

# Initial Setup and Reset of CyberSecurity for LMD Ethernet Devices

Schneider Electric Motion Applications Note  
SEM-AN-2001:A 06/20

## Summary

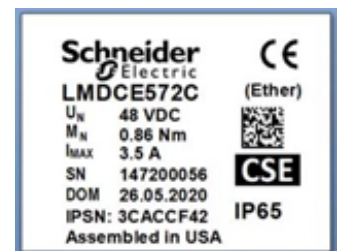
This document provides information for the initial setup and reset of the CyberSecurity feature for the Lexium MDrive (LMD) regular and high-torque ethernet devices with CyberSecurity protection enabled.

## Introduction

LMD ethernet devices with a “CSE” marking on the product label of the motor indicates that CyberSecurity has been enabled on the device. Additional setup will be required before the motor can be used.

Once power is applied to the unit, notice that the module status (MS) and network status (NS) LED's produce a flashing red behavior confirming that CyberSecurity is enabled and a password needs to be configured.

**NOTE:** When CyberSecurity is enabled, it is not possible to change the devices IP address or application protocol via third party controller/software.

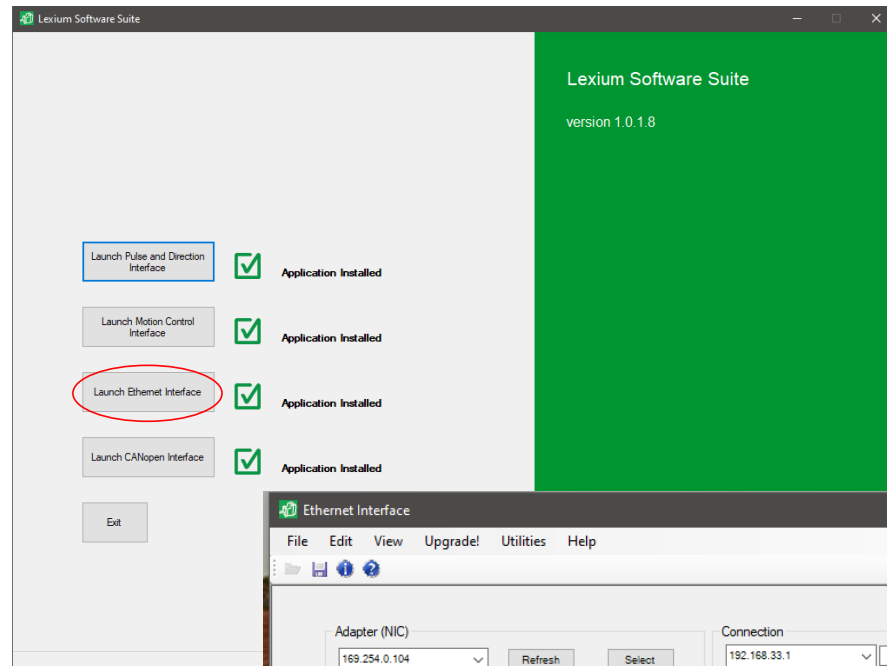


## Initial Configuration Process

For LMD ethernet devices with CyberSecurity enabled, perform the following steps for first time use.

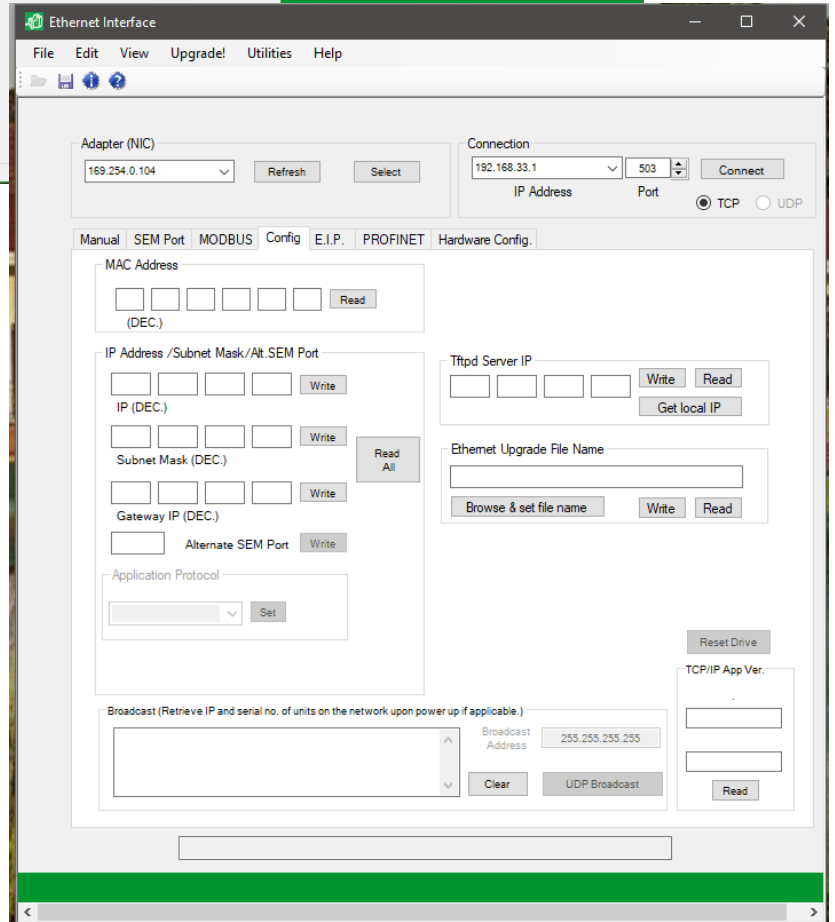
### Step 1

Use the Lexium Software Suite desktop icon to launch version 1.0.1.8 of the Lexium Software Suite. The Lexium Software Suite launch screen will be displayed.



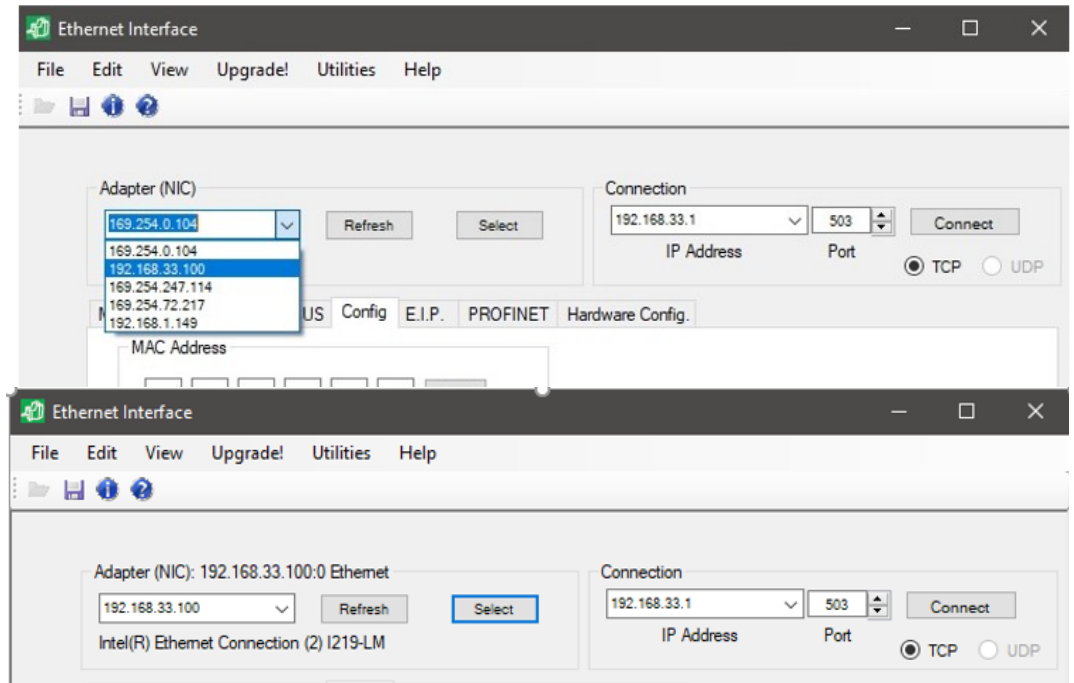
### Step 2

On the launch screen, click the "Launch Ethernet Interface" button. The "Ethernet Interface" will be displayed.



### Step 3

Select the Adapter (NIC) from the dropdown menu to which the Lexium MDrive Ethernet device is interfaced with and click “Select”. For this example, 192.168.33.100 was used for the Adapter (NIC).

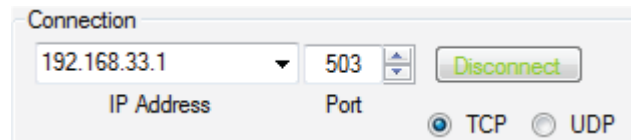


**NOTE:** The refresh button may be used if the associated NIC IP is not shown on the dropdown. Once selected, the NIC information will display above and below the selector as shown above.

### Step 4

In the section labeled “Connection”, ensure that the default IP Address, 192.168.33.1 is visible in the dropdown box and 503 in the port field.

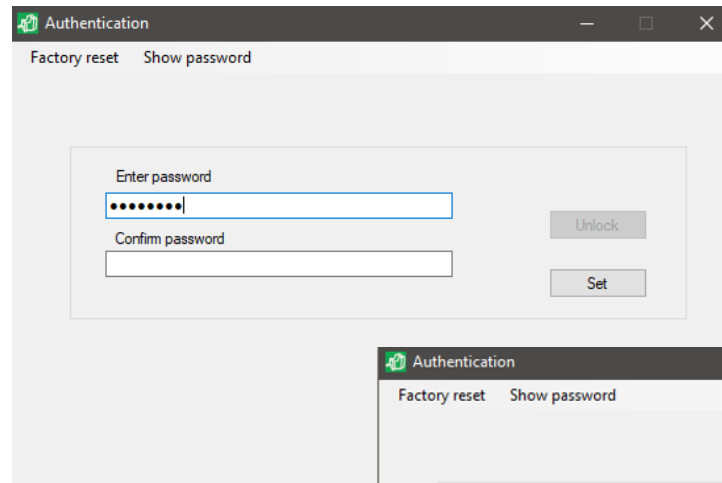
Click the “Connect” button. Connection active status will be indicated by the button text turning green showing “Disconnect”, and the status bar showing a connected status.



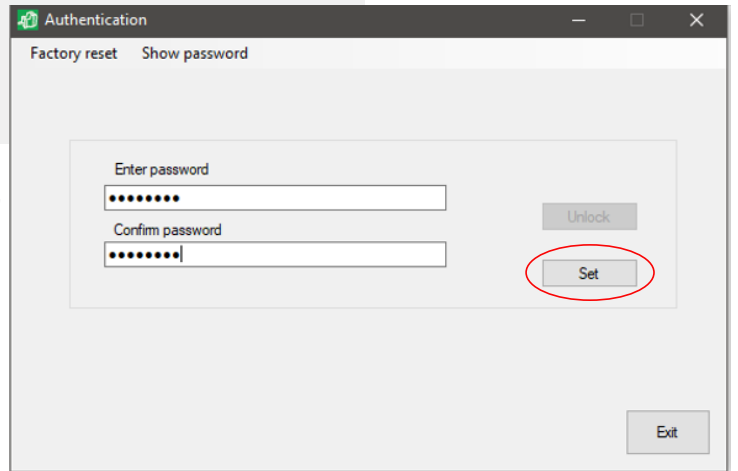
192.168.33.100:49836 is connected to: 192.168.33.1:503

**Step 5**

After clicking “Connect”, an Authentication screen will be displayed, allowing for a password to be setup. Enter a password in the first field of the Authentication dialog box.

**Step 6**

Enter the same password in the second field of the Authentication dialog box.

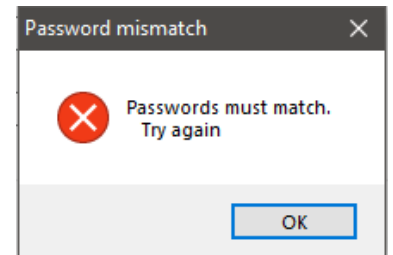


**NOTE:** The “Show password” option can be clicked to show the password as it is typed.

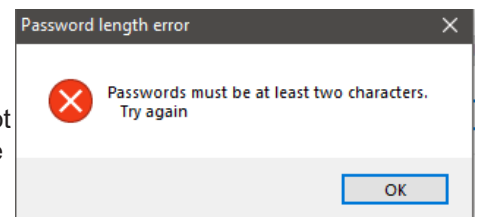
**Step 7**

Click “Set”.

**NOTE:** If the passwords do not match, a message will be displayed indicating that the passwords do not match, and the passwords will have to be entered again.



**NOTE:** If the password does not meet the minimum two-character requirement, a message will be displayed indicating that the password is not a sufficient length. A new password will need to be entered to meet this requirement.

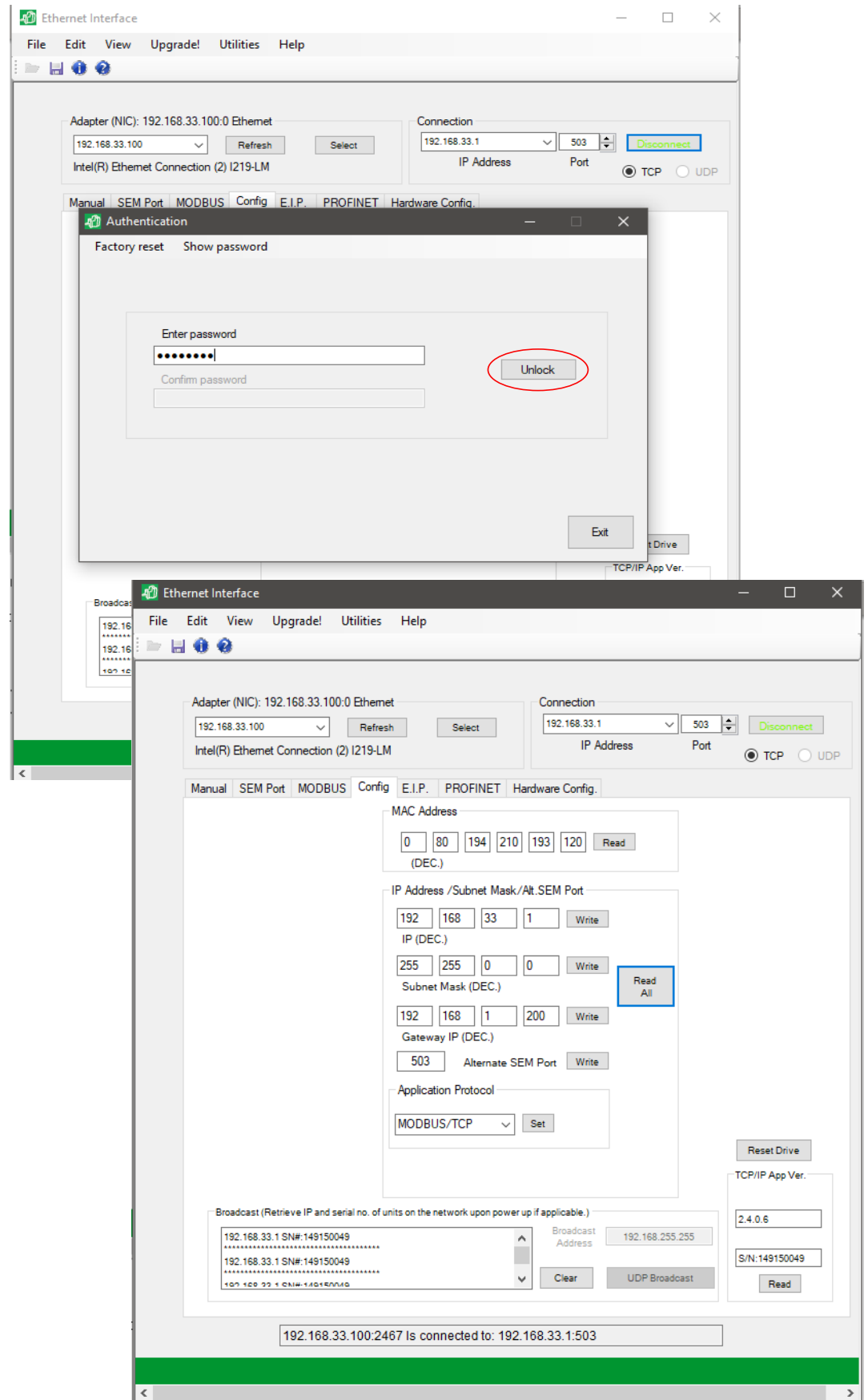


**Step 8**

After pressing the “Set” button, a connection to the device must be made. Press the “Connect” button. You will be prompted to enter the newly created password.

**Step 9**

Enter the correct password and click the “Unlock” button. The interface will connect with the device and the Config. tab will be displayed.



## Resetting the CyberSecurity Password

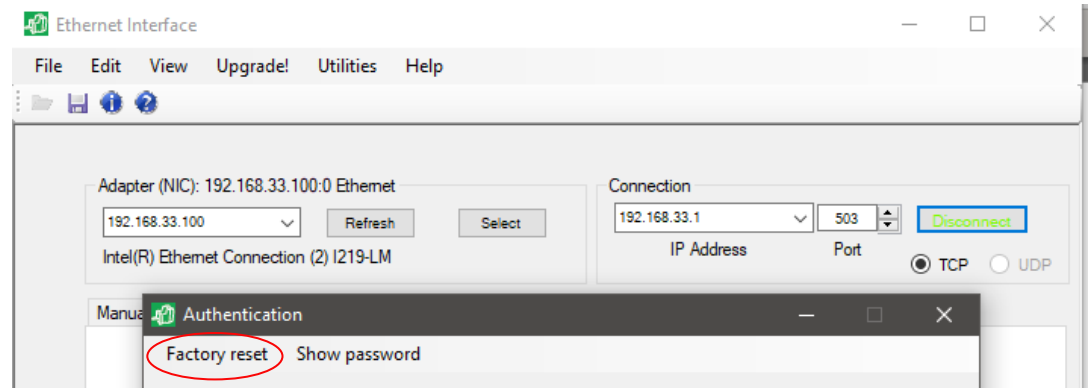
Perform the following steps to reset the CyberSecurity password and return the device to factory default.

### Step 1

Click the “Connect” button in the Connection section of the ethernet application.

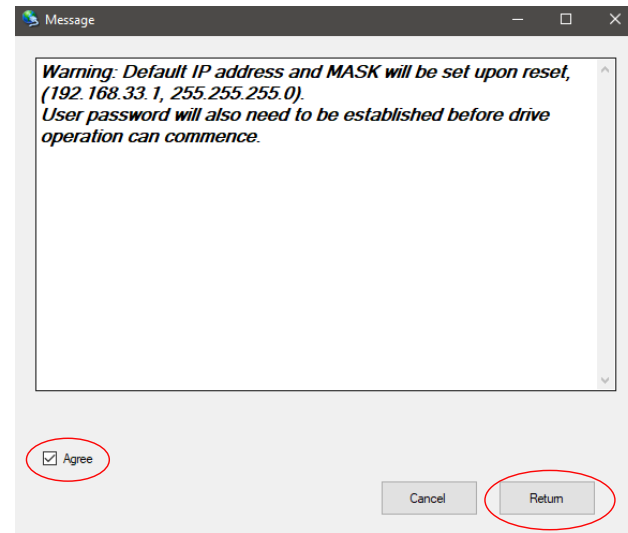
### Step 2

When the Authentication screen is displayed, select “Factory reset”.



### Step 3

A message will be displayed providing information about the reset process. Click the “Agree” check box and click “Return”. The Factory password, and IP Configuration reset dialog box will be displayed.



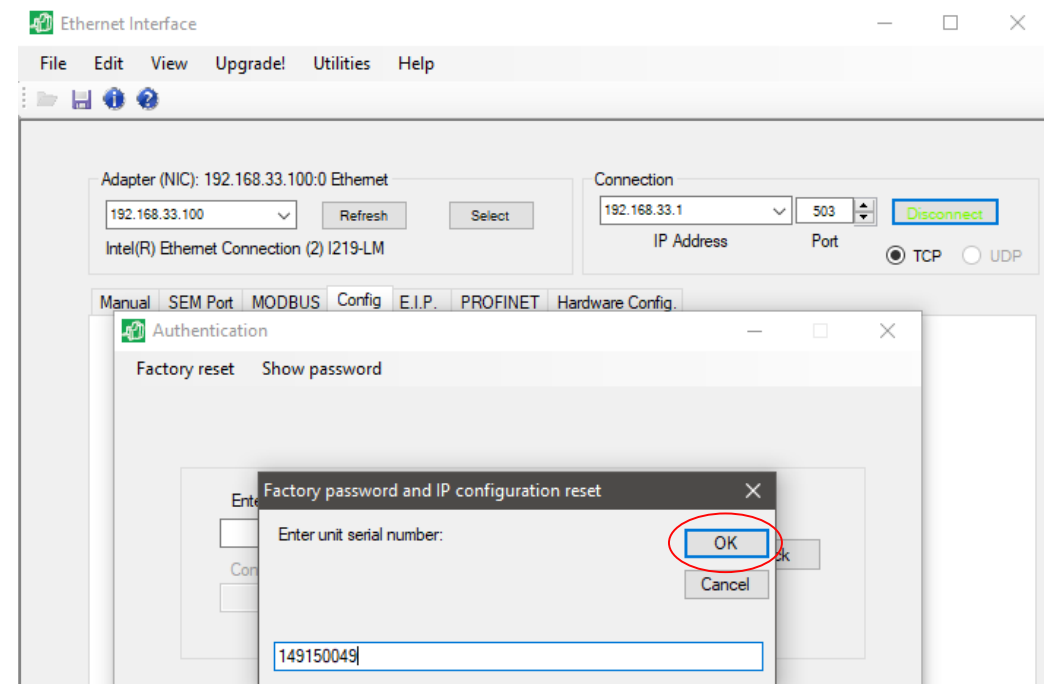
### NOTE:

The “Return” button will not be available until the “Agree” check box has been clicked.

### Step 4

On the Factory password and IP Configuration reset dialog box, enter the serial number of the device being reset. Click “OK”.

An attempt to reconnect the device will result in an initial password setup as indicated in “Initial Configuration Process” on page 2.



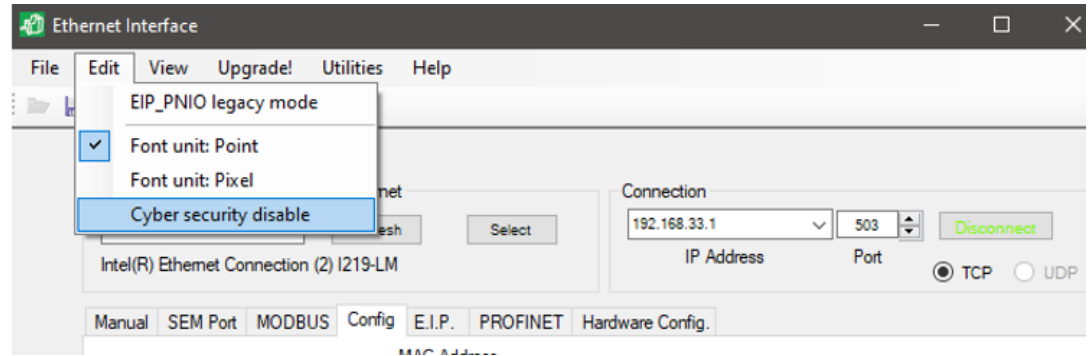
## Disabling the CyberSecurity Password

If the user chooses to disable the CyberSecurity feature, it can be disabled via the Edit menu.

Perform the following steps to disable the CyberSecurity Password.

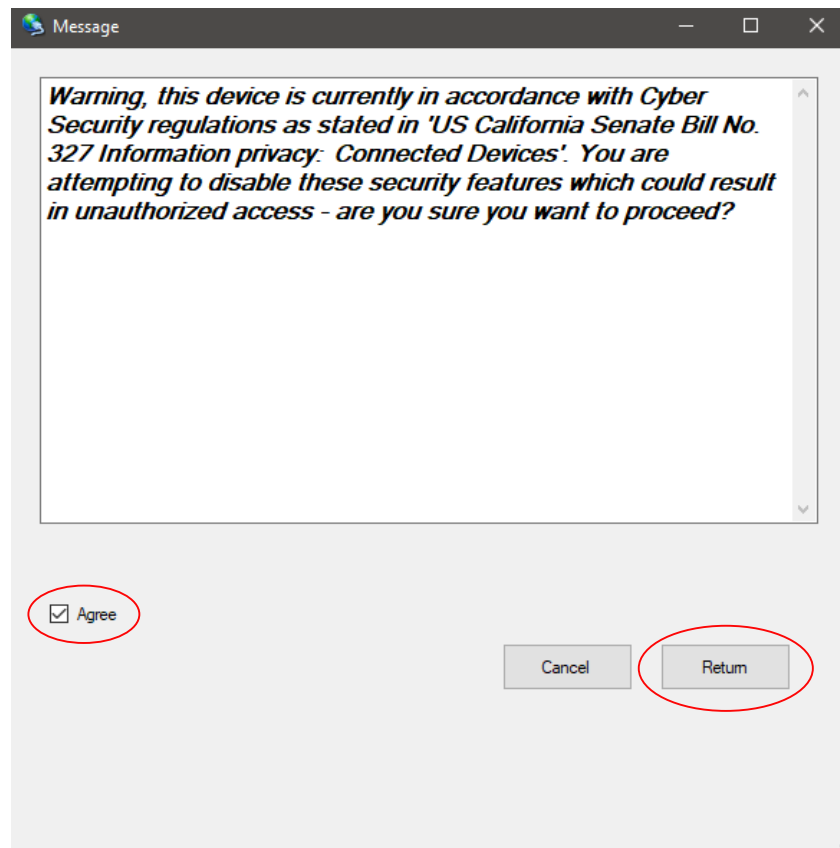
### Step 1

In the Edit menu, click “Cyber security disable”. A check mark will appear next to the menu option and a message screen will display a CyberSecurity compliance warning.



### Step 2

To proceed with the disable of the CyberSecurity option, click the “Agree” check box and the “Return” button.



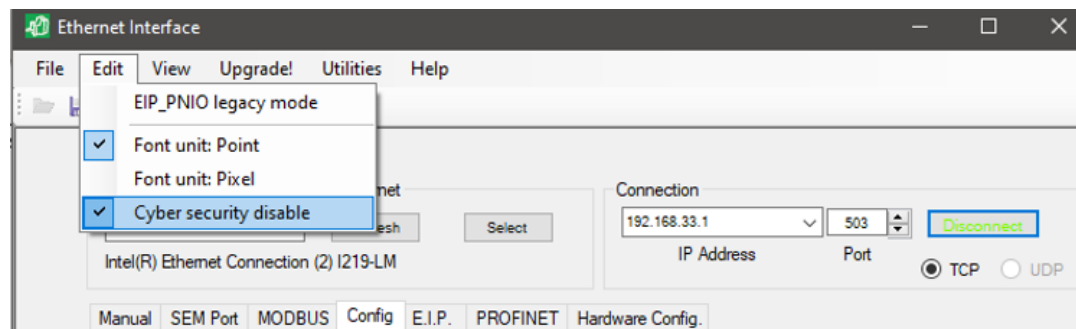
**NOTE:** The “Return” button will not be available until the “Agree” check box has been clicked.

## Re-Enabling the CyberSecurity Password

Perform the following steps to re-enable the CyberSecurity password.

### Step 1

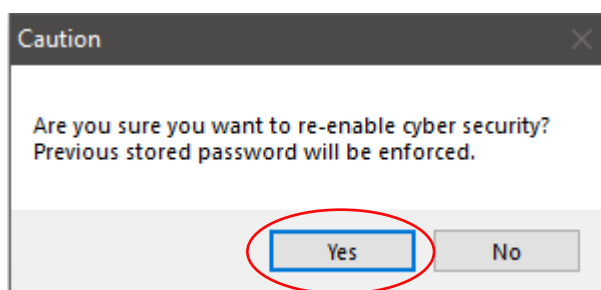
In the Edit Menu, deselect "Cyber Security disable". The check mark will be removed from the menu option and a Caution screen will be displayed confirming the re-enable of CyberSecurity.



### Step 2

Click "Yes" to proceed with the re-enable of the CyberSecurity feature.

The feature will be re-enabled and set to the previously established password used prior to the disable.



#### Schneider Electric Motion - Applications Group

370 N. Main Street, Marlborough, CT 06447

Telephone: +1 (860) 365-3907

[etech@imshome.com](mailto:etech@imshome.com)

© 2020 Schneider Electric Software, LLC. All rights reserved.

PN SEM-AN-2001:A Rel. 06/20