Advance Cybersecurity features

What’s new with Free Studio Plus 1.2 and bios 596.10 - 668.10

Federico Marcassa Sr Solution Architect Expert - Application Center

Cybersecurity settings of Free Advance

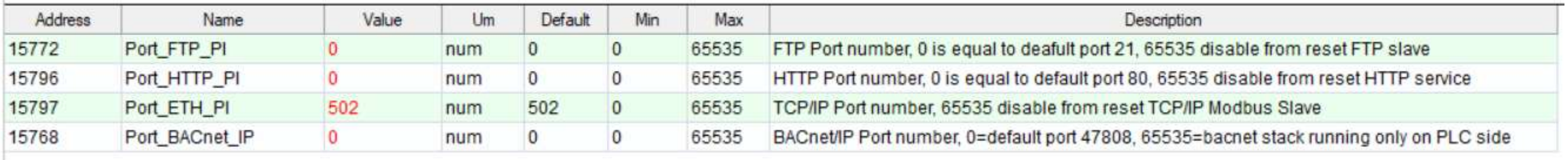
- HTTP is unsecure, but still enabled since a user authentication mechanism exists:
  - Being the factory credentials the same for all the PLC controllers, the user is forced to change the password at first access.
- The factory default configuration of the controller must be secure, following unsecure protocols are disabled by default:
  - Modbus TCP
  - BACnet IP
  - FTP
  - **These protocols are disabled regardless of the related bios settings until the user will change the factory web credential**

Cybersecurity settings of Advance

- Administrator password is internally crypted and stored in a safe area:
  - It is no longer need to save password into an EEprom location
  - It can be changed using:
    - the embedded website, automatic redirect to page evopsw.htm
    - First connection with Free Studio Plus 1.2
    - Modbus/CAN from local or remote HMI
- If the password is not modified at least one time:
  - **Modbus/TCP, FTP and BACnet IP are disabled regardless of the related bios settings**
  - Green and yellow led will blink once at the same time during the boot procedure

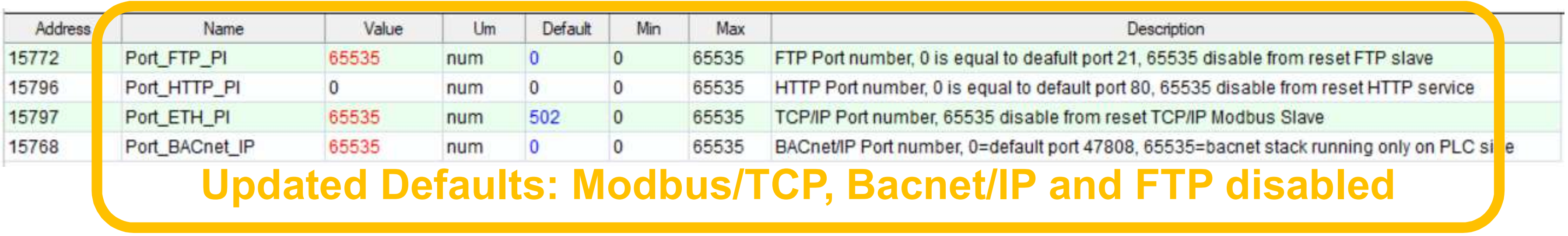
New factory settings of Advance

- Bios Parameters Default:
  - Target 596.9 668.9



Address	Name	Value	Um	Default	Min	Max	Description
15772	Port_FTP_PI	0	num	0	0	65535	FTP Port number, 0 is equal to deafult port 21, 65535 disable from reset FTP slave
15796	Port_HTTP_PI	0	num	0	0	65535	HTTP Port number, 0 is equal to default port 80, 65535 disable from reset HTTP service
15797	Port_ETH_PI	502	num	502	0	65535	TCP/IP Port number, 65535 disable from reset TCP/IP Modbus Slave
15768	Port_BACnet_IP	0	num	0	0	65535	BACnet/IP Port number, 0=default port 47808, 65535=bacnet stack running only on PLC side

  - Target 596.10 668.10



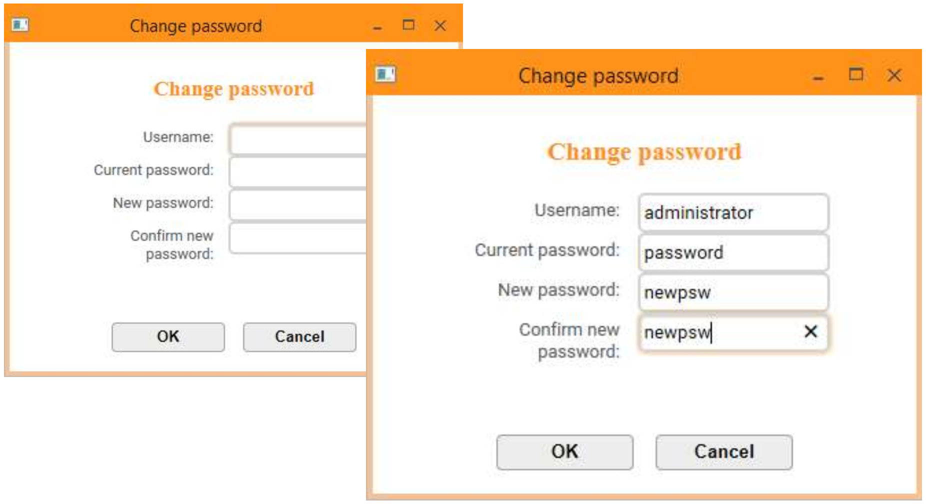
Address	Name	Value	Um	Default	Min	Max	Description
15772	Port_FTP_PI	65535	num	0	0	65535	FTP Port number, 0 is equal to deafult port 21, 65535 disable from reset FTP slave
15796	Port_HTTP_PI	0	num	0	0	65535	HTTP Port number, 0 is equal to default port 80, 65535 disable from reset HTTP service
15797	Port_ETH_PI	65535	num	502	0	65535	TCP/IP Port number, 65535 disable from reset TCP/IP Modbus Slave
15768	Port_BACnet_IP	65535	num	0	0	65535	BACnet/IP Port number, 0=default port 47808, 65535=bacnet stack running only on PLC side

Updated Defaults: Modbus/TCP, Bacnet/IP and FTP disabled

  - **These protocols are disabled regardless of the related bios settings until the user will change the factory web credential**

First connection via mini-USB or Modbus SL

- Free Studio Plus will ask you to change the PLC password:



Username: administrator

Current password: password

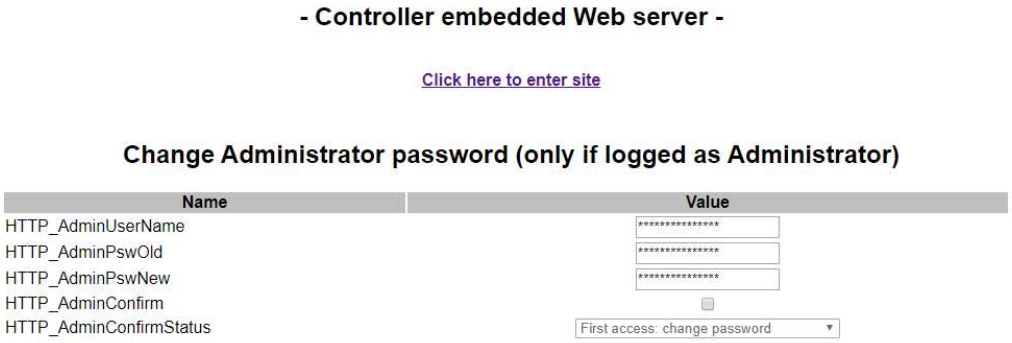
New password: newpsw

Confirm new password: newpsw

- FS+ Connection is allowed only after password has been changed
- Modbus SL protocol via RS485/mini-USB is always enabled for read/write registers

First connection via Ethernet

- Since Modbus/TCP is disabled, when you try to connect with FS+:
  - An error message will be shown and the default browser will be open trying to reach the PLC webserver
    - After entering the default credential: user: administrator, password:password
    - Change password
    - Enter again the new web credential



- Controller embedded Web server -

Click here to enter site

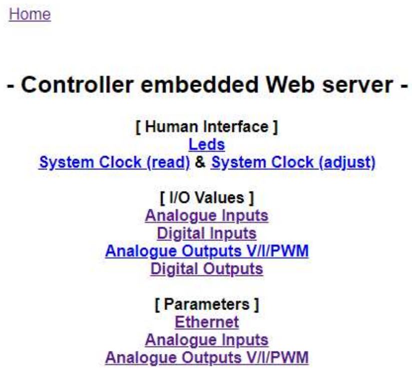
Change Administrator password (only if logged as Administrator)

Name	Value
HTTP_AdminUserName	***************
HTTP_AdminPswOld	***************
HTTP_AdminPswNew	***************
HTTP_AdminConfirm	□
HTTP_AdminConfirmStatus	First access: change password ▾

    - Open link ‘Click here to enter site’

First connection via Ethernet

- Open ‘Ethernet’ link:



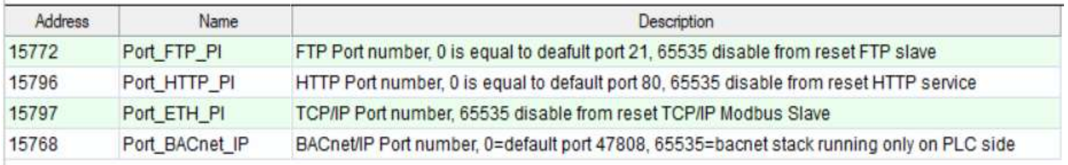
Home

- Controller embedded Web server -

[Human Interface]
Leds
System Clock (read) & System Clock (adjust)

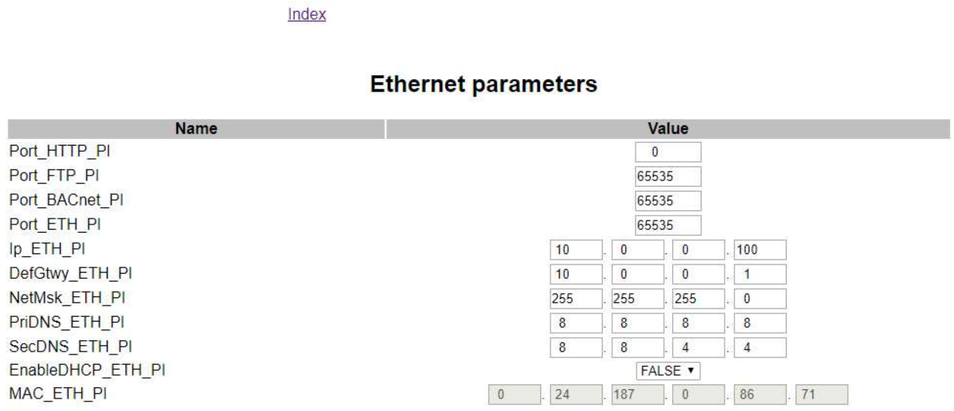
[I/O Values]
Analogue Inputs
Digital Inputs
Analogue Outputs V/I/PWM
Digital Outputs

[Parameters]
Ethernet
Analogue Inputs
Analogue Outputs V/I/PWM



Address	Name	Description
15772	Port_FTP_PI	FTP Port number, 0 is equal to deafult port 21, 65535 disable from reset FTP slave
15796	Port_HTTP_PI	HTTP Port number, 0 is equal to default port 80, 65535 disable from reset HTTP service
15797	Port_ETH_PI	TCP/IP Port number, 65535 disable from reset TCP/IP Modbus Slave
15768	Port_BACnet_IP	BACnet/IP Port number, 0=default port 47808, 65535=bacnet stack running only on PLC side

- Set protocol ports as desired:
  - 502 is the standard for Modbus/TCP
  - 21 for FTP, 47808 for Bacnet
- Go back to FS+ and connect



Index

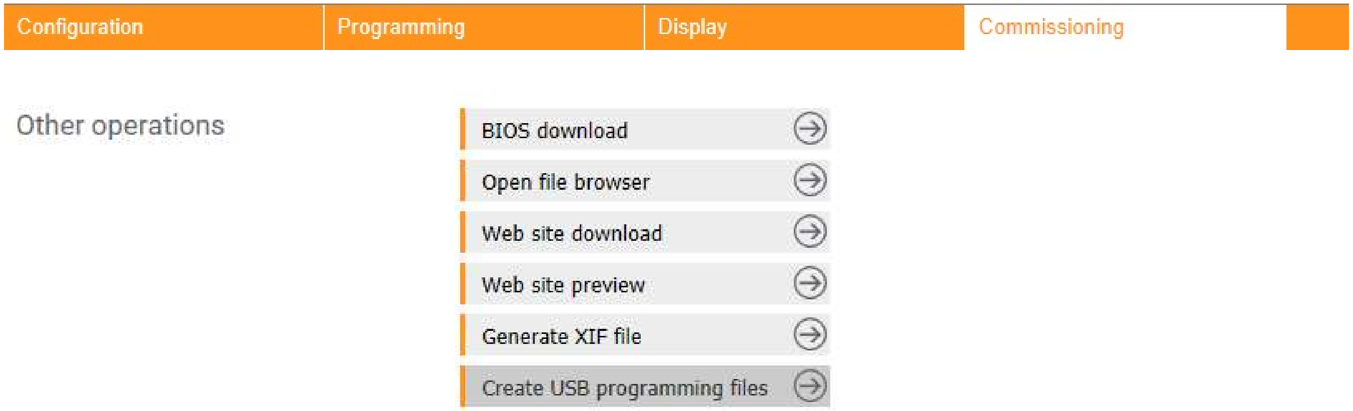
Ethernet parameters

Name	Value
Port_HTTP_PI	0
Port_FTP_PI	65535
Port_BACnet_PI	65535
Port_ETH_PI	65535
Ip_ETH_PI	10 . 0 . 0 . 100
DefGtwy_ETH_PI	10 . 0 . 0 . 1
NetMsk_ETH_PI	255 . 255 . 255 . 0
PriDNS_ETH_PI	8 . 8 . 8 . 8
SecDNS_ETH_PI	8 . 8 . 4 . 4
EnableDHCP_ETH_PI	FALSE ▾
MAC_ETH_PI	0 . 24 . 187 . 0 . 86 . 71

Life Is On | eliwell by Schneider Electric

Programming with USB memory key

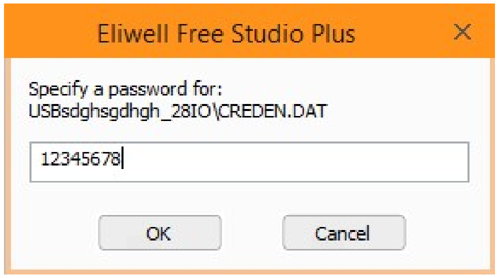
- The USB programming files are created by the usual command in Commissioning:



Other operations

- BIOS download
- Open file browser
- Web site download
- Web site preview
- Generate XIF file
- Create USB programming files

- FS+ will ask the developer to define the web password:



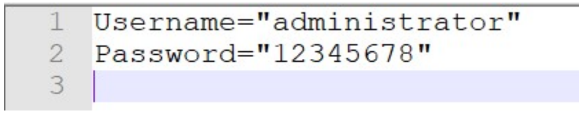
Eliwell Free Studio Plus

Specify a password for:
USBsdghsgdhgh_28IO\CREDEN.DAT

12345678

Programming with USB memory key

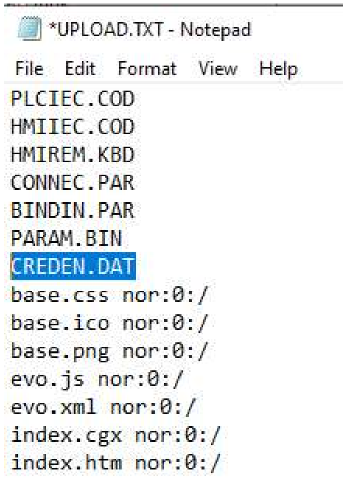
- Web password will be stored in a new programming file named CREDEN.DAT
- It must be called by UPLOAD.TXT as last system file (before the web and extra files as in the example):
- Content of CREDEN.DAT:



```
Username="administrator"
Password="12345678"

```

  - Max length is 15 chars
  - File must end with a CR+LF



```
PLCIEC.COD
HMIIEC.COD
HMIREM.KBD
CONNEC.PAR
BINDIN.PAR
PARAM.BIN
CREDEN.DAT
base.css nor:0:/
base.ico nor:0:/
base.png nor:0:/
evo.js nor:0:/
evo.xml nor:0:/
index.cgx nor:0:/
index.htm nor:0:/
```

Programming with USB memory key

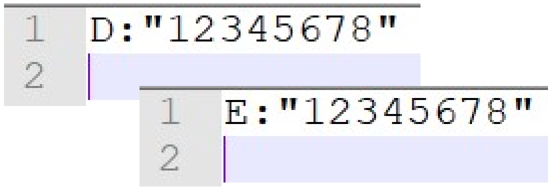
- Result of a USB memory key upload:

	Bios 596.10 668.10 or newer		Previous Bios Version
	Web password not changed yet	Web password already changed	
CREDEN.DAT present and called by UPLOAD.TXT	Password is changed first, then USB content is uploaded	USB content is uploaded **Password file is downloaded but does not trigger any action**	Upload fails
CREDEN.DAT not present or not called by UPLOAD.TXT	USB content is not uploaded Red led will blink 3 times	USB content is uploaded	USB content is uploaded

- **USB programming files generated by FS+ 1.1 or FS 3.x must be updated adding CREDEN.DAT when used with bios 596.10 668.10 or newer**

How to manage manufacturing process or connect with FS+ 1.1

- Developers can create a file named: OEMFILE.TXT
  - File content must be:
    - D="<newpassword>" or E="<newpassword>“ + <CR LF>
    - **D** means web password is changed and after PLC reboot unsecure protocol status will depend on bios/target block settings
    - **E** means do not change web password (unsecure protocol disabled after reboot)
  - This file works only on brand new plc with web password not changed yet
  - Plugging a USB stick at PLC boot with web password not yet changed will temporarily enable all unsecure protocols



```
D:"12345678"

```

```
E:"12345678"

```

How to restore cybersecurity factory settings

- Call *sysHTTP_Authentication()* with the following input:
  - MACaddress as string *‘00:18:BB:XX:XX:XX’*
  - ‘administrator’
  - ‘password’
- Reboot the PLC

Code example:

```
IF xReset THEN
// restore Cybersecurity factory settings
        sMacString := ‘’;
        FOR i:=0 TO 5 DO
                // With FS+ 1.1 sysMacAddress[i] must be first converted
                into a INT var and then used as input of TO_STRINGFORMAT()
                sByte := TO_STRINGFORMAT(sysMacAddress[i],'%02X');
                sMacString := CONCAT(sMacString,sByte);
                IF i<5 THEN
                        sMacString := CONCAT(sMacString,':');
                END_IF;
        END_FOR;
        // MacAddress format: "00:18:BB:XX:XX:XX"
        usiRet := sysHTTP_Authentication(sMacString,'administrator','password');
        xReset := FALSE;
END_IF;
```

- Bios default related to Modbus/TCP, FTP and BACnet IP are not modified

Life Is On

Schneider Electric