

### Minimum system requirements for on premise installation

Microsoft Windows 10

Microsoft Windows Server 2016 or later

1 core CPU

8 GB RAM

100 GB available disk space

Internet connection, TCP inbound and outbound connections on port 443

Note that a remote connection is required for initial setup and installation

In order to complete the installation of WaterNet Advisor, DHI will require access to the PC in which the software will be hosted on. We can do this via a remote desktop connection or by the Team Viewer software (free download). Approximately 1,500 MB of data will be downloaded onto the selected PC, and the download and configuration will take approximately 2-3 hours, this can all be done by DHI to make the process as smooth as possible. The following is a list of the technical aspects of the installation.

### Software configuration requirements

TCP inbound and outbound connections on port 443

*SMTP server configuration (optional)*

Administrator account

TeamViewer, AnyDesk, or VPN connection with a remote desktop, or a client's administrator assisted installation.

### Software which will be installed and actions which will be performed during deployment

.NET Framework 4.7.2

Visual C++ redistributed package Studio 2015

PostgreSQL 15.2-1 64bit on port 5432

Postgis 3.3.2-2

JDK 21

Install Native JAI libraries

Install and configure Apache Tomcat 9.0.82 on port 8080

Install and configure Geoserver 2.23.2 (instance package with our data)

Install and configure Windows IIS with ASP.NET 4.0 on port 80/443

Install the WCF Windows service

Deploy backend (Web API) package

Deploy frontend (UI) package

Deploy simulation runner

Install DHI License manager

Install and configure WNA updater

Install Chrome x64 bit

Configure the user account using installer account and disable the installer account

### **Data access security**

Hosting arranged by DHI is provided by Microsoft Azure cloud computing service. A separate (private) VM instance is acquired for each WaterNet Advisor installation i.e., the space is not shared with other customers. A secure HTTPS protocol over which the data is sent between your browser and the website that you are connected to is part of the installation.

Alternatively, we will install WaterNet Advisor application into your own Microsoft Azure account. Hosting arranged by a customer i.e., on-premise installation is entirely within the responsibility of a customer and it will adhere to the respective IT standards.

The following security settings can be enforced in Microsoft Azure installations:

- Install endpoint protection solution on virtual machines
- Install monitoring agent on your virtual machines
- Apply disk encryption on your virtual machines
- Add a web application firewall
- Install a vulnerability assessment solution on your virtual machines
- Resolve monitoring agent health issues on your machines
- WaterNet Advisor should only be accessible over HTTPS
- Function App should only be accessible over HTTPS
- Configure IP restrictions for WaterNet Advisor
- CORS should not allow every resource to access WaterNet Advisor
- Web Sockets should be disabled for WaterNet Advisor

The secure access to WaterNet Advisor application is ensured by these steps:

- Application runs on a machine with its own network and firewall
- Application runs on a machine where Windows firewall is enabled
- Application runs on a machine with updated operated system
- Application runs on a machine where strong password policy is applied
- Two-level authentication is enforced

### **Web browser**

It is recommended to use the latest version of your Web browser such as Edge, Firefox, Chrome, or Safari. Please note that Microsoft Internet Explorer does not longer support all WaterNet Advisor features.

### **Windows password change**

Please note that changes to the password on the machine and user profile where the application is running would prevent WaterNet application from running until corresponding adjustments to the IIS and Windows services are made.

### **Antivirus program**

Please note that that when the application automatic update is enabled it might be necessary to add an exception into the virus checking program and to allow the “auto updater” to run autonomously.