



# Citrix Secure Developer Spaces™

## Contents

|  |           |
|--|-----------|
| <b>Citrix Secure Developer Spaces™</b>                           | <b>4</b>  |
| <b>Getting Started</b>   | <b>4</b>  |
| <b>Architecture Diagram</b>                                      | <b>5</b>  |
| <b>Citrix Secure Developer Spaces Setup Guide</b>                | <b>6</b>  |
| <b>Setup Code Repository Applications</b>                        | <b>8</b>  |
| <b>Azure Dev Ops integration as Code Repository Provider</b>     | <b>9</b>  |
| <b>Bitbucket Cloud Integration as Code Repository Provider</b>   | <b>11</b> |
| <b>GitHub Integration as Code Repository Provider</b>            | <b>15</b> |
| <b>GitLab Integration as Code Repository Provider</b>            | <b>17</b> |
| <b>Configure Platform Login</b>                                  | <b>19</b> |
| <b>Google Configuration as Identity Provider (OIDC)</b>          | <b>21</b> |
| <b>Microsoft Azure Configuration as Identity Provider (OIDC)</b> | <b>28</b> |
| <b>OpenID Connect Configuration as Identity Provider (OIDC)</b>  | <b>32</b> |
| <b>SAML Service Provider</b>                                     | <b>33</b> |
| <b>Nginx Ingress Recommended Settings</b>                        | <b>34</b> |
| <b>Third Party Application Setup</b>                             | <b>35</b> |
| <b>Register JFrog as Third Party App</b>                         | <b>35</b> |
| <b>How to Use this Guide</b>                                     | <b>38</b> |
| <b>Platform Level</b>  | <b>39</b> |
| <b>Organizations</b>   | <b>40</b> |
| <b>Projects</b>  | <b>42</b> |
| <b>Overview Page</b>   | <b>43</b> |
| <b>Self-Served Developer</b>                                     | <b>46</b> |



|                                  |            |
|----------------------------------|------------|
| <b>Guest Developer</b>           | <b>50</b>  |
| <b>Project Owner</b>             | <b>52</b>  |
| <b>What Is a Workspace?</b>      | <b>57</b>  |
| <b>Workspaces Page</b>           | <b>58</b>  |
| <b>Create a Workspace</b>        | <b>59</b>  |
| <b>Manage Workspaces</b>         | <b>64</b>  |
| <b>Workspace Apps</b>            | <b>66</b>  |
| <b>Templates</b>                 | <b>69</b>  |
| <b>Coding in a Workspace</b>     | <b>71</b>  |
| <b>SSH Into Your Workspace</b>   | <b>73</b>  |
| <b>Resources Page</b>            | <b>92</b>  |
| <b>Code Repositories</b>         | <b>93</b>  |
| <b>Data Buckets</b>              | <b>95</b>  |
| <b>Secrets</b>                   | <b>97</b>  |
| <b>Connected HTTP Services</b>   | <b>99</b>  |
| <b>Connected SSH Services</b>    | <b>102</b> |
| <b>Container Images</b>          | <b>104</b> |
| <b>People Page</b>               | <b>109</b> |
| <b>Users</b>                     | <b>110</b> |
| <b>Access Control</b>            | <b>114</b> |
| <b>Audit Page</b>                | <b>120</b> |
| <b>Insights Page</b>             | <b>123</b> |
| <b>Resource Allocation</b>       | <b>123</b> |
| <b>Container Process Metrics</b> | <b>124</b> |

|                                      |            |
|--------------------------------------|------------|
| <b>Profile and Account Settings</b>  | <b>127</b> |
| <b>Profile Overview</b>              | <b>131</b> |
| <b>Integration</b>                   | <b>135</b> |
| <b>Configuration</b>                 | <b>138</b> |
| <b>Security</b>                      | <b>141</b> |
| <b>Organization General Settings</b> | <b>143</b> |
| <b>Workspace Settings</b>            | <b>145</b> |
| <b>General Settings</b>              | <b>150</b> |
| <b>Security Settings</b>             | <b>154</b> |
| <b>User Access Control</b>           | <b>158</b> |
| <b>Workspace Settings</b>            | <b>160</b> |
| <b>Resource Settings</b>             | <b>167</b> |
| <b>Analytics</b>                     | <b>168</b> |
| <b>Import and Export</b>             | <b>171</b> |
| <b>VDI Application</b>               | <b>171</b> |
| <b>Project General Settings</b>      | <b>172</b> |
| <b>Workspace Settings</b>            | <b>173</b> |
| <b>Help</b>                          | <b>178</b> |
| <b>REST API</b>                      | <b>178</b> |
| <b>IDE Troubleshooting Tool</b>      | <b>179</b> |

## Citrix Secure Developer Spaces™

August 26, 2025

Citrix Secure Developer Spaces, formerly known as Strong Network is a secure, cloud-based development environment (CDE) platform that enhances developer productivity while maintaining enterprise-grade security. It provides fast onboarding through preconfigured workspaces that are accessible from anywhere—ideal for hybrid and remote teams.

The platform helps protect source code, credentials, and data by eliminating local dependencies and enforcing strong access controls. Its container-based environments integrate with common DevOps tools, CI/CD workflows, and security models such as Zero Trust. Organizations can reduce costs associated with laptops, maintenance, and security software, while gaining real-time visibility and governance over the development lifecycle.

## Getting Started

August 29, 2025

### Overview

Citrix Secure Developer Spaces (SDS), formerly known as the Strong Network platform, is a secure, cloud-based development environment (CDE) designed to enhance developer productivity while maintaining enterprise-grade security. The platform's primary purpose is to streamline the provisioning and management of coding environments, allowing organizations to boost efficiency and collaboration among internal and external teams.

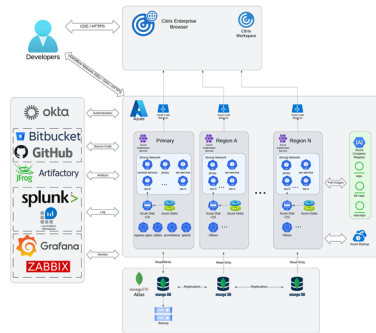
It provides fast onboarding through preconfigured, container-based workspaces that are accessible from anywhere, making it ideal for hybrid and remote teams. The platform can be deployed flexibly on public or private clouds and self-hosted servers, and it even supports fully air-gapped modes for high-security settings.

By centralizing development resources and eliminating local dependencies, SDS helps protect source code, credentials, and intellectual property. It enforces strong access controls and integrates with security models like Zero Trust, reducing the risk of data leaks and supporting DevSecOps practices.

Ultimately, the platform helps organizations reduce costs associated with high-spec laptops, maintenance, and security software, while gaining real-time visibility and governance over the development lifecycle. Its environments seamlessly integrate with common DevOps tools and CI/CD workflows to improve IT efficiency, developer productivity, and overall governance.

## Architecture Diagram

August 29, 2025



The architectural diagram of a CDE has the following components:

- One Kubernetes cluster with auto-scaling node and storage Container Storage Interface(CSI) driver capacity to host the SDS platform and workspace.
- A container registry
- MongoDB database
- Code repositories, for example, Bitbucket or GitHub
- Optional: Additional Kubernetes clusters set up in different regions to ensure global access with optimized network latency.
- Optional: An identity provider (SAML), such as Okta
- Optional: Observability
- Optional: Private access using Citrix Workspace, Enterprise Browser, or SPA

The key components of SDS - the Cloud Development Environment (CDE) Platform include Kubernetes clusters, a container registry, and a MongoDB database. You can leverage resources from any cloud service provider, use your hardware in a data center, or even use a hybrid.

The core components of the Azure-based sample deployment depicted in the architecture diagram above are:

- Azure Kubernetes Services for platform and regions
- Service node pool with two Standard\_D8as\_v5 VMs
- Workspace node pool with Standard\_D16as\_v5 VMs with auto-scaling
- Azure Container Registry
- Premium Tier
- Geo Replication peers
- MongoDB Atlas cluster
- M10 (2 GB RAM, 8 GB Storage) with auto-scaling
- Read-only nodes for regions

If you are not using Azure, you can choose from the following alternatives:

- Kubernetes Cluster:
  - Amazon Elastic Kubernetes Service
  - Google Kubernetes Engine
- Container Registry
  - Amazon Elastic Container Registry
  - Google Container Registry

**Note:**

Further deployment guidance and best practices can be found on [Citrix Tech Zone](#)

## Citrix Secure Developer Spaces Setup Guide

August 29, 2025

This repository contains various guides on how to set up the Citrix Secure Developer Spaces platform. It is intended for administrators of the platform.

Need help? [Support Center](#)

### Technical Requirements

- An AWS, Azure, GCP account or any on-prem Kubernetes (Openshift, Tanzu) deployment with appropriate permissions for cloud infrastructure
- Kubernetes cluster, version 1.20+, we can share the cluster with other applications (not recommended)
- Ingress gateway: we are using the Nginx ingress controller [Welcome - Ingress-Nginx Controller](#). NetScaler and Istio gateway are supported as well.

---

Network Policy: we are relying on the [networking.k8s.io/v1](#) API. If not available you can install: Calico ( [Project Calico

Tigera - Creator of Calico](<https://www.tigera.io/project-calico/>) ) or (Cilium) ([Cilium - Cloud Native, eBPF-based Networking, Observability, and Security](#) )

---

•

- Persistent Volume Claims API, for creating persistent volumes.
- In case of AWS, Amazon Linux should be used for Kubernetes nodes.

---

Helm CLI tool for deploying the product, we provide a helm chart to our customers.  
Installation guide: [Helm

Installing Helm](<https://helm.sh/docs/intro/install/>)

---

- 
- Two DNS domains with appropriate SSL certificates (optional but recommended for PoC deployment), one is a wildcard domain. We recommend the following: `example.com` and `*.proxy.example.com`
- For production deployments it is recommended to use a MongoDB Atlas subscription for database management, for PoC by default we deploy an internal MongoDB container
- For production deployments it is recommended to use an identity provider (SAML or OIDC), such as Okta, for identity and access management. Email/password identities

You should also be able to access the following URLs needed for the installation:

- Our license server is at: `api.enterprise.strong.network`  
It is used to get a license and generate a temporary access token to the artifactory where we store images. It is also possible to perform the installation (production or PoC) without having access to this endpoint and in that case we can supply you with an offline license.
- [europe-docker.pkg.dev/strong-network-release/images](https://europe-docker.pkg.dev/strong-network-release/images) is the artifactory URL hosted on GCP. We have mirrors in the US and Asia, if needed: [asia-docker.pkg.dev/strong-network-release/images](https://asia-docker.pkg.dev/strong-network-release/images) and [us-docker.pkg.dev/strong-network-release/images](https://us-docker.pkg.dev/strong-network-release/images)
- **gs://strong-network-helm-chart** (<https://storage.cloud.google.com/strong-network-helm-chart/>)  
It is a Google bucket where the helm chart is stored
- The installer itself is stored on dockerhub under our account: [https://hub.docker.com/r/strongnetwork/strong\\_installer](https://hub.docker.com/r/strongnetwork/strong_installer) (`docker pull strongnetwork/strong_installer`)

The exact list of URLs that you should be able to access is:

Helm chart package:

<https://storage.cloud.google.com/strong-network-helm-chart/ninjahchart-2025.5.4.tgz>

List of service images:

[europe-docker.pkg.dev/strong-network-release/images/browser\\_in\\_browser:2025.5.4](#)  
[europe-docker.pkg.dev/strong-network-release/images/cloud\\_editor\\_sidecar\\_proxy:2025.5.4](#)  
[europe-docker.pkg.dev/strong-network-release/images/frontend:2025.5.4](#)  
[europe-docker.pkg.dev/strong-network-release/images/sn\\_enterprise\\_bundle:2025.5.4](#)

Workspace Images:

[europe-docker.pkg.dev/strong-network-release/images/ws-images/android\\_studio:2.2.5](#)  
[europe-docker.pkg.dev/strong-network-release/images/ws-images/cloud\\_editor\\_generic:2.2.9](#)  
[europe-docker.pkg.dev/strong-network-release/images/ws-images/goland\\_go:2.2.5](#)  
[europe-docker.pkg.dev/strong-network-release/images/ws-images/intellij\\_java:2.2.5](#)  
[europe-docker.pkg.dev/strong-network-release/images/ws-images/intellij\\_ultimate:2.2.5](#)  
[europe-docker.pkg.dev/strong-network-release/images/ws-images/phpstorm\\_php:2.2.5](#)  
[europe-docker.pkg.dev/strong-network-release/images/ws-images/pycharm\\_python:2.2.5](#)  
[europe-docker.pkg.dev/strong-network-release/images/ws-images/webstorm\\_image:2.2.5](#)

Installer Image:

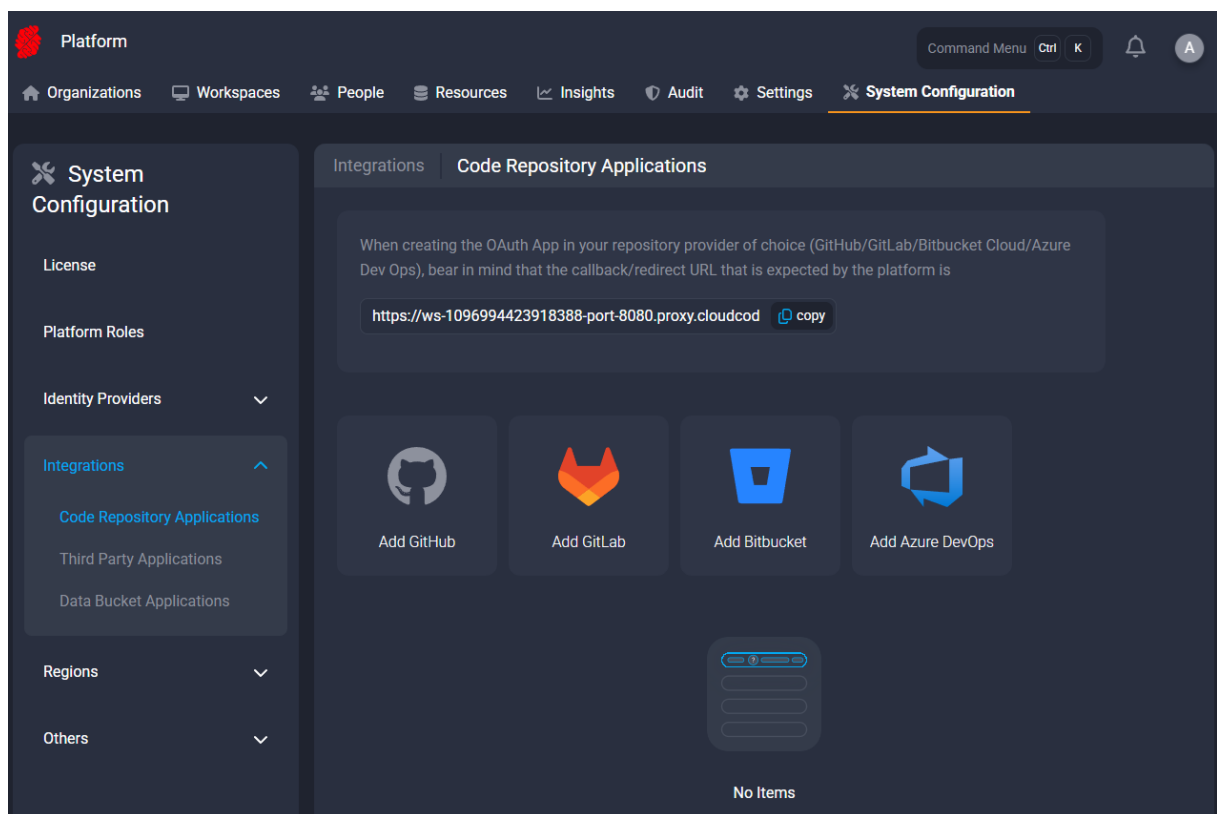
[strongnetwork/strong\\_installer:2025.5.4](#)

## Setup Code Repository Applications

August 28, 2025

This folder contains a list of guides on how to set up different code repositories:

- [GitHub](#)
- [GitLab](#)
- [Bitbucket](#)
- [Azure DevOps](#)



## Azure Dev Ops integration as Code Repository Provider

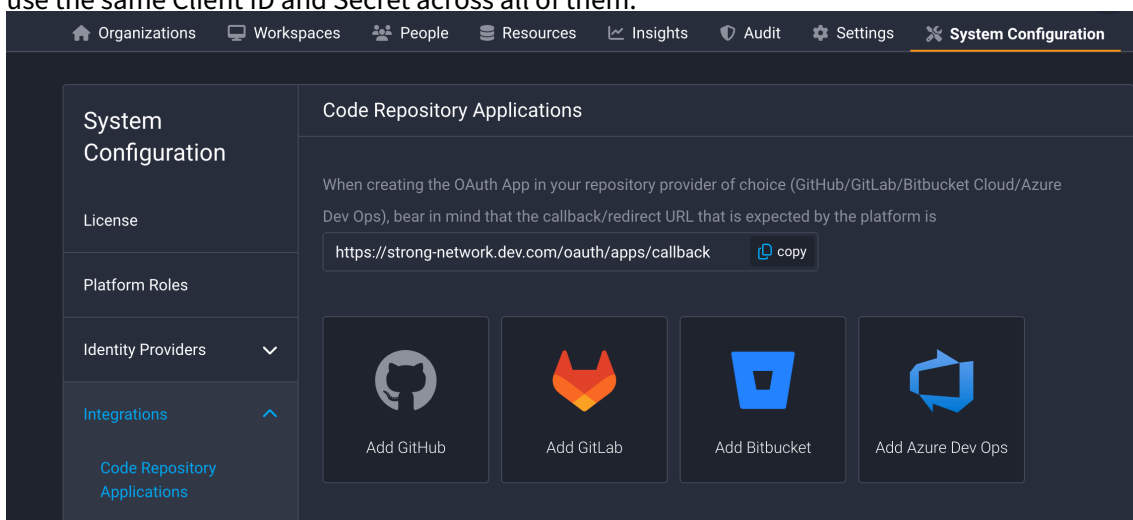
August 28, 2025

Follow these steps to create an OAuth App in Azure DevOps to connect it to the platform.

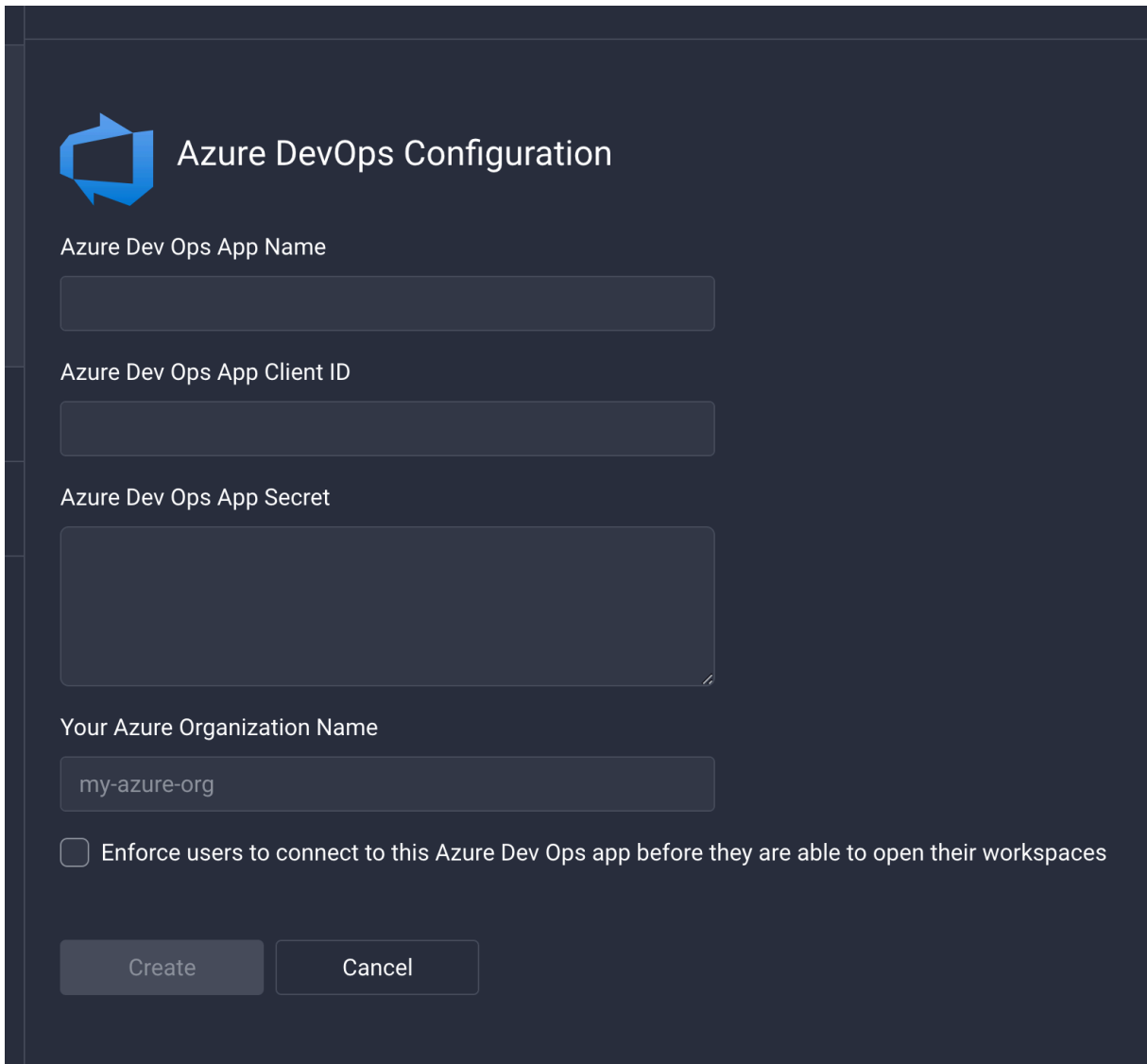
- Using an Azure DevOps account, go to the following link:  
[Register an application](#)
- Click on the “Add consumer” button and set the following fields:
  - **Company Name:** Your company’s name.
  - **Application Name:** The name you want to give to the application. It will be public.
  - **Application Website:** Set to <https://example.com/oauth/apps/callback> (replace [example.com](https://example.com) with the proper domain name).
  - **Authorization Callback URL:** Set to <https://example.com/oauth/apps/callback> (replace [example.com](https://example.com) with the proper domain name). This URL can be found in the admin panel of the Strong Network platform.
  - **Authorized Scopes:** [Code \(read and write\)](#) and [Project and team \(read\)](#).



- Once done, click the “Create Application” button. You will be presented with the Client ID (called App ID) and the Secret (called Client Secret) after clicking the “Show” button. Enter these fields in the Admin configuration of the Strong Network™ platform.
  - [Register an application](#)
  - `https://example.com/oauth/apps/callback`
- Specify the Azure Organization name. This application can only access repositories under this specific organization. To access repositories from different organizations, create multiple Azure DevOps Code Repository Applications, each with its corresponding organization name. You may use the same Client ID and Secret across all of them.



Paste Client ID, App Secret and Organization name from steps above:



The screenshot shows a dark-themed dialog box titled "Azure DevOps Configuration". It features the Azure DevOps logo (a blue square with a white 'A' and a blue arrow) on the left. The form contains four input fields: "Azure Dev Ops App Name", "Azure Dev Ops App Client ID", "Azure Dev Ops App Secret" (a larger text area), and "Your Azure Organization Name" (which contains the text "my-azure-org"). Below these fields is a checkbox labeled "Enforce users to connect to this Azure Dev Ops app before they are able to open their workspaces". At the bottom are two buttons: "Create" and "Cancel".

## Bitbucket Cloud Integration as Code Repository Provider

August 28, 2025

Follow these steps to create an OAuth App in Bitbucket Cloud to connect it to the platform:

- **Navigate to OAuth Consumers:**
  - Using a Bitbucket account, go to the main organization settings and then to “OAuth consumers”
  - You can follow this [https://bitbucket.org/\[YOUR\\_DOMAIN\\_NAME\]/workspace/settings/api](https://bitbucket.org/[YOUR_DOMAIN_NAME]/workspace/settings/api) to reach this menu directly.

- **Add a New Consumer:**

- Click on the “Add consumer” button and set the following fields:
  - **Name:** The name you want to give to the application. It will be public.
  - **Callback URL:** The URL should have a structure similar to <https://example.com/oauth/apps/callback>, where “example.com” should be replaced with the proper domain name. This URL can be seen from the admin panel of the Strong Network platform.
  - **This is a private consumer:** This should already be selected by default; leave it as it is.
  - **Scopes:** Select “Read” under the Account section and “Write” under the Repositories section. This can also be checked in the Strong Network™ Platform when clicking the “Add Bitbucket” button.

- **Complete the Registration:**

- After clicking the “Save” button, you will be presented with the Client ID (called Key) and Secret, which you need to enter in the platform configuration.

## Bitbucket Server or Data Center Integration as Code Repository Provider

In this section, we will see how to connect the Strong Network platform to a self-hosted Bitbucket instance:

- **Configure Strong Network Platform:**

- Go to the Strong Network platform settings and open the “Code Repository Applications” menu.
- Click on the “Add Bitbucket” button.
- Select the checkbox for “Bitbucket Server or Data Center (self-hosted)”.

- **Set the Following Fields:**

- **Bitbucket App Name:** It can be anything. This is what users will see when using this Code Repository Provider.
- **Custom Domain:** Enter the URL where the Bitbucket instance is hosted. If no scheme is given, HTTPS will be chosen by default.
- **Enforce Users to Connect:** If selected, users will need to connect to Bitbucket before they can open their workspaces. This can prevent misconfiguration/permission issues on the user side.

- **Complete the Registration:**

- Click the “Create” button to complete the configuration on the Strong Network platform side.
- Save the “Bitbucket Server Public Key” for later use. This can also be found in the edit menu after clicking the “Create” button.

- **Configure Bitbucket Instance (Version 7.20 or Later):**

- Go to Administration > Applications > Application Links and click on “Create link”:
  - **Application Type:** External application
  - **Direction:** Incoming
  - Click on continue
  - Set a unique name
  - **Redirect URL:** Set to <https://example.com/oauth/apps/callback>, where “example.com” should be replaced with the proper domain name.
  - **Application Permissions:** Account: Write, Repositories: Admin
  - After clicking the “Save” button, enter “strong\_network” for both Client ID and Client Secret.

- **Configure Bitbucket Instance (Version 7.20 or Earlier):**

- Go to Administration > Application Links.
- Enter the platform URL (e.g., <https://example.com>, where “example.com” should be replaced with the proper domain name).
- Click on “Create new link”. If you see a “No response received” error, ignore it and click Continue.
- In the following menu, enter:
  - **Application Name:** It can be anything.
  - **Application Type:** Generic Application
  - **Service Provider Name:** It can be anything (recommended: “strong\_network”).
  - **Consumer Key:** Set to “strong\_network”.
  - **Shared Secret:** Set to “strong\_network”.
  - **Request Token URL:** Set to <http://example.com>, where “example.com” should be replaced with the proper domain name.
  - **Access Token URL:** Set to <http://example.com>, where “example.com” should be replaced with the proper domain name.
  - **Authorize URL:** Set to <http://example.com>, where “example.com” should be replaced with the proper domain name.
  - Check “Create incoming link” and click Continue.

## Link applications

You are creating a link from:

 **Application URL:** http://18.197.156.97:7990

**Name:** Bitbucket

**Application:** Bitbucket Server

To this application:

**Application URL:** https://banana.conceptcloud.network

|                       |  |
|-----------------------|--|
| Application Name*     | <input type="text" value="My new application"/>                  |
| Application Type*     | <input type="text" value="Generic Application"/>                 |
| Service Provider Name | <input type="text" value="strong_network"/>                      |
| Consumer key          | <input type="text" value="strong_network"/>                      |
| Shared secret         | <input type="text" value="strong_network"/>                      |
| Request Token URL     | <input type="text" value="https://banana.conceptcloud.network"/> |
| Access token URL      | <input type="text" value="https://banana.conceptcloud.network"/> |
| Authorize URL         | <input type="text" value="https://banana.conceptcloud.network"/> |
| Create incoming link  | <input checked="" type="checkbox"/>                              |


**Continue**

Cancel

- In the following menu, enter:
  - **Consumer Key:** Set to “strong\_network”.
  - **Consumer Name:** Set to “strong\_network”.
  - **Public Key:** Enter the value that can be seen in the platform.

## Link applications

You are creating a link from:

 **Application URL:** http://18.197.156.97:7990

**Name:** Bitbucket

**Application:** Bitbucket Server

To this application:

**Application URL:** https://banana.conceptcloud.network

**Consumer Key\***

**Consumer Name\***

**Public Key\***

**Continue**

Cancel

- **Complete the Configuration:**
- Click on Continue. The configuration is complete.

## GitHub Integration as Code Repository Provider

August 28, 2025

Follow these steps to create an OAuth App in GitHub to connect it to the platform:

- **Navigate to Developer Settings:**
- Using a GitHub account, go to its settings and then to “Developer settings”.
- Inside this menu, click on “OAuth Apps”.
- You can follow this <https://github.com/settings/developers> to reach this menu directly.

[Settings](#) / Developer settings

|                        |
|------------------------|
| GitHub Apps            |
| <b>OAuth Apps</b>      |
| Personal access tokens |

### No OAuth applications

OAuth applications are used to access the GitHub API. [Read the docs](#) to find out more.

**Register a new application**

- **Register New Application:**

- Click on “Register new application” and you will be presented with a screen to set:
  - **Application Name:** At your discretion.
  - **Homepage URL:** The main route of the domain where the platform is running.
  - **Authorization Callback URL:** The URL should have a structure similar to <https://example.com/oauth/apps/callback>, where “example.com” should be replaced with the proper domain name (same as the Homepage URL).

## Register a new OAuth application

---

Application name \*

Your application name

Something users will recognize and trust.

Homepage URL \*

<https://example.com>

The full URL to your application homepage.

Application description

Application description is optional

This is displayed to all users of your application.

Authorization callback URL \*

<https://example.com/oauth/apps/callback>

Your application’s callback URL. Read our [OAuth documentation](#) for more information.

Register application

Cancel

- 
- **Complete the Registration:**
    - When this process is done, click on the green button “Register application”.
    - You will be redirected to a new application page where you can see the Client ID and generate the Secret that needs to be set in the platform configuration.
  - **Give Organization Access:**

- You will need to grant the organization access to this newly created OAuth app in the organization you want to connect to the platform.

## GitLab Integration as Code Repository Provider

August 28, 2025

Follow these steps to create an OAuth App in GitLab to connect it to the platform:

- **Navigate to Applications:**
  - Using a GitLab account, go to user settings and then to “Applications”.
  - You can follow this [https://gitlab.com/-/user\\_settings/applications](https://gitlab.com/-/user_settings/applications) to reach this menu directly.
- **Create a New OAuth App:**
  - Click on “New application” and set the following fields:
    - **Name:** The name you want to give to the application. It will be public.
    - **Redirect URI:** The URL should have a structure similar to <https://example.com/oauth/apps/callback>, where “example.com” should be replaced with the proper domain name.
    - **Confidential:** This should already be selected by default; leave it as it is.
    - **Scopes:** Add the [api](#) and [write\\_repository](#) scopes. These are needed to automatically deploy deployment keys.



User Settings &gt; Applications

## Applications

Manage applications that can use GitLab as an OAuth provider, and applications that you've authorized to use your account.

### Add new application

#### Name

#### Redirect URI



Use one line per URI

#### ☒ Confidential

Enable only for confidential applications exclusively used by a trusted backend server that can securely store the client secret. Do not enable for native-mobile, single-page, or other JavaScript applications because they cannot keep the client secret confidential.

#### Scopes

##### ☒ api

Grants complete read/write access to the API, including all groups and projects, the container registry, and the package registry.

##### ☐ read\_api

Grants read access to the API, including all groups and projects, the container registry, and the package registry.

##### ☐ read\_user

Grants read-only access to the authenticated user's profile through the /user API endpoint, which includes username, public email, and full name. Also grants access to read-only API endpoints under /users.

##### ☐ read\_repository

Grants read-only access to repositories on private projects using Git-over-HTTP or the Repository Files API.

##### ☒ write\_repository

Grants read-write access to repositories on private projects using Git-over-HTTP (not using the API).

##### ☐ read\_registry

Grants read-only access to container registry images on private projects.

##### ☐ write\_registry

Grants write access to container registry images on private projects.

##### ☐ sudo

Grants permission to perform API actions as any user in the system, when authenticated as an admin user.

##### ☐ admin\_mode

Grants permission to perform API actions as an administrator, when Admin Mode is enabled.

##### ☐ openid

Grants permission to authenticate with GitLab using OpenID Connect. Also gives read-only access to the user's profile and group memberships.

##### ☐ profile

Grants read-only access to the user's profile data using OpenID Connect.

##### ☐ email

Grants read-only access to the user's primary email address using OpenID Connect.

[Save application](#)

- **Complete the Registration:**

- After clicking the “Save application” button, you will be presented with the Client ID (called Application ID) and Secret, which you need to enter in the platform configuration.

User Settings > Applications > Your application name

The application was created successfully. 

×

Q

 Search page

Application: Your application name

Application ID

9d5355d72e8319cc6c972d4

Secret

Copy

 This is the only time the secret is accessible. Copy the secret and store it securely.

Callback URL

https://example.com/oauth/apps/callback

Confidential

Yes

Scopes

- **api** (Access the authenticated user's API)
- **write\_repository** (Allows read-write access to the repository)

Continue

Edit

Destroy

## Configure Platform Login

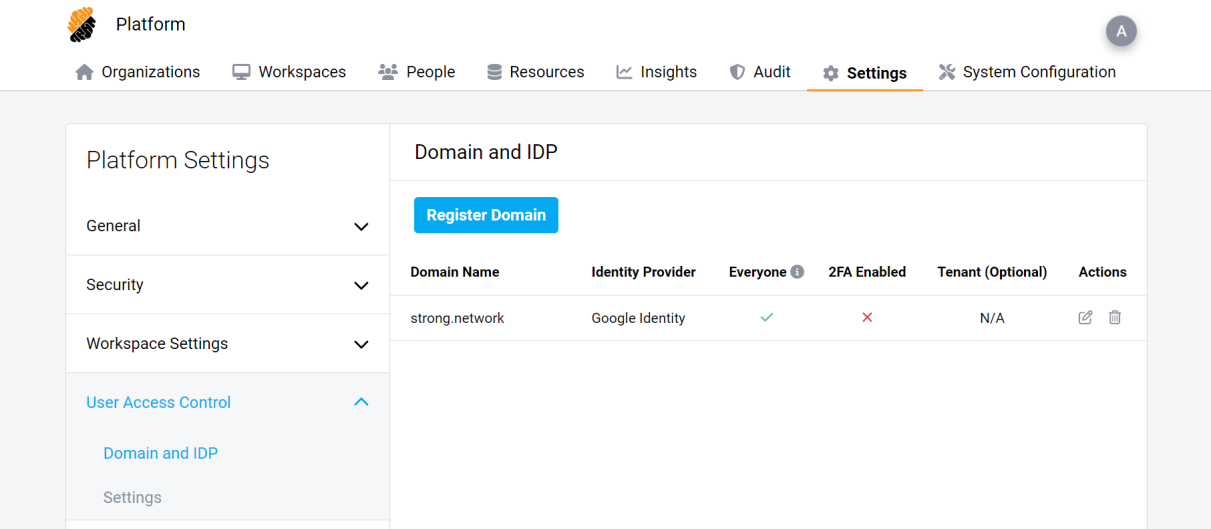
August 28, 2025

### Configure Login for Users

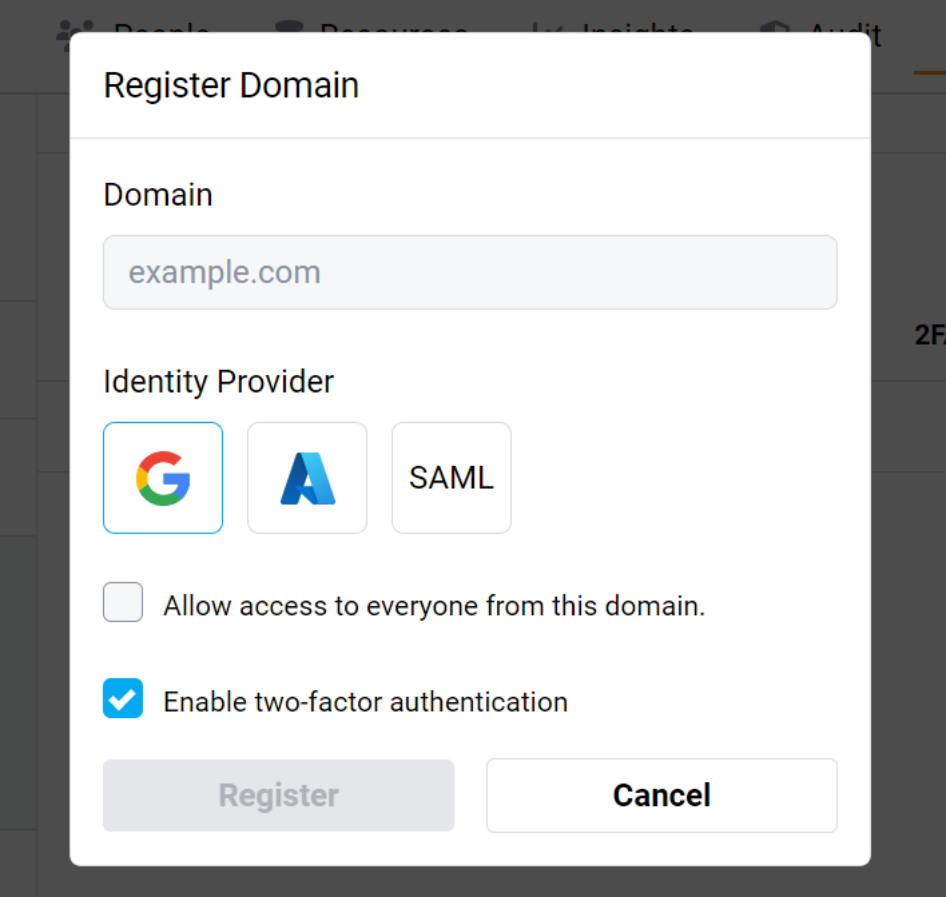
There are five ways users can log in to the platform:

- Google OAuth provider
- Microsoft OAuth provider (Azure)
- SAML
- OpenID Connect
- Username and password

After configuring the Identity Provider of choice (any of the first 4 options), it can be used to authenticate users of specified domains. These can be configured under User Access Control, in the submenu “Domain and IDP”.



If a domain is added, it means that when adding a user to the platform, that user will authenticate using the chosen Identity Provider.



In this menu, you may choose to check “Allow access to everyone from this domain” which will create user accounts on the fly, without the need to create the account beforehand. This is called Just-in-Time provisioning. This new user will not have any organization or project assigned to them.

You may also enable two-factor authentication which will use OTP on any user from the specified domain. If two-factor authentication is desired, we recommend setting it up either in your Identity Provider or in the platform to avoid asking the user to do the process twice.

## Google Configuration as Identity Provider (OIDC)

August 28, 2025

To create an OAuth Client to use Google as an Identity Provider, follow these steps to obtain the OAuth Client ID and Secret required in the platform configuration:

- Go to the [Google API Console](#) and create a new project (or use an existing one). The project name, organization, and location are left at your discretion.

Google APIs

New Project

You have 9 projects remaining in your quota. Request an increase or delete projects. [Learn more](#)

[MANAGE QUOTAS](#)

Project name \*

My Project 64161

Project ID: macro-aurora-305709. It cannot be changed later. [EDIT](#)

Organisation \*

No organisation

Select an organisation to attach it to a project. This selection can't be changed later.

Location \*

BROWSE

Parent organisation or folder

CREATE

CANCEL

- Inside the project, click on “+ Create Credentials” and select “OAuth client ID” from the submenu.

☰

Google APIs

ManualProject ▼

API

APIs & Services

Dashboard

Library

Credentials

OAuth consent screen

Domain verification

Page usage agreements

Credentials

[+ CREATE CREDENTIALS](#)

🗑️ DELETE

Create credentials to access your enabled APIs. [Learn more](#)

⚠️ Remember to configure the OAuth consent screen with information about your application.

API keys

☐

Name

Creation date

No API keys to display

OAuth 2.0 Client IDs

☐

Name

Creat

No OAuth clients to display

Service Accounts

☐

Email

No service accounts to display

- You will be presented with a warning to first configure an OAuth consent screen. Click on it. Select an external consent screen and click create. Fill in the fields at your discretion. The app name will be seen by users trying to log in to the platform.

## App domain

To protect you and your users, Google only allows apps using OAuth to use Authorised Domains. The following information will be shown to your users on the consent screen.

Application home page

Provide users a link to your home page

Application privacy policy link

Provide users a link to your public privacy policy

Application Terms of Service link

Provide users a link to your public Terms of Service

## Authorised domains

When a domain is used on the consent screen or in an OAuth client's configuration, it must be pre-registered here. If your app needs to go through verification, please go to the [Google Search Console](#) to check if your domains are authorised. [Learn more](#) about the authorised domain limit.

[+ ADD DOMAIN](#)

## Developer contact information

Email addresses \*

These email addresses are for Google to notify you about any changes to your project.

[SAVE AND CONTINUE](#)

CANCEL

- In the authorized domain, specify the domain in which the platform is deployed.
- Click on “Save and Continue” in the following menus without adding anything until you reach the summary page, then click on “Back to Dashboard”.
- Click on “Publish App”.

## OAuth consent screen

eeee  EDIT APP

### Publishing status

Testing

PUBLISH APP

### User type

External 

MAKE INTERNAL

### Test users

While publishing status is set to 'Testing,' only test users are able to access the app. Allowed user cap prior to app verification is 100, and is counted over the entire lifetime of the app. [Learn more](#)

+ ADD USERS

 0 users (0 test, 0 other) / 100 user cap 

- Return to the Credentials page and create the credentials for an OAuth client ID.
- On this page, set the application type to “Web application”. The name is left at your discretion.
- In “Authorised JavaScript origins”, specify the domain name in which the platform is deployed. In “Authorised redirect URIs”, enter the redirect URL, similar to:



- <https://example.com/oauth/callback>
- Where “example.com” should be set to the proper domain name.



Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information.

Application type \*

Web application

[Learn more](#) about OAuth client types

Name \*

Web client 1

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.



The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorised domains](#).

Authorised JavaScript origins ?

For use with requests from a browser

URIs

https://example.com

+ ADD URI

Authorised redirect URIs ?

For use with requests from a web server

URIs

https://example.com/oauth/callback

+ ADD URI

CREATE

CANCEL

- Click on “Create” and note the Client ID and Secret for the platform configuration.

## OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services



OAuth is limited to 100 [sensitive scope logins](#) until the [OAuth consent screen](#) is verified. This may require a verification process that can take several days.

Your Client ID



Your Client Secret



OK





## Microsoft Azure Configuration as Identity Provider (OIDC)

August 28, 2025

The platform supports integration with Azure Active Directory for logging in with your Microsoft Azure account. To configure it:




















- Go to the [Microsoft Azure portal](#).
- Navigate to the Azure Active Directory.




-  Overview
-  Getting started
-  Preview hub
-  Diagnose and solve problems

## Manage

---

-  Users
-  Groups
-  External Identities
-  Roles and administrators
-  Administrative units
-  Enterprise applications
-  Devices
-  App registrations
-  Identity Governance
-  Application proxy
-  Licenses
-  Azure AD Connect
-  Custom domain names
-  Mobility (MDM and MAM)
-  Password reset
-  Company branding
-  User settings
-  Properties
-  Security

- Click on “App registrations” and then “New registration”. Set the following:
- **App name:** Choose a name that will be publicly visible to users logging into the platform.
- **Supported account types:** We recommend selecting “Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g., Skype, Xbox)” to allow registered users to log in with their public domain accounts.
- **Redirect URI:** Set the selector to “Web” and enter a URI similar to `https://example.com/oauth/callback`.


 Microsoft Azure

[Home](#) > [Directorio predeterminado](#) >

## Register an application

**\* Name**

The user-facing display name for this application (this can be changed later).



**Supported account types**

Who can use this application or access this API?

☐ Accounts in this organizational directory only (Directorio predeterminado only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)


☒ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)


☐ Personal Microsoft accounts only

[Help me choose...](#)

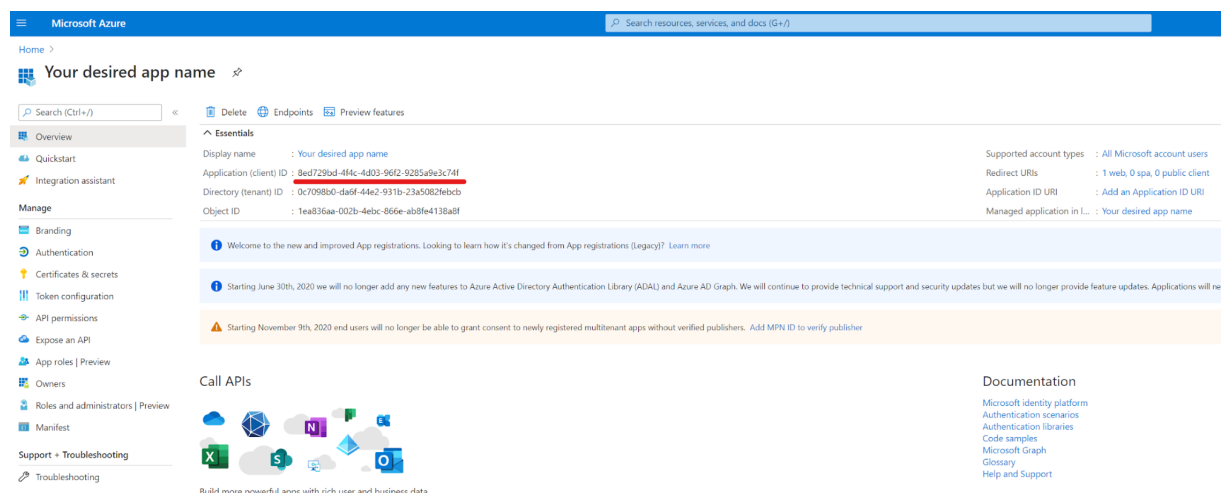
**Redirect URI (optional)**

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.



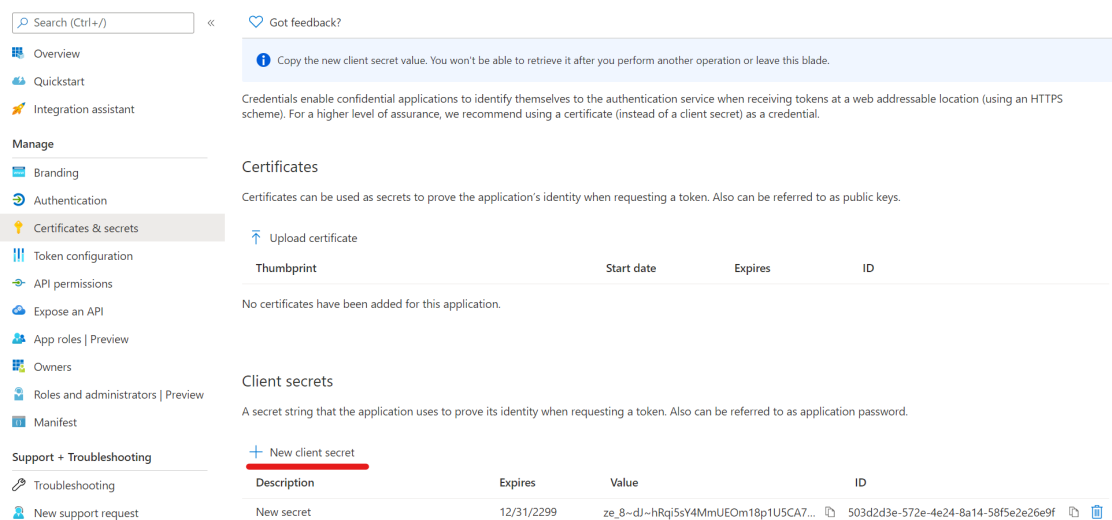


- Click on “Register” at the bottom.
- On the next page, note the OAuth Client ID for the platform configuration.



- To obtain the secret, go to “Certificates & secrets” of the newly created app and click on “New client secret”.

🔑 Your desired app name | Certificates & secrets ✕



## Single Logout (SLO) for Microsoft Azure

To enable Single Logout for the OIDC flow with Azure, configure the following:

- To log out users from Microsoft when they log out of the Strong Network™ platform, add another URL in the Redirect URI section with just the domain name used by the Strong Network platform. This URL is used to redirect users back after they log out of their Microsoft accounts.
- Add the optional claim called “login\_hint” to the ID token:
- Go to “Token configuration” and click on “Add optional claim”.
- Select ID as token type and then select “login\_hint”.

- To log the user out of the Strong Network platform when they log out of their Microsoft account, add the optional claim called “sid” to the ID token type.
- Add a Logout URL under the “Authentication” menu with the structure [https://\[domain\\_name\]/auth/logout](https://[domain_name]/auth/logout), where [domain\\_name](#) is the domain under which you have the Strong Network platform. This endpoint will be called by Microsoft when a user logs out to also log out the user from the Strong Network platform.

## OpenID Connect Configuration as Identity Provider (OIDC)

August 28, 2025

This platform supports integration with OpenID Connect for logging in.

### Registering the Application

- Go to the OpenID Provider’s Developer Portal.
- Navigate to the Applications or Clients section.
- Click on “Create New Application” or equivalent. Set the following:
  - **App Name:** Choose a name that will be displayed to users logging in.
  - **Application Type:** Select “Web Application”.
  - **Redirect URIs:** Add the following URI to handle login redirects: <https://example.com/oauth/callback>
  - **Logout Redirect URI:** Add the following URI to handle logout redirects: <https://example.com/auth/logout>
- Save the application.

Note the Client ID and Client Secret generated during this process. These will be required for platform configuration.

### Configuring Scopes and Claims

Under the Scopes or Permissions section of your application, ensure the following scopes are included:

- [openid](#)
- [email](#)
- [profile](#)
- Any additional scopes your platform requires.

Configure claims if necessary. Common claims include:

- **sub**: Unique identifier for the user.
- **email**: User's email address.
- **name**: Full name of the user.
- **preferred\_username**: Username or handle.

## Enabling Single Logout (SLO)

To enable Single Logout (SLO) for OpenID Connect:

Navigate to the Advanced Settings or Logout Configuration section.

Enable Single Logout if supported by the provider.

Add the Logout Redirect URI configured earlier:

<https://example.com/auth/logout>

Optionally, add the following claims to the ID token:

- **sid**: Session identifier.
- **logout\_hint**: Provides context for logging out.

## SAML Service Provider

August 28, 2025

To seamlessly onboard your users already registered in Okta to the Strong Network Platform using the SAML 2.0 protocol, follow these steps:

- **Configure Your SAML Identity Provider:**

- **Single Sign-On URL**: Set to [http\(s\)://example.strong.network/saml/acs](http(s)://example.strong.network/saml/acs) where “example.strong.network” is the domain where the platform is deployed.
- **Audience URI**: Set to [http\(s\)://example.strong.network/saml/metadata](http(s)://example.strong.network/saml/metadata)
- **Attribute Statements**:
- **email**: This attribute is mandatory, and the configuration won't work without it.
- **firstName**: Optional; if not set, the email will be used as the username.
- **lastName**: Optional; if not set, the email will be used as the username.

- **Configure the Strong Network™ Platform:**

- Log in to the platform as the administrator.



- Navigate to `http(s)://example.strong.network/platform/system_configuration/saml_sp` or click on System Configuration -> SAML Service Provider Configuration.
- Click on the “Configure” button to upload the metadata of your SAML Identity Provider. You can upload it either through a metadata URL or by uploading a .xml file.

## Security Assertion Markup Language (SAML) Configuration

|  |         |
|--|---------|
| Identity Provider Metadata URL           | Not Set |
| Service Provider Metadata URL            | Not Set |
| SSO URL (Assertion Consumer Service URL) | Not Set |

[Configure](#)

Below are the attributes that are needed to configured for the identity provider to be set up properly.

| Attribute                | Type        | Description  |
|--------------------------|-------------|--|
| <code>email</code>       | Required    | The user email that is used for registration on the platform.  |
| <code>displayName</code> | Recommended | The user's display name shown on the platform. When empty, attributes <code>firstName</code> and <code>lastName</code> are used instead. |
| <code>uid</code>         | Optional    | A unique identifier, usually provided for cross-platform traceability of user's operations.  |
| <code>firstName</code>   | Optional    | First name of the user, only used if <code>displayName</code> is empty.  |
| <code>lastName</code>    | Optional    | Last name of the user, only used if <code>displayName</code> is empty.   |

The SAML configuration is now complete and ready to use.

## Nginx Ingress Recommended Settings

August 28, 2025

This is a recommended Nginx configuration to speed up the platform in customer deployments. A default configmap exists in the `ingress-nginx` namespace, typically named `ingress-nginx-controller`. The name may vary depending on how the ingress was installed on the cluster.

```
1 kubectl edit configmap ingress-nginx-controller
```

The configmap data:

```
1 apiVersion: v1
2 data:
```

```
3 allow-snippet-annotations: "true"
4 enable-brotli: "true"
5 keep-alive: 120s
6 keep-alive-requests: "10000"
7 use-gzip: "true"
8 use-http2: "true"
9 kind: ConfigMap
```

## Third Party Application Setup

August 28, 2025

[Jfrog Integration Setup](#)

## Register JFrog as Third Party App

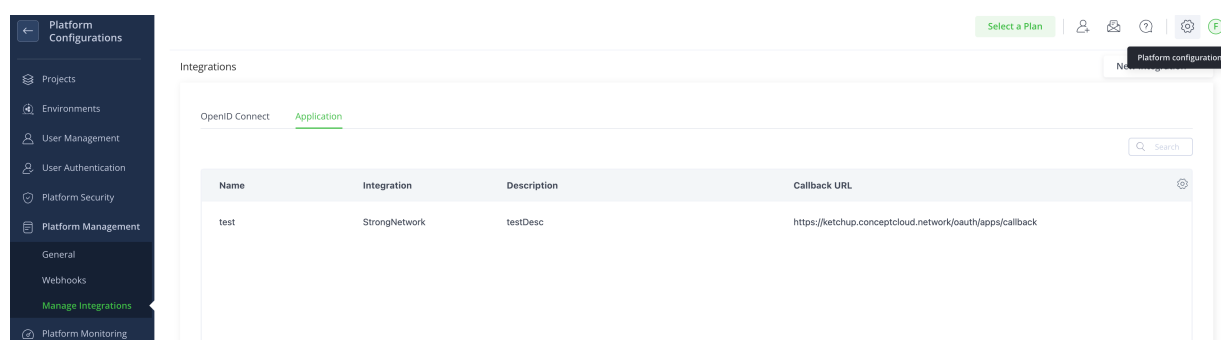
August 28, 2025

You can follow these steps to connect your JFrog instance and the Strong Network™ Platform.

At the moment this configuration can only be done in self-hosted JFrog instances or by asking the JFrog support team in the SaaS version.

Log in to your JFrog deployment as the admin go to Platform Management, then Manage Integrations. Go to the tab called “Application”. You can also follow the link:

[https://\[your\\_domain\\_name\].jfrog.io/ui/admin/configuration/integrations](https://[your_domain_name].jfrog.io/ui/admin/configuration/integrations)



Click on “New Integration” of type “Application” and fill in the following fields:

- **Application Name:** Up to you.
- **Application Type:** Select the template you added in the values.yaml file.

- **Description:** Up to you.
- **Callback URL:** You can find it in the Third Party Applications admin menu in the Strong Network platform and has the format of `https://[your_strong_network_domain]/oauth/apps/callback`

## Create New Application Integration

\* Application Name  
StrongNetwork

\* Application Type  
StrongNetwork

Description  
My Strong Network OAuth app

Callback URL  
https://ketchup.conceptcloud.network/oauth/apps.

Client ID and Secret  
[Generate Client ID & Secret](#)

Click on **Generate Client ID & Secret** and copy the values.

Lastly, log in as admin in the Strong Network Platform, go to System Configuration → Third Party Applications, and select JFrog. You will need to introduce:

- **Name:** Up to you, it will be displayed to the platform users
- **Client ID and Secret:** Values copied from JFrog
- **Domain:** Your JFrog domain

You can choose if you want the platform to trust insecure TLS certificates in case your JFrog deployment doesn't have a valid certificate. You may also want users to always connect to JFrog before they access their workspaces, in this case, they will get a popup where they have to connect before opening them. If you don't select this option they will get the popup but can dismiss it.

JFrog App Name

My JFrog

JFrog App Client ID

app@g4y544tg45g54yu6u67

✓

JFrog App Secret

mysecret

✓

JFrog Domain


strongnetworktest2.jfrog.io

☐ Trust insecure TLS Certificates (self-signed)

☐ Enforce users to connect to JFrog before they are able to open their workspaces

Create

Cancel



When the application is configured you can edit it by clicking on the edit icon on the right side.

System Configuration

License

Platform Roles

Identity Providers

Integrations

Code Repository Applications

Third Party Applications



Data Bucket Applications

Third Party Applications

When creating the JFrog App integration, bear in mind that the redirect URL that is expected by the platform is

https://strong-network.dev.com/oauth/apps/callback

copy

| App Name | Client ID  | JFrog Domain |   |
|----------|------------|--------------|---|
| JFrog1   | ferferfefe | test.com     |   |

Close

You will see a menu in which you can change some settings. In said menu, you may change the default JFrog startup script. This is a script that will run in every workspace that is owned by a user who has connected their JFrog account. It can be useful to set up specific configurations in all workspaces, for example, to configure the different programming languages to fetch the dependencies from your JFrog platform. Each user can build on top of this script, to customize it to their own needs.

If this default script is updated it will be automatically changed for users who haven't defined their custom script.

The screenshot shows the 'Configuration' page for JFrog integration. The left sidebar contains a navigation menu with the following items: Configuration (selected), License, Platform Roles, Identity Providers, Integrations (expanded), Code Repository Applications, Third Party Applications, Data Bucket Applications, Regions, and Others. The main content area is titled 'JFrog App Name' and includes the following configuration options:

- Redirect URL:** A text field containing 'https://strong-network.dev.com/oauth/apps/callback' with a 'copy' button.
- JFrog App Name:** A text field containing 'JFrog1'.
- Enforce users to connect to JFrog before they are able to open their workspaces:** An unchecked checkbox.
- Script:** A code editor containing a bash script for installing JFrog CLI and configuring Docker login.

```

1  #!/bin/bash
2
3  # If a command fails with exit!= 0 the script will continue executing the next command
4  set +e
5
6  # Install JFrog CLI if it's not already installed
7  jfrog_dep="deb https://releases.jfrog.io/artifactory/jfrog-debs xenial contrib"
8  wget -qO - https://releases.jfrog.io/artifactory/jfrog-gpg-public/jfrog_public_gpg.key | sudo
9  apt-key add -
10 if ! grep -q "${jfrog_dep}" /etc/apt/sources.list; then
11     echo "${jfrog_dep}" | sudo tee -a /etc/apt/sources.list;
12 fi
13 sudo apt update;
14 sudo apt install -y jfrog-cli-v2-jf;
15
16 # Connect the JFrog CLI
17 jf config add --url https://${JFROG_URL} --access-token=${JFROG_ACCESS_TOKEN} --
18 user=${JFROG_USER} --interactive=false ${JFROG_URL}
19
20 # Configure Docker login
21 echo ${JFROG_ACCESS_TOKEN} | \
22     docker login -u${JFROG_USER} --password-stdin ${JFROG_URL}
  
```

Finally, if you want to save the changes click on “Save”.

Now JFrog is configured across the Strong Network Platform, ready to be used seamlessly by the users.

## How to Use this Guide

This guide is here to provide you with a description of the main functions provided by Citrix Secure Developer Spaces.

The guide covers the initial setup, configuration and general usage of [workspaces](#), which are online

Cloud Development Environments (CDEs) available for coding and data science. Workspaces can be accessed [using a cloud IDE](#), include Microsoft Visual Studio Code, all JetBrains' IDEs or through an SSH connection from a local installed IDE (see remote development for [Microsoft Visual Studio Code](#))

This documentation is generally organized in a manner that follows the platform's UI pages. This provides a natural way to find information once on one of the [platform's](#) pages.

## Content

- [Platform](#)
- [Organization](#)
- [Project](#)
- [Overview Page](#)

## Platform Level

August 28, 2025

The platform is organized in [organizations](#) and [projects](#). A series of operations are readily available at platform level. For example, workspaces, resources and users can be managed at platform-level by users

with a platform role, such as the administrator or the security officer. Governance metrics such as insights and audit logs are also aggregated at the platform level.

The platform administrator has a view on all [workspaces](#) running on the platform, i.e. across organizations and projects, so that they can be updated rapidly, e.g. container configuration. The administrator can also have an overall view on the onboarded users.

[Resources](#) can be managed at the platform level so that they become available across organizations and projects. This applies to all types of resources supported by the platform.

[Insights](#) and [audits](#) dashboards are available at the platform level, allowing metrics to be selected and aggregated across organizations and projects.

Finally, a variety of settings and operations are relevant at the platform level. For example, these include global workspace settings regarding performance and security, global authentication settings, and compliance functions, to name a few.

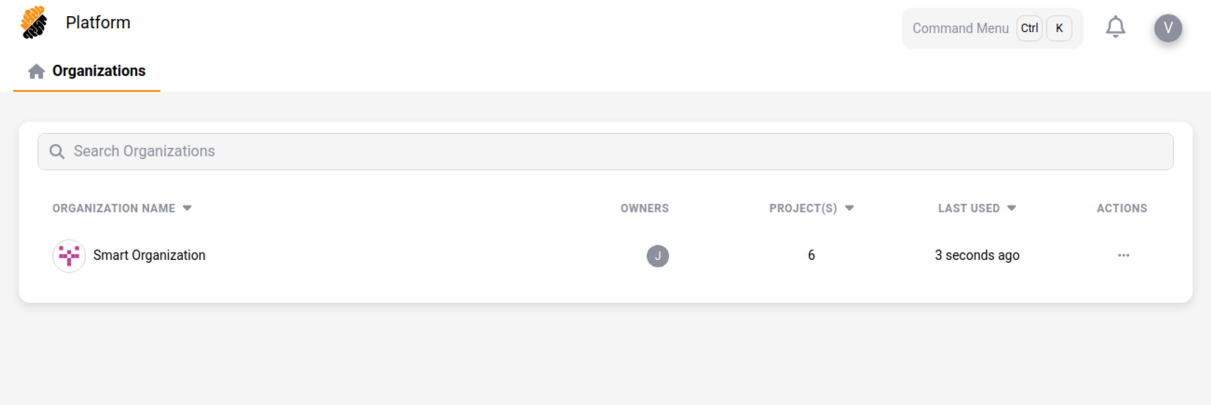
- [View Organizations](#)
- [Platform Settings](#)

## View Organizations

Organizations can be viewed at the level of the platform and listed in a table.

An administrator can [create an organization](#).

Click on the Strong Network™ logo to **view your organizations** to which you belong.



*Organizations List*

## Platform Settings Admin

For comprehensive control over your Platform's configurations, visit the dedicated [Platform Settings](#) page.

## Organizations

August 28, 2025

The platform allows administrators and platform owners to organize projects into organizations.

An **Organization** is the main entity regrouping [projects](#), developers, [resources](#), and security rules for one development project.

- [Organization's Characteristics](#)
- [View Organization's Projects](#)
- [Create an Organization](#)
- [Organization Settings](#)

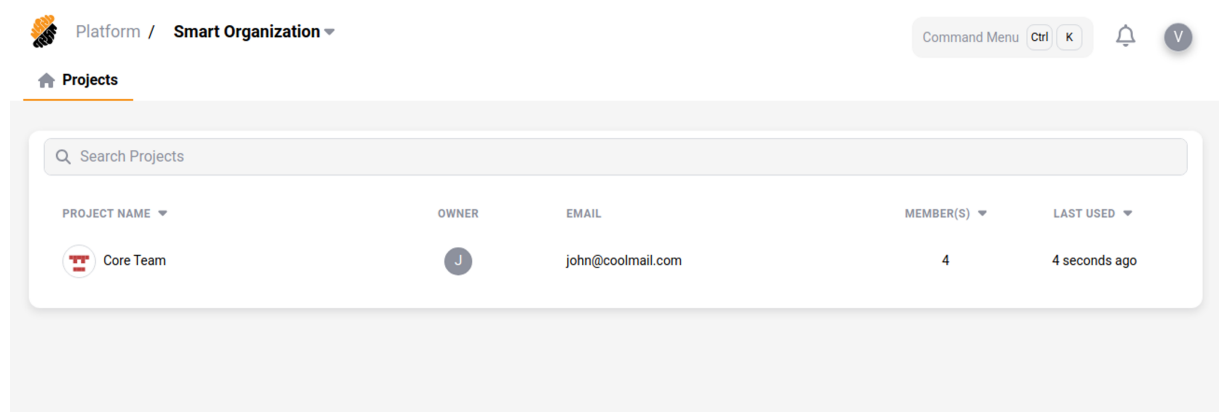
### Organization's Characteristics

An organization is defined by the following characteristics:

- **Organization Name,**
- **Organization owner,**
- **Organization owner's email,**
- **Project(s)** that it contains,
- **Resources, such base containers, policies, etc.**

## View Organization's Projects

In a project, by clicking on the name of your **organization** at the top left corner of the screen, you can display all of the **projects** contained in it.



## Create an Organization Admin

You can create an organization by pressing the “**Add New Organization**” button.

You will need to select the following information:

- **Organization Name,**
- **Owner.** i.e. any user with the right permissions to own an organization.

### Info

To create an organization, you must be an **Admin**.

An **Admin** can create an organization on behalf of an owner with the permissions to be the **Organization Owner**.

## Organization Settings Admin

For comprehensive control over your Organization's configurations, visit the dedicated [Organization Settings](#) page.



## Projects

August 28, 2025

A **Project** within an [Organization](#) regroups developers, resources, and security rules. The aim of a project is to provide the development team with all resources required for development, as well as access control and governance mechanisms to the project owner.

- [Project's Characteristics](#)
- [Create a Project](#)
- [Project Settings](#)

### Project's Characteristics

A project is defined by the following characteristics:

- **Name**,
- **Project owner**, i.e. any user with the right permissions to own a project,
- **Project owner's email**,
- **Member(s)**, i.e. the user belonging to the project,
- **Resources, including workspaces, base containers, repositories, etc.**

### Create a Project Admin

You can create a project by pressing the “**Add New Project**” button.

You will need to select the following information:

- **Project Name**,
- **Owner**, i.e. any existing user on the platform or a new user (to onboard).

#### Info

To create a project, you must be an **Organization Owner**.

An **Admin** can create a project and assign it to a user.

### Project Settings Project Owner

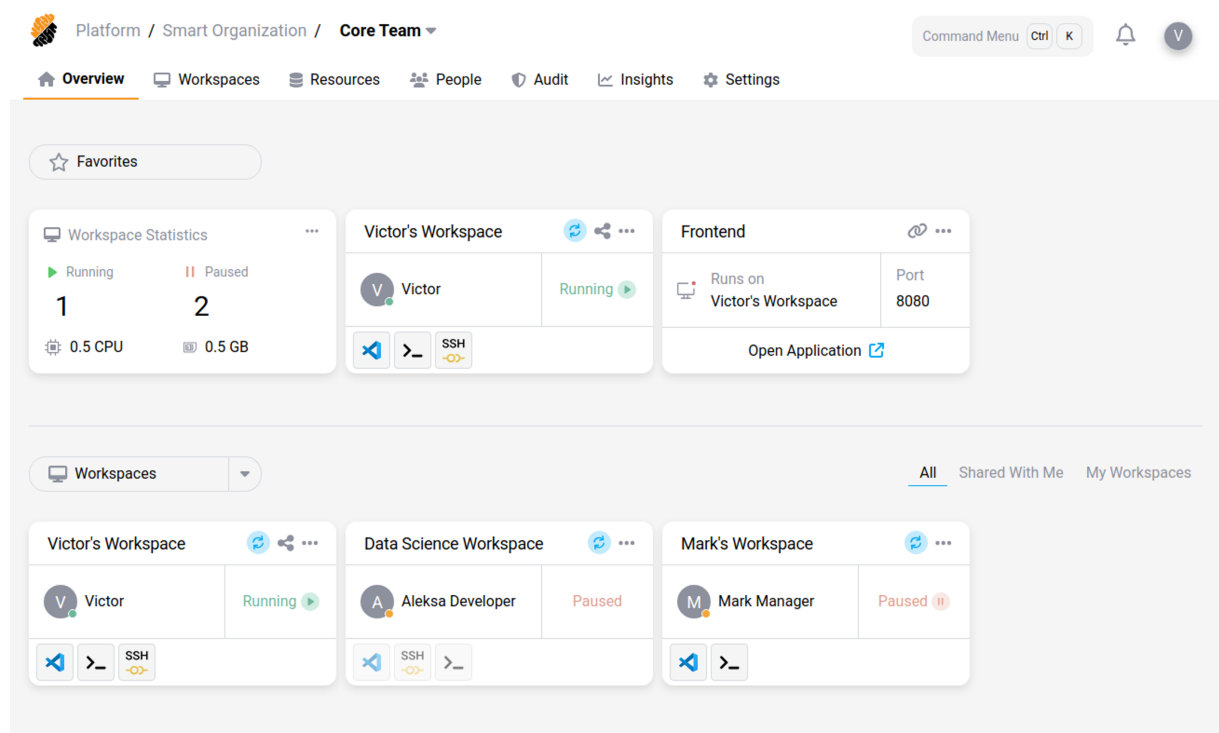
For comprehensive control over your Project's configurations, visit the dedicated [Project Settings](#) page.

## Overview Page

August 28, 2025

The Overview page is the first page displayed when you access the platform's user interface. It contains the essential components to allow quick access to resources such as workspaces, apps, secure web apps and metrics.

The **Overview Page** is customizable. All components can be reordered according to your preferences.

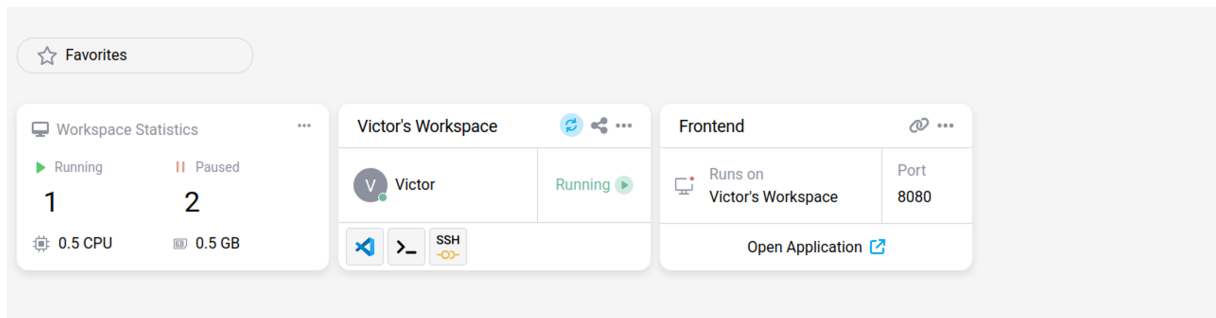


- [Display Sections](#)
  - [Favorites](#)
  - [Workspaces](#)
  - [Workspace Apps](#)
  - [People & Other Metrics](#)

## Display Sections

### Favorites

The **Favorites** section displays your personal favorite list of components, from any section of the **Overview Page**.



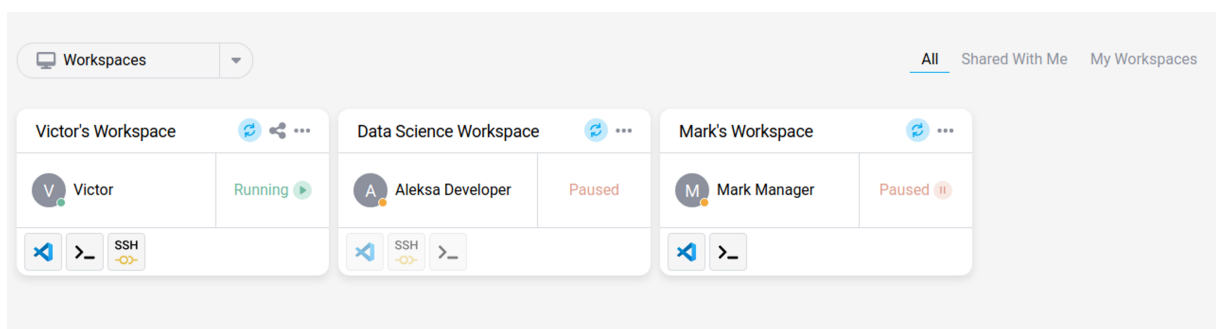
- To **add an element** to your list, click its “...” button and “**Add to Favorite**”.
- To **remove an element** from your list, click its “...” button and “**Remove from Favorite**”.

Tip:

Entries in the list of favorite components can only be components on the **Overview Page**.

### Workspaces

The **Workspaces** section displays all the project’s [Workspaces](#) to which you have access.

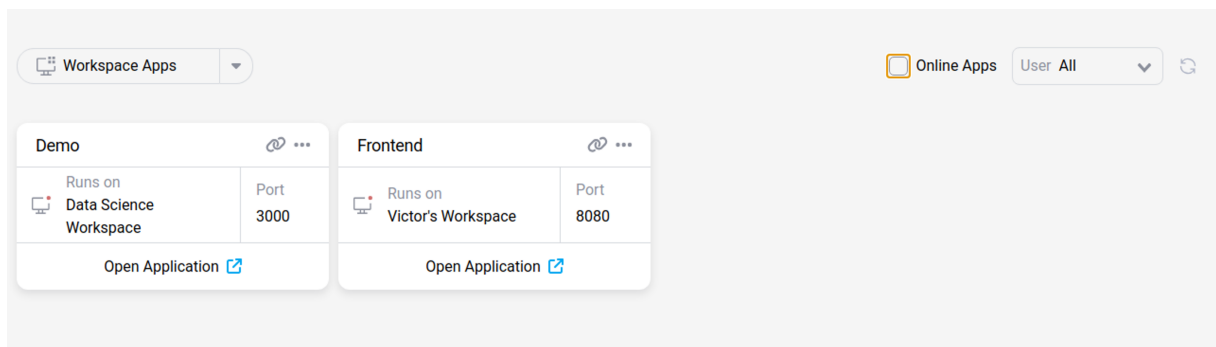


To only view your workspaces, select “**My Workspaces**”.

- To [create a new workspace](#) click on the “**Workspaces**” drop-down menu.
- To manage workspaces, view [Manage Workspaces](#).

### Workspace Apps

The **Workspace Apps** section displays all the project’s [workspace apps](#) to which you have access.

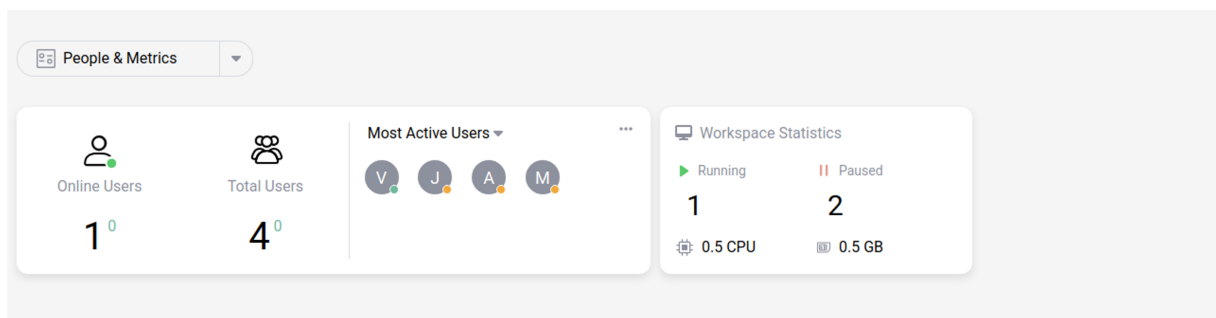


To only view your own, or any online workspace apps select “**My Apps**” or “**Online Apps**” respectively.

- To [create a new workspace app](#) click the “**Workspace Apps**” drop-down menu.
- To manage a workspace app click its “...” button.

## People & Other Metrics

The **People & Metrics** section displays statistics about the users in the project and metrics about resources’ utilization.



**People** metrics display:

- The amount of project users online.
- The total amount of project users.
- Statistics about the amount of users online over the past seven days.

**Workspace** metrics displays:

- How many workspaces are running or paused.
- The current total CPU and RAM usage for your Project.

Check the [Insights Page](#) for more detailed metrics.

## Self-Served Developer

August 26, 2025

### Developer

This workflow exemplifies the most common onboarding case: a developer with the permission to create workspaces, i.e. a self-served onboarding process. This is typically an “internal” developer with permissions to access resources associated with the project, e.g. containers, services, secrets, etc. These resources are set up by the project owner and self-served developers are able to configure a workspace’s access control setting.



1. [Log In & Create a Workspace](#)
2. [Configure Workspace Settings \(Optional\)](#)
3. [Access Workspace & Connect Platform Applications](#)
4. [Run, Open and Share Applications \(Optional\)](#)

## 1. Log In & Create a Workspace

After logging in –having already been added to a project on the platform –the developer can independently create a workspace. This can be done using one of the pre-defined templates available on the platform or by following a guided setup process.

Platform / Smart Organization / Core Team

Command Menu Ctrl K

OverviewWorkspacesResourcesPeopleAuditInsightsSettings

Create Workspace

Create from Existing

Create from Template

Create from Template

Select Template

Monitored VSCode Template

Version

1

Last Published Version 1

Owner

John ProjectOwner

Workspace Name

John's Workspace

Shared With

LaunchCustomize

Specification for Workspace "John's Workspace"

| Template Name / Version | Owner             | Workspace Access | Image                         |
|-------------------------|-------------------|------------------|-------------------------------|
| John's Workspace        | John ProjectOwner |                  | Default Generic Image (2.2.5) |

Specification Template

Total CPUs2

Memory (GB)4

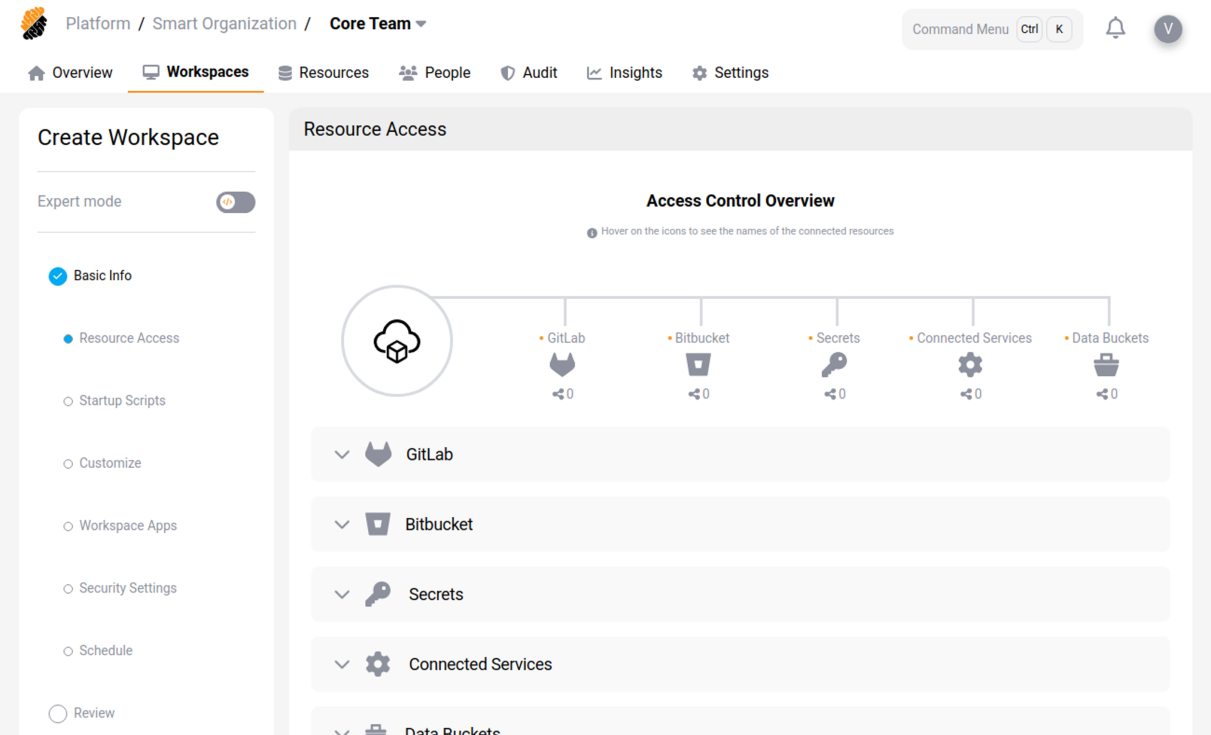
Storage (GB)20

## 2. Configure Workspace Settings (Optional)

Through the guided setup (the wizard), the developer can configure the workspace’s general settings, which include naming the workspace, selecting a specification template, and adjusting sharing preferences. Additionally, the developer can establish access controls to their entitled resources, covering options for git repositories, applications, services, and secrets.

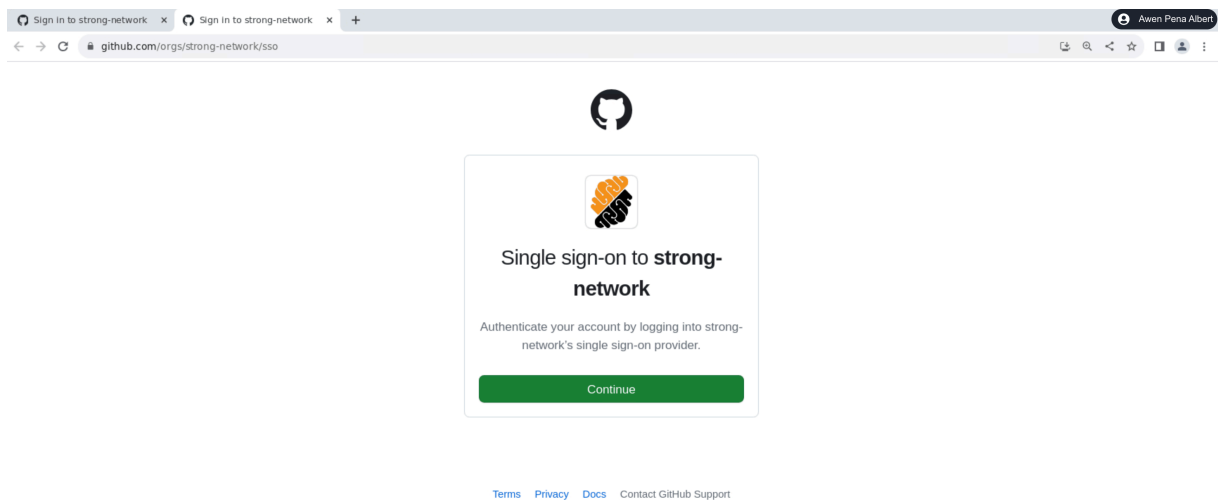
Implementing access control is not mandatory and can be addressed when the workspace is accessed

for the first time.



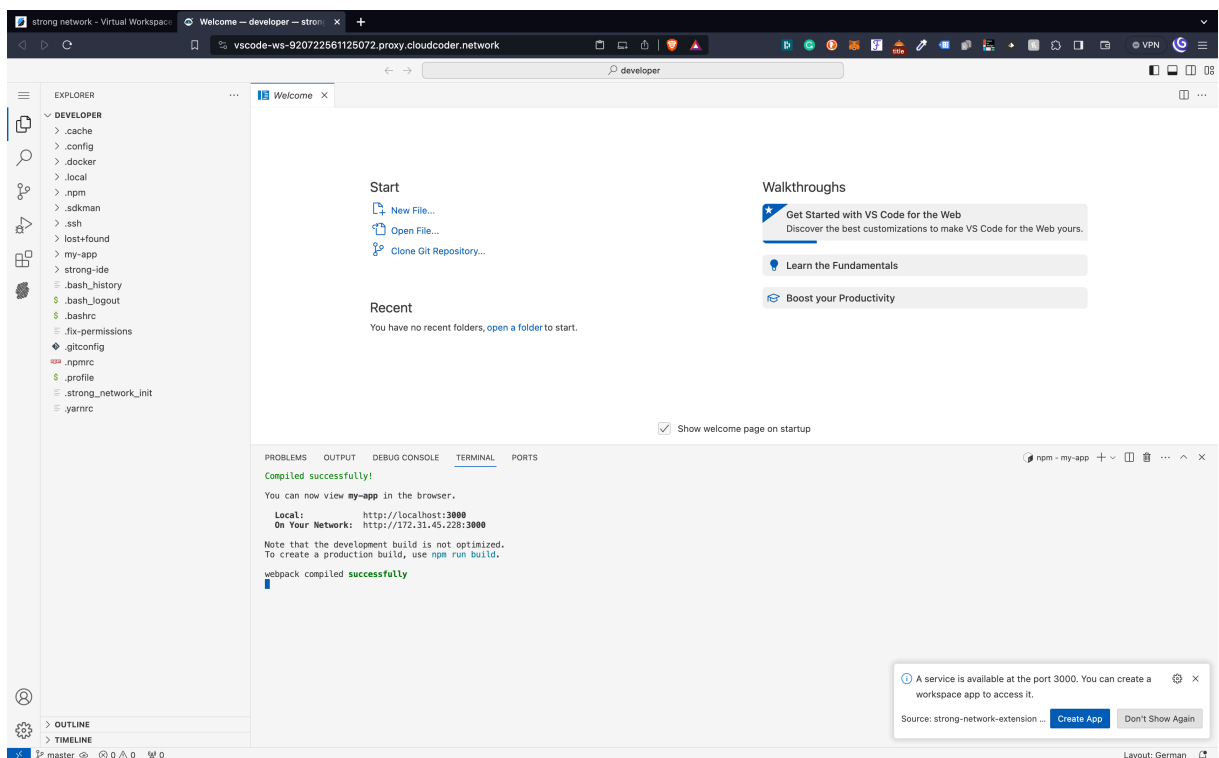
3. Access Workspace & Connect Platform Applications

When first accessing a workspace, the developer may employ the single sign-on feature to gain entry to one or more gate applications linked to the platform, contingent upon the applications made available by the administrator.



#### 4. Run, Open and Share Applications (Optional)

Once workspace access is secured, the developer is permitted to execute and, where authorized, access and share applications.



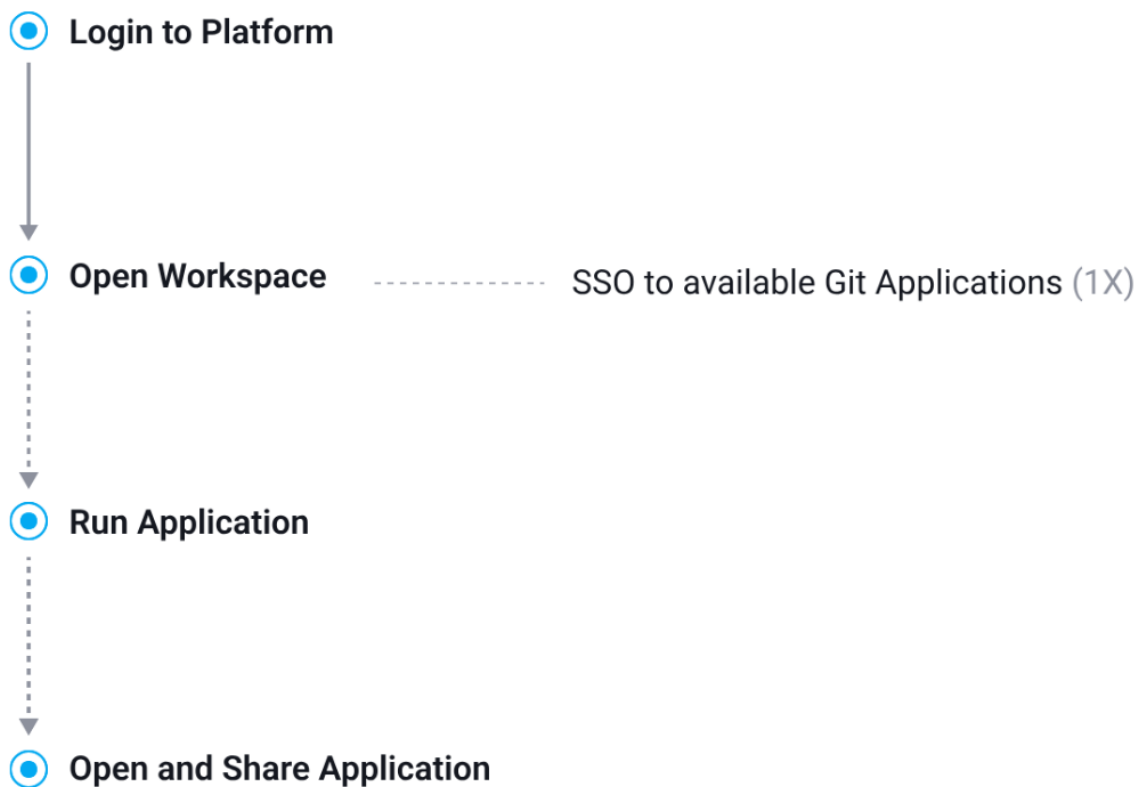


## Guest Developer

August 26, 2025

### Developer

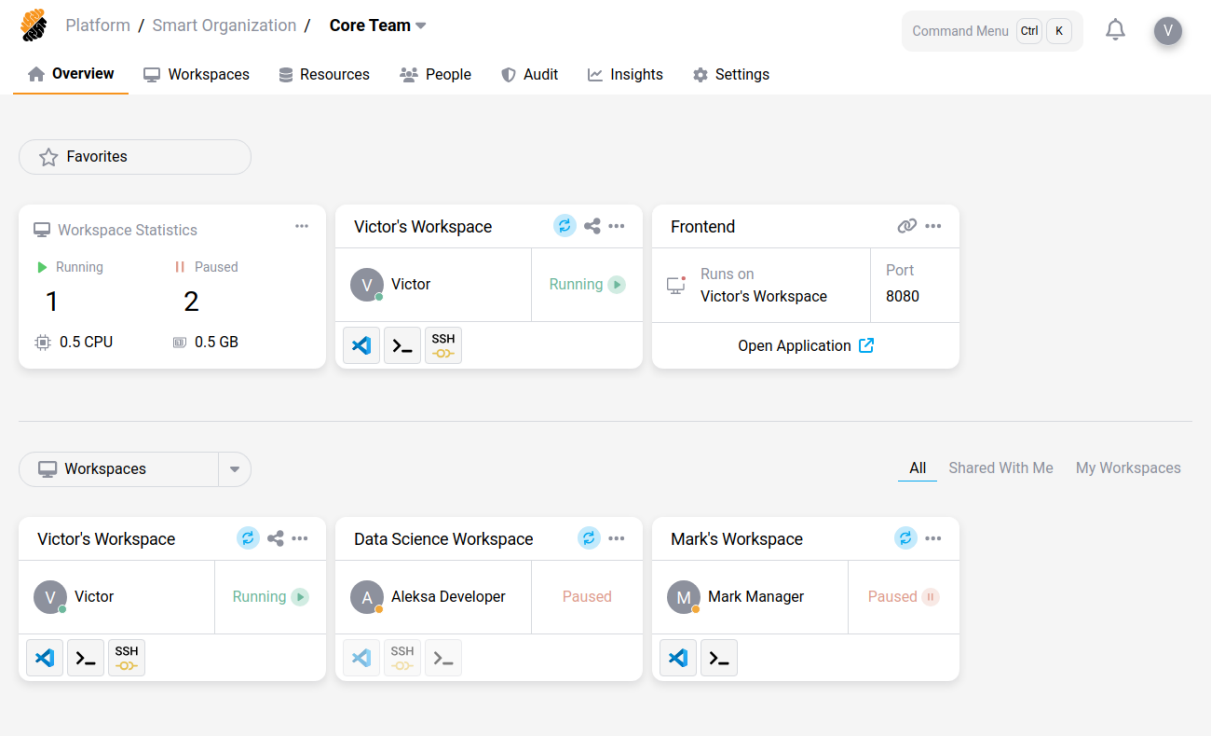
This workflow exemplifies a particular onboarding case: a “guest” developer with permissions limited to access pre-configured workspaces, i.e. pre-set and immutable settings spanning resource access to security. This is typically a temporary developer, a contractor or an external collaborator. The entire workspace set-up is defined by the project owner and created in anticipation of onboarding the developer. Expectedly the developer cannot edit the workspace settings.



1. [Log In & Access Workspace](#)
2. [Connect Platform Applications \(Optional\)](#)
3. [Run, Open and Share Applications \(Optional\)](#)

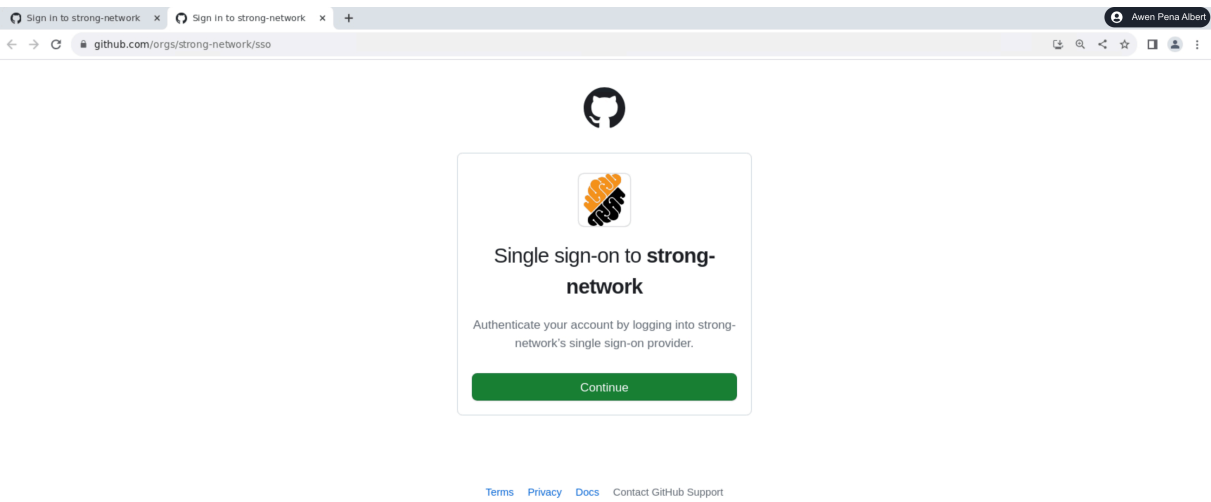
### 1. Log In & Access Workspace

After logging in –having already been added to a project on the platform –the developer can access his assigned workspaces.



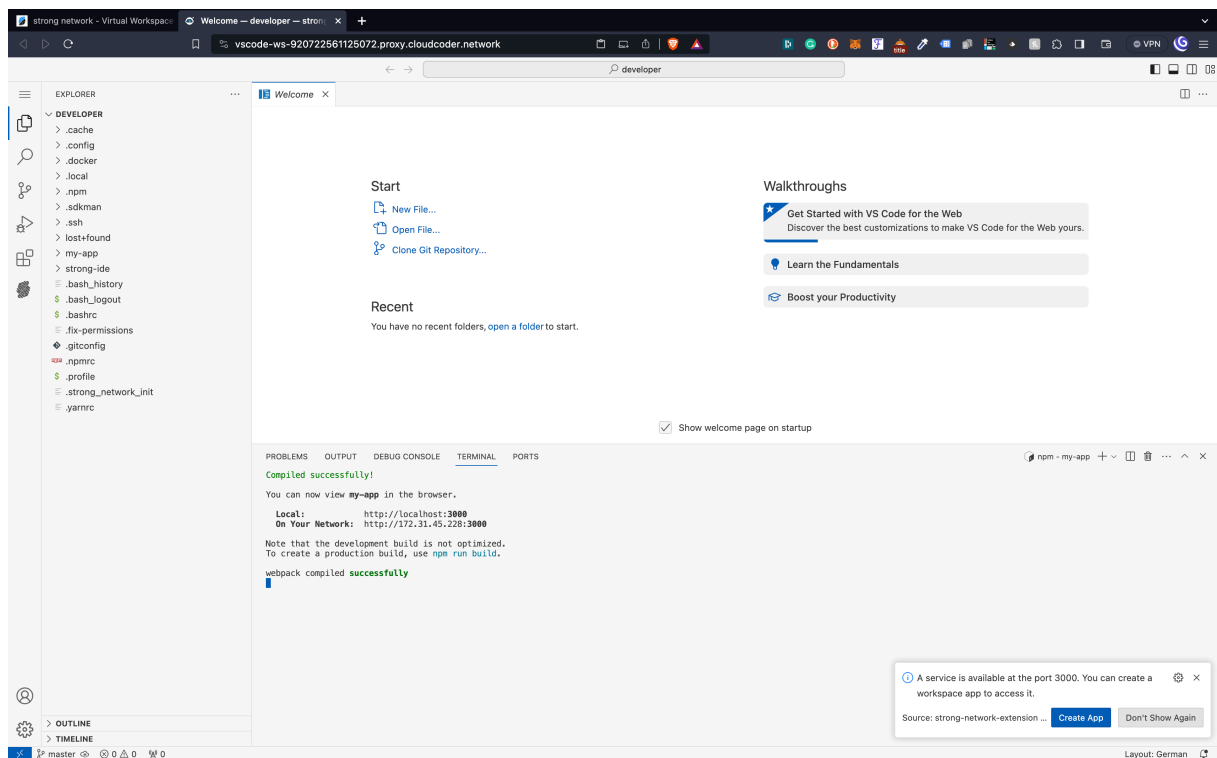
## 2. Connect Platform Applications (Optional)

When first accessing a workspace, the developer may employ the single sign-on feature to gain entry to one or more gate applications linked to the platform, contingent upon the applications made available by the administrator.



### 3. Run, Open and Share Applications (Optional)

Once workspace access is secured, the developer is permitted to execute and, where authorized, access and share applications.

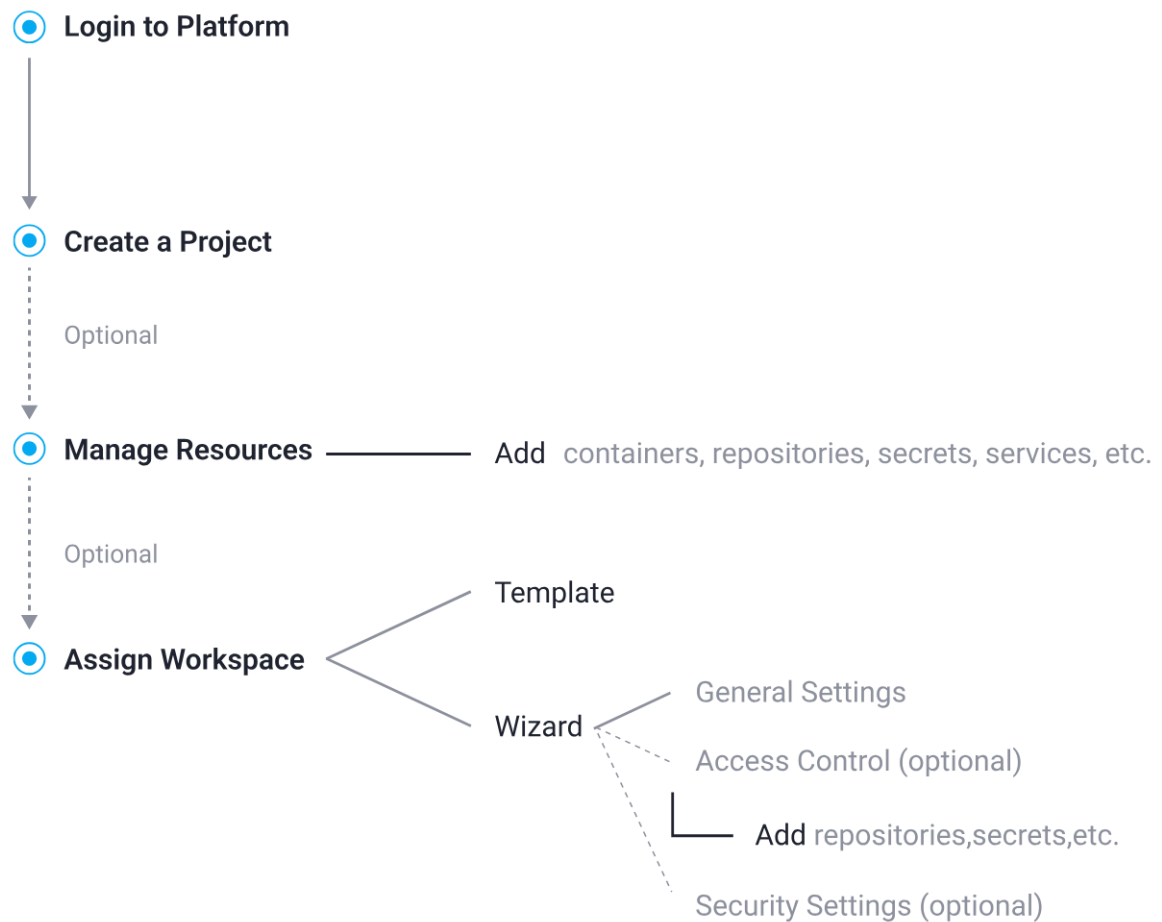


## Project Owner

August 26, 2025

### Project Owner

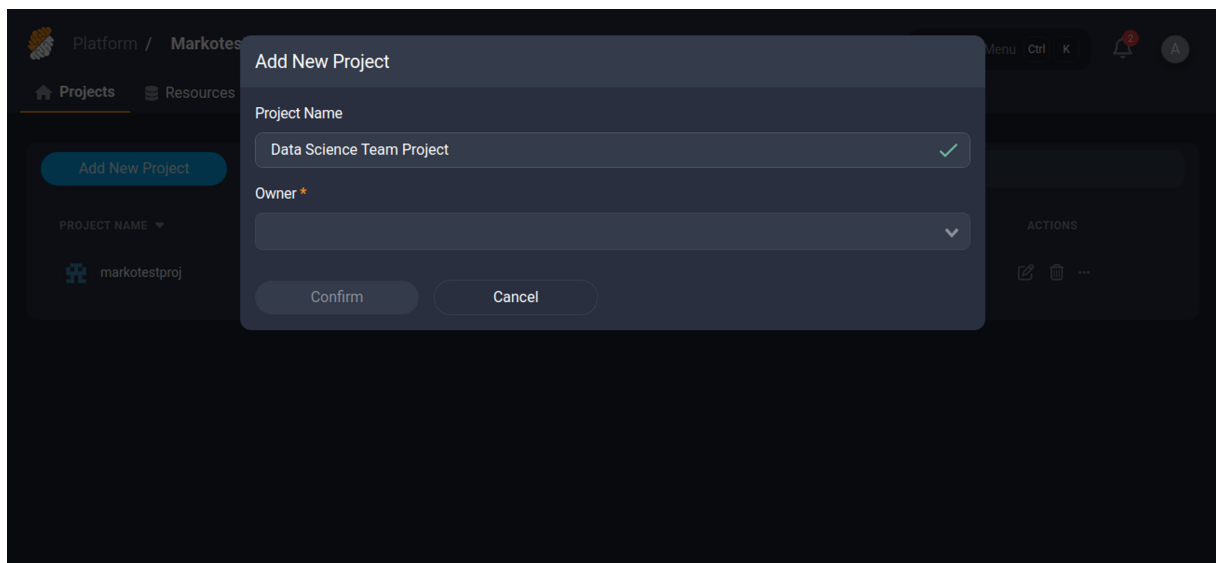
This workflow exemplifies the onboarding case of a project owner. Users with this role can create and edit settings of all the project's workspaces, including the workspace's access control and security settings. The project owner also creates workspaces for "guest" developers. In addition, he can manage resources for the project, such as importing containers, git repositories, secrets, etc.



1. [Log In & Create a Project](#)
2. [Manage Resources \(Optional\)](#)
3. [Assign a Workspace \(Optional\)](#)
4. [Configure Workspace Settings \(Optional\)](#)

## 1. Log In & Create a Project

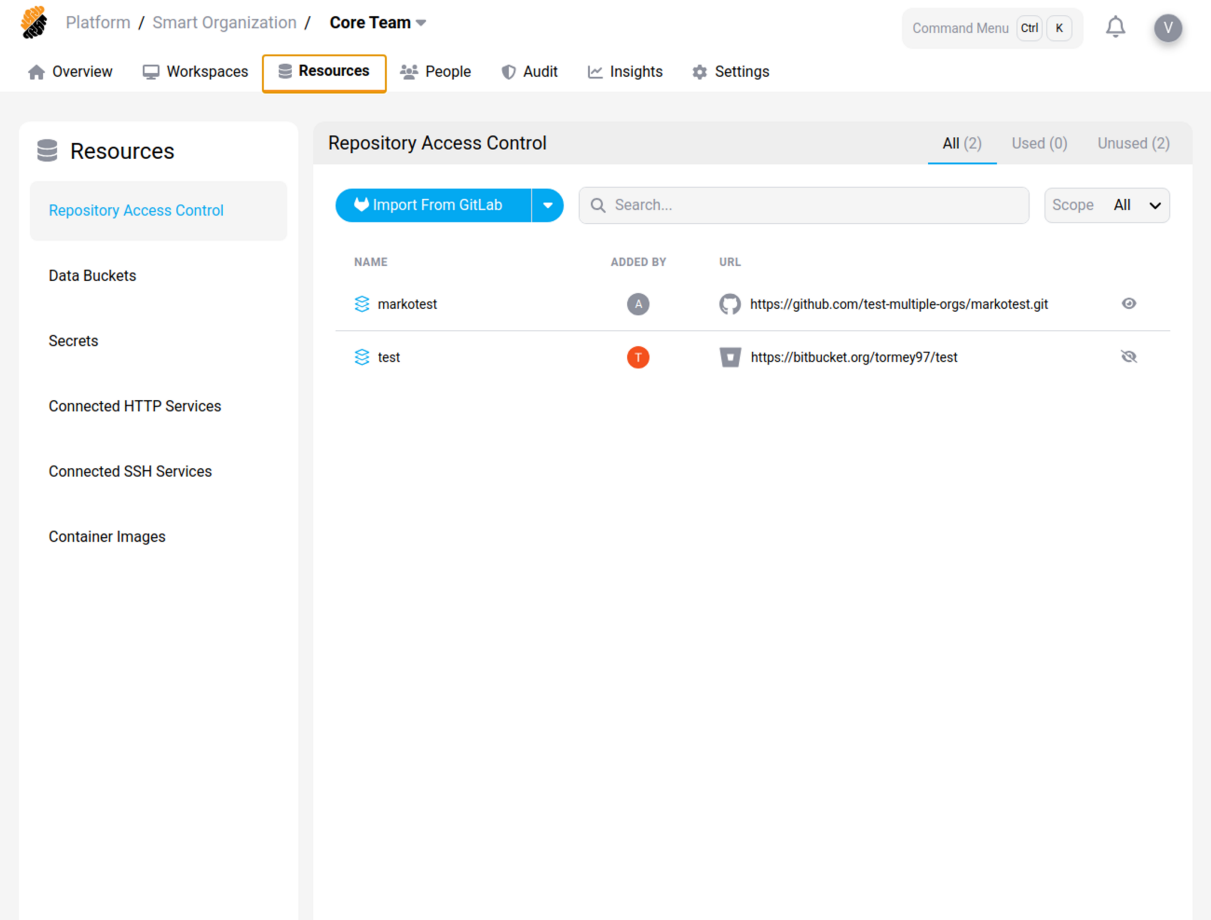
Upon logging in –having been affiliated with an organization on the platform –the project owner is equipped to establish a project for their team.



## 2. Manage Resources (Optional)

Additionally, a project owner can add and manage the resources leveraged by the development team.

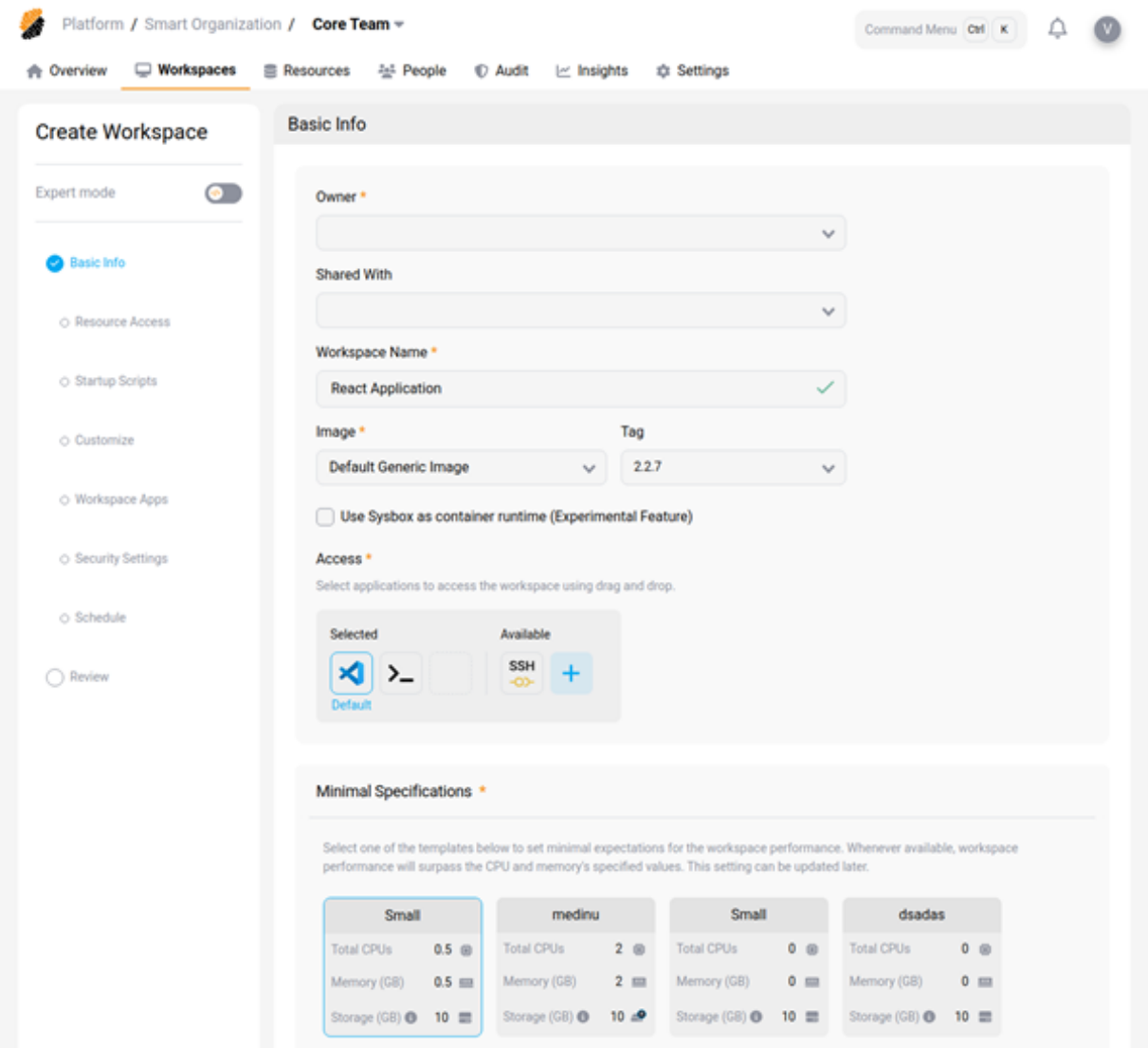
Resources on the platform encompass code repositories, secrets, services, and data buckets. The project owner is responsible for determining user permissions, and stipulating who can view or alter resources to prevent unauthorized access.



### 3. Assign a Workspace (Optional)

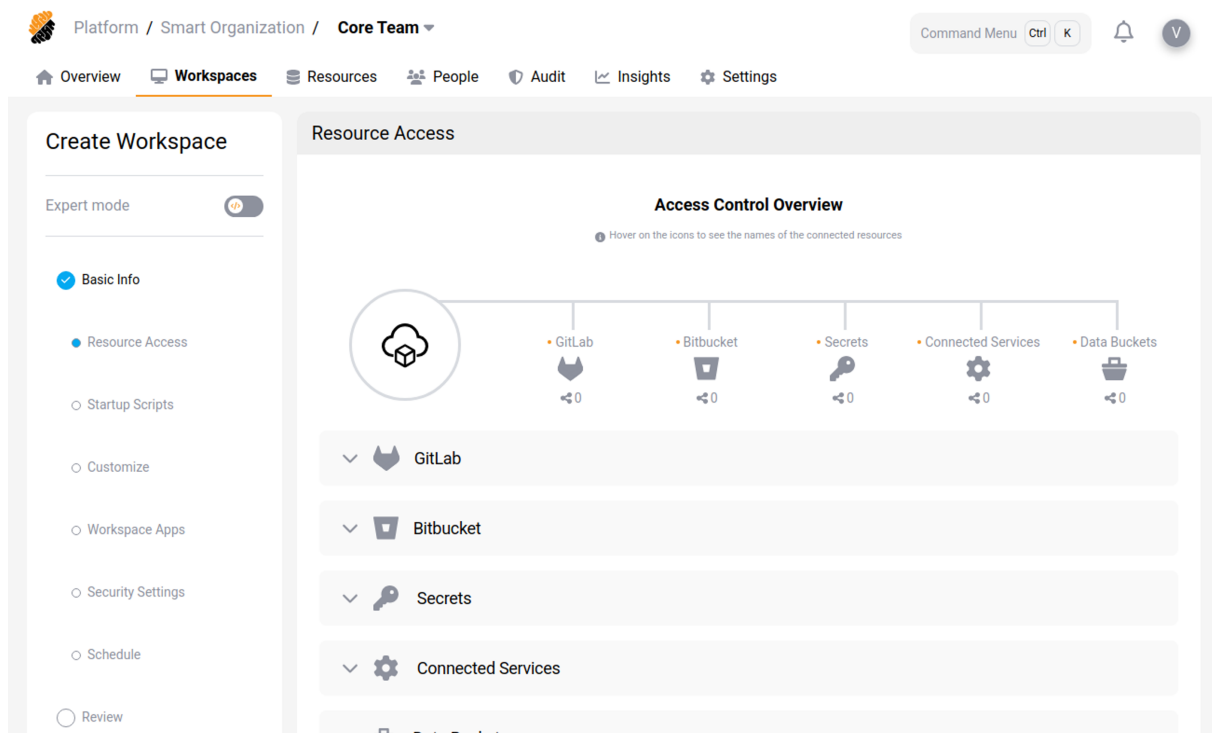
The project owner can create and assign a workspace to any user, however since developers with the permission `Workspace:Manage Personal` create their own workspaces (self-service), a project owner most commonly creates workspaces for developers without this permission, i.e. in order to onboard freelancers and contractors under a lesser permission model.

Therefore, project owners will create a workspace with a template or the workspace wizard and assign it to a user who is not entitled create it by himself.



#### 4. Configure Workspace Settings (Optional)

When the project owner creates a workspace on behalf of another user as explained in the previous section, he likely needs to set-up the access control and security settings. If the workspace is assigned to a user with the permission Workspace:Access (the user cannot create his/her own workspaces), the user won't be able to change the access control settings.



## What Is a Workspace?

August 1, 2025

A workspace is a Cloud Development Environments (CDEs) available for coding and data science. Workspaces can be accessed [using a cloud IDE](#) or through an [SSH connection](#) from a local installed IDE.

Workspaces are running online on top of a virtual machine and managed using a container orchestrator for resilience. The performance of a workspace, i.e. compute and storage capabilities, are set by the specifications of the underlying virtual machine.

Workspaces are technically speaking virtual processes, with the aim of replacing the use of a virtual machine for code development and data science. They are lightweight and so that they can be started and paused much quicker than a VM counterpart.

A Workspace is defined by the following characteristics:

- **Basic Information:** such as name, owner, sharing options,
- **CPU/RAM/Storage:** performance allotted to the workspace.
- **Ports:** ports to run applications on,
- **Status:** i.e. running, deploying, or paused



Where to go next

- Get to know the [Workspaces page](#)
- [Create a Workspace](#)
- [Manage Workspaces](#)
- [Workspace Apps](#)
- [Use templates](#)
- [Use a Workspace](#)
- [SSH into your workspace](#)

Workspaces Page

August 26, 2025

In the scope of a project, the **Workspaces Page** displays all [workspaces](#) created for that particular project to which you have access or you can view, depending on your permission level.

This includes personal workspaces and the workspaces shared with you. In some cases, it also includes [workspace’s Templates](#) available in the [project](#).

Platform / Smart Organization / Core Team

Command Menu Ctrl K

Overview Workspaces Resources People Audit Insights Settings

Workspaces Templates

Show Update Center

Create Workspace

Search Workspaces

☐ Shared With Me ☐ My Workspaces

Running 1 Paused 2 CPU 0.5 Memory (GB) 0.5

| NAME                   | OWNER | SHARED WITH | OPEN PORTS     | STATUS  | ACCESS | ACTIONS |
|------------------------|-------|-------------|----------------|---------|--------|---------|
| Victor's Workspace     | V     | not shared  | 8080           | Running |        |         |
| Data Science Workspace | A     | not shared  | 3000           | Paused  |        |         |
| Mark's Workspace       | M     | V           | No port opened | Paused  |        |         |

Below the search bar are displayed the number of running and paused workspaces, as well as how

much total CPU and GB of RAM is being used.

## Where to go next

- [Create a Workspace](#)
- [Manage Workspaces](#)
- [Create and manage Workspace Apps](#)
- [Create and manage templates](#)

## Create a Workspace

August 26, 2025

A [workspace](#) is created from the [Workspaces Page](#). A workspace is, in essence, an online Cloud Development Environment (CDE) accessible via a [Cloud IDE](#), a [terminal](#) or an [SSH connection](#). Using an SSH connection is possible from a locally installed IDE supporting development from a remote container.

- [Basic Set-Up](#)
  - [Basic info](#)
  - [Resource Access Control](#)
  - [Data Loss Prevention Permission: Security::Manage](#)
  - [Custom Work Schedule](#)
  - [Launch it](#)
- [From an existing Workspace](#)
- [From a template](#)

### Basic Set-Up

You can create a workspace by pressing the “**Create Workspace**” button.

Platform / Smart Organization / Core Team

Command Menu Ctrl K

Overview Workspaces Resources People Audit Insights Settings

Create Workspace

Expert mode

Basic Info

Resource Access

Startup Scripts

Customize

Workspace Apps

Security Settings

Schedule

Review

Basic Info

Owner

Shared With

Workspace Name

Image Tag

Use Sysbox as container runtime (Experimental Feature)

Access

Minimal Specifications

Launch

Next

Cancel

Owner

Shared With

Workspace Name

Image Tag

Use Sysbox as container runtime (Experimental Feature)

Access

Minimal Specifications

Selected

Available

Default

SSH

Small

medinu

Small

dsadas

Total CPUs

Memory (GB)

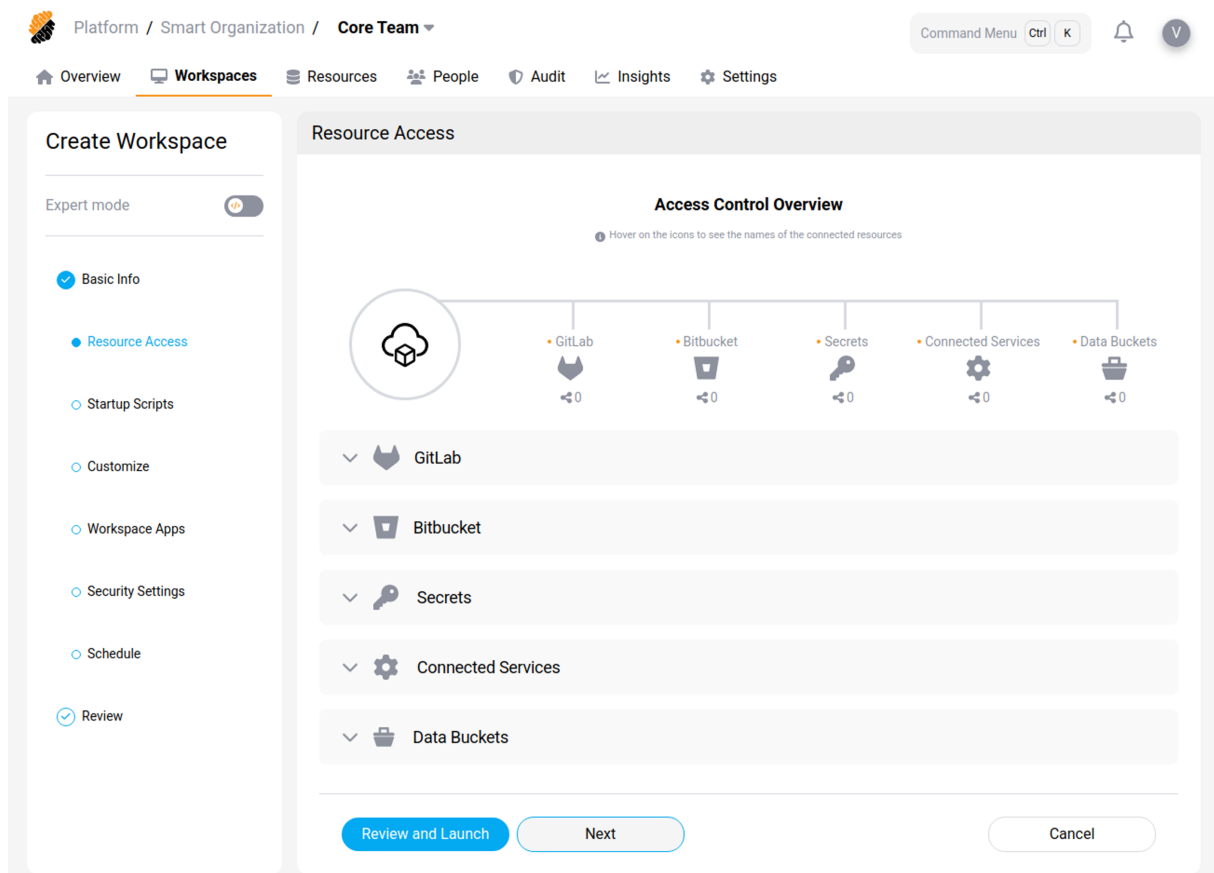
Storage (GB)

You will need to select the following information:

## Basic info

1. **Workspace Name**
2. **Embedded Cloud IDE**
3. **User Sharing Options**
4. **Docker Image**
5. **Image Version**
6. **Minimal Resource Specifications**

## Resource Access Control



You can attach various project resources to your workspace. [Resources](#) must have been previously added to the project. In addition, you might need the appropriate access rights to access them.

You can add the following resource:

- **Git Applications And [Repositories](#):** You can connect the entire GIT applications available from your platform or single repositories that have been previously imported to the project's or organization's resources. Additionally, you can specify a default folder location within your workspace where the Git files will be cloned.
- **[Secrets](#):** You can import secrets to the workspace as files or environment variables in the workspace. Choose from existing secrets or [create a new one](#).
- **Connected [HTTP](#) and [SSH](#) Services:** You can connect services to appear as environment variables in the workspace. Supported and available services are part of the project's and organization's resources and depend on the platform's configuration.
- **Startup Script:** Finally, you can set-up a startup script to be executed automatically at workspace's boot time. This allows you to customize the software available in the container.

**Data Loss Prevention Permission: `_Security::Manage_`**

Platform / Smart Organization / Core Team

Overview Workspaces Resources People Audit Insights Settings

### Create Workspace

Expert mode

- Basic Info
- Resource Access
- Startup Scripts
- Customize
- Workspace Apps
- Security Settings**
- Schedule
- Review

### Security Settings

#### Workflow Data Protection

Policy: Applied Missing

Secure Browser IDE Apps

Clipboard Security Network Security

#### Network Security

Choose a network security policy for the workspace. [View Summary](#)

No Policy Selected

#### Clipboard Security

Prevent paste operations outside the IDE and the secure browser

#### Enable Personal SSH Identity

Use the Personal SSH Identity tab in Profile to create a private/public key pair to manually configure services.

[Review and Launch](#) [Next](#) [Cancel](#)

In the Data Loss Prevention section you can configure the security of your workspace.

Under **Security Settings** you can configure:

- **Network Policy:** Select a network policy to enforce on the workspace. [Network policies](#) are part of the project's and organization's resources and are defined by the user with the `_Security::Manage` permission. In particular, policies allow you to control outbound network traffic from the workspace.
- **Clipboard Security:** Prevent pasting outside of the IDE and the Secure Browser for this workspace.

- **Apps Security:** Configure [Workspace Apps](#) to be accessed only through the Secure Browser.

Under **Secure Access Management** you can configure:

- **Enable Remote Development Over SSH:** Allow connection to the workspace via SSH.
- **Enable Personal SSH Identity:** Allow users to use their personal SSH identity from within the workspace.

## Custom Work Schedule

You can define a custom work schedule for your workspace.

Platform / Smart Organization / Core Team

Command Menu Ctrl K

Overview Workspaces Resources People Audit Insights Settings

### Create Workspace

Expert mode

- Basic Info
- Resource Access
- Startup Scripts
- Customize
- Workspace Apps
- Security Settings
- Schedule**
- Review

### Schedule

Custom Workspace Schedule ☒

⚠ This will override your Profile's workspace schedule.

#### Work Schedule ⓘ

##### Timeout Outside Schedule

Select a timeout after which the workspace will be automatically paused when not in use and running outside of scheduled hours. You can remove specific timeout options, making those options unavailable to users.

30 minutes

##### Idle Timeout

Select a timeout after which the workspace will be automatically paused when not in use, regardless of the schedule. You can remove specific timeout options, making those options unavailable to users.

8 hours

Select a daily schedule such that your main workspace (i.e. last used) automatically runs during set hours.

- Note that any workspace will pause automatically when not used after the set timeout time.
- When a workspace is paused voluntarily, it will not be started by this schedule.

M T W T F S S

Review and Launch Next Cancel

## Launch it

Finally, review your Workspace configuration, and launch it. Your workspace will be automatically deployed.

You can [edit its configuration](#) at any time from the [Overview](#) or Workspaces pages.

## From an existing Workspace

You can create a workspace from an existing one by pressing the “**Create from Existing**” button on the drop-down button of the “**Create Workspace**” button.

You will need to provide the following information:

1. **Workspace to Copy**
2. **Owner for the Workspace**

### Tip

Click on “Customize” to edit the workspace as if you were creating it from scratch.

Once done, press the “**Launch**” button.

## From a template

You can create a workspace from an existing one by pressing the “**Create from Template**” button on the drop-down button of the “**Create Workspace**” button.

You will need to provide the following information:

1. **Template Name**
2. **Owner for the Workspace**

### Tip

Click on “Customize” to edit the workspace as if you were creating it from scratch.

Once done, press the “**Launch**” button.

## Manage Workspaces

August 1, 2025

**Workspaces** are managed from the [Overview](#) and [Workspaces pages](#). Once one or more workspaces have been assigned to you, they appear on both pages mentioned above. The last used workspace will be automatically started based on the schedule in your profile. In addition, a workspace might be paused automatically based on the settings of your platform after a period of inactivity.

## View Workspaces

The list of your workspaces (owned by you or shared with you) is displayed on the [Overview](#) and [Workspaces pages](#).

The **status** of the workspace is displayed next to its name.

| NAME                   | OWNER | SHARED WITH | OPEN PORTS     | STATUS  | ACCESS | ACTIONS             |
|------------------------|-------|-------------|----------------|---------|--------|---------------------|
| Victor's Workspace     | V     | not shared  | 8080           | Running | SSH    | Eye icon, More icon |
| Data Science Workspace | A     | not shared  | 3000           | Paused  | SSH    | Eye icon, More icon |
| Mark's Workspace       | M     | V           | No port opened | Paused  | SSH    | Eye icon, More icon |

- To **open a paused workspace**, click on the “**start**” button. This will open the workspace’s Cloud IDE in your browser.
- To **open a running workspace**, click on the “**running**” button. This will open the workspace’s Cloud IDE in your browser.
- To **open your workspace using a CLI terminal**, click on the drop-down menu next “**running text**” and then on the “**Open Terminal**” button.

## Workspaces Actions

By clicking on the “...” icon on a workspace, you can select additional actions as explained below.

- **Run** or **Pause** allow you to start and pause the workspace, respectively.
- **Edit** allows you to change the workspace’s settings as selected when [creating it](#).
- **Delete** erases its configuration and local files. You will need to confirm the action by inserting the name of the workspace.
- **Edit Ports** lets you manage [workspace apps](#) running on the ports of your workspace.
- **Personalize Environment** lets you update the [IDE configuration file] based on your profile settings (*Only if Workspace is yours*).



- **Update** redeploys the workspace to synchronize it with its latest configuration.
- **Share** lets you share the workspace access with another [project](#)'s user. Learn how to work with a [shared workspace](#) (*Only if Workspace is yours*).
- **Save As Template** lets you save the workspace's configuration as a template for later reuse (requires the *Workspaces::Manage Project* permission).

| OPEN PORTS     | STATUS  | ACCESS     | ACTIONS |
|----------------|---------|------------|---------|
| 8080           | Running | SSH        |         |
| 3000           | Paused  | SSH        |         |
| No port opened | Paused  |            |         |
|                |         |            |         |
|                |         | Run        |         |
|                |         | Edit Ports |         |

## Workspace Apps

August 26, 2025

A **workspace app** lets you access a local application running on a port of your [Workspace](#).

Depending on your workspace security's settings, your workspace app might open in a separate tab of your

web browser or in the Secure Browser. You can have multiple workspace apps attached to a single workspace, each accessing an application running on a different port.

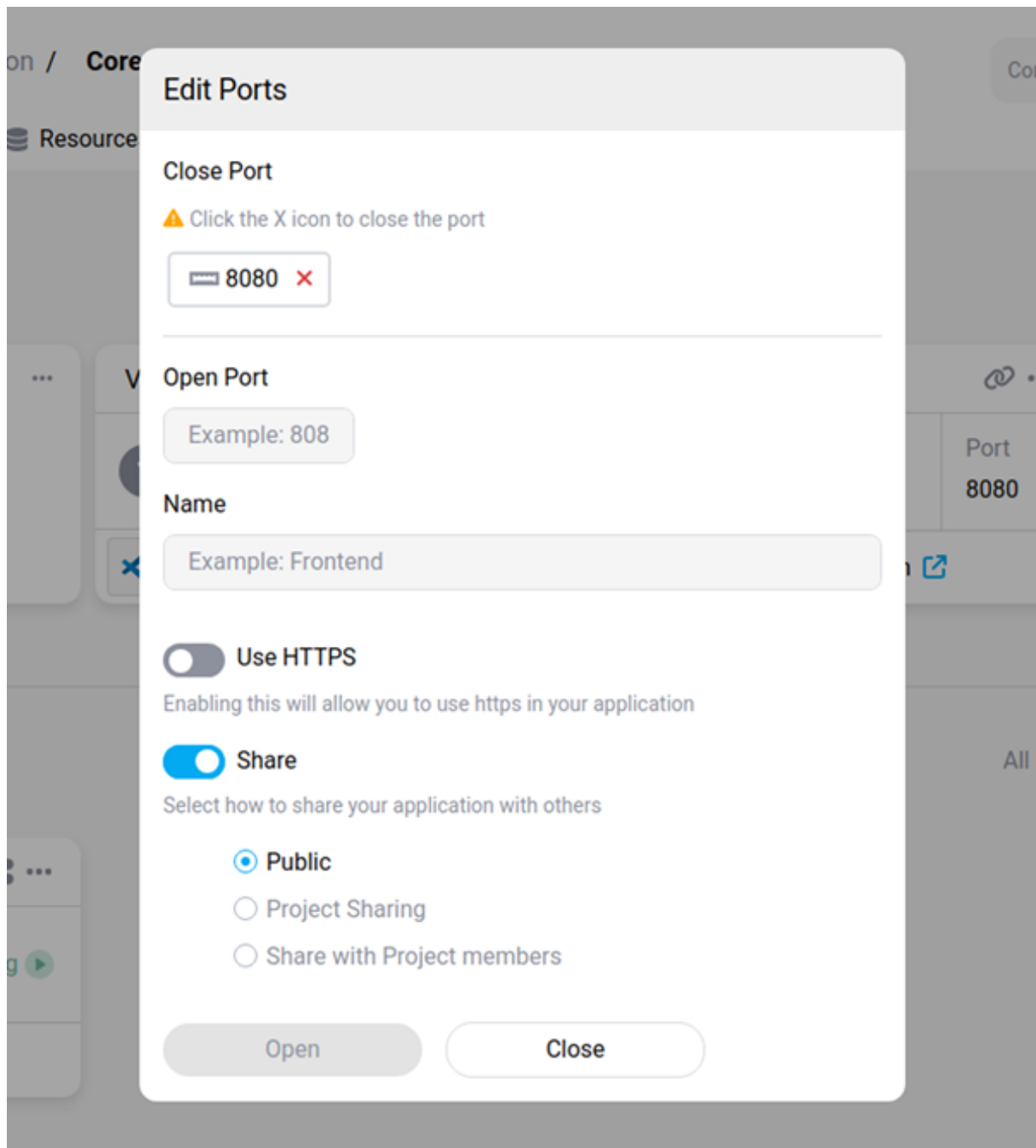
### Create a Workspace App

You can create a workspace app by pressing the “**Create Workspace App**” button from the [Overview Page](#) by selecting the drop-down menu next to “Workspace Apps”.

#### Tip:

You can create a workspace app by clicking the “...” icon and select **Edit Ports** from a

Workspace on the Overview or Workspaces Pages.



You will need to enter the following information:

1. **Port** where the app is running,
2. **Name** for the app,
3. **Use HTTPS** to allow to use https in the application,
4. **Share** to allow others to access the application (Public, Project Sharing or Share With Project-mate).

**Tip:**

When you create an app for a Node Js project, make sure the port number is the same as the one opened in the localhost of the workspace.

## Share a Workspace App

You can share a workspace app when [creating it](#) or by editing an existing one.

To update the properties of a workspace app, click the “...” icon and on the **Edit Ports** button from one of your workspaces.

There are two sharing options:

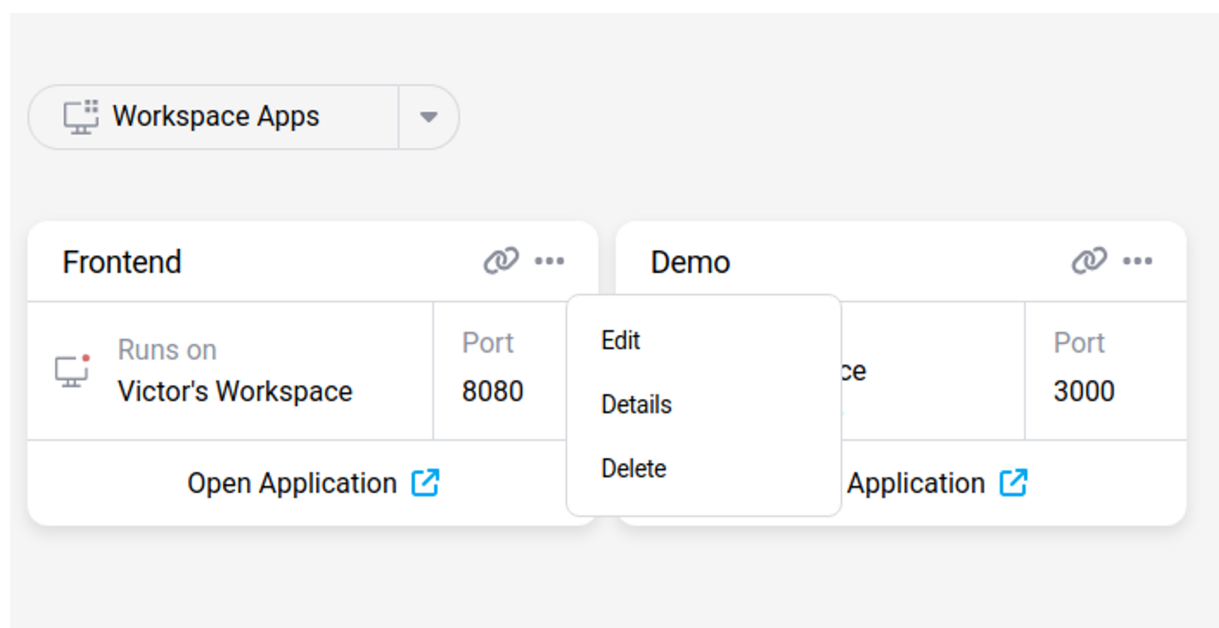
- With a **group of users**: public (any external user) or project (all of your project-mates).
- With a **specific user**.

Granting access to one of your workspace apps does not provide access to the workspace running the app. To share a workspace with another user, check out the [share a Workspace](#) section.

## Delete a Workspace App

You can delete a workspace app from the [Overview Page](#) by pressing the “...” icon and clicking the **Delete** button.

You can also delete a workspace app from a Workspace by clicking the “...” icon and select **Edit Ports** from a Workspace on the Overview or Workspaces Pages.



## Templates

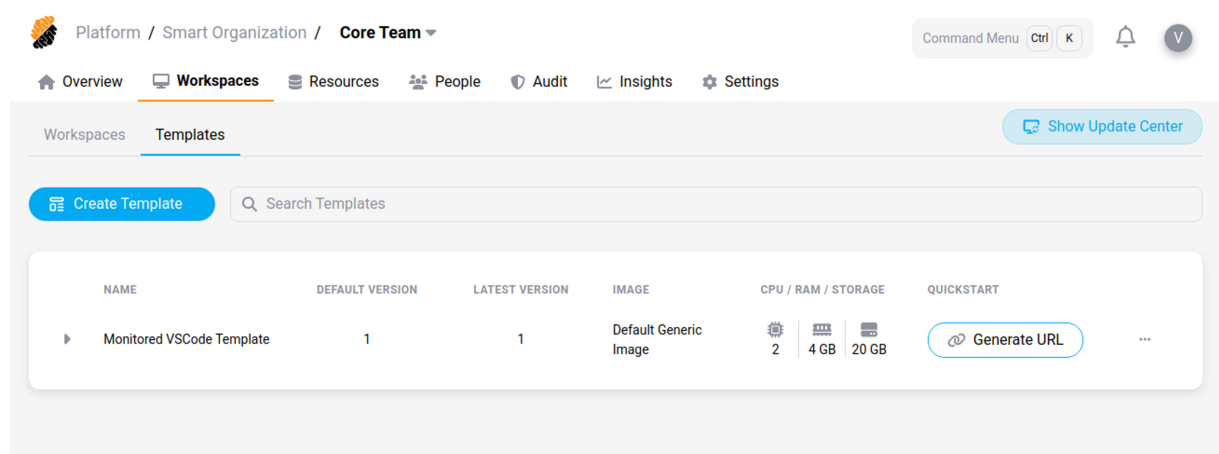
August 26, 2025

A **Template** is a particular [workspace](#) configuration stored for later reuse. They are useful to quickly create new workspaces with the same configuration as a previous one.

- [View Templates](#)
- [Default Templates](#)
- [Create a Template Permission: Workspaces::Manage Project](#)
- [Create a Workspace from a Template](#)

### View Templates

Templates are displayed in the “Templates” section of the [Workspaces Page](#).



A template is defined by the following characteristics:

- **Basic Information:** name, container image, CPU/RAM/Storage settings, and description,
- **Class Level:** confidential or regulated,
- **Workspace Configuration:** All the other elements describing a workspace.

### Default Templates

There are a few example templates provided in a standard project: Monitored VSCode, Restricted VS-Code and Inspected VSCode. They are provided as examples with the characteristics below:

| Name                              | Image                 | CPU / RAM / Storage  | Description  |
|-----------------------------------|-----------------------|----------------------|--|
| <b>Monitored VSCode Template</b>  | Default Generic Image | 2 CPU / 4 GB / 20 GB | This is a standard template to create an instance of a fully-updated Ubuntu container with monitored traffic and clipboard.  |
| <b>Restricted VSCode Template</b> | Default Generic Image | 2 CPU / 4 GB / 20 GB | This is a standard template to create an instance of a fully-updated Ubuntu container with restricted traffic with a series of exceptions (apt, npm, pip) and monitored clipboard. |

**Warning**

For the **Inspected VSCode Template**, applications using certificates in custom locations (folders) in the container will likely fail. Contact your administrator for more details.

**Create a Template Permission: `_Workspaces::Manage Project_`**

On the [Workspaces Page](#), in the “Templates” section, you can create a template by clicking on the “**Create Template**” button.

You will be asked to follow the same steps as if you were creating a workspace from scratch.

**Tip**

You can save a workspace as a Template by clicking on the “...” button and on **Save As Template**.

**Create a Workspace from a Template**

You can create a [workspace from an existing one](#) by pressing the “**Create from Template**” button on the drop-down button of the “**Create Workspace**” button.

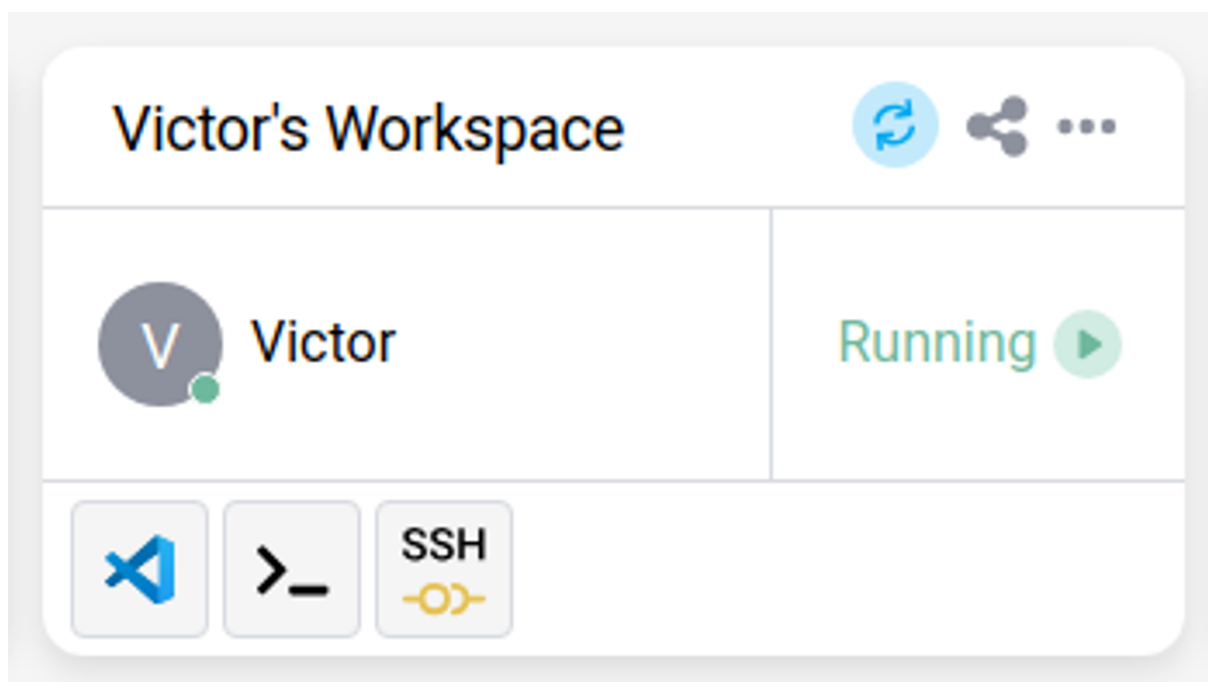
## Coding in a Workspace

August 26, 2025

The easiest way to code in a [workspace](#) is through a Cloud IDE. A Cloud IDE runs directly in the web browser and does not require other software installation on the endpoint, i.e. your development machine. Alternatively, a workspace can be accessed via an SSH connection from a locally installed IDE that allows “remote development”. See how it works in [Microsoft vscode](#).

### Cloud-Based Integrated Development Environments (Cloud IDEs)

The platform supports a series of Cloud IDEs that might differ based on your particular deployment. Typically supported IDEs are [Microsoft Visual Studio Code](#) and [Jetbrains’ IDEs](#). Note that the version of The vscode running in the web browser is the same as the one available for local installation (including the marketplace). Hence, you can refer to any available documentation online to understand [its functioning and options](#).

**Tip:**

To access a workspace using the Cloud IDE attached to it, just click the button indicating the workspace execution status. This is only possible if you own or have shared access to the workspace.

## Import Local Files in a Cloud IDE

The ability to import local files in the Cloud IDE depends on the setting of your platform. The most common way to do so is to simply drag a file from a user interface such as a browser, to the IDE interface. Please contact the platform administrator to inquire about potential security restrictions imposed on such an operation.

## Workspace Access Using SSH With a Local IDE

You can access your workspace using SSH via a locally installed IDE such as Microsoft VSCode or using [JetBrains Gateway](#). For this, you must [register a SSH authentication key](#) to your account in your [Profile Page](#).

Once the key has been registered, you can access the workspace via a two-factor authentication process. This process ensures that you are indeed accessing your workspace remotely and at preventing an authorized user to do so.

You can find a full guide on how to SSH into your Workspace [here](#).

## Work With a Shared Workspace

After [sharing a workspace](#), you may work with other users in the same workspace. Working in a shared workspace is similar in a way to use work simultaneously in the same document. The benefit of doing so is that it provides a way to co-edit content, also known as **peer editing**.

### Tip:

When modifying files on the same workspace, **changes are displayed in real-time**. You may see who is accessing the workspace live from the “*(show component)*”.

## Recover a deleted Workspace

After deleting a Workspace, you may recover it for 7 days from the [Project Settings](#).

### Note:

Only a project owner can recover a workspace. If you do not have the necessary privileges, please contact the owner of your project.

## SSH Into Your Workspace

August 26, 2025

This guide provides instructions for accessing your workspace via SSH, enabling you to edit code directly using a local command-line editor. This process requires the generation of an SSH Key pair.

- [1. Generate an SSH Key Pair on UNIX and UNIX-like Systems](#)
- [2. Upload Your Public Key to the Platform](#)
- [3. Authorize Your Workspace to Use Your SSH Key](#)
- [4a. Connect to Your Workspace Using a Shell](#)
- [4b. Connect to Your Workspace via SSH Using VSCode](#)
  - [4b.1. Install the VSCode SSH Extension](#)
  - [4b.2. Initiate a New SSH Connection from the VSCode SSH Extension](#)
  - [4b.3. Input the SSH Command into the Extension Prompt](#)
  - [4b.4. Select the Default SSH Configuration](#)
  - [4b.5. Click the “Connect” Button after the Host is Added](#)
- [4c. Connect to Your Workspace via SSH Using JetBrains Gateway](#)
  - [4c.1. Install JetBrains Gateway](#)
  - [4c.2. Begin a New SSH Connection](#)
  - [4c.3. Create an SSH Configuration](#)
  - [4c.4. Enter the Host and Username Information](#)
  - [4c.5. Choose Authentication Method and Test Your SSH Configuration](#)
  - [4c.6. Select an SSH Configuration](#)
  - [4c.7. Verify Your SSH Configuration and Connect to Your Workspace](#)
  - [4c.8. Choose and Download the JetBrains IDE](#)
  - [4c.9. Access Your Workspace](#)

### 1. Generate an SSH Key Pair on UNIX and UNIX-like Systems

- To generate an SSH key pair on UNIX and UNIX-like systems, run the `ssh-keygen` command in your terminal:

```
1 ssh-keygen
```

- The terminal will suggest a default path and file name (for example, `/home/user_name/.ssh/id_rsa`). To accept the default path and file name, press Enter. If you want to specify a different path and file name, enter those details and then press Enter.



- The command prompts you to enter a passphrase. Although optional, it's recommended to set a passphrase for additional security against unauthorized use of your private key.
- If you set a passphrase, you will be prompted to enter it again for confirmation. If you didn't set a passphrase, simply press Enter.
- The command generates an SSH key pair - a public key and a private key - and saves them in the specified path. The public key file name is automatically created by appending .pub to the private key file name. For instance, if the private key file is named id\_rsa, the public key file will be named id\_rsa.pub.

```

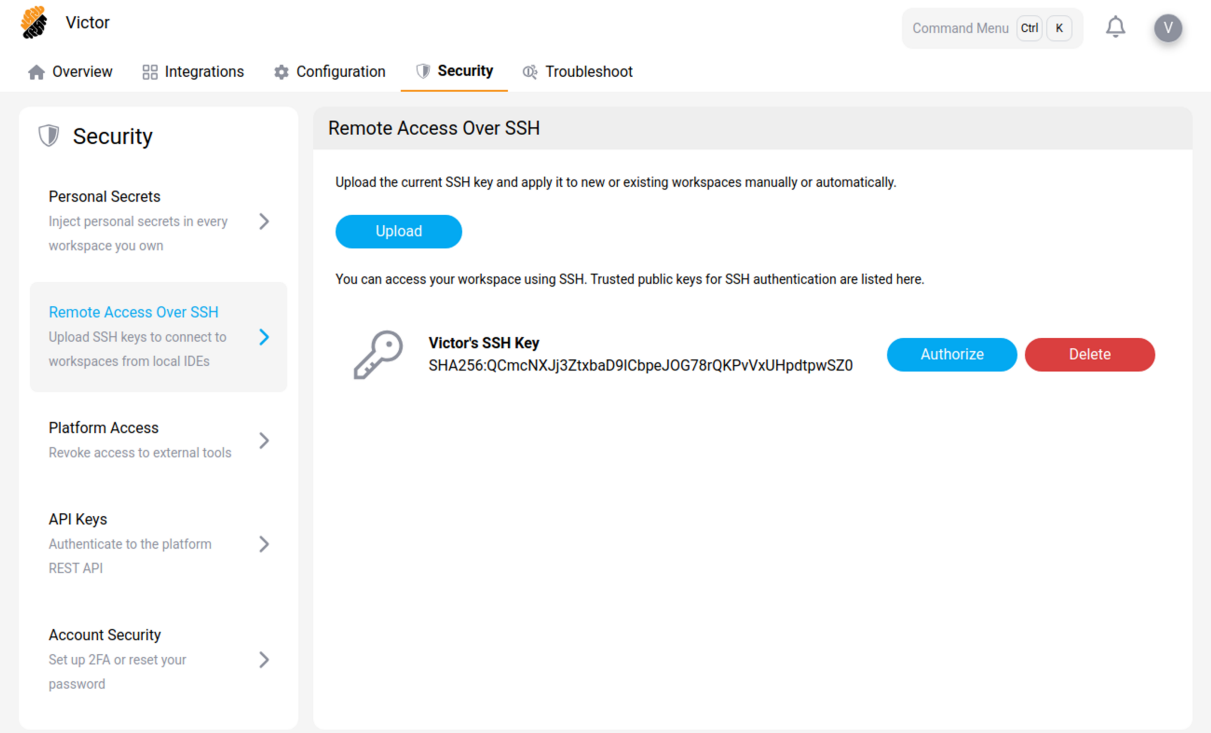
wepzen — developer@ws-932331191353506-0: ~ — zsh — 105x24
(base) wepzen@Awens-MacBook-Pro ~ % ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/wepzen/.ssh/id_rsa): id_rsa2
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_rsa2
Your public key has been saved in id_rsa2.pub
The key fingerprint is:
SHA256:PALbYrSmP/QpP337zLotdElqs3lcbk1E0U2N2Hj8pPo wepzen@Awens-MacBook-Pro.local
The key's randomart image is:
+----[RSA 3072]-----+
|
|      =.+
|      o * =
|      o      o +
|      . = .      . o .
|      * o S      o +
|      +. . . = + o
|      .. . o o * = .
|      .o + . =+o E
|      .+. . +B=.
+----[SHA256]-----+
(base) wepzen@Awens-MacBook-Pro ~ % █

```

## 2. Upload Your Public Key to the Platform

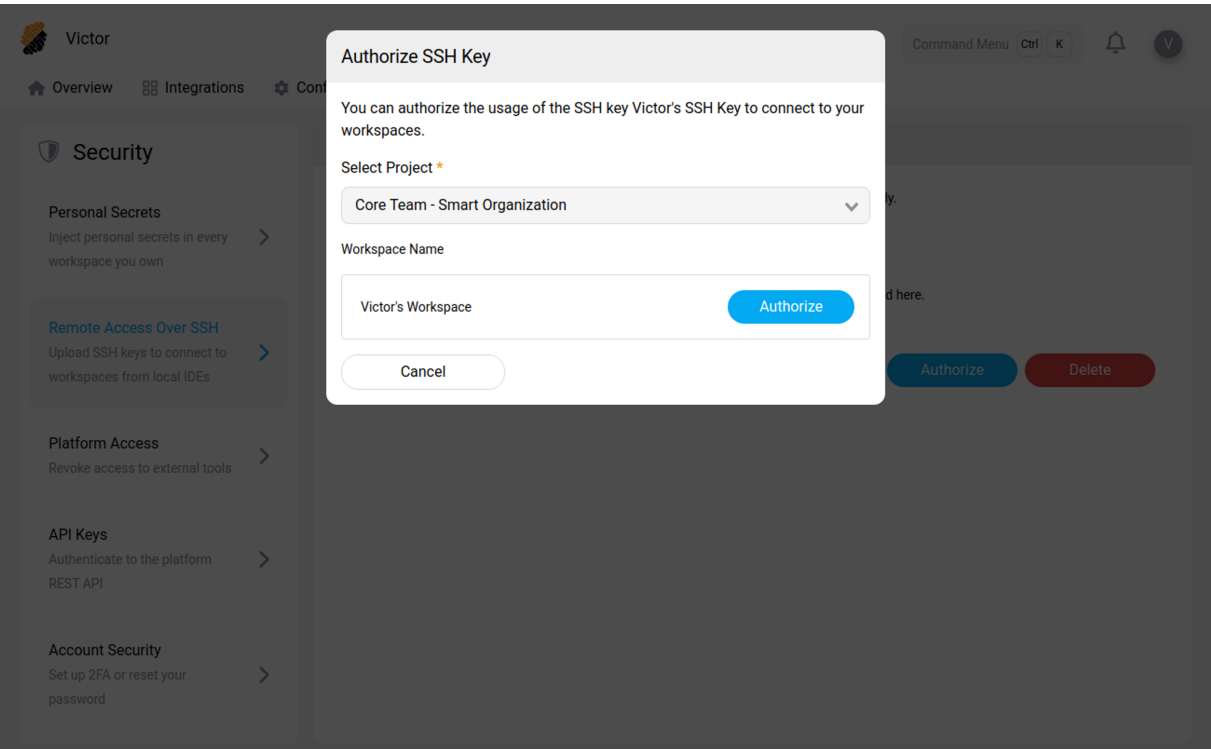
Once your SSH Key pair is generated, you need to upload it to the [SSH Keys Section](#) in your [Profile](#).

The key begins with 'ssh-rsa', 'ecdsa-sha2-nistp256', 'ecdsa-sha2-nistp384', 'ecdsa-sha2-nistp521', 'ssh-ed25519', 'sk-ecdsa-sha2-nistp255@openssh.com' or 'sk-ssh-ed25519@openssh.com'.



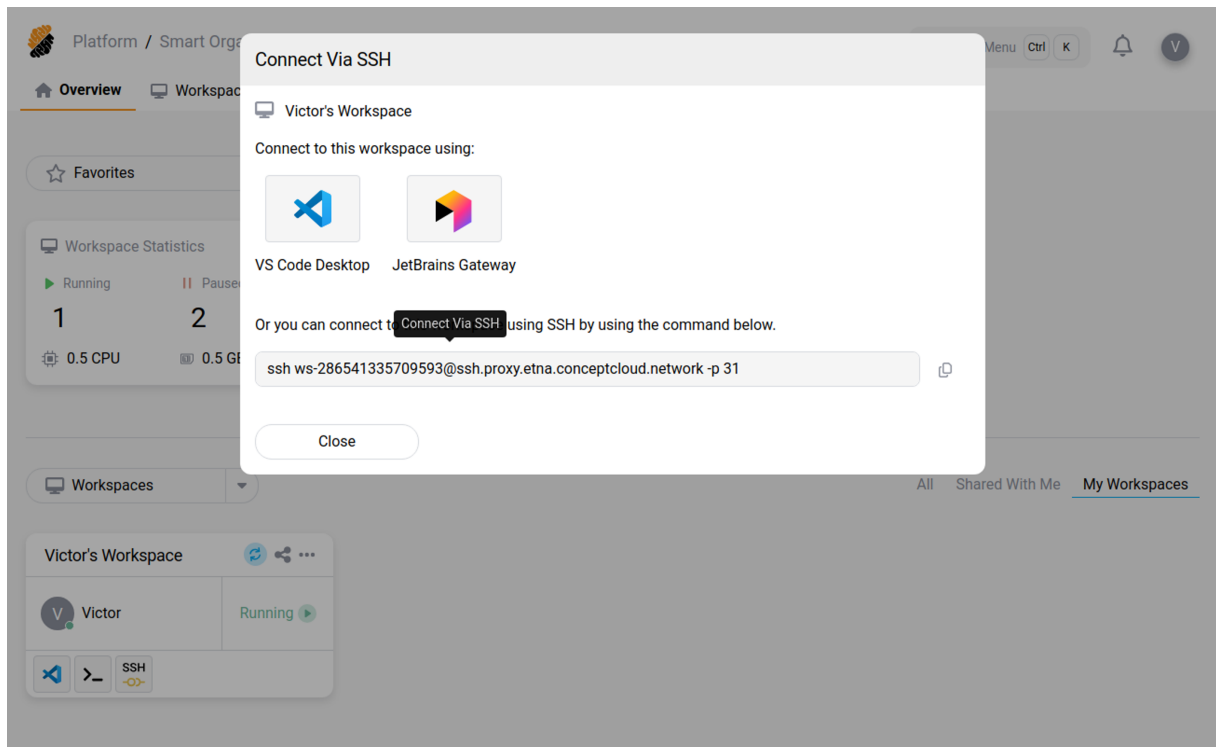
3. Authorize Your Workspace to Use Your SSH Key

After uploading your SSH key to your profile, you need to authorize your workspace(s) to access it.

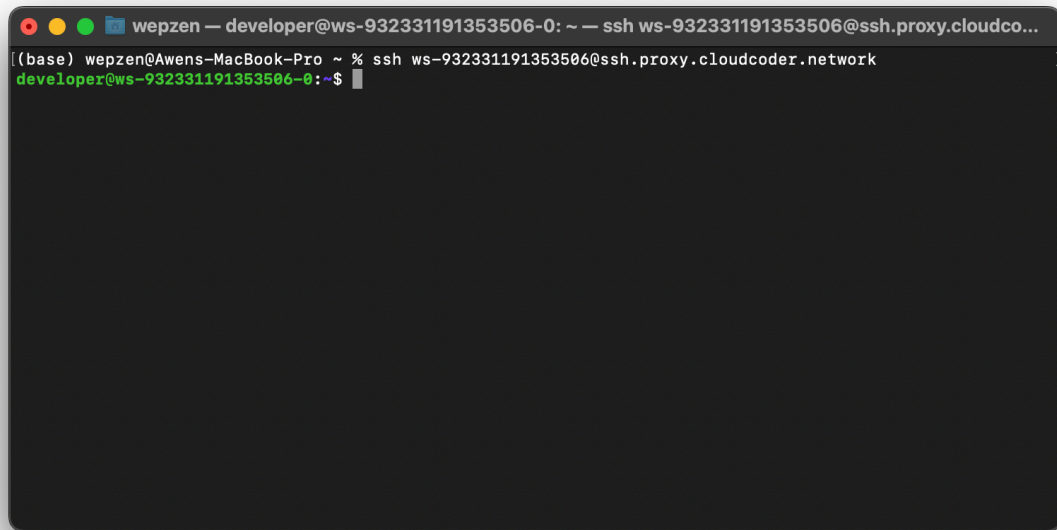


#### 4a. Connect to Your Workspace Using a Shell

Navigate to the [Running Actions List of Your Workspace](#) and select the “Connect With SSH” option. This action will display the `ssh` command that you need to establish an SSH connection to your Workspace.



Input this command in your terminal.



Once this is done, you will have successfully established an SSH connection to your Workspace!

#### **4b. Connect to Your Workspace via SSH Using VSCode**

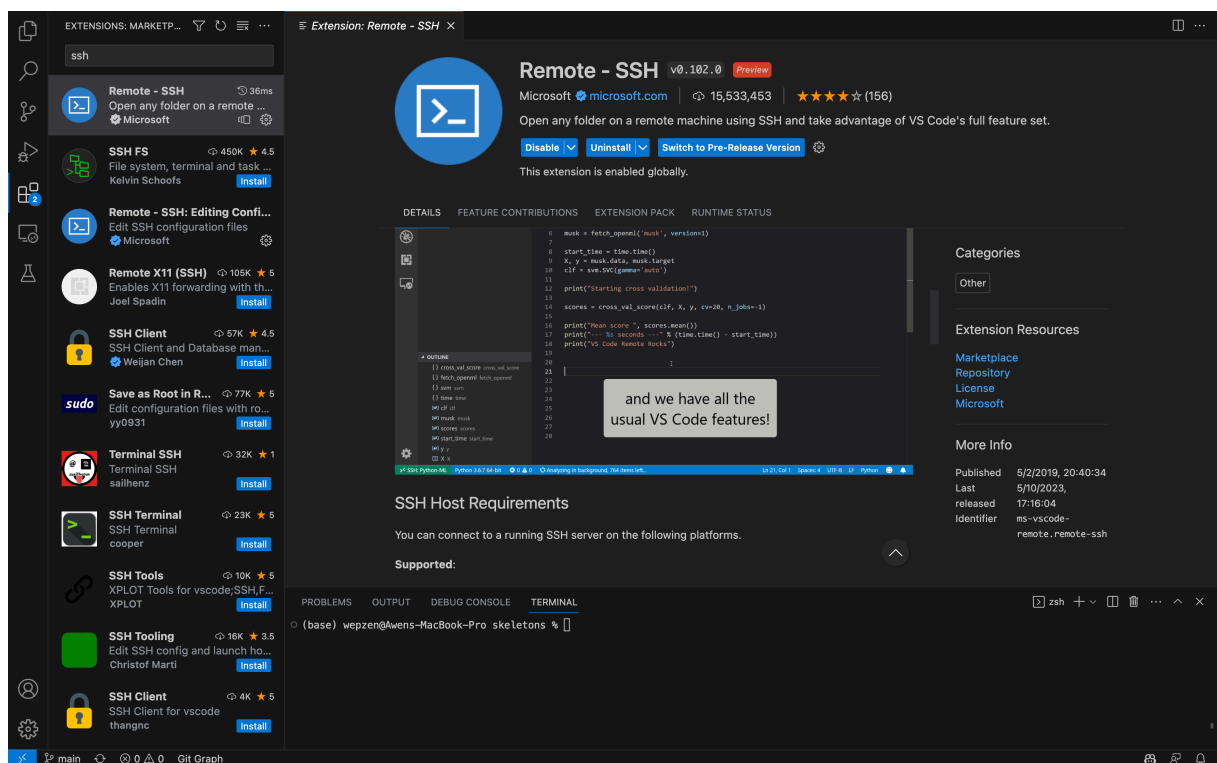
This section provides a detailed walkthrough on setting up an SSH connection to your workspace using the VSCode SSH extension.

##### **Tip**

Note that you can execute the same steps directly from your terminal, beginning with step 5b.3.

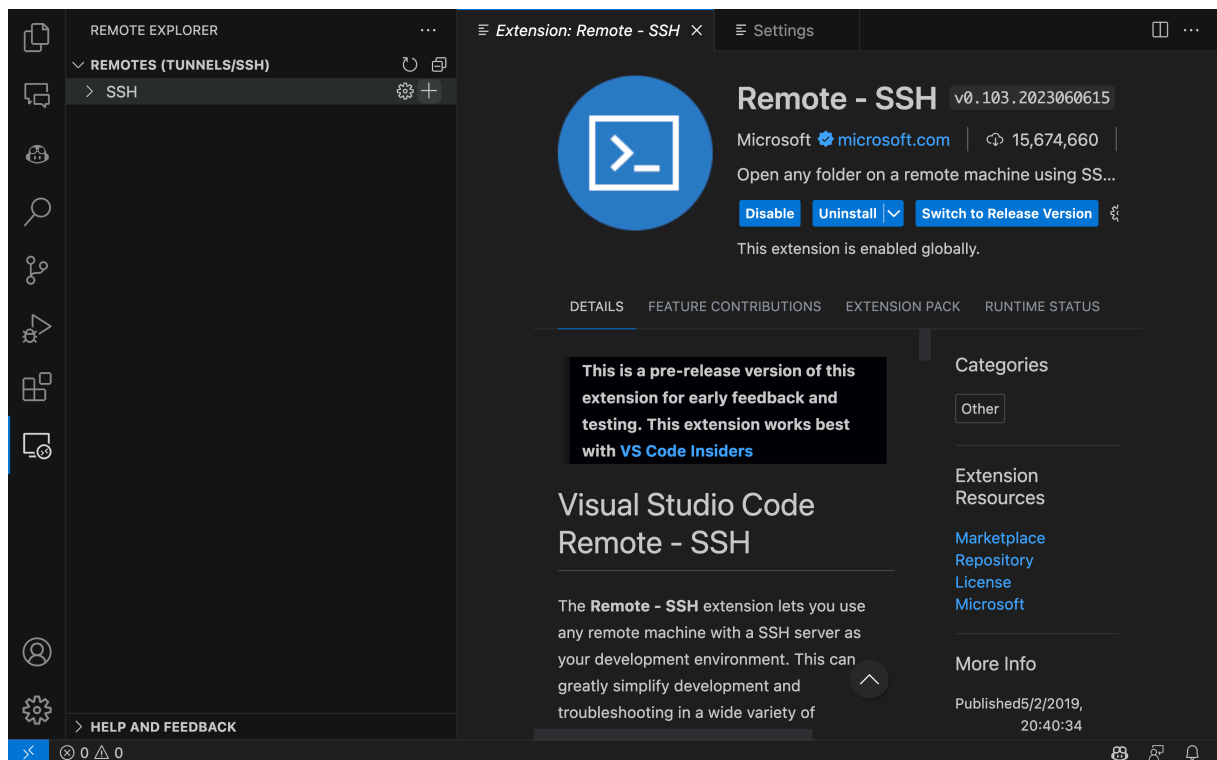
##### **4b.1. Install the VSCode SSH Extension**

To SSH into your workspace directly from your local VSCode IDE, you can download the [Microsoft SSH Extension](#). This extension replicates the usual SSH command you would perform from your terminal, but allows you to work directly within your local VSCode.



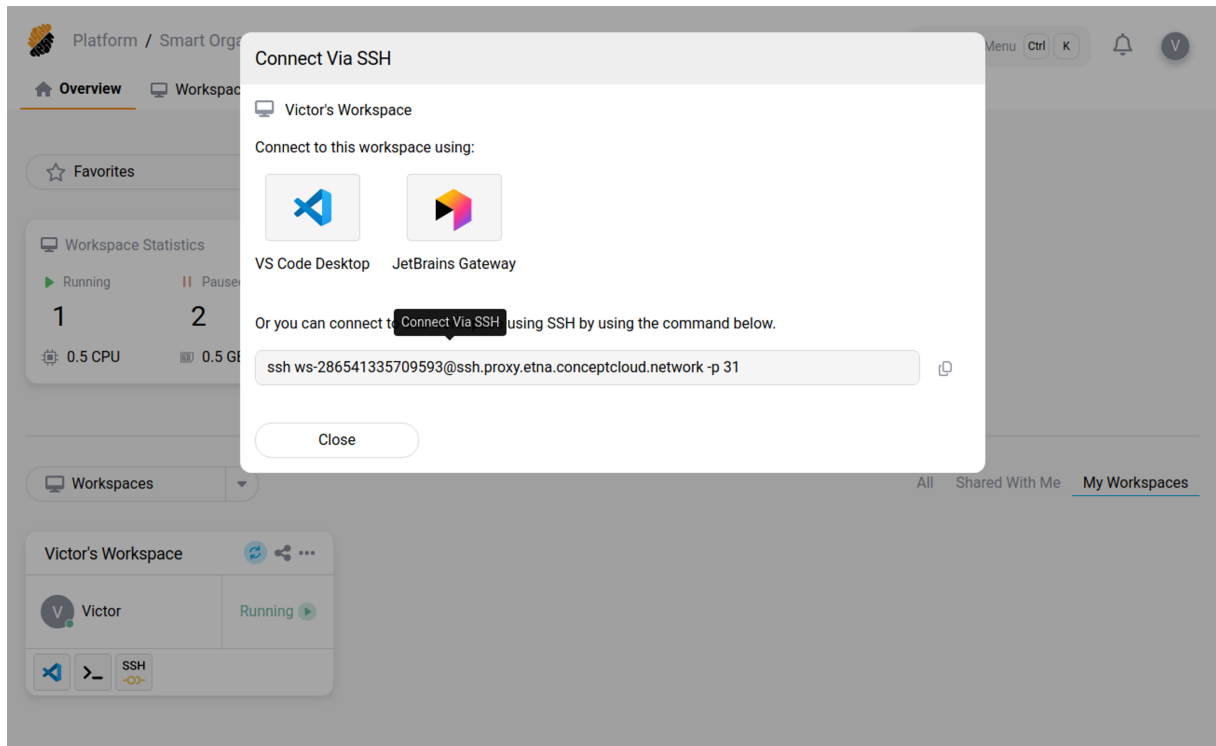
#### 4b.2. Initiate a New SSH Connection from the VSCode SSH Extension

By clicking the “+” button next to the “SSH” panel in the VSCode Extension section.

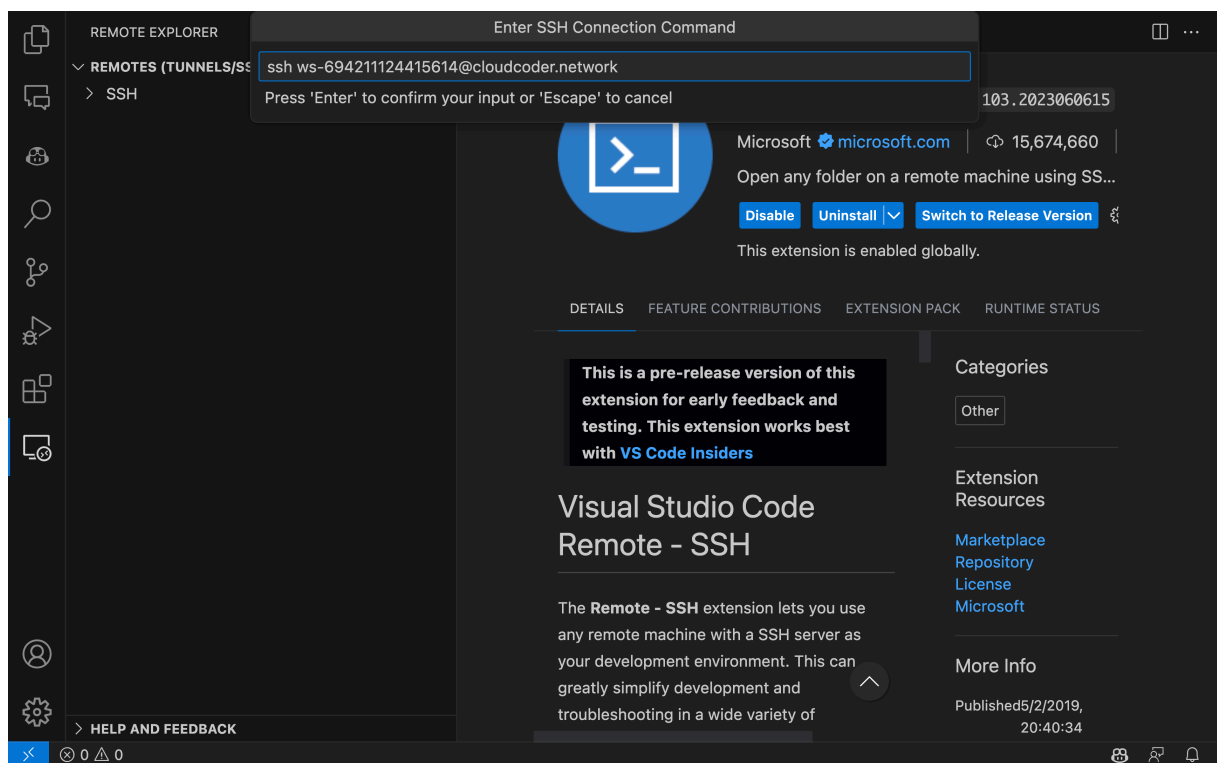


### 4b.3. Input the SSH Command into the Extension Prompt

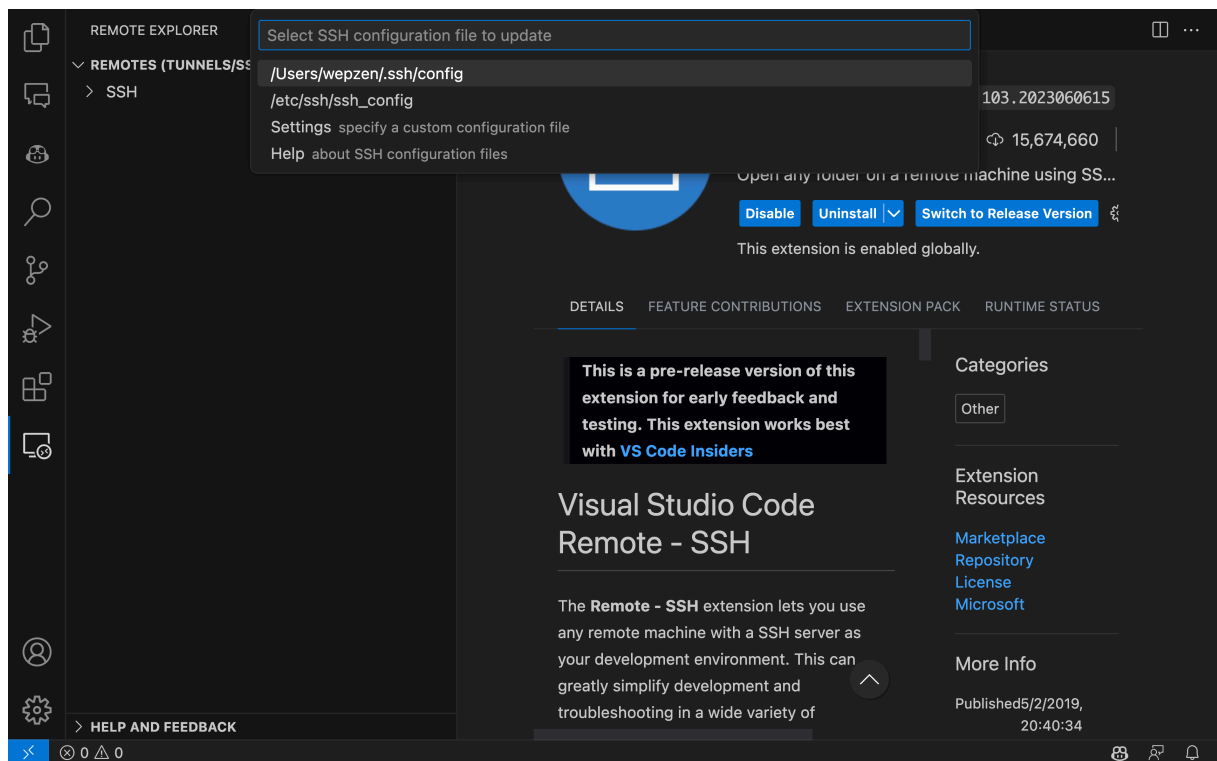
From your [Workspace's Running Actions List](#) select the “Connect With SSH” option to display the `ssh` command you need to connect to your Workspace via SSH.



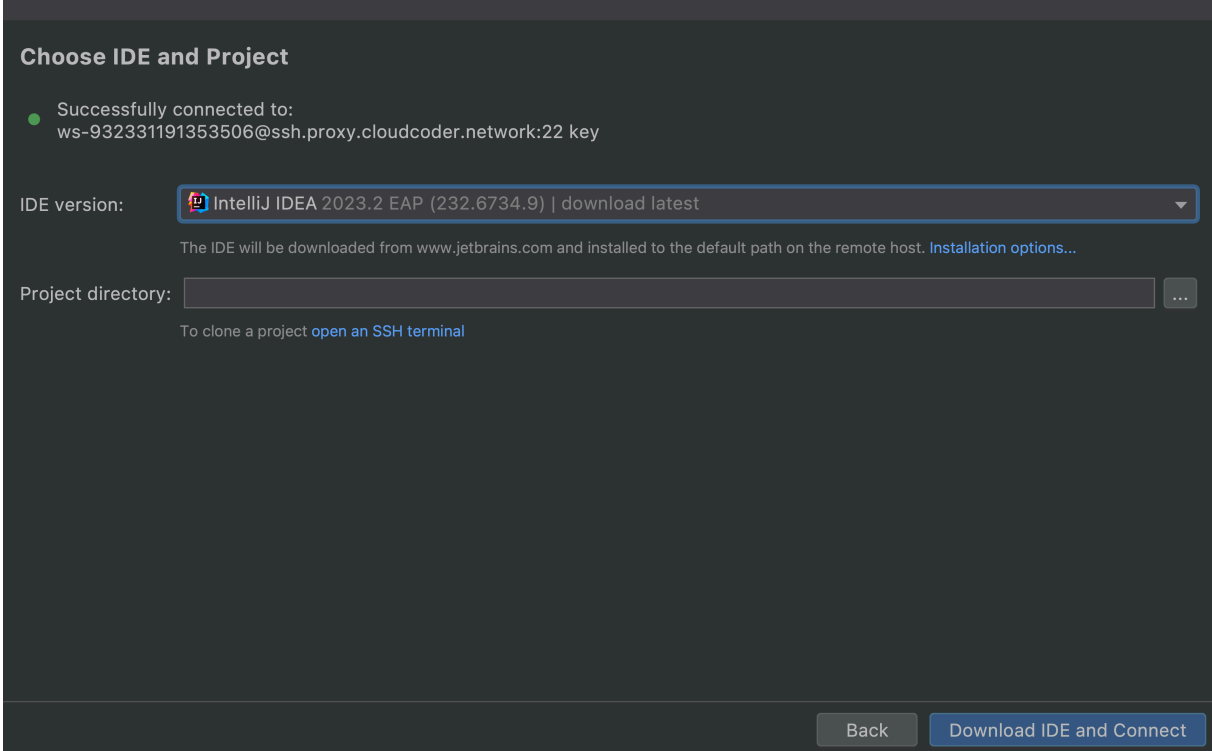
Enter this command in the VSCode extension prompt.



#### 4b.4. Select the Default SSH Configuration



#### 4b.5. Click the “Connect” Button after the Host is Added



The screenshot shows a dark-themed window titled "Choose IDE and Project". At the top, a green status indicator and text confirm a successful connection to the workspace: "Successfully connected to: ws-932331191353506@ssh.proxy.cloudcoder.network:22 key". Below this, the "IDE version:" is set to "IntelliJ IDEA 2023.2 EAP (232.6734.9) | download latest". A note states: "The IDE will be downloaded from www.jetbrains.com and installed to the default path on the remote host. [Installation options...](#)". The "Project directory:" field is empty, with a button to open a file explorer and a link to "open an SSH terminal" for cloning a project. At the bottom right, there are two buttons: "Back" and "Download IDE and Connect".

You are successfully connected to your Workspace with SSH!

#### 4c. Connect to Your Workspace via SSH Using JetBrains Gateway

This section offers a comprehensive guide on establishing an SSH connection to your workspace using JetBrains Gateway.

##### 4c.1. Install JetBrains Gateway

To access your workspace directly from your local JetBrains IDE, download [JetBrains Gateway](#). This software enables SSH connection to your workspace using JetBrains.



**Remote Development**

JetBrains Gateway is a compact desktop app that allows you to work remotely with a JetBrains IDE without even downloading one.

**Install JetBrains Gateway**

[Download](#) [.dmg](#)

Space Gateway Fleet

Matt Ellis, Nov 29, 2021

**JetBrains Gateway is a key to remote development.**

Use JetBrains Gateway to access your IntelliJ IDEs running on remote backends via SSH. Read more about how to get started in the blog post

Featured blog posts

**Gateway is where it all gets started:**

#### 4c.2. Begin a New SSH Connection

Start by clicking the “New Connection” button found below the “SSH Connection” title.

JetBrains Gateway  
2023.1.2

All Providers

Connections

SSH

JetBrains Space

Connect with a Link

Run the IDE Remotely

SSH Connection

New Connection More

Connect to Space More

Install More Providers

Gitpod

Install More

Google Cloud

Install More

GitHub Codespaces

Install More

Amazon CodeCatalyst

Install More

### 4c.3. Create an SSH Configuration

Click the “settings icon” next to the “New Connection” option.

**Connect to SSH**

ⓘ Ensure Linux is installed on the remote machine.  
As of now, only Linux is supported. The support of macOS and Windows machines will be available in one of the upcoming product versions.

Connection: <New Connection> ⚙

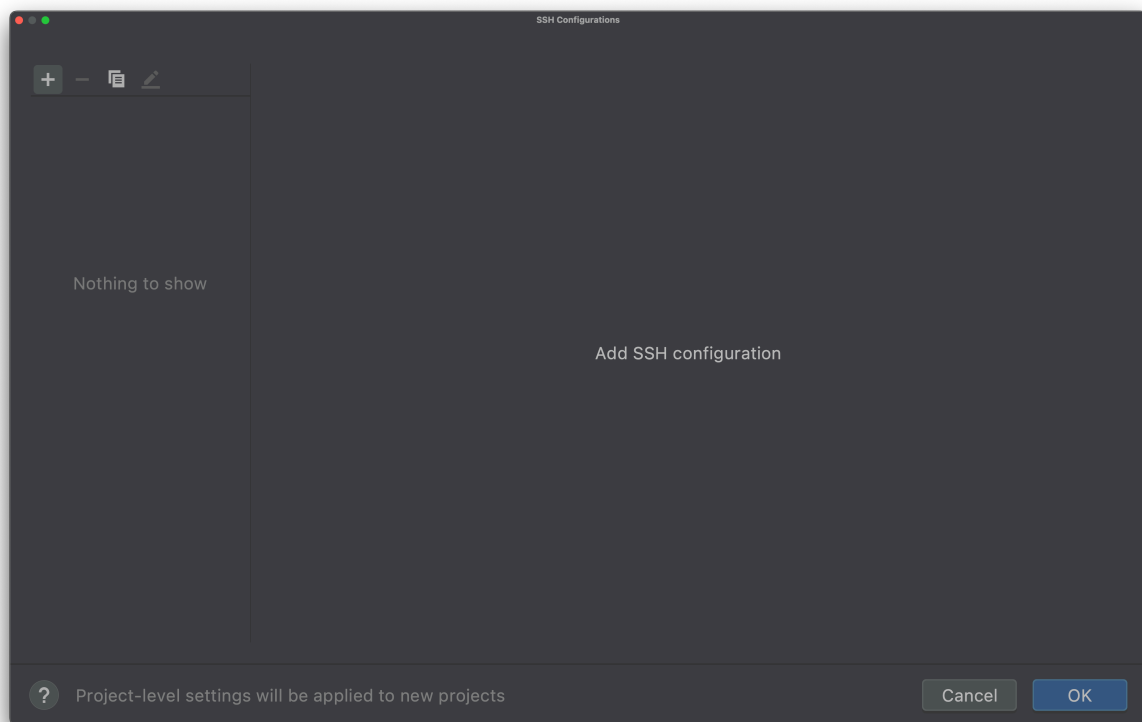
Username:

Host:  Port:

☐ Specify private key

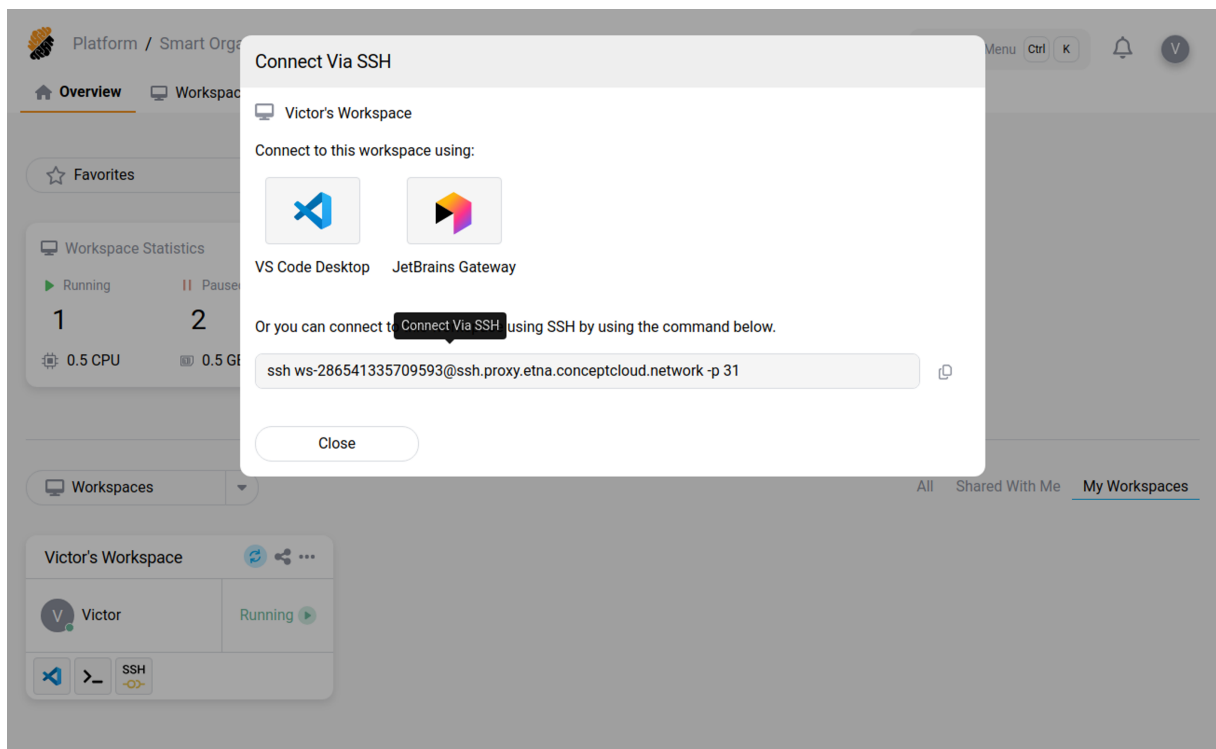
Back Check Connection and Continue

Then click the “+” icon to add a new SSH configuration.



#### 4c.4. Enter the Host and Username Information

Select the “Connect With SSH” option from your [Workspace’s Running Actions List](#) to view the `ssh` command necessary for the SSH connection to your workspace.

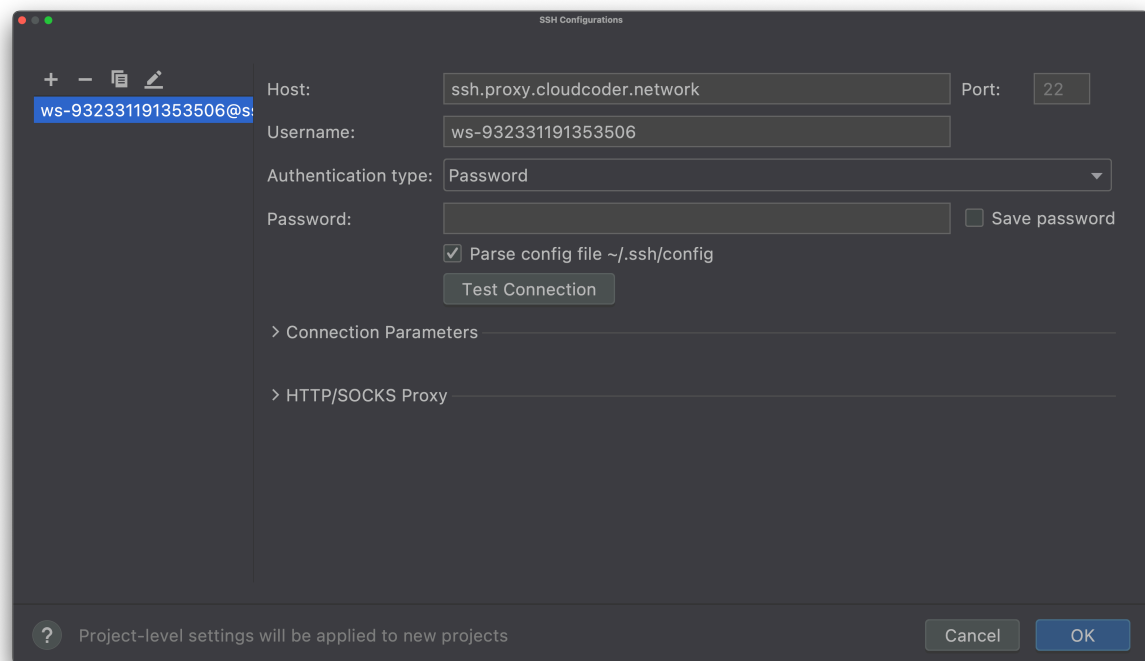


Enter the command details into the SSH configuration settings.

**Tip**

- Host = second part of the command (example: `ssh.proxy.cloudcoder.network`)
- Username = first part of the command (example: `ws-694211124415614`)

Disregard the `ssh` and `@` characters.

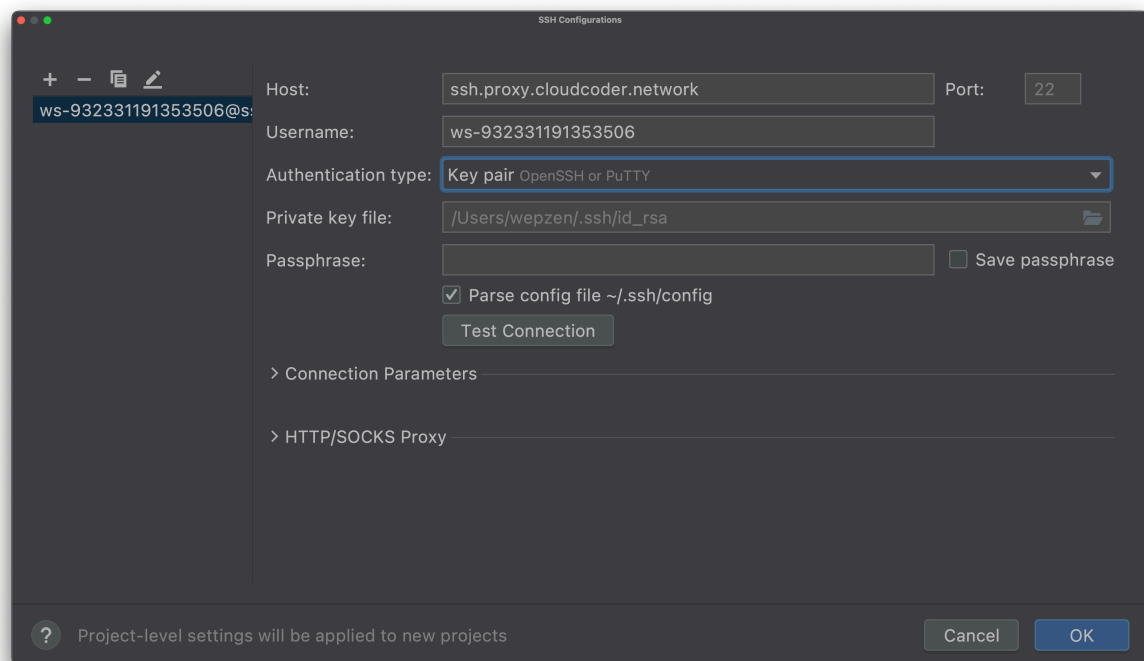


#### 4c.5. Choose Authentication Method and Test Your SSH Configuration

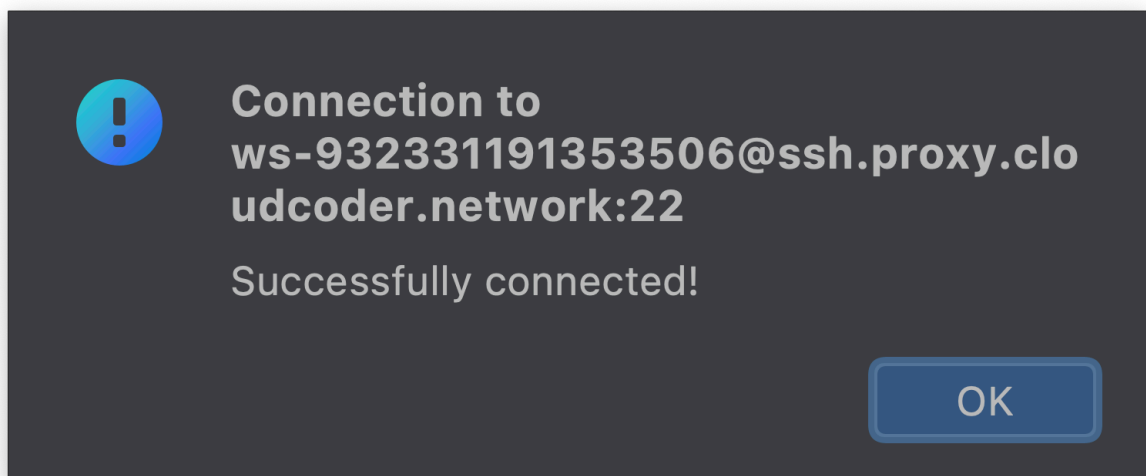
Select “Key Pair” as the “Authentication type” and provide the path for your key (the default field can be left as is).

##### Warning

By default, the “Password” option is selected as the authentication method.



After filling in the “Host”, “Username”, and “Authentication method” fields, test your SSH configuration by clicking the “Test Connection” button. You should see the following:



#### 4c.6. Select an SSH Configuration

Upon validating your SSH configuration by clicking “Ok”, select your new configuration as the “Connection” in the “Connect to SSH” menu.

**Connect to SSH**

Connection: ws-932331191353506@ssh.proxy.cloudcoder.network:22 key ⚙

Username: ws-932331191353506

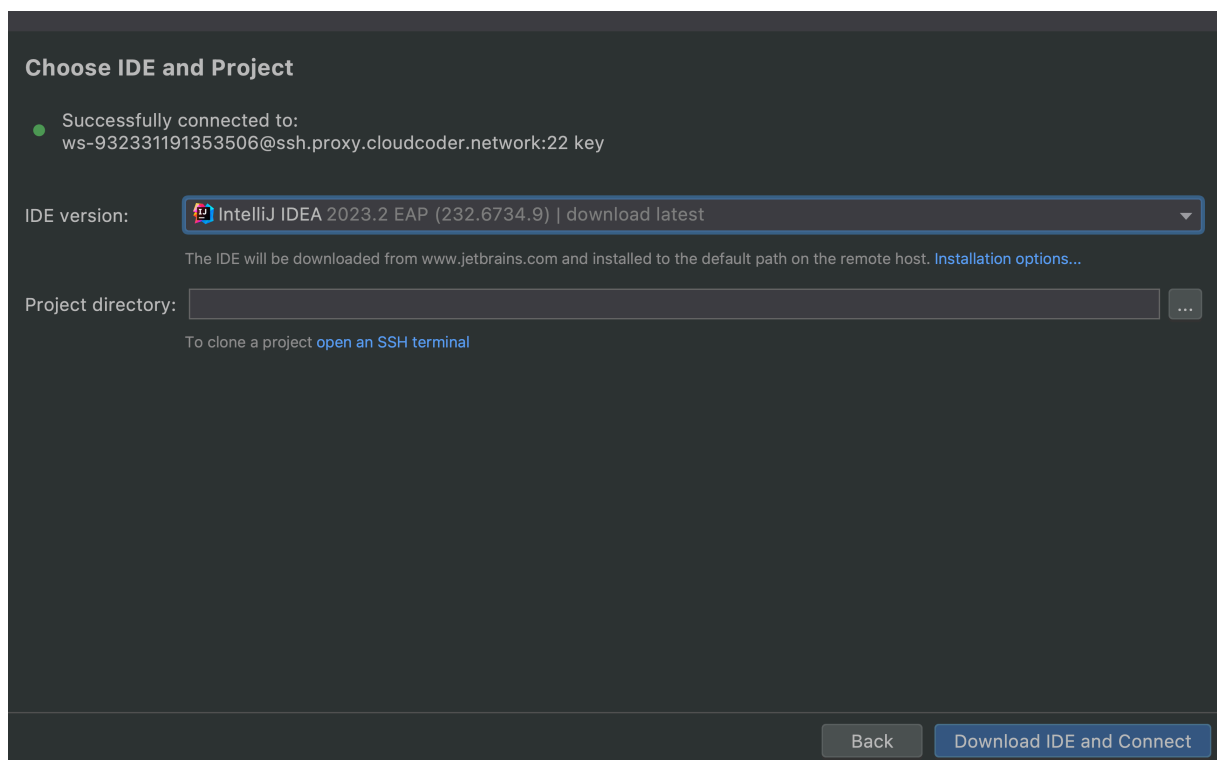
Host: ssh.proxy.cloudcoder.network Port: 22

☒ Specify private key /Users/wepzen/.ssh/id\_rsa 📁

Back Check Connection and Continue

#### 4c.7. Verify Your SSH Configuration and Connect to Your Workspace

Validate your connection by clicking the “Check Connection and Continue” button. If the connection is successful, you will be directed to the following screen:



#### 4c.8. Choose and Download the JetBrains IDE

On the successful connection screen, select the JetBrains IDE you wish to use and the folder you intend to open.



### Choose IDE and Project

● Successfully connected to:  
ws-932331191353506@ssh.proxy.cloudcoder.network:22 key

IDE version: IntelliJ IDEA 2023.2 EAP (232.6734.9) | download latest

The IDE will be downloaded from [www.jetbrains.com](https://www.jetbrains.com) and installed to the default path on the remote host. [Installation options...](#)

Project directory: /home/developer/monorepo

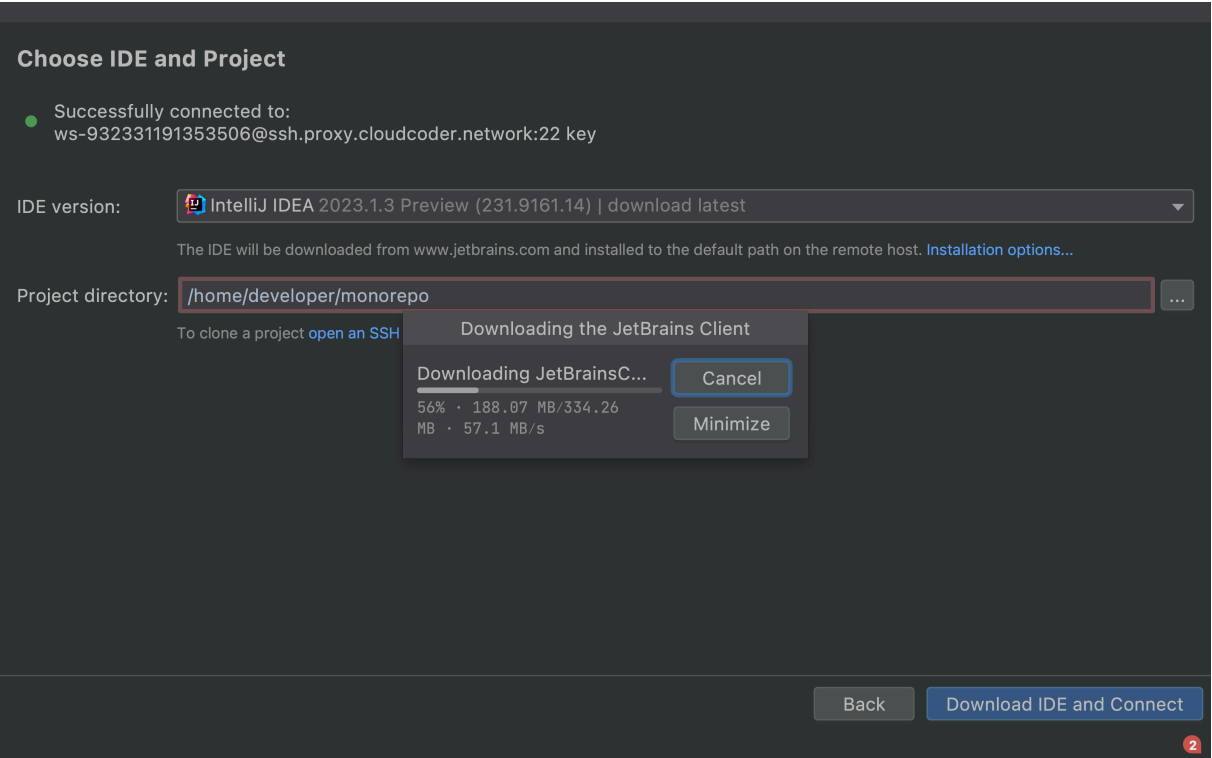
To clone a project [open an SSH terminal](#)

Back Download IDE and Connect

Confirm your selections by clicking “Download IDE and Connect”. The following screen indicates that the IDE is being downloaded to your workspace.

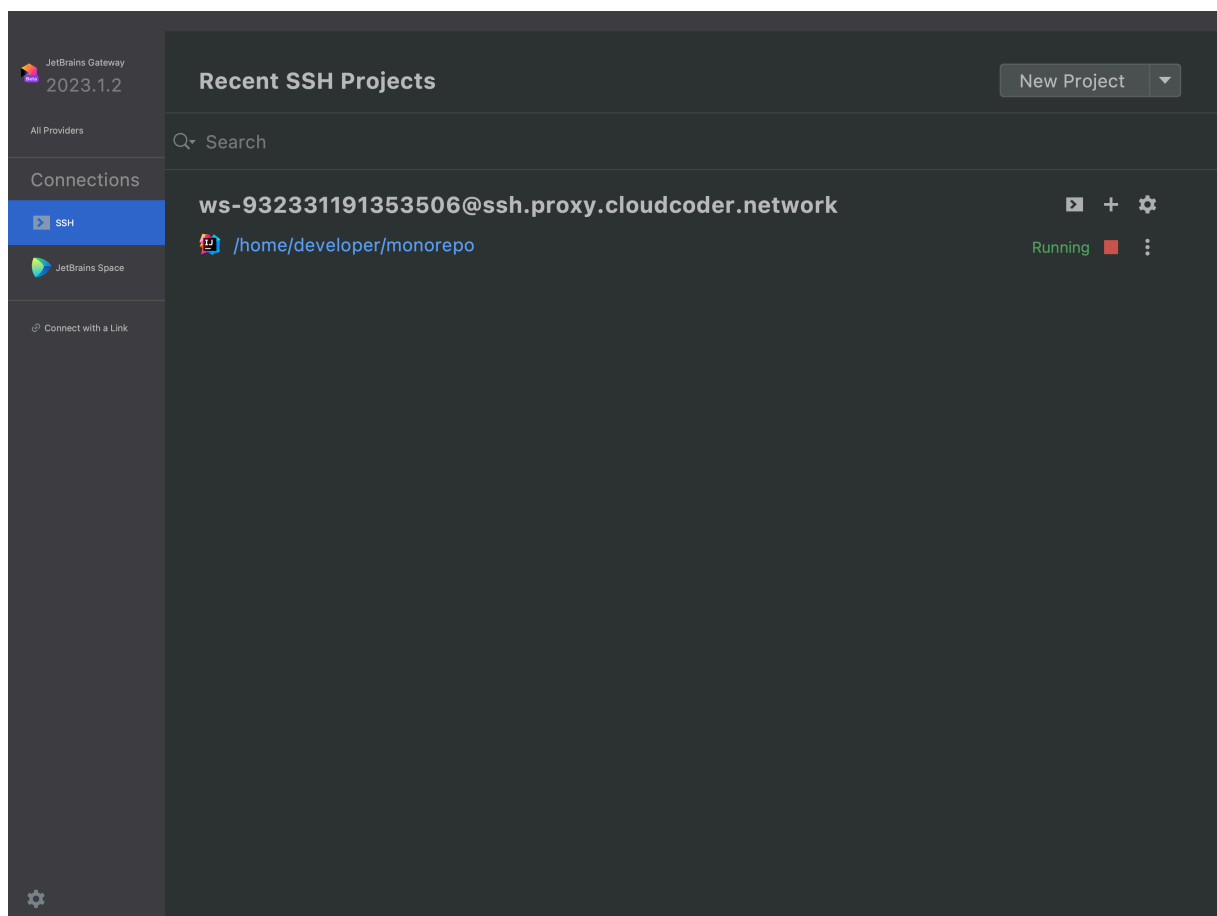
#### Tip

The IDE is downloaded to your workspace, not to your local machine.



**4c.9. Access Your Workspace**

After the completion of the IDE installation, you can now access your workspace via JetBrains Gate-  
way!



## Resources Page

On the resources page, you can view and manage the different resources used in the [project](#).

Resources are used to define workspace properties such as container configuration and network policies, or the information available to users for development

such as code repositories, data buckets, secrets and services. Resources are managed at three levels of granularity depending on the intended scope of use: platform, organization and project.

Resources are attached to a [workspace](#) during the setup and update process. When resources are accessible to users, this process is a means to define a fine-grain access control policy on an individual workspace basis.

The screenshot displays the Citrix Secure Developer Spaces web interface. At the top, the breadcrumb navigation shows 'Platform / Smart Organization / Core Team'. The main navigation bar includes 'Overview', 'Workspaces', 'Resources' (highlighted), 'People', 'Audit', 'Insights', and 'Settings'. The 'Resources' section is active, showing a sidebar with 'Repository Access Control' (selected), 'Data Buckets', 'Secrets', 'Connected HTTP Services', 'Connected SSH Services', and 'Container Images'. The 'Repository Access Control' panel shows a table of repositories. The table has columns for 'NAME', 'ADDED BY', and 'URL'. There are two repositories listed: 'markotest' and 'test'. The 'markotest' repository was added by user 'A' and has a URL 'https://github.com/test-multiple-orgs/markotest.git'. The 'test' repository was added by user 'T' and has a URL 'https://bitbucket.org/tormey97/test'. The table also shows counts for 'All (2)', 'Used (0)', and 'Unused (2)'.

| NAME      | ADDED BY | URL   |
|-----------|----------|---|
| markotest | A        | https://github.com/test-multiple-orgs/markotest.git |
| test      | T        | https://bitbucket.org/tormey97/test                 |

## Content

- [Repository access control](#)
- [Data buckets](#)
- [Secrets](#)
- [Connected HTTP services](#)
- [Connected SSH services](#)
- [Container images](#)

## Code Repositories

August 26, 2025

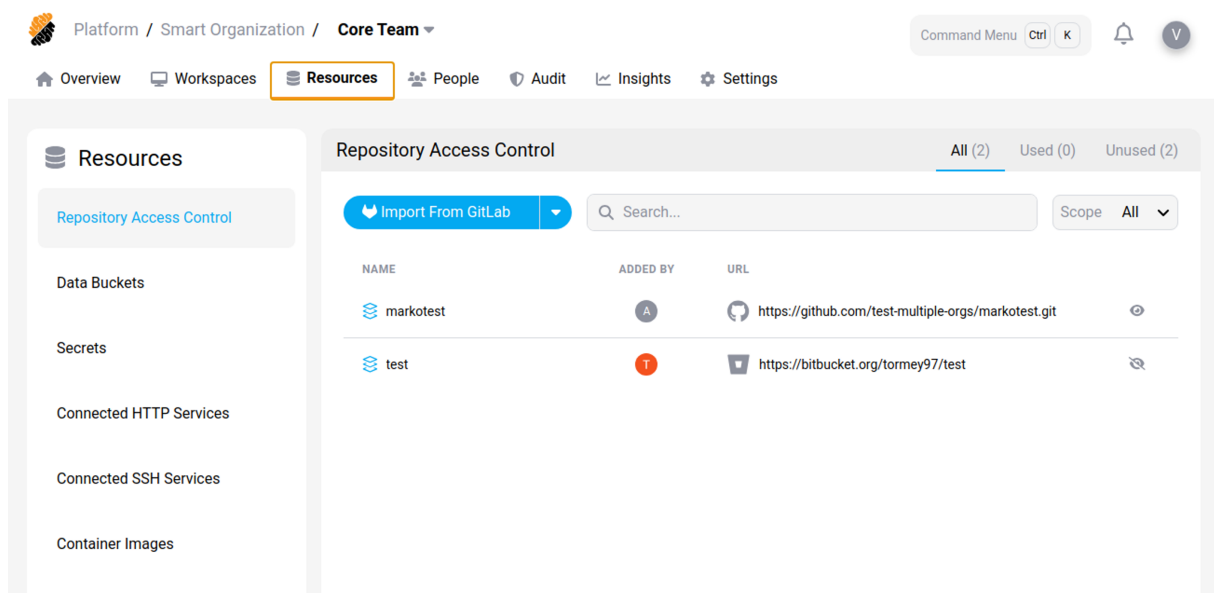
Code repositories are used for storing, tracking, and collaborating on source code developed using software development projects. The format supported by the

platform to manage source code repositories is GIT. Therefore assets from providers using this format can be imported to the platform and attached to workspaces. Currently, providers such as GitHub, GitLab and BitBuckets are supported. In addition, you can import GIT repositories manually by providing the necessary information.

- [View Repositories](#)
- [Import a Repository Permission: Resources::Import](#)

## View Repositories

Code Repositories whose information has been imported in the project are displayed in the table. You may search for one or filter those used in [workspaces](#).

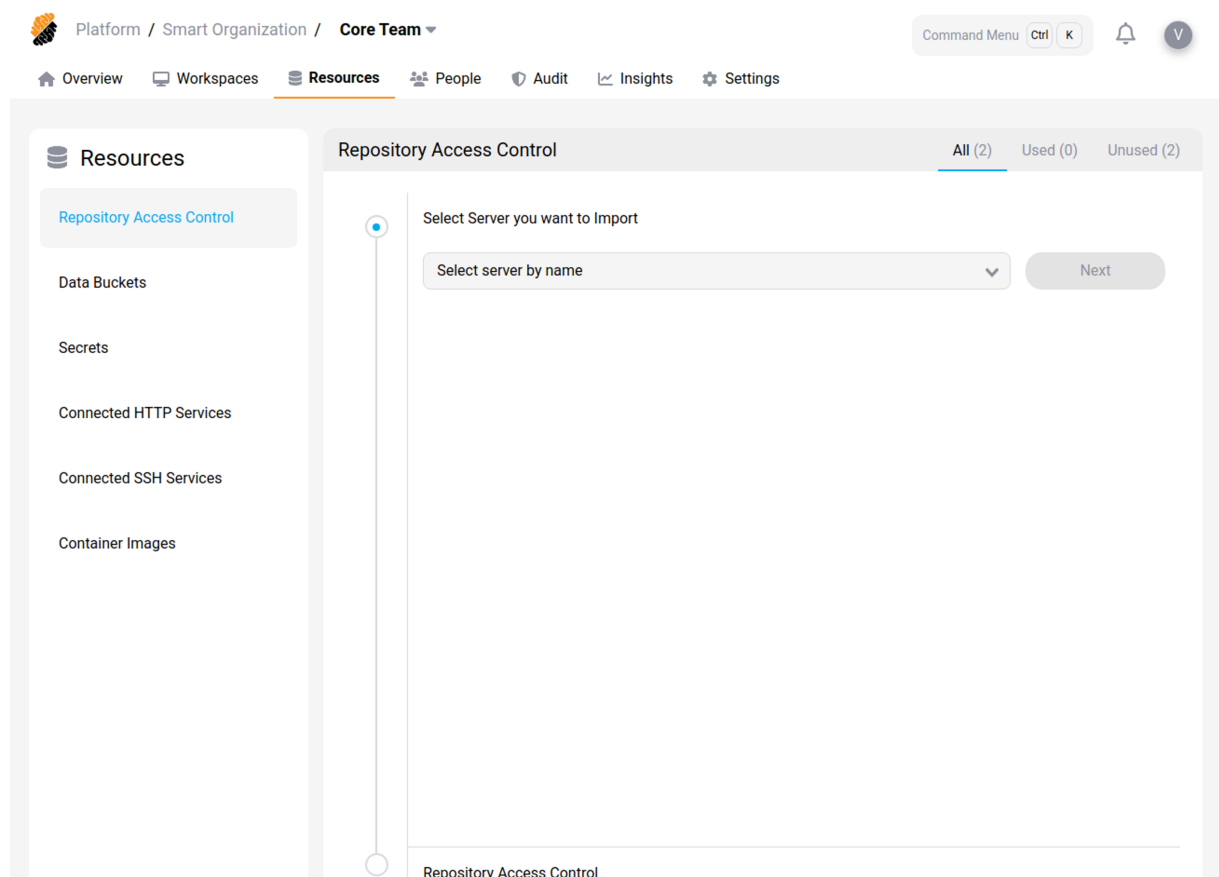


A code repository is defined by the following characteristics:

- **Basic information:** Information such as name, scope of use (platform, organization or project), the user who added it, GIT service provider e.g. GitHub, GitLab, BitBucket, URL.
- **Class Level:** This option defines the visibility for the repository based on the user's permissions.
- **Asset Information:** This option allows for providing a description of the repository.

## Import a Repository Permission: `_Resources::Import_`

You can import a code repository by pressing the “**Import Repository**” button. Make sure to select the actual provider, i.e. GitHub, GitLab or Bitbucket. The remote GIT application is scanned for code repositories and you can import the repo information by clicking the button next to the name.



## Data Buckets

July 8, 2025

A **Data Bucket** is used for general, unstructured storage of data online. This is basically a folder in S3 format that is commonly used to store and access large datasets. Most cloud vendors offer S3 data buckets as a general storage data mechanism. The platform supports buckets from vendors such as Azure, Google and Amazon Web Services. They are particularly popular for Data Science applications.

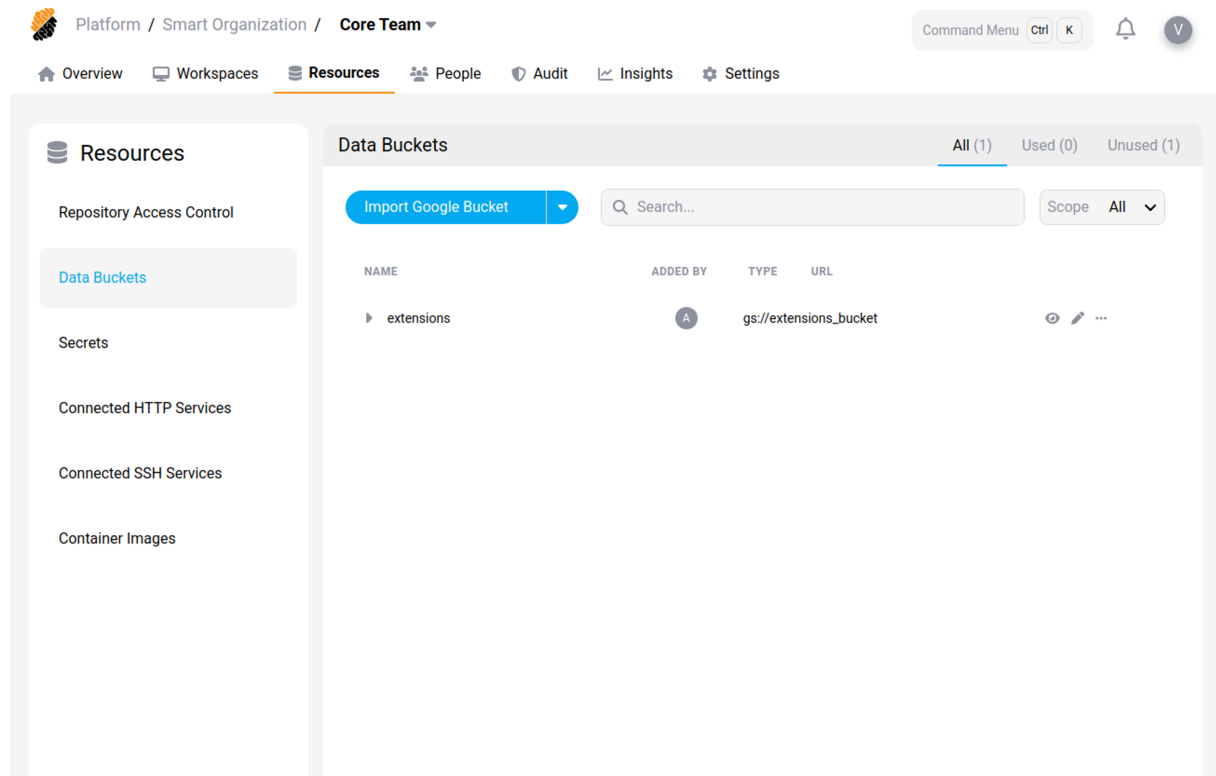
Data Buckets allow you to use your external datasets inside a [workspace](#). A data bucket attached to a workspace is automatically mounted as a folder to the container's filesystem.

As for the other types of resources, data buckets are first imported to the platform such that they become available when creating or updating the configuration of a workspace.

- [View Data Buckets](#)
- [Import a Data Bucket Permission: Resources::Manage](#)

## View Data Buckets

Data Buckets used in the [project](#) are being displayed. You may filter those in use.



A Data Bucket is defined by the following characteristics:

- **Basic information:** Information such as name, the user who added it, service provider (Google, Amazon or Microsoft) and URL.
- **Class Level:** This option defines the visibility for the container based on the user's permissions.
- **Permissions:** This option lets you define access to a data bucket as read or read and write.
- **Asset Information:** This option allows for providing a description of the data bucket.

The platform provides a mechanism to create versions of buckets. A new version is created when data is uploaded to a bucket from a workspace (with write access).

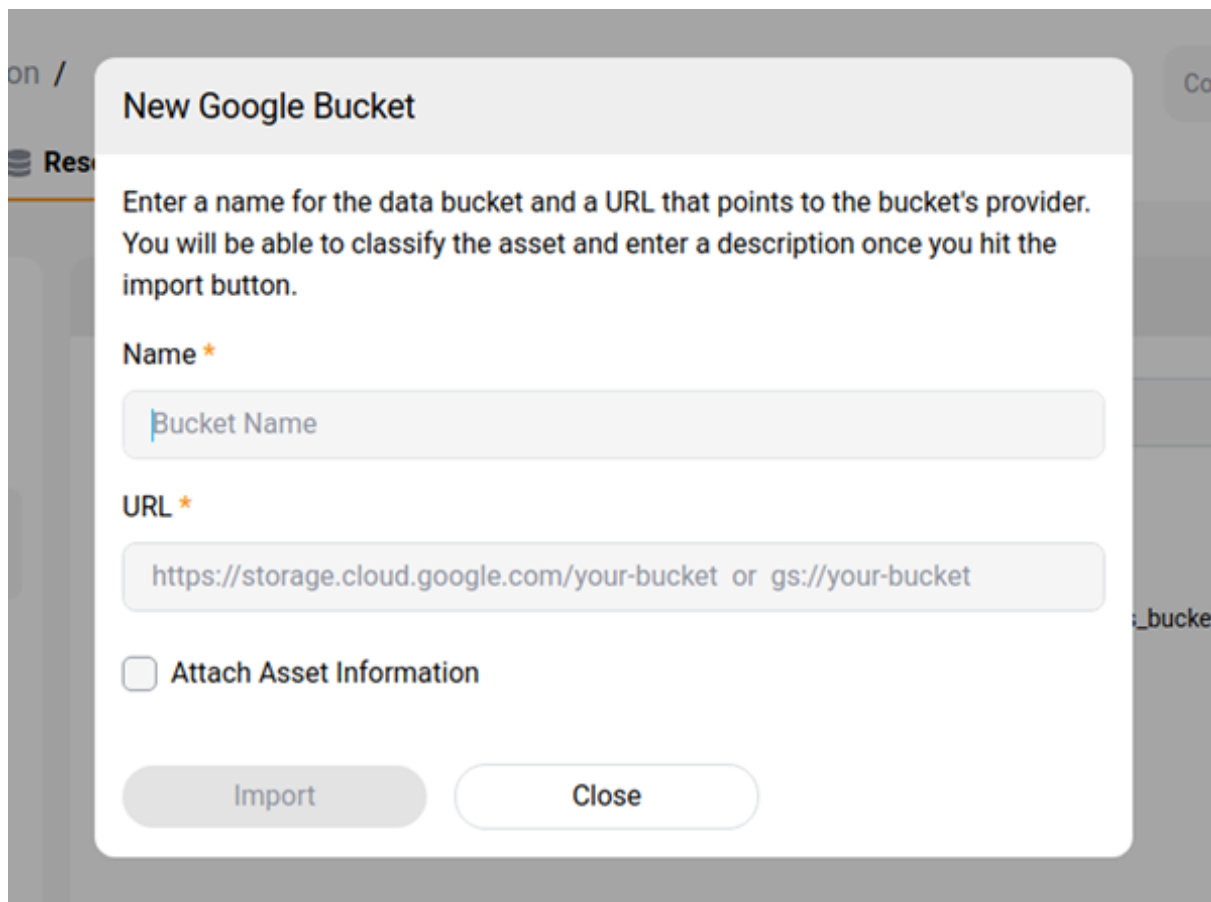
By clicking on a bucket you can see a list of versions followed by basic details (creation date, size, status, connections) as well as its content by clicking on the *book icon*.

### Import a Data Bucket Permission: `_Resources::Manage_`

You can import a bucket by pressing the “**Import Bucket**” button. Make sure to select the correct provider of your bucket (Google, Amazon or Microsoft).

You will need to enter the following information:

1. **Name**, a name to identify the data bucket, and a
2. **Bucket URL** that points to the Cloud provider's storage location.



**New Google Bucket**

Enter a name for the data bucket and a URL that points to the bucket's provider. You will be able to classify the asset and enter a description once you hit the import button.

**Name \***

Bucket Name

**URL \***

https://storage.cloud.google.com/your-bucket or gs://your-bucket

☐ **Attach Asset Information**

Import Close

#### Info

When importing Amazon buckets, you need to specify its region to optimize the data access performance.

## Secrets

August 26, 2025

Secret management allows developers to securely store sensitive data such as passwords, keys, and tokens, in a protected environment with access controls capabilities.

Generally, the term “secret” points to any necessary credentials (e.g. cryptographic keys, tokens and password) necessary to authenticate with a service during the development process. The storage of secrets is a service that can be provided by the platform or



by an external mechanism. Once registered on the platform, secrets attached to [workspaces](#) are available in the container’s filesystem as environment variables or files. This section explains how secrets are managed by the platform, but note that your platform might use an external service for that purpose.

- [View Secrets](#)
- [Add a New Secret Permission: Resources::Manage](#)

View Secrets

Secrets used in the organization or project are displayed in a table. You may search for one or filter those used in workspaces.

Platform / Smart Organization / Core Team

Command Menu Ctrl K

V

OverviewWorkspacesResourcesPeopleAuditInsightsSettings

Resources

Repository Access Control

Data Buckets

Secrets

Connected HTTP Services

Connected SSH Services

Container Images

Secrets

All (9)Used (0)Unused (9)

Add New Secret

Secret Name

⚠ Secret names cannot contain spaces, hyphens and special characters as they are used as environment variable names.

Value

☐ Attach Asset Information

Add

Q Search...

Scope All

| NAME                   | ADDED BY | CREATED ON           |  |
|------------------------|----------|----------------------|--|
| azure_secret           | A        | 26 March 2025, 09:23 |  |
| azure_secret_staging_1 | A        | 26 March 2025, 09:23 |  |
| cypress_token          | A        | 26 March 2025, 09:24 |  |
| modal_secret_1         | J        | 4 July 2024, 17:38   |  |
| modal_secret_4         | J        | 4 July 2024, 17:38   |  |
| secret_1               | J        | 4 July 2024, 17:41   |  |
| secret_2               | J        | 4 July 2024, 17:41   |  |

A Secret is defined by the following characteristics:

© 1997–2025 Citrix Systems, Inc. All rights reserved.

98

- **Basic information:** Information such as name, the user who added it, scope of use (platform, organization or project).
- **Class Level:** This option defines the visibility for the secret based on the user's permissions.
- **Asset Information:** This option allows for providing a description of the secret.

## Add a New Secret Permission: `_Resources::Manage_`

You can create a secret at the top of the **Secret Page**.

The screenshot shows the Citrix Secure Developer Spaces interface. The top navigation bar includes the Citrix logo, the breadcrumb 'Platform / Smart Organization / Core Team', and a 'Command Menu' with 'Ctrl' and 'K' shortcuts. Below the navigation bar is a menu with 'Overview', 'Workspaces', 'Resources', 'People', 'Audit', 'Insights', and 'Settings'. The 'Resources' section is expanded, showing a list of resource types: 'Repository Access Control', 'Data Buckets', 'Secrets' (highlighted), 'Connected HTTP Services', 'Connected SSH Services', and 'Container Images'. The 'Secrets' page is displayed, showing a list of secrets with tabs for 'All (9)', 'Used (0)', and 'Unused (9)'. The 'Add New Secret' form is visible, with fields for 'Secret Name' and 'Value'. A warning message states: 'Secret names cannot contain spaces, hyphens and special characters as they are used as environment variable names.' There is also a checkbox for 'Attach Asset Information' and an 'Add' button.

You will need to enter the following information:

1. **Name**, a name to identify the secret,
2. **Value**, i.e. the secret's value, and an
3. **Asset information**, a description of the secret.

## Connected HTTP Services

July 8, 2025

**Connected HTTP Services** consist of services used for the implementation of software applications. These services are typically providing functions, data or host access via APIs over the HTTP network protocol.

Tip

The nature and protocol of services that can be attached to [workspaces](#) depend on your platform's implementation.

As it is the case with other types of resources, HTTP services are attached to workspaces during the creation or the update of the workspace's settings.

- [View Connected HTTP Services](#)
- [Add an HTTP Service Permission: Resources::Manage](#)

View Connected HTTP Services

Platform / Smart Organization / Core Team

OverviewWorkspacesResourcesPeopleAuditInsightsSettings

Resources

Repository Access Control

Data Buckets

Secrets

Connected HTTP Services

Connected SSH Services

Container Images

Connected HTTP Services

All (3)Used (0)Unused (3)

Create Service

Search...

Scope All

| NAME              | ADDED | ENVIRONMENT VARIABLE NAME | CREATED ON           |     |
|-------------------|-------|---------------------------|----------------------|-----|
| http_service      | A     | dsadas                    | 26 March 2025, 09:25 | ... |
| http-connection   | A     | we                        | 26 March 2025, 09:25 | ... |
| test-http-service | J     | httpTest                  | 4 July 2024, 17:41   | ... |

Connected HTTP services are defined by the following characteristics:

- **Basic information:** Name, scope of use (platform, organization or project), URL and tag.
- **Class Level:** This option defines the visibility for the service based on the user's permissions.
- **Asset Information:** This option allows for providing a description of the container.
- **Environmental Variable Name:** This allows access to the service simply by naming an environment variable.


## Add an HTTP Service Permission: `_Resources::Manage_`

You can register a service by selecting “**New HTTP Service**” and provide the following information:

1. **Name**, a name to identify the service,
2. **Service URL** that points to the service location,
3. **Environment Variable Name**, to name the service in the context of the container’s environment,
4. **HTTP headers (optional)**, used to pass authentication data when necessary to access the service,
5. **Asset Information**, used to provide a description of the service.

### Create Service

Enter the name and URL of the HTTP service to which you would like to provide access and the name for an environment variable to refer to it in a workspace.

 The environment variable name should not contain any space characters.

Service Name \*

External URL \*

Default Path (Optional)

Environment Variable Name \*

☐ Trust Self-Signed Certificates

☐ Connect HTTP Headers

☐ Attach Asset Information

## Connected SSH Services

August 26, 2025

**Connected SSH Services** consist of services used for the implementation of software applications. These services are typically providing functions, data or host access via APIs over the SSH network protocol.

**Tip**

The nature and protocol of services that can be attached to [workspaces](#) depend on your platform's implementation.

As it is the case with other types of resources, SSH services are attached to workspaces during the creation of the update of the workspace's settings.

- [View Connected SSH Services](#)
- [Add an SSH Service Permission: Resources::Manage](#)

## View Connected SSH Services

Platform / Smart Organization / Core Team

Overview

Workspaces

Resources

People

Audit

Insights

Settings

Command Menu Ctrl K

V

Resources

Repository Access Control

Data Buckets

Secrets

Connected HTTP Services

Connected SSH Services

Container Images

Connected SSH Services

All (3) Used (0) Unused (3)

Create Service

Search...

Scope All

| NAME                         | ADDED BY | HOSTNAME/IP | AUTHENTICATION MODE | CREATED ON         |     |
|------------------------------|----------|-------------|---------------------|--------------------|-----|
| test-ssh-private-key-service | J        | 127.0.0.1   | Upload Private Key  | 4 July 2024, 17:42 | ... |
| test-ssh-service             | J        | 127.0.0.1   | Generated           | 4 July 2024, 17:42 | ... |
| test-ssh-service-2           | J        | 127.0.0.1   | Password            | 4 July 2024, 17:42 | ... |

Connected SSH services are defined by the following characteristics:

- **Basic information:** Name, scope of use (platform, organization or project), URL and tag.
- **Class Level:** This option defines the visibility for the service based on the user's permissions.
- **Asset Information:** This option allows for providing a description of the container.
- **Environmental Variable Name:** This allows access to the service simply by naming an environment variable.
- **Hostname/IP:** The IP address or hostname of the SSH host,
- **Authentication Mode:** the mechanism to authenticate with the service.

### **Add an SSH Service Permission: `_Resources::Manage_`**

You can register a connected service by selecting “**New SSH Service**”.

You will need to enter the following information:

1. **Name**, a name to identify the host,
2. **SSH Username**, a username to access the host,
3. **Hostname or IP address of the SSH service**, that points to the host location,
4. **Port number the SSH service is running on**, a port number for the service,
5. **Authentication method**, an authentication method to access the service, and choose one of the methods:
  - “Generated”: A pair of keys will be generating when adding the SSH service
  - “Upload Private Key”: Upload the private key that will be used to authenticate you to the ssh service
  - “Password”: Insert the password associated to your ssh username previously entered
6. **Asset Information**, a description of the service.

### Create Service

Enter the name and URL of the HTTP service to which you would like to provide access and the name for an environment variable to refer to it in a workspace.

⚠ The environment variable name should not contain any space characters.

Service Name \*

External URL \*

Default Path (Optional)

Environment Variable Name \*

☐ Trust Self-Signed Certificates

☐ Connect HTTP Headers

☐ Attach Asset Information

## Container Images

August 1, 2025

Container images or also Cloud Development Environments (CDEs) are used to define the configuration of a development environment. Typically, CDEs define all the software dependencies necessary for building the intended application once implemented. Users create [workspaces](#) with such an image as “blueprint”, and begin contributing code to the project within this context.

CDE images are imported from a registry as part of the [resources](#) available to users on the platform. Registries are either public or private.

For private registries, you need to provide credentials to authenticate properly before importing the image. Public registries, by definition, do not need credentials.

- [View CDE Images](#)
- [Add a CDE Image Permission: Security::Manage](#)
- [View Registry Credentials](#)
- [Add a Registry Credential Permission: Security::Manage](#)

## View CDE Images

The panel displays the available CDE images in the [project](#). You may search for one or filter those used in workspaces.

The screenshot shows the Citrix Secure Developer Spaces interface. The top navigation bar includes 'Platform / Smart Organization / Core Team', a 'Command Menu' with 'Ctrl K', and a user profile icon. The sidebar on the left has 'Resources' selected, with sub-items like 'Repository Access Control', 'Data Buckets', 'Secrets', 'Connected HTTP Services', and 'Connected SSH Services'. The 'Container Images' panel is active, showing a table of images. The table has columns for 'NAME', 'URL', and 'DEFAULT TAG'. The images listed are: Default Android studio image, Default Generic Image, Default GoLand Image, Default IntelliJ Java Image, Default IntelliJ Ultimate, Default PHPStorm Image, and Default PyCharm Image. Each image has a corresponding URL and a default tag (e.g., 2.2.5, 2.2.7, 2.2.2). There are also icons for each image, likely representing the registry or source.

| NAME                         | URL  | DEFAULT TAG |
|------------------------------|--|-------------|
| Default Android studio image | registry.digitalocean.com/cloud-mvp/public-ima...  | 2.2.5       |
| Default Generic Image        | strongnetworkstagings.azurecr.io/cloud_editor_...  | 2.2.7       |
| Default GoLand Image         | registry.digitalocean.com/cloud-mvp/public-ima...  | 2.2.2       |
| Default IntelliJ Java Image  | strongnetworkstagings.azurecr.io/intellij_java     | 2.2.5       |
| Default IntelliJ Ultimate    | strongnetworkstagings.azurecr.io/intellij_ultimate | 2.2.5       |
| Default PHPStorm Image       | strongnetworkstagings.azurecr.io/phpstorm_php      | 2.2.5       |
| Default PyCharm Image        | strongnetworkstagings.azurecr.io/pycharm_pyt...    | 2.2.5       |

A CDE image is defined by the following characteristics:

- **Basic information:** Name, scope of use (platform, organization or project), URL and tag.
- **Class Level:** This option defines the visibility for the CDE image based on the user's permissions.
- **Asset Information:** This option allows for providing a description of the CDE.

By clicking on a CDE image, you can see a list of the CDE's versions followed by basic details such as imported date, status.



## Add a CDE Image Permission: `_Security::Manage_`

You can add a CDE image by pressing the “**Add New Image**” button. You will need to provide the following information:

1. **Name**, a name to identify the CDE,
2. **Images URL**, that points to the CDE’s location,
3. **Image’s latest tag**,
4. **Private registry** (optional),
5. **Asset Information** (optional).

The screenshot shows a 'New Workspace Image' dialog box. At the top, it says 'Enter a name for the image, a URL that points to the container image, and a tag specifying the version.' Below this is a warning icon and text: 'The image should fulfill the following requirements:'. The requirements are listed as bullet points: 'Contain a SSH client, e.g., OpenSSH', 'Have the Git and Git LFS clients installed', and 'Have a user "developer" with id 1000, i.e., run the command "adduser -u 1000 developer"'. The form has three input fields: 'Image Name' with the placeholder 'Default Image', 'URL' with the placeholder 'Image URL', and 'Image Tag' with the placeholder 'e.g., v1.0.0'. There is a checked checkbox for 'Private Registry' and a dropdown menu for 'Registry Credential' currently set to 'No credential'. There is also an unchecked checkbox for 'Attach Asset Information'. At the bottom are 'Import' and 'Cancel' buttons.

### Warning

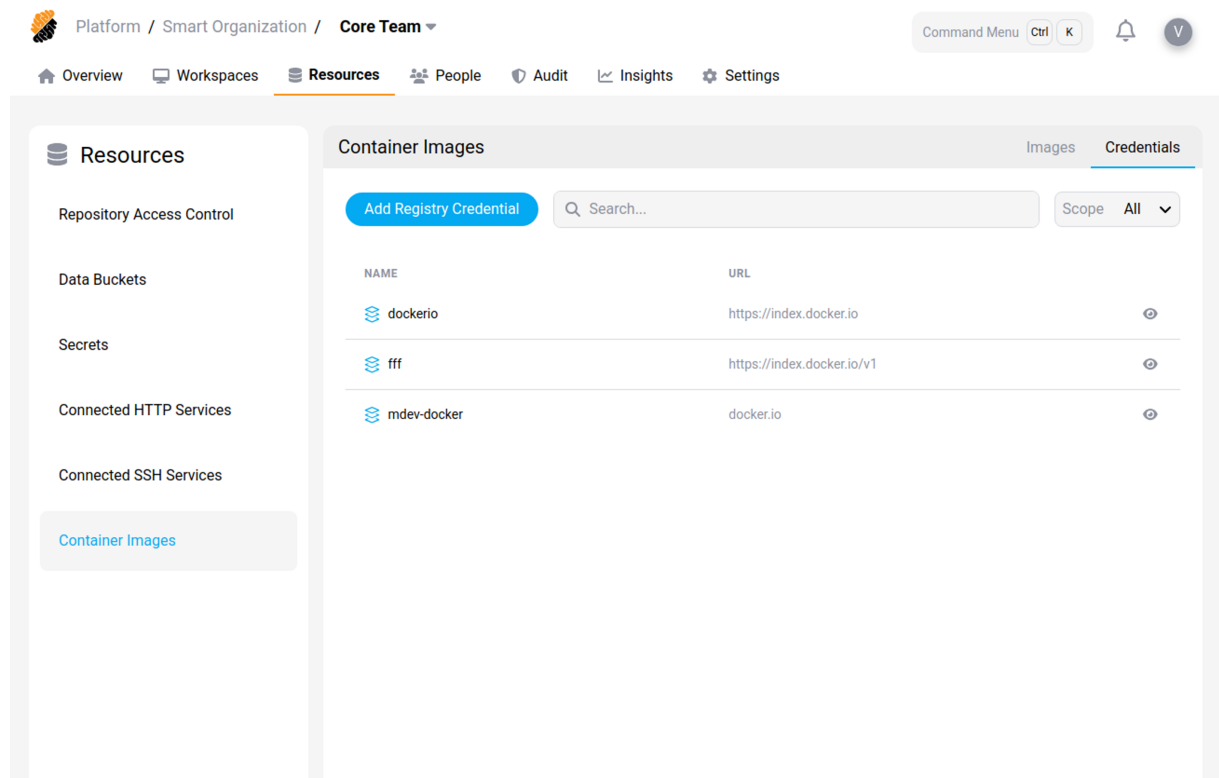
The CDE image should fulfill the following requirements:

1. It should contain an SSH client.
2. It should have both GIT and GIT LFS clients installed.
3. It should have a user named “developer” with ID 1000 (this is obtained by running the command “adduser -u 1000 developer”).

You can edit or delete a CDE image by clicking on the “...” icon next to its class level.

## View Registry Credentials

To display credentials used in the project click on the “**Credentials**” button on the top right of the panel. You may search for one or filter those used in workspaces.



A Registry Credential is defined by the following characteristics:

1. **Name**,
2. **Scope** and
3. a **URL**.

For security purpose, no credentials are directly exposed or available for consultation.

## Add a Registry Credential Permission: `_Security::Manage_`

You can add a Registry Credential by pressing the “**Add Registry Credential**” button.

**Add New Registry Credential**

Create a new docker registry credential.

**Name**

my\_registry\_credential

**Username**

**Password**

**URL**

☐ **Attach Asset Information**

You will need to enter the following information:

1. **Name**, to identify the credentials when needed during the registration of a CDE image,
2. **Username**:, and
3. **Password**:, as credential values, and an
4. **URL**: where the authentication is performed.
5. **Asset information**, a description of the registry credential.

## People Page

The People page contains information about users onboarded to a project, an organization or the entire platform. Switching projects or organizations therefore updates the membership in the table.

You can see the role, permissions and public details for each user in the [View User](#) panel.

This page provided typical team management functions to users with the appropriate permissions. The [project owner](#) has permissions to update the roles of the users in the project.

In addition, the project owner can create new roles or update existing ones from the [Permission Management](#) panel.

Platform / Smart Organization / Core Team ▾

Command Menu **Ctrl** **K**

[Overview](#) [Workspaces](#) [Resources](#) [People](#) [Audit](#) [Insights](#) [Settings](#)

Online Users 1 | Total Users 4 [Users](#) [Roles & Permissions](#)

[+ Add](#)

- Victor (You)**  
Project Owner 1 minute ago [>](#)
- Mark Manager**  
Security Manager 9 months ago
- Aleksa Developer**  
Developer 9 months ago
- John ProjectOwner**  
Primary Project Owner 18 days ago

**User Details**

**Victor**  
victor@company.com

Time Zone  
**Europe/Zurich (GMT+2)**

Location  
**London, UK**

Groups  
**No Groups**

**Your Role** [Project Owner](#)

**Your Permissions**

|                |                                |   |
|----------------|--------------------------------|---|
| Workspace Apps | <a href="#">Manage</a>         | User can open and close ports of workspaces   |
| Workspaces     | <a href="#">Manage Project</a> | User can create custom workspaces, assign them to any user in the project, and edit or delete any workspaces within the project |
| Resources      | <a href="#">Import</a>         | User can import new Git repositories, manage container images, as well as manage all resources                                  |
| Security       | <a href="#">Manage</a>         | User can add, edit and delete registry credentials, network policies, generate platform API keys and update project settings    |
| Metrics        | <a href="#">Access Project</a> | User can access the Insights dashboard and see both personal and project metrics  |
| Members        | <a href="#">Manage</a>         | User can add and remove members to project with the People dashboard  |
| Permission     | <a href="#">Manage</a>         | User can manage roles and permissions and control permissions of other people.  |

### Info:

A regular user can view all of the roles in the project and the associated permissions even if he

does not have the **Members::Manage** permission.

## Content

- **View Users** panel.
- **Access Control** panel.

## Users

August 26, 2025

Users participating in the project or organization are displayed in the table at the top of the [People](#) page.

You can see the role, permissions and public details for each user.

Platform / Smart Organization / Core Team

Command Menu Ctrl K

Overview Workspaces Resources **People** Audit Insights Settings

Online Users 1 | Total Users 4

Users Roles & Permissions

Search Users + Add

Victor (You)  
Project Owner  
1 minute ago

Mark Manager  
Security Manager  
9 months ago

Aleksa Developer  
Developer  
9 months ago

John ProjectOwner  
Primary Project Owner  
18 days ago

User Details

V

Victor

victor@company.com

Time Zone  
Europe/Zurich (GMT+2)

Location  
London, UK

Groups  
No Groups

Your Role Project Owner

Your Permissions

|                |                |   |
|----------------|----------------|---|
| Workspace Apps | Manage         | User can open and close ports of workspaces   |
| Workspaces     | Manage Project | User can create custom workspaces, assign them to any user in the project, and edit or delete any workspaces within the project |
| Resources      | Import         | User can import new Git repositories, manage container images, as well as manage all resources                                  |
| Security       | Manage         | User can add, edit and delete registry credentials, network policies, generate platform API keys and update project settings    |
| Metrics        | Access Project | User can access the Insights dashboard and see both personal and project metrics  |
| Members        | Manage         | User can add and remove members to project with the People dashboard  |
| Permission     | Manage         | User can manage roles and permissions and control permissions of other people.  |

- [Search for Users](#)
- [Onboard a User in a Project](#) `Permission:Members::Manage`
- [Remove a User](#) `Permission:Members::Manage`
- [Public Details](#)
- [Roles and Permissions](#)

Search for Users

You can look for a specific user in the project using the *search bar* or by *browsing the tabs*.

Recent activity and roles are displayed next to the username. Counts of connected users and total users are visible above the search bar.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

111

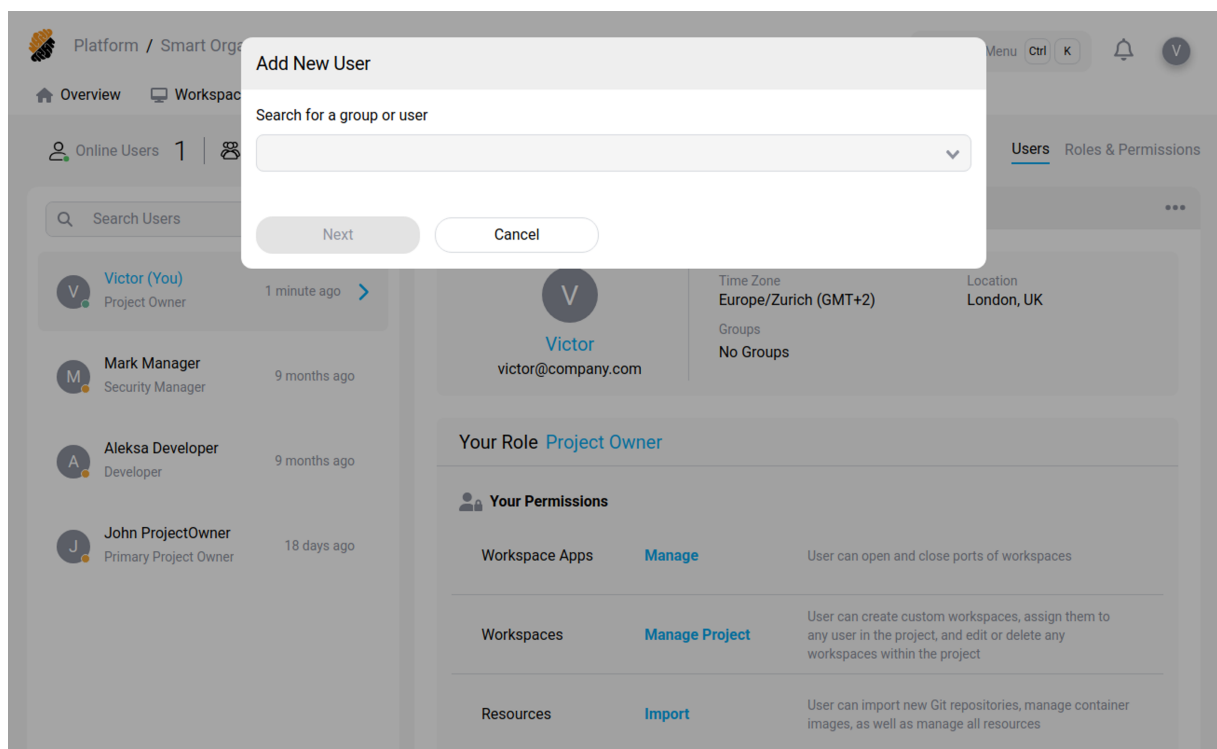
## Onboard a User in a Project Permission: **\_Members::Manage\_**

By clicking on the “Add New User” button, you will be prompted to enter the email address of the user to be added. Based on the email’s domain name, an appropriate identity provider (IdP) is selected. Domain names have to be registered with the Settings menu at platform-level to attach it to the correct IdP.

When the domain is not detected, a temporary password can be generated for the user. This password will have to be communicated to the user, unless a mechanism to do so is available with your instance.

Each user must be assigned a role in the scope of a project during the onboarding process. Once a user has been onboarded in the project, a workspace can be assigned to her or She can create a workspace on her own granted she has the appropriate permission, at least

**Workspaces::Manage Personal.**

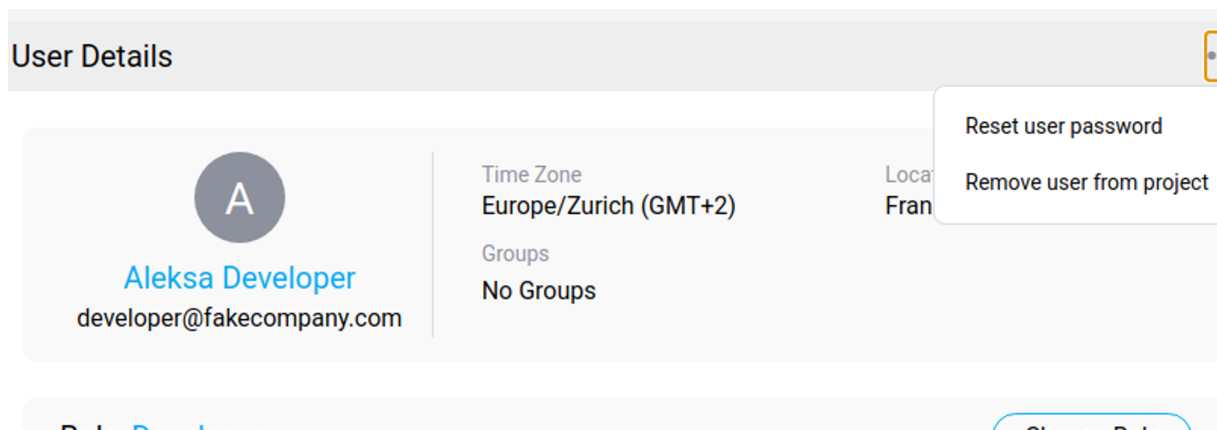


### Tip

You can set an expiration date to the participation of the user in the project. Once the date is passed, the user won't have access to the project, the workspaces or to any resource associated with it.

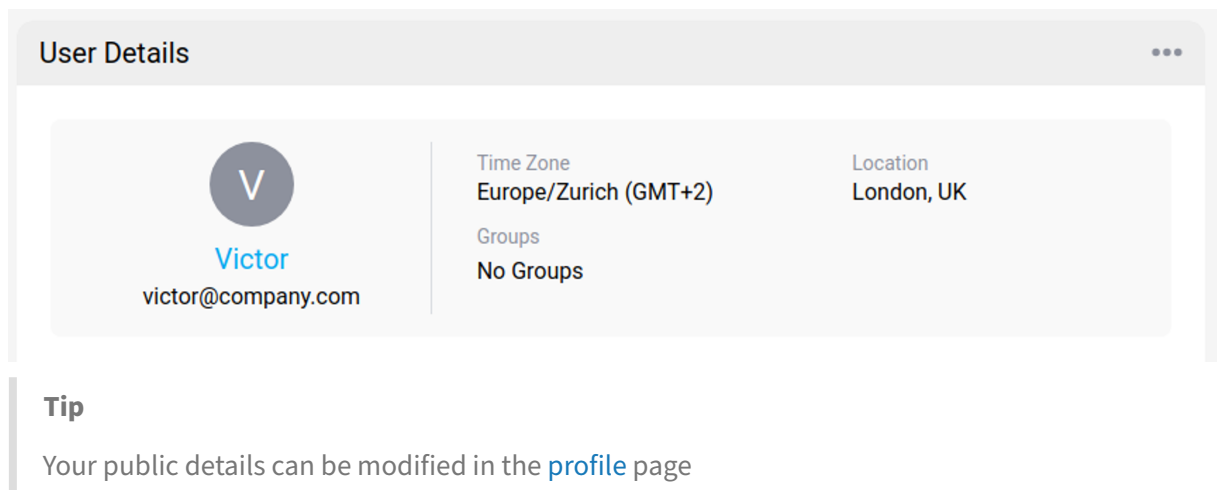
## Remove a User Permission: `_Members::Manage_`

By clicking on the “...” icon on the top right of the user detail you can remove him from the project. The user won't have access to the project or to any resource associated with it. The user is however still in the platform database. To fully remove a user from the platform, the user has to be removed from the list of users, i.e. People Dashboard, when accessed at the platform level. This can be done with a user with a platform-level role such as *admin* or *security officer*.



## Public Details

On the user profile you can see his email address, time-zone and location. These details are visible by everyone with the `Members::Access` [permission](#) in the project.



## Roles and Permissions

On the user profile you can view your current role in context of the currently selected project.



Roles & Permissions

Users

Roles & Permissions

Roles <sup>4</sup>

+ New Role

Project Owner

Manager

Developer

Security Manager

Project Owner Role Permissions

Set Permissions

Workspace Apps

Access and execution of workspace applications

No Access Access Manage

User can open and close ports of workspaces

Workspaces

Access and management of workspaces

No Access Access Manage PersonalManage Project

User can create custom workspaces, assign them to any user in the project, and edit or delete any workspaces within the project

Resources

Access and management of resources

No Access Access Manage Import

User can import new Git repositories, manage container images, as well as manage all resources

☒ Confidential ☒ Regulated

Access to regulated and confidential resources

Security

Access and management of project security

No Access Access Manage

User can add, edit and delete registry credentials, network policies, generate platform API keys and update project settings

Metrics

Access to insights and metrics

No Access Access Personal Access Project

User can access the Insights dashboard and see both personal and project metrics

Members

Access and management of project members

No Access Access Manage

User can add and remove members to project with the People dashboard

☒ User can manage roles and permission of other users (enable all permissions)

Tip

Tip for privileged users with permission *Members::Manage*  
The user role can be modified using the user table found on the people page.

Refer to the [Access Control](#) page for more details around the access control policies on the platform.

Access Control

August 1, 2025

Roles and permissions in the organization are displayed on the [People](#) page.  
If you are a *project owner*, you can create new roles or update existing ones from the access control panel.

**Roles & Permissions**

Users **Roles & Permissions**

**Roles** <sup>4</sup> [+ New Role](#)

**Project Owner**

**Manager**

**Developer**

**Security Manager**

**Project Owner Role Permissions**

**Set Permissions**

**Workspace Apps**  
Access and execution of workspace applications

No Access Access Manage

User can open and close ports of workspaces

**Workspaces**  
Access and management of workspaces

No Access Access Manage Personal Manage Project

User can create custom workspaces, assign them to any user in the project, and edit or delete any workspaces within the project

**Resources**  
Access and management of resources

No Access Access Manage Import

User can import new Git repositories, manage container images, as well as manage all resources

☒ Confidential ☒ Regulated

Access to regulated and confidential resources

**Security**  
Access and management of project security

No Access Access Manage

User can add, edit and delete registry credentials, network policies, generate platform API keys and update project settings

**Metrics**  
Access to insights and metrics

No Access Access Personal Access Project

User can access the Insights dashboard and see both personal and project metrics

**Members**  
Access and management of project members

No Access Access Manage

User can add and remove members to project with the People dashboard

☒ User can manage roles and permission of other users (enable all permissions)

- [Roles](#)
- [Default roles](#)
- [Create a new role Project Owner](#)
- [Permissions](#)

## Roles


Roles define a set of permissions given to a user or a group of user.

They allow to determine the rights given to each user. Roles are project bound. This means that the same user may have a different role depending on the project. Roles defined on the project level are only available within that project.


Roles <sup>4</sup>

+ New Role


Project Owner

 >


Auditor

 >

Strong Developer

 >

Guest role

 >

Warning

Roles are a crucial element to consider when securing your resources. Roles must be attributed following a **least privilege** policy to avoid any unwarranted access.

Default roles

There are 4 default roles in a standard project: **Guest**, **Developer**, **Manager** and **Project Owner**. They are meant for the following use:

- **Guest:** The guest role allows a user to view the platform without having access to sensitive data or the ability to make any modifications.
- **Developer:** The “default” developer will be able to create workspaces based on admin-defined project rules.
- **Manager:** The manager has all the tech lead’s permissions.
- **Project Owner:** The project owner has all the manager’s permissions, in addition to accessing the [project’s audit](#) and manage the user’s security feature, such privilege elevation.

To each role is attached the set of permissions described below.

Refer to the [permissions](#) section for an explanation about each permission.

| Permission                    | Guest      | Developer  | Manager    | Project Owner |
|-------------------------------|------------|------------|------------|---------------|
| <b>Workspace Apps::Access</b> | <b>Yes</b> | <b>Yes</b> | <b>Yes</b> | <b>Yes</b>    |

| Permission                     | Guest      | Developer  | Manager    | Project Owner |
|--------------------------------|------------|------------|------------|---------------|
| <b>Workspace</b>               | <b>Yes</b> | <b>Yes</b> | <b>Yes</b> | <b>Yes</b>    |
| <b>Apps::Manage</b>            |            |            |            |               |
| <b>Workspaces::Access</b>      | <b>Yes</b> | <b>Yes</b> | <b>Yes</b> | <b>Yes</b>    |
| <b>Workspaces::Manage</b>      | No         | <b>Yes</b> | <b>Yes</b> | <b>Yes</b>    |
| <b>Personal</b>                |            |            |            |               |
| <b>Workspaces::Manage</b>      | No         | <b>Yes</b> | <b>Yes</b> | <b>Yes</b>    |
| <b>Project</b>                 |            |            |            |               |
| <b>Resources::Access</b>       | <b>Yes</b> | <b>Yes</b> | <b>Yes</b> | <b>Yes</b>    |
| <b>Resources::Manage</b>       | No         | <b>Yes</b> | <b>Yes</b> | <b>Yes</b>    |
| <b>Resources::Import</b>       | No         | No         | No         | <b>Yes</b>    |
| <b>Resources::Regulated</b>    | No         | <b>Yes</b> | <b>Yes</b> | <b>Yes</b>    |
| <b>Resources::Confidential</b> | No         | <b>Yes</b> | <b>Yes</b> | <b>Yes</b>    |
| <b>Security::Access</b>        | No         | <b>Yes</b> | <b>Yes</b> | <b>Yes</b>    |
| <b>Security::Manage</b>        | No         | No         | No         | <b>Yes</b>    |
| <b>Metrics::Access</b>         | No         | <b>Yes</b> | <b>Yes</b> | <b>Yes</b>    |
| <b>Personal</b>                |            |            |            |               |
| <b>Metrics::Access</b>         | No         | No         | <b>Yes</b> | <b>Yes</b>    |
| <b>Project</b>                 |            |            |            |               |
| <b>Members::Access</b>         | No         | <b>Yes</b> | <b>Yes</b> | <b>Yes</b>    |
| <b>Members::Manage</b>         | No         | No         | <b>Yes</b> | <b>Yes</b>    |

## Create a new role **Project Owner**

By clicking on the button at the top left of the **access control** panel, you can create a new role. Select a name and the set of permissions that characterize the new role.

### Warning

Granted permissions must follow a **least privilege** policy.

Be careful when naming a role, a poorly chosen name can be misused and end up giving too much privilege to a user.

Permissions

Permissions describe the rights given to a user for a specific access.

Project Owner Role Permissions

Set Permissions

Workspace Apps

Access and execution of workspace applications

No Access

Access

Manage

User can open and close ports of workspaces

Workspaces

Access and management of workspaces

No Access

Access

Manage Personal

Manage Project

User can create custom workspaces, assign them to any user in the project, and edit or delete any workspaces within the project

Resources

Access and management of resources

No Access

Access

Manage

Import

User can import new Git repositories, manage container images, as well as manage all resources

☒ Confidential

☒ Regulated

Access to regulated and confidential resources

Security

Access and management of project security

No Access

Access

Manage

User can add, edit and delete registry credentials, network policies, generate platform API keys and update project settings

Metrics

Access to insights and metrics

No Access

Access Personal

Access Project

User can access the Insights dashboard and see both personal and project metrics

Members

Access and management of project members

No Access

Access

Manage

User can add and remove members to project with the People dashboard

☒ User can manage roles and permission of other users (enable all permissions)

Please find below the detail of each access mentioned above.

| Permissions                        | Description  |
|------------------------------------|--|
| <b>Workspace Apps::No Access</b>   | The user cannot access apps running on the workspace.  |
| <b>Workspace Apps::Access</b>      | The user can access and view apps shared with the user by other users.   |
| <b>Workspace Apps::Manage</b>      | The user can open and close ports of workspaces.   |
| <b>Workspaces::No Access</b>       | User cannot access workspaces  |
| <b>Workspaces::Access</b>          | User can access workspaces assigned to her, but cannot edit properties or modify access control to resources, or delete her workspace.                             |
| <b>Workspaces::Manage Personal</b> | User can create personal workspaces (i.e. with admin pre-defined characteristics), manage access control to the project resources, and delete personal workspaces. |
| <b>Workspaces::Manage Project</b>  | User can create custom workspaces and assign it to any user in the project. The user can edit or delete any workspaces in the project.                             |
| <b>Resources::No Access</b>        | The user cannot access the Resources dashboard and see registered resources.   |
| <b>Resources::Access</b>           | The user can access the Resources dashboard and see registered resources, but cannot edit or delete them.  |
| <b>Resources::Manage</b>           | The user can access the Resources dashboard and see, edit and delete project repositories, secrets, external services and data buckets.                            |
| <b>Resources::Import</b>           | The user can import new git repositories, container images and SAML connected apps, as well as manage all resources.   |
| <b>Resources::Regulated</b>        | The user can access resources registered as regulated, i.e. falling under some regulations   |
| <b>Resources::Confidential</b>     | The user can access resources registered as confidential such as intellectual property, etc.   |
| <b>Security::No Access</b>         | The user does not have access to security metrics.   |
| <b>Security::Access</b>            | The user has access to the Audit dashboard, define network policies (Resource Dashboard), but cannot add, edit or delete them.                                     |

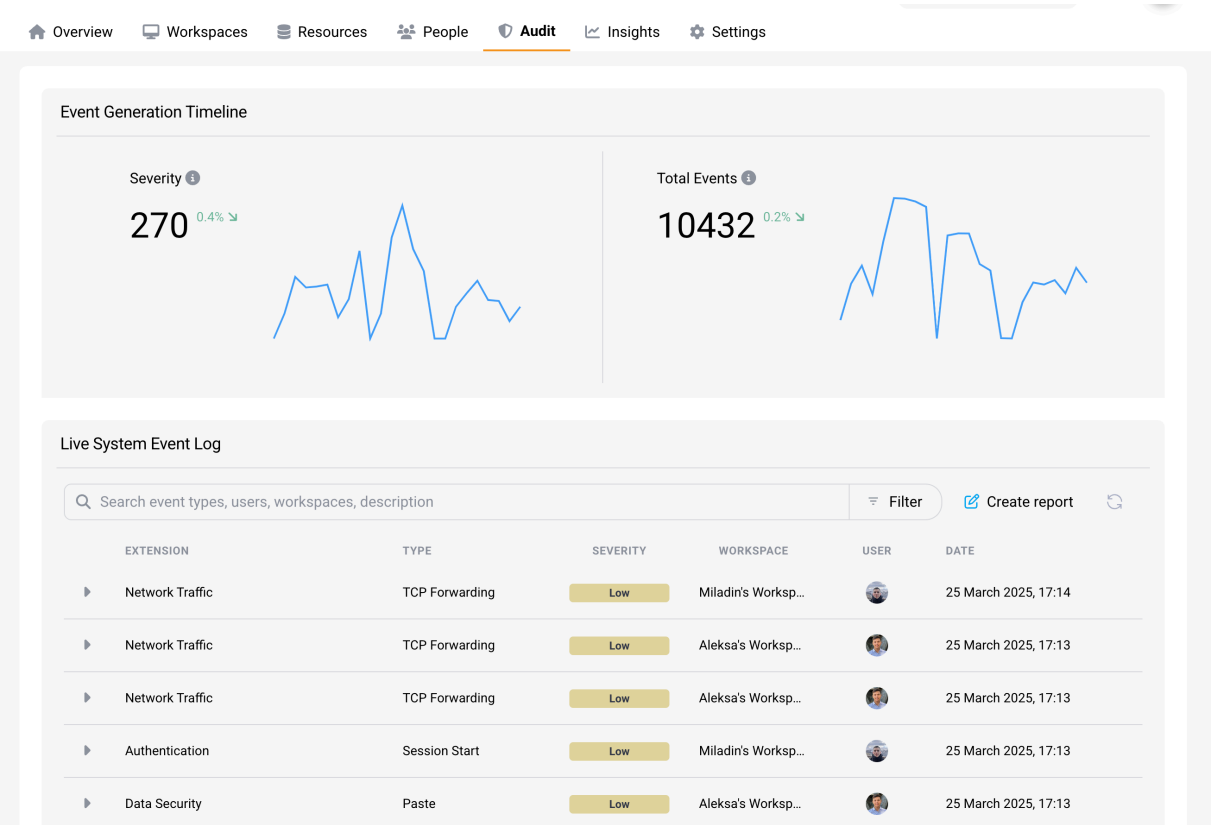
| Permissions                     | Description   |
|---------------------------------|---|
| <b>Security::Manage</b>         | The user can add, edit and delete workspace images, registry credentials, network policies, generate platform API keys and update project settings. |
| <b>Metrics::No Access</b>       | The user has no access to the Insights dashboard.   |
| <b>Metrics::Access Personal</b> | The user has access to the Insights dashboard and see only personal metrics.  |
| <b>Metrics::Access Project</b>  | The user has access to the Insights dashboard and see both personal and project-level metrics.  |
| <b>Members::No Access</b>       | The user cannot see the project's members (no People dashboard).  |
| <b>Members::Access</b>          | The user can see the project's members in the People dashboard.   |
| <b>Members::Manage</b>          | The user can add and remove members to the project with the People dashboard.   |

## Audit Page

August 1, 2025

Permission: `_Security::Access_`

The **Audit page** provides insights into the security of your **Project**, including a **Event Generation Timeline** graph that illustrates the timeline of events triggered by **workspaces** within the current project. Additionally, the **Live System Event Log** presents a table displaying detailed logs of each event.





### Event Logs

The **Live System Event Log** displays records of security events triggered by [workspaces](#) within a specific [project](#). These events can take many forms, such as clipboard monitoring or network alerts, like a DNS request. These logs are significant as they have the ability to uncover potential security vulnerabilities.

**Tip**

Events are triggered once you enabled the option “Log and record outbound network traffic” for the associated [Network Policy](#).

Live System Event Log

Q Search event types, users, workspaces, description

Filter

Create report

| EXTENSION        | TYPE   | SEVERITY | WORKSPACE | USER | DATE                |
|------------------|--------|----------|-----------|------|---------------------|
| ▶ Authentication | Login  | Low      | None      | V    | 8 April 2025, 12:23 |
| ▶ Authentication | Login  | Low      | None      | V    | 8 April 2025, 12:23 |
| ▶ Authentication | Login  | Low      | None      | V    | 8 April 2025, 12:23 |
| ▶ Authentication | Login  | Low      | None      | V    | 8 April 2025, 12:22 |
| ▶ Authentication | Login  | Low      | None      | V    | 8 April 2025, 12:22 |
| ▶ Authentication | Logout | Low      | None      | V    | 8 April 2025, 12:22 |
| ▶ Authentication | Login  | Low      | None      | V    | 8 April 2025, 12:21 |
| ▶ Authentication | Login  | Low      | None      | V    | 8 April 2025, 12:21 |
| ▶ Authentication | Login  | Low      | None      | V    | 8 April 2025, 12:19 |

### Filtering Logs

The log view allows users to easily filter and search through the system’s event logs. This feature makes it very convenient to identify possible issues, troubleshoot and also to monitor the usage of the system in a more granular level. To display filter options, press the “**Filter**” button located at the top right of the **Live System Event Log** panel.

Filter logs by:

- **Type** of the event,
- **Severity** level,
- **Workspace** from where the event was triggered,
- **User** that triggered the event,

- **Date** and time at which the event was triggered.

In addition to filtering logs, you can search through them by typing key words in the search bar below the date range (e.g. search for a specific user).

## Log Display

The log view provides detailed information about each event that occurs within the system. For each log, you can view the following information:

1. **Type:** What kind of event was triggered,
2. **Severity:** Severity level of the event,
3. **Workspace:** Workspace from where event was triggered,
4. **User:** User who triggered the event,
5. **Date:** Date and time at which the event was triggered,
6. **Description:** Describes action that triggered the event.

To view more details about an event, press the dropdown menu button to the left of the event's log.

## Insights Page

The **Insights Page** displays information about the activity of the **Project**'s members, resource allocation and container process' metrics. The information displayed on this page depends on the implementation of the platform in your organization. This section provides a general view of the information commonly found across deployments.

### Info

Depending on your permissions within the project, some of this information may not be available.

## Content

- **Resource Allocation** Permission: `_Metrics::Access Project_`
- **Container Process Metrics**

## Resource Allocation

August 1, 2025

Permission:\_Metrics::AccessProject\_

Within the **Resource Allocation** tab, you can view the current usage of resources by your workspace.

- [Resource Allocation Graph](#)

## Resource Allocation Graph



You can also view a sortable list of the total consumption based on activities for each workspace in the project.

### Note

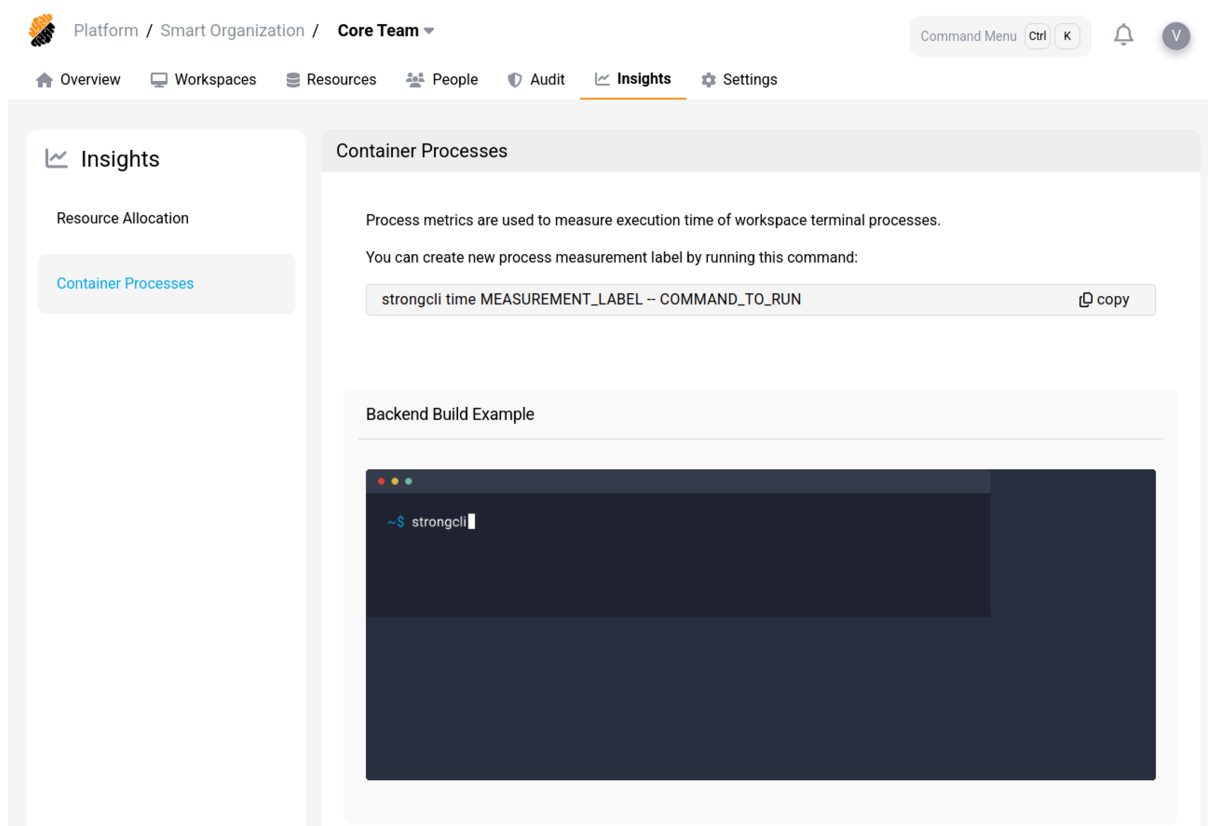
Each workspace is assigned a CPUs/Memory/Memory specification. You can see the current level of usage for workspaces in the project in the Workspace Consumption list.

## Container Process Metrics

August 1, 2025

The section **Container Process** displays time metrics registered using the platform Command Line Interface (CLI) **strongcli** available in [developers workspaces](#).

Metrics are registered using the 'time' option and become available in the Insight dashboard's section **Container Process**. This CLI is typically used in scripts embedded in the project containers such that, at startup a selection of processes can be registered for performance assessment. Once registered in a fleet of workspaces, metrics are aggregated and eventually displayed in the Insights page.



- [Track a Container Process](#)
- [Insights' Period](#)
- [Container Process Insights](#)
  - [Average](#)
  - [Total](#)

## Track a Container Process

You can track the execution time of container processes in workspaces using the platform's Command Line Interface (CLI) **strongcli**.

Use the following command to do so:

```
1 > strongcli time LABEL -- COMMAND_TO_RUN
```

Where:

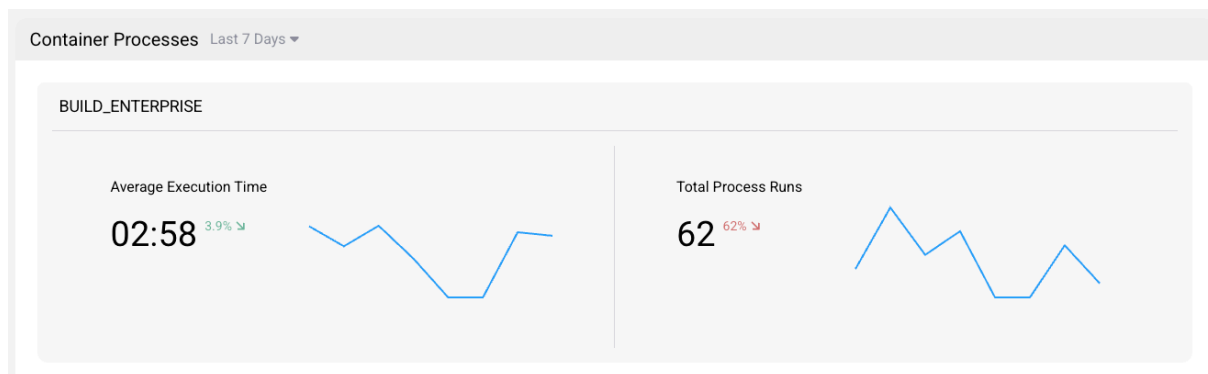
- **LABEL:** This allows setting a label to identify the process in the Insight dashboard,
- **COMMAND\_TO\_RUN:** The terminal command for which you would like to measure the execution time.

This registers a new process for your workspace among the **container processes** and measures its execution time.

## Insights'Period

After selecting a container process, you can vary the span of the statistics from a 7-day execution average to a yearly average.

- Click on the drop-down menu to the right of “**Last 7 days**” to change the evaluation period.

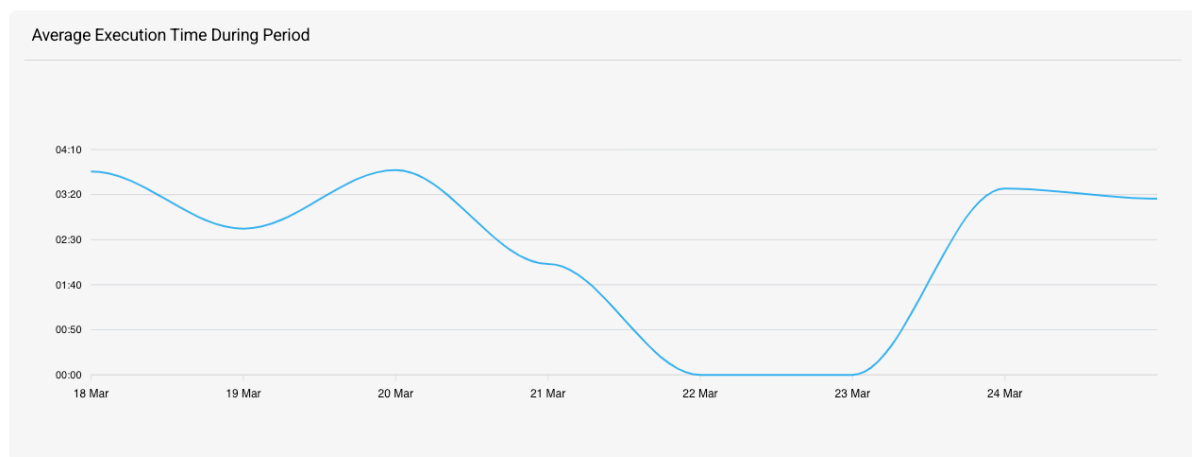


Based on selected period, the graph scale will be adapted accordingly.

## Container Process Insights

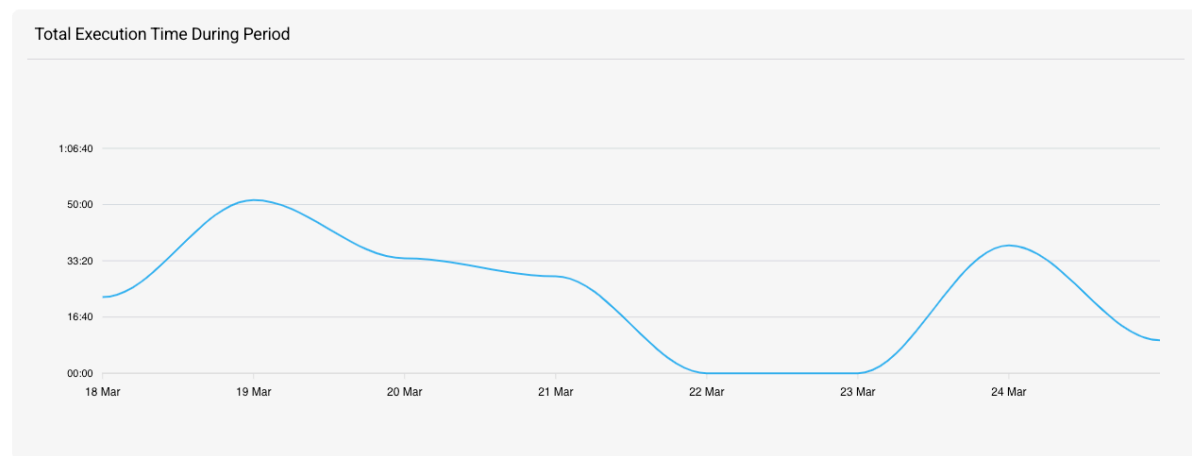
### Average

The “average execution time” graph in the container Process section of the Insight dashboard shows the average amount of time it took for a command to be executed within a developer’s workspace, as recorded by the platform’s Command Line Interface (CLI). The period of time displayed on the average execution time graph can be adjusted, allowing you to view metrics for a specific date range.



## Total

The “total execution time” graph in the **container process** section of the Insight dashboard shows the total amount of time the command has been executed in a developer’s workspace. The period of time displayed on the total execution time graph [can be adjusted](#), allowing you to view metrics for a specific date range.



## Profile and Account Settings

The **Profile and Account Settings** pages lets you manage personal data and set preferences around your work habits. For example, you can set-up a [work schedule](#) such that your workspace is automatically deployed at pre-set hours.

The profile is used also to store any personal configuration files such as `.bashrc`, etc needed to customize your workspaces.

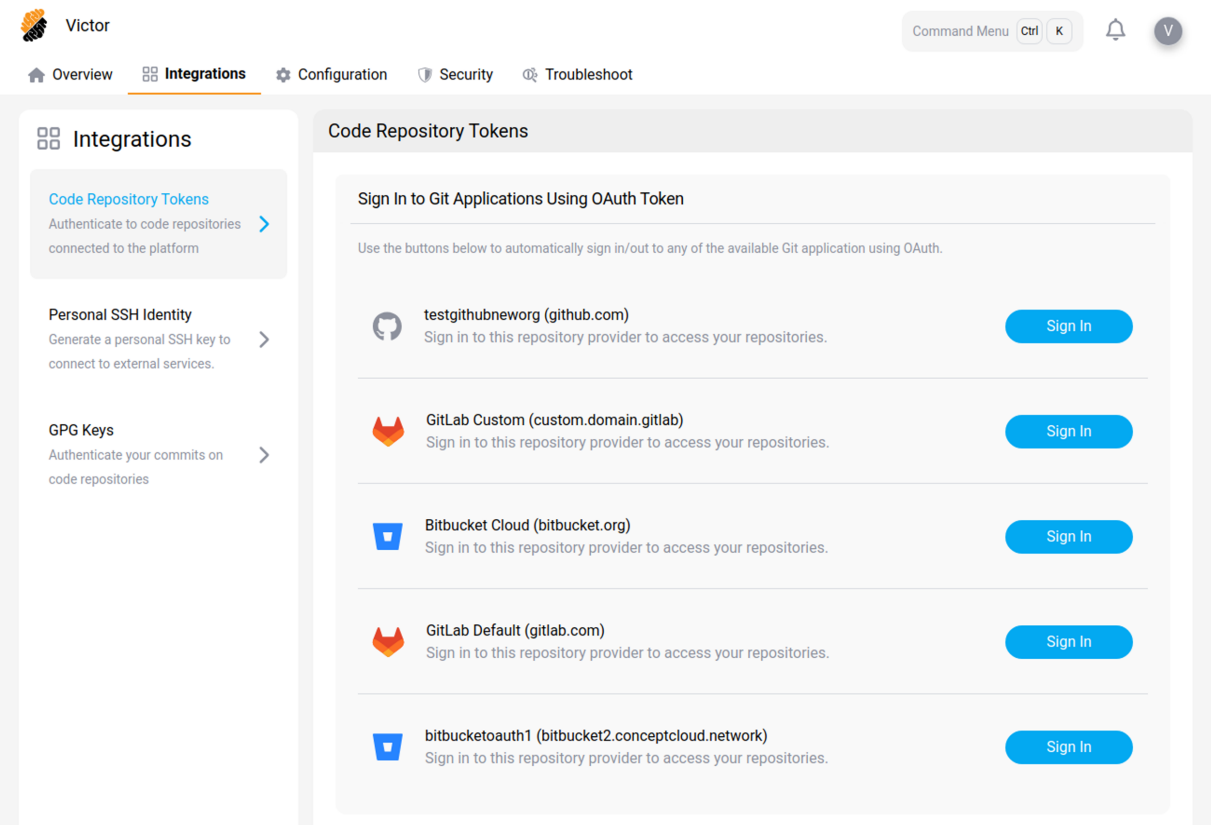
In addition, you can use the profile to record IDE configurations, including installed plug-ins, and replicate them across workspaces. Finally, the profile is the place to manage the different [authentication tokens](#) and access keys to authenticate to GIT applications attached to the platforms and accessible from the workspaces.

The **Overview Page** allows you to edit personal information, define a work schedule, view owned workspaces and project membership.

The screenshot shows the 'Overview' page for a user named Victor. The page has a top navigation bar with 'Overview', 'Integrations', 'Configuration', 'Security', and 'Troubleshoot'. The left sidebar contains links for 'Overview', 'User Information', 'Work Schedule', 'Workspaces', and 'Projects'. The main content area is titled 'User Information' and contains several sections: 'Full Name' (Victor) and 'Email' (victor@company.com); a toggle for 'Set the time zone automatically' (checked); 'Time Zone' (Europe/Zurich (GMT+2)); 'Time Format' (24-Hour Clock) and 'Date Format' (Day Month Year); 'Color Mode' (Light); and a toggle for 'Automatically choose the region with lowest latency' (checked). Below this is a table with columns 'REGION NAME' and 'ROUND TRIP TIME (MS)'. The table has one row with 'Default Region' and a 'Check' button.

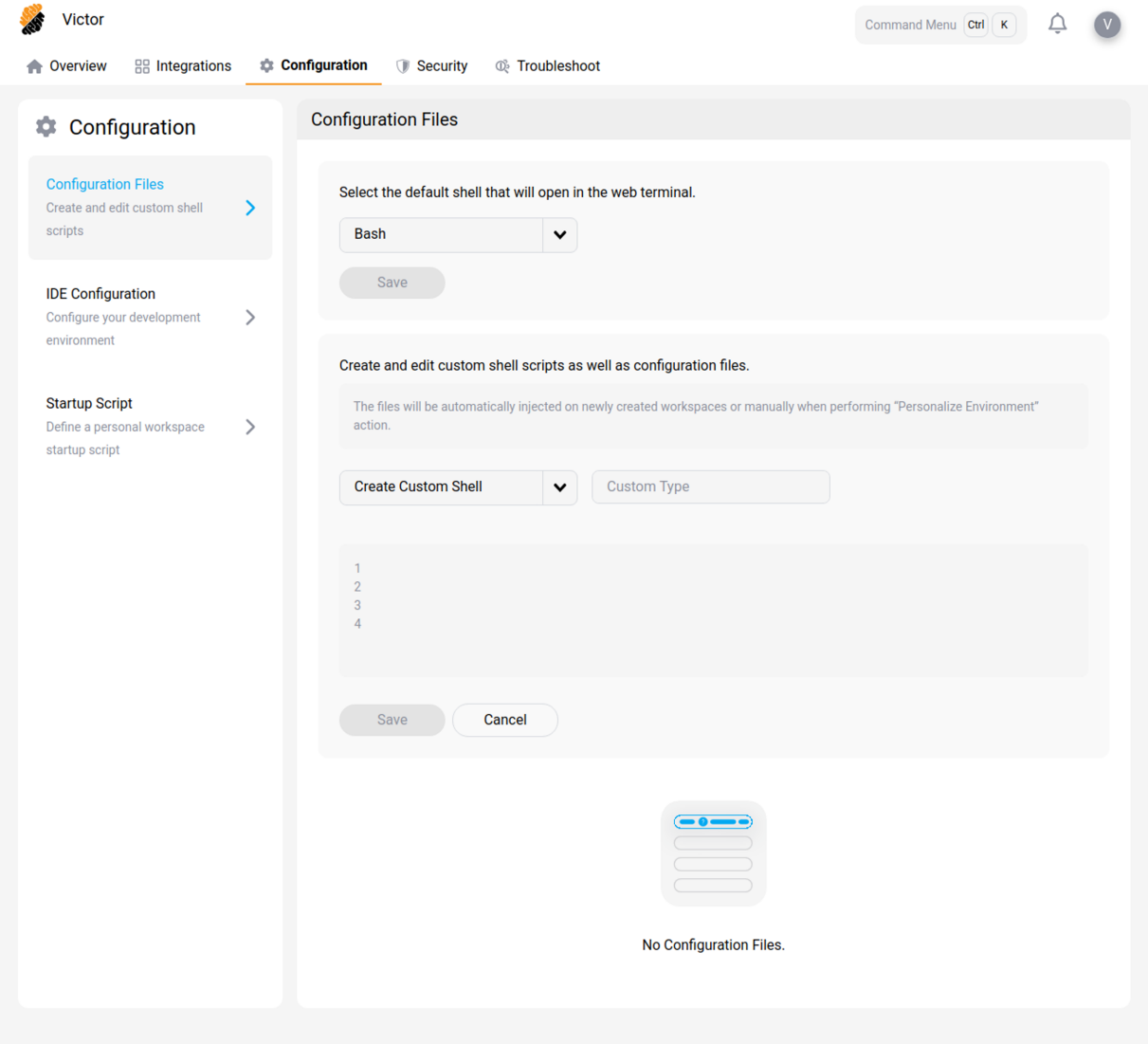
| REGION NAME    | ROUND TRIP TIME (MS)  |
|----------------|-----------------------|
| Default Region | <a href="#">Check</a> |

The **Integration Page** allows you to create and edit different authentication tokens, personal SSH identity and GTG keys.

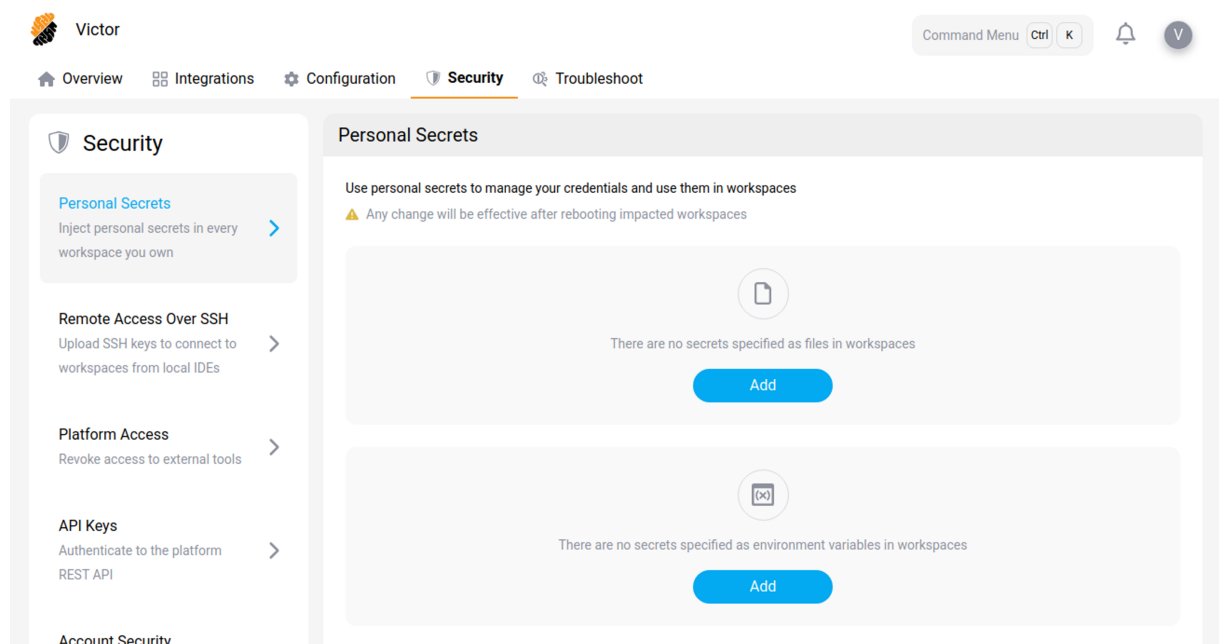


The **Configuration Page** allows you to create and edit custom configuration files, IDE configurations and workspace startup scripts.





The **Security Page** allows you to create and edit API keys, SSH keys and personal secrets.



## Content

- [Overview Page](#)
- [Integration Page](#)
- [Configuration Page](#)
- [Security Page](#)

## Profile Overview

August 26, 2025

The **Profile Overview Page** serves as a comprehensive summary of the user's information, their workspace ownership and project membership.

- [User Information](#)
- [Work Schedule](#)
- [Workspaces](#)
- [Projects](#)


## User Information

In the **User Information** section you can modify your user’s name and time zone.

The email linked to your profile cannot be modified.

The profile picture is retrieved from your identity provider when available.

User Information



Full Name

Victor

Email

victor@company.com

☒ Set the time zone automatically

Time Zone

Europe/Zurich (GMT+2)

Time Format

12-Hour Clock

24-Hour Clock

Day Month Year

Year Month Day

Month Day Year

12:24 PM

12:24

08/04/2025

2025/04/08

04/08/2025

Color Mode

Choose how Strong Network looks to you. Select a single theme, or sync with your system and automatically switch between dark and light themes.

Light

Dark

System

☒ Automatically choose the region with lowest latency

REGION NAME

ROUND TRIP TIME (MS)

☒ Default Region

×

Check

## Work Schedule

In the **Work Schedule** section, you can configure your profile’s work schedule. During set hours your main workspace (i.e. last used) is automatically deployed.

© 1997–2025 Citrix Systems, Inc. All rights reserved.

132

Work Schedule

Timeout Outside Schedule

Select a timeout after which the workspace will be automatically paused when not in use and running outside of scheduled hours. You can remove specific timeout options, making those options unavailable to users.

30 minutes ▼

Idle Timeout

Select a timeout after which the workspace will be automatically paused when not in use, regardless of the schedule. You can remove specific timeout options, making those options unavailable to users.

8 hours ▼

Select a daily schedule such that your main workspace (i.e. last used) automatically runs during set hours.

- Note that any workspace will pause automatically when not used after the set timeout time.
- When a workspace is paused voluntarily, it will not be started by this schedule.

M

T

W

T

F

S

S

Save

**Tip:**

Workspaces will pause automatically when not used for over a pre-set time, typically 60 minutes, depending on the setup of your platform.

When a workspace is paused voluntarily, it will not be impacted by the schedule.

## Workspaces

In the **Workspaces** section, you can find details about your individual workspaces across all projects that you are a part of. By selecting the “...” option on a specific workspace, you can directly perform actions such as running, pausing, editing, viewing details, or deleting the workspace.

Workspaces

Q Search




| NAME               | SHARED WITH | ORGANIZATION/PROJECT           | STATUS ▾ | ACCESS | ACTIONS |
|--------------------|-------------|--------------------------------|----------|--------|---------|
| Victor's Workspace | not shared  | Smart Organization / Core Team | Running  |        | ...     |

Projects

The **Projects** section displays information about every project that you are a member of, within the organizations to which you belong. This includes details such as the project name, the organization hosting the project, your role within the project, the project owner, and the number of users involved in the project. By clicking on a project’s name, you can access its dashboard for more information.

Projects

Q Search

| PROJECT NAME  | ORGANIZATION   | ROLE          | PROJECT OWNER ▾   | USER COUNT ▾ |
|---|--|---------------|---|--------------|
|  Core Team |  Smart Organization | Project Owner |  J | 4            |

## Integration

August 26, 2025

In the **Integration Page** you can manage the different access keys, secrets and tokens that are linked to the user’s profile.

This includes **Code Repository Tokens**, **Personal SSH Identity** and **GPG Keys**. The keys and tokens are used to authenticate and authorize access to different services, such as remote repository applications. By managing their keys, tokens and secrets in one location, users can easily keep track of which ones are being used, for what purpose and can revoke or add new ones as needed. The page also allows the user to view, create, and remove them, to manage access levels and to have an overview of their expiration date. This helps to ensure that only authorized users have access to the necessary resources and services, and that access is revoked when necessary.

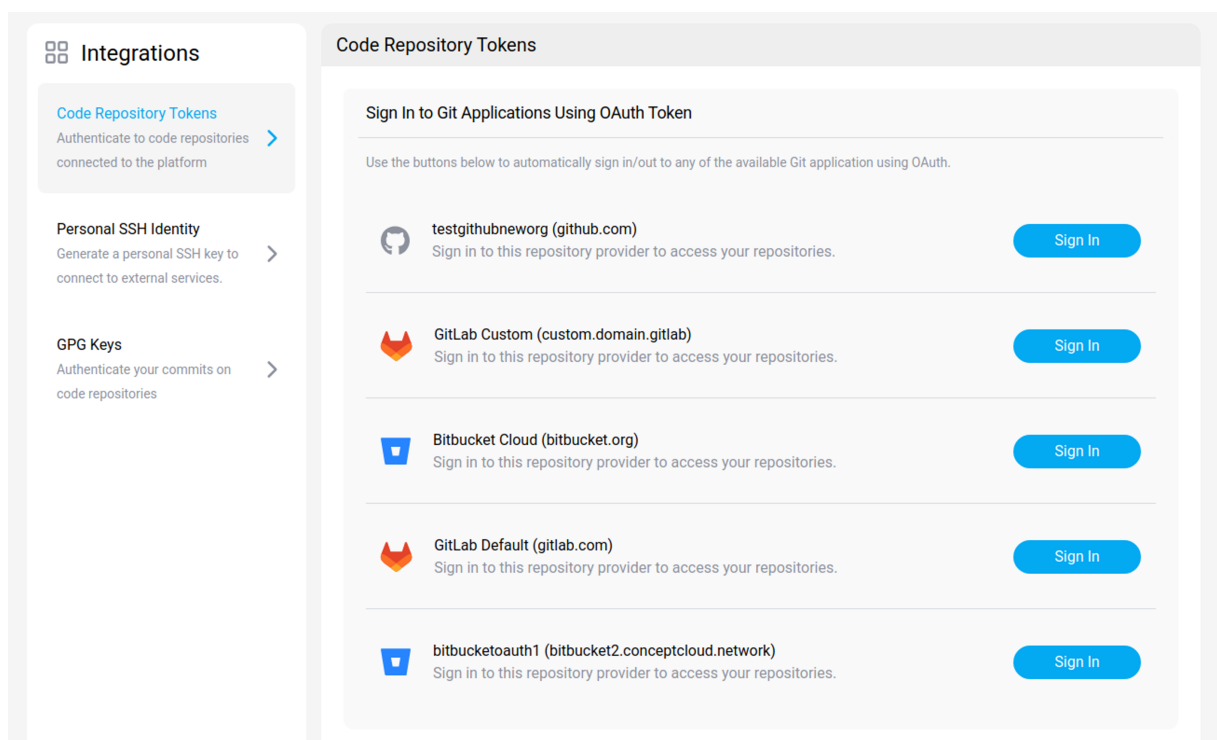
- [Code Repository Tokens](#)
- [Personal SSH Identity](#)
- [GPG Keys](#)

## Code Repository Tokens

Under **Code Repository Tokens**, you can configure authentication, using **OAuth Authentication Tokens** or **Personal SSH Keys**, to the following git providers:

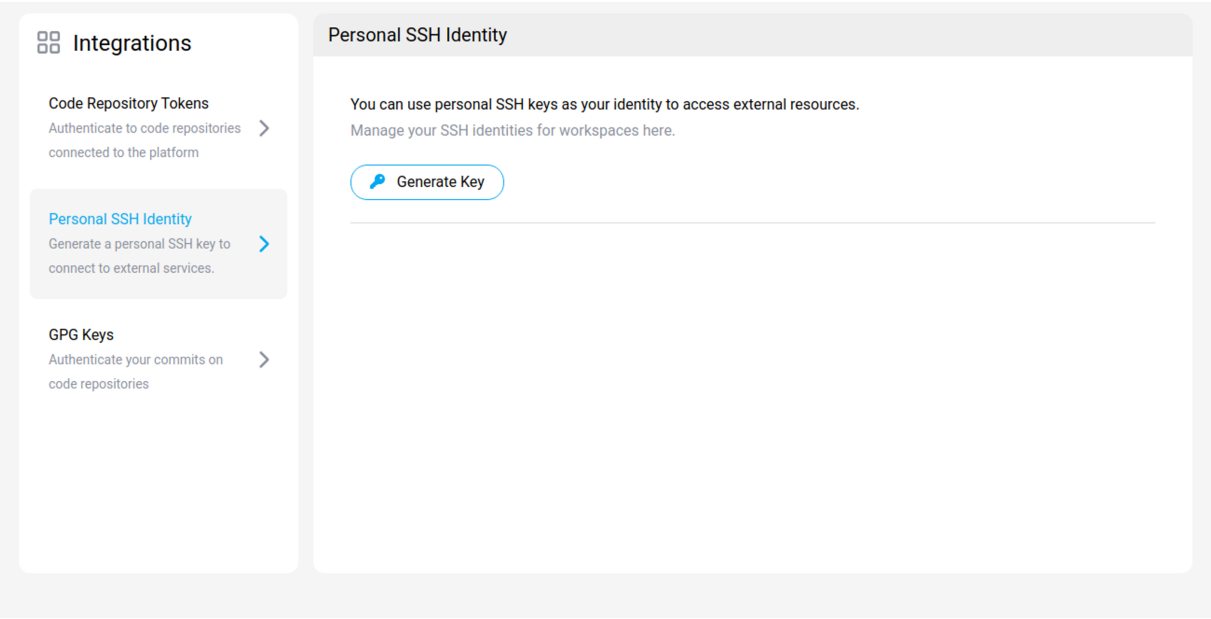
- **GitHub**,
- **GitLab**,
- and **Bitbucket**.

For certain of these git providers, you have the option to choose between the ‘Default’ or ‘Internal’ options. An ‘Internal Service’ is self-hosted, whereas a ‘Default Service’ is hosted on the cloud.



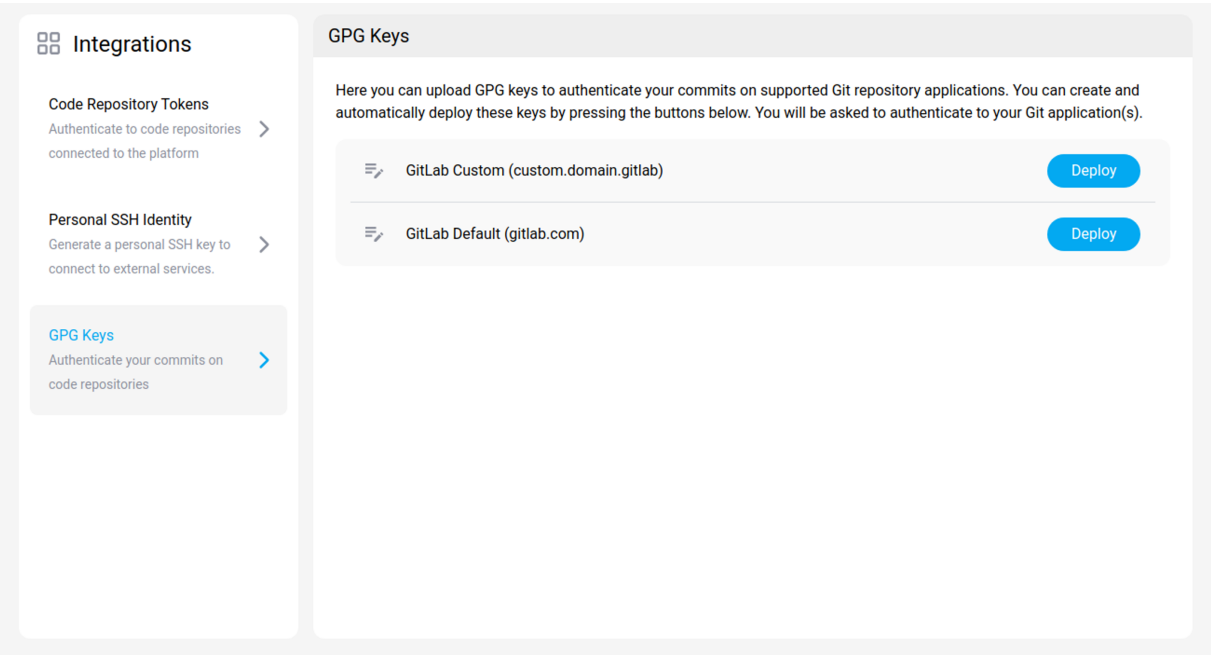
## Personal SSH Identity

You can generate a personal SSH key to authenticate yourself when accessing external resources. The SSH key will be applied to new or existing workspaces.



GPG Keys

You can generate and automatically deploy GPG keys to authenticate your commits on supported Git repository applications (i.e. GitHub).





## Configuration

August 26, 2025

The **Configuration Page** is used to create and edit custom shell scripts and configuration files, configure your IDE and define personal workspace startup scripts. You can also configure additional settings (e.g. [theme](#)) by clicking on the profile picture on the top right of the screen.

- [Configuration Files](#)
- [IDE Configuration](#)
- [Startup Script](#)
- [Theme](#)
- [Language](#)

### Configuration Files

Personal configuration files can be managed from the **Profile Settings**.

These files can be injected in any new or existing workspaces automatically using the ... icon and the option **personalize environment**.

The screenshot shows the 'Configuration' settings page. On the left is a sidebar with three options: 'Configuration Files' (selected), 'IDE Configuration', and 'Startup Script'. The main area is titled 'Configuration Files' and contains two sections. The first section, 'Select the default shell that will open in the web terminal.', has a dropdown menu set to 'Bash' and a 'Save' button. The second section, 'Create and edit custom shell scripts as well as configuration files.', includes a text box with instructions, a 'Create Custom Shell' dropdown, a 'Custom Type' input field, a text area with line numbers 1-4, and 'Save' and 'Cancel' buttons.

You can edit and manage typical shell scripts attached to Linux-based environments such as:

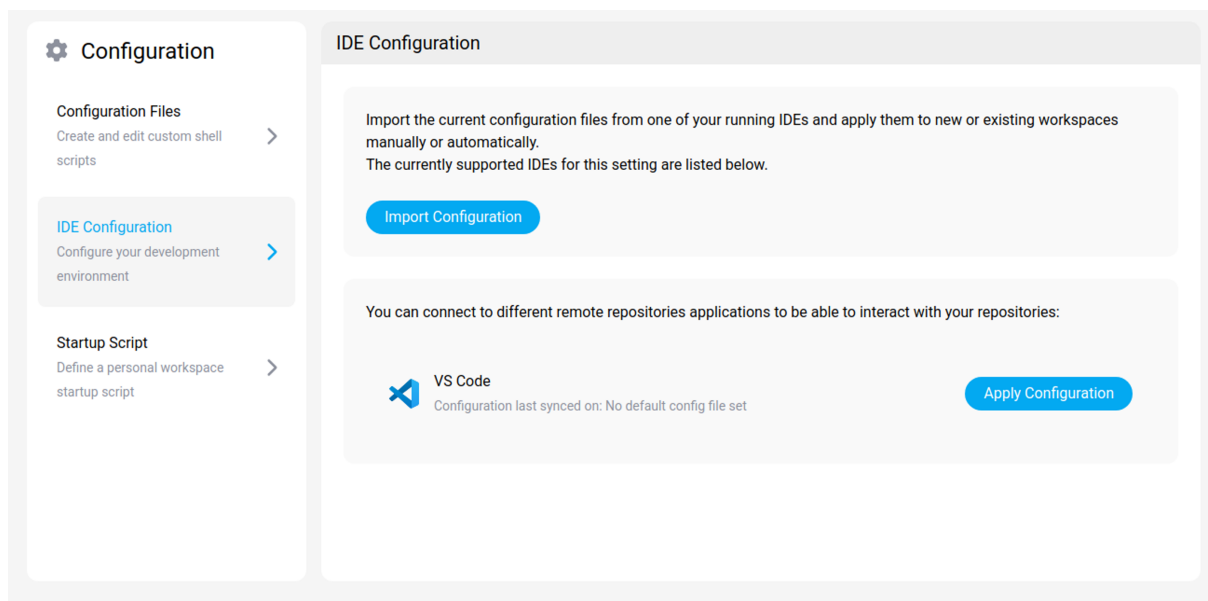
- **.bashrc**,

- **.zshrc**,
- **.profile**, or any file of your choice using the
- **custom**: option.

## IDE Configuration

IDE configuration files can be managed from the **profile settings**. A configuration must be initially imported from a **running** workspace.

Then, it can be applied to new or existing workspaces manually or automatically.



Currently supported IDEs are:

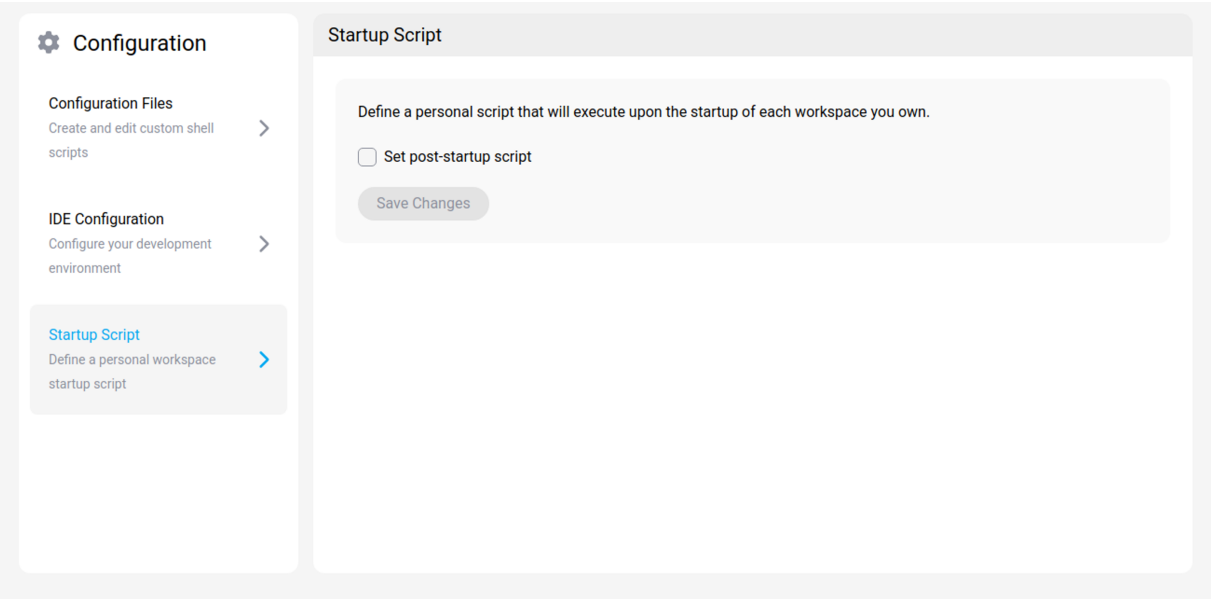
- **VSCode**,
- **any IDEs from JetBrains.**

## Startup Script

You can define a personal script that will be executed upon each startup of the workspaces that you own

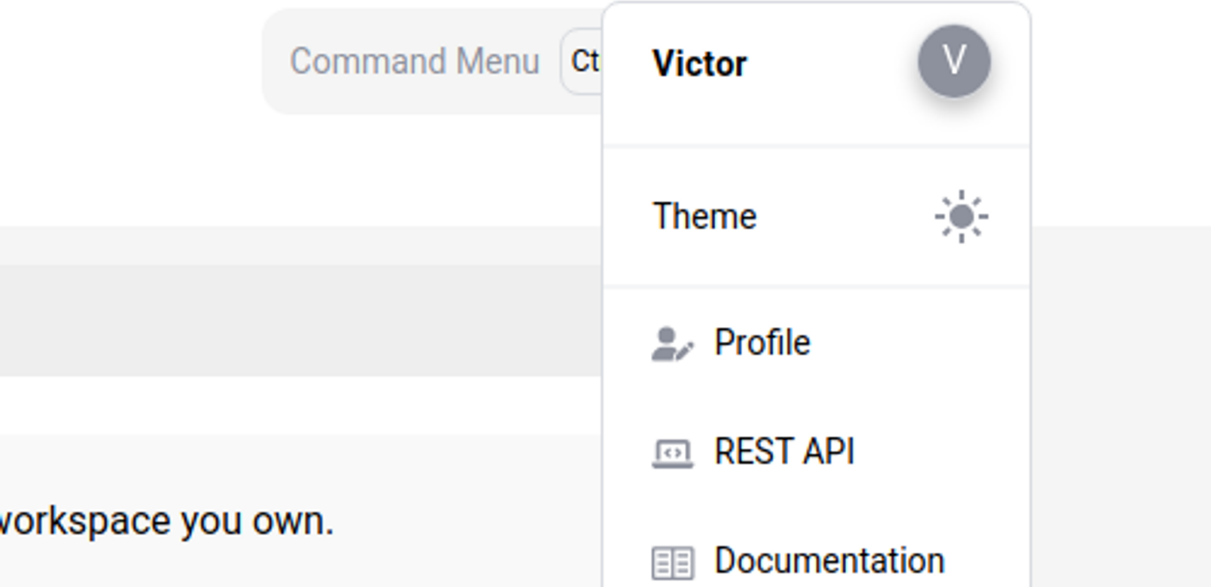
Tip:

Note that if you defined a startup script for a given workspace, then it will override this one



Theme

Two color themes for dashboards are available in the **Profile Menu**. You can switch between a **light** and **dark** theme for the User Interface (UI) display.



Language

A language for the UI can be selected from the footer. Supported languages for the platform UI are:

- **English,**

- **French.**

## Security

August 26, 2025

In the **Security Page** you can manage the different access keys, secrets and tokens that are linked to the user's profile.

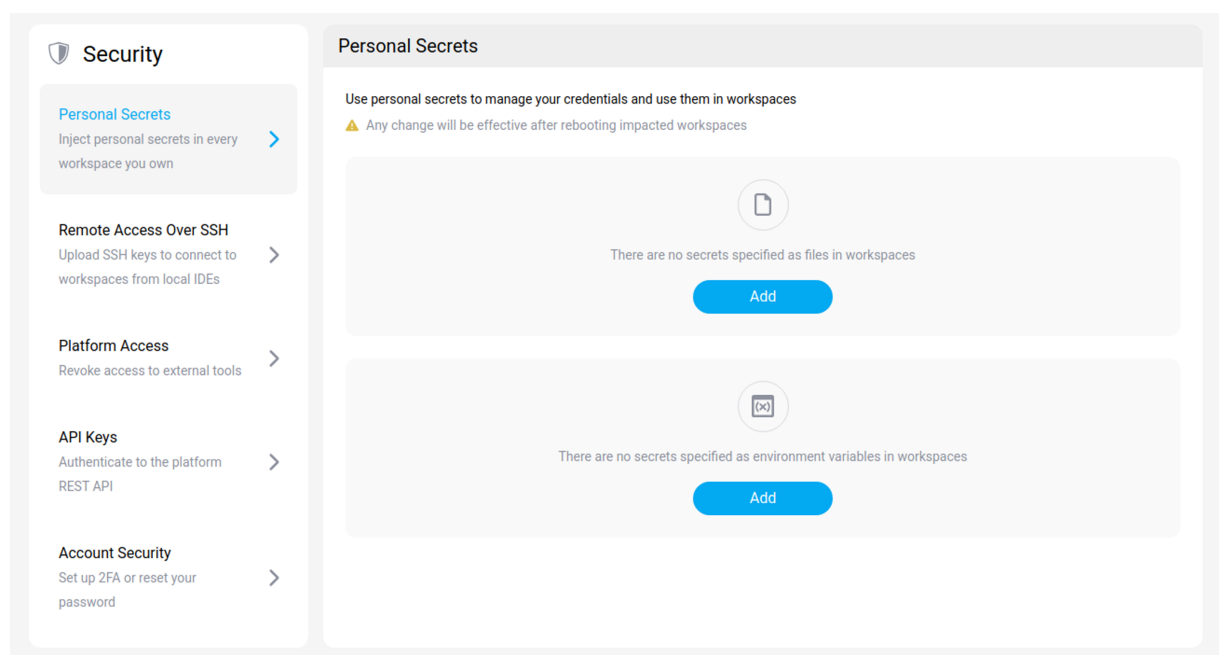
This includes **Personal Secrets**, **Remote Access Over SSH** keys, **API Keys** and **GPG Keys**. By managing their keys, tokens and secrets in one location, users can easily keep track of which ones are being used, for what purpose and can revoke or add new ones as needed. This helps to ensure that only authorized users have access to the necessary resources and services, and that access is revoked when necessary.

- [Personal Secrets](#)
- [Remote Access Over SSH](#)
- [API Keys](#)

### Personal Secrets

Under **Personal Secrets**, you can manage your secrets.

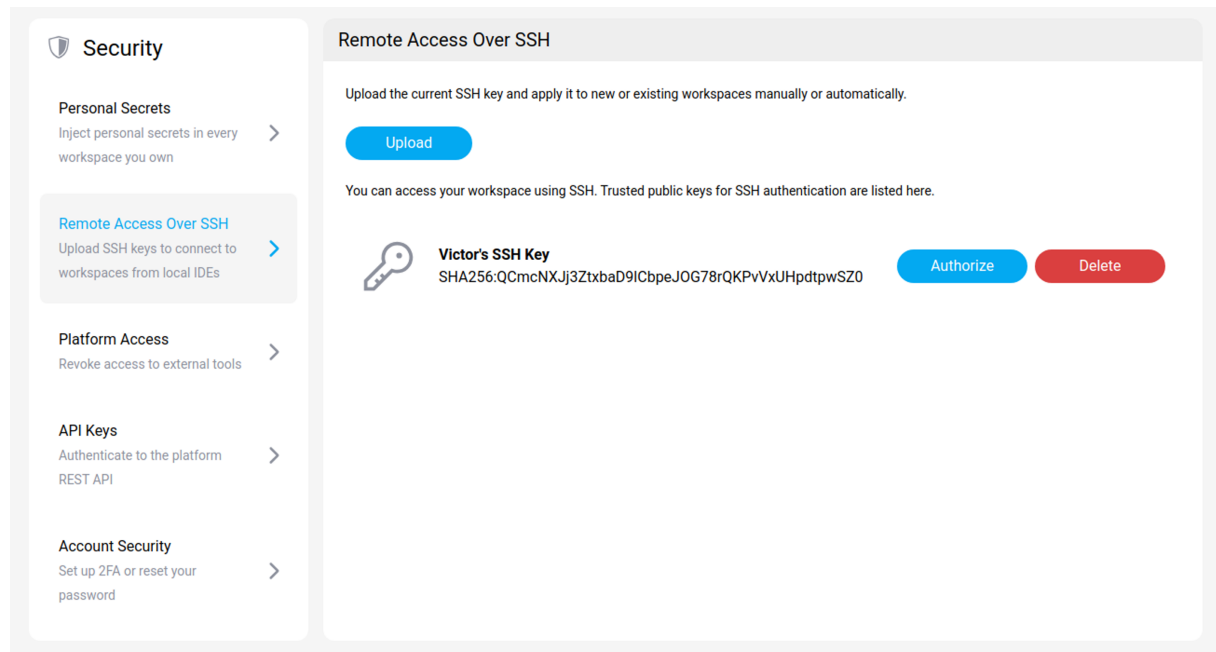
You add secrets that appear as files in your workspace, or add them as environment variables.



## Remote Access Over SSH

You can [access your workspace using SSH](#), which allows you to run VSCode locally. Trusted public keys for SSH authentication are displayed in this section. Each key is linked to your profile.

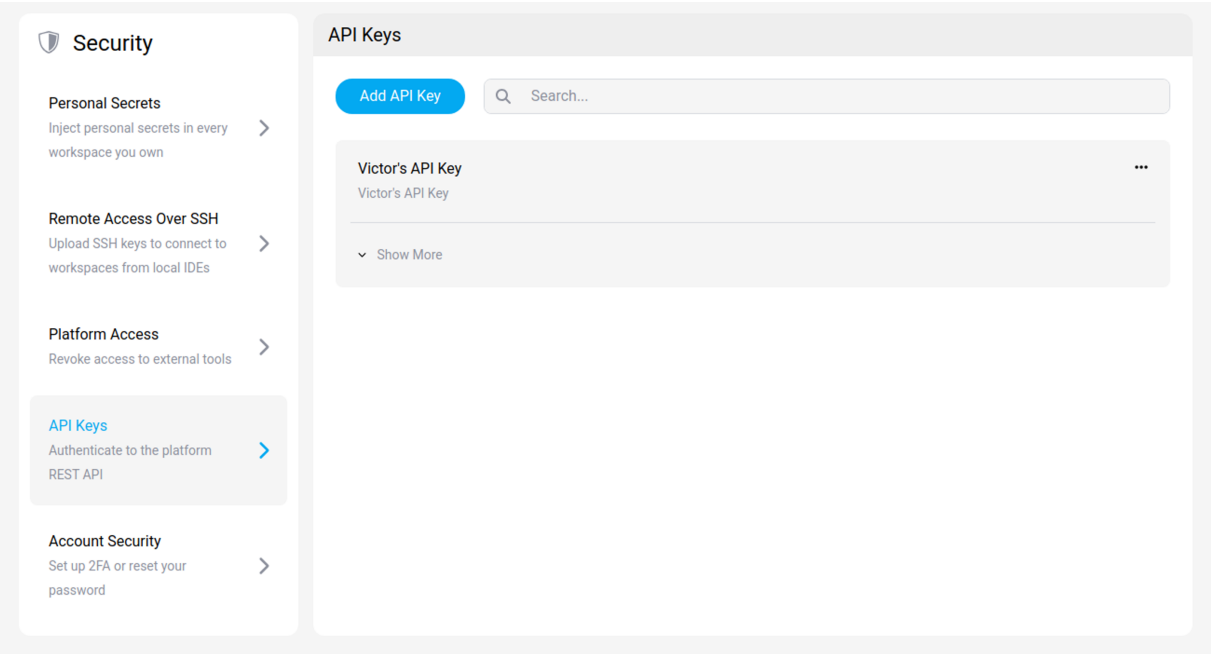
One benefit of accessing your workspace using SSH is flexibility. By allowing you to run VSCode on your local machine, you can still leverage the powerful hardware of the remote machine and still not give up on security. View [SSH Into Your Workspace](#) to set it up.



## API Keys

An **API key** is a unique identifier used to establish a connection to an API call. Once connected, the API service will be available in your workspaces.

API keys are used to authenticate the source of a request and make sure that the API is only used as intended. API keys are often used by web and mobile apps to connect to web-based services and retrieve or update data.



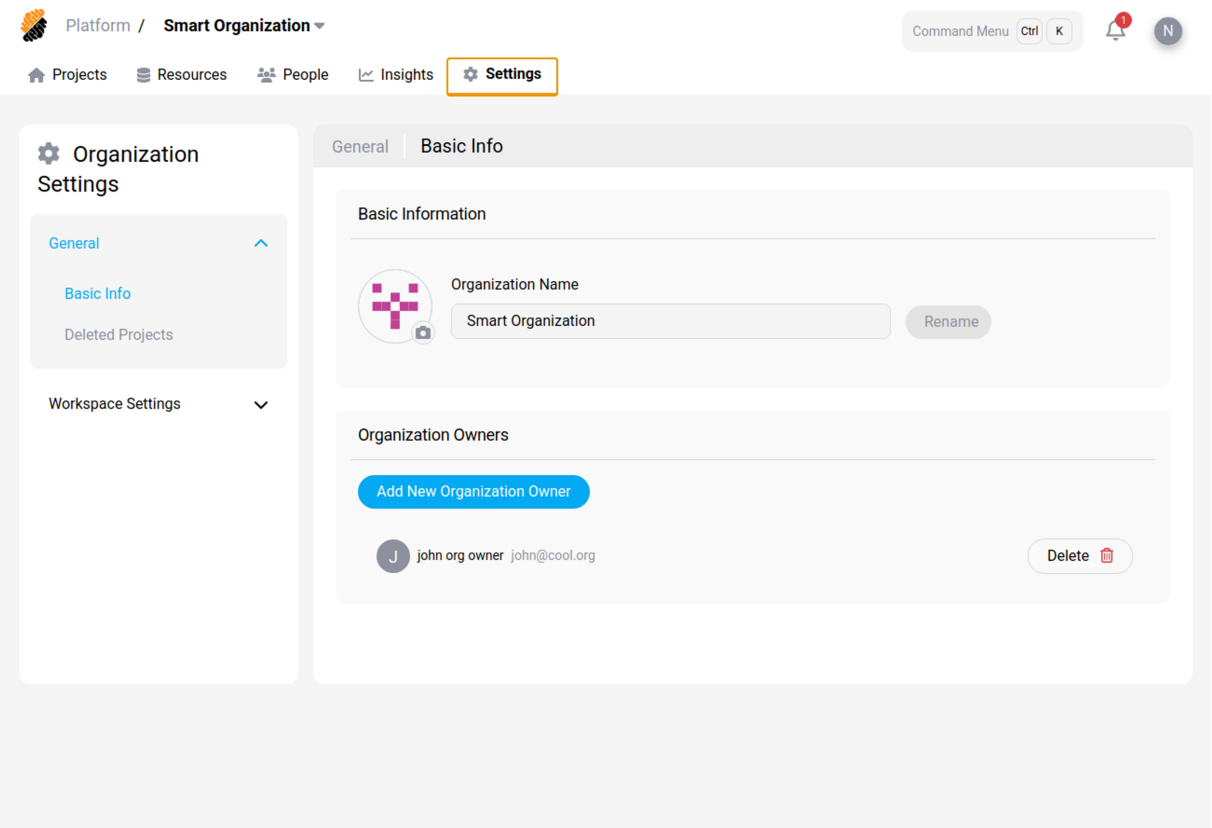
## Organization General Settings

August 1, 2025

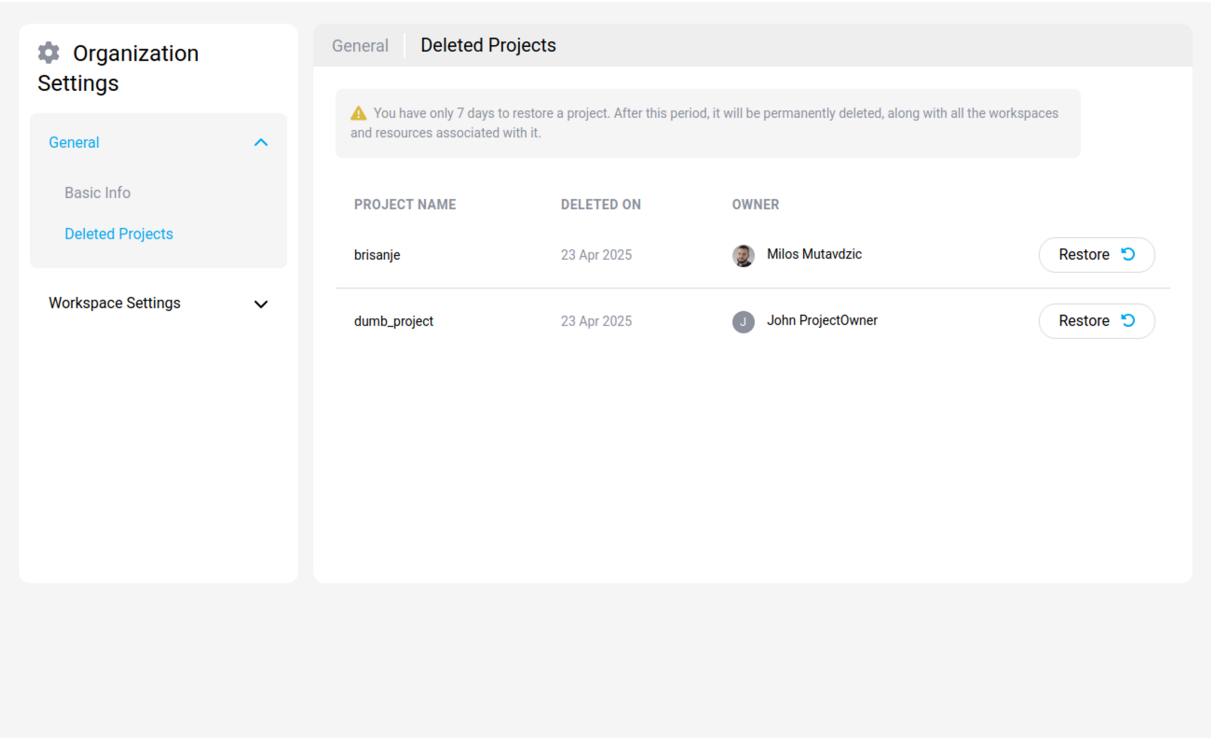
### Admin

The Organization Settings serve as the overarching control center for administering and standardizing configurations across all projects within the organization. By defining settings at the organizational level, you can enforce a consistent set of protocols, security measures, and resource limitations that will automatically apply to each new and existing project. This ensures uniform compliance and operational efficiency throughout the organizational ecosystem.

For detailed configurations at the project level, please refer to the [Project Settings](#) page.



Additionally, Organization Settings provide a safeguard against accidental deletions by allowing you to recover deleted projects for up to 7 days. After this period, the projects are permanently deleted. This recovery window helps prevent the permanent loss of project data.



## Workspace Settings

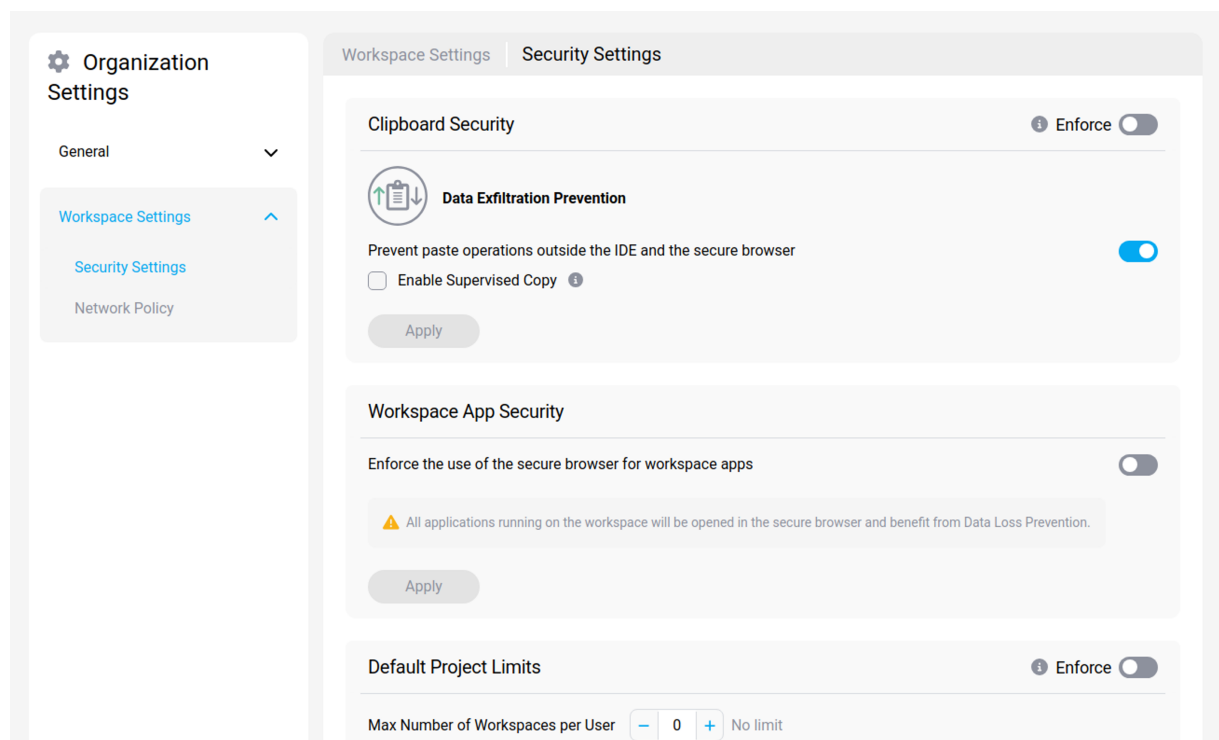
August 26, 2025

This section focuses on configuring settings for workspaces that apply across the entire organization. Define organization-wide security policies governing aspects like data handling and access, and establish network policies to control workspace traffic consistently for all projects within the organization.

### Security Settings

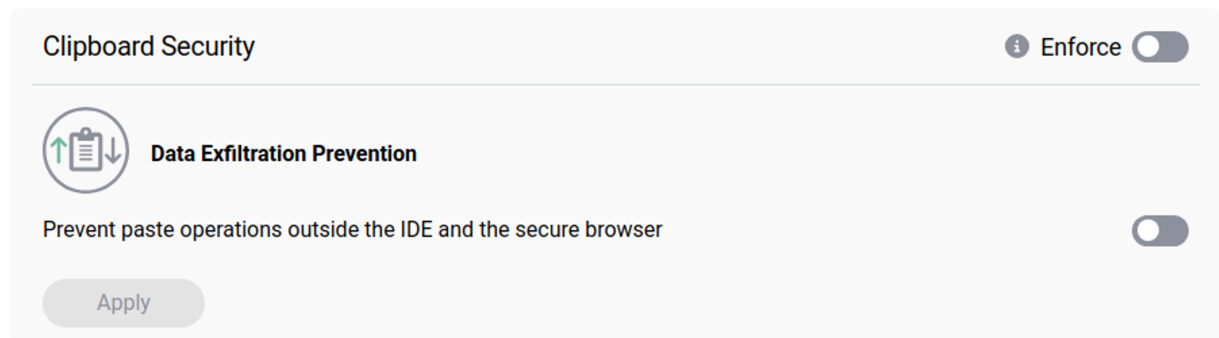
In the “Workspace Settings” section, the “Security Settings” enable you to implement multiple policies including Clipboard Monitoring, Workspace App Security, and Default Project Limits. These policies can be enforced to establish a foundational level of security across all workspaces within your project.





## Clipboard Security

Clipboard Security implements Data Loss Prevention policies to safeguard against data leaks by disabling the ability to paste content from the IDE and secure browser into external applications.




## Workspace App Security

Workspace App Security allows you to mandate the use of a secure browser for workspace applications, ensuring that developers can share the applications they are developing in a protected environment. When used in conjunction with the Clipboard Security policy, this feature helps to prevent any potential data exfiltration from workspace applications.

Workspace App Security

Enforce the use of the secure browser for workspace apps

 All applications running on the workspace will be opened in the secure browser and benefit from Data Loss Prevention.

Apply

**Default Project Limits**

Default Project Limits can be set to cap the number of workspaces a user can create. This not only aids in resource monitoring and reduces unnecessary workspace proliferation but also contributes to cost efficiency by avoiding the operation of unused workspaces.

Default Project Limits

Max Number of Workspaces per User

–

0

+

No limit

Apply

**Enable Remote Development Over SSH**

Remote Development Over SSH gives you the option to permit or deny developers the ability to connect to their workspaces via SSH. While convenient for certain tasks, this feature must be used judiciously as it can reduce the effectiveness of local IDE data loss prevention measures.

Remote Development Over SSH


Enable

Set as Default

When creating a new workspace, SSH is part of the access toolset.

Update All Workspaces

Use this button to add SSH in the access toolkit to all workspaces in this project.

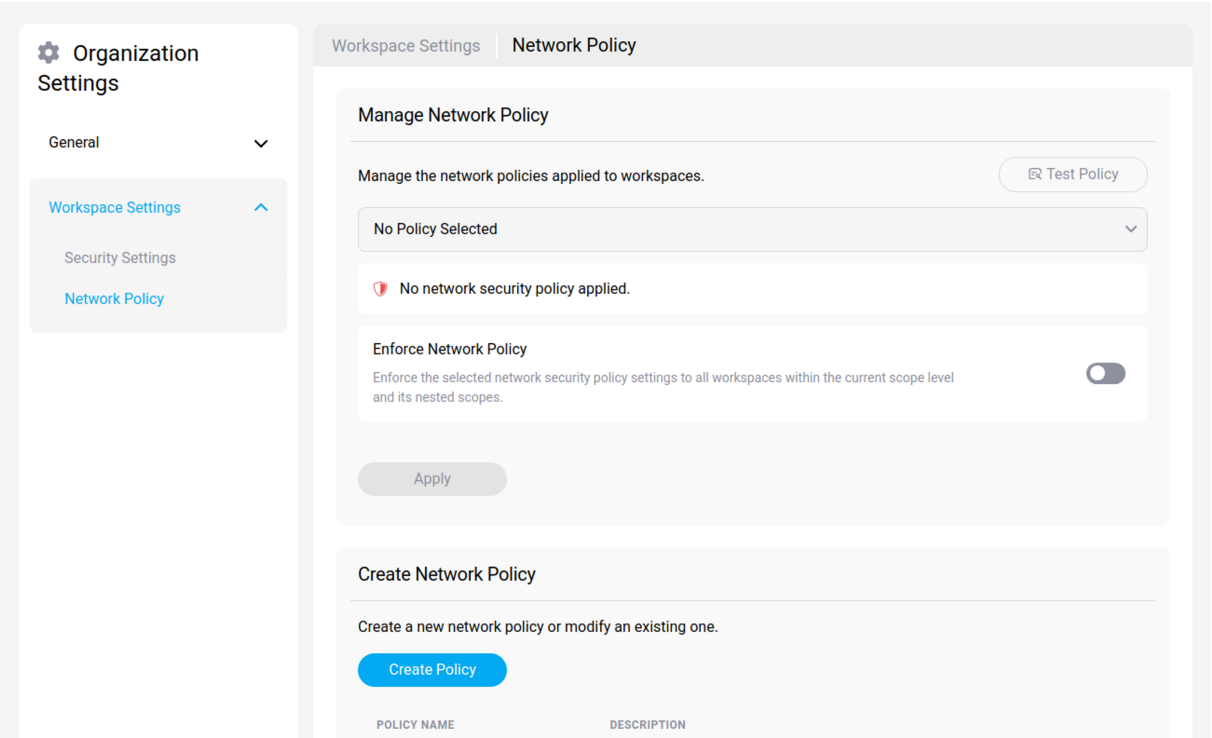
 Data exfiltration prevention will be disabled on all workspaces.

Apply

Update All

## Network Policy

Network policies are attached to [workspace](#) and enable fine-grained network traffic control. Network traffic is identified using combinations of IP addresses, port and domain names. Once a network policy is attached to a workspace, all **out-bound** traffic is enforced by the rules in the policy and the workspace’s user cannot circumvent the restrictions.



## Default Network Policies

Three default policies are available in a project. An administrator can create a new Network Policy if needed.

| Name                   | Scope   | Description  |
|------------------------|---------|--|
| <b>Monitor Traffic</b> | Project | This is a standard policy to monitor the outgoing traffic to the workspace. It will cause the generation of log events in the Audit dashboard. |

| Name                    | Scope   | Description   |
|-------------------------|---------|---|
| <b>Restrict Traffic</b> | Project | This is a standard policy to restrict outgoing traffic from the workspace. It will block all traffic except to attached repositories and domains. Failed network requests are shown in the log events in the Audit dashboard. |

**Add a Network Policy**

You can create a Network Policy by pressing the “**Create Policy**”button.

Workspace Settings | Network Policy

Define Network Policy

Expert mode

Use the options below to define a network policy to assign to workspaces.

Policy Name \*

Description \*

Restrict Traffic to Selected Resources

Enabling this option, outbound traffic is restricted to authorized resources, e.g. Git repositories, connected services, etc. In addition, you may define a whitelist of domains and IP addresses

+ Add Domain

+ Add IP Address

Add Policy

Cancel

Test Policy

You will need to enter the following information:

1. **Name**, a name to identify the policy,
2. **Description**,

### Warning

Be careful when naming and describing a new policy. A misleading name can end up in giving too many permissions to a user.

1. **Log and record outbound network traffic** (default),
2. **Restrict Traffic to Selected Resources** (optional),  
All traffic will be restricted, except for end systems added to your **whitelist**
  - Add each application that you want to whitelist
  - Add Domains that you want to whitelist, and indicate whether to include subdomains
  - Add IPs that you want to whitelist

### Edit or Delete a Network Policy

You can edit or delete a Network Policy by clicking on the “...” icon next to its class level.

## General Settings

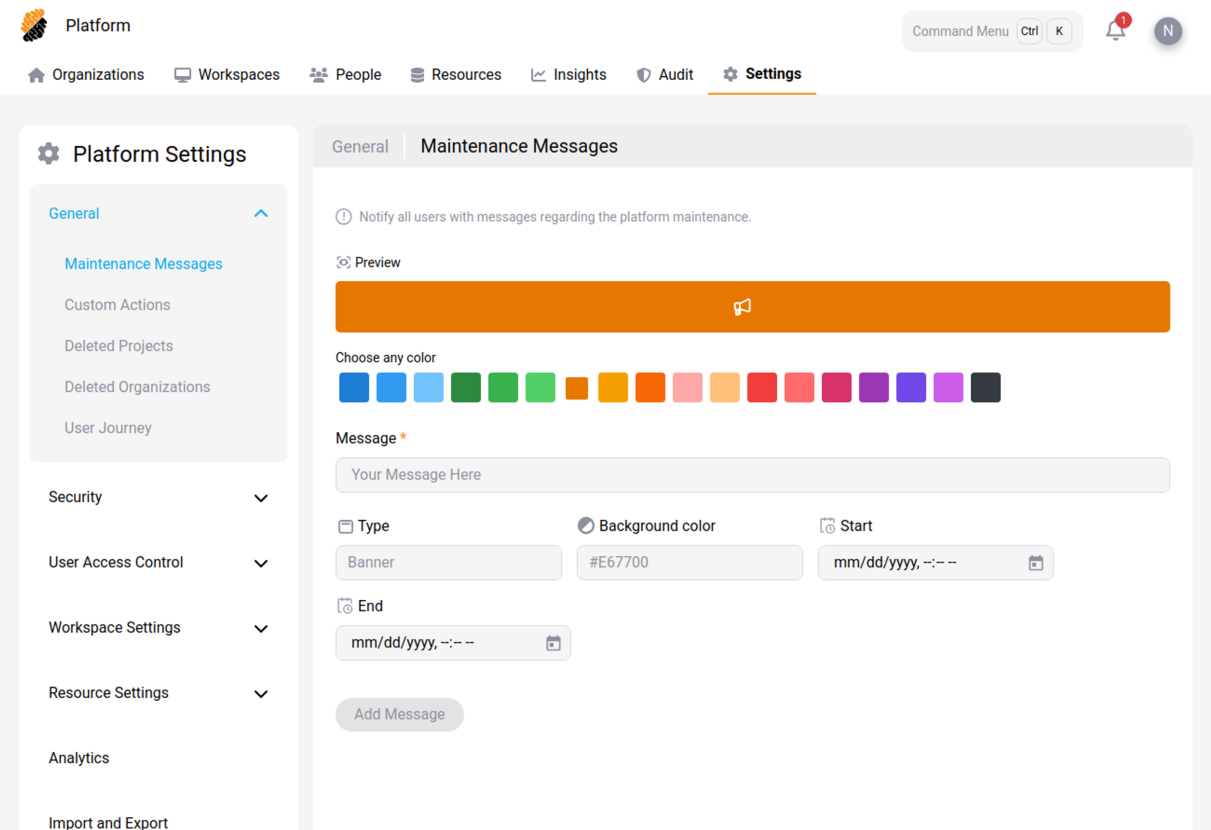
July 8, 2025

This section covers fundamental platform-wide configurations. Here, administrators can manage **Maintenance Messages**, configure **Custom Actions**, handle the recovery of **Deleted Projects** and **Deleted Organizations**, and adjust settings related to the initial **User Journey**. These settings govern the overall operational aspects and user experience defaults of the platform.

- [Maintenance Messages](#)
- [Custom Actions](#)
- [Deleted Projects](#)
- [Deleted Organizations](#)
- [User Journey](#)

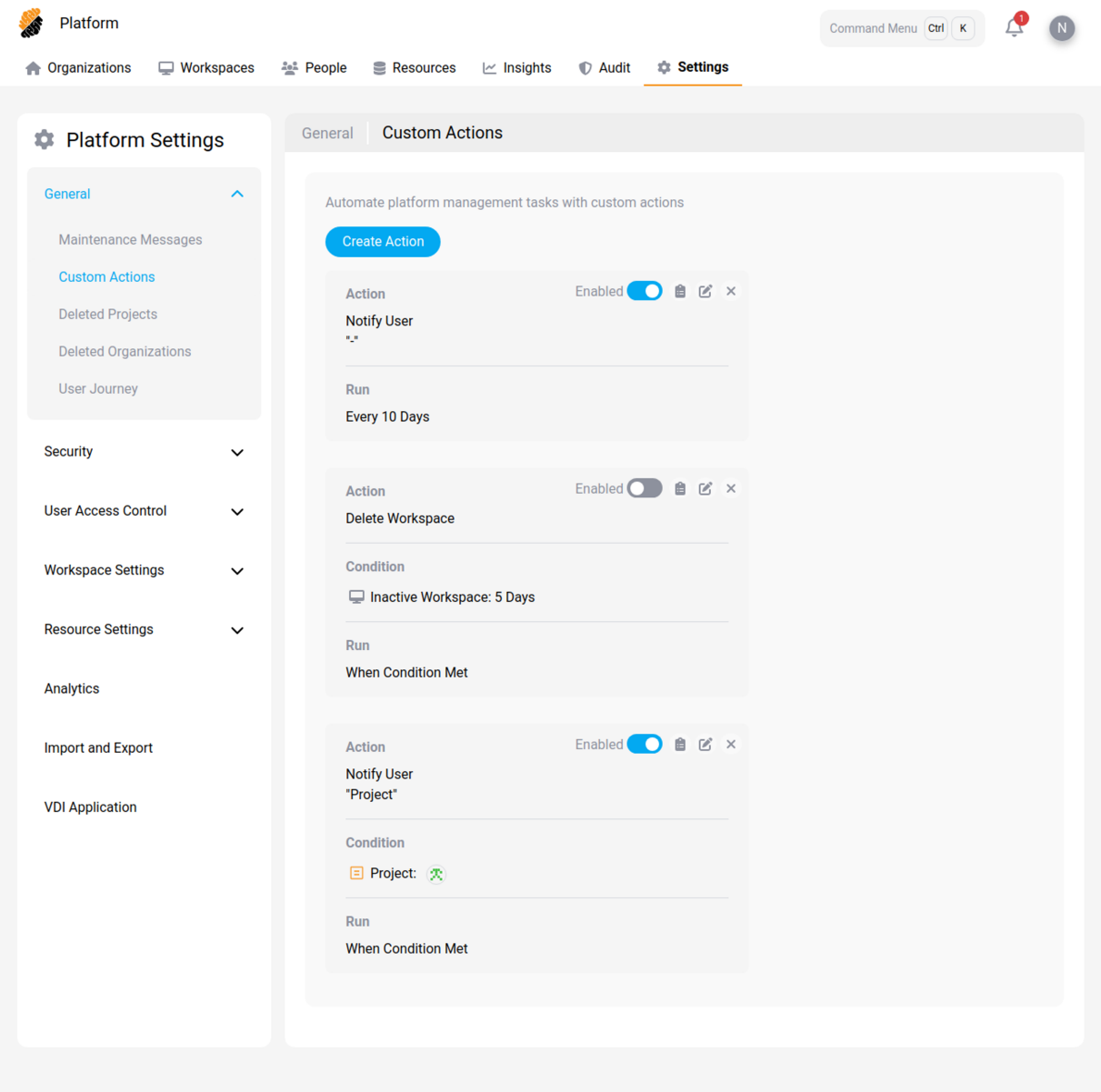
### Maintenance Messages

You can configure and display maintenance messages to users. These messages can inform users about scheduled downtime, ongoing maintenance activities, or other important platform-wide notifications.



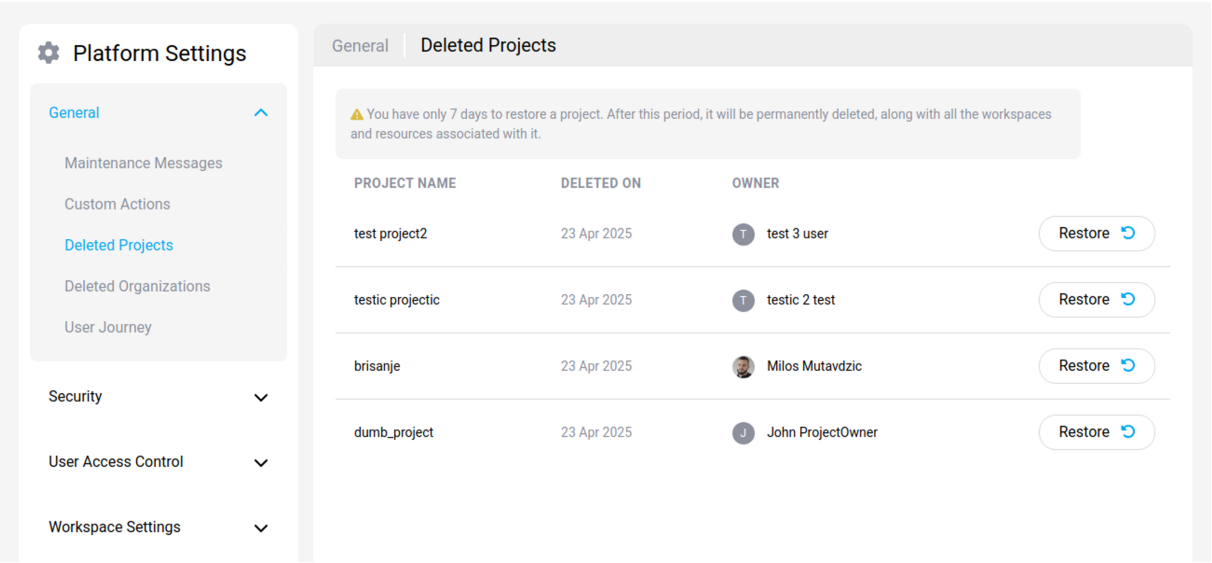
Custom Actions

Configure custom actions that can be triggered within the platform. This allows for extending platform functionality with specific automated tasks or integrations tailored to your organization’s workflows.



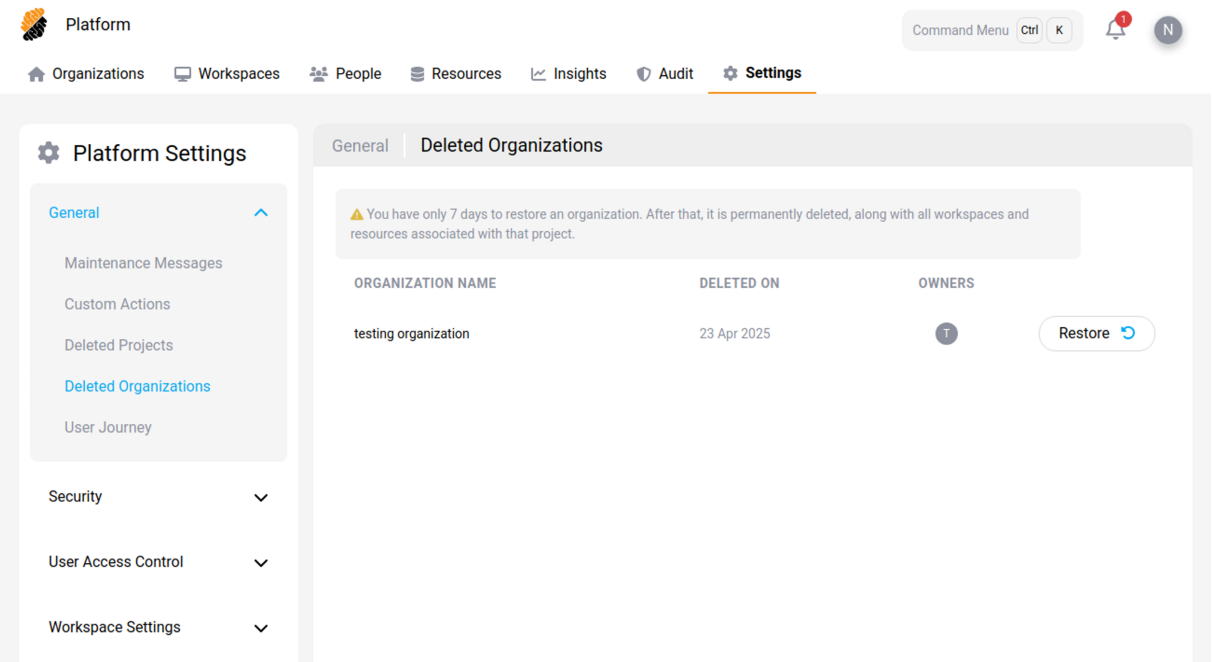
Deleted Projects

You can recover a deleted [project](#) for a period of 7 days on the **Deleted Projects** tab. Simply press the **Recover** button the right of the project you want to restore.



Deleted Organizations

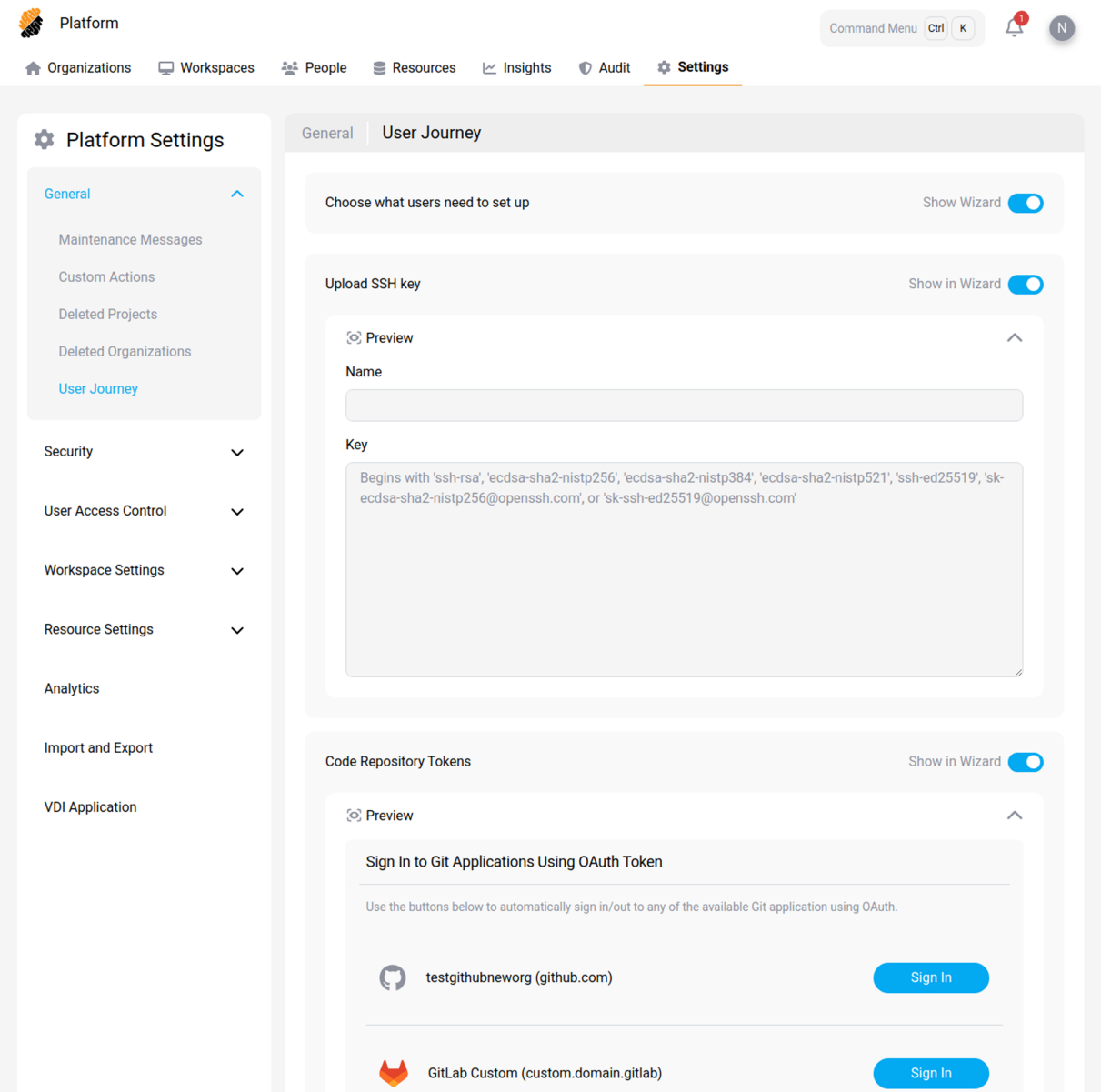
You can recover a deleted organization for a period of 7 days on the Deleted Organizations tab. Simply press the **Recover** button to the right of the organization you want to restore.



User Journey

This section allows administrators to configure the initial setup wizard presented to users upon their first interaction with the platform.





## Security Settings

August 1, 2025

Configure critical security parameters for the entire platform. This includes managing **SAML Integration** for secure web application access via RBI, setting up **SIEM Integration** for centralized logging, getting a **Network Policy Overview**, and establishing platform-wide **Information Security Policy** settings. These settings are essential for protecting platform resources and ensuring secure user access.

- [Network Policy Overview](#)
- [SAML Integration](#)
- [SIEM Integration](#)
- [Information Security Policy](#)

## Network Policy Overview

Get a summary view of the network policies currently applied across the platform. This overview helps administrators quickly understand the existing network security configurations and rules at a high level.

Platform Settings

General

Security

Network Policy Overview

SAML Integration

SIEM Integration

Information Security Policy

User Access Control

Workspace Settings

Resource Settings

Analytics

Import and Export

VDI Application

Security

Network Policy Overview

Search...

Download Report

Platform

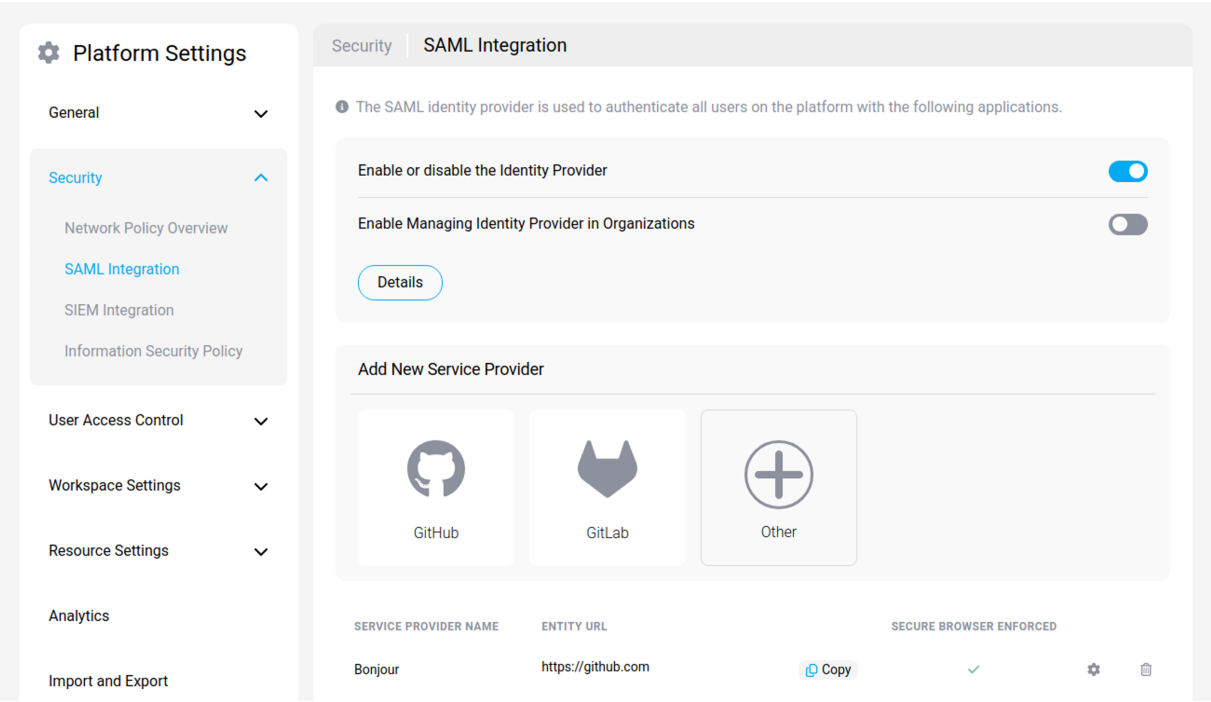
Edit

| POLICY LEVELS      | APPLIED POLICY | STATUS       | ACTION |
|--------------------|----------------|--------------|--------|
| oz-org             | No Policy      | Not enforced | Edit   |
| marko              | No Policy      | Not enforced | Edit   |
| bjorg              | No Policy      | Not enforced | Edit   |
| fer                | No Policy      | Not enforced | Edit   |
| Bastian            | No Policy      | Not enforced | Edit   |
| oz-github          | No Policy      | Not enforced | Edit   |
| Smart Organization | No Policy      | Not enforced | Edit   |
| dule org           | No Policy      | Not enforced | Edit   |
| Markntest          | No Policy      | Not enforced | Edit   |

## SAML Integration

The **SAML Integration** section is responsible for authenticating all users on the platform when accessing web applications. Users access these Web Applications through Remote Browser Isolation (RBI), known on the platform as the “Secure Browser”. The Secure Browser offers DLP-enabled access to any sensitive domains, such as GitHub, Jira, and GitLab. Users are restricted to accessing these Web Applications solely through the platform, prohibiting access via external browsers.

Administrators have the option to enable or disable a pre-configured identity provider. They can also allow organizations to oversee their own identity providers.



**SIEM Integration**

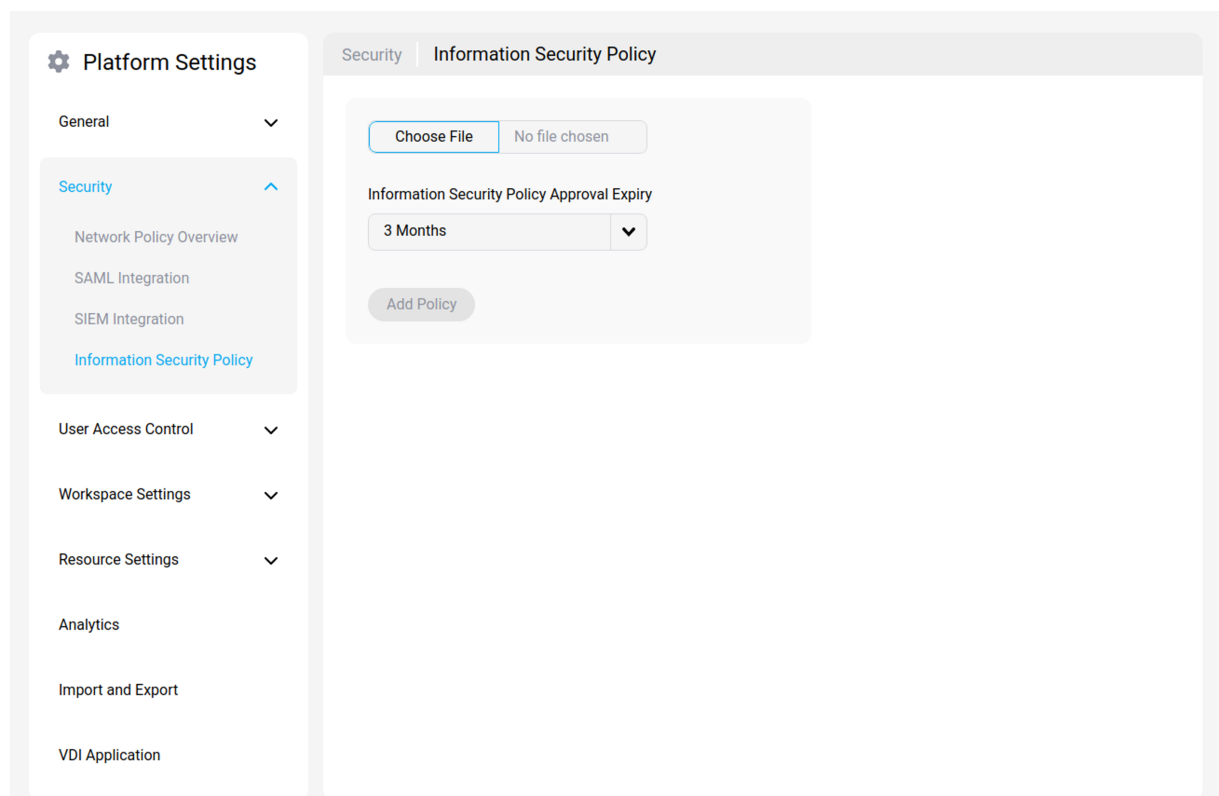
Configure the integration of the platform with your Security Information and Event Management (SIEM) system. This allows for forwarding logs and security events from the platform to your central SIEM for monitoring, analysis, and alerting.

The screenshot displays the 'Platform Settings' interface. On the left is a sidebar with a 'Platform Settings' header and a gear icon. Below it are several expandable sections: 'General', 'Security' (which is expanded), 'User Access Control', 'Workspace Settings', 'Resource Settings', 'Analytics', 'Import and Export', and 'VDI Application'. The 'Security' section contains links for 'Network Policy Overview', 'SAML Integration', 'SIEM Integration' (highlighted in blue), and 'Information Security Policy'. The main content area is titled 'SIEM Integration' and includes a sub-header 'Security'. It contains a message: 'Establish a connection to a SIEM tool using the Common Event Format (CEF). SIEM integration not deployed. Check the YAML example below on how to set-up it using a Filebeat agent.' Below this message is a code block containing a YAML configuration for Filebeat and a ConfigMap. The code is as follows:

```
1 ---
2 apiVersion: v1
3 kind: ServiceAccount
4 metadata:
5   name: release-filebeat
6   namespace: release
7   labels:
8     k8s-app: filebeat
9 ---
10 apiVersion: v1
11 kind: ConfigMap
12 metadata:
13   name: release-filebeat-config
14   namespace: release
15   labels:
16     k8s-app: filebeat
17 data:
18   filebeat.yml: |-
19     filebeat.inputs:
20     - type: log
21       paths:
22         - /var/strong-network/*.log
23
24   processors:
25     - add_cloud_metadata:
26     - add_host_metadata:
27
28   cloud.id: ${ELASTIC_CLOUD_ID}
```

## Information Security Policy

Define and manage the information security policies enforced by the platform. This section may include settings related to data handling, access controls, and compliance standards that users and the system must adhere to.



## User Access Control

August 1, 2025

Manage how users authenticate and what they can access at the platform level. This involves configuring **Registered Domains and Identity Providers** (IDPs), including multi-factor authentication, and setting platform-wide rules via **User Access Control Settings** which encompass compliance features, platform constraints, and container image URL constraints.

- [Domain and IDP](#)
- [User Access Control Settings](#)

### Domain and IDP

The **Registered Domains and Identity Providers** section offers a centralized control over user authentication processes. By defining specific domain names from which your users originate, you can associate them with a corresponding identity provider (IDP). As a result, users from the designated domain will be authenticated using the chosen IDP.

This section allows you to set access permissions based on specific domains and also offers the option to enable two-factor authentication, enhancing overall security.

Platform Settings

General

Security

User Access Control

Domain and IDP

Settings

Workspace Settings

Resource Settings

Analytics

Import and Export

VDI Application

User Access Control

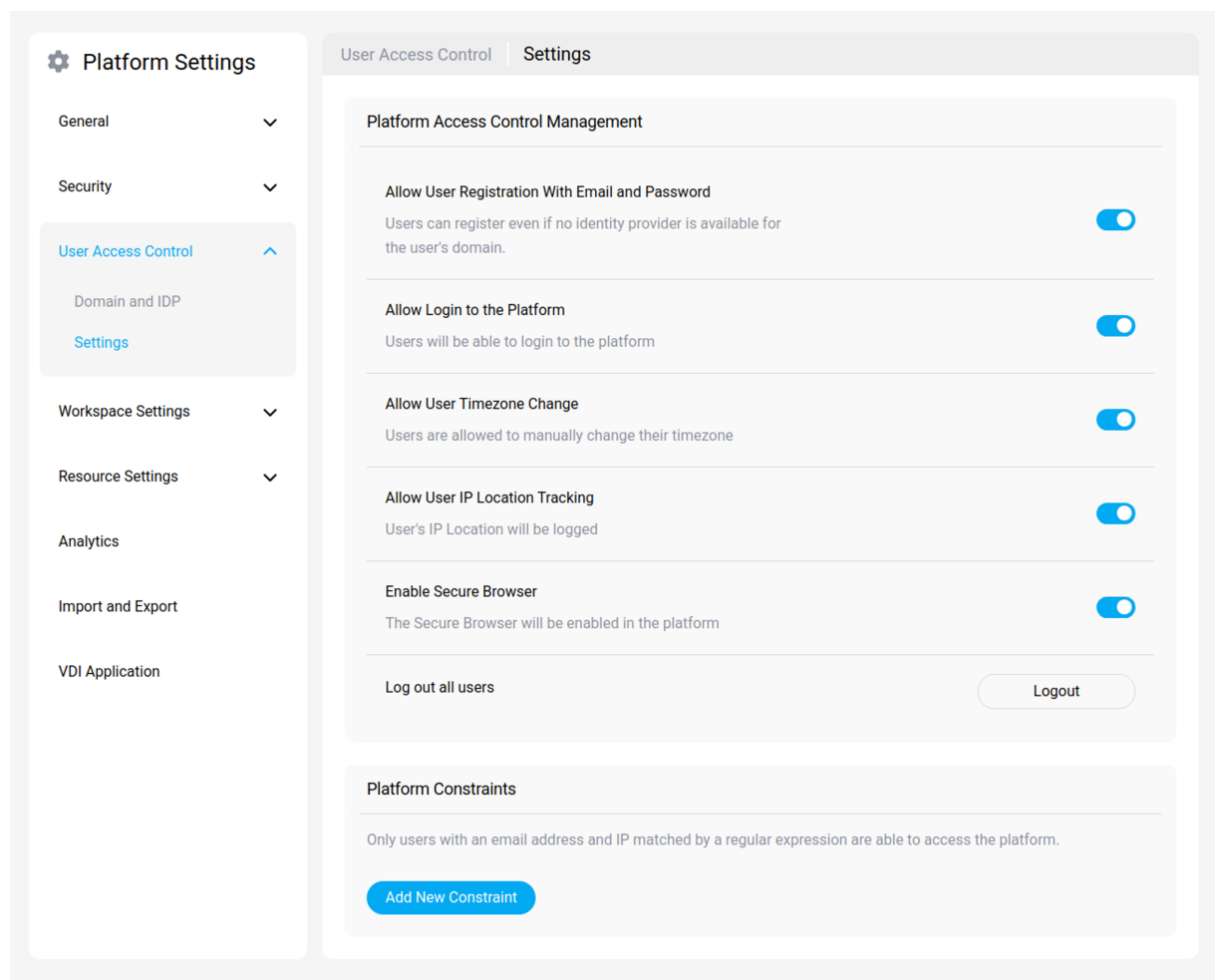
Domain and IDP

Register Domain

| DOMAIN NAME    | IDENTITY PROVIDER | EVERYONE | 2FA ENABLED | TENANT (OPTIONAL) | ACTIONS |
|----------------|-------------------|----------|-------------|-------------------|---------|
| strong.network | Google            | ✓        | ✗           | N/A               |         |
| sa.eert        | Microsoft Azure   | ✗        | ✓           | None              |         |
| trgwrg.ethwrth | Google            | ✗        | ✓           | N/A               |         |
| test.com       | Google            | ✗        | ✗           | N/A               |         |
| happycorp.info | Google            | ✗        | ✓           | N/A               |         |
| cloud.com      | Google            | ✓        | ✗           | N/A               |         |

User Access Control Settings

The **User Access Control Settings** section offers features essential for meeting compliance requirements. These features encompass *Platform Access Control Management* and *Platform constraints*.



## Workspace Settings

July 8, 2025

Define the rules and defaults that govern individual workspaces created within the platform. Configure workspace-specific **Security Settings** like clipboard control and SSH access, manage **Schedule Settings** for workspace uptime, set policies via **Workspace Apps Settings**, define allowed **Workspace Specification** options (CPU/RAM), control workspace **Network Policy**, and manage workspace-specific **Registry Access**.

- [Security Settings](#)
- [Schedule Settings](#)
- [Workspace Apps Settings](#)
- [Workspace Specification](#)
- [Network Policy](#)

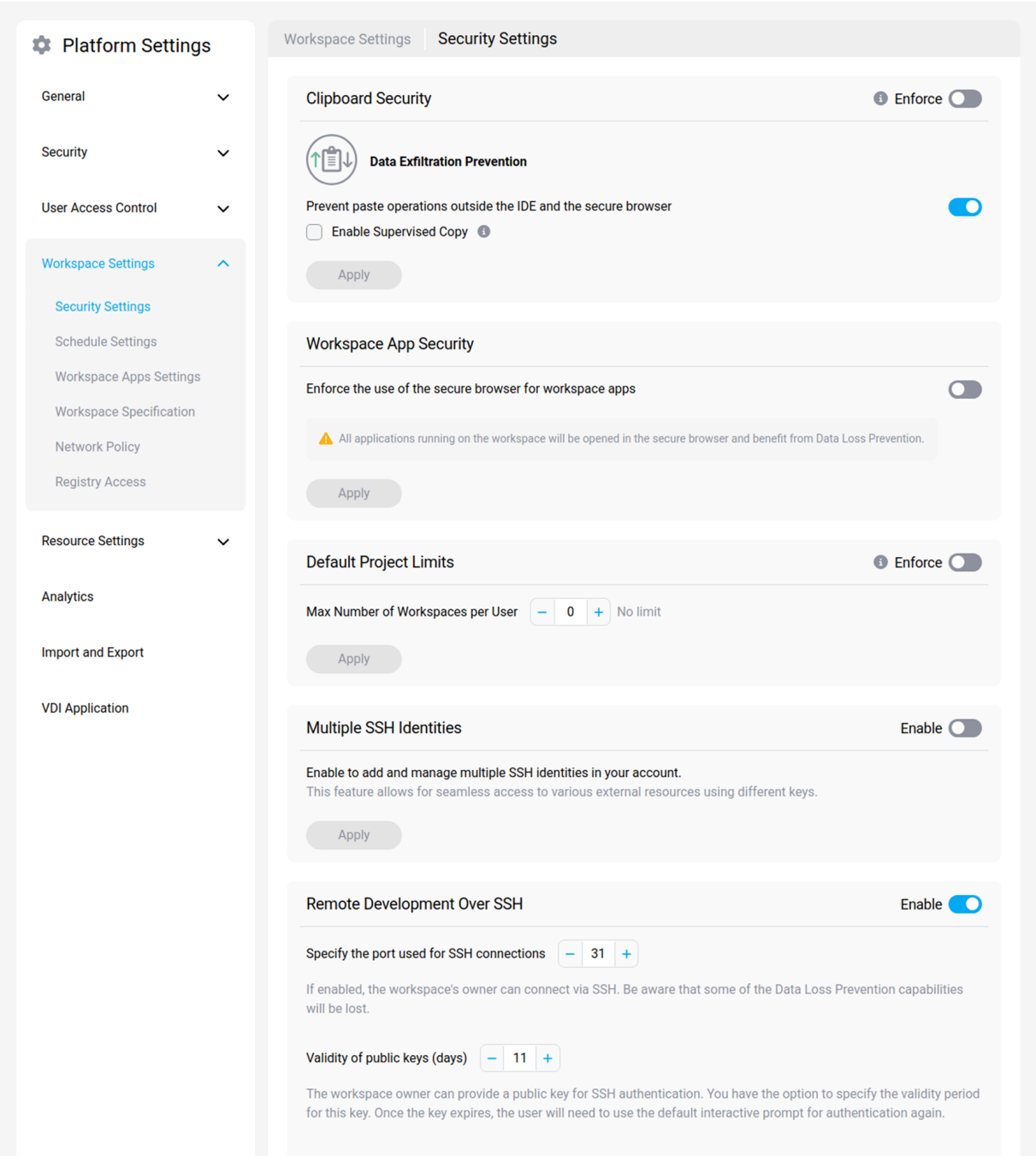
- [Registry Access](#)

## Security Settings

The **Security Settings** let you enforce security rules within underlying organizations and projects.

1. Clipboard Security: If enabled, users are prevented from pasting content outside of the IDE and the Secure Browser.
2. Personal Key Settings: If enabled, it permits workspace owners to use their personal OAuth tokens to authenticate with external repositories.
3. Default Project Limits: If enabled, it restricts users to a specified maximum number of workspaces, ensuring resource conservation.
4. Connect via SSH: If enabled, it grants the workspace's owner permission to connect via SSH. However, it's crucial to note that certain Data Loss Prevention functionalities might be compromised.





**Schedule Settings**

Configure automatic scheduling for workspaces, such as setting operational hours or defining auto-shutdown policies. This helps manage resource consumption and ensures workspaces are only running when needed.

**Platform Settings**

- General
- Security
- User Access Control
- Workspace Settings**
  - Security Settings
  - Schedule Settings**
  - Workspace Apps Settings
  - Workspace Specification
  - Network Policy
  - Registry Access
- Resource Settings
- Analytics
- Import and Export
- VDI Application

**Workspace Settings | Schedule Settings**

**Timeout Outside Schedule**

Select a timeout after which the workspace will be automatically paused when not in use and running outside of scheduled hours. You can remove specific timeout options, making those options unavailable to users.

- ☐ No timeout
- ☐ 15 minutes
- ☒ 30 minutes default
- ☐ 60 minutes
- ☐ 90 minutes
- ☐ 120 minutes

**Idle Timeout**

Select a timeout after which the workspace will be automatically paused when not in use, regardless of the schedule. You can remove specific timeout options, making those options unavailable to users.

- ☐ No timeout
- ☒ 1 hour default
- ☐ 2 hours
- ☐ 4 hours
- ☐ 8 hours
- ☐ 24 hours

**Allow Users to Change Timeouts** ☒

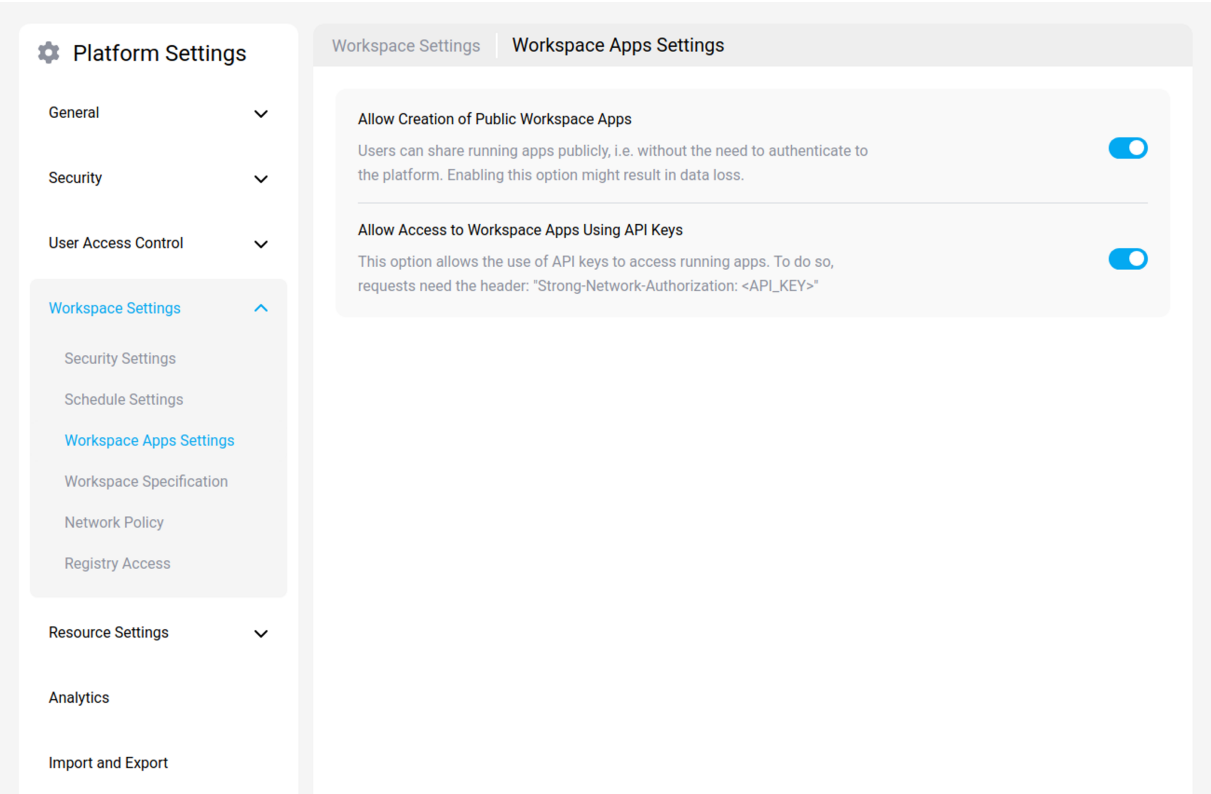
Users are allowed to set their own timeouts.

Apply

## Workspace Apps Settings

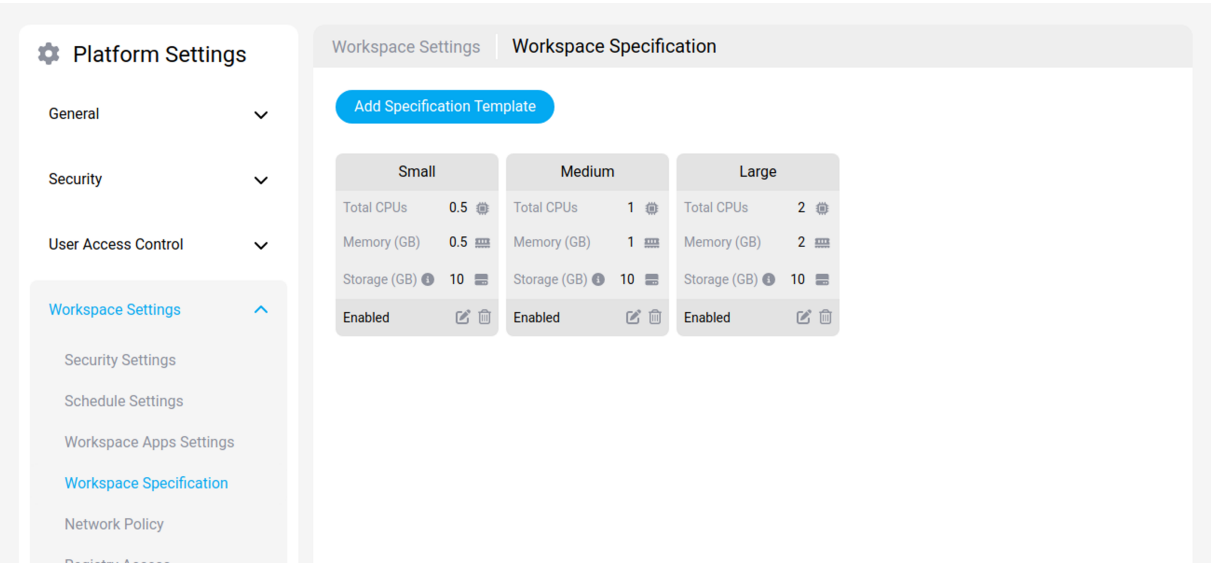
The **Workspace Apps Settings** section establishes guidelines for Workspace Apps within underlying organizations and projects.

- **Allow Creation of Public Workspace Apps:** This feature permits users to share active apps with the public, meaning there's no requirement for authentication to the platform. However, activating this option may lead to potential data loss.
- **Allow Access to Workspace Apps Using API Keys:** This option grants users the ability to utilize API keys for accessing active apps. When doing so, requests should include the header: "Strong-  
Network-Authorization: ".



Workspace Specification

The **Workspace Specification** section allows administrators to create predefined templates that define resource allocations for workspaces.



When creating a template, you can set both initial ‘request’ values and maximum ‘limit’ values for CPU, RAM, and storage. You can also customize template availability, restricting specific templates to cer-

tain organizations or projects. When users later create a new workspace, they will only see the templates applicable to their context.

Platform Settings

General

Security

User Access Control

Workspace Settings

Security Settings

Schedule Settings

Workspace Apps Settings

Workspace Specification

Network Policy

Registry Access

Resource Settings

Analytics

Import and Export

VDI Application

Workspace Settings

Workspace Specification

Enable or disable the workspace specification template

Specification Template Name

New Specs Template

Show the user the maximum number of CPUs and available memory

Total CPUs

Enter min and max CPUs

Request

0

Limit

Memory (GB)

Enter min and max memory

Request

0

Limit

Allow users to increase storage

Storage (GB)

Use the slider or enter min and max storage

Min

10

Max

100

Storage Type

default

Edit

Template Preview

Total CPUs

0

Memory (GB)

0

Storage (GB)

10

Select the organizations and projects where the workspace specification template should be displayed

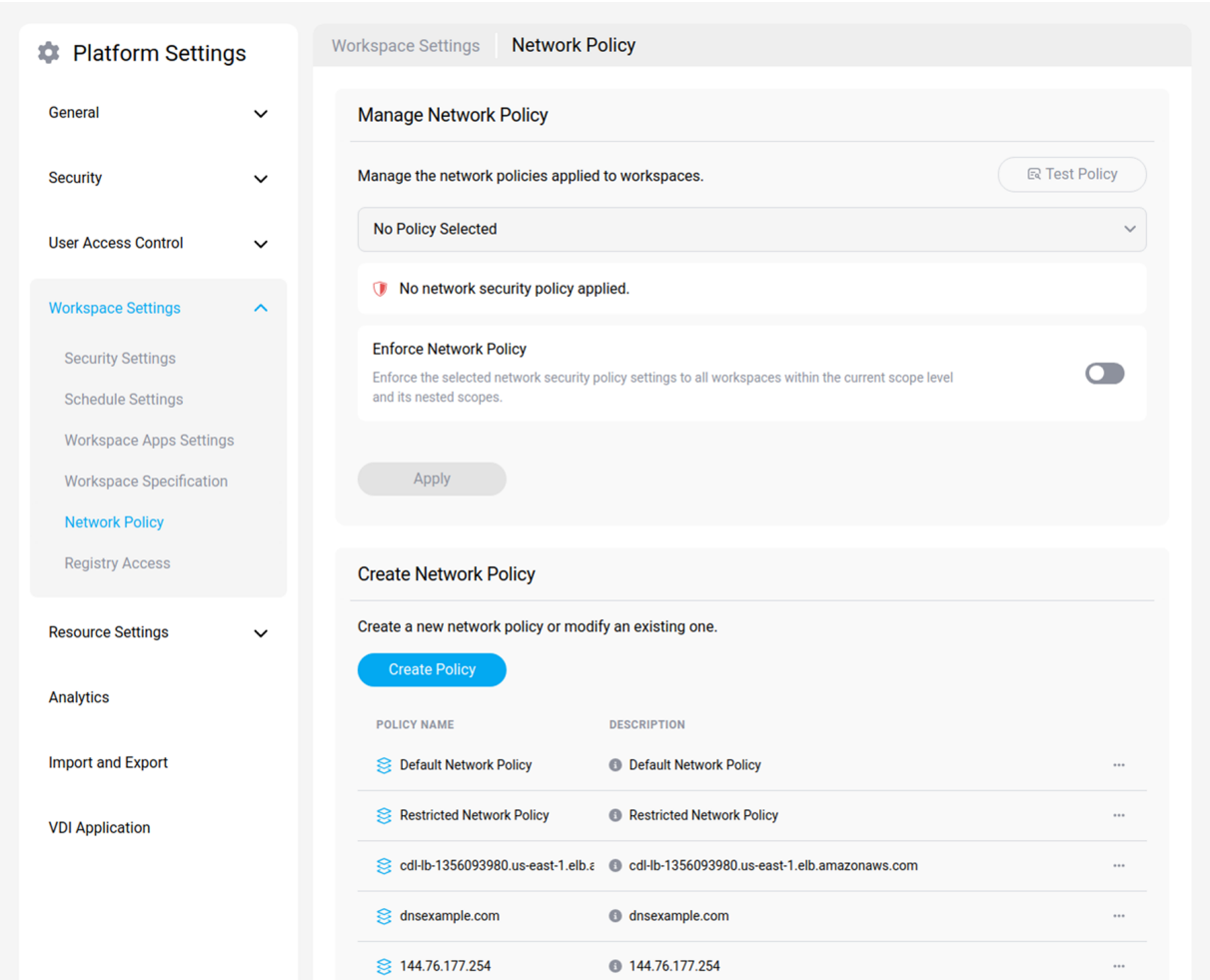
Customize

Add

Cancel

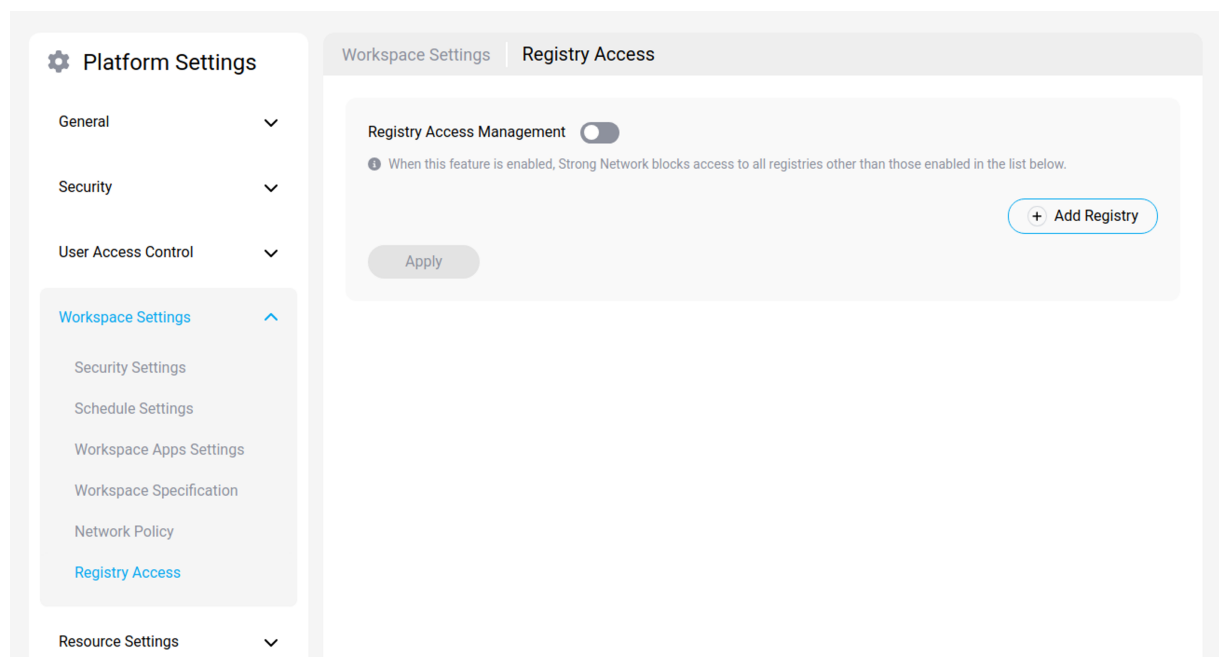
Network Policy

Define specific network policies that apply to workspaces created within the platform. This allows administrators to control network traffic flow, segment networks, and enforce security rules at the workspace level.



Registry Access

Manage and control which container image registries workspaces are allowed to pull images from. This enhances security by ensuring that only trusted and approved image sources are used within development environments.



## Resource Settings

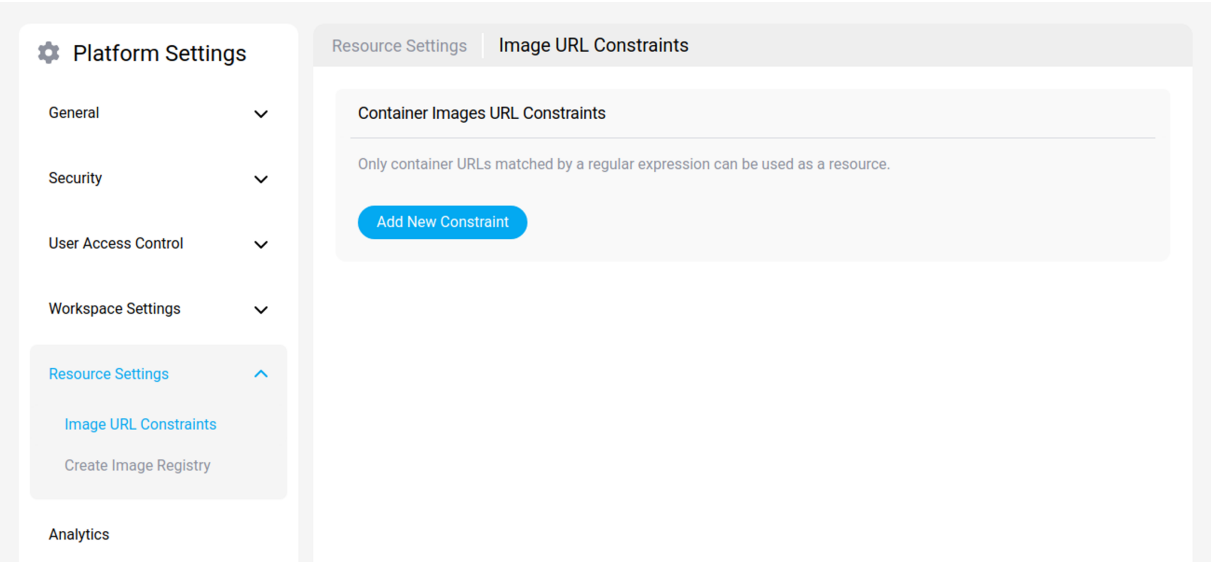
August 1, 2025

Control access to external resources used by the platform and workspaces. Primarily, this involves **Registry Access Management** (restricting allowed registries) and configuring connections to private registries via **Create Image Registry**.

- [Image URL Constraints](#)
- [Create Image Registry](#)

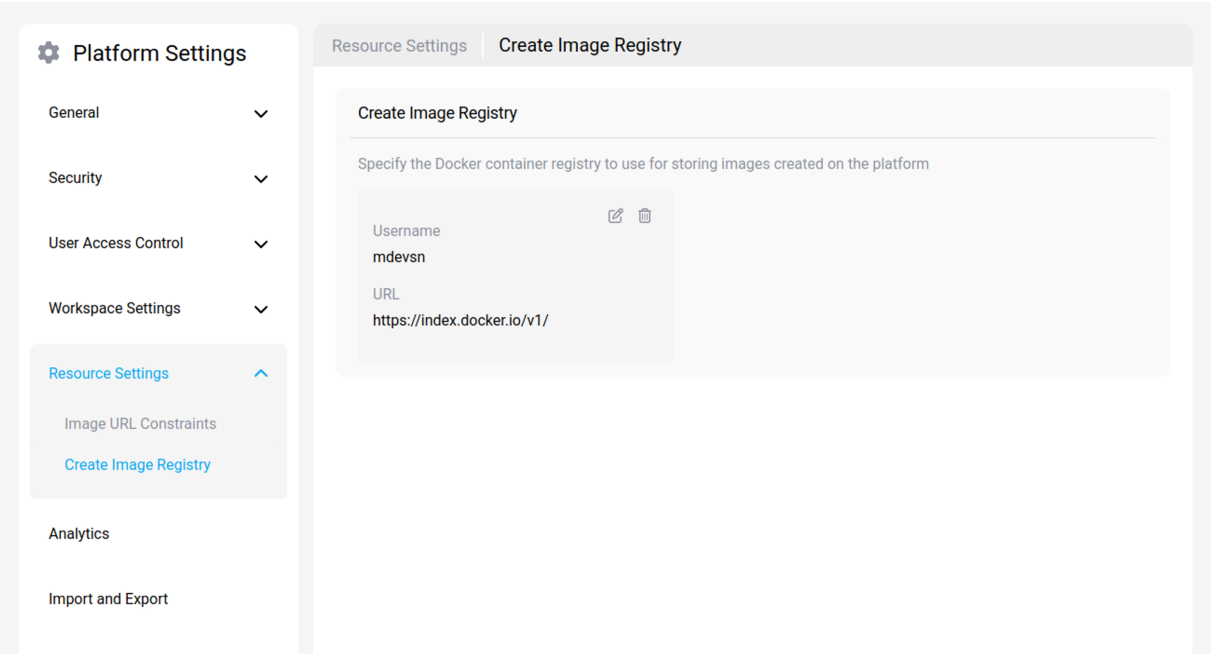
### Image URL Constraints

The **Image URL Constraints** section lets administrators ensure that their developers only access registries that are allowed. When this feature is enabled, Strong Network™ restricts access to all registries except those explicitly permitted in the list provided.



Create Image Registry

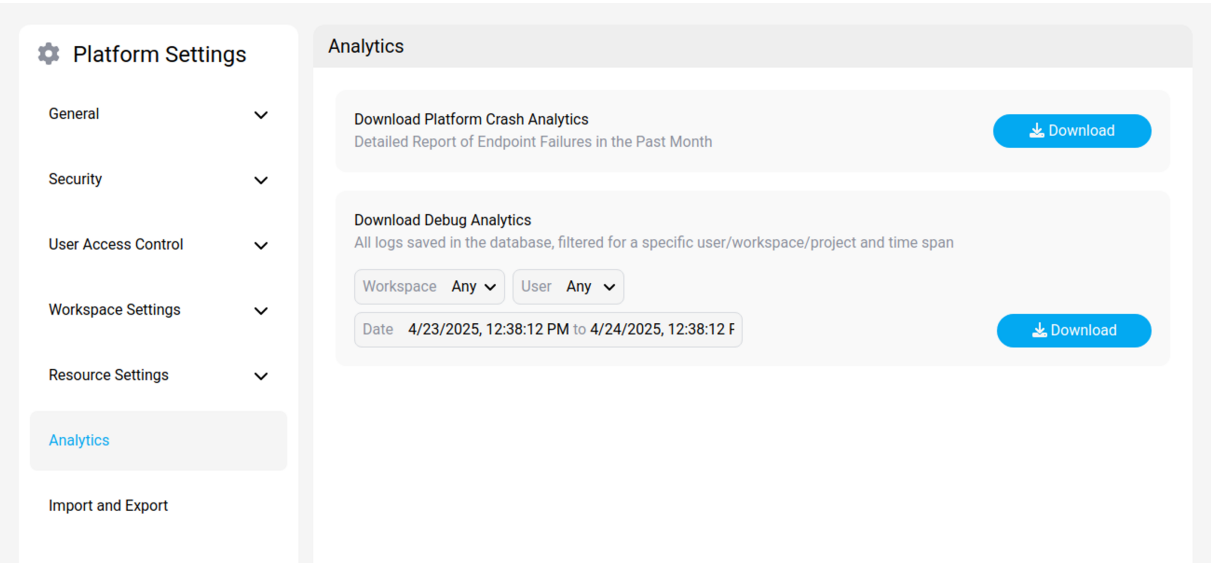
Configure and manage connections to private or custom container image registries. This section allows you to add new registry credentials and endpoints for use across the platform.



Analytics

July 8, 2025

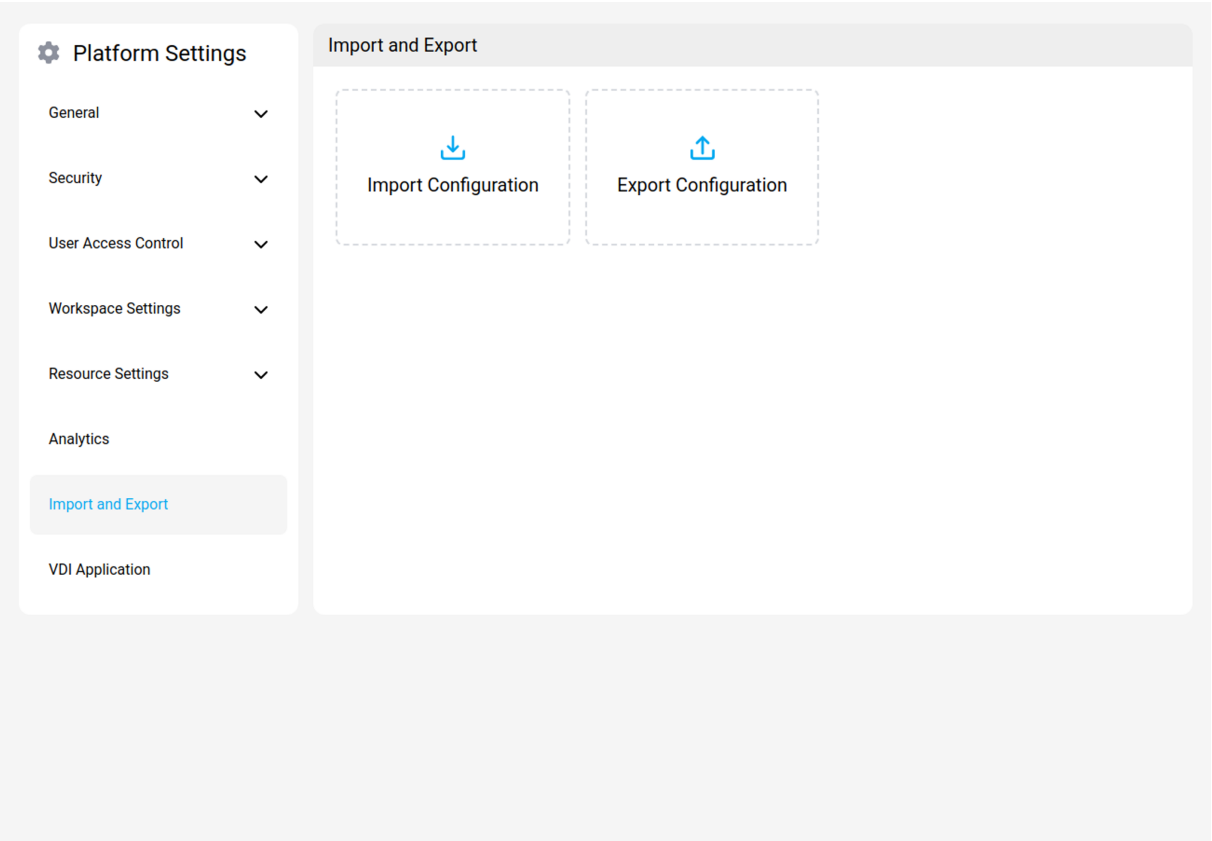
The **Analytics** section allows you to download crash analytics for the platform as a CSV file. This document offers detailed information about the recorded errors on the platform.



### Import and Export

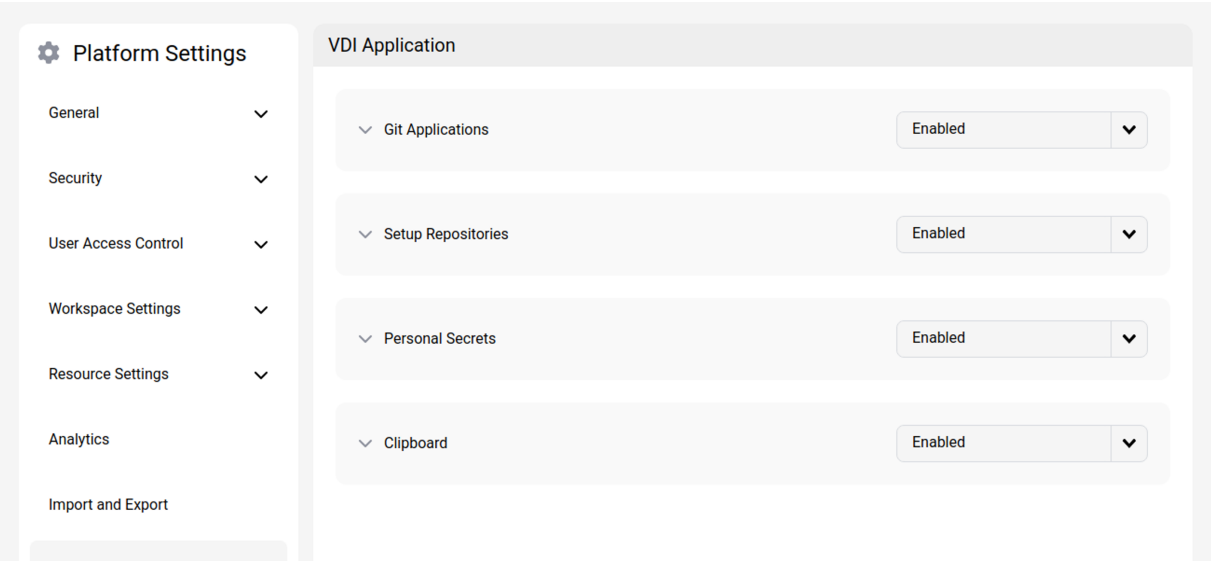
This section provides options for importing and exporting platform configurations or data. This can be useful for backups, migrations, or sharing settings between different platform instances.





**VDI Application**

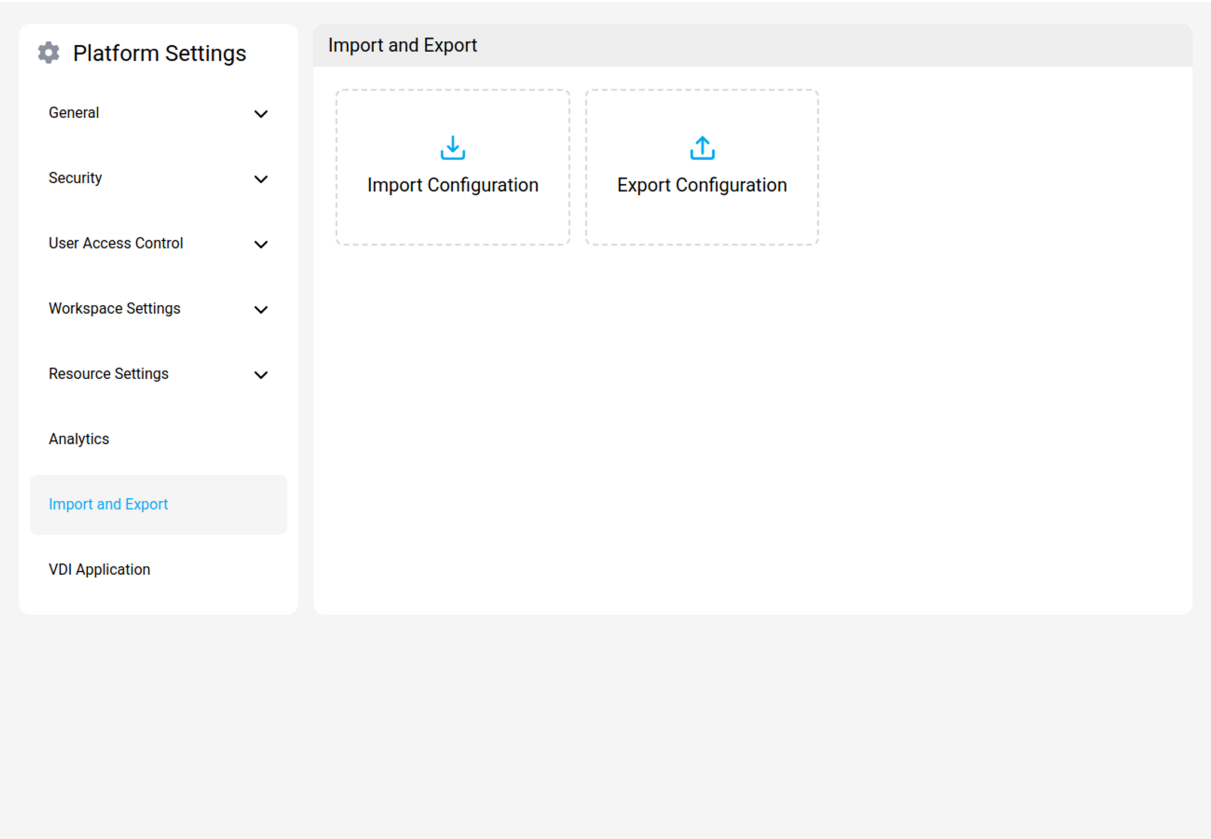
Configure settings related to Virtual Desktop Infrastructure (VDI) Agent accessible through the platform.



# Import and Export

August 1, 2025

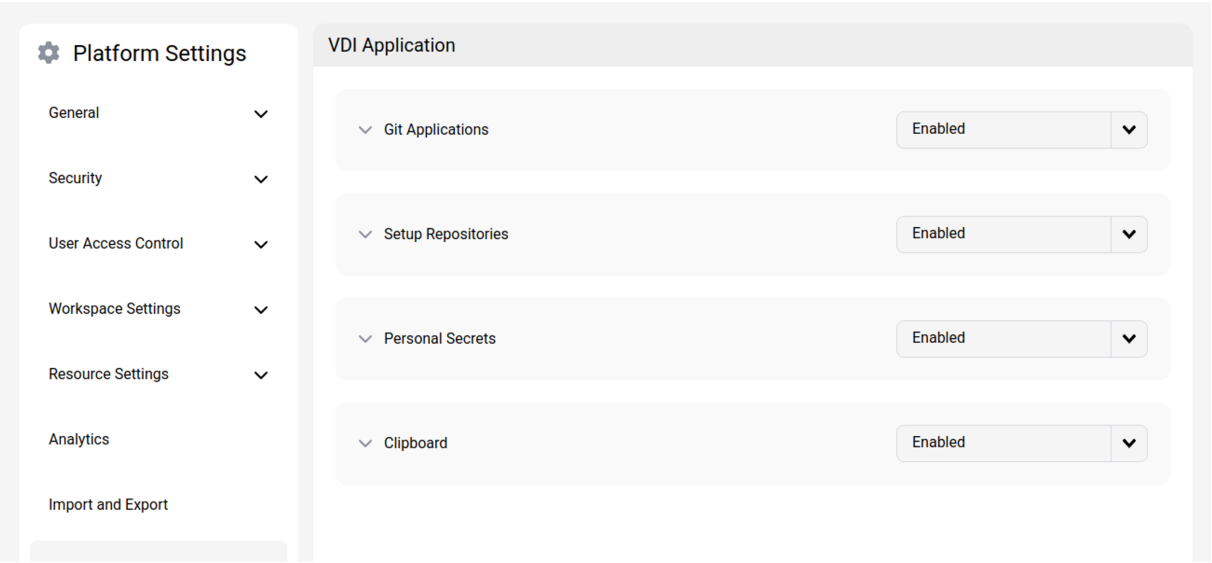
This section provides options for importing and exporting platform configurations or data. This can be useful for backups, migrations, or sharing settings between different platform instances.



# VDI Application

August 26, 2025

Configure settings related to Virtual Desktop Infrastructure (VDI) Agent accessible through the platform.

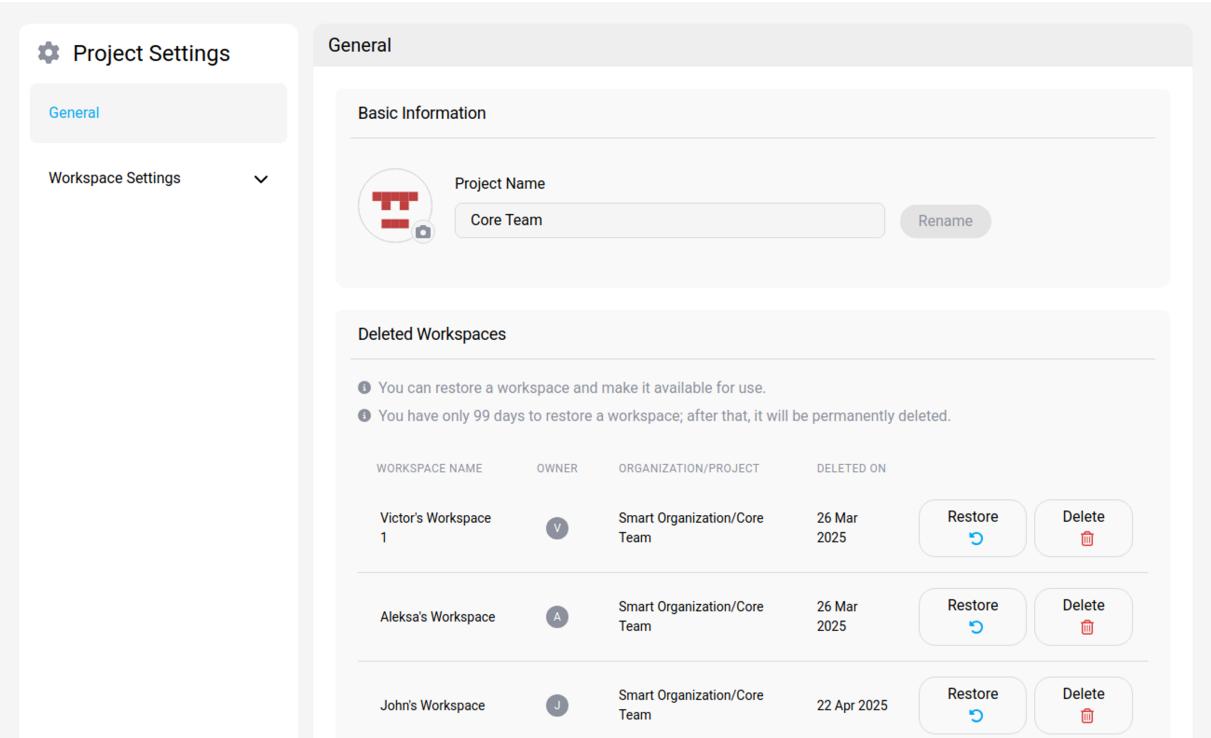


## Project General Settings

August 1, 2025

In the Project General Settings, you can update your project’s name within the Basic Information panel.

Additionally, workspaces that have been deleted can be restored within seven days of their deletion. After this period, they will be permanently deleted.



## Workspace Settings

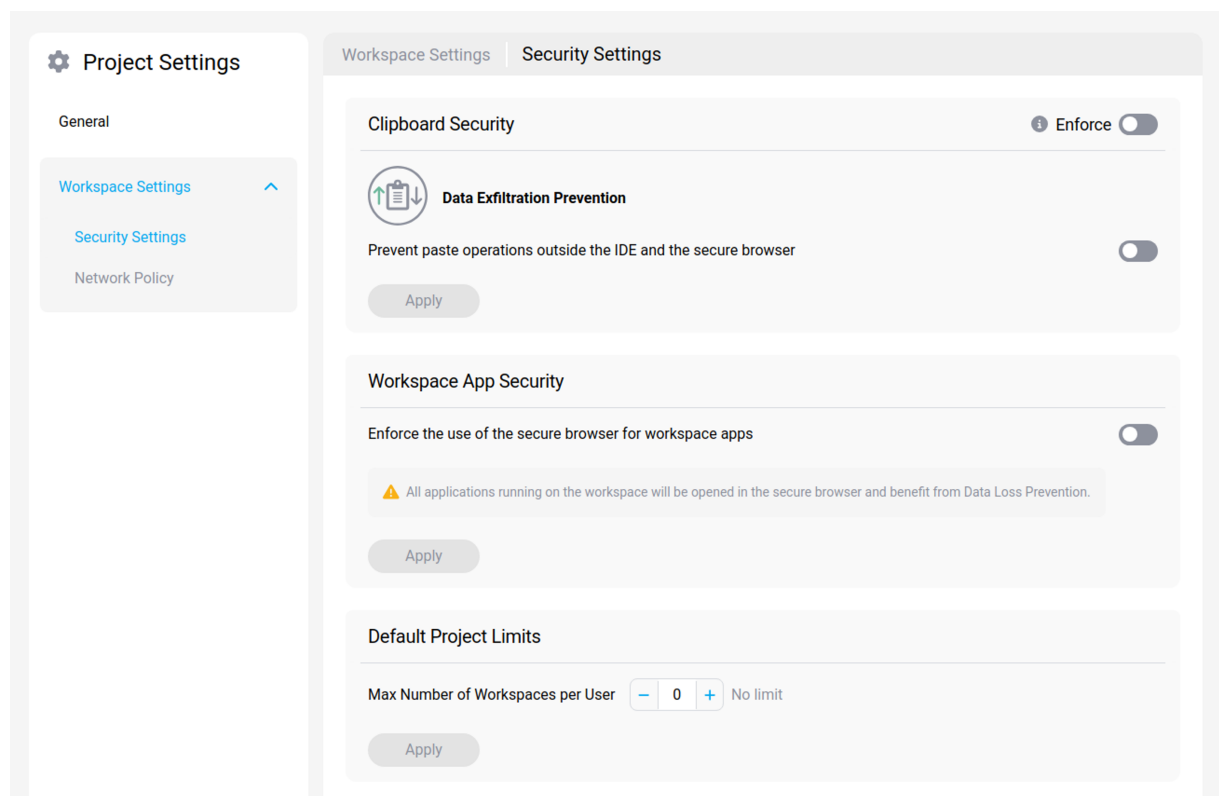
August 26, 2025

This section allows you to configure workspace settings specifically for this project. Define project-level security policies for data handling and access, and establish network policies to control workspace traffic within the context of this project.

- [Security Settings](#)
- [Network Policy](#)

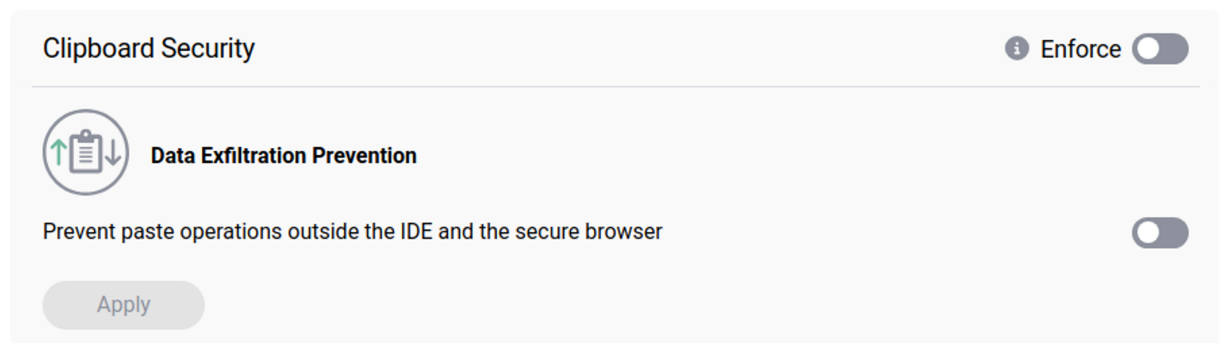
### Security Settings

In the “Workspace Settings” section, the “Security Settings” enable you to implement multiple policies including Clipboard Monitoring, Workspace App Security, and Default Project Limits. These policies can be enforced to establish a foundational level of security across all workspaces within your project.



## Clipboard Security

Clipboard Security implements Data Loss Prevention policies to safeguard against data leaks by disabling the ability to paste content from the IDE and secure browser into external applications.



## Workspace App Security

Workspace App Security allows you to mandate the use of a secure browser for workspace applications, ensuring that developers can share the applications they are developing in a protected environment. When used in conjunction with the Clipboard Security policy, this feature helps to prevent any potential data exfiltration from workspace applications.

### Workspace App Security

Enforce the use of the secure browser for workspace apps

All applications running on the workspace will be opened in the secure browser and benefit from Data Loss Prevention.

Apply

**Default Project Limits**

Default Project Limits can be set to cap the number of workspaces a user can create. This not only aids in resource monitoring and reduces unnecessary workspace proliferation but also contributes to cost efficiency by avoiding the operation of unused workspaces.

### Default Project Limits

Max Number of Workspaces per User

-

0

+

No limit

Apply

**Enable Remote Development Over SSH**

Remote Development Over SSH gives you the option to permit or deny developers the ability to connect to their workspaces via SSH. While convenient for certain tasks, this feature must be used judiciously as it can reduce the effectiveness of local IDE data loss prevention measures.

### Remote Development Over SSH

Enable

Set as Default

When creating a new workspace, SSH is part of the access toolset.

Update All Workspaces

Use this button to add SSH in the access toolkit to all workspaces in this project.

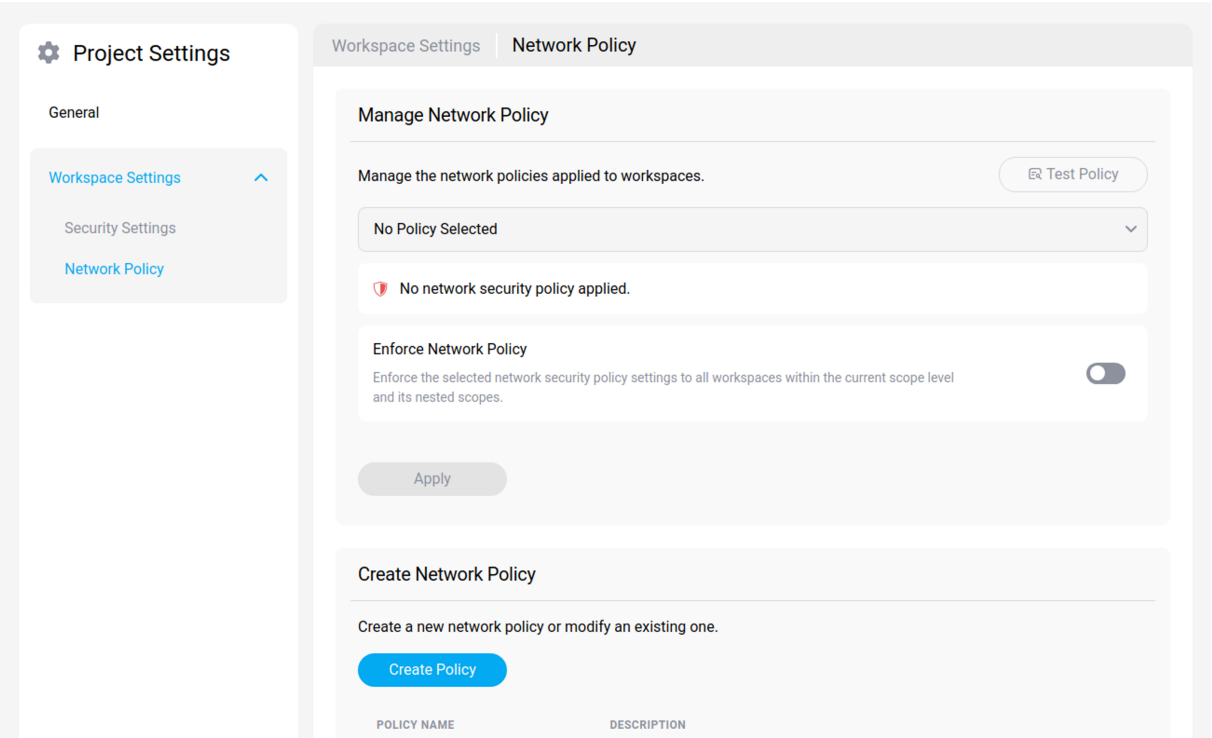
Update All

Data exfiltration prevention will be disabled on all workspaces.

Apply

## Network Policy

Network policies are attached to [workspace](#) and enable fine-grained network traffic control. Network traffic is identified using combinations of IP addresses, port and domain names. Once a network policy is attached to a workspace, all **out-bound** traffic is enforced by the rules in the policy and the workspace’s user cannot circumvent the restrictions.



## Default Network Policies

Three default policies are available in a project. An administrator can create a new Network Policy if needed.

| Name                   | Scope   | Description  |
|------------------------|---------|--|
| <b>Monitor Traffic</b> | Project | This is a standard policy to monitor the outgoing traffic to the workspace. It will cause the generation of log events in the Audit dashboard. |

| Name                    | Scope   | Description   |
|-------------------------|---------|---|
| <b>Restrict Traffic</b> | Project | This is a standard policy to restrict outgoing traffic from the workspace. It will block all traffic except to attached repositories and domains. Failed network requests are shown in the log events in the Audit dashboard. |

**Add a Network Policy**

You can create a Network Policy by pressing the “**Create Policy**”button.

Workspace Settings | Network Policy

Define Network Policy

Expert mode

Use the options below to define a network policy to assign to workspaces.

Policy Name \*

Description \*

Restrict Traffic to Selected Resources

Enabling this option, outbound traffic is restricted to authorized resources, e.g. Git repositories, connected services, etc. In addition, you may define a whitelist of domains and IP addresses

+ Add Domain

+ Add IP Address

Add Policy

Cancel

Test Policy

You will need to enter the following information:



1. **Name**, a name to identify the policy,
2. **Description**,

### Warning

Be careful when naming and describing a new policy. A misleading name can end up in giving too many permissions to a user.

1. **Log and record outbound network traffic** (default),
2. **Restrict Traffic to Selected Resources** (optional),  
All traffic will be restricted, except for end systems added to your **whitelist**

- Add each application that you want to whitelist
- Add Domains that you want to whitelist, and indicate whether to include subdomains
- Add IPs that you want to whitelist

## Edit or Delete a Network Policy

You can edit or delete a Network Policy by clicking on the “...” icon next to its class level.

## Help

In the help section, you can find the resources you need to make the most of the platform. Whether you're a beginner or an advanced user and find the documentation unhelpful, there are alternative options to get help.

- You can use the [troubleshooting](#) tool in case you experience problems.

## REST API

August 1, 2025

The Strong Network™ platform can be fully controlled and integrated via an API of over 150 endpoints (detailed on the platform's API page) for complete control of enterprise applications and integration with security and analytics tools such as Splunk, Sumologic, etc.

Info:

Only users authenticated on the Strong Network Platform can have access to the API documentation.

Strong Network REST API

1.0 OAS 2.0

The Strong Network REST API exposes endpoints to manage platform resources.

Authorize

Strong Network REST API

Platform Metrics

GET

/v1/metrics/k8s-current

Retrieve current k8s usage and availability

GET

/v1/metrics/workspace-metrics

Retrieve a list of workspace usage for the entire platform.

GET

/v1/metrics/workspace-utilizations

Retrieve a list of workspace utilization for the entire platform.

Configuration

POST

/v1/platform/add\_agreement\_document

Add Agreement Document to platform

POST

/v1/platform/add\_region

Add new region to platform

POST

/v1/platform/add\_security\_officer

Add Security Officer to platform

GET

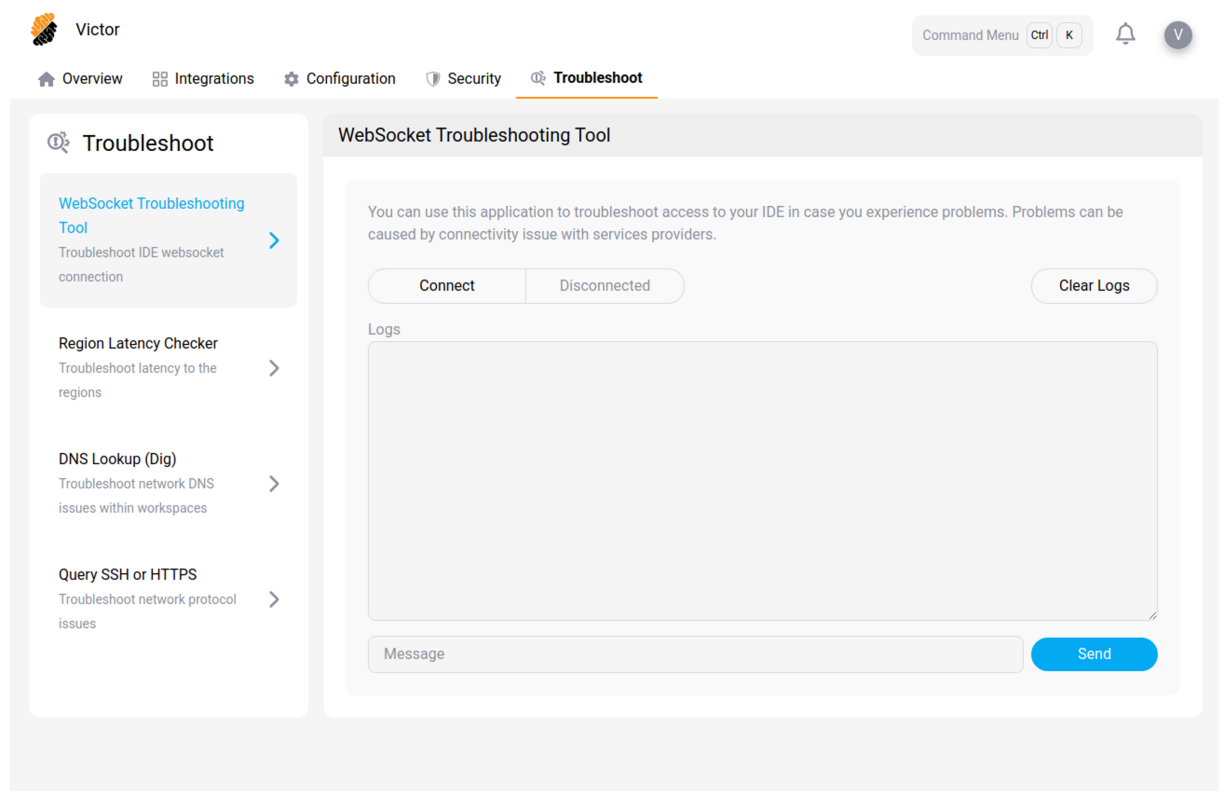
/v1/platform/agreement\_documents

Get all agreement documents

## IDE Troubleshooting Tool

August 26, 2025

In the [Profile Settings](#) you can setup the IDE WebSocket Troubleshooting Tool. You can use this application to troubleshoot access to your IDE in case you experience problems. Problems can be caused by connectivity issues with service providers.



You can also troubleshoot latency to regions with the **Region Latency Checker** tool.



© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at <https://www.cloud.com/legal>. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (<https://www.cloud.com/legal>) for more information.