

Advanced Cyber Security

Introduction

The first chapter explained the very important Cyber Security feature of the M580; the activation/deactivation of its services.

In this topic we will discover more Cyber Security features such as:

- Password management
- Integrity Checks
- Memory and Run/Stop Protect
- IP address restrictions

Chapter Objectives

By the end of this chapter the student will be able to:

- Deploy advanced Cyber Security measures in M580 architecture.

Application Security

Password Management

Password management is one of the fundamental tools of device hardening, which is the process of configuring a device against communication-based threats. Schneider Electric recommends the following password management guidelines:

Enable password authentication on all email and Web servers, CPUs, and Ethernet interface modules.

Change all default passwords immediately after installation, including those for:

- user and application accounts on Windows, SCADA, HMI, and other systems
- scripts and source code
- network control equipment
- devices with user accounts
- FTP servers

Passwords in Unity Pro

When creating an application in Unity Pro, Schneider Electric recommends creating an application password.

Guidelines for creating a strong password are to choose a password that contains alphanumeric characters, and is case-sensitive. Unity Pro encrypts the password, and stores it in the application:

- Choose a password that contains a minimum of 8 characters.
- Choose a password that is difficult to guess.
- The password should combine upper and lower case letters, digits, and special characters.

When you open an existing application, the **Application Password** dialog box opens. Type the password, and click OK.

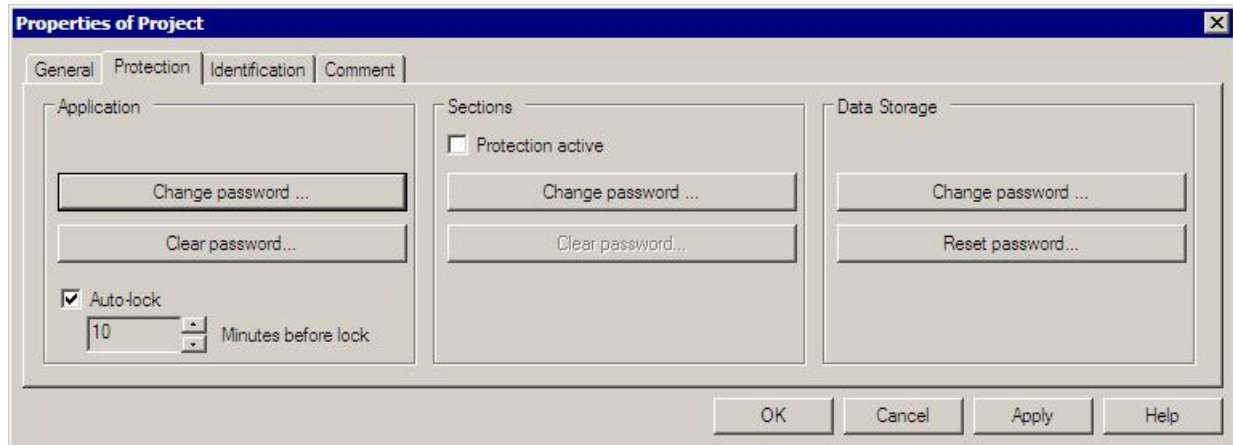


Application Security (cont.)

Auto-Lock

Within Unity Pro it is possible to **Auto-Lock** the application based upon a time period.

This means that after the allocated Auto-Lock timeout is exceeded the application will time out and prompts the user to login again.



Exercise - Password Management

Learning Outcomes

By the completion of this exercise you will:

- implement an application password within Unity Pro.
- prove the application password feature.
- implement the Auto-Lock functionality.



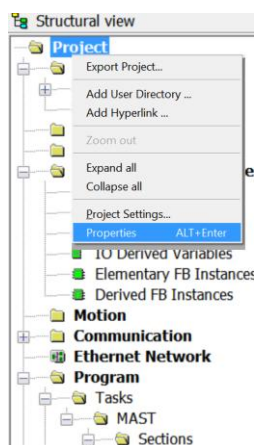
Note:

For this exercise the **Simulator Mode within Unity Pro** will be used. Please disconnect from and turn off the physical simulator / PAC now.

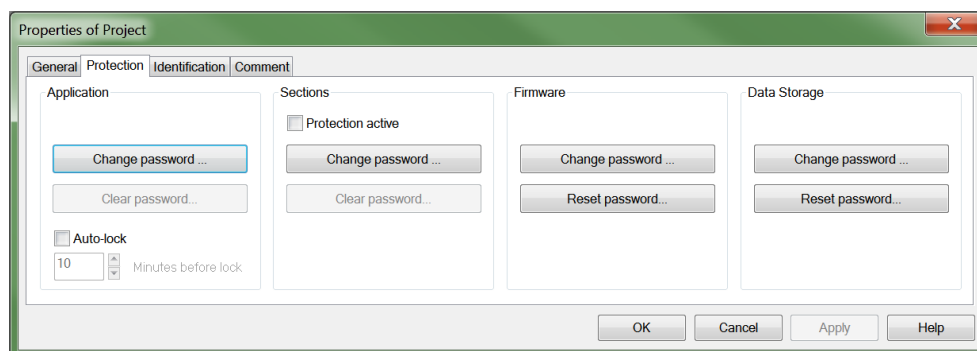
If you are unsure how to achieve this please ask the instructor.

Open the Project Properties and create an Application Password.

- Open the **Project Properties** by right clicking on the **Root** of the **Application** in the **Project Browser**. Select **Properties** from the popup menu:

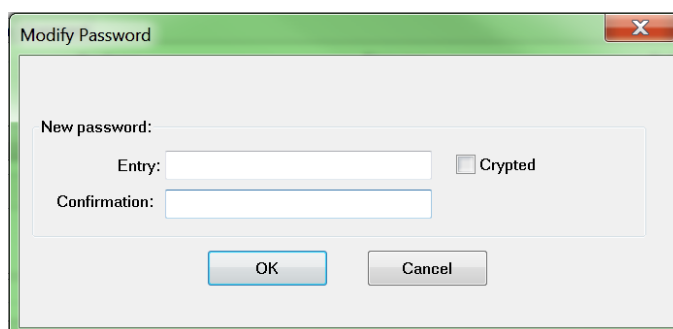


- Select the **Protection** tab:

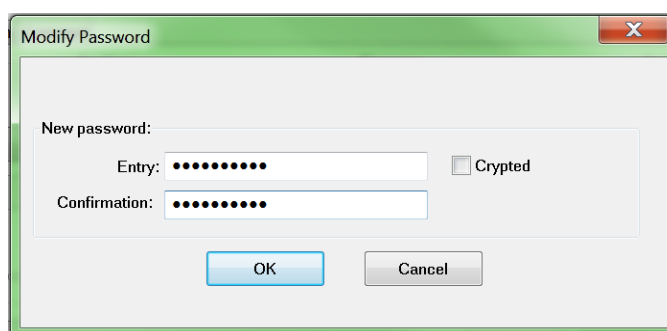


Exercise - Password Management (cont.)

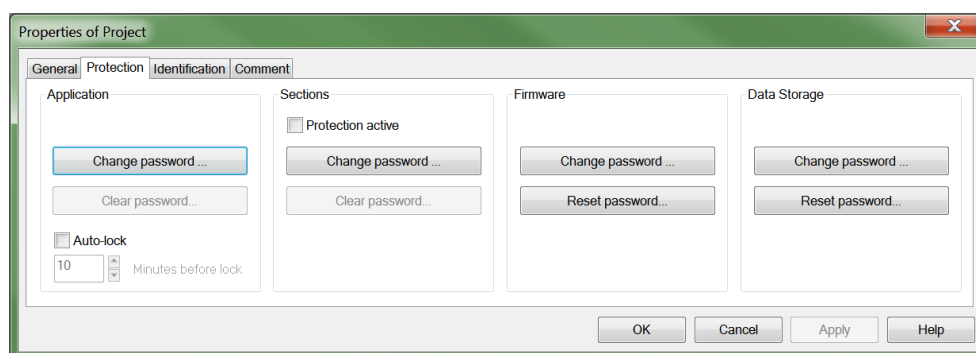
- iii. From the **Application** section. Click the **Change Password...** button. The **Modify Password** dialog appears.



- iv. Enter the password automation into both fields. Click **OK**:

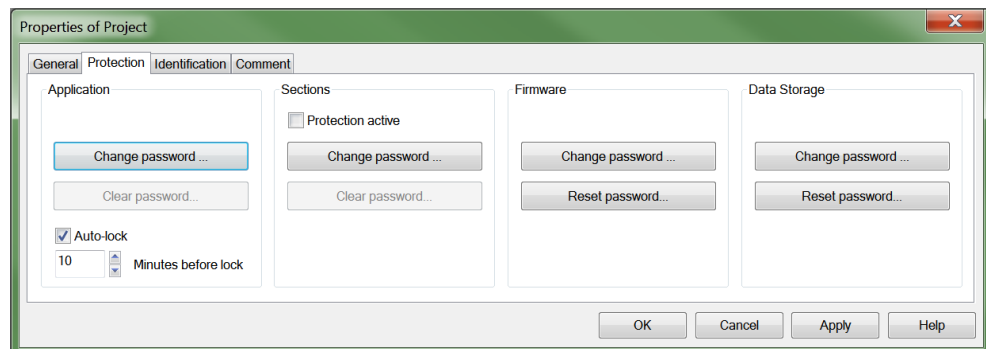


- v. The user is returned to the **Protection** tab:



Exercise - Password Management (cont.)

- vi. Enable the **Auto-lock** function, by selecting the tick box, leave the default of 10 minutes. Click **Apply**:



- vii. **Build, Connect & Transfer** the application to the Simulator.
viii. **Save** and **Close** the application.



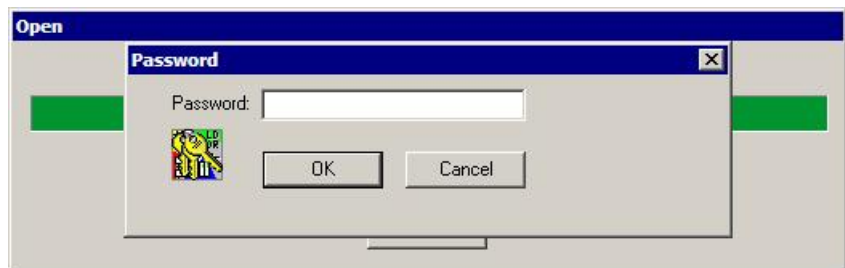
Note:

In a real project, make sure you do not forget the password!

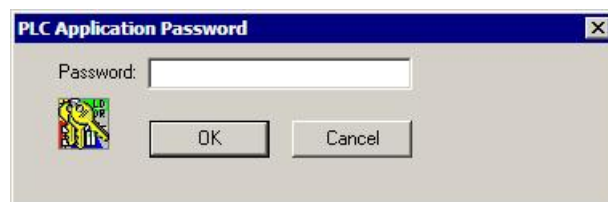
Exercise - Password Management (cont.)

Test the Password Management settings:

- i. Re-open the previous application within Unity Pro. This time the user will be prompted to enter the application password created in step (iv) of the previous exercise:



- ii. Unity Pro will open the application if the correct password is entered. **Close** the application again.
- iii. **Connect** directly to the PLC without opening the application. This time the user will be prompted for the **PLC Application Password**. Enter the correct password. Click **OK**:



- iv. Without the password the user is unable to connect to the PLC.
- v. **Transfer** the application from the **PLC** to the **PC**.
- vi. **Save** the application.

