.** Displays a full list of users who have the assigned entitlements. You can drill down and see each user's entitlements details by clicking on the user's name.

## A Tour of the User Entitlement Detail Page

The User Entitlement Detail displays the confidence score and the justified attributes for an entitlement assigned to the user. You can also view a comparison of the driving attribute factors and any differences between the user's attributes to that of the driving factors.

+ *The Autonomous Identity User Entitlement Detail Page*



The User Entitlement Detail is partitioned into several modules as you scroll down:

- **Confidence Score and Justification.** Displays the confidence score for the user's assignment of the entitlement and the user attributes that justified this score.
- **Confidence Score Comparison.** Displays the attributes, driving factors, and user attribute values that are compared for the confidence score. The key attributes and their driving factors that lead to a high confidence score is compared to the user's attribute values. Any variance is highlighted in red.
- **Employees associated with This Entitlement.** Displays the list of users with the entitlement and their confidence scores. If the users in this list have low confidence scores, the entitlement may be a good candidate for removal.
- **User Attributes.** On the right, the user's profile attributes are displayed that were ingested into Autonomous Identity.

## Performing Supervisor Tasks

+ *Check Non-Scored Users or Users with No Entitlements*

Follow these steps to check Non-Scored Users or Users with No Entitlements:

1. On the Employee Overview page, click the exclamation point button with the associated number of unscored entitlements, and then click View All to view the list.
2. Click a user, and then view the Entitlement assigned to the user.
3. In the search menu, select Entitlement, and then enter the specific entitlement to view its details.

#### + *Approve or Revoke Access*

Follow these steps to investigate a confidence score and approve or revoke access:

1. On the Employee Overview page, view the average confidence score graph by hovering over a confidence score.
2. Click a circle, and then click the user in the list on the right.
3. On the User Detail page, click a confidence circle on the graph to highlight the entitlement below.
4. Click **Approve Access** or **Revoke access**. If you want to drill down for information on the specific entitlement, click the entitlement, and then click Approve Access or Revoke Access.

#### + *Apply Filters*

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

1. On the Employee Overview page, view the average confidence score graph.
2. On the right, enable **Remove High Scores from Average** or enable any filter in the Application Filters section.
3. To add a filter, click a category, and then click Add Filter.

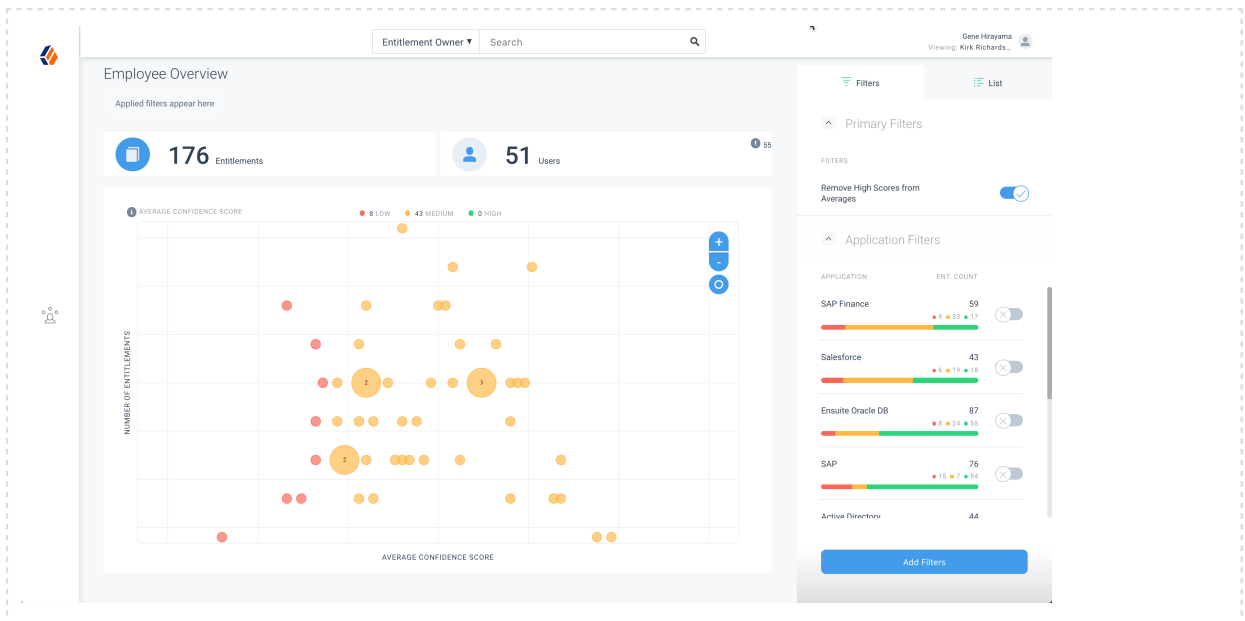
## Chapter 7 Entitlement Owner Tasks

An *Entitlement Owner* is one one who has responsibility for a given access to a resource, but may not be a supervisor.

### A Tour of the Entitlement Overview Page

The Entitlement Overview page displays a summary of all entitlements, confidence scores, and users for which the entitlements owner is responsible. Entitlement owners cannot view the entitlements of other entitlements owners.

#### + *The Autonomous Identity Entitlement Owner Page*



The Entitlement Overview page is partitioned into different screen elements:

- **Total Number of Entitlements.** Displays the total number of entitlements that the entitlement owner has responsibility for.

- **'Not-scored Entitlements' & 'Entitlements with No Users'**. Displays a list of unscored entitlements with the associated employee count. These unscored entitlements may occur if there are too few users assigned to determine access patterns for scoring confidence scores.
- **Total Number of Users**. Displays the total number of users that are assigned the entitlements.
- **Average Confidence Score**. Displays the number of confidence scores for high, mid, and low for the chart.
- **Graph of Average Confidence Scores**. Displays 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 to the user. If you double-click a circle, you can see the user's in the list on the right.
- **Primary Filters**. Enable the **Remove High Scores from Averages** filter to view only the mid and low confidence scores.
- **Application Filters**. Enable any of the application filters to determine the type of entitlement in this dataset. Click the **Add Filters** button to add more filters.
- **List**. Displays a full list of assigned entitlements. You can drill down to see the details by clicking on the entitlement's name.

## Performing Entitlement Owner Tasks

### + *Check Non-Scored Users or Users with No Entitlements*

Follow these steps to check Non-Scored Users or Users with No Entitlements:

1. On the Entitlement Overview page, click the exclamation point button with the associated number of unscored entitlements, and then click View All to view the list.
2. Under the Entitlements heading, select an entitlement to see the users associated with it.
3. In the search menu, select Entitlement, and then enter the specific entitlement to view its details.

### + *Apply Filters*

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

1. On the Entitlement Overview page, view the average confidence score graph.
2. On the right, enable **Remove High Scores from Average** or enable any filter in the Application Filters section.

3. To add a filter, click a category, and then click Add Filter.

## Chapter 8

# User Tasks

The User View displays a user's entitlements and profile.

## A Tour of the User Detail Page

The User Detail displays a summary of all of the entitlements and confidence scores for a particular user.

+ *The Autonomous Identity User Detail Page*

The screenshot displays the 'Entitlements for Janis Ito' page. At the top, there is a progress bar showing confidence scores from 0 to 100. Below the bar is a table of entitlements with columns for Entitlement, Confidence, Application, Justification, Pending Request By, Pending, and Last Access Date. At the bottom of the table are 'Approve Access' and 'Revoke Access' buttons. To the right of the table is a user profile sidebar with fields for User Name, Chief, City, Cost Center, Job Code Name, LOB, LOB Sub Group, and Manager.

ENTITLEMENT	CONFIDENCE	APPLICATION	JUSTIFICATION	PENDING REQUEST BY	PENDING	LAST ACCESS DATE
<input type="checkbox"/> WEB_user_Web_Servic...	7%	Care	Chief_Job Code Name...	-	-	02.13.20
<input type="checkbox"/> WEB_user_Web_Cogn...	45%	Ensulte Oracle DB	Chief_Job Code Name...	-	-	02.13.20
<input type="checkbox"/> WEB_user_pyroTD_Co...	62%	SAP Finance	Chief_LINE_OF_BUSIN...	-	-	02.13.20
<input type="checkbox"/> WEB_user_Web_pyroT...	75%	Care	Chief_Job Code Name...	-	-	02.13.20
<input type="checkbox"/> TES2 Group Security (...)	83%	SAP	Chief_LINE_OF_BUSIN...	-	-	02.13.20
<input type="checkbox"/> Outlook_LotusNotes_L...	86%	Ensulte Oracle DB	Job Code Name, Depa...	-	-	02.13.20
<input type="checkbox"/> Web_RCQ Flare NoteIT...	93%	Salesforce	Cost Center Power, Jo...	-	-	02.13.20
<input type="checkbox"/> Web_Local Access 32...	95%	SAP	Cost Center Power, Lin...	-	-	02.13.20

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

- **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. To investigate further, click an entitlement in the list to see the User's Entitlement Detail page.



- **Not Scored Entitlements.** Displays the list of entitlements that could not be scored by Autonomous Identity.
- **Recommended Entitlements.** Displays the recommended entitlements for the user.
- **Assigned Entitlements.** Displays the list of user's assigned entitlements. Admins and supervisors can approve or revoke access for a specific entitlement.
- **User Detail.** Displays the user's attributes within the company as ingested from the company's HR database.

## Performing User Tasks

### + *View Not Scored Entitlements*

Follow these steps to view not scored entitlements:

1. On the Entitlements for <User> page, click the Not Scored button.
2. Review the list and then ask your supervisor to approve or remove it.

### + *How to Log Out*

Follow these steps to log out of Autonomous Identity:

1. On the Entitlements for <User> page, click the user icon on the top left.
2. Click Logout on the top right.

### + *Return to the User Detail Page*

Follow these steps to view return to the User Detail page:

1. On the Entitlements for <User> page, if you click an entitlement, you may see a 403 Access Forbidden page. General users cannot see the details of an entitlement for security purposes.
2. Click the ForgeRock icon on the top left to return to the User Detail page.

# 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.
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 <a href="#">assignment</a> . 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 <code>conf_thresh</code> 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.