NWC OT Cybersecurity RCBU L1 Devices Hardening Design

National Water Company (NWC), KSA

SCADA/OT Information Security Implementation Project

Document Number:	A01001045-RCBU-HDN-L1
Document Title:	NWC OT Cybersecurity RCBU L1 Devices Hardening Design
Document Version:	1
NWC Contract No.:	101200487
[atm] PO Ref.:	ATMPO2020-034

1400 Broadfield Blvd Suite 200 Houston TX, 77084
Tel: +1 832 386 5593 | Fax: +1 832 201 0337
Email: sales@acetsolutions.com |
URL: www.acetsolutions.com

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 by 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.

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 | URL: www.acetsolutions.com

APPROVALS

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

REVISION HISTORY

Rev No.	Date	Author	Checked By	Approved By	Comments
00	24-Aug-2021	HMA/UK	SH	MM	Issued For Approval
01	15-Nov-2021	HMA/UK	SH	MM	Issued For Approval

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
6	ECC – 1: 2018	KSA NCA Essential Cybersecurity Controls (ECC – 1: 2018)
7	ISA–62443-1-1 (99.01.01)–2007	Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models

Table of Contents

1. DOCUMENT PURPOSE

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

Following are list of L1 Devices installed in Malaz WTP:

- Modicon Quantum
- Schneider M340
- Siemens S7-1200
- Rockwell Micro-850
- Schneider Twido
- Delta DVP-20EX
- ELPRO 245UE

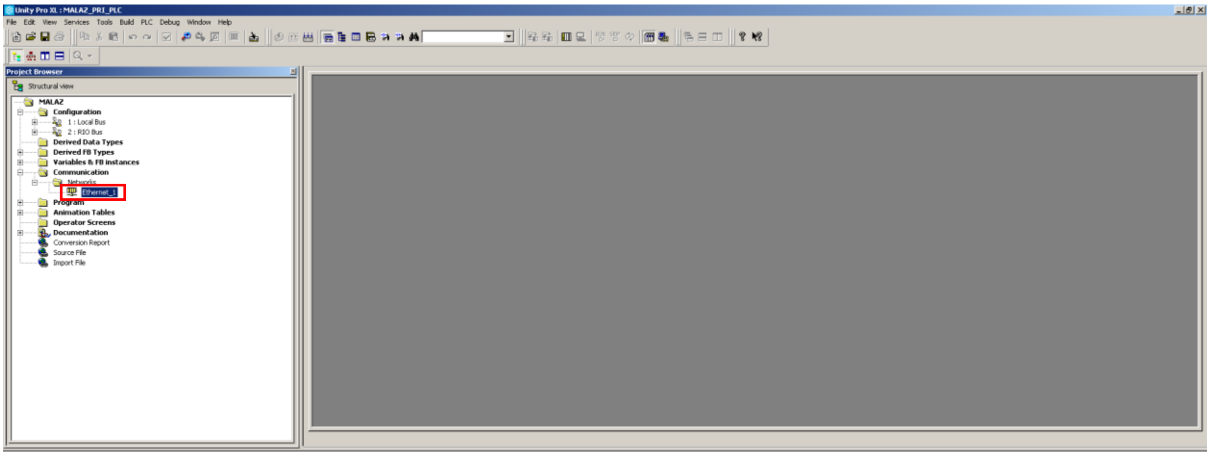
2. RCBU LEVEL 1 DEVICE HARDENING SETTINGS

2.1 MODICON QUANTUM HARDENING

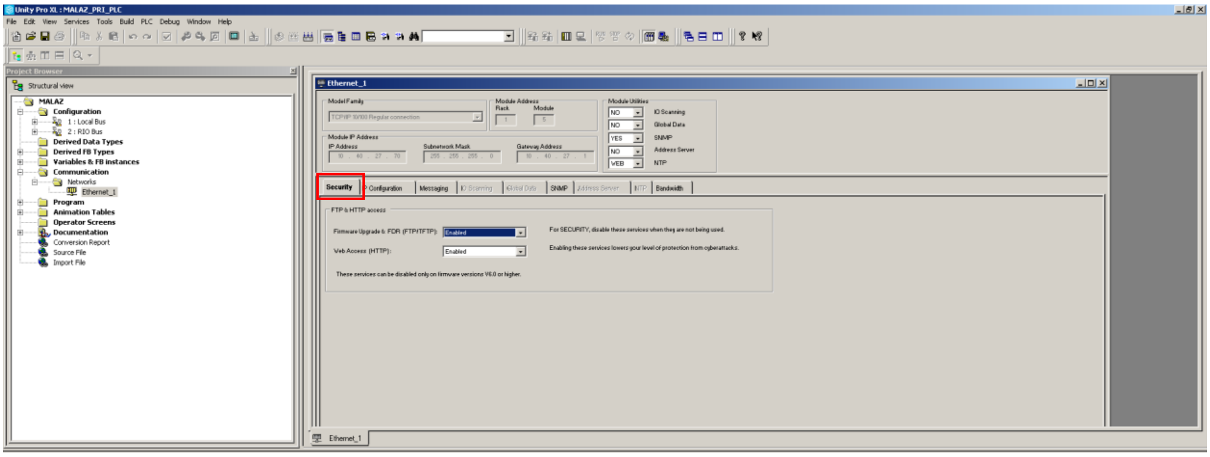
- Upgrade firmware
- Set password for security lock feature
- Disable HTTP/FTP ethernet services

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



Model Family: TCP/IP 10/100 Regular connection

Module Address: Rack 1, Module 5

Module IP Address: IP Address 10 . 40 . 27 . 70; Subnetwork Mask 255 . 255 . 255 . 0; Gateway Address 10 . 40 . 27 . 1

Module Utilities: NO IO Scanning; NO Global Data; YES SNMP; NO Address Server; WEB NTP

FTP & HTTP access

Firmware Upgrade & FDR (FTP/TFTP): Enabled

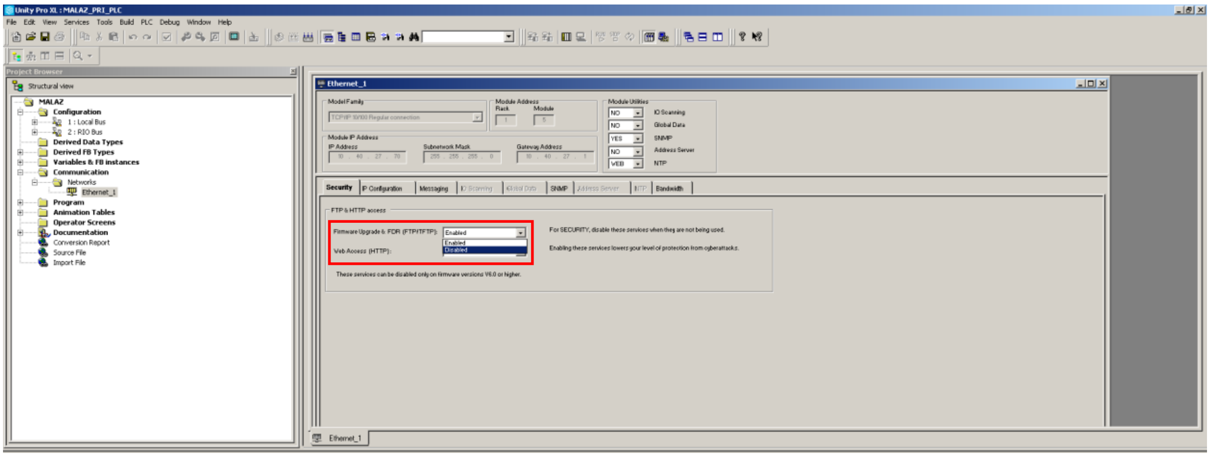
Web Access (HTTP): Enabled

For SECURITY, disable these services when they are not being used.

Enabling these services lowers your level of protection from cyberattacks.

These services can be disabled only on firmware versions V6.0 or higher.

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



Model Family: TCP/IP 10/100 Regular connection

Module Address: Rack 1, Module 5

Module IP Address: IP Address 10 . 40 . 27 . 70; Subnetwork Mask 255 . 255 . 255 . 0; Gateway Address 10 . 40 . 27 . 1

Module Utilities: NO IO Scanning; NO Global Data; YES SNMP; NO Address Server; WEB NTP

FTP & HTTP access

Firmware Upgrade & FDR (FTP/TFTP): Enabled

Web Access (HTTP):

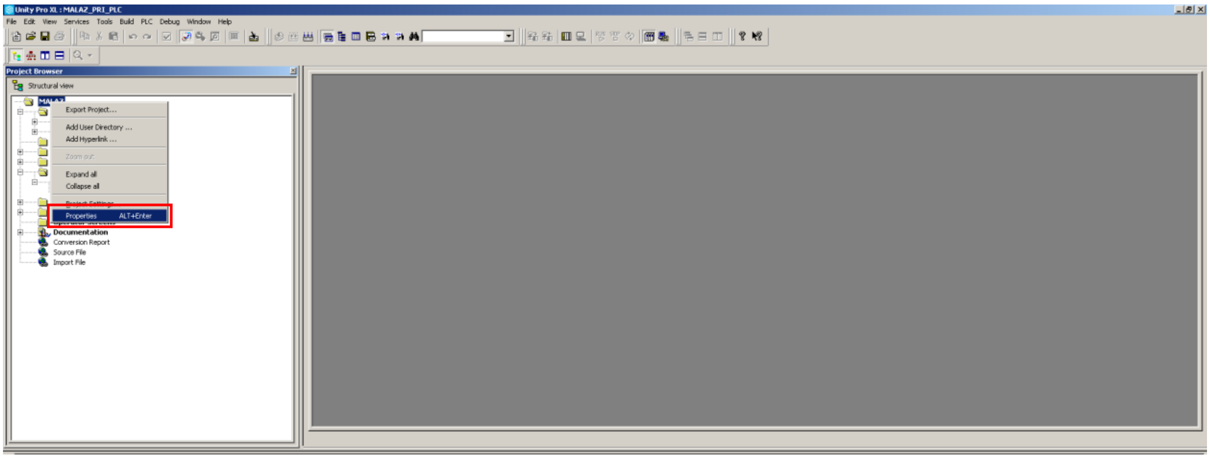
For SECURITY, disable these services when they are not being used.

Enabling these services lowers your level of protection from cyberattacks.

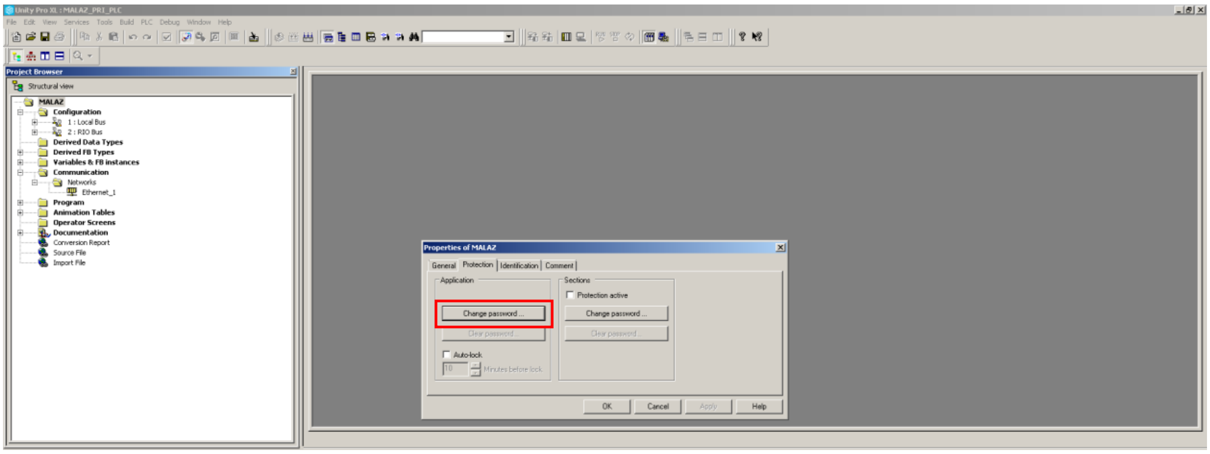
These services can be disabled only on firmware versions V6.0 or higher.

Following is the procedure of how to password protect the application:

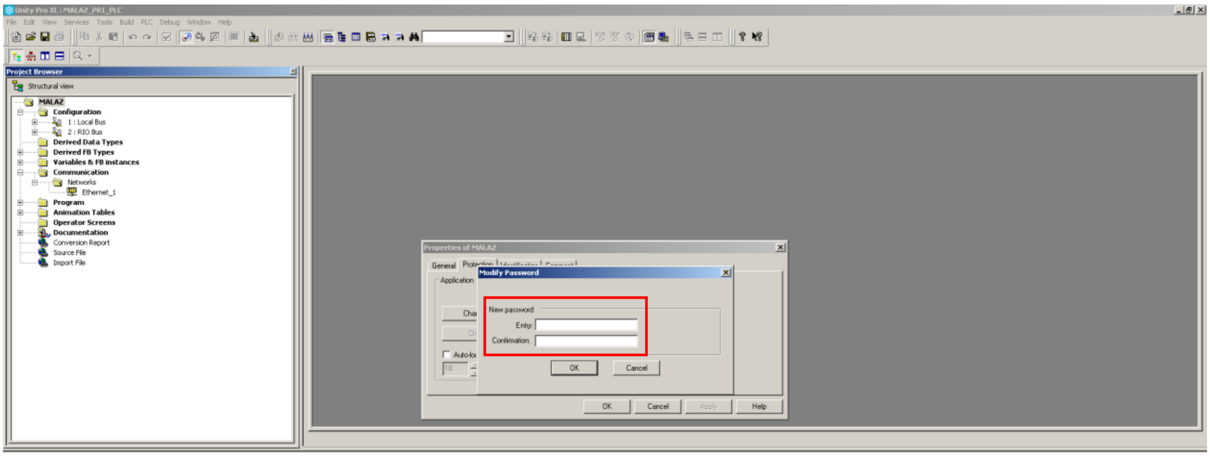
Step 1: Select the project and right click to select the properties



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



Step 3: Enter the new password and confirm it



For IP Setting, see attachment Section 2.1 - Modicon Quantum_Setting the IP Address

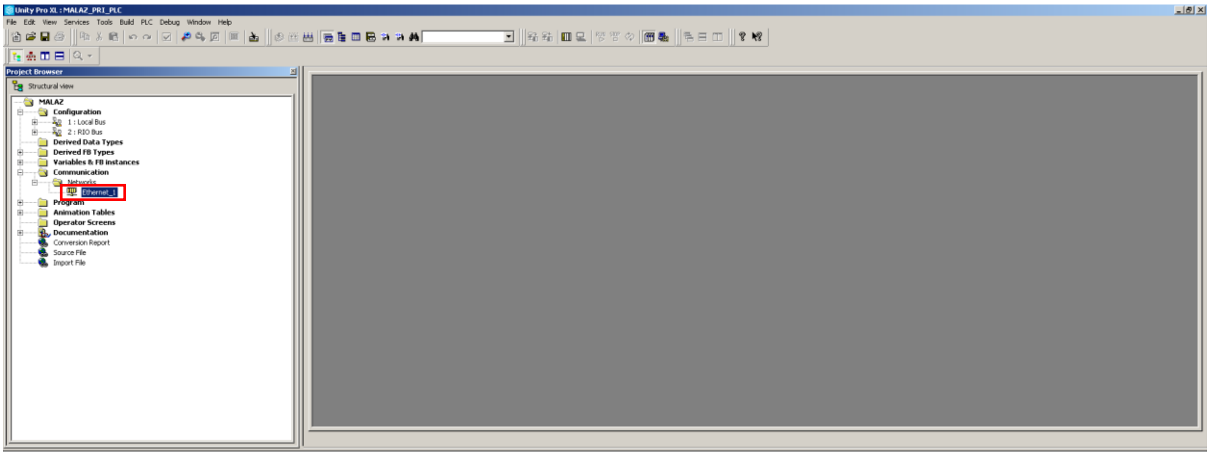
For firmware upgrade, see attachment Section 2.1 - Modicon Quantum_Firmware Upgrade Process

2.2 SCHNEIDER M340 HARDENING

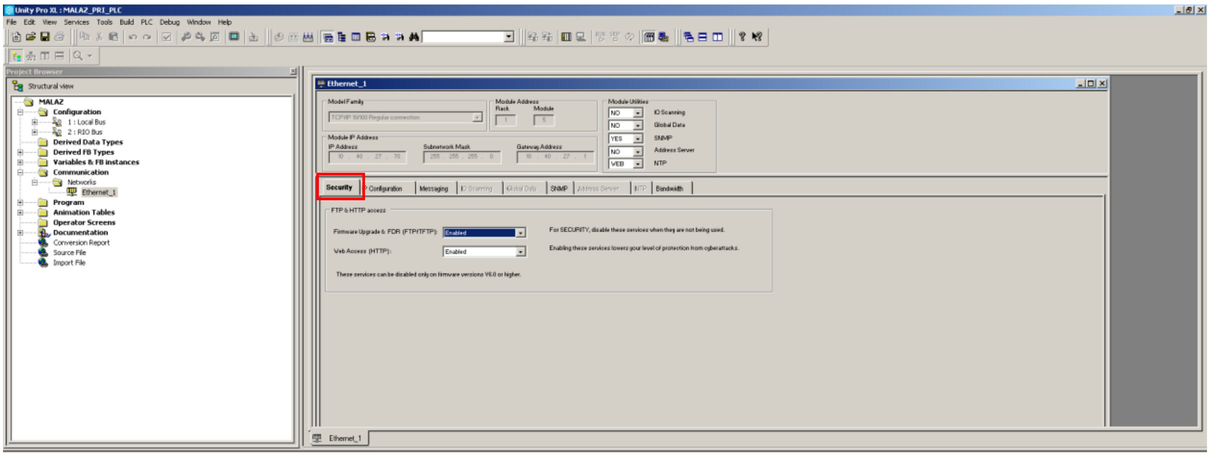
- Upgrade firmware
- Set password for security lock feature
- Disable HTTP/FTP ethernet services

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



Ethernet_1

Model Family: TCP/IP 10/100 Regular connection

Module Address: Rack 1, Module 5

Module IP Address: IP Address 10 . 40 . 27 . 70; Subnetwork Mask 255 . 255 . 255 . 0; Gateway Address 10 . 40 . 27 . 1

Module Utilities: NO IO Scanning; NO Global Data; YES SNMP; NO Address Server; WEB NTP

FTP & HTTP access

Firmware Upgrade & FDR (FTP/TFTP): Enabled

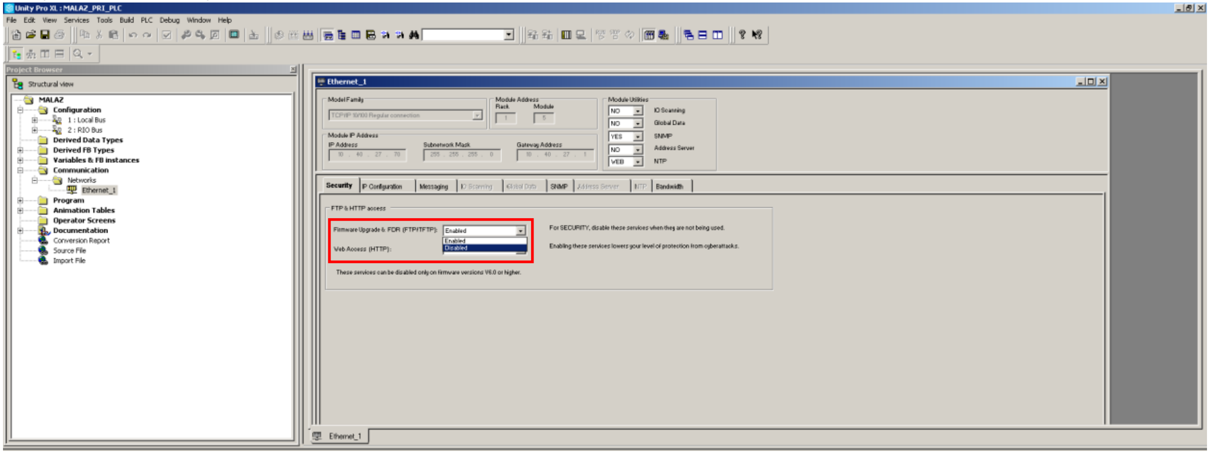
Web Access (HTTP): Enabled

For SECURITY, disable these services when they are not being used.

Enabling these services lowers your level of protection from cyberattacks.

These services can be disabled only on firmware versions V6.0 or higher.

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



Model Family: TCP/IP 10/100 Regular connection

Module Address: Rack 1, Module 5

Module IP Address: IP Address 10 . 40 . 27 . 70; Subnetwork Mask 255 . 255 . 255 . 0; Gateway Address 10 . 40 . 27 . 1

Module Utilities: NO IO Scanning; NO Global Data; YES SNMP; NO Address Server; WEB NTP

FTP & HTTP access

Firmware Upgrade & FDR (FTP/TFTP): Enabled (options: Enabled, Disabled)

Web Access (HTTP):

For SECURITY, disable these services when they are not being used.

Enabling these services lowers your level of protection from cyberattacks.

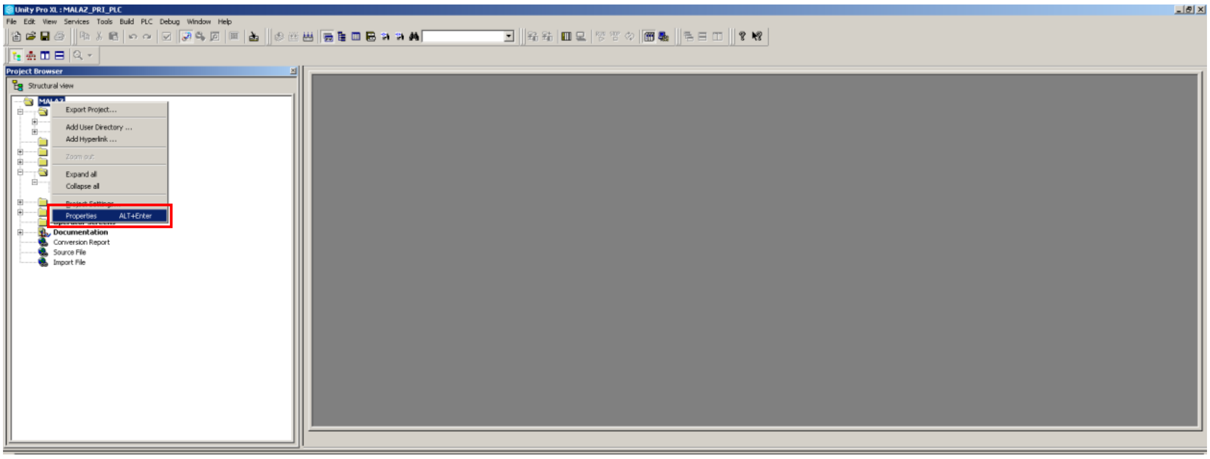
These services can be disabled only on firmware versions V6.0 or higher.

For IP Setting, see attachment Section 2.2 - Schneider M340_Modicon Setting the IP Address

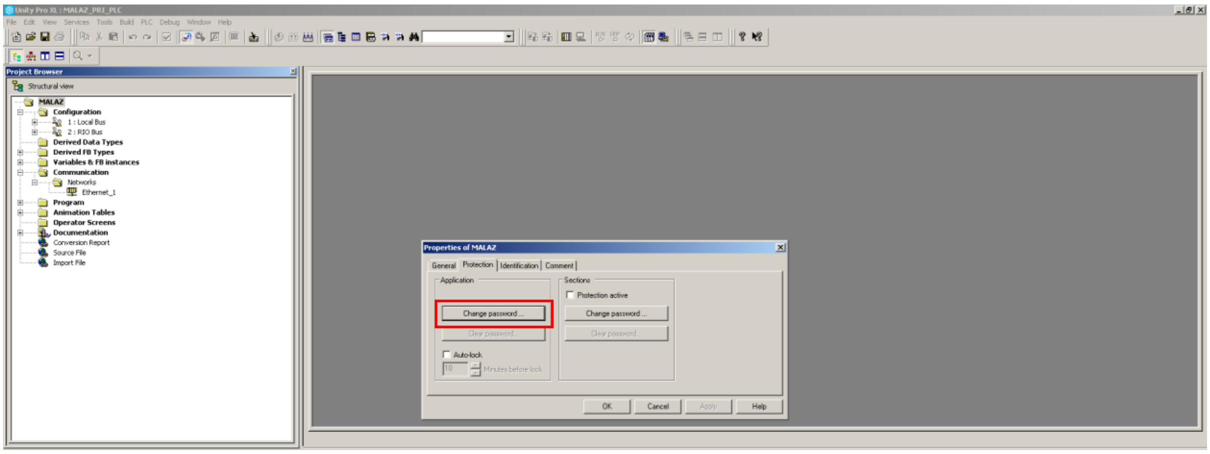
For firmware upgrade, see attachment Section 2.2 - Schneider M340_Firmware Upgrade Process

Following is the procedure of how to password protect the application:

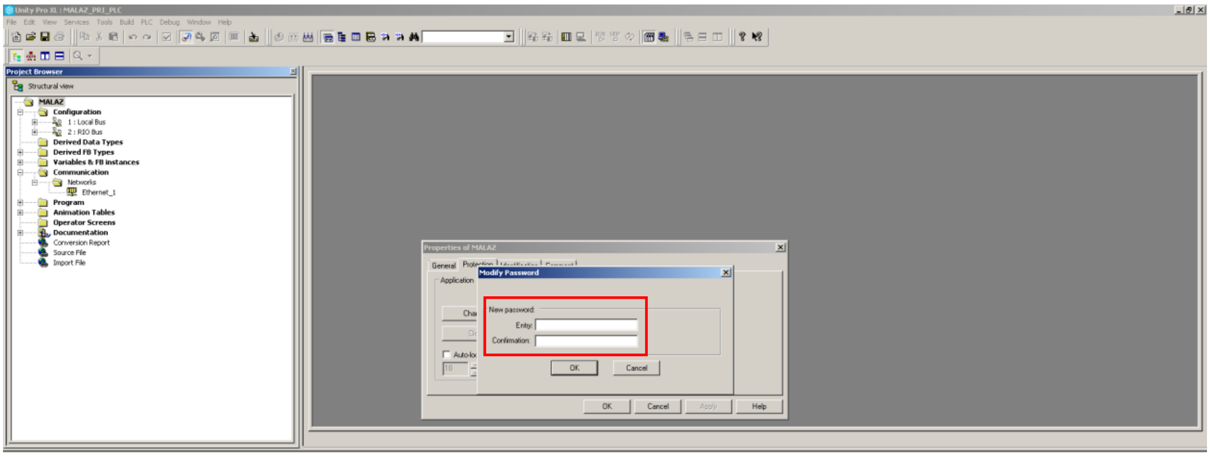
Step 1: Select the project and right click to select the properties



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



Step 3: Enter the new password and confirm it



For IP Setting, see attachment

For firmware upgrade, see attachment

2.3 SIEMENS S7-1200 HARDENING

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

For IP Setting, see attachment Section 2.3 - Siemens S7-1200_Setting the IP Address

For firmware upgrade, see attachment Section 2.3 - Siemens S7-1200_Firmware Upgrade Process

2.4 ROCKWELL MICRO-850 HARDENING

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

For IP Setting, see attachment Section 2.4 - Rockwell Micro-850_Setting the IP Address

For firmware upgrade, see attachment Section 2.4 - Rockwell Micro-850_Firmware Upgrade Process

2.5 SCHNEIDER TWIDO HARDENING

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

For IP Setting, see attachment Section 2.5 - Schneider Twido_Setting the IP Address

For firmware upgrade, see attachment Section 2.5 - Schneider Twido_Firmware Upgrade Process

2.6 ELPRO 245UE

- Upgrade the firmware
- Change default username/password
- Change the SSID/ESSID
- Use strong radio encryption method (like WPA2 AES)
- Disable Spanning Tree Protocol if no redundancy is used for communication
- Disable unused services

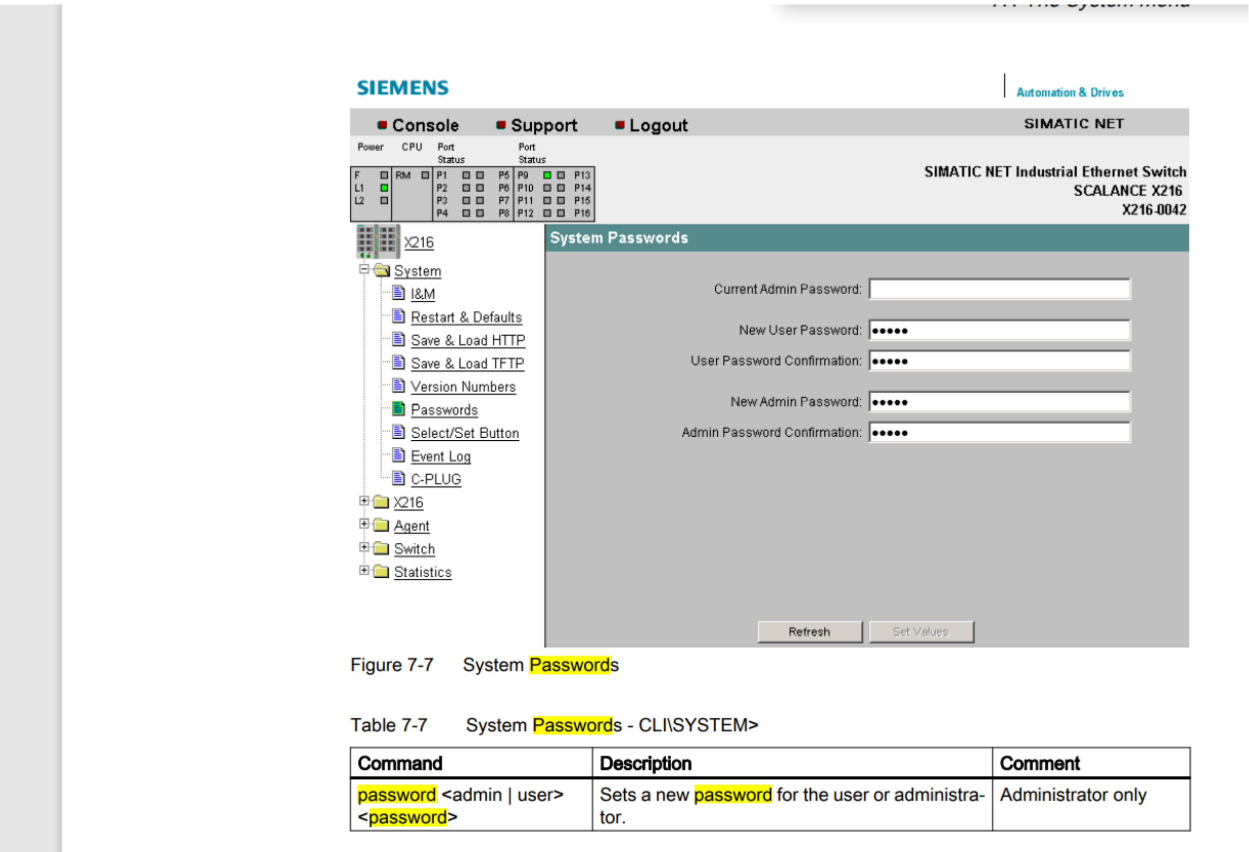
For IP Setting, see attachment Section 2.7 - 245UE-Manual-v2.24- IP Address - Page 82-85

For firmware upgrade, see attachment Section 2.7 - 245UE-Manual-v2.24 - Appendix A - Firmware Upgrade

2.7 SEIMENS_SCALANCE-X-204

- Default username and password should be changed

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



Current Admin Password:

New User Password: •••••

User Password Confirmation: •••••

New Admin Password: •••••

Admin Password Confirmation: •••••

Figure 7-7 System Passwords

Table 7-7 System Passwords - CLI\SYSTEM>

Command	Description	Comment
password <admin | user> <password>	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 disable only HTTPs/ssh/sftp should used
- Serial Access should be password Protected
- Should configure the Login Banner
- Firmware needs to be upgraded from vendor release

2.8 CONNEXIUMTCSESM, TCSESM-E MANAGED SWITCH

- Default username and password should be changed

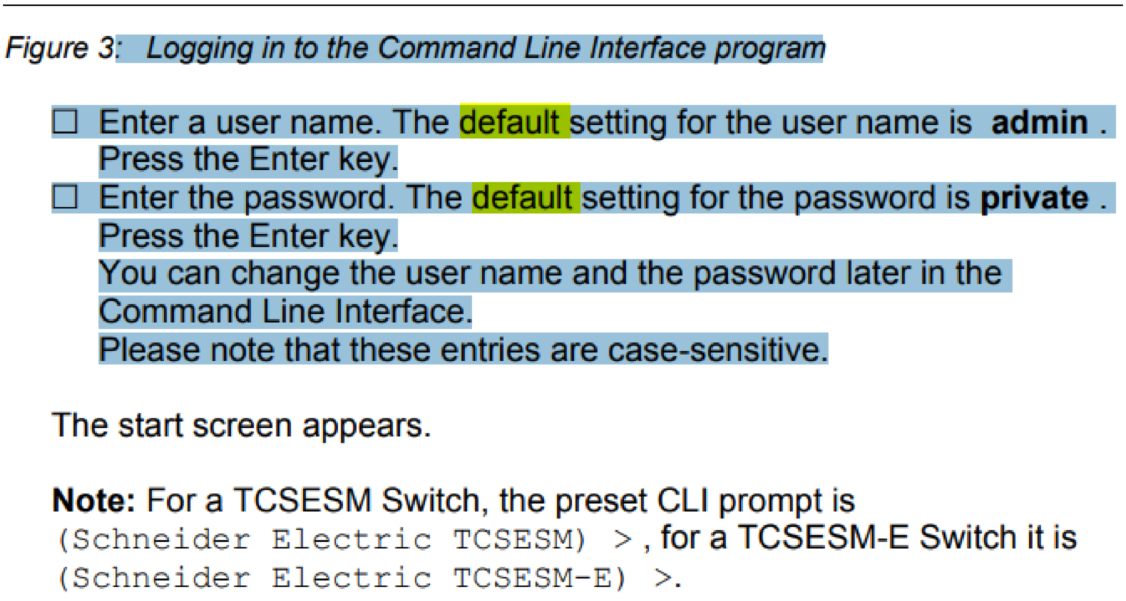


Figure 3: Logging in to the Command Line Interface program

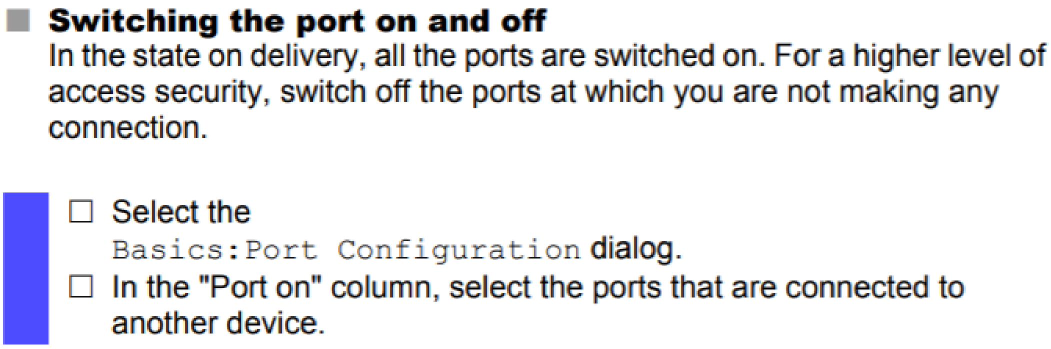
□ Enter a user name. The default setting for the user name is **admin** . Press the Enter key.

□ 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) >`.

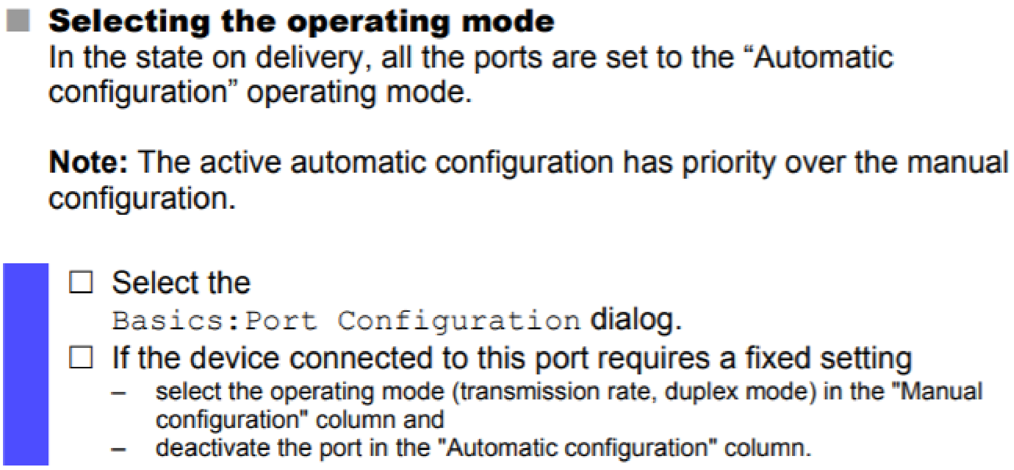
- Unused Port should be block for Managed switch



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.



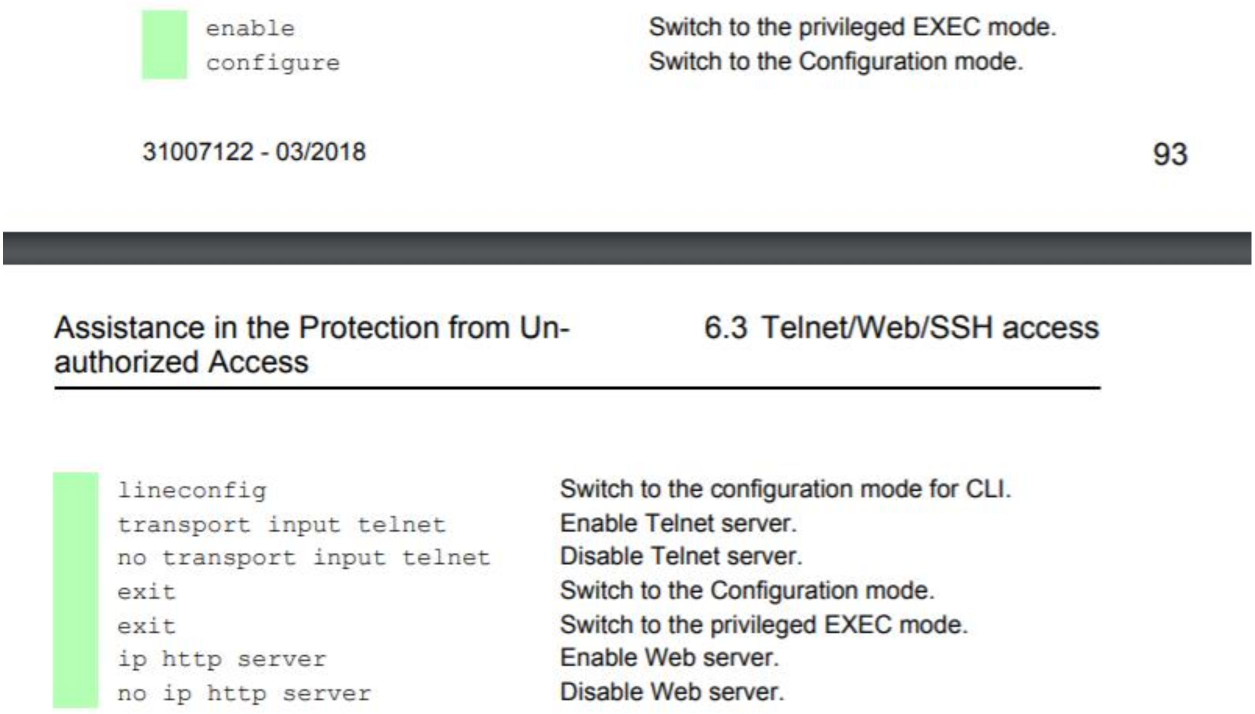
Selecting the operating mode
In the state on delivery, all the ports are set to the “Automatic configuration” operating mode.

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

31007122 - 03/2018

93

Assistance in the Protection from Unauthorized Access

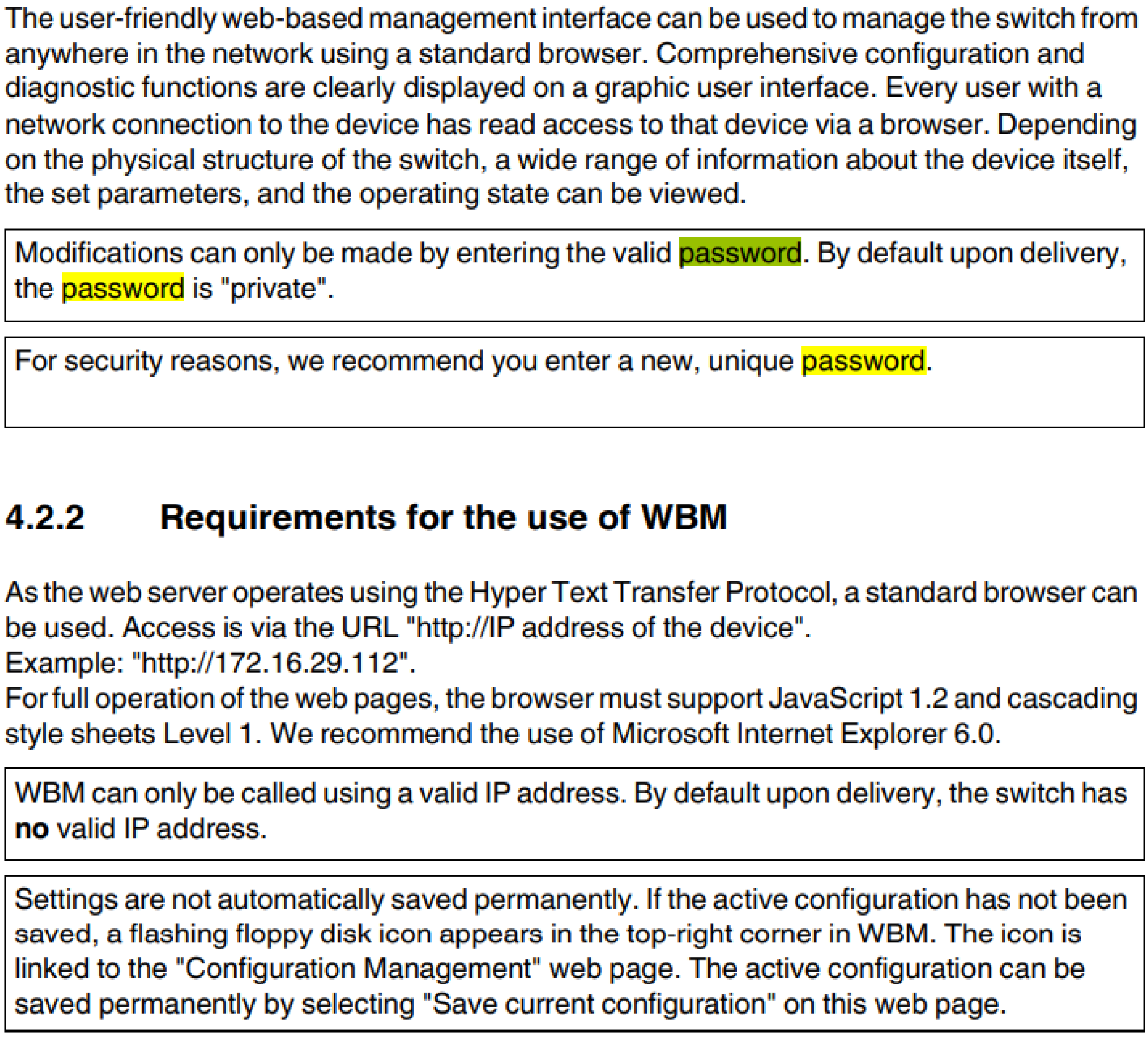
6.3 Telnet/Web/SSH access

`lineconfig`	Switch to the configuration mode for CLI.
`transport input telnet`	Enable Telnet server.
`no transport input telnet`	Disable Telnet server.
`exit`	Switch to the Configuration mode.
`exit`	Switch to the privileged EXEC mode.
`ip http server`	Enable Web server.
`no ip http server`	Disable Web server.

- Serial Access should be password Protected
- Should configure the Login Banner
- Firmware needs to be upgraded from vendor release

2.9 INDUSTRIAL ETHERNET SWITCH - FL SWITCH MCS 14TX/2FX - 2832713

- Default username and password should be changed



The user-friendly web-based management interface can be used to manage the switch from anywhere in the network using a standard browser. Comprehensive configuration and diagnostic functions are clearly displayed on a graphic user interface. Every user with a network connection to the device has read access to that device via a browser. Depending on the physical structure of the switch, a wide range of information about the device itself, the set parameters, and the operating state can be viewed.

Modifications can only be made by entering the valid password. By default upon delivery, the password is "private".

For security reasons, we recommend you enter a new, unique password.

4.2.2 Requirements for the use of WBM

As the web server operates using the Hyper Text Transfer Protocol, a standard browser can be used. Access is via the URL "http://IP address of the device".
Example: "http://172.16.29.112".
For full operation of the web pages, the browser must support JavaScript 1.2 and cascading style sheets Level 1. We recommend the use of Microsoft Internet Explorer 6.0.

WBM can only be called using a valid IP address. By default upon delivery, the switch has **no** valid IP address.

Settings are not automatically saved permanently. If the active configuration has not been saved, a flashing floppy disk icon appears in the top-right corner in WBM. The icon is linked to the "Configuration Management" web page. The active configuration can be saved permanently by selecting "Save current configuration" on this web page.

- Unused Port should be block for Managed switch
- IP http should be disable only HTTPs should
- Serial Access should be password Protected
- Should configure the Login Banner
- Firmware needs to be upgraded from vendor release
- Latest Firmware as per vendor 4.94

ACET SOLUTIONS

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 | www.acetsolutions.com