

Unity Loader V14.0 Readme

Table of Contents

1	MAIN FEATURES.....	2
2	SYSTEM REQUIREMENTS	2
3	SETUP PROCEDURE	3
3.1	Recommendations before installation	3
3.2	Unity Loader Setup procedure	3
3.3	Communication Drivers installation	3
3.4	Recommendations to increase Security	4
4	REGISTRATION	4
5	UNINSTALL.....	4
6	NEW FEATURES	5
7	CYBER SECURITY FEATURES.....	7
7.1	Managing the Application Password in Control Expert	7
7.1.1	Creating / Changing the Application Password in Control Expert.....	7
7.1.2	Removing the Application Password in Control Expert.....	7
7.1.3	Resetting a Forgotten Application Password in Control Expert	8
7.2	Managing the Data Storage Password in Control Expert.....	8
7.2.1	How to Change the Data Storage Password in Control Expert	8
7.2.2	How to Reset the Data Storage Password in Control Expert.....	8
7.3	Managing the Firmware Protection Password in Control Expert	9
7.3.1	How to Change the Firmware Protection Password in Control Expert	9
7.3.2	How to Reset the Firmware Protection Password in Control Expert	9
8	README LAST MINUTE INFORMATION.....	11

1 MAIN FEATURES

Unity Loader is a utility to exchange data with the Modicon M340, Modicon M580, Modicon Momentum, Premium TSX PLC and Quantum TSX PLC platforms:

- Firmware download in Modicon M340, Modicon M580 and Modicon Momentum PLCs.
- Firmware download in Modicon X80 and eX80 modules that embed a firmware.
- Download / upload of project information:
 - Program
 - Variables
 - User files on the memory cartridge
- USB, UNITELWAY and MODBUS driver to communicate between the PC and the PLC.
- The documentation is provided as online help inside the software and installed as PDF on the PC.

2 SYSTEM REQUIREMENTS

The Unity Loader software requires one of the following operating systems:

- Microsoft Windows 7 Professional 32-bit / 64-bit
- Microsoft Windows 10 Pro 32-bit / 64-bit
- Microsoft Windows Server 2016 Standard 64-bit

System with Microsoft Windows 7 Professional 32-bit / 64-bit

System: Minimum Pentium Processor 2.4 GHz, recommended 3.0 GHz or higher.
RAM memory: Minimum 4 GB, recommended 8 GB or more.
Hard disk: 100 MB for the software installation.

Remark: On Microsoft Windows 7 Professional, installation of **Service Pack 1 is mandatory**.

System with Microsoft Windows 10 Pro 32-bit / 64-bit

System: Minimum Pentium Processor 2.4 GHz, recommended 3.0 GHz or higher.
RAM memory: Minimum 4 GB, recommended 8 GB or more.
Hard disk: 100 MB for the software installation.

System with Microsoft Windows Server 2016 Standard 64-bit

System: Recommended 3.2 GHz or higher.
RAM memory: Recommended 16 GB or more.
Hard disk: 100 MB for the software installation.

Drive (optional): DVD-ROM drive to install the software.

Display: Minimum VGA (800 x 600), recommended SVGA (1024 x 768 or more) with high color (24-bit).

Pointing device: Mouse or compatible pointing device.

PDF Reader: To open the EULA, Readme, and User Manual files installed in PDF format.

Remark: When Chinese is used as Unity Loader Setup or Runtime Language on a non-Chinese Windows it is recommended to select “Chinese (Simplified)” as language for non-Unicode programs in the “Region and Language” settings.

3 SETUP PROCEDURE

3.1 Recommendations before installation

- Check that you have Administrator rights.
- Check that the latest available Service Packs and Security Patches for Windows are installed.
- Close all other applications running.
- During the installation phase, it is recommended to temporarily disable all Antivirus services.

3.2 Unity Loader Setup procedure

If you have:

- the packaged distribution of Unity Loader, the installation software is on the installation media in your package.
To start the installation, enter D:\setup.exe, where D: is the drive letter for your CD/DVD/USB drive.
- the electronic distribution, the installation software is included in the file you downloaded.
Browse to the directory where you saved the downloaded file and either decompress the file or make a CD to start the installation.

When you start the installation, the Installation Wizard will guide you through the installation procedure.

3.3 Communication Drivers installation

The USB driver is required to exchange data with Modicon M340, M580 or Momentum PLC platforms through the USB console port. If the driver has not been installed previously, for example with Unity Pro or Control Expert, please proceed as follows:

1. Browse the content of your installation media.
2. Open the folder "**Communication Drivers**".
3. Run the executable file "**SchneiderPLCUSBDriverSuite.exe**".
4. Follow the instructions of installation.

The UNITELWAY driver is required to exchange data with Premium TSX PLC platforms via a serial connection. If the driver has not been installed previously, for example with Unity Pro or Control Expert, please proceed as follows:

1. Browse the content of your installation media.
2. Open the folder "**Communication Drivers**".
3. Run the executable file "**SchneiderUnitelwayDriverSuite.exe**".
4. Follow the instructions of installation.

Remark: For operation UNITELWAY driver requires installation of Microsoft .NET Framework 2.0.

The MODBUS driver is required to exchange data with Quantum TSX PLC platforms via a serial connection. If the driver has not been installed previously, for example with Unity Pro or Control Expert, please proceed as follows:

1. Browse the content of your installation media.
2. Open the folder "**Communication Drivers**".
3. Run the executable file "**SchneiderModbusDriverSuite.exe**".
4. Follow the instructions of installation.

Remark: For more information please refer to the Communication Drivers Release Notes and Readme.

NOTE: Unity Pro is the former name of Control Expert for version 13.1 or earlier.

3.4 Recommendations to increase Security

- Frequently update your virus definitions.
- Regularly apply available Security Updates for Windows.
- Ensure you have up-to-date backups.
- Enable strong spam filters to prevent phishing e-mails from reaching the end users and authenticate in-bound e-mail.
- Disable macro scripts from Microsoft Office files transmitted via e-mail.
- Inform and educate your employees to identify scams, malicious links, and social engineering attempts.
- Configure access controls including file, directory, and network share permissions with least privilege in mind.
- Restrict TCP ports and traffic to where it is absolutely needed using router ACLs.
- Use host-based firewalls to limit communication on TCP ports, especially between workstations.
- Ensure all other cyber-defenses are up-to-date. If you are unclear then seek engagement with the cyber-services team: <http://www.schneider-electric.com/b2b/en/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp>

To obtain assistance on how to protect your installation, please contact your local Schneider Electric representative.

For further information on vulnerabilities in Schneider Electric's products, please visit Schneider Electric's cybersecurity web page at <http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page>.

4 REGISTRATION

Unity Loader is distributed as a free tool, which runs without registration.

5 UNINSTALL

To uninstall Unity Loader, please proceed as follows:

1. Call the setup of Unity Loader
or
2. Open the Windows Control Panel, select "Add or Remove Programs" and "Unity Loader" from the list

Click the "Remove" button

6 NEW FEATURES

Version V14.0 brings the following features:

- Support of firmware download for additional modules through update of device profiles (e.g. BME NOC 0321 module, BME NOR 2200 module).
- Support of project transfer for additional modules through update of device profiles (e.g. BMX NOC 0401 module, BMX NOC 0402 module).
- Further improvements for Cyber Security protection.
- End User License Agreement (EULA) updated.

Version V12.0-SP1 brings the following updates:

- Support of firmware download and application transfer for additional devices through update of device profiles (e.g. BME P58 xxxx S and BME H58 xxxx S controllers).
- Improvements for Cyber Security protection due to fixes for known vulnerabilities (CVE-2016-10395, CVE-2017-9765) and support of "Secure Boot" option on Windows 10 with latest version of the Communication Drivers included.
- Treatment of application password corrected because depending on the application structure under certain conditions the comparison of the password entered by the user with the password retrieved from the PLC didn't succeed.
- Reference to the Instruction Sheet in downgrade message replaced by a search on the "Support > Download Center" section.
- Reminder for an optional registration removed.

Version V12.0 brings the following features:

- Support of firmware download for additional modules through update of device profiles (e.g. PME UCM 0202 module, PME GPS 0100 module, 140 CRA 31 908 module, BME NOP 0300 module, BMX NOR 0200 module).
- Installation of Schneider Electric Software Update (SESU) to provide automatic access to available software updates.
- To prevent potential equipment damage when downgrading the firmware of certain CRA devices the corresponding downgrade message now refers to an Instruction Sheet that provides some advice.

Version V11.1 brings the following features:

- Support of firmware download for a certain kind of modules through specific device profiles (e.g. 140 CRA 312xx module, TCSEGDB23F24FA Modbus Plus Proxy module, NOS module, ...).

Version V11.0 brings the following features:

- Firmware download capability for Modicon M580 HSBY PLCs.

Version V10.0 brings the following features:

- Improvements for Cyber Security protection (synchronized with Unity Pro V10.0):
 - o Enhance existing protection mechanism to reserve the Modicon M580 and M340 PLCs.
 - o Customize FTP password for firmware download to the Modicon M580 PLC platforms.

Version V8.1 brings the following features:

- Support of firmware download for modules that only support FTP connection (e.g. BMEAH10812 and BMEAH00412 HART modules or PMESWT0100 Weighing module).
- To prevent potential equipment damage when downgrading the firmware of a device the corresponding downgrade message now refers to an Instruction Sheet that provides some advice.

Version V8.0 brings the following features:

- Firmware download capability for Modicon M580 and Momentum PLC platforms.
- Cyber Security protection with new application password and encryption algorithm:
 - o Protect start/stop of PLC.
 - o Protect transfer of project and project data.
 - o Protect transfer of firmware.
- Cyber Security protection with new data storage password:
 - o Protect transfer of project files.
- Modbus TCP offered as additional connection media for Quantum PLC platforms.
- Registration / Licensing:
 - o Unity Loader now checks the registration data using the OneLicensing mechanism.
 - o Due to changes in the licensing policy, the registration data from previous versions will not be retained.
 - o Registration as free tool by Web and reminder every 21 days if product is not registered.
 - o End User License Agreement (EULA) updated for OneLicensing and format changed from HTML to PDF (requires installation of PDF reader on the PC).

Version V2.3 brings the following features:

- Adaptation of Unity Loader User Interface for CRA 312xx:
 - o These modules don't support a SD-card, but only have internal memory:
 - Checkbox "Save on Memory Card" renamed to "No Memory Card" and disabled.
 - Item "Memory Card" renamed to "Internal Memory"
 - o It is not possible to start or stop these modules, as they do not contain an application.
 - o For this reason, it is also not possible to download or upload applications or application-related data.
 - o New messages displayed in case of firmware download.
- Registration / Licensing:
 - o Registration is disabled in this version; Unity Loader runs without license check.
- UAC improvement for Windows Vista and Windows 7:
 - o Save settings in HKCU (for Windows XP in HKLM)
 - o Default path for log files now in TEMP folder

Version V2.2 brings the following features:

- Firmware download capability for CRA 312xx modules.
- Setup changed from Wise Installer to InstallShield.

Version V2.1 brings the following features:

- Additional possibility of download or upload projects and project data for all Quantum PLC platforms via the Modbus protocol. The Modbus protocol can be chosen at the "Connection" area of the Unity Loader.

Version V2.01-SP1 brings the following features:

- Additional possibility of download or upload projects and project data for all Premium PLC platforms via the Unitelway protocol. The Unitelway protocol can be chosen at the "Connection" area of the Unity Loader.

Version V2.0 brings the following features:

- Firmware download capability for all modules that embed a firmware (CPU, Ethernet, Analog, Motion)
- Update at once a CPU firmware and the project with a single memory card
 - o A firmware update can be stored inside the memory card to be downloaded later in another PLC (Modicon M340 only).
- Automated and transparent use of Unity Loader
 - o Third party software can execute Unity Loader services through a batch file.

7 CYBER SECURITY FEATURES

In Unity Pro V8.0 or later it is possible now to protect access to the application and application data on the PLC with a user-defined password.

In Unity Pro V10.0 or later it is possible now to protect the firmware transfer with a user-defined password.

When activating the protection in Unity Pro or Control Expert, Unity Loader will query for the corresponding passwords before executing the concerned operations.

NOTE: Unity Pro is the former name of Control Expert for version 13.1 or earlier.

7.1 Managing the Application Password in Control Expert

CPU application protection by a password prevents unwanted application modification, download, or opening (.STU and .STA files). The password is stored encrypted in the application.

An application is not password protected by default.
It is possible to create or change a password at any time.

7.1.1 Creating / Changing the Application Password in Control Expert

To create or change the Control Expert application password, follow these steps:

Step	Action
1	Right-click your project name → Properties in the Project Browser . Result: The Properties of Project dialog box opens.
2	Select the Protection tab.
3	In the Application area, click the Change password ... button. Result: The Modify Password dialog box opens.
4	<ul style="list-style-type: none">To enter a new password, type the password in the Entry field. Retype the password in the Confirmation field and click OK.To change an existing password, type the current password in the Old password field. Type the new password in the Entry field. Retype the new password in the Confirmation field and click OK.
5	In the Properties of Project dialog box, click Apply to save the changes, or click OK to save and close.

7.1.2 Removing the Application Password in Control Expert

To remove the Control Expert application password, follow these steps:

Step	Action
1	Right-click your project name → Properties in the Project Browser . Result: The Properties of Project dialog box opens.
2	Select the Protection tab.
3	In the Application field, click the Clear password ... button. Result: The Password dialog box opens.
4	Type the password in the Password field and click OK .
5	In the Properties of Project dialog box, click Apply to save the changes, or click OK to save and close.

7.1.3 Resetting a Forgotten Application Password in Control Expert

If you forget the Control Expert application password, follow these steps to reset it:

Step	Action
1	When the Application Password dialog box opens, press SHIFT+F2 . Result: A grayed number is displayed in the Application Password dialog box.
2	Contact your Schneider Electric Support and give this number to the support representative.
3	In the Application Password dialog box enter the received password. NOTE: It is a temporary password, available as long as you do not modify the application.
4	Modify the password (old password = password provided by Schneider Electric Support).
5	Click Build → Build Changes .
6	Save the application.

7.2 Managing the Data Storage Password in Control Expert

Data storage protection by a password helps prevent unwanted access to the data storage zone of the SD memory card (if a valid card is inserted in the CPU).

The data storage area is password protected by default with the following password: **datadownload**. It is possible to **change** or **reset** the password at any time.

NOTE: When importing a ZEF file, the data storage password of the application is set to its default value.

7.2.1 How to Change the Data Storage Password in Control Expert

To change the data storage password, follow these steps:

Step	Action
1	Right-click your project name → Properties in the Project Browser . Result: The Properties of Project dialog box opens.
2	Select the Protection tab.
3	In the Data Storage area, click the Change password ... button. Result: The Modify Password dialog box opens.
4	Enter the previous password in the Old password field.
5	Type the new password in the Entry field.
6	Confirm the new password in the Confirmation field.
7	Click OK to save the changes. NOTE: If you enter an incorrect old password, the message Wrong Password! is displayed.

7.2.2 How to Reset the Data Storage Password in Control Expert

To reset the data storage password, follow these steps:

Step	Action
1	Right-click your project name → Properties in the Project Browser . Result: The Properties of Project dialog box opens.
2	Select the Protection tab.
3	In the Data Storage area, click the Reset password ... button. Result: The Password dialog box opens.
4	Enter the current password in the Password field.
5	Click OK to reset the password to its default value: datadownload . NOTE: If you enter an incorrect old password, the message Wrong Password! is displayed.

7.3 Managing the Firmware Protection Password in Control Expert

Firmware protection by a password helps prevent unwanted access to the module firmware via FTP.

NOTE: Firmware password is implemented from Unity Pro V10.0. An application created with Unity Pro V10.0 cannot be opened with an earlier version of Unity Pro.

The firmware is password protected by default with the following password: **fwdownload**. It is possible to **change** or **reset** the password at any time.

NOTE: When importing a ZEF file, the firmware password of the module is set to its default value.

7.3.1 How to Change the Firmware Protection Password in Control Expert

To change the firmware protection password, follow these steps:

Step	Action
1	Right-click your project name → Properties in the Project Browser . Result: The Properties of Project dialog box opens.
2	Select the Protection tab.
3	In the Firmware area, click the Change password ... button. Result: The Modify Password dialog box opens.
4	Enter the previous password in the Old password field.
5	Type the new password in the Entry field.
6	Confirm the new password in the Confirmation field.
7	Click OK to save the changes. NOTE: If you enter an incorrect old password, the message Wrong Password! is displayed.

7.3.2 How to Reset the Firmware Protection Password in Control Expert

To reset the firmware protection password, follow these steps:

Step	Action
1	Right-click your project name → Properties in the Project Browser . Result: The Properties of Project dialog box opens.
2	Select the Protection tab.
3	In the Firmware area, click the Reset password ... button. Result: The Password dialog box opens.
4	Enter the current password in the Password field.
5	Click OK to reset the password to its default value: fwdownload . NOTE: If you enter an incorrect old password, the message Wrong Password! is displayed.

The application password protects the following operations in Unity Loader:

- Start/stop of PLC
- Transfer of project and project data in “Project” tab

The data storage password protects the following operations in Unity Loader:

- Transfer of project files in “Project” tab

The FTP password protects the following operations in Unity Loader:

- Transfer of firmware in “Firmware” tab

NOTE: With introduction of the Cyber Security protection since V8.0, it is not possible to access the location for “User Web Files” on the PLC anymore. Thus, for legacy platforms “User Web Files” are no longer included as part of the project files (*.CAR).

Furthermore, due to limitations on the platform side for Modicon M580 PLCs and Modicon Momentum PLCs the transfer of project files (*.CAR) is not available.

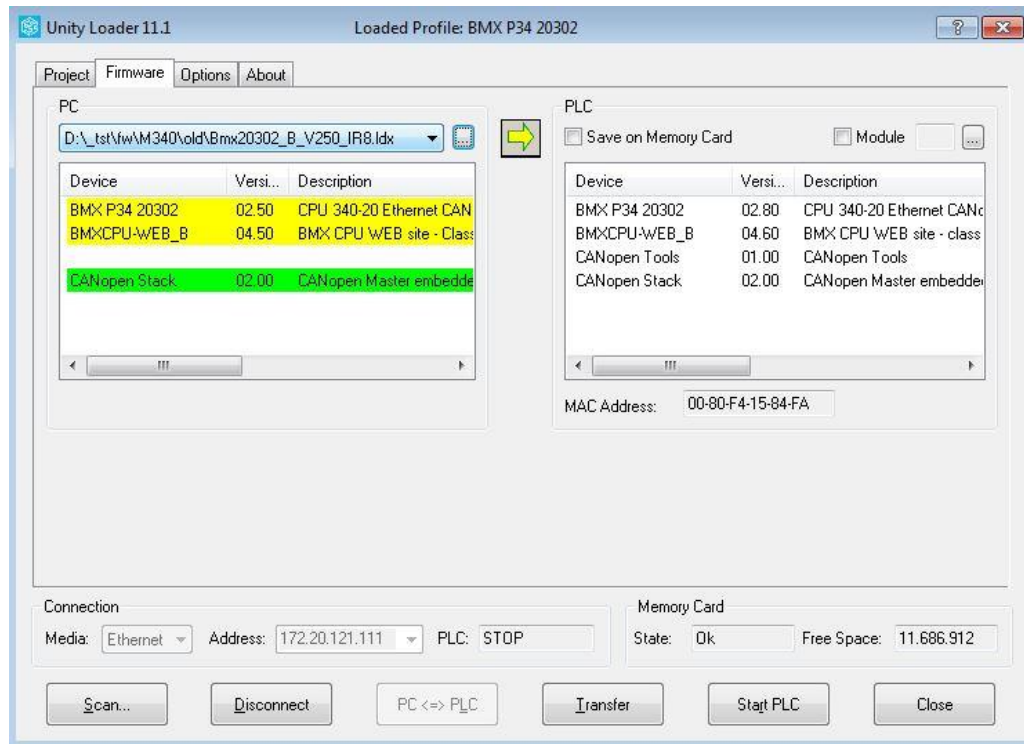
NOTE: If you once entered the requested password correctly if you are connected to the PLC Unity Loader normally will not query for this password again.

NOTE: While connected to the PLC with Unity Loader it might happen that the password entered in Unity Loader before could have changed (e.g. parallel connection with Control Expert to the same PLC). In this case, you must enter the new password in Unity Loader for the next operation.

NOTE: If you download a protected STU / STA to the PLC in case you do not know the associated application password, you will have to use the Control Expert password recovery mechanism to operate the PLC again.

8 README LAST MINUTE INFORMATION

- The order of the FW file entries displayed in the PC list box is aligned with the entries in the PLC list box obtained from the connected device. Additionally, the background color reflects the compatibility state:
 - Green indicates that the firmware of the PC is identical or greater than the firmware of the PLC.
 - Yellow indicates that the firmware of the PC is earlier than the firmware of the PLC.
 - Red indicates that the firmware of the PC and the PLC are not compatible.



- PLC status displayed in the Connection area:
 - RUN
 - STOP
 - HALT
 - LOADING
 - NOCONF
 - ERROR
 - --- (displayed in case the connected device is not able to provide the state of the PLC)
- When creating an application in Unity Pro V8.0 or later for the Modicon M580 platform please enable FTP before you build and download the application, otherwise Unity Loader will not be able to connect to the PLC.
- Cyber Security protection with application password or data storage password is not supported for UIUmas.exe and UIftp.exe command line interfaces in this version. Thus, scripting through command line interfaces can only be used if the PLC is not protected by password.

-
- Upgrading the firmware of any module (except Ethernet modules like AHI / AHO, SCAIME, NOC, NOE, CRA, ...) must be done through the CPU connection.
 - Upgrading the NOE communication module must be done through the connection port of the NOE module itself. It is not possible to download the firmware through the CPU.
 - Upgrading the CRA module could be done either through a connection to the service port of the corresponding CRP using the IP address of the CRA or a connection to the service port of the CRA module itself.
 - After upgrading a module with firmware, the firmware version displayed in Unity Loader is not always refreshed immediately. Some modules show the correct version immediately, for other modules a reset of the PLC is required.
 - For upgrading a firmware of a Modicon M340 PLC via an Ethernet connection, please assure that no other Ethernet connection is established in parallel at the PC. This could disturb the Ethernet connection of the Modicon M340 PLC during the Firmware update and could result in an unsuccessful transfer.
 - In case you get the message "**Transfer error: Not enough free space available on target device**" during firmware download to a Modicon M340 PLC:
 - The firmware download process needs free space on the memory card to store the firmware, until the update was successful. If there is not enough free space on the memory card, this message appears. Please free some space on the memory card by deleting files.
 - In case you get the message: "**Warning: File could not be transferred. FTP server rejects file name. One or more files have not been transferred**" during firmware download to a Modicon M340 PLC:
 - The firmware download process could not write the specified file to the memory card. The firmware update process is aborted in this case, since the firmware files must be consistent for a successful update. This can happen, if the file to be written is read-only on the memory card. Please check the file attributes on the memory card in this case and remove the read-only flag, if it is set.
 - Today it is not possible to download an application or project data to a Quantum PLC with no valid application. If the Quantum PLC owns no valid application, like after an OS exchange, a valid application must be downloaded first via Unity Pro, before a communication with the Unity Loader is possible.