

Security

help.fractal.com/hc/en-us/articles/25054283385613-Security

It is an add-on where certain parameters for user access to the platform can be configured and established, as well as obtaining the connection keys for the APIs.

The image shows two screenshots of the Fractal platform interface. The top screenshot is the 'Dashboard' page, which displays various metrics and charts. The bottom screenshot is the 'Settings' page, specifically the 'Security' tab, which allows users to configure login and password settings.

Dashboard Metrics:

- WOs in Process: 37
- WOs in Review: 14
- Closed WOs: 45
- Pending Tasks with Delay: 19
- Scheduled vs. Unplanned Tasks: 38.8% (Planned Tasks), 61.2% (Unplanned Tasks)
- Compliance Percentage: 46.9% (Closed WOs)
- Failures that Caused Damage: 2
- Currently stopped assets: 139
- Planned downtimes: 16
- Unplanned downtimes: 12

Work Orders Chart:

Category	Value
WO's C...	96
Finished...	10
Pending ...	10

Work Requests Chart:

Category	Value
Created	32
Solved	9

Settings - Security Tab:

- Login and password settings:**
 - Minimum password length: 6
 - Frequency in months for password change: 3
 - Number of unsuccessful login attempts before blocking account: 5
 - ☐ Must contain special characters
- Change Password:**
 - To continue please enter your password
 - Password field
 - Continue button

These tabs make up the parameters and configurations:

- Password
- Two-step authentication
- API connection
- SSO

Password

In this tab you can establish the configuration of passwords for access and starting a session on the platform with these parameters:

- Minimum password length
- Frequency in months for password change
- Number of unsuccessful login attempts before blocking account
- Must contain special characters

Settings

Activación Fractal - Español - 477

Save

General

User Accounts

Business Calendar

Modules

Financial

Auxiliary Catalogs

Document Management

Transactions Log

Security

API Connections

Guest Portal

Account

Password

Two step authentication

SAML 2.0

Login and password settings

Minimum password length

6

Frequency in months for password change

3

Number of unsuccessful login attempts before blocking account

5

☐ Must contain special characters

Change Password

To continue please enter your password

Password

Continue

Note: The above options depend on the type of plan or add-ons that have been contracted. There is also an addition that allows users to update the passwords on the platform.

Settings

Activación Fractal - Español - 477

Save

General

User Accounts

Business Calendar

Modules

Financial

Auxiliary Catalogs

Document Management

Transactions Log

Security

API Connections

Guest Portal

Account

Password

Two step authentication

SAML 2.0

Login and password settings

Minimum password length

6

Frequency in months for password change

3

Number of unsuccessful login attempts before blocking account

5

☐ Must contain special characters

Change Password

To continue please enter your password

Password

Continue

Two-step authentication

In this tab you can establish a two-step configuration with a QR code reading that can be verified with applications like Google Authenticator, Microsoft Authenticator or Authy from a smartphone. This way you'll have an extra level of security for accessing the platform.

Settings

Activación Fractal - Español - 477

Save

General

User Accounts

Business Calendar

Modules

Financial

Auxiliary Catalogs

Document Management

Transactions Log

Security

API Connections

Guest Portal

Account

Password

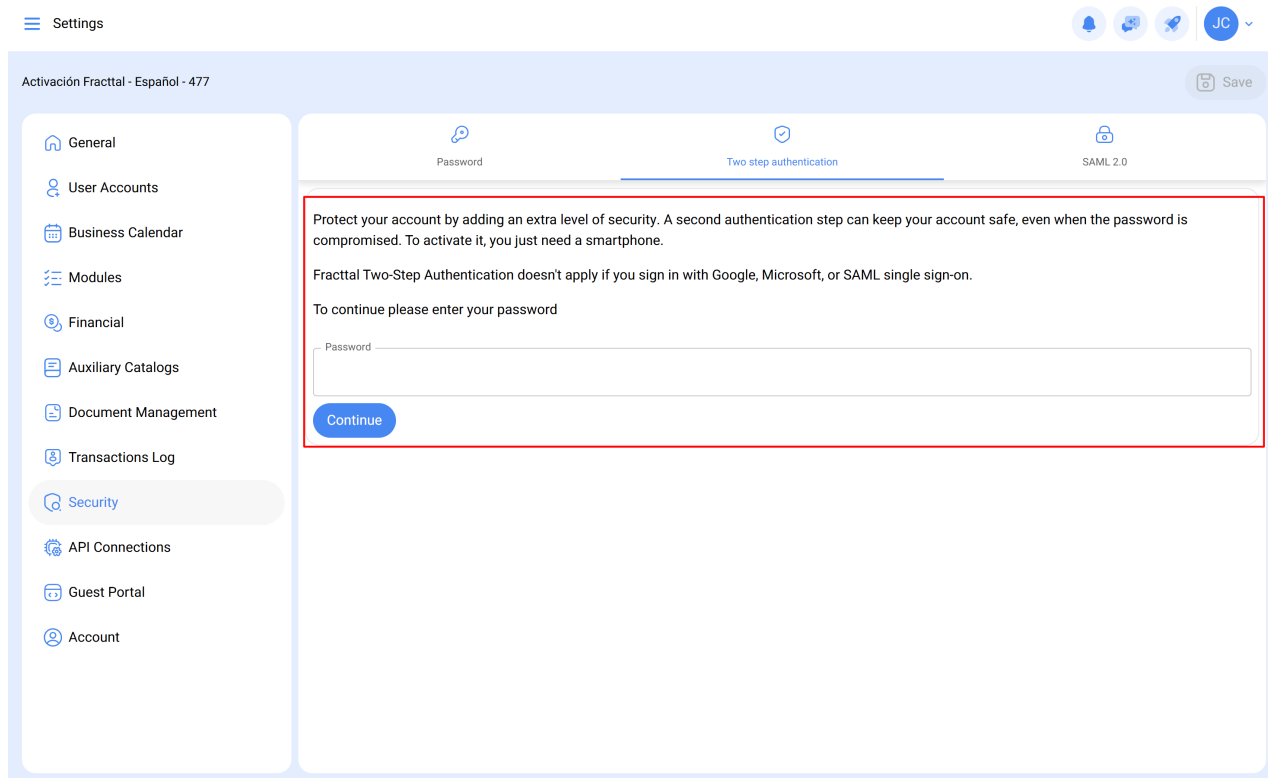
Two step authentication

SAML 2.0

Protect your account by adding an extra level of security. A second authentication step can keep your account safe, even when the password is compromised. To activate it, you just need a smartphone.

Fractal Two-Step Authentication doesn't apply if you sign in with Google, Microsoft, or SAML single sign-on.

Enable two step authentication



When you enter your access password, the following instructions with the QR code will be displayed:

- 1. Install a verification app on your phone**

You will need to use a verification app such as Google Authenticator, Microsoft Authenticator, or Authy.

- 2. Scan the QR code with your app**

- 3. Enter the 6-digit code generated**

Once the code is entered, we will remember your phone so you can use it every time you sign in.

SSO

In this tab you can establish parameters for authenticating access to the platform by means different from those predetermined (Google or Microsoft accounts).

Settings

Activación Fractal - Español - 477

Save

General

User Accounts

Business Calendar

Modules

Financial

Auxiliary Catalogs

Document Management

Transactions Log

Security

API Connections

Guest Portal

Account

Password

Two step authentication

SAML 2.0

SAML Connection

Configure Fractal as a SAML Service Provider and delegate your users' authentication to an external Identity Provider, such as Azure Active Directory, Okta, Auth0, among others.
Before proceeding, make sure you have already set up your Identity Provider. If you need more information on how to configure SAML in Fractal, check our documentation [here](#)

Connection name

Sign in URL

This is a logical identifier for the connection. Try to use a text that clearly identifies your company, as it must be unique across all companies using Fractal.

It corresponds to the SingleSignOnService of the Identity Provider.

Issuer

Single Logout URL

It corresponds to the EntityID of the identity provider.

It corresponds to the SingleLogoutService of the Identity Provider.

Certificate

SAML (Security Assertion Markup Language), is a standard that allows the exchange of information for starting a session (authentication and authorization) or SSO between different parts (applications). The participants in this authentication are the identity provider and the service provider. The service provider is the entity that gives a user permission to access a resource.

Fractal acts as the service provider. The identity provider is the entity that provides the infrastructure necessary for user authentication. In this case, the identity provider is the application that is registered with users and that controls their access. Some examples of applications that can be identity providers are Active Directory and Okta, among others.

Authentication SSO