



Jedox Cloud Console

You can use the [Jedox Cloud Console](#) to administer your Jedox Cloud instances.

Connection to Cloud Console

After your registration, you will receive an email with a link to activate your personal Cloud instance. Follow the link to login with your email and your password.

After logging in, you will be presented with the Jedox Cloud Console. The numbered sections are described below the screenshot.

jedox.

jedox. CLOUD CONSOLE
2

Instances
1
jedox Logs
Open Instance

Statistics

CPU Usage
0.01 %

Memory Usage
1 GB

Storage Usage
21 GB / 512 GB

Snapshot Usage
658 MB / 512 GB

Uptime Report [↓](#)

CPU usage over time (Local time)

Services

	Version	Status	RAM	CPU	
In-Memory DB	20.1.5.10x97.7	Active	295.78 MB	0m	Stop Restart
Spreadsheet Server	20.1.0.10014.16	Active	46.31 MB	0m	Stop Restart
Web Frontend	20.1.0.23989.406	Active	51.29 MB	0m	Restart
Web Backend	20.1.0.23992.408	Active	212.11 MB	1m	Stop Restart
Integrator	20.1.0.9229.12	Active	553.79 MB	5m	Stop Restart

Connection

Host: `efap-...@cloud.jedox.com` [Copy excel connection details to clipboard](#)

Description: [Save](#)

Port:

Username:

Password:

PEM SFTP Access Key: [Get access key](#)

PPK SFTP Access Key: [Get access key](#)

Due to Google's new policy on Trusted CA, all jedox Cloud instances will have their certificates updated. For more details regarding Google's Distrust of the Symantec PKI, you can click [here](#)
 Since jedox Cloud instances will use new certificates, all jedox Excel Add-in users will have to update their client.pem file, located at jedox install Path\roadmin\cert or follow the steps from here to add the new SSL Certificate.
 Download your Excel Add-in Certificate: [Excel Add-in Certificate](#)

Snapshot

Maintenance time: [▼](#)

Date	Name	Size	
20.03.2020	daily_backup_5.tar.gz	131.68 MB	📄
21.03.2020	daily_backup_4.tar.gz	131.68 MB	📄
22.03.2020	daily_backup_3.tar.gz	131.68 MB	📄
22.03.2020	daily_backup_2.tar.gz	131.68 MB	📄
23.03.2020	daily_backup_1.tar.gz	131.68 MB	📄

Jedox

- [Knowledge Base](#)
- [Training and Tutorials](#)
- [Support Portal](#)
- [Download Center](#)

Copyright © Jedox AG



1 - Instance

Select the instance you want to manage from the drop-down menu. Most accounts come with multiple instances. The drop-down menu will display all available instances, their names, and the version of Jedox running on them.

2 - Account Settings

Here you can adjust your name, email, and password for the Jedox Cloud Console.

3 - Statistics

Displays real-time information about CPU, storage, and snapshot usage, including CPU usage graph. **Uptime report** allows you to download availability reports for the current and previous two months. The reports are downloaded in .csv format as a zip file.

4 - Services

Controls status of each service individually by providing buttons to stop/start/restart/kill (force stop) each service individually. Please note that Web Frontend can only be restarted.

5 - Connection

Displays information relevant for connecting to the instance from a remote Excel Add-in front end. This section also contains a field for the

Security Token, which is necessary for [connections from Excel Add-in to the Cloud](#).

6 – Snapshots

Here you can define a time slot for instance-maintenance time by picking the hour (in UTC) at which regular maintenance will be performed. Furthermore, this section provides a list of the last 5 snapshots, including download functionality. Snapshots contain all the instance data (database, reports, log files, etc.).

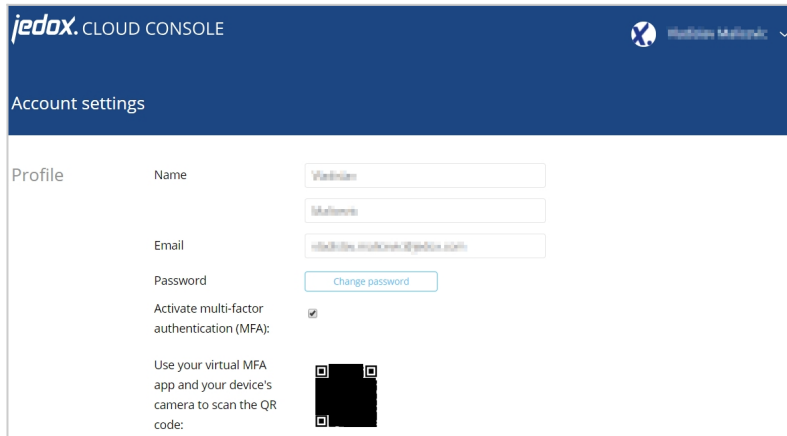
7 – Jedox

Displays help information and links.

Enabling multi-factor authentication

Your cloud console now allows you to enable multi-factor authentication. To enable it, follow these steps:

1. Log in to your [cloud console](#).
2. Go to **Account Settings**. A QR code is displayed.



jedox. CLOUD CONSOLE Malaysia

Account settings

Profile


Name:

Email:

Password: [Change password](#)

Activate multi-factor authentication (MFA):

Use your virtual MFA app and your device's camera to scan the QR code:



3. Enable the **Activate multi-factor authentication** option.
4. Scan the QR code using the camera of your device and your virtual MFA application (e.g. Microsoft Authenticator).

Once the multi-factor authentication is enabled, you will be prompted to input the authentication token in addition to your password on your login screen.