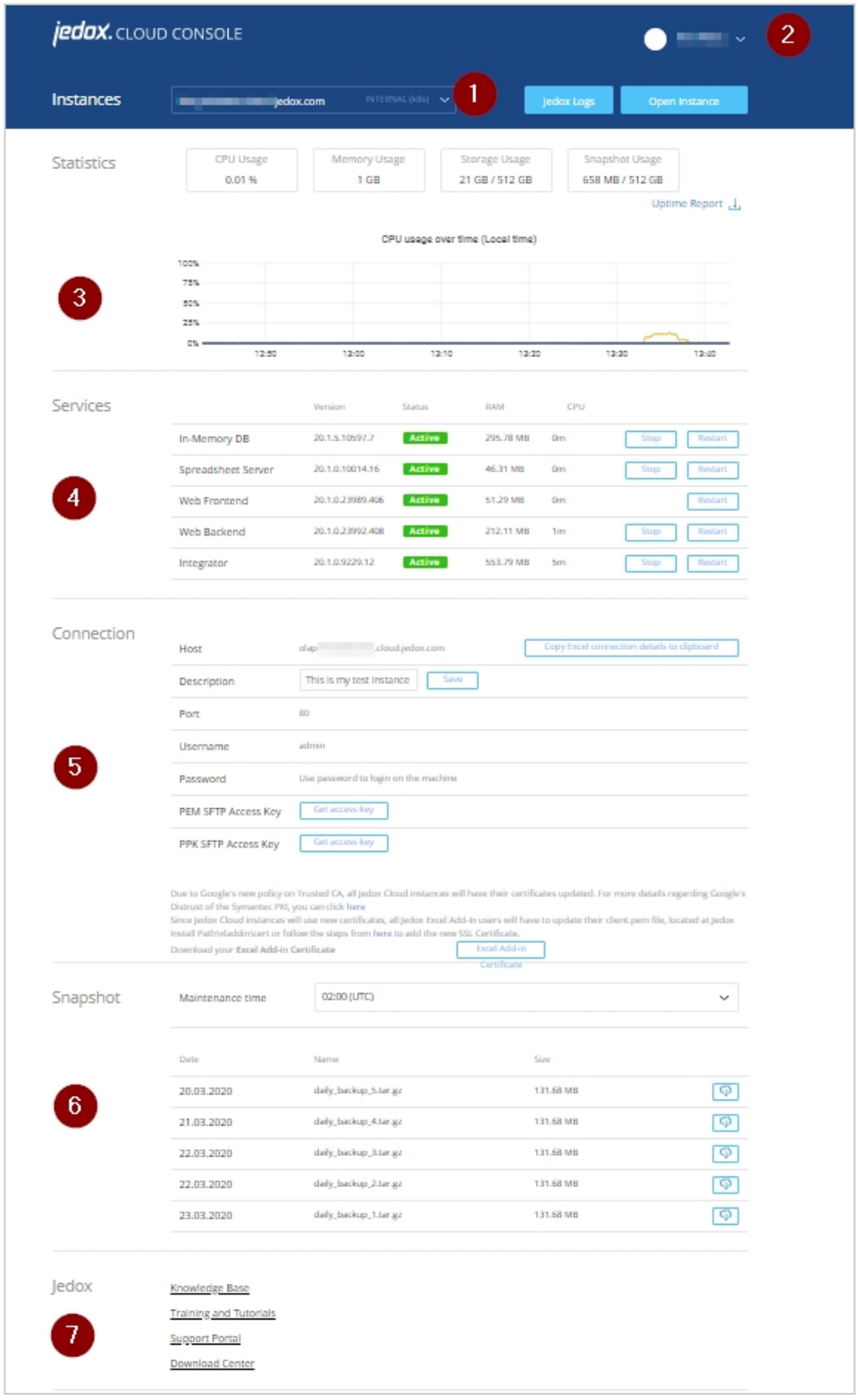
Jedox Cloud Console

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.



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.).

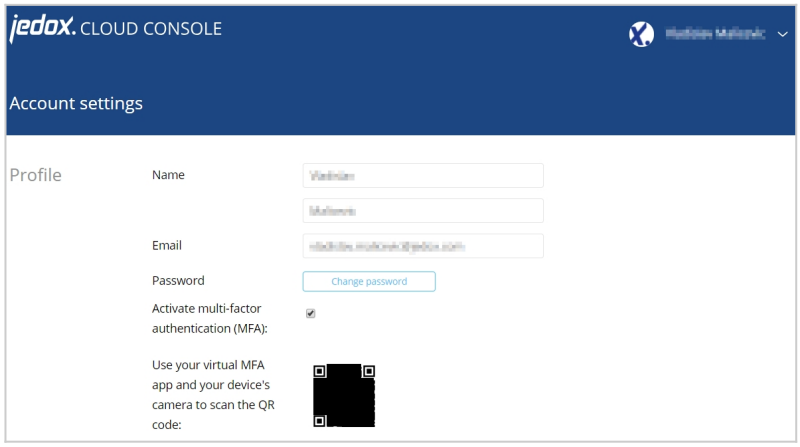
7 – Jedox

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.



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.