

Digital.ai Platform User Guide



Table of contents:

- [Digital.ai Platform User Documentation](#)
- [Release Notes](#)
- [Getting Started](#)
- [Frequently Asked Questions \(FAQ\)](#)
- [Digital.ai Assistant](#)
- [Vanity Subdomains in the Platform](#)
- [Key Uses of Vanity Subdomains](#)
- [Edit Your Vanity Subdomain](#)
- [Account Settings](#)
- [Monitor Activity with the Audit Log](#)
- [How to Integrate Release with the Platform](#)
- [How to Integrate Agility with the Platform](#)
- [How to Integrate Deploy with the Platform](#)
- [Source Integrations](#)
- [Manage Applications](#)
- [Users](#)
- [User Groups](#)
- [User Self-Registration](#)
- [Resetting A User's Password](#)
- [Sign-in Helper](#)
- [Add OIDC SSO Connection](#)
- [Add SAML SSO Connection](#)
- [User Merge Flow](#)
- [Enable IP Address Allow List](#)
- [Manage Identity Providers](#)
- [Connect to OIDC Provider](#)
- [Connect to SAML Provider](#)
- [Map User Data](#)
- [Map User Group Assignments](#)
- [Map User Roles](#)
- [Set a Default IdP](#)
- [SSO Certificates](#)
- [API Overview](#)
- [API Reference](#)
- [Access Tokens](#)
- [Data API](#)

- [What is a Dashboard?](#)
- [Accessing Dashboards](#)
- [Recommendations for Custom Dashboards](#)
- [Viewing Dashboard Details](#)
- [Filtering Dashboards](#)
- [Security Implementation in Dashboards](#)
- [Creating Dashboards](#)
- [Editing Dashboards](#)
- [Adding an existing dataset](#)
- [Link Shared Data Across Multiple Datasets](#)
- [Viewing and hiding panels](#)
- [Editor Panel](#)
- [Format Panel](#)
- [Selecting which attribute forms to display in a visualization](#)
- [Introduction to chapters and pages](#)
- [Adding, renaming, copying, moving or deleting Pages](#)
- [Adding, renaming, copying, moving, or deleting Chapters](#)
- [Adding an image](#)
- [Add Shapes](#)
- [Add Rich Text](#)
- [Adding a text field](#)
- [Editing, moving, or deleting a text field](#)
- [Introduction to Visualizations](#)
- [Creating a Classic Grid](#)
- [Creating a Heat Map](#)
- [Creating a Bar Chart](#)
- [Creating a Line Chart](#)
- [Creating a Bubble Chart](#)
- [Creating a Pie or Ring Chart](#)
- [Creating a Network Visualization](#)
- [Create a Histogram](#)
- [Creating a KPI Visualization](#)
- [Changing the visualization type](#)
- [Duplicating a visualization](#)
- [Moving a visualization](#)
- [Deleting a visualization](#)
- [Enabling a Legend](#)
- [Viewing and editing visualization filter targets](#)

- [Using Free-Form Layout](#)
- [Enabling Outline Mode for a Grid](#)
- [Saving a dashboard](#)
- [Sort Data in a Grid](#)
- [Advanced Thresholds Editor](#)
- [Creating a threshold on an attribute or metric in the Advanced Thresholds editor](#)
- [Adding Information Windows](#)
- [Show Data Dialog](#)
- [Using natural language queries](#)
- [Copying rows of data from a Grid](#)
- [Managing Datasets](#)
- [What is a Dataset?](#)
- [Datasets Creation](#)
- [Previewing Datasets](#)
- [Exploring Datasets](#)
- [Listing dataset](#)
- [Viewing Existing Dataset](#)
- [Actioning in Created Datasets](#)
- [Custom Field Dataset](#)
- [Base and Advanced Datasets](#)
- [What is Code Standardization](#)
- [What is Code Class](#)
- [Code Standardization](#)
- [Application Properties](#)
- [Metadata Viewer](#)
- [Glossary](#)
- [Copyright](#)

Digital.ai Platform User Documentation

Welcome to the user documentation for the Digital.ai Platform, a cloud-based hub that serves as the foundation for the entire Digital.ai ecosystem, providing a unified experience with seamless user authentication across all Digital.ai applications and portals.

This documentation is primarily aimed at customer administrators, and provides instruction on configuring the various parts that make the unified experience possible, such as centralized user management and application access. However, the concepts and tasks described herein will likely be useful to any Platform user.

What's New

See the [Release Notes](#) to learn about the latest features and enhancements.

Get Started

If you're a new Digital.ai Platform user, we recommend reviewing the following topics:

- [Getting Started](#)
- [Glossary](#)

Otherwise, use the navigation and search at the left and top of the page to find the info you need.

Account Administrator Handbook

To support the onboarding of new customers, we created a standalone document that aims to help customers understand the features and benefits of Digital.ai Identity, with an overview of the service and suggestions on how to get started. The *Account Administrator Handbook* is intended as a supplement to this documentation.

Questions?

For questions, product advice, tips, use cases, and more, visit the Digital.ai [Customer Support Portal](#).

Release Notes

New features and enhancements in the current and previous versions of the Digital.ai Platform.

July 17, 2025

This release includes the following improvements:

- Users now have the ability to "unpublish" a dashboard to temporarily hide it from other users without deleting it. For more information, see [Unpublish a Dashboard](#).
- We have improved the [Audit Log](#) topic to be more informative.

June 09, 2025

- This release adds a new topic called [User Merge Flow](#), in which the system detects a new user but with an existing email address. This happens when there is a change in users' identification or authentication method. This flow links information to a single user even though the login method may have changed.
- This release adds a new topic called [Editing Dashboards](#), Which explains you how a dashboard enters the **Published** state when created, and switches to **Edit-in-progress** state and **locked** state for the editing user until changes are published or reverted.
- This release adds a new topic called [Map User Roles](#), which explains you the process of relating user attributes from an external Identity Provider (IDP) to corresponding roles within the Digital.ai Platform console. This feature allows you to utilize existing roles or group membership in your company's IdP to automatically assign the correct role membership in the Digital.ai Platform.
- This release adds a new topic called [Frequently Asked Questions](#), which gives you a basic concepts and workflows to guide you and resolve your basic queries while experiencing Digital.ai Platform.

March 25, 2025

- This release adds a new topic called [How to Integrate Deploy with the Platform](#), which provides end-to-end instructions for integrating Digital.ai Deploy with the Platform. Follow this guide to learn how to

connect with your corporate SSO provider for federated user access to Deploy and ensure that your users inherit all of their associated roles and permissions.

- This release adds a new topic called [IP Address Allow List](#), By adding an external party's IP address to the allow list, administrators ensure that these users can connect to the Platform without compromising security..

February 04, 2025

- This release adds a new topic called [Connect to Entra ID for SSO](#), which provides detailed information to customers on how to connect to the Entra ID.
- This release adds a new topic called [Vanity Subdomains](#), Which lets you specify the customer-specific part of the URL to which your users will navigate to reach the Platform Console.
- This release adds a new topic called [Source Integrations](#), Which helps you to add and view Source Integrations in Digital.ai products.
- This release also includes an updated version of the Map User Data topic [MAP User Data](#).

December 10, 2024

- This release adds a new topic called [Sign-in Helper](#), which provides information to customers on signing in to the digital.ai website for the first time using their login ids. This release also includes an updated version of the map user group assignments topic.

October 20, 2024

- This release adds a new topic called [Access Tokens](#), which provides information on what access tokens are, how to generate them, and how to use them for making authenticated API requests. This release also includes an updated version of the user documentation and a topic which explains how to delete dashboards.

August 20, 2024

- This release adds a new topic called [How to Integrate Agility with the Platform](#), which provides end-to-end instructions for integrating Digital.ai Agility with the Platform. Follow this guide to learn how to connect with your corporate SSO provider for federated user access to Agility and ensure that your users inherit all of their associated roles and permissions.

August 6, 2024

- Added documentation to describe how to use and manage SSO Certificates. No functional changes have been made to the product - this is a documentation change only. To view the new documentation, see [SSO Certificates](#).

June 5, 2024

This release introduces Analytics Dashboards. This new feature serves as a pivotal component for users to visualize, interpret, and interact with data insights generated by Digital.ai products. For more information about Dashboards and how to use them, see the following new topics:

- [What is a Dashboard](#)
- [Managing Datasets](#)
- [Code Standardization](#)

NOTE

Analytics Dashboards are part of our Premium product offerings. You will only be able to view this feature if you have the relevant role and entitlements.

May 15, 2024

- This release adds a new topic called [How to Integrate Release with the Platform](#), which provides end-to-end instructions for integrating Digital.ai Release with the Platform. Follow this guide to learn how to connect with your corporate SSO provider for federated user access to Release and ensure that your users inherit all of their associated roles and permissions.

April 9, 2024

- This release introduces some doc improvements to make the Identify Provider configuration material easier to follow. We revised some topics, reorganized the table of contents, and removed other topics that were no longer necessary. No functional changes have been made to the product - this is a documentation change only. To view the updated documentation, see [Manage Identity Providers](#) and [Map User Data](#).

October 18, 2023

- The emails which are sent by the Digital.ai Platform now have a new look and feel.
- Resolved an issue where certain special characters in the vanity domain name prevented some accounts from accessing the Digital.ai Platform. Affected accounts can now properly access the Platform.

September 13, 2023

- Account admins can now download their OIDC or SAML configuration files from the Account settings page, to authorize single sign-on integration.

August 8, 2023

- Digital.ai users can now effortlessly access specific sections or pages of the documentation, enabling to quickly locate relevant information without the need to browse through multiple pages.
- Account admins can now easily map their IdP based user groups to Platform groups, which allows them to manage all types of user groups conveniently from one place.
- The Digital.ai Platform documentation is updated with the [Account Settings](#), and [User Groups](#).

July 7, 2023

- Adding Applications method is now enhanced with an advanced manner.
- AgilitySync customers can now integrate with the Digital.ai Platform.

- Administrators now have the capability to independently refresh their IDP certificates through the Platform user interface, eliminating the need for Digital.ai Support.
- The Digital.ai Platform documentation is updated with the [Account Settings](#), [Manage Identity Providers](#), and [API Overview](#) topics.

June 6, 2023

- Account admins can now disable the `Product analytics and guidance` option in the Account Settings page in order to turn-off usage tracking.
- Account admins can now define default group memberships for new users, eliminating the need for manually assigning access permissions to each automatically provisioned user.
- The Digital.ai Platform documentation is updated with the [Account Settings](#) topic.

May 5, 2023

- Updated the Account Settings page for a more intuitive and streamlined user experience.
- Platform admins can now control support portal access (logging in and raising a ticket) for users within their organization.
- Platform admins can now control the visibility of application instances for users within their organization.
- API rate limiting has been implemented to ensure a more stable and secure service.
- TeamForge has been added to the list of product offerings available in the Platform, which means TeamForge customers can now use the Digital.ai Platform for authentication.
- The 'from' email address for automated Platform notifications is updated to `no-reply@digital.ai`.
- When a user's session expires in multiple pages or tabs at the same time, re-logging into one page will now auto-refresh all the other pages.
- Inactive users in the Platform can now be identified based on their "Last Activity Date".

- The Digital.ai Platform documentation is now updated with the [API Overview](#) and [API Reference](#) topics.

April 6, 2023

Mappers

The Digital.ai Platform documentation is now updated with the Mappers section, which includes an overview, Group Map Data, and the Client Mappers.

Please refer to [Mappers](#) for more information.

March 2, 2023

Data Retention Policy

As per the Data Retention policy, whenever a user is removed from the Digital.ai Platform, all of their personal related details are also removed.

User's Origin and User Management

- The users can now be recognized based on their origin, whether IdP or Local in the User's page.

[Accounts](#)

>

[Agility Sync Test](#)

>

Users

Add user

Users

Q

Type to search

▼

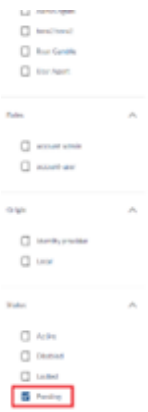
☐	Name ↑	Origin	Username	User Groups	Roles	Status
☐	Nithya Pattabiraman nithya.pattabiraman@digital.ai	Identity provider	nithya.pattabiraman@digital...		account-admin account-user	Active
☐	Nithya Pattabiraman Nithya.Pattabiraman+test@digital...	Local	nithya		account-admin account-user	Active
☐	Vetrivel Vaithilingam vetrivel.vaithilingam@digital.ai	Identity provider	vetrivel.vaithilingam		account-admin account-user	Active

- Administrators have an option to filter 'Pending' state users for better user management. From the Users page, you have an option to select only the users with pending status. To do this, click the 'filter' icon and select the 'Pending' status.

Users Q Type to search ▼

☐	Name ↑	Origin	Username	User Groups	Roles	Status	Actions
☐	Acme User acme@email.com	Local	acme		account-admin account-user +1	Active	✎ ✉ 🔒 🗑
☐	Admin Agent agent-admin@email.org	Local	agent-admin		account-admin account-user	Active	✎ ✉ 🔒 🗑
☐	bora2 bora2 baybora.aksoy@digital.ai	Local	baybora.aksoy@digital.ai		account-user	Pending	✎ ✉ 🔒 🗑
☐	Ryan Gamble rgamble@digital.ai	Local	rgamble		account-user account-admin	Active	✎ ✉ 🔒 🗑
☐	User Agent agent-user@email.org	Local	agent-user		account-user	Active	✎ ✉ 🔒 🗑

Rows per page: 25 ▼ 1-5 of 5 < >



Users Q Type to search ▼

☐	Name ↑	Origin	Username	User Groups	Roles	Status	Actions
☐	bora2 bora2 baybora.aksoy@digital.ai	Local	baybora.aksoy@digital.ai		account-user	Pending	✎ ✉ 🔒 🗑

Rows per page: 25 ▼ 1-1 of 1 < >

Create Applications

The process for creating applications has now been improved, so that it is now more intuitive and simpler to follow. For more information, see [Create Applications](#).

Manage Clients

Clients are now automatically created as part of our improved application workflow. However, Administrators can also create standalone clients with specific configurations if necessary. For more information, see [Clients](#).

Audit Log

Audit Log records now provide additional information – User details, target entity details, and the change summary. For more information, see [Audit Log](#).

Miscellaneous Changes

- The Call-To-Action (CTA) links sent to a user via email to perform an operation are now valid for a longer time.
- Administrators now have more enhanced control over the self-registration feature. For more information, see [Account Settings](#) and [Default IdP](#).

January 12, 2023

Group Data Mappers

Administrators can create group mappers to ensure that users are added to Platform groups based on assignments in the customer's corporate identity provider. For more information, see [Map Group Data](#)

Miscellaneous Changes

- Initial admin users are no longer created automatically. Digital.ai support will create the first admin user for new customers.
- If a customer account is already configured to use a corporate identity provider, any users that try to self-register on that account will now be redirected to the corporate login page.

December 1, 2022

User Self-Registration Enhancements

Administrators can now automatically assign self-registered users to a specific user group (or groups) by choosing the new **Assign new self-registered users to this group** option when creating or editing a group. For more information, see [User Groups](#).

All new self-registered users are added to a group called **Self-Registered** by default.

User group detail

Group name *

Description

☒ Assign new self-registered users to this group

Add users

☐ All users
0/2 users selected

🔍 Type to search

- ☐ Administrator Account-Admin
- ☐ Steve Falcon

Add >

< Remove

☐ Users added to the group
0/0 users selected

🔍 Type to search

Cancel

Create user group

Additionally, administrators can now use the Settings page to enable or disable self-registration and manage a whitelist of approved domains. For more information, see [Account Settings](#).

Account Settings

Name *

ExampleTech

Vanity Domain *

exampletech

External ID

☐ Disabled

Self Registration

Domain Whitelist

Add

☒ Allow user registration from domain whitelist

Local User Password Improvements

Previously, when administrators created a local user they were required to manually set a password for the user and communicate that password with the user directly.

Now, when a local user is created the Platform automatically sends an email to the user prompting them to set a password. If necessary, administrators can resend this email from the Users page.

[illegible]

October 19, 2022

Digital.ai Identity

This release introduces the concept of *Digital.ai Identity*, which is a simplified way of describing the unified identity management that allows users to seamlessly move between Digital.ai products and services. This is not a change in functionality, but rather an improvement on the way we communicate about the integrated authentication capabilities offered by the Digital.ai Platform.

User Self-Registration

This feature allows customer end users to create their own Digital.ai Identity without being provisioned by an administrator. This is especially useful because it provides users with access to the Digital.ai community, support, and documentation portals before an administrator has had a chance to set up the account.

For more information, see [User Self-Registration](#).

Overview Page

The newly redesigned Overview page gives all users a way to quickly navigate to their Digital.ai products and services; shows administrators additional information about their account; and provides administrators with direct access to manage applications, users, and SSO integrations.

ExampleTech

Overview

Applications

Audit log

Settings

USER MANAGEMENT

Users

User groups

SSO

Identity providers

Clients

Platform overview

The Platform enables you to manage users and SSO.

SS

Steve Smith

ssmith@example.com

Account Admin

Edit Profile

E

ExampleTech

https://exampletech.staging.digital.ai

Support portal

Community

Product documentation

Create new application

There are no applications configured for your account. Click below to get started by creating a new application.

Create new application

Read documentation

View All

Users

You have 3 users.

Create user

Active users

3

Disabled users

0

Read documentation

View All

SSO / Identity providers

You have 3 identity providers.

Setup Identity Provider

Identity Provider Okta 2

Redirect Uri: https://identity.staging.digit...

Disabled

digital.ai

Manage Applications

Platform administrators can now create and manage applications on the new Applications page, which can be accessed from the side navigation or the Create new application button on the Overview page.

digital.ai[™]

Platform

?

SS

ExampleTech

Overview

Applications

Audit log

Settings

USER MANAGEMENT

Users

User groups

SSO

Identity providers

Clients

<

digital.ai[™]

Applications

>

Create application

Application

Select product
Intelligence

Name *

URL *

Description

Enabled

Instance details

Production instance

Non-production instance

Authentication

Federate Digital.ai Identities to this application

Cancel

Create application

As a reminder, an application is any Digital.ai product or service that is connected to the Platform in order to provide federated user access based on a customer's identity provider.

For more information, see [Applications](#).

Miscellaneous Changes

- Local users can now reset their own password via a new [Forgot Password?](#) link on the Platform login page.
- A new question mark (?) icon at the top of the page provides users with direct access to the Support, Documentation, and Community portals.
- Improved the log in flow with additional help text and guidance for determining which credentials to use for a user's Digital.ai Identity.

September 12, 2022

- This is the initial release of the Digital.ai Platform, with a focus on providing customers with a unified authentication experience for all users across certain products as well as the Digital.ai support, documentation, and community portals. To learn more, see [Getting Started](#).

 Getting Started

Introduction to basic instructions and key concepts for administrators getting started with the Digital.ai Platform.

 FAQ

This topic provides answers to common questions related to using the Digital.ai Platform

 Digital.ai Assistant

Learn to use the Digital.ai Assistant for instant information on Digital.ai products along with its features, limitations, ...

 Vanity Subdomains

The Vanity Subdomain account setting lets you specify the customer-specific part of the URL to which your users w...

 Account Settings

Overview of account configuration options for administrators on the Digital.ai Platform.

 Monitor Activity with the Audit Log

Learn how to use the Audit Log to monitor user and system activity across the Platform.

Getting Started

New Digital.ai Platform administrators may be wondering where to start. The following basic concepts and workflows will guide you in making the most out of your Digital.ai experience.

Key Concepts

Before you dig in to everything the Platform has to offer, you should familiarize yourself with the following terms:

- **The Digital.ai Platform:** An integrated set of shared services that provides a unified experience with seamless user authentication across all Digital.ai applications and portals (documentation, support, etc).
- **Account:** An instance of the Digital.ai Platform dedicated to a specific customer, with a unique domain, users, data, and applications. Also known as a tenant.
- **Single sign-on (SSO):** An authentication method that allows users to log into multiple services and applications using the same credentials.
- **Identity provider (IdP):** A single sign-on service that owns and maintains a directory of user credentials and an authentication mechanism. For example, Azure AD or Okta.
- **Application:** Any Digital.ai product or service (such as Intelligence or Continuous Testing) that is connected to the Platform in order to provide federated user access based on your IdP. Also known as a Client.

Account Setup

Before you can begin configuring the Platform to integrate SSO and add applications, a representative from your company must work with Digital.ai to create an account. During this process Digital.ai will provide you with a Vanity Subdomain and administrator user credentials. Digital.ai may even walk you through most of this process. For more information see [Vanity Subdomains](#)

Your Vanity Subdomain is formatted like this: `https://<customername>.<region>.digital.ai`

For example: `https://exampletech.us.digital.ai`

Contact Digital.ai [Customer Support](#) if you have questions about getting this process started.

Recommended Workflow for Configuring the Platform

Once your account is created you can begin adding additional users, connecting your Digital.ai applications, etc.

For product-specific workflows, see:

- [How to Integrate Release with the Platform](#)

Create Local Users

It may be useful to add additional administrator users in the Platform. For example, you could create a user for the DevOps or IT administrator responsible for managing your SSO connections or your existing Digital.ai applications.

NOTE

Administrators can review the list of local users to identify whether self-registered users should be in the system or not, and remove them if necessary.

To learn about user roles and how to manually create a local user, see [Users](#).

Connect to your Identity Provider for SSO

Adding a few local users is easy, but your organization likely has hundreds of employees who will need access to the Platform, so adding them all manually would be a truly laborious task.

Instead, we recommend integrating the Platform into your existing corporate SSO ecosystem. This will allow your users to securely authenticate and access their Digital.ai applications and portals with the same corporate credentials they already use.

Keep the following tips in mind when connecting to your identity provider:

- You are not required to integrate with an identity provider; you could create and manage all users locally within the Platform if you want.
- You can add more than one identity provider if necessary.

- We recommend that you set an identity provider as default to skip the Digital.ai login screen entirely and send users directly to the identity provider login.

To learn more about managing SSO for the Platform, see [Manage Identity Providers](#).

Integrate your Digital.ai Applications

In order for your users to seamlessly authenticate through the Platform into your Digital.ai applications, you may need to add those applications on the Platform.

For more information about applications and how to add them, see [Manage Applications](#).

Onboard Users

Your SSO is configured. Your users are authenticating. Your applications are integrated. What to do now?

We recommend making an announcement to your team that they can begin using the Digital.ai Platform authentication to access the Digital.ai applications and customer portals.

If you're an existing customer completing a migration, keep the following in mind:

- The login process may look slightly different because users will be redirected to the Platform login screen.
- When you connect to an identity provider after creating local users, those local users will be prompted to merge their local user account with their SSO user account.
- Instruct your users to stop using their old application-specific login credentials to avoid any confusion caused by using multiple user accounts.
- Some Digital.ai product URLs have changed as part of the Platform integration, so you may need to update bookmarks.

Frequently Asked Questions (FAQ)

Welcome to the **FAQ** page. Below you will find answers to the most commonly asked questions about the Platform's features, access, integrations, analytics, and troubleshooting.

Access and Configuration

1. How do I access the Platform?

You can access the Platform using your organization's configured URL. You must have valid login credentials provisioned by your administrator.

For more information, see [Sign-in Helper](#) and [Getting Started](#).

2. How to Configure the IDP?

Digital.ai Platform supports the following :

- Username/password login
- Single Sign-On (SSO) via SAML 2.0 or OIDC
- Multi-Factor Authentication (MFA) based on your organization's configuration

For detailed steps, [Configuring IDP](#).

3. I forgot my password. What should I do?

Click **Forgot Password?** on the login page and follow the instructions. If you are using SSO, contact your IT administrator for account recovery.

For more details, see [Reset Password](#).

4. How do I self-register for an account?

Users with approved email domains can self-register themselves and create their own Digital.ai Identity without being provisioned by an administrator. This is especially useful for providing users with access to

the Digital.ai community, support, and documentation portals before an administrator has had a chance to set up the account.

If your organization allows self-registration, you can create your own account using your corporate email. For more information, see [User Self-Registration](#).

5. What is a Vanity Subdomain?

A vanity subdomain is a unique, customer-specific part of the URL for accessing the Platform Console. For more information, see [Vanity Subdomains](#).

Users and Roles

6. What roles are available on the Platform?

The Platform includes several roles, including:

- `account-admin`
- `account-user`
- `account-analytics-author`
- `account-application-admin`
- `account-service`

Each role comes with specific permissions for managing users, applications, analytics, and integrations.

[Learn more about roles](#)

7. How do I assign roles to users?

Administrators can assign roles through the **Identity & Access Management** settings. You can assign roles manually, through SSO group mapping, or using mappers.

For more information, see [User Groups](#) and [Map Group Data](#).

8. How do I merge or link user accounts?

If you have multiple accounts (e.g., local and SSO), you can merge them for a unified experience. See [User Merge Flow](#).

Integrations

9. What systems can the Platform integrate with?

Digital.ai Platform supports integration with:

- Identity providers (e.g., Azure AD, Okta)
- CI/CD tools (e.g., Jenkins, GitLab)
- ITSM tools (e.g., ServiceNow, Jira)
- Source control (e.g., GitHub, Bitbucket)

For more, see [Source Integrations](#).

10. How do I add a new integration with Platform products?

Navigate to **Integrations** in the Platform settings and select the integration type. Each integration comes with a guided setup process. Refer to [Integration Guide](#), [Integrate Release](#), or [Integrate Deploy](#) for step-by-step instructions.

Analytics and Reporting

11. How do I access analytics dashboards?

Users with the `account-analytics-author` role can access dashboards under **Analytics** in the main navigation. Dashboards can be customized and shared with other users.

See [Accessing Dashboards](#).

12. How do I create or customize dashboards?

You can create, customize, and manage dashboards using the Analytics module. For more, see [Creating Dashboards](#), [Customizing Dashboards](#), and [Manage Dashboards](#).

13. How do I filter or view dashboard details?

You can filter dashboards by author, category, or state, and view detailed metadata. See [Filtering Dashboards](#) and [Viewing Dashboard Details](#).

14. Can I export reports?

Yes. Reports and dashboards can be exported in formats such as **PDF**, **CSV**, or **Excel** for offline analysis.

Datasets

15. How do I create and manage datasets?

You can create, edit, duplicate, extend, and publish datasets. For more information, see [Datasets Creation](#), [Managing Datasets](#), and [Actioning in Created Datasets](#).

16. How do I preview or explore datasets?

Preview datasets using the **Preview dataset** option, and explore details such as columns, types, and expressions. See [Previewing Datasets](#) and [Exploring Datasets](#).

API and Technical Questions

17. Where can I find the API documentation?

API documentation is available under **API > API Docs** in the Platform, or directly at [API Reference](#) and [API Overview](#).

18. How do I use access tokens for API authentication?

Access tokens are used for API authentication and integration. For more, see [Access Tokens](#).

Security and Compliance

19. How do I manage IP allow lists?

Administrators can add external IP addresses to the allow list for secure access. See [IP Address Allow List](#).

20. Where can I find information about copyright and usage rights?

See [Copyright](#) for details on ownership, licensing, and usage rights.

Other Resources

- [Glossary](#)
- [Release Notes](#)
- [Digital.ai Assistant](#)
- [Metadata Viewer](#)
- [Code Standardization](#)

For further assistance, visit the [Customer Support Portal](#).

Digital.ai Assistant

Introduction

The Digital.ai Assistant uses the power of AI to provide instant and secure information about all Digital.ai products. Powered by OpenAI, the Digital.ai Assistant is hosted locally on our own servers, and pulls information from a variety of Digital.ai resources (including documentation, support tickets, and knowledge base articles).

Things to Know

As the Digital.ai Assistant is in an early access (beta) release, the feature is still being improved and as such you should keep the following in mind:

- Referential links to product docs are not yet supported.
- Information from product documentation is retrieved for the latest version only.
- Conversational questions and answers are not supported. For example, questions like "tell me more" would not return any result.

How to Use the Assistant

From the Digital.ai Platform:

1. Click the Digital.ai Assistant icon on the top right corner of the page.



2. Identify the product for which you need assistance (for example, Release) and click the **Ask a question** button in that product box.
3. Enter your query in the chat box.

Vanity Subdomains in the Platform

A **vanity Subdomain** is a distinct, user-friendly, and URL-friendly identifier assigned to each account or tenant within the Digital.ai Platform. It is designed to simplify tenant identification and enhance usability by providing a clean and meaningful representation of the tenant in URLs.

Vanity Subdomains are frequently used in multi-tenant SaaS applications, as they provide unique identifiers for different customers accessing a web application, such as **staging**, **EU**, and **US**.

WARNING

Changing the vanity subdomain offers flexibility but comes with important considerations. Always evaluate the potential impacts on **IDP configurations**, **user bookmarks**, and **invitations** before making changes.

When a customer's tenant is automatically created in the Digital.ai Platform, the tenant name undergoes a standardization process. This ensures the name is formatted appropriately to create the default subdomain. The standardization process includes the following steps:

- Converting the name to **lowercase**.
- Removing any **spaces** and **special characters**.
- Producing a clean, URL-safe subdomain name.

For example, if a customer like **The Widget Emporium** wants their Platform to be represented by the acronym "widget", the user-defined subdomain might look like `widget.us.digital.ai`.

Customers have the flexibility to edit this **vanity subdomain** in the **Account Settings** page to better suit their branding needs. However, changing the vanity subdomain can have significant implications that users must be aware of.

Key Uses of Vanity Subdomains

1. Account-Specific URLs

Vanity Subdomains are embedded in URLs to uniquely identify a Platform account.

- The **Digital.ai Platform UI**, for instance, incorporates the vanity domain to route users directly to their Platform interface.

2. Authentication and Identity Service Integration

Vanity domains are integral to the **identity service**, where they are used to:

- Map incoming authentication requests to the correct tenant.
- Determine customer-specific **authentication rules** and **identity provider (IDP) configurations**.
- Ensure secure and seamless handling of user authentication.

Edit Your Vanity Subdomain

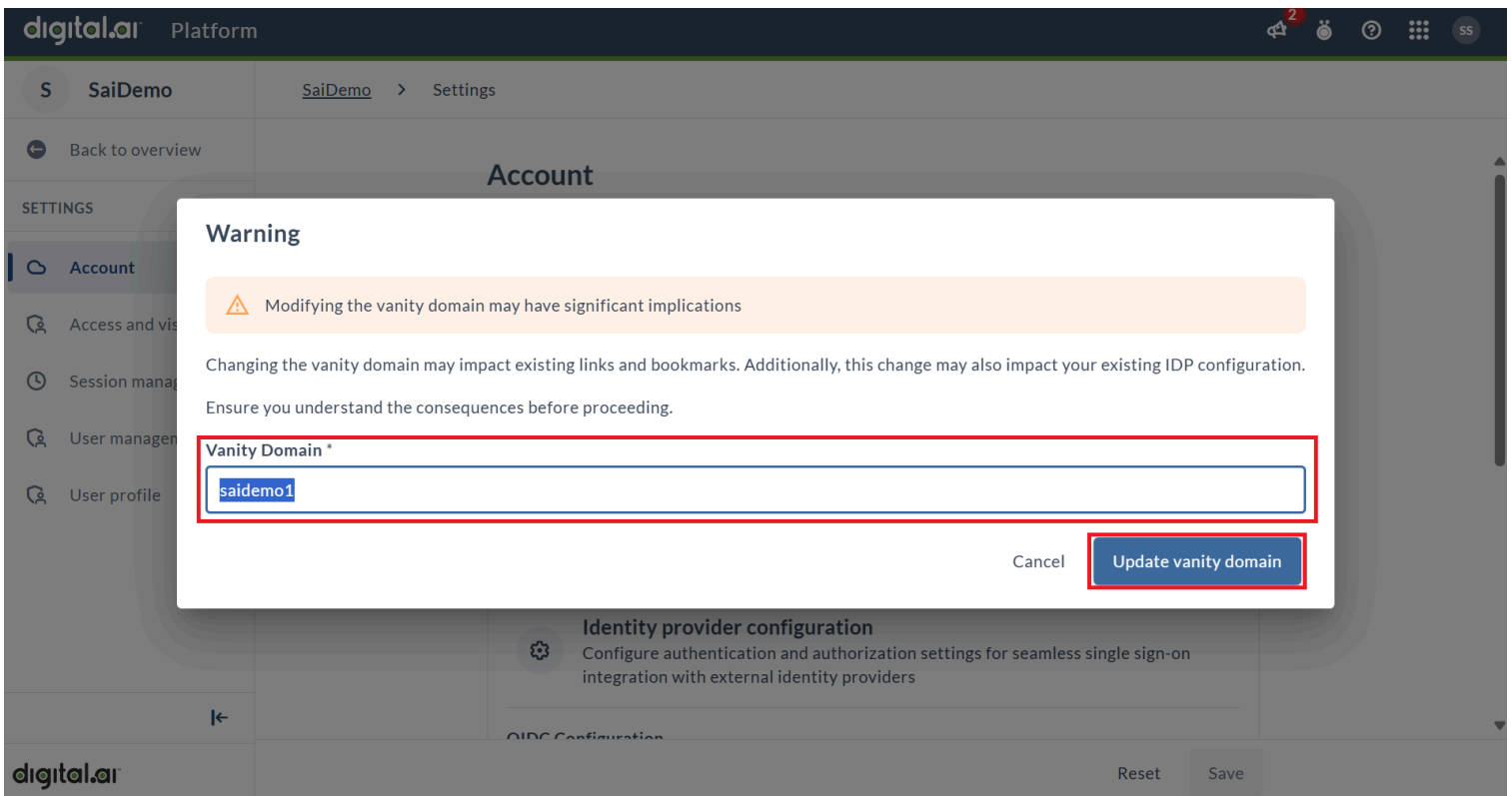
A vanity subdomain allows you to customize the URL used to access your account. Follow these steps to edit your vanity subdomain.

1. Log in to your account. Go to the **Accounts** section under **Settings**

The screenshot shows the digital.ai Platform interface. The top navigation bar includes the logo, the word 'Platform', and several utility icons. The left sidebar contains a 'SailDemo' header and a 'SETTINGS' menu with options like 'Account', 'Access and visibility', 'Session management', 'User management', and 'User profile'. The main content area is titled 'Account' and contains two sections. The first section, 'Account settings', includes a 'Name' field with the value 'SailDemo' and a 'Vanity domain' field with the value 'saildemo'. The 'Vanity domain' field is highlighted with a red rectangular box, and an 'Edit' button is located to its right. Below this is an 'Enable' checkbox which is checked. The second section, 'Identity provider configuration', includes a gear icon and a description: 'Configure authentication and authorization settings for seamless single sign-on integration with external identity providers'.

2. Locate the **Vanity Domain** field. Click **Edit**.

3. Enter the new vanity subdomain in the provided field. Click **Update Vanity Domain** to save your changes.



Side Effects of Editing Vanity Subdomains

Impact on IdP Configuration

If an **Identity Provider (IdP)** configuration is already configured, modifying the vanity subdomain will require the following actions:

- The IDP configuration will need to be **updated or recreated** to reflect the new URLs.
- For example, IDPs like **Entra ID** rely on the correct URLs for proper authentication. Any mismatch in the URL can result in authentication failures.

NOTE

Ensure that your IDP configuration is updated immediately after changing the vanity subdomain to avoid service disruptions.

Broken Bookmarks

Editing the vanity subdomain will result in any **bookmarks** created with the previous URL becoming invalid. Users who rely on these bookmarks will need to:

- Locate the new URL.
- Update their bookmarks manually.

i NOTE

This may lead to confusion or difficulty accessing the Platform until the bookmarks are corrected.

Broken User Invitations

Any **user invitations** sent before the vanity subdomain change will no longer be functional. This is because:

- The invitation URLs embed the vanity subdomain.
- When the subdomain changes, the links within the invitations will point to a non-existent or incorrect location.

i NOTE

After updating the vanity subdomain, notify your users of the new URL and the need to update their bookmarks.

Account Settings

Administrators have the ability to access and manage all configurations from one location through the Settings page, giving them an overview of the Platform's configurable options.

When you expand the Settings option in the Overview page, you gain access to various tabs, which are described in this topic.

Account

Account settings

In this section, your account information is displayed, which include details such as the account name and the vanity domain. The vanity domain refers to the domain used to access your organization's tenancy. For more information see [Vanity Subdomains](#)

Identity provider configuration

In this section, your Identity provider's configuration files are available for download. You can download OIDC or SAML configuration file for use to authorize single sign-on integration with your identity providers.

Product analytics and guidance

Enabling this option allows the application to provide personalized feature guidance in the Platform's Overview page by tracking anonymous usage data. If you choose to disable this option, the product analytics banner will disappear, and you will no longer have access to the feature guidance.

Access and visibility

Support

In this section, access to support portal will be restricted only to the user group names mentioned in the "User groups" field. You can provide privilege to only users mentioned in this section's User groups field

for raising support tickets. By implying this restriction, you can reduce the number of support tickets being raised.

** NOTE**

Users with the Account admin role will always have unrestricted access to support.

Applications visibility

This section restricts the visibility of application instances in the Platform UI to only those belonging to the user groups specified in the "User group" field. By implementing this, the Platform UI does not display all application instances associated with that account.

** NOTE**

If no user groups are specified for application instances, all users associated with that account can view the instances.

Session management

Session lifespan

Platform Session Lifespan is the duration set for a Platform session to be active.

Access token lifespan

Platform Access Token Lifespan is an access token you get to enter the Platform. There can be multiple access tokens created within a Platform session.

Once the configured time for an access token expires, the user's session will be automatically refreshed until the specified Platform Session Lifespan is reached. However, once the Platform Session Lifespan expires, the user will be logged out of the Platform and will need to reenter their credentials to log in.

For example, set the Platform Session Lifespan to 10 hours and the Platform Access Token Lifespan to 5 minutes. In this scenario, the access token will refresh automatically every 5 minutes, and the user remains continuously logged in. However, once the 10-hour Platform session time expires, the user will be logged out and will need to reenter their credentials to log in.

User management

Self registration

In the User Self-Registration, users with approved email domains are allowed to create their own Digital.ai Identity without being provisioned by an administrator. This enables them to gain access to the Digital.ai community, support, and documentation portals. For more information, see [User Self-Registration](#).

In the following section, only users whose email domain matches with the one added in the list will be allowed to self-register.

To add approved email domains:

1. In *New Domain* field, enter all the approved email domains of the account one by one and click **Add**.
2. **Allow user registration from domain whitelist** is enabled by default, which allows only self-registered users with approved email domains.

You can optionally disable **Allow user registration from domain whitelist** if you want to restrict users from self-registering such as when an IdP is set as the "default".

Default user groups for Self-Registered users

In this section, you can designate default user groups for self-registered users only.

Default user groups for new users

In this section, you can designate default user groups for new users added through SSO or created locally. However, you have the ability to edit other user group assignments, either during manual user creation, or after the user has been created.

NOTE

Self-registered users are excluded in this field.

Monitor Activity with the Audit Log

Administrators can use the **Audit Log** page to view a detailed history of user and system activity. This feature helps track changes, monitor access, and support compliance efforts by recording key events across the Platform.

digital.aiPlatform

E

ExampleTech

ExampleTech

>

Audit log

Export to CSV

Overview

Applications

Audit log

Settings

USER MANAGEMENT

Users

User groups

SSO

Identity providers

Audit log

Type to search

Date & Time (UTC)	Performed by	Entity type	Event	Change summary	Action
July 10, 2025 - 11:07 AM	service-account-dai-svc-...	identity.user	Update...	Pending, Last Login Date	
July 10, 2025 - 11:06 AM	service-account-dai-svc-...	identity.user.passwo...	Update...		
July 10, 2025 - 8:03 AM	DAI User	identity.user	Created		
July 10, 2025 - 8:02 AM	DAI User	identity.user	Update...	Given Name, Family Name	
July 10, 2025 - 7:58 AM	DAI User	licensing.application	Created		
July 10, 2025 - 7:45 AM	service-account-dai-svc-...	identity.user	Update...	Pending, Last Login Date	
July 10, 2025 - 7:45 AM	service-account-dai-svc-...	identity.user.passwo...	Update...		

Rows per page: 251-9 of 9

Each entry in the Audit Log includes:

- **Date and time** of the event
- **Actor** who performed the action (e.g., a user)
- **Entity type** affected (e.g., Account, User, Application)
- **Event type** (e.g., Created, Updated, Deleted)
- **Change summary** (for update events only), including before and after values

View Audit Log Entries

Use the Audit Log to review historical activity across Platform, including who did what and when.

1. Log in to the Platform as an administrator.
2. In the left navigation, click **Audit log**.
3. Use the search bar to find entries by the actor's **username**, **first name**, or **last name**.
4. Apply filters to narrow results by:
 - **Actor**
 - **Action type**
 - **Target entity type**
 - **Action date**

View Entry Details

To view more information about a specific event:

- Click the **View audit log entry details** icon in the Action column, or click anywhere in the row, to open the event summary panel.
- The panel shows a summary of changes, including the exact values before and after the update.

Export the Audit Log

You can export the current view of the Audit Log in either **CSV** or **JSON** format. This is useful for offline analysis or compliance reporting.

NOTE

Exported data reflects the current filters applied.

How to Integrate Release with the Platform

Step-by-step guide for integrating Digital.ai Release with the Digital.ai Platform using existing SSO for user authentic...

How to Integrate Agility with the Platform

Step-by-step guide for integrating Digital.ai Agility with the Digital.ai Platform using existing SSO for user authentic...

How to Integrate Deploy with the Platform

Step-by-step guide for integrating Digital.ai Deploy with the Digital.ai Platform using existing SSO for user authentic...

How to Integrate Release with the Platform

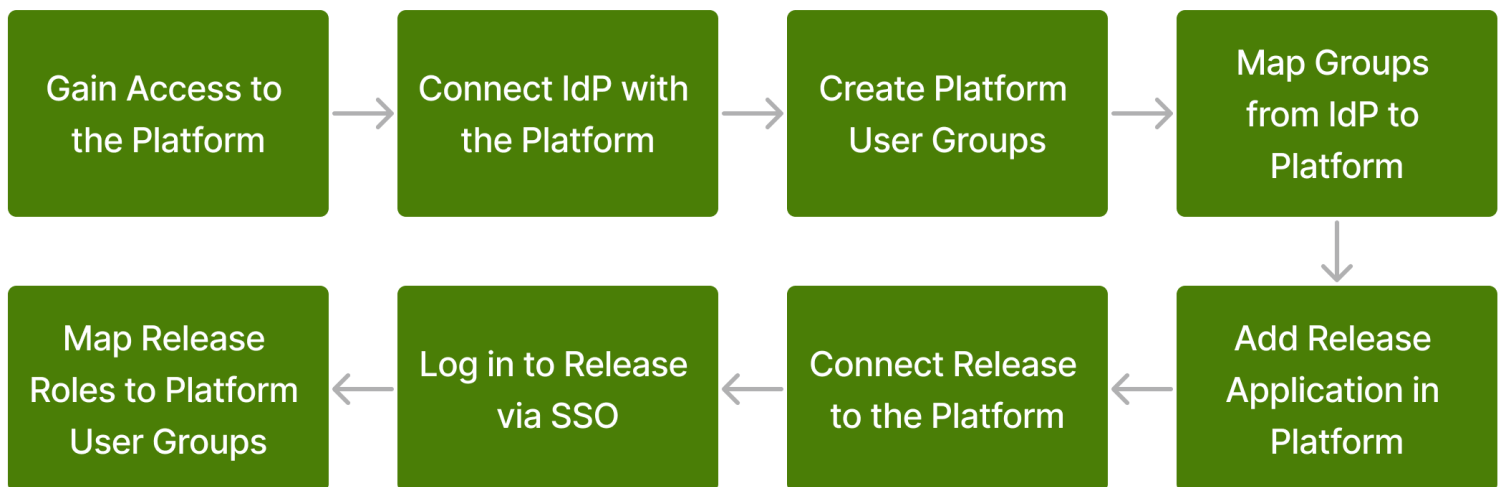
This guide provides step-by-step instructions for integrating Digital.ai Release with the Digital.ai Platform.

The Platform uses your existing single-sign on (SSO) infrastructure to securely authenticate users in Release using the same corporate credentials they already use. Acting as a bridge between your identity provider (IdP) and Release, the Platform grants access to Release based on user data from your IdP, eliminating the need for unique credentials in Release. This integration also allows you to map user groups in your IdP to specific roles in Release.

NOTE

This guide assumes that you have already installed Release and configured one or more roles. If you have not yet done so, see the [Release documentation](#)

The following diagram summarizes the workflow required to complete this integration:



If you have any questions or run into any issues following this guide, please reach out to [Customer Support](#).

Step 1: Gain Access to the Platform

Before doing anything else, you need an administrator user for your Platform account.

It is possible that an initial admin user could have already been created for you when your Digital.ai account was established, so we recommend checking for an existing administrator in your organization before reaching out to Digital.ai support. However, if you have no record of an administrator being created, then you should contact your Digital.ai representative to request an initial set of credentials. This initial administrator can invite others as needed.

During this process, you should have also received a unique URL for your Platform account, which you will use to perform all the tasks in this guide.

Your unique URL is formatted like this: `https://CUSTOMERNAME.REGION.digital.ai`

For example: `https://exampletech.us.digital.ai`

Step 2: Connect Identity Provider with the Platform

In this step, you'll learn how to connect your corporate IdP with the Digital.ai Platform.

NOTE

The process differs slightly based on whether you are using an OIDC provider or SAML provider. These differences are noted when appropriate.

Gather Required Data

Before you begin, you must obtain some essential details from your IdP.

This information can be obtained by reviewing the Digital.ai application configured in your IdP. If you have not already created an application for Digital.ai, you must do so before continuing. We recommend working with your IT team or whoever manages SSO administration at your company.

For OIDC Connections

- Client ID
- Client secret
- metadata URL (`.well-known/openid-configuration` endpoint)
- The claim names for the following user information: first name, last name, username, email

For SAML Connections

- metadata URL (different IdPs may have different names for this)
- The assertion names for the following user information: first name, last name, username, email.

Establish SSO Connection

To start, click the **Setup identity provider** button on the Overview page to open the configuration wizard. Alternatively, you can click **Identity Providers** in the left navigation, then click the **Add identity provider** button.

The screenshot shows the digital.ai Platform interface. The top navigation bar includes the digital.ai logo, the word "Platform", and several icons (notifications, settings, help, and a red "SF" button). The left sidebar contains a navigation menu with "ExampleTech" at the top, followed by "Overview" (highlighted), "Applications", "Audit log", "Settings", and a "USER MANAGEMENT" section with "Users", "User groups", and "SSO". Below "SSO" is "Identity providers". The main content area is divided into two sections. The top section, titled "Users", shows "You have 1 users." and a "Create user" button. It also displays "Active users: 1" and "Disabled users: 0". The bottom section, titled "SSO / Identity providers", includes the text "User will be either automatically created once you set up SSO, or you can start creating internal users." and a prominent blue button labeled "Setup identity provider" which is highlighted with a red rectangle. An illustration of a person holding a shield with a keyhole and a gear is also present. Both sections have a "Read documentation" link.

This wizard leads you through all the steps necessary to connect your IdP to the Platform. Most pages in the wizard include descriptions for each field and option, so you should be able to follow along easily, but this section includes some conceptual and clarifying information that will help you through the process.

Select provider

Overview

Applications

Audit log

Settings

USER MANAGEMENT

Users

User groups

SSO

Identity providers

digital.ar

Select provider

Config identity provider and metadata

General

Advanced config

Add mappers

Summary

Select authentication service

Select your organizations SSO protocol service

☒ Add OIDC provider

☐ Add SAML provider

Select identity provider

Select identity provider from the list for setting up authentications

☒ Azure AD

☐ Okta

☐ Other

Configure your identity provider

You can give your identity provider a custom name. This is the name that will be displayed in the configured identity provider's page and also on SSO button on the login page.

Identity Provider display name *

Azure AD

Cancel

Next >

On this page you'll enter basic details about your IdP, such as the SSO protocol service and the name that will appear on the login button.

Config identity provider and metadata

Overview

Applications

Audit log

Settings

USER MANAGEMENT

Users

User groups

SSO

Identity providers

Select provider

Config identity provider and metadata

General

Advanced config

Add mappers

Summary

Redirect URI

Use this redirect URI to setup your identity provider.

[https://identity.maging.digital.ai/auth/realms/default/protocol/openid-connect/callback](#)

How would you like to configure this metadata?

You need to configure your identity provider's metadata

☒ I have the metadata URL for my identity provider

☐ I have a file which contains the metadata

☐ I want to manually configure the identity provider

Enter Metadata URL *

[https://identity.maging.digital.ai/auth/realms/default/protocol/openid-connect/callback](#)

Metadata URL link from which Identity Provider configuration can be fetched

Import

Cancel

Previous

Next

This page provides you with the Redirect URI for your Platform site, and gives you the opportunity to prepopulate the rest of the wizard with necessary details

First, you'll need to copy the **Redirect URI** and then open a new browser tab or window to move over to your IdP account. There, use the Redirect URI to identify the Digital.ai Platform as a valid redirect URL in your IdP account. The process for completing this task will differ depending on which IdP you use. Depending on your role in your organization, you may need assistance from IT or whoever manages SSO administration at your company.

Once you've done this, you should be able to find the *metadata URL* if you hadn't already.

Now choose **I have the metadata URL for my identity provider** and paste the *metadata URL* into the **Enter Metadata URL field**, then click **Import**.

General

Overview

Applications

Audit log

Settings

USER MANAGEMENT

Users

User groups

SSO

Identity providers

1 Select provider

2 Config identity provider and metadata

3 General

4 Advanced config

5 Add mappers

6 Summary

Configure client credentials

Provide the client ID and client secret obtained from the identity provider

Client ID *

Client Secret *

Issuer

Authentication method

Defines the requested authentication method for the token endpoint. Possible values are 'Post' (application uses HTTP POST parameters) or 'Basic' (application uses HTTP Basic).

Client Authentication *

Client secret as post

Default Scopes

OpenID Connect defines the following scope values that are used to request Claims

Default Scopes

openidprofileemail

Authorization and token URL

Description

Authorization URL *

Token URL *

Cancel

Previous

Next

On this page, paste your Client ID and Client Secret values (which you obtained in the prerequisite step) into the appropriate fields.

The remaining fields on the page will be automatically completed, so you can accept all the defaults and continue to the next step in the wizard.

Advanced config

Overview

Applications

Audit log

Settings

USER MANAGEMENT

Users

User groups

SSO

Identity providers

Select provider

Config identity provider and metadata

General

Advanced config

Add mappers

Summary

Advanced Configuration

Optional

☐ Trust Email?

☐ Account Linking Only?

☐ Hide on Login Page?

First Login Flow

first broker login

Post Login Flow

Sync Mode

FORCE

Allowed clock skew (seconds)

3

☐ Pass login_hint?

☐ Pass current locale?

Cancel

Previous

Next

This page is entirely optional. Unless you have been specifically told otherwise, you can accept all the defaults and click **Next**.

Add mappers

The screenshot shows the Digital.ai user interface for configuring identity providers. On the left is a sidebar with navigation links: Overview, Applications, Audit log, Settings, and a section for USER MANAGEMENT containing Users, User groups, and Identity providers (which is highlighted). Below the sidebar is the Digital.ai logo. The main content area has a vertical progress bar with steps: Select provider, Config identity provider and metadata, General, Advanced config, Add mappers (the current step, highlighted with a blue circle and icon), and Summary. The 'Mappers' section features a table with columns 'Name', 'Category', and 'Type'. The table is currently empty, displaying 'No data found'. An 'Add' button with a dropdown arrow is in the top right corner. A context menu is open, showing 'Group mapping' and 'Mapper' (the latter is highlighted with a red box). At the bottom right of the section are 'Cancel', 'Previous', and 'Next' buttons.

This page allows you to add mappers to ensure that user data from your IdP is properly understood by the Platform. Your identity provider shares information about your users with Digital.ai in the form of key/value pairs (known as claims or assertions, depending on the IdP), and the Platform uses this data to create users in our system.

NOTE

Mappers are required for SAML connections, but optional for OIDC connections unless your IdP uses non-standard claim names.

OIDC

Whether or not you need to use mappers to handle this data is entirely dependent on your organization's unique situation, and in general the Digital.ai Platform expects to receive user attributes based on the set of standard *claims* as defined by OpenID. You can view the list of standard claims here:

https://openid.net/specs/openid-connect-core-1_0.html#StandardClaim.

If your data is stored as the claims identified in this list (i.e. `given_name`, `family_name`, `email`, etc.), then you typically would not need to bother creating any attribute mappers.

For example, if your IdP uses the standard claim `"email": john@example.com`, the Platform will automatically map that to the Platform's `email` user attribute.

However, if your IdP uses a claim called `"email_address": john@example.com`, then you would need to create a mapper to correctly get that data into the Platform's `email` user attribute.

SAML

Unlike OIDC, the SAML protocol has no standard naming conventions for the attributes it stores (which SAML tokens refer to as *assertions*). That is why we require mappers for SAML connections, because each IdP's assertions may be named differently. So in order for the Platform to understand the data correctly, you must provide the assertion values as they are named in your IdP.

When creating mappers for SAML connections, you *must* add mappers for the following user data: first name, last name, email.

Username data is automatically pulled from the `NameID` attribute (based on the `NameID Policy Format / Principal Type` fields defined in the SAML IdP). You do not need to create a mapper for `username` if you need to override the default assertion.

How to Add Mappers

If you have determined that you need to add mappers, then follow this procedure:

1. Click the **Add** drop-down arrow, and select **Mapper**.
2. In the **Add mapper** window, set the following fields:
3. **Name** is merely a way to identify the mapper. Enter something like `First Name Mapper`.
4. **Sync Mode** controls whether an update to a user attribute in your IdP will cause an update in the platform. We suggest using **INHERIT**.
 - FORCE always updates the Platform user when there is a change in your IdP.
 - IMPORT never updates the Platform user after they are created the first time, regardless of changes in your IdP.
 - INHERIT uses the value that has been configured on the **Advanced config** page of this IdP connection.
5. **Mapper Type** should be set to **Attribute Importer**.
6. (For OIDC providers only) **Claim** is the name of the claim as specified by your IdP.
7. **User Attribute Name** is the Platform user attribute that the data will be mapped to. This should be set to `username`, `email`, `firstName`, or `lastName` depending on the data you're mapping.

8. (For SAML providers only) **Attribute name** is the name of the assertion as specified in your IdP's SAML token. You can add the name in either **Attribute Name** or **Friendly Name** (you must complete at least one of the fields, but you do not need to complete both).
9. Click **Add Mapper**.
10. Repeat the previous steps to add additional mappers.

Summary

Overview

Applications

Audit log

Settings

USER MANAGEMENT

Users

User groups

SSO

Identity providers

<

digital.ai

Select provider

Config identity provider and metadata

General

Advanced config

Add mappers

Summary

Identity provider display name

Azure OIDC

Configuration detail

Authorization URL

Token URL

Client ID

Client secret

Authentication

Issuer

Scopes

Enabled

☒ Enabled

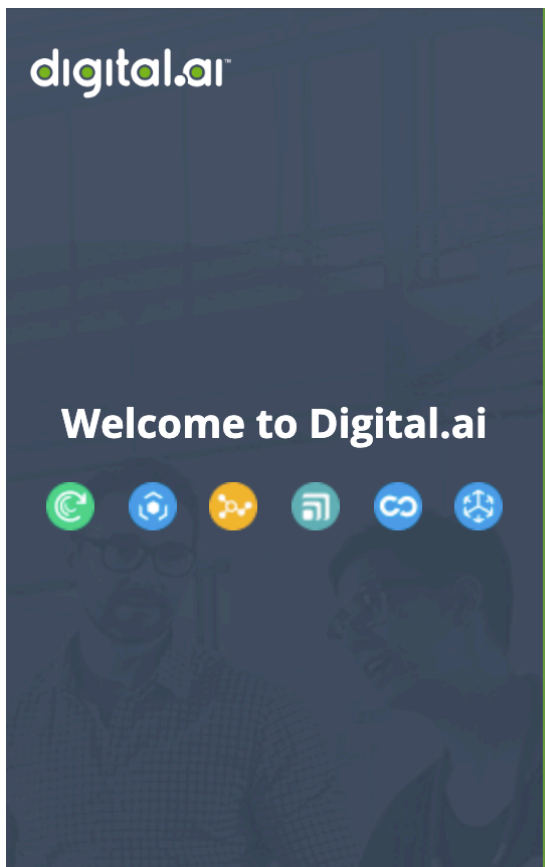
Cancel

< Previous

Create identity provider >

This page provides an overview of the configuration details for informational purposes.

To complete the wizard, click **Create identity provider**. A new button will now appear on the Platform login page with the name you added at the beginning of this procedure.



Sign in to your account

By signing in, I agree to Digital.ai's [Privacy Policy](#).

SSO Login

Or

Sign In Locally

If you do not have a user account, you can [self-register](#)

Set IdP as Default

We recommend setting this IdP as default, which will skip the Platform login screen and send users to the IdP authentication page as if they had clicked the button for it. If they already have an active session, most IdPs will redirect the user to the application directly and they will not see a login screen at all.

To set the IdP as default, return to the Identity providers page and click the **star** icon under Actions.

Identity providers



Name	Provider	Enabled	Redirect URI	Default	Actions
SSO Login	OIDC	True		★	  



TIP

If you need to override the default IdP login screen and authenticate using your local credentials, you can append the following query parameter to the end of your Digital.ai Platform account URL: `/?loginIdp=local`. For example: `https://exampletech.digital.ai/?loginIdp=local`.

Test SSO Connection

To ensure that you have properly connected with your IdP, you should now log out of the Platform and attempt to log in again using the newly configured IdP button (or via automatic redirect to your IdP if you set it as default per the previous section).

If everything has been configured properly, and as long as you are logged into a session with your IdP, you will be automatically logged in to the platform.

Assign Administrator Role to SSO User

We recommend continuing through the rest of this guide while logged in as your SSO user. However, as you will notice, your SSO user does not have administrator permissions by default. So, you should now use your local admin user to give the administrator role to your SSO user.

To get back to your local administrator user account, you can use the URL override mentioned previously. You can then use your local administrator account to assign the `account-admin` role to your SSO user (**Users > Actions > Edit > Roles**).

You can now log back in as your SSO user and continue on through the rest of the process.

Step 3: Manage Roles and User Groups

In this step, you'll learn how to create user groups in the Platform and use them to ensure that your users inherit specified group assignments from your IdP in order to have the proper roles and permissions in Release.

Let's assume that you have the following *user groups* configured in your IdP:

- allAdmins
- analysts
- endUsers

And you have the following *roles* configured in Release:

- Administrator User
- Digital.ai Analytics Service User
- End User

Here, the Platform will act as a bridge between the data in your IdP (user groups) and the permissions in Release (roles). Once you've completed this rest of this guide, all of your users will be automatically assigned roles in Release based on their associated user groups in the IdP.

For example, if Doug is part of the `allAdmins` group in Azure AD, then he will automatically be assigned the `Administrator User` role in Release.

 NOTE

Group mapping is only available for OIDC connections.

Find Group Name / ID

Before you proceed, you must retrieve the name or object ID (Azure AD only) of the group claim from your IdP. Where and how you find this information will differ depending on what IdP you're using.

 TIP

Specifically for Azure AD, you must use the object ID of the group, rather than the group name, because that is the field which Azure AD passes to OIDC applications like the Platform.

Create User Groups

Before group membership can be inherited from your IdP, you need to create one or more user groups in the Platform.

The Platform does not create any groups automatically; you must manually create a corresponding group in the Platform for every IdP group that you want to map.

The screenshot shows the 'User groups' management interface. The left sidebar contains navigation links: Overview, Applications, Audit log, Settings, and a 'USER MANAGEMENT' section with 'Users' and 'User groups' (highlighted). The main area shows a table of user groups with columns for Group name, Description, Synced with IDP, Users, and Actions. Two groups are listed: 'Self-Registered' and 'allAdmins'. An 'Add group' button is located in the top right corner.

☐	Group name ↑	Description	Synced with IDP	Users	Actions
☐	Self-Registered	Users created via self-registration will automatically ...	No	0	⋮
☐	allAdmins	A group to collect all site admins.	Yes	2	⋮

Rows per page: 25 ▾ 1-2 of 2 < >

To begin adding a group, click **User groups** in the left navigation, and then click **Add group**.

1. In **Group name**, add a name for the group. **This name must exactly match the group name or object ID (Azure AD only) as it exists in your IdP.**
2. In **Description**, you can elaborate on the purpose of the group.
3. Select **Sync with IdP**.
4. For this initial setup, you do not need to manually add any users.
5. Click **Create user group**.

Repeat this process to add additional groups as necessary.

IdP Group to Platform Group Mapping

Now, you'll create a mapper to enroll users in the correct Platform groups. This is important in order to bridge the gap between your IdP and Release, so that users can be automatically assigned the appropriate roles in Release.

You only need to create one mapper for this purpose, as it will pass all group IDs from your IdP and place users in correct groups in the Platform.

1. In the left navigation, under SSO, click **Identity providers**.
2. Find the IdP you want to edit, then click the **Edit** icon under Actions.
3. Click **Next** until you reach the **Mappers** page.
4. Click the **Add** dropdown and click **Group mapping**.
5. In **Claim**, enter the name or object ID (Azure AD only) of the group claim from your IdP.

6. Click **Add mapper**.

IdP Group to Platform Role Mapping

You may also want to create mappers to assign Platform-specific roles to users based on their group assignments in your IdP (for example, if you want to give the `account-admin` Platform role to users in the `allAdmins` IdP group).

NOTE

This will only affect users that need to work in the Platform itself (administrators, dashboard authors, IT personnel, etc), and would not have any impact on users or permissions in Release. Release-specific roles will be configured later in this guide.

Users are automatically assigned the `account-user` Platform role by default if you do not create these mappers.

The available Platform roles are:

- `account-admin`: Users with this role have access to all aspects of the Platform, including user management, dataset and dashboard configuration, SSO configuration, account settings, audit logs, etc.
- `account-application-admin`: Users with this role has all the same permissions as the `account-admin`, except for SSO configuration.
- `account-analytics-author`: Users with this role can view, add, and edit datasets and dashboards, as well as access assigned Digital.ai applications, support and documentation portals, and edit their own basic preferences.
- `account-user`: Users with this role are limited to viewing dashboards, accessing assigned Digital.ai applications, support and documentation portals, and editing their own basic preferences.

TIP

This mapping can be especially useful if you know that certain non-admin users will be responsible for managing your analytics dashboards. You should be sure to assign the `account-analytics-author` to any users who do not also need administrator permissions.

1. On the same **Mappers** page, click the **Add** dropdown and click **Mapper**.
2. In **Name**, enter something descriptive like `allAdmins mapper`.

3. Leave **Sync Mode** as **INHERIT**.
4. In **Mapper Type**, choose **Advanced Claim to Role**.
5. In **New Key**, enter `groups`.
6. In **New Value**, enter the name or object ID (Azure AD only) of the group claim from your IdP.
7. In **Select Role**, choose the Platform role that this group's users should belong to.
8. Click **Add mapper**.
9. Repeat the previous step for each group that you want to map to a role.

Step 4: Connect Release to the Platform

In this step, you'll learn how to establish a connection between the Platform and your Release instance for user management / login purposes. This step does not cover setting up the Cloud Connector or Data Collector.

Add Release as an Application in the Platform

First, you need to define your Release instance as an application in the Platform. This will then allow you to download a configuration file that you can embed into your Release build in order for Release to understand the configurations you've been making in the Platform.

1. In the left navigation, click **Applications**.
2. Click **Applications**.
3. Click **Create application**.
4. In **Select application**, choose **Release**.
5. In **Instance name**, enter a descriptive name for this instance.
6. Choose whether this will be a production or non-production instance.
7. Enter the URL for your Release instance.
8. On the **Advanced configuration** page, click **Next**.
9. On the **Mappers** page, click **Next**.
10. On the Get client ID & secret page, click **Download** to download the Release configuration file. There are a lot of details about Release integration on this page, and the release configuration file compiles everything into a format that Release will understand. You can always return here later to obtain specific details if necessary.
11. Click **Complete**.

Embed Release Config File into Release

The previous step downloads a file called `xl-release.conf`, aka the *Release configuration file*.

Rename this file to `reference.conf` and move it to the `ENVIRONMENT_NAME/digitalai-release/default-conf` directory in your Release instance (where `ENVIRONMENT_NAME` is the name of the directory where you have Release installed).

Restart the Release Server

Restart the release server and navigate to appropriate instance URL. If you set a default IdP earlier, you should now be automatically redirected to the Platform authentication and seamlessly logged in to Release. If not, you should use the SSO login button to log into Release as your SSO user.

Configure Roles in Release

For this last step, you must update your roles in Release to ensure that they properly sync with the Platform user groups you created earlier.

In Release, go to **Settings > Users and permissions > Roles** and edit any of the roles. In **Principals**, add the Platform user group name that corresponds to this role. Repeat this for all roles that you want to inherit group assignments. You may optionally want to create new roles for this purpose, depending on how your workflow is configured.

For example, edit the role called `Administrator User`, and add `allAdmins` as a Principal for the role.

Next Steps

At this point you have successfully connected Release with the Platform. From here, you can move on to any of the following tasks (and more that aren't listed here):

- Inform your users that they can begin accessing Release with their corporate SSO credentials.
 - You may also want to instruct them to stop using their old application-specific login credentials entirely to avoid any confusion caused by using multiple user accounts.
- Begin configuring Analytics dashboards. For more information, see [Dashboards](#).

How to Integrate Agility with the Platform

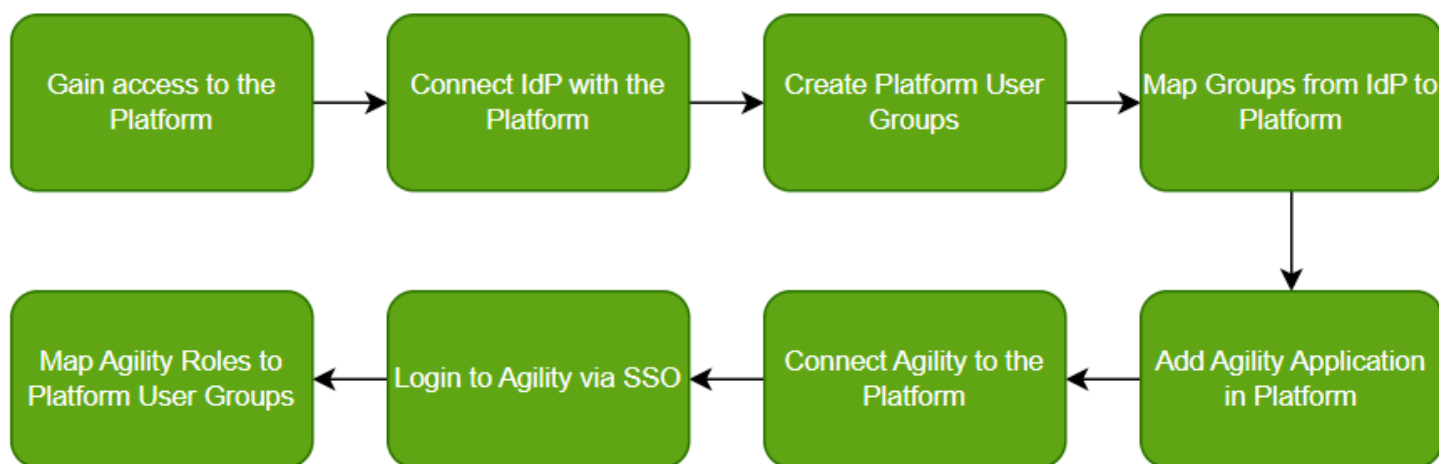
This guide provides step-by-step instructions for integrating Digital.ai Agility with the Digital.ai Platform.

The Platform uses your existing single sign-on (SSO) infrastructure to securely authenticate users in Agility using the same corporate credentials they already use. Acting as a bridge between your identity provider (IdP) and Agility, the Platform grants access to Agility based on user data from IdP, eliminating the need for unique credentials in Agility. This integration also allows you to map user groups in your IdP to specific roles in Agility.

i NOTE

This guide assumes that you have already installed Agility and configured one or more roles. If you have not yet done so, see the [Agility documentation](#)

The following diagram summarizes the workflow required to complete this integration:



If you have any questions or run into any issues following this guide, please reach out to Customer Support.

Step 1: Gain Access to the Platform

Before doing anything else, you need an administrator user for your Platform account.

It is possible that an initial admin user could have already been created for you when your Digital.ai account was established, So we recommend checking for an existing administrator in your organisation before reaching out to Digital.ai support. However, if you have no record of an administrator being created, then you should contact your Digital.ai representative to request an initial set of credentials. This initial administrator can invite others as needed.

During this process, you should have also received a unique URL for your Platform account, which you will use to perform all the tasks in the guide.

Your unique URL is formatted like this: `https://CUSTOMERNAME.REGION.digital.ai` For example:
`https://exampletech.us.digital.ai`

Step 2: Connect Identity Provider with the Platform

In this step, you'll learn how to connect your corporate IdP with the Digital.ai Platform.

NOTE

The process differs slightly based on whether you are using an OIDC provider or SAML provider. These differences are noted when appropriate.

Gather Required Data

Before you begin, you must obtain some essential details from your IdP.

This information can be obtained by reviewing the Digital.ai application configured in your IdP. If you have not already created an application for Digital.ai, you must do so before continuing. We recommend working with your IT team or whoever manages SSO administration at your company.

For OIDC Connections

- Client ID
- Client Secret
- Metadata URL ([.well-known/openid-configuration endpoint])

- The claim names for the following user information: first name, last name, username, email

For SAML Connections

- Metadata URL (different IdPs may have different names for this)
- The assertion names for the following user information: first name, last name, username, email.

Establish SSO Connection

To start, click the Setup identity provider button on the Overview page to open the configuration wizard. Alternatively, you can click Identity Providers in the left navigation, then click the Add identity provider button.

The screenshot displays the digital.ai Platform interface. The top navigation bar includes the digital.ai logo, the word "Platform", and several icons: a bell with a red "5" badge, a person icon, a question mark, and a red "SF" badge. The left sidebar features a navigation menu with "ExampleTech" at the top, followed by "Overview" (highlighted with a blue bar), "Applications", "Audit log", and "Settings". Below these is a "USER MANAGEMENT" section containing "Users", "User groups", and "SSO". Under "SSO", there is an "Identity providers" link. The main content area is divided into two sections. The top section, titled "Users", states "You have 1 users." and includes a "Create user" button. It also shows "Active users" as 1 and "Disabled users" as 0, with a "Read documentation" link and a "View all" link. The bottom section, titled "SSO / Identity providers", explains that users will be either automatically created or manually added. It features a prominent blue button labeled "Setup identity provider" which is highlighted with a red rectangle. Below this button is another "Read documentation" link. To the right of the text is an illustration of a person standing next to a large blue shield with a keyhole, with a gear icon nearby.

This wizard leads you through all the steps necessary to connect your IdP to the Platform. Most pages in the wizard include descriptions for each field and option, so you should be able to follow along easily, but this section includes some conceptual and clarifying information that will help you through the process.

Select provider

🏠

Overview

📦

Applications

📄

Audit log

⚙️

Settings

USER MANAGEMENT

👤

Users

👥

User groups

SSO

🔒

Identity providers

digital.ar

✍️

Select provider

●

Config identity provider and metadata

●

General

●

Advanced config

●

Add mappers

●

Summary

Select authentication service

Select your organizations SSO protocol service

☒ Add OIDC provider

☐ Add SAML provider

Select identity provider

Select identity provider from the list for setting up authentications

☒ Azure AD

☐ Okta

☐ Other

Configure your identity provider

You can give your identity provider a custom name. This is the name that will be displayed in the configured identity provider's page and also on SSO button on the login page.

Identity Provider display name *

Azure AD

Cancel

Next >

On this page you'll enter basic details about your IdP, such as the SSO protocol service and the name that will appear on the login button.

Config identity provider and metadata

Overview

Applications

Audit log

Settings

USER MANAGEMENT

Users

User groups

SSO

Identity providers

Select provider

Config identity provider and metadata

General

Advanced config

Add mappers

Summary

Redirect URI

Use this redirect URI to setup your identity provider.

<https://identity.maging.digital.ai/auth/realms/your-domain/protocol/openid-connect/callback>

How would you like to configure this metadata?

You need to configure your identity provider's metadata

☒ I have the metadata URL for my identity provider

☐ I have a file which contains the metadata

☐ I want to manually configure the identity provider

Enter Metadata URL *

<https://identity.maging.digital.ai/auth/realms/your-domain/protocol/openid-connect/callback>

Metadata URL link from which Identity Provider configuration can be fetched

Import

Cancel

Previous

Next

This page provides you with the Redirect URI for your Platform site, and gives you the opportunity to prepopulate the rest of the wizard with necessary details

First, you'll need to copy the **Redirect URI** and then open a new browser tab or window to move over to your IdP account. There, use the Redirect URI to identify the Digital.ai Platform as a valid redirect URL in your IdP account. The process for completing this task will differ depending on which IdP you use. Depending on your role in your organization, you may need assistance from IT or whoever manages SSO administration at your company.

Once you've done this, you should be able to find the *metadata URL* if you hadn't already.

Now choose **I have the metadata URL for my identity provider** and paste the *metadata URL* into the **Enter Metadata URL field**, then click **Import**.

General

Overview

Applications

Audit log

Settings

USER MANAGEMENT

Users

User groups

SSO

Identity providers

1 Select provider

2 Config identity provider and metadata

3 General

4 Advanced config

5 Add mappers

6 Summary

Configure client credentials

Provide the client ID and client secret obtained from the identity provider

Client ID *

Client Secret *

Issuer

Authentication method

Defines the requested authentication method for the token endpoint. Possible values are 'Post' (application uses HTTP POST parameters) or 'Basic' (application uses HTTP Basic).

Client Authentication *

Client secret as post

Default Scopes

OpenID Connect defines the following scope values that are used to request Claims

Default Scopes

openidprofileemail

Authorization and token URL

Description

Authorization URL *

Token URL *

Cancel

Previous

Next

On this page, paste your Client ID and Client Secret values (which you obtained in the prerequisite step) into the appropriate fields.

The remaining fields on the page will be automatically completed, so you can accept all the defaults and continue to the next step in the wizard.

Advanced config

Overview

Applications

Audit log

Settings

USER MANAGEMENT

Users

User groups

SSO

Identity providers

Select provider

Config identity provider and metadata

General

Advanced config

Add mappers

Summary

Advanced Configuration

Optional

☐ Trust Email?

☐ Account Linking Only?

☐ Hide on Login Page?

First Login Flow

first broker login

Post Login Flow

Sync Mode

FORCE

Allowed clock skew (seconds)

3

☐ Pass login_hint?

☐ Pass current locale?

Cancel

Previous

Next

This page is entirely optional. Unless you have been specifically told otherwise, you can accept all the defaults and click **Next**.

Add mappers

The screenshot displays the 'Add mappers' configuration page in the Digital.ai interface. The left sidebar contains navigation links: Overview, Applications, Audit log, Settings, and Identity providers (selected). Below these are sections for USER MANAGEMENT (Users, User groups) and SSO. The main content area shows a progress bar with steps: Select provider, Config identity provider and metadata, General, Advanced config, Add mappers (active), and Summary. The 'Mappers' table is currently empty, with columns for Name, Category, and Type. A dropdown menu is open next to the 'Add' button, showing 'Group mapping' and 'Mapper' (highlighted with a red box). At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

This page allows you to add mappers to ensure that user data from your IdP is properly understood by the Platform. Your identity provider shares information about your users with Digital.ai in the form of key/value pairs (known as claims or assertions, depending on the IdP), and the Platform uses this data to create users in our system.

(i) NOTE

Mappers are required for SAML connections, but optional for OIDC connections unless your IdP uses non-standard claim names.

OIDC

Whether or not you need to use mappers to handle this data is entirely dependent on your organization's unique situation, and in general the `{{site.data.identifiers.companyName}}` `{{site.data.identifiers.productName}}` expects to receive user attributes based on the set of standard *claims* as defined by OpenID. You can view the list of standard claims here: https://openid.net/specs/openid-connect-core-1_0.html#StandardClaim.

If your data is stored as the claims identified in this list (i.e. `given_name`, `family_name`, `email`, etc.), then you typically would not need to bother creating any attribute mappers.

For example, if your IdP uses the standard claim `"email": john@example.com`, the Platform will automatically map that to the Platform's `email` user attribute.

However, if your IdP uses a claim called `"email_address": john@example.com`, then you would need to create a mapper to correctly get that data into the Platform's `email` user attribute.

SAML

Unlike OIDC, the SAML protocol has no standard naming conventions for the attributes it stores (which SAML tokens refer to as *assertions*). That is why we require mappers for SAML connections, because each IdP's assertions may be named differently. So in order for the Platform to understand the data correctly, you must provide the assertion values as they are named in your IdP.

When creating mappers for SAML connections, you *must* add mappers for the following user data: first name, last name, email.

Username data is automatically pulled from the `NameID` attribute (based on the `NameID Policy Format / Principal Type` fields defined in the SAML IdP). You do not need to create a mapper for `username` if you need to override the default assertion.

How to Add Mappers

If you have determined that you need to add mappers, then follow this procedure:

1. Click the **Add** drop-down arrow, and select **Mapper**.
2. In the **Add mapper** window, set the following fields:
3. **Name** is merely a way to identify the mapper. Enter something like `First Name Mapper`.
4. **Sync Mode** controls whether an update to a user attribute in your IdP will cause an update in the platform. We suggest using **INHERIT**.
 - FORCE always updates the Platform user when there is a change in your IdP.
 - IMPORT never updates the Platform user after they are created the first time, regardless of changes in your IdP.
 - INHERIT uses the value that has been configured on the **Advanced config** page of this IdP connection.
5. **Mapper Type** should be set to **Attribute Importer**.
6. (For OIDC providers only) **Claim** is the name of the claim as specified by your IdP.
7. **User Attribute Name** is the Platform user attribute that the data will be mapped to. This should be set to `username`, `email`, `firstName`, or `lastName` depending on the data you're mapping.

8. (For SAML providers only) **Attribute name** is the name of the assertion as specified in your IdP's SAML token. You can add the name in either **Attribute Name** or **Friendly Name** (you must complete at least one of the fields, but you do not need to complete both).
9. Click **Add Mapper**.
10. Repeat the previous steps to add additional mappers.

Summary

Overview

Applications

Audit log

Settings

USER MANAGEMENT

Users

User groups

SSO

Identity providers

Select provider

Config identity provider and metadata

General

Advanced config

Add mappers

Summary

Identity provider display name

Azure OIDC

Configuration detail

Authorization URL

Token URL

Client ID

Client secret

Authentication

Issuer

Scopes

Enabled

Enabled

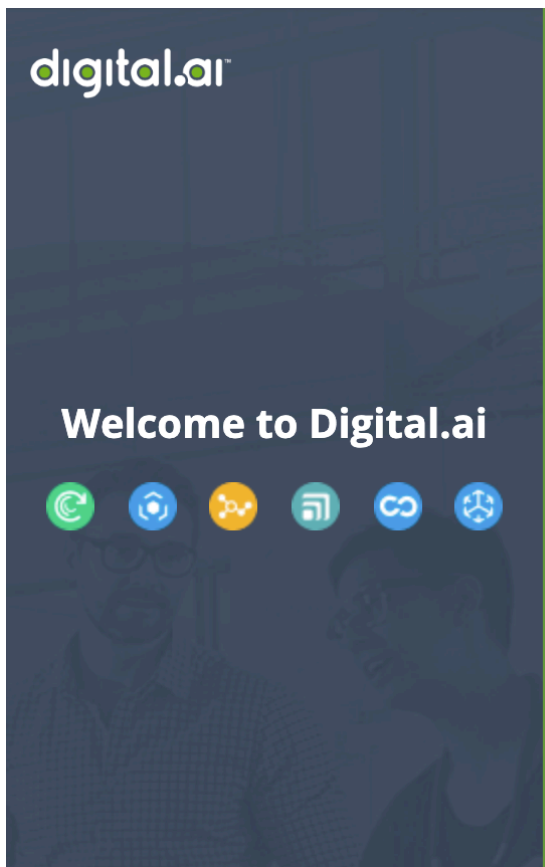
Cancel

Previous

Create identity provider

This page provides an overview of the configuration details for informational purposes.

To complete the wizard, click **Create identity provider**. A new button will now appear on the Platform login page with the name you added at the beginning of this procedure.



Sign in to your account

By signing in, I agree to Digital.ai's [Privacy Policy](#).

SSO Login

Or

Sign In Locally

If you do not have a user account, you can [self-register](#)

Set IdP as Default

We recommend setting this IdP as default, which will skip the `{{site.data.identifiers.productName}}` login screen and send users to the IdP authentication page as if they had clicked the button for it. If they already have an active session, most IdPs will redirect the user to the application directly and they will not see a login screen at all.

To set the IdP as default, return to the Identity providers page and click the **star** icon under Actions.

Identity providers



Name	Provider	Enabled	Redirect URI	Default	Actions
SSO Login	OIDC	True		★	  



TIP

If you need to override the default IdP login screen and authenticate using your local credentials, you can append the following query parameter to the end of your Digital.ai Platform account URL: `/?loginIdp=local`. For example: `https://exampletech.digital.ai/?loginIdp=local`

Test SSO Connection

To ensure that you have properly connected with your IdP, you should now log out of the Platform and attempt to log in again using the newly configured IdP button (or via automatic redirect to your IdP if you set it as default per the previous section).

If everything has been configured properly, and as long as you are logged into a session with your IdP, you will be automatically logged in to the platform.

Assign Administrator Role to SSO User

We recommend continuing through the rest of this guide while logged in as your SSO user. However, as you will notice, your SSO user does not have administrator permissions by default. So, you should now use your local admin user to give the administrator role to your SSO user.

To get back to your local administrator user account, you can use the URL override mentioned previously. You can then use your local administrator account to assign the `account-admin` role to your SSO user (**Users > Actions > Edit > Roles**).

You can now log back in as your SSO user and continue on through the rest of the process.

Step 3: Manage Roles and User Groups

In this step, you'll learn how to create user groups in the Platform and use them to ensure that your users inherit specified group assignments from your IdP in order to have the proper roles and permissions in Agility.

Let's assume that you have the following *user groups* configured in your IdP:

- allAdmins
- analysts
- endUsers

And you have the following *roles* configured in Agility:

- Administrator User
- Digital.ai Analytics Service User
- End User

Here, the Platform will act as a bridge between the data in your IdP (user groups) and the permissions in Agility (roles). Once you've completed this rest of this guide, all of your users will be automatically assigned roles in Agility based on their associated user groups in the IdP.

For example, if Doug is part of the `allAdmins` group in Azure AD, then he will automatically be assigned the `Administrator User` role in Agility.

 NOTE

Group mapping is only available for OIDC connections.

Find Group Name / ID

Before you proceed, you must retrieve the name or object ID (Azure AD only) of the group claim from your IdP. Where and how you find this information will differ depending on what IdP you're using.

 TIP

Specifically for Azure AD, you must use the object ID of the group, rather than the group name, because that is the field which Azure AD passes to OIDC applications like the Platform.

Create User Groups

Before group membership can be inherited from your IdP, you need to create one or more user groups in the Platform.

The Platform does not create any groups automatically; you must manually create a corresponding group in the Platform for every IdP group that you want to map.

The screenshot shows the 'User groups' management interface. The left sidebar contains navigation links: Overview, Applications, Audit log, Settings, and a 'USER MANAGEMENT' section with 'Users' and 'User groups' (highlighted). The main area shows a table of user groups with columns for Group name, Description, Synced with IDP, Users, and Actions. Two groups are listed: 'Self-Registered' and 'allAdmins'. An 'Add group' button is located in the top right corner.

☐	Group name ↑	Description	Synced with IDP	Users	Actions
☐	Self-Registered	Users created via self-registration will automatically ...	No	0	⋮
☐	allAdmins	A group to collect all site admins.	Yes	2	⋮

Rows per page: 25 ▾ 1-2 of 2 < >

To begin adding a group, click **User groups** in the left navigation, and then click **Add group**.

1. In **Group name**, add a name for the group. **This name must exactly match the group name or object ID (Azure AD only) as it exists in your IdP.**
2. In **Description**, you can elaborate on the purpose of the group.
3. Select **Sync with IdP**.
4. For this initial setup, you do not need to manually add any users.
5. Click **Create user group**.

Repeat this process to add additional groups as necessary.

IdP Group to Platform Group Mapping

Now, you'll create a mapper to enroll users in the correct Platform groups. This is important in order to bridge the gap between your IdP and Agility, so that users can be automatically assigned the appropriate roles in Agility.

You only need to create one mapper for this purpose, as it will pass all group IDs from your IdP and place users in correct groups in the Platform.

1. In the left navigation, under SSO, click **Identity providers**.
2. Find the IdP you want to edit, then click the **Edit** icon under Actions.
3. Click **Next** until you reach the **Mappers** page.
4. Click the **Add** dropdown and click **Group mapping**.
5. In **Claim**, enter the name or object ID (Azure AD only) of the group claim from your IdP.

6. Click **Add mapper**.

IdP Group to Platform Role Mapping

You may also want to create mappers to assign Platform-specific roles to users based on their group assignments in your IdP (for example, if you want to give the `account-admin` Platform role to users in the `allAdmins` IdP group).

NOTE

This will only affect users that need to work in the Platform itself (administrators, dashboard authors, IT personnel, etc), and would not have any impact on users or permissions in Agility. Agility-specific roles will be configured later in this guide.

Users are automatically assigned the `account-user` Platform role by default if you do not create these mappers.

The available Platform roles are:

- `account-admin`: Users with this role have access to all aspects of the Platform, including user management, dataset and dashboard configuration, SSO configuration, account settings, audit logs, etc.
- `account-application-admin`: Users with this role has all the same permissions as the `account-admin`, except for SSO configuration.
- `account-analytics-author`: Users with this role can view, add, and edit datasets and dashboards, as well as access assigned Digital.ai applications, support and documentation portals, and edit their own basic preferences.
- `account-user`: Users with this role are limited to viewing dashboards, accessing assigned Digital.ai applications, support and documentation portals, and editing their own basic preferences.

NOTE

This mapping can be especially useful if you know that certain non-admin users will be responsible for managing your analytics dashboards. You should be sure to assign the `account-analytics-author` to any users who do not need administrator permissions.

1. On the same **Mappers** page, click the **Add** dropdown and click **Mapper**.
2. In ad

3. In **New Value**, enter the name or object ID (Azure AD only) of the group claim from your IdP.
4. In **Select Role**, choose the Platform role that this group's users should belong to.
5. Click **Add mapper**.
6. Repeat the previous step for each group that you want to map to a role.

Step 4: Connect Agility to the Platform

In this step, you'll learn how to establish a connection between the Platform and your Agility instance for user management / login purposes. This step does not cover setting up the Cloud Connector or Data Collector.

Add Agility as an Application in the Platform

First, you need to define your Agility instance as an application in the Platform. This will then allow you to download a configuration file that you can embed into your Agility build in order for Agility to understand the configurations you have been making in the Platform.

1. In the left navigation, click **Applications**.
 - Alternatively, you can click the **Create Application** button on the Platform Overview page.
2. Click Applications button.
3. On the Select application page:
 - In **Select application**, choose **Agility** application from the list.
 - In **Instance name**, enter the application's custom name. (For example, Agility_demo)
 - In URL, enter the application's URL.
 - In Description, enter the application's description.
 - Click **Next**.
4. The Advanced configuration page is optional, and depending on the selection you made in the previous step, the majority of fields may be automatically filled in.
5. Click Next.
6. The Mappers page is optional, because mappers are automatically created as part of this process.
7. Click Next.
8. On the Get client ID and secret page, you can view a summary of the application details.
9. Click **Complete**.

Edit the Agility Config File

Now you need to edit the `versionone.web/user.config` file in your Agility instance to add entries for OIDC login. To do so, add or edit the following entries, using the application detail values that you obtained after adding Agility as an application in the Platform:

```
<add key="IsFederatedAuthModuleEnabled" value="true" />
<add key="AuthProvider" value="Oidc" />
<add key="Oidc:DiscoveryUri" value="DISCOVERY_URL_VALUE" />
<add key="Oidc:ClientID" value="OIDC_CLIENT_ID" />
<add key="Oidc:Secret" value="OIDC_SECRET" />
<add key="Oidc:Audience" value="OIDC_AUDIENCE" />
<add key="WebRoot" value="ROOT_OF_WEB_APPLICATION" />
```

If you need to allow logout, you must also add or update the following `user.config` entries:

```
<add key="DelegatedLogoutAllowed" value="true" />
<add key="LogoutRedirectUrl"
value="ROOT_OF_WEB_APPLICATION/APPLICATION_INSTANCE/OidcAuth.mvc/LogOut" />
<add key="FederatedLogoutRedirectUrl" value="DESTINATION_URL" />
```

- `DelegatedLogoutAllowed` to be true.
- `LogoutRedirectUrl` reflects your environment instance.
- `FederatedLogoutRedirectUrl` reflects the final URL destination after logout is complete.

Create Corresponding Users within Agility

It is essential to ensure that a corresponding member account is created within Agility with a **username** that aligns with what is provided by the platform.

The following warning will appear if a user does not have a corresponding member account in Agility.



Identity

[Redacted User Name]

You are not authorized to access this system.

Agility recognized you as the user shown above, but does not have a corresponding member account configured for that user. Please contact your internal Digital.ai Agility administrator for further assistance.

Next Steps

At this point you have successfully connected Agility with the Platform. From here, you can move on to any of the following tasks (and more that aren't listed here):

- Inform your users that they can begin accessing Agility with their corporate SSO credentials.
 - You may also want to instruct them to stop using their old application-specific login credentials entirely to avoid any confusion caused by using multiple user accounts.
- Begin configuring Analytics dashboards.

How to Integrate Deploy with the Platform

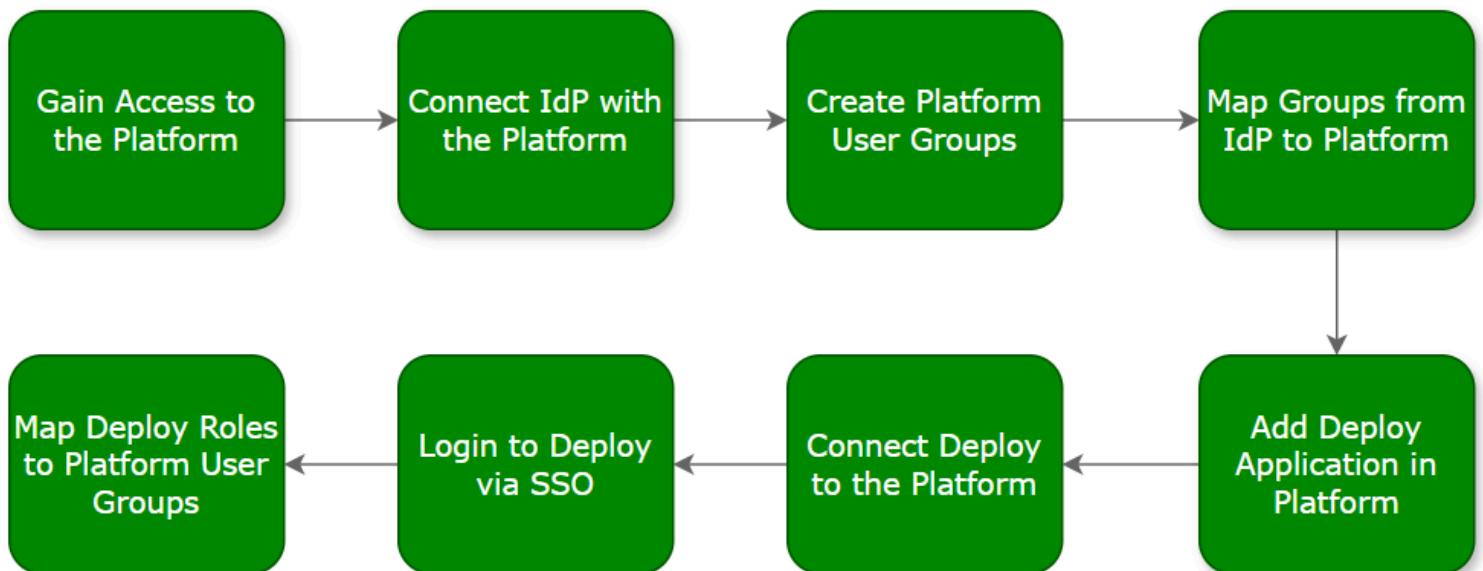
This guide provides step-by-step instructions for integrating Digital.ai Deploy with the Digital.ai Platform.

The Platform uses your existing single-sign on (SSO) infrastructure to securely authenticate users in Deploy using the same corporate credentials they already use. Acting as a bridge between your identity provider (IdP) and Deploy, the Platform grants access to Deploy based on user data from your IdP, eliminating the need for unique credentials in Deploy. This integration also allows you to map user groups in your IdP to specific roles in Deploy.

i NOTE

This guide assumes that you have already installed Deploy and configured one or more roles. If you have not yet done so, see the [Deploy documentation](#)

The following diagram summarizes the workflow required to complete this integration:



Step 1: Gain Access to the Platform

Before doing anything else, you need an administrator user for your Platform account.

It is possible that an initial admin user could have already been created for you when your Digital.ai account was established, so we recommend checking for an existing administrator in your organization before reaching out to Digital.ai support. However, if you have no record of an administrator being created, then you should contact your Digital.ai representative to request an initial set of credentials. This initial administrator can invite others as needed.

During this process, you should have also received a unique URL for your Platform account, which you will use to perform all the tasks in this guide.

Your unique URL is formatted like this: `https://CUSTOMERNAME.REGION.digital.ai`

For example: `https://exampletech.us.digital.ai`

Step 2: Connect Identity Provider with the Platform

In this step, you'll learn how to connect your corporate IdP with the Digital.ai Platform.

NOTE

The process differs slightly based on whether you are using an OIDC provider or SAML provider. These differences are noted when appropriate.

Gather Required Data

Before you begin, you must obtain some essential details from your IdP.

This information can be obtained by reviewing the Digital.ai application configured in your IdP. If you have not already created an application for Digital.ai, you must do so before continuing. We recommend working with your IT team or whoever manages SSO administration at your company.

For OIDC Connections

- Client ID
- Client secret
- metadata URL (`.well-known/openid-configuration` endpoint)
- The claim names for the following user information: first name, last name, username, email

For SAML Connections

- metadata URL (different IdPs may have different names for this)
- The assertion names for the following user information: first name, last name, username, email.

Establish SSO Connection

To start, click the **Setup identity provider** button on the Overview page to open the configuration wizard. Alternatively, you can click **Identity Providers** in the left navigation, then click the **Add identity provider** button.

The screenshot shows the digital.ai Platform interface. The top navigation bar includes the digital.ai logo, the word "Platform", and several icons (notifications, settings, help, and a red "SF" button). The left sidebar contains a navigation menu with "ExampleTech" at the top, followed by "Overview" (highlighted), "Applications", "Audit log", "Settings", and a "USER MANAGEMENT" section containing "Users", "User groups", "SSO", and "Identity providers". The main content area is divided into two sections. The top section, titled "Users", states "You have 1 users." and includes a "Create user" button. It also displays two metrics: "Active users" with a value of 1 and "Disabled users" with a value of 0. Below these metrics is a "Read documentation" link and a "View all" link with a right arrow. The bottom section, titled "SSO / Identity providers", contains the text: "User will be either automatically created once you set up SSO, or you can start creating internal users." Below this text is a blue button labeled "Setup identity provider", which is highlighted with a red rectangular border. To the right of the text is an illustration of a person standing next to a large blue shield with a keyhole, with a gear icon nearby. At the bottom of this section is another "Read documentation" link.

This wizard leads you through all the steps necessary to connect your IdP to the Platform. Most pages in the wizard include descriptions for each field and option, so you should be able to follow along easily, but this section includes some conceptual and clarifying information that will help you through the process.

Select provider

Overview

Applications

Audit log

Settings

USER MANAGEMENT

Users

User groups

SSO

Identity providers

Select provider

Config identity provider and metadata

General

Advanced config

Add mappers

Summary

Select authentication service

Select your organizations SSO protocol service

Add OIDC provider

Add SAML provider

Select identity provider

Select identity provider from the list for setting up authentications

Azure AD

Okta

Other

Configure your identity provider

You can give your identity provider a custom name. This is the name that will be displayed in the configured identity provider's page and also on SSO button on the login page.

Identity Provider display name *

Azure AD

Cancel

Next

On this page you'll enter basic details about your IdP, such as the SSO protocol service and the name that will appear on the login button.

Config identity provider and metadata

Overview

Applications

Audit log

Settings

USER MANAGEMENT

Users

User groups

SSO

Identity providers

Select provider

Config identity provider and metadata

General

Advanced config

Add mappers

Summary

Redirect URI

Use this redirect URI to setup your identity provider.

<https://identity.maging.digital.ai/auth/realms/your-tenant/protocol/openid-connect/callback>

How would you like to configure this metadata?

You need to configure your identity provider's metadata

☒ I have the metadata URL for my identity provider

☐ I have a file which contains the metadata

☐ I want to manually configure the identity provider

Enter Metadata URL *

<https://identity.maging.digital.ai/auth/realms/your-tenant/protocol/openid-connect/callback>

Metadata URL link from which Identity Provider configuration can be fetched

Import

Cancel

Previous

Next

This page provides you with the Redirect URI for your Platform site, and gives you the opportunity to prepopulate the rest of the wizard with necessary details

First, you'll need to copy the **Redirect URI** and then open a new browser tab or window to move over to your IdP account. There, use the Redirect URI to identify the Digital.ai Platform as a valid redirect URL in your IdP account. The process for completing this task will differ depending on which IdP you use. Depending on your role in your organization, you may need assistance from IT or whoever manages SSO administration at your company.

Once you've done this, you should be able to find the *metadata URL* if you hadn't already.

Now choose **I have the metadata URL for my identity provider** and paste the *metadata URL* into the **Enter Metadata URL field**, then click **Import**.

General

Overview

Applications

Audit log

Settings

USER MANAGEMENT

Users

User groups

SSO

Identity providers

1 Select provider

2 Config identity provider and metadata

3 General

4 Advanced config

5 Add mappers

6 Summary

Configure client credentials

Provide the client ID and client secret obtained from the identity provider

Client ID *

Client Secret *

Issuer

Authentication method

Defines the requested authentication method for the token endpoint. Possible values are 'Post' (application uses HTTP POST parameters) or 'Basic' (application uses HTTP Basic).

Client Authentication *

Client secret as post

Default Scopes

OpenID Connect defines the following scope values that are used to request Claims

Default Scopes

openidprofileemail

Authorization and token URL

Description

Authorization URL *

Token URL *

Cancel

Previous

Next

On this page, paste your Client ID and Client Secret values (which you obtained in the prerequisite step) into the appropriate fields.

The remaining fields on the page will be automatically completed, so you can accept all the defaults and continue to the next step in the wizard.

Advanced config

Overview

Applications

Audit log

Settings

USER MANAGEMENT

Users

User groups

SSO

Identity providers

Select provider

Config identity provider and metadata

General

Advanced config

Add mappers

Summary

Advanced Configuration

Optional

☐ Trust Email?

☐ Account Linking Only?

☐ Hide on Login Page?

First Login Flow

first broker login

Post Login Flow

Sync Mode

FORCE

Allowed clock skew (seconds)

3

☐ Pass login_hint?

☐ Pass current locale?

Cancel

Previous

Next

This page is entirely optional. Unless you have been specifically told otherwise, you can accept all the defaults and click **Next**.

Add mappers

The screenshot shows the Digital.ai user management interface. On the left is a sidebar with navigation links: Overview, Applications, Audit log, Settings, USER MANAGEMENT (Users, User groups), and Identity providers (selected). A central breadcrumb trail shows the steps: Select provider, Config identity provider and metadata, General, Advanced config, Add mappers (active), and Summary. The main content area is titled 'Mappers' and contains a table with columns 'Name', 'Category', and 'Type'. The table is currently empty, displaying 'No data found'. An 'Add' button with a dropdown arrow is in the top right, and a 'Group mapping' dropdown menu is open, showing 'Mapper' as the selected option. At the bottom right are 'Cancel', 'Previous', and 'Next' buttons. The Digital.ai logo is in the bottom left corner.

This page allows you to add mappers to ensure that user data from your IdP is properly understood by the Platform. Your identity provider shares information about your users with Digital.ai in the form of key/value pairs (known as claims or assertions, depending on the IdP), and the Platform uses this data to create users in our system.

NOTE

Mappers are required for SAML connections, but optional for OIDC connections unless your IdP uses non-standard claim names.

OIDC

Whether or not you need to use mappers to handle this data is entirely dependent on your organization's unique situation, and in general the Digital.ai Platform expects to receive user attributes based on the set of standard *claims* as defined by OpenID. You can view the list of standard claims here:

https://openid.net/specs/openid-connect-core-1_0.html#StandardClaim.

If your data is stored as the claims identified in this list (i.e. `given_name`, `family_name`, `email`, etc.), then you typically would not need to bother creating any attribute mappers.

For example, if your IdP uses the standard claim `"email": john@example.com`, the Platform will automatically map that to the Platform's `email` user attribute.

However, if your IdP uses a claim called `"email_address": john@example.com`, then you would need to create a mapper to correctly get that data into the Platform's `email` user attribute.

SAML

Unlike OIDC, the SAML protocol has no standard naming conventions for the attributes it stores (which SAML tokens refer to as *assertions*). That is why we require mappers for SAML connections, because each IdP's assertions may be named differently. So in order for the Platform to understand the data correctly, you must provide the assertion values as they are named in your IdP.

When creating mappers for SAML connections, you *must* add mappers for the following user data: first name, last name, email.

Username data is automatically pulled from the `NameID` attribute (based on the `NameID Policy Format / Principal Type` fields defined in the SAML IdP). You do not need to create a mapper for `username` if you need to override the default assertion.

How to Add Mappers

If you have determined that you need to add mappers, then follow this procedure:

1. Click the **Add** drop-down arrow, and select **Mapper**.
2. In the **Add mapper** window, set the following fields:
3. **Name** is merely a way to identify the mapper. Enter something like `First Name Mapper`.
4. **Sync Mode** controls whether an update to a user attribute in your IdP will cause an update in the Platform. We suggest using **INHERIT**.
 - FORCE always updates the Platform user when there is a change in your IdP.
 - IMPORT never updates the Platform user after they are created the first time, regardless of changes in your IdP.
 - INHERIT uses the value that has been configured on the **Advanced config** page of this IdP connection.
5. **Mapper Type** should be set to **Attribute Importer**.
6. (For OIDC providers only) **Claim** is the name of the claim as specified by your IdP.
7. **User Attribute Name** is the Platform user attribute that the data will be mapped to. This should be set to `username`, `email`, `firstName`, or `lastName` depending on the data you're mapping.

8. (For SAML providers only) **Attribute name** is the name of the assertion as specified in your IdP's SAML token. You can add the name in either **Attribute Name** or **Friendly Name** (you must complete at least one of the fields, but you do not need to complete both).
9. Click **Add Mapper**.
10. Repeat the previous steps to add additional mappers.

Summary

Overview

Applications

Audit log

Settings

USER MANAGEMENT

Users

User groups

SSO

Identity providers

Select provider

Config identity provider and metadata

General

Advanced config

Add mappers

Summary

Identity provider display name

Azure OIDC

Configuration detail

Authorization URL

Token URL

Client ID

Client secret

Authentication

Issuer

Scopes

Enabled

☒ Enabled

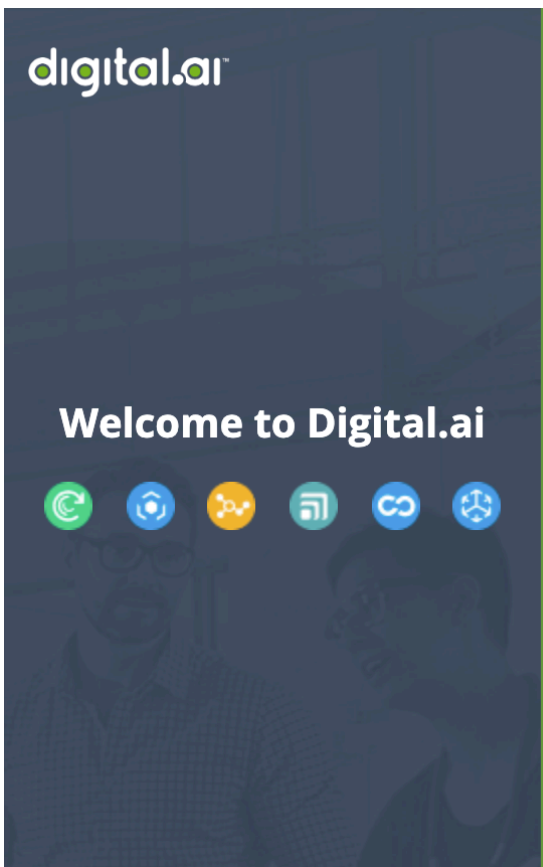
Cancel

Previous

Create identity provider

This page provides an overview of the configuration details for informational purposes.

To complete the wizard, click **Create identity provider**. A new button will now appear on the Platform login page with the name you added at the beginning of this procedure.



Sign in to your account

By signing in, I agree to Digital.ai's [Privacy Policy](#).

SSO Login

Or

Sign In Locally

If you do not have a user account, you can [self-register](#)

Set IdP as Default

We recommend setting this IdP as default, which will skip the Platform login screen and send users to the IdP authentication page as if they had clicked the button for it. If they already have an active session, most IdPs will redirect the user to the application directly and they will not see a login screen at all.

To set the IdP as default, return to the Identity providers page and click the **star** icon under Actions.

Identity providers



Name	Provider	Enabled	Redirect URI	Default	Actions
SSO Login	OIDC	True		★	  



TIP

If you need to override the default IdP login screen and authenticate using your local credentials, you can append the following query parameter to the end of your Digital.ai Platform account URL: `/?loginIdp=local`. For example: `https://exampletech.digital.ai/?loginIdp=local`.

Test SSO Connection

To ensure that you have properly connected with your IdP, you should now log out of the Platform and attempt to log in again using the newly configured IdP button (or via automatic redirect to your IdP if you set it as default per the previous section).

If everything has been configured properly, and as long as you are logged into a session with your IdP, you will be automatically logged in to the Platform.

Assign Administrator Role to SSO User

We recommend continuing through the rest of this guide while logged in as your SSO user. However, as you will notice, your SSO user does not have administrator permissions by default. So, you should now use your local admin user to give the administrator role to your SSO user.

To get back to your local administrator user account, you can use the URL override mentioned previously. You can then use your local administrator account to assign the `account-admin` role to your SSO user (**Users > Actions > Edit > Roles**).

You can now log back in as your SSO user and continue on through the rest of the process.

Step 3: Manage Roles and User Groups

In this step, you'll learn how to create user groups in the Platform and use them to ensure that your users inherit specified group assignments from your IdP in order to have the proper roles and permissions in Deploy.

Let's assume that you have the following *user groups* configured in your IdP:

- allAdmins
- analysts
- endUsers

And you have the following *roles* configured in Deploy:

- Administrator User
- Digital.ai Analytics Service User
- End User

Here, the Platform will act as a bridge between the data in your IdP (user groups) and the permissions in Deploy (roles). Once you've completed this rest of this guide, all of your users will be automatically assigned roles in Deploy based on their associated user groups in the IdP.

For example, if Doug is part of the `allAdmins` group in Entra ID, then he will automatically be assigned the `Administrator User` role in Deploy.

 NOTE

Group mapping is only available for OIDC connections.

Find Group Name / ID

Before you proceed, you must retrieve the name or object ID (Entra ID only) of the group claim from your IdP. Where and how you find this information will differ depending on what IdP you're using.

 TIP

Specifically for Entra ID, you must use the object ID of the group, rather than the group name, because that is the field which Entra ID passes to OIDC applications like the Platform.

Create User Groups

Before group membership can be inherited from your IdP, you need to create one or more user groups in the Platform.

The Platform does not create any groups automatically; you must manually create a corresponding group in the Platform for every IdP group that you want to map.

The screenshot shows the 'User groups' management interface. The left sidebar contains navigation links: Overview, Applications, Audit log, Settings, Users, **User groups**, SSO, and Identity providers. The main area is titled 'User groups' and includes a search bar. Below the search bar is a table with the following data:

☐	Group name ↑	Description	Synced with IDP	Users	Actions
☐	Self-Registered	Users created via self-registration will automatically ...	No	0	⋮
☐	allAdmins	A group to collect all site admins.	Yes	2	⋮

At the bottom of the table, there is a pagination control: 'Rows per page: 25' and '1-2 of 2' with navigation arrows. An 'Add group' button is located in the top right corner of the interface.

To begin adding a group, click **User groups** in the left navigation, and then click **Add group**.

1. In **Group name**, add a name for the group. **This name must exactly match the group name or object ID (Entra ID only) as it exists in your IdP.**
2. In **Description**, you can elaborate on the purpose of the group.
3. Select **Sync with IdP**.
4. For this initial setup, you do not need to manually add any users.
5. Click **Create user group**.

Repeat this process to add additional groups as necessary.

IdP Group to Platform Group Mapping

Now, you'll create a mapper to enroll users in the correct Platform groups. This is important in order to bridge the gap between your IdP and Deploy, so that users can be automatically assigned the appropriate roles in Deploy.

You only need to create one mapper for this purpose, as it will pass all group IDs from your IdP and place users in correct groups in the Platform.

1. In the left navigation, under SSO, click **Identity providers**.
2. Find the IdP you want to edit, then click the **Edit** icon under Actions.
3. Click **Next** until you reach the **Mappers** page.
4. Click the **Add** dropdown and click **Group mapping**.
5. In **Claim**, enter the name or object ID (Entra ID only) of the group claim from your IdP.

6. Click **Add mapper**.

IdP Group to Platform Role Mapping

You may also want to create mappers to assign Platform-specific roles to users based on their group assignments in your IdP (for example, if you want to give the `account-admin` Platform role to users in the `allAdmins` IdP group).

NOTE

This will only affect users that need to work in the Platform itself (administrators, dashboard authors, IT personnel, etc), and would not have any impact on users or permissions in Deploy. Deploy-specific roles will be configured later in this guide.

Users are automatically assigned the `account-user` Platform role by default if you do not create these mappers.

The available Platform roles are:

- `account-admin`: Users with this role have access to all aspects of the Platform, including user management, dataset and dashboard configuration, SSO configuration, account settings, audit logs, etc.
- `account-application-admin`: Users with this role has all the same permissions as the `account-admin`, except for SSO configuration.
- `account-analytics-author`: Users with this role can view, add, and edit datasets and dashboards, as well as access assigned Digital.ai applications, support and documentation portals, and edit their own basic preferences.
- `account-user`: Users with this role are limited to viewing dashboards, accessing assigned Digital.ai applications, support and documentation portals, and editing their own basic preferences.

TIP

This mapping can be especially useful if you know that certain non-admin users will be responsible for managing your analytics dashboards. You should be sure to assign the `account-analytics-author` to any users who do not also need administrator permissions.

1. On the same **Mappers** page, click the **Add** dropdown and click **Mapper**.
2. In **Name**, enter something descriptive like `allAdmins mapper`.

3. Leave **Sync Mode** as **INHERIT**.
4. In **Mapper Type**, choose **Advanced Claim to Role**.
5. In **New Key**, enter `groups`.
6. In **New Value**, enter the name or object ID (Entra ID only) of the group claim from your IdP.
7. In **Select Role**, choose the Platform role that this group's users should belong to.
8. Click **Add mapper**.
9. Repeat the previous step for each group that you want to map to a role.

Step 4: Connect Deploy to the Platform

In this step, you'll learn how to establish a connection between the Platform and your Deploy instance for user management / login purposes. This step does not cover setting up the Cloud Connector or Data Collector.

Add Deploy as an Application in the Platform

First, you need to define your Deploy instance as an application in the Platform. This will then allow you to download a configuration file that you can embed into your Deploy build in order for Deploy to understand the configurations you've been making in the Platform.

1. In the left navigation, click **Applications**.
2. Click **Applications**.
3. Click **Create application**.
4. In **Select application**, choose **Deploy**.
5. In **Instance name**, enter a descriptive name for this instance.
6. Choose whether this will be a production or non-production instance.
7. Enter the URL for your Deploy instance.

```
<deploy url>/oidc-login
```

8. On the **Advanced configuration** page, click **Next**.
9. On the **Mappers** page, click **Next**.
10. On the Get client ID & secret page, click **Download** to download the Deploy configuration file. In Deploy configuration file, you can view the configuration file for this application. Copy and save this

information when configuring Deploy.

11. Click **Complete**.

At the end of creating an application, a summary of the application and instance details are displayed. In Deploy configuration file, you can view the configuration file for this application. Copy and save this information for configuring your application **as mentioned in the 10th point**.

NOTE

Digital.ai Deploy has no direct support for SAML. However, you can integrate Deploy as an OIDC client with the Digital.ai Platform Identity Service and in turn connect the Digital.ai Platform Identity Service to your SAML-compliant IDP.

JVM Sites

Java Virtual Machine (JVM) is a software-based engine that runs Java programs. It takes the bytecode (compiled Java code) and converts it into machine code that your computer can understand. It allows Java programs to be written once and run anywhere (Write Once, Run Anywhere).

The Deploy product is a Java-based application, meaning it runs within a Java Virtual Machine (JVM). JVM provides the runtime environment to execute the Deploy server's application code. Since Deploy runs on a JVM, it can be deployed on various operating systems (Linux, Windows, macOS) without modification, supporting the platform's integration needs.

The OIDC Authentication plugin is a Java-based component that runs within the Deploy server's JVM. Configuring it allows secure communication between Deploy and the Identity Service.

Do this on the Digital.ai Deploy server to integrate Deploy as on OIDC client with the Digital.ai Identity Service.

1. Install and enable the OIDC Authentication plugin, modify the `Default` configuration property to `OIDC` in the `XL_DEPLOY_SERVER_HOME/centralConfiguration/deploy-server.yaml` file.
2. To configure the OIDC Authentication plugin, add the following YAML code snippet to the `XL_DEPLOY_SERVER_HOME/centralConfiguration/deploy-oidc.yaml` file.

```
deploy.security:
  auth:
    providers:
      oidc:
```



```
loginMethodDescription:
clientId: "<Your client ID>"
clientSecret: "<Your client secret>"
issuer: "<Enter the Open ID Provider Issuer>" # for example
"https://identity.staging.digital.ai/auth/realms/demoaccount"
redirectUri: "<deploy url>/login/external-login"
postLogoutRedirectUri: "<deploy url>/login/external-login"
rolesClaimName: "realm_access.roles"
userNameClaimName: "preferred_username"
emailClaim: "email"
fullNameClaim: "name"
```

NOTE

The above configuration automatically fetches the required configuration from the discovery endpoint.

Log on to Deploy and Add the Admin User

Log on to Deploy and add the local Admin User.

1. Log on to Deploy as an Administrator.
2. Create a role named `Admin` and add the Digital.ai Platform's admin user to that role.
3. Assign Admin permissions to this `Admin` role you created.

Restart the Deploy Server

Restart the Deploy server and navigate to appropriate instance URL. If you set a default IdP earlier, you should now be automatically redirected to the Platform authentication and seamlessly logged in to Deploy. If not, you should use the SSO login button to log into Deploy as your SSO user.

Configure Roles in Deploy

For this last step, you must update your roles in Deploy to ensure that they properly sync with the Platform user groups you created earlier.

In Deploy, go to **Settings > Users and permissions > Roles** and edit any of the roles. In **Principals**, add the Platform user group name that corresponds to this role. Repeat this for all roles that you want to

inherit group assignments. You may optionally want to create new roles for this purpose, depending on how your workflow is configured.

For example, edit the role called `Administrator User`, and add `allAdmins` as a Principal for the role.

Next Steps

At this point you have successfully connected Deploy with the Platform. From here, you can move on to any of the following tasks (and more that aren't listed here):

- Inform your users that they can begin accessing Deploy with their corporate SSO credentials.
 - You may also want to instruct them to stop using their old application-specific login credentials entirely to avoid any confusion caused by using multiple user accounts.
- Begin configuring Analytics dashboards. For more information, see [Dashboards](#).

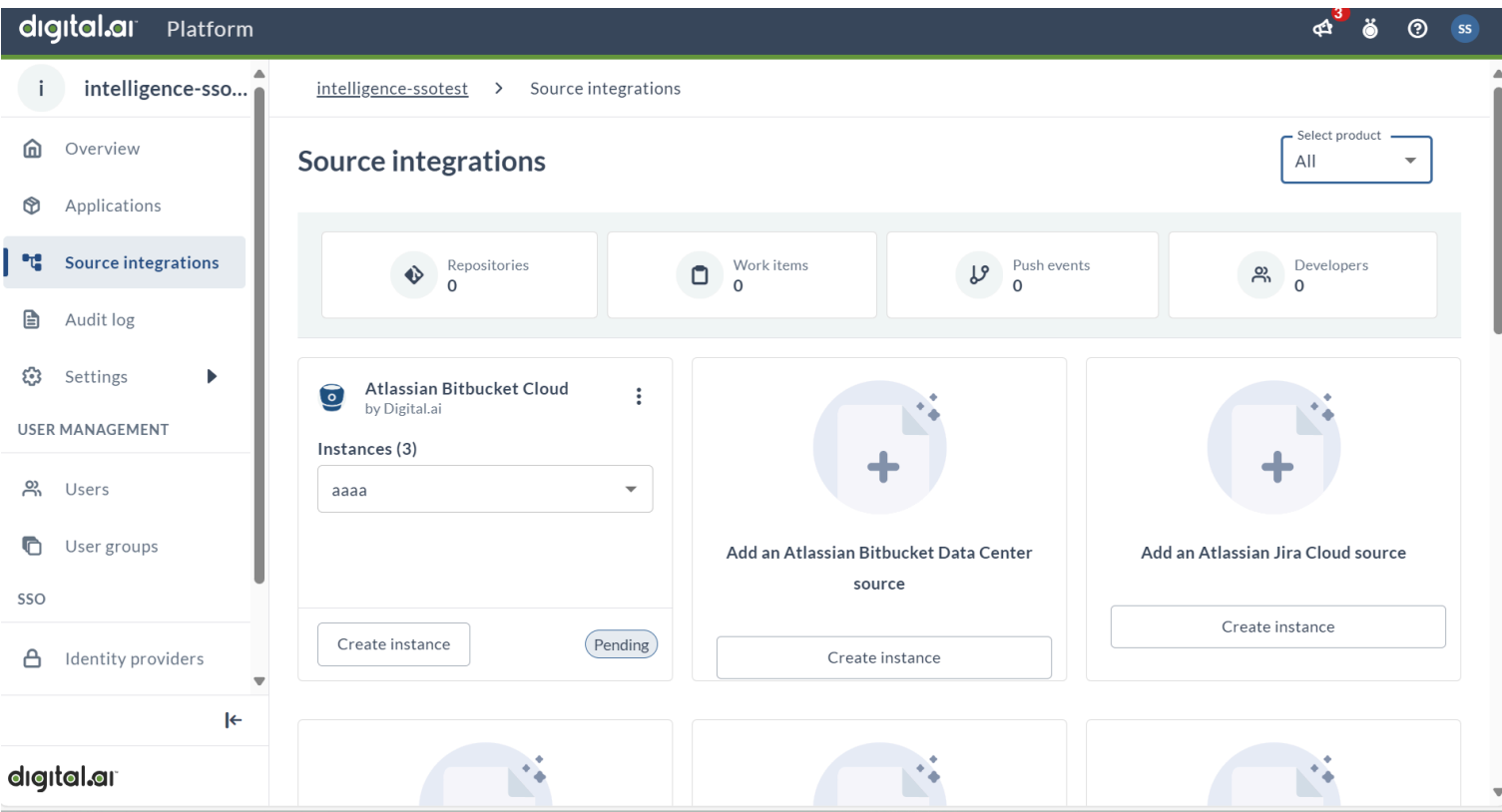
 Source Integrations

Learn how to add and view Source Integrations in Digital.ai products.

Source Integrations

Source Integrations Overview

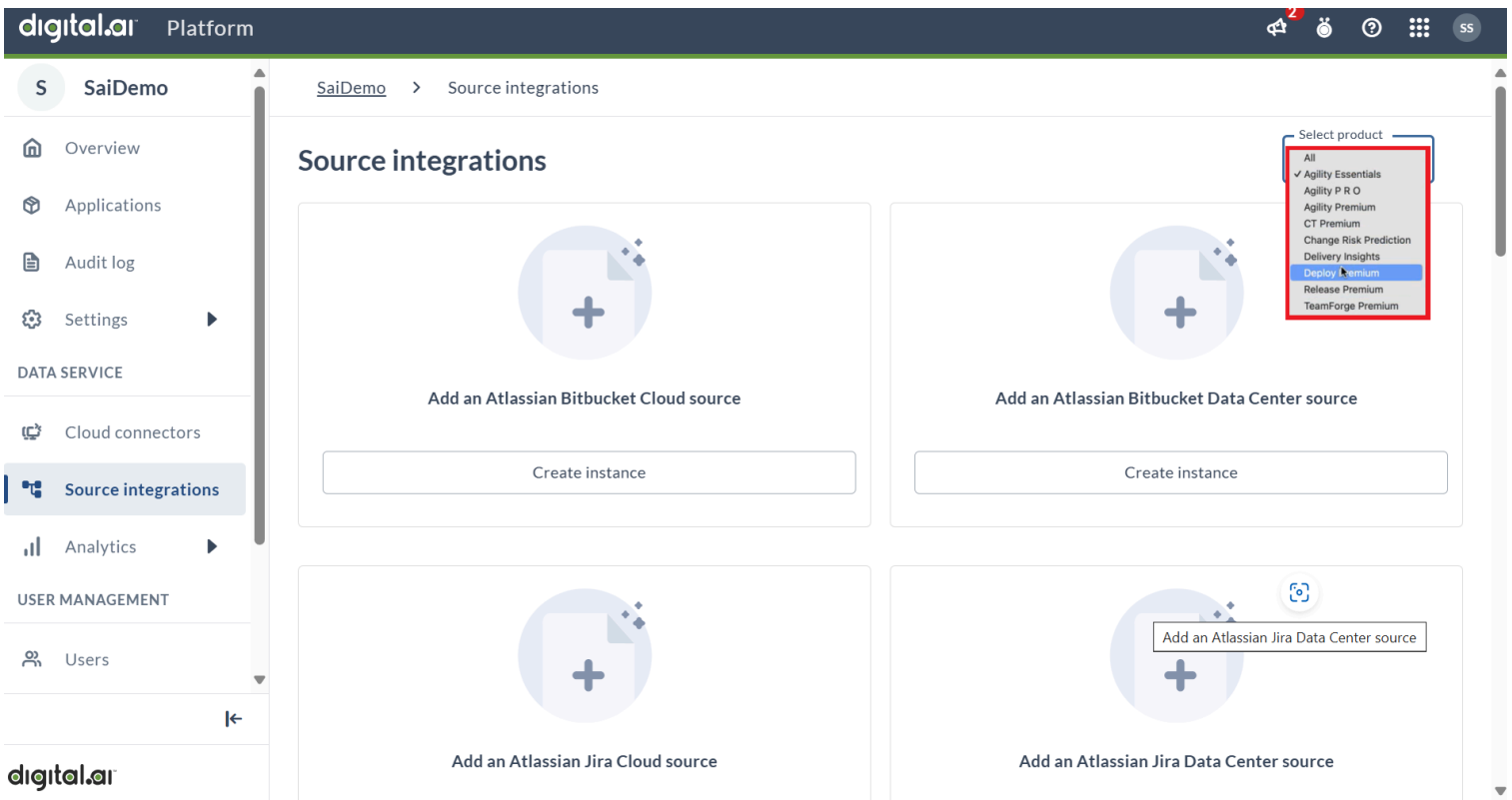
The Source Integrations functionality of Platform allows you to configure your integrations for data ingestion into the Digital.ai Intelligence Platform. These ingestion sources feed data into your Intelligence Analytics products, such as CRP or Embedded Analytics.



Add a Source Integration

Select product

The **Select Product** drop-down menu allows you to choose the desired product (you are entiteled to) for which the third-party integration needs to be created.



Create Instance

A source instance refers to a specific deployment of that source that holds significance for the customer. By creating or configuring an instance, we are indicating, for example, that the customer has a (Release or Agility) product instance running in their data center.

To create an instance, select the empty cart of your choice and click **Create Instance**.

digital.ai Platform

intelligence-sso... intelligence-sstest > Source integrations

Source integrations

Select product: All

Repositories
0

Work items
0

Push events
0

Developers
0

Atlassian Bitbucket Cloud
by Digital.ai

Instances (3)
aaaa

Create instance Pending

Add an Atlassian Bitbucket Data Center source

Create instance

Add an Atlassian Jira Cloud source

Create instance

Fill out the form by providing the **Integration Instance Name**, **Integration Instance Description**, **Bitbucket API Base URL**, **Username**, and **Password**. You can also choose to **Disable SSL Verification** if needed. Once all required fields are filled, click **TEST** to verify the new integration if required. After successful testing, click **Save** to finalize the integration.

digital.ai Platform

← Back

Atlassian Bitbucket Data Center

Name *

Integration instance name

Description

Integration instance description

URL *

Bitbucket API Base URL

User *

Username for the user.

Password *

Password for the user.

☐ Disable SSL verification

Test

Cancel

Save

Manage Applications

An application is any Digital.ai product or service that is connected to the Platform in order to provide federated user access. The created applications appear as links or bookmarks on the Overview page.

To add an application

2. In the left navigation, click **Applications**.
 - Alternatively, you can click the **Create application** button on the Platform Overview page.
3. Click **Applications** button.
4. On the Select application page:
 - i. In Select application, choose the type of application from the list. (For example, Release)
 - ii. In Instance name, enter the application's custom name. (For example, Release_demo)
 - iii. In URL, enter the application's URL.
 - iv. In Description, enter the application's description.
 - v. Click **Next**.
5. The Advanced configuration page is optional, and depending on the selection you made in the previous step, the majority of fields may be automatically filled in.
6. Click **Next**.
7. The Mappers page is optional, because mappers are automatically created as part of this process.
8. Click **Next**.
9. On the Get client ID and secret page, you can view a summary of the application details.
10. Click **Complete**.

Integrate your Applications

Adding an application identifies it in the Platform, which is an integral part of fully integrating a product with the Platform.

However, there are additional steps necessary for fully configuring an end-to-end integration between the Platform and any Digital.ai product. See the following guides for more information, or contact customer support for further assistance.

[How to Integrate Release with the Platform](#)

[Digital.ai AgilitySync Documentation](#)

[Digital.ai Deploy Documentation](#)

 Users

Guide for administrators to create and manage users on the Digital.ai Platform.

 User Groups

Guide for administrators to create and manage user groups on the Digital.ai Platform.

 User Self-Registration

Guide for users to self-register on the Digital.ai Platform along with self-registration workflow.

 Resetting A User's Password

Instructions for resetting passwords of local users on the Digital.ai Platform, including administrator notifications an...

 Sign-in Helper

Guide for users to sign-in to the digital.ai portal.

 Connect to Entra ID for SSO.

Step-by-step guide for connecting users to Entra ID.

User Merge Flow

Guide for User Merge Flow in the Digital.ai Platform, including supported scenarios, troubleshooting, and steps for li...

Enable IP Address Allow List

Learn how to enable IP address allow List.

Users

Administrators can use the Platform to create and manage users in one of two ways:

- Manually add local users
- Automatically provision users through SSO

Additionally, any user can self-register to create their own Digital.ai Identity without input from an administrator. For more information, see [User Self-Registration](#).

User Roles

Users can be assigned one of the following roles within the Platform:

- *account-user*: A basic user with the lowest level of access, limited to Digital.ai application access, support and documentation portal access, and basic preferences. This documentation refers to a user with this role as an "end user".
- *account-admin*: An advanced user with access to user management, SSO configuration, account settings, audit logs, etc. This documentation refers to a user with this role as an "administrator".

Add a Local User

Local users are stored directly in the Platform database and are not associated with any outside user management system.



TIP

We recommend creating only a few local users at first; enough to perform administrative tasks before you connect to your corporate identity provider to onboard the rest of your users.

1. Log in to the Platform as an administrator.
2. In the left navigation, under User Management, click **Users**.
3. Click the **Add User** button.
4. In User Information, enter the user's details (including the Username they'll use to log into the Platform).

5. In Roles, choose a role to assign to the user.
6. In User Groups, choose one or more user groups to assign to the user.
7. Click **Create user**.

At this point, the user will receive an email notification that prompts them to create a password and log in.

You can return to the Users page at any time to view the list of all local users, edit users' details, delete users, or reset passwords.

Add Users from an Identity Provider

To learn how to connect the Platform to your existing identity provider, see [SSO Configuration](#).

After you have connected the Platform to your corporate SSO, users are provisioned in the Platform when the user logs in for the first time through that identity provider.

User Self-Registration

Any user can create their own Digital.ai Identity without being provisioned by an administrator. This is especially useful for providing users with access to the Digital.ai community, support, and documentation portals before an administrator has had a chance to set up the account.

For more information, see [User Self-Registration](#).

Merge Local and SSO Users

The Platform provides an option to merge local and SSO user accounts when the system identifies conflicting user credentials (that is, when an already existing local user logs in through SSO with the same username, email address, or both). This functionality will also catch any users that self-registered prior to integrating with an external identity provider.

The workflow for merging users is as follows:

1. If you log in through SSO and the system finds a conflict, a warning message appears prompting you to either review the profile or to add it to an existing account.

2. Review the profile: Review your account to check if the conflict is true. For example, when the username is the same but not the email address, you could consider this to be two different users. In this case, review your account and make necessary changes so that there is no conflict.
3. Add to existing account: Click this option to merge accounts if you reviewed the profile and identified the users to be the same. After you activate this action, an email notification is sent to the email address mentioned in the local user profile.
4. When you receive the email and click the confirmation link (this link expires in five minutes), the merge process completes and you are logged into the Platform.

 WARNING

After the users are merged, your local user password is deleted and you will no longer be able to log in as that local user.

User Groups

User groups allow administrators to categorize multiple users together. For example, you could create a group that includes all administrators in your organization, or one that collects all users who have self-registered for a Digital.ai Identity. For more information about users, see [Users](#).

NOTE

All self-registered users are added to a group called **Self-Registered** by default, but you can change the default group if you want.

Users can belong to multiple groups. Users can also inherit group membership based on data from your corporate identity provider. For more information, see [Map Group Data](#).

NOTE

Renaming a user group name can impact user login if the group is directly referenced within any Digital.ai applications (for example: Intelligence). Therefore, you should check with Digital.ai Customer Support before making any changes to the user group name.

Create a user group

1. Log in to the Platform as an administrator.
2. In the left navigation, under User Management, click **User groups**.
3. Click the **Add group** button.
4. (Required) In Group name, add a descriptive name for the group.
5. In Description, you can elaborate on the purpose of the group.
6. Select **Sync with IdP** option if this user group's name matches with the group name in the IdP. Enabling this option displays "Yes" in the User groups' summary page, which determines that this user group membership is provisioned through the IdP.
7. In Add Users, select one or more users on the left (or select **All users**), then click **Add** to add the users to the group.
8. When you're finished, click **Create user group**.

Modify a user group

1. Log in to the Platform as an administrator.
2. Click **User groups**.
3. Find the group you want to modify and click the **Edit** icon under Actions.
4. Change the details as necessary.
5. Click **Save changes**.

Delete a user group

1. Log in to the Platform as an administrator.
2. Click **User groups**.
3. Find the group you want to remove and click the **Delete** icon under Actions.
4. If you're sure, click **Delete**.

User Self-Registration

Users with approved email domains can self-register themselves and create their own Digital.ai Identity without being provisioned by an administrator. This is especially useful for providing users with access to the Digital.ai community, support, and documentation portals before an administrator has had a chance to set up the account.

The self-registration process begins when users log in with their approved email to access Digital.ai portals, but do not have a Digital.ai Identity. The system then prompts the users with a link to self-register. After self-registering, they can access the portal services.

Approved email domains are listed in the Domain whitelist. Domain whitelist is a way by which administrators can control self-registration. For more information about managing the domain whitelist and disabling self-registration, see [Account Settings](#).

All self-registered users are added to a user group called **Self-Registered** by default, but you can change the default group if you want. Administrators can monitor the users in this group to identify whether the users should actually be in the system, and remove them if necessary. For more information, see [User Groups](#).

Self-registered users are stored locally and are given the account-user role only.

Self-Registration workflow

1. When users logs in to the portal services, they are prompted with a link to self-register.
2. In the *Register for a Digital.ai Identity* page, user must enter their corporate email address, acknowledge terms and conditions, and click **Register**.
3. The user then receives an email to validate their email address.
4. On validating, the User Registration confirmation page opens.
5. The user must enter their details, that is, username, first name, last name, and password.
6. On clicking **Register User**, the user is granted access to the Platform.
7. The user will then be directed to sign in to the Platform to access the portal services.



NOTE

Self-registered users can access the Digital.ai portals but do not have access to any connected Digital.ai applications."

Resetting A User's Password

Any local user can reset their own password. As an administrator, you can also notify the user to reset their password if you think their credentials have been compromised.

NOTE

Resetting a password in this way only applies to local users. SSO user passwords must be managed through your identity provider.

Reset a User's Password as an Administrator

1. Log in to the Platform.
2. In the left navigation, under User Management, click **Users**.
3. On the Users page, find the user whose password needs to change and click the **Reset Password** icon under Actions.

After this step, the user receives an email notification to update their password.

User then clicks the **Link to account update** link received in the email and updates the password by following instructions. By clicking the **Back to Application** link, user can login to their account using the new password.

Reset Password as a Local User

1. Users can use the **Forgot Password** link on the login page to reset their password.
2. If a user is already logged in and wants to change their password:
 - a. The user must click **Edit Profile** on the Overview page in the Profile section. They can also click on their profile initials on the top right corner and select *View Profile*.
3. The user must enter their new password adhering to the complex password policy and click **Change password**.

Password Policy

The following table lists the default password policy for the Platform:

Required Parameters	Default Value	Minimum Value
Number of digits	1	0
Number of lower-case characters	0	0
Number of upper-case characters	0	0
Number of special characters	1	0
Number of days valid	180	1
Number of passwords remembered (Kept in history)	3	1
Minimum password length	12	8
Username		Not same as username
Email Id		Not same as email address

The system prompts the user for a password reset during the following scenarios:

- When the user logs in for the first time after the minimum value has increased (for example, If the default value for the password length was 12 and then the minimum password length changes to 24).

i NOTE

If the minimum length changes to a lower value, the users need not update their password."

- When the password exceeds the valid number of days (for example, if the valid number of days is 150, and the user logs into the account after day 150).

Sign-in Helper

What is the sign-in helper

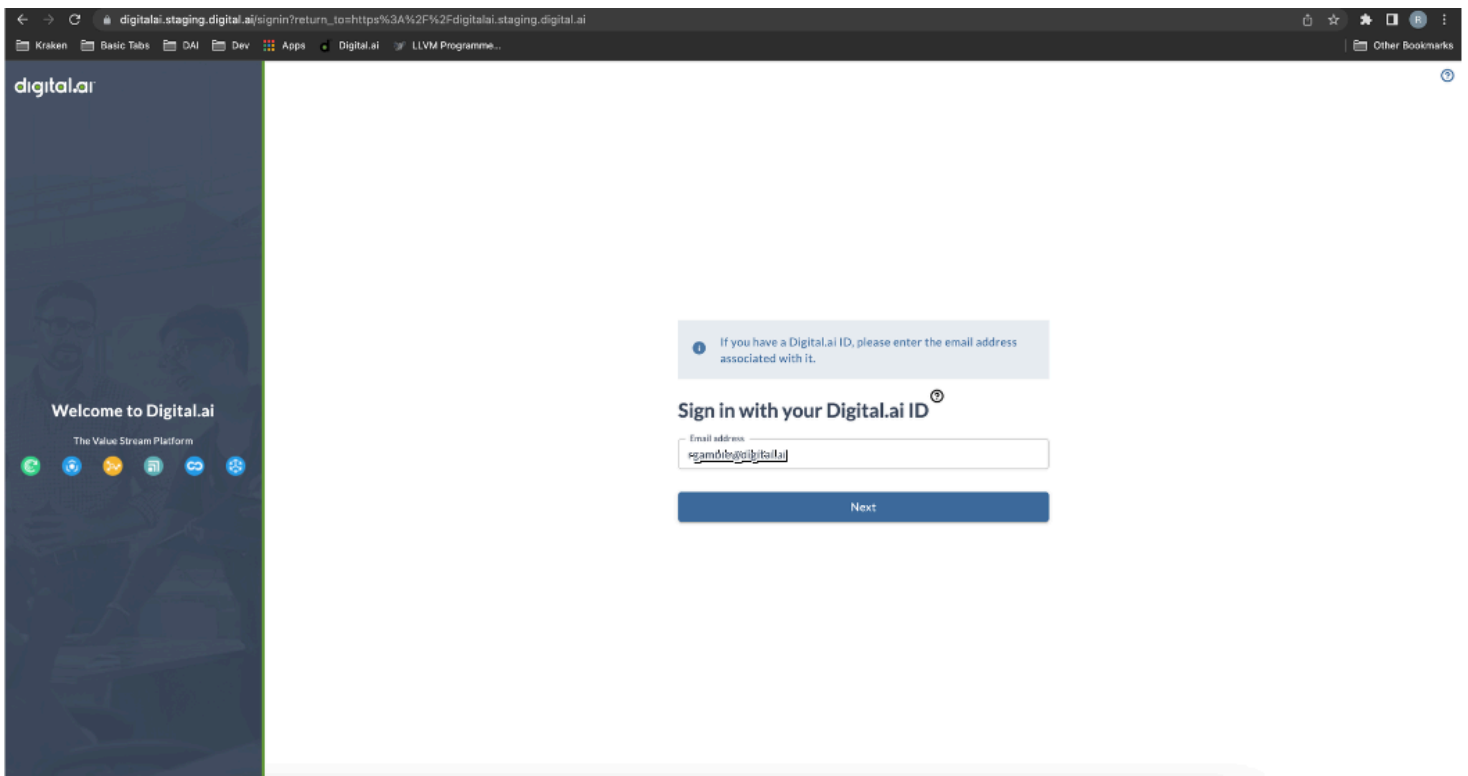
The sign-in helper is a feature of the Digital.ai Platform that assists unauthenticated users when they try to access a page that requires login, providing them with access to the based on their Platform tenant and permissions. Sign-in helper helps users log into the Platform and send them back to the application with an authentication token.

How the sign-in helper helps users

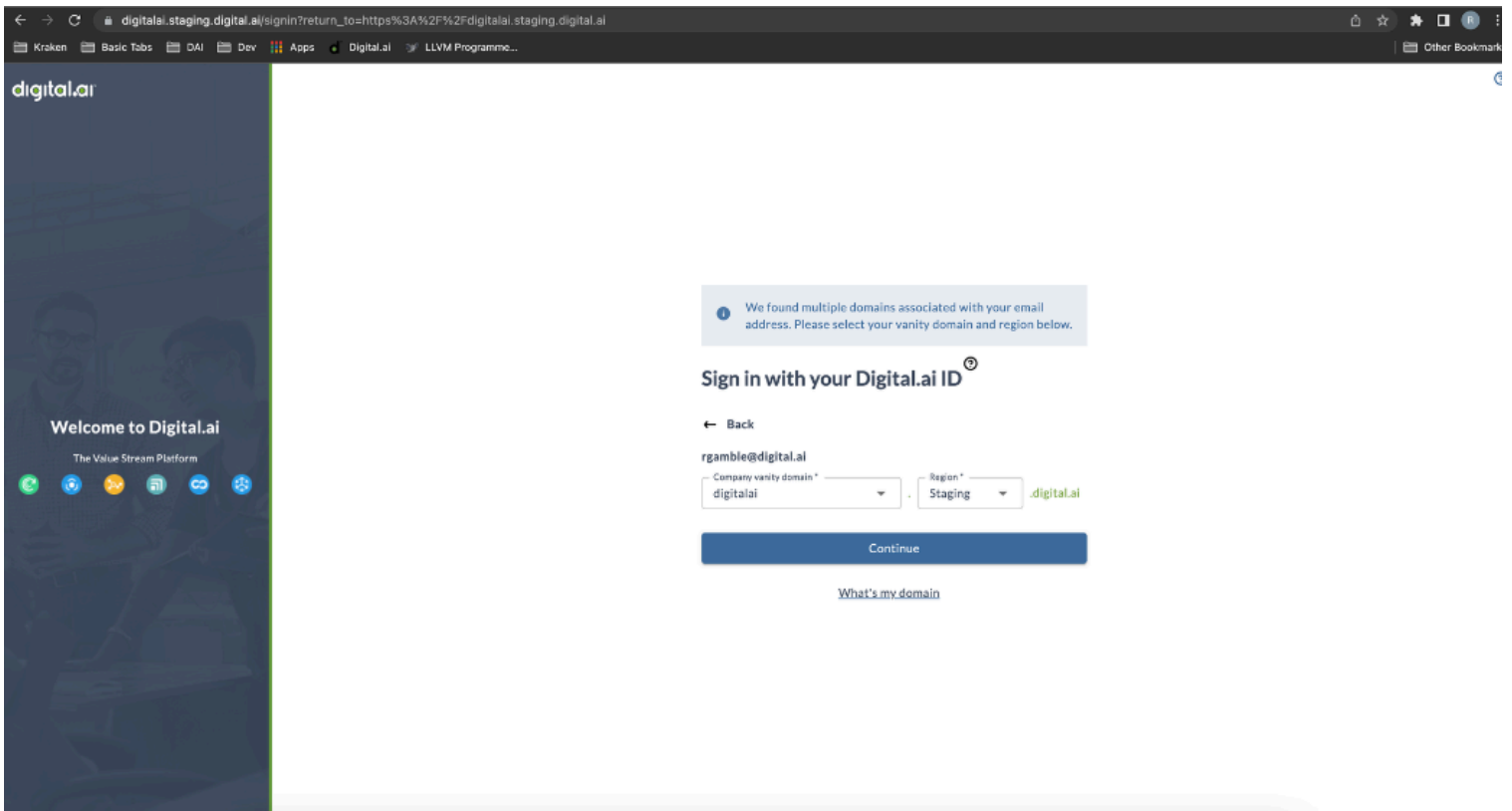
The sign-in helper helps users identify the correct platform tenant to sign into by checking their email. When users are only associated with one tenant (the most common case) entering their email is enough to send them straight along to their tenant sign-in page and the next time they use the flow their email should be auto-populated in the form to make the process easier. Additionally, if they already have an active session in the platform console then they should be authenticated automatically, skipping the sign-in flow completely, and being directed back to the application.

User Experience

First, assuming there is no active platform session, the users will either enter their email or have it auto-populated and they will click **Next**.



If the user's email is associated with multiple platform tenants, they will be prompted to select the domain and region they wish to sign in to. For most users who are linked to only one platform tenant, this page will be bypassed altogether.



Click [What's my domain](#) to login to the required domain.

digital.ai



Welcome to Digital.ai

The Value Stream Platform

Sign in to your account

By signing in, I agree to the digital.ai's [Privacy Policy](#).

☐ Remember me

Sign In

Or

OIDC

SAML

Azure AD

Azure SAML

Okta - OIDC

Okta - SAML

As an administrator, you can connect the Digital.ai Platform to Microsoft Entra ID Directory (Entra ID) to create a seamless login experience for your users when they log in to Digital.ai applications and portals. You only need to follow this procedure if your company uses Entra ID as an identity provider. For more information about SSO, see [Manage Identity Providers](#).

i NOTE

Certain parts of these procedures include instructions for a third-party website. These instructions may occasionally become outdated based on changes in the third-party website.

Add OIDC SSO Connection

Prerequisites

Before you begin, you need to retrieve the following details from the Entra ID tenant you want to use to establish this OIDC SSO connection. You can find this information in your Microsoft Entra ID account by going to Manage Entra ID **Active Directory > App registrations** and opening the appropriate application (tenant).

- Client ID
- Client secret
- .well-known endpoint - In Azure AD this is known as OpenID Connect metadata and it looks like this:

i NOTE

Save the values to use later in this procedure.

Logging in

1. Log in to the Platform as an administrator.
2. Select **Identity providers** navigation item from the left side panel.

digital.ai Platform

Overview

Platform overview

Power of Platform enables you to control users and SSO

Account admin
Edit profile

Single Account
Edit account

Contact support
Community
Read documentation

Identity providers

Client

Audit log
Account settings

Release orchestration powered by digital.ai

SSO / Identity providers

User will be either automatically created once you set up SSO, or you can start creating internal users.

Setup Identity provider

Read documentation

Users

You have 1 user

Create user

Active users: 1
Disabled users: 0

Read documentation

View all >

3. Click **Create identity provider** primary action button in the top right corner.

digital.ai Platform

SaiDemo > Identity providers

+ Create identity provider

Identity providers

Name	Provider	Enabled	Redirect URI	Default	Actions
No data found					Redirect URI

Select Provider

4. Select **Add OIDC Provider** as the authentication service and **Entra ID** as the provider. In **Identity Provider display name**, add a unique, user-friendly name for the IdP. This name will appear on the Digital.ai Platform login page and then click **Next**.

digital.ai Platform

SaiDemo > Identity providers > Create identity provider

Select provider

- Config identity provider and metadata
- General
- Advanced config
- Create mappers
- Summary

Select authentication service
Select your organizations SSO protocol service

☒ **OIDC provider**

☐ SAML provider

Select identity provider
Select identity provider from the list for setting up authentications

☒ **Azure AD**

☐ Okta

☐ Other

Cancel **Next >**

Config Identity Provider and Metadata

digital.ai Platform

FedEx

Accounts > FedEx > Identity providers > Add provider

Select provider
Select the protocol and provider to use with your application

Config IDP and metadata
You need to configure your IDP's name and metadata

General
General configuration

Advanced config
Advanced config

Summary
About summary

Redirect URI
Use this redirect URI to setup your identity provider.

https://identity.staging.digital.ai/auth/realms/fedex/broker/azure_ad_oidc/endpoint

How would you like to configure this metadata?
you need to configure your IDP's metadata

☒ I have the metadata URL for my IDP

☐ I have a file which contains the metadata

☐ I want to manually configure the IDP

Enter Metadata URL *
0fe-4945-b137-f2dfda2c0275/v2.0/.well-known/openid-configuration

Metadata URL link from which IDP configuration can be fetched

Import

Cancel Previous Next

5. Copy the Redirect URI to setup your identity provider. Ensure to share this information with your IT/Security/SSO team.

- Your IT/Security/SSO team will use the Redirect URI to configure your corporate IdP and provide the SSO setup details in one of the following three formats:
- If you select **I have the metadata URL for my identity provider**, then paste the **.well-known endpoint** into the Enter Metadata URL field and click Import. You will receive a success message once the data is imported. This import should update several fields in the configuration on the General page.

digital.ai Platform

Accounts > Identity providers > Add provider

Select provider
Select the protocol and provider to use with your application

Config IDP and metadata
You need to configure your IDP's name and metadata

General
General configuration

Advanced config
Advanced config

Summary
About summary

Redirect URI
Use this redirect URI to setup your identity provider

https://identity.staging.digital.ai/auth/realms/fedex/broker/azure_ad_oidc/endpoint

How would you like to configure this metadata?
you need to configure your IDP's metadata

☒ I have the metadata URL for my IDP
☐ I have a file which contains the metadata
☐ I want to manually configure the IDP

Enter Metadata URL *
https://login.microsoftonline.com/4605c06d-20fe-4945-b137-f2dfda2
Metadata URL link from which IDP configuration can be fetched

Import

Cancel Previous Next

- If you select **I have a file which contains the metadata**, then select the file and upload.
- If you select **I want to manually configure the identity provider**, then enter the fields manually.

General

6. In **Client ID**, paste the **Client ID value** provided by your IT/Security/SSO team.
- In **Client Secret**, paste the **Client Secret value** provided by your IT/Security/SSO team.
 - In **Issuer**, enter the issuer of the token received from the IdP.
 - In **Authentication method**, choose **Client secret as post**.
 - In **Default scopes**, type: **openid profile email**. These are the scopes required by Digital.ai for retrieving user data, but you may add others at your discretion. Without this setting, the correct user data will not be pulled out of Entra ID.
 - In **Authorization and token URL**, enter the authorization URL and token URL of your IdP. Verify the details and then click **Next**.

NOTE

If the **Issuer** section is not provided, platform identity service will not validate the issuer.

digital.ai

Value Stream Platform

KS

Applications

Audit log

Settings

Intelligence

User management

Users

User groups

SSO

Identity providers

Clients

Home > Accounts > > Identity providers > Add provider

Select provider

Select the protocol and provider to use with your application

Config IDP and metadata

You need to configure your IDP's name and metadata

General

General configuration

Advanced config

Advanced config

Summary

About summary

Configure client credentials

Provide the client ID and client secret obtained from the identity provider

Client ID *

e7300629-2e6a-4f63-96ea-522abc088f9e

Client Secret *

.....

Issuer

https://login.microsoftonline.com/4605c06d-20fe-4945-b137-f2dfda2c0275/v2.0

Authentication method

Defines the requested authentication method for the token endpoint. Possible values are 'Post' (application uses HTTP POST parameters) or 'Basic' (application uses HTTP Basic).

Client Authentication *

Client secret as post

Default Scopes

OpenID Connect defines the following scope values that are used to request Claims

Default Scopes

openid profile email

Authorization and token URL

Description

Authorization URL *

https://login.microsoftonline.com/4605c06d-20fe-4945-b137-f2dfda2c0275/oauth2/v2.0/authorize

Token URL *

https://login.microsoftonline.com/4605c06d-20fe-4945-b137-f2dfda2c0275/oauth2/v2.0/token

Cancel

Previous

Next

Advance Config

NOTE

Advanced Configuration page is optional.

Depending on the selection you made in the previous step, the majority of fields may be automatically filled in.

7. Ensure that **Sync Mode** is set to **FORCE**. **Sync Mode** is set to **FORCE** by default, which allows Digital.ai to update a stored user's data whenever it is changed in the IdP. If you set it to **IMPORT**, user data is only imported the first time they log in through the IdP. Click **Next**.

Applications

Audit log

Settings

Intelligence

User management

Users

User groups

SSO

Identity providers

Clients

Select provider

Select the protocol and provider to use with your application

Config IDP and metadata

You need to configure your IDP's name and metadata

General

General configuration

Advanced config

Advanced config

Summary

About summary

Advanced Configuration

Optional

☐ Trust Email ?☐ Account Linking Only ?☐ Hide on Login Page ?

First Login Flow

first broker login

Post Login Flow

Sync Mode

FORCE

Allowed clock skew (seconds)

3

☐ Pass login_hint ?☐ Pass current locale ?☐ Backchannel Logout ?☐ Disable User Info ?

Prompt

The prompt parameter in the OIDC specification. See the specification for more details.

☐ Accepts prompt=none ?☐ Validate Signatures ?

Forwarded Query Parameters

Cancel

Previous

Next

Create Mappers

Select provider

Config identity provider and metadata

General

Advanced config

 Add mappers

Summary

Mappers

Add ▼

Name	Category	Type	Actions
No data found			

Cancel < Previous Next >

i NOTE

Create Mappers page is optional.

8. Adding mappers to this configuration ensures that user and user group attributes from your IdP are correctly mapped with the Digital.ai Platform. For more information check [Map User Data](#)

To enable Digital.ai Platform to inherit user groups defined in your IdP, perform the following steps:

Add Group Mappers

- Click **Add** and select **Group mapper**. All the fields are populated by default.
- Enter the **Claim** value.

Add group mapper

Name *

Groups

Sync Mode

FORCE

Mapper Type

Attribute Importer

Claim *

User Attribute Name *

groups

Cancel

Add mapper

For more information see [Group Mappers](#)

Add Mapper

- Click **Add** and select **Mapper**.
- In **Name**, enter the name of the mapper.
- In **Sync Mode**, select **INHERIT**.
- In **Mapper Type**, choose Hardcoded Attribute (for example).
- In **User Attribute**, enter the attribute name.
- In **User Attribute Value**, enter the attribute value.

Select provider

Config identity provider and metadata

General

Advanced config

 Add mappers

Summary

Mappers

Add ▼

Name	Category	Type	Actions
No data found			

Cancel < Previous Next >

For more information on Mappers see [Mappers](#)

Summary

- The Summary step displays the general configuration of the identity provider. Click **Create identity provider** to create the new record.

digital.ai Platform

Accounts > FedEx > Identity providers > Add provider

Select provider
Select the protocol and provider to use with your application

Config IDP and metadata
You need to configure your IDP's name and metadata

General
General configuration

Advanced config
Advanced config

Summary
About summary

IdP display name
Azure_AD_OIDC

Configuration detail

Authorization URL	https://login.microsoftonline.com/4605c06d-20fe-4945-b137-f2dfda2c0275/oauth2/v2.0/authorize
Token URL	https://login.microsoftonline.com/4605c06d-20fe-4945-b137-f2dfda2c0275/oauth2/v2.0/token
Client ID	e7300629-2e6a-4f63-96ea-522abc088f9e
Client secret	*****
Authentication	client_secret_post
Issuer	https://login.microsoftonline.com/4605c06d-20fe-4945-b137-f2dfda2c0275/v2.0
Scopes	openid profile email

Enabled

☒ Enabled

Cancel Previous **Create identity provider**

10. Copy the **Redirect URI** for the newly created identity provider.

digital.ai Platform

Accounts > FedEx > Identity providers

Identity providers

Name	Provider	Enabled	Redirect URI	Default	Actions
Azure_AD_OIDC	OIDC	True	https://identity.staging.digital.ai/auth/realms/fedex/broker/azure_ad_oidc/endpoint		

Entra ID Account

11. Log into your Microsoft Entra ID account to identify the Platform as a valid redirect URL. Go to Manage Entra ID Active Directory.

12. Select **App Registrations** from the menu.

Microsoft Azure Upgrade Search resources, services, and docs (G+I)

Home > Default Directory | Overview

Azure Active Directory

Overview Preview features Diagnose and solve problems

Manage

- Users
- Groups
- External identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations**
- Identity Governance
- Application proxy
- Custom security attributes (Preview)
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- User settings

Overview Monitoring Tutorials

Search your tenant

Basic information

Property	Value	Count
Name	Default Directory	Users: 6
Tenant ID	b5045cac-bff5-482b-9b8b-57e644b73d2c	Groups: 1
Primary domain	afinleytest2@gmail.onmicrosoft.com	Applications: 4
License	Azure AD Free	Devices: 0

Alerts

Upcoming TLS 1.0, 1.1 and 3DES deprecation
Please enable support for TLS 1.2 on clients(applications/platform) to avoid any service impact.
[Learn more](#)

My feed

Andrew Finley
7d5d4d4d-4d81-4a8d-9eee-39f523b92935
Global Administrator
[View role information](#)

Azure AD Connect
Not enabled
Sync has never run

13. Select **Owned Applications** tab and from the list Select **DigitalAIdentityService**.

Microsoft Azure Upgrade Search resources, services, and docs (G+I)

Home > Default Directory

Default Directory | App registrations

Azure Active Directory

New registration Endpoints Troubleshooting Refresh Download Preview features Got feedback?

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

All applications **Owned applications** Deleted applications Applications from personal account

Start typing a display name to filter these results Application (client) ID starts with Add filters

2 applications found

Display name	Application (client) ID	Created on	Certificates & secrets
LocalTest	68f5ac5a-df13-49af-bd56-e0f9de4bcd9b	1/28/2022	Current
DigitalAIdentityService	6bca28bc-8edd-465d-83d8-9af204711ccf	2/1/2022	Current

14. Select **Authentication** from the menu.

Microsoft Azure Upgrade Search resources, services, and docs (0+)

Home > Default Directory > DigitalAidentityService

DigitalAidentityService | Authentication

Search (Cmd+/) Save Discard Got feedback?

Overview Quickstart Integration assistant Manage Branding & properties Authentication Certificates & secrets Token configuration API permissions Expose an API App roles Owners Roles and administrators | Preview Manifest Support + Troubleshooting Troubleshooting New support request

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Web

Quickstart Docs

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

This app has implicit grant settings enabled. If you are using any of these URIs in a SPA with MSAL.js 2.0, you should migrate URIs. →

https://identity.dev.digital.ai.cloud/auth/realm/s/idp_test/broker/azure_ad/endpoint

Add URI

Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. <https://example.com/logout>

Implicit grant and hybrid flows

Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. [Learn more about](#)

17. Click **Save** to save your application changes.

When you're finished, a new button will appear on the Digital.ai Platform login page with the name you added under Display Name.



Welcome to Digital.ai



Sign in to your account

By signing in, I agree to the digital.ai's [Privacy Policy](#).

Azure AD

or

Sign In Locally

Add SAML SSO Connection

In the OIDC procedure you used an existing Entra ID tenant. However, each SAML connection requires a unique tenant so part of this procedure will involve creating a new Entra ID tenant rather than using information from an existing one.

Prerequisites

Before you begin, ensure to have the following details from your IdP readily available:

- Descriptor Endpoint

NOTE

This may be unavailable until you have a Redirect URI and Entity ID, which is configured in step 5 of the following steps.

Logging In

1. Log in to the Platform as an administrator.
- In the left navigation, under SSO, click **Identity providers**.
 - Alternatively, you can click the **Setup identity provider** on the Platform overview page.
 - Click **Create identity provider** button.

digital.ai Platform

Account Overview

Platform overview

Power of Platform enables you to control users and SSO

Account admin

Account admin

Contact support

Community

Read documentation

SSO / Identity providers

User will be either automatically created once you set up SSO, or you can start creating internal users.

Setup Identity provider

Users

You have 1 user

Create user

Active users 1

Disabled users 0

Read documentation

View all >

Select Provider

2. Choose **Add SAML Provider** as the authentication service.

- In **Select identity provider**, choose **Other**.
- In **IdP display name**, add a unique, user-friendly name for the IdP. This name will appear on the Digital.ai Platform login page.
- Click **Next**.

Config identity provider and metadata

3. Copy the Redirect URI and Service Provider Entity ID to setup your identity provider. Ensure to share this information with your IT/Security/SSO team.

NOTE

If a descriptor endpoint was unavailable at the start, you should be able to provide one now.

NOTE

Do not save the Identity Provider at this time. We will revisit this page later to complete the process of creating the Identity Provider.

Add New Application in Entra ID

4. Login to your Entra ID account to add a new application for this connection.

- Log in to your **Microsoft Entra ID account**, and go to **Manage Entra ID Active Directory**.
- Go to **Manage > App registrations**.

- Click **+ New registration**.
- In **Name**, add a unique, user-friendly name for this connection.
- In the **Redirect URI section**:
 - In **Select a platform**, choose **Web**.
 - In the text box, paste the value of **Redirect URI** that you saved previously.
- Click **Register**.
- On the new tenant you just created, go to **Manage > Token configuration**.
- Click **+ Add optional claim**.
- Choose **SAML** and select all 3 options (**acct, email, upn**).
- Go to **Manage > API permissions**.
- Click **+ Add a permission** then choose **Microsoft Graph**.
- Click **Delegated permissions**.
- Under **OpenId permissions**, select **email** and **profile**.
- Go to **Manage > Expose an API**.
- Beside **Application ID URI**, click **Set**.
- In **Application ID URI**, paste the value of **Service Provider Entity ID** you saved previously.
- Go to **Overview** and click **Endpoints** tab.
- Copy the value of the **Federation Metadata URL** from the list of endpoints.
- Go to **Overview** and click **Endpoints** tab.
- Copy the value of the **Federation Metadata URL** from the list of endpoints.

Finish Creating the Connection in Config identity provider and metadata

5. Next you will return to the Platform SAML connection you left previously.
 - Your IT/Security/SSO team will use the **Redirect URI** and **Service Provider Entity ID** to configure your **Corporate IdP** and provide the **SSO setup details** in one of the following three formats::
 - If you select **I have the metadata URL** for my identity provider, then paste the **.well-known endpoint** into the **Enter Metadata URL** field and click **Import**. You will receive a success message once the data is imported. This import should update several fields in the configuration on the General page.
 - If you select **I have a file which contains the metadata**, then choose the file and upload.

- If you select **I want to manually configure the identity provider**, then enter the fields manually.
Click **Next**.

General

6. Depending on the selection you made in the previous step, the majority of fields may be automatically filled in.
- In **SAML configuration**, enter the **Single Sign-On Service URL**.
 - Click **Next**.

The screenshot shows a multi-step configuration wizard. The breadcrumb trail at the top reads: [Accounts](#) > [Staging Champagne](#) > [Identity providers](#) > [Add provider](#). On the left, a vertical sidebar lists the steps: 'Select provider', 'Config identity provider and metadata', 'General' (which is highlighted with a blue icon and text), 'Advanced config', 'Add mappers', and 'Summary'. The main content area is titled 'SAML Configuration' with the subtitle 'Configure SAML identity provider for single sign on.' Below this, there is a text input field labeled 'Single Sign-On Service URL *'. To the right of the input field, there are three buttons: 'Cancel', '< Previous', and 'Next >'. The 'Next >' button is highlighted with a red border.

Advanced Config

NOTE

Advanced Configuration page is optional.

7. Depending on the selection you made in the previous step, the majority of fields may be automatically filled in. Click **Next**.

NOTE

Ensure that Sync Mode is set to FORCE. Sync Mode is set to FORCE by default, which allows Digital.ai to update a stored user's data whenever it is changed in the IdP. If you set it to IMPORT, user data is only imported the first time they log in through the IdP.

SAML Advanced Configuration
Optional

- ☐ Trust Email ⓘ
- ☐ Account Linking Only ⓘ
- ☐ Hide on Login Page ⓘ
- First Login Flow
first broker login
- Post Login Flow
- Sync Mode**
FORCE
- Allowed clock skew (seconds)
3
- Single Log Out Service URL
- ☐ Backchannel Logout
- NameID Policy Format
Persistent
- Principal Type
Subject NameID
- ☐ HTTP-POST Binding Response
- ☐ HTTP-POST Binding for AuthnRequest
- ☐ HTTP-POST Binding Logout
- ☐ Want AuthnRequests Signed
- ☐ Want Assertions Signed

Cancel < Previous **Next >**

Mappers

i NOTE

Mappers page is optional.

8. Adding mappers to this configuration ensures that user and user group attributes from your IdP are correctly mapped with the Digital.ai Platform.

Accounts > Staging Champagne > Identity providers > Add provider

Select provider

Config identity provider and metadata

General

Advanced config

Add mappers

Summary

Mappers

Add ▼

Name	Category	Type	Actions
No data found			

Cancel < Previous Next >

To enable Digital.ai Platform to inherit user groups defined in your IdP, perform the following steps:

Add Group Mapper

- Click **Add and select Group mapper**. All the fields are populated by default.
- Enter the **Claim value**.

Add group mapper

Name *

Groups

Sync Mode

FORCE

Mapper Type

Attribute Importer

User Attribute Name *

groups

Attribute name*

i

At least one of these fields is required

Attribute Name

Friendly Name

Cancel

Add mapper

To add additional mappers, perform the following steps:

Add Mapper

- Click **Add** and select **Mapper**.
- In **Name**, enter the name of the mapper.
- In **Sync Mode**, select **INHERIT**.
- In **Mapper Type**, choose **Hardcoded Attribute** (for example).
- In **User Attribute**, enter the attribute name.
- In User **Attribute Value**, enter the attribute value.

Add mapper

Name *

Sync Mode

INHERIT

Mapper Type

Hardcoded Attribute

User Attribute *

User Attribute Value *

Cancel

Add mapper

Summary

9. On the **Summary** page you can review the configuration details.

- Click **Create identity provider**.

A new button will now appear on the Digital.ai Platform login page with the name you added under Display Name.

Add Attribute Mappers

10. Add the attribute mappers, which are required to map attributes in the SAML token coming from Entra ID to user attributes in the Platform. To do this, you'll need to edit the identity provider you just created.

- On the **Identity providers** page, click **Actions menu** and click **Edit**.
- Edit identity provider.
- Click **Mappers**.

- Click **Add Mapper**, fill in the details, then click **Create Mapper** to save the mapper. Repeat for each additional mapper in the list.
- Name: username
- Mapper Type: Attribute Importer
- Attribute Name:
- Friendly Name:
- User Attribute Name: username
- Name: email
- Mapper Type: Attribute Importer
- Attribute Name:
- Friendly Name:
- User Attribute Name: email
- Name: firstName
- Mapper Type: Attribute Importer
- Attribute Name:
- Friendly Name:
- User Attribute Name: firstName
- Name: lastName
- Mapper Type: Attribute Importer
- Attribute Name:
- Friendly Name:
- User Attribute Name: lastName

User Merge Flow

Users are presented with the User Merge Flow when the system detects a new user but with an existing email address. This happens when there is a change in users' identification or authentication method, for example, when users migrate from local authentication to Identity Provider (IdP) authentication. This flow links information to a single user even though the login method may have changed.

NOTE

A user may enter the **User Merge Flow** regardless of whether their Identity Provider uses **OIDC** or **SAML**. For instance, a company may have initially configured a SAML Identity Provider and later switched to an OIDC Identity Provider (or the other way around).

Scenarios That Trigger the User Merge Flow

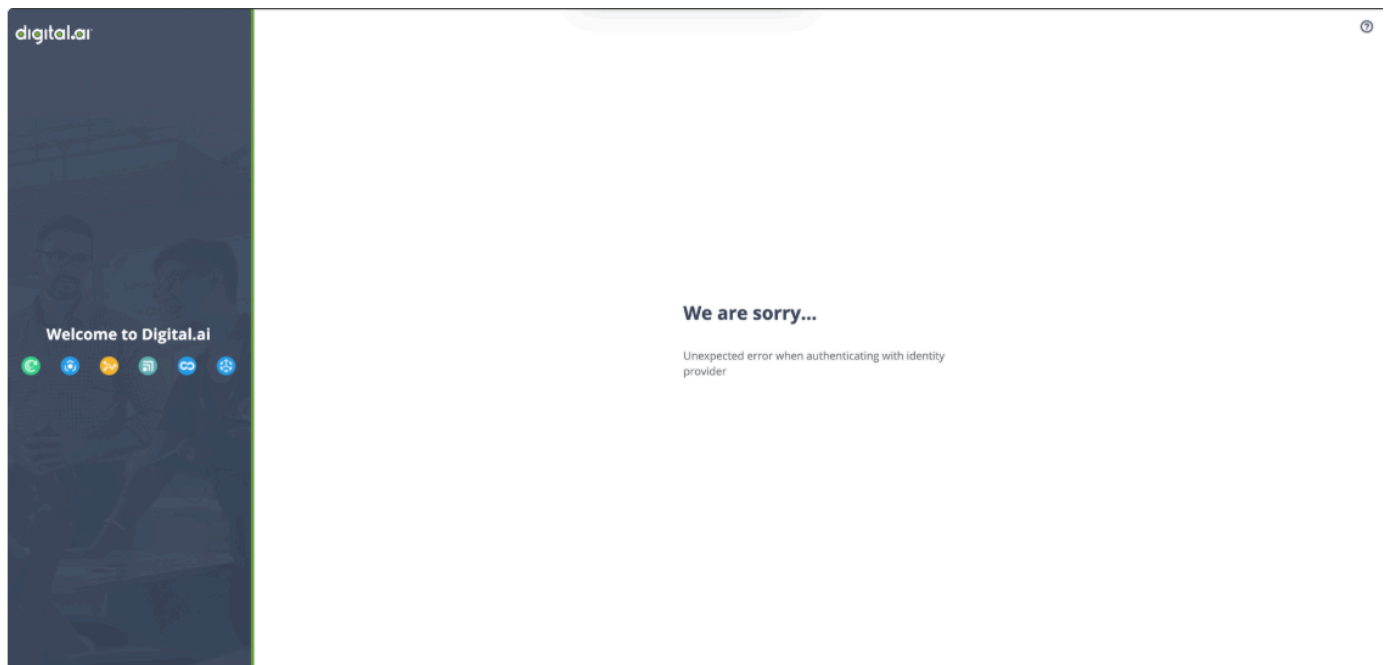
This section describes scenarios where the user merge flow will be triggered.

Supported Scenarios

- Logging in via an Identity Provider when a local user exists with the same email.
 - This scenario usually occurs during the initial account setup, where account-admins first create a local user to configure Single Sign-On (SSO).
- Logging in via a new Identity Provider after previously logging in through a different one (using the same email)
 - This typically happens when migrating to a new identity provider.
- The user's information has been updated, for example, a change in their last name.

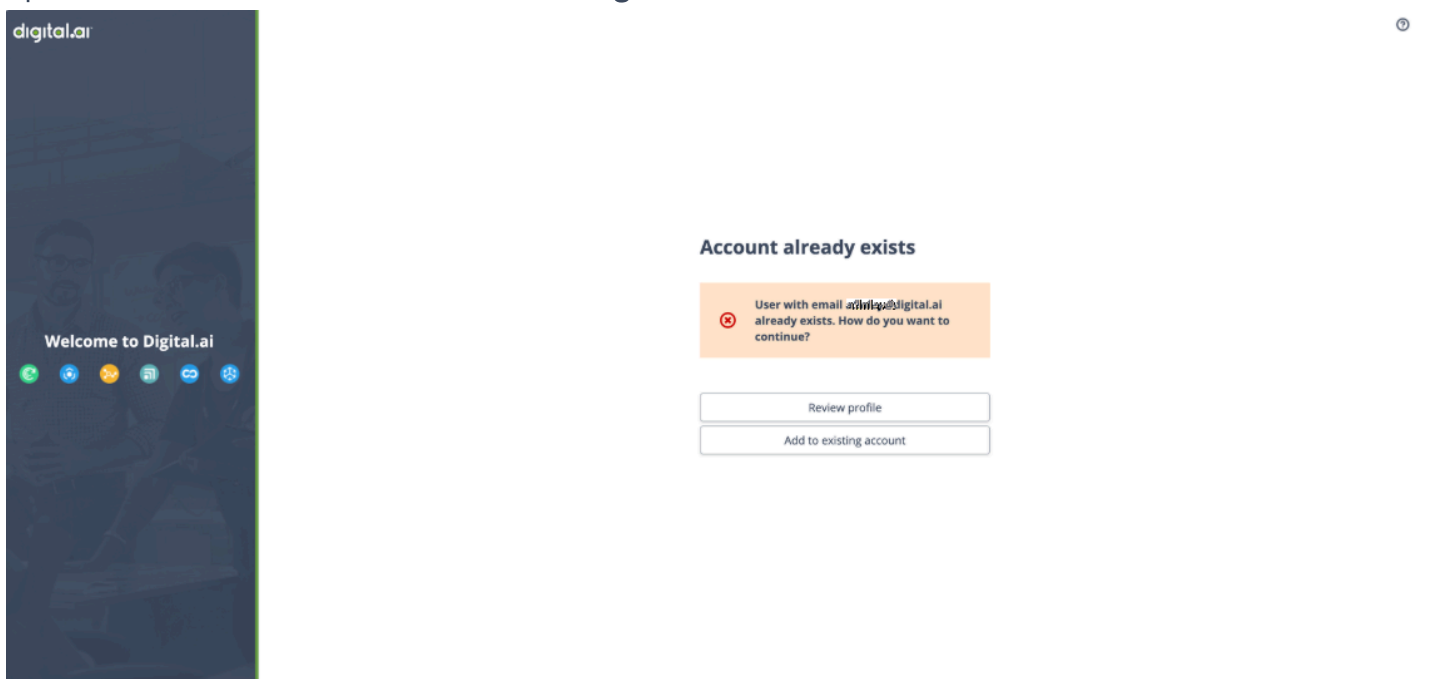
Unsupported Scenarios

- Modifying the NameID Format Policy of a SAML Identity Provider can result in the user being recognized as a new user (refer to Common Problems below).
 - This usually occurs when the configuration of an active (in-use) Identity Provider is modified.
 - This will cause an error when the user selects **Add to existing account** as shown in the figure below.



Steps after user starts the User Merge Flow

1. When the **User Merge Flow** is triggered, the user will be presented with a screen displaying the options **Review Profile** and **Add to existing account**.



2. **Review Profile** option takes the user to a page displaying their updated information. This step is optional and allows the user to verify their details before linking their account.



* Required fields

Update Account Information

Username *

Email *

First name *

Last name *

NOTE

After logging in, the user's First Name and Last Name are updated to reflect the information shown here. However, the Username remains unchanged.

- Click **Submit** to navigate back to the previous page.

3. The **Add to Existing Account** option will direct the user to the next page, where they will be prompted to verify their email address.



Link Azure - OIDC



You need to verify your email address to link your account with Azure - OIDC.

An email with instructions to link Azure - OIDC account afinley@digital.ai with your demoaccountafinley account has been sent to you.

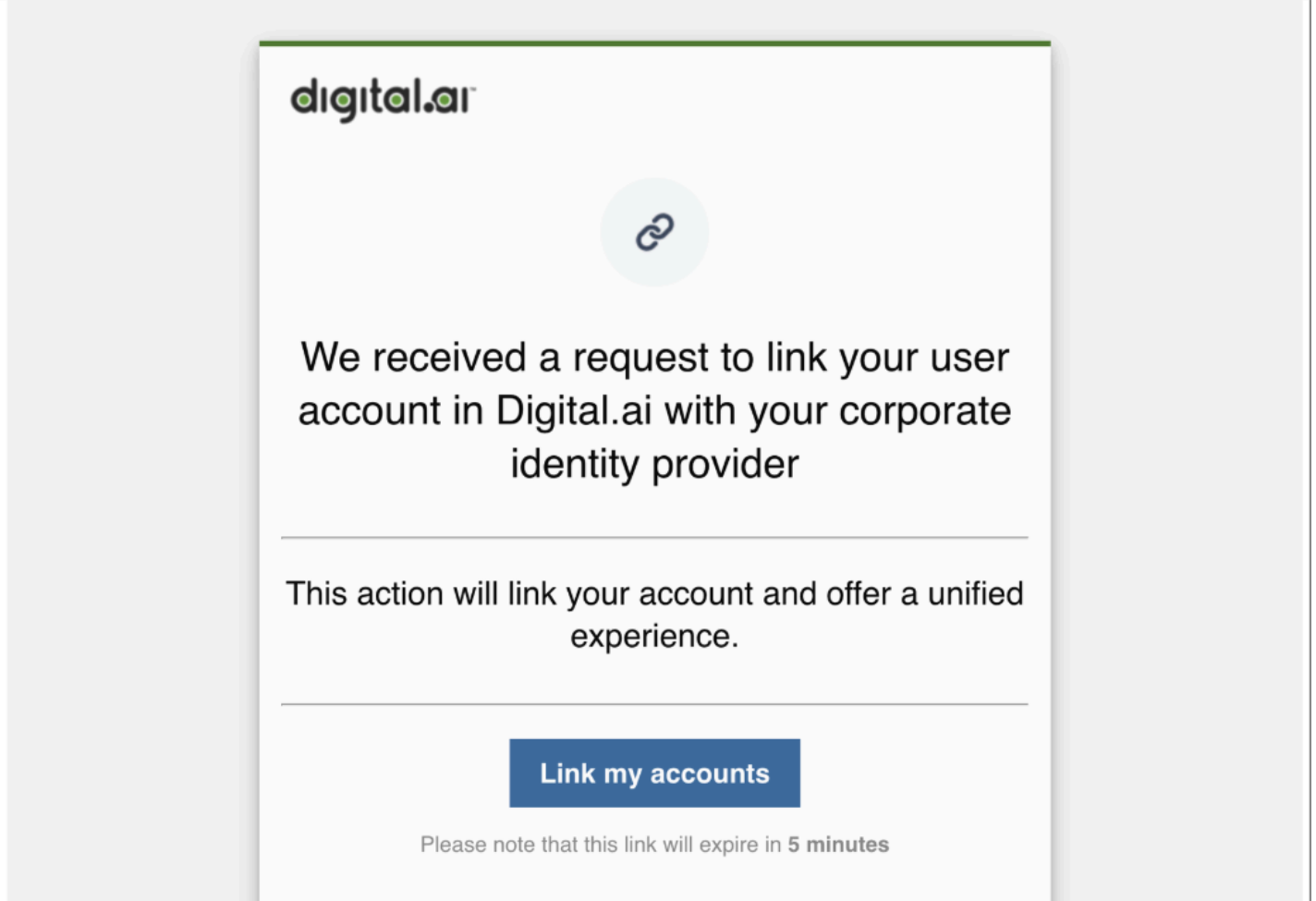
Haven't received a verification code in your email? [Click here](#) to re-send the email.

If you already verified the email in different browser [Click here](#) to continue.

[Try Another Way](#)

4. The user must check their inbox for an email from Digital.ai to confirm the merge. If the email does not arrive, they can use the provided link in step 3 to resend the confirmation email.

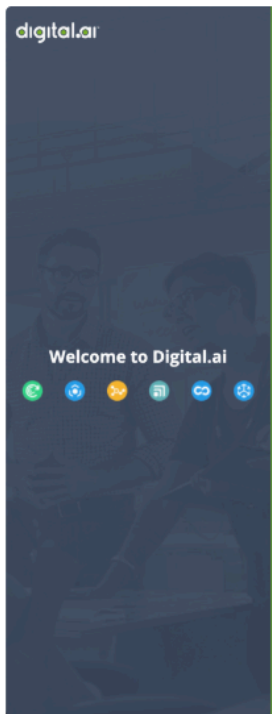
The following is an example of the email the user will receive:



Once the user clicks the **Link my accounts** button in the received email, they will automatically be logged in.

Common Problems and Solutions

1. Incomplete Information during the **User Merge Flow** (e.g., Missing First Name or Last Name).
 - If the Identity Provider is misconfigured, Digital.ai may be unable to accurately populate the user's information. In such cases, the user will be directed to the **Review Profile** page at the beginning of the flow and will be required to complete any missing fields before continuing:



* Required fields

Update Account Information

Username *

Email *

First name *

Last name *

Submit

- This is typically an indication that the necessary mappers have not been set up on the Identity Provider, so Digital.ai is unable to determine the source of the missing field information.

Solution

Review the Identity Provider configuration and ensure that the mappers are correctly referencing the appropriate attributes or assertions sent by the Identity Provider. For more information on how to setup mappers check [Map User Data](#)

2. Modifying the NameID Format Policy for a SAML Identity Provider

- For SAML Identity Providers, the **NameID Format Policy** determines which attribute uniquely identifies the user. If this setting is changed for an Identity Provider currently in use, the Platform may treat existing users as new users and trigger the **User Merge Flow**. This process will fail, and the user will encounter the following message:

Welcome to Digital.ai



We are sorry...

Unexpected error when authenticating with identity provider

Solution

Reverting the change to the **NameID Format Policy** field will resolve the issue. If reverting is not an option, deleting the affected users from the Platform and having them log in again will also resolve the problem.

Enable IP Address Allow List

The IP address Allow List is a security feature that controls and restricts access to the Digital.ai Platform based on specified IP addresses. When an IP allow list is configured, only the approved IP addresses or IP ranges can access the Platform, while all other connections are blocked.

By adding an external party's IP address to the allow list, administrators ensure that these users can connect to the Platform without compromising security.

Steps to Enable IP Address Allow List

1. Log in to the **Platform**. Click **Settings** and then Click **Access and Visibility** in the left-side navigation menu.

DS

Digital.ai Support



Overview



Applications



Audit log



Settings



USER MANAGEMENT



Users



User groups

SSO



Identity providers



Clients

2. Locate the **IP Allow List** option. Check the box labeled **Enable IP Allow List** to activate this feature.
3. Click **Add IP Address**. In the space provided, type the IP address that you want to allow access to the platform. Ensure that the IP address is correctly formatted (e.g., `192.168.1.1`).

The screenshot shows the Digital.ai Platform Settings interface. The left sidebar contains navigation links: 'Back to overview', 'Account', 'Sub-accounts', 'Access and visibility' (highlighted), 'Session management', 'User management', and 'User profile'. The main content area is titled 'Settings' and includes a breadcrumb trail: 'Accounts > Digital.ai Support > Accounts > Settings'. Under the 'User groups' section, there is a dropdown menu labeled 'Select groups'. The 'IP allow list' section is expanded, showing a description: 'An IP allow list helps your enterprise control access by allowing only trusted IP addresses, enhancing security and reducing unauthorized access risks.' Below this, the 'Enable IP allow list' checkbox is checked. The 'IP address' field contains '1.1.1.1' and has an 'Add IP address' button. A note under 'Applications visibility' states: 'Please note that using this feature will not block access to Digital.ai applications. Instead, it ensures that the links to restricted applications are not visible in the platform UI.' At the bottom right, there are 'Reset' and 'Save' buttons.

NOTE

This feature supports both IPv4 and IPv6 address formats.

4. Click **Save** to apply the settings. The platform will now allow access only from the specified IP addresses.

NOTE

If multiple external users need access, repeat **Step 3** to add additional IP addresses. Ensure that the IP allow list is regularly updated to reflect changes in authorized users.

Steps to Delete IP to Restrict Access

1. To remove an IP address, locate the entry in the list which needs to be blocked and click **Delete** option.

Manage Identity Providers

Guide for administrators to integrate corporate SSO identity providers with Digital.ai Platform.

Connect to OIDC Provider

Instructions for integrating an identity provider using the OIDC protocol with the Digital.ai Platform.

Connect to SAML Provider

Instructions for integrating an identity provider using the SAML protocol with the Digital.ai Platform.

Map User Data

Instructions for configuring attribute mappers to integrate user data from identity providers with the Digital.ai Platform.

Map User Group Assignments

Instructions for configuring mappers to automate user group assignments from OIDC identity providers on the Digital.ai Platform.

Map User Roles

Instructions for configuring mapper roles to integrate user data from identity providers with the Digital.ai Platform.

Set a Default IdP

Instructions for administrators to set, remove, and override default Identity Providers (IdPs) on the Digital.ai Platform.

SSO Certificates

Instructions for adding a sso certificates and managing expired certificates.

Manage Identity Providers

As an administrator, you can provide a seamless authentication and login experience for your users by connecting your corporate SSO identity provider with the Digital.ai Platform.

The Digital.ai Platform uses your existing SSO infrastructure to securely authenticate users in Digital.ai applications and portals using the same corporate credentials they already use. Acting as a bridge between your identity provider (such as Okta or Azure AD) and your Digital.ai applications, the Digital.ai Platform grants access to those applications based on user data that already exists in your identity provider, eliminating the need for unique credentials in each application. This single point of entry also allows users to log in to the Digital.ai documentation, support, and community portals for a more personalized experience there as well.



TIP

It is possible to connect to multiple identity providers. However, Digital.ai recommends setting one identity provider as default to skip the Digital.ai login screen entirely and send users directly to your trusted identity provider login. For more information, see [Set a Default IDP](#).

Authentication Protocol Procedures

In general, the Digital.ai Platform can integrate with identity providers that support the **OIDC** and **SAML 2.0** protocols. The process for integrating each with Digital.ai Identity is fairly similar, but there are unique requirements depending on which protocol your company uses.

Click one of the following buttons to read the procedure for each protocol:

Click here for
OIDC

Click here for
SAML

Key Concepts

Here are some basic concepts related to SSO that will help you better understand how everything works together:

- **Identity provider (IdP):** A single sign-on service that owns and maintains a directory of user credentials and an authentication mechanism. For example, Azure AD or Okta.
- **Service provider:** A web server that hosts a resource and provides access based on authentication information supplied by an identity provider. In this case, the Digital.ai applications such as Intelligence or Continuous Testing are considered service providers.
- **Identity broker:** An intermediary service that connects a service provider to an identity provider. The Digital.ai Platform, and more specifically Digital.ai Identity, is the identity broker between your IdP and Digital.ai applications such as Intelligence or Continuous Testing.
- **Identity federation:** A system of trust between two parties that links a user across each system without compromising security. As it relates to Digital.ai, the Platform handles user management by connecting to your IdP and then providing (federating) those users with access to your Digital.ai applications.
- **SAML:** Security Assertion Markup Language (SAML) is an XML-based open standard for exchanging authentication data across different systems. For more information on the SAML standard, see [SAML 2.0](#).
- **OIDC:** OpenID Connect (OIDC) is a JSON-based open protocol that extends OAuth 2.0 to add authentication data and allow for multiple connections to one IdP. For more information on the OIDC protocol, see [OpenID Connect](#).

The User Experience

When SSO is configured for your organization, an additional button appears on the Digital.ai Platform login page. When users click this button they are automatically passed over to your IdP for authentication.

Welcome to Digital.ai



Sign in to your account

By signing in, I agree to Digital.ai's [Privacy Policy](#).

SSO Login

Or

Sign In Locally

If you do not have a user account, you can [self-register](#)

TIP

You can specify the text on this button when you configure the SSO integration.

Additionally, once your Digital.ai applications are connected to the Platform, this Platform login page will appear for your users whenever they navigate directly to an application URL (from a bookmark or existing link). For more information about connecting applications, see [Applications](#).

WARNING

Once you have connected your identity provider to the Digital.ai Platform, we recommend that you no longer manage users in the individual Digital.ai products. Doing so may cause you to experience duplicate users, mismatched user info, or other inconsistencies.

Connect to OIDC Provider

In this topic, you will find instructions on how to establish a connection with an identity provider using the OIDC protocol.

Prerequisites

Before you begin, ensure to have the following details from your IdP readily available:

- Client ID
- Client secret
- .well-known/openid-configuration endpoint
- The claim names for the following user information: first name, last name, username, email. For more information, see [Map User Data](#).

NOTE

This information can be obtained by reviewing the Digital.ai application instance configured in your IdP. If you have not already created an app instance for Digital.ai, you must do so before continuing. We recommend working with your IT team or whoever manages SSO administration at your company.

Log in to the Digital.ai Platform

1. Log in to the Platform as an administrator.
2. In the left navigation, under SSO, click **Identity providers**.
 - Alternatively, you can click the **Setup identity provider** on the Platform overview page.
3. Click **Add identity provider** button to open the identity provider configuration wizard.

Step 1: Select provider Page

On the **Select provider** page, do the following:

1. In **Select authentication service**, choose **Add OIDC Provider**.

2. In **Select identity provider**, choose the provider that your company uses. If your provider is not listed, choose **Other**.
3. Under Configure your Identity provider, in Identity Provider display name, add a unique, user-friendly name for the IdP. This name will appear on the Digital.ai Platform login page.
4. Click **Next**.

Step 2: Config identity provider and metadata Page

On the **Config identity provider and metadata** page, do the following:

1. Copy the Redirect URI.
2. Now, in another browser window, you'll need to move over to your IdP account and use the Redirect URI to identify the Digital.ai Platform as a valid redirect URL. The process for completing this task will differ depending on which IdP you use. After you do this, you should be able to find the *.well-known endpoint* if you hadn't already.

NOTE

Depending on your role in your organization, you may need assistance from IT or whoever manages SSO administration at your company.

3. Select **I have the metadata URL for my identity provider** and paste the *.well-known endpoint* into the **Enter Metadata URL field**.
 - You can alternatively choose one of the other options here if it makes more sense for your situation.
4. Click **Import**.
5. Click **Next**.

Step 3: General Page

On the **General** page, do the following:

Depending on the selection you made in the previous step, the majority of fields may be automatically filled in.

1. In Client ID, paste the `Client ID` value from the prerequisites.
2. In Client Secret, paste the `Client Secret` value from the prerequisites.
3. Click **Next**.

Step 4: Advanced config Page

This is an advanced configuration page and is optional. Depending on the selection you made in the previous step, some of the fields may be automatically filled in.

1. Review the page and make any necessary selections.
2. Ensure that **Sync Mode** is set to `FORCE`. Sync Mode is set to FORCE by default, which allows Digital.ai to update a stored user's data whenever it is changed in the IdP. If you set it to IMPORT, user data is only imported the first time they log in through the IdP.
3. Click **Next**.

Step 5: Mappers Page

Mappers are optional, but can be useful if there are differences between data attribute names in your IdP and those expected by Digital.ai. For more information about mappers and how to configure them on this page if necessary, see [Map User Data](#).

Step 6: Summary Page

1. On the Summary page you can review the configuration details.
2. Click **Create identity provider**.

A new button will now appear on the Digital.ai Platform login page with the name you added at the beginning of this procedure.

Connect to SAML Provider

In this topic, you will find instructions on how to establish a connection with an identity provider using the SAML protocol.

Prerequisites

Before you begin, ensure to have the following details from your IdP readily available:

- metadata URL (different IdPs may have different names for this)
- The assertion names for the following user information: first name, last name, username, email. For more information, see [Map User Data](#).

NOTE

This information can be obtained by reviewing the Digital.ai application instance configured in your IdP. If you have not already created an app instance for Digital.ai, you must do so before continuing. We recommend working with your IT team or whoever manages SSO administration at your company.

Log in to the Digital.ai Platform

1. Log in to the Platform as an administrator.
2. In the left navigation, under SSO, click **Identity providers**.
 - Alternatively, you can click the **Setup identity provider** on the Platform overview page.
3. Click **Add identity provider** button to open the identity provider configuration wizard.

Step 1: Select Provider Page

On the **Select provider** page, do the following:

1. In **Select authentication service**, choose **Add SAML Provider**.
2. In **Select identity provider**, choose the provider that your company uses. If your provider is not listed, choose **Other**.

3. Under Configure your Identity provider, in **Identity Provider display name**, add a unique, user-friendly name for the IdP. This name will appear on the Digital.ai Platform login page.
4. Click **Next**.

Step 2: Config identity provider and metadata Page

On the **Config identity provider and metadata** page, do the following:

1. Copy the Redirect URI and Service Provider Entity ID.
2. Now, in another browser window, you'll need to move over to your IdP account and use the Redirect URI and Service Provider Entity ID to identify the Digital.ai Platform as a valid redirect URL. The process for completing this task will differ depending on which IdP you use.

NOTE

Depending on your role in your organization, you may need assistance from IT or whoever manages SSO administration at your company.

TIP

After you do this, you should be able to find the *metadata URL* if you hadn't already.

3. Select **I have the metadata URL for my identity provider** and paste the *metadata URL* into the **Enter Metadata URL field**.
 - You can alternatively choose one of the other options here if it makes more sense for your situation.
4. Click **Next**.

Step 3: General Page

On the **General** page, do the following:

1. In SAML configuration, enter the Single Sign-On Service URL.

2. Click **Next**

Step 4: Advanced config Page

1. Review the page and make any changes if necessary.
2. Ensure that **Sync Mode** is set to **FORCE**. Sync Mode is set to FORCE by default, which allows Digital.ai to update a stored user's data whenever it is changed in the IdP. If you set it to IMPORT, user data is only imported the first time they log in through the IdP.
3. Click **Next**.

Step 5: Mappers Page

Mappers are required to ensure that the Platform correctly parses user information from your IdP. For more information and instructions on how to add mappers on this page, see [Map User Data](#).

Step 6: Summary Page

1. On the Summary page you can review the configuration details.
2. Click **Create identity provider**.

A new button will now appear on the Digital.ai Platform login page with the name you added at the beginning of this procedure.

Map User Data

Your identity provider shares information about your users with Digital.ai in the form of key/value pairs (known as claims or assertions, depending on the IdP), and the Platform uses this data to create users in our system.

Platform administrators can use attribute mappers to ensure that user data from your IdP is properly understood by the Digital.ai Platform.

NOTE

The Platform requires first name, last name, email address, and username to create a user. You don't need mappers for any other data.

TIP

Mappers are also used when transmitting data from the Platform to other Digital.ai applications, but those mappers are configured automatically while connecting an application.

When to Use Mappers

Mappers are used within the Digital.ai Identity service which allows integration between a customer's Identity Provider (IdP) and the Digital.ai Platform. They serve as a bridge to translate the claims or attributes sent by the IdP into corresponding fields within a user profile in the Digital.ai Identity service

NOTE

Claims are pieces of information (attributes) about a user provided by the IdP. Examples include email addresses, usernames, roles, or custom-defined attributes such as department or region. These attributes are typically sent in the form of SAML assertions, OIDC tokens, or similar protocols used by the IdP during authentication.

OIDC

Mappers may be optional for OIDC connections.

Whether or not you need to use mappers to handle this data is entirely dependent on your organization's unique situation, and in general the Digital.ai Platform expects to receive user attributes based on the set of standard claims as defined by OpenID. You can view the list of standard claims here:

https://openid.net/specs/openid-connect-core-1_0.html#StandardClaim.

Digital.ai expects that `given_name`, `family_name`, `username` and `email` are included as claims. If these standard claims are included, they will automatically be mapped to the correct user attributes on the Digital.ai side. If this data is being sent in other claims, a mapper will be needed to map the claim name used by the customer to correct field on the Digital.ai side.

For example, if your IdP uses the standard claim `email`: `john@example.com`, the Platform will automatically map that to the Platform email user attribute.

However, if your IdP uses a claim called "email_address": `john@example.com`, then you would need to create a mapper to correctly get that data into the Platform email user attribute. See below for an example of how to map `email_address` to `email`:

Example Mapper: `Mapper Type`: The type of mapper, for mapping user data you should always use `Attribute Importer` `Claim`: The name of the claim in the customer's token `User Attribute Name`: The user attribute in Digital.ai that you are mapping to. This can be `firstName`, `lastName`, `username` or `email`.

SAML

Unlike OpenID Connect (OIDC), the SAML protocol does not follow standard naming conventions for the attributes it stores. These attributes, referred to as **assertions** in SAML tokens, can vary significantly across different Identity Providers (IdPs). This lack of standardization necessitates the use of **mappers** for SAML connections to ensure the Platform can correctly interpret the data provided by the IdP.

Why Mappers Are Required for SAML Connections

Each IdP defines the names of its assertions differently. For example, one IdP might use `givenName` for a user's first name, while another might use `first_name`. Without mappers, the Platform would not be able to recognize or use these attributes effectively.

To address this, you need to configure mappers to align the IdP's assertion names with the corresponding fields in the Digital.ai Identity service. By explicitly mapping these attributes, you ensure the Platform can accurately understand and process the user data.

Essential Mappers for SAML Connections

When setting up SAML connections, you *must* create mappers for the following critical user data:

- **First Name** : Map the IdP's attribute that represents the user's first name (e.g., `givenName`, `first_name`, etc.).
- **Last Name** : Map the IdP's attribute for the user's last name (e.g., `surname`, `last_name`, etc.).
- **Email** : Map the IdP's attribute for the user's email address (e.g., `email`, `emailAddress`, etc.).

Handling Username Data

The **username** field is treated differently in SAML connections. By default, the username is derived from the `NameID` attribute, which is defined in the IdP's SAML configuration. This behavior is governed by the following settings:

- **NameID Policy Format**
- **Principal Type**

You do not need to create a mapper for the `username` field unless you need to override the default `NameID` assertion. If an override is required, you can configure the mapper accordingly.

Example Scenario

Problem

An IdP sends SAML assertions with the following attribute names:

- `first_name` for the user's first name
- `surname` for the user's last name
- `emailAddress` for the user's email

Solution

Configure mappers in the Digital.ai Identity service as follows:

- Map `first_name` to the **firstName** field.
- Map `surname` to the **lastName** field.
- Map `emailAddress` to the **email** field.

The username will automatically be extracted from the `NameID` attribute based on the configured `NameID Policy Format` or `Principal Type`.

By carefully setting up mappers for SAML connections, you ensure that the Digital.ai Platform can process user data accurately, providing a integration experience with the IdP.

Entra ID Assertion Names

If you are using **Entra ID** the default assertion names are as follows:

- `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name`
- `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`
- `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname`
- `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname`

User Group Mappers

You can also use mappers if you want users to inherit group assignments from your IdP in the Platform or Digital.ai applications. To learn more about mapping group data, see [Map User Group Assignments](#).

Add or Edit Mappers

You can add mappers during the initial IdP configuration process, or at any time after you've already established the connection by returning to edit the identity provider.

1. Log in to the Platform as an administrator.
2. In the left navigation, under SSO, click **Identity providers**.
3. Find the SSO connection you want to modify and click the **Edit** icon under Actions.

4. Click **Next** until you get to the Mappers page.
5. Click the **Add** drop-down arrow, and select **Mapper**.
6. In the **Add mapper** window, set the following fields:
 - i. **Name** is merely a way to identify the mapper. Enter something like `First Name Mapper`.
 - ii. **Sync Mode** controls whether an update to a user attribute in your IdP will cause an update in the Platform. You are suggested to use **INHERIT**.
 - FORCE always updates the Platform user when there is a change in your IdP.
 - IMPORT never updates the Platform user after they are created the first time, regardless of changes in your IdP.
 - INHERIT uses the value that has been configured on the **Advanced config** page of this IdP connection.
 - iii. **Mapper Type** should be set to **Attribute Importer**.
 - iv. **(For OIDC providers only) Claim** is the name of the claim as specified by your IdP.
 - v. **User Attribute Name** is the Platform user attribute that the data will be mapped to. This should be set to `username`, `email`, `firstName`, or `lastName` depending on the data you're mapping.
 - vi. **(For SAML providers only) Attribute name** is the name of the assertion as specified in your IdP's SAML token. You can add the name in either **Attribute Name** or **Friendly Name** (you must complete at least one of the fields, but you do not need to complete both).
7. Click **Add Mapper**.
8. Repeat step 6 for any additional mappers.

Map User Group Assignments

You can use attribute mappers to ensure that your users inherit the correct user group assignments in the Digital.ai Platform. For You can use attribute mappers to ensure that your users inherit the correct user group assignments in the Digital.ai Platform. For more information about mappers and what they do, see [Map User Data](#).

Prerequisites

Before you begin, you must have already configured your SSO connection. For more information, see [Manage Identity Providers](#).

Add any groups you want to map in the Platform and check `Sync with IdP`. The name of the Groups in the Platform needs to match exactly the Group name that is being sent from the IdP.

NOTE

For Azure AD, only Group ID's are sent, so the Group names in the Platform need to be the Group ID's being sent.

IdP Group to Platform Group Mapping

You can create a mapper to enroll your SSO users in the correct Platform groups. This is important in order to bridge the gap between your IdP and a Digital.ai Products, so that users can be automatically assigned appropriate roles in each Product.

You only need to create one mapper for this purpose. This mapper identifies and informs the system which claim from the Identity Provider (IDP) contains the groups the user belongs to.

1. In the left navigation, under SSO, click **Identity providers**.
2. Find the IdP you want to edit, then click the **Edit** icon under Actions.
3. Click **Next** until you reach the **Mappers** page.
4. Click the **Add** dropdown and click **Group mapping**.
5. In **Claim**, enter the name of the group claim from your IdP.

6. Click **Add mapper**.

IdP Group to Platform Role Mapping

By default, any users created when logging into the Platform via an IdP are assigned the account-user role. If you would like to assign users a different role based on their Group access in the IdP that can be accomplished using a Group to Roles mapper.

This will only affect the user's role in the Platform itself, and will not have any impact on users or permissions in any individual products.

NOTE

This will only affect the user's role in the Platform itself, and will not have any impact on users or permissions in any individual products.

This is how to assign the account-admin role to any users in the IdP Group allAdmins.

1. On the same **Mappers** page, click the **Add** dropdown and click **Mapper**.
2. In **Name**, enter something descriptive like `allAdmins mapper`.
3. Leave **Sync Mode** as **INHERIT**.
4. In **Mapper Type**, choose **Advanced Claim to Role**.
5. In **New Key**, enter `groups`.
6. In **New Value**, enter `allAdmins` (the name of the group coming from the IdP).
7. In **Select Role**, choose `account-admin` (the Platform role that this group's users should belong to)
8. Click **Add mapper**.
9. Repeat the previous step for each group that you want to map to a role.

Group Mapping Workflow

Any group mapping for a user will be applied after the user logs into the Platform via their IdP. When a user logs in via the IdP, here are the steps that take place:

1. The Platform checks the token sent over from the IdP to see if there are any groups.

NOTE

The claim/assertion checked is the claim/assertion defined in the Group Mapper added to your IdP.
See [step 5 in IdP Group to Platform Group Mapping](#).

2. The Platform places the user in any Groups that have a name that matches the Group sent from the IdP if `Sync with IdP` is set to **True** for the Group.

Map User Roles

Mapping user roles refers to the process of relating user attributes from an external Identity Provider (IDP) to corresponding roles within the Digital.ai Platform console. This feature allows you to utilize existing roles or group membership in your company's IdP to automatically assign the correct role membership in the Digital.ai Platform.

To achieve this, User role mappers are created within the Identity Provider configuration. These mappers examine user's attributes role and assign a specific role within the Platform accordingly. For example, suppose your IDP is configured, and it defines a role called System Administrator. This document will show you how to grant the Platform's account-admin role to users who already have the System Administrator role in your IdP. Once the mapping is configured, users signing in through the IdP who have the System Administrator role will automatically be assigned the account-admin role with the Platform.

One common scenario is when organizations want to manage user roles centrally in their corporate IDP. These mappers can be used to ensure IdP roles correctly translate into Platform permissions.

You need to have an IDP configured for your organisation. To configure IDP follow these steps [Configure IDP](#)

To Map User Roles

For mapping user roles follow these steps:

1. On the **Mappers** page, click the **Add** dropdown and click **Mapper**.
2. In **Name**, enter something descriptive like `allAdmins mapper`.
3. Leave **Sync Mode** as **INHERIT**.

NOTE

Sync Mode controls whether an update to a user attribute in your IdP will cause an update in the Platform.

- **FORCE** always updates the Platform user when there is a change in your IdP.
- **IMPORT** never updates the Platform user after they are created the first time, regardless of changes in your IdP.

- INHERIT uses the value that has been configured on the **Advanced config** page of this IdP connection.

4. In **Mapper Type**, choose **Advanced Claim to Role**.

5. In **New Key**, enter `groups`.

i NOTE

`groups` is not a constant value; it can change based on what customer's IdP sends.

6. In **New Value**, enter `allAdmins` (the name of the group coming from the IdP).

7. In **Select Role**, choose `account-admin` (the Platform role that this group's users should belong to)

8. Click **Add mapper**.

9. Repeat the previous step for each group that you want to map to a role.

In the **Select Role** dropdown, Below are the available roles you can assign in the mapper:

- `account-admin`: Grants full administrative access to the account. Users with this role can manage users and roles, Configure account settings, Perform high-level administrative tasks across all applications.
- `account-analytics-author`: Provides access to analytics dashboards and the ability to create or modify reports.
- `account-application-admin`: Provides admin-level access to manage applications under the account.
- `account-service`: A special service-level role used for automated systems or backend services. Users with this role can authenticate as service accounts, Access APIs or services as per assigned scopes.
- `account-user`: The default role for regular users. Users with this role can login to the system, Access features and services permitted by the account's policy, View their own data or perform user-level tasks.

Summary Page

On the Summary page you can review the configuration details.

Set a Default IdP

As an administrator, when you have multiple IdPs configured for your account, you can set one of them as the default.

Setting an IdP as the default will skip the Platform login screen and send users to the IdP as if they had clicked the button for it. If they already have an active session with the IdP, most IdPs will redirect the user to the application directly and they will not see a login screen at all.

Set a Default IdP

- 1. Log in to the Platform as an administrator.
- 2. Click **Identity providers** from the left side OR click **View All** from the *SSO / Identity providers* section on the Overview page.
- 3. On the Identity providers page, click the **star** icon for the IdP that you want to set it as default.

Identity providers ⌵

Name	Provider	Enabled	Redirect URI	Default	Actions
SSO Login	OIDC	True		★	  

- 4. Optionally, you can disable self registration from this page. If you do select the checkbox to disable self registration, the **Allow user registration from domain whitelist** option in the [Account Settings Page](#) will be automatically disabled.
- 5. In the confirmation dialog, type the IdP name and click **I understand the risks**.

Now in the Identity providers list, a star icon appears under the *Default* column corresponding to the default IdP. Additionally, a **Default** label appears in the *SSO / Identity providers* section on the Overview page.

SSO / Identity providers

You have 1 identity providers.

Setup identity provider



Identity Provider Azure OIDC

Redirect Uri: <https://identity.staging.digital.ai>

Default



Active

Remove Default IdP

1. On the Identity providers page, click the transparent **star** icon under the Actions column for the IdP that you want to unset.
2. In the confirmation dialog, click **Unset**.

Now the **star** icon against the default Identity provider and the **Default** label in the *SSO / Identity providers* section on the Overview page are removed and the Platform's local login screen reverts.

Override a Default IdP

Certain users (for example, support personnel or account administrators) may need to override the default IdP login screen and authenticate using their local user credentials. To do so, append the following query parameter to the end of your Platform account URL: `/?loginIdp=local`

For example: `https://exampletech.digital.ai/?loginIdp=local`

SSO Certificates

What is SSO Certificate?

The Digital.ai Identity Service supports a Signature Validation feature that uses a Signing Certificate to validate any responses from the IdP. We refer to this Signing Certificate as the **SSO Certificate**. It can be included in the Identity Provider config in the Platform Console.

NOTE

Customers will very rarely update a Signing Certificate directly. Usually, they will provide a well-known endpoint and the Platform Console will pull the **Signing Certificate** from there directly when creating the Identity Provider.

Add a Signing Certificate to an IdP

There are two different ways that a Signing Certificate can be provided to an IdP:

1. Add the certificate directly to the IdP.
2. Add a certificate URL that can be called to get the certificate.

Using option 2 is the preferred method because it prevents the user from needing to update the certificate in the Platform console when it expires.

Open ID Connect (OIDC)

For an OIDC Identity Provider: The field for the SSO certificate is **Public Key Signature Verifier Key**. This only shows up if **Validate Signature** is checked.

Add certificate directly

1. Navigate to the **Advanced Config** section of the Identity Provider config.
2. Check the **Validate Signature** checkbox.

- Under the **Public Key Signature Verifier Keys** field, add the public key of the Signing certificate in PEM format.
- Under the **Public Key Signature Verifier Key ID** field, add the ID of the validating public key given in the previous step.

3

☐ Pass login_hint ⓘ

☐ Pass current locale ⓘ

☐ Backchannel Logout ⓘ

☐ Disable User Info ⓘ

Prompt ▼

The prompt parameter in the OIDC specification. See the specification for more details.

☐ Accepts prompt=none ⓘ

☒ Validate Signatures ⓘ

☐ Use JWKS URL ⓘ

Public Key Signature Verifier Key

Public Key Signature Verifier Key ID

Forwarded Query Parameters

Cancel < Previous Next >

Add Certificate URL

- Navigate to the **Advanced Config** section of the identity provider config.
- Check the **Validate Signature** checkbox.
- Check the **Use JWKS URL** checkbox.
- Set the **JWKS URL** to the URL where the identity provider's keys in JWK format are stored.

Select provider

Config identity provider and metadata

General

Advanced config

Add mappers

Summary

FORCE

Allowed clock skew (seconds)

3

☐ Pass login_hint ⓘ

☐ Pass current locale ⓘ

☐ Backchannel Logout ⓘ

☐ Disable User Info ⓘ

Prompt

The prompt parameter in the OIDC specification. See the specification for more details.

☐ Accepts prompt=none ⓘ

☒ Validate Signatures ⓘ

☒ Use JWKS URL ⓘ

JWKS URL

https://identity.staging.digital.ai/auth/realms/external-idp-release-demo/protocol/openid-connect

Forwarded Query Parameters

Cancel

< Previous

Next >

Security Assertion Markup Language (SAML)

For a SAML Identity Provider: The field for the SSO certificate is **Signing Certificate**. This only shows up if **Validate Signature** is checked.

Add certificate directly

To add an SSO Certificate to a SAML Identity Provider, follow the following steps.

1. Navigate to the **Advanced Config** section of the Identity Provider config.
2. Check the **Validate Signature** checkbox.
3. Add your signing certificate under the **Signing Certificate** field.

Select provider

Config identity provider and metadata

General

Advanced config

Add mappers

Summary

☐ HTTP-POST Binding Logout

☐ Want AuthnRequests Signed

☐ Want Assertions Signed

☐ Want Assertions Encrypted

☐ Force Authentication

☒ Validate Signature

Metadata Descriptor URL

☐ Use Metadata Descriptor Url

Signing Certificate

☐ Sign Service Provider Metadata

Requested AuthnContext Constraints
You can specify constraints on the authentication method verifying the user identity.

Comparison
Exact

Cancel Previous Next

Add Certificate URL

To add a certificate URL to a SAML Identity Provider, follow the following steps.

1. Navigate to the **Advanced Config** section of the Identity Provider config.
2. Check the **Validate Signature** checkbox.
3. Check the **Use Metadata Descriptor URL** checkbox.
4. Add the certificate URL under the **Metadata Descriptor URL** field.

Select provider

Config identity provider and metadata

General

Advanced config

Add mappers

Summary

☐ Want Assertions Signed

☐ Want Assertions Encrypted

☐ Force Authentication

☒ Validate Signature

Metadata Descriptor URL *

☒ Use Metadata Descriptor Url

☐ Sign Service Provider Metadata

Requested AuthnContext Constraints
You can specify constraints on the authentication method verifying the user identity.

Comparison
Exact

AuthnContext ClassRefs (comma-separated)

AuthnContext DeclRefs (comma-separated)

Cancel

< Previous

Next >

How to Manage Expired SSO Certificates

i NOTE

This section only applies to SAML Identity Providers who have added the **Signing Certificate** directly from the Identity Provider (Option 1 above). If you are using a certificate URL, the certificate will be controlled by your organization and it is upto your organization to update it.

The Platform Console runs a report daily that checks for expiring certificates, and will email account administrators when a certificate is close to expiring. An email will be sent under the following conditions:

- An Identity Provider has an SSO certificate expiring in the next 21 days.
- An Identity Provider has an SSO certificate that expired within the past 10 days.

This email will be sent to all account-admin users on the Identity Provider's account.

Sample Email:

SSO Certificate is expiring in the next 21 days:

Digital.ai SSO Certificate Expiring



no-reply@digital.ai
To: rrello+pr1025qa1@digital.ai

Reply

Reply All

Forward

Thu 9/14/2023 2:57 PM

If there are problems with how this message is displayed, click here to view it in a web browser.

[EXTERNAL]

Your certificate is expiring

The signing certificate used for your SAML Identity Provider with name 'expiring' is expiring in 1 days (on 2023-09-15 19:29:09+00:00).

Please update the signing certificate before the expiration date to prevent your users from losing the ability to sign in.

Why am I receiving this email?

You are receiving this email because you have a SAML Identity Provider configured for the Digital.ai platform and it has an expiring signing certificate.

Please note: This is an automated email. Please do not reply. This email was sent by Digital.ai.

SSO Certificate has expired:

Digital.ai SSO Certificate has Expired



no-reply@digital.ai
To: rrello+pr1025qa1@digital.ai

Reply

Reply All

Forward

Thu 9/14/2023 2:57 PM

If there are problems with how this message is displayed, click here to view it in a web browser.

[EXTERNAL]



Your certificate has expired

The signing certificate used for your SAML Identity Provider with name 'expired' has expired on 2023-09-05 00:10:11+00:00.

Please update the signing certificate to restore login functionality for this Identity Provider. If you can no longer login, please contact our support team for assistance.

If the certificate is not updated, we will stop notifying you of this certificate in 1 days.

Why am I receiving this email?

You are receiving this email because you have a SAML Identity Provider configured for the Digital.ai platform and it has an expired signing certificate.

Please note: This is an automated email. Please do not reply. This email was sent by Digital.ai.

API Overview

Overview of the Digital.ai Platform REST API, detailing HTTP methods, data exchange formats, and CRUD operations.

API Reference

Explore API operations with examples and understand how to implement pagination, sorting, filtering, and bulk oper...

Access Tokens

Overview of the Digital.ai Platform access tokens.

API Overview

The Digital.ai Platform API reference documentation describes the HTTP method, path, and parameters for every operation. It also displays example requests and responses for each operation.

For more information, see [API Reference](#).

The Digital.ai Platform API is a REST API, which means that you can use standard HTTP methods (GET, POST, PATCH, PUT, and DELETE) to retrieve, submit, change, and delete data. To ensure data privacy, the API is served over HTTPS; unencrypted HTTP is not supported.

REST also uses Uniform Resource Identifiers (URIs) and most often JavaScript Object Notation (JSON) conventions for data exchange between the client and the server.

How It Works

Each interface provides a set of API resources that let you perform various Platform tasks. Each resource has a URL (or endpoint) on the Digital.ai server. To call a resource, you send a request to the appropriate URL, and the Digital.ai server responds with JSON-formatted data.

When you make a request to the REST API, you will specify an HTTP method and a path. Additionally, you might also specify request headers and path, query, or body parameters. The API will return the response status code, response headers, and a response body.

The REST operations GET, POST, PATCH, PUT, and DELETE are described as follows:

- GET - The GET method is used to retrieve/request data for a resource.
- POST - The POST method is used to create a data resource or invoke an operation resource.
- PATCH - The PATCH method is used to create or update a sub-resource within the target resource. If the target resource instance does not exist, the server will not create it.
- PUT - The PUT method is used to create or replace the target resource.
- DELETE - The DELETE method is used to delete the target resource.

Authentication

Rest API authentication is used to authenticate users and applications when performing API tasks. Authentication is a must to ensure that APIs are secure and accessible only to authorized users.

Digital.ai Platform supports Token Authentication. The token can be obtained via Basic or OAuth mechanisms but the API accepts only bearer tokens.

The majority of our API endpoints are secured, so you must authenticate before use. However, in other scenarios, the service may require separate authentication with the Platform. This section provides a detailed explanation of the authentication process for such services.

To consume our APIs, whether through Swagger, Postman, Curl, or a custom script, you must use the OAuth 2.0 Client Credentials grant. Before you can authenticate, you need to create **For API Use** application that represents your client. Once the Client is created, you can use the associated `client_id` and `client_secret` to obtain an access token.

For more information refer [RFC 6749](#)

Perform the following steps to do this action:

Prerequisite

You must have a Client that you can use to authenticate. This client should be created as **For API Use** application.

If you don't have one yet, follow the steps below to create it.

Create Client

To create a client, you need to create an application:

NOTE

You only need to do this once. Once you have a client, it remains valid until you delete it.

1. Log in to Digital.ai Platform.
2. In the left navigation, click **Applications**.

Alternatively, you can click the **Create application** button on the Platform Overview page.

3. In Select application, choose `For API Use` as the application type.
4. In Instance name, assign the application's user defined name for your application.
5. Click **Next** to proceed to the Advanced configuration section.
6. Accept the default values on the Advanced configuration and Mappers pages.
7. On the Get client ID & secret page save the Client ID and Client Secret values.
8. Click **Complete** to finish creating the application and the associated client.

2. Use /token to get a token (as described in the OIDC spec)

To get a token:

1. Determine token URL
 - a. Call this endpoint, provide your vanity domain in the `?hint=` parameter.

```
https://api.us.digital.ai/identity/v1/accounts/{account_identifier}/.well-known/openid-configuration/?hint=<vanity domain here>
```

For example:

```
curl -X GET "https://api.digital.ai/identity/v1/accounts/auth/configuration/?hint=champagne" -H "accept: application/json"
```

- b. In the response, retrieve the `token_endpoint` value, for example:

```
https://identity.us.digital.ai/auth/realms/champagne/protocol/openid-connect/token
```

For more information refer [RFC 6749](#)

2. Prepare POST request with the following details:
 - a. Headers:
 - content-type = `application/x-www-form-urlencoded`

- Default headers usually ok for most HTTP Clients
- b. Body: (x-www-form-urlencoded)
- grant_type = client_credentials
 - client_id = insert Client ID from "Create Client" section.
 - client_secret = insert Client Secret from "Create Client" section.
 - scope = openid dai-svc
- c. Retrieve access_token from token endpoint response.

Example request:

```
curl --location --request POST \
'https://identity.us.digital.ai/auth/realms/champagne/protocol/openid-
connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=<client id retrieved from create client section>' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_secret=<client secret retrieved from create client
section>' \
--data-urlencode 'scope=openid dai-svc'
```

Example response:

```
{
  "access_token": "S1AV32hkKG",
  "token_type": "Bearer",
  .....
}
```

3. Use the token to authenticate a request

To interact with the API:

1. Identify the API endpoint you want to call.
2. Include the access_token in the Authorization Header:

a. Authorization = Bearer (insert access token)

Example request:

```
curl --location --request GET 'https://api.us.digital.ai/licensing/products' \
--header 'Authorization: Bearer <access_token>'
```

API Reference

The Digital.ai Platform API reference documentation describes the HTTP method, path, and parameters for every operation. It also displays example requests and responses for each operation.

To view a list of all endpoints with examples, see: [Digital.ai Platform API Reference](#).

The following sections describe the API usage parameters such as Pagination, Sorting, Filtering, Bulk Operations, and Error types. These parameters are included in the request URL as query parameters.

Pagination

Pagination is necessary when you are dealing with a lot of data and endpoints. When you use a GET API request to retrieve information from a server via an API endpoint, the returned JSON file will sometimes include a large amount of data. In order to search through the database and retrieve data in smaller pieces, pagination is used, which helps in querying the database efficiently.

All endpoints that support pagination accept *count* and *start* integer query parameters. The response will include pagination meta data.

Pagination meta data:

```
{
  ...
  "pagination": {
    "start": integer, # the requested start value
    "count": integer, # the requested count value
    "next_start": integer, # optional, included only if there are more records
to retrieve
    "previous_start": integer, # optional
    "total_available": integer
  }
}
```

Sorting

Sorting helps you to arrange data in either ascending or descending order. When you request data and want to sort the results by a condition, then you may want to use the sorting parameter to arrange the response in either ascending or descending order (sort direction).

The endpoints that support sorting accept *sort* query parameter. The parameter value is a comma-separated list of field names. To reverse sort direction, prefix the field name with `-`.

Filtering

Filtering helps you to filter out a subset of data for which the conditions applied are true.

Endpoints support multiple *filter* query parameters, separated by `&` (http url standard). For example,

`...?filter="filter1"&filter="filter2"`. This is used to combine results of filter1 and filter2 (i.e. OR).

Each filter can contain one or more entries for "fields". For example,

`...?filter="field1[operator]:value;field2[operator]:value"&filter="field1:value"`. In this case, the "field" entries are separated by a semicolon `;`, and the result will include only the entities that satisfy all field entries (i.e. AND).

The Operators could be eq, ne, lt, le, gt, ge, in, and so on.

Bulk Operations

Using bulk operations, you can run the same operations on one or more resources within a single request.

You can use each PATCH, PUT, and DELETE endpoint to update or delete a list of entities in a single request to affect all of them. Any bulk operation must include the X-Action: bulk header.

Example:

When updating, use the PATCH or PUT route for that entity type without an ID, providing a list of objects with fields to be updated and the ID for each, rather than a single object.

The return response would include a list of updated entities, not_updated IDs, failed IDs, and errors containing the entity ID along with the error message from the server. If no entities were updated the response would be `HTTP 304 Not Modified`.

Error Types

All errors (4xx, 5xx) are returned in the following JSON format:

```
{
  "error": {
    "guid": "<uuid>",
    "code": 123,
    "message": "Message here",
    "error_details": "Optional error details"
  }
}
```

Access Tokens

Access Tokens

An access token is an API token that can be used to access our APIs. It needs to be provided under the `Authorization` header when making API requests. This token is used to determine the user, user's account, and the users permissions.

NOTE

Access tokens provide a convenient way to enable specific integrations, such as Webhooks, but they are not a substitute for OIDC (OpenID Connect) based authentication. Not all parts of the API grant the same permissions or actions for access tokens compared to other authentication methods. While a user cannot use an access token to perform actions beyond their role's permissions, permissions may be even more restricted depending on the API or endpoint. Access tokens are designed for specific use cases and should not be viewed as a comprehensive authentication solution.

digital.aiPlatform

CChampagne

Back to overview

ANALYTICS

Metadata viewer

Datasets

Dashboards

CONFIGURATION

Application properties

Code standardization

Snapshots

Transformed data stores

Champagne > Dashboards

Dashboards

Select applicationAgility

Search

SSSalor JsaC S'13TV

View profile

Access tokens

Sign out

All dashboards ☆ Favorites

Name ↑	Description	Categories
☆ Demo obsolete	Demo	Agility Analy
☆ Agile earned value	The Agile earned value dashboard enables you to compare the planned work, actua...	Agility Analy
☆ Agile earned value (JFJ test)	The Agile earned value dashboard enables you to compare the planned work, actua...	Agility Analy
☆ Agile earned value (JFJ2)	The Agile earned value dashboard enables you to compare the planned work, actua...	Agility Analy

Rows per page: 25 1-25 of 97

Generate New Tokens

digital.ai

Platform

3

SS

Profile

Access tokens

Sign out

← Back

Personal access tokens

You can use the personal access tokens as an alternative to passwords when accessing the public API.

Generate new tokens

Token name

Demo

Expiration

30 days

Generate

⚠

Make sure to copy your personal access token now. You won't be able to see it again!

✓ a8d633d1-cc7b-42a1-be48-78d2dfbee2e2

Copy token

Tokens in use

Name	Created ↓	Expiration	Actions
Demo	11/10/2024, 11:47:12 pm	10/11/2024, 11:47:10 pm	🗑

Rows per page: 25 0-0 of 0 < >

Follow the steps below to create a new access token:

1. Click your profile in the top-right corner, then click **Access Tokens**.
2. In the **Token Name** field, provide a clear and descriptive name for the access token. This should describe the purpose of the token.
3. Choose an expiration date for the token. You can select a duration between **30 days** and **Never**, depending on how long you need the token to be valid.
4. Once the details are filled, click on the **Generate** button to create the access token.
5. After generating, the access token will appear below. **Make sure to save it**, as you will not be able to view the token again.

⚠ CAUTION

The token will also appear in the **Tokens in Use** list, but the actual token value will not be displayed again.

📘 NOTE

Remember, the token is tied to your user account, so ensure it is securely stored.

Make a Request to the API Using the API Token

API tokens can be used to make API requests. In order to use the API token in a request, you will need to include it in the `Authorization` header with the prefix `Token`.

The generated token is prefixed with `Token`, followed by a space. For example `Token 7d7ddd46-4799-4c3d-96bd-b16ddb6a2eb`

Data API

The Digital.ai Data API service enables you to accurately assess your IT effectiveness and determine failure factors that could lead to an incident. The Data API service provides you with [Change Failure Predictions](#) and [Change Credit Score](#) APIs. The service provides details about indicators of a potential change failure, along with predictions of success or failure based on historical performance, current context, and quality checks. The use of Change Failure Predictions and Change Credit Score APIs enables Change Executives more informed decision-making within the source system.

Digital.ai manages the client credentials required for authenticating with the Data API using an API token. The source system will invoke the Data API to retrieve the following:

- **Change Failure Predictions API:** An AI-powered solution that analyzes change requests to predict failure probability and identify specific risk factors.
- **Change Credit Score API:** A sophisticated scoring system that evaluates and rates the reliability of teams, groups, or projects based on historical performance.

Key capabilities include:

- **Predictive Analytics:** Forecast potential change failures before they occur.
- **Risk Assessment:** Identify and quantify risk factors in your IT changes.
- **Performance Scoring:** Evaluate team and project performance through credit scoring.
- **Historical Analysis:** Leverage past data to improve future outcomes.

Authentication

API authentication is the process of verifying the identity of a user who is making an API request, usually treated like passwords.

Refer to [Authentication](#) to generate a token and authenticate.

Change Failure Predictions

The Change Failure Predictions API offers insights into the likelihood of change failure and the key risk factors contributing to it. By leveraging machine learning models it enables you to make informed

decisions through predictions of change failure probabilities and associated risk scores. The API accepts business IDs as input and returns predicted outcomes, contributing features, and model information.

• **REST API Endpoint and Details**

Details the endpoint URLs, HTTP methods, and structure for accessing the API services.

- Endpoint: `https://api.us.digital.ai/ml-inference/store/{project_name}/{model_name}` or `https://api.eu.digital.ai/ml-inference/store/{project_name}/{model_name}`
- Details:
 - Digital.ai Platform URL: `https://api.us.digital.ai` or `https://api.eu.digital.ai`
 - API Path: `/ml-inference/store/{project_name}/{model_name}`
 - Method: `POST`

• **Path Parameters**

Describes the required and optional parameters that must be included in the API endpoint path.

- `project_name`: Unique identifier of the initiative or project. For example, `ChangeFailure`.
- `model_name`: Name of the model used in the project. For example, `CatBoostClassifier`.

i NOTE

The values of `project_name` and `model_name` are based on the subscription and are shared by Digital.ai.

• **Request**

Specifies the structure and required fields for making a valid API request.

Parameter	Type	Required	Description
<code>business_ids</code>	Array	Yes	List of change IDs to analyze for failure prediction

For example:

```
{
  "business_ids": ["CHG1", "invalid_id"]
}
```

- **Response**

Explains the structure and fields included in the API response.

Field	Description
id	Object with name (usually "business_id") and value (the change ID)
features	Array of feature objects: each has name, value, and feature_importance. The feature_importance value shows how much a feature influenced the prediction. High values highlight key risk drivers, while low or zero values indicate minimal impact
predictions	Array of prediction objects: each has name (e.g., "probability_N", "probability_Y") and value
ml_model_id	Identifier for the machine learning model used
message	Status message (e.g., success or error)
created_on	Timestamp of the response creation

For example:

```
[
  {
    "id": {
      "name": "business_id",
      "value": "CHG1"
    },
    "features": [
      {
        "name": "feature_1",
        "value": "feature_1_value",
        "feature_importance": 0.023064278053662977
      },
    ],
  },
]
```

```
{
  "name": "feature_2",
  "value": "feature_2_value",
  "feature_importance": 0.32746387262962945
},
{
  "name": "probability_N",
  "value": 0.6417114272690727
},
{
  "name": "probability_Y",
  "value": 0.35828857273092724
},
{
  "ml_model_id": 42,
  "message": "Data retrieved successfully",
  "created_on": "2023-10-03T12:00:00Z",
},
{
  "id": {
    "name": "business_id",
    "value": null
  },
  "features": [
    {
      "name": "feature_1",
      "value": null,
      "feature_importance": null
    },
    {
      "name": "feature_2",
      "value": null,
      "feature_importance": null
    }
  ],
  "predictions": [
    {
      "name": "probability_N",
      "value": null,
    },
    {
      "name": "probability_Y",
      "value": null,
    }
  ]
}
```

```
],  
  "ml_model_id": 42,  
  "message": "Business id not found",  
  "created_on": null  
},  
]
```

- **Error Codes**

Lists possible error codes returned by the API and their meanings.

Code	Message	Description
200	Success	Response would include a JSON with the requested prediction values for the respective ID
400	Invalid input	Project and/or model do not exist
401	Issue with Authentication and displays one of the errors	Missing authentication credentials, Unauthorized access, or Invalid API token
403	ML Inference Service is not enabled for your account	The ML Inference Service is not enabled for your account; contact support to enable access
422	Invalid or issues with payload	The request payload is invalid or contains issues such as missing required fields or incorrect data types
500	Unexpected error	An unexpected server error occurred while processing the request

Change Credit Score

The Change Credit Score API provides a credit score for a specified group or entity, along with the associated group name. This score is computed using historical data and contextual analysis, with which you can evaluate the reliability or risk profile of the group. The API takes dataset names as input and returns the credit score along with relevant metadata.

- **REST API Endpoint and Details**

Details the endpoint URLs, HTTP methods, and structure for accessing the API services.

- Endpoint: `https://api.us.digital.ai/analytics/query/dataset/{dataset_name}?column_name=<column_name>&values=<value>` or `https://api.eu.digital.ai/analytics/query/dataset/{dataset_name}?column_name=<column_name>&values=<value>`
- Details:
 - Digital.ai Platform URL: `https://api.us.digital.ai` or `https://api.eu.digital.ai`
 - API Path: `/analytics/query/dataset/{dataset_name}`
 - Method: `GET`

Parameters

Describes the required parameters that must be included in the API endpoint path.

- Path Parameter:** Located within the endpoint’s path, before the '?' symbol. It is used to specify or access a particular resource directly.
 - `dataset_name`: The name of the dataset to query. This is used to identify the source of the data. For example, `CHANGE_CREDIT_SCORE`.
- Query Parameters:** Located after the '?' symbol in the endpoint URL. It is used to filter, sort, or modify the response data.
 - `column_name`: The column in the dataset to filter on. For example, `BUSINESS_ID`.
 - `values`: The value(s) to filter the specified column. For example, `CHG12345`.

Response

Explains the structure and fields included in the API response.

Field	Description
<code>chg_id</code>	The unique identifier for the change
<code>chg_name</code>	The name of the change or group
<code>credit_score</code>	The calculated credit score for the change or group

For example:

```
{
  "columns": ["chg_id", "chg_name","credit_score"],
  "result": [
    ["CHG12345", "chg1_name", 12.234],
    ["CHG12346", "chg2_name", 23.456]
  ]
}
```

• **Error Codes**

Lists possible error codes returned by the API and their meanings.

Code	Message	Description
200	Success	The request was successful, and the response contains the requested data
400	Invalid input	The input provided in the request is invalid or does not meet the criteria
404	No data found	The requested data could not be found in the dataset
422	Validation Error	The input payload failed validation checks
500	Error fetching data	An unexpected error occurred while processing the request

Dashboards

7 items

Dataset

10 items

Code Standardization

3 items

Application Properties

1 item

Metadata Viewer

1 item

Glossary

A comprehensive list of terms and definitions to understand key concepts and terminology used in the Digital.ai Plat...

Copyright

Information about the copyright, ownership, and usage rights related to the Digital.ai Platform.

 What is a Dashboard?

Brief knowledge about dashboard components

 Accessing Dashboards

Explore how to access dashboards.

 Recommendations for Custom Dashboards

This document provides recommendations for creating and using custom dashboards effectively.

 Viewing Dashboard Details

Learn how to view dashboards.

 Filtering Dashboards

Learn how to filter dashboards.

 Security Implementation in Dashboards

Learn how to implement row-level security in analytics dashboards using security datasets.

Creating a Dashboard

33 items

What is a Dashboard?

A dashboard is a visual representation of data that presents the data in a summarized format, making it easier to monitor trends and track performance at a glance. It provides a quick overview of KPIs, metrics, and other relevant information to help you make informed decisions.

Out-of-the-box dashboard

An out-of-the-box dashboard is a pre-built or ready-to-use dashboard that comes with your product. These dashboards provide you with immediate access to key metrics, visualizations, and insights without requiring extensive customization. These dashboards are typically built using best practices and industry standards, incorporating commonly used metrics and visualizations.

Custom dashboard

You can copy an out-of-the-box dashboard and customize it based on your requirements and preferences. It offers flexibility and customization, allowing you to choose the metrics, visualizations, and layouts that best suit your needs.

Dashboard components

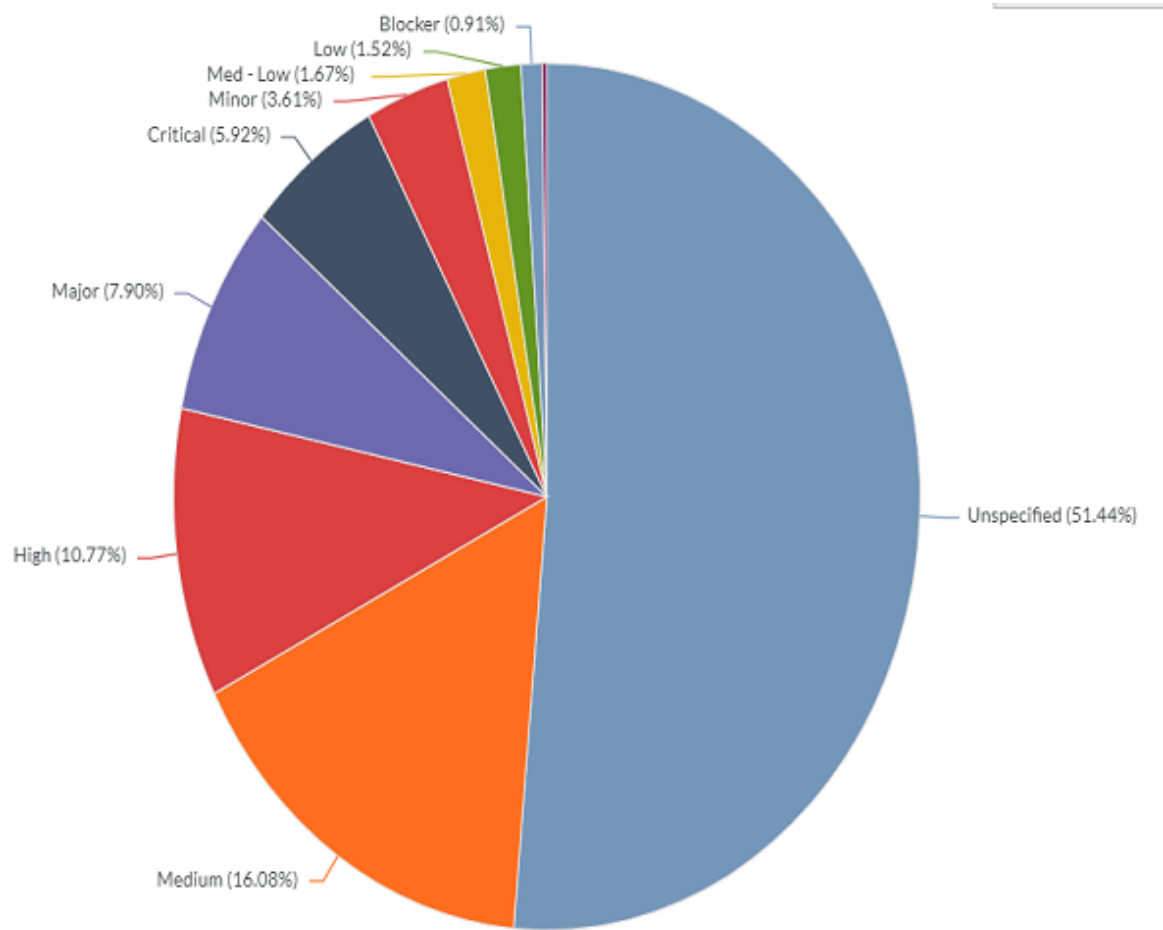
A dashboard has the following key components and sections:

- **KPIs:** Displays important metrics that represent the performance of the system or the process. Here is an example KPI.

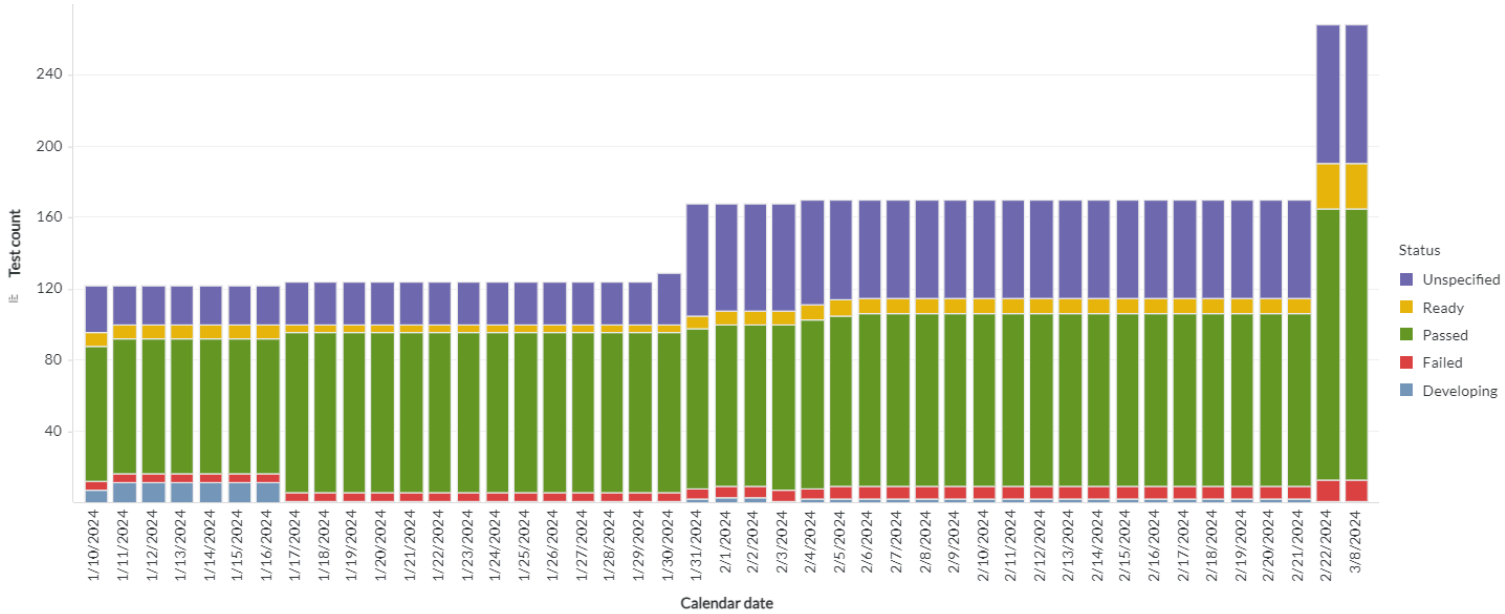


- **Panel:** It refers to a container or a section within the dashboard layout where visualizations, widgets, or other dashboard elements are placed. You can use the panel to visualize various aspects of your data, such as KPIs, trends, comparisons, or detailed reports. You can use the panel as a chart or grid. The chart is a graphical representation of data that conveys trends, patterns, and insights. The chart types are bar, line, pie, scatter plot, and heatmap. Grid is a tabular representation of data, organized

in rows and columns. Here is an example panel.



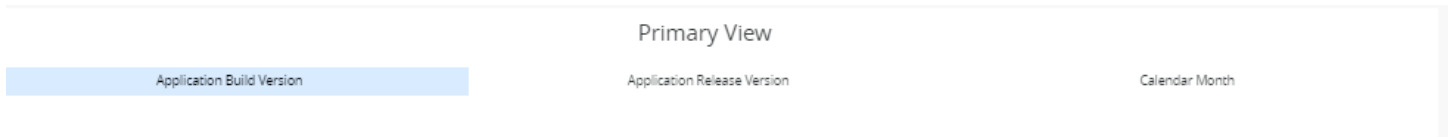
Here is an example chart.



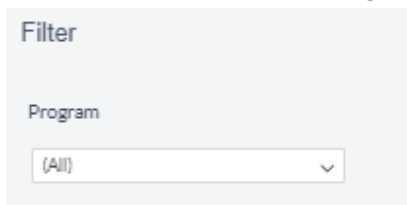
Here is an example grid.

All backlog items - Days in cycle				
Portfolio item	Avg cycle time days	Maximum	Minimum	Backlog item count
E-13728	0.0	0.0	0.0	1
E-15384	0.0	0.0	0.0	1
E-15604	0.0	0.0	0.0	1
E-15382	1.0	1.0	1.0	1
E-14833	2.0	2.0	2.0	1

- **Tab:** It refers to a navigational element that allows you to switch between different sections or views within the dashboard. You can use tabs to view multiple sets of related content or analyses in a single dashboard. Here is an example tab.

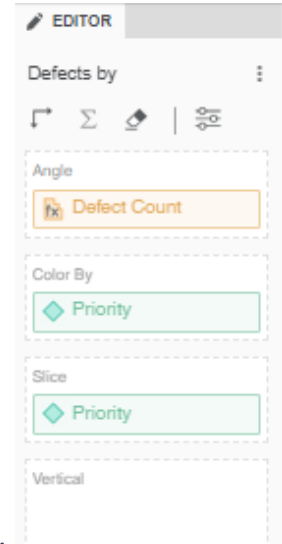


- **Filter:** Filters in a dashboard serve as a tool to selectively control the data presented in visualizations and other dashboard elements. You can refine your analysis by setting specific criteria or conditions that the data must meet. Each filter allows you to focus on different aspects of the data, enabling comparisons across panels based on various parameters. Additionally, cascading filters enhance usability by dynamically adjusting the filter values based on the selection made in a dashboard. For example, selecting a value in one filter triggers other filters to display related values, facilitating a more streamlined and targeted analysis process. Here is an example filter.



- **Chapter:** Chapters provide a hierarchical structure for organizing the content of the dashboard. They help break down large amounts of information into smaller, more manageable sections. Each chapter typically focuses on a specific topic, analysis, or set of data. This segmentation allows users to navigate directly to the sections that are most relevant to their interests or needs.
- **Dataset:** It refers to a collection of data organized and stored together. Data stored in a structured format in the form of a table related to a specific domain or business process is a dataset. Each dataset contains rows and columns of data, where each row represents a record, and each column represents a data attribute or field.
- **Attribute:** It refers to a characteristic or property of an entity or object. Attributes provide descriptive information about the entity and are stored in database tables or datasets as columns.
- **Metric:** It refers to a quantitative measure or indicator used to assess, analyze, and track the performance or behavior of a business process, system, or activity. Metric helps you measure various

aspects of your organization's operations. You can make informed decisions and evaluate success in



achieving specific objectives. Here is an example attribute and metric.

You can perform other tasks like exporting and duplicating in a dashboard.

Exporting a dashboard

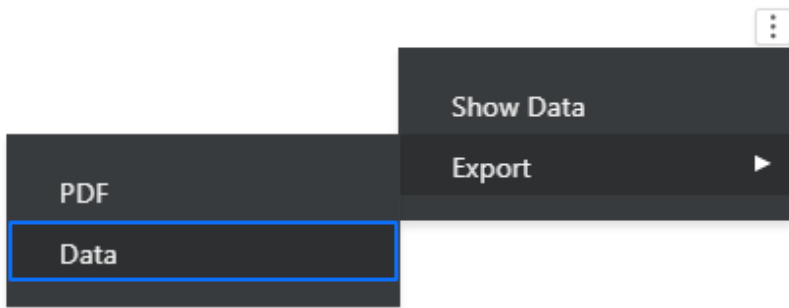
Exporting a dashboard allows you to view the dashboard outside your product. For example, you can view the dashboard results in a PDF file within Adobe Reader for viewing or printing. You can export a dashboard to the following formats:

- PDF file
- Excel spreadsheet
- Email

You can use the exported dashboard for the following purposes:

- **Further analysis:** Exported data enables advanced analysis using tools like Excel, R, or Python for tasks like statistical analysis, predictive modeling, or data mining.
- **Reporting:** Exported data allows for customized reports to meet stakeholder needs, with formatting and insights tailored accordingly.
- **Data sharing:** Exported data facilitates collaboration and decision-making by enabling sharing with stakeholders who lack dashboard access or prefer offline work.

You can export a dashboard by selecting a grid or panel visualization and then clicking **Export** from the three-dot menu.



Duplicating a dashboard

You can create a new dashboard by duplicating an existing dashboard and then modifying it. Duplicating a dashboard allows you to quickly and easily create a new version of an existing dashboard without having to recreate it from scratch. You can use the duplicated dashboard for the following purposes:

- **Backup and versioning:** Duplicating data serves as a backup for protection against loss or corruption and enables versioning for comparison and experimentation.
- **Data manipulation:** Duplicating data allows experimentation with various manipulations without altering the original dataset, facilitating analysis before permanent modifications.

Previewing data

The Show Data dialog box in a dashboard enables you view the underlying attribute and metric data of a visualization in an easy-to-read grid format. You can can preview data by selecting a grid or panel visualization and then clicking **Show Data** from the three-dot menu. Here is an example preview data.

Show Data

13 Rows



Add Data



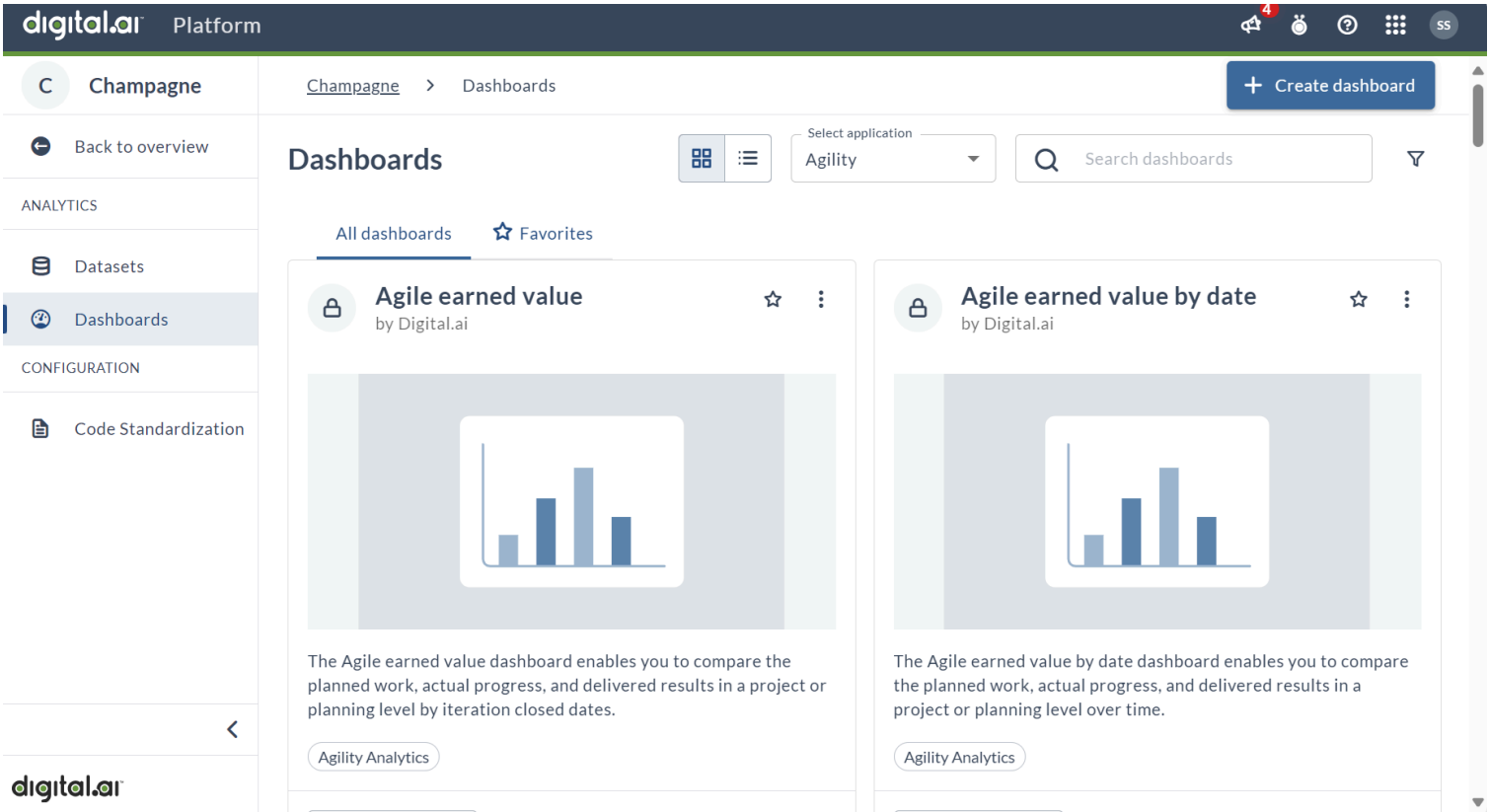
Version	DEVICE_MODEL	DEVICE_OS	Name	Duration (S)
1.2499	Unspecified	Unspecified	<Experibank-Payment>	
1.2499	Unspecified	Unspecified	Experibank-Login	
1.2499	Unspecified	Unspecified	Experibank-Login-Demo	
1.2499	Unspecified	Unspecified	Experibank-Payment	
1.2499	Unspecified	Unspecified	Experibank-Payment-Demo	
1.2468	Unspecified	Unspecified	Experibank-Login-Demo	
1.2468	Unspecified	Unspecified	Experibank-Payment-Demo	
1.3010	SM-T870	Android	build 3051	
1.3010	SM-T870	Android	build 3210	
1.3010	Unspecified	Unspecified	Experibank-Login-Demo	
1.3010	Unspecified	Unspecified	Experibank-Payment-Demo	

Close

Accessing Dashboards

Dashboards can be accessed in two ways:

You can access dashboards from the Platform itself.



You can also access dashboards that are embedded in the individual Digital.ai products, such as Agility or Release. Click **Digital.ai Analytics** option in the hamburger menu.

For example, in Agility:

Depending on whether or not you have configured SSO integration, users may encounter a login screen when viewing a dashboard from the product.

Users with the `account-user` role can only view dashboards, while users with the `account-analytics-author` role can edit and create dashboards.

Recommendations for Custom Dashboards

This guide provides recommendations for creating and using custom dashboards. It includes basic instructions to help you customize and manage dashboard components effectively.

The following are the recommendations:

Maximum number of datasets that can be blended in a dashboard: Digital.ai recommends using maximum six datasets in a dashboard. Dashboard performance depends on several factors including the size of the datasets, the number of objects, rows, and cache size. As the number of datasets increases, performance may deteriorate because the server creates a virtual dataset by joining all datasets included in the dashboard. Therefore, the more datasets you add, the longer it may take for the dashboard to execute.

NOTE

All the datasets being used are linked and form a virtual dataset for the faster analysis of the dashboard.

Maximum number of chapters and pages allowed in a dashboard: It is recommended for each dashboard to have a maximum of 2 chapters and no more than 5 pages in total across all chapters.

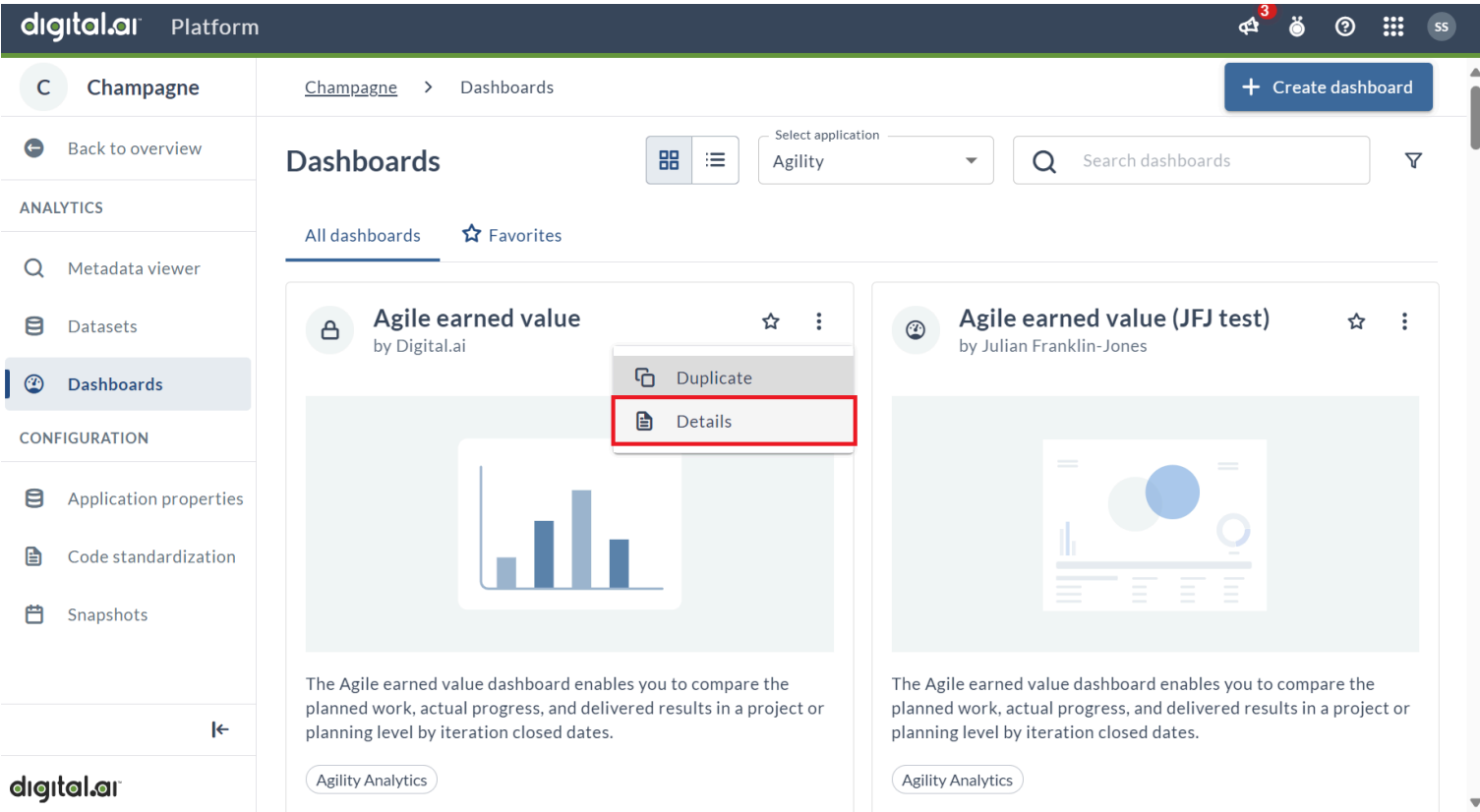
Basic instructions for creating a derived metric: Derived metrics and derived attributes are calculated dynamically during dashboard execution. The calculation time can vary based on the size and complexity of the data, and may occasionally take several seconds. To ensure optimal performance, create derived metrics according to clear business definitions and regularly remove any unused derived metrics or attributes.

Maximum number of derived metrics that can be created in a dashboard: Consider creating derived metrics based on business definition requirements and routinely removing any unnecessary objects. The suggested maximum number of derived metrics per dashboard is 50.

By following these recommendations, you can create and maintain custom dashboard efficiently. Regularly reviewing and optimizing your dashboard components will help ensure good performance and allow your dashboards to adapt to changing business requirements.

Viewing Dashboard Details

The **Details** feature provides a convenient drawer that allows you to access comprehensive information about the dashboard.



Within **Details**, you can view a detailed description of the dashboard, mark it as a favorite or remove it from your favorites, and see a list of all pages contained within the dashboard. Additionally, it displays the current status of the dashboard, along with metadata such as the creation date, the last modified date, and the user who made the most recent modifications.

digital.aiPlatform

3

SS

CChampagne

Champagne

>

Dashboards

Back to overview

Agility

Dashboards

All dashboards

☆ Favorites

Agile earned value

by Digital.ai

The Agile earned value dashboard enables you to compare the planned work, actual progress, and delivered results in a project or planning level by iteration closed dates.

Agility Analytics

Open dashboard

Published

Agile earned value

by Julian Fra

The Agile earned value dashboard enables you to compare the planned work, actual progress, and delivered results in a project or planning level by iteration closed dates.

Agility Analytics

Open dashboard

Published

Agile earned value (JFJ2)

Agile earned value

Details

Description

The Agile earned value dashboard enables you to compare the planned work, actual progress, and delivered results in a project or planning level by iteration closed dates.

Created by

Chandrasekhar Jandhyam

Status

Published

Category

Agility Analytics

DASHBOARD PAGE SUMMARY

Pages

1

ADDITIONAL DETAILS

Created on

Apr 4, 2024 - 07:20 PM

Modified on

Aug 7, 2024 - 05:47 PM

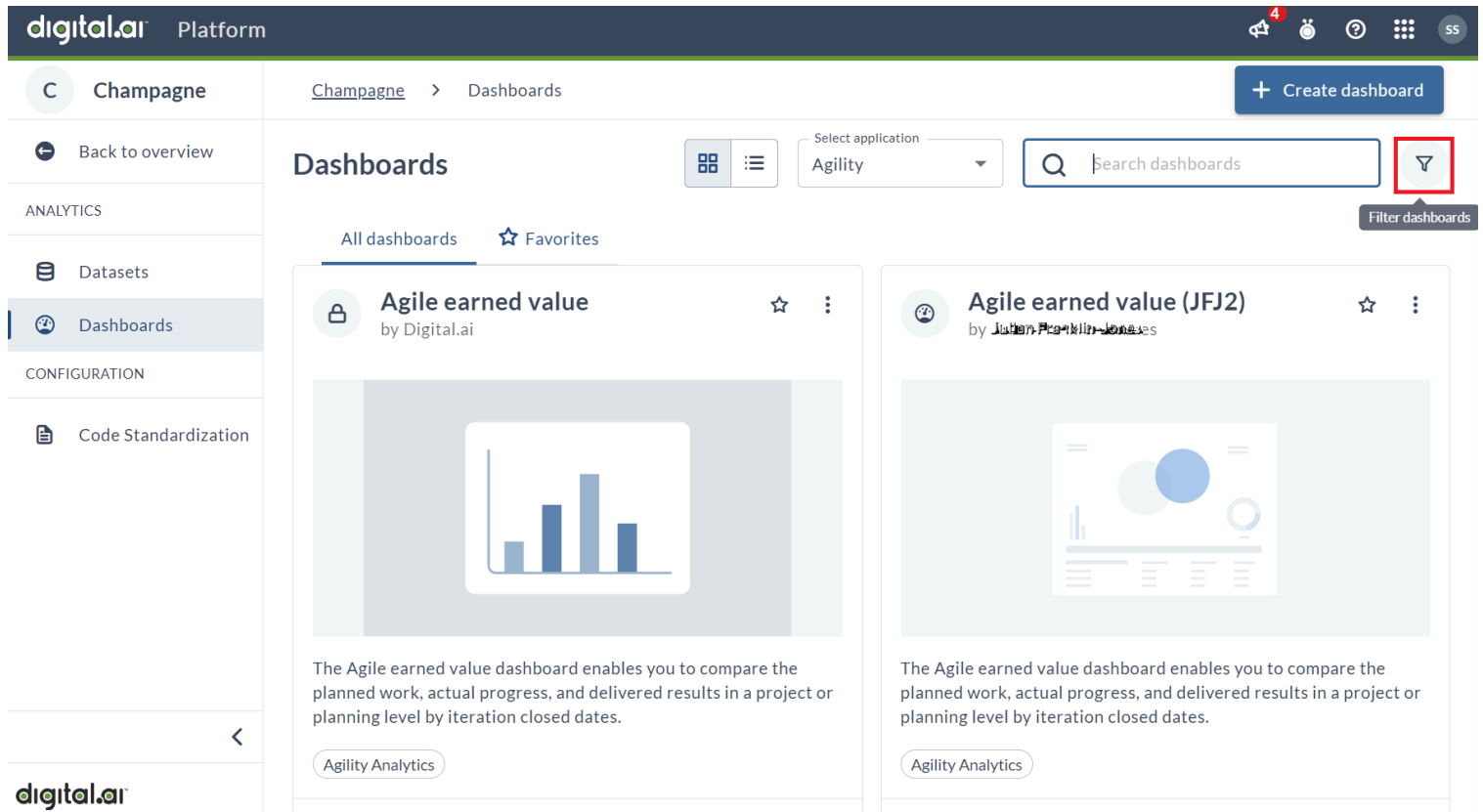
Modified by

service-account-analytics-provisioner-client

C

Filtering Dashboards

Dashboard filters are applied globally across all panels or widgets featured on a dashboard.



Filter By Author

Filtering dashboards by Author allows users to sort through content based on who customized it. When the dashboard heading includes **Digital.ai**, it signifies pre-configured offerings provided to customers out of the box. However, in cases of customization, the name of the individual who customized it will be displayed while sorting.

Filter By Category

Filtering dashboards by category helps to tailor insights to specific stakeholders. This is simply a way for grouping dashboards into sets and each set represents the most common use cases of a particular user persona - like Scrum Master, Release Manager etc.

Filter By State

In the dashboard system, there exist two primary states: **Draft** and **Published**. By default, upon creation, all dashboards are designated as **Draft**. The **Draft** state indicates that work is currently in progress on the dashboard, with ongoing edits, additions, or adjustments being made.

The **Published** state signifies that the dashboard has been finalized and made ready for consumption by users. Until a dashboard is published, it remains inaccessible to users, ensuring that only completed and verified dashboards are made available for viewing. This distinction between **Draft** and **Published** states serves to streamline the dashboard development process, allowing for thorough review and refinement before sharing it with users.

Security Implementation in Dashboards

In analytics dashboards, applying security ensures users only access data they are authorized to view. However, enabling security for all datasets and dashboards can affect overall performance. To improve performance, security is removed from most datasets and dashboards. Applying security across all dashboards and datasets can negatively affect performance.

This topic explains the steps to implement security for dashboards where it is required. When duplicating or creating a custom dashboard, you can apply row-level security by using the appropriate security datasets.

When to Apply Security

- Apply security only to dashboards that require restricted access to sensitive data.
- Use security datasets to enforce row-level security for specific asset types or business needs.

How to Implement Security

To implement row-level security in your dashboards:

1. Identify which datasets in your dashboard require security.
2. Add the relevant security dataset(s) to your dashboard.
3. Blend or join the security dataset with your target dataset using the appropriate attributes.
4. Add the security flag as a global filter and set its value to 'Y'.
5. Test your dashboard to ensure users see only the data they are authorized to access.

Security Datasets

Use the following topics for detailed, step-by-step instructions and example use cases:

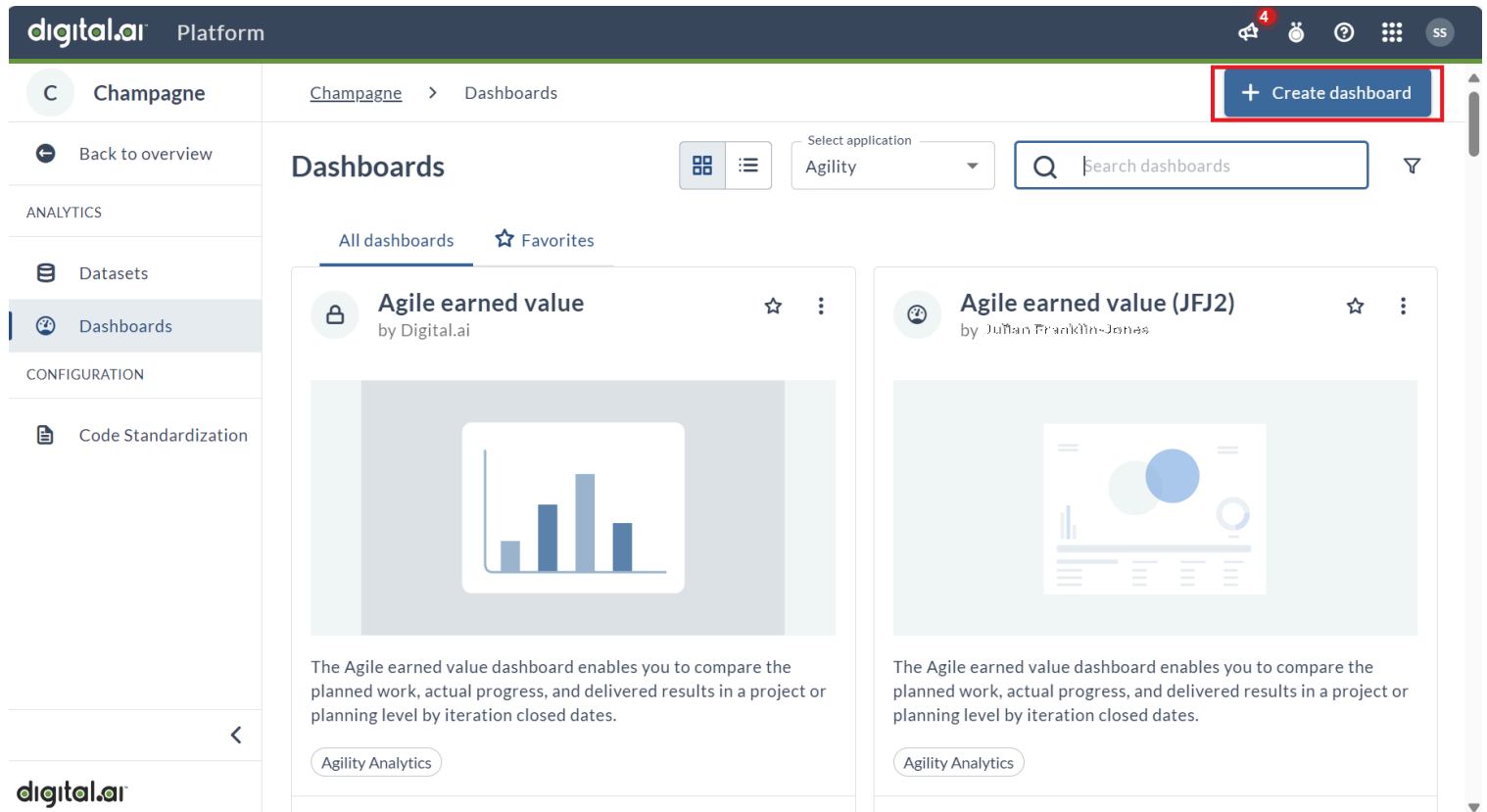
- [Agility security dataset](#)

- [CT security dataset](#)
- [Release security dataset](#)
- [Deploy security dataset](#)
- [TeamForge security dataset](#)

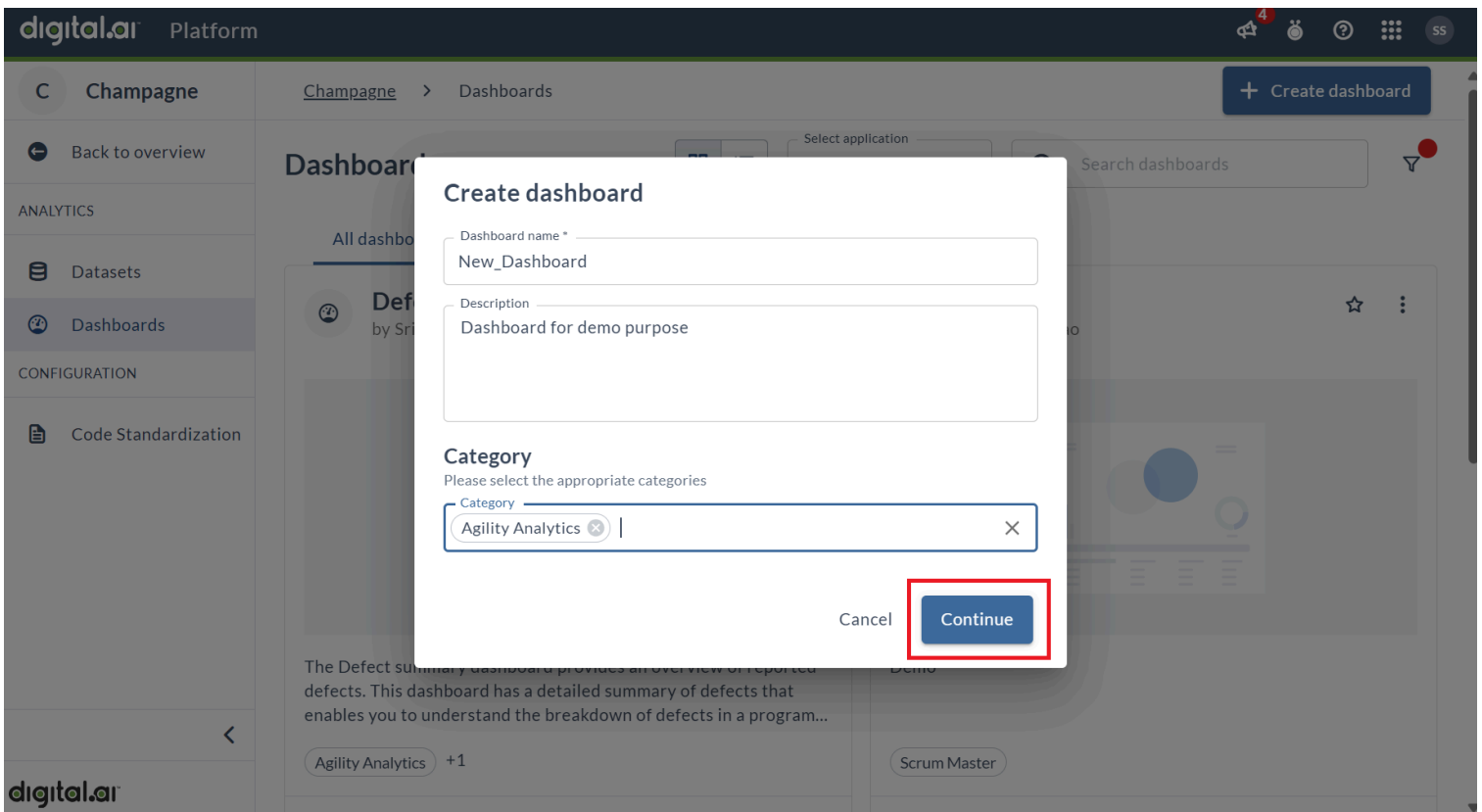
Refer to these topics whenever you apply security to duplicated or custom dashboards. Each topic provides guidance tailored to the specific dataset and includes example scenarios to help you implement security effectively.

Creating Dashboards

Click **Create Dashboard** to create a new customized dashboard.

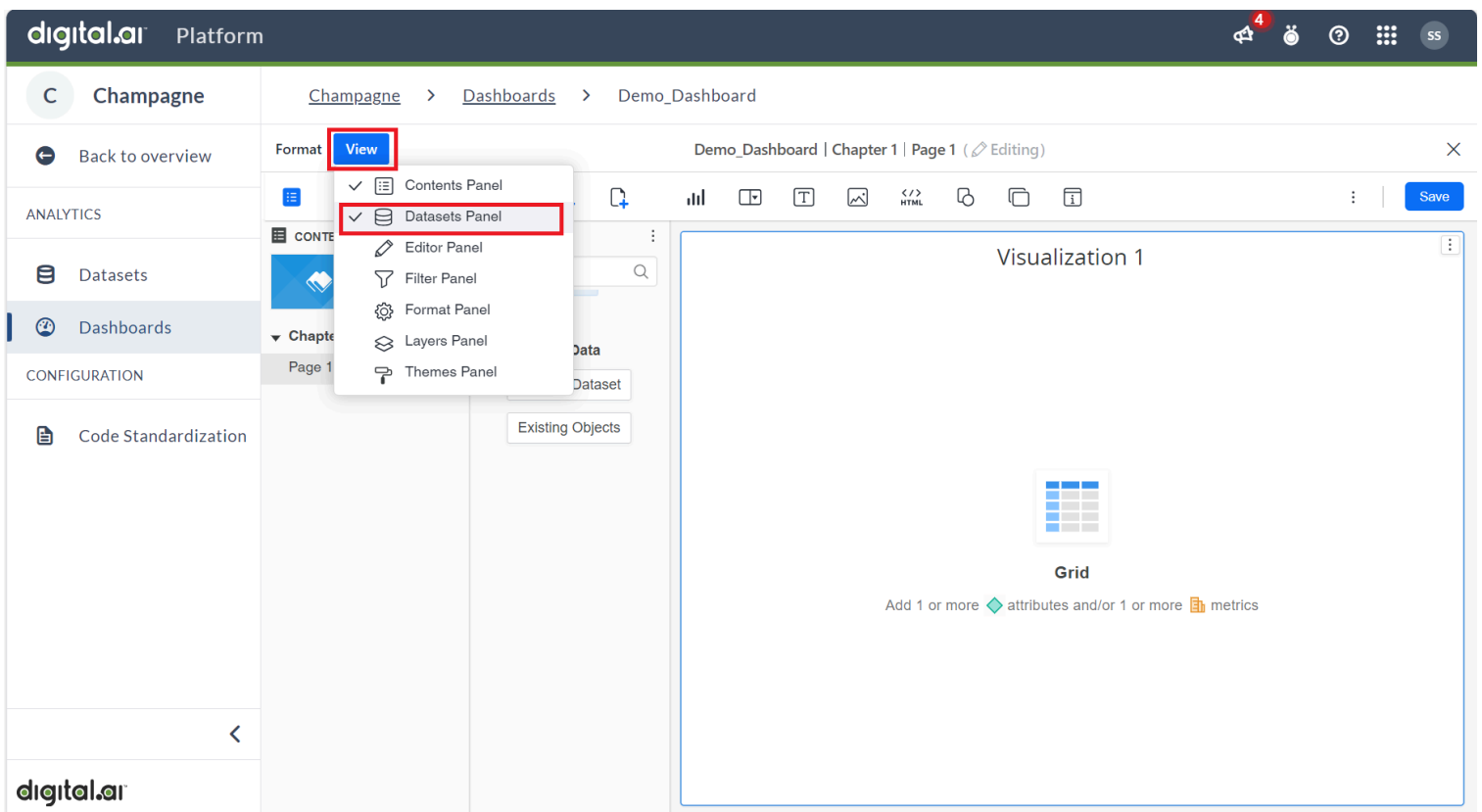


In the dashboard creation process, it is mandatory to provide a **Dashboard name**, as it serves as a unique identifier for the dashboard. However, filling in the **Description** and **Category** fields is optional, allowing users the flexibility to provide additional context and categorization if desired. Once the required **Dashboard name** field is populated, Click **Continue**.

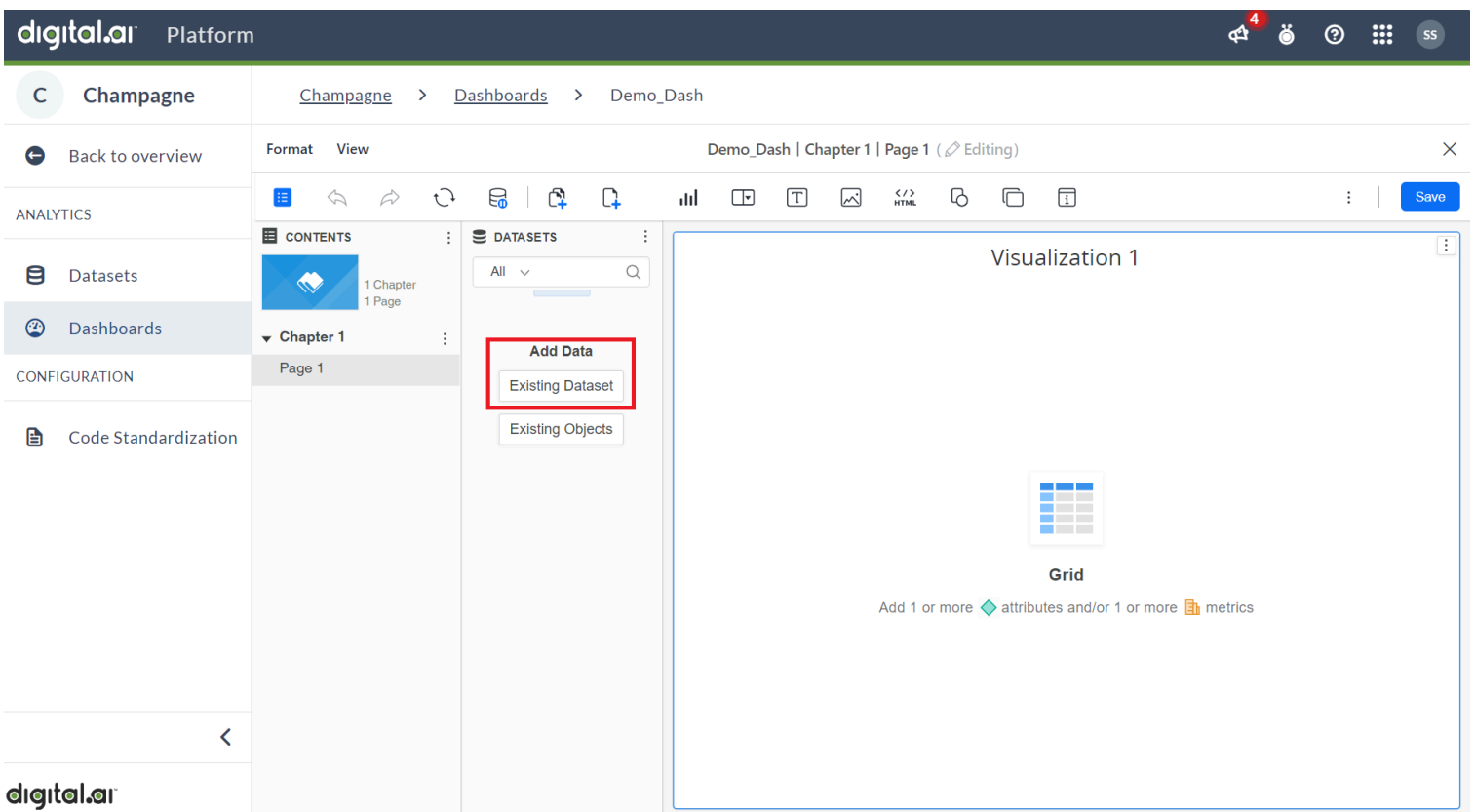


For each dashboard to function effectively, it requires a reliable source of data. In the context of Digital.ai Analytics, datasets serve as the foundational structures for organizing and presenting this data. Digital.ai has a diverse array of datasets to support various use cases, ensuring that users have access to relevant and structured information. Additionally, depending on your licensing agreement with us, you may be granted the ability to create and customize your own datasets, tailored to meet your specific needs. Click **View** and then select the **Datasets Panel** to create a dashboard using datasets.

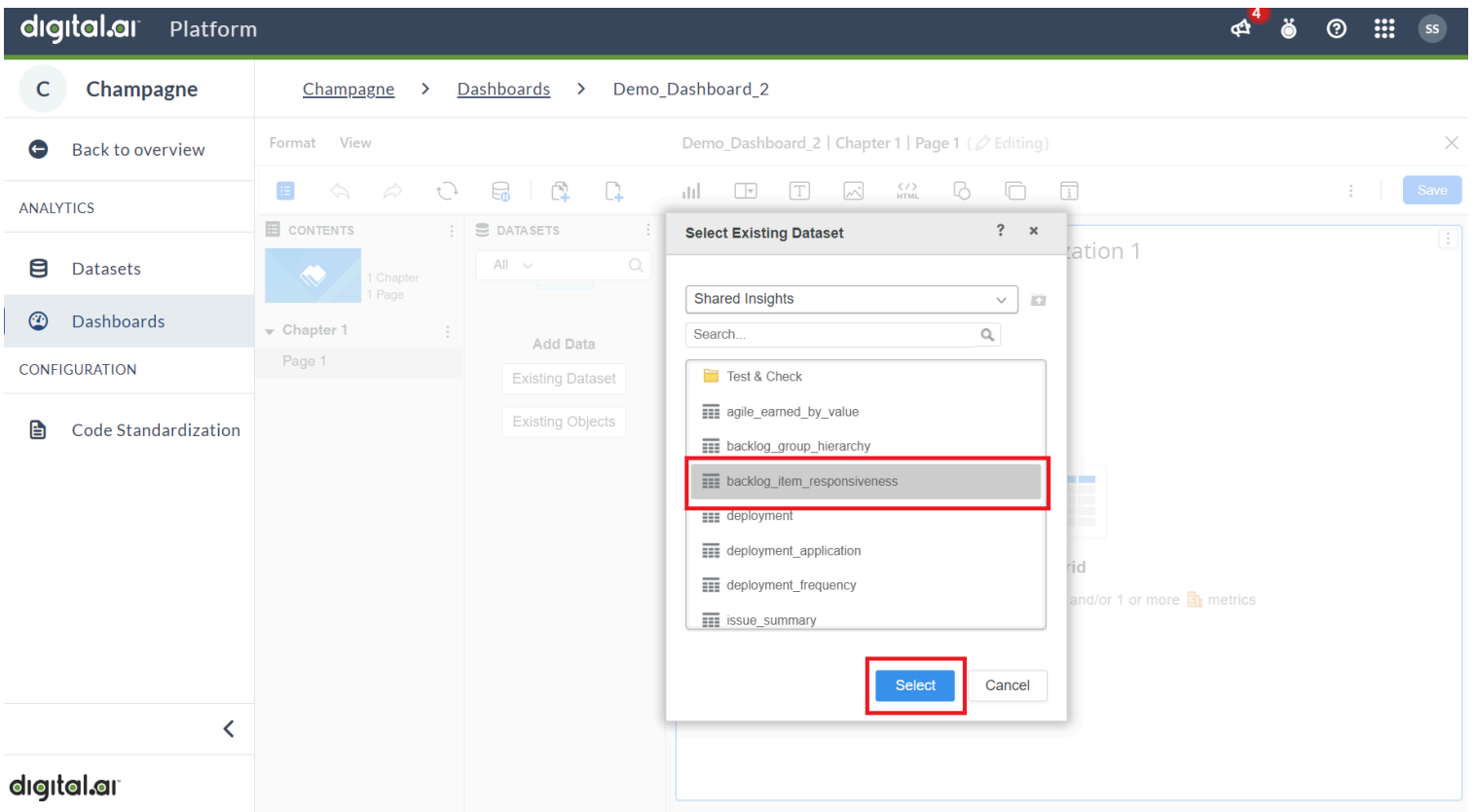
For more information about datasets, see [Managing Datasets](#).



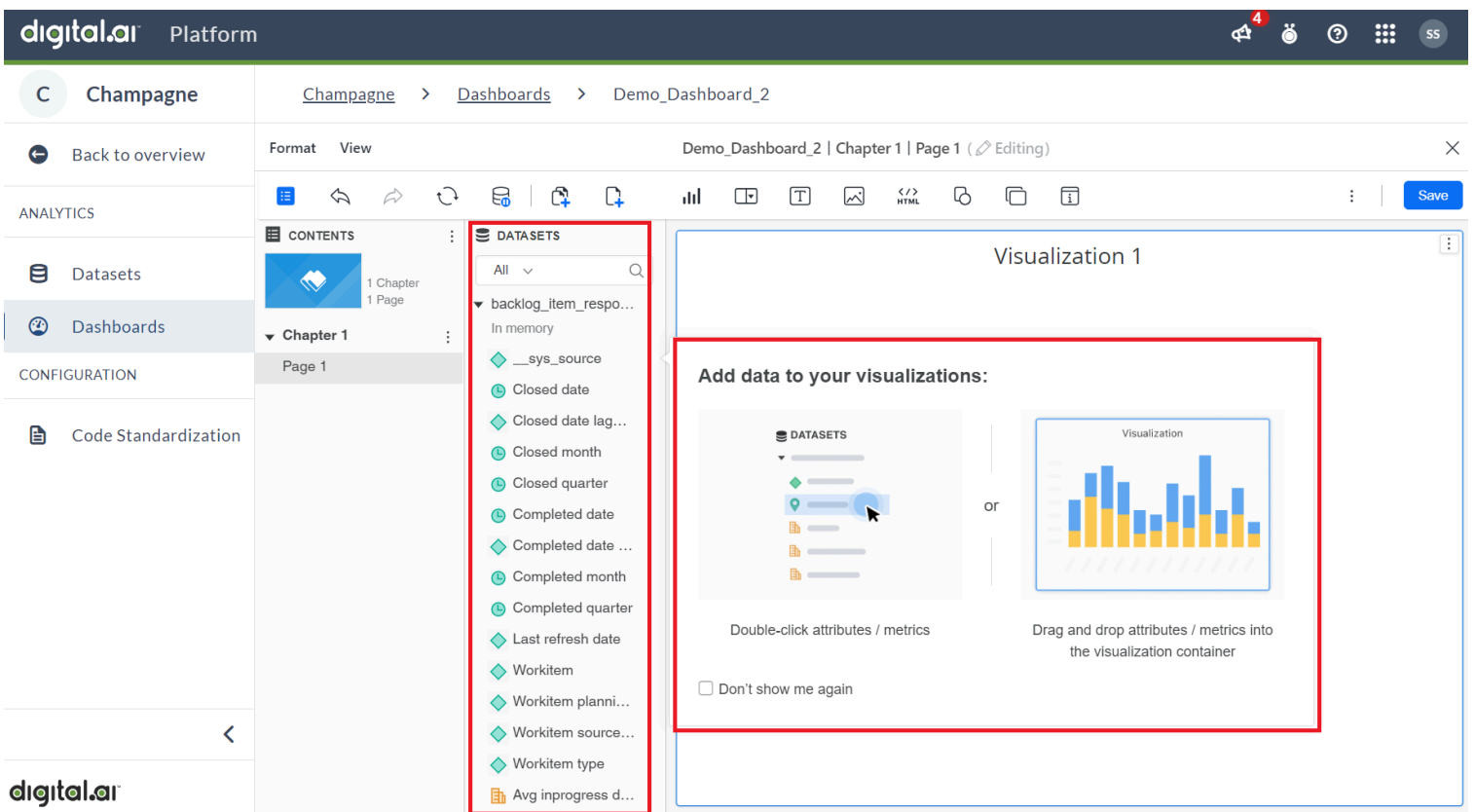
Click **Existing Dataset** to create a dashboard.



To proceed further, click on the required dataset from the list of available datasets and then click **Select** option.



Double-click on the required attributes to select them.



You can see the selected attributes appear on the **Visualization** screen. After confirming your choices click **Save** to create the dashboard.

digital.ai Platform

Champagne > Dashboards > Demo_Dashboard_2

Format View Demo_Dashboard_2 | Chapter 1 | Page 1 (Editing)

Save

CONTENTS

1 Chapter
1 Page

Chapter 1

Page 1

DATASETS

All

backlog_item_r...
In memory

__sys_source
Closed date
Closed date lag...
Closed month
Closed quarter
Completed date
Completed date ...
Completed month
Completed quarter
Last refresh date
Workitem
Workitem planni...
Workitem source...
Workitem type
Avg inprogress d...

Visualization 1

Closed date lagging count of months	Closed month	Completed date lagging count of months	Last refresh date
0	May 2024	0	May 16, 2024 - 04:32 AM
		1	May 16, 2024 - 04:32 AM
			May 16, 2024 - 04:32 AM
1	Apr 2024	1	May 16, 2024 - 04:32 AM
			May 16, 2024 - 04:32 AM
		0	May 16, 2024 - 04:32 AM
		1	May 16, 2024 - 04:32 AM

The created dashboard appears in the list of dashboards in the **Draft** state. Work-in-progress dashboards are saved as **Draft**, accessible only to users with the role of **Author** or above. Once the author determines that the **Draft** version is ready for end-user consumption, they must click **Publish**. Publishing the dashboard makes it available for regular users to view in both the platform and the source application.

digital.ai Platform

Champagne

Open dashboard Published Open dashboard Published

Demo by harish R...

Demo_Dashboard by saprasad shetty

Edit
Publish
Duplicate

Demo

Scrum Master

Open dashboard Draft

Demo_Dashboard_1 by saprasad shetty

Demo_Dashboard_2 by saprasad shetty

Draft

Editing Dashboards

When a dashboard is created and published, it enters the Published state [Creating and Publishing a Dashboard](#). When a user makes an edit to a **Published** dashboard, that dashboard is locked for that user and put into an **Edit-in-progress** state so that no other users can edit the dashboard. The dashboard will remain in an **Edit-in-progress** state until the user publishes or reverts their changes.

Any other user viewing the **Edit-in-progress** dashboard will see the original **Published** dashboard without any of the **in-progress** changes. The user will also see a **Locked** icon next to the status pill, indicating that this dashboard cannot be edited. Hovering over this icon will display the name of the user currently editing the dashboard, ensuring transparency in editing access.

NOTE

The users who can edit a **Custom, Published** dashboard are those users with any of these roles: account-admin, account-analytics-author, account-application-admin.

In general, users with any of these roles can edit (or create or delete) any custom (non-Out Of the Box) dashboard that they can see in the Grid/Table views, whether they are in Draft or Published mode. Users with just account-user role can only view existing dashboards.

Editing and Saving Changes

If a user initiates editing by selecting **Edit** or **Edit properties** for a Published dashboard, the dashboard transitions into the **Edit-in-progress** state and is locked to the current user. While in the **Edit-in-progress** state, any modifications made are only visible to the current user. These changes do not affect the published version until the current user publishes their changes.

Any other users viewing this dashboard will see the status as **Published** with a lock icon, indicating that the dashboard is temporarily locked for editing by another user.

NOTE

Navigating to the **Edit** page for a **Published** dashboard will automatically put the dashboard in an **Edit-in-progress** state. When using the Edit properties modal, the dashboard will not actually go into the **Edit-in-progress** state until the edits are saved.

Publish the Modified Dashboard

Once finished with dashboard updates, the dashboard needs to be **Published** to commit the changes, and unlock the dashboard. Upon publishing, the dashboard returns to the **Published** state, making the updated version visible to all users and releasing the editing lock, thereby allowing others to initiate new edits.

Additionally, the editing user can use the **Revert** option to discard any **in-progress** changes. Reverting a dashboard discards all unsaved changes and restores the dashboard to its original **Published** state and status for everyone, removing the lock icon and effectively treating it as if no edits were ever started.

Unpublish a Dashboard

Users can unpublish a dashboard to temporarily hide it from other users without deleting it. To unpublish a dashboard, click the **Actions** icon (:) on any published dashboard (excluding out-of-the-box dashboards), and click **Unpublish**. Once unpublished, the dashboard is in Draft state and no longer visible to end users, and the **Publish** option becomes available again.

NOTE

Dashboards with in-progress changes cannot be unpublished. Additionally, out-of-the-box dashboards cannot be unpublished.

Adding an existing dataset

You can add existing datasets from your environment to a dashboard.

To add existing datasets

1. Create a blank dashboard or open an existing one.
2. To add a dataset from your cloud environment or local machine, click **View** and select **Datasets Panel** to view the panel.
3. Click **More**  **DATASETS**  at the top of the datasets panel and choose **Add Data > Existing Dataset**. The Select Existing dataset dialog opens.
4. Select the required Source System and navigate to the dataset you want to add to your dashboard.
5. Click **Select**. The new dataset appears in the Datasets panel.

Link Shared Data Across Multiple Datasets

When you are creating a dashboard, you can:

- Display data from multiple datasets in the same visualization.
- Use a visualization based on one dataset as a filter to update the data displayed in a visualization based on another dataset.
- Group data from one dataset based on an attribute that exists in another dataset.

To achieve any of these goals, you must link the attributes that are shared in common across multiple datasets.

Important: You have one dataset that contains Customer ID, Customer Name, and Profit data, and another dataset that contains Customer ID and Shipping Cost data. You can link the two Customer ID attributes, allowing you to display Customer Name, Profit, and Shipping Cost in one visualization, group Shipping Cost data by Customer Name, etc.

You can also manually link attributes when you are editing a dashboard. Manually linking attributes allows you to link attributes across multiple existing datasets. The attributes that you link to each other should uniquely identify each record, to ensure that the results are calculated accurately. In most cases, an ID attribute can be used to link attributes. The attributes that you link must be the same data type. You can link an attribute to attributes in one or more datasets.

An attribute that is linked across multiple datasets appears with a link icon  and appears as one attribute when added to a visualization.

You can choose to unlink attributes that are already linked, if the link is incorrect for your needs. Unlinked attributes with the same name are treated as two separate attributes when they appear in a visualization.

Link Data in a Dashboard

1. Open a dashboard that contains at least two datasets. You must have write access to the datasets you intend to link.

2. In the Datasets panel, right-click the attribute you want to link and choose **Link To Other Dataset**. The Link Attributes Dialog opens.

Note: Linked attributes appear with a Link icon  in the Datasets panel.

3. In the first drop-down list, select the attribute to which you are linking the current attribute. You can type the name of an attribute in the field to narrow the list of choices.
4. Click **Show Attribute Forms** to define the attribute forms on which to base the link.

Note: At least one of the attribute forms that you link must be the ID attribute form.
5. Select the attribute form to link from the first drop-down list.
6. Select the attribute form to link to from the third drop-down list.
7. To link additional pairs of attributes, click **Add a Link** and repeat the steps to define a link for each pair.
8. To delete a link, hover over it and click **Delete** ✕.
9. Click **OK**. The attributes appear with a Link icon  in the Datasets panel.

Unlink Data in a Dashboard

1. Open the dashboard you want to modify.

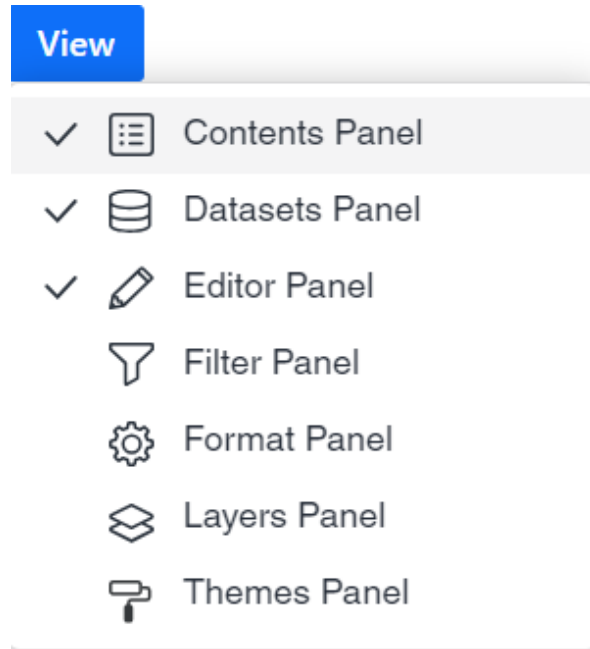
Note: Linked attributes appear with a Link icon  in the Datasets panel.

2. Right-click the attribute to unlink and select **Unlink**.

Viewing and hiding panels

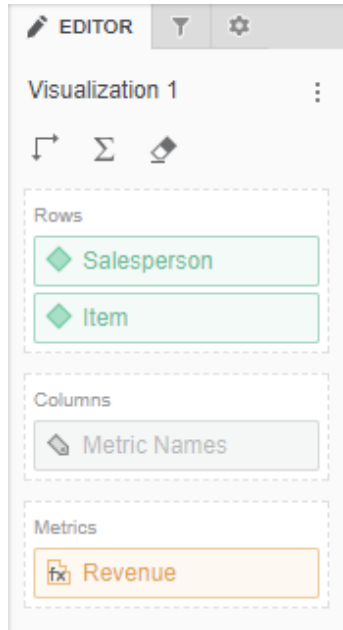
You can view and hide the panels used for editing, filtering, and formatting visualizations within a dashboard.

Click **View** in the title bar to show or hide the corresponding panels. The selected panel indicates the corresponding panel is open.



Editor Panel

The Editor panel contains a list of all the attributes and metrics that appear as data in the selected visualization. To view the dataset objects for a specific visualization, click the visualization in the dashboard.



Access

1. Open an existing dashboard that contains the visualization you want to edit.
2. Select the visualization in the dashboard.
3. Click **View** and then select **Editor Panel**.
4. To add data to your visualization, drag attributes or metrics from the Datasets panel to the Editor panel. A blue indicator line appears in the area to which you add the attribute or metric.

Format Panel

There are multiple formatting options for a visualizations. You can choose the font, background color, and borders for each part of the visualization, such as the column headers, row headers, values, container, and title. You can define the padding, column height, row height, whether to merge row and column headers, and so on.

1. Click on the grid visualization you want to format. If necessary, you can select a specific object in the visualization for formatting.
2. Right-click and choose Format. If you selected a specific object in the visualization, a pop-up menu displays the appropriate formatting options for that object. In addition, the Format panel automatically updates the first drop-down list with the area of the visualization you are formatting and the corresponding format options appear.
3. Select the appropriate options to format the visualization.
4. You can highlight data for an attribute or metric by applying formatting when the data fulfills a specific condition.
5. You can apply general formatting options used for all types of visualizations, such as renaming attributes or metrics, choosing whether to display a visualization's title bar, and so on.

Selecting which attribute forms to display in a visualization

You can choose which attribute forms appear for a specific attribute. An attribute is a business concept, such as Region or Income Bracket, that provides a label for the numerical data (that is, metrics) in your dashboard. An attribute form is a descriptive category for an attribute. While most attributes have only the forms ID and Description, an attribute such as Customer can have many other forms, such as First Name, Last Name, Address, Email Address, etc. See [Introduction to Attributes](#) for a more detailed description of attributes and attribute forms.

Selecting which attribute forms to display is helpful when you are working with attributes containing geographic information. You can select whether to display the latitude and longitude information for an attribute, when that information is stored in separate attribute forms.

You can also determine what attribute information appears in the attribute and attribute form headers in the visualization.

Note: You can choose to have a header containing the attribute form name automatically display above each attribute form shown in a grid, or have a single header display for each attribute in a grid, with each header containing only the attribute name.

To select which attribute forms to display in a visualization

1. Open a dashboard.
2. Click on the visualization in which you want to display attribute forms and select the required attributes.
3. In the Editor panel, right-click the attribute for which you want to display attribute forms and choose **Display Attribute Forms**.
4. To display an attribute form in the visualization, select the corresponding checkbox.
5. To hide an attribute form in the visualization, clear the corresponding checkbox.
6. To automatically display the attribute's name, select **Off** (default) from the **Display Attribute Form Names** drop-down list. No attribute form name appears for the attribute.

or

To automatically display the attribute's name, as well as the selected attribute form names, select **On** from the **Display Attribute Form Names** drop-down list.

or

If your visualization is a grid, you can automatically display a single header for each selected attribute form. Select **Form name only** from the **Display Attribute Form Names** drop-down list.

or

If your visualization is a grid, you can display a header for each attribute form and include the attribute name only in the header for the first attribute form for each attribute, select **Show attribute name once** from the **Display Attribute Form Names** drop-down list. The remaining attribute forms display with only the attribute form name.

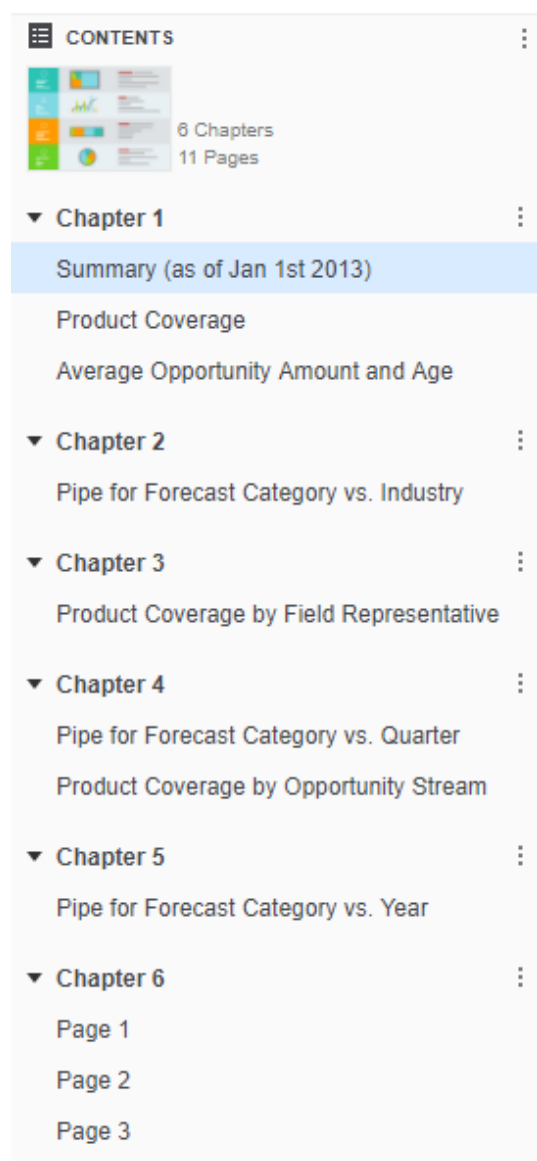
or

If your visualization is a grid, you can display either headers for each attribute or attribute form, depending on the number of attribute forms visible in the grid for each attribute, select **Automatic** from the **Display Attribute Form Names** drop-down list. If only one attribute form appears in the grid for an attribute, the attribute appears with a header containing the attribute's name. If more than one of the attribute's forms are visible in the grid, each attribute form appears with a header containing the attribute name, followed by the attribute form name.

7. Click **OK**.

Introduction to chapters and pages

Dashboards are organized into chapters and pages. Each chapter contains one or more pages. Each page can contain multiple visualizations and other dashboard objects such as text and images. Use the Contents panel to view the structure of chapters and pages within your dashboard, as well as navigate between them. Click on a page to open it. Click on a chapter to open the first page of that chapter.



The structure of chapters and pages allows a dashboard to be filtered in the following ways:

- Each chapter contains its own filters that are applied across all pages and visualizations within the chapter.

- A visualization can contain its own filters, in addition to the existing chapter filters.
- A visualization can be filtered by another visualization or filter.

Adding, renaming, copying, moving or deleting Pages

You can add, rename, copy, move, or delete pages in a dashboard.

To add a page

1. Open the dashboard you want to modify.
2. In the Contents panel, click **More**  next to the chapter you want to add a page to and choose **Insert Page**.

To rename, copy, move, or delete a page

1. In the Contents panel, right-click the page you want to modify.
2. Choose **Rename** to rename the page.
or
Choose **Duplicate Page** to copy the page.
or
Choose **Delete** to remove a page.
3. Drag a page to its new location to rearrange it within the list.

Adding, renaming, copying, moving, or deleting Chapters

You can add, rename, copy, move, or delete chapters in a dashboard.

To add a chapter

1. Open the dashboard you want to modify.
2. In the Contents panel, click **More**  next to an existing chapter and choose **Insert Chapter**.

To rename, copy, move, or delete a chapter

1. In the Contents panel, click **More**  next to the chapter you want to modify.
2. Choose **Rename** to rename the chapter.
3. Choose **Duplicate Chapter** to copy the chapter.
4. Choose **Delete** to remove the chapter.
5. Drag a chapter to its new location to rearrange it within the list.

Adding an image

You can add either a URL or an embedded image to the dashboard.

- Embedded images are portable and are available when the dashboard is opened offline. The dashboard will initially display with embedded images shown as placeholders, since the images are loaded last.
Images larger than 3 MB are compressed, unless they are a .gif file. If the compression does not result in a file smaller than 3 MB, the image cannot be embedded. Use a URL to specify the image's location instead.
Only one copy of each image is included in the dashboard file, even if the image is used on different chapters.
- Large images (over 10 MB or a gif file over 3 MB) should use a URL rather than embedding.

To add an image to your dashboard

1. In the dashboard, in the toolbar, click **Image** . A placeholder is automatically added to the dashboard and displayed in an image container.
2. To embed the image in the dashboard, click **Browse** in the image container. Navigate to and select the image and click **Open**.

You can also drag and drop an image file into the image container.

Note: Embedding images is recommended because it ensures that the image can be commonly accessed outside of Web.

or

To specify the image location using a URL, enter the URL of the image in the **Enter an image** URL field and click **OK**.

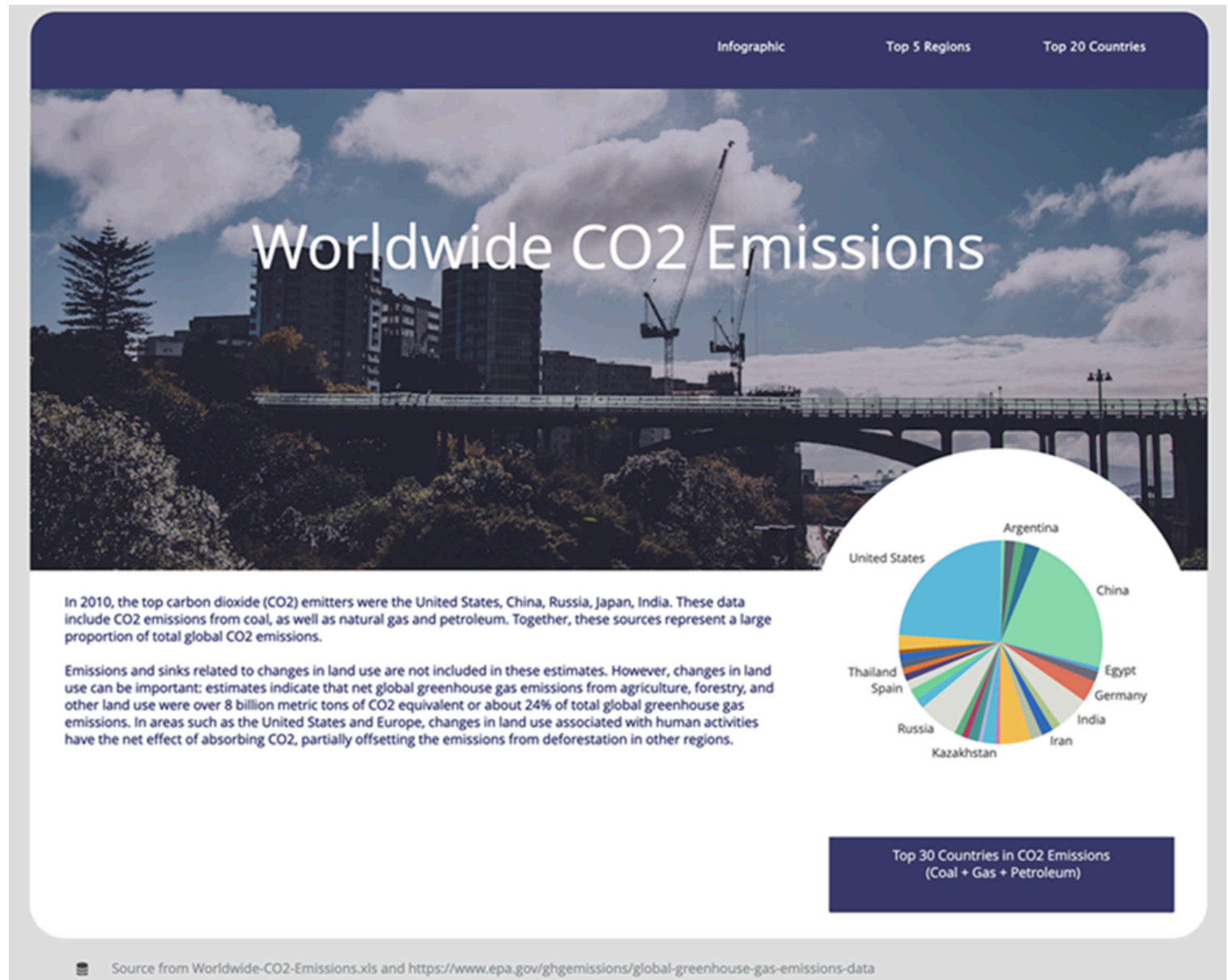
Note: Both absolute URLs (<https://www.example.com/etc/logo.jpg>) and relative paths (such as `/images/logo.jpg`) are supported, but relative paths are not recommended.

Relative paths point to locations that are relative to the application that they were originally created for.

3. To move the image, click and drag the image to its new location in the dashboard. An indicator line appears in the location where you can add the image. Release the mouse button to place the image in the new location.

Add Shapes

Use shapes in your dashboard to help frame a visualization, create a layered effect, or visually group elements together.



1. Open a new or existing dashboard.

2. In the top toolbar, click **Shape** .

3. Select a shape:

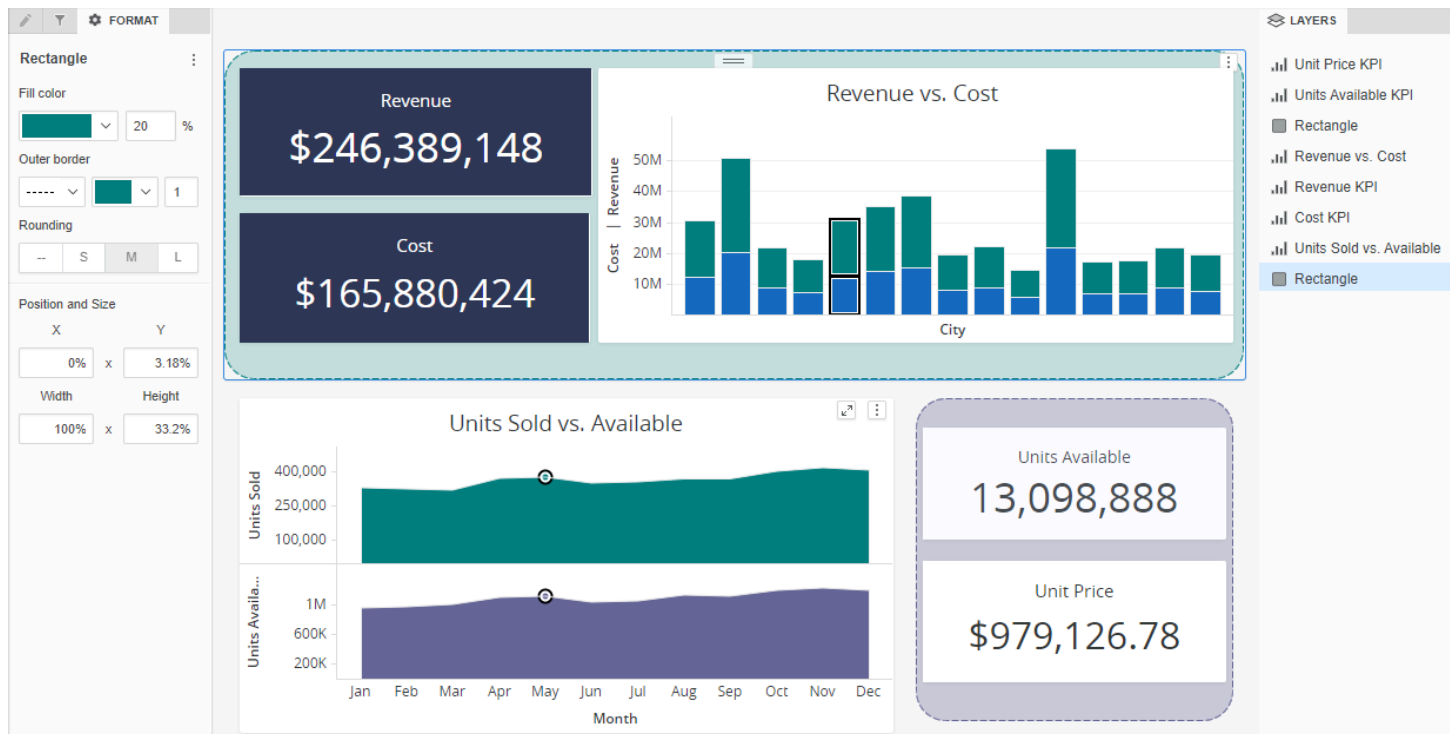
- Line

- Rectangle
- Ellipse
- Triangle
- Polygon

4. Click and drag where you want the shape to appear.

Info: If a shape overlaps another container, you can resize and reposition it by right-clicking on its layer and selecting **Hide on Default View** from the Layers panel.

5. Use the options in the Format panel to customize your shape.

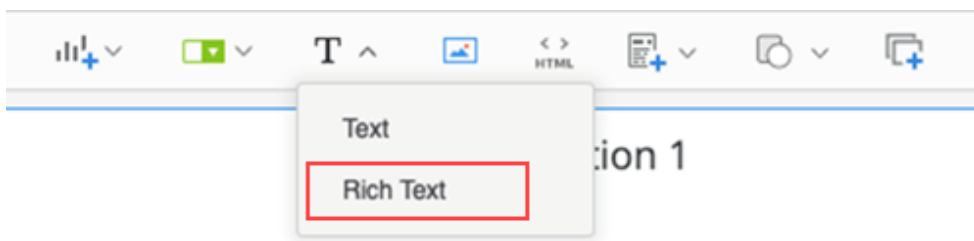


Add Rich Text

Unlike regular text fields, you can use rich text to apply rich formatting to the individual character level to create compelling infographic style dashboards.

Important: Autosizing stops at a six point font before a scroll bar is introduced. This is to prevent cases where a string of text ends up being shrunk to an unreadable size. To prevent the scroll bar from appearing, expand the container size to give the text more room.

1. In the top toolbar, choose **Text**  > **Rich Text**.



2. In the text box, type or paste your text.
3. Highlight your text and use the Format panel to modify your rich text.

FORMAT

Rich Text Title

Open Sans

B

I

U

U

10

Padding

Wrap text

Overflow:

Fill color

Outer border

Position and Size

X

Y

Width

Height

Color palette

35.89% x 0%

62.44% x 10.74%



Adding a text field

1. In the dashboard's toolbar, click Text **T**.

The text field is automatically added to the dashboard and your cursor placed in the field.

2. Add text in field by typing the text you want to display.
3. Click outside of the text field to save your text.

Editing, moving, or deleting a text field

1. To edit a text field, click the text field and enter the new text to display.

or

Click **More**  and choose **Edit** to highlight the current text. Type the new text to display.

2. To move a text field, drag it to a new location. A blue indicator line appears in the location where you can place the text field. Release the mouse button to place the text field in the new location.

3. To resize a text field, hover the cursor over its edge. Drag the edge to change the size of the text field.

4. To delete a text field, hover over it, click **More** , and choose **Delete**.

Introduction to Visualizations

A visualization is a visual representation of the data in a dashboard, such as a grid, line chart, or heat map. Visualizations provide a variety of ways for you to display and interact with the data in a dashboard. You can explore the relationships between data elements by creating a network visualization, or create visually striking graphs that summarize key business indicators in a clear, easy-to-understand format. Each visualization can include data from multiple datasets at once. Each panel or chapter in a dashboard can contain multiple visualizations.

You can add the following visualization to a dashboard:

- [Grid](#)
- [Heat Map](#)
- [Bar Graph](#)
- [Line Chart](#)
- [Bubble Chart](#)
- [Pie or Ring Chart](#)
- [Network](#)
- [Histogram](#)
- [KPI](#)

Creating a Classic Grid

You can create a classic grid in a dashboard.

- 1. Open a dashboard.
- 2. In the top toolbar, click **Visualization** .

- 3. Choose **Grid** > **Grid** .

4. In the Datasets panel, double-click attributes and metrics to add them to the visualization. A grid requires at least one attribute and one metric.

- 5. In some situations, a Metrics header is automatically generated. You can hide or show the text in this header, by right-clicking it and choosing **Hide/Show "Metrics" Label**.

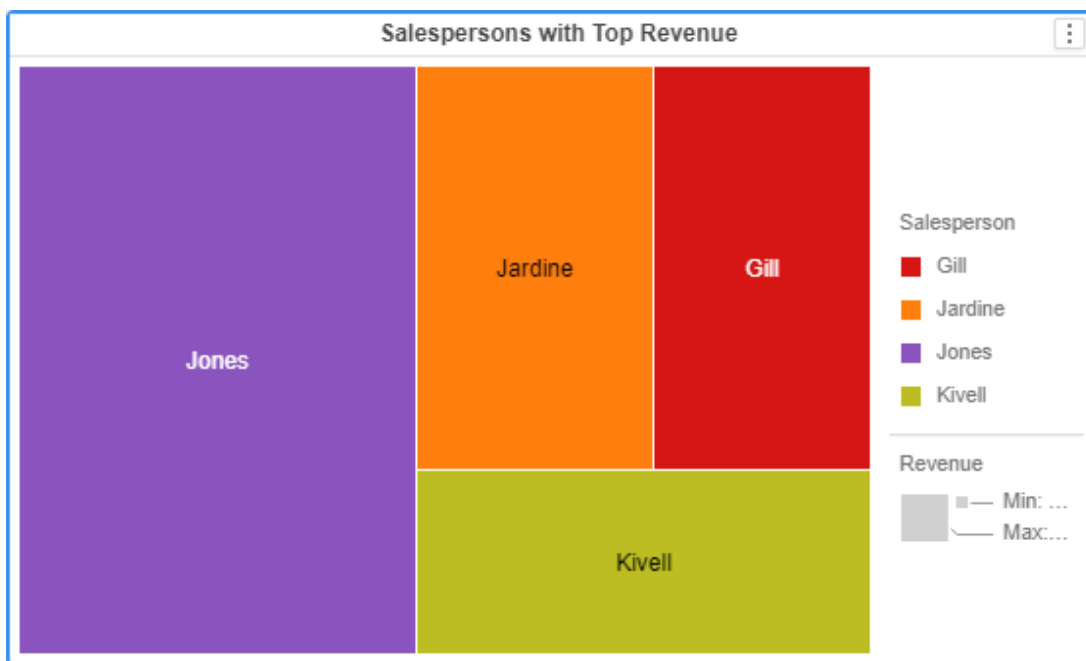
Year	2008	2008	2008	2008
Metrics	Customers LY Q			
Branch	Hide "Metrics" Label			
	Q2	Q3	Q4	
#8 Kemah Boardwalk	165,884	165,720	176,866	182,562
#814 Trans Canada Hwy Sicamous	41,592	31,621	41,760	36,908
1 - 1220 Brant St Burlington	41,592	31,621	41,760	36,908

Creating a Heat Map

You can create a heat map visualization in a dashboard.

1. Open a dashboard.
2. In the top toolbar, click **Visualization** .
3. Choose **More > Heat Map** .
4. In the Datasets panel, double-click attributes and metrics to add them to the visualization. A heat map requires at least one attribute and one metric.

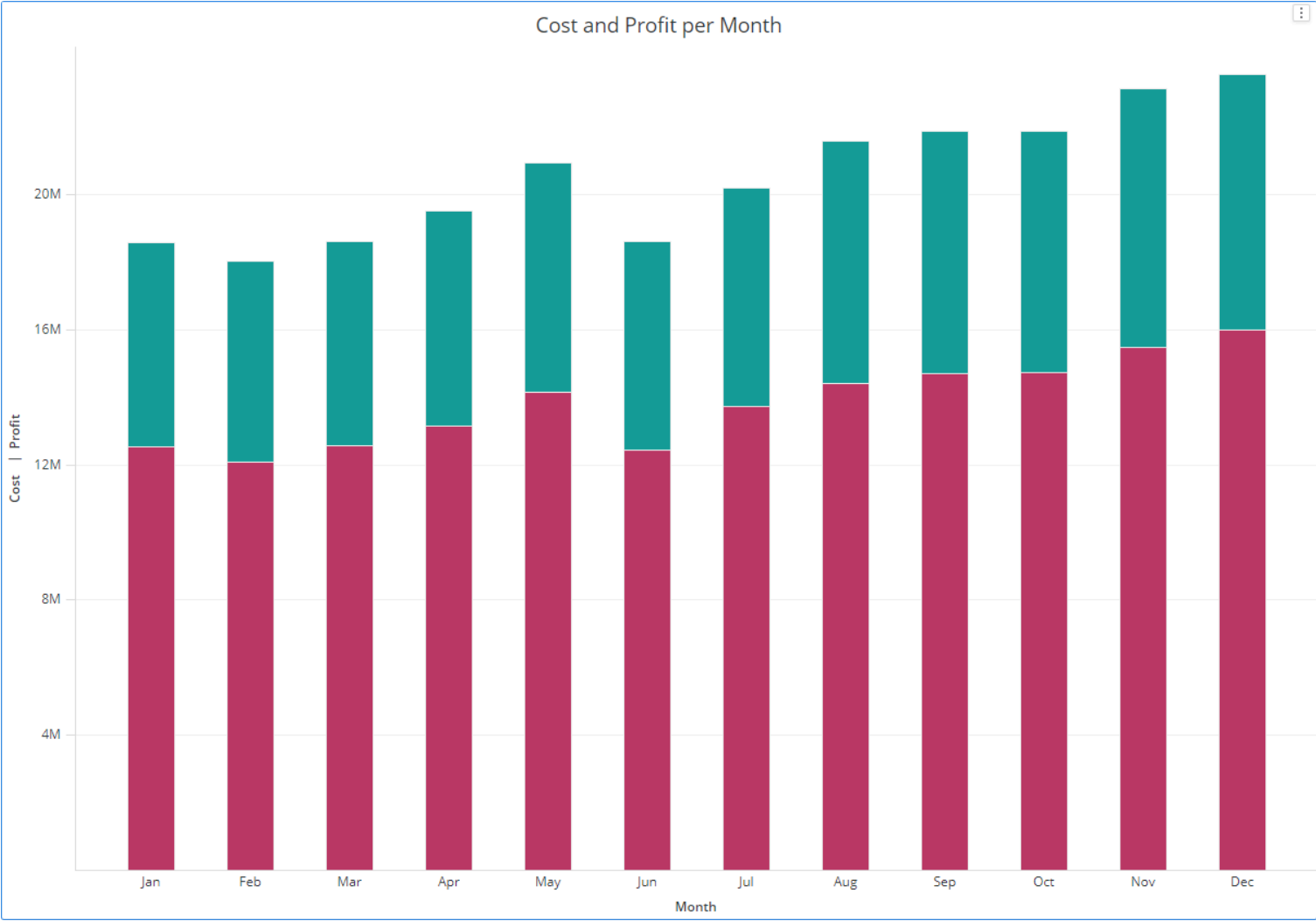
Example Heat Map



Creating a Bar Chart

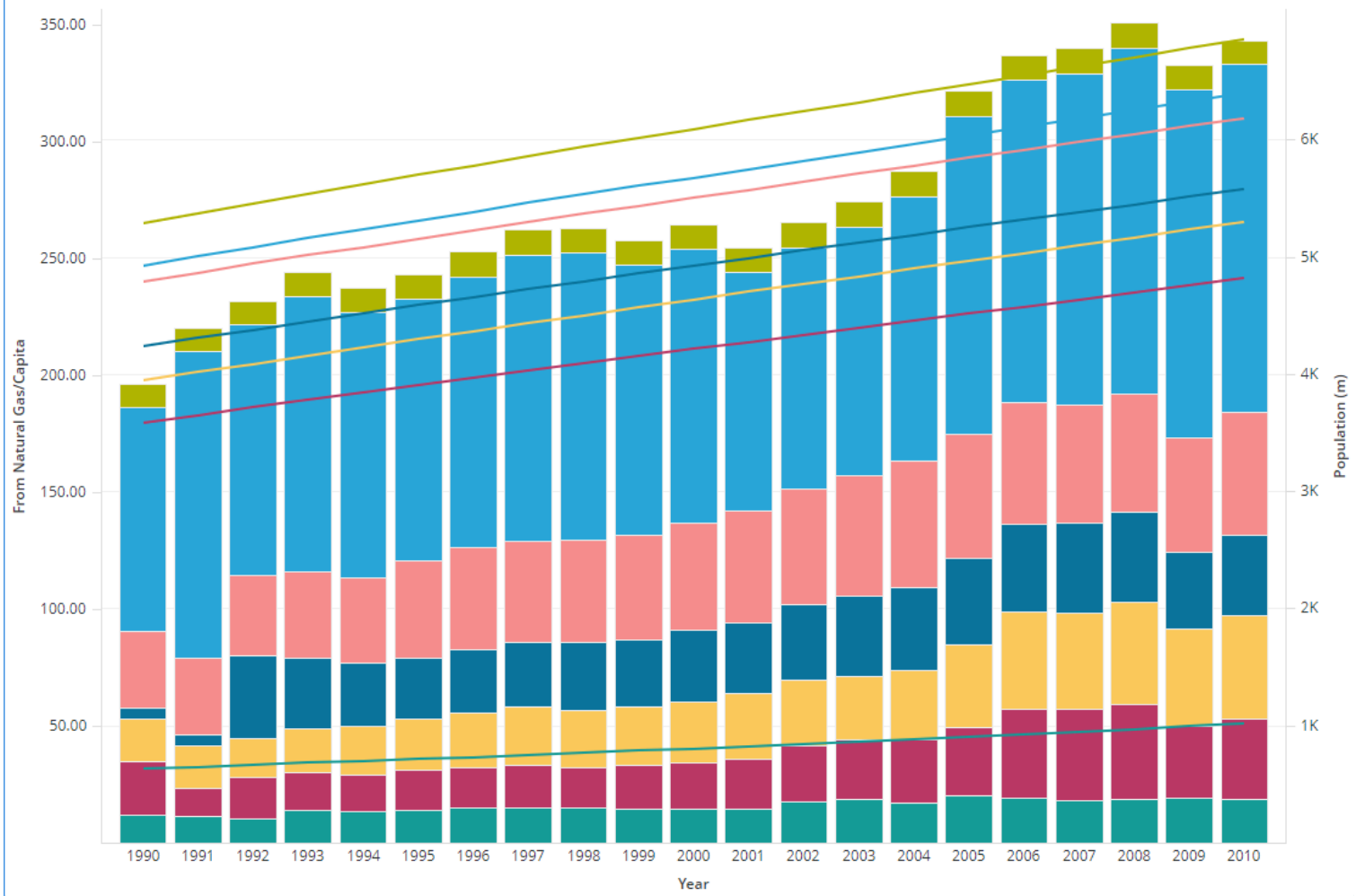
- 1. Open a dashboard.
- 2. In the top toolbar, click **Visualization**  .
- 3. Choose **Bar** and one of the many bar chart options. A bar chart requires at least one attribute and one metric.
- 4. In the Datasets panel, double-click attributes and metrics to add them to the visualization.

Example Vertical Stacked Bar Chart



Example Combo Chart

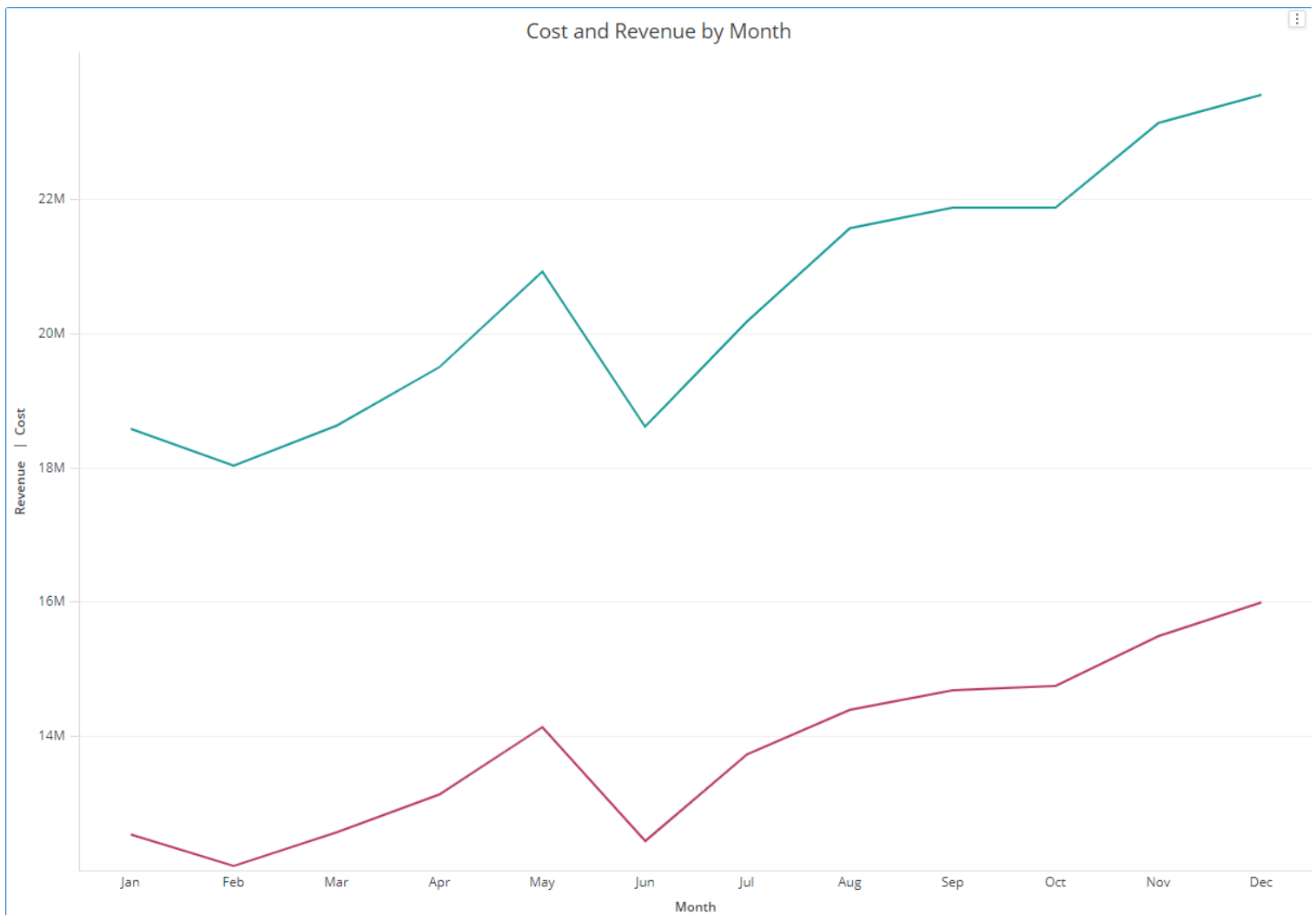
Visualization 1



Creating a Line Chart

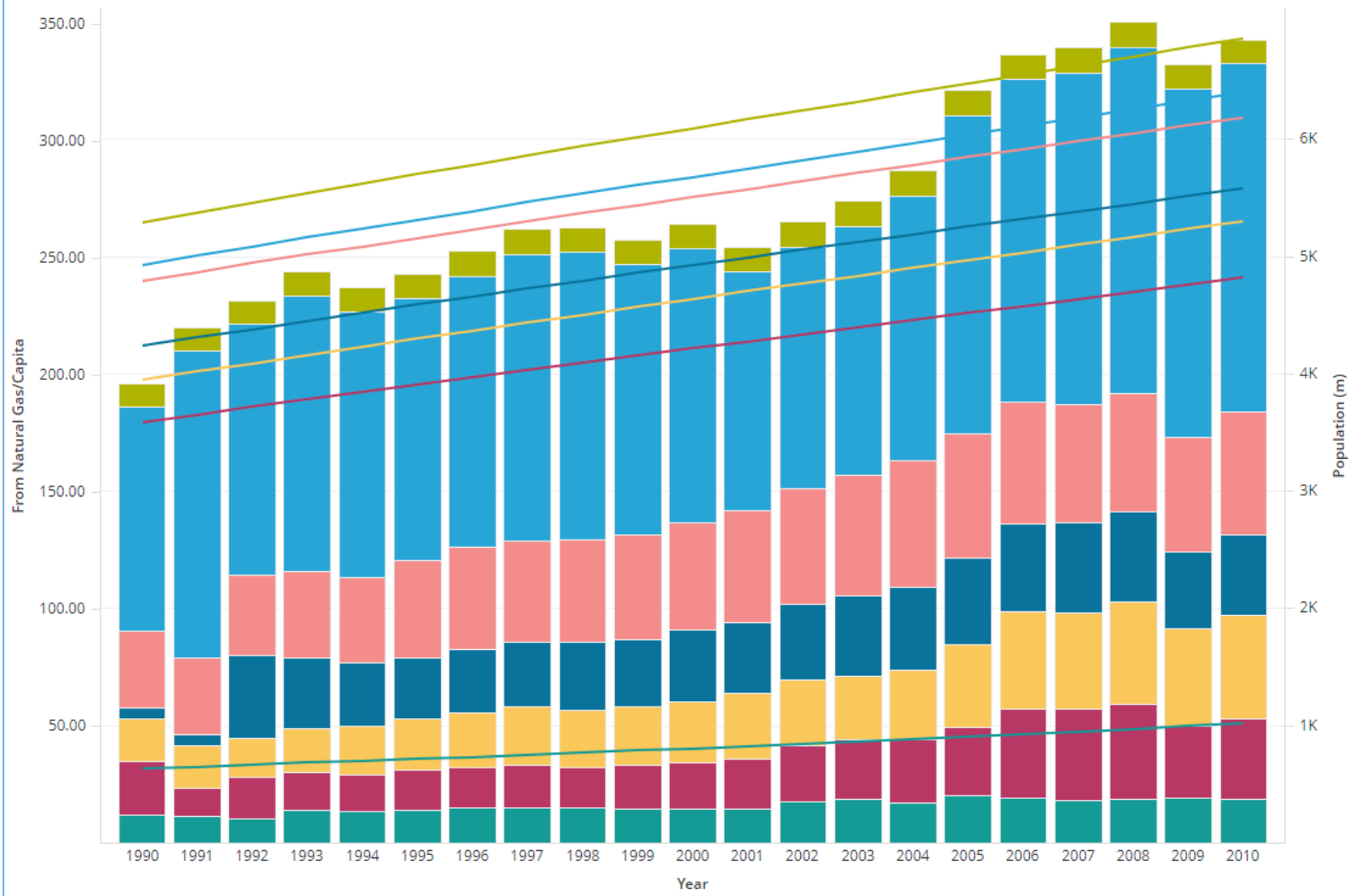
1. Open a dashboard.
2. In the top toolbar, click **Visualization** .
3. Choose **Line** and one of the many line chart options.
4. In the Datasets panel, double-click attributes and metrics to add them to the visualization. A line chart requires at least one attribute and one metric. Time attributes are recommended for line charts and dual axis line charts.

Example Line Chart



Example Combo Chart

Visualization 1



Creating a Bubble Chart

A bubble chart requires at least one attribute and one metric. The markers are not sized and do not overlap.

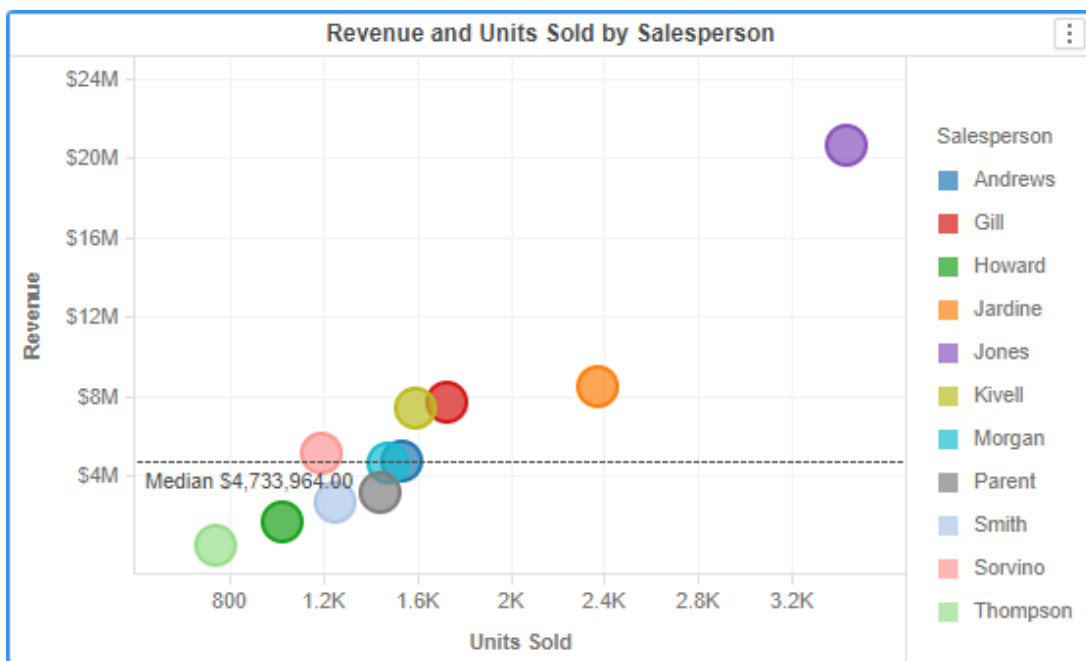
1. Open a dashboard.

2. In the top toolbar, click **Visualization** .

3. Choose **More > Bubble Chart** .

4. In the Datasets panel, double-click attributes and metrics to add them to the visualization.

Example Bubble Chart



Creating a Pie or Ring Chart

You can view the contribution of attribute elements or metrics to a total by displaying your data in a pie or ring chart.

You can use a variety of display styles to produce pie and ring charts. You can display pie charts in a grid layout or display ring charts in scatter layout.

To Create a Pie or Ring Chart

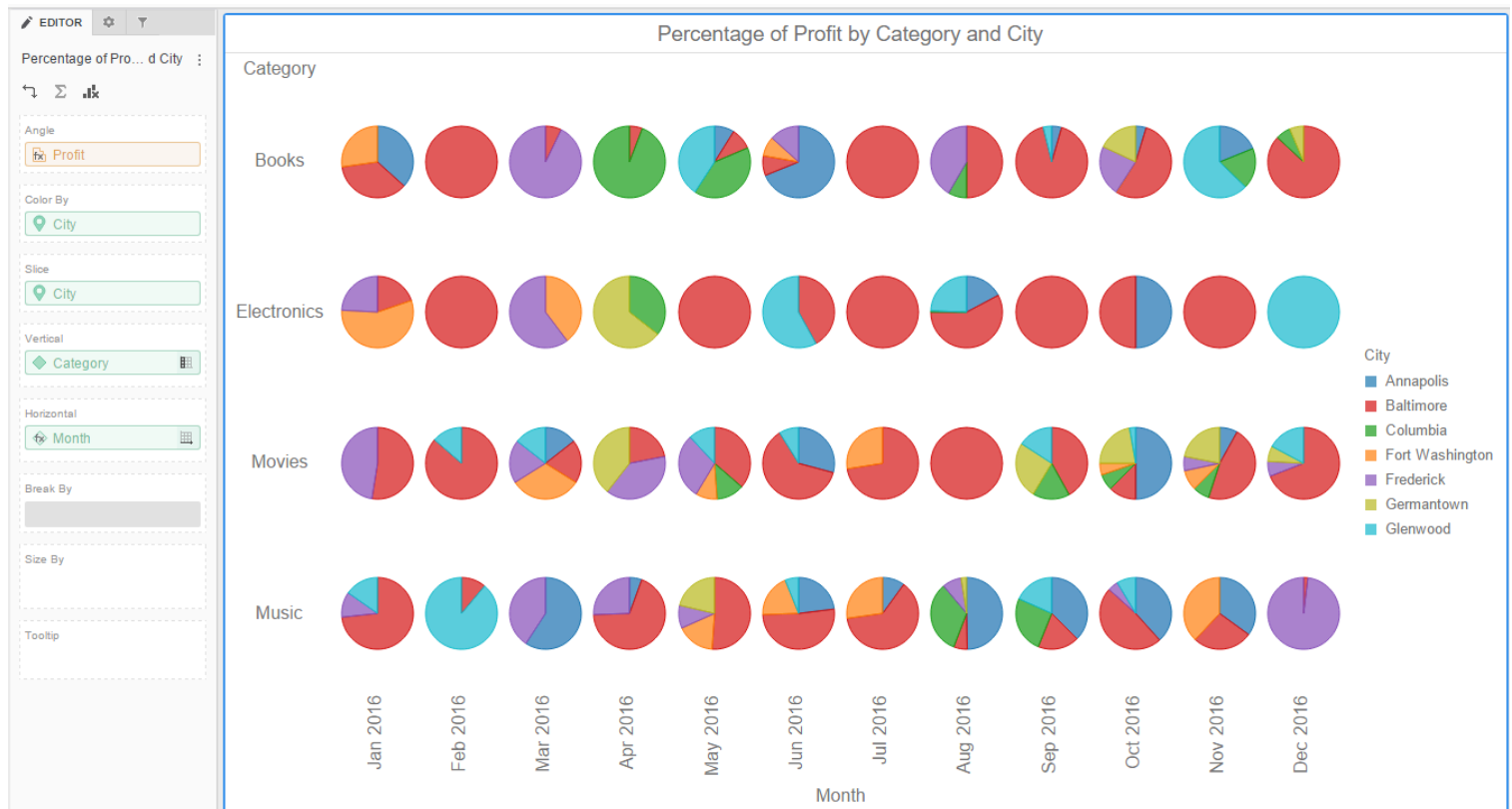
1. Open a dashboard.
2. In the top toolbar, click **Visualization** .
3. Choose **Pie > Pie Chart**  or **Ring Chart** .
4. In the Datasets panel, double-click attributes and metrics to add them to the visualization. A pie or ring chart requires at least one attribute and one metric.

Example Pie and Ring Charts

Display pie or ring charts in a grid layout. The pies or rings do not overlap.

This style requires:

- One metric in each of the following areas: **Angle**
- One attribute in each of the following areas: **Color By, Slice, Vertical, and Horizontal**



Display pie or ring charts in a scatter chart layout. The pies or rings can overlap and may or not be sized.

This style requires:

- One metric in each of the following areas: **Angle**, **Vertical**, and **Horizontal**
- One attribute in each of the following areas: **Color By**, **Slice**, and **Break By**

EDITOR

Cost and Profit by... tegory

↶

Σ

📊

Angle

Revenue

Color By

Category

Slice

Category

Vertical

Cost

Horizontal

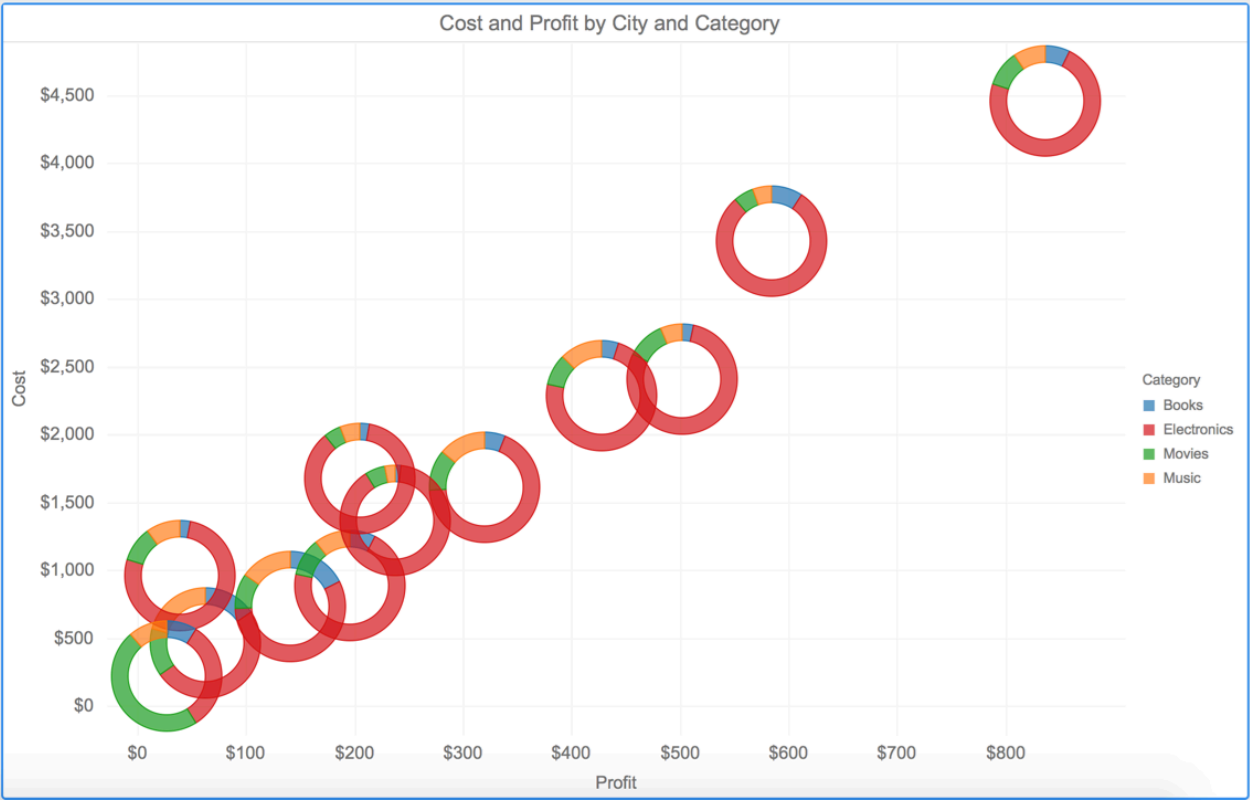
Profit

Break By

City

Size By

Tooltip



Creating a Network Visualization

You can create a network visualization in a dashboard.

1. Open a dashboard.

2. In the top toolbar, click **Visualization** .

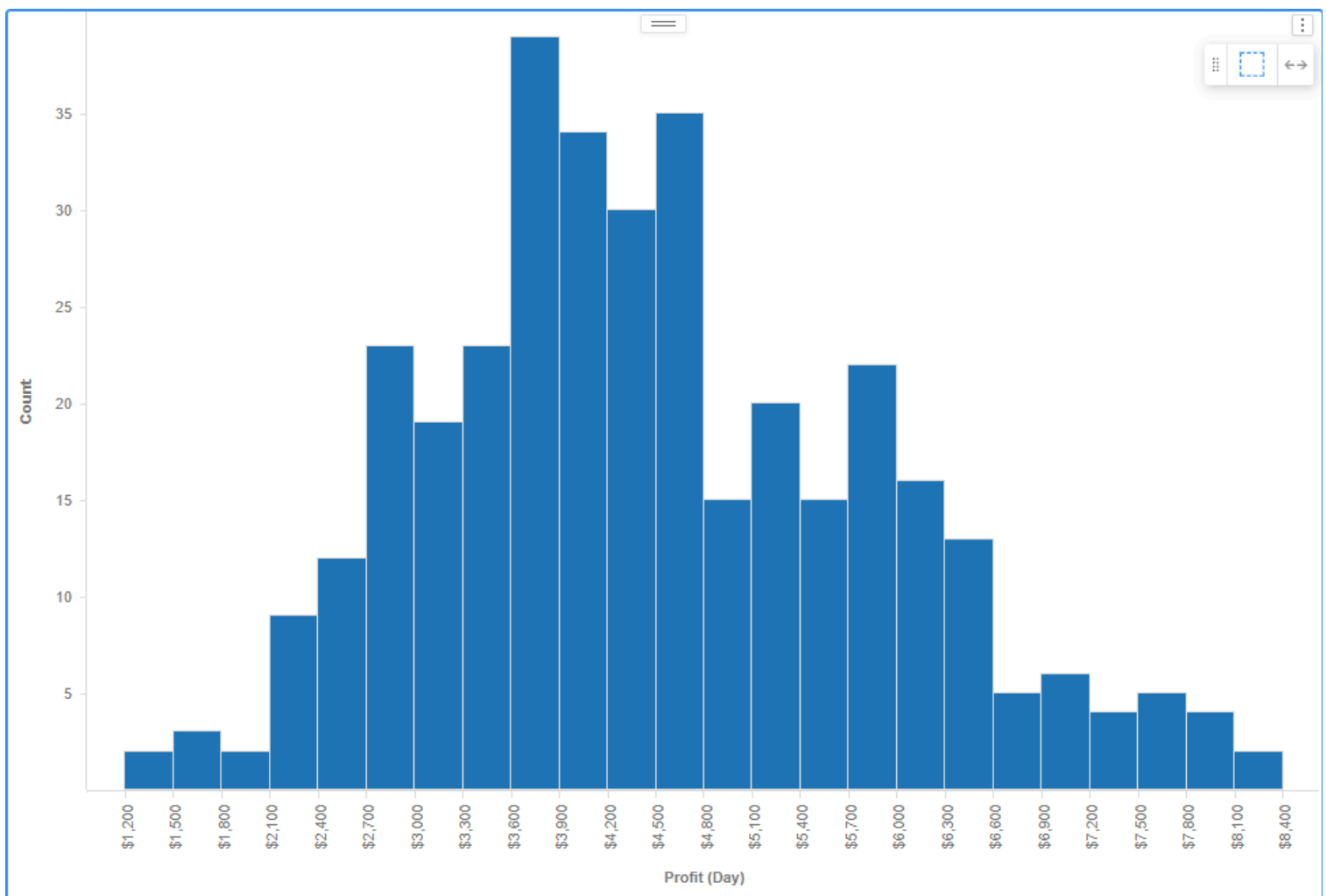
3. Choose **More > Network** .

4. In the Datasets panel, double-click attributes and metrics to add them to the visualization. A network visualization requires at least two attributes and one metric.

Create a Histogram

1. Open a dashboard.
2. In the top toolbar, click **Visualization** .
3. Choose **More > Histogram** .
4. In the Datasets panel, double-click attributes and metrics to add them to the visualization. A histogram requires at least one attribute and one metric.
5. Open the Format panel to modify formatting options, specific to histograms.

Histogram Example



Creating a KPI Visualization

1. Open a dashboard.
2. In the top toolbar, click **Visualization**  .
3. Choose **KPI > KPI**  .
4. In the Datasets panel, double-click attributes and metrics to add them to the visualization. A KPI visualization requires at least one attribute and one metric.
5. Open the Format panel to select formatting options, specific to KPI visualizations.

KPI Example



Changing the visualization type

After you have added a visualization to a dashboard, you can quickly change the type of visualization used to display your data. Follow these steps to change the visualization's display type:

1. Open an existing dashboard.
2. Select the visualization you need to change.
3. In the top toolbar, click **Visualization**  .
4. In the Visualization Gallery, click the icon that corresponds with the new visualization type.

Note: Hover over the icons to view the name and data requirements for each visualization type.

5. You can customize the display of the visualization by adding, replacing, and removing attributes and metrics from the visualization.

Duplicating a visualization

You can create a new visualization by duplicating an existing visualization, and then modifying it. When you duplicate an existing visualization, you can add it to any page or chapter in your dashboard.

1. Open an existing dashboard.
2. Click **More**  in the title bar of the visualization you want to duplicate and choose **Duplicate**.

Moving a visualization

After you create a visualization in a dashboard, you can change the position of the visualization within the dashboard. You can move a visualization:

- To a different position within the same page

To move the visualization, click and drag the visualization to its new location in the dashboard. An indicator line appears in the location where you can add the visualization. Release the mouse button to place the visualization in the new location.

- To a different page

- i. Click **More**  in the title bar of the visualization you want to move.
- ii. Click **Move to** and select the appropriate page.

- To a different chapter

- i. Click **More**  in the title bar of the visualization you want to move.
- ii. Click **Move to** and select the appropriate chapter.

Note: Moving a visualization between chapters leads to clearing all filters.

You can create layers of data in a dashboard using chapters, with each chapter displayed on a separate tab and filtered differently. Switch between chapters by selecting the corresponding tab for a chapter.

Each chapter can contain multiple pages, or layers of data, that are filtered in the same way. When a chapter contains multiple pages, a row of dots, each representing a page, appears at the bottom of the chapter. The current page is marked with a blue dot. Click one of the other dots to switch to a different page.

Deleting a visualization

To Delete a visualization from a dashboard, perform these steps:

1. Open an existing dashboard.
2. Click **More**  in the title bar of the visualization you want to delete and choose **Delete**.

Enabling a Legend

A legend in a data visualization, is a guide that clarifies the meaning of colors, symbols, or patterns in a chart or graph, helping users interpret the data accurately.

Note: Only bar, line, area, scatter, and pie charts are supported.

1. Open a dashboard.
2. Choose your visualization type.
3. In the Format panel, enable **Legend**.
4. Drag the legend to one the following positions:
 - Top/bottom: left, center, right
 - Right/left: top, center, bottom

Viewing and editing visualization filter targets

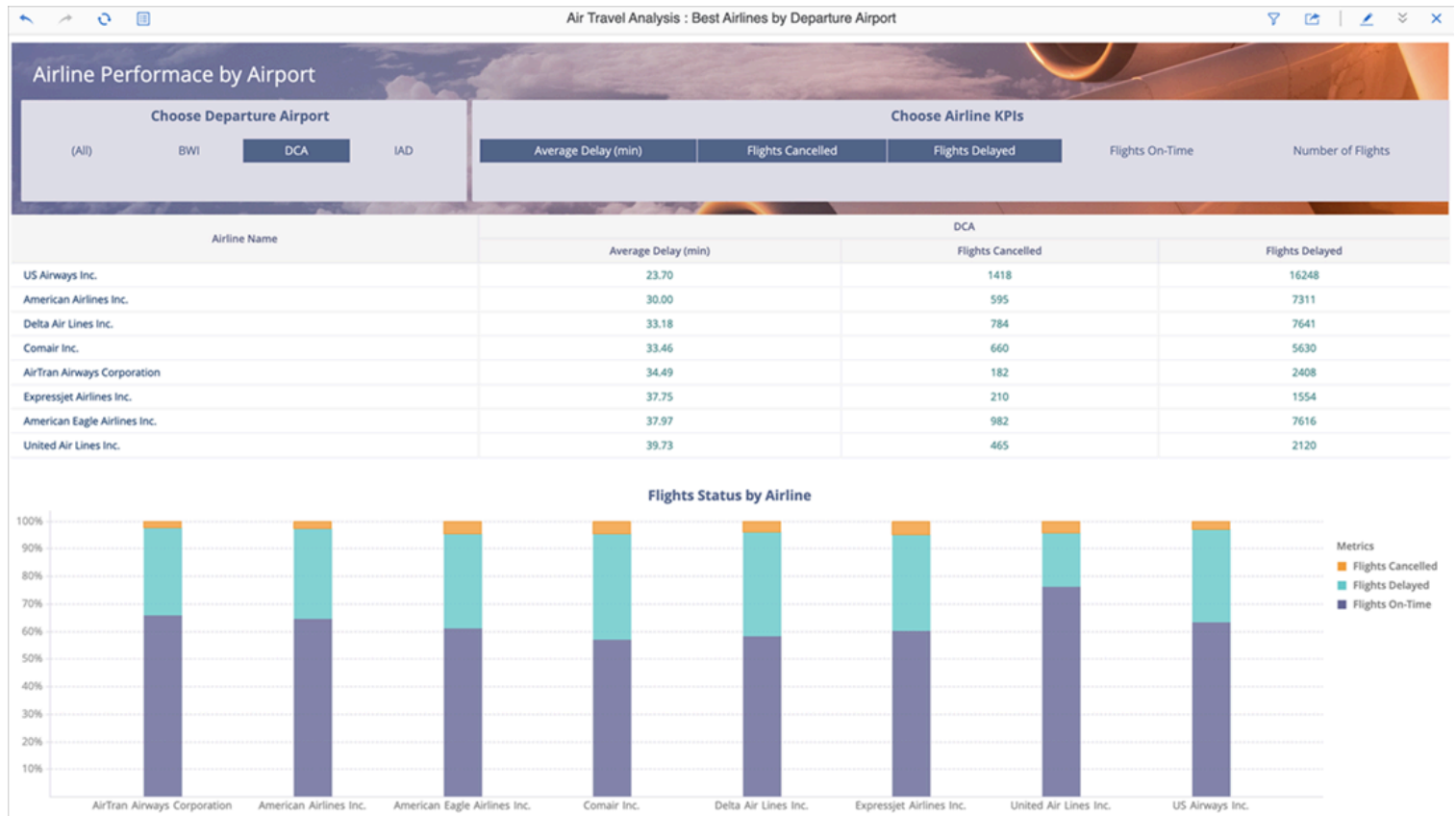
You can view and edit visualization targets. Targets include both visualization and filters that are affected by a visualization filter.

To view and edit visualization filter targets

1. Open the dashboard you want to modify.
2. Select the chapter that contains the visualization.
3. Hover over visualization, click **More**  in the top right, and choose **Select Target**.
A pop-up menu appears. The targeted visualizations and filters appear with checkmarks.
4. Select the checkboxes that correspond with the visualizations and filters you want to target.
5. Deselect the checkboxes that correspond with the visualizations and filters you no longer want to target.

Using Free-Form Layout

Use free-form layout to organize and overlap the containers that contain your visualizations, filters, selectors, images, HTML, and so on. You can independently position, size, and layer containers on a page.



1. Open or create a new dashboard. Your containers appear in auto layout by default. In auto layout, containers automatically fill the entire canvas and can be repositioned around each other.
2. Open the page in which you want to use free-form layout.
3. Click **Convert to Free-form Layout** .
4. You can revert back to auto layout by clicking the same button. When reverting back to auto layout, it is possible that your dashboard may not look exactly the same as it did before you converted it. If necessary, you can undo your change to revert back to free-form layout.

Enabling Outline Mode for a Grid

You can enable outline mode to make grid visualizations easier to analyze.

1. Create a grid visualization.
2. Click **View** and then select **Format Panel** .
3. Under **Visualization Options** , select **Layout**.
4. Select **Enable Outline**. The grid appears in outline mode.
5. Click the **+** or **–** icons to expand and collapse attributes and display more or less detail. You can also expand or collapse an entire level by clicking the attribute header. The expand or collapse state of the attribute header is saved with the dashboard.

Saving a dashboard

You can make changes to a dashboard, then save it for easy access at a later date. The entire dashboard, including visualizations, filters, and associated datasets, are saved in the file format. You can share the file with other web users. Other users can open the file in their own environments and modify the dashboard.

To save a dashboard:

1. Click **Save** 

Or

Choose **File > Save As** to save a copy of an existing dashboard using a different name.

2. Navigate to and select the location in which to save the dashboard.

Sort Data in a Grid

You can sort data in grid based on a single object.

1. Select a grid visualization.
2. In the Editor panel, right-click the attribute or metric to sort.
3. Choose **Sort Ascending** to sort the values in ascending order (that is, A to Z or 1 to 100).

or

Choose **Sort Descending** to sort the value in descending order (that is, Z or A or 100 to 1).

Advanced Thresholds Editor

The Advanced Thresholds Editor displays a list of all thresholds currently defined for the visualization. Use thresholds to format data in a visualization based on multiple attribute or metric qualifications.

Pre-requisites:

- Your dashboard must contain a grid visualization. You can only use the Advanced Thresholds Editor for grid visualizations.
- You have placed a metric in the Metrics area or an attribute in the Rows or Columns area.

Access

To access the Advanced Thresholds Editor:

1. In the Editor panel, right-click an attribute or metric and choose **Thresholds**. If you select an attribute, the Advanced Thresholds Editor opens. If you select a metric, the Quick Thresholds Editor opens.
2. If you opened the Quick Thresholds Editor, select the **Advanced Thresholds Editor** link to open the Advanced Thresholds Editor.

Fields

New Threshold: Select this link to add a new threshold.

Order: Displays the order in which the system evaluates a threshold. Click and drag a threshold to reorder it.

Threshold Conditions: Displays the threshold conditions. Select a threshold condition to edit its corresponding metrics, attributes, filter options, qualifications, operators, elements, or values.

Add Condition: Select this link to add a new condition.

Group Conditions: Select this link to group conditions together. A threshold must contain multiple conditions for this link to appear.

Operator: Select the drop-down between conditions and choose an operator for combining conditions (for example, AND, OR, AND NOT, and OR NOT). A threshold must contain multiple conditions for this drop-down to appear.

Format Preview: Displays a preview for displaying data that meets the threshold's condition. Click on the preview to select formatting options for the condition. Click **More**  to perform the following actions:

- **Apply to:** Select whether to apply the condition to **Metrics Only**, **Subtotals Only**, or **Metrics and Subtotals** that meet the threshold conditions.
- **Formatting:** Allows you to select the following formatting options for the condition:
 - **Replace Data:** Select the **Enable Data Replace** checkbox to replace the data that meets the threshold condition with the options in the corresponding drop-downs.
 - **Font:** Select font formatting options.
 - **Color and Border:** Select fill color and border options.
- **Duplicate:** Adds a copy of the current condition to the end of the list.
- **Move Up/Move Down:** Change the order in which the system evaluates a condition by moving it up or down in the list.
- **New Condition:** Add a new condition to the end of the list.

Quick Thresholds Editor: Select this link to open the Quick Thresholds Editor.

Creating a threshold on an attribute or metric in the Advanced Thresholds editor

You can create a threshold on an attribute or metric in the Advanced Thresholds Editor.

Your dashboard must contain a grid visualization. You can only use the Advanced Thresholds Editor for grid visualizations.

You have placed a metric in the **Metrics** area or an attribute in the **Rows** or **Columns** area.

To Create a Threshold on an Attribute or Metric in the Advanced Thresholds Editor for a Grid Visualization

1. In the Editor panel, right-click an attribute or metric and choose **Thresholds**. If you select an attribute, the Advanced Thresholds Editor opens. If you select a metric, the Quick Thresholds Editor opens.
2. If you opened the Quick Thresholds Editor, select the **Advanced Thresholds Editor** link to open the Advanced Thresholds Editor.
3. Click **New Threshold**.
4. In the **Based On** list, select the object to base the threshold on. The condition is based on either an attribute or metric. If you are creating a condition based on a metric, go to step 5. If you are creating a condition based on an attribute, go to step 6.
5. In the **Operator** list, select a comparison operator (Greater Than, Less Than, etc). To compare the metric to a specific value, enter the value in the text box. To compare the metric to the value of another metric, select the metric from the **Metric** list. Go to step 7.
6. To define the condition based on attributes in or not in a checklist, select **Selecting in list** from the **Choose elements by** drop-down. Then, select **In List** or **Not in List** and select the attribute elements you want to use. **In List** formats data only for the attribute elements you select. **Not in List** formats data for all attribute elements, except those you select.

or

To define the condition based on attribute form values, select **Qualification on** from the **Choose elements by** drop-down. You can qualify the condition based on the attribute element's ID form, one of its description forms, or the DATE form if the attribute is time-based using the radio buttons. Next, select an operator from the **Operator** list. To compare the attribute to a specific value, enter the value in the **Value** field. To compare the attribute form to another attribute form, select the attribute from the **Attribute** drop-down. Then, select the corresponding attribute form.

7. Click **OK**. The Advanced Thresholds Editor opens.

8. Click **More**  to the right of the threshold condition and choose **Formatting**.

Select formatting options for displaying the threshold.

9. Click **OK** .

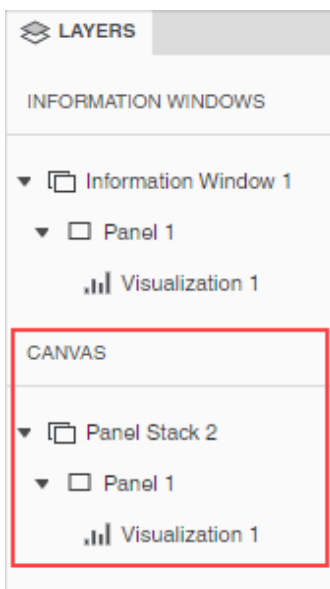
10. Click **OK**.

Adding Information Windows

You can add information windows to your dashboard to enhance the visual interactivity for the user. Information windows allow you to include additional context that is critical to the data point without overcrowding the canvas.

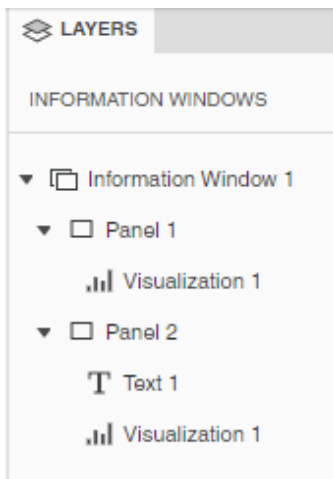
1. In the top toolbar, click **Information Window** .

The Information Window editor appears. You can return to the dashboard canvas by selecting an element under Canvas in the Layers panel.



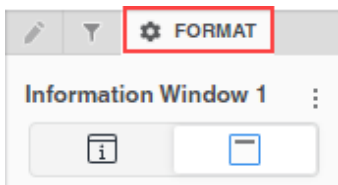
2. Add visualizations, text boxes, images, panel stacks, and any dashboard object to your information window.

The information window elements appear under Information Windows in the Layers panel. Navigate to a specific element by selecting it.



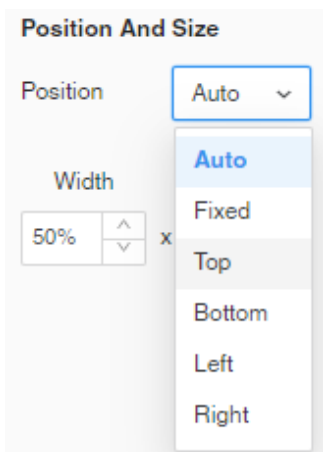
3. To change the visualization type, right-click the information window > **Change Visualization**.

4. To format the information window and its title, container, and other elements, go to the **Format panel**.

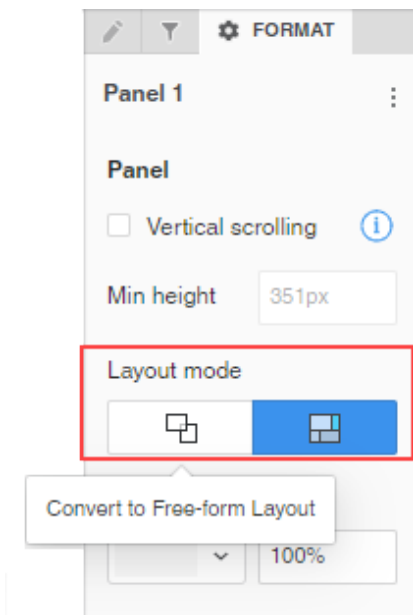


You can control the window positioning for when it is triggered.

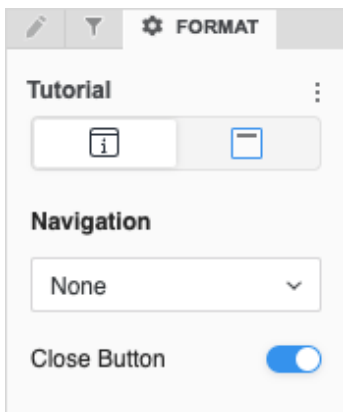
Info: The Left, Right, Top, and Bottom positions are in relation to the selected data point. If there is not enough space in the specified position based on the selected point, the information window will automatically display in a position where there is enough space.



5. In the Format panel of a Panel element, choose between **Free-form Layout** and **Auto-Layout**.



6. Add a Close button to control how your users dismiss the information window.



7. From the dashboard canvas, select a visualization, text box, or image that should trigger the information window.

Info: To trigger an information window for a Time Series visualization, use the horizontal selector to choose your desired data point(s). This includes a range of 1 to pass one data point.

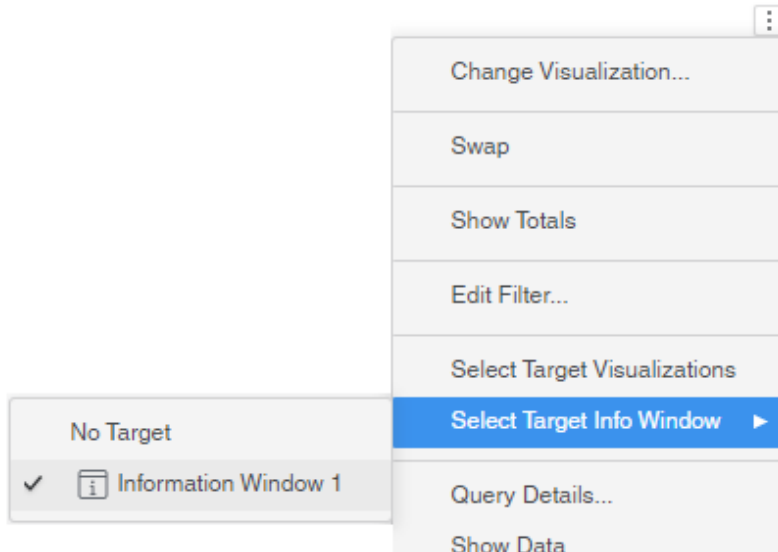
-84,966.88 (3.6%) ↑

3M 6M YTD 1Y 5Y ALL



Horizontal selection

8. In the upper right corner of the visualization, text box, or image, click **More**  > **Select Target Info Window**.



9. Select the information window.

10. To pass in-canvas filters and visualizations as filters to target the information window source visualization, right-click the information window > **Apply Additional Filter Conditions**.

Now, when you click on the visualization, text box, or image, the relevant information window appears and passes the selected element.

Show Data Dialog

Use the Show Data dialog box to examine the underlying attribute and metric data of a visualization in a simple grid format.

Access

To access the Show Data dialog:

1. Select a grid visualization.
2. Click **More**  in the top right of the visualization and choose **Show Data**.

Fields

- **Add Data:** Click to add data from the visualization's primary dataset to the grid.
- **Rows:** Displays the number of rows in the grid.
- **Export Data:** Select this drop-down to export the data on this dialog to Excel, PDF, or CSV format.
- **Add as Grid:** Click to create a new grid visualization using the data in the grid.
- **Grid:** Displays the underlying data for the selected area of the visualization. You can perform the following actions in the grid:
 - Resize columns by clicking and dragging column edges.
 - Reorder columns by clicking and dragging headers.
 - Sort columns by selecting the drop-down in the column header and choosing **Sort Ascending** or **Sort Descending**.
 - Copy the grid data to the clipboard so you can paste it into another application. Click on a row to select it for copying. Press and hold the Ctrl key to select specific rows. Press and hold the Shift key to select consecutive rows. Then press Ctrl + C to copy the data to the clipboard.

Note: The Show Data dialog box is not available for visualizations created using the data in a dataset imported from a server.

Using natural language queries

Natural language queries enable you to quickly find insights by entering questions, rather than manually building out a visualization.

Note: Natural-language queries are only supported in English.

To use natural language queries

1. Open a new or existing dashboard.
2. In the toolbar, click .
3. A list of sample questions appears. Choose a sample question or enter a question regarding the type of data you want to view in your dashboard. You must use the correct metric and attribute names in your query. As you enter attribute and metric names, you can select matching ones from the list.
4. Press **Enter**.
5. A new visualization appears, providing the data to answer your question.

Copying rows of data from a Grid

You can copy rows of data from a grid and paste them into another application. This option is available only in the Windows version of Digital.ai Intelligence Applications.

1. Select a grid visualization.
2. Select the data you want to copy in the grid.
3. Right-click and choose **Copy Rows**.
4. Paste the rows into another application (for example, Excel) as necessary.

Managing Datasets

The Datasets feature allows you to streamline and enhance the overall process of handling datasets, promoting data...

What is a Dataset?

A Dataset refers to a collection of data that is organized and stored together. The dataset presents structured data i...

Datasets Creation

Learn to create a dataset

Previewing Datasets

Learn how to preview a dataset

Exploring Datasets

Understanding datasets type, key expression and rule

Listing dataset

View the list of datasets and their uses



Viewing Existing Dataset

Explore the details of dataset



Actioning in Created Datasets

You can do the following actions using this option:



Custom Field Dataset

Custom Field is a feature provided by Digital.ai that enables you to add new data columns to existing dataset tables,...



Base and Advanced Datasets

A dataset refers to a collection of data that is organized and stored together. The dataset presents structured data i...

Managing Datasets

The Datasets feature allows you to streamline and enhance the overall process of handling datasets, promoting data integrity, security, and collaboration within the Digital.ai platform. Datasets are essential in data analysis and decision-making processes as they provide structured collections of data that can be analyzed to extract valuable insights and trends.

The following topics describe how to use and manage datasets:

- [What is a Dataset?](#)
- [Datasets](#)
- [Previewing Datasets](#)
- [Exploring Datasets](#)
- [Listing Datasets](#)
- [Viewing Existing Datasets](#)
- [Actioning in Created Datasets](#)

What is a Dataset?

A Dataset refers to a collection of data that is organized and stored together. The dataset presents structured data in tabular form, relevant to a particular domain or business process. Each dataset contains attributes and metrics of data, where each row represents a record, and each column represents a data attribute or field.

An entity of a dataset represents a distinct object or a concept about which data is collected and stored. It is a fundamental building block and serves as the basis for creating a dashboard.

Example: Consider a dataset named 'Customers,' containing an entity named 'Customer' representing distinct data, where each row contains information about an individual customer, and each column represents attributes like customer ID, name, address, email, and so on.

Customer ID	Customer Name	Address	Email
001	ABC	123 Main St	abc@example.com
002	DEF	456 XYZ Avenue	def@example.com
003	GHI	789 ABC Street	ghi@example.com

The Dataset is designed for creating out-of-the-box and self-service dashboards. You can develop reusable, and reliable datasets tailored for your specific business use case.

The Dataset serve as the foundation for out-of-the-box dashboards. It provides the data that drives visualizations and insights. Utilizing pre-built components and configurations, you can create informative and interactive dashboards with minimal coding or development.

For more information about dashboards, see [Dashboards](#).

Datasets Creation

The dataset page helps you view, create, edit, duplicate, extend, and publish the dataset to meet your requirements. It facilitates the integration of datasets from various sources, allowing you to work with diverse data types and formats.

The dataset page has the following options:

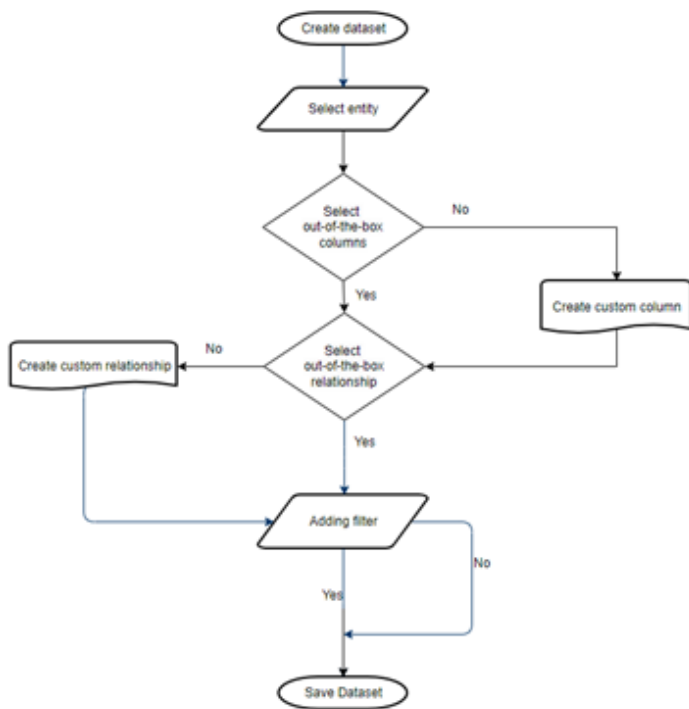
- **Select source instance:** It enables you to choose the desired source instance to access datasets created within that specific environment. A source instance refers to a particular system or database from which data is extracted and integrated into the data warehouse environment.
- **Grid and list view:** You can view the datasets in grid and list view using these options. The list view presents data in a tabular format with rows and columns, making it easier to scan and compare values visually. The grid view presents data in a structured grid format, with each grid representing a dataset. The grid view is useful for comparing and analyzing multiple datasets simultaneously.
- **Search dataset:** It helps you to search for a dataset.
- **Create dataset:** It helps you to create a dataset.

Searching dataset

You can type a keyword in the Search dataset to search for a dataset.

Creating a dataset

This task enables you to create a dataset. It enables you to create new datasets, defining the structure, schema, and properties of the data. It supports importing data from various sources and integrating it into datasets seamlessly. You can also edit, modify, or transform data within datasets, ensuring data quality and consistency. Here's a flowchart to understand the dataset creation process.



Prerequisites

Analytics author Access is required to duplicate out-of-the-box datasets and create or edit custom datasets.

Complete the following steps to create a dataset:

Selecting an entity

Entities are crucial in dataset creation as they provide a structured framework for organizing and representing data. Defining entities enables a clear understanding of the data stored and the relationships among various pieces of information. Complete the following steps to select an entity:

1. Click **Create dataset**.
2. Click **Select source instance**, and then select the required source instance.
3. Click **Linked instance**, and then select the required instance.
4. Click the **+** icon against entities to add the required entities from the entity list. If you accidentally closed the Add panel, you can reopen it by clicking on the **Add entity** button. By clicking on **Add entity** the panel should reappear, allowing you to resume the entity addition process without losing any progress.

NOTE

You can search or use the scroll bar to select entities.

Add entity ▼

Add

×

Entity

Filter

DigitalAI_Agility_Tenant

▼

Linked Instance

DigitalAI_Agility_Tenant

▼

Q

search

Name

Actions

▲

Actual_Now

Add

AssetAudit

Add

Choosing out-of-the-box columns

Out-of-the-box columns are vital for dataset entities, providing a foundation for data organization, standardization, and efficiency. They ensure data consistency and enhance the dataset's value for analysis and decision-making. Complete the following steps to select the out-of-the-box columns:

1. Click the entity.
2. In the Column tab, select the required columns, and then click **Add**. Note: You can do a single or multiple selection of columns.
3. Click the edit button in the **Explore dataset** pane to modify the column's name.

Creating custom object or column

The custom columns are typically derived from existing data within the dataset through calculations, transformations, or other manipulations to generate new insights or information. You can create a custom object or column using this option.

NOTE

You cannot change the data object type that is attribute and metrics for the created data object.

Complete the following steps to create the attributes:

1. In the **Explore dataset** pane, click **Create object**.
2. In the **Data Object** window, type the column or object name.

i NOTE

The column or object name must not contain any blank spaces.

1. Select **Attribute**.
2. Click **KeyColumnDatatype**, then select the required data type.
3. Type **Key expression**.

i NOTE

Key column datatype and key expression are mandatory to create a custom column.

1. Click **DisplayColumnDatatype**, then select the required data type.
2. Type **Display expression**.
3. Click **Save**.

Data Object

Object name*

Test_dataset

☒ Attribute ☐ Metric

KeyColumnDatatype

LARGETEXT

Key Expression

DisplayColumnDatatype

LARGETEXT

Display Expression

Cancel

Save

Complete the following steps to create the metrics:

1. In the **Explore dataset** pane, click Create object.

2. Type of the object or column name.
3. Select **Metric**.
4. Click **Aggregation Rule**, then select the required aggregation.
5. Click **KeyColumnDatatype**, then select the required data type.
6. Type **Key expression**.
7. Click **Save**.

Data Object

Object name*

Test_metric

☐ Attribute ☒ Metric

Aggregation Rule

SUM

KeyColumnDatatype

LARGETEXT

Key Expression

Cancel

Save

NOTE

You get a **Data Object ABC was successfully created** message once the data object or column is created.

Key expression

The key expression enables you to create a column or attribute that helps identify, organize, and relate data across tables. You can transform existing attributes to ensure uniqueness and aid in efficient querying and analysis. This expression plays a vital role in schema design and data modeling.

Example: Consider you have an Orders table that contains information about orders placed by customers. Each order has an Order ID and is associated with a Customer ID. you want to count the number of orders placed by each customer.

Here's how you can use a key expression along with the COUNT function to achieve this:
"COUNT(OrderID)"

NOTE

You can type # to select an entity.

CustomerID	OrderCount
101	3
102	1
103	1

This result shows the count of orders placed by each customer. Customer 101 has placed 3 orders, customer 102 has placed 1 order, and customer 103 has also placed 1 order.

Editing custom object or column

You can edit the existing object or column using this option. You can rename the column, adjust the property, edit the data, and rearrange the structure. Complete the following steps to edit the object or column:

1. On the **Explore dataset** pane, click the edit button against the data object name.
2. In the **Data object** dialog box, edit the required details.
3. Click **Save**.

NOTE

You get a **Data Object ABC was successfully updated** message once the object or column is edited.

Deleting custom object or column

This feature enables you to delete the custom object or column. Complete the following steps to delete the object or column:

1. On the **Explore dataset** pane, click the delete button against the data object name.
2. You get a **Data Object ABC was successfully deleted** message once the object or column is deleted.

Selecting out-of-the-box relationship

You can select a predefined relationship using this option. Out-of-the-box relationship provides a convenient and reliable approach to establishing data connections and promoting efficiency, accuracy, and consistency in data analysis and reporting processes. This option displays the out-of-the-box relationships between the selected entity and the other entities in the selected source. Complete the following steps to select the relationship.

- 1. Click the entity.
- 2. In the entity, click **Relationship**.
- 3. Click the **Link** against the required relationship.

Adding custom relationship

You can create custom relationships using this option. Custom relationships offer flexibility, control, and adaptability in establishing data connections, allowing you to address your business needs, accommodate complex data structures, and optimize data analysis processes. Complete the following steps to add a custom relationship.

- 1. Click and draw a line between two entities.
- 2. Click **join type** and select the required join type.
- 3. Enter an expression in **Expression**.
- 4. Click **Add Join**.

Add join

Primary entity

Access

Related entity

Access_Now

Join type

INNER JOIN

Expression

Access_Now__sys_row_key = Access__sys_row_key

Hint: Use ! for Properties, # for Entities, . for Attributes and @ for Intelligence Functions

Cancel

Add Join

Join type

The join type refers to the method used to combine rows from two or more tables in a relational database based on a related column between them. The join types determine how the database engine matches rows from different tables and includes them in the result set. You can use any of the following types to create a relationship based on your requirements:

- **Inner join:** This type of join returns only the rows from both tables that have matching values in the specified columns. It combines rows from two tables where the join condition is met.
- **Left outer join:** This join returns all the rows from the left table (the table mentioned first in the SQL query) and the matching rows from the right table. If there are no matching rows in the right table, NULL values are returned.
- **Right outer join:** It returns all the rows from the right table and the matching rows from the left table. If there are no matching rows in the left table, NULL values are returned.
- **Full outer join:** This join returns all rows from both tables, regardless of whether there is a match or not. If there is no match, NULL values are returned for the columns from the table that lack a matching row.
- **Cross join:** This type of join returns the Cartesian product of the two tables, meaning it combines each row of the first table with every row of the second table. It does not require a join condition.

Example: Consider the Employees and Departments tables. The Employees table contains information about each employee, such as their ID, name, department ID, and salary. The Department's table contains information about each department, such as its ID and name. Now, let's say you want to join these two tables to get a result set that contains each employee's ID and the department name.

You can achieve this by using the following SQL query with an inner join:

```
#Employees.Department_ID = #Departments.Name
```

i NOTE

You can type # to select an entity.

The Inner Join specifies that only the rows with matching values in both tables will be included in the result. You get the following table as a result:

ID	Department
101	HR

ID	Department
102	Marketing
103	Finance

Adding filter

This feature enables you to create a filter. The filter feature enhances the dataset view in data exploration capabilities, empowering users to extract meaningful insights from the dataset more efficiently. Complete the following steps to add a filter.

1. Click the **Filter** tab.
2. On the **Filter** tab, type the filter condition.
3. Click **Save**.



The screenshot shows a user interface for adding a filter. At the top, there is a header bar with a grid icon, the text 'Add', and a close button (X). Below this is a tabbed interface with two tabs: 'Entity' and 'Filter'. The 'Filter' tab is currently selected, indicated by a blue underline. Under the 'Filter' tab, there is a large text input field labeled 'Filter condition'. Below the input field, a hint text reads: 'Hint: Use ! for Properties, # for Entities, . for Attributes and @ for Intelligence Functions'.

Example: consider a Students table with columns for StudentID, Name, and Age. Let's say you want to filter out students who are older than 18 years old..

Here's how you can write a filter condition for this scenario: " Students.Age > 18"

NOTE

You can type # to select an entity.

The result of this query would include only the students who are older than 18 years old.

Saving custom Dataset

The Save Custom Dataset feature enables you to save customized datasets with specific configurations, filters, or transformations applied. By saving a custom dataset, you can easily access and reuse your tailored data views for ongoing analysis or reporting tasks. Complete the following steps to save a dataset:

- 1. To enable the preview dataset feature, click **Save** or **Save and continue**. Selecting **Save and continue** enables you to preview the dataset without closing the dataset creation page.
- 2. In **Save dataset**, type the dataset name and description.

i NOTE

The Dataset name must not contain any blank spaces

- 3. Type the mapping name.
- 4. Click **Save**. You get a **Dataset XYZ was successfully created** message once the dataset is saved.

i NOTE

The dataset is created, and it is in a draft state.

Save dataset

Dataset name *

Description

Mapping name
Mapping name helps identify the dataset when extended to different instance.
Please provide a unique name

Mapping name *

☐ Enable

Cancel

Save

Previewing Datasets

You can preview the dataset using the **Preview dataset** option. The **Preview dataset** option is available once you save the dataset. It gives you 50 rows of dataset data. Complete the following steps to preview the dataset:

1. Click **Open dataset** in a dataset.
2. In the Explore dataset pane, click **Preview dataset**.

Exploring Datasets

The **Explore dataset** pane provides you with the details of data objects. You can also view and edit the following details in the pane:

- Object or Column name
- Type
- Aggregation rule
- Key data type
- Key expression
- Display data type
- Display expression

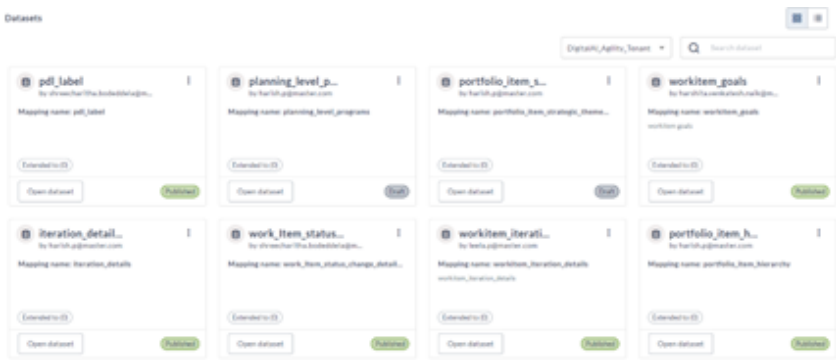
Object name	Type	Agg rule	Key data type	Key expression	Display data type	Display expression
__sys_source_id	attribute		INTEGER	dep_deployment_s"__sys_source_id"		
application_id	attribute		INTEGER	PII_LOVER(dep_deployment_s"application_n...		
application_name	attribute		INTEGER	dep_deployment_s"application_name"		
calendar_date	attribute		INTEGER	whs_calendar_dateL"calendar_date"		

Listing dataset

This option enables you to view the created s. You can view the existing by selecting **Select source instance**, and then selecting a source instance. You can view the s in the grid and list view.

NOTE

This option lists the s created under the selected source instance.



You can view the following details for each :

- Name of the
- Description of the
- Type of the
- Extended to count
- Visibility
- Owner of the

NOTE

The flag indicates the 's ownership, either by Digital.ai for out-of-the-box or by the customer for custom s. For out-of-the-box s, the owner is automatically set as Digital.ai, while for custom s, the owner's name corresponds to the customer's name.

- Status of the

The has the following three statuses:

- **Draft:** is created but not published.

- **Published:** is published and ready for usage in your BI tool.
- **Modified:** Published is modified.

Viewing Existing Dataset

You can explore the details of a dataset using this option. You can see the extended view of the dataset and preview the dataset. You can perform the following actions on this page.

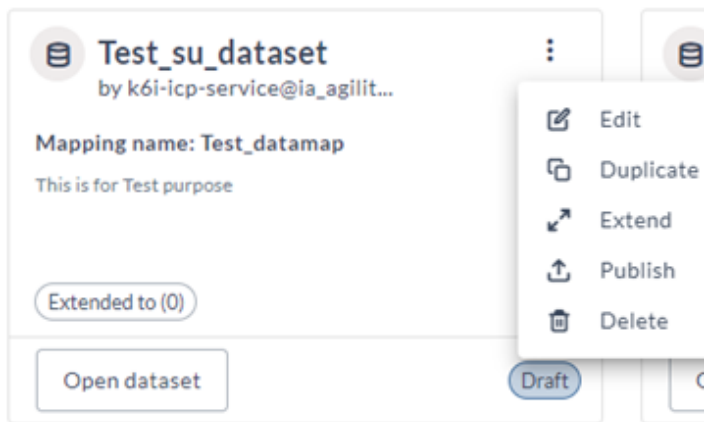
1. You can go into a dataset by clicking **Open dataset** on an existing dataset.
2. You can expand the dataset view by clicking the expand ^ icon.
3. You can expand the preview dataset view by clicking the expand  icon.



Actioning in Created Datasets

You can do the following actions using this option:

- Editing
- Duplicating
- Extending
- Publishing
- Deleting



Editing dataset

The Editing dataset enables you to modify the dataset's structure, content, or properties to suit your requirements. This feature typically provides tools or interfaces to perform various actions like adding or removing columns, adjusting data types, applying filters or transformations, and updating data records.

NOTE

You can edit only customized dashboards.

You can perform the following actions using this feature:

- You can explore the dataset data using the Exploring dataset feature.
- You can edit or add columns to the dataset.
- You can preview the data using the Previewing dataset feature.
- You can save the modified changes in the dataset.

WARNING

You cannot delete the added columns in the dataset.

Complete the following steps to edit the custom dataset:

1. Click **Open dataset** in a dataset.
2. Edit or add columns in the dataset.
3. Modify other changes based on your requirements.
4. Click **Save**. You get a **Dataset XYZ was successfully updated** message once the dataset is updated.

Duplicating dataset

The duplicating dataset feature enables you to copy an existing dataset. You can create a customized dataset from an out-of-the-box dataset using this feature. Complete the following steps to duplicate an existing dataset:

1. Click **Select source instance**, and then select the required source instance.
2. In **Search dataset**, enter your dataset name.
3. On the dataset, click the three-dots menu, and then select **Duplicate**.
4. In **Duplicate – abc_sample_dataset**, type a name and description of the dataset in the respective fields.
5. In **Extended details**, select the instances where you want to duplicate this dataset.
6. Click **Duplicate**.

NOTE

You see a **Success** message once the dataset is duplicated to the selected source instance.

Duplicate - portfolio_item_hierarchy

Name *

portfolio_item_hierarchy_copy

Description

You are about to duplicate dataset "portfolio_item_hierarchy". Click duplicate button to continue

Cancel Duplicate

Extending dataset

The extending dataset feature enables you to extend a dataset from one instance to another instance using this feature. You can copy a dataset between and within source instances and reuse the same. This feature copies only the data object or column, and you need to create data mapping for the extended dataset. You can extend customized datasets but not out-of-the-box datasets. Complete the following steps to extend a created dataset:

NOTE

You need to select enable while saving the dataset to extend the same dataset.

Save dataset

Dataset name *

Description

Mapping name
Mapping name helps identify the dataset when extended to different instance.
Please provide a unique name.

Mapping name *

☐ Enable

Cancel Save

1. Click **Select source instance**, and then select the required source instance.
2. In **Search dataset**, enter your dataset name.
3. On the dataset, click the three-dots menu, and then select **Extend**.
4. In **Extend dataset – abc_sample_dataset**, select the instance you want to extend.
5. Type the mapping name.

NOTE

You can click **Enable** to enable the multi-instance dataset extension.

1. Click **Extend dataset**.

NOTE

You see a **Dataset abc_sample_dataset was extended successfully** message once the dataset extends to the selected source instance.

You can hover the cursor over the **Extended to ()** button to view the name of the extended source instance.

Publishing dataset

The publishing dataset feature enables you to share datasets effectively and collaborate on data-driven initiatives within your organization. It promotes data transparency, accessibility, and reuse, facilitating informed decision-making and innovation. This feature is typically used when a dataset is ready to be shared and utilized for various purposes such as reporting, analysis, or application development.

Complete the following steps to publish a dataset:

1. Click **Select source instance**, and then select the required source instance.
2. In **Search dataset**, enter your dataset name.
3. On the dataset, click the three-dot menu in the dataset, and then select **Publish**.

NOTE

Once the dataset is published, you get a **Success** message. You can see the dataset in the published status.

Deleting dataset

The Delete feature allows you to remove outdated, irrelevant, or incorrect datasets, helping you maintain databases and interfaces clean and organized.

Refer the following steps to delete a dataset:

1. Click **Select product**, and then select the required product. The **Source integration** is selected by default.
2. Navigate to the dataset or enter the dataset name in the **Search datasets** text box.
3. Click the three-dot menu on the dataset, and then select **Delete**.

Note: The dataset deleted cannot be retrived.

4. Click **Delete** to re-confirm.
- You must either have an Admin or Author access to delete a dataset.
 - You cannot delete a Digital.ai authored dataset and an extended dataset.
 - Dataset with dashboard dependency (used to create a dashboard) needs to be unlinked to delete.
 - Verify dataset dependency before deleting datasets with tools other than MicroStrategy.

Custom Field Dataset

Custom Field is a feature provided by Digital.ai that enables you to add new data columns to existing dataset tables, allowing for tailored data modeling and extended analysis capabilities. When a custom data column also known as custom field is added to a dataset, the corresponding table is automatically updated and represented with the suffix `_custom_field` to distinguish it from the regular datasets.

For example, if a custom field is added to a table named `table_name`, the updated table will appear as `table_name_custom_field`. This naming convention helps users easily identify which tables have been extended with custom fields, ensuring better traceability and data governance.

How to link a Custom Field Dataset

You can add an existing custom field datasets from your environment to a dashboard.

1. Add the required datasets. Refer [Adding an existing dataset](#) topic for more details.
2. Link the added datasets. Refer to [Link Data in a Dashboard](#) topic for more details.

ⓘ IMPORTANT

Manually linking attributes allows you to link attributes across multiple existing datasets. The attributes that you link to each other should uniquely identify each record, to ensure that the results are calculated accurately. For datasets with custom fields, use the **Identifier** attribute to establish a link to the business ID in the related dataset. The attributes that you link must be the same data type. You can link an attribute to attributes in one or more datasets.

Related Topics: Refer [Creating Dashboards](#) section for more details on how to create and customize a dashboard.

Base and Advanced Datasets

A dataset refers to a collection of data that is organized and stored together. The dataset presents structured data in tabular form, relevant to a particular domain or business process. Each dataset contains attributes and metrics of data, where each row represents a record, and each column represents a data attribute or field. Datasets are broadly classified into two categories:

- Base Dataset
- Advanced Dataset

What is a Base Dataset?

A base dataset is the raw or initial collection of data, often unprocessed or minimally processed, and used for initial analysis. It may contain raw numbers or text data without much or any transformation, extracted from the source directly and stored in the Master Data Store (MDS).

What is an Advanced Dataset?

An advanced dataset refers to data that has undergone transformation or additional processing to provide deeper insights, make it more useful for specific tasks, or reporting, and stored as a Transformed Data Store (XDS).

Blending Base and Advanced Datasets

The advanced dataset, which contains transformed data and derived metrics, is seamlessly integrated with a base dataset, which contains core information using common identifiers known as keys. For example, if you have a base dataset with employee information (employee id, job titles, departments) and an advanced dataset with performance metrics (monthly evaluations, project outcomes), you would use employee IDs as keys to combine them. This would create a dataset that includes both employee details and performance data, providing a comprehensive view for making decisions related to promotions, training, or workload management.

It is important to use combinations that are logically supported by their content when blending datasets. Merging datasets that share the same keys ensures that the merged dataset is coherent and meaningful.

When merging datasets base and advanced datasets, the process relies on matching records based on these primary attributes. A primary attribute is a main feature or variable in a dataset used to identify, organize, or analyze the data. It can be a key (like a unique ID), but it doesn't have to be unique. It helps in linking or blending different datasets. For example, in an employee database, 'Employee ID' is a primary key, while attributes like "Job Title" or "Department" could be considered primary attributes used for analysis but may not be unique.

Blending datasets based on a primary attribute integrates information from multiple tables, enriching the dataset, ensuring accuracy, enabling multi-dimensional analysis, and simplifying reporting by unifying data around a common key for more actionable insights.

Examples of Blending Analytics Datasets

The examples provided below are determined by a specific attribute that aligns with the focus of the analysis or report.

- Release Base and Release Advanced datasets - You could blend the release base and release advanced dataset on the Release attribute (primary attribute) to analyze data related to a software release which facilitates specific releases merged across datasets, ensuring all release-related data is consolidated.
- Release Phase Base and Release Phase Advanced datasets - You could blend the release phase base and release phase advanced datasets on the Phase attribute (primary attribute) to analyze data related to release phase which facilitates releases and release phases merged across datasets, to conduct phase by phase analysis.
- Release Task Base and Release Task Advanced datasets - You could blend the release task base and release task advanced datasets on the Task attribute (primary attribute) to analyze data related to release task which facilitates releases and release tasks merged across datasets, to track task status, such as in-progress, failed, and completed.

The table below outlines the data tables that can be blended. The row header and column header indicate the names of the data tables, while the intersecting cells specify the attributes used for blending.

Datasets	release_base	release_advanced	release_ic
release_base	NA	release_id, __sys_source_id	release_ic __sys_soi

Datasets	release_base	release_advanced	release_I
release_advanced	NA	NA	release_ic __sys_soi
release_phase_advanced	NA	NA	NA
release_tag_base	release_id, __sys_source_id	release_id, __sys_source_id	NA
release_task_tag_base	release_id, __sys_source_id	release_id, __sys_source_id	NA
release_environment_label_base	NA	NA	NA
release_team_advance	release_id, __sys_source_id	release_id, __sys_source_id	NA
release_dependent_advanced	release_folder_id, release_id, __sys_source_id	release_folder_id, release_id, __sys_source_id	release_fc release_ic release_p __sys_soi
release_dependency_advanced	release_folder_id, release_id, __sys_source_id	release_folder_id, release_id, __sys_source_id	release_fc release_ic release_p __sys_soi
release_multi_level_dependency_advanced	release_folder_id, release_id, __sys_source_id	release_folder_id, release_id, __sys_source_id	release_fc release_ic release_p __sys_soi

Stand Alone Datasets

- release_daily_snapshot
- release_weekly_snapshot
- release_task_daily_snapshot
- release_task_weekly_snapshot
- release_phase_daily_snapshot
- release_phase_weekly_snapshot
- release_task_type_deployments_base

What is Code Standardization

Learn how code standardization brings uniformity across datasets

What is Code Class

Explore the category of code values and how each code adds unique perspectives to data interpretation.

Code Standardization

Learn how Code Standardization page helps to view and edit the code classes available in a tenant including certain...

What is Code Standardization

Code standardization is essential in data management to ensure uniformity across datasets. Different sources may use different codes or labels for categories like status, priority, severity, and gender. Since the data lakehouse combines data from multiple sources into a single dataset for analysis, it needs to standardize these category values so they are uniformly understood. This process is called Code standardization. Digital.ai Analytics has standardized codes for these category values from different sources to ensure consistency.

For example, different departments might use various codes for the same status, such as "Active," "A," or "1." Without standardization, conforming and analyzing this data can cause inaccuracies. Standardizing these source codes or labels ensures smooth integration and comparison across sources.

The benefits include cleaner, more reliable data, improved analytics across sources, and efficient data integration. Standardized data ensures consistent reporting which is crucial for making informed, analytics-driven decisions.

Some Digital.ai sources allow the addition of custom categories or new source codes or labels to existing categories. When these are added, especially when new source codes are introduced to existing out-of-the-box categories or the meaning of custom source codes is modified, customer admins need to map the new or modified source codes/labels to the appropriate standardized codes for analytics.

This screen allows customer admins to perform this activity directly in the Digital.ai Platform UI.

What is Code Class

A code class refers to the category of code values or labels in the source, such as transaction status, transaction type, and task priority. Each code class adds unique perspectives to data interpretation, enriching analysis. For instance, by categorizing various status codes or labels into standardized values, you create a unified framework that supports the development of derived analysis (metrics, attributes), leading to meaningful and consistent insights across similar domain sources. This categorization process structures the data, making it easier to analyze and report, ensuring consistency and clarity in data representation and analysis.

Within the Digital.ai Platform, you can map a source code or label from a code class to a specific standardized value available in the selected account. You can also configure both the source and warehouse code classes and establish mappings between them as part of an advanced modeler profile. Alternatively, a source admin can simply map their existing category codes or labels to standardized values.

Each set of values specific to a source application is managed and stored in a single physical table known as the xds table. A Transformed Data Store (XDS) table typically refers to a table where data has been processed or transformed from its original format into a structured, usable format for analysis or storage.

Code Standardization

The Code Standardization page helps you view and edit the code classes that are available in a tenant.

The Code Standardization page has the following options:

- **Select source instance:** It enables you to choose the desired source instance to access code classes created within that specific environment. A source instance refers to a particular system or database from which data is extracted and integrated into the data warehouse environment.
- **Search code class:** It helps you to search for a code class.
- **Edit code class:** It helps you to edit a code class.

WARNING

You cannot create a code class within Digital.ai Platform. However, you can map codes according to your specific requirements.

You can view the following details of code classes in the Code Standardization page:

- Name of the xds table
- Name of the code class
- Mapping status
- Actions

Code class has the following three statuses:

- **All mapped:** represents that all codes are mapped. It is in green color.
- **Some mapped:** represents that some codes are mapped and some are unmapped. It is in amber color.
- **Unmapped:** represents that none of the codes are mapped. It is in grey.

Prerequisites:

Analytics authors can edit code classes in the Digital.ai platform. You can map the code classes with values that are available in the code class.

Searching code class

You can type a keyword in the **Search** field to search for a code class.

Editing code class

The edit code class feature  allows you to modify and manage predefined sets of values associated with attributes or fields within an application. This feature enables you with the flexibility to fine-tune and optimize the set of values associated with attributes or metrics. This capability enhances data management and boosts usage efficiency within the application. This feature has the following options:

- **Code Mapping:** Implementing a user-friendly interface for mapping codes to standard categories or statuses. You can easily identify and update mappings as needed.
- **Customization:** Offering options for customizing code class mapping based on specific organizational needs or industry standards, ensuring flexibility in data management.

Mapping code class

The code class page enables you to map source code classes to their corresponding value. For example, you can map the Assigned or New state of a source code class to an Open state of the same dimension class of the warehouse code class.

NOTE

Unmapping of code class is not supported. However, you can map a source code class to another warehouse code class.

Complete the following steps to edit the code class:

1. Click the edit button next to the code class.
2. Click **show only unmapped** to view only unmapped codes.

NOTE

Alternatively, you can search for a specific code by typing a keyword associated with the code you're looking for.

1. Select a standardized label from the drop-down menu next to the code to map it. You can map one or multiple codes simultaneously.
2. Click **Save**.

Map your source label

Map source labels to standardized labels

rel_release_task_type_class_x

Class name: RELEASE_TASK~TYPE

Code class

☒ show only unmapped

Q

Search

Source Label		Standardized Label
Source code: XLRELEASE.GATETASK	→	UNSPECIFIED Standardized code: UNSPECIFIED
Source code: XLRELEASE.GROOVYSCRIPTTASK	→	UNSPECIFIED Standardized code: UNSPECIFIED
Source code: XLRELEASE.SCRIPTTASK	→	UNSPECIFIED Standardized code: UNSPECIFIED

Rows per page: 10

1-3 of 3

<

>

Cancel

Save

Application Properties

Overview of the application properties.

Application Properties

Application properties is a set of configurable parameters or settings that define the behaviors, configurations, and environment-specific settings. These properties are tailored to the specific application and helps you customize various aspects of the application, such as application setup, calendar configuration, currency preferences, email settings, target modeling, timezone configuration, Data warehouse, ETL configuration, and so on.

Accessing Application Properties

You can access application properties from the Digital.ai Platform.

The Application Properties page helps you view and edit the properties that are available for an application.

Change Risk Prediction

CRP.Risk Predictors

Following are the CRP.Risk Predictors property group that helps you specify the columns that you want to use as predictors to predict change failures:

Name	Description	Value (Default)
01 Crp risk predictor	Risk Factor1	Assignee prior failure rate (last 180 days)
02 Crp risk predictor	Risk Factor2	Assignment group prior failure rate (last 180 days)
03 Crp risk predictor	Risk Factor3	Count of change tasks
04 Crp risk predictor	Risk Factor4	Lead time duration (days)
05 Crp risk predictor	Risk Factor5	Assignee prior changes
06 Crp risk predictor	Risk Factor6	Assignment group prior changes

Name	Description	Value (Default)
07 Crp risk predictor	Risk Factor7	Change impact
08 Crp risk predictor	Risk Factor8	Planned start day of week

PCS.Credit Score

The PCS.Credit Score property group enables you to specify properties to configure the Change Credit Score dashboard.

Name	Description	Value (Default)
01 Problem points bucket upper limit	Upper limit for point buckets for calculation of debit score. This is used as a filter to fetch Problems in last 120 Days by default	120
02 Problem default credit score	Default credit score for problem module	850
03 Problem minimum credit score	Minimum credit score for problem module	300
04 Problem normal deduction	Normal deduction for problem	25
05 Problem due date deduction	Due date deduction for problem	50
06 P1 Priority Open Problem deduction	P1 priority problem deduction for open problem	150
08 Problem avg age days upper limit	Average Age upper limit for Problem	5

Name	Description	Value (Default)
09. Ags for scoring no of problem implemented	Minimum number of problem implemented by an Assignment Group that have to be considered. Enter a value > 0	1

Release Premium

The following property group enables you to specify properties to configure the Release Premium offering:

Name	Description	Value (Default)
RELEASE_APPLICATION_IDEAL_DEPLOYMENT_FAILURE_RATE	Defines the ideal deployment failure rate to track applications in DAI Release source, used in Application Maturity Analysis Dashboard	0.05

Name	Description	Value (Default)
RELEASE_DEPENDENCY_TIME_ESTIMATE_HOURS_THRESHOLD	Time estimate for the dependency commencement or closure (in hours). For Example, to determine the numner of dependencies commencing or closing in next N hours. This value determines the value of N (example: 24.0)	120.0



Metadata Viewer

Metadata is data that describes other data. Metadata summarizes basic information about data that helps in searchi...

Metadata Viewer

Metadata is data that describes other data. Metadata summarizes basic information about data that helps in searching and working with particular instances of data. For example, author, date created, date modified, and file size are typical examples of a document's metadata.

Metadata Viewer as a feature provides the ability to view the metadata associated with a specific instance, which allows you to access information about data, gain a deeper understanding of the data and ensure that certain metadata are present and accurate.

Accessing Metadata Viewer

1. From the left navigation menu, click **Metadata viewer**.
2. In the Metadata viewer page, click **Select Source** drop-down and then select the required source.
3. Optional: You may change the view to tile or list using the icon.
4. Select the required entity to view the metadata details.
5. Select the respective tab for following details:
 - **Overview**: Provides details of all the columns within an entity.
 - **Keys and Indices**: Provides details of Keys and Indices of an entity.

Task Result: Access to all metadata related to an entity is available, including columns, keys, and indices.

Glossary

A list of terms that you may encounter while perusing this documentation or discussing the Digital.ai Platform.

Platform

A cloud-based hub that serves as the foundation for the entire Digital.ai ecosystem, providing a unified experience including integrated SSO, seamless user authentication, and more.

Digital.ai Identity

Unified identity management that allows users to seamlessly move between Digital.ai products and services. Also, the credentials used to log in to the Digital.ai Platform.

Account

An instance of the Digital.ai Platform dedicated to a specific customer, with a unique domain, users, data, and applications. Also known as a tenant.

Application

Any Digital.ai product or service (such as Intelligence or Continuous Testing) that is connected to the Platform in order to provide federated user access based on your IdP. Also known as a Client.

Single Sign-On (SSO)

An authentication method that allows users to log into multiple services and applications using the same credentials.

Identity provider (IdP)

A single sign-on service that owns and maintains a directory of user credentials and an authentication mechanism. For example, Azure AD or Okta.

Service provider

A web server that hosts a resource and provides access based on authentication information supplied by an identity provider. In this case, the Digital.ai applications such as Intelligence or Continuous Testing are considered service providers.

Identity broker

An intermediary service that connects a service provider to an identity provider. The Digital.ai Platform, and more specifically Digital.ai Identity, is the identity broker between your IdP and Digital.ai applications such as Intelligence or Continuous Testing.

Identity federation

A system of trust between two parties that links a user across each system without compromising security. As it relates to Digital.ai, the Platform handles user management by connecting to your IdP and then providing (federating) those users with access to your Digital.ai applications.

SAML

Security Assertion Markup Language (SAML) is an XML-based open standard for exchanging authentication data across different systems.

OIDC

OpenID Connect (OIDC) is a JSON-based open protocol that extends OAuth 2.0 to add authentication data and allow for multiple connections to one IdP.

Mappers

Mappers are used to map user attributes coming from external Identity Providers to attributes in the Digital.ai Platform, and to map attributes going from the Digital.ai Platform to Applications. You can add mappers to ensure that user attributes are correctly integrated with the Digital.ai Platform.

Copyright

The services, software, and related documentation provided under the Digital.ai Master Subscription Agreement ([located at](#)) ("Master Subscription Agreement"), and all other Digital.ai products (a list of such products is ([located at](#)) (<https://digital.ai/product-service-descriptions>))), are the intellectual property of and are owned by Digital.ai and/or its suppliers and affiliates. The structure, organization, and source code of such software, services, and related documentation are the valuable trade secrets and confidential information of Digital.ai and its suppliers and are protected by law, including but not limited to the copyright, trademark, patent, and trade secret laws of the United States and other countries or any other intellectual property laws, and by international treaty provisions.

During the Initial Term and any Extension Term(s) (collectively, the "Term") of your Master Subscription Agreement, Digital.ai grants you a revocable, non-transferable, non-exclusive license to use the services and any object code version of the software that you purchased or subscribed to in connection with the Master Subscription Agreement and that was provided by Digital.ai, and any documentation relating to the access, use, operation, or functionality of such software and such services (together, the "Licensed Software and Services") for your internal use only during the Term of the Master Subscription Agreement and solely for the purposes defined therein. The term "Licensed Software and Services" includes any updates, bug fixes, and versions provided to you by Digital.ai in connection with a support services entitlement or subscription license grant, but does not include any other Digital.ai software, services, or documentation not specified in the Master Subscription Agreement, except to the limited extent that such other software or services integrate with and are necessary to the functionality of the Licensed Software and Services.

Nothing in the Master Subscription Agreement or this disclaimer shall be understood to grant you any right, title, ownership, or interest in or to Licensed Software and Services (or any other of Digital.ai's software, services, or documentation), whether expressly, by implication, estoppel or otherwise, other than the aforementioned limited right for you to use the Licensed Software and Services. All copyrights, patents, trade secrets, trademarks, service marks, trade names, moral rights, confidential information, and other intellectual property and proprietary rights in the Licensed Software and Services provided by Digital.ai will remain the sole and exclusive property of Digital.ai or its licensors and suppliers, as applicable. All rights not expressly granted herein are reserved by Digital.ai and/or its licensors or suppliers.

Except as expressly permitted by your Master Subscription Agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, create derivative works of, license, transmit, distribute, exhibit, perform, publish, or display any part of the Licensed Software and Services, in any form, or by any

means. Reverse engineering, disassembly, or decompilation of the Licensed Software and Services, unless required by law for interoperability, is prohibited. Except to the extent expressly permitted by your Master Subscription Agreement, you may not assign, sublicense, rent, timeshare, loan, lease or otherwise transfer the Licensed Software or Services or your rights therein, or directly or indirectly permit any third party to use or copy the Licensed Software or Services.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is a service, software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS:

For U.S. Government End Users, the Licensed Software and Services are "Commercial Item(s)," as that term is defined at 48 C.F.R. Section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. Section 12.212 or 48 C.F.R. Section 227.7202, as applicable, pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. Consistent with 48 C.F.R. Section 12.212 or 48 C.F.R. Sections 227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

The Licensed Software and Services are developed for general use in a variety of information management applications. They are not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Digital.ai and its affiliates disclaim any liability for any damages caused by use of this service or software in dangerous applications.

Digital.ai and its logo are trademarks of Digital.ai Software, Inc. Other product or service names, slogans, or logos contained on Digital.ai's website and in the Licensed Software and Services (whether registered or unregistered in the U.S. or other countries) may be trademarks of Digital.ai and/or its subsidiaries, affiliates, suppliers, licensors, partners, or other third parties. This software and documentation may provide access to or information about content, products, and services from third parties. Digital.ai and its

affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Digital.ai. Digital.ai and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Digital.ai.

Attribution for OEM Use of Digital.ai Documentation

The information contained in any documentation to the Licensed Software and Services ("Documentation") is copyrighted and all rights are reserved by Digital.ai. Copying, duplicating, selling, or otherwise distributing any part of the Documentation without prior written consent of an authorized representative of Digital.ai is prohibited.