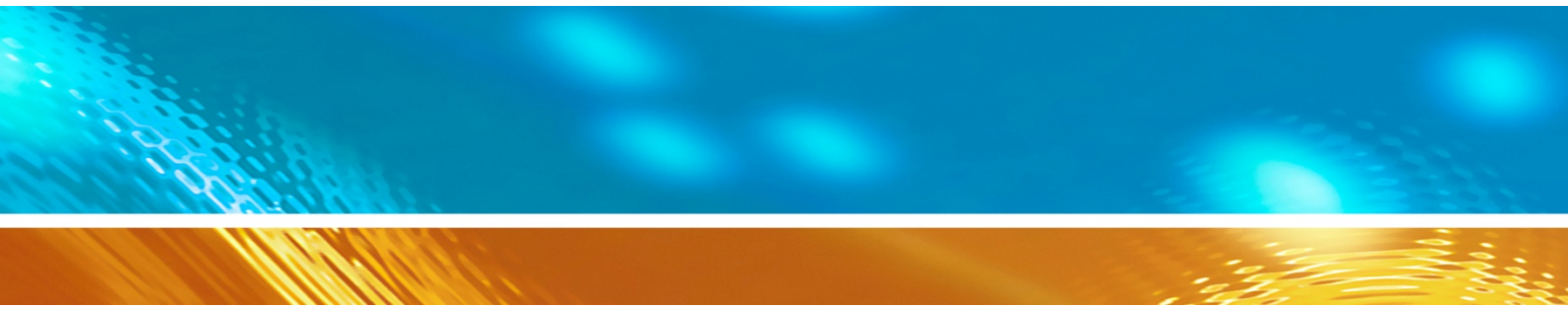
VAISALA

TECHNICAL REFERENCE



Network Manager NM10
Field Installation for MW41

DOC235403-F

PUBLISHED BY

Vaisala Oyj
Street address: Vanha Nurmijärventie 21, FI-01670 Vantaa, Finland
Mailing address: P.O. Box 26, FI-00421 Helsinki, Finland
Phone: +358 9 8949 1
Fax: +358 9 8949 2227

Visit our Internet pages at www.vaisala.com.

Table of Contents

CHAPTER 1

GENERAL INFORMATION

This chapter provides general notes for the product.

About This Document

This document describes how to perform field installation of the Vaisala Observation Network Manager deployment.

CAUTION This document is intended for Vaisala internal use only. Installing the Network Manager system is only allowed by authorized Vaisala personnel or by authorized customer representative only after receiving the specific training from Vaisala.

Version Information

Table 1 Manual Revisions

Manual Code	Description
DOC235403-A	January 2017. NM10 Field Installation for MW41
DOC235403-B	March 2017. Updated for NM10 version 3.5
DOC235403-C	June 2017. Updated for NM10 version 3.5.1
DOC235403-D	November 2017. Updated for NM10 version 3.6
DOC235403-E	March 2018. Updated for NM10 version 3.6.1
DOC235403-F	November 2018. Updated for NM10 version 3.8

CHAPTER 2
INSTALLER

Vaisala Observation Network Manager is installed using the Network Manager installation media, for example, USB stick (version 3.8 or higher) located in the NM10 media enclosure.

CHAPTER 3

INSTALLATION PROCESS

1. Log in as an administrator.
2. Connect the computer to Internet using DHCP if the connection is available and select "Work Network" as the network location if asked.

3.1. IP Address and Names

The network and host configuration is instructed in document PI215523.

3.2. Before Installation

1. Make sure that the server **time zone is set to UTC** in the **Control Panel** > **Date and Time**.
2. Connect the system to NTP server. This can be done from **Control Panel** > **Date and Time** > **Internet Time** > **Change settings** > **Synchronize with an Internet time server**. Use any available NTP server, for example *time.windows.com* can be used. If no NTP servers are available, a new one can be set up on a server that is otherwise synchronized, like MW41 is server getting the time from the GPS.

3.3. Installation

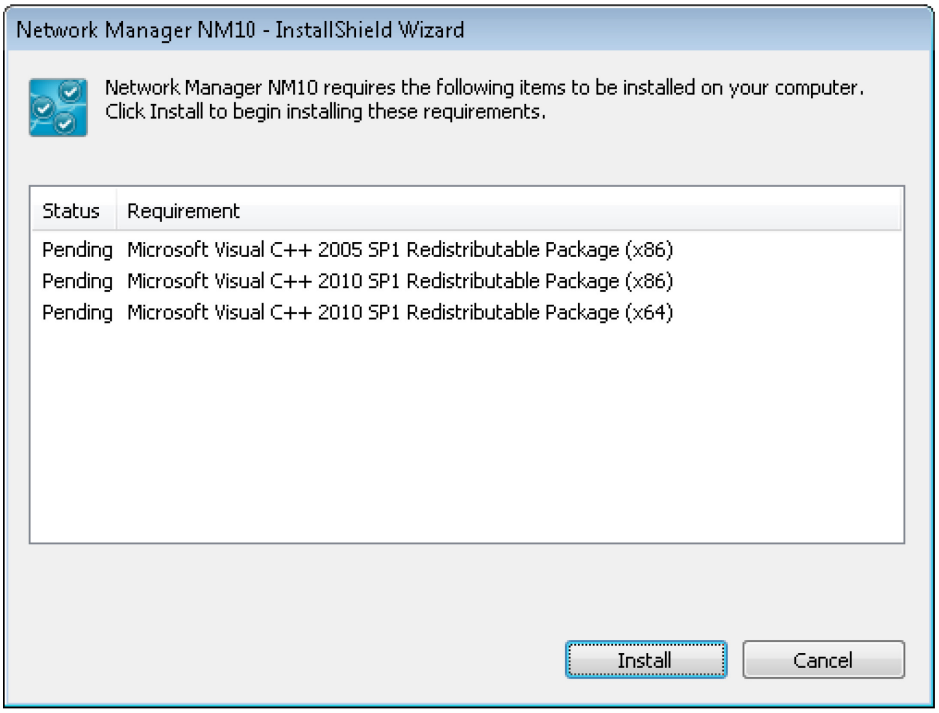
NOTE	During installation firewall might ask permissions to perform some actions made by the installer. Just allow all.

1. Insert the NM10 USB stick (*NM10 Software Installer for Windows*) into the workstation's USB port. Use USB-port 3.0, if available. Or insert the NM10 Installation DVD into the DVD drive.
2. Find location of the installer from the USB stick or DVD (StartHere)
3. Run the installer as Administrator.

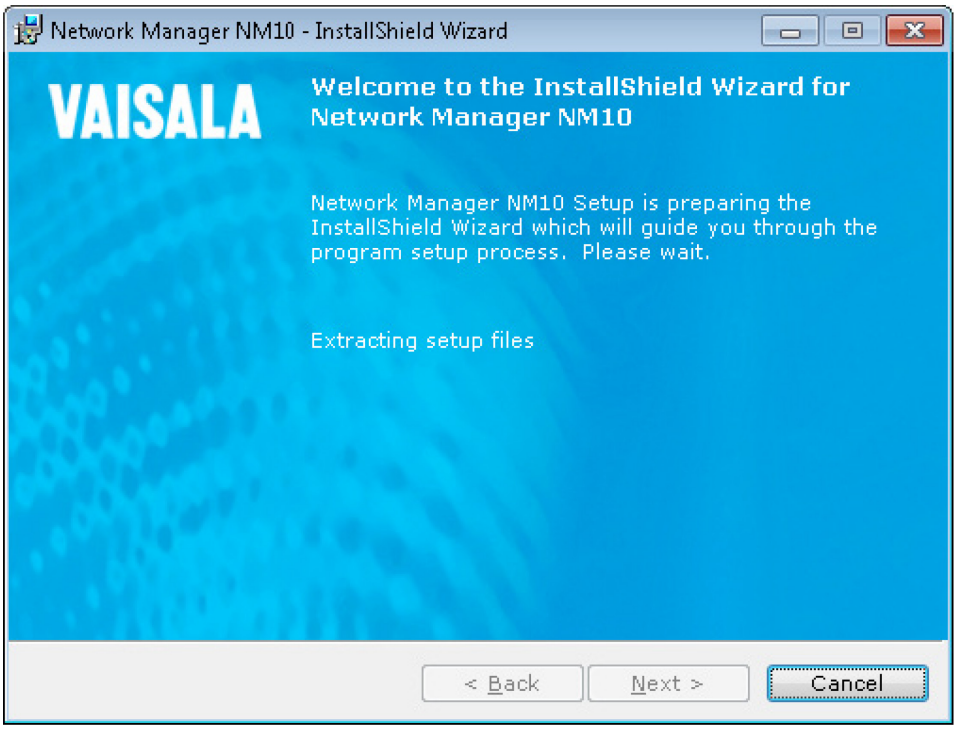
NOTE	The decompression of installation files might take more than 30 minutes.

4. The installation start-up dialog is shown. Click **Install NM10 version 3.8**.

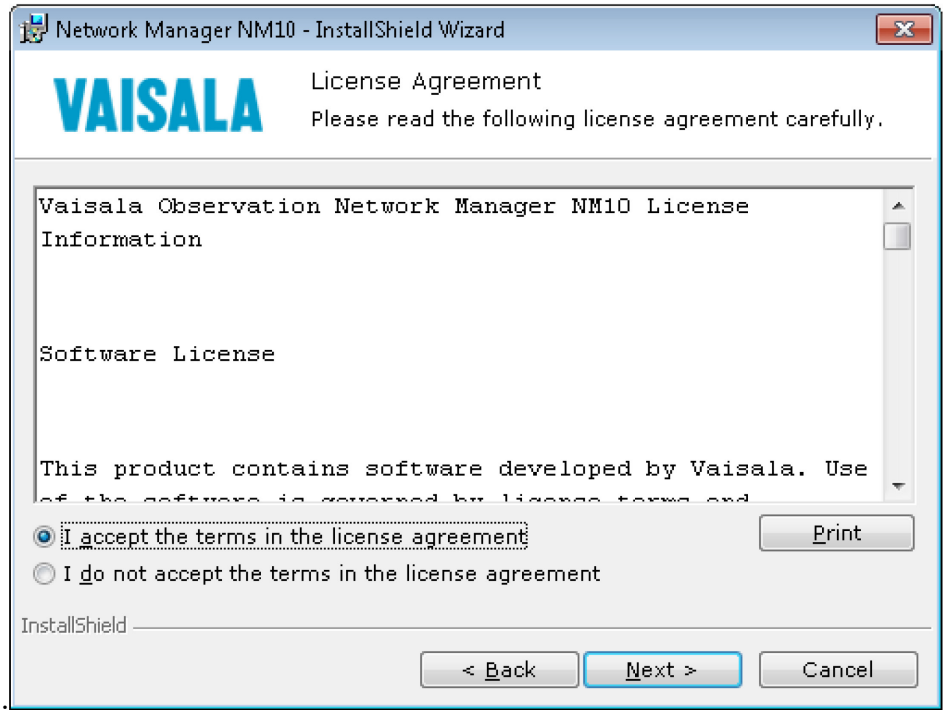
5. Depending on the system it might require to install some additional software modules, click **Install**.



6. Welcome dialog is shown.



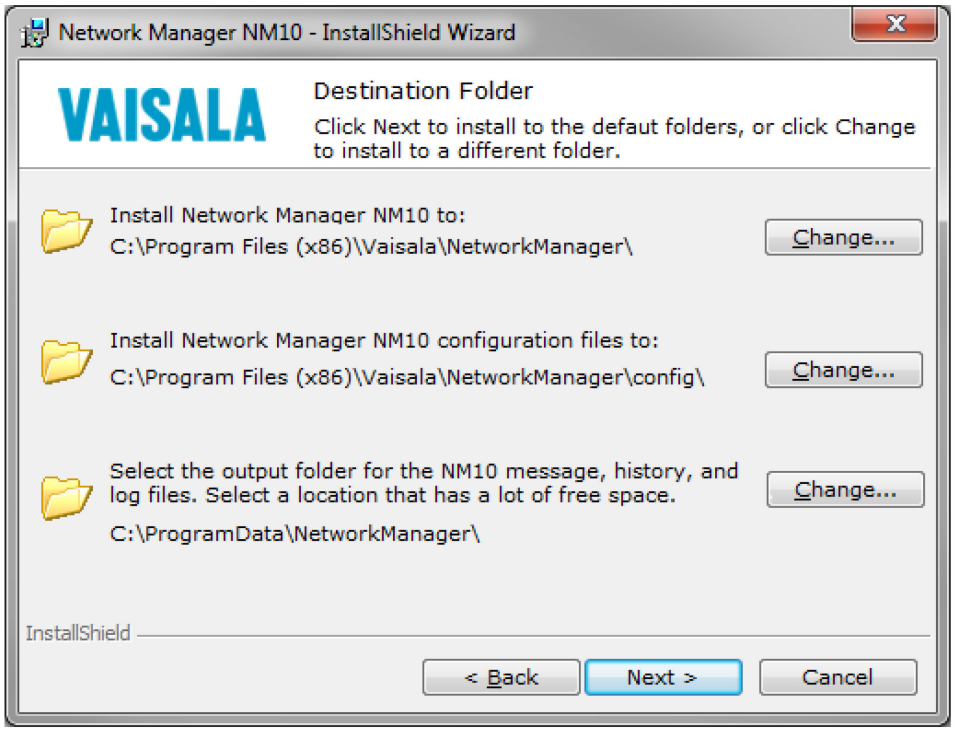
7. Accept licenses and click **Next**.



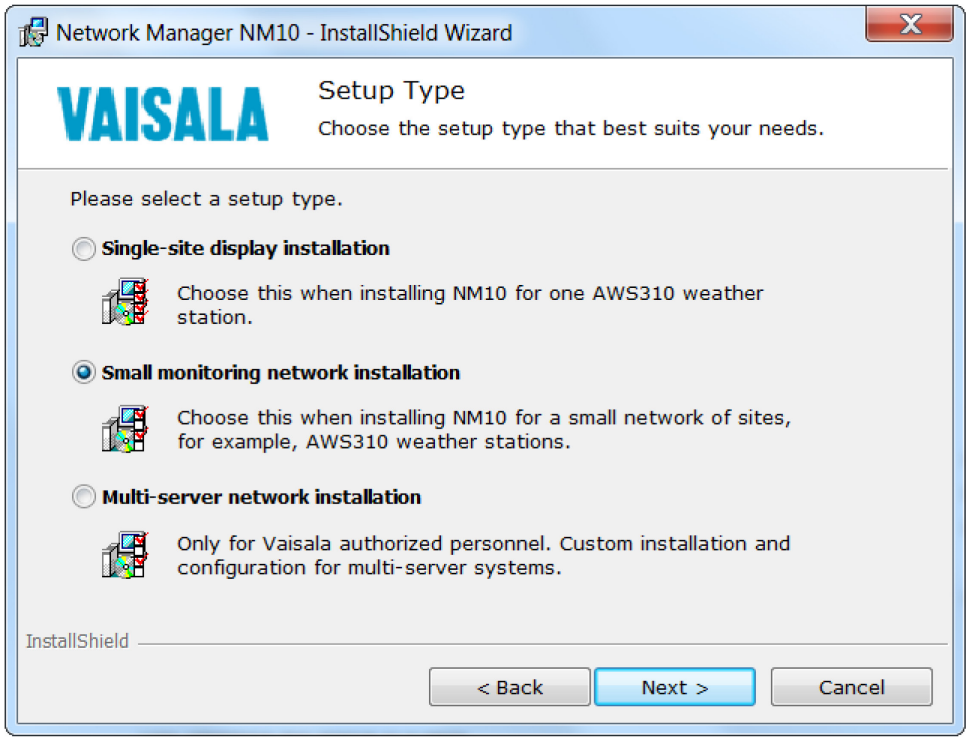
8. Select location for NM10, configuration files and history/message files.
   - For history and message files select location (drive) where there is enough space at the moment and also in future for history files. You should select the biggest drive that is connected to the system.

- If there is more than one suitable drive available use D:\ or E:\, using system drive (C:\) to store history files in is **not recommended**.

Click **Next** to continue installation.

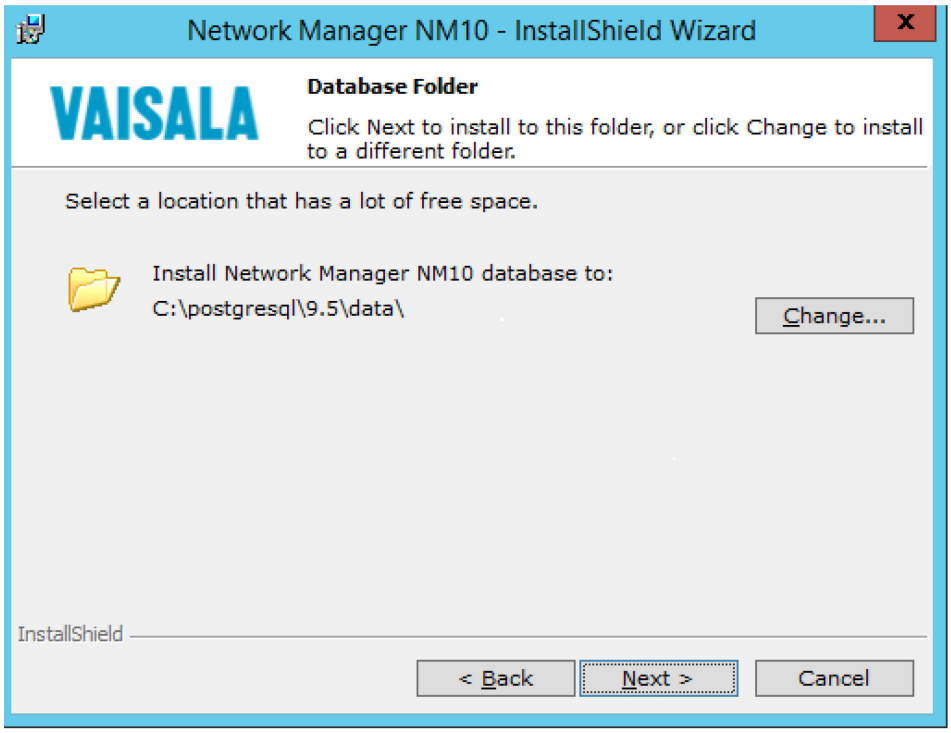


9. Select **Small monitoring network installation** for the installation type and click **Next**.

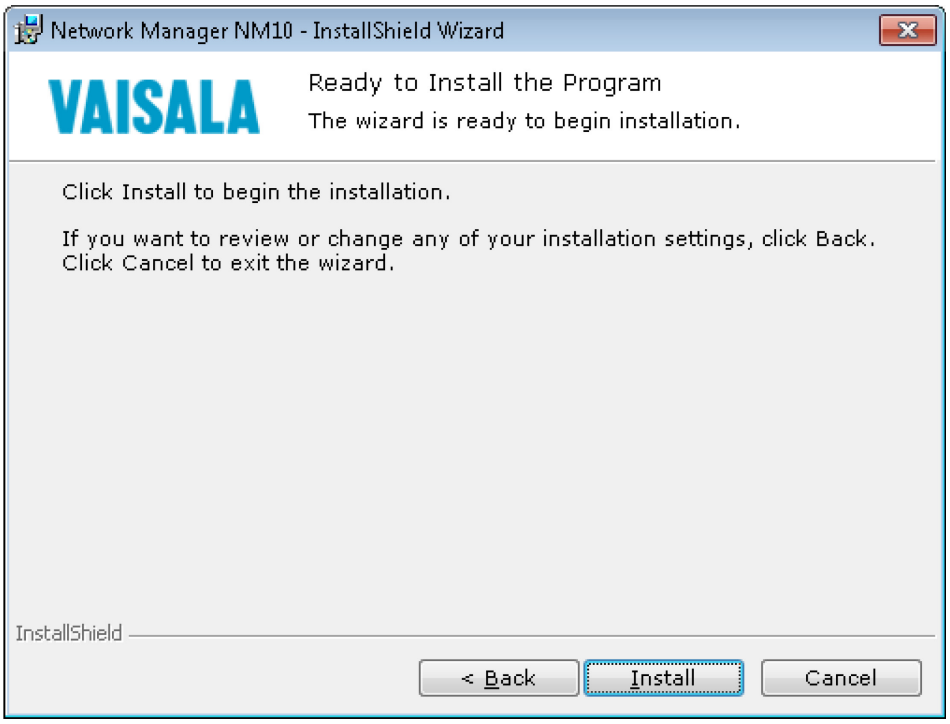


10. Select a location for the database.
    - Select a location (drive) where there is enough space at the moment and also in the future. Click **Next** to continue installation. You should select the biggest drive that is connected to the system.
    - If there is more than one suitable drive available, use D:\ or E:\, using the system drive (C:\) is **not recommended**.

Click **Next** to continue installation.

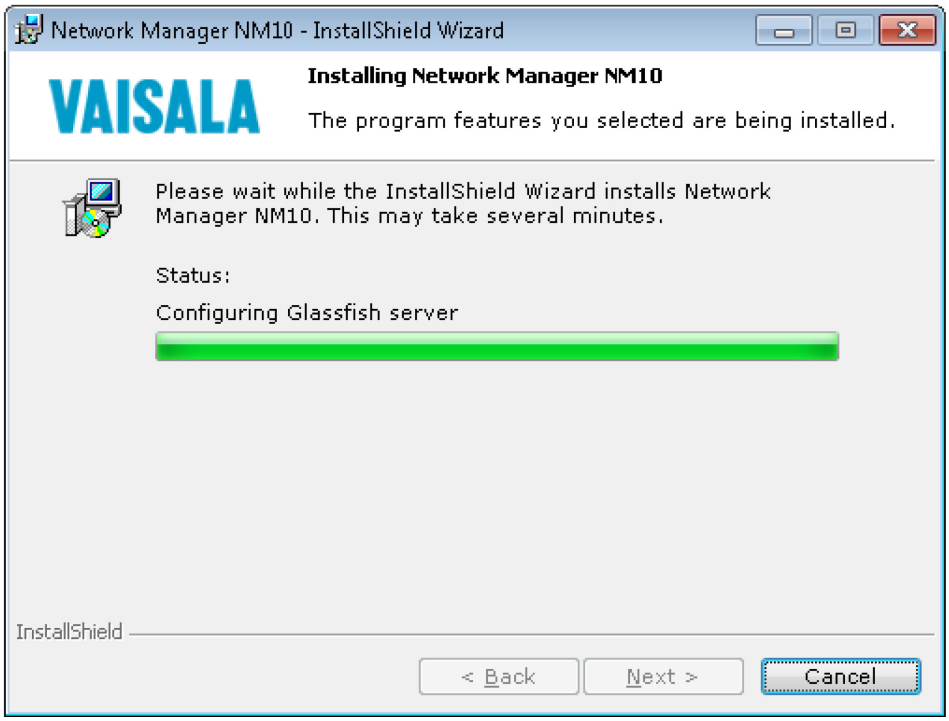


11. After the settings start the installation by clicking **Install**.

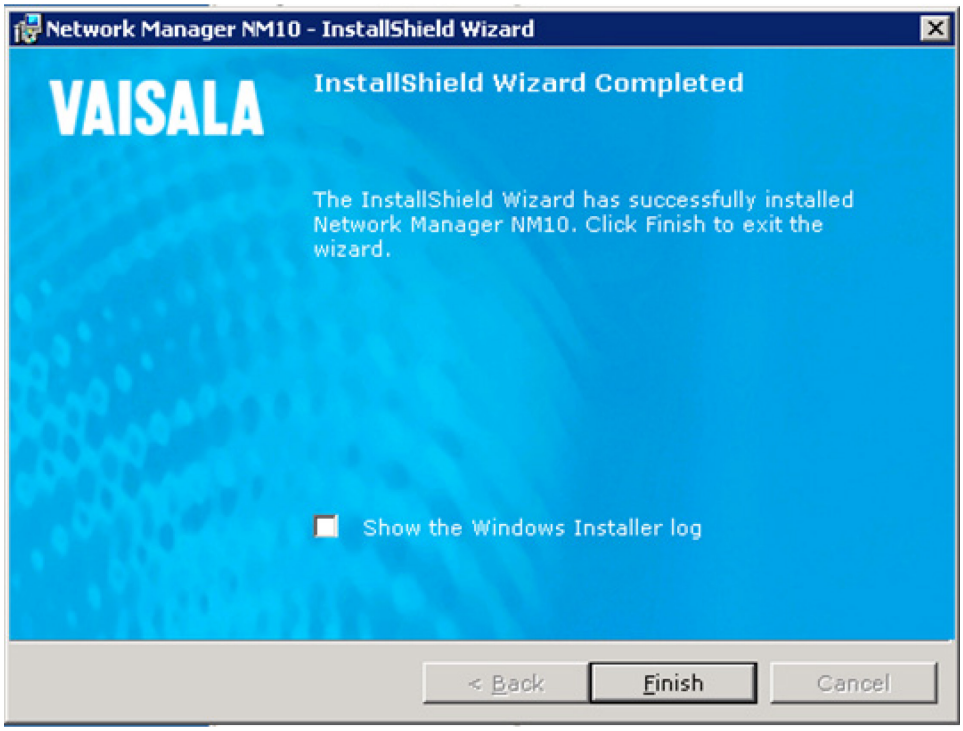


12. Installation starts. Wait for it to complete the installation. The installation process takes about 30 minutes.

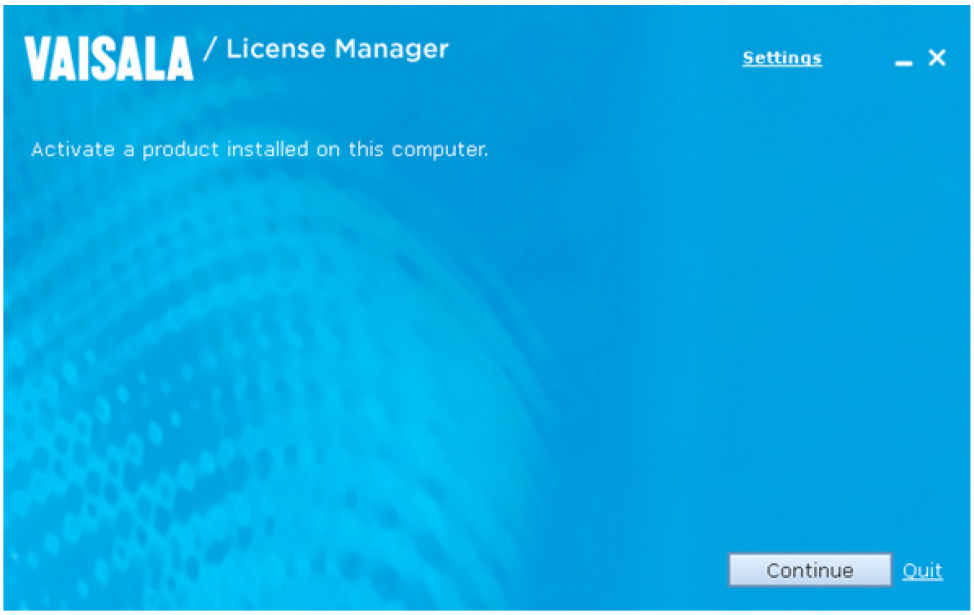
NOTE	If installing from DVD, there will be a note about the missing map material. For installing the map files, see Chapter 12, Installing Map Database from DVD, on page 65.



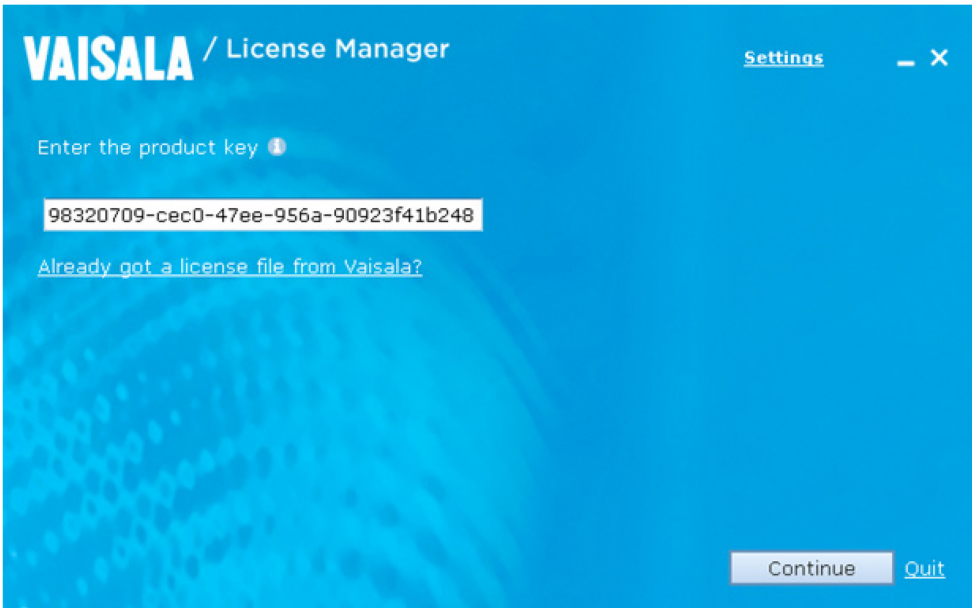
13. After the installation click **Finish**.



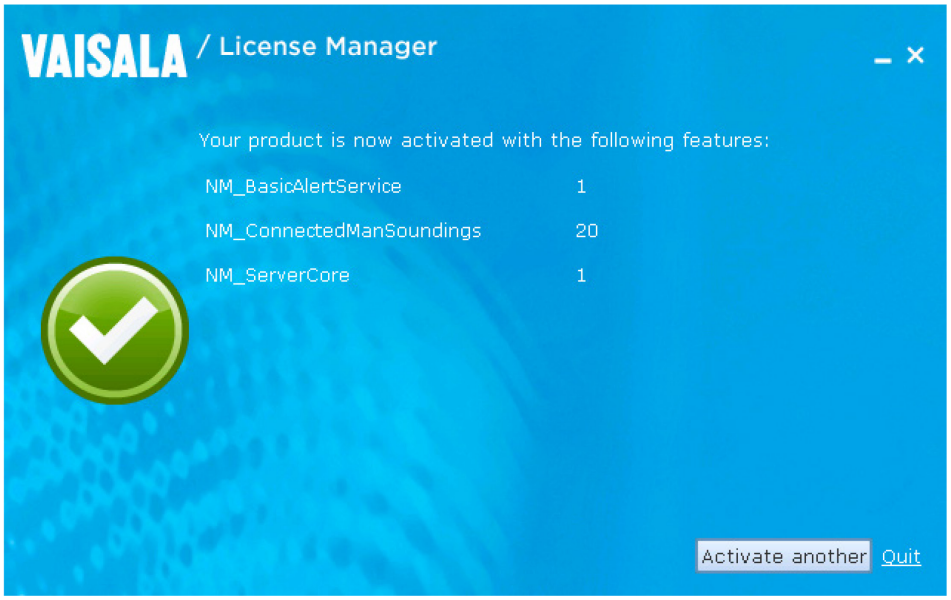
14. When the installation is finished, License Manager is automatically opened. If for some reason this does not happen or License Manager is closed before the license is activated, License Manager can be started from the **Start** menu > **All programs** > **Vaisala** > **Vaisala License Manager** > Vaisala License Manager.
15. Click **Continue**.



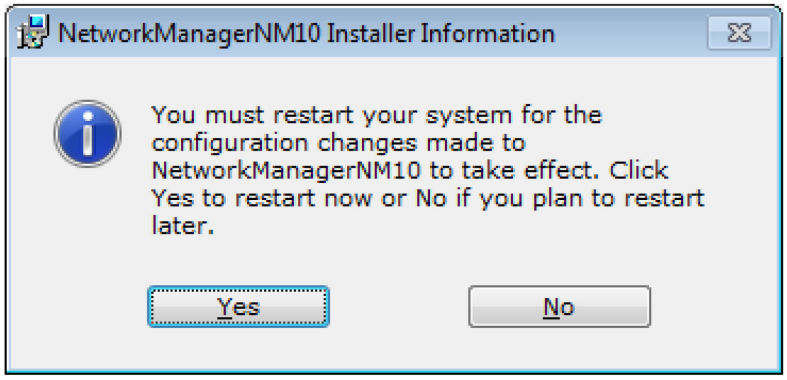
16. Enter the product key in the appropriate text field and click **Continue**.



17. Confirmation of the successful activation with the included features is shown. Check that the information corresponds to the sales order. Click **Quit**.



18. After License Manager configuration is closed, remove the workstation from the Vaisala network and set the static IP address for the workstation. Use 192.168.1.11 if the customer does not provide valid IP address.
19. Reboot the system after IP change, click **Yes** to reboot.



20. After the system has restarted, make sure that NM10 workstation and MW41 workstations are in the same network.
21. Verify that the services on the workstation are correctly up and running by opening a web browser at the workstation with the address *https://<hostname>/nm10/login* .
    a. When connecting to the Network Manager for the first time, there is a prompt to accept unsafe connection. Accept the connection.

    b. Login as **admin** with password **#4dMin:36,** to https://localhost/nm10/login

NOTE	The comma is a part of the password.

    c. If your license includes the Map feature, verify on the Map page that the map images are received.

    d. Verify that there are no alarms (no red alarm in page header).

CHAPTER 4

CONNECTING

4.1. Configure etc/Hosts

When connecting MW41 LOCAL WORKSTATION to Network Manager you need to add the MW41 LOCAL WORKSTATION IP address and DNS name to Network Manager workstation's

C:\Windows\System32\drivers\etc\hosts file.

You also must remember to add the Network Manager IP and DNS name to MW41 LOCAL WORKSTATION workstations

C:\Windows\System32\drivers\etc\hosts file.

Hosts file can only be edited when using the text editor in administrative mode, as saving the edited file without admin privileges is restricted. To open the Notepad in admin mode, open the **Start menu**, type "notepad" in the search field and right click the notepad.exe. Select **Run as Administrator** from the menu.

The edited hosts file should look something like this:

```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
        192.168.1.12       MW41HOSTNAME1
        192.168.1.13       MW41HOSTNAME2
        192.168.1.14       MW41HOSTNAME3
```

After saving the hosts file, test the connection by connecting to the MW41 web UI from remote workstation using a web browser with address post

.

4.2. Certificates

By default NM10 installer will create certificates for NM10 frontend and NM10 backend. Certificate will be valid for 30 years.

4.2.1. NM10-Backend Certificates

Keystore used by nm10-backend can be found from *C:\Program Files (x86)\Vaisala\NetworkManager\config\keystore\xxxxxx_nm10_backend.jks*.

4.2.1.1. Importing Trusted Certificates into NM10-backend Trust Store

In order to create M2M (Machine-to-Machine) connection between NM10-backend and other systems, NM10-backend must trust the certificates provided by other systems. There is a directory

C:\Program Files (x86)\Vaisala\NetworkManager\config\jdcp_conf\certificates

which should contain all certificates or related CA certificates which are to be trusted by nm10-backend.

During Network Manager installation, certificate provided by WEB server will be automatically copied under

C:\Program Files (x86)\Vaisala\NetworkManager\config\jdcp_conf\certificates

and connection between NM10 backend and WEB server will not need any additional configuration.

However when connecting with MW41, we need to copy certificate provided by MW41 under

C:\Program Files (x86)\Vaisala\NetworkManager\config\jdcp_conf\certificates

manually. If you do not have the MW41 certificate in your possession, you can export the certificate using web browser and then copy the certificate file under

C:\Program Files (x86)\Vaisala\NetworkManager\config\jdcp_conf\certificates

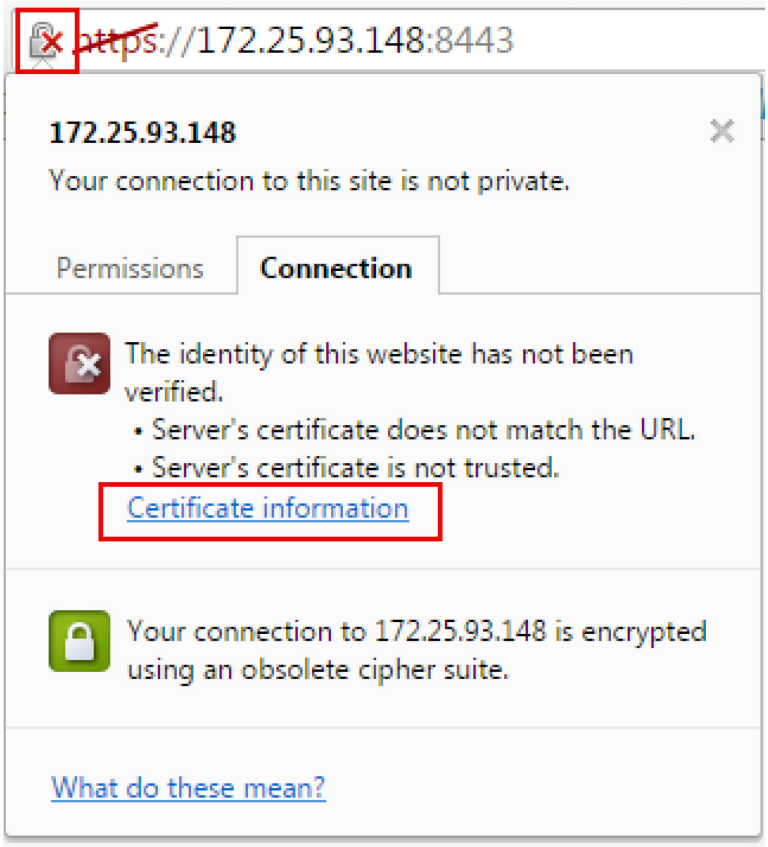
on NM10 workstation.

NOTE	Later on if MW41 certificate needs to be replaced, the old certificate must be removed from directory *C:\Program Files (x86)\Vaisala\NetworkManager\config\jdcp_conf\certificates*, the new certificate file placed there instead, and NM10-backend service restarted.

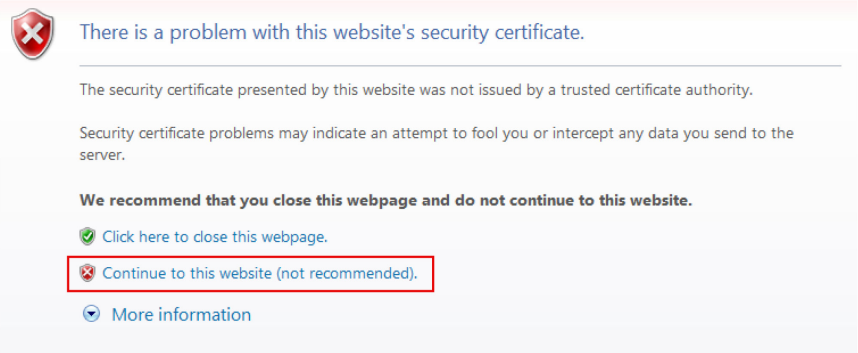
The following example will show how to get MW41 certificate via Internet Explorer and Chrome:

1. Open web browser and navigate to:
   https://<MW41_address>:8443

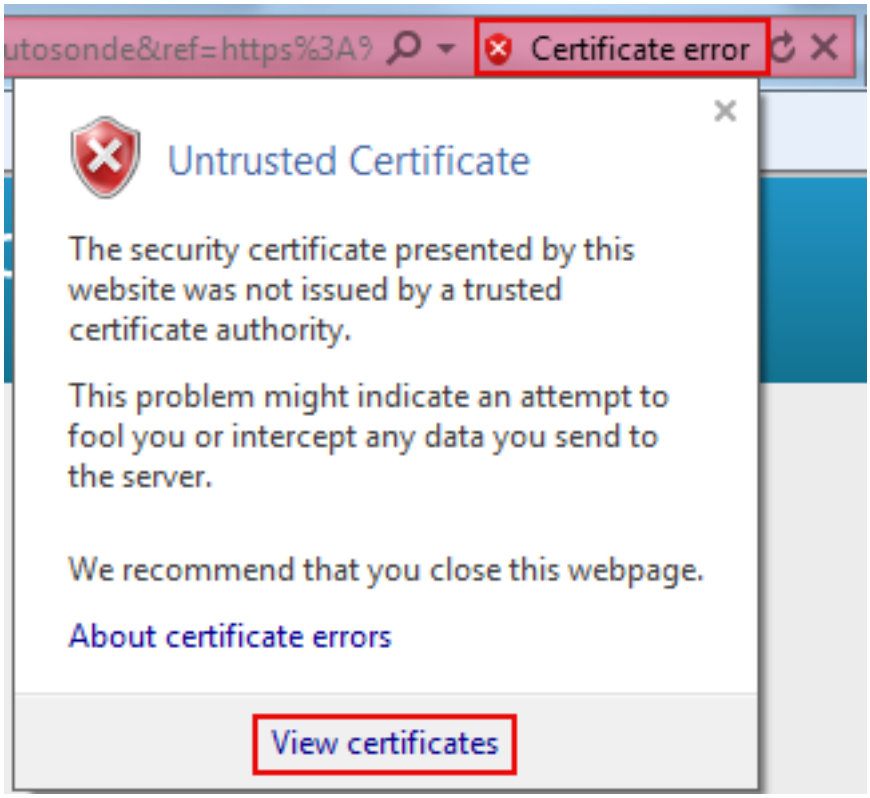
2. View the certificate provided by that address:
   - In Chrome:
     Click the lock icon in address bar and then click **Certificate information**.



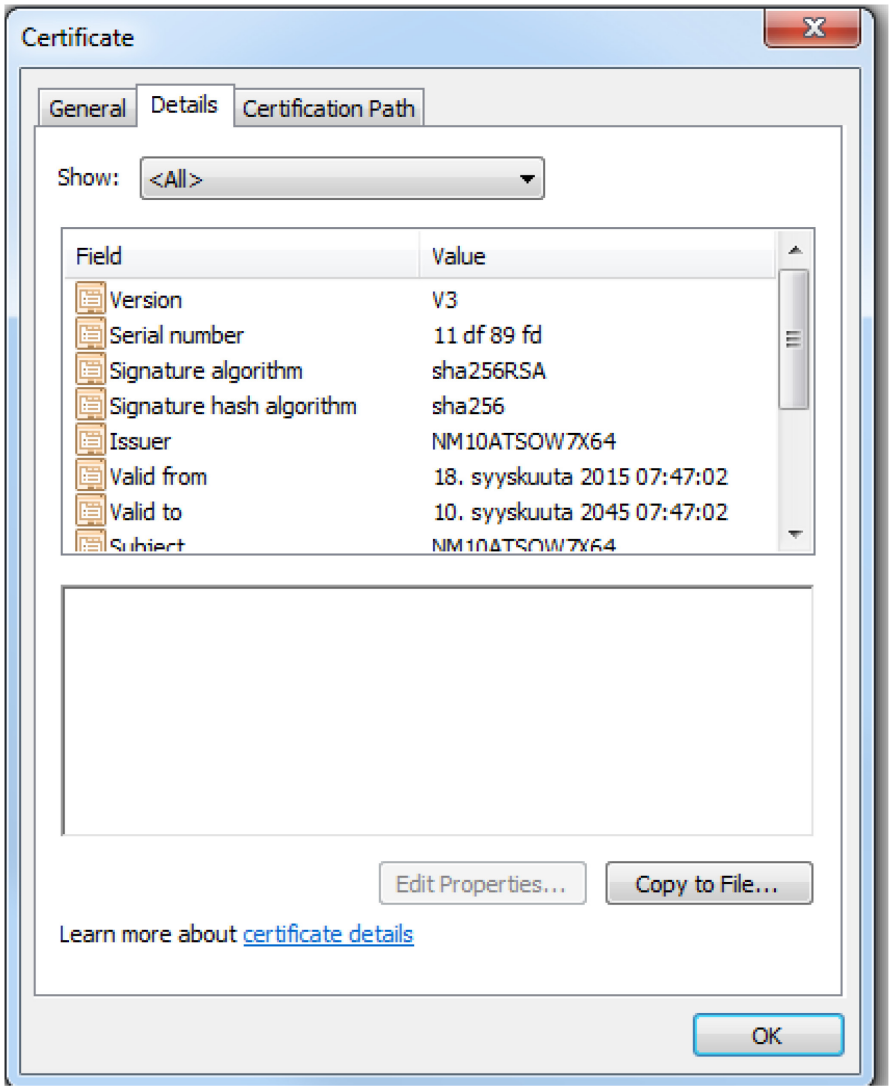
   - In Internet Explorer:
     Click **Continue to this website**.



and then click the **Certificate error** in address bar and **View certificates**.

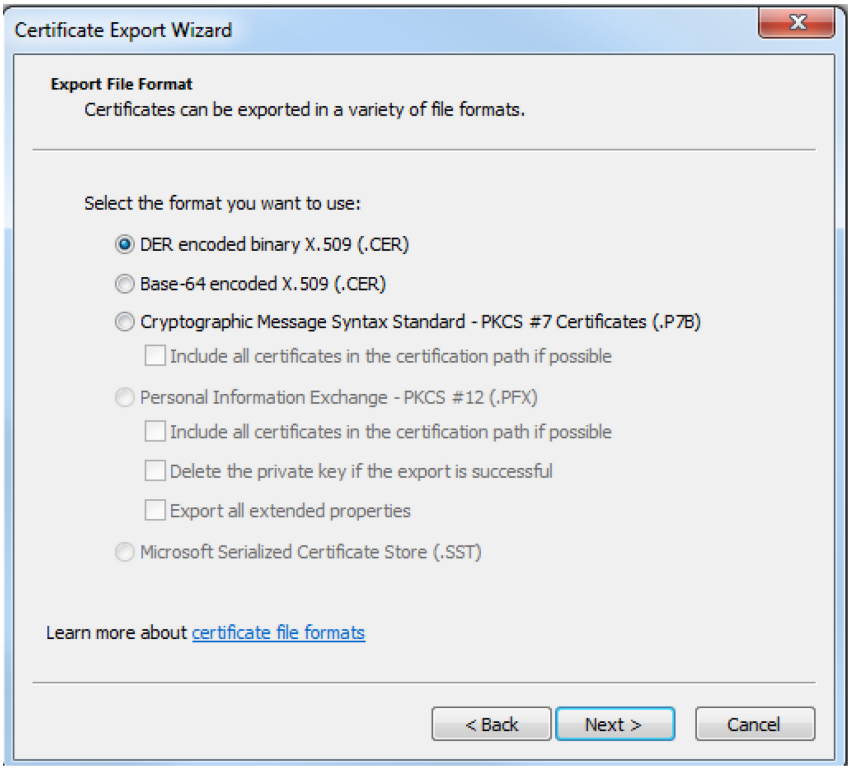


3. Export the certificate using the wizard provided by the browser. From the opened dialog select **Details** tab and click **Copy to File** to open the certificate export wizard.

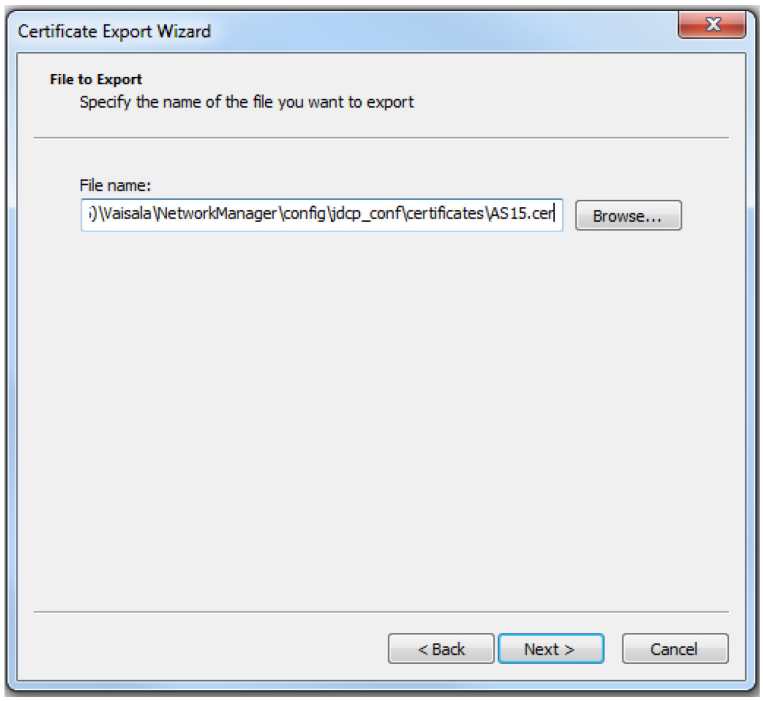


4. On the first page select **Next**.

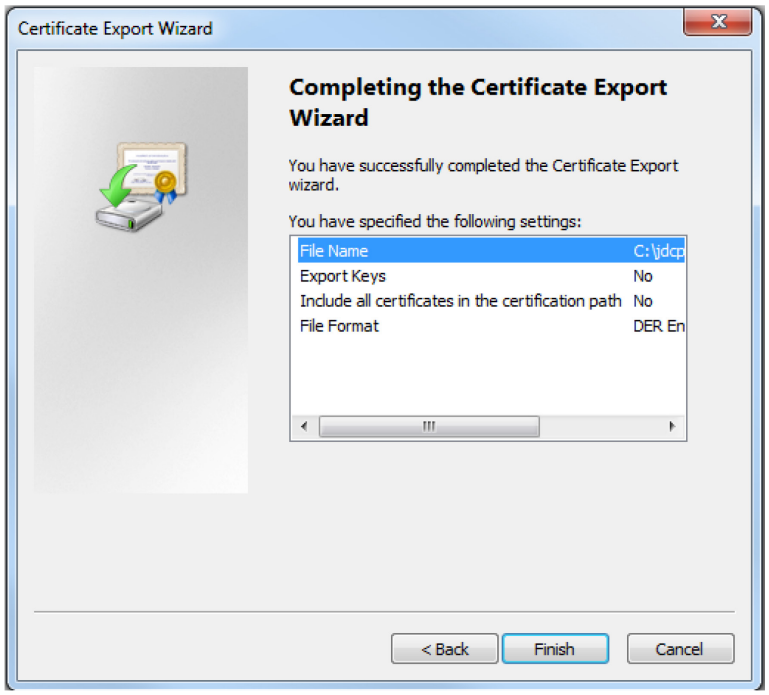
5. Network Manager supports X.509 standard certificates so select the first or the second format and click **Next**.



6. Click the **Browse** button and navigate to *C:\Program Files (x86)\Vaisala\NetworkManager\config\jdcp_conf\certificates*. Give a unique name for your certificate file (MW_sitename.cer) and click **Save**. Then click **Next**.



7. In the wizard summary page click **Finish** to create the certificate file.



8. After a while you should get an event to NM10 Web UI events page (Trusted certificate '<certificate_name>' was added.), informing that your certificate has been successfully imported into Network Manager trust store.

4.2.1.2. Importing Trusted Certificates into MW41 Trust Store

You need to import the NM10 backend certificate to MW41 trust store to provide the two-way trust. For this you have to log in to the MW41 LOCAL WORKSTATION and get the NM10 backend certificate in the same manner than was done in the last step:

1. On the MW41 local workstation open the web browser and navigate to https://<NM10_address>:8443/
2. Ignore the prompt for credentials and view and export the certificate provided by that address as instructed earlier.
3. Copy the exported certificate to the MW41 local workstation folder *C:\ProgramData\MW41\observation-network-manager\trusted-servers*.

   The ProgramData folder is hidden, so it might be necessary to select to show the hidden files and folders in **Tools** > **Folder Options** > **View** > **Show hidden files**.

4. Restart the service **MW41 Software Monitor** from the service console.

4.2.2. Problem Solving

If NM10 or MW41 provided certificates have expired you will experience following problems:

- MW41 certificate expires: No effects in current version.
- NM10 certificate expires: remote systems can no longer register, update registration or send events to NM10.

4.3. Authentication Keys

NOTE	It is mandatory to configure MW41 system parameters before connecting MW41 to Network Manager. At least GPS location, altitude and site name have to be set.

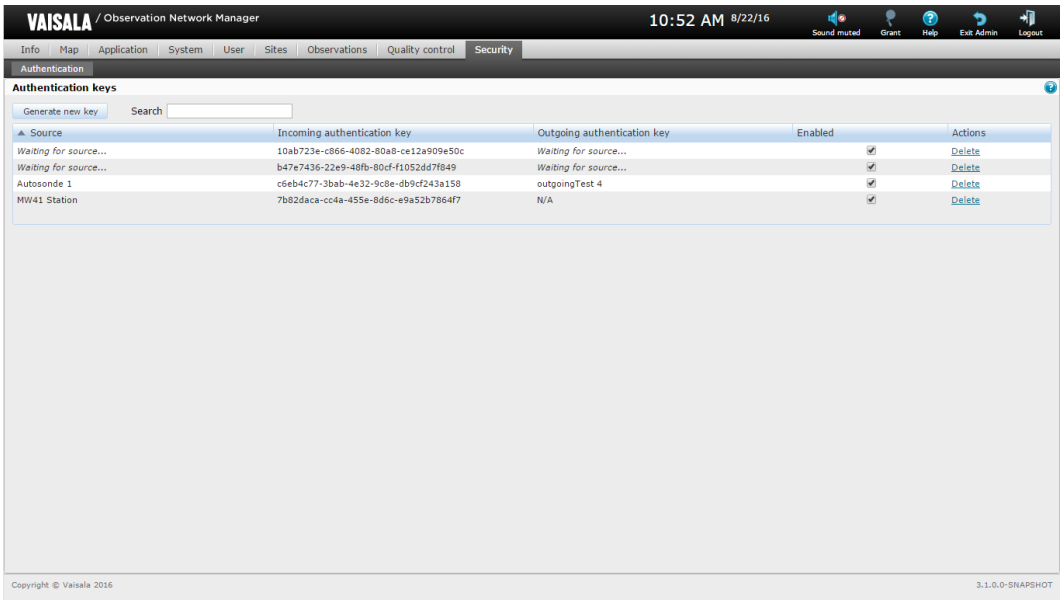
Authentication keys are like username and password that allow access to NM10 REST interfaces that remote systems like MW41 use to communicate with NM10.

Before authentication can be done with authentication keys, systems must have imported certificates:

- NM10-backend certificate -> MW41
- MW41 certificate -> NM10

It is also mandatory to configure MW41 system parameters before connecting MW41 to Network Manager. At least location, altitude and site name have to be set.

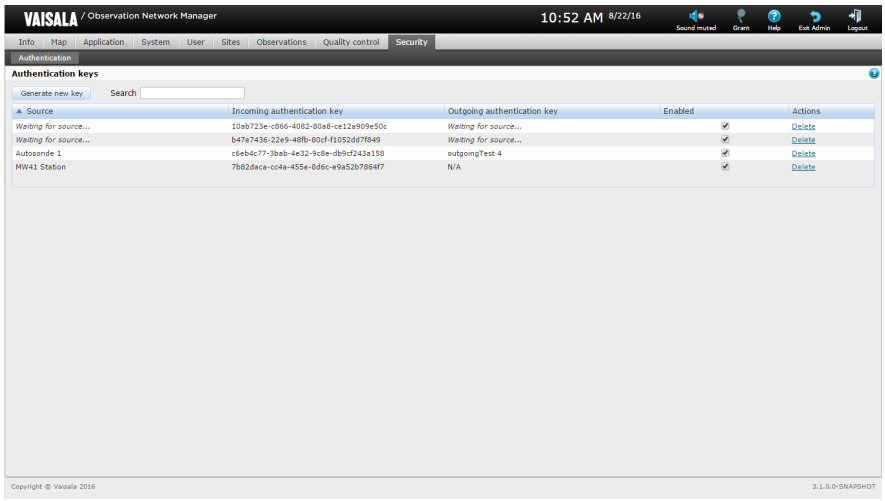
To view, create or manage the authentication keys in NM10, log in as an Admin, go to the admin view from the header and open the **Security** tab.



4.3.1. Authentication Key Creation

1. Log in as admin.
2. Open the **Admin** > **Security** > **Authentication** tab in NM10.

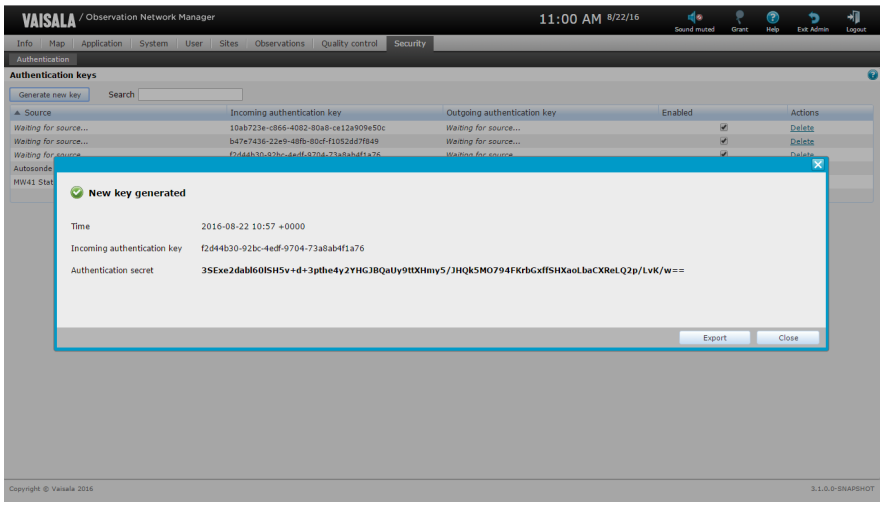
3. Click the **Generate new key** button.



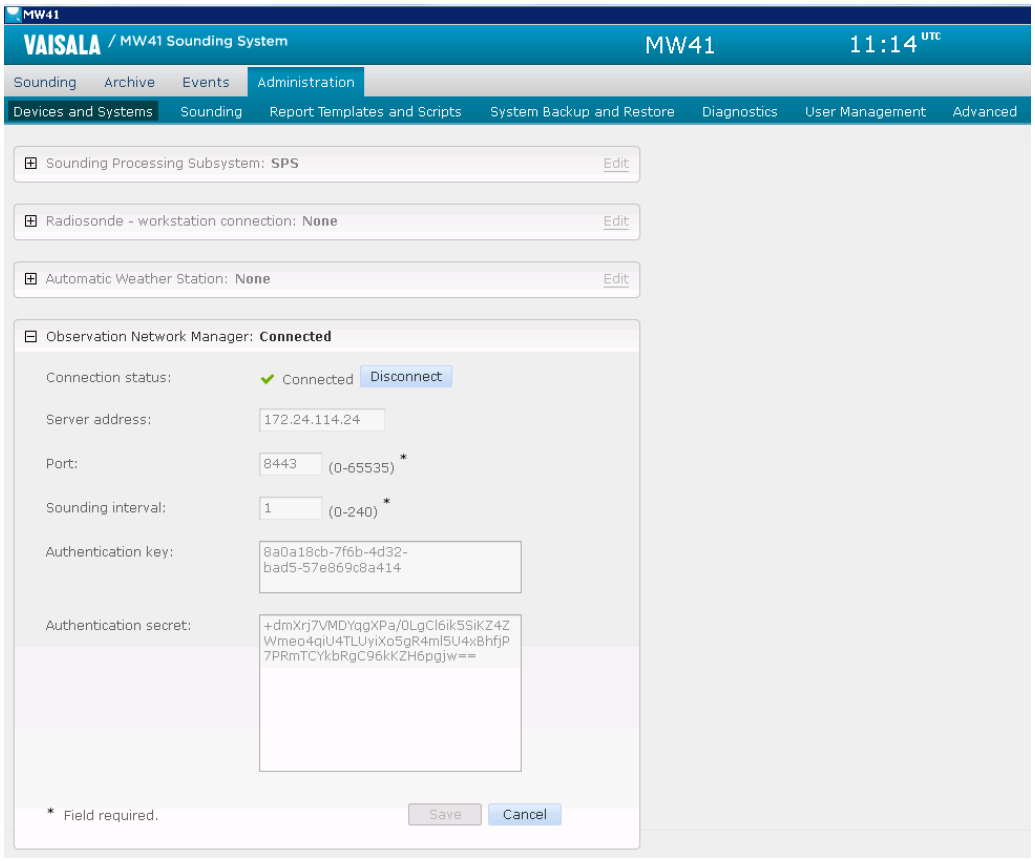
4. A pop-up window opens with the new key information. Click on the **Export** button to save the information to a text file for later use. Save the file as a text file to accessible location, like

c:\Program Files (x86)\Vaisala\NetworkManager\AuthenticationKey

NOTE	It is impossible to get the authentication secret after closing this window unless it is exported.



5. Log in to MW41 web UI and open **Administration** > **Devices and Systems > Observation Network Manager**.



6. Insert the NM10 hostname to the server address and 8443 to the port.
7. Sounding interval default value is 12 hours, change if needed.
8. Insert the Authentication key from the exported authentication key file to the **Authentication key** field.
9. Insert the Authentication secret from the exported authentication key file to the **Authentication secret** field.
10. Confirm that the MW41 site configuration has been done.
11. Click **Connect**.
12. Once the **Connect** button changes to **Disconnect**, the connection is established. To verify this go to NM10 web UI and refresh the **Admin** > **Security** > **Authentication** page. The MW41 name can be seen in the source field of the used key.

If authentication key is removed from NM10, the source registrations and events are not received from the source that used the removed authentication key.

Authentication key creation and managing is further described in NM10 online help.

4.3.2. Authentication Key Troubleshooting

Steps to verify when authentication fails when trying to connect a source:

- Verify that the MW41 name and location have been set correctly in the web UI. The name and location information is mandatory for the MW41 to register on Network Manager.
- Verify that that the authentication key and authentication secret are exactly as they appear when the key was generated. You can always delete the old unused key, generate a new one and attempt to use that.
- Verify from WEB UI that the key is not already in use by some other source. A key cannot be used for multiple sources. A key is unused if the **Source** column states "Waiting for source...". Attempt to register or update a source with an authentication key that is already in use will raise an event in the Events list: "Could not persist source: Authentication key already in use.".
- Verify from WEB UI that the key is not disabled.

CHAPTER 5

ADDITIONAL SOFTWARE AND CONFIGURATION

5.1. Installation of Additional Software

In addition to Network Manager you must install the following software from the NM10 installation media:

- **Bitvise** (Instructions in document: DOC232979)
- **Thinfinity** (Instructions in document: DOC232980)

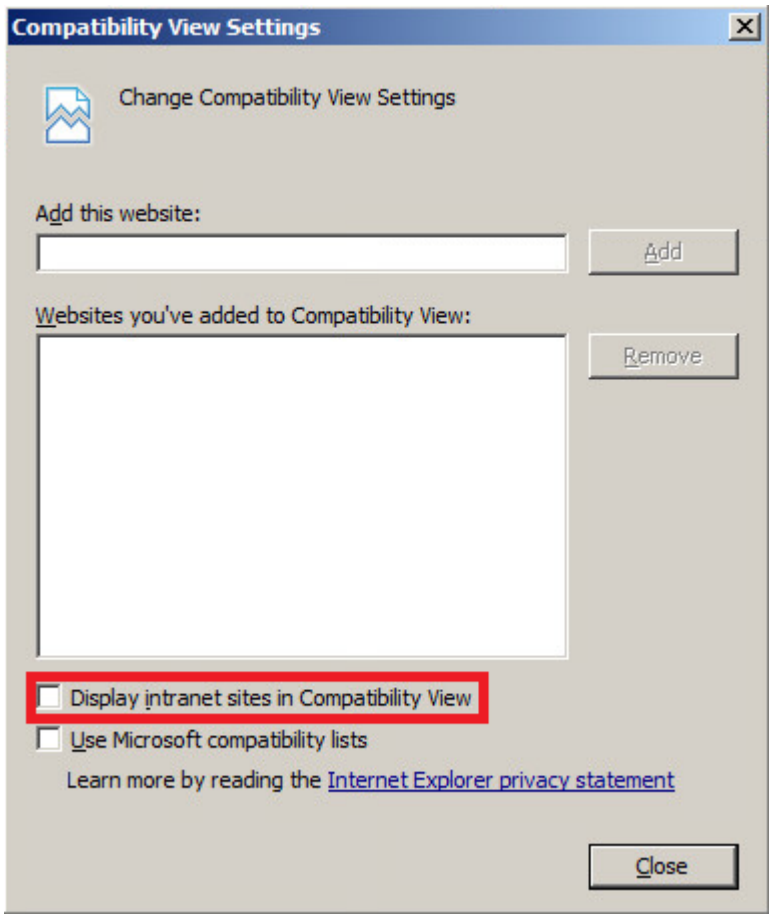
NOTE	Thinfinity is installed only on the MW41 LOCAL WORKSTATION. Bitvise is installed only on the REMOTE WORKSTATION.

5.2. Browser Compatibility View Settings

If you are using Internet Explorer 11 or later, the compatibility view settings are set on by default in a local network. This will cause problems with Thinfinity if the compatibility mode is not turned off.

To turn off the compatibility view, open the options from top right corner of the browser and select **Compatibility View settings**.

From the settings uncheck the **Display intranet sites in Compatibility view** and close the window.



CHAPTER 6

CONFIGURATION FOR SFTP

In Network Manager Bitvise SSH Server is used as a SFTP server. Bitvise SSH Server installation and configuration instructions can be found from document DOC232979. Network Manager does not read or modify files that are received with SFTP, it is used just to route files from MW41 systems to one or more customer systems.

Sending files from Network Manager can be done with FTP or SFTP. SFTP is recommended to be used if possible.

6.1. Receiving of Files

Bitvise SSH Server is only a tool to receive files, Network Manager knows it existence only by noticing that file(s) are appearing to directories that are configured for the file transfer jobs.

To forward those files to other locations you have to configure additional file transfer jobs from the Network Manager UI as a root admin.

6.2. File Housekeeping

Network Manager has functionality that removes files older than configured from directories. This configuration also affects directories where files are received with SFTP.

It is recommended to check and change those settings to fit the real needs. File housekeeping can be done from Web UI admin page **Storing Policy > Files**. Select the suitable storage period for received files and save the settings.

6.3. Configuring File Transfer Jobs

Network Manager supports many file transfer jobs that may have different scheduling, source directory or remote system (target where files are sent).

The transferred files are moved from the source directory to a working directory (by default *D:\NetworkManager\work*) once per minute, and sent from the working directory to remote systems when the scheduled file transfer job is triggered. If the file transfer fails, the file remains in

the working directory and it is resent until successful transfer is made. After the transfer is complete, the file is removed from the working directory.

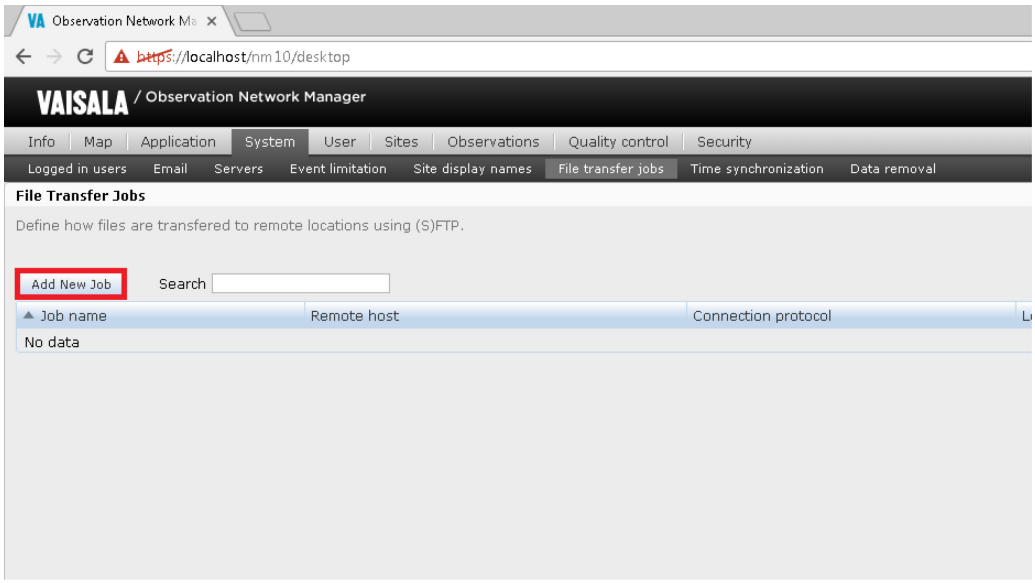
As Bitvise and Network Manager are very loosely coupled it is important to configure Bitvise SSH server user's directories and Network Manager file transfer job source directories correctly.

File transfer file filter supports * wild card, and that also expands to sub-directories, e.g. "*.log" will match files: "test.log" and "directory\test2.log" but "direct**.log" matches only "directory\test2.log"

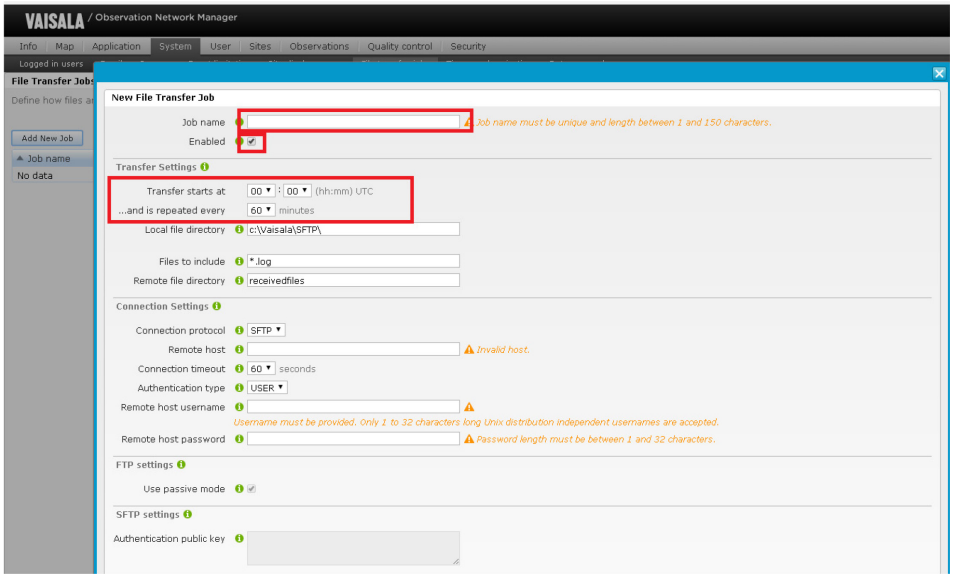
If some files are received to directories that are set for jobs, but file filter does not match with file names then warnings are written to JDCP_server.log. It is recommended to check JDCP log files and/or file receiving folders after configuring file transfer jobs and receiving files from MW41 systems.

To configure a file transfer job:

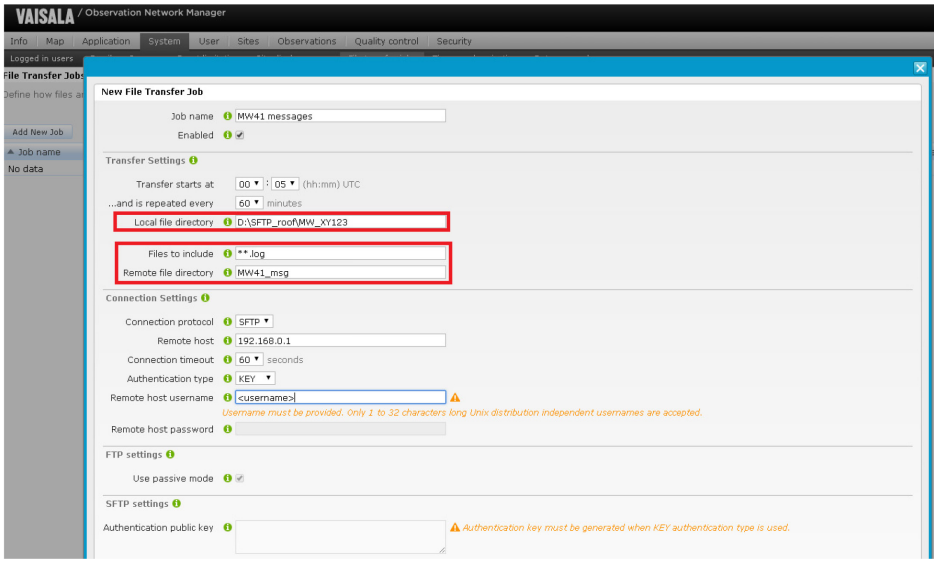
1. Log in as a root admin, go to **Admin > System** > **File transfer jobs** and click the **Add New Job** button.



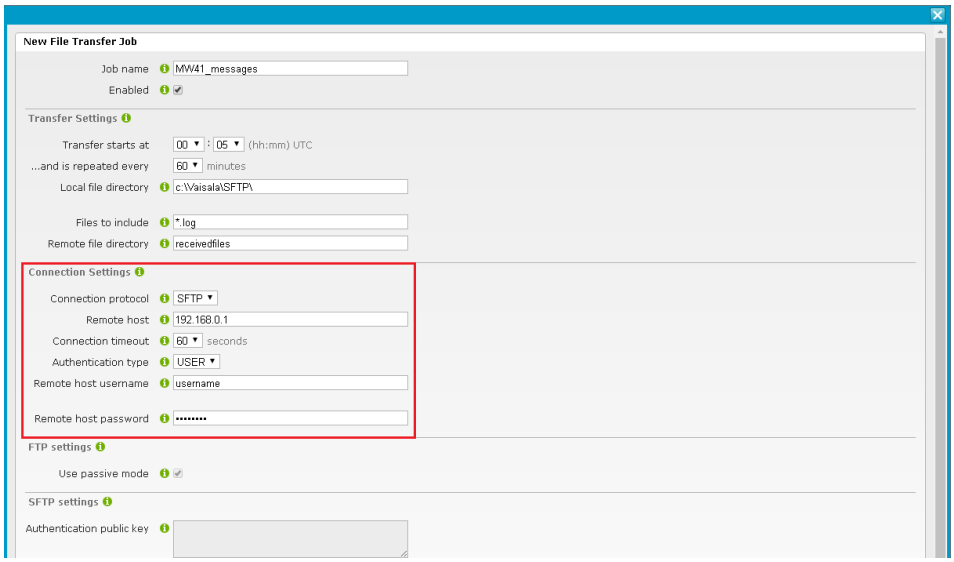
2. In the **New File Transfer Job** window enter a unique job name, check that the job is enabled and set the transfer schedule. Using the MW41 site name as a part of the job name is useful when handling several file transfer jobs later.



3. After the scheduling is set, define the local (source) file directory where the files to be sent are located. You can select which files to include, using the wildcards as explained before. Also you can define the directory where the files will be sent on the remote (S)FTP server.

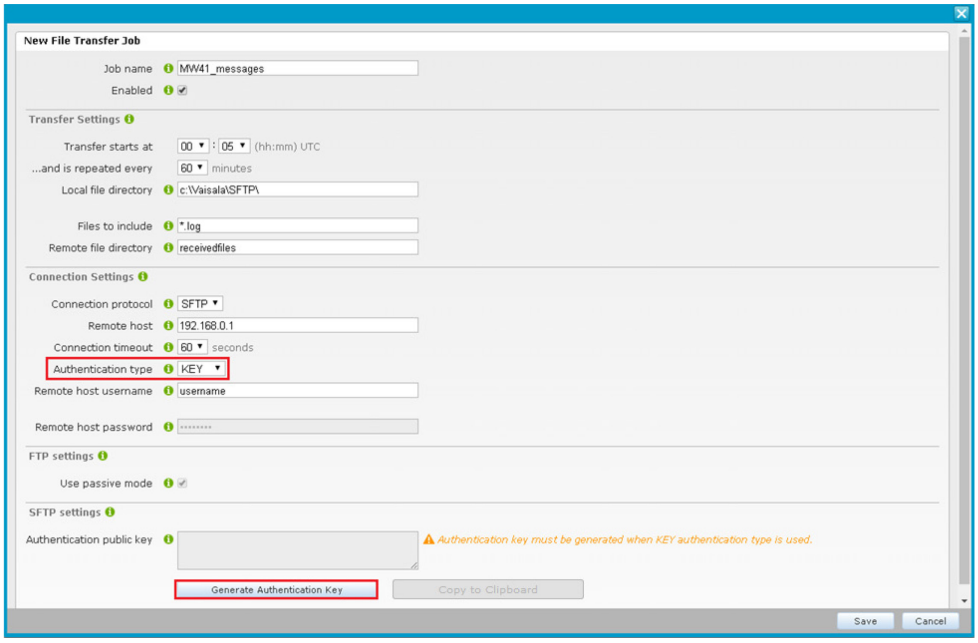


4. Configure the connection settings next. For this you have to know the remote host address, and the authentication information (either username / password with USER type of authentication or username / public key with KEY authentication). If USER authentication is used the configuration is complete and can be saved by clicking the **Save** button on bottom right corner.
   - If using KEY type of authentication, proceed to next step.

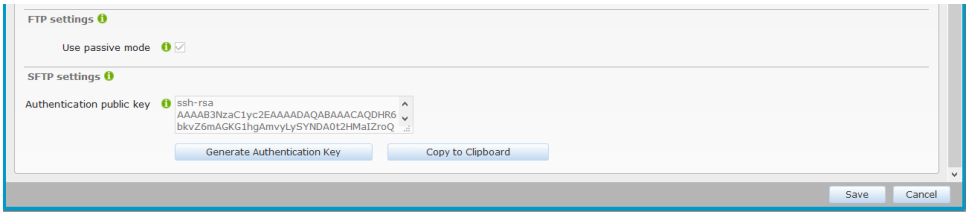


5. If KEY type of authentication is used, the authentication public key has to be created on Network Manager and imported to the remote SFTP server. Please consult the remote host SFTP server guide for the import process.

   The key can be created from the SFTP settings if the KEY authentication type is selected. Click the **Generate authentication key** button.



6. Insert an authentication key comment if you want to have identifiable information on the key. This is not mandatory. Click **Generate**.
7. Public key is generated to the text field under the STFP settings. Copy the key text by selecting **Copy to Clipboard**.



8. Copy the public key to a text editor and save it to be used on the remote host authentication key import process.
9. Confirm that the file transfer job works by adding a mock file to the local file directory matching the files to include filter. Wait until the scheduled file transfer is started and confirm that the file can be found on the remote host in the defined directory.

Table 2 Things To Check in Problem Cases

Type	Where	When	What
Folder	D:\NetworkManager\work	Files are not sent to the remote system with FTP or SFTP, but Files are received with Bitvise SSH Server.	If files are coming to the sub directories of the work directory, the files are not sent to the remote system. Is the network connection working to the remote system? Is remote FTP or SFTP server running?
Folder	C:\Program Files (x86)\Vaisala\NetworkManager\glassfish3\glassfish\domains\domain1\logs	Files are not sent to remote system with FTP or SFTP, but Files are received with Bitvise SSH Server.	Log files can contain entries that relate to file sending or selecting files to be sent.
Application	Bitvise SSH Server	No files received to NM10.	Check activity log. Activity log should contain information when connection is made from remote system (MW41). If such log entries are not found, then problem may be in remote system (configuration?), network between Network Manager and remote system (MW41) or firewalls between those systems.
Folder	Bitvise users directories	No files received to NM10.	Check users locations from Bitvise SSH Server control application, and check if those directories contain files. If there are correct files then problem may be in file transfer job configuration source directory (should match to Bitvise SSH Server users home directory) or in file filter.

6.4. File Transfer Security

Network Manager now supports two protocols for transferring files, FTP and SFTP. As FTP is sending authentication information and all data without encryption it can expose customer's credentials and data. Because of this FTP should not be used anywhere outside customer's network unless connection is through secure VPN tunnel.

CAUTION SFTP should always be preferred whenever possible. In case FTP has to be used, the security has to be provided by other means.

The most secure combination is to use SFTP with Key authentication.

CHAPTER 7

CONFIGURING SOUNDING NOTIFICATIONS AND AUDIO MESSAGES

Notification messages (a.k.a. toasts) may be displayed on top of the application header and other page content to inform the user about new sounding events and alerts. Notifications can be displayed when the sounding system sends events about the main sounding phases, alerts about problems, or when messages have been generated. In addition to a toaster text, an audio message can be played consisting of a severity beep sound and a prerecorded spoken message.

The notification text message is defined in the event / alert received from a sounding site. These event / alert messages are localized in all supported languages. Notification audio messages are played from pre-recorded spoken message files mapped to event/alert code or severity. Currently, spoken audio messages are only available in English and Japanese. For other languages, English audio messages are used.

Instructions for enabling and configuring notifications and related audio can be found from the online help:

1. Login to Web UI as admin.
2. Click **Help** icon on the application header.
3. Form help Contents menu, click **Administrator View** > **Managing System Settings** > **Configuring Sounding Notifications and Audio Messages**.

In order for a user to see the notifications, all of the following must be true:

1. User is logged in.
2. Desktop view is open (not Admin view).
3. A sounding event/alert is received from a sounding site.
4. Notification message has been configured and enabled for the incoming event/alert type (find instructions below).
5. Sounding site is visible for the user's organization (see the next chapter for more details).
6. Received event/alert timestamp is 'fresh enough'.

7.1. Event/Alert Mapping in Different AUTOSONDE Versions and in MW41

Events and alerts sent by sounding systems vary by the sounding site type and version. When in doubt, it should be safe to add a new notification configuration for all available triggering event/alerts.

However, the new AUTOSONDE release (1.3) sends both “sounding completed successfully” and ‘‘sounding terminated” events that have been mapped to identical Japanese spoken messages. In this case, just choose “sounding completed successfully”. See the following table for more information about notification triggers.

Table 3 Notification Trigger – AUTOSONDE and MW41 Event/Alert Mapping

Triggering Event / Alert	MW41	AUTOSONDE 1.2.1	AUTOSONDE 1.3	Notes
VAI_SO_SOUNDING_PREPARATION_ STARTED	X	X	X	
VAI_SO_BALLOON_READY_FOR_ RELEASE	X	X	X	
VAI_SO_BALLOON_REMOTE_ RELEASE_PERMISSION		X	X	
VAI_SO_BALLOON_RELEASED	X	X	X	
VAI_SO_100HPA_LEVEL_REACHED	X	X	X	
VAI_SO_ACCEPTANCE_LEVEL_ REACHED	X	X	X	
VAI_SO_MESSAGE_GENERATED			X	
VAI_SO_SOUNDING_COULD_NOT_ BE_PERFORMED		X	X	Japanese audio message: "sounding terminated with issues"
VAI_SO_SOUNDING_COMPLETED	X			Japanese audio message: "sounding terminated successfully". **Note**: MW41 Accepted YES/NO is mapped to the same notification spoken message.
VAI_SO_SOUNDING_COMPLETED_ SUCCESSFULLY			X	Japanese audio message: "sounding terminated successfully"
VAI_SO_SOUNDING_TERMINATED		X	X	Japanese audio message:

Triggering Event / Alert	MW41	AUTOSONDE 1.2.1	AUTOSONDE 1.3	Notes
				"sounding terminated successfully"
VAI_GEN_EMERGENCY_SWITCH_ PRESSED		X	X	
Other sounding events and alerts (Warning): WARNING -severity	X	X	X	
Other sounding events and alerts (Alarm):				
VAI_SO_SOUNDING_PREPARATION_ FAILED, or		X	X	
VAI_GEN_MESSAGE_GENERATION_ FAILED, or	X	X	X	
VAI_GEN_MESSAGE_TRANSMISSION _FAILED or	X	X	X	
ALARM -severity		X	X	

7.2. Configuring Expiration Time

In order to prevent displaying old events/alert as notifications, events older than 30 minutes are not shown as notifications. To change this event "expiration time":

1. Go to web UI configuration directory, e.g. *C:\Program Files (x86)\Vaisala\NetworkManager\config\webui_conf*
2. Open **vsoweb-client.ini** (e.g. Edit with Notepad++)
3. Scroll to **[notificationSettings]**
4. Set **maxNotificationEventAgeInMinutes**
5. Save changes
6. Restart **Vaisala nm10-frontend Apache Tomcat s**ervice

The maximum number of concurrent visible notifications is 10. When the notification bar displays 10 notifications, oldest notifications are automatically replaced with the latest received. The maximum number of visible notifications is not currently configurable.

CHAPTER 8

CONFIGURING VISIBLE SOUNDING SITES FOR USERS

Organization members can be configured to see only specific sounding sites. Basic steps for this are:

1. Login as root admin.
2. Configure the sounding site(s).
3. Select the visible sounding sites for an organization: In Admin view: **User > Organizations** > **Edit**, or **Add New Organization**.
4. Verify that users belong to the correct organization. In Admin view: **User > Users**

In **root** organization all sites are always visible. By default, the **guest** user belongs to the root organization. To limit the visibility sites for the guest user, move the guest to a another organization. See section 11.8 Changing Organization for Guest User on page 61.

CHAPTER 9

POST INSTALLATION TESTS

These tests are supposed to be executed after connecting the MW41 to NM10 system. They do not replace the FIT/FAT tests, but validate the basic functionality and configuration of MW41 and NM10 systems.

NOTE	The following are available depending on the purchased licenses.

9.1. Map View

9.1.1. Instructions

1. Open the NM10 web UI: https://<hostname>/nm10/desktop
2. Open the Map tab.
3. Click on the MW41 site icon on the map.
4. Close the MW41 site detail window.

9.1.2. Expected Results

1. NM10 web UI is opened and no login is required.
2. Map tab is opened, world map can be seen and the configured number of MW41 sites is displayed on the map. The location of the sites on the map match the coordinates configured to each MW41.
3. The MW41 site detail window is opened, containing all the events sent from the site after the registration. At least the info event containing message "Source registered." is seen. There are no links to AS15, MW41 or RDP in the bottom of the window.
4. Site detail window is closed.

9.2. MW41 List View

9.2.1. Instructions

1. Open the NM10 web UI login page: https://localhost/nm10/login

2. Log in as a user with credentials user/user123.
3. Open the **Soundings** tab.
4. Click on the MW41 site name on the list.
5. Close the MW41 site detail window.

9.2.2. Expected Results

1. NM10 web UI login page is opened.
2. Login is successful and web UI is loaded.
3. **Soundings** tab is opened and all the configured sites are listed on the page.
4. The MW41 site detail window is opened, containing all the events sent from the site after the registration. At least the info event containing message "Source registered." is seen. There are links to MW41 (Sounding Data) and RDP in the bottom of the window if the MW41 site configuration included those.
5. Site detail window is closed.

9.3. External Links

This test case is only applicable if the site has the corresponding features enabled.

9.3.1. Instructions

1. Open the All Measurements page on NM10 UI while logged in as a user.
2. Click on the MW41 site name.
3. Click on the Sounding data link on the bottom of the site detail window.
4. Insert the MW41 credentials and log in to the UI.
5. On the NM10 UI click on the **Sounding Data** link on the bottom of the site detail window.
6. On the NM10 UI click the **Remote Desktop** link on the bottom of the site detail window.
7. Insert the Thinfinity admin credentials. These credentials were set when installing Thinfinity.
8. Select **Remote Desktop** and click **Connect**.
9. Insert the MW41 workstation/server credentials (these are the normal Windows credentials).
10. Disconnect from the MW41 workstation/server from the **Start** menu / more options next to **Log Off / Disconnect**.

9.3.2. Expected Results

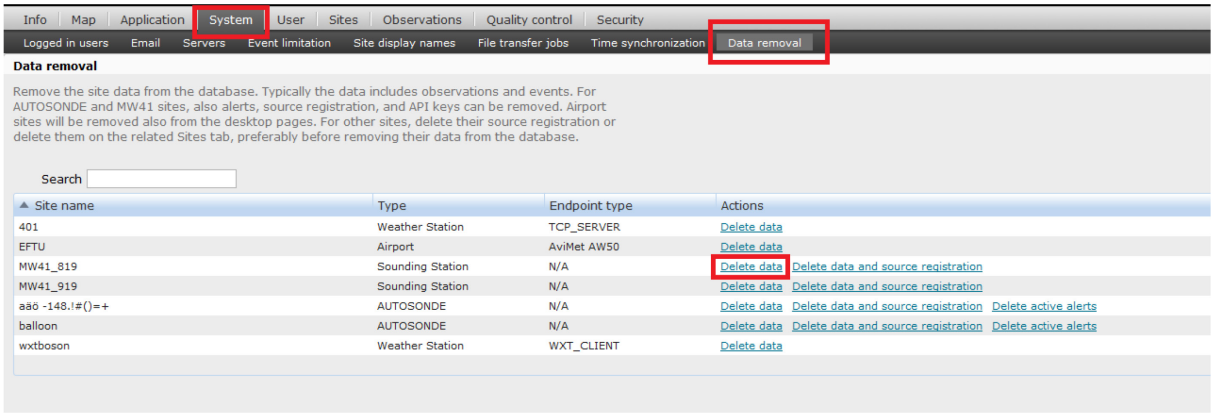
1. All Measurements page is opened, all the configured sites including the MW41 are listed.
2. MW41 site detail window is opened, there are links to, Sounding Data and Remote Desktop available on the bottom of the window.
3. MW41 web UI login screen is opened in a new browser tab.
4. Credentials are accepted and the MW41 web UI is opened.
5. MW41 web UI is opened in a new browser tab. No login is required as the MW41 web UI login is still valid.
6. New tab is opened and there is a pop up window asking for credentials to the remote host.
7. Credentials are accepted and the Thinfinity remote access selection page is opened to the new tab.
8. The Thinfinity selection page is replaced by a pop up window asking for remote access credentials.
9. Credentials are accepted and remote connection is opened to the browser window.
10. Connection to the remote host is closed.

CHAPTER 10

SYSTEM CLEAN UP AFTER FIT/FAT(/SAT)

Delete the alerts and events created during testing:

1. Log in as administrator.
2. Switch to admin view by clicking **Admin** in the page header.
3. Go to **System** tab and click **Data removal**.
4. Click **Delete data** for the site. This deletes only events and alerts. Source registration and authentication keys will not be deleted.



Deleting data for a site can take several minutes if there is lots of data in the database.

10.1 After Data Removal

NM10 workstation should be restarted to verify data is cleaned and everything is working correctly.

CHAPTER 11

ADDITIONAL TOPICS

11.1. What to Do When Installation Fails or Installation is not Working Correctly

11.1.1. Services

Table 4 Services

Service (or process) name	Description
Geoserver 2.5.2	Provides standard map material
VBoxHeadles.exe (process)	Provides enhanced map material
VBoxVmService	Provides enhanced map material
VONMPostgreSQL	Observations and back-end configuration
VONMPostgreSQL	Web UI configuration, user information
VONMPostgreSQL	Standard map material
Vaisala nm10-frontend Apache Tomcat	Server web UI application
domain1 GlassFish Server	Process observations and stores those to database
Vaisala nm10-backend Apache Tomcat	Handles sources and events coming from other systems
Vaisala Remote Object Events	One of core DCP roa services
Vaisala Remote Object Monitor	One of core DCP roa services
Vaisala Remote Object Persistent	Handles DCP ini file configuration for other DCP services
Vaisala Remote Object Server	One of core DCP roa services
Vaisala Formatter Service	With default configuration not in use.
Vaisala ASCII Database Service	Creates raw ascii logs from alarms and observation messages
Vaisala Data Collection Service	Handles data post collection checks and requests
Vaisala DB Inserter Service	Used to mark checked handled data gaps from data post collection
Vaisala DB Query Service	Used to check data gaps for data post collection
Vaisala File Input Service	With default configuration not in use
Vaisala Message Parser Service	Old message parser service
Vaisala Quality Control Service	Old quality control service
Vaisala Sensor IO Service	Handles messaging to/from weather stations and AviMet observation messages
Vaisala Temp File Service	With default configuration not in use
Vaisala Sensor Time Service	Handles weather stations' time synchronizations
Vaisala Remote Object Connection	One of core DCP roa services

11.1.2. Configuration File Directories

NOTE	The paths can be changed with the installer, so these are only valid if default paths were used during installation.

Table 5 Default Configuration File Directories

Default Path	Description
C:\Program Files (x86)\Vaisala\NetworkManager\config	DCP configuration
C:\Program Files (x86)\Vaisala\NetworkManager\config\jdcp_conf	JDCP configuration
C:\Program Files (x86)\Vaisala\NetworkManager\config\webui_conf	WEB UI configuration
C:\Program Files (x86)\Vaisala\NetworkManager\glassfish3\glassfish\domains\domain1\config	Glassfish configuration
C:\Program Files (x86)\Vaisala\NetworkManager\nm10-backend\conf	Backend Tomcat configuration
C:\Program Files (x86)\Vaisala\NetworkManager\nm10-frontend\conf	Frontend Tomcat configuration

11.1.3. Log Information

NOTE	These are only valid if default paths were used during installation.

Table 6 Log Information Directories

Default Path	Description
C:\Program Files (x86)\Vaisala\NetworkManager\glassfish3\glassfish\domains\domain1\logs	GlassFish logs. Also license and license usage information logged on startup and every full hour.
C:\Program Files (x86)\Vaisala\NetworkManager\glassfish3\glassfish\domains\domain1\logs\	JDCP specific logs. Also license and license usage information logged on startup and every full hour.
C:\Program Files (x86)\Vaisala\NetworkManager\nm10-backend\logs	Backend Tomcat logs. Also license and license usage information logged on startup and every full hour.
C:\Program Files (x86)\Vaisala\NetworkManager\nm10-frontend\logs	Frontend Tomcat logs
D:\postgresql\9.3\data\vonm\pg_log	PostgresSQL logs

More log information can be found from:

- Windows event log (**Event Viewer** > **Windows Logs** > **Application**)
- WEB UI events page, if problem is such that event list can be opened and there is events available

11.1.4. Other Tools for Diagnosing Problems

Table 7 Other Diagnostic Tools

Tool default location	Description
C:\Program Files (x86)\Vaisala\NetworkManager\pgsql\bin\pgAdmin3.exe	pgAdmin can be used to inspect database content and also monitor database connections (**Tools** > **Server Status**)
C:\Program Files (x86)\Vaisala\NetworkManager\bin\diagnostics.exe	Diagnostics can be used to find reasons for issues in DCP
C:\Program Files (x86)\Vaisala\NetworkManager\bin\vtermin.exe	Can be used to see information about Weather station and AviMet connections

11.1.5. Common HTTP Error Codes from WEB UI

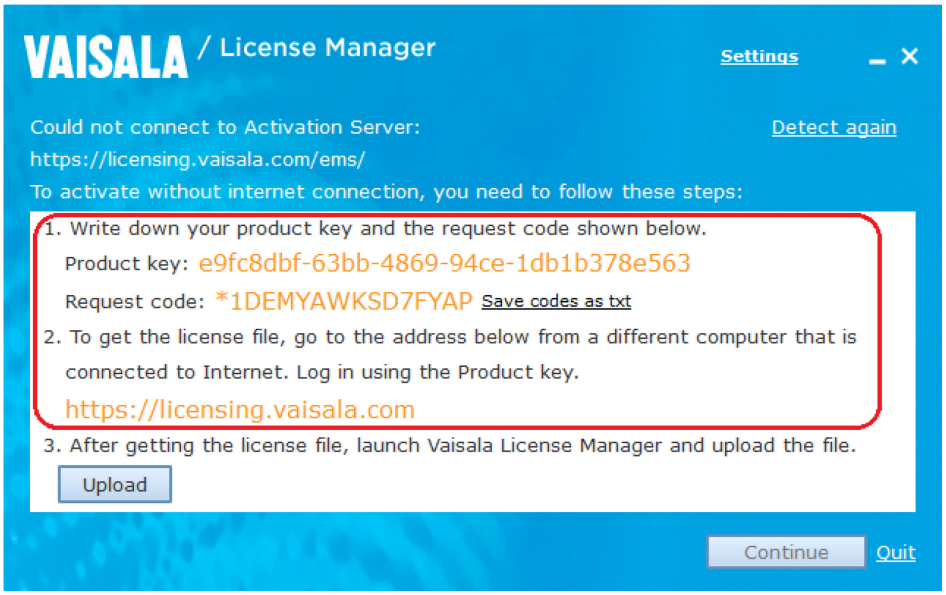
When trying to access NM10 WEB UI some error codes might be returned. Some are normal after installation or system reboot.

Table 8 Common HTTP Error Codes

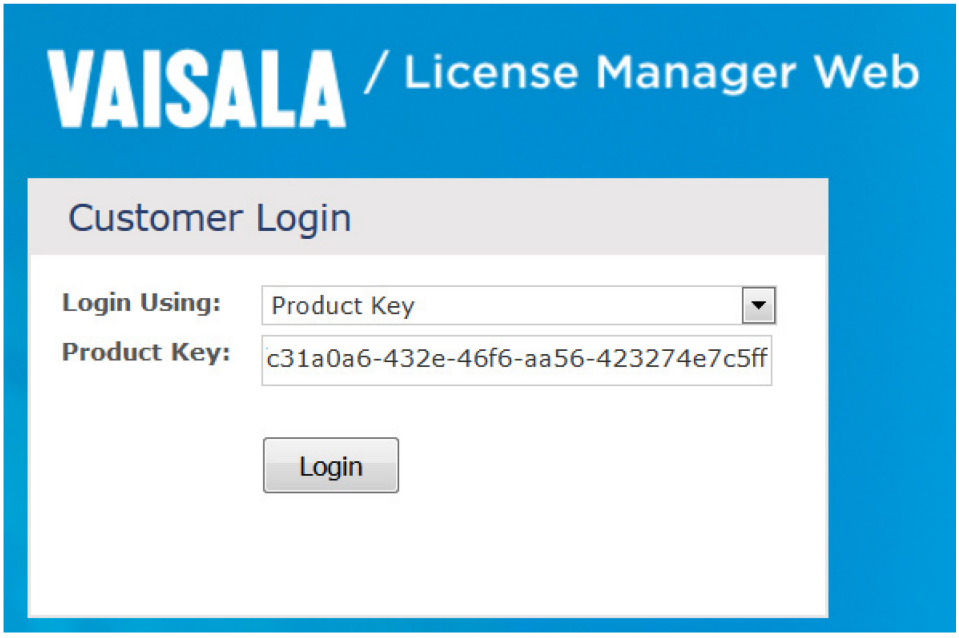
HTTP Status Code	Description
404	Requested source is not available. This can happen right after system restart (e.g. after installation). Wait 10 minutes and try again. If that does not help, follow system resource usage with Windows Task manager and if there are no high resource usage then: 1. Check that webui is deployed correctly 1. Open browser in workstation. 2. Open url https://localhost/manager (username: admin password: admin) 3. Check that applications list contains path **/nm10** and running status is **true** If **/nm10** is not found from applications list (i.e. not deployed) then inspect frontend Tomcat logs mentioned earlier in previous chapters.
500	Internal server error. Inspect frontend Tomcat logs mentioned earlier in previous chapters, there may be hints why this error code is returned. Make sure that service **VONMPostgreSQL** is running. If not, then start it and restart service **Vaisala nm10-frontend Apache Tomcat**.

11.2. Offline License Activation

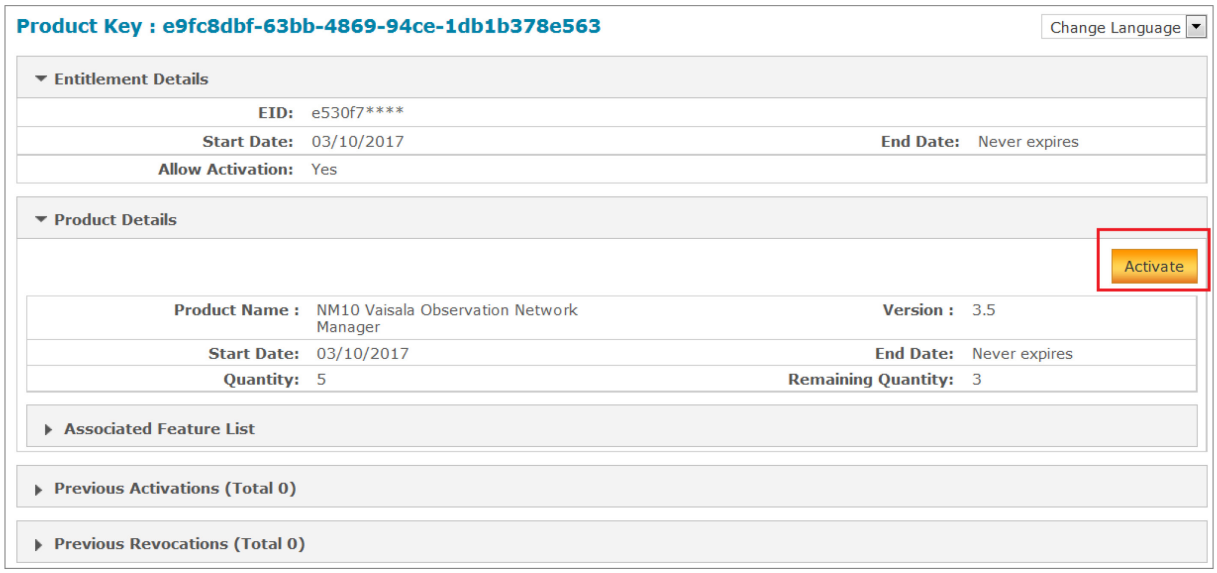
When following the official license activation instructions without a working internet connection, the notification about missing connection is opened:



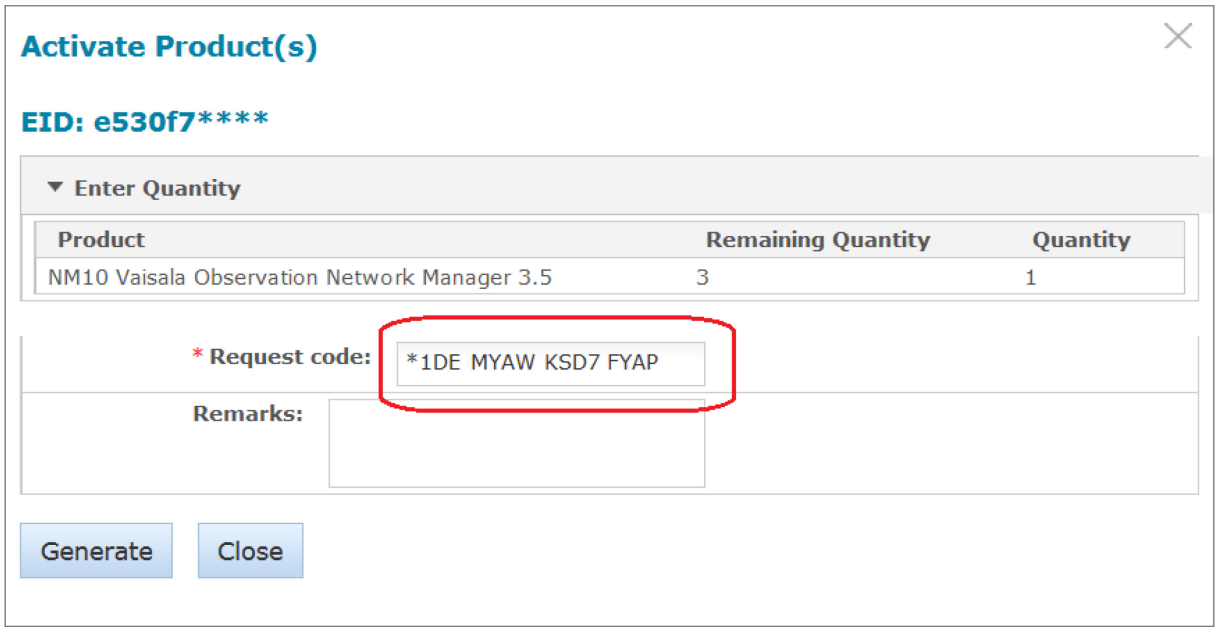
1. Follow the instructions in the window and copy the file from the license activation server to the workstation.



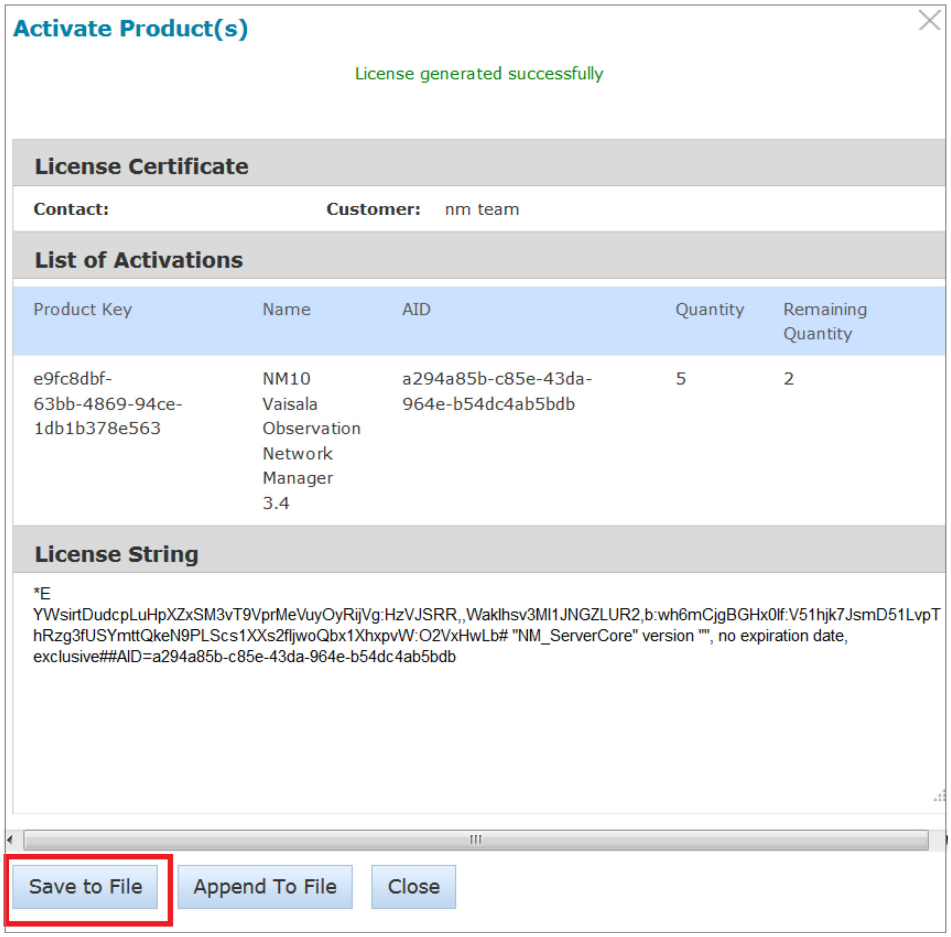
2. Click on the **Activate** button in the **Product Details** after logging in to the activation server.



3. Insert the Request Code from License Manager into the **Request code** field, manually add spaces after every 4 characters and click **Generate**.



4. Click the **Save to File** button to save the License String into a text file.



5. Copy the file you get from the activation to the NM10 workstation and upload it using the button on the License Manager. Continue as in normal license activation.

11.3. Web UI Certificate

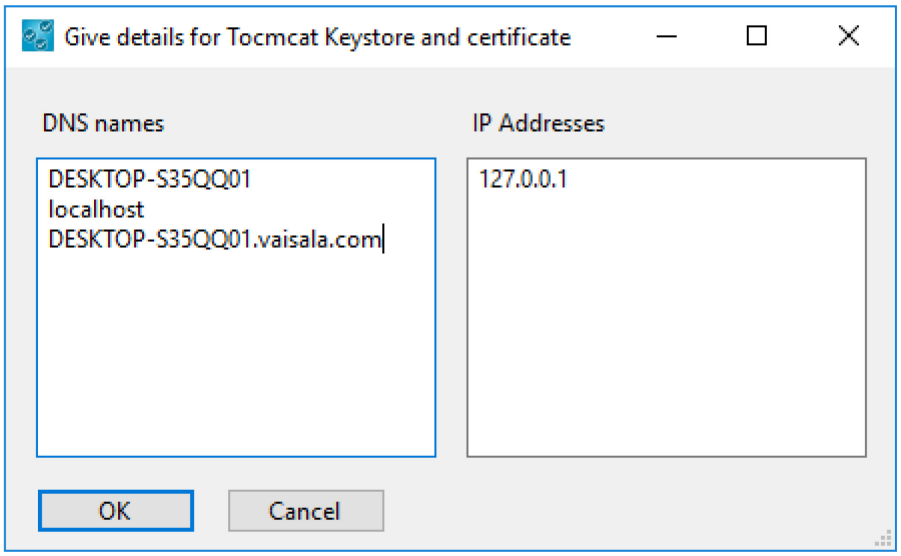
Web UI certificate is used when users connect to NM10 and when NM10-backend sends events to NM10-frontend.

If the “StartHere” installer is used to install NM10, certificates will be made automatically. If the hostname or domain name is changed after the installation, certificates should be renewed. There are different options for creating and/or taking the new certificates into use. The options are listed below. Options a) and b) are used to create new certificates for both NM10-frontend and NM10-backend. The rest of the options apply only to NM10-frontend.

11.3.1. Option A) Create a New Self-signed Certificate Using the Installer

1. Open the "StartHere" installer in the USB stick and select **Create self-signed SSL certificates**.

2. Enter all the needed hostnames and localhost to the left panel and IP addresses including 127.0.0.1 to the right panel:



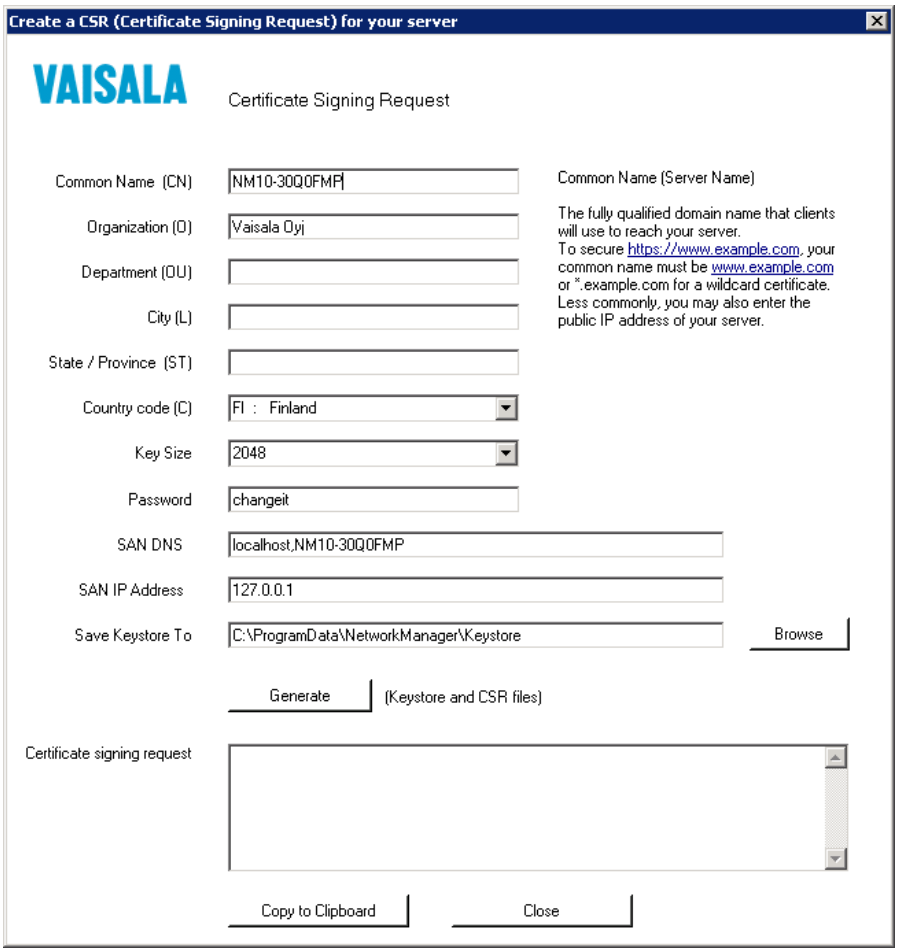
3. StartHere.exe will create keystores and certificates for both NM10-frontend and NM10-backend. Creating new certificates by StartHere installer will require only to manually change new domain/hostname name in server.xml files if computer hostname was also changed after NM10 installation.

4. Proceed to section 11.3.4. Taking New Keystore and Certificates to Use, Refreshing and Restarting Services on page 54.

11.3.2. Option B) Taking a Commercial or a Certificate Signed by the Customer Company's Own CA into Use Using the Installer

1. Open the "StartHere" installer from the USB stick or DVD and select **Create Certificate Signing Request (CSR)**.

2. Fill in the information for the certificate signing request similarly to the screenshot below.

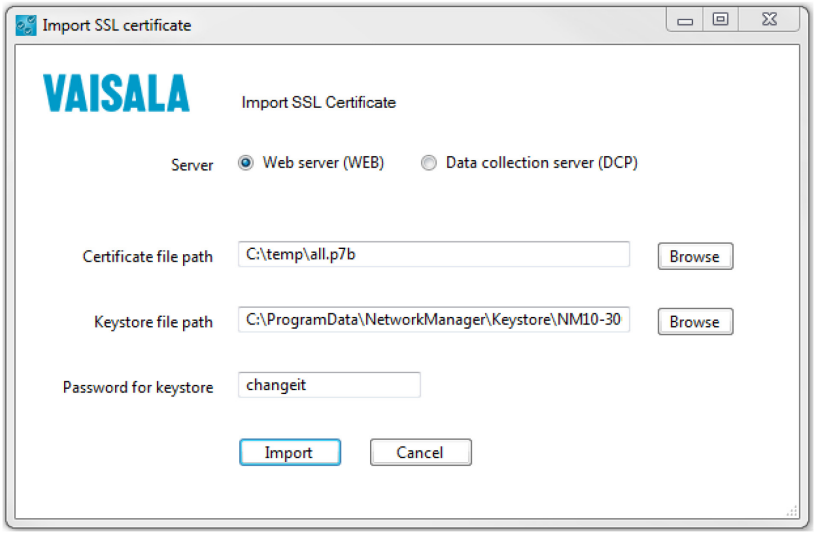


3. Click **Generate** to generate the keystore and the certificate signing request.

4. Send the CSR file or the CSR from the clipboard to a commercial certificate authority or a customer company's own certificate authority from which you will receive the signed certificate.

5. When you have received the signed certificate from the certificate authority, open the "StartHere" installer and select **Import SSL certificate**.

6. Fill in the information similarly to the screenshot below. For the server option, to import a certificate for nm10-frontend, select **Web server (WEB)**. To import a certificate for nm10-backend, select **Data collection server (DCP)**. In the case of a commercial certificate it is ok if the certificate file has a different file extension from what is shown in the screenshot below.



7. In the case of a certificate signed by the customer company's own CA, you need to have a .p7b certificate file that contains all the needed certificates: customer company's root certificate (ca.crt), customer company's intermediate certificate (intermediate.crt) and the signed certificate itself. If you don't have a .p7b file but you have the needed certificates separately, you can run the following commands from the command line to create a .p7b file.

```
openssl x509 -inform der -in ca.crt -outform pem -out ca.pem
openssl x509 -inform der -in intermediate.crt -outform pem -out
intermediate.pem
openssl crl2pkcs7 -nocrl -certfile ca.pem -certfile
intermediate.pem -certfile nm10srv.example.com.cer -out all.p7b
```

8. Finally, restart the NM10 frontend service to take the new certificate into use.

11.3.3. Updating Certificates

If a certificate has expired, create a new certificate using the same steps that were used to create the old certificate.

11.3.4. Taking New Keystore and Certificates to Use, Refreshing and Restarting Services

NOTE	You do not need to do this if option b) was used to create the new web UI certificates.

Modify two server.xml files.

Locations of server.xml file for frontend:

```
C:\Program Files (x86)\Vaisala\NetworkManager\nm10-
frontend\conf\server.xml
```

NOTE	New frontend certificates does not have affect to MW41 connections.

Open server.xml file by notepad++ or notepad. Find **keystoreFile="C:\Program Files (x86)\Vaisala\NetworkManager\config\keystore\NMINST1_nm10-frontend.jks"** and edit "**NMINST1**" to match current hostname

Locations of server.xml file for backend:

```
C:\Program Files (x86)\Vaisala\NetworkManager\nm10-
backend\conf\server.xml
```

NOTE	When new backend certificate and keystores are taken in use then new NM10 backend certificate needs to be installed to MW41 systems.

Open server.xml file by notepad++ or notepad. Find **keystoreFile="C:\Program Files (x86)\Vaisala\NetworkManager\config\keystore\NMINST1_nm10-backend.jks**" and edit "**NMINST1**" to match current hostname

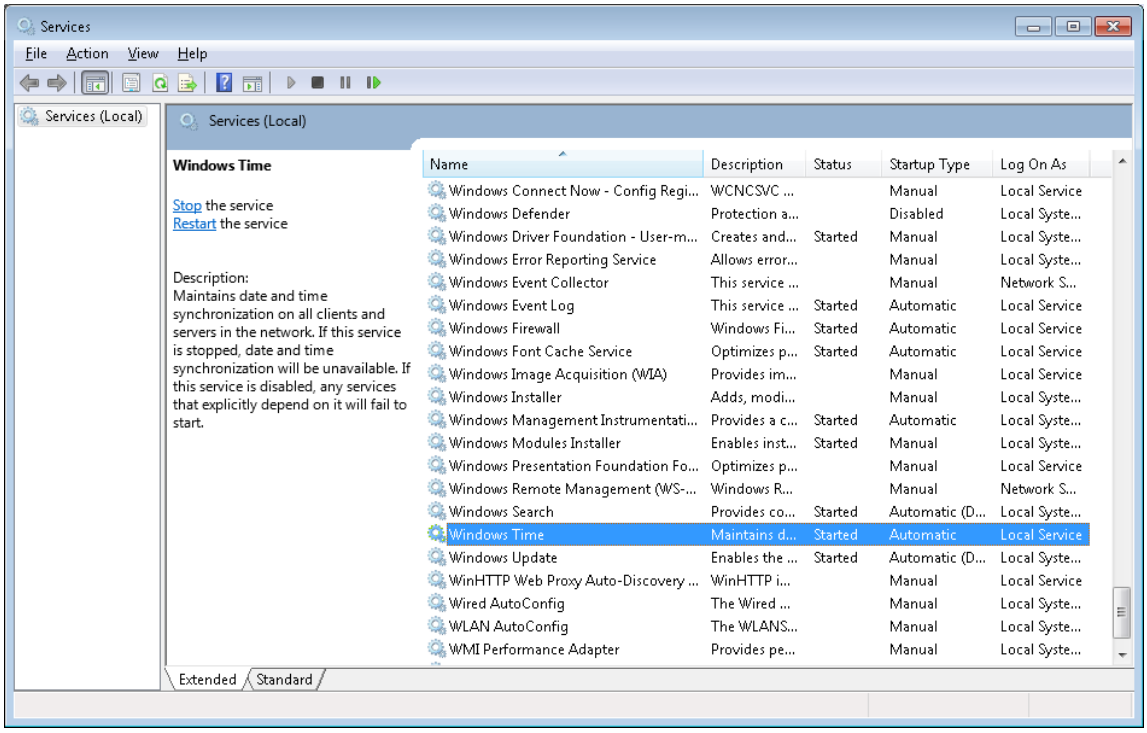
Save both files and restart NM10-frontend & NM10-backend services.

11.4. Setting up Local NTP Server

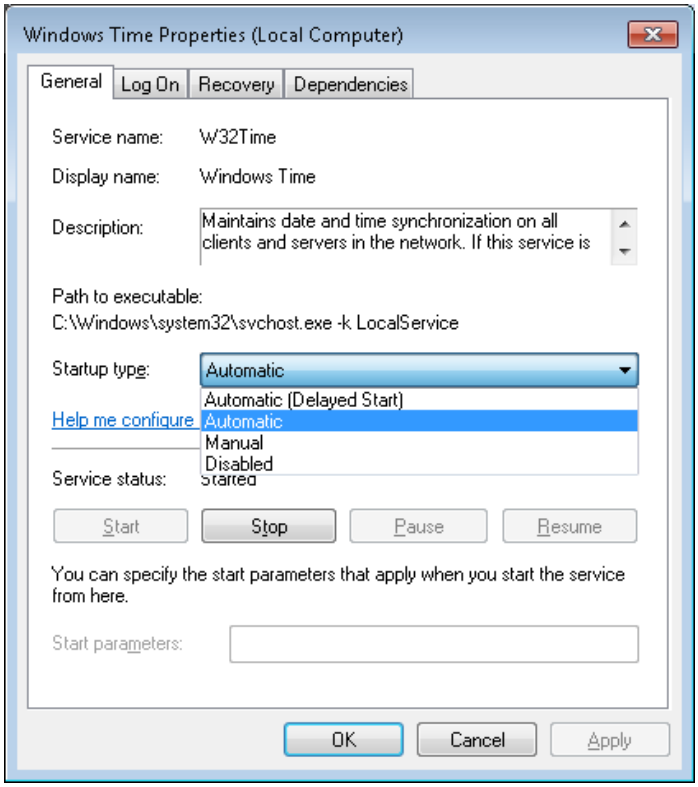
If there is no public network access available and there are no NTP servers in the customers network, it is possible to add a local NTP server on one of the computers in the network. This is useful to keep all the connected servers in sync. The NTP server can be set up for example in the NM10 (remote) server and it can be connected from each of the local computers by setting the NM10 IP/hostname as the NTP server address.

11.4.1. Configuring Windows as a Standalone NTP Server

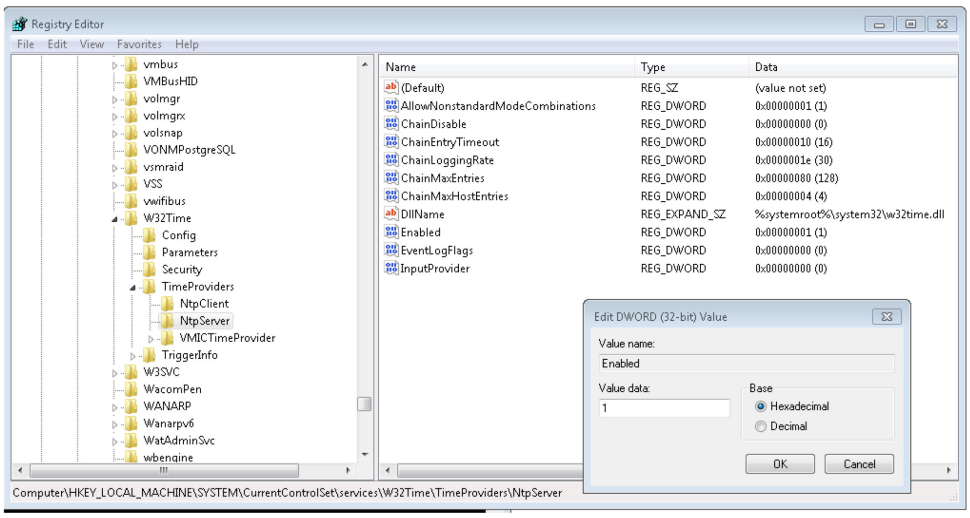
1. Go to the server that has the time synchronized from GPS (e.g. MW41 server).
2. Open the command prompt as an administrator and type **gpupdate /force**
3. Open the services console and find the Windows Time service.



4. Open the properties of the Windows Time service and set it to start automatically. Start the service from the service status before closing the window.



5. Confirm that the status of the service is **Started** and the startup type is **Automatic**.
6. Open **RegEdit.exe** and navigate to **HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ W32Time \ TimeProviders \ NtpServer**
7. Edit the value of **Enabled** by double clicking it. Set it to **1** (Hexadecimal).



8. In RegEdit navigate to **HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ W32Time \ Config \ AnnounceFlags** and set the value to **5**
9. Open the command prompt with administrator rights and type **net stop w32time && net start w32time** and after the service has been restarted, type **w32tm /config /update**
10. To confirm that the NTP service is running, type **w32tm /query /configuration** to the command prompt and observe the value of **Enabled** in the **VMICTimeProvider** section. If the value is 1, the NTP server is running.

11.4.2. Connecting to the Local NTP Server

Go to the NM10 remote workstation and connect to the NTP server that was set up earlier, open the **Control Panel** / **Date and Time** / **Internet Time** / **Change settings** / **Synchronize with an Internet time server**. Enter the local NTP server IP or host name to the server field and click **Update now** to check the connection. If there is a message about clock being successfully synchronized, the connection is working.

11.5. Changing the Hostname of NM10 Workstation

11.5.1. NM10 Hostname Reconfiguration

1. Change the hostname from **Control Panel** / **System** / **System Properties** / **Computer name** / **Change**.
2. Restart the workstation when prompted.
3. Recreate NM10 certificates by following instructions in section 11.3.1. Option A) Create a New Self-signed Certificate Using the Installer on page 50.
4. In NM10 server open browser and connect to https://localhost/nm10/login and log in as an administrator.
5. Confirm that the map can be seen and that the admin options are available (link on the header).

11.5.2. AS15 / MW41 Reinstall

1. Change the hostname on the AS15 local workstation and follow the necessary steps to fix the MW41 from the respective installation guide.

11.5.3. MW41 <-> NM10 Connection

1. Edit the *C:\Windows\System32\drivers\etc\hosts* file on NM10 workstation and add (or edit) the following line using notepad as administrator. The IP should match the new hostname of the MW41 local workstation:
   - 192.168.1.11 <MW41HOSTNAME>
2. Edit the same file on the MW41 local workstation and add or edit the NM10 hostname and IP in a similar way:
   - 192.168.1.12 <NM10HOSTNAME>
3. Confirm that the hostname IP mapping works from each side with ping.
   - Ping <MW41HOSTNAME> from NM10 workstation
   - Ping <NM10HOSTNAME> from MW41 local workstation
4. Connect to MW41 web UI from NM10 server and extract the certificate as instructed earlier in this document.
5. Copy the certificate to *C:\Program Files (x86)\Vaisala\NetworkManager\config\jdcp_conf\certificates*
6. Wait for a few minutes and check that the certificate was taken in use from NM10 web UI events: *Trusted certificate '<certificate_name>' was added.*
7. Add the NM10 certificate to MW41 local workstation:
   - Go to MW41 local workstation.
   - With browser connect to https://<NM10HOSTNAME>:8443
   - Accept the unsafe connection and cancel the login.
   - Export the certificate like with the NM10 side, instructed earlier in this document.
   - Copy the exported certificate to *C:\ProgramData\MW41\observation-network-manager\trusted-servers*
   - Restart the service MW41 Software Monitor.
8. Go to NM10 web UI and log in as admin.
9. Go to admin configuration and open the Security / Authentication.
10. Generate a new key and export it to file.
11. Open the file to text editor and in another browser tab open the MW41 web UI (log in as soundingadmin.)
12. Go to **Maintenance** > **System Settings** > **Observation Network Manager**.
13. Insert the following parameters:
    - The new NM10 workstation hostname to server address
    - Port: 8443

- Connection status interval: 60
- Authentication key
- Authentication secret

14. Click connect and confirm that the button changes to "Disconnect".
15. Open the NM10 web UI and confirm that the MW41 site can be seen on the MW41 list view.

11.5.4. Bitvise Configuration

1. Log in to MW41 web UI as soundingadmin and take full control.
2. Open **Administration** > **Sounding** > **Messages** > **Message destinations** > **SFTP** and edit the existing NM10 bitvise configuration.
   - Change the server address to the new NM10 hostname.
   - Click "Test connection" on the bottom of the window and confirm that the connection is ok.
   - If the connection fails, create a new SFTP transfer connection from scratch following the instructions in document DOC232979.
   - Save the changes.
3. Go to NM10 workstation and confirm that the SFTP connection test was successful from the Bitvise log:
   - Double click the Bitvise SSH server icon on the icon tray (bottom right).
   - Select **Activity** tab.
   - Confirm that there is an accepted connection logged from the test connection try.

11.5.5. Thinfinity Configuration

1. From the NM10 web UI logged in as admin, go to MW41 list view and click on the MW41 site.
2. Click the Remote Desktop link on the site detail window.
3. New tab is opened to the browser, accept the unsafe connection and enter the Thinfinity admin credentials (set when installing Thinfinity) and MW41 local workstation credentials (administrator / adpw_VA1).
4. Confirm that the remote desktop connection is established.

11.6. Fixing NM10 after Hardware Changes

11.6.1. CPU or Motherboard

Changing the CPU or motherboard causes the license to expire, as it is tied to the hardware that was present when the license was activated. In case the hardware changes, the license needs to be reactivated from the License Manager.

As a normal license only has a single activation available, the license has to be extended by Vaisala personnel. Please contact Vaisala helpdesk for further help.

Once the license has been extended, start the License Manager from the **Start** menu **> All Programs** > **Vaisala** > **Vaisala License Manager** > **Vaisala License Manager** and follow the instructions earlier for activating license. If there is no Internet connectivity available for the NM10 workstation, follow the offline activation process as explained earlier in this document.

11.6.2. Hard Drive

If there is a hard drive backup image available from the original installation, it can be used to set up a NM10 system to a new hard disk. The license has to be reactivated after this, as the HW related license request code changes if the HD is changed. The license activation process is explained earlier.

If the hard drive backup image is not available, the NM10 system has to be reinstalled from the beginning.

11.7. Firewall Port Table

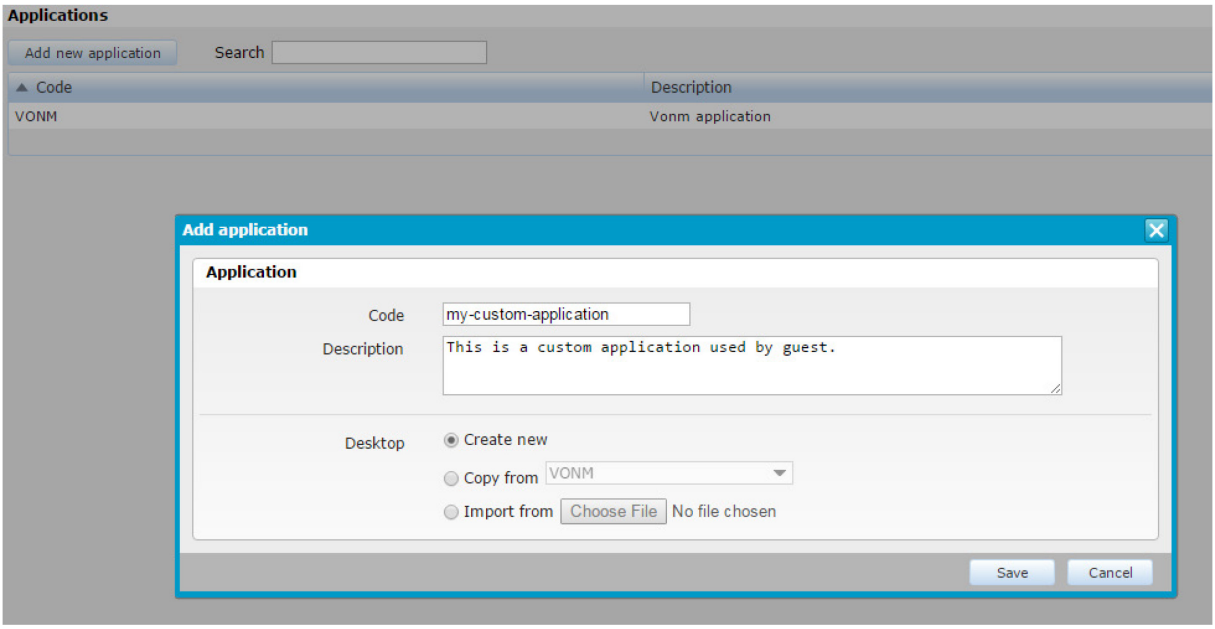
Table 9 Firewall Open Ports

From	To	Protocol	Target Port	Purpose
MW41	Network Manager DCP Server	TCP	22	SFTP file transfer from MW41
MW41	Network Manager DCP Server	TCP	8443	HTTPS connection from MW41
Network Manager DCP Server	MW41	TCP	8443	HTTPS connection to MW41
Network Manager users network	MW41	TCP	8443	MW41 Web UI and MW41 RDP connection
Network Manager DCP Server	Network Manager DB Server	TCP	5432	Database connection
Network Manager Map Server	Network Manager DB Server	TCP	5432	Database connection for WFS
Network Manager Web Server	Network Manager DCP Server	TCP	8080, 8181, 8443	Observations, events, alerts and network status
Network Manager Map Server	Network Manager Web Server	TCP	2080	Map tiles and WFS
Network Manager users network	Network Manager Web Server	TCP	443	Network Manger Web UI, WFS interface

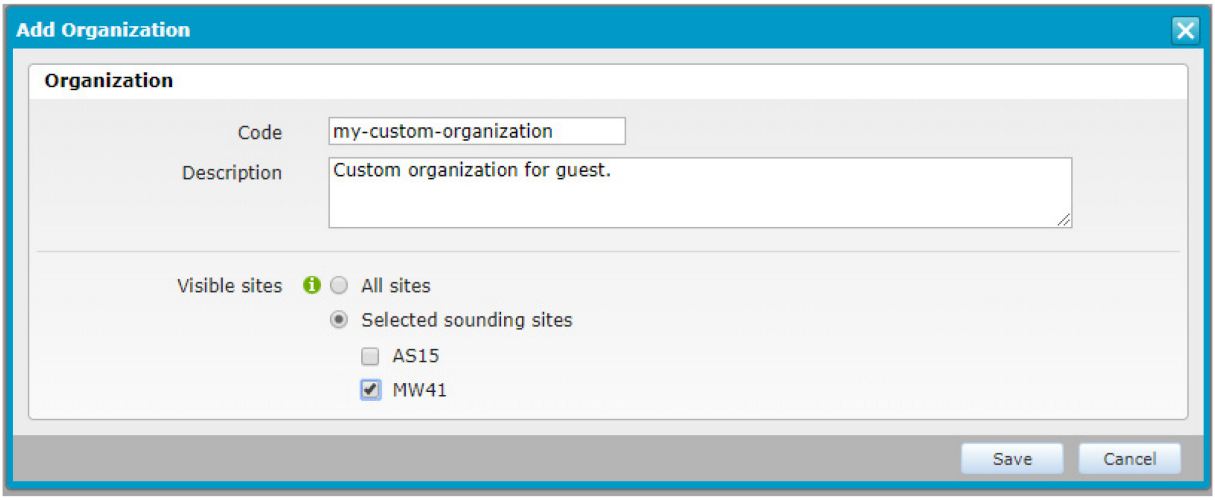
11.8 Changing Organization for Guest User

By default, the **guest** user belongs to the root organization where all sites are always visible. If you need to limit the visibility of the sites for the guest user, move the guest user to a another organization.

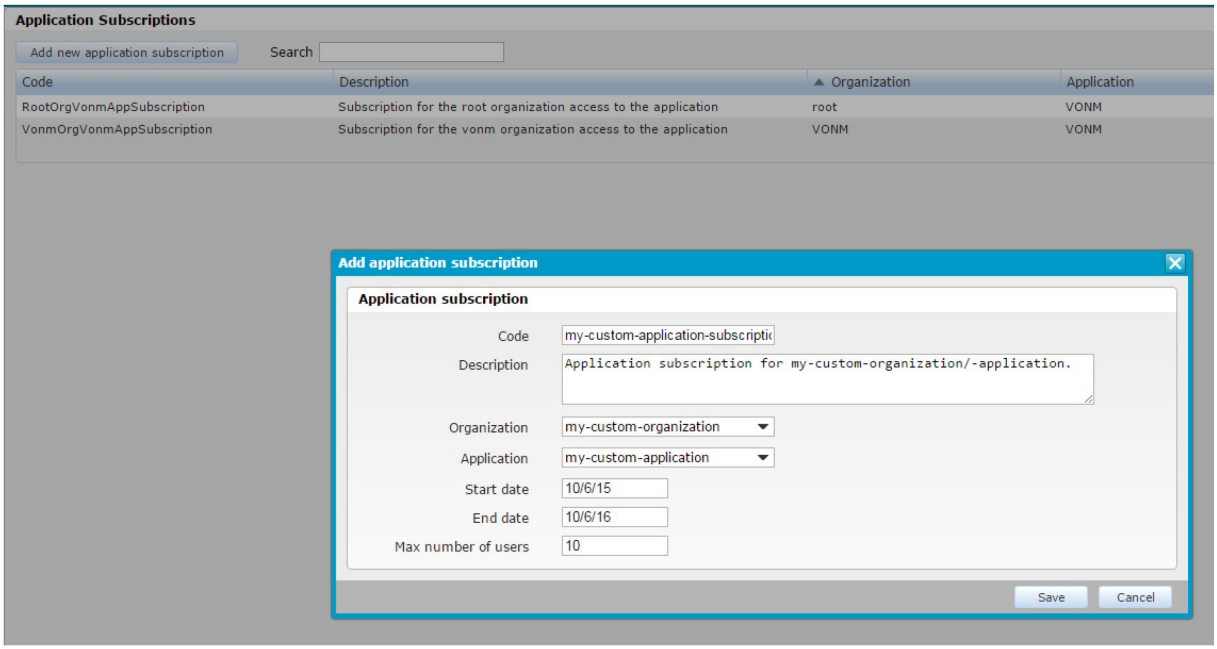
1. Log in as root admin.
2. Select **Admin** > **Application** > **Applications**.
3. Click the **Add new application** button.
4. Fill in the form and remember the application code you defined for your custom application:



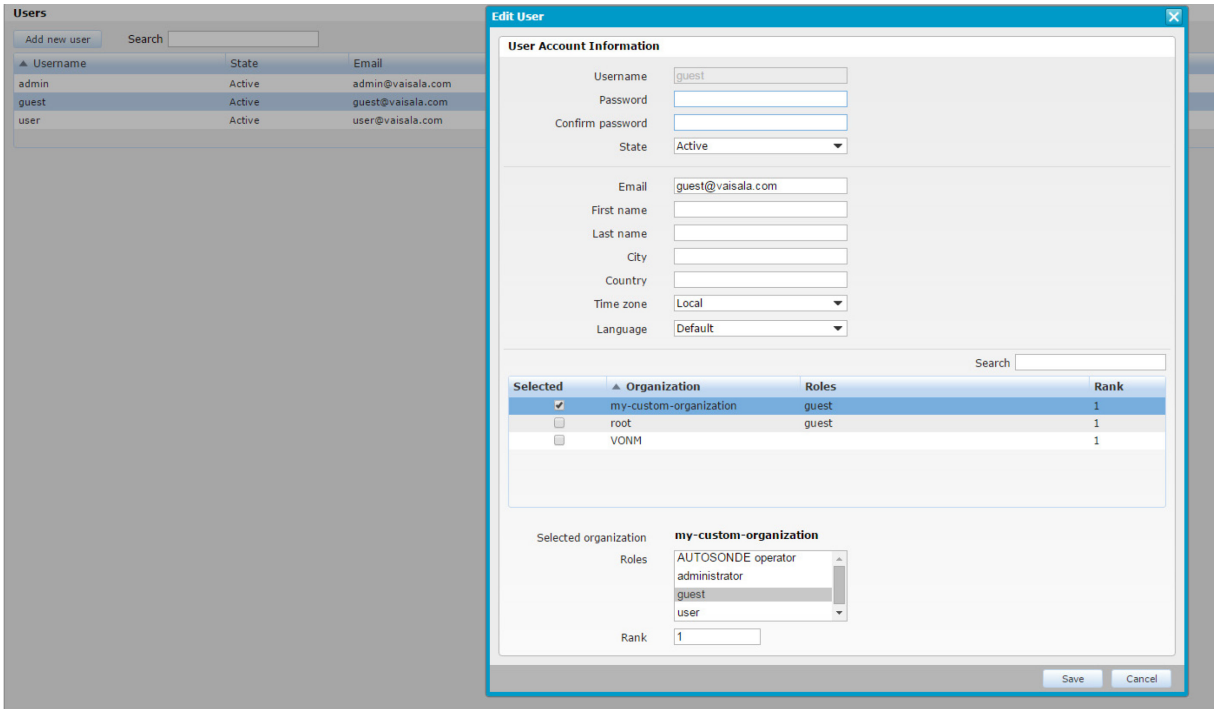
5. Click **Save**.
6. Next create an organization: Select **User** > **Organization**.
7. Click the **Add new organization** button.
8. Fill in the form using the organization code you defined for your custom application, then click **Save**:



9. Click **Save**.
10. Next, link the application with the organization: Select **Application** > **Application Subscriptions**.
11. Click the **Add new application subscription** button.
12. From the **Organization** dropdown list, select the organization you created earlier and from the **Application** dropdown list the application you created earlier:



13. Fill in the other values as needed and click **Save**.
14. Next make the guest user use the application you created earlier: Select **User** > **Users**.
15. Find the row with the username 'guest' and click the **Edit** link for that row.
16. From the **Organization** list unselect the currently selected organization and select the organization that you created earlier. Then select the role 'guest' from the **Roles** list:



17. Click **Save**.

18. Logout from Network Manager.
19. Go to the server where NM10 frontend application is running and open the following file with an advanced file editor such as **Notepad++** (**not** normal Windows Notepad): *C:\Program Files (x86)\Vaisala\NetworkManager\config\webui_conf\vsoweb.ini*.

    Set the following properties:

    - autologinapplication=<*custom_application_code*> (in the example screenshots above “my-custom-application”)
    - autologinOrganizationCode=<*custom_organization_code*> (in the example screenshots above “my-custom-organization”)
20. Save the vsoweb.ini file and restart the service running NM10 frontend application server (Tomcat or in older installations Glassfish).

After this the guest user will use your custom application/organization and any layout modification made to other applications will not affect the guest user desktop.

CHAPTER 12

INSTALLING MAP DATABASE FROM DVD

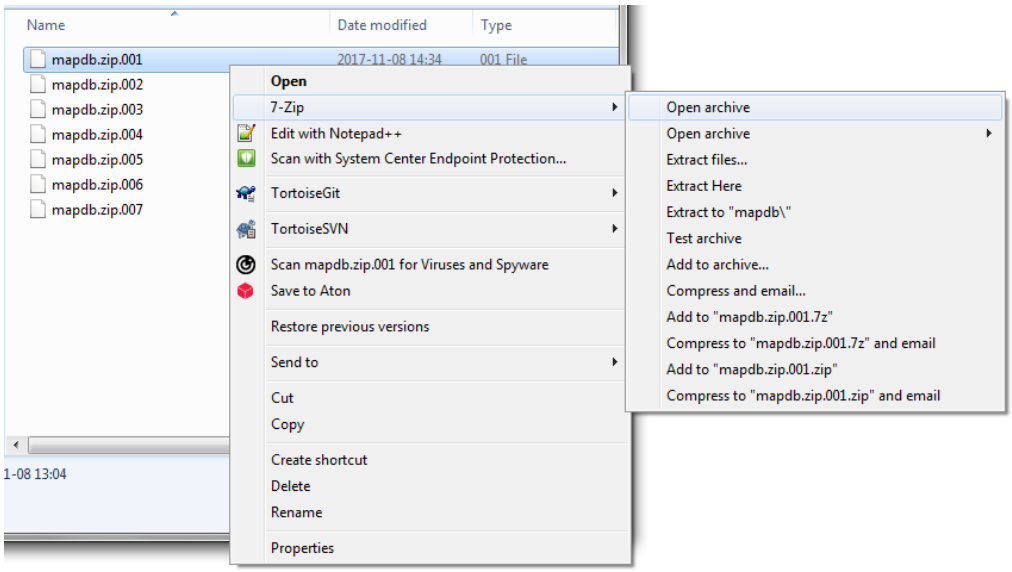
If installing from DVD, the map database must be installed from separate DVDs by doing the following:

12.1. Preparing

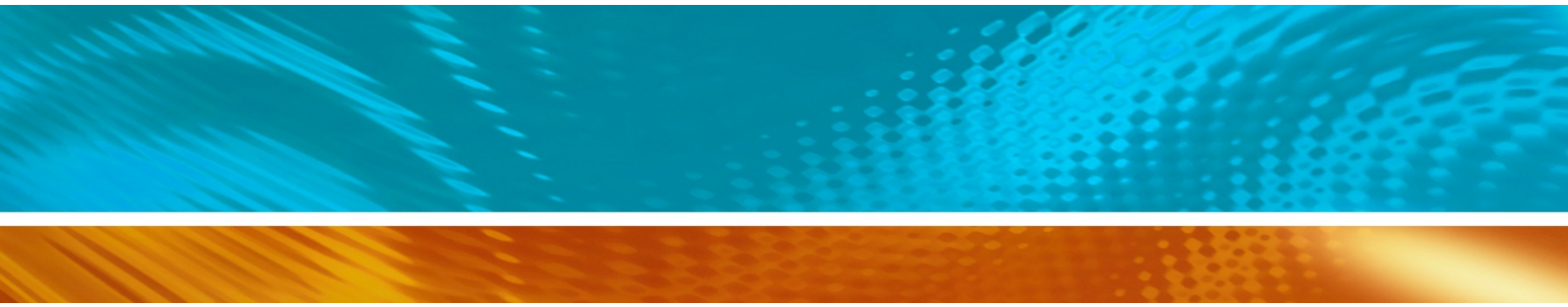
1. Download 7-zip from the map DVD #7.
2. Install 7-zip.

12.2. Unzipping

1. Insert the first map dvd to the DVD drive.
2. Start Windows file explorer and navigate to the DVD drive.
3. Copy the DVD content (mapdb.zip.001-7) to a temp folder, for example, c:\temp.
4. Repeat steps 1 – 3 for all other 6 DVDs.
5. Right-click **mapdb.zip.001** and select **7-Zip** and **Open archive**. (or select **Extract to** or use drag and drop to the target folder with right mouse button).



6. Select **Extract**.
7. Select the target folder. The map database should be located under the postgresql data folder. (the default is: C:\postgresql\9.5\data)
8. Restart NM10.



www.vaisala.com

DOC235403