



# NWC OT Cybersecurity TCBU L1 Devices Hardening Design

National Water Company (NWC), KSA  
SCADA/OT Information Security Implementation Project

Document Number: A01001045-TCBU-HDN-L1  
Document Title: NWC OT Cybersecurity TCBU L1 Devices Hardening Design  
Document Version: 0  
NWC Contract No.: 101200487  
[atm] PO Ref.: ATMPO2020-034

## NOTES AND COPYRIGHTS

The information contained in this document is confidential, privileged, and only for the intended recipient's information and may not be used, published, or redistributed without the prior written consent of ACET Solutions LLC. This document contains confidential, sensitive information of National Water Company (NWC).

Information contained herein is for the sole use of the customer (NWC) receiving this document. Acceptance of the document by the customer constitutes agreement by the customer & ACET Solutions that either party shall not disclose confidential information to any third party and shall not transmit any documents or copies thereof containing confidential information to any third party except as may be authorized in writing by NWC & ACET Solutions.

NWC has contracted this project to [atm] under contract number 101200487. ACET Solutions is the technical consultant of [atm] responsible for planning and execution of this project. All references to ACET Solutions in this document should be construed as [atm]/ACET Solutions for contractual purpose. Acceptance of this deliverable by NWC shall meet the requirements of the respective deliverable under NWC contract number 101200487.

No part of this document may be used, translated into another language, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written approval from ACET Solutions.

Questions or comment regarding this deliverable should be directed to the ACET Solutions Project Director.

ACET Solutions LLC  
1400 Broadfield Blvd Suite 200  
Houston TX, 77084  
Email: [sales@acetsolutions.com](mailto:sales@acetsolutions.com) | URL: [www.acetsolutions.com](http://www.acetsolutions.com)

## APPROVALS

| Name   | Company        | Signature | Date |
|--|----------------|-----------|------|
| Mubarik Mustafa<br>(Project Director)        | ACET Solutions |           |      |
| Abdulhadi G. Alshammari<br>(Project Manager) | NWC            |           |      |
| Ahmed I. Almutairi<br>(Project Sponsor)      | NWC            |           |      |

## REVISION HISTORY

| Rev No. | Date             | Author | Checked By | Approved By | Comments |
|---------|------------------|--------|------------|-------------|----------|
| 00      | 15 February 2022 | AMS    | RAS        | MM          |          |
|         |                  |        |            |             |          |
|         |                  |        |            |             |          |
|         |                  |        |            |             |          |

## GLOSSARY

| Acronyms | Meaning   |
|----------|---|
| ACL      | Access Control Lists                            |
| AD       | Active Directory                                |
| ADC      | Additional Domain Controller                    |
| ATM      | Advance System and Technology                   |
| ATP      | Adaptive Threat Protection                      |
| BOM      | Bill of Material                                |
| BU       | Business Unit                                   |
| BYOD     | Bring Your Own Device                           |
| CAP      | Client Authorization Policy                     |
| CAS      | Central Administration Server                   |
| CIP      | Critical Infrastructure Protection              |
| CMC      | Central Management Console (Nozomi)             |
| CSMS     | Cyber Security Management System                |
| DCS      | Distributed Control System                      |
| DLD      | Detailed-Level Design                           |
| DMZ      | Demilitarized Zone                              |
| DNS      | Domain Name System                              |
| DNS      | Domain Name System                              |
| ECC      | Essential Cybersecurity Controls                |
| ePO      | ePolicy Orchestrator                            |
| EPP      | End Point Protection                            |
| GPS      | Global Positioning System                       |
| HCIS     | High Commission for Industrial Security         |
| HLD      | High Level Design                               |
| HMI      | Human Machine Interface                         |
| HSE      | Health, Safety, And Environmental               |
| ICS      | Industrial Control System                       |
| IDS      | Intrusion detection System                      |
| IPS      | Intrusion Prevention System                     |
| ISA      | International Society of Automation             |
| ISO      | International Organization for Standardization  |
| IT       | Information Technology                          |
| JCBU     | Jeddah Central Business Unit                    |
| KSA      | Kingdom of Saudi Arabia                         |
| MBSS     | Minimum Baseline Security Standards             |
| MCBU     | Makkah Central Business Unit                    |
| MDCBU    | Madinah Central Business Unit                   |
| MGMT     | Management                                      |
| NCA      | National Cybersecurity Authority                |
| NERC     | North American Electric Reliability Corporation |
| NGFW     | Next Generation Firewall                        |

| Acronyms | Meaning   |
|----------|---|
| NIST     | U.S. National Institute of Standards and Technology |
| NTP      | Network Time Protocol                               |
| NWC      | National Water Company                              |
| OT       | Operational Technology                              |
| PDC      | Primary Domain Controller                           |
| PLC      | Programmable Logic Controller                       |
| RAP      | Resource Authorization Policy                       |
| RCBU     | Riyadh Central Business Unit                        |
| RD       | Remote Desktop                                      |
| RDS      | Remote Desktop Services                             |
| RTO      | Recovery Time Objective                             |
| RPO      | Recovery Point Objective                            |
| SCADA    | Supervisory Control and Data Acquisition            |
| SIEM     | Security Incident & Event Management Solution       |
| SSL      | Secure Socket Layer                                 |
| TCBU     | Taif Central Business Unit                          |
| VLAN     | Virtual Local Area Network                          |
| VM       | Virtual Machine                                     |
| VPN      | Virtual Private Network                             |

## REFERENCE DOCUMENTS

| S/N | Document No.                  | Title   |
|-----|-------------------------------|---|
| 1   | A01001045-HLD-ARCH.00         | NWC OT Cybersecurity HLD Reference Architecture   |
| 2   | A01001045-HLD                 | NWC OT Cybersecurity High-Level Design  |
| 3   | A01001045-INV.00              | NWC SCADA/OT Asset Inventory  |
| 4   | ECC – 1: 2018                 | KSA NCA Essential Cybersecurity Controls (ECC – 1: 2018)  |
| 5   | ISA–62443-1-1 (99.01.01)–2007 | Security for Industrial Automation and Control Systems<br>Part 1-1: Terminology, Concepts, and Models |

## Table of Contents

|   |    |
|---|----|
| 1. Document purpose.....                            | 7  |
| 2. TCBU Level 1 Device Hardening Settings.....      | 7  |
| 2.1 Modicon Quantum & Premium .....                 | 7  |
| 2.2 Siemens S7-1200, S7-400 & S7-300 .....          | 11 |
| 2.3 Rockwell MICROLogix 1400 .....                  | 13 |
| 2.4 Motorola ACE3600 .....                          | 14 |
| 2.5 Seimens SCALANCE-X-204 .....                    | 14 |
| 2.6 ConneXium TCSESM, TCSESM-E Managed Switch ..... | 15 |

## 1. DOCUMENT PURPOSE

The purpose of this document is to describe the Hardening Configuration of different L1 Devices in TCBU.

Following are list of L1 Devices installed at sites:

- Modicon Quantum & Premium
- Siemens S7-1200, 400 & 300
- Rockwell MicroLogix 1400
- Motorola ACE3600
- Siemens Scalene X-204
- ConneXium TCSESM

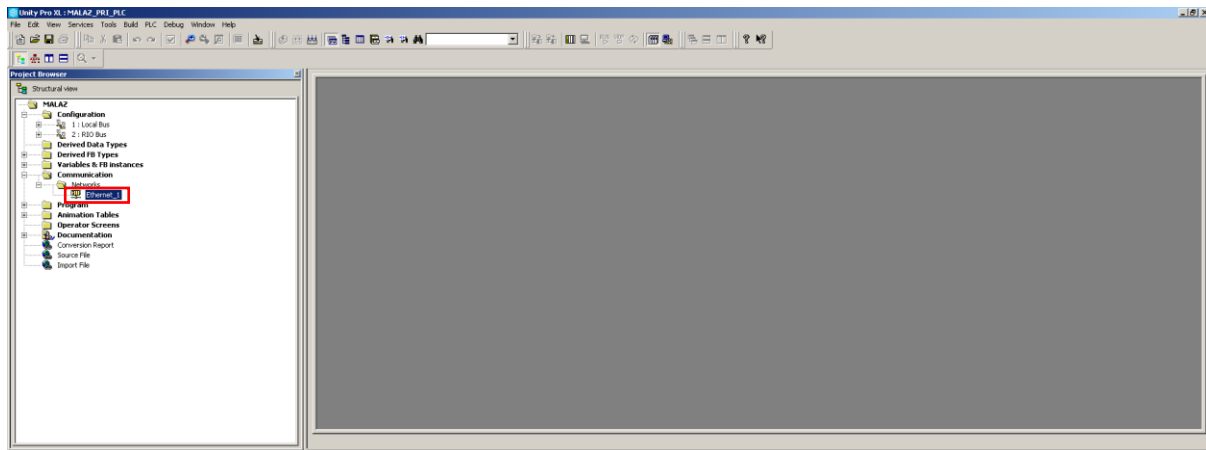
## 2. TCBU LEVEL 1 DEVICE HARDENING SETTINGS

### 2.1 MODICON QUANTUM & PREMIUM

- Upgrade firmware
- Set password for security lock feature
- Disable HTTP/FTP ethernet services

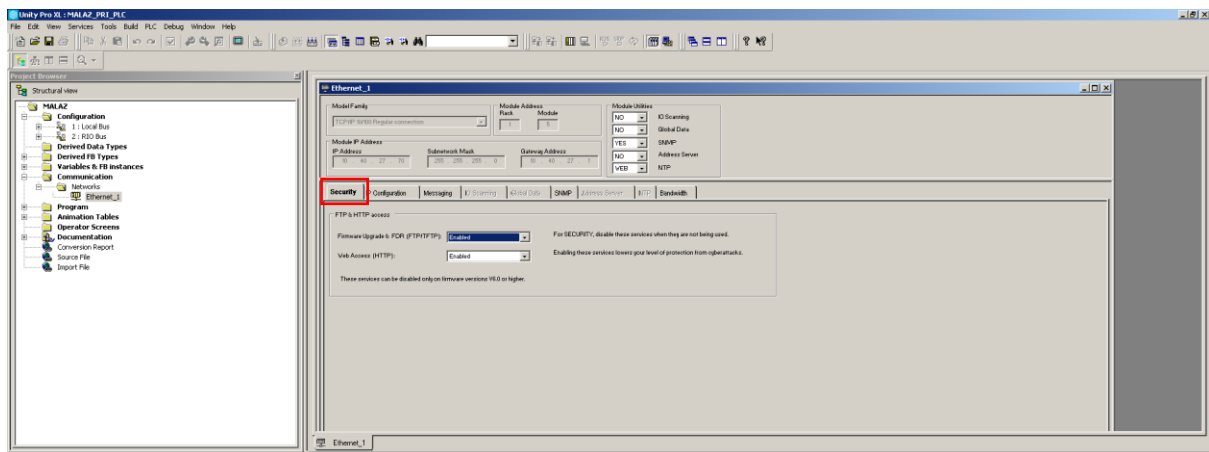
Following is the procedure of how to disable HTTP/FTP services:

Step 1: Select Communication >> Networks >> Ethernet\_1

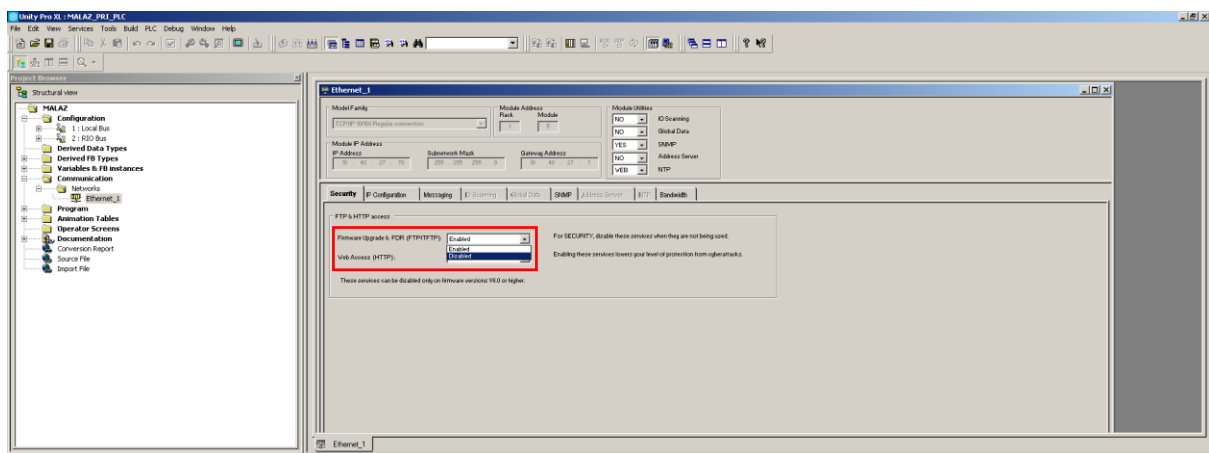




## Step 2: Select Security tab in Ethernet\_1 window



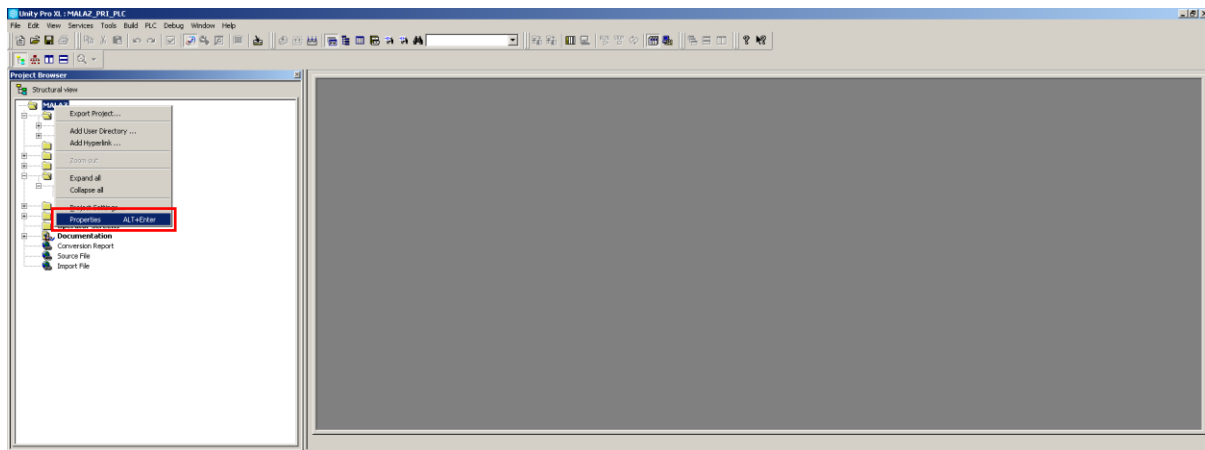
## Step 3: In security tab, disable HTTP/FTP services



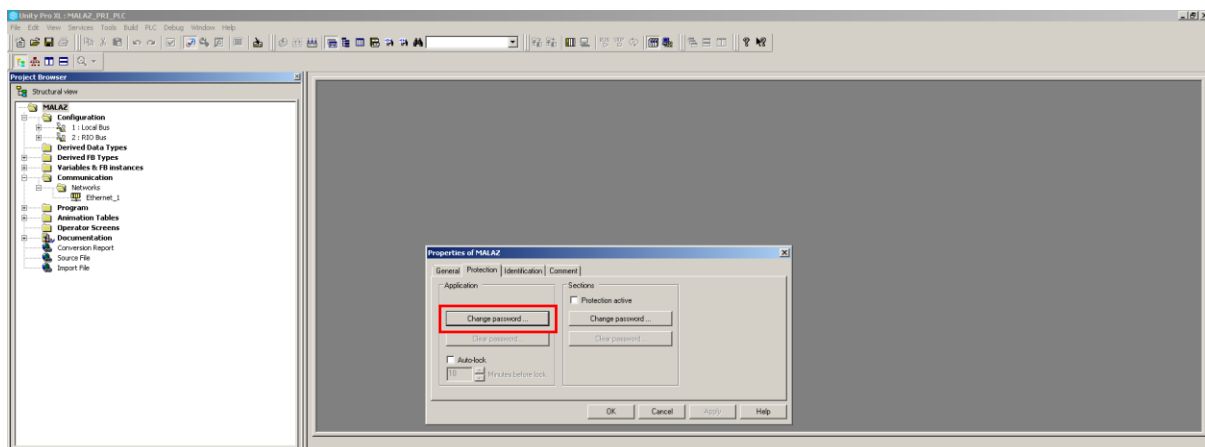


Following is the procedure to password protect the application:

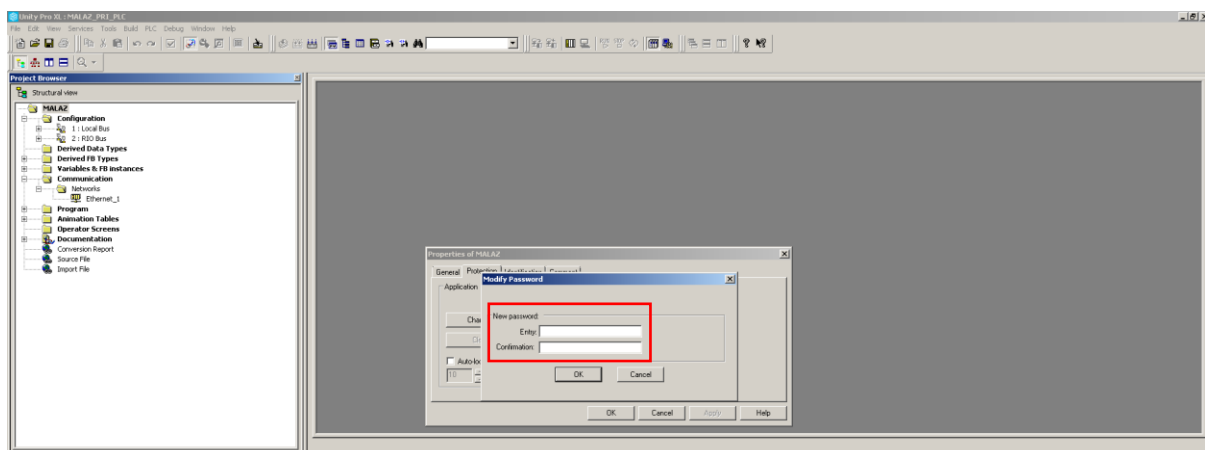
Step 1: Select the project and right click to select the properties



Step 2: Select "Protection" tab in properties, select change password



Step 3: Enter the new password and confirm it



For IP Setting:

Step 1: Go to Communication > Networks > Ethernet\_1 and double click Ethernet\_1

The screenshot shows the 'Ethernet\_1' configuration window. The 'Model Family' is set to 'TCP/IP 10/100 Regular connection'. The 'Module Address' section has 'Rack', 'Module', and 'Channel' fields. The 'Module IP Address' section shows 'IP Address' as '0 . 0 . 0 . 0', 'Subnetwork Address' as '255 . 0 . 0 . 0', and 'Gateway Address' as '0 . 0 . 0 . 0'. The 'Module Utilities' section has dropdowns for 'IO Scanning' (NO), 'Global Data' (NO), 'SNMP' (YES), 'Address Server' (NO), and 'NTP' (WEB). The 'Messaging' tab is selected, showing a 'Connection configuration' table with columns 'Access' and 'IP address'. The 'Access Control' checkbox is unchecked.

|    | Access                              | IP address |
|----|-------------------------------------|------------|
| 1  | <input checked="" type="checkbox"/> |            |
| 2  | <input checked="" type="checkbox"/> |            |
| 3  | <input checked="" type="checkbox"/> |            |
| 4  | <input checked="" type="checkbox"/> |            |
| 5  | <input checked="" type="checkbox"/> |            |
| 6  | <input checked="" type="checkbox"/> |            |
| 7  | <input checked="" type="checkbox"/> |            |
| 8  | <input checked="" type="checkbox"/> |            |
| 9  | <input checked="" type="checkbox"/> |            |
| 10 | <input checked="" type="checkbox"/> |            |
| 11 | <input checked="" type="checkbox"/> |            |
| 12 | <input checked="" type="checkbox"/> |            |

Step 2: Select the IP Configuration tab and change the IP settings

The screenshot shows the 'Ethernet\_1' configuration window with the 'IP Configuration' tab selected. The 'Model Family' is 'TCP/IP 10/100 Regular connection'. The 'Module Address' section has 'Rack', 'Module', and 'Channel' fields. The 'Module IP Address' section shows 'IP Address' as '13 . 12 . 10 . 14', 'Subnetwork Address' as '25 . 25 . 0 . 0', and 'Gateway Address' as '13 . 12 . 10 . 1'. The 'Module Utilities' section has dropdowns for 'IO Scanning' (NO), 'Global Data' (NO), 'SNMP' (YES), 'Address Server' (NO), and 'NTP' (WEB). The 'IP address configuration' section has radio buttons for 'Configured' (selected) and 'From a server'. The 'Ethernet configuration' section has radio buttons for 'Ethernet II' (selected) and '802.3'.

IP address configuration

☒ Configured

IP address: 13 . 12 . 10 . 14

Subnetwork mask: 25 . 25 . 0 . 0

Gateway address: 13 . 12 . 10 . 1

☐ From a server

Ethernet configuration

☒ Ethernet II ☐ 802.3

For firmware upgrade, see "Attachment 1-Section 2.1 - Modicon Quantum\_Firmware Upgrade Process"

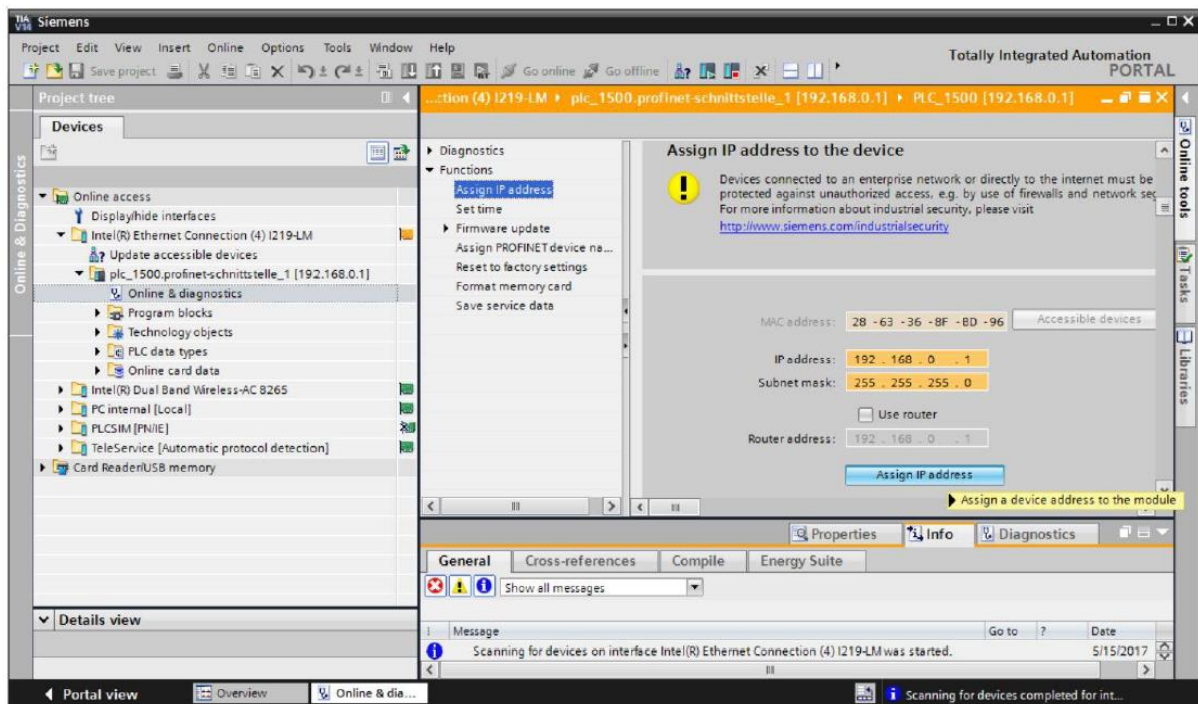
## 2.2 SIEMENS S7-1200, S7-400 & S7-300

- Upgrade firmware
- Set password for security lock feature
- Disable HTTP/FTP ethernet services

For IP Setting:

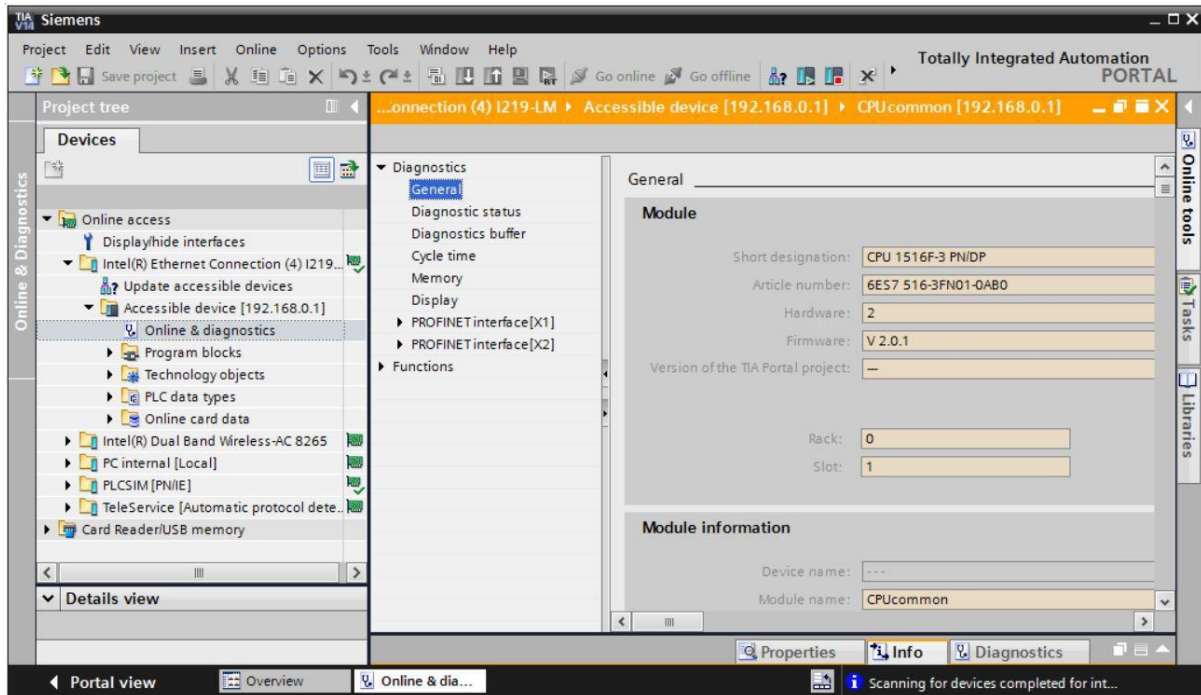
Step 1: Go to "Online & Diagnostics"

Step 2: Under "Functions", you now find the "Assign IP address" item. Enter the following IP address here (example): IP address: 192.168.0.1 Subnet mask 255.255.255.0. Next, click "Assign IP address" and this new address will be assigned.

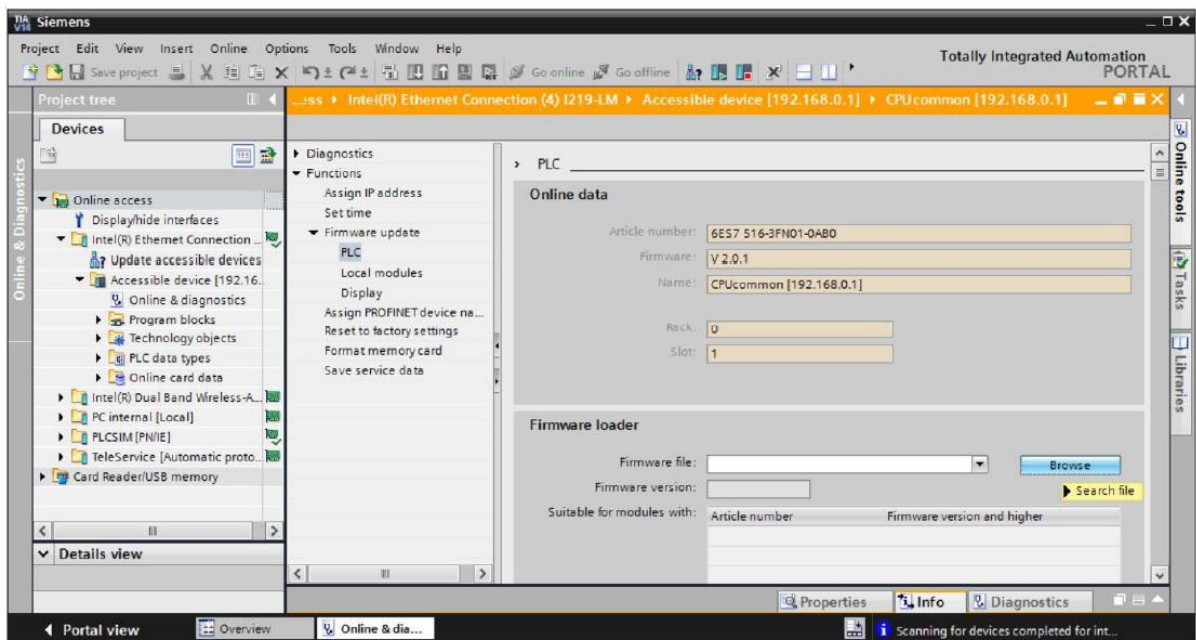


For firmware upgrade:

Step 1:

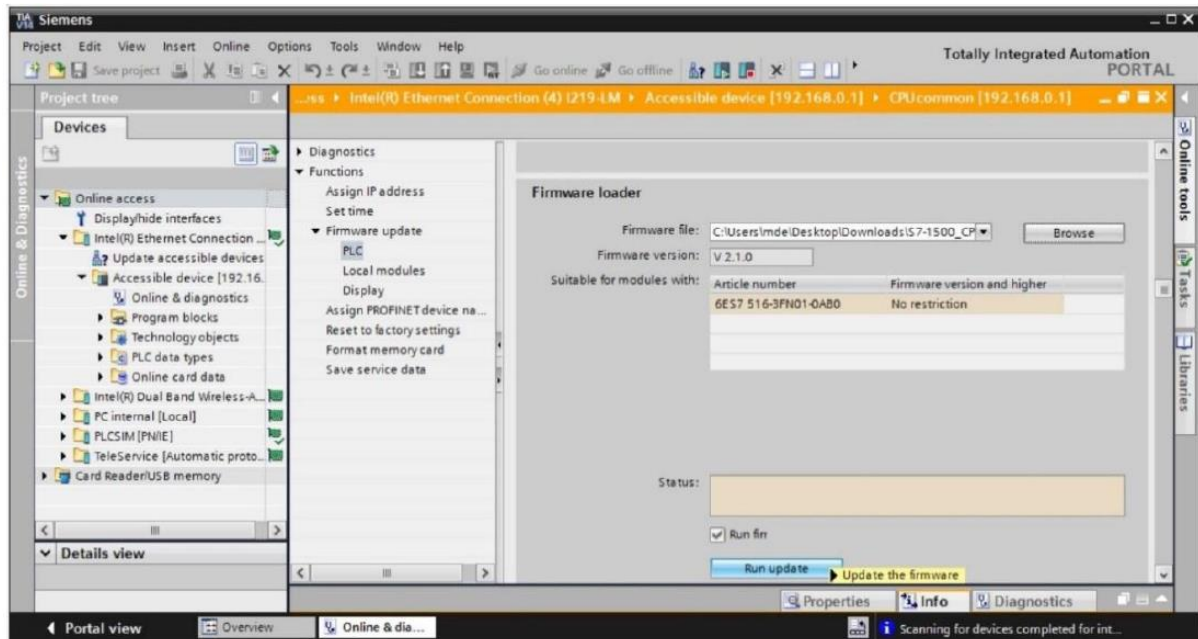


Step 2: In the "Functions" menu, change to "Firmware update" > "PLC". In the "Firmware loader" sub-item, click "Browse".

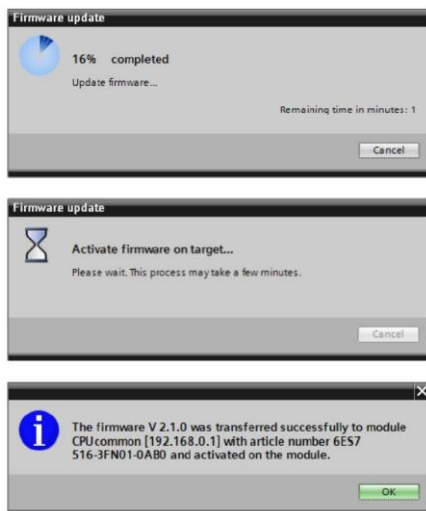


Step 3: Select the downloaded and extracted firmware file.

Step 4: The following dialog indicates whether your firmware file is compatible with your CPU. Now start the update. ("Run update")



Step 5: The progress of the update and its successful completion are indicated with the following dialogs. Click "OK" to confirm.



## 2.3 ROCKWELL MICROLOGIX 1400

- Upgrade firmware
- Set password for security lock feature
- Disable HTTP/FTP ethernet services

For IP Setting:



Step 1: Using RS Logix 500, go to Channel configuration, Channel 1, uncheck the BootP/DHCP tick box, edit the IP and subnet mask fields (gateway too if necessary), then apply the changes.

Step 2: Power cycle the PLC.

For firmware upgrade, refer to the “Attachment 2-MicroLogix 1400 Firmware Upgrade”.

## 2.4 MOTOROLA ACE3600

- Upgrade firmware
- Set password for security lock feature
- Disable HTTP/FTP ethernet services

For IP Change refer to the “Attachment 3-Motorola ACE3600 IP Config”.

For Firmware Upgrade refer to “Attachment 4-Motorola ACE3600 Firmware Upgrade”.

## 2.5 SEIMENS SCALANCE-X-204

- Default username and password should be changed

**Note Default password when supplied • For Admin: admin • For the user: user.**

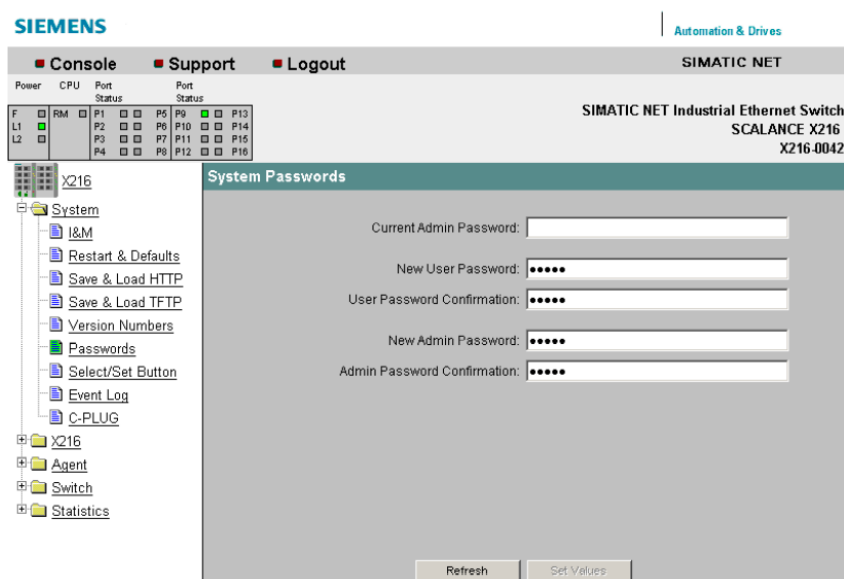


Figure 7-7 System Passwords

Table 7-7 System Passwords - CLISYSTEM>

| Command   | Description  | Comment            |
|---|--|--------------------|
| <code>password &lt;admin   user&gt; &lt;password&gt;</code> | Sets a new password for the user or administrator. | Administrator only |

- Unused Port should be block for Managed switch

- IP http/telnet/ftp should be disabled only HTTPs/ssh/sftp should be used
- Serial Access should be password Protected
- Should configure the Login Banner
- Firmware needs to be upgraded from vendor release

## 2.6 CONNEXIUM TCSESM, TCSESM-E MANAGED SWITCH

- Default username and password should be changed

---

*Figure 3: Logging in to the Command Line Interface program*

- Enter a user name. The default setting for the user name is **admin**. Press the Enter key.
- Enter the password. The default setting for the password is **private**. Press the Enter key.  
You can change the user name and the password later in the Command Line Interface.  
Please note that these entries are case-sensitive.

The start screen appears.

**Note:** For a TCSESM Switch, the preset CLI prompt is (Schneider Electric TCSESM) >, for a TCSESM-E Switch it is (Schneider Electric TCSESM-E) >.

- Unused Port should be blocked for Managed switch



### ■ Switching the port on and off

In the state on delivery, all the ports are switched on. For a higher level of access security, switch off the ports at which you are not making any connection.

- ☐ Select the Basics:Port Configuration dialog.
- ☐ In the "Port on" column, select the ports that are connected to another device.

### ■ Selecting the operating mode

In the state on delivery, all the ports are set to the "Automatic configuration" operating mode.

**Note:** The active automatic configuration has priority over the manual configuration.

- ☐ Select the Basics:Port Configuration dialog.
- ☐ If the device connected to this port requires a fixed setting
  - select the operating mode (transmission rate, duplex mode) in the "Manual configuration" column and
  - deactivate the port in the "Automatic configuration" column.

- IP http/telnet should be disable only HTTPs/ssh should be used for access

```
enable
configure
```

Switch to the privileged EXEC mode.  
Switch to the Configuration mode.

31007122 - 03/2018

93

## Assistance in the Protection from Unauthorized Access

### 6.3 Telnet/Web/SSH access

```
lineconfig
transport input telnet
no transport input telnet
exit
exit
ip http server
no ip http server
```

Switch to the configuration mode for CLI.  
Enable Telnet server.  
Disable Telnet server.  
Switch to the Configuration mode.  
Switch to the privileged EXEC mode.  
Enable Web server.  
Disable Web server.

- Serial Access should be password Protected

- Should configure the Login Banner
- Firmware needs to be upgraded from vendor release



**ACET Solutions LLC**

1400 Broadfield Blvd Suite 200 Houston TX, 77084.  
United States of America.

Tel: +1 832 386 5593 | Fax: +1 832 201 0337

[sales@acetsolutions.com](mailto:sales@acetsolutions.com) | [www.acetsolutions.com](http://www.acetsolutions.com)