TP6 - Cybersecurity - Setting up an Administrable Switch

Operational objectives :

- Understand the benefits of a ConneXium managed switch
- To be able to configure a ConneXium managed switch
- Be able to supervise a network with a ConneXium managed switch

Prerequisites :

- To have set up a ConneXium manageable switch on your network

The problem:

- Configure a ConneXium managed switch on your network and supervise your network using this component.

Les ressources :

- **Documentation constructeur**
  - Schneider Electric
    - ➢ site web
    - ➢ TCSESM Web-based Interface Manual.pdf
- **Specific documentation**
  - Architectures Maquette Cybersec_anglais.pptx
- **Applications made available for the realization of this TP :**
  - M580 application (Control Expert): md1ae58ecyb.stu
  - HMI application (Vijeo Designer) : MD1AE58ECYB

- **Software provided to be installed on the working PC (console) for the realization of this TP :**
  - Ethernet Switch Configurator (Schneider Electric): Configuration of a switch on a network via a proprietary protocol
  - ConneXium Network Manager (Schneider Electric): Network supervision from a ConneXium switch
  - Control Expert (Schneider Electric) : Programming of Schneider Electric M340, M580, ...
  - Vijeo Designer V6.2 SP8 : Design of Magelis HMI applications (execution including in Simulation mode on the Workstation)
  - Web Gate Client (Schneider Electric): complement to Vijeo Designer [option] (remote client of the Magelis HMI) (remote client of the Magelis HMI, running in an Internet Browser)
  - Internet Explorer : Microsoft Internet Browser

Evaluation criteria :	😀	😐	😟
Understanding the value of a managed switch			
Be able to configure a manageable switch			
Be able to monitor a network with a manageable switch			
Autonomy - Quality of work/restitution			

Time spent :	1 h 30	**Objective(s) :**		Comment(s) :
Evaluation :	/ 20	Reached(s)	Not reached	

Note :

In this tutorial, the ConneXium switch will be configured within the local industrial network. Also the architecture (phase) chosen to carry out this test is not important, as this local network is the same whatever the architecture set up.

After each execution of this test, it is important to reset the Connexium manageable switch to its original state. To do this, follow the instructions in the appendices at the end of the document.

Practical work - Setting up an Administrable Switch

1. Assign an IP address to the ConneXium manageable switch in the local network based on the document "Architectures Maquette Cybersec.pptx".

2. Log on as an administrator, activate the security in configuration mode, then set up the basic switch parameters.

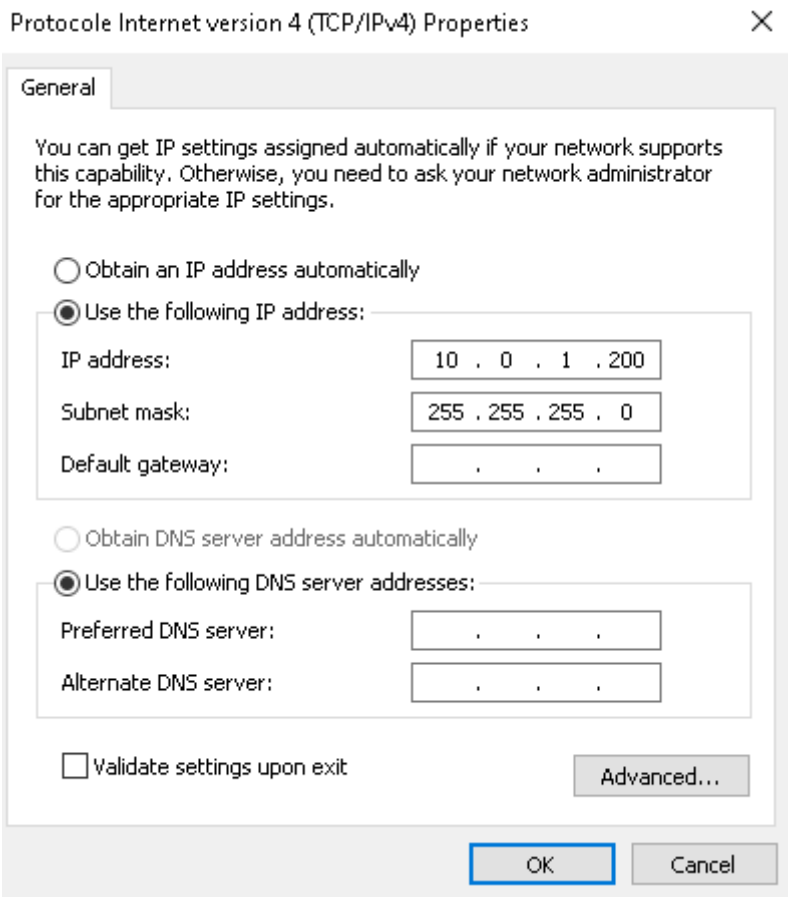
3. Configure the security settings to restrict access to the various features on the switch. Set up the necessary restrictions to allow only known network devices to communicate through the switch.

4. Using ConneXium Network Manager, create a network configuration linked to the switch in order to monitor the network. Highlight a possible malfunction of a network device in order to demonstrate the ability of the software to monitor a network.

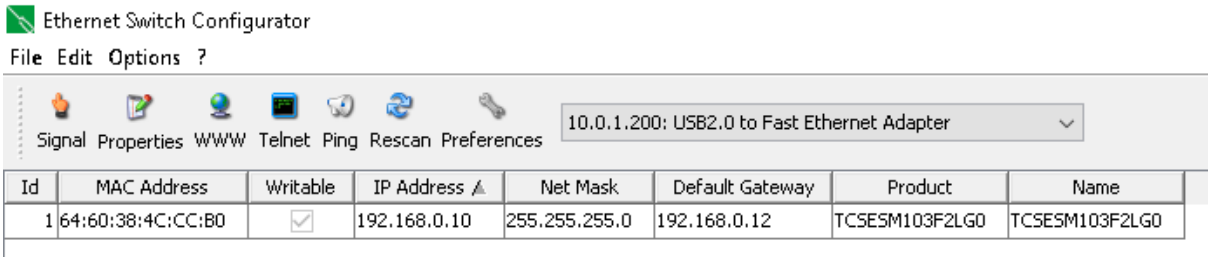
Details of expected operations

1. **Assigning an IP address to the manageable switch**

Connect your PC via an Ethernet cable to the ConneXium managed switch, and configure your network access as follows:

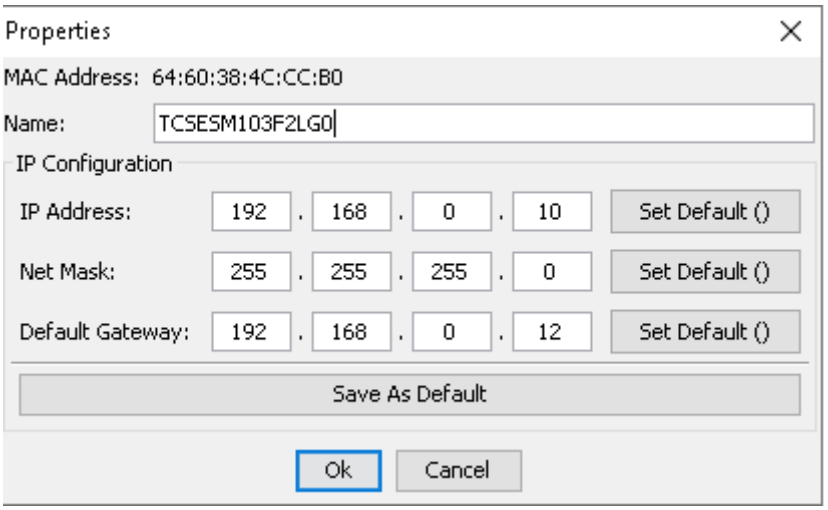


Launch the Ethernet Switch Configurator, which scans the network linked to the default Ethernet cable connected to the PC. The software should find a single result corresponding to the Connexium Switch:



If not, check that the switch is powered on, that the Ethernet cabling is correct and that the software is scanning the correct network (drop-down menu at the top allowing you to choose the network interface to scan).

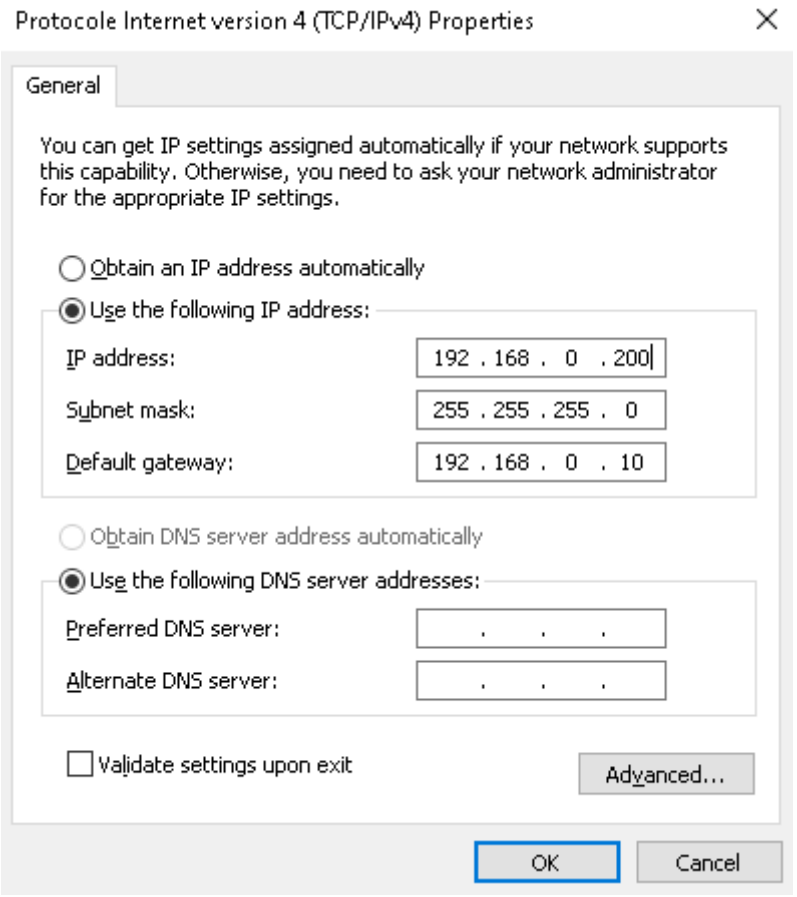
Set the IP configuration of the switch as follows (in case it is not already set up):



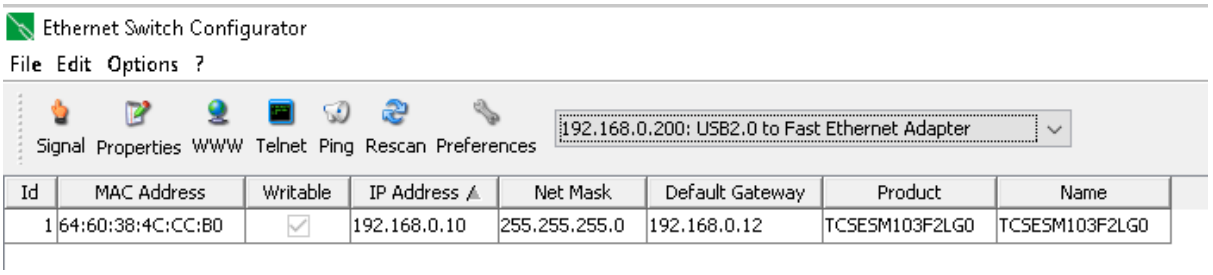
Note: The default gateway should only be configured if the NOC associated with the M580 is present in the network.

Cancel the network scan launched by the software after validation of the IP configuration.

Reconfigure your network access according to the following configuration:

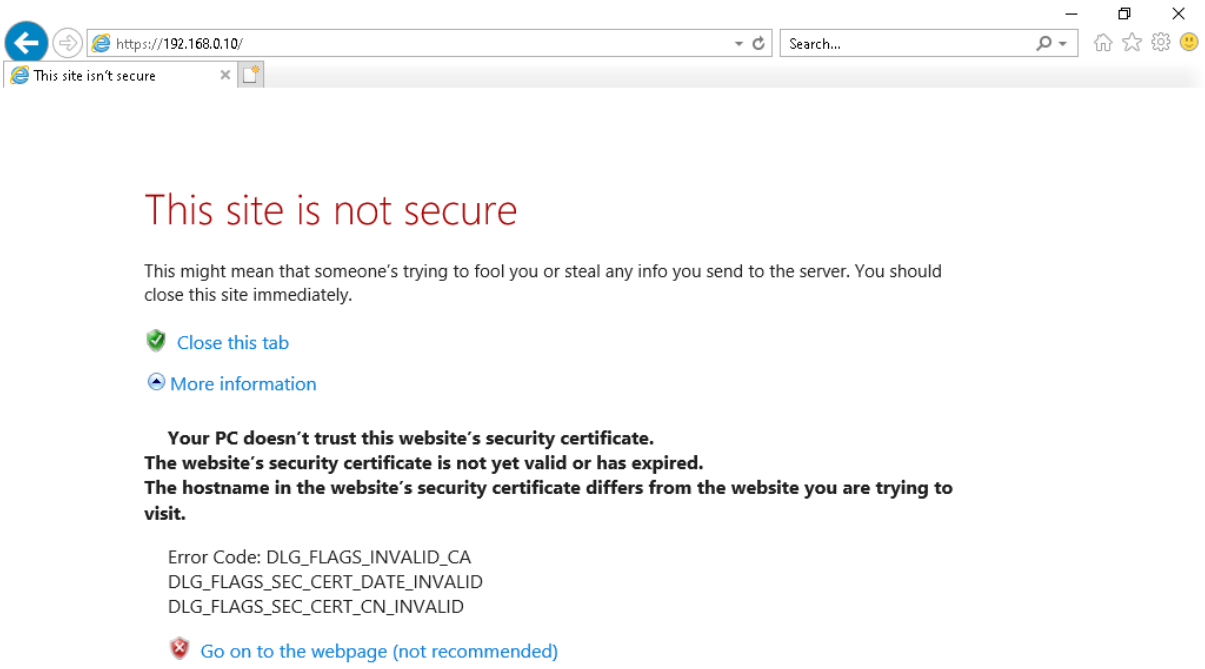


Close and restart the Ethernet Switch Configurator software. The software performs a new scan on the 192.168.0.0/24 network and should find the switch:

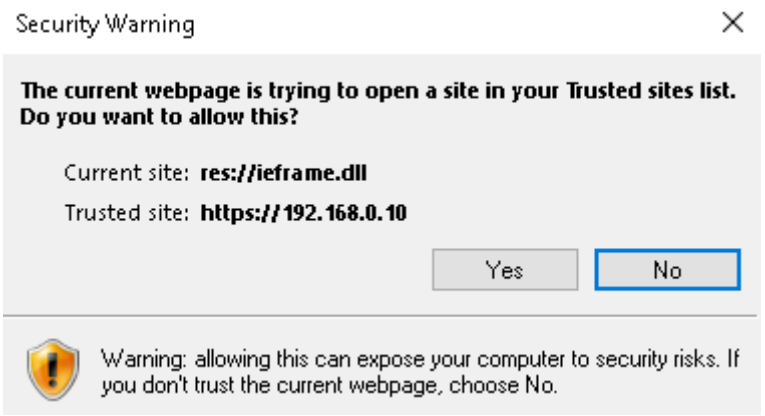


Finally, check that you can access the switch's configuration web page, using Internet Explorer at the following address: https://192.168.0.10/.

Ignore the warning about a security problem related to access to the site by clicking on "Go to the web page", if necessary:

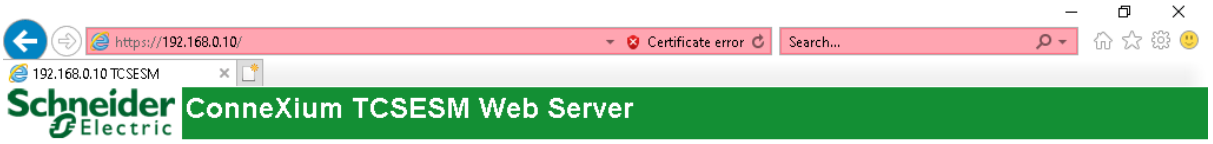


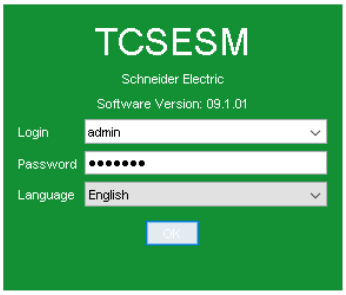
If requested, click on "Continue":



One must then obtain access to the switch's configuration web service:

Credentials: admin/private



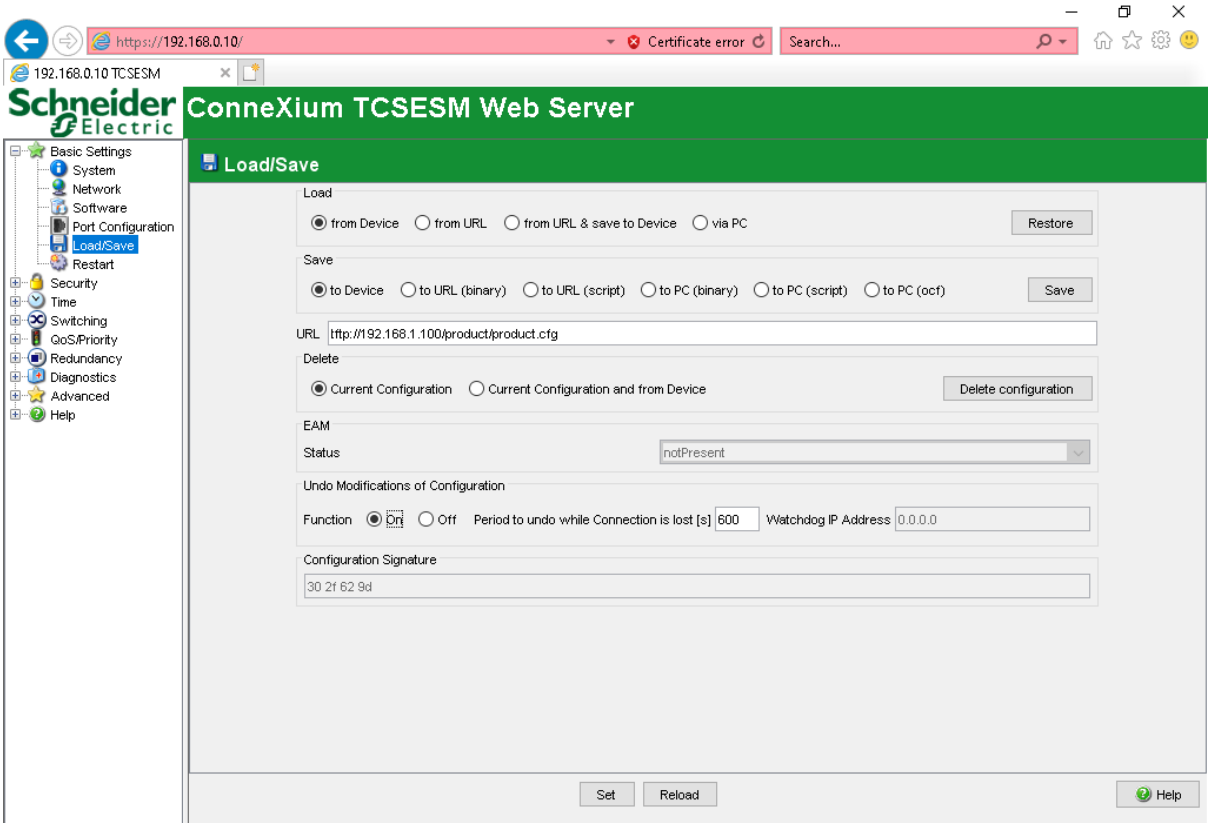


Warning: As this configuration web service uses a Java module, it will not be possible to access the service from other browsers that no longer support Java modules (only IE still supports these modules).

2. **First, connect to the switch using the admin / private login.**

N.B.: The connection may take some time.

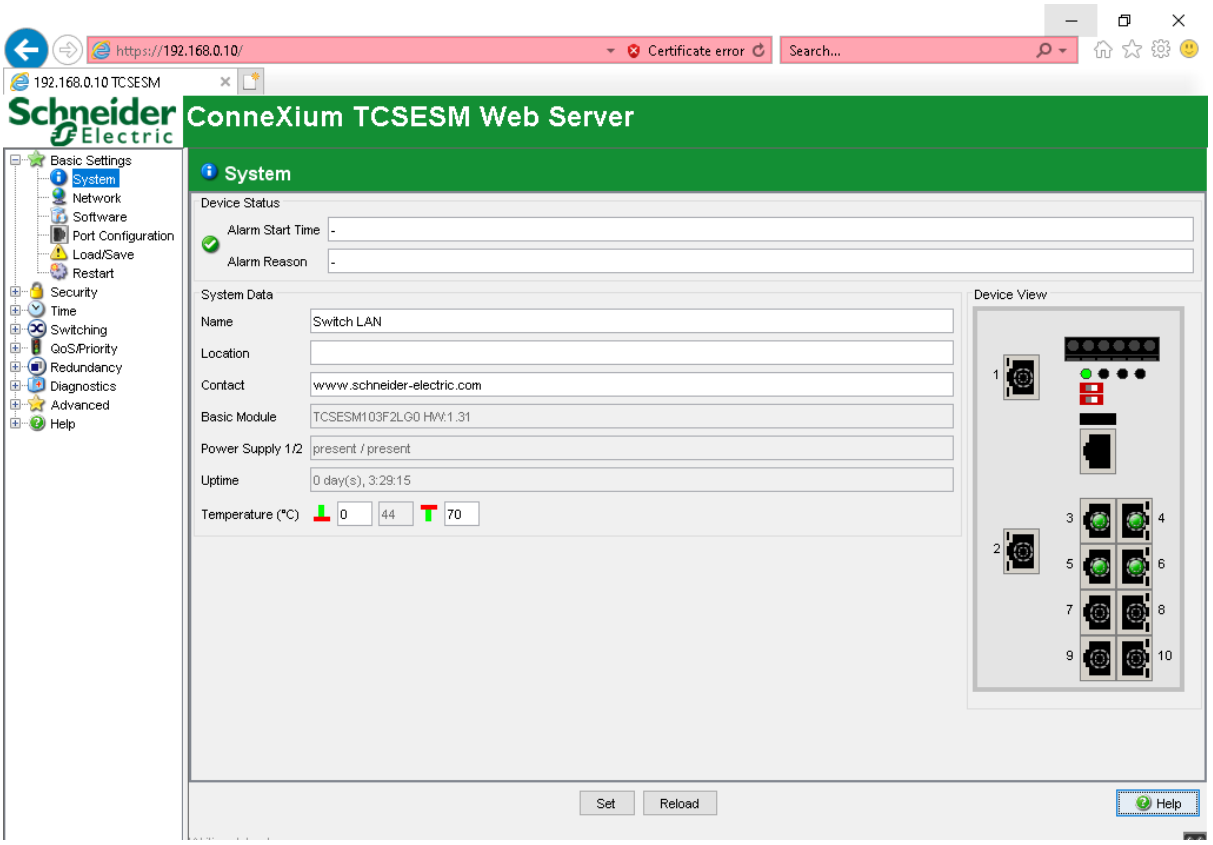
Before modifying the switch configuration, activate the security in configuration mode by going to the **Basic Settings > Load/Save** menu and activating the "Undo Modifications of Configuration" function:



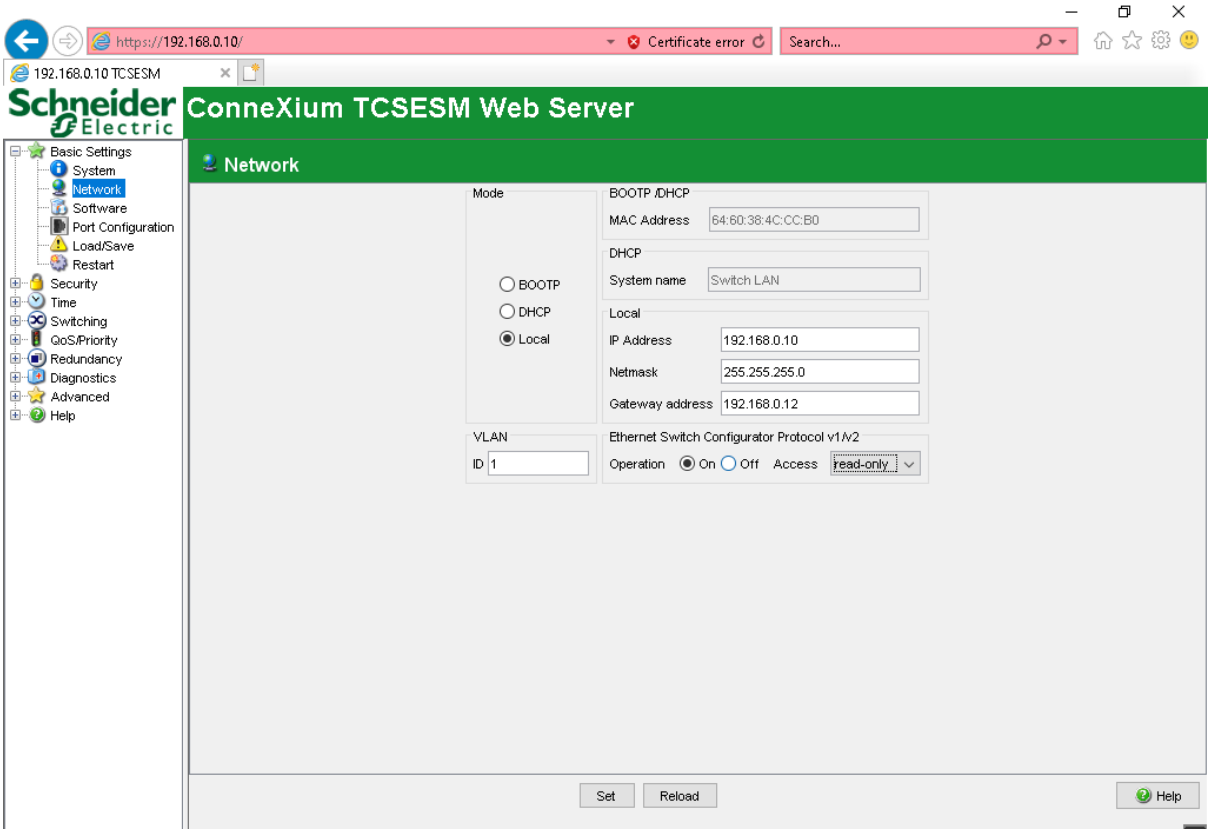
Validate the modification by clicking on "Set".

The purpose of this security is to cancel the last changes in the event of loss of connectivity (or inactivity) after 600 seconds, i.e. 5 minutes. **It should only be disabled when the switch configuration is complete AND functional.** As the purpose of this tutorial is to learn how to configure the switch, it will not be disabled. Without this feature enabled, a permanent loss of access to the switch configuration could occur due to a bad configuration.

Then go to the **Basic Settings > System** page and assign a name (and possibly a contact) to the switch, then validate by pressing "Set":

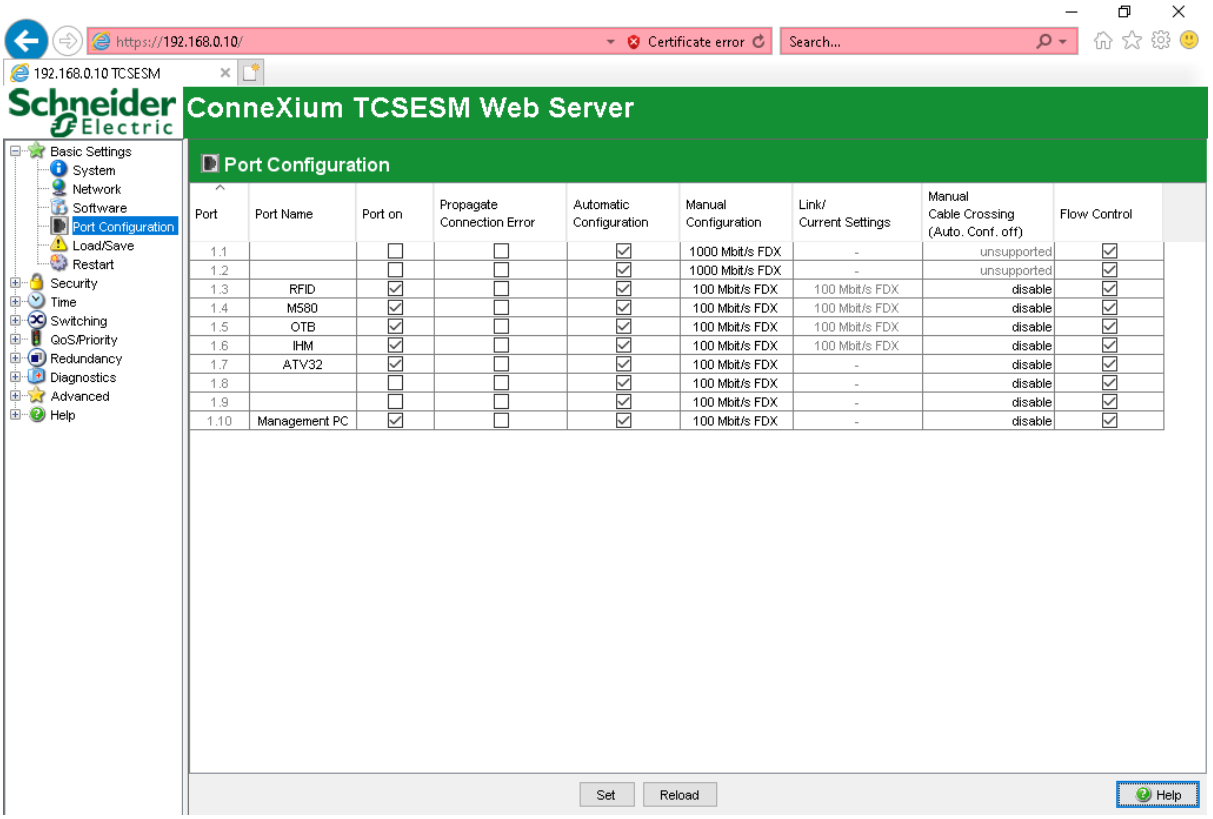


In the **Basic Settings > Network tab**, you can check that the IP configuration of the switch corresponds to the one previously set. Then disable the possibility of modifying this configuration from the Ethernet Switch Configurator by setting the access to "read-only":



Note that it is not mandatory to completely disable this protocol, as this allows access to the IP configuration (read only) of the switch.

In the **Basic Settings > Port Configuration tab**, you can disable unused ports and assign a port name to each port according to the equipment connected to that port:

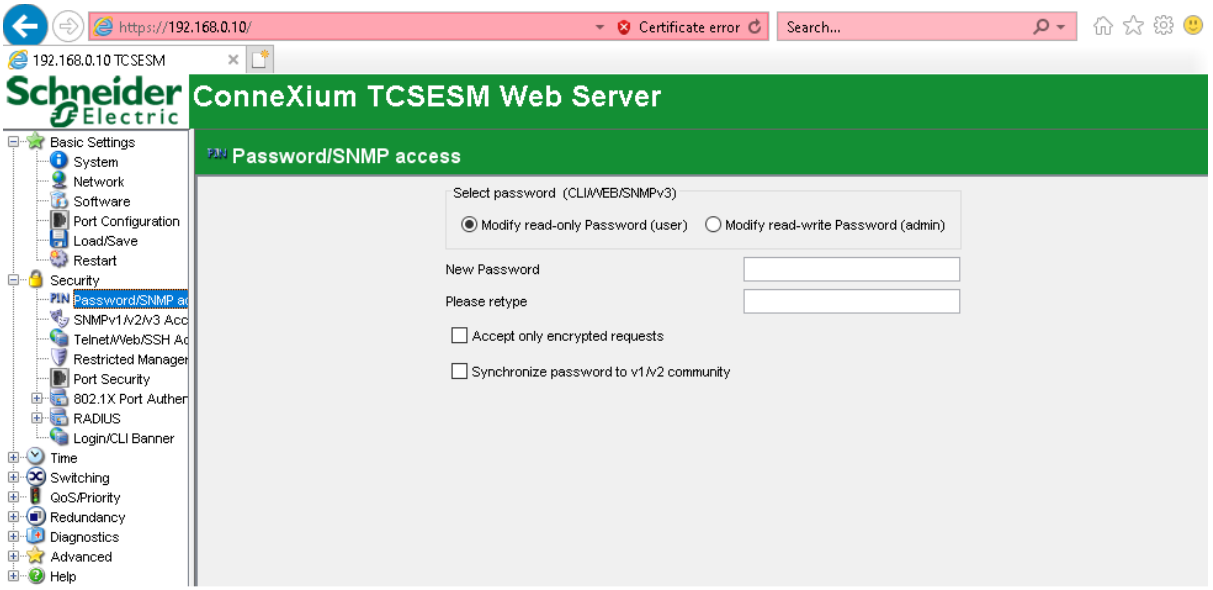


N.B.: This configuration depends on the Ethernet cabling in place, check for each port the equipment that is connected to the port and disable only the unused ports.

Caution: Always keep one port active to connect the switch management PC.

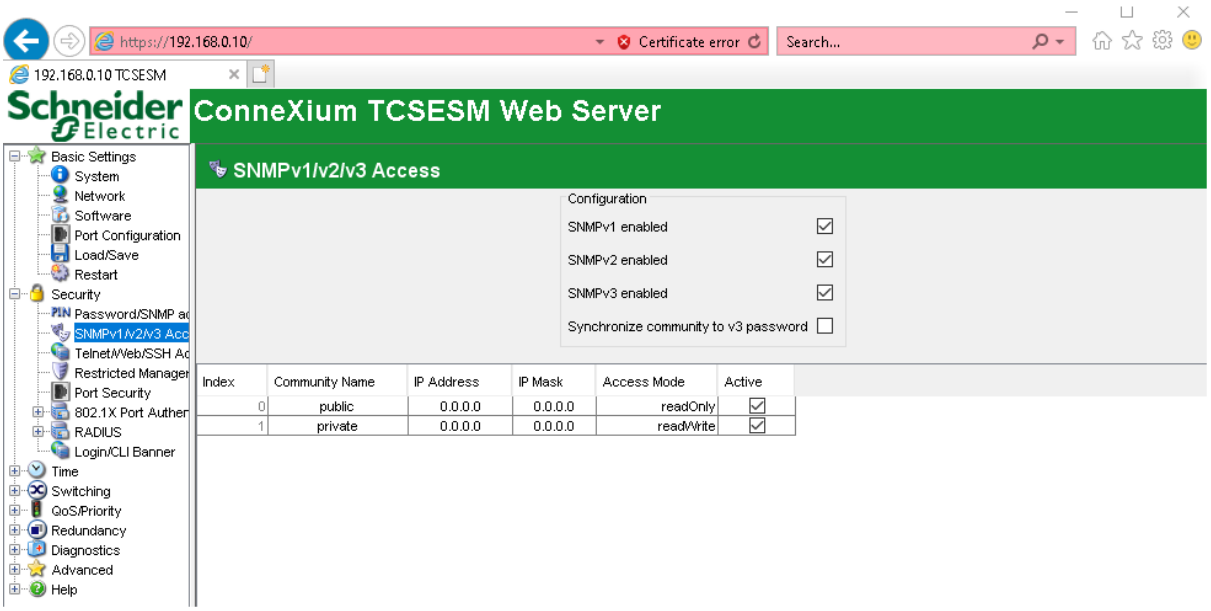
You can check that this security measure is working properly by disabling the port linked to the HMI. After a few seconds, the HMI will lose the connection to the M580. By reactivating the associated port, the HMI will return to its normal state.

3. A first tab **Security > Password/SNMP** access offers the possibility to modify the passwords of the SNMP service used to supervise the network connected to the switch. Two users are available: **user / public** which only has read access and **admin / private** which has full access (read and write) to the SNMP directory.



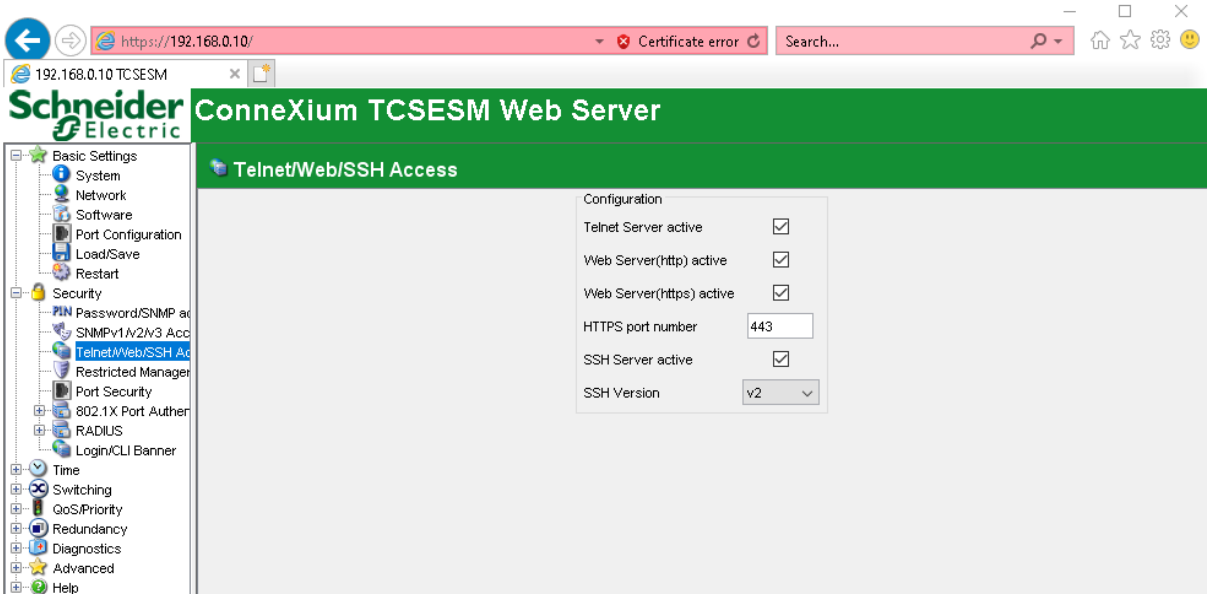
In the case of a production use, these passwords will obviously have to be modified, which will not be done during this tutorial.

In the continuity, the **Security > SNMPv1/v2** Access tab allows to restrict the SNMP accesses of a community to an IP address or a complete network (according to the network mask):



It also allows you to enable/disable these communities and change their read and write access. As mentioned before, the **user** belongs to the public community while admin belongs to the **private** community. In our case we will not restrict these accesses.

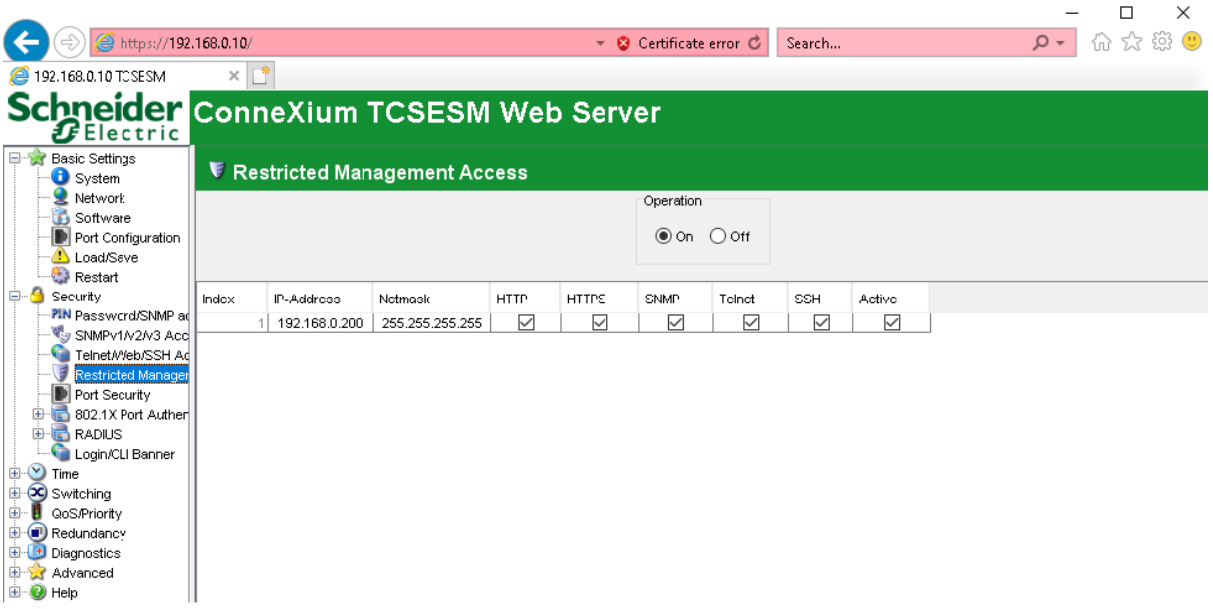
The **Security > Telnet/Web/SSH Access** tab allows you to enable or disable the various services that manage the switch:



For this tutorial, we will not bother to modify these parameters.

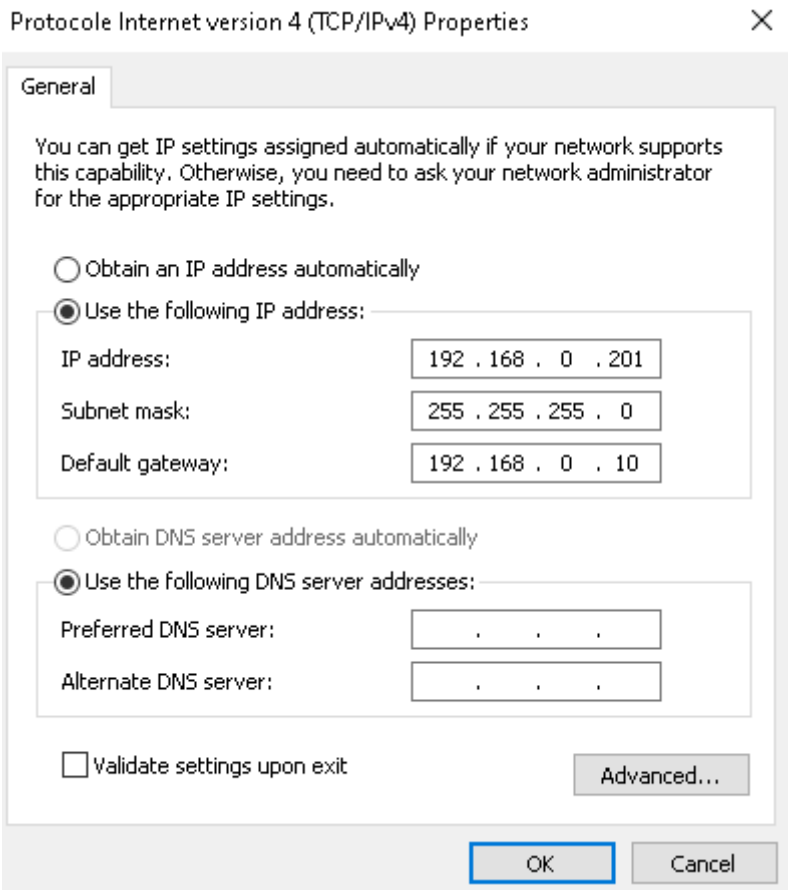
Next, access the **Security > Restricted Management Access** control panel, whose role is to set up access restrictions by IP filtering to the various switch services.

Activate this service and configure access to these services only for the IP address of the switch's management PC, i.e. the IP **192.168.0.200** :



Check that the web service is still functional, otherwise the web page will indicate a loss of connection to the service.

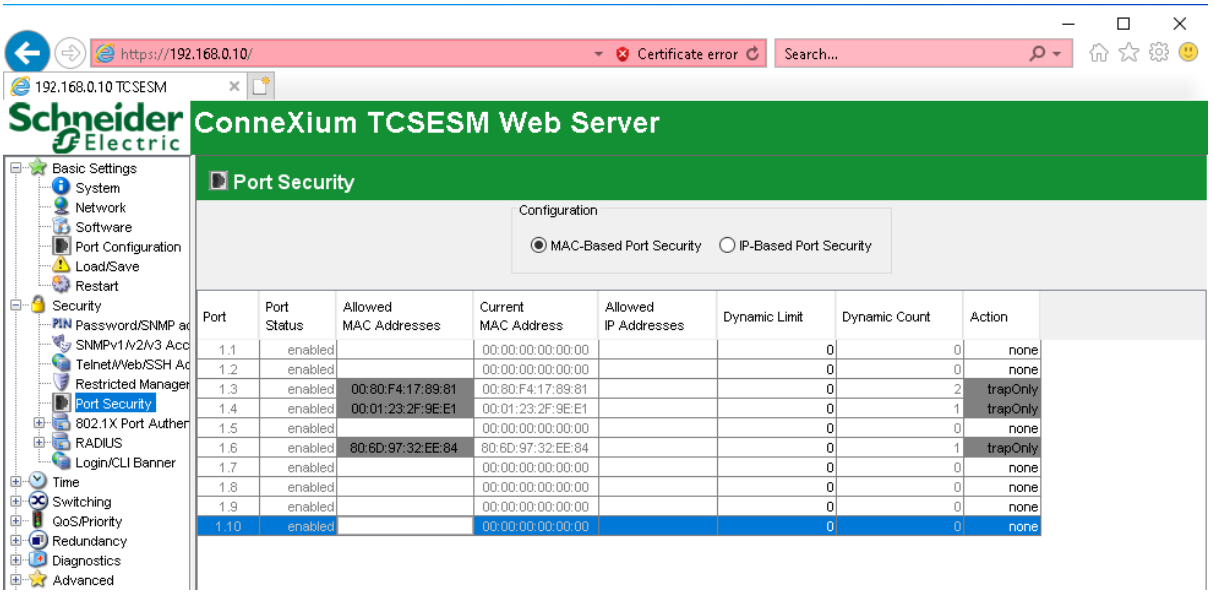
You can also check that the restriction is in place by reconfiguring its IP on the network:



When reloading the web page, it can be seen that access to the web service is no longer available.

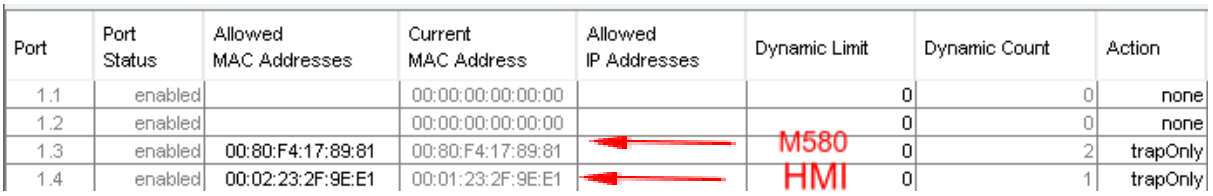
Warning: Do not forget to reconnect to the service within 5 minutes after the operation, to avoid the previous configuration being reloaded (security in active configuration mode).

Finally, go to the **Security > Port Security** tab. This tab allows you to establish MAC or IP filtering on the switch's ports, thus preventing physical intrusions into the network. You can easily define the authorised MAC addresses for each port by copying the "Current MAC Address" field which indicates the MAC address of the equipment currently connected to the port:

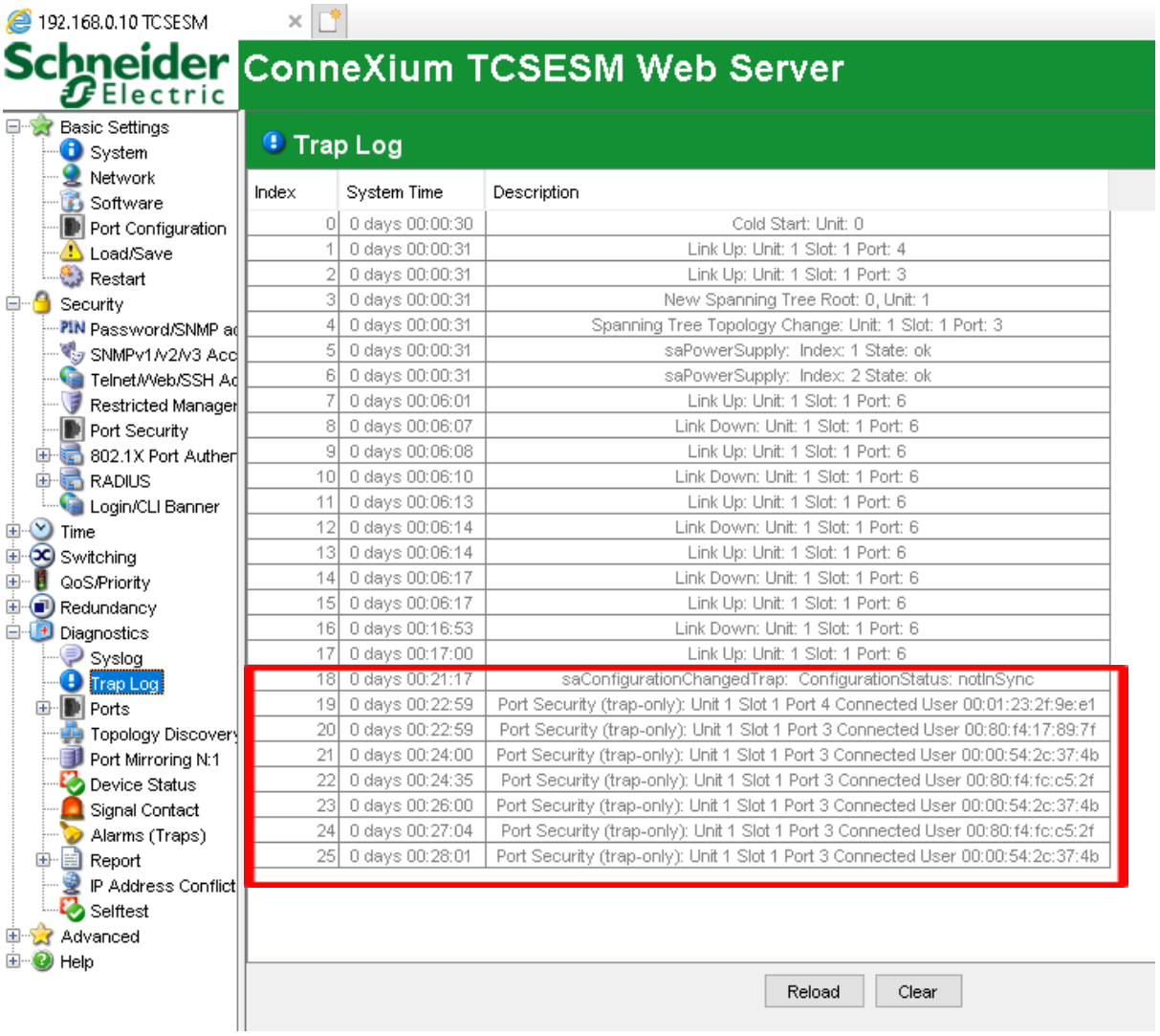


The TCSESM Web-based Interface Manual can be consulted for a more detailed understanding of the various actions associated with an unauthorized access attempt. The **trapOnly** value simply raises an alarm when an unauthorized port access attempt is made.

Change the value of the MAC address associated with the HMI to a different MAC address from that of the HMI in order to check that the filtering is working correctly.

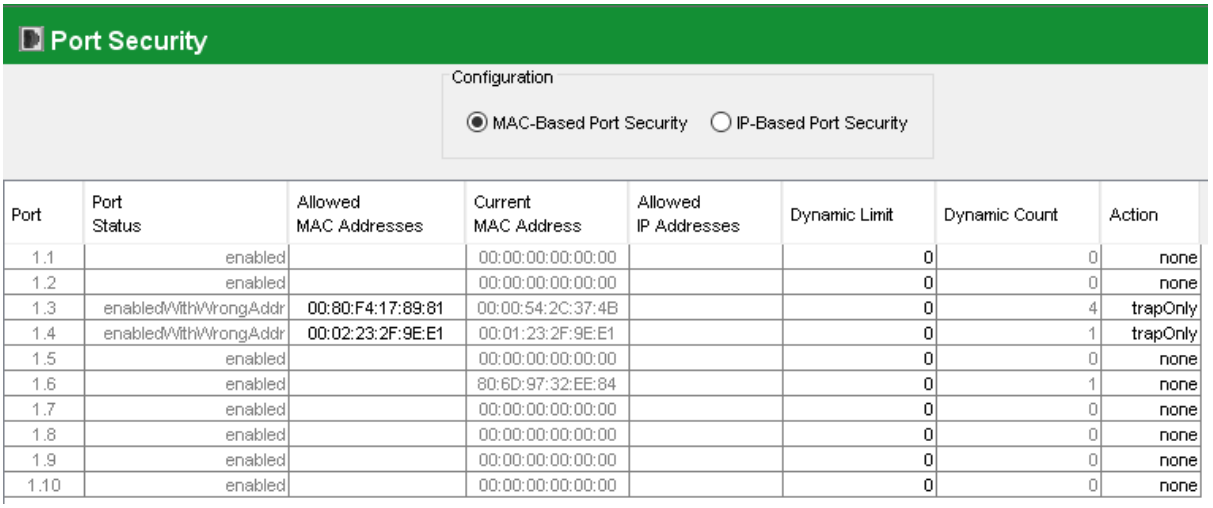


Then go to the **Diagnostics > Trap Logs** tab, where you will see an alarm associated with the port to which the HMI is connected:



Important : Other alarms should have been raised (here on port 3) on the port dedicated to the M580. These alarms have been raised because the M580 has several components each with their own MAC address (and IP address), so to overcome this problem it would be necessary to set up several MAC addresses (or IP addresses) on this same port. The ConneXium switch allows up to 10 MAC (or IP) addresses separated by a space. In addition, each MAC (or IP) address can be given a mask (@/XX) at the end, allowing the use of address ranges.

It can also be seen in the MAC filtering configuration tab that the status of the port that raised the alarm has changed, indicating that the MAC address of the connected device does not match but that it is still allowed to communicate on the network (trapOnly):



Port	Port Status	Allowed MAC Addresses	Current MAC Address	Allowed IP Addresses	Dynamic Limit	Dynamic Count	Action
1.1	enabled		00:00:00:00:00:00		0	0	none
1.2	enabled		00:00:00:00:00:00		0	0	none
1.3	enabledWithWrongAddr	00:80:F4:17:89:81	00:00:54:2C:37:4B		0	4	trapOnly
1.4	enabledWithWrongAddr	00:02:23:2F:9E:E1	00:01:23:2F:9E:E1		0	1	trapOnly
1.5	enabled		00:00:00:00:00:00		0	0	none
1.6	enabled		80:6D:97:32:EE:84		0	1	none
1.7	enabled		00:00:00:00:00:00		0	0	none
1.8	enabled		00:00:00:00:00:00		0	0	none
1.9	enabled		00:00:00:00:00:00		0	0	none
1.10	enabled		00:00:00:00:00:00		0	0	none

To go further, change the action associated with unauthorised access to the HMI port from trapOnly to portDisable :

Port	Port Status	Allowed MAC Addresses	Current MAC Address	Allowed IP Addresses	Dynamic Limit	Dynamic Count	Action
1.1	enabled		00:00:00:00:00:00		0	0	none
1.2	enabled		00:00:00:00:00:00		0	0	none
1.3	enabledWithWrongAddr	00:80:F4:17:89:81	00:00:54:2C:37:4B		0	4	trapOnly
1.4	enabledWithWrongAddr	00:02:23:2F:9E:E1	00:01:23:2F:9E:E1		0	1	portDisable
1.5	enabled		00:00:00:00:00:00		0	0	none
1.6	enabled		80:6D:97:32:EE:84		0	1	none
1.7	enabled		00:00:00:00:00:00		0	0	none
1.8	enabled		00:00:00:00:00:00		0	0	none
1.9	enabled		00:00:00:00:00:00		0	0	none
1.10	enabled		00:00:00:00:00:00		0	0	none

The HMI loses its connection to the M580, indicating that the port has been disabled after unauthorised access to the equipment port. In addition, the LED on the port flashes green at a rate of 3 times, which is due to the port being disabled after unauthorised access.

Reset the correct MAC address of the HMI, and in the Basic Settings > Port Configuration tab, re-enable the port that was disabled. Then check that the HMI is working again.

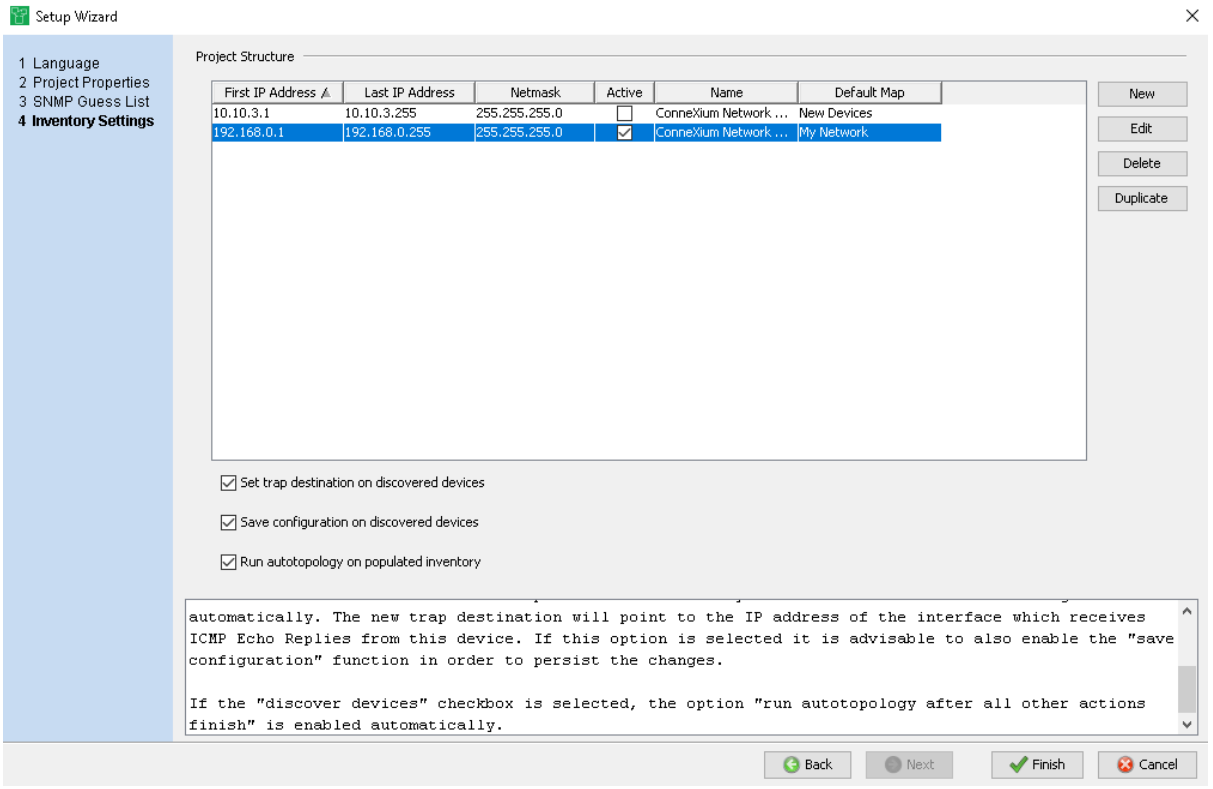
N.B.: Automatic reactivation of the port according to a timer is possible, consult the associated documentation for more information.

N.B.: The same manipulations can also be tested using filtering by IP address rather than by MAC address. (MAC address filtering is more interesting because it is more difficult to spoof a MAC address than an IP address).

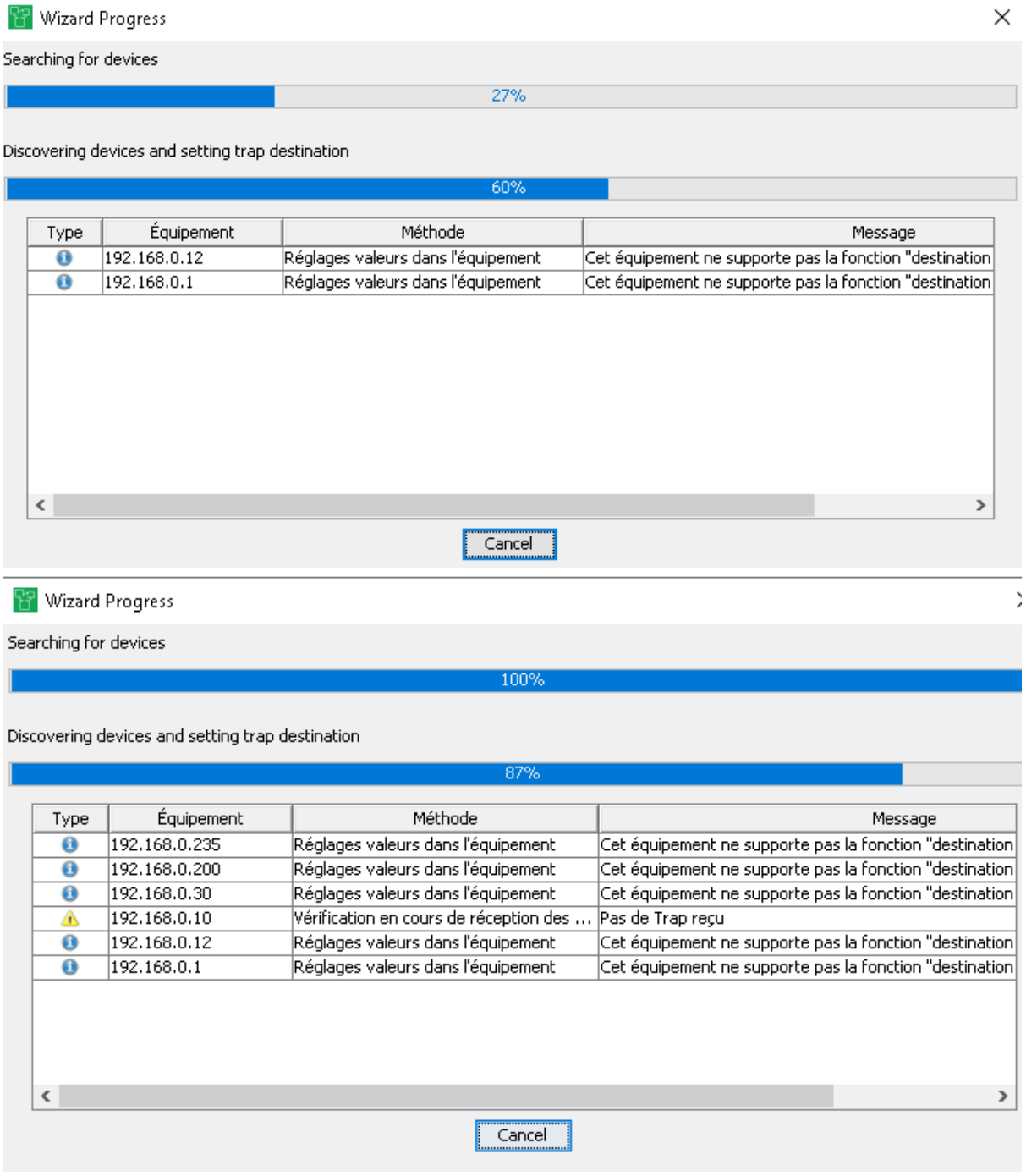
4. Open the **ConneXium Network Manager** software and create a new project via the menu **File > New project.**

Follow the project configuration instructions, leaving the default settings or making changes if necessary, until you reach **Inventory Setup**.

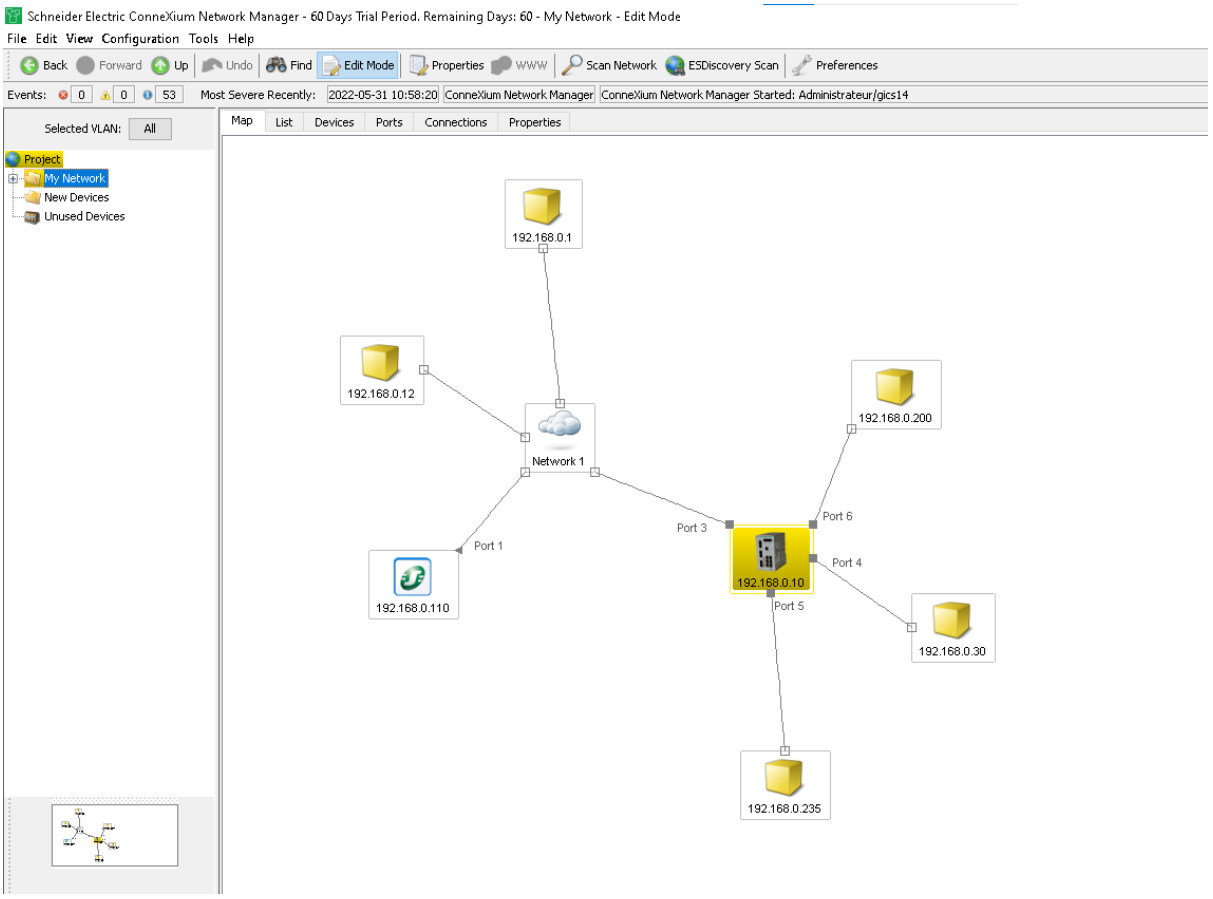
In this last tab, activate the IP range **192.168.0.0/24** corresponding to the network of the ConneXium switch and define **My Network** as the default topology:



The software then scans the network of the switch to determine all available equipment:



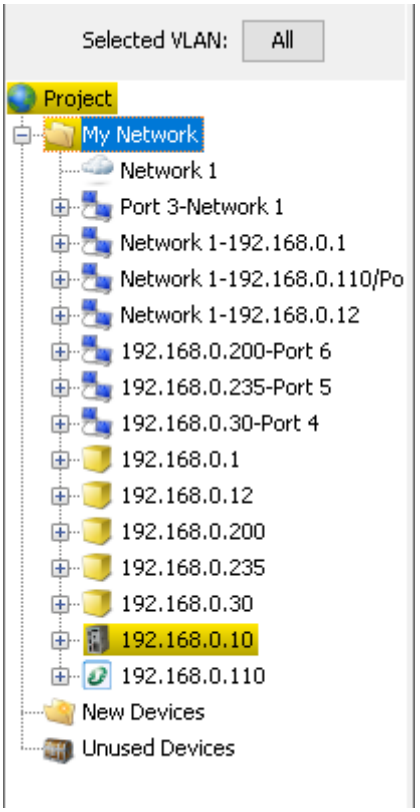
Once the equipment search is complete, by clicking on the My Network directory, the network topology (determined automatically by the software) is displayed:



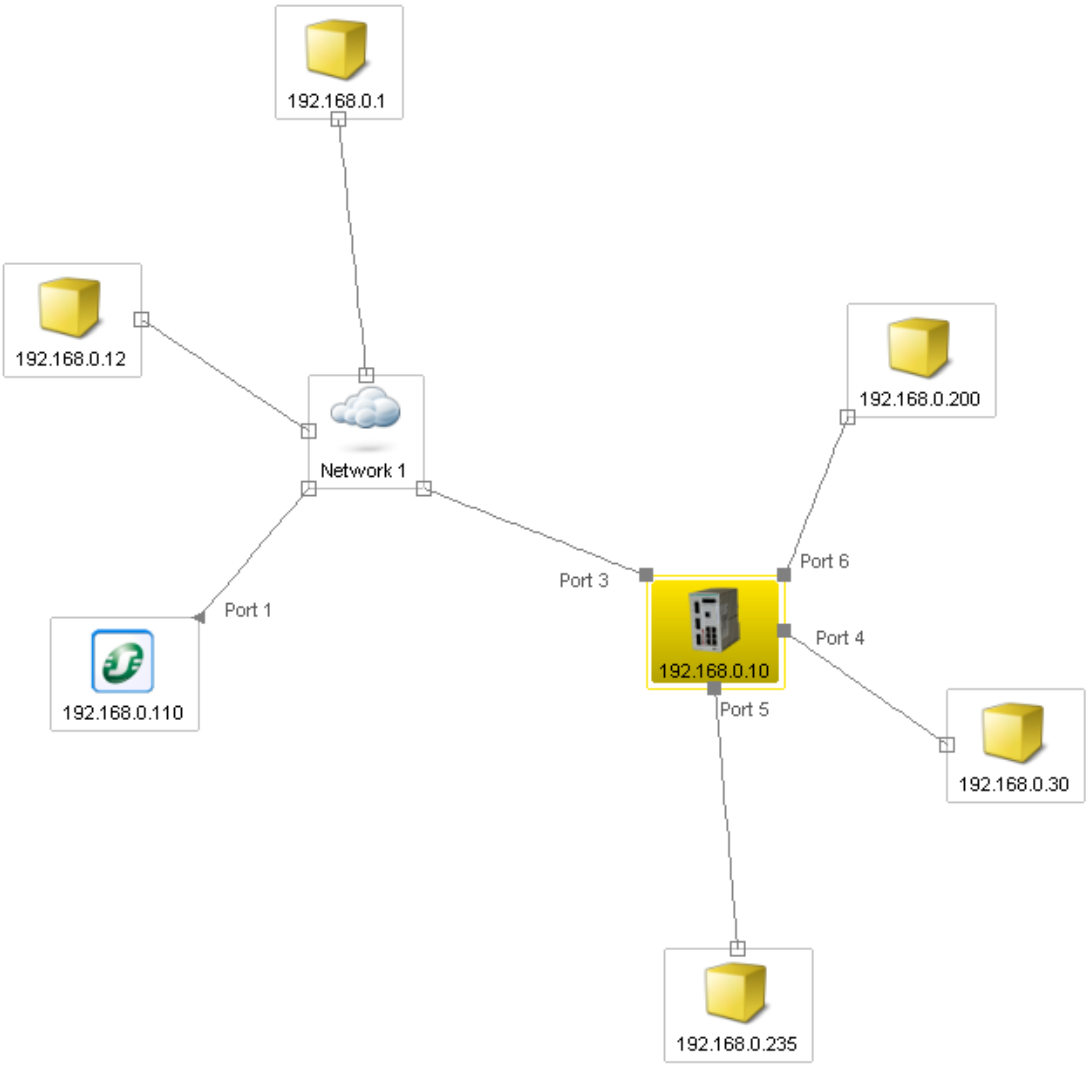
We will note the presence of all the elements defined (on the **192.168.0.0/24** network) in the document "Architectures Maquette Cybersec_anglais". The **Network 1** device actually corresponds to the M580, which has several devices and which are therefore all available from the port to which it is connected (hence the absence of the IP 192.168.0.100 corresponding to the M580).

The interface of the software has different parts:

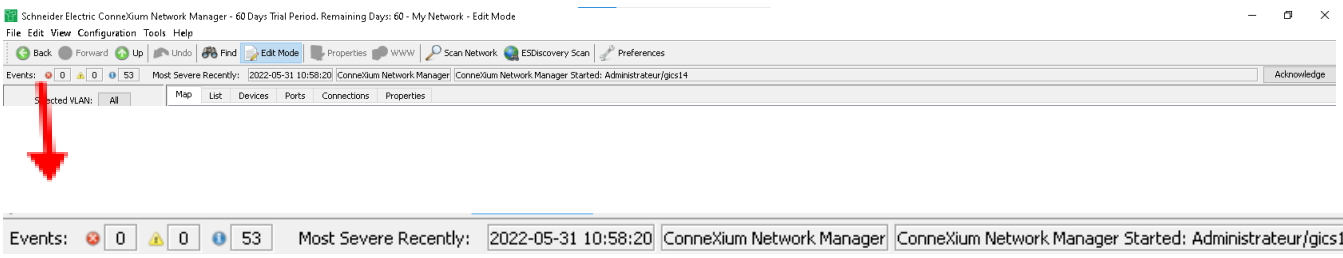
- A list of all the devices available (or that were available at one time) on the network:



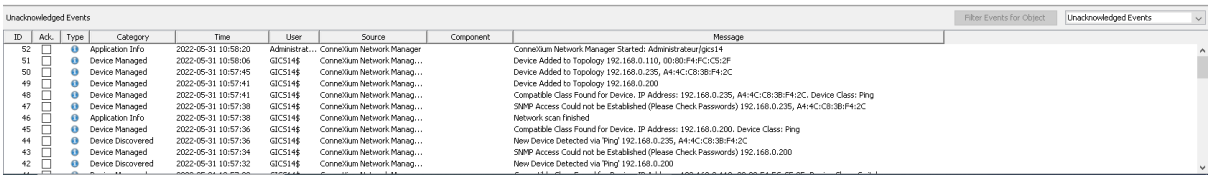
- A network topology in graphical form :



- An event counter (errors, warnings and information) with the last most critical status:

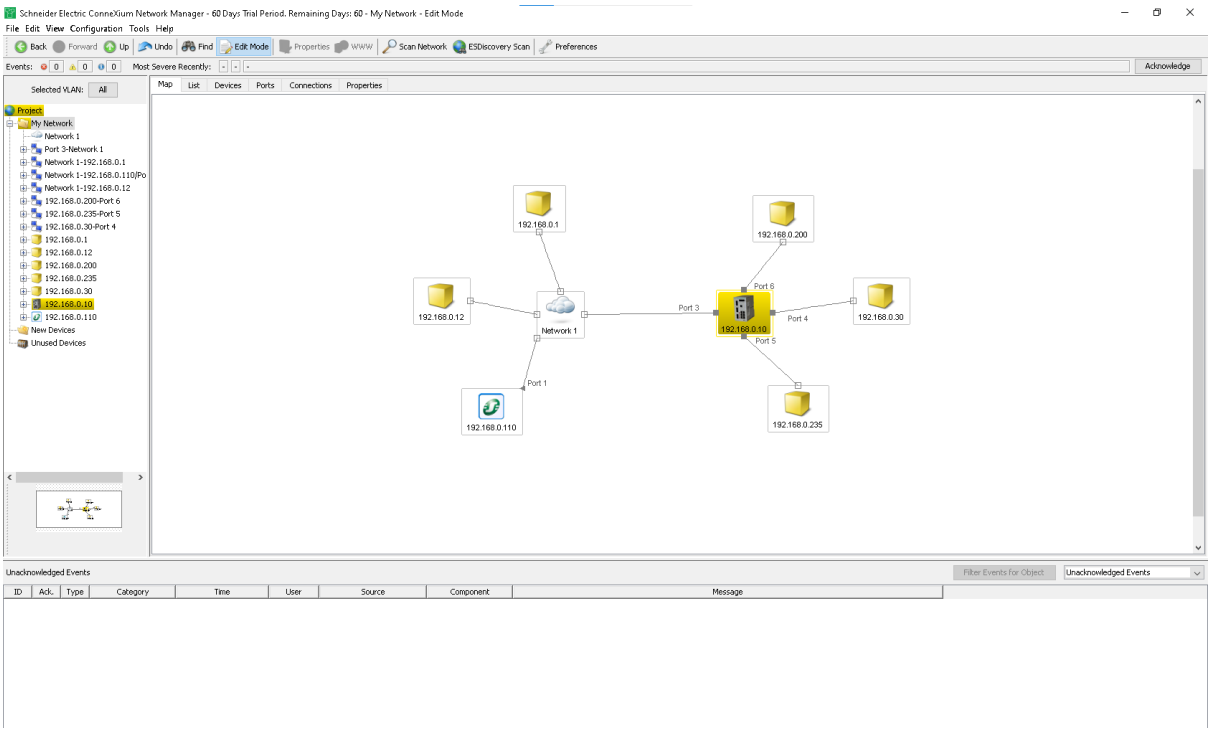


- A list of events according to the filtering set up:

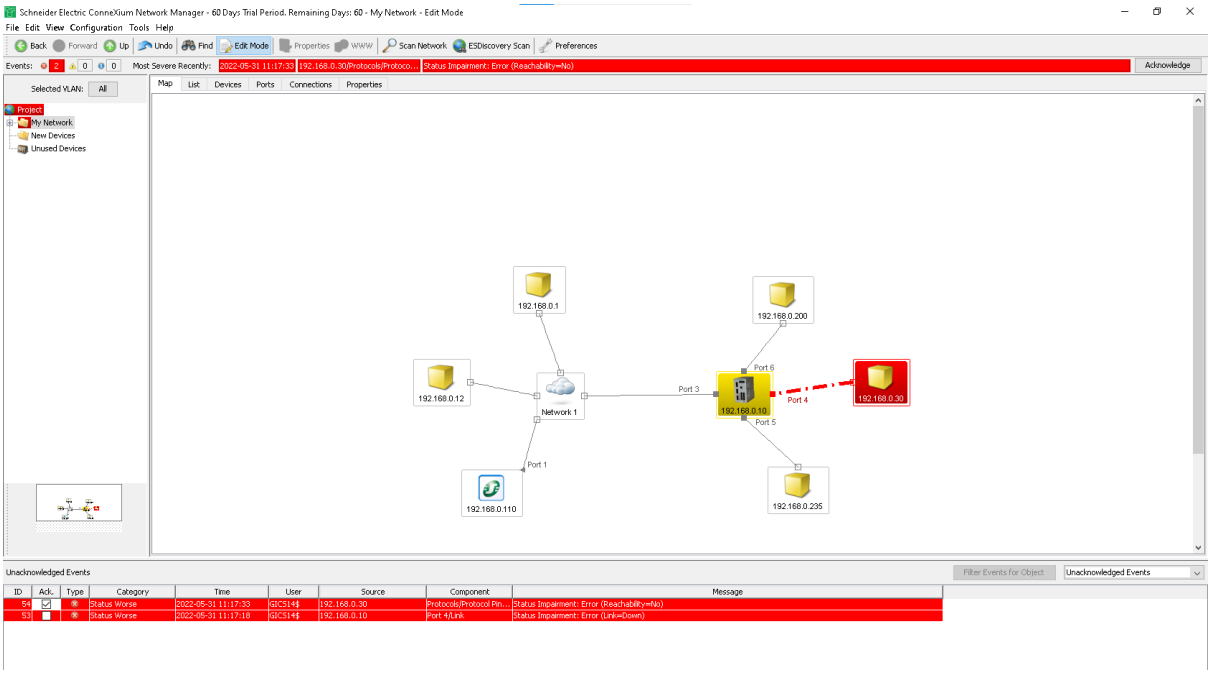


The software works by events: events (more or less important) occurring in the network are recorded using different protocols (ICMP, SNMP, ...). The user can then acknowledge or not these events: he operates as a supervisor and can intervene (or have a competent person intervene) on the network (physically or remotely) if necessary.

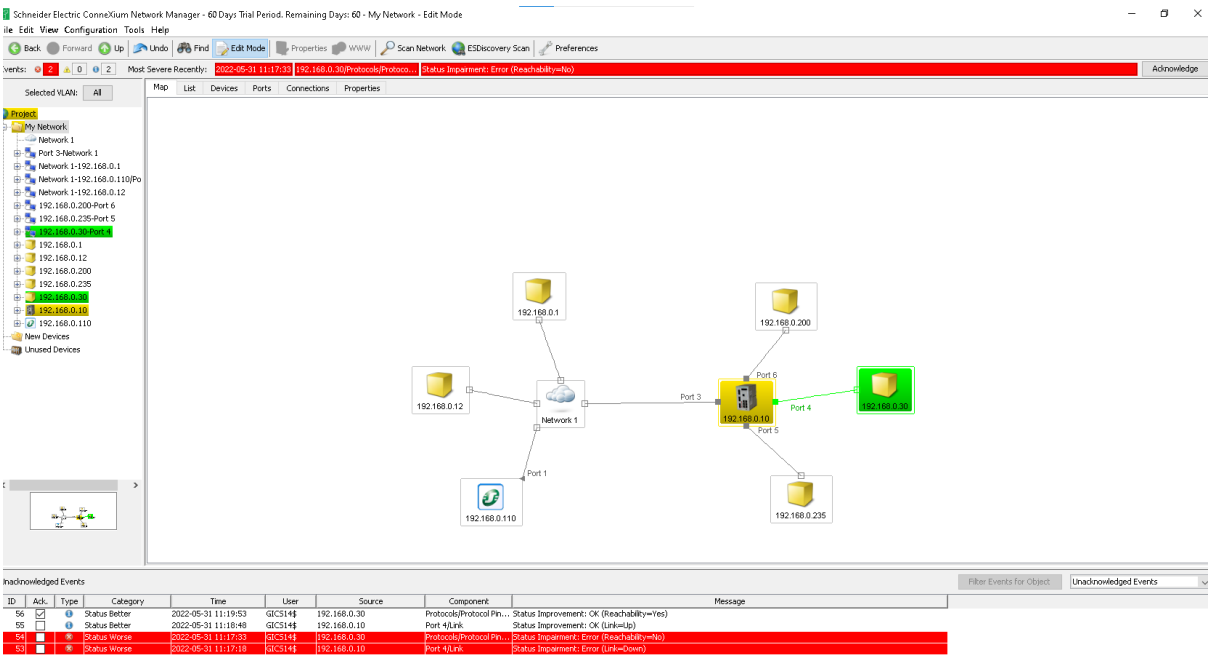
The graph of the network equipment varies according to the events that occur, in a normal state without any particular event, it takes the following form



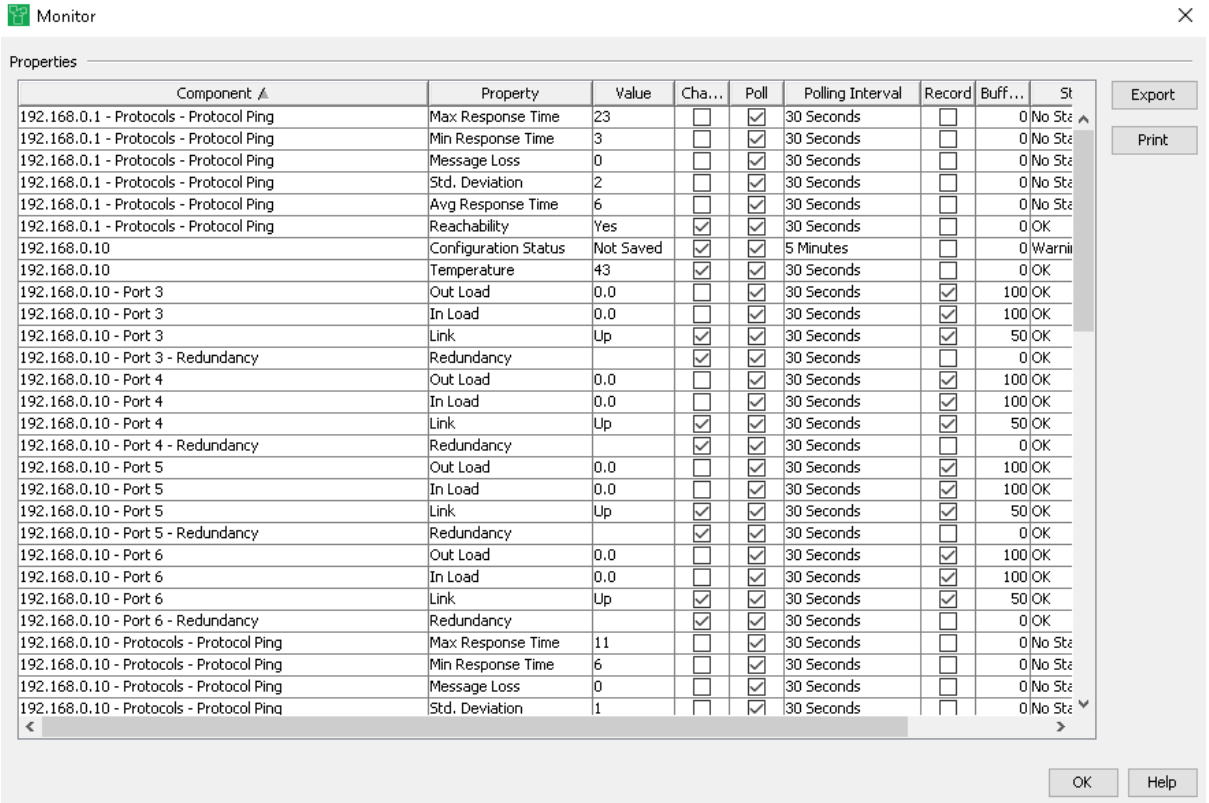
To highlight a malfunction, we can, for example, disconnect the Ethernet cable from the HMI, an event then occurs after a few moments, the HMI becomes unavailable:



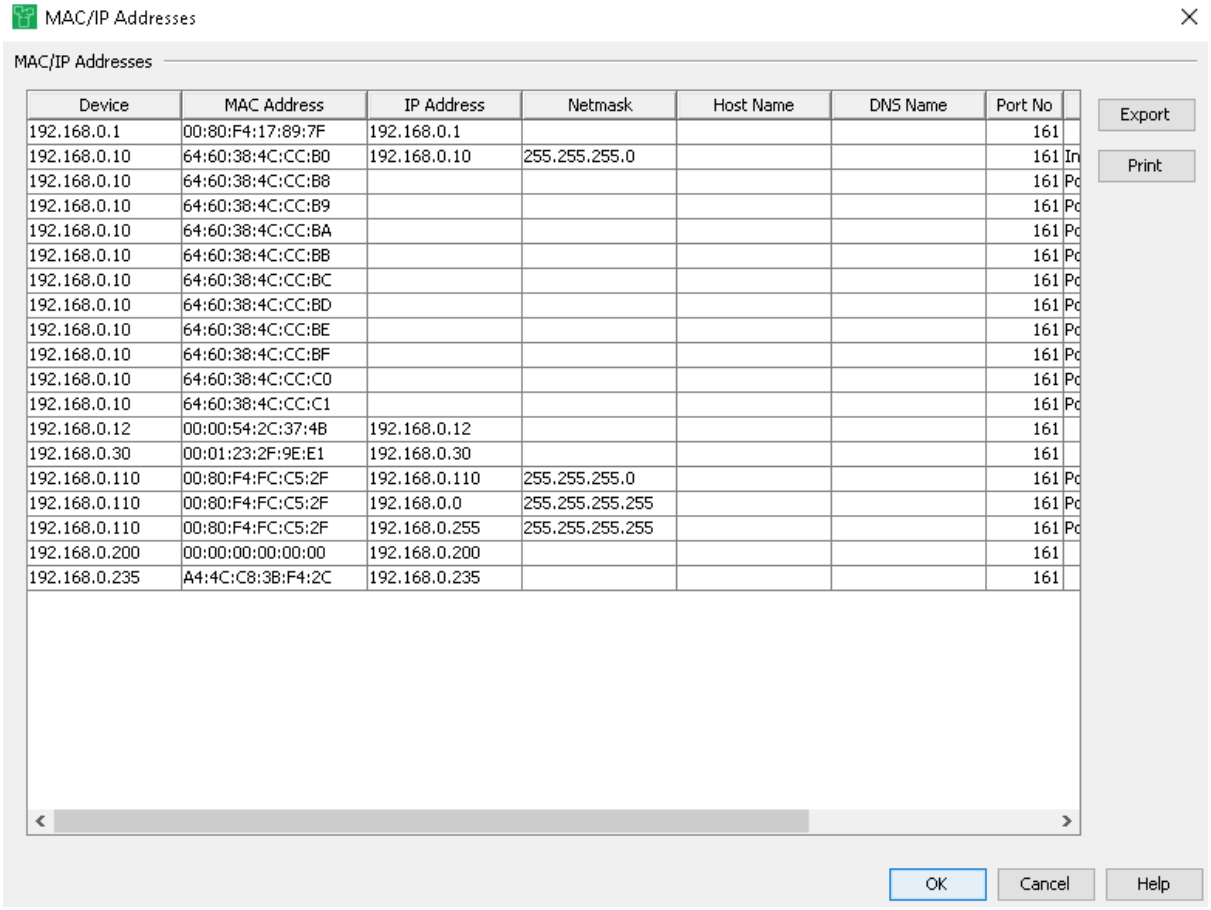
When the Ethernet cable is reconnected, the software will detect after a few seconds that access to the HMI is restored:



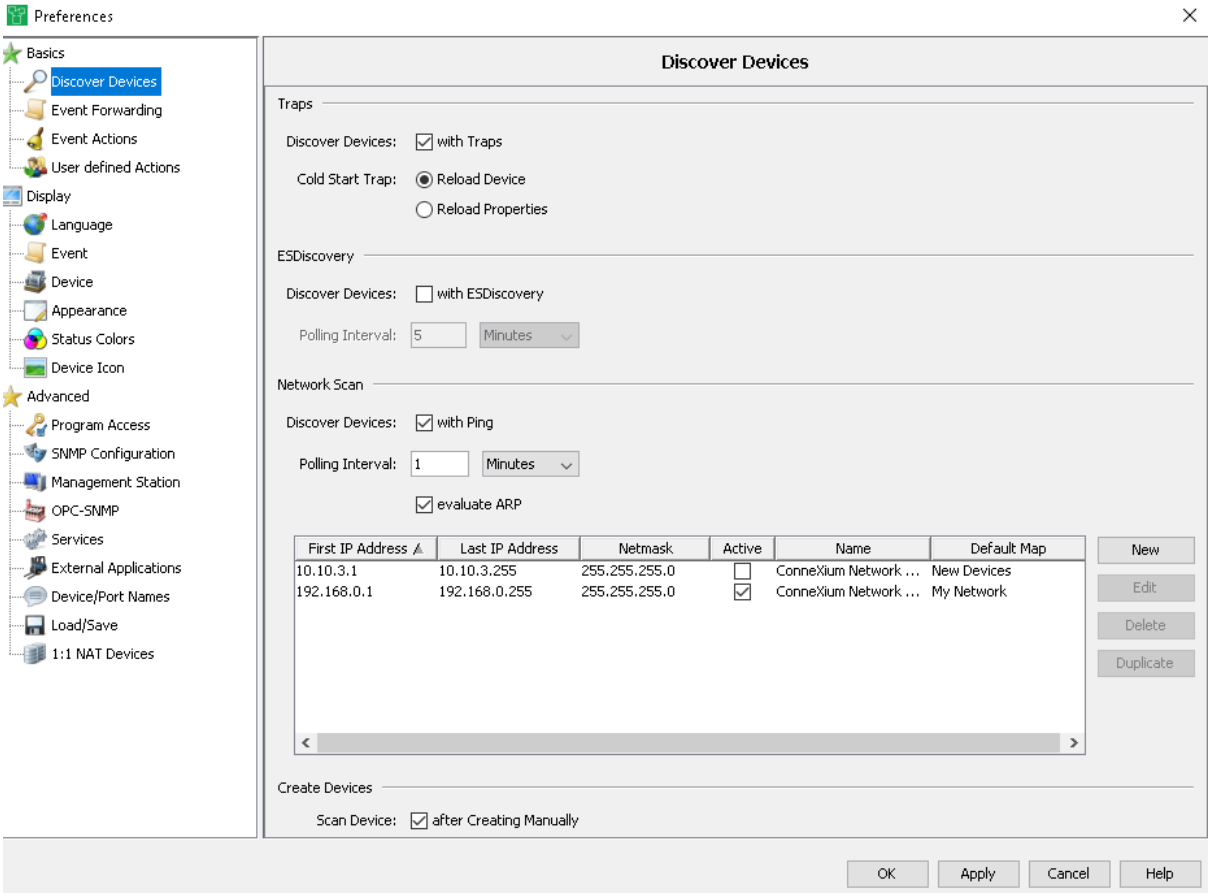
The menu Configuration > Monitor gives a lot of information about the state of the network, such as the results of the last ping made on a device, the state of the links etc... :



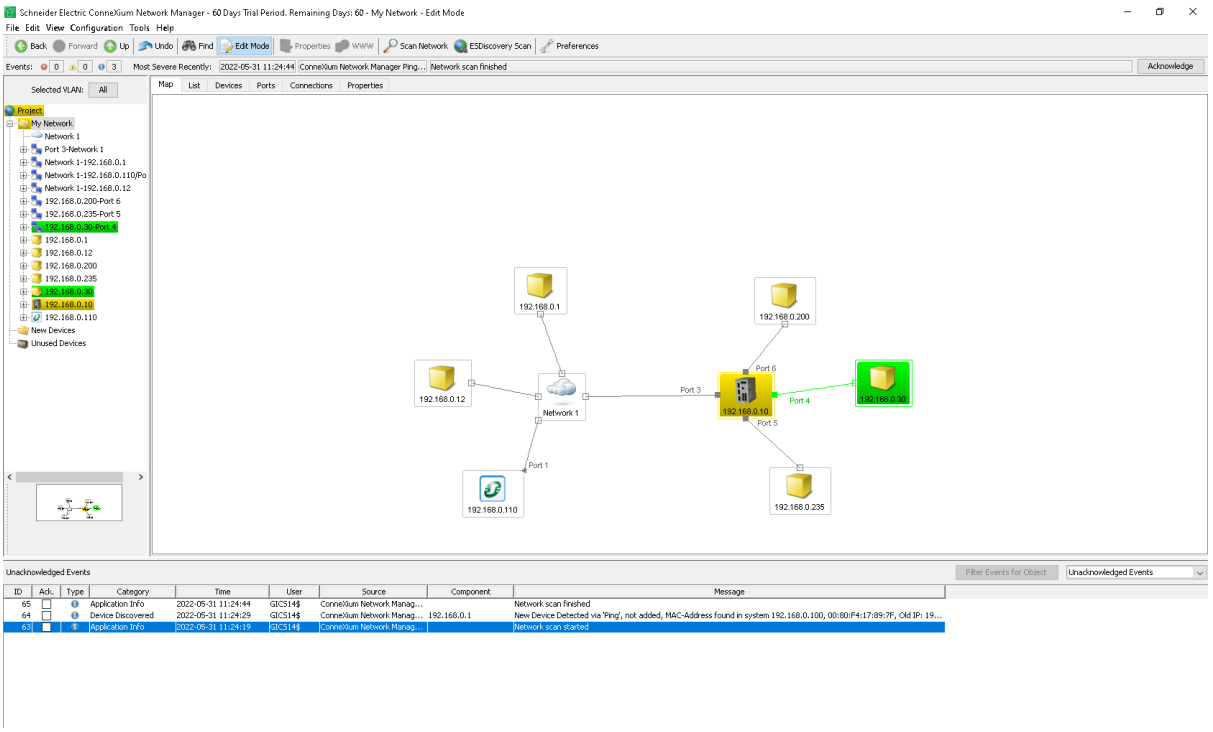
It is also possible to retrieve the complete list of devices with their associated MAC and IP addresses via the menu **Configuration > MAC/IP List** :



The **Configuration > Preferences** menu allows you to modify many useful parameters for a good network supervision, for example it is possible to establish a network scan at regular intervals. Define a network scan with Ping at 1-minute intervals:

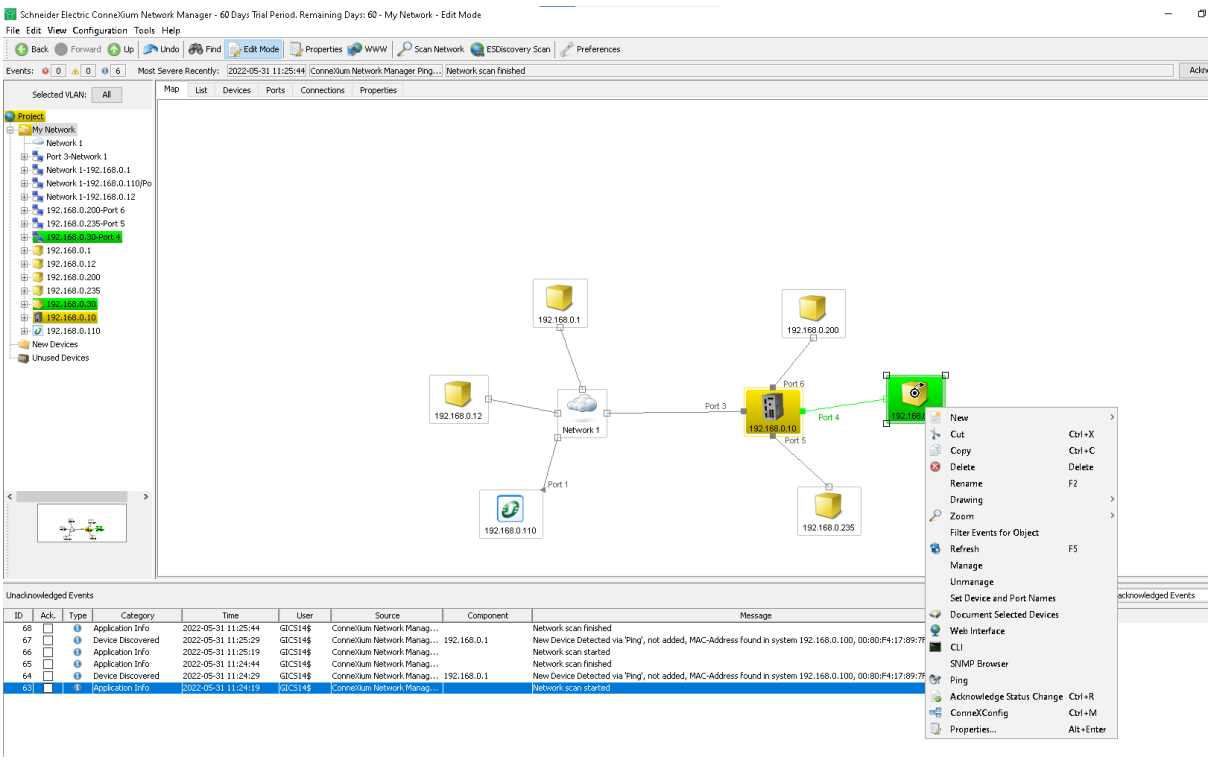


After one minute a network scan is automatically started:



N.B.: Regular network scans are very useful in network supervision. However, the refresh interval must be adapted according to the size of the network: the time of a network scan varies according to the number of IP addresses to be scanned in the IP range and the number of devices on the network.

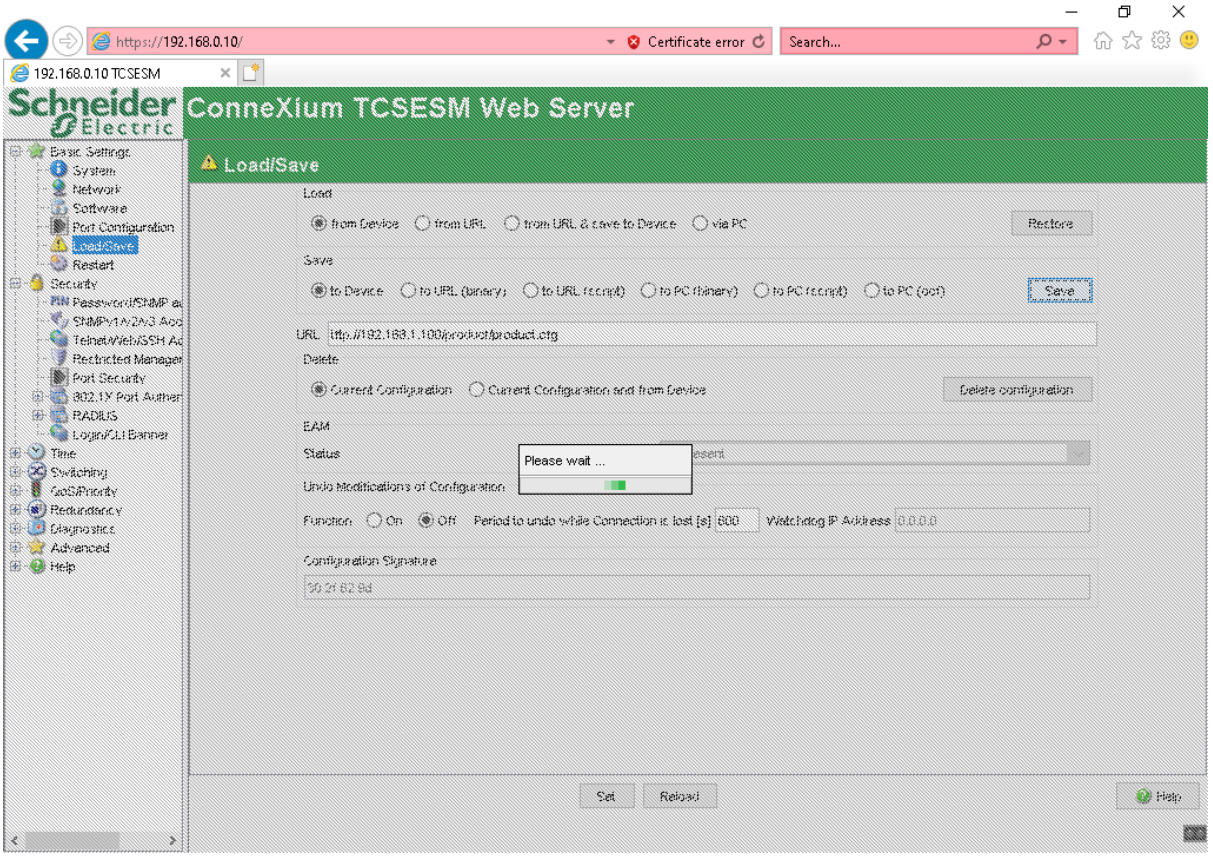
By right-clicking on a device, you can also perform several operations on the device, but also access (if available on the device) its services (Web, CLI, Ping, etc...):



Appendix 1: Saving the configuration

Once established, the switch configuration is not permanently saved on the switch. In particular, when the switch is rebooted, it will recover its previous configuration (the factory configuration if no configuration has been saved).

To save your configuration, go to the **Basic Settings > Load/Save** tab and in the "**Save**" box, select "**to Device**" then click on the "**Save**" button. Wait for the backup to take place:



Warning: Make sure that the configuration is functional before saving!

N.B.: It is also possible to save the configuration on your PC and load it from your PC. However, it is recommended to always have a backup on the switch so that it can reload the correct configuration in case of reboot. A sample configuration is provided "switch-config-sample.cfg".

Appendix 2: Reset to factory state

In order to be able to run this test again, it is possible to reset the switch to its factory state. To do this, go to the **Basic Settings > Load/Save** tab, in the "**Delete**" box, select "**Current Configuration and from Device**" then click on the "**Delete configuration**" button. The switch will then return to its original configuration.