

Contents

1	L-STUDIO Secure Projects.....	2
1.1	Introduction.....	2
1.2	Concepts.....	2
2	Workflows.....	3
2.1	Creating secure projects	3
2.2	Converting clear text to secure projects	4
2.3	Archiving/Unarchiving secure projects.....	5
2.3.1	“Use project password” - Secure Project Sharing	5
2.3.2	“Use custom password” – Share to Others.....	6
2.4	Changing a Project Password.....	6
2.5	Resetting Project Passwords (Recovery).....	7
3	Technical Information.....	9
3.1	Password Complexity.....	9
3.2	Credential Encryption	9
3.3	Device Communication.....	10
3.4	Runtime Encryption	10
4	Changelog	11

1 L-STUDIO Secure Projects

1.1 Introduction

L-STUDIO, starting from version 3.2.14, will provide new features for creating secure projects. These features will be extended in future versions to comply with the requirements of the EU Cyber Resilience Act.

A secure project provides the following advantages:

- Administrative credentials are stored encrypted on disk.
- Communication paths (Deploy, Watch, Tools) use only HTTPS or Websockets over HTTPS.
- The runtime cross-communication (as used for the LROC system) is encrypted and authenticated.

1.2 Concepts

Project password: A secure project is protected by a project password with complexity requirements. This project password is used to encrypt communication and administrative credentials.

Secure project: A secure project is an L-STUDIO project which is protected by a project password.

Default passwords: Devices in a secure project have **project-specific** passwords for devices. They are used instead of the former default passwords in the device templates. These passwords have also complexity requirements to avoid brute-force attacks.

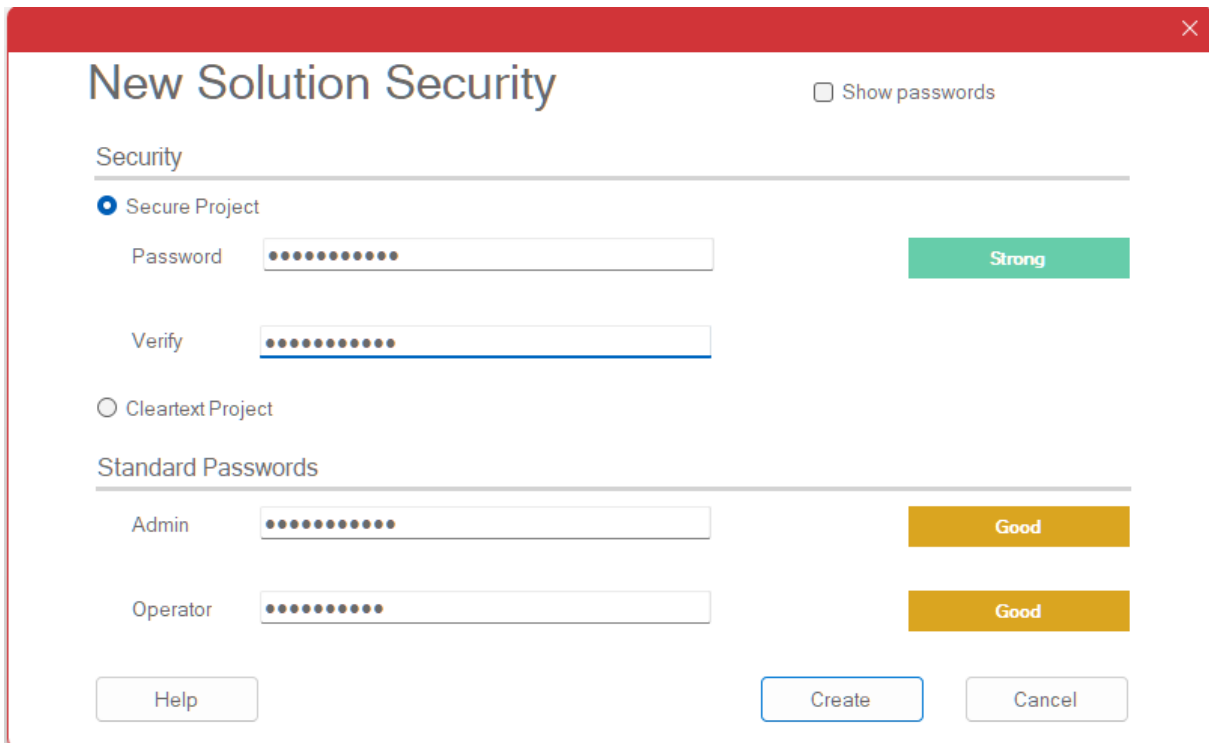
Windows credentials store: The project password is stored in the Windows credentials store (just as browser or Windows credentials). This is a convenience feature to avoid entering the project password again once a secure project is created.

2 Workflows

2.1 Creating Secure Projects

When a new project is created, the user can choose between creating a clear-text and a secure project. When choosing a secure project the following additional information must be provided:

1. Project password: This password is used to encrypt credentials in the L-STUDIO project. It must be a *strong* password to be accepted.
2. Standard admin password: This password is used as admin password for new devices. It needs to be at least a *good* password.
3. Standard operator password: This password is used as operator password for new devices. It needs to be at least a *good* password.



It is recommended to use *strong* passwords also for admin/operator passwords. The requirements might be tightened in future for regulation compliance.

After creating a secure project, it can be used like a clear-text project on the same PC. The project password is stored in the Windows credentials store and does not need to be entered again.

2.2 Converting Clear-Text to Secure Projects

A clear text project can be converted into a secure project. This is done by using the “Convert to secure project” dialog.



Then, a dialog like the secure password creation dialog appears:

 The dialog box is titled 'Convert To Secure Project' and has a red header bar. It contains several sections:

- ☐ Create cleartext archive before conversion
- ☒ Security
 - ☒ Secure Project
 - Password: [masked] [Strong]
 - Verify: [masked]
 - ☐ Cleartext Project
- ☐ Standard Passwords
 - Admin: [masked] [Good]
 - Operator: [masked] [Good]

 At the bottom, there is a warning message: 'Warning: You must keep the project password in a safe place. There is no way to recover the password else.' and two buttons: 'Convert' and 'Cancel'.

The following additional information must be provided:

1. Project password: This password is used to encrypt credentials in the L-STUDIO project. It must be a *strong* password to be accepted.
2. Standard admin password: This password is used as admin password for new devices. It needs to be at least a *good* password.

3. Standard operator password: This password is used as operator password for new devices. It needs to be at least a *good* password.

There is an option to create a clear-text archive before the credentials are encrypted. The clear-text archive must be protected by security means defined by the user.

When clicking on the “Convert” button, the credentials will be encrypted, and a runtime communication key will be created. Then L-STUDIO will clean and rebuild the project to remove any intermediate files of the former clear-text project. The project password is stored in the Windows credentials store, so that there is no need to enter the project password again on the same PC.

The conversion does not change any device credentials. In the conversion case you need to secure the existing passwords manually. This is to avoid breaking existing systems.

Important: After conversion you need to deploy all devices to enable encrypted runtime communication. It is not possible to use a mix of unencrypted and encrypted devices.

2.3 Archiving/Unarchiving Secure Projects

For archiving secure projects, several workflows are possible and supported by L-STUDIO:

Archive type	Project Password	Custom Password
Archive encrypted	Yes, using project password	Yes, if custom password is not empty
Device credentials	Included	Excluded
Runtime communication	Included	Excluded
Security GUID	Included	Excluded

When choosing the archive function, another dialog appears after selecting the target folder:

2.3.1 “Use project password” - Secure Project Sharing

To use the same project on different PCs, the project must be archived on the source machine and unarchived on the destination machine. Using this workflow, the credentials are retained.

The ZIP file is encrypted with the project password and contains the credentials file.

When unarchiving the project, the user must enter the project password. Then the project will be unarchived and the project password will be stored in the Windows credential store.

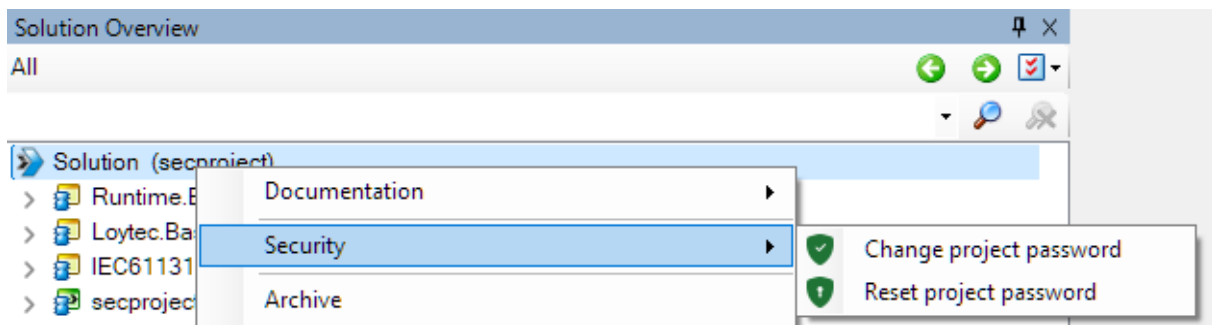
2.3.2 “Use custom password” – Share to Others

This option is intended to share a secure project with someone else, for example LOYTEC support. The archive will be encrypted with the custom password (or none, if the custom password is empty). This archive does not contain the original credentials, so the receiver has no information on the device credentials.

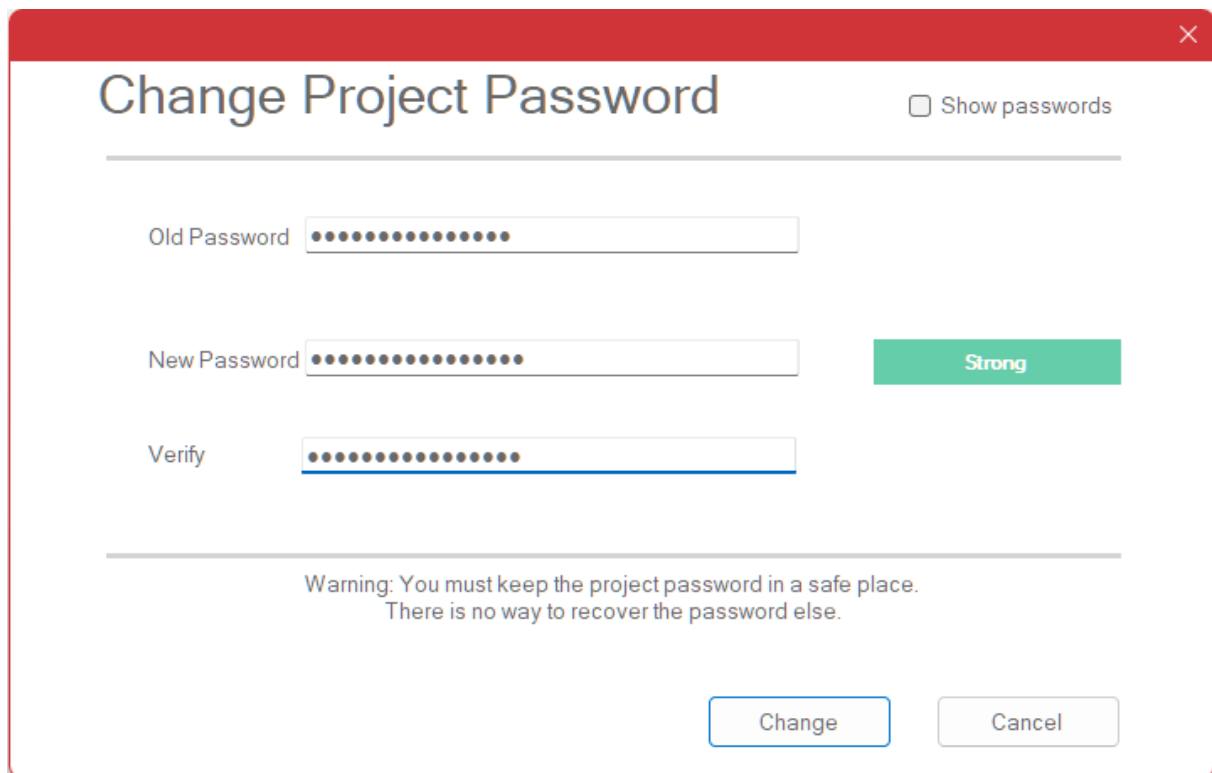
When unarchiving a custom encrypted archive, the user must enter the custom password. Then the archive is unarchived, and the device credentials are cleared. The user then needs to set the device credentials to the passwords used in the target devices.

2.4 Changing a Project Password

In case a project password is compromised, or regulations require a password change, the password can be changed. This change does not affect the device credentials. All contained credentials are transparently re-encrypted using the new project password.



In the change project password dialog, the old and the new project password must be entered:



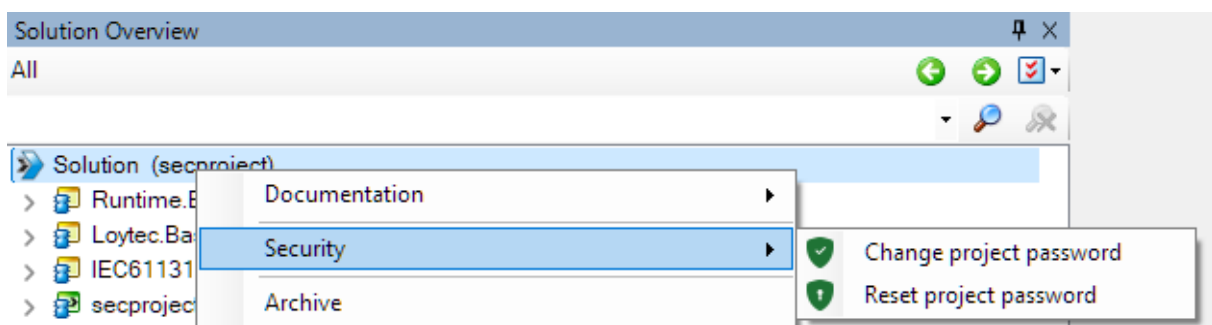
The dialog box is titled "Change Project Password" and has a red header bar with a close button (X) in the top right corner. In the top right of the main area, there is a checkbox labeled "Show passwords". Below the title bar, there are three input fields: "Old Password", "New Password", and "Verify". Each field contains a series of dots representing masked characters. To the right of the "New Password" field is a green button labeled "Strong". Below the input fields is a warning message: "Warning: You must keep the project password in a safe place. There is no way to recover the password else." At the bottom right, there are two buttons: "Change" and "Cancel".

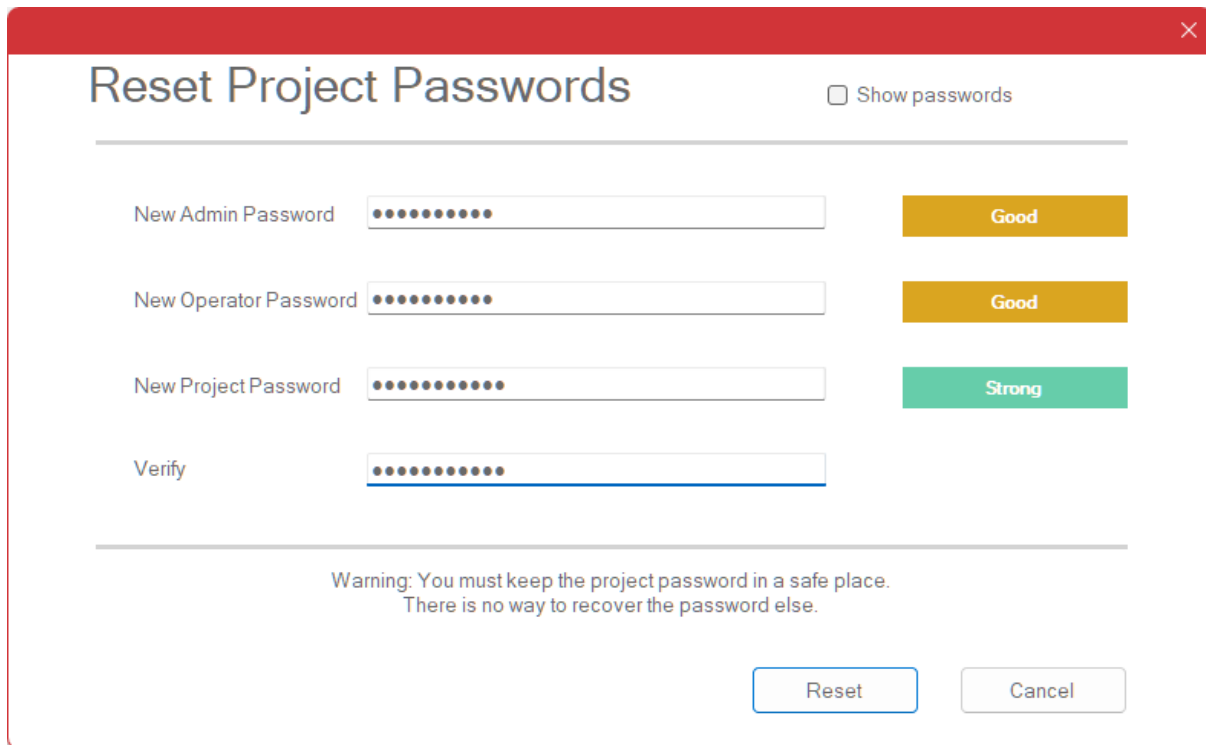
After clicking “Change”, the credentials are re-encrypted and the new project password is stored in the Windows credential store.

2.5 Resetting Project Passwords (Recovery)

The project password, once lost, cannot be recovered from the L-STUDIO project.

However, it is possible to recreate new credentials using the “Reset project password” dialog.





The dialog box is titled "Reset Project Passwords" and has a red header bar with a close button (X) in the top right corner. Below the title bar, there is a checkbox labeled "Show passwords". The main area contains four password input fields, each with a strength indicator to its right:

- New Admin Password:** The input field shows 10 dots. The strength indicator is a yellow box labeled "Good".
- New Operator Password:** The input field shows 10 dots. The strength indicator is a yellow box labeled "Good".
- New Project Password:** The input field shows 10 dots. The strength indicator is a green box labeled "Strong".
- Verify:** The input field shows 10 dots.

Below the input fields, there is a warning message: "Warning: You must keep the project password in a safe place. There is no way to recover the password else." At the bottom right, there are two buttons: "Reset" (highlighted with a blue border) and "Cancel".

In the reset project passwords dialog, the following information must be provided:

1. **Project password:** This password is used to encrypt credentials in the L-STUDIO project. It must be a *strong* password to be accepted.
2. **Standard admin password:** This password is used as admin password for new devices. It needs to be at least a *good* password.
3. **Standard operator password:** This password is used as operator password for new devices. It needs to be at least a *good* password.

When clicking on Reset, a new secure project will be created, the project password will be stored in the Windows credentials store and the device credentials will be replaced with the new admin and operator password.

To recover a project password loss, the following steps must be taken in the following order:

1. Set device passwords to a known state (skip if device passwords are still known).
2. Perform the L-STUDIO reset project passwords step
3. Deploy project (all devices).
4. Reimport project in LWEB-900.

3 Technical Information

3.1 Password Complexity

L-STUDIO classifies passwords into the following complexity classes: *Blank, Weak, Fair, Good, Strong, Stronger*.

Currently, the project password requires *Strong* complexity while device credentials require *Good* complexity. This might change in later versions.

The complexity is calculated based on password entropy, so there are no fixed rules on length. Thus, a shorter password with more different characters is accepted as well as a longer password with only lowercase characters.

The password complexity follows these rules:

- Choosing at least one character from the lowercase/uppercase/digit/special group increases complexity.
- Repeated characters do not increase complexity, so “password!!!!” is not better than “password!”.
- Complexity increases with password length.

Note, that the calculated complexity needs to be thought of as a lower boundary. Organization or regulatory requirements might be higher.

3.2 Credential Encryption

The on-disk encryption of the secure project credentials is implemented using the following measures:

- The runtime communication and administrative credentials are encrypted using a random AES-256-CBC data encryption key.
- The data encryption key is encrypted using the AES key wrap, employing PBKDF-2 with salted project password. Thus, the data encryption key can be re-encrypted when the project password is changed.
- Credentials between L-STUDIO and the LINX/LVIS configurators are passed in-memory.
- The project password is stored in the user’s Windows credentials store. The protection level depends on the organization’s security architecture and deployment.

3.3 Device Communication

Secure projects use solely HTTPS for device communication. Other protocols (HTTP, SSH) are not allowed to reduce the attack surface of communication.

The HTTPS communication either employ using web services (like SOAP) or web sockets for the watch function and use the same communication path to the device's embedded web server.

The used cipher suites depend on the device firmware version. For firmware 8.4.x the chosen cipher is `TLS_AES_256_GCM_SHA384`. This might change due to Windows and firmware versions.

3.4 Runtime Encryption

In a secure project the runtime communication is wrapped by DTLS v1.2 as defined in RFC6347. DTLS was chosen to retain the real-time properties of the communication protocol while providing authentication and encryption.

The devices use a random project 128-bit communication secret which is downloaded during deployment. This secret is solely used for authentication. The encryption keys are created during the DTLS handshake.

The communication secret is automatically created during secure project creation and requires no user interaction.

As the runtime protocol contains routing elements, all devices need to use DTLS in a secure project. Therefore, it is mandatory to deploy all devices to switch them to DTLS.

Runtime communication encryption is supported in Firmware 8.4.2 and higher.

To verify that a device uses DTLS, check the log file for the following line:

2025-08-17 16:02:52.707 NOTE Application RT61499: Using DTLS.

Encrypted runtime communication uses the fixed UDP port 61499 for the responder side and a random client UDP port on the initiator side.

If two devices are connected in the L-STUDIO projects, then both devices open a DTLS connection to its peer.

4 Changelog

2025-09-18: Initial version [TR]