PORT-IT

Safely connected at sea.

Vanir Installation

0 Before installing Vanir:

NOTE: Before installing Vanir, please remove any other antivirus or endpoint security software or any older versions of an ESET NOD32 installation.

Please use the Windows Control Panel -> Add remove programs to remove the software.

Also make sure the following is in order:
• The communication PC has a static IP address on the vessel network

• **Windows 7 SP1 is installed or higher.**

• The user has administrator rights during installation.

• The setup process can take some time, you will not be able to use the PC for normal operations during this procedure

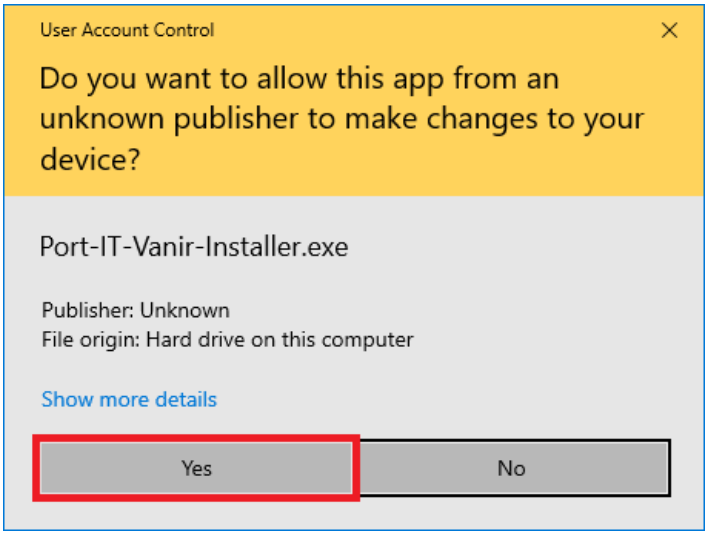
• Make sure all work has been saved and that all programs have been closed.

1 Generic Installation Vanir:

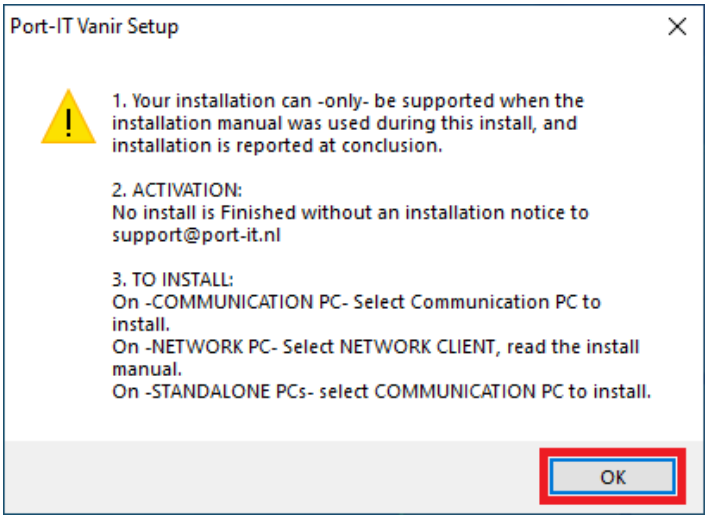
In this chapter we will guide you through the general setup which will be later split into 2 other chapters, one for the Communication PC / Standalone PC and one for the Network Client PC.

1. Please run the file called: **Port-IT-Vanir-Installer.exe** by double-clicking it.
   If you are installing from a CD or a USB, it can be found in the Zip File named: **VanirLite-Latest**.

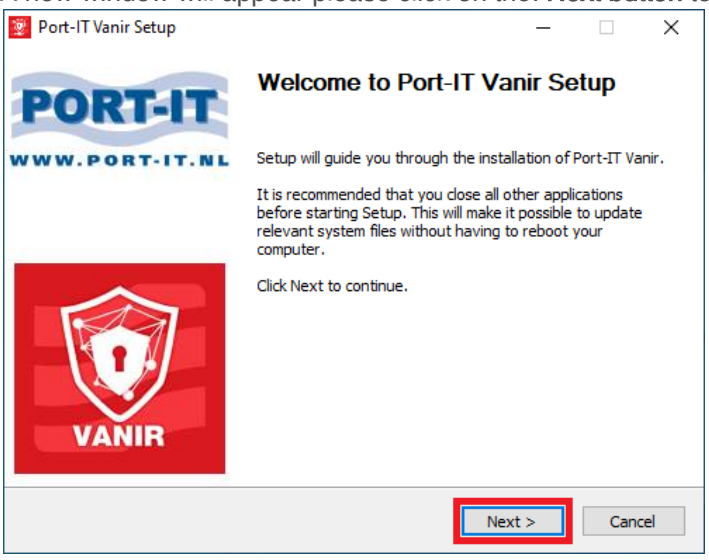
2. You might see the: **User Account Control** notification depending on your Operating Systems Security.
   If you do, please click on: **Yes** to proceed.



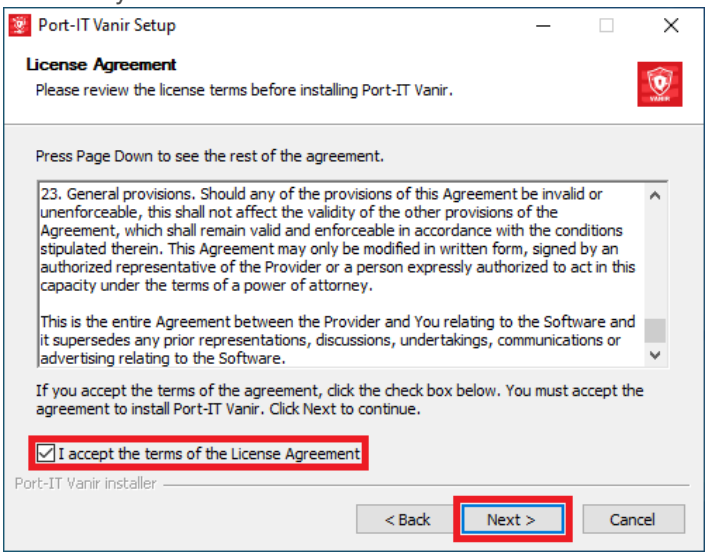
3. A new window will appear that will inform you what must be done and what you can install. Click on the: **OK button** to continue with the installation wizard.



4. A new window will appear please click on the: **Next button** to continue the wizard.

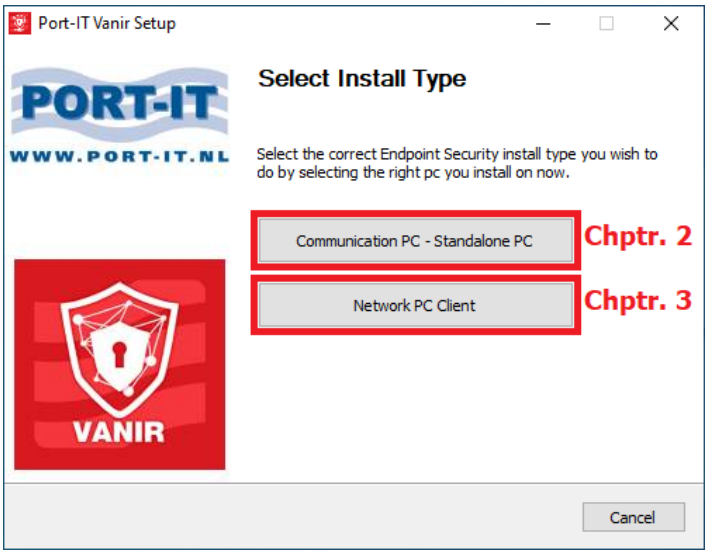


5. In the next window you will see the License agreement. Please read it carefully and mark the checkbox in-front of: **I accept the terms of the License Agreement** if you accept the terms.
   After that you will be able to click on the: **Next button** to continue the wizard.



6. In the next window you can choose what you would like to install
   Please refer to the below chapters for the respective installation types:

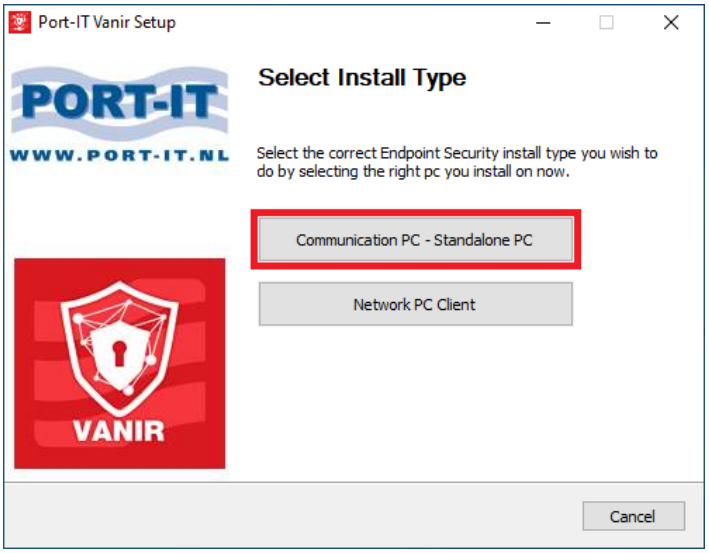
- **Chapter 2:** Communication PC & Standalone PC.
- **Chapter 3:** Network Client PCs.



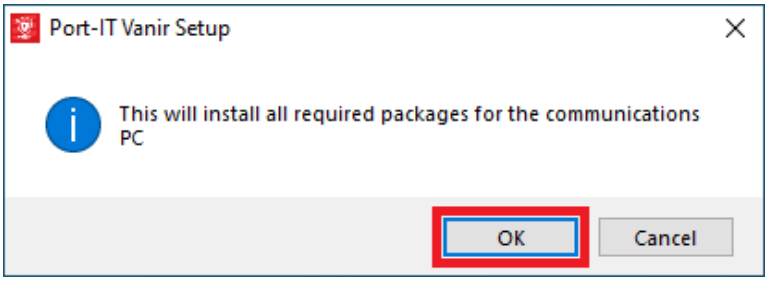
2 Communication PC & Standalone PC Vanir:

In this chapter we will guide you through the process of installing the Communication PC.

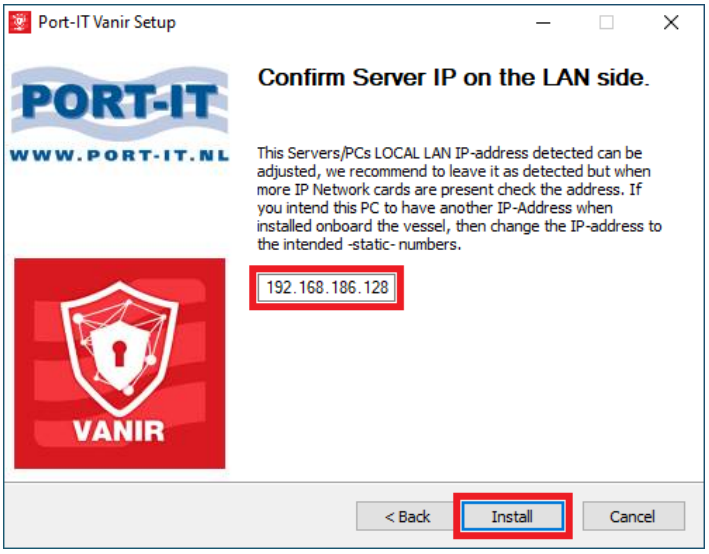
1. Choose: **Communication PC – Standalone PC.** The communication PC is also commonly referred to as Comm PC.



2. You will be notified of the installation for the Communication PC. Continue by clicking on the: **OK button**.

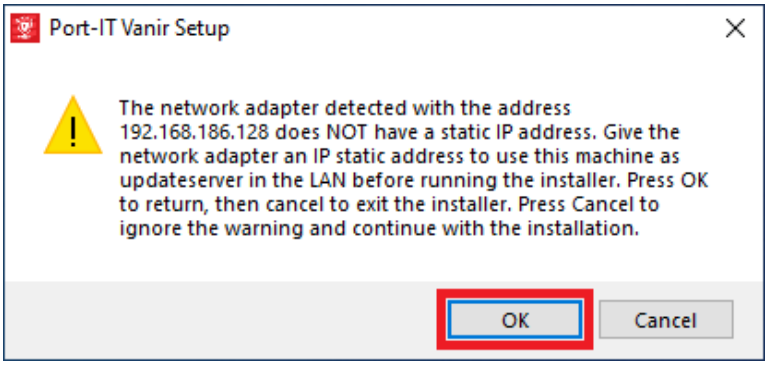


3. In the next window, the software will detect the system's initial IP settings.
   Please check if the IP address is the correct local address. If it is correct, click on: **Next** to continue the installation wizard for the Communication PC.



(Please note the IP in this image could be different for your vessel.)

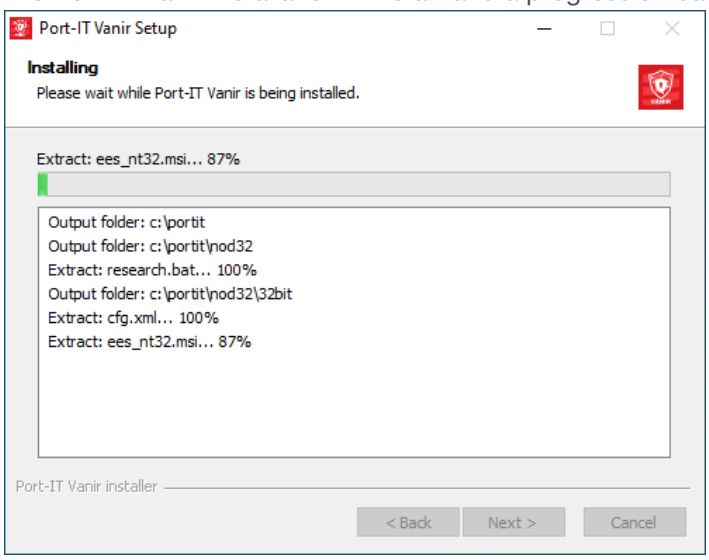
4. It is possible you will see the following window (if not, you can continue with: **Step 5**.).
   If you see this, it means you need to configure the communication PC to have a: **Static IP** address because **DHCP is enabled**.
   Please do so before proceeding with the installation.



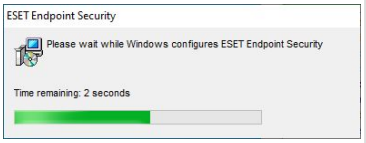
If you do not know how to do this, do not continue with the installation, please contact your IT-Department and ask for assistance. Afterwards if your IP has not been changed but has been set to a static you can click on cancel. If it has changed please restart the installation process.

5. The installation of Port-IT Vanir will start and multiple windows will appear as seen below.

The Port-IT Vanir Installation will start and a progression bar will be shown



ESET will be installed as well.



6. Once you have reached 90% of the installation, a new window will be shown where you can preset a range of IP's. If a client PC is unable to connect to the communication PC they will start scanning the network you configure in this step to find the communication PC.
This feature is often used on vessels that have multiple networks that need to be secured.
You can also close the window by clicking the: **Exit without saving** button if you do not want to use this feature and continue with the installation wizard. Doing so will leave the Guardian in its default state and only the network configured at step 3 will be scanned in case a client loses connection.

1. By default, the current IP range will be scanned starting with 1 and ending with 255 which is also the max.

2. By clicking on the: **Trash icon**, you will be able to remove a rule.

3. If you want the entire list to be cleared, you can click on the: **Clear button**.

4. To set a range kindly enter the starting IP and the Ending IP.

For example: your vessel has 2 networks (VSat & FBB)
VSat operates on the IP range: **192.168.1.XXX**
FBB operates on the IP range **10.1.100.XXX**

The **default rule** is set to scan the **full range** of the **VSat** network which takes around 1 hour max.

You can add another range for the **FBB** network by entering the following:

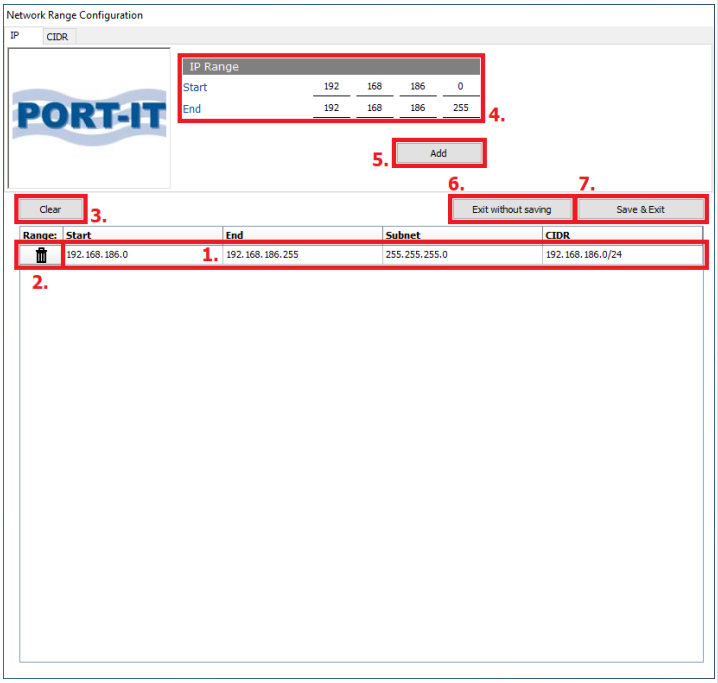
Start: 10.1.100.0
End: 10.1.100.255

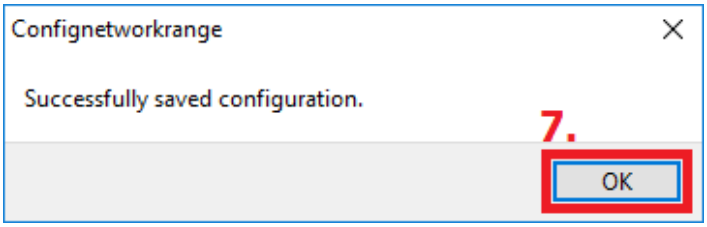
(The IPs above are an example)

5. Click on the: **Add button** to add the range to the list.

6. If you made changes and don't want them, you can click on the button: **Exit without saving**.

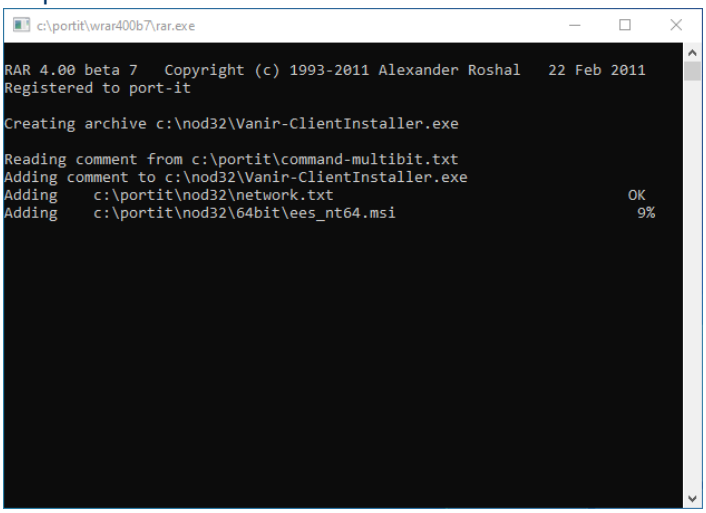
7. Once done you can click on the: **Save & Exit button.**



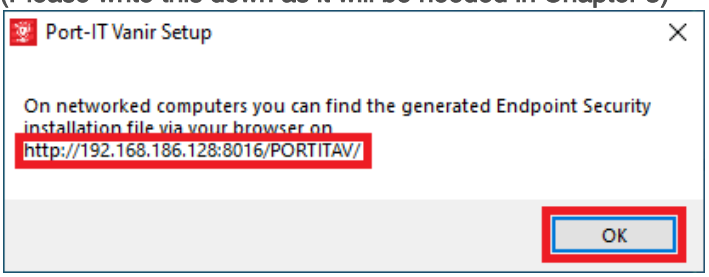


You will also receive a notification, click on the: **OK button**. The installation will continue.	

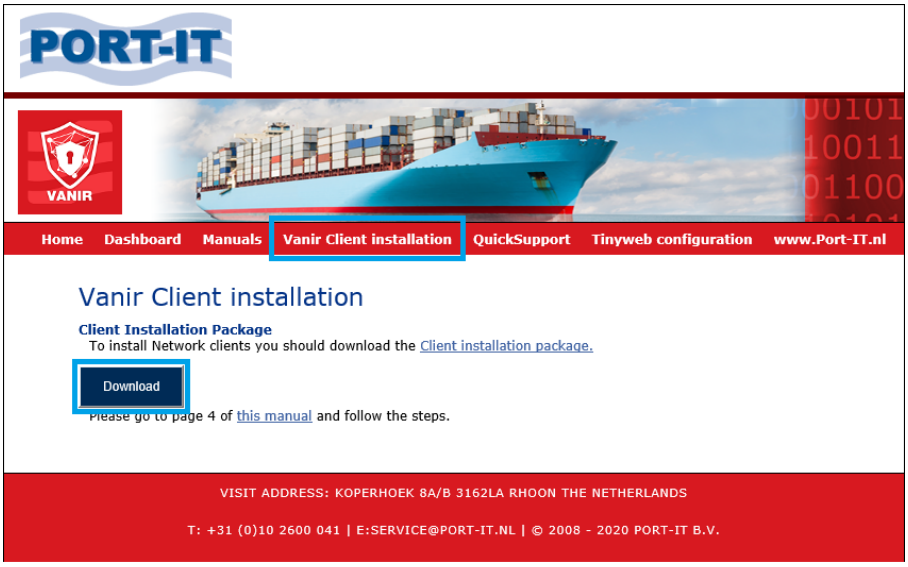
7. The installation will continue and a black window will appear. (Please do not close it and wait for it to finish) This is the process that creates the Local network Client PC Installation file which is needed in the next chapter.



8. Once the process in the black window has finished it will close automatically and the installation wizard will create an offline web-page that all the PCs that are connected to the local network can access.
It will also inform you where you can find the Client PC installation file by showing you another windows with the link to the offline web-page.
(Please write this down as it will be needed in Chapter 3)



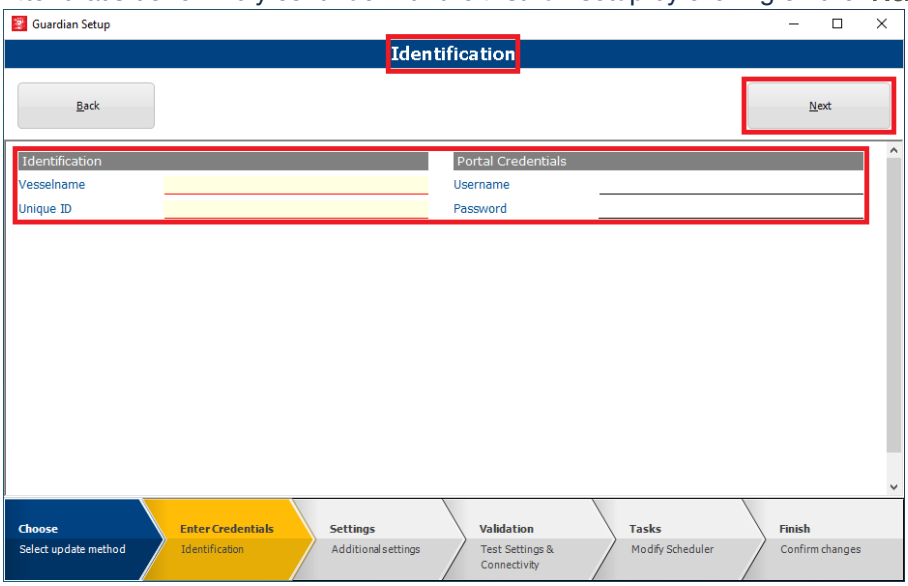
By clicking on the: **OK button**, the offline web-page will be opened on the default selected internet browser (Internet Explorer, Firefox, Google Chrome etc.).



The offline web-page can be used by your client to download the installation file. For now, you can close it.

9. At the same time the: **Guardian Setup** will open.
On the screen named: **Identification** you will be asked to enter the Vessel Identification and Portal credentials.
Vessel name: Enter your vessel name.
Unique ID: Your vessel IMO number can be used as Unique ID.
Username: This can be found in the welcome letter/mail, or you can contact the Port-IT Support department: support@port-it.nl
Password: This can be found in the welcome letter/mail, or you can contact the Port-IT Support department: support@port-it.nl

After that's done kindly continue with the first run setup by clicking on the: **Next button**.

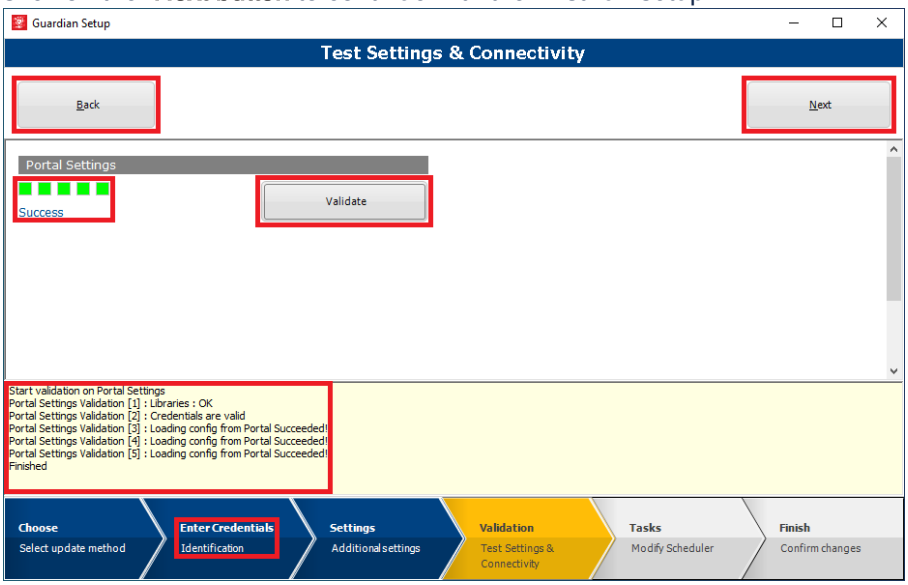


10. On the next page named: Test settings & Connectivity, you can click on the: **Validate** button to test the credentials and connection.
If successful you will see the 5 cubes turn green, if not they will turn red. If this is the case you will find the reason at the bottom

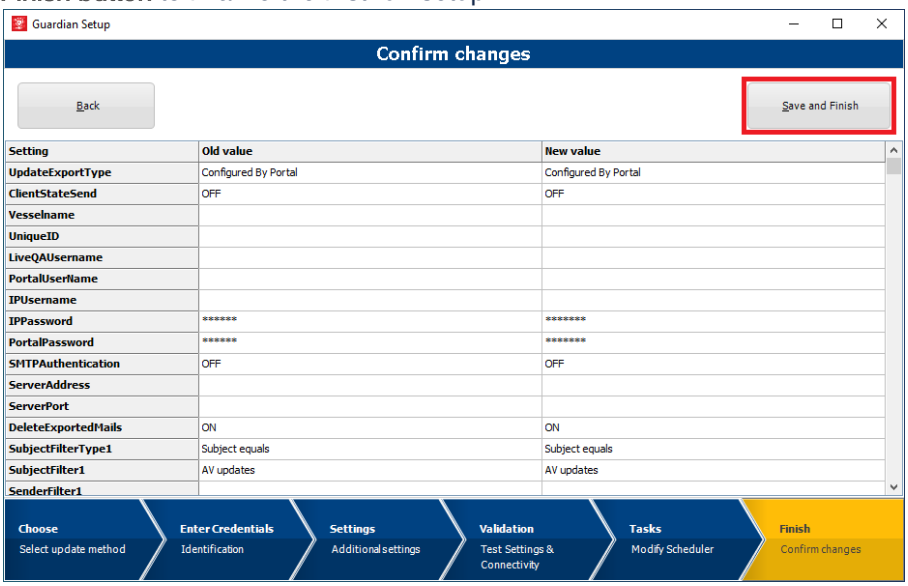
If there is an error please make sure that you have internet access and check on the: **Enter Credentials page** if the username and password are entered correctly. (we recommend copy-pasting them in the respective fields)

You can go there by clicking on the arrow shaped progress bar or by clicking on the: **Back button** in the top-left corner

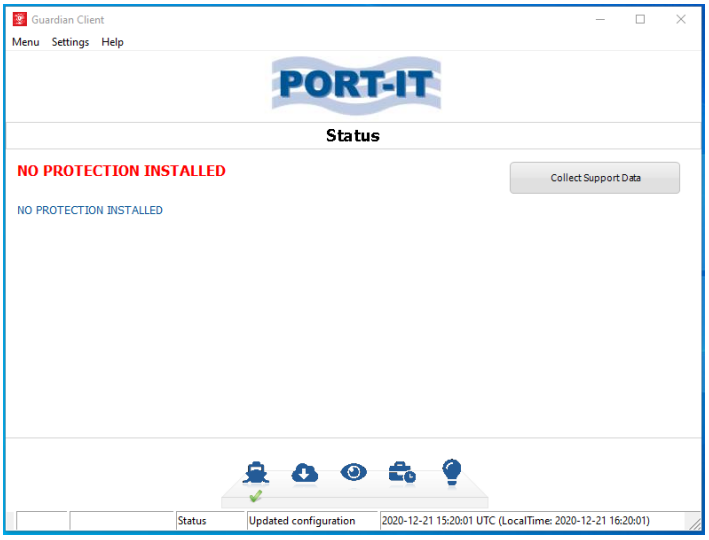
Click on the: **Next button** to continue with the First run setup.



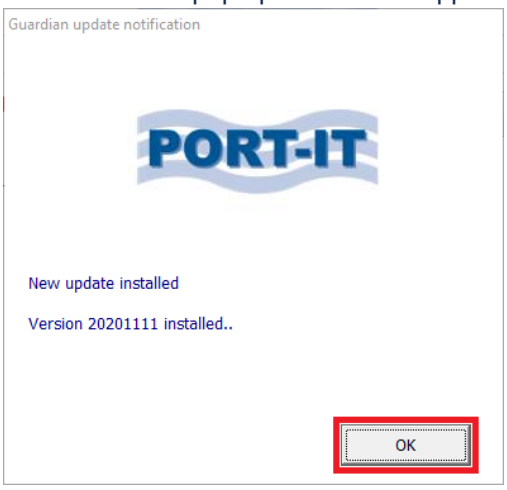
12. The next window will inform you of the settings that will be applied to the Guardian. Click on the: **Save and Finish button** to finalize the first run setup.



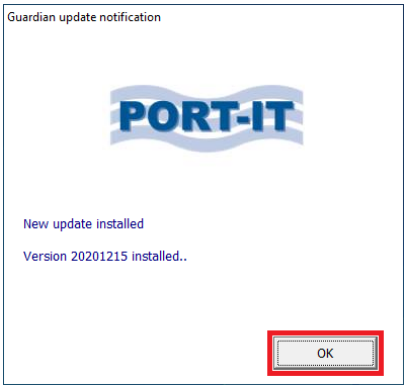
13. The Guardian will start and show you a warning that no protection is installed.

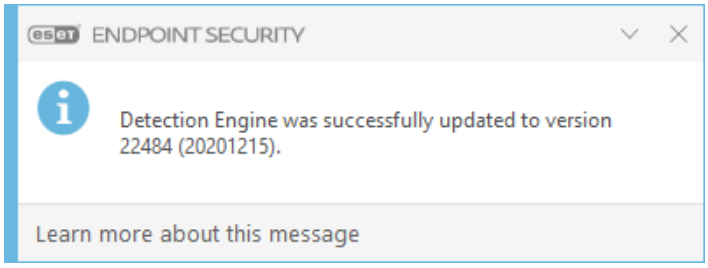


It needs some time to detect ESET and after that's done, it will also apply the update your installation package came with.
Once finished a pop up window will appear to notify you of the newly applied update.



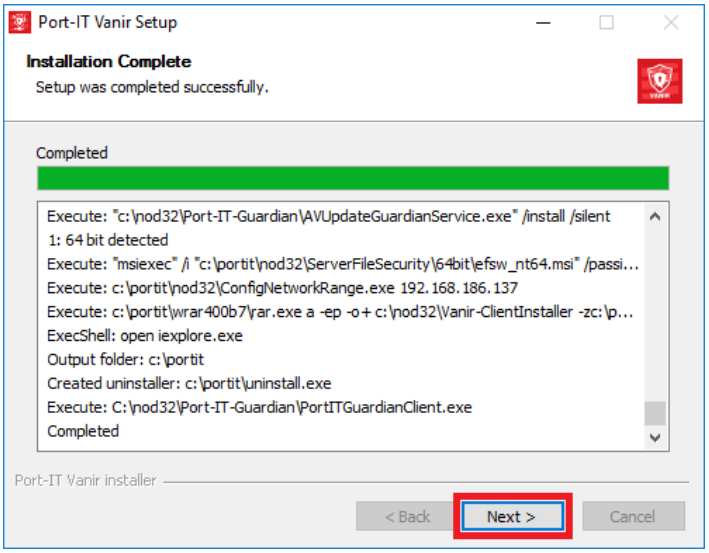
14. The Guardian will also check if there are any new updates available and if so it will download them. Once that is done the updates will be applied, and you will see another popup notifying you of this by ESET and the Guardian, click on the: **OK button**.



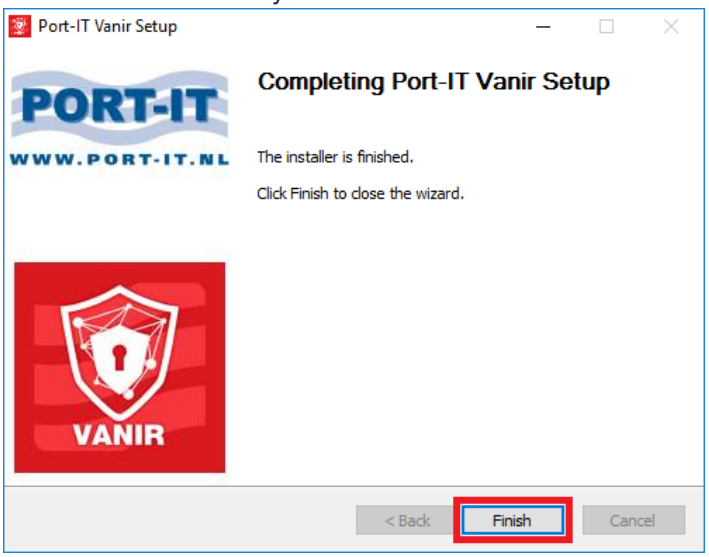


(For now you can close the Guardian client. We will go on to explain the basic functions of the Guardian in chapter 4.)

15. In the Installation wizard click on the **Next button** to continue.

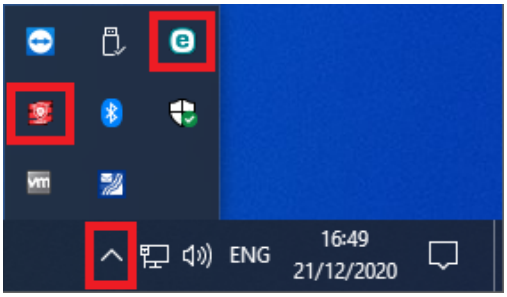


16. In the next window you can finish the installation wizard by clicking the **Finish button**.



17. An icon will be created on your desktop, double-clicking on this will take you to the offline web-page also known as the: **Vanir Dashboard**.

18. There will also be 2 Icons visible in the bottom right corner, one for ESET and one for the Guardian.

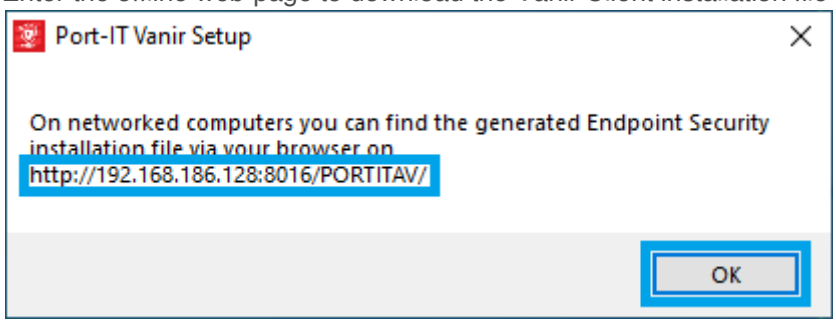


3 Network Client PCs Vanir

In this chapter we will guide you through the process of installing Vanir on a network connected Client PC.

1. Open your preferred web browser (Internet Explorer, FireFox, Google Chrome or Microsoft Edge)

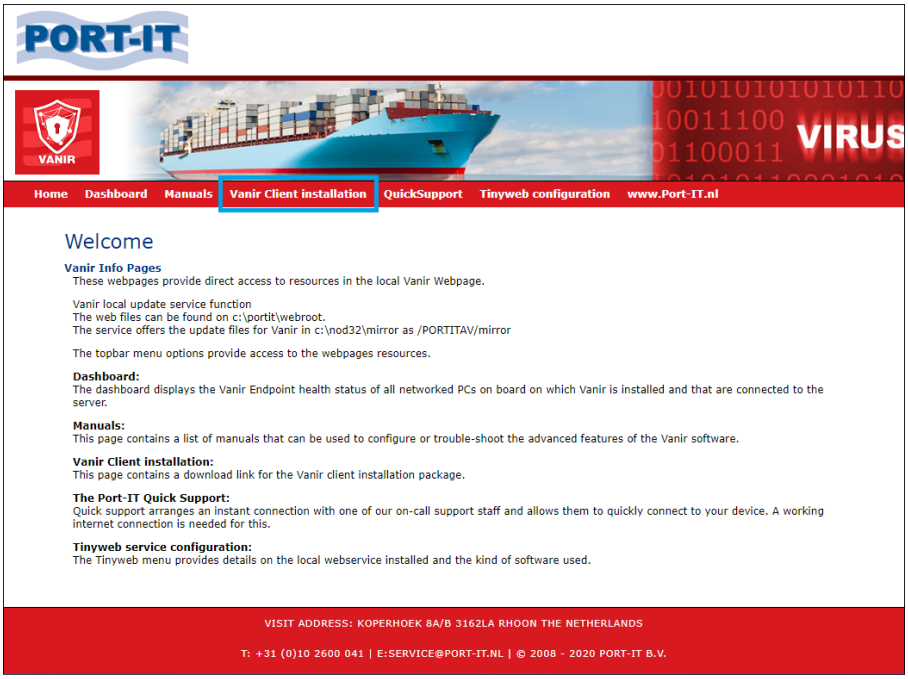
2. Enter the offline web-page to download the Vanir Client installation file



(This is the address we suggested you write down during the Communication PC installation.)

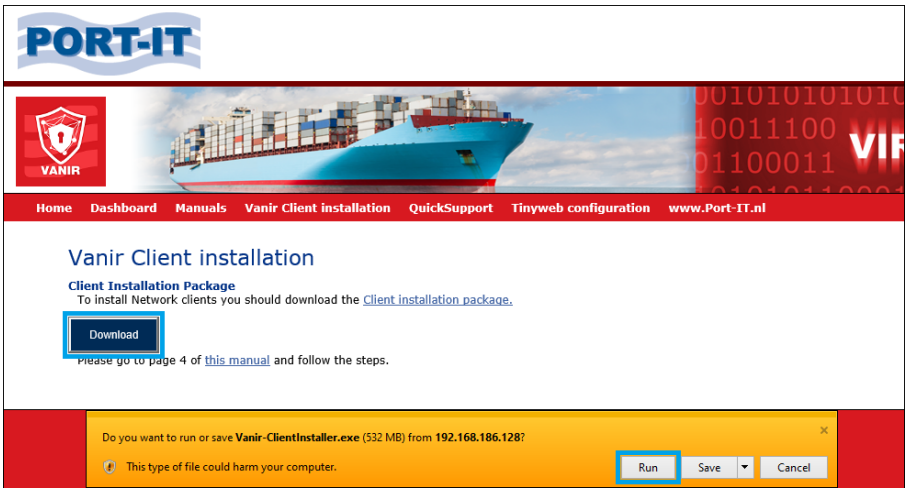
The address should look like this
http://IP ADDRESS COMM PC:8016

3. You will see the following offline page as shown in the picture.
Please click on **Vanir Client installation**.



(Please note that your IP could be different based on the network on-board.)

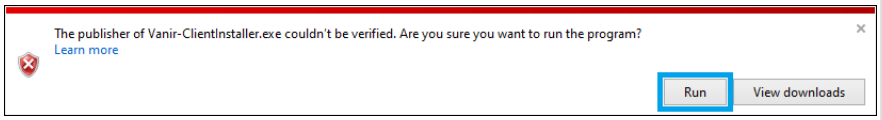
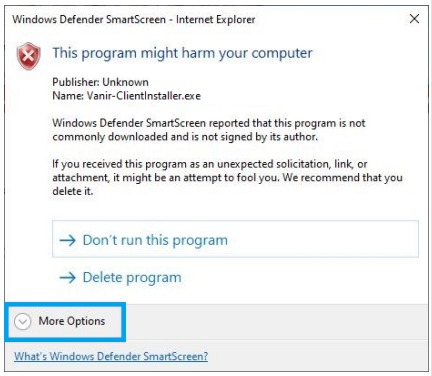
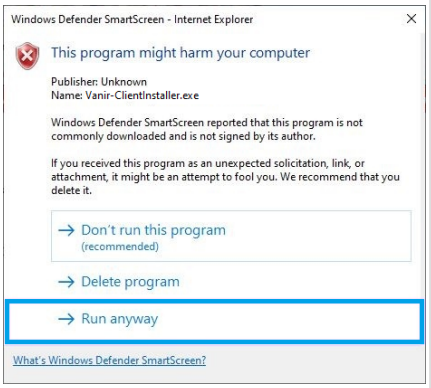
4. On the next page click on the **Download** button and once the download has finished click on the **Run button** which is shown on the bottom.



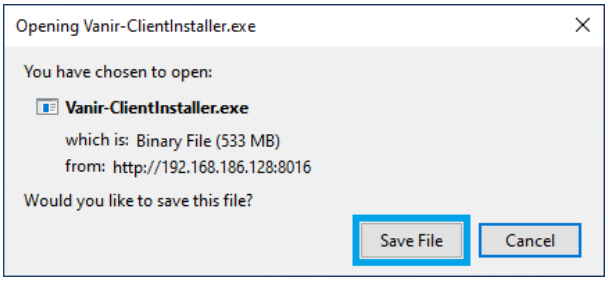
(Depending on the browser you are using the interface may not match the one shown in the picture.)

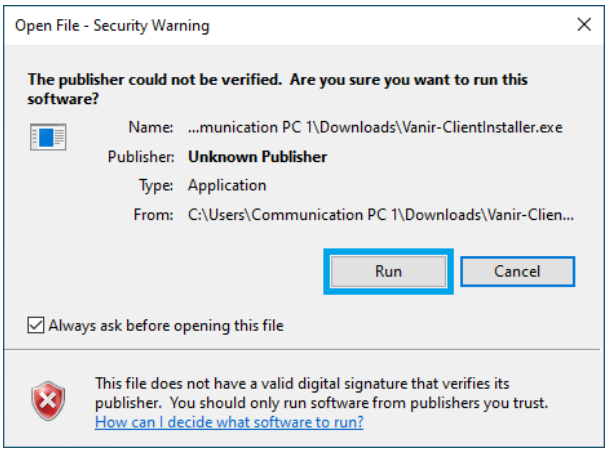
5. Depending on your operating system and browser you might get a warning as shown below if **Internet Explorer** is being used.
   a.

For Windows 8, 8.1 & 10:	Internet Explorer
1. Click on **Run**.	

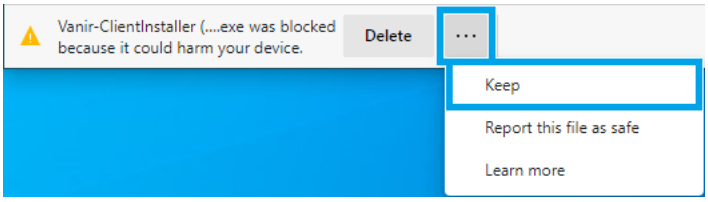
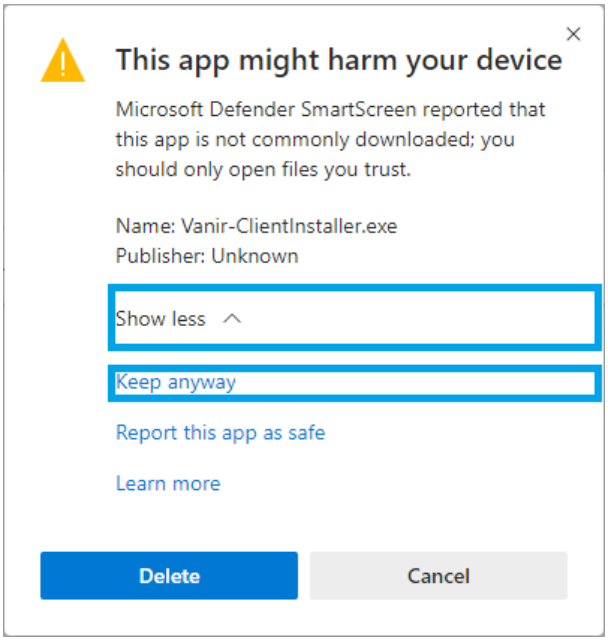
For Windows 8, 8.1 & 10:	Internet Explorer
2. Another window will appear. Click on the **Action button**.	
3. In the new window, click on **More options** to select **Run anyway.**	 

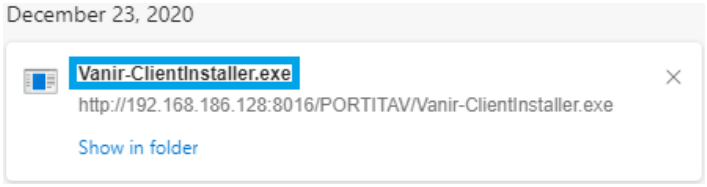
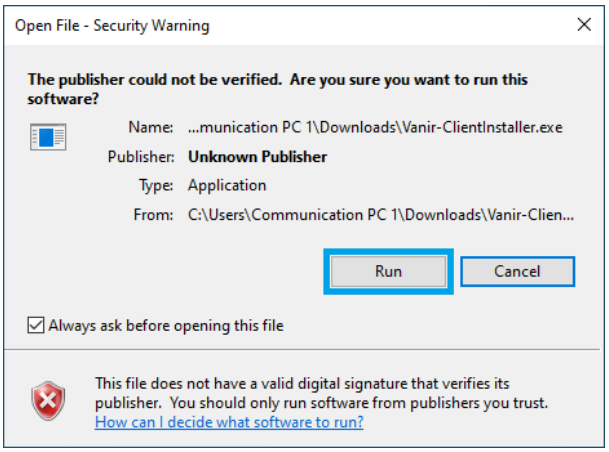
b.

For Firefox & Chrome	
1. After clicking the Download button on the offline webpage, click on the: **Save File button** if requested.	

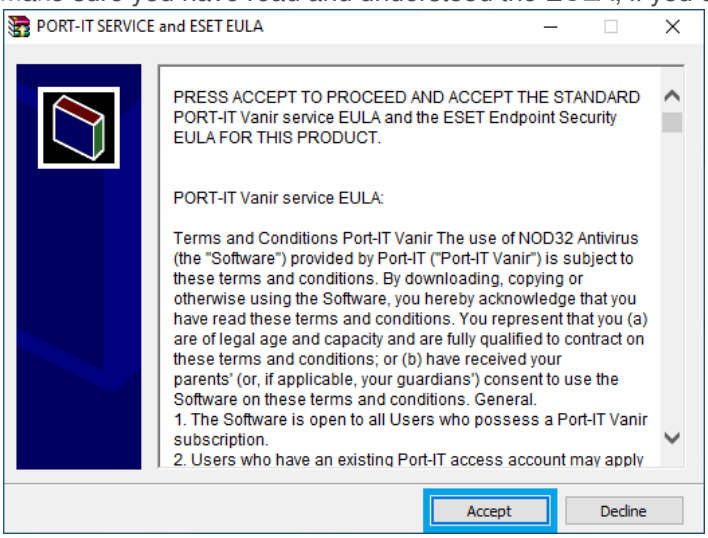
For Firefox & Chrome	
2. Once the download is completed, navigate to the download location and execute the file named: Vanir-ClientInstaller.exe. A new window will appear. Click on the: **Run button.**	

c.

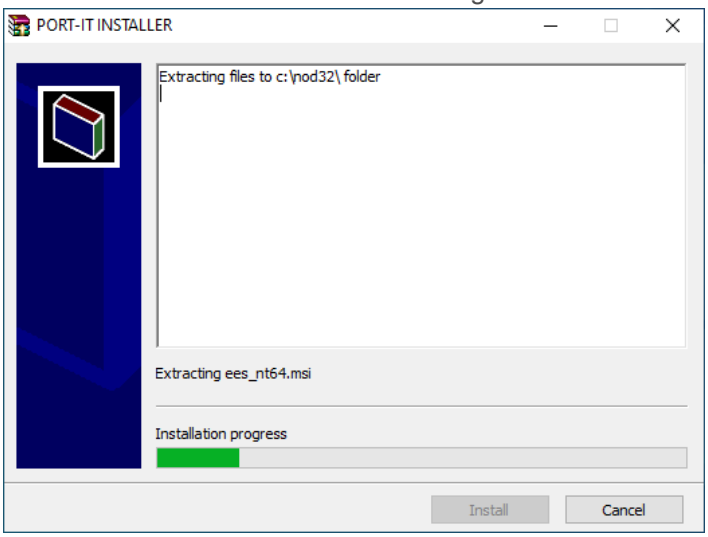
For Windows 10: Microsoft Edge.	
1. After clicking the Download button on the offline webpage, click on the button with **3 dots [...]**	
2. A new page will be opened where you will have to take action. Click on: **Show more** and choose: **Keep anyway.**	

For Windows 10: Microsoft Edge.	
3. Click on the file name: **Vanir_ClientInstaller.exe** to start the installation file.	
4. A new window will come again to request permission.	

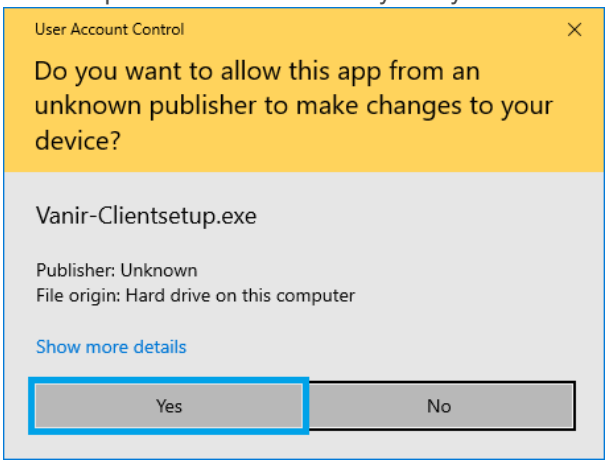
6. Make sure you have read and understood the EULA, if you do click on the **Accept button**.



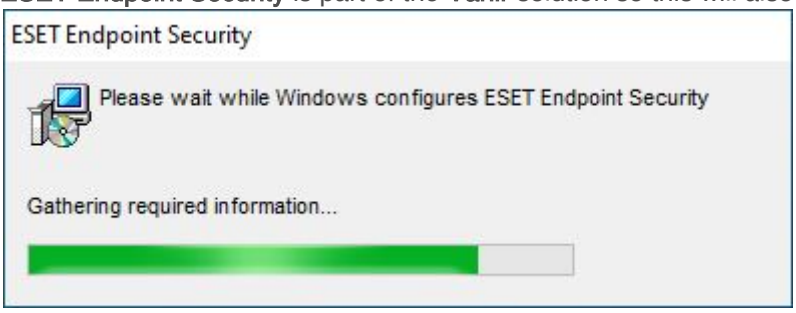
7. Now the self-extractor will start extracting the installation files and install **Vanir Lite** for the **Client PCs**.



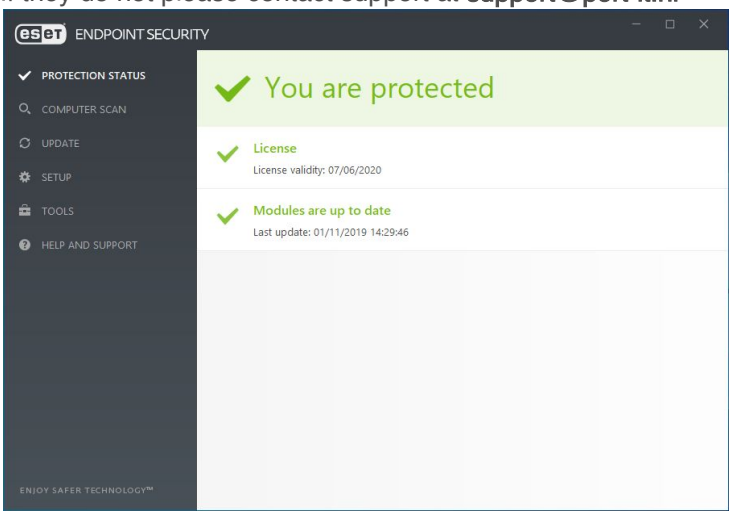
8. At some point Windows will ask you if you want to continue the installation. Choose **Yes**



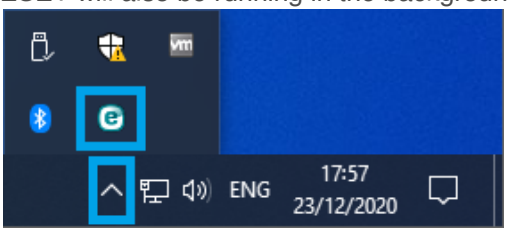
9. **ESET Endpoint Security** is part of the **Vanir** solution so this will also be installed.



When the installation has finished it will open ESET, ESET will show a few warnings that should go away within 15 to 60 minutes.
If they do not please contact support at **support@port-it.nl**



10. ESET will also be running in the background and has an icon in the bottom-right corner.



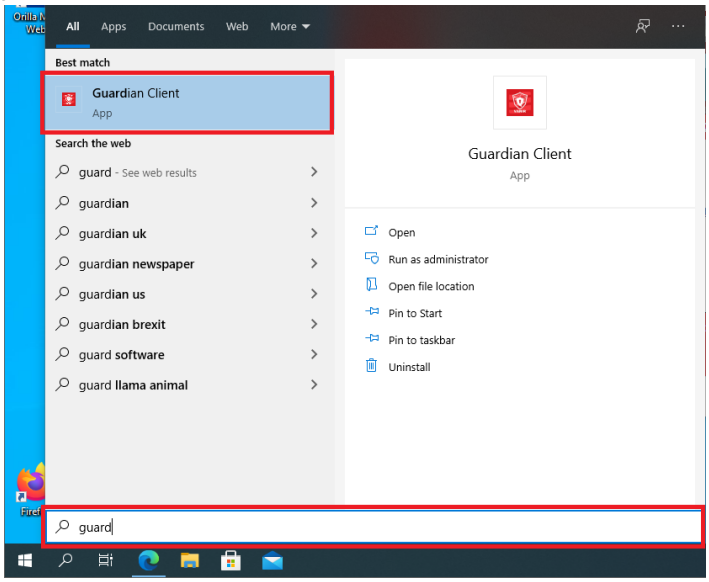
This concludes the client installation

4 Vanir Guardian:

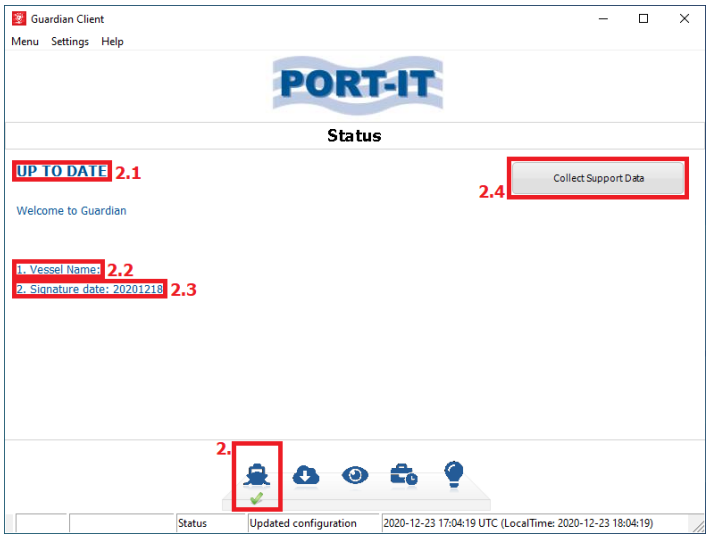
In this chapter we will guide you through the options of the Guardian.

Please know that the Guardian will only be installed on the Communication PC and Standalone PCs.

1. To open the Guardian, click on start and search for **Guardian** then click on the icon that appears, as seen on the picture.

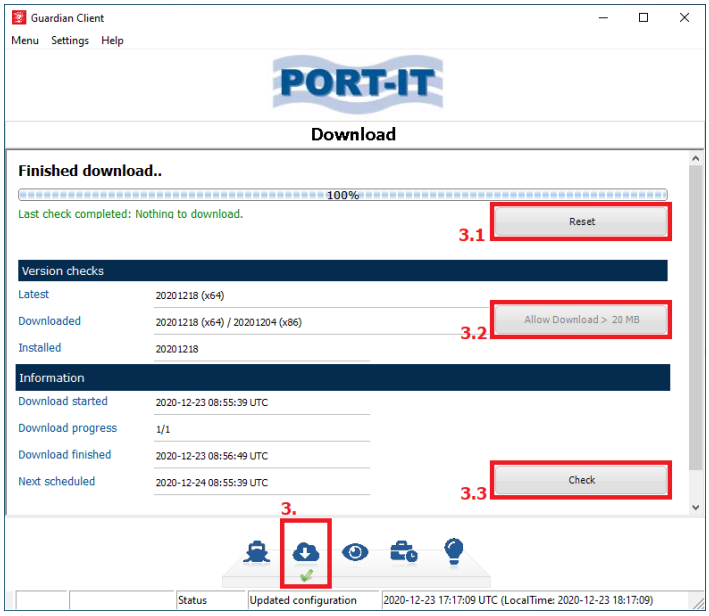


2. You will see the following window named **Status.** This window will inform you of the following:



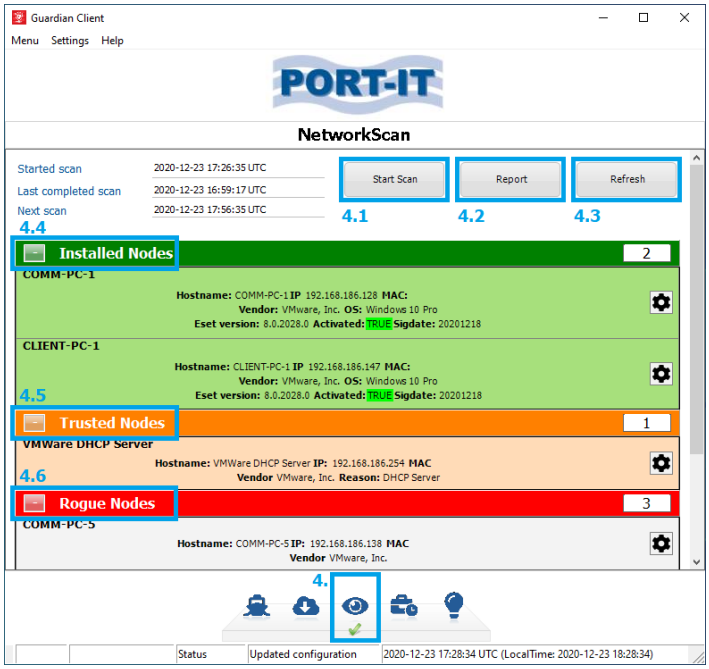
2.1 The Status of : **Fleet Secure Endpoint** (FSE in short).
2.2 The: **Vessel name.**
2.3 The latest: **Signature date** processed by the Fleet Secure Endpoint
2.4 If Fleet Secure Endpoint is outdated you can gather some basic information the Support team needs by clicking on the: **Collect Support Data** button

3.1 After the Guardian has been successfully activated it will begin to download the license and also the missing updates.



3.1 If the download gets stuck because of an unstable network connection or the hard drive is full and was cleared afterwards you can click on the: **Reset** button to restart the download process.
3.2 If your vessel is missing a large amount of updates, the total amount of missing updates to download might become large (total size larger than 20 MB).
To allow a download larger than 20 MB please click on the: **Allow Download > 20 MB** button:
3.3 If you want to check if an update is available you can click on: **Check**

4. The Guardian is also able to monitor the network and inform you of the devices connected (also known as nodes) to the network. There are 3 categories of nodes which will be explained below in addition to the Guardians NetworkScan functionality:



4.1 You can start a new network scan by clicking on the button named: **Start Scan** (a scan could take up to 15 minutes)

4.2 When a scan has been completed you can manually report the results to the Web-Portal by clicking on the **Report** (The guardian will send its results automatically every 7 days.)

4.3 You can refresh the list by clicking on the **Refresh**

4.4 **Installed nodes**: Devices listed here have Fleet Secure Endpoint installed and will show whether they have been activated.

You will also find the following information about these devices:

- Mac address
- IP address
- Vendor of the network device
- Windows version
- ESET Version
- Whether ESET has been activated
- Signature date

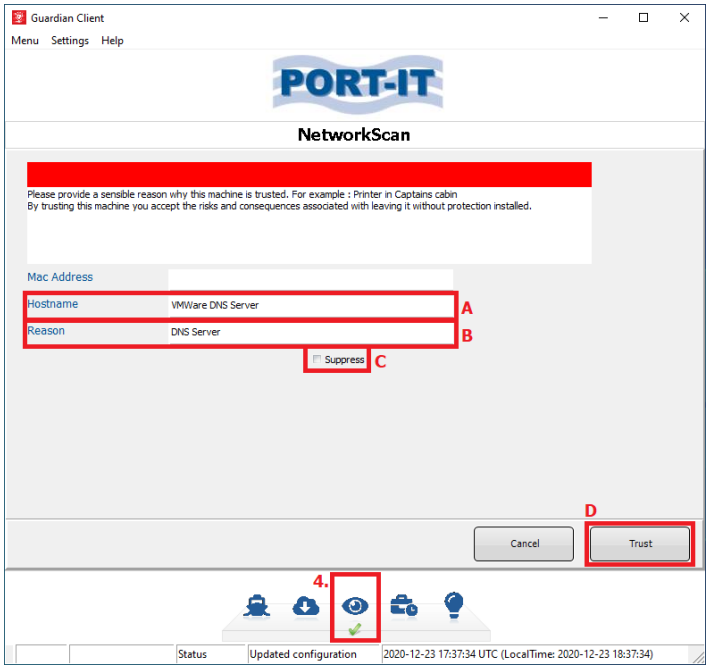
4.5 **Trusted nodes**: Trusted nodes are devices that you have marked as trusted. You trust devices when Fleet Secure Endpoint cannot be installed on the device. Usually these are devices such as printers or scanners. Trusted nodes can only be added manually.

The Guardian will show the following information about these devices.

- Device Name (this can be adjusted)
- IP address
- Mac address
- Vendor of the network device
- Reason why you added the device to the trusted node list.

4.6 **Rogue nodes**: Devices that do not have Fleet Secure Endpoint installed will be listed here. Devices that have been detected should be investigated, and you should try to install Fleet Secure endpoint on the device. If it cannot be installed you can add it to the trusted nodes list. Once rogue nodes have been detected a notification will appear and will keep appearing periodically until the rogue node has been investigated and added to the trusted or installed nodes list.

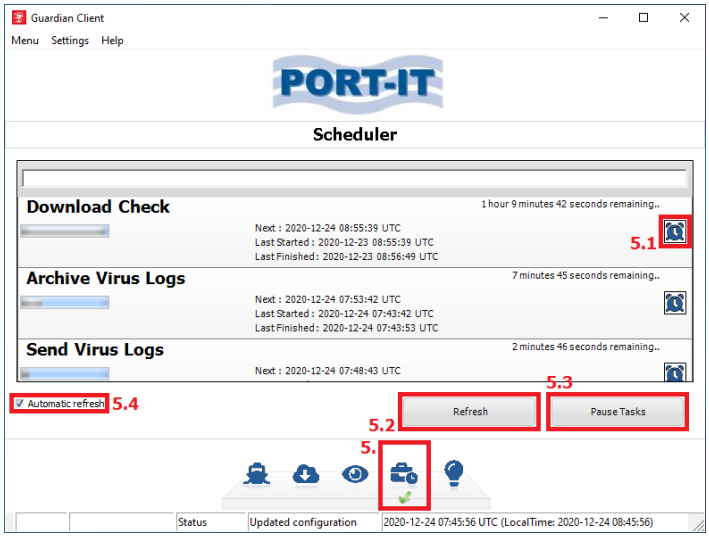
By double-clicking on a device in the Rogue node section you can add the device to the trusted nodes list.



A. Please enter the device name this can be a Computer, phone or a master cabin printer for example.
B. You must enter a reason why you want to add the device to the trusted nodes list.
C. When you click on **suppress**, the notification for that rogue node will be suppressed, but it will still be shown as a rogue node.
D. Please click on Trust to trust rogue node. (Trusted devices can be removed by double-clicking on the trusted node.)

5. The scheduler menu shows the intervals at which the different Fleet Secure Endpoint tasks run.

Here you can see when a task will run, when it last completed successfully, and you can manually start the task.



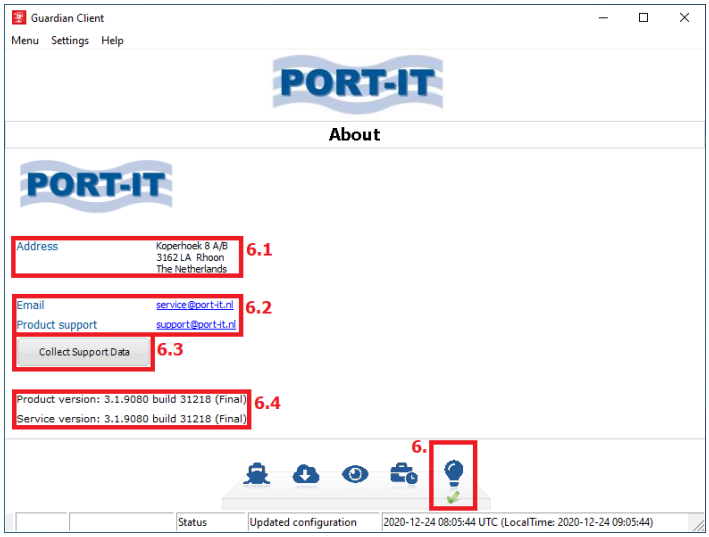
5.1 When you click on the **clock** next to a task, the task will be performed as soon as possible.

5.2 The **refresh** button will manually refresh the task information, this is useful for when you want to see if a task has been performed after you manually executed it.

5.3 When you click on **pause tasks** all tasks will be paused. If you click on the same button again all tasks will continue.

5.4 Automatic refresh automatically refreshes the information of each task, we recommend you keep this option enabled.

6. To see the Guardians version, you can click on the: **About** button, here you will find the following information:



6.1 This is the address of Port-IT's head office.

6.2 If you are experiencing issues with Vanir Lite, or you have questions you can contact us with these E-mail addresses.

6.3 You can click the **Collect Support data** button to create an in-depth log that will be used by Port-IT Support department to resolve any issues you may have.

6.4 The support department will often ask for the **Product** and **Service version** this will show which version of Fleet Secure Endpoint is installed.

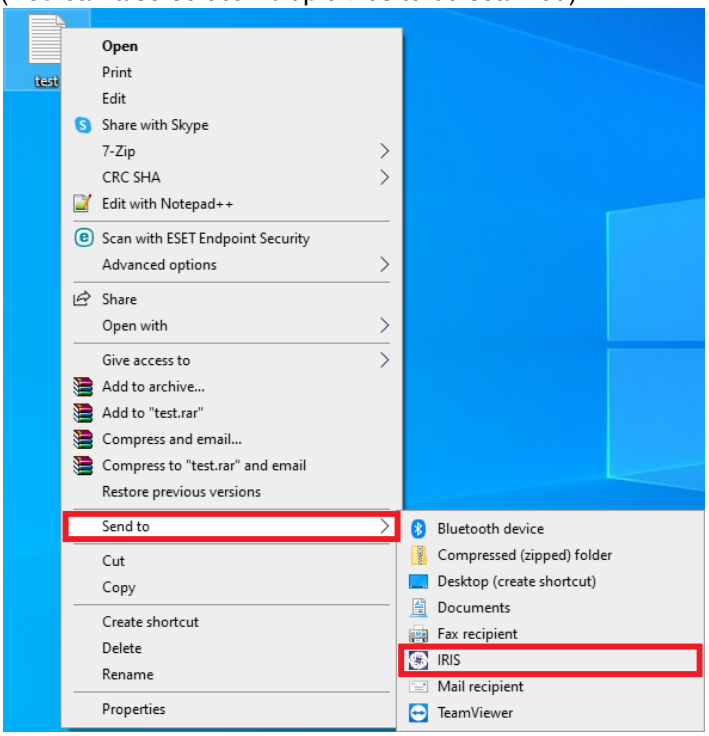
5 Iris Functionality Vanir

In this chapter we will explain the functionality of Iris.

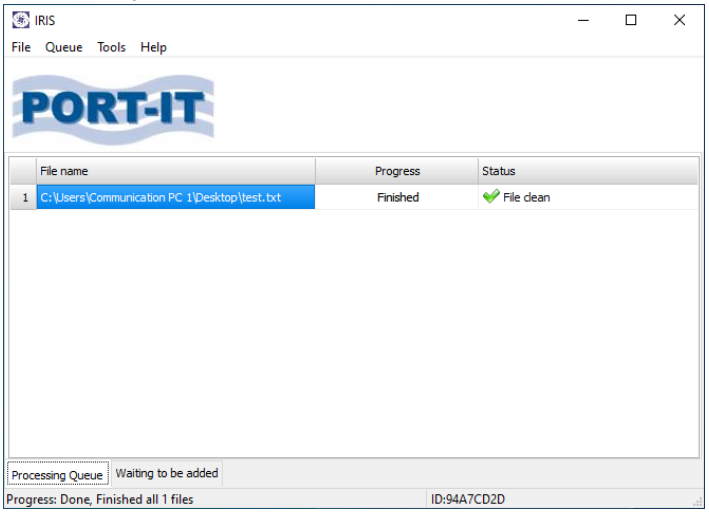
Iris can be used to scan items with multiple antivirus software to confirm if it is a virus.

To do so, kindly follow the instruction below:

1. Kindly locate the file you want to be scanned thoroughly, right-click on it and go to: **Send to** and choose: **IRIS**
   (You can also select multiple files to be scanned)

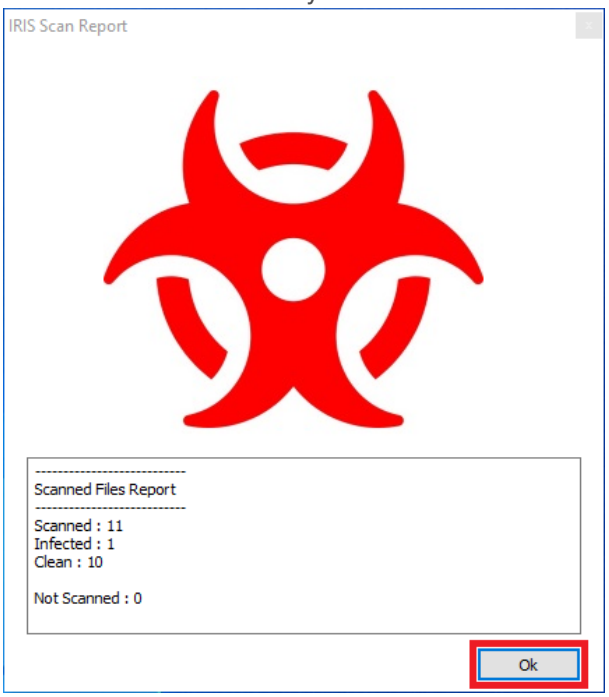


2. Iris will open and show a list of files that are being scanned.
   Please keep in mind this is done online and the files will be uploaded first.

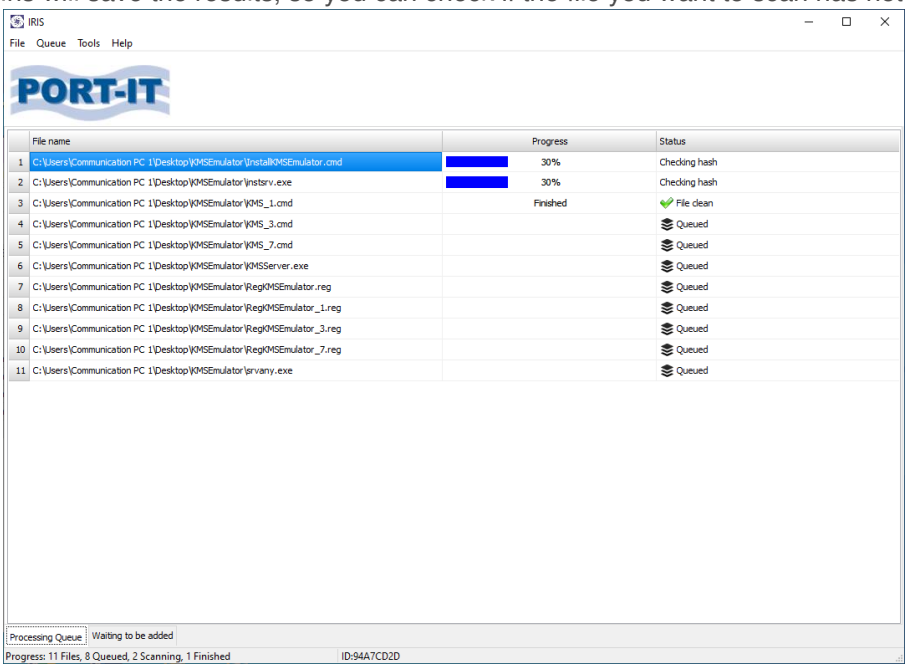


3. If the files are clean you will see a green check mark and a popup will also notify you.
   Click on the: **OK button** to close the pop-up.

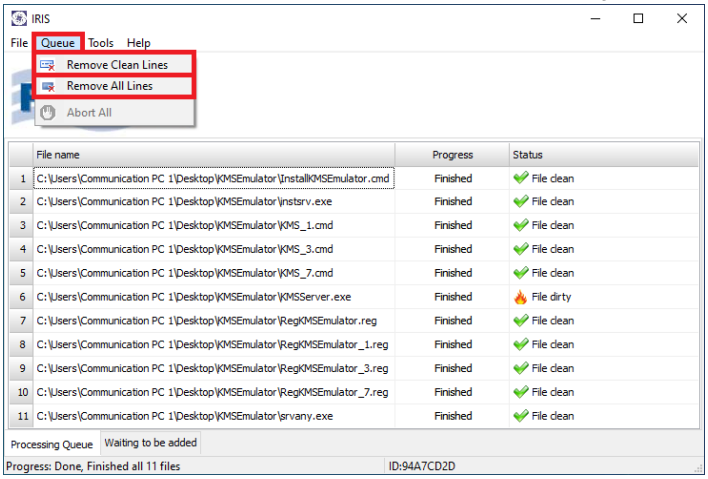
In case the file is infected you will see a red hazmat icon with a description that the file is infected.



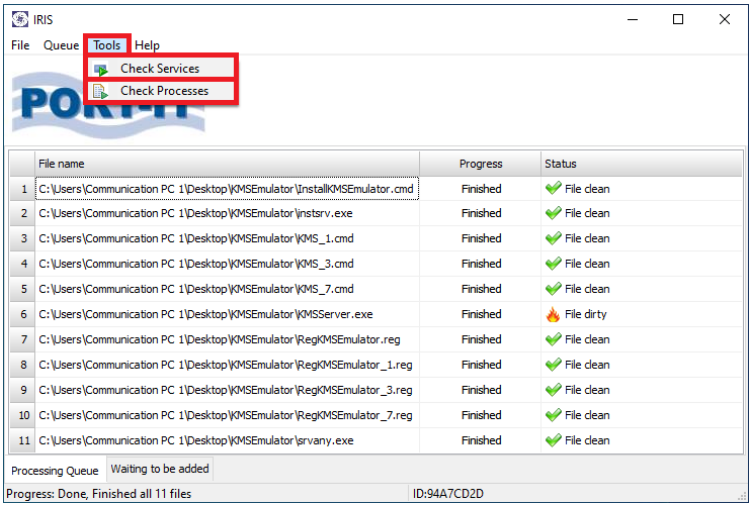
4. Iris will save the results, so you can check if the file you want to scan has not been scanned already.



5. To clear the results you can click on: **Queue** which is located in the top-left corner.
   Then click on: **Remove clean lines** to remove all the files that are clean and keep an overview of all the malicious files.
   Or click on: **Remove all lines** to clean the list entirely.



6. Iris can also scan all running services and processes but do keep in mind that the files will be uploaded which will **consume a lot of data**.
   To scan all services and processes please click on tools and choose the preferred option.



-End of Manual-

www.port-it.nl

Koperhoek 8 A/B
3162 LA RHOON
The Netherlands

sales@port-it.nl
support@port-it.nl

EMEA: +31 (0) 10 260 00 41
APAC: +65 3158 16 17

PORT-IT

Safely connected at sea.