User Manual

Ledger Nano S Plus

Contributors

- Cécile Leang | Knowledge Base Manager

Document history

Author	Date	Modification purpose
Cécile Leang	25/01/2022	Document creation
Benoit Lucet	02/02/2022	Document review
Cécile Leang	19/02/2022	Modifications after review
Romain Muguet	21/02/2022	Document review
Cécile Leang	22/02/2022	Modifications after review

About this document

What is the Ledger Nano S Plus?

The Ledger Nano S Plus is an improved version of the world's most famous hardware wallet, boasting a larger and higher-quality screen, more storage capacity, and many more plugins and apps to support a wide variety of coins and functions such as DeFi and NFTs.

The Nano S Plus is equipped with the industry-leading security element, which combined with Ledger's operating system allows developers to load and test their applications directly onto the product.

Purpose

This document provides an overview of the main functionalities of the Nano S Plus to help you get started. After reading this document, you should be able to set up your Nano S Plus, use the main features, and protect your device.

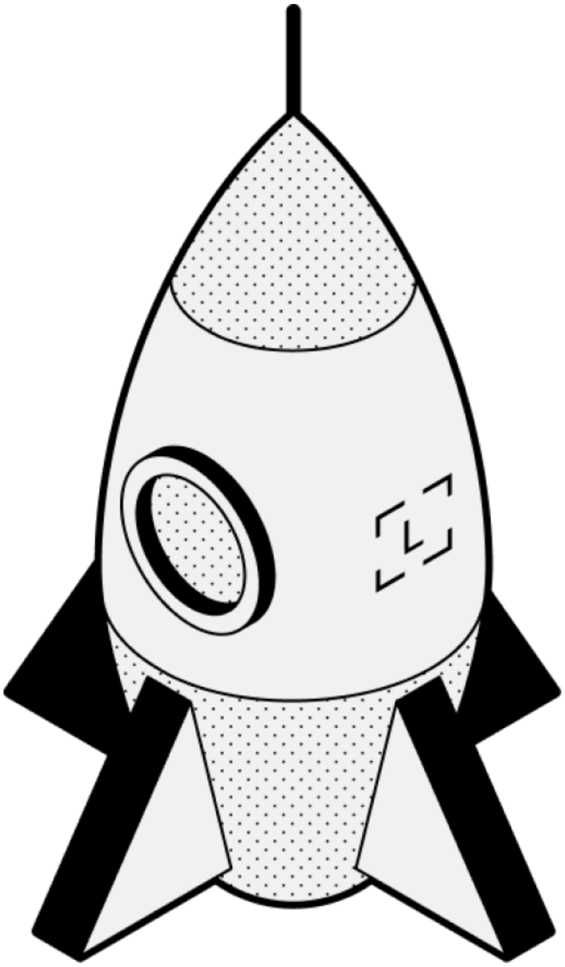
Prerequisites

Before you start using your Nano S Plus, you need to make sure that you complete the following requirements:

- A computer with at least Windows 8.1, macOS 10.14 (64-bit), or Linux Ubuntu 16.10 (64-bit) or a smartphone with at least Android 8.1 or i0S 13+.
- Download and install the Ledger Live application.

Content

Getting Started



1 - Checking if your Ledger Nano S Plus is genuine

Ledger products are built around a combination of hardware and software security, meant to protect your private keys from a wide range of potential attacks. Use this guide to make sure your Ledger device is genuine, and not fraudulent or counterfeit.

A few simple checks will assure you that your device is a genuine Ledger product:

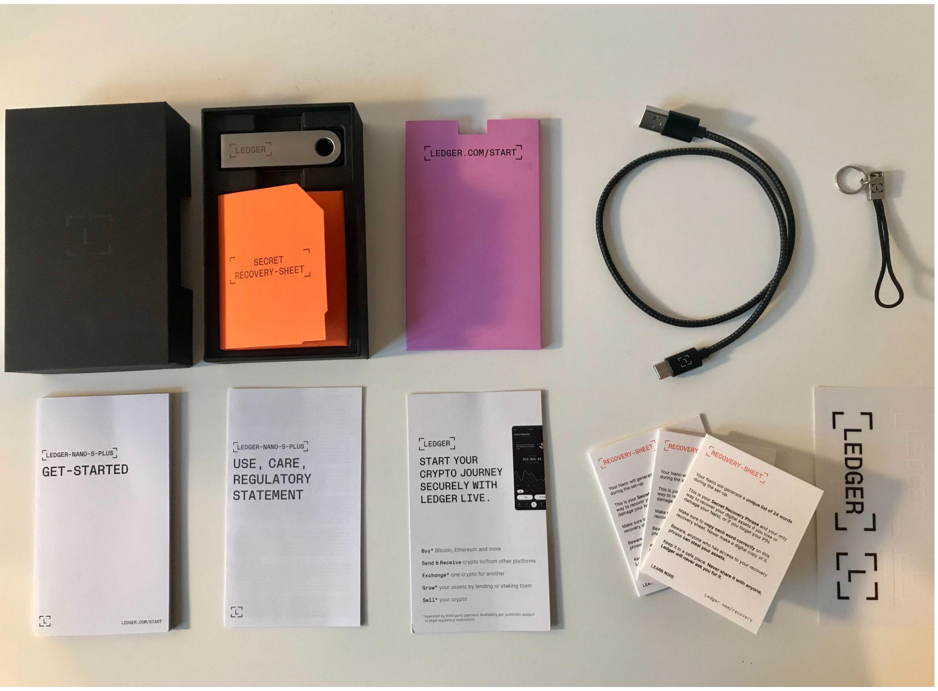
- ☐ Box contents
- ☐ Condition of the Recovery sheet
- ☐ Initial state of the Ledger device
- ☐ (advanced) Hardware integrity

Note: Since Ledger devices are manufactured in different periods of time, some characteristics such as the packaging and the color of internal components can present some slight differences. Don’t worry, this has no impact on the functionality of your device and your device is safe to use.

1.1- Checking the box contents

The package of a Ledger hardware wallet includes:

- A Ledger Nano S Plus
- USB A to USB Type-C cable
- An envelope including 3 blank **Recovery sheets**
- An envelope, including:
  - **Get started** leaflet
  - **Start your crypto journey securely with Ledger Live** card
  - **Use, Care and Regulatory Statement** leaflet
- Accessories:
  - A keychain
  - Ledger stickers
- Packaging: Ledger-branded cardboard box and sleeve



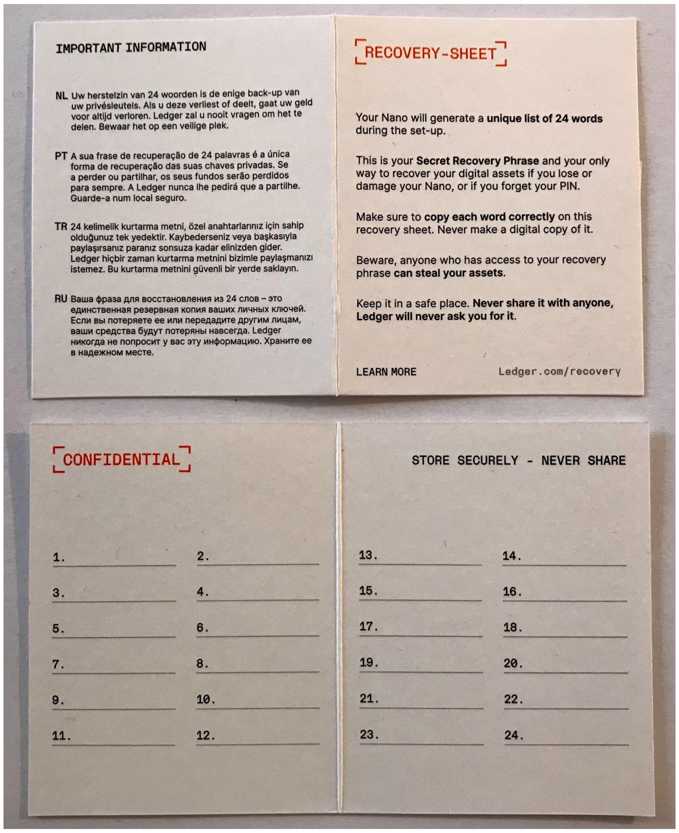
(Box contents of the Ledger Nano S Plus)

1.2- Checking the recovery sheets came blank

Upon setup, your Ledger device will generate a new, unique set of 24 words called a **recovery phrase**. All the words should be backed up onto a blank recovery sheet.

Please note that you cannot choose your recovery words yourself. Instead, your Ledger device will randomly select your recovery words for you. All recovery words are picked from a standardized list called the **BIP-39 list**. It's important to let your Ledger device pick the words because humans are very bad at creating randomness.

Your recovery phrase is critically important to the security of your crypto. If someone else were to access your recovery phrase, they would be able to steal all your crypto assets secured by your Ledger device.



IMPORTANT INFORMATION

NL Uw herstelzin van 24 woorden is de enige back-up van uw privésleutels. Als u deze verliest of deelt, gaat uw geld voor altijd verloren. Ledger zal u nooit vragen om het te delen. Bewaar het op een veilige plek.

PT A sua frase de recuperação de 24 palavras é a única forma de recuperação das suas chaves privadas. Se a perder ou partilhar, os seus fundos serão perdidos para sempre. A Ledger nunca lhe pedirá que a partilhe. Guarde-a num local seguro.

TR 24 kelimelik kurtarma metni, özel anahtarlarınız için sahip olduğunuz tek yedektir. Kaybederseniz veya başkasıyla paylaşırsanız paranız sonsuza kadar elinizden gider. Ledger hiçbir zaman kurtarma metnini bizimle paylaşmanızı istemez. Bu kurtarma metnini güvenli bir yerde saklayın.

RU Ваша фраза для восстановления из 24 слов – это единственная резервная копия ваших личных ключей. Если вы потеряете ее или передадите другим лицам, ваши средства будут потеряны навсегда. Ledger никогда не попросит у вас эту информацию. Храните ее в надежном месте.

RECOVERY-SHEET

Your Nano will generate a **unique list of 24 words** during the set-up.

This is your **Secret Recovery Phrase** and your only way to recover your digital assets if you lose or damage your Nano, or if you forget your PIN.

Make sure to **copy each word correctly** on this recovery sheet. Never make a digital copy of it.

Beware, anyone who has access to your recovery phrase **can steal your assets.**

Keep it in a safe place. **Never share it with anyone, Ledger will never ask you for it.**

LEARN MORE Ledger.com/recovery

CONFIDENTIAL

1. ____ 2. ____
3. ____ 4. ____
5. ____ 6. ____
7. ____ 8. ____
9. ____ 10. ____
11. ____ 12. ____

STORE SECURELY - NEVER SHARE

13. ____ 14. ____
15. ____ 16. ____
17. ____ 18. ____
19. ____ 20. ____
21. ____ 22. ____
23. ____ 24. ____

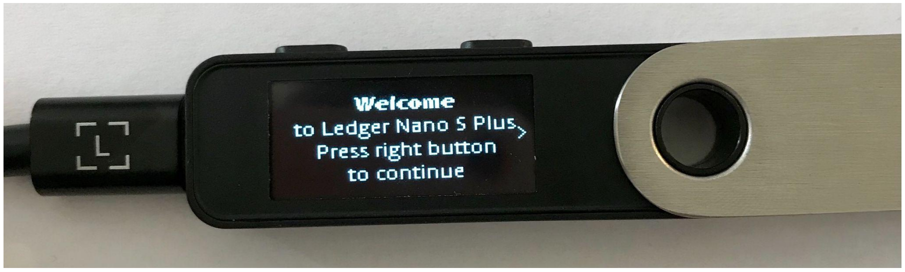
(Blank Recovery sheets)

Important information regarding your recovery phrase and recovery sheets

- Ledger will never provide you with a 24-word recovery phrase, pre-filled recovery sheet(s), or individual recovery words.
- Recovery words must be generated on your Ledger device screen during the initial setup and copied down on a blank recovery sheet.
- If your Ledger device came with pre-filled recovery sheets. Your device should be considered unsafe to use.
- If your Ledger device did not generate recovery words during setup. Your device should be considered unsafe to use.
- In those cases, please refrain from sending crypto assets to your Ledger device and immediately **contact Ledger Support** for assistance.

1.3- Checking for factory settings

- Make sure your Ledger device was not preconfigured with a PIN code that you did not choose yourself. The device should display the following: "**Welcome to Ledger Nano S Plus. Press right button to continue**."
  when you turn it on for the first time.
- Ledger never provides a PIN code in any way, shape, or form. Always choose the PIN code yourself.
- If a PIN code is given to you or if the device requires a PIN code you did not choose: it is not safe for you to use the device. Please contact **Ledger Support** for assistance.



(Ledger Nano S Plus: Welcome to Ledger Nano S Plus)

1.4- Checking hardware integrity

All Ledger devices pass the genuine check during the onboarding process and then each time when they connect to Manager in Ledger Live. Genuine Ledger devices hold a secret key that is set during manufacture. Only a genuine Ledger device can use its key to provide the cryptographic proof required to connect with Ledger's secure server.

Advanced users additionally can check the hardware integrity of the Ledger device to check that it has not been tampered with. This article contains detailed technical information about the security of your device.

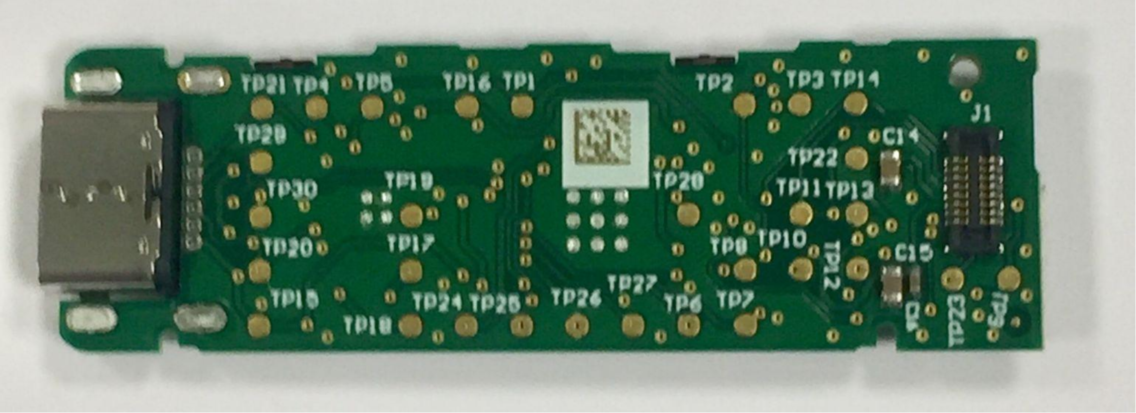
Important notice

- Please note that opening your Ledger device will void the warranty.

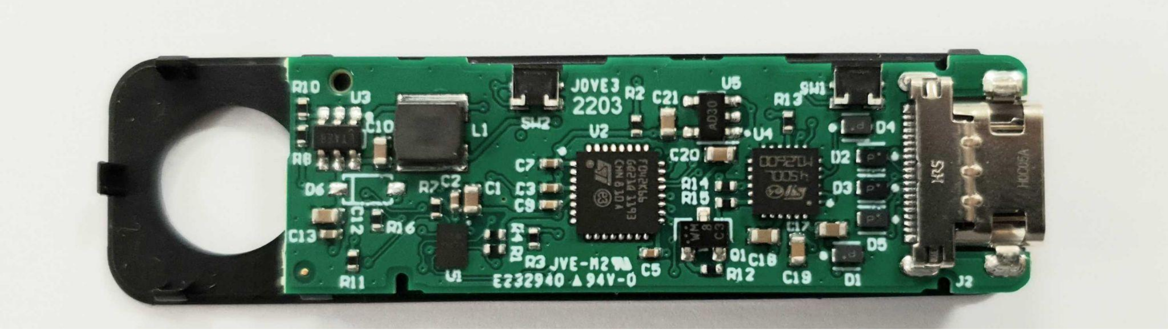
- Once opened, your Ledger device will no longer be refundable or exchangeable.

Microcontroller (MCU)

The Secure Element checks the full microcontroller flash at boot, as described in **this blog post**. If it has been modified, you'll get a warning at boot. As an additional check, you can open the device to verify that no additional chip has been added, compared with the images below, and that the MCU is an STM32F042K6U6.



(Front of the PCB)



(Back of the PCB)

Secure Element attestation

The Secure Element itself is personalized at factory with an attestation proving that it has been manufactured by Ledger. You can verify it by running:

```
pip install --no-cache-dir ledgerblue
```

```
python -m ledgerblue.checkGenuine --targetId 0x33100004
```

The source code **is available here.**

Application verification

When opening an application, a Non Genuine warning is displayed if the app has not been signed by Ledger. A modified User Interface (as found in https://github.com/LedgerHQ/nanos-ui) will also display a warning message on boot.

Root of trust

The root of trust for the current batch is the following secp256k1 public key:

```
0490f5c9d15a0134bb019d2afd0bf297149738459706e7ac5be4abc350a1f818057224fce12ec9a65de18ec34
d6e8c24db927835ea1692b14c32e9836a75dad609
```

- as checked here **Genuine.py**

2 - Setting up your Ledger Nano S Plus

To get started, you can either set up your Ledger Nano S Plus as a new device or restore your device from your recovery phrase:

- Set up your Nano S Plus as a new device: it will generate new private keys so you can manage your crypto assets. You will also write down a new 24-word recovery phrase, the only backup of your private keys.
- Restore your device from a recovery phrase: it will recover the private keys linked to an existing recovery phrase.

Important disclaimer

When you first receive a Ledger wallet, it must always be initialized by following this process: plugging in the device, generating a pin code, and then generating 24 words. If you were to receive a device containing a pre-completed recovery phrase or a pin code, you should not use the device, as it means that the device may have already been used by somebody else.
Ledger will never provide a pin code or recovery phrase with the product, nor ever ask for them. Under these circumstances, you must contact Ledger customer support.

2.1- Setting up as a new device

Set up your Ledger Nano S as a new device to get started. Your device will generate new private keys providing access to your crypto assets. You'll also write down your unique 24-word recovery phrase, the only backup of your private keys.

Prerequisites

☐ Ledger Nano S Plus with the supplied USB-C cable.

☐ A computer with at least Windows 8.1, macOS 10.14 (64-bit), or Linux Ubuntu 16.10 (64-bit) or a smartphone with at least Android 8.1 or i0S 13+.

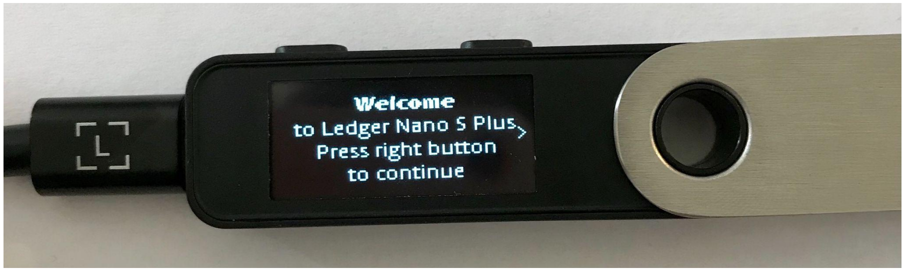
☐ The Ledger Live application downloaded and installed on your computer or your smartphone.

Instructions

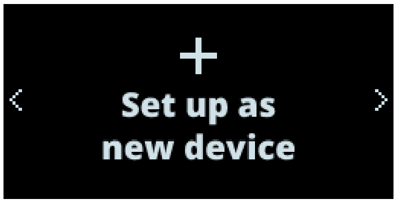
Ledger Live features interactive setup instructions. Simply open the app to get started.

2.1.1 - Setting up as a new device

1. Connect the Ledger Nano S Plus to your computer using the supplied USB-C cable. Your device should display the following: “**Welcome to Ledger Nano S Plus. Press right button to continue**.”
   Note: Please contact us if the device immediately asks for a PIN code. It may not be safe to continue using this device.

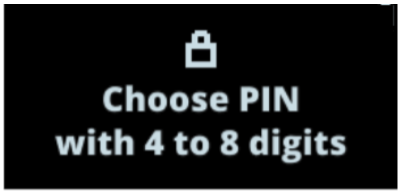


2. Press the right button to navigate through the on-screen instructions.
3. Press both buttons simultaneously to choose the option **Set up as new device**.


Set up as
new device

2.1.2 - Choosing your PIN code

1. Press both buttons when **Choose PIN with 4 to 8 digits** is displayed on the device.


Choose PIN
with 4 to 8 digits

2. Press the right or left button to choose the first digit of your PIN code.
3. Press both buttons to enter a digit.
4. Repeat the process until you've entered 4 to 8 digits.

5. Select the checkmark (✓) and press both buttons to confirm the PIN code. Use the backspace icon to erase a digit.
6. Confirm your PIN code by entering it once more.

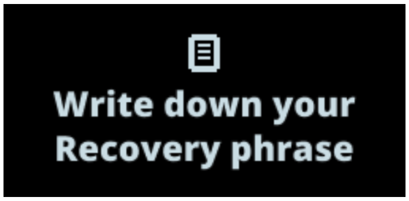
Security tips

- ✓ Choose your own PIN code. This code unlocks your device.
- ✓ An 8-digit PIN code offers an optimal level of security.
- ✓ Never use a device supplied with a PIN code and/or a recovery phrase.
- ✓ Contact Ledger Support in case of doubt.

2.1.3 - Writing down your recovery phrase

Your 24-word recovery phrase will now be displayed word by word on the Ledger Nano S Plus screen. The recovery phrase is the only backup of your private keys. It will be displayed only once.

1. Take a blank Recovery sheet supplied in the box.
2. Press both buttons when **Write down your recovery phrase** is displayed.



Write down your
Recovery phrase

3. Press the right button to navigate through the on-screen instructions. Then press both buttons to continue.
4. Write down the first word (**Write word #1**) on the Recovery sheet. Verify that you have copied it correctly in position 1.
5. Press the right button to move to the second word (**Write word #2**). Write it in position 2 on the Recovery sheet. Verify that you've copied it correctly. Repeat the process until the twenty-fourth word (**Write word #24**).
6. *(optional)* To verify your 24 words, press the left button.
7. Press both buttons to **Confirm your recovery phrase**.
8. Select the requested word by navigating with the left or right button. Validate the word by pressing both buttons. Repeat this step for each requested word.

Your device will display **Your Recovery phrase is set. Keep it in a secure place**.

9. Press the right button to navigate through the on-screen instructions. Then press both buttons to continue.
   Your device will display **Processing** and then **Your device is ready** once you've successfully completed the setup process.
10. Hold both buttons for 3 seconds to access the **Control Center**. The **Control Center** is where you can access the apps and settings on your device.

You've successfully set up your device. You can now install apps on your device and add accounts in Ledger Live.

Security tips

- ✓ Anyone with access to your recovery phrase could take your assets, store it securely.
- ✓ Ledger does not keep a backup of your 24 words.
- ✓ Never use a device supplied with a recovery phrase and/or a PIN code.
- ✓ Contact Ledger Support in case of doubt.

2.2 - Restoring a device from your recovery phrase

Restore a Ledger device from your recovery phrase to restore, replace or back up your Ledger hardware wallet. The Ledger device will recover the private keys backed up by your confidential recovery phrase.

Prerequisites

- ☐ Get the recovery phrase to restore. BIP39/BIP44 recovery phrases are supported.
- ☐ A computer with at least Windows 8.1, macOS 10.14 (64-bit), or Linux Ubuntu 16.10 (64-bit).
- ☐ The Ledger Live application downloaded and installed on your computer.

Instructions

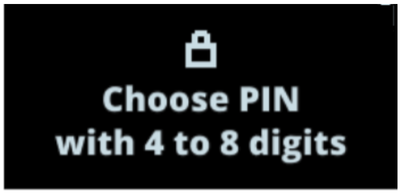
Ledger Live features interactive setup instructions. Simply open the app to get started.

2.2.1 - Restoring from recovery phrase

1. Connect the Ledger Nano S Plus to your computer using the supplied USB-C cable. Your device should display the following: “**Welcome to Ledger Nano S Plus. Press right button to continue**.”
   Note: Please contact us if the device immediately asks for a PIN code. It may not be safe to continue using this device.
2. Press the right button to navigate through the on-screen instructions.
3. Press both buttons simultaneously to choose the option **Restore from recovery phrase**.

2.2.2 - Choosing your PIN code

1. Press both buttons when **Choose PIN with 4 to 8 digits** is displayed on the device.



Choose PIN
with 4 to 8 digits

2. Press the right or left button to choose the first digit of your PIN code.
3. Press both buttons to enter a digit.
4. Repeat the process until you've entered 4 to 8 digits.
5. Select the checkmark (✓) and press both buttons to confirm the PIN code. Use the backspace icon to erase a digit.
6. Confirm your PIN code by entering it once more.

Security tips

- ✓ Choose your own PIN code. This code unlocks your device.
- ✓ An 8-digit PIN code offers an optimal level of security.

- ✓ Never use a device supplied with a PIN code and/or a recovery phrase.
- ✓ Contact Ledger Support in case of doubt.

2.2.3 - Entering your recovery phrase

1. Choose the length of your recovery phrase (12, 18, or 24 words). Press both buttons to validate.
   Make sure the correct recovery phrase length is selected. Always enter all words of a recovery phrase.
2. Enter the first letters of Word #1 by selecting them with the right or left button. Press both buttons to validate each letter.
3. Choose Word #1 from the suggested words. Press both buttons to validate it.
4. Repeat the process until the last word of your recovery phrase.
   Your device is ready is shown once you've successfully completed the setup process.
5. Press both buttons for 3 seconds to open the **Control Center**.

Security tips

- ✓ Anyone with access to your recovery phrase could take your assets, store it securely.
- ✓ Ledger does not keep a backup of your 24 words.
- ✓ Never use a device supplied with a recovery phrase and/or a PIN code.
- ✓ Contact Ledger Support in case of doubt.

3 - Updating your Ledger Nano S Plus firmware

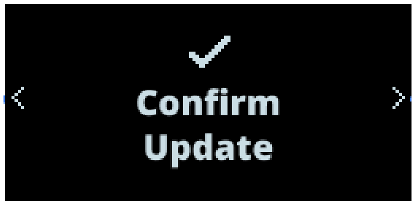
Update your Ledger Nano S Plus to benefit from the optimal security level and user experience offered by our products. Updating your device has no impact on your crypto assets or the functionality of your device.
Please find more information about this update in the **release notes**. Check our **troubleshooting article** if you need help.

Prerequisites

- □ Update Ledger Live through the notification banner or **download the latest version**. The mobile app does not support firmware updates.

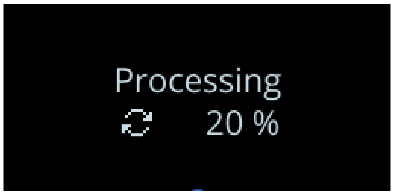
Instructions

1. Click on **Update firmware** in the orange notification banner.
   Note: If you don't see the notification banner, please try again later as the release is rolled out progressively.
2. Carefully read all instructions on the window that appears.
3. If your recovery phrase is written down and accessible, tick the checkbox at the bottom and click on **Continue**.
   The update process normally does not require the recovery phrase, but you should have it available as a precaution.
4. Your device will show **New firmware** and the **version** number.
   - Press the right button to select **Confirm update**. Press both buttons to confirm.



   - Enter your PIN code to confirm. Your device will then restart and install the update.

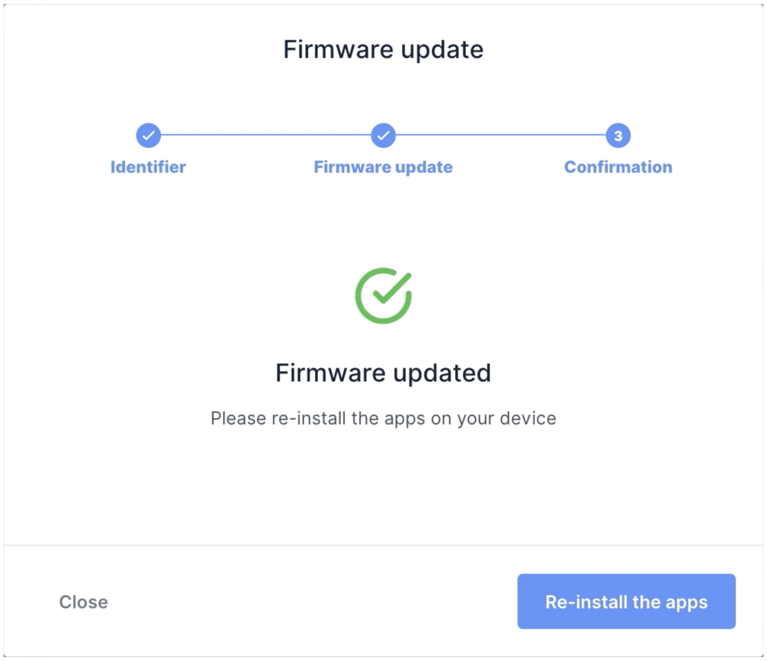
5. The update process will continue automatically. Ledger Live will display multiple progress loaders, while your Ledger Nano S Plus displays **Processing**.



Processing

20 %

Your device is successfully updated once Ledger Live displays **Firmware updated**.



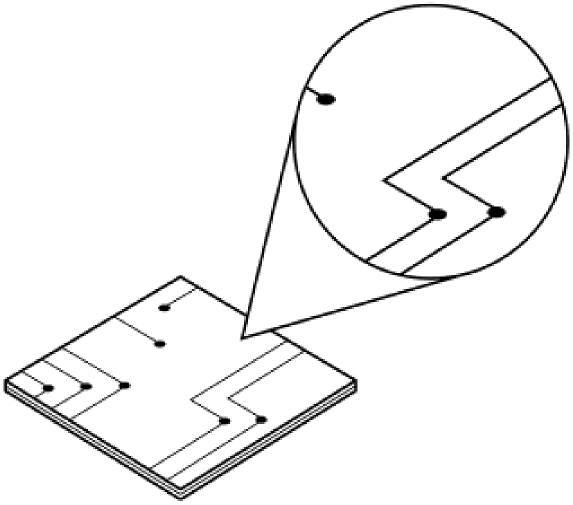
Firmware update

Firmware updated

Please re-install the apps on your device

You've successfully updated your Ledger Nano S Plus firmware. Ledger Live will automatically reinstall apps on your device. You may notice an increase in app storage capacity.

Exploring features



1- Downloading and installing Ledger Live

Ledger Live lets you manage your crypto assets with the security of your Ledger device. It supports the Ledger Nano S Plus via USB.

Prerequisites

- ☐ A Ledger Nano S Plus
- ☐ A computer (at least Windows 8.1, macOS 10.10, or Linux Ubuntu 16.10) with an internet connection.
- ☐ An internet connection and an available USB port. Use an **adapter** for USB-C ports.

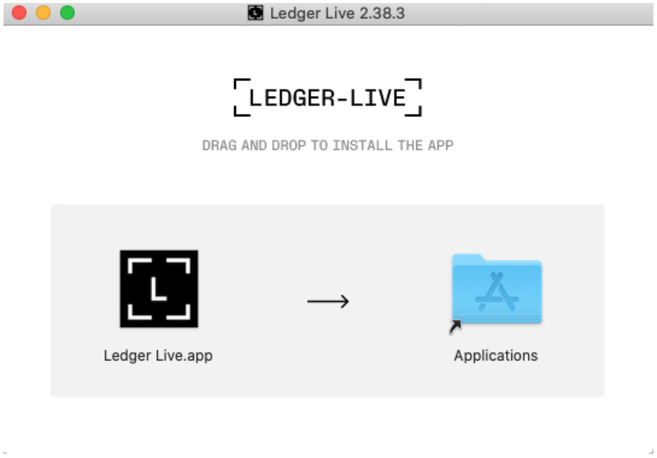
Instructions

Depending on your OS, follow the steps to install Ledger Live:

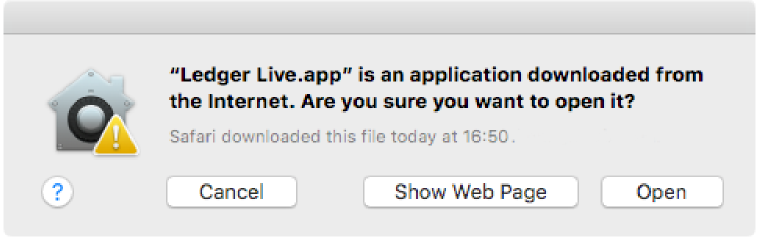
- Mac installation
- Windows installation
- Linux installation

1.1- Installing Ledger Live on Mac

1. Navigate to **ledger.com/ledger-live/download**.
2. Download the Ledger Live application.
3. Double-click the .dmg file you downloaded.
4. Drag and drop the Ledger Live application to the Applications folder.



5. Start Ledger Live from Launchpad or Spotlight.
6. Depending on your macOS version, the following message displays. Click **Open** to allow the installation.

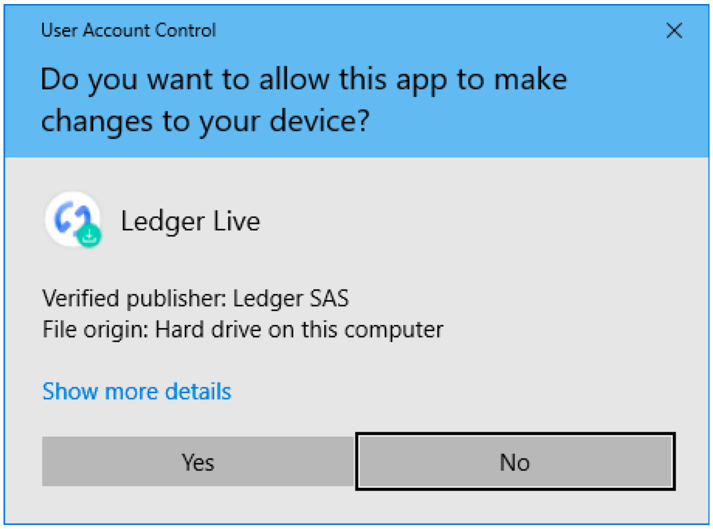


"Ledger Live.app" is an application downloaded from the Internet. Are you sure you want to open it?

Safari downloaded this file today at 16:50.

1.2- Installing Ledger Live on Windows

1. Navigate to ledger.com/ledger-live/download.
2. Download the Ledger Live application.
3. Double-click the Ledger Live executable file you downloaded.
4. If a warning displays, click **Yes** to allow the installation of Ledger Live.



User Account Control

Do you want to allow this app to make changes to your device?

Ledger Live

Verified publisher: Ledger SAS
File origin: Hard drive on this computer

5. Once the installation completes, click **Finish**.

1.3- Installing Ledger Live on Linux

You can install **Ledger Live** on Linux using the command line or the graphical user interface.

Using the command line

1. Navigate to **ledger.com/ledger-live/download**.
2. Download the Ledger Live AppImage.
3. Make the file executable in a terminal:
   ```
   chmod +x ledger-live-*.AppImage
   ```
4. Enter the following command to automatically add the udev rules and reload udev to allow USB access to your Ledger device:
   ```
   wget -q -O -
   https://raw.githubusercontent.com/LedgerHQ/udev-rules/master/ad
   d_udev_rules.sh | sudo bash
   ```
5. Launch the AppImage by double-clicking on it or via your terminal.
   If you get a sandboxing error, run the app with **--no-sandbox**:
   ```
   ./ledger-live-desktop-*.AppImage --no-sandbox
   ```

Using the graphical user interface

1. Navigate to **ledger.com/ledger-live/download**.
2. Download the Ledger Live AppImage.
3. Go to the **Downloads** folder.
4. Right-click on the Ledger Live AppImage you downloaded and click **Properties**.
5. Go to the **Permissions** tab.
6. In the **Execute** field, tick **Allow executing file as program**.

2- Getting started with Ledger Live

The first time you use the Ledger Live application, it will help you set up your Ledger device and configure the app. Ledger Live stores your accounts and settings on your computer or phone. You will have to set up your accounts again on any additional computer or phone.

Prerequisites

- ☐ Get your Ledger Nano S Plus
- ☐ Download and install Ledger Live

Instructions

2.1- Getting started

1. Start the Ledger Live application.
2. On the welcome screen, click on **Get started**.
3. Select **Connect your device**.
4. Choose your device, then click on **Continue**.

2.2- Security checklist

Complete the security checklist to verify that you benefit from the optimal level of security.

1. Click on **Check now**, to verify that your device is a genuine Ledger device. Only a genuine Ledger device can provide the cryptographic proof required to connect with Ledger's secure server.
   NOTE: This process might take a few moments.
2. Click on **Continue** once you see: **Your device is genuine**.

2.3- (optional) Choosing a password

Choose an optional password that unlocks the application to enhance your privacy. You should set a password if others have access to your computer.

1. Click on **Skip this step** if you do not want to set a password.
2. Enter your password in the **New password** field.
3. Enter your password again in the **Confirm password** field.
4. Click on **Continue**.

Make sure to remember your password. Losing it requires resetting Ledger Live and re-adding your accounts. This does not affect your crypto assets.

3- Installing and uninstalling apps

Use the Manager in Ledger Live to install or uninstall apps on your Ledger hardware wallet.

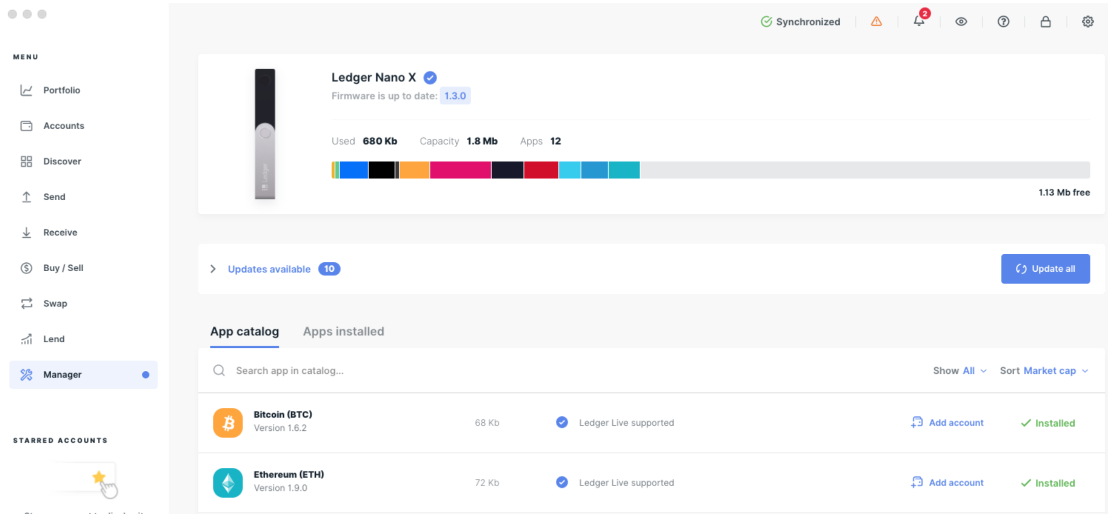
How apps work

- Your Ledger device securely stores your private keys giving access to your crypto assets.
- You need to install apps on your Ledger device to manage different crypto assets. Install the Bitcoin app to manage Bitcoin accounts.
- Ledger devices have limited storage and the sizes of apps vary. You can safely install and uninstall apps when needed. Your private keys stay safe on your device and backed up on your Recovery sheet.

Instructions

3.1- Installing an app

1. Click on the **Manager** in the left panel.
2. Connect and unlock your Ledger device.
3. Press both buttons to allow the **Manager** on your device.
   The Manager will show your device information as well as the **App catalog** and the **Installed apps** below it.



4. Search for the app to install in the **App catalog**.
5. Click the **Install** button of the app. Your device will display **Processing…**
   The app will be installed on your device.
6. You can install multiple apps at once by clicking their **Install** buttons. Wait for the installations to finish before you quit the **Manager.**

3.2- Uninstalling an app

You can uninstall the app from your Ledger device.

1. Connect and unlock your Ledger Nano S Plus by entering your PIN code.
2. Hold both buttons to access **Settings > General**.
3. Choose **Uninstall all apps** and press both buttons to validate.
4. Press the right button to confirm the uninstallation of all apps.
5. Press both buttons to **Confirm action**.

4- Adding your accounts

Add accounts in Ledger Live to manage the crypto assets secured by your Ledger hardware wallet. By adding your accounts, your public addresses are stored on your computer or smartphone so you don't need your Ledger device every time you want to check your balance.

Prerequisites

- □ Ledger Live is **ready to use**.
- □ Check which crypto assets are **supported in Ledger Live**. Others require an **external wallet**.
- □ Make sure the required crypto asset app is installed on your device.

Instructions

1. On the left panel, click on **Accounts**. If the **Accounts** button is greyed out, click on **Portfolio**.
2. Click the **Add account** button.
3. Type or click the drop-down list to choose the crypto asset of the account to add. Click **Continue**. If you cannot find a crypto asset, it is likely not supported in Ledger Live. Check **this article** to learn how to manage crypto assets that are not supported in Ledger Live.
4. Connect and unlock your device, open the app of the selected crypto asset. Click **Continue**. Ledger Live will look for existing accounts in the blockchain. These are then displayed one by one.
5. In the **Accounts** step, different sections can appear:
    a. In the **Select existing accounts** section, accounts are shown that already have blockchain transactions. Add a checkmark to the account(s) to add and choose a name for them.

    b. In the **Add new account section,** you can add a new account by adding a checkmark. This is not possible when the last created account of that crypto asset has not received a transaction yet.
    c. The **Accounts already in Portfolio** section lists the accounts that are already in Portfolio and thus can not be added.
6. Click **Continue**. Your account(s) will be added to the Portfolio.
7. Click **Add more** to continue adding accounts. Otherwise, close the **Add accounts** window.

5- Sending crypto assets

You can send crypto assets from your accounts in the Ledger Live application to a recipient address. Use your Ledger device to verify and approve the transaction.

Security tips

Always send a small amount first. Then verify that the transaction was properly received on the recipient address before proceeding to send larger amounts. If there's a doubt whether a transaction has gone through, simply check back a few minutes later.

Prerequisites

- ☐ You can only send crypto assets that are **supported in Ledger Live**.
- ☐ Check that the right app is installed on your device.
  Ex: install the Bitcoin app to send Bitcoin.

Instructions

5.1- Entering transaction details

1. Click the **Send** button on the left panel or at the top of an account page.
2. Type or use the drop-down list to select the **Account to debit**.
3. Enter the **Recipient address**. For optimal security, make sure always to **double-check addresses** that you copy and paste. Click on Continue.
4. Enter the **Amount** to send or its countervalue. You can also click on **Send Max** to empty the account.
5. Choose the **Network fees** from the drop-down list and click on **Continue**. A higher fee leads to faster processing of the transaction. **Learn more >**
6. Verify the transaction summary before clicking on **Continue**.

5.2- Verifying and signing

1. Connect and unlock your Ledger device.
2. Open the app as instructed and click on **Continue**.
3. Carefully verify all transaction details on your device by pressing the right or left button to view all transaction details.
4. Press both buttons to **Accept and send** the transaction if everything is correct. The transaction is then signed and sent to the network for confirmation. Choose **Reject** to cancel the transaction.
5. By clicking on **View details** you may **track the transaction** until it gets confirmed.

Disconnecting safely

You may safely disconnect your hardware wallet once you've verified an address or approved a transaction. Crypto assets are transferred on their blockchain network to the address generated by your device, nothing gets physically sent to your device.

6- Receiving crypto assets

You can receive crypto assets on accounts managed by your Ledger device by generating a receive address in the Ledger Live app. Assets not supported by Ledger Live can be managed through an **external wallet**.

Security tips

Always send a small amount first. Then verify that the transaction was properly received by the recipient address before proceeding to send larger amounts.

Prerequisites

- □ Ledger Live should be ready to use.
- □ The right app should be installed on your Ledger device.
  Ex: install the Bitcoin app to receive Bitcoin.
- □ **Add an account** if you're using Ledger Live.

Instructions

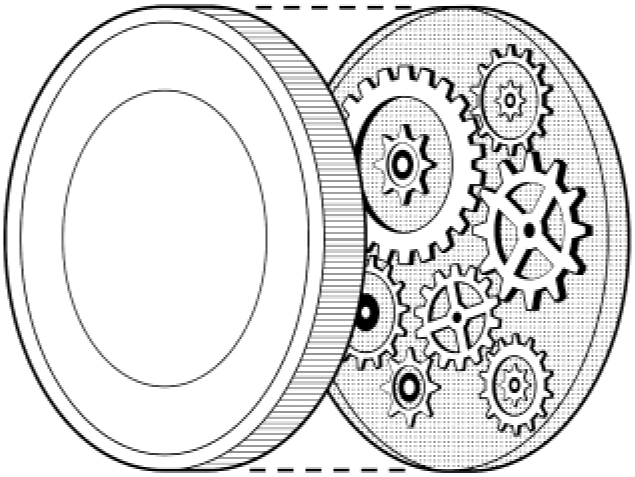
1. Click **Receive** in the menu on the left-hand side.
2. Type or use the drop-down list to choose the account to credit.
3. Click **Continue**.
4. Connect and unlock your Ledger device. Open the crypto asset app as instructed and click **Continue**.
5. Read the on-screen instructions and click on **Verify** to display an address on your device.
6. Verify that the address shown on your screen is the same as the address shown in Ledger Live.
   NOTE: For optimal security, you should copy and send the address to the sender of the transaction. Then verify with the sender of the transaction that the address received matches the one shown on your device.

7. Approve the address on your device if it is the same. The receive modal cannot be closed until the address is rejected or approved on the device.
8. Copy the address to share it with the sender of the transaction. Carefully check that the address does not change after you copy and paste it. It is recommended to click **Re-verify** after you've entered the address somewhere else to double-check it with your hardware wallet.

Disconnecting safely

You may safely disconnect your hardware wallet once you've verified an address or approved a transaction. Crypto assets are transferred on their blockchain network to the address generated by your device, nothing gets physically sent to your device.

Changing device settings



1- Accessing Control Center

Access the **Control Center** on your Ledger Nano S Plus device to lock and access device settings.

Instructions

1. Hold both buttons for 3 seconds at any time to open the **Control Center**.
2. Navigate the **Control Center** by pressing either the left or right button.
3. Validate a selection by pressing both buttons.
    - **Settings**: Press both buttons to enter the **Settings**.
    - **Lock device**: Press both buttons to show screen saver. The PIN code is required to unlock.
    - **Close**: Return to the previous activity.

2- Changing display brightness

You can adjust the brightness of your Ledger Nano S Plus device according to your preference.

Instructions

1. Connect and unlock your Ledger Nano S Plus by entering your PIN code.
2. Hold both buttons for 3 seconds to open the **Control Center**.
3. Navigate to **Settings** and press both buttons to enter.
4. Select the **General** menu option by pressing both buttons.
5. Navigate to **Brightness** and press both buttons to enter.
6. Choose either **Low**, **Medium**, or **High** and press both buttons to validate.

3- Configuring PIN lock

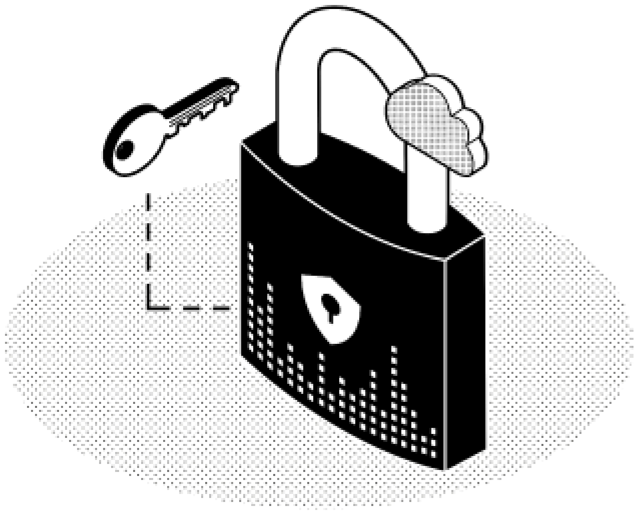
Configure PIN lock to lock your Ledger Nano S Plus device after a defined period of inactivity. The PIN code is then required to unlock it. By default, your device is locked after 10 minutes of inactivity. It is recommended to enable PIN lock for optimal security.

Instructions

1. Connect and unlock your device using your PIN code.
2. Hold both buttons for 3 seconds to open the **Control Center**.
3. Go to **Settings > Security** and press both buttons to validate.
4. Press both buttons to enter the **PIN lock** menu.
5. Select one of the following options:
    - **No PIN lock**
    - **1 minute**
    - **2 minutes**
    - **5 minutes**
    - **10 minutes**
6. Press both buttons to activate the corresponding PIN lock option.

If you've enabled PIN lock, your device will show the Ledger logo screen saver. To unlock the device, press both buttons and enter your PIN code.

Protecting your device



1- Securing your recovery phrase and PIN code

Ledger products have a combination of hardware and software security features to protect your crypto assets from potential attacks. Follow the guidelines below to benefit from the optimal level of security offered by your Ledger Nano S device.

Securing your 24-word recovery phrase

Your 24-word recovery phrase is the only backup of your private keys. It allows you to **restore** the private keys providing access to your crypto assets in case you lose access to your Ledger device. The recovery phrase is sometimes called (mnemonic) seed.

Anyone who gets your recovery phrase can take your crypto assets. Ledger does not store your private keys, nor ever asks for it.

Always ensure your 24-word recovery phrase is obtained from the device screen.

- ✓ Always double-check the spelling and list position of each recovery phrase word.
- ✓ Keep your Recovery sheet physically secure to make sure you can’t lose or destroy it by accident.
- ✓ Always store the copies of the recovery phrase in secure locations, out of sight.

- × Never ever share your 24-word recovery phrase, in any form, with anyone.
- × Never enter your recovery phrase on any device other than your hardware wallet.
- × Never take a picture of the 24-word recovery phrase.

Securing your PIN code

During the setup process you choose a PIN code.

- ✓ Always choose a PIN code by yourself.

✓ Always enter your PIN code out of sight.

✓ Change your PIN code if needed. **Learn more**

✓ Remember that three wrong PIN code entries in a row will reset the device.

× Never use an easy PIN code like 0000, 123456, or 55555555.

× Never share your PIN code with anyone else.

× Never use a PIN code you did not choose yourself.

× Never store your PIN code on a computer or phone.

2- Changing your PIN code

The PIN code of your Ledger Nano S Plus device prevents unauthorized access to your crypto assets. Your PIN code is chosen when you first set up the device, but you can change it at any time.

Instructions

1. Connect and unlock your Ledger Nano S Plus by entering your PIN code.
2. Hold both buttons for 3 seconds to open the **Control Center**.
3. Navigate to **Settings** > **Security** > **Change PIN**.
4. Choose a new PIN code of 4 to 8 digits.
5. Confirm the new PIN code by entering it again.
6. Enter your old PIN code to validate.
7. Your new PIN code is now set.

Security tips

- ✓ Choose your own PIN code. This code unlocks your device.
- ✓ An 8-digit PIN code offers an optimum level of security.
- ✓ Choose a PIN code that's hard to guess.

3- Resetting to factory settings

Resetting the device to factory settings removes all private keys, applications, and settings from your Ledger Nano S device. You can reset to set it up as a new device, restore another recovery phrase, or safely transfer the device to someone else.

Instructions

The device can either be reset from its settings menu or by entering three incorrect PIN codes when unlocking it.

Got your Recovery phrase?

If you reset your device without having your Recovery sheet, the private keys providing access to your crypto assets will be erased. You will permanently lose access to your crypto assets.

3.1 - Resetting from device settings

1. Connect and unlock your Ledger Nano S Plus by entering your PIN code.
2. Hold both buttons for 3 seconds to open the **Control Center**.
3. Go to the **Settings** and press both buttons to validate.
4. Choose **Security** and press both buttons to validate.
5. Choose **Reset device** by pressing both buttons.
6. Read the warning by pressing the right button to continue.
7. Press both buttons to **Reset device**.
8. Enter your PIN code to confirm. Your device will then be reset.

3.2 - Resetting from PIN code

1. Connect the USB cable to your Ledger Nano S Plus to turn it on.
2. Enter an incorrect PIN code three times in a row.
3. The device will reset after the third incorrect attempt as a security measure.

4- Setting up a passphrase

Set up a passphrase to add a layer of security to your crypto assets. This option is only recommended for advanced users. Carefully read this article before setting up a passphrase.

> **Security tips**
>
> The recovery phrase and passphrase functionalities enable a range of security setups. You may use them to design the security strategy that meets your personal situation. Please do not overcomplicate things, the best security setup is one that you master and can execute with confidence.

How the passphrase works

The 24-word recovery phrase saved during the initial setup of your Ledger hardware wallet fully backs up the private keys providing access to your accounts. You must store it in a secure place.

- The passphrase is essentially a password added to your 24-word recovery phrase that provides access to a whole new set of accounts.
- The passphrase protects your crypto assets if your 24-word recovery phrase were to be compromised. To access passphrase-protected accounts, an attacker will need your recovery phrase as well as your secret passphrase.
- Each different passphrase unlocks a unique set of accounts. You can use as many passphrases as you like.
- The passphrase can be applied to every coin managed by the Ledger device.

Prerequisites

☐ Your device is set up and runs the latest firmware.
☐ Ensure your recovery phrase is accessible, just in case.
☐ Read this article fully before you start.

Instructions

3.1 - Setting up a passphrase

1. Connect your Ledger Nano S Plus and enter your PIN code.
2. Navigate to **Settings** > **Security** > **Passphrase**.
3. Click past the warning and choose **Set up passphrase**.
4. Choose either of two options:
   - **Attach to PIN**: Creates a second PIN code to unlock passphrase-protected accounts.
     Note: you can only have one secondary PIN code.
   - **Set temporary**: Enter the passphrase each time you wish to access passphrase-protected accounts.

3.1.1 - Attaching to PIN code

Attaching a passphrase to a new PIN code creates a new set of accounts on your Ledger Nano S Plus based on a secret passphrase of your choice. You can access the accounts protected by this passphrase by entering a secondary PIN code.

- Only one passphrase can be attached to a PIN code. If you add another passphrase to the PIN code, you will overwrite the secondary PIN code and the passphrase.
- The passphrase will be stored on the device until you overwrite it with another passphrase or until the device is reset.
- Store a physical backup of the secret passphrase in a secure place. The device cannot display it after you've set it.

Instructions

1. Choose **Attach to a PIN** option from the **Passphrase** menu in the device security settings.
2. Choose the PIN code that will activate the passphrase.
3. Re-enter the secondary PIN code to confirm it.

4. Choose and confirm a secret passphrase (max 100 characters).
5. Enter your current PIN code to validate. Your device will display **Processing** and confirm that the passphrase is set.
6. Your device will continue managing the accounts based on your recovery phrase without passphrase. Please turn off the device and enter your secondary PIN code to access the passphrase-protected accounts.

3.1.2 - Setting a temporary passphrase

Using a temporary passphrase provides access to a new set of accounts on your Ledger Nano S Plus **for the duration of the session**. Follow the instructions below each time you wish to access the accounts protected by the passphrase.

- The accounts are based on a secret passphrase of your choice.
- Store a physical backup of the secret passphrase in a secure place. The device cannot display it after the initial setup.

Instructions

1. Choose **Set temporary** option from the **Passphrase** menu in the device security settings.
2. Choose and confirm a secret passphrase (max 100 characters).
3. Enter your current PIN code to validate. Your device will display **Processing** and confirm that the passphrase is set.
4. Your device will now manage the accounts protected by this passphrase. To access your regular accounts, please restart the device and enter your PIN code as usual.

3.2 - Recovering passphrase accounts

In case of loss or a reset of your Ledger Nano S, you can recover access to your crypto assets on any Ledger device as long as you have both your 24-word recovery phrase and secret passphrase.

Instructions

1. Take out your recovery phrase and passphrase.
2. Restore the Ledger device from your recovery phrase.
3. Follow the instructions above for a **temporary passphrase** or **attach to PIN** while taking into account:
    - **Temporary passphrase**: Simply enter the passphrase you've set up earlier to access the accounts protected by that passphrase.
    - **Attach to PIN code**: You can choose any PIN code, but you need to **enter the passphrase you've set up earlier** to access the accounts protected by that passphrase.

3.3 - Passphrase security in practice

3.3.1 - Adding accounts to Ledger Live

When you add an account, its extended public key (xpub) is stored in Ledger Live's user data folder, where it is encrypted by your password if you've set up password lock.

To be sure that Ledger Live does not store information about passphrase-protected accounts, you may simply remove these accounts after you're done managing them in Ledger Live.

3.3.2 - Plausible deniability

To protect yourself in case of physical threat, make sure your primary PIN code unlocks only a minor part of your crypto assets. Then set up a passphrase attached to a PIN code and store a more significant amount of crypto assets on the passphrase-protected accounts.

If you are under duress to unlock your Ledger Nano S, you can surrender your main PIN code to the attacker while hiding the PIN code that unlocks your passphrase-protected accounts.

3.3.3 - Recovery phrase protection

It’s a good security practice to keep multiple copies of your Recovery sheet and to store them in different geographic locations. To mitigate the risk of losing your crypto assets if one of the copies of your recovery phrase is compromised, you can set up a passphrase. If you do so, make sure to store paper/metal backups of your passphrase, preferably in geographic locations that are different from the locations where you keep a backup of your recovery phrase.