User Manual
Ledger Nano S

Version control **4**

Check if device is genuine **6**
- Buy from an official Ledger reseller 6
- Check the box contents 6
- Check the Recovery sheet came blank 7
- Check the device is not preconfigured 8
- Check authenticity with Ledger applications 9
- Summary 9
- Learn more 9

Initialize your device **10**
- Before you start 10
- Start initialization 10
- Choose a PIN code 10
- Save your recovery phrase 11
- Next steps 11

Update the Ledger Nano S firmware **12**
- Before you start 12
- Step by step instructions 12

Restore a configuration **18**
- Before you start 19
- Start restoration 19
- Choose a PIN code 19
- Enter recovery phrase 20
- If your recovery phrase is not valid 20
- Next steps 21

Optimize your account security **21**
- Secure your PIN code 21
- Secure your 24-word recovery phrase 21
- Learn more 22

Discover our security layers **22**

Send and receive crypto assets **24**

List of supported applications **26**
- Applications on your Nano S 26
- Ledger Applications on your computer 27
- Third-Party applications on your computer 27

If a transaction has two outputs **29**

Receive mining proceeds **29**
- Receiving a large amount of small transactions is troublesome 29

In case you received a large amount of small payments 30
Prevent problems by batching small transactions 30
Set up and use Electrum 30
Set up your device with EtherDelta 34
Connect with Radar Relay 36
Check the firmware version 37
A new Ledger Nano S 37
A Ledger Nano S in use 38
Update the firmware 38
Change the PIN code 39
Hide accounts with a passphrase 40
Advanced Passphrase options 42
How to best use the passphrase feature 43
Temporary Passphrase 43
Export your accounts 44
Before you begin 44
Use your recovery phrase 45
Compatible Ledger devices 45
Arbitrary list of thirdartp-party software wallets 45
Generate private keys (advanced) 45
Generate your private keys 45
Import your private keys 45
Check hardware integrity 46
Firmware Update - FAQ 51
Unable to install OS Updater 54
Connection issues with Windows or Linux 55
Lost device, PIN code or recovery phrase 56
Browser support 56
Ledger Nano S 57
Step by step instructions 57
Troubleshoot hardware issues 57

Version control

Version	Date	Comments
1.0	19-07-2018	First issue for publication.

Getting Started

Check if device 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:

- the origin of your Ledger product;
- the content of the box of the Ledger device;
- the condition of the Recovery sheet;
- the initial state of the Ledger device.

Note: advanced users that want to check the device hardware integrity: please refer to the last section of this article.

Buy from an official Ledger reseller

Purchase your device directly from Ledger or through the authorized distributor / reseller network to make sure you receive an authentic Ledger product. Our official sales channels include:

- our official e-commerce website www.ledgerwallet.com
- our official Amazon stores:
  - USA
  - Canada
  - United Kingdom
  - Germany
  - France
  - Spain
  - Italy
  - Japan

Note: Ledger devices purchased from other vendors are not necessarily dubious. However, we do strongly recommend that you meticulously perform the safety checks below to ensure that your Ledger is genuine.

Check the box contents

The package of a Ledger hardware wallet should include:

- A Ledger device (Ledger Nano S, a Ledger Blue, etc.)
- 3 paper cards, including:
- - a *Getting started* card;
- - a *Did you notice* card;
- - A blank *Recovery sheet*, of which there may be 3 copies;
- Additional accessories, such as a keychain and a lanyard;

- Additional packaging (unmarked foam / cardboard).

Note: The paper cards and their envelope do not necessarily carry the Ledger logo.

Box contents of the Ledger Nano S

Check the Recovery sheet came blank

- Make sure your *Recovery sheet* came in blank
- Ledger never provides a 24-word recovery phrase in any way, shape or form. Only accept a recovery phrase obtained from the screen of the Ledger device.
- If your *Recovery sheet* already has words on it: the device may be preconfigured. It is not safe for you to use the device. Please contact Ledger Support for assistance.

a blank Recovery sheet

Check the device is not preconfigured

- Make sure your Ledger device was not preconfigured with a PIN code that you did not choose yourself. The device should display *Welcome* and *Press both buttons to begin* 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: *Welcome*

Ledger Nano S: Press both buttons to begin

Check authenticity with Ledger applications

- Connect your Ledger device to any of Ledger's applications to verify its authenticity.
- 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.

Summary

- Check your *Recovery sheet* came in blank;
- Initialize your Ledger device yourself at first use. The *Welcome* screen should be displayed when connecting your device for the first time;
- Choose your own PIN code;
- Contact Ledger Support in case of doubt.

Learn more

Anti tamper seals

Ledger deliberately chooses not to use anti tamper seals on its packaging. These seals are easy to counterfeit and can therefore be misleading. Rather, genuine Ledger devices contain a secure chip that prevents physical tampering: this provides stronger security than any sticker possibly could.

Hardware integrity check

Advanced users can check the hardware integrity on the inside of their Ledger device. This article provides a non-exhaustive chronology of the different revisions of the Ledger Nano S build. Please be aware that normal usage does not involve opening your Ledger device. Proceed to do so at your own risk. Ledger can not be held liable for any possible damage resulting from opening the device.

Initialize your device

Initialize your Ledger Nano S device to get started. The Ledger Nano S will generate new private keys to securely manage your crypto assets.
Note: Restore a configuration to recover the private keys associated with an existing recovery phrase.

Before you start

- Make sure your device has the latest firmware installed.
- Verify your computer has:
- - Windows 7+, macOS 10.8+ or Linux;
- - a USB port. Use an adapter for USB-C ports;
- - an internet connection and Google Chrome / Chromium installed.
-

Start initialization

1. Connect the Ledger Nano S to your computer using the supplied USB cable.
2. Read the instructions on the screen. Press both buttons simultaneously to proceed.
3. Press the right button located above the validation icon when *Configure as new device?* is displayed.

Choose a PIN code

- Firmware version 1.3 or higher requires a PIN code between 4 and 8 digits long.
-
- Firmware version 1.2 or lower requires a 4-digit PIN code.
-

To set your PIN

1. Press both buttons when *Choose a PIN* is displayed on the device.
2. Press the right or left button to choose the first digit of your PIN code.
3. Press both buttons to select the digit.
4. Repeat the process until all digits of your PIN code are selected.
5. Select the check icon (✓) and press both buttons to confirm the pincode.

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

Save your recovery phrase

Your 24-word recovery phrase will now be displayed word by word on the Ledger Nano S screen. Be careful, your recovery phrase will be displayed only once.

1. Take the blank *Recovery sheet* supplied in the box.
2. Write down the first word (*Word #1*) on the *Recovery sheet*. Verify that you have copied it correctly in position 1.
3. Press the right button to move to the second word (*Word #2*). Write it in position 2 on the Recovery sheet. Verify that you've copied it correctly.
4. Repeat the process until the twenty-fourth word (*Word #24*). *Confirm your recovery phrase* will be shown on the screen after word 24.
5. 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.
6. *Your device is now ready* is shown once you've successfully completed the initialization.

> - Make sure you are the sole holder of the 24-word recovery phrase.
> - Ledger does not keep any backup of your 24 words.
> - Never use a device supplied with a recovery phrase and/or a PIN code.
> - Please contact Ledger Support in case of doubt.

Next steps

You've successfully initialized your device. Proceed to:

- Optimize your account security.
- Use the Ledger Manager to install apps on your device.

Update the Ledger Nano S firmware

The update to firmware version 1.4.2 introduces minor security as well as user experience improvements. Please check our blog post for full details on the changes included in this update.
Check our update FAQ for troubleshooting tips in case you encounter any issue.

Before you start

- Make sure you have downloaded and installed the Ledger Manager.
- Ensure your 24-word recovery phrase is accessible if your device is already initialized.

Step by step instructions

Step 1 - Check the current firmware

1. Check the current firmware version.
2. Select your case
3. - If the firmware version is 1.4.2, your device already has the latest firmware.
4. - If the firmware version is 1.4.1 or lower, continue to Step 2.

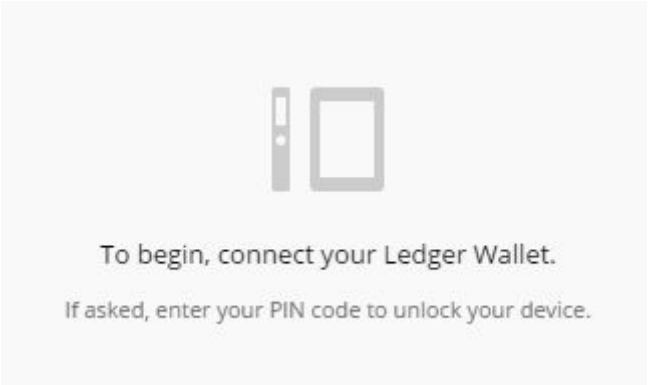
Step 2 - Connect to Ledger Manager

For a Ledger Nano S in use

1. Launch the Ledger Manager on your computer.
2. Connect the Ledger Nano S to the computer using the USB cable.
3. Enter your PIN code to unlock the Ledger Nano S.

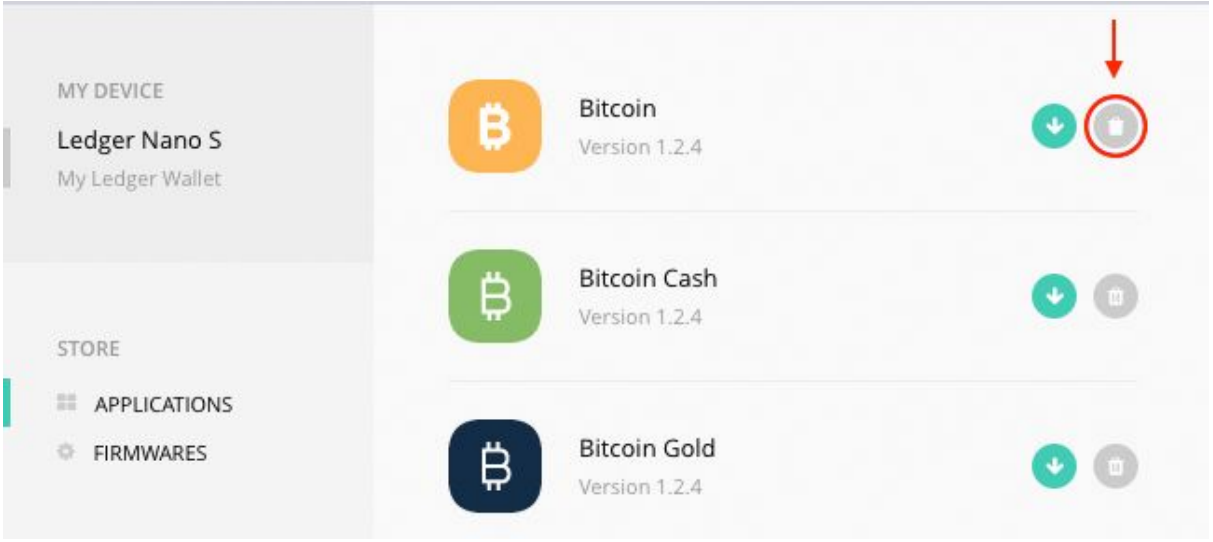
For a new Ledger Nano S

1. Press and hold the right button. The right button is the one far away from the USB connector, closest to the swivel hole.
2. Connect the USB cable from your computer to your Ledger Nano S while holding the right button until *Recovery* is displayed.



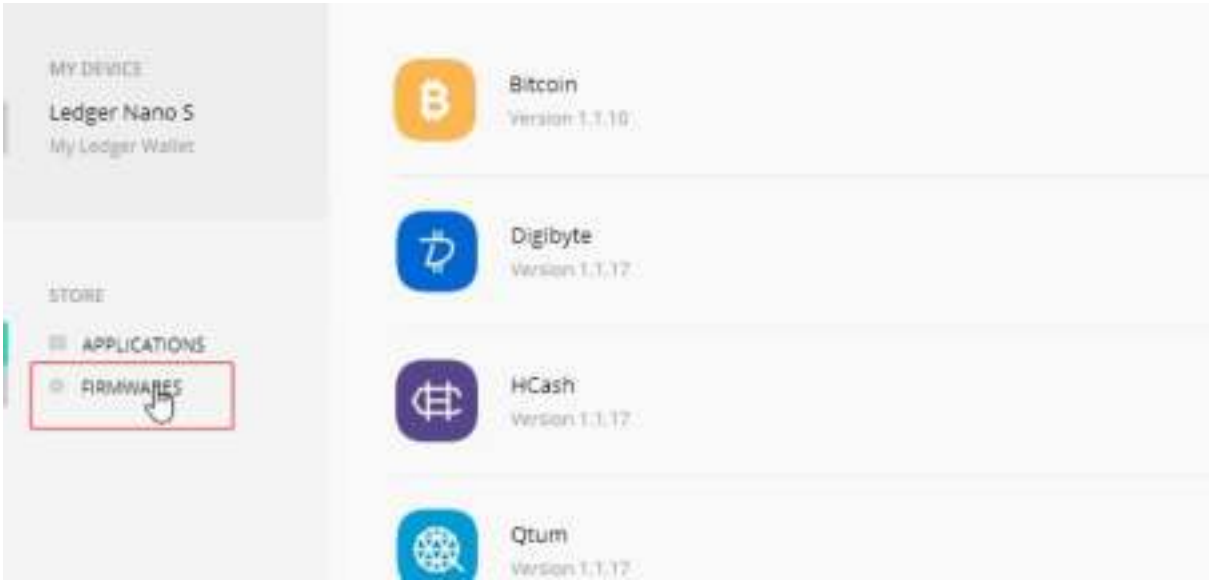
Step 3 - Uninstall applications

1. Click on the *APPLICATIONS* tab of the Ledger Manager.
2. Click on the grey trash icon for all applications that are currently on the Ledger Nano S. This makes room for the firmware installer.

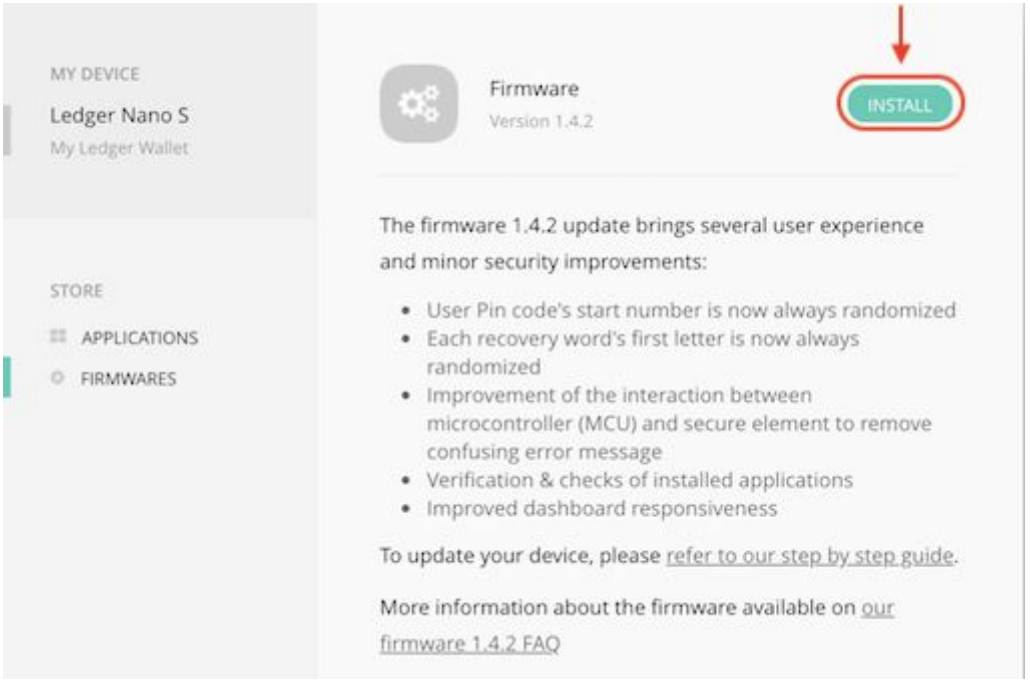


Step 4 - Download and start the update

- Navigate to *FIRMWARES* on the sidebar of the Ledger Manager.

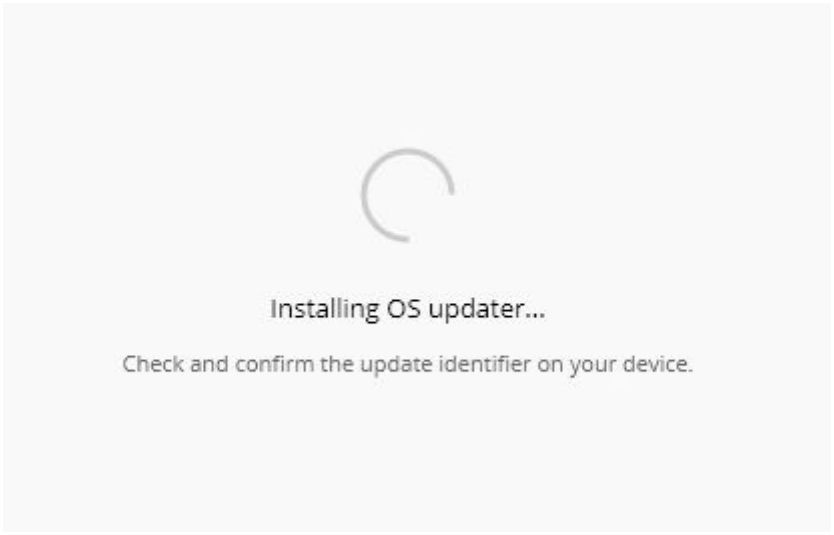


- Click on the green *INSTALL* button.



- Confirm *Allow Ledger manager?* on the Ledger Nano S by pressing the right button. The right button is the one far away from the USB connector, closest to the swivel hole.

- The Ledger Manager will now display the installation screen while the updater is installed on the device.



Note: try updating at a later moment in case the update fails at this stage.

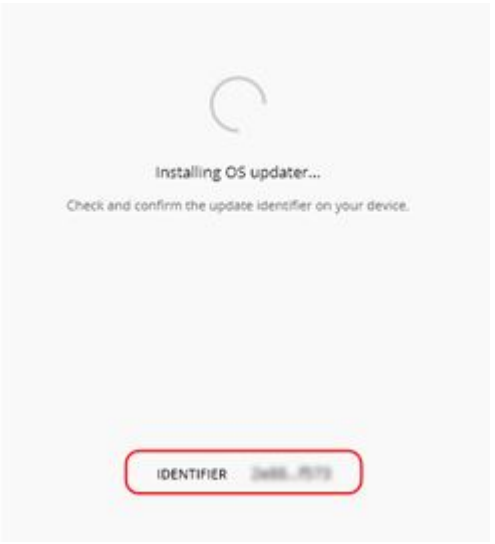
Step 5 - Proceed with firmware update

The Ledger Nano S will now show three screens after each other in a slider. Before pressing the right button to confirm, make sure that:

1. You see the *Update firmware* screen.
2. The firmware *Version* is 1.4.2.
3. You have checked that the identifiers shown on both the Ledger Nano S and the Ledger Manager are the same.

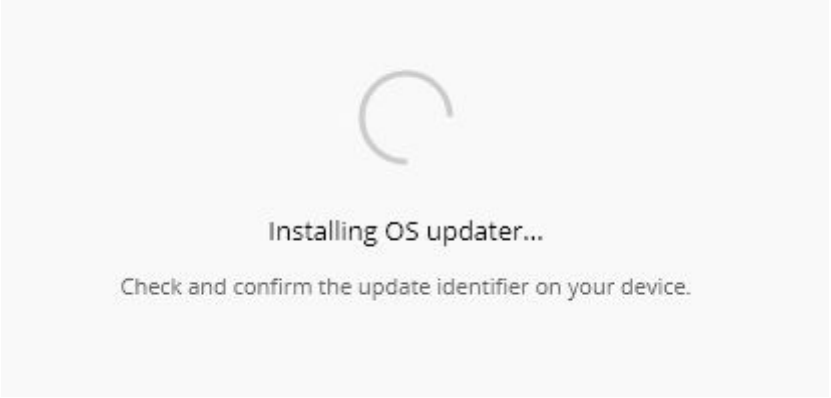
The first screen of the slider: Update firmware.

The second screen of the slider: Version 1.4.2.



The third screen of the slider displays the identifier. Verify that it matches the identifier shown on the Ledger Manager.

- After verification of the three screens, proceed with the update by pressing the right button.
- Enter your PIN code to continue.
- The OS updater will now be installed.



- The device will reboot after installing the firmware.
- At this stage, two cases are possible, depending on the firmware version that was identified in Step 1:

- If the firmware version identified in Step 1 was 1.4.1, the update is now complete. In this case the Ledger Nano S will boot as normal. Please skip Step 6 and directly go to Step 7.
- If the firmware version identified in Step 1 was 1.3.1 or lower, the Ledger Nano S will display *MCU firmware is outdated* (left side of the image below) and *To begin, connect your Ledger Wallet* on the Ledger Manager (right side of the image below). In this case, go to Step 6.

Step 6 - Reboot the Ledger Nano S

- Unplug and replug your Ledger Nano S to your computer while holding the left button. The left button is the one near the USB connector.
- *Bootloader* is displayed on the Ledger Nano S while *Restoring MCU* is shown on the Ledger Manager.

- During the MCU update, *Update* then *Processing* will be displayed on the Ledger Nano S and *Installing firmware* on the Ledger Manager. This procedure can take a few minutes.

Please check our FAQ in case of an issue at this stage.

Select your case
- If you have updated a new device, go to .
- If the firmware version identified in Step 1 was 1.3.1 or higher, go directly to Step 7.
- If the firmware version identified in Step 1 was 1.2 or lower, the 24 word seed now has to be re-entered to restore the wallet. Make sure the left button is pressed when asked: *Configure as new device?* Refer to this article for assistance during the recovery process.

Step 7 - Verify the firmware and MCU versions of the Nano S

- Enter your PIN to unlock the Ledger Nano S.
- *Note: if your PIN code includes less than 8 digits, please type in your PIN code as usual, and use the right / left button until you reach a check mark (✓). Then, confirm your PIN code by pressing both buttons.*
- Navigate to the settings app on the Ledger Nano S: *Settings* > *Device* > *Firmware.*

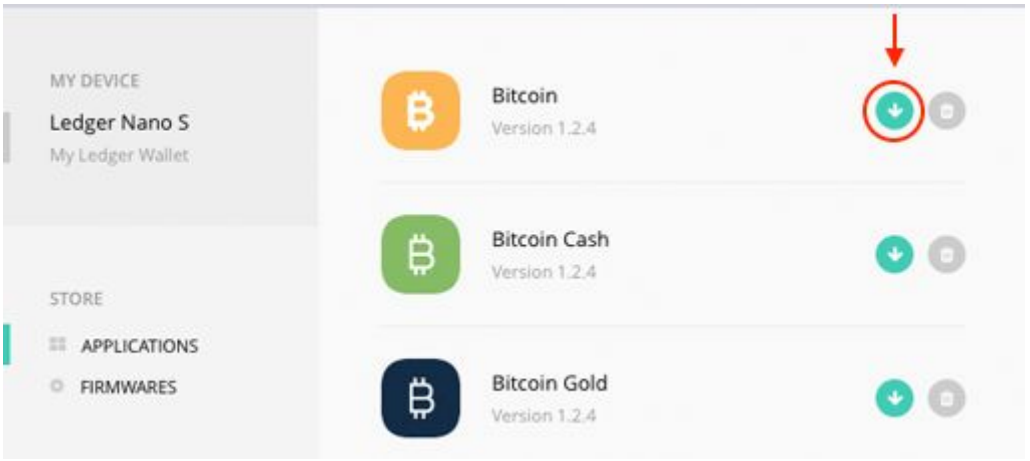
- Check the *Secure Element* version is 1.4.2.

- Click on the right button. Check the *MCU* version is 1.5.

You've successfully updated the firmware of your Ledger Nano S.

Step 8 - Reinstall applications

- The Ledger Nano S is now updated. You can install applications and use the device.
- Go to to the *APPLICATIONS* tab on the Ledger Manager. For each application you wish to install, click on the green download icon. If the application installation fails, please try to disconnect the Ledger Nano S and reconnect it.
- Please install the Bitcoin app first: all other apps require the Bitcoin app installed to operate properly.



Restore a configuration

Restore a configuration on a Ledger Nano S device to restore, replace or clone a device. The Ledger Nano S will recover the private keys associated with an existing recovery phrase.
Note: Initialize your device to generate new private keys and save the associated recovery phrase.

Before you start

- Get the recovery phrase to restore. *BIP39/BIP44 recovery phrases are supported.*
- Update to the latest firmware version.
- Verify your computer has:
- - at least Windows 7, macOS 10.8 or Linux.
- - a USB port. Use an adapter for USB-C ports.
- - an internet connection and Google Chrome / Chromium installed.

Start restoration

1. Connect the Ledger Nano S to your computer using the micro USB/USB cable.
2. Press both buttons simultaneously as instructed on the device.
3. Press the left button located above the cancel icon when asked *Configure as new device?*
4. Press the right button located above the validation icon to select *Restore a configuration?*

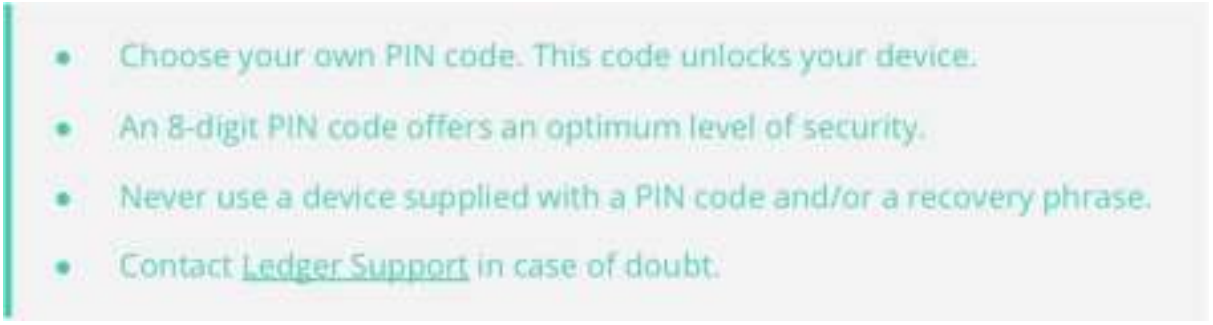
Choose a PIN code

The length of the required PIN code varies:

- Firmware version 1.3 or higher requires a PIN code between 4 and 8 digits long;
- Firmware version 1.2 or lower requires a 4-digit PIN code.

To set your PIN code:

1. Press both buttons when *Choose a PIN code* is shown on the device.
2. Press the right or left button to choose the first digit of your PIN code.
3. Press both buttons to select the digit.
4. Repeat the process until all digits of your PIN code are selected.
5. Select the check icon (✓) and press both buttons to enter the PIN code.
6. Enter the PIN code again to confirm.
7.



Enter recovery phrase

1. Press the right button to choose the length of your recovery phrase (12, 18 or 24 words). Press both buttons to enter.
2. Choose the first letter of Word #1 by pressing the right or left button. Press both buttons to select the letter.
3. Select the second letter of Word #1. Repeat until the device shows suggested words to choose from.
4. Choose Word #1 from the suggested words. Press both buttons to select it.
5. Repeat the process for each word of your recovery phrase.
6. *Your device is now ready* is displayed if you've successfully entered your recovery phrase.

- Make sure you are the sole holder of the 24-word recovery phrase.
- Ledger does not keep any backup of your 24 words.
- Never use a device supplied with a recovery phrase and/or a PIN code.
- Please contact Ledger Support in case of doubt.

If your recovery phrase is not valid

1. Make sure the correct recovery phrase length is selected. Always enter all words of a recovery phrase.
2. Verify that the order of the words entered on the device matches the order written on your *Recovery sheet*.
3. Check that all the words of your recovery phrase are on the BIP39 word list.
4.

Next steps

You've successfully restored a configuration on your device. You may proceed to:

- Optimize your account security.
- Use the Ledger Manager to install apps on your device.
- Send or receive crypto assets.

Optimize your account security

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.

Secure your PIN code

During the initialization process you choose a PIN.
ALWAYS

- Choose a PIN code by yourself.
- Enter your PIN code out of sight.
- Change your PIN code if needed.

- 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.
- Share your PIN code with anyone else.
- Use a PIN code you did not choose yourself.
- Store your PIN code on a computer or phone.

Secure your 24-word recovery phrase

The 24-word recovery phrase is the only backup to your crypto assets.

ALWAYS

- Ensure your 24-word recovery phrase is obtained from the device screen.
- Create multiple written copies of the recovery phrase.
- Store the copies of the recovery phrase in secure locations, out of sight.

NEVER

- Enter the 24-word recovery phrase into your computer or phone.
- Take a picture of the 24-word recovery phrase.
- Share your recovery phrase with anyone else.

Learn more

- Maximize your account security with a passphrase (advanced users).
- Contact Ledger Support when in doubt.

Discover our security layers

1. Ledger does not know your private keys

Ledger utilizes a decentralized wallet system. You generate the private keys on your Ledger device during the initialization process, and they are then stored within the Secure chip of your Ledger device. Ledger never has the opportunity to make a copy of your private keys.

2. No one can access your secrets

Your private keys are held in a Secure chip, and they never leave it. Whenever a transaction is signed within the Secure chip, the private keys never become visible to the computer the Ledger device is connected to. A compromised computer will never be able to access the contents of the Secure chip.

3. Personal PIN code

Every time you connect the Ledger device to the your computer's USB port, you need to enter a PIN code. If you fail to enter the proper PIN code three times, and the Ledger Device will reset, erasing all of its entire contents. A malware cannot reset the wallet by sending

three wrong PIN codes because before trying a new PIN code it is necessary to physically unplug and replug the wallet into the USB port.

4. Two verifications
Every time you want to authenticate a transaction, a second verification is made. With a Ledger Nano or a Ledger HW.1, you need to enter a code stored on a separate offline card, providing an additional off-line security mechanism for the Ledger device. With the Ledger Nano S and Ledger Blue, manual consent is required on your device's screen to sign the transaction. There is no known attack vector that could result in the exposure of your private keys or cryptocurrencies. Even if your computer was completely compromised and was able to replace the receiving address of a transaction on its own, the second factor verification would prevent that from happening.

5. Backup
During the initialization process of the Ledger Wallet, a passphrase is generated and given to you (a sequence of 24 random words). This passphrase allows you to retrieve your cryptocurrencies should your Ledger device be stolen, lost, or damaged.

6. Entropy (randomness) generator
The Nano S and Blue use a ST RNG chip to generate the entropy used to create the seed. The ST RNG has been evaluated by a 3rd party laboratory and obtained highest level certifications EAL5+, AIS-31. This methodology includes a mathematical proof of randomness and very large number of tests. The RNG is tested under various conditions of temperatures, frequency, voltage and must pass all the statistical tests. It also includes randomness defects and attacks detection mechanisms. AIS31 certified RNG are the best RNG in the world in terms of entropy, and ensure a proper seed generation using the highest possible level of randomness.

What if Ledger goes out of business?
If Ledger shuts down all its activities, the Ledger Chrome app will most probably stop to function as our API servers would be stopped.
However, this would only be an inconvenience, as your bitcoins would stay completely safe so long as you have your 24 words recovery phrase.
With your recovery sheet, and your 24 words, you can anytime restore your balance to another BIP39 compatible wallet, following this guide.

Send & Receive

Send and receive crypto assets

In order to be able to send and receive cryptocurrencies using your Ledger Nano S, you must first initialize your device. Once initialized you will need to download the Ledger Manager application, along with the Ledger Bitcoin Wallet, Ledger Ethereum Wallet, or Ledger Ripple Wallet (more information about cryptocurrencies and wallets compatibility on this link) using the instructions below:

1. the Ledger Manager: go to this page in your Chrome browser, and click on "Available on Chrome" to download and install it.
2. the Ledger Bitcoin Chrome app: go to this page in your Chrome browser, and click on "Available on Chrome" to download and install it.
3. the Ledger Ethereum Chrome app: go to this page in your Chrome browser, and click on "Available on Chrome" to download and install it.
4. the Ledger Ripple app: go to this page in your Chrome browser, and click on "Available on Chrome" to download and install it.

Once the Ledger Bitcoin Wallet (or Ledger Ethereum Wallet or Ledger Ripple Wallet) Chrome application is installed on your computer:

1. Connect your Ledger Nano S to a USB port on your computer and enter your PIN code
2. Launch your Ledger Bitcoin, (Ethereum, or Ripple) Wallet Chrome application
3. Open the cryptocurrency app of your choice on your Ledger Nano S (downloaded from your Ledger Manager application onto your Ledger Nano S)

Then you can see your account and manage your coins. If you want to manage other coins or applications with your Nano S, you can manage your applications through the Ledger manager. See here how to use it.

How to transfer Bitcoins to your Ledger Wallet
When you want to receive coins, you just have to provide your address to the payer. Your Ledger Nano S does not need to be connected as the transaction is made on the blockchain, not on the device itself. Next time you connect your wallet, it will synchronize to the blockchain to display all of your past operations and your balance.

To receive cryptocurrencies on your Ledger Wallet you will need to locate your Bitcoin (or Ether, Ripple, etc.) address. To find your Bitcoin address follow the instructions listed below:

1. Connect your Ledger device
2. Enter your PIN code
3. Open the Bitcoin application on your device
4. Launch your Bitcoin Chrome application on your computer
5. Click on "Receive", a popup window opens
6. Copy the "Bitcoin address" which is displayed

7. Paste this address into the send/receiving address of the Bitcoin wallet that currently holds your coins
8. Verify that you have the correct address as sending cryptocurrencies to the wrong address could result in the loss of the coins

Your Ledger Bitcoin wallet generates a new address each time you want to receive a payment, thanks to the Hierarchical Deterministic (HD) support. Each address generated by your wallet is yours forever, you can use them several times or just once at your convenience, it won't cause problems although it may be safer to use each address only once.

Check out this article to learn more about Ledger and the blockchain ecosystem.

How to send a Bitcoin payment from my Nano S to a different wallet

1. Connect your Ledger Nano S
2. Enter your PIN code
3. Open the Bitcoin app on your Nano S (right click)
4. Launch your Ledger Bitcoin (Ethereum, Ripple) Wallet Chrome application on your computer
5. Click on "Send", and a popup window will open
6. Fill in the required fields: amount, recipient address (you can paste or scan), level of fees
7. Click on the "Send" button
8. Your Nano S requires your manual consent to authenticate this transaction: press the right button (above the "V" check icon) to confirm and initiate your transaction once you have verified the details of your transaction are right and wait until your Chrome app displays "validated"
9. Your transaction is validated and will be tracked on the Blockchain as soon as it is confirmed by miners in accordance with Bitcoin protocol. While waiting for this confirmation, your Ledger device can be disconnected as your transactions are tracked on the Blockchain. These transactions will be synchronized on your wallet when you open it.

List of supported applications

To open and manage a wallet, you need to :

1. launch the wallet application on your computer,
2. open the dedicated companion application on your Nano S to unlock and synchronize the wallet.

So for each wallet you need 2 applications: 1 on your computer or browser, 1 on your Ledger Nano S.

Applications on your Nano S

Your Nano S is a multi-application device, so you can install and uninstall several applications on it, like Bitcoin, Ethereum, XRP a.k.a Ripple, and many other ones (altcoins, authentication, etc.), some of them provided by Ledger, some of them by other companies.
By default, your Nano S has some applications already installed:

- Bitcoin
- Ethereum
- and FIDO U2F

They can be removed, replaced, and you can add new applications thanks to the the Ledger Manager, which is like a free app store to download and delete your applications.
WARNING
Note that your Nano S can hold about 5 applications at the same time, but you can deal with many more applications - as many as stated on the Ledger Manager - by removing and installing the ones you need to manage. Removing an application won't make you lose your coins: you will be able to see your balance and transact as soon as the coin application has been installed again.

1. Install the Ledger Manager on your computer:
    - In your Chrome browser, go to this page
    - Click on "Add to Chrome"
2. Launch the Ledger Manager
3. See: how to launch the application once it is installed
4. Remove the applications you don't want by clicking on the bin, install the ones you need by clicking on the green arrow
5. See: how to use the Ledger Manager

Ledger Applications on your computer

Ledger provides 3 different Ledger Wallet applications to download.

- Ledger Wallet Bitcoin
- Follow the guide to install and use it: How to install and use the Bitcoin Chrome application
- It supports
    - Bitcoin
    - Bitcoin Cash
    - Dogecoin
    - Komodo
    - Litecoin
    - Stratis
    - Dash
    - Zcash
    - PivX
    - Viacoin
    - Vertcoin

- Ledger Wallet Ethereum
- Follow the guide to install and use it: How to install and use Ethereum and Ethereum Classic
- It supports
    - Ethereum (single account)
    - Ethereum Classic (single account)
    - To use this wallet, the companion application on your Nano S must have the "browser support" option set on YES.
- Ledger Wallet XRP
- Follow the guide to install and use it: How to install and use XRP a.k.a Ripple
- It supports
    - XRP a.k.a Ripple
    - To use this wallet, the companion application on your Nano S must have the "browser support" option set on YES.

Third-Party applications on your computer

There are also applications not provided by Ledger but by third-party, that can be used with the Nano S. Your private keys remain securely held by the Ledger device while transacting on such integrated wallets.

- MyEtherWallet
- Follow here the guide to install and use it: How to use MyEtherWallet with Ledger
- To use this wallet, the companion application on your Nano S must have the "browser support" option set on YES.
- It supports
    - Ethereum (multiple addresses and accounts)
    - Ethereum Classic (multiple addresses and accounts)
    - Expanse (multiple addresses and accounts)
    - and all ERC20 tokens (multiple addresses and accounts) like Expanse (EXP), Golem (GNT), Iconomi (ICN), Augur (REP), and hundreds of tokens.
- BitGo
- Follow the guide to install and use it: How to use BitGo with your Nano S
- To use this wallet, the companion application on your Nano S must have the "browser support" option set on YES.
- It supports
    - Bitcoin
- GreenBits / GreenAddress
- To use this wallet, the companion application on your Nano S must have the "browser support" option set on YES.
- It supports
    - Bitcoin
- Mycelium (Android)
- To use this wallet, the companion application on your Nano S must have the "browser support" option set on NO.

- Follow the guide to install and use it: How to use your Ledger on Android with Mycelium
- It supports
    - Bitcoin
- Electrum
- To use this wallet, the companion application on your Nano S must have the "browser support" option set on NO.
- Follow the guide to install and use it: How to use Electrum with your Nano S
- It supports
    - Bitcoin
- Ark
- To use this wallet, the companion application on your Nano S must have the "browser support" option set on YES.
- Follow here the guide to install and use it: How to install and use Ark with my Ledger
- It supports
    - Ark
- Ubiq
- To use this wallet, the companion application on your Nano S must have the "browser support" option set on YES.
- Follow the guide to install and use it: How to install and use Ubiq (UBQ)
- It supports
    - Ubiq

Please note that the Ledger Authenticator application is not required with the Nano S, this app is only suited for Nano and HW.1.

If a transaction has two outputs

When you send a Bitcoin transaction, you send an output from a former transaction, becoming an input of a new transaction. When the output of a transaction is used as the input of another transaction, it must be spent in its entirety. Sometimes the coin value of the output is higher than what the user wishes to pay. In this case, the client generates a new Bitcoin address, and sends the difference back to this address. This is known as change. See https://en.bitcoin.it/wiki/Change to know more about this important Bitcoin protocol topic.
These operations are normally calculated and done all-in-once when you send a transaction from your Ledger wallet. In some cases, a minor bug can make these outputs visible on your device, requiring 2 authentication on your side instead of one. If 2 outputs are displayed on your Ledger device, the second output (Output #2) is the one corresponding to your change address, to send the rest of your bitcoins to yourself.
If this happens, it is likely because you use a Segwit address with an old version of the Chrome application, not adapted to Segwit.

If so, you need to update your Chrome application by removing and reinstalling it:

1. In your Chrome browser go to chrome://extensions/
2. Click on the bin below "Ledger Wallet Bitcoin"
3. Go to https://chrome.google.com/webstore/detail/ledger-wallet-bitcoin/kkdpmhnladdopljabkgpacgpliggeeaf
4. Click on the "Add to Chrome" blue button and launch it again

Receive mining proceeds

Participants in mining activities may want to securely store their mining proceeds by using a Ledger device. This article explains why sending a large amount of small transactions to a hardware wallet is troublesome, offers potential solutions and provides instructions on how to properly send mining proceeds to an address controlled by your Ledger device.
Note: Failing to follow the instructions in this article may lead to your funds becoming inaccessible on the Ledger device.

Receiving a large amount of small transactions is troublesome

Receiving a large number of small payments, or *dust payments*, on an address controlled by your hardware wallet causes:

- the saturation of the synchronization of your Blockchain transactions; and
- an extremely long duration of transaction construction or validation.

Therefore, hardware wallets are not directly suited for receiving a large amount of small transactions, such as the proceeds of mining activities.
Example
Imagine that you have received 1,000 payments of 0.001 BTC and that you want to spend the total of 1 BTC. The secure chip in the hardware wallet will then have to construct a transaction of 1,000 inputs and sign each single input. This might take a few hours or might not succeed at all, since the chip may overheat and make a computation error.

In case you received a large amount of small payments

If you have already sent a large number of small payments to your hardware wallet:

- Try to consolidate your coins by sending a few larger payments to yourself. If you have received 1,000 times 0.001 BTC, consolidate these inputs by sending 0.1 BTC to yourself and repeat this 10 times.
- Alternatively, import your 24-word recovery phrase into a software wallet, preferably an offline one, and empty your wallet into an address that is derived from a newly generated seed.

Prevent problems by batching small transactions

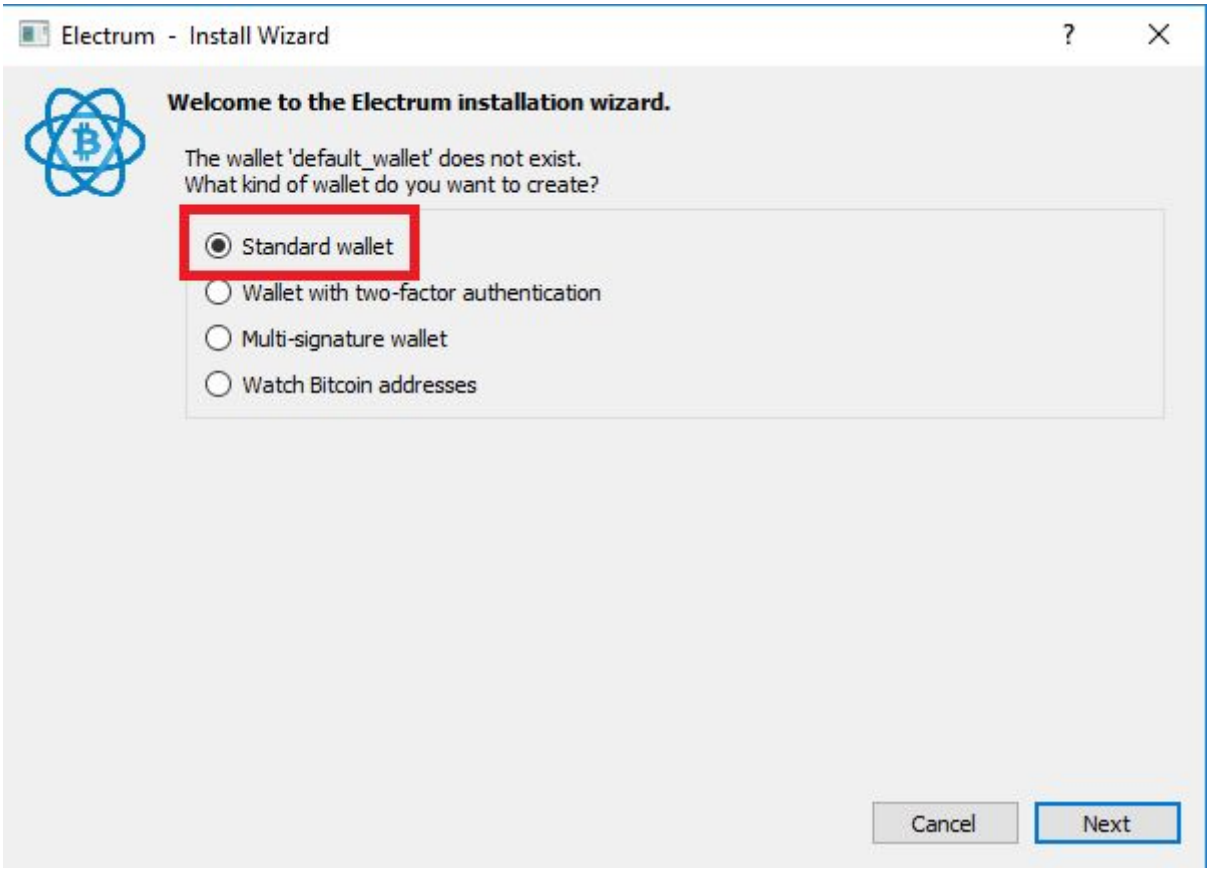
- Set up a software wallet that receives the small payments;
- Regularly batch these proceeds into a larger transaction to send onto a hardware wallet.

Set up and use Electrum

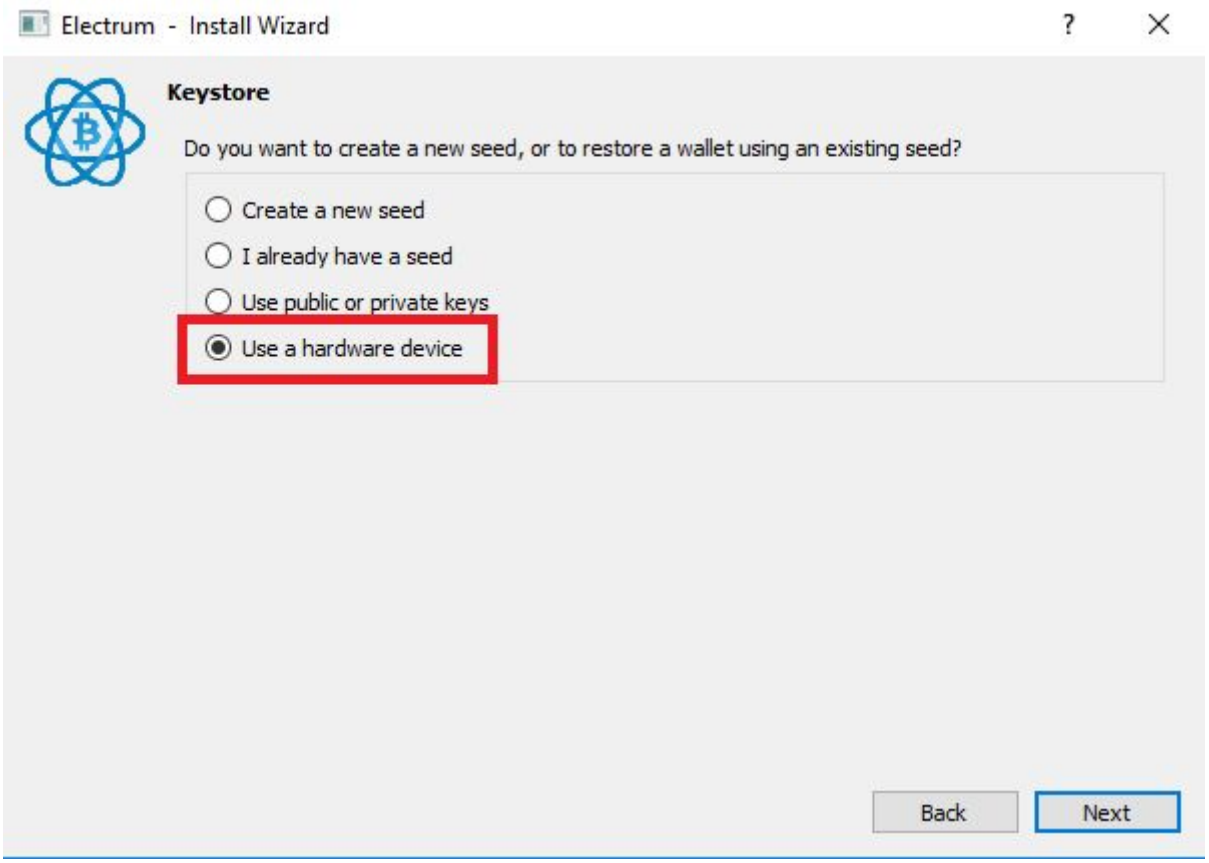
Electrum (from version 2.7.0) features support for the Ledger Nano S (Linux, Windows, OS X).

Install Electrum
Download and install Electrum from the official site.

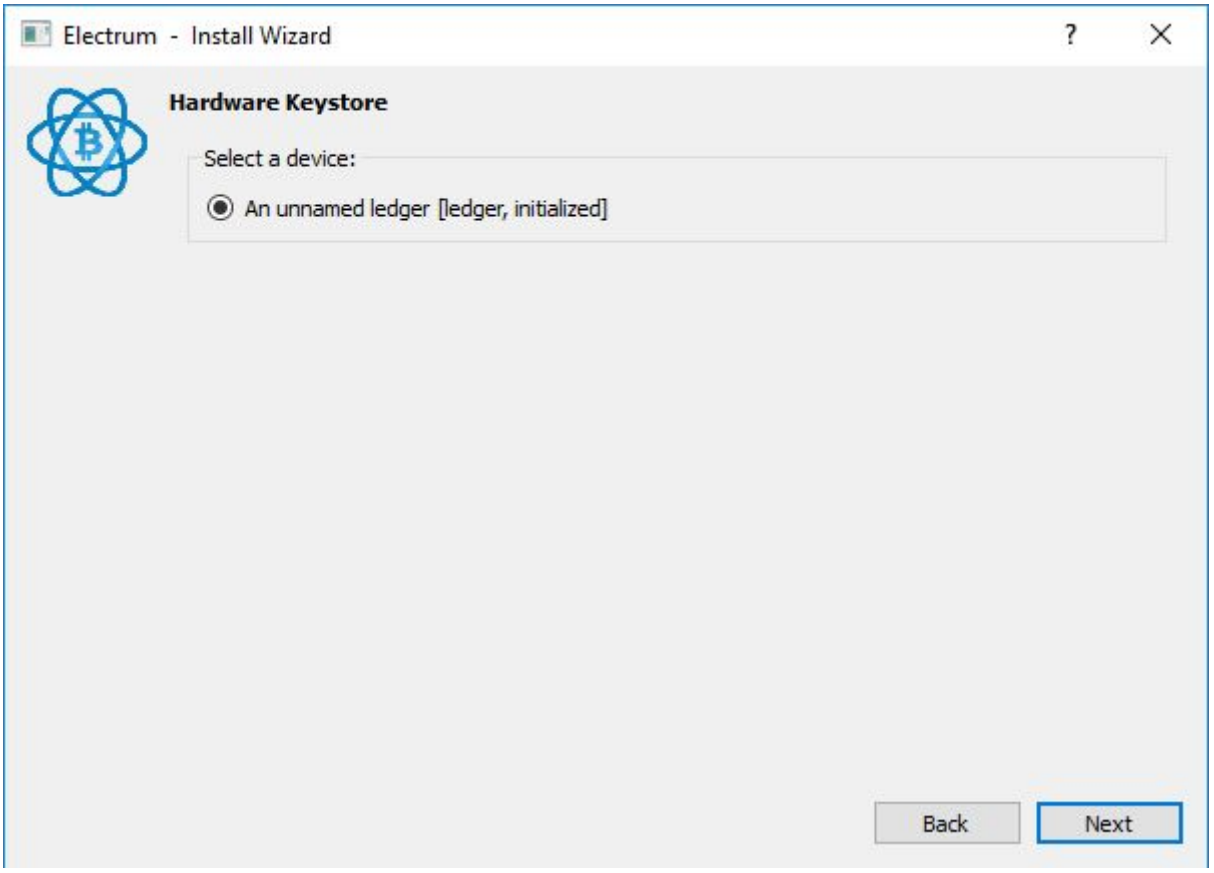
Configure Electrum
Select "Standard wallet"



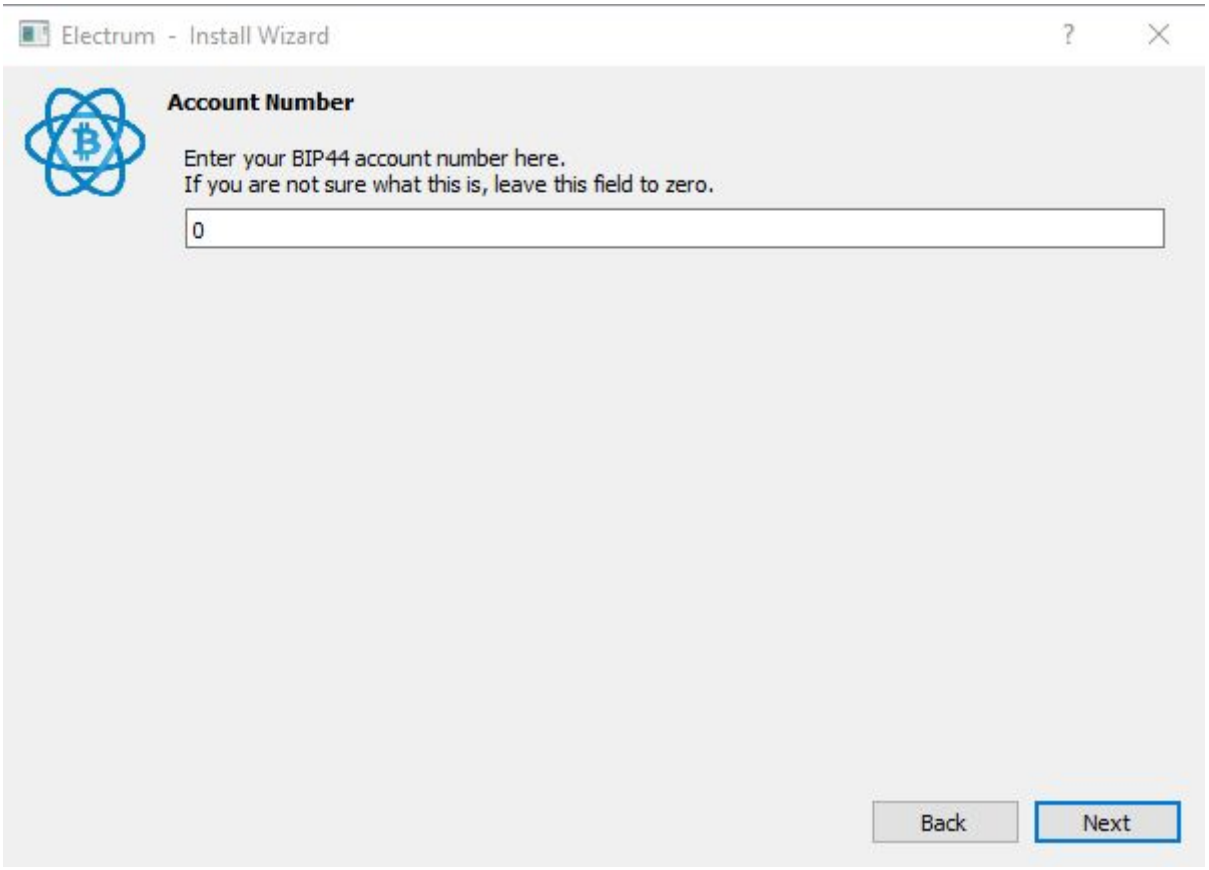
Connect your Nano S to your computer, enter the PIN and select the Bitcoin app.
Then select "Use a hardware device"



Once your Ledger Nano S is detected:



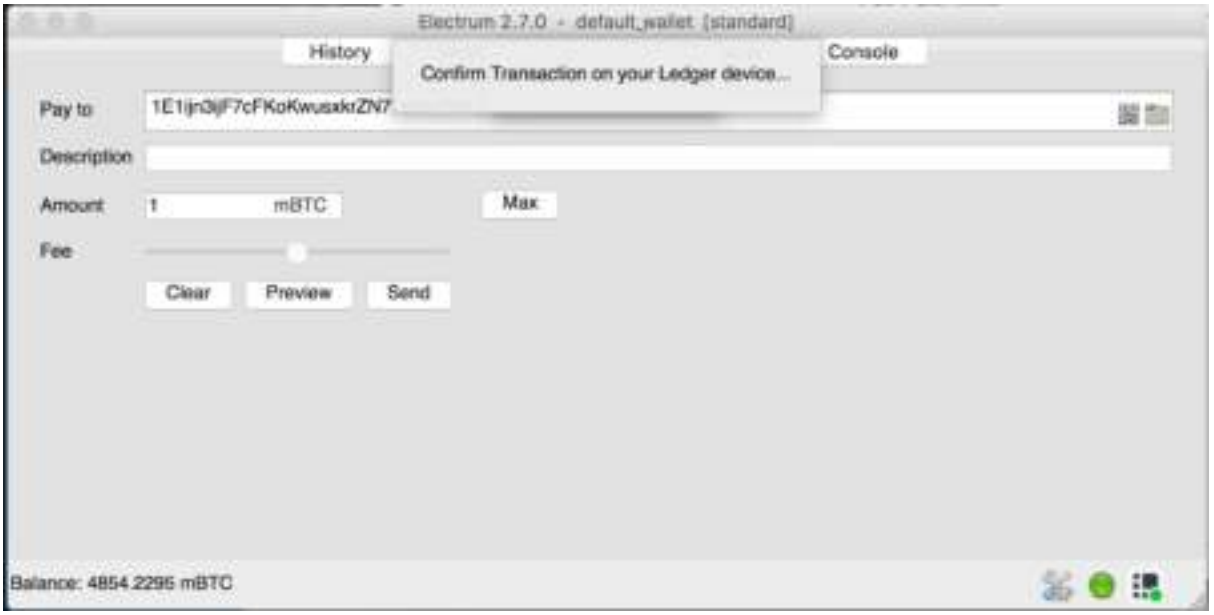
Press "Next", and select your "Account Number". If you are not sure, leave the field with "0", otherwise enter the index of the account you want to import.



Click on "Next", and Electrum will synchronize your account. Depending on your connection and the server, it may take from a few minutes to half an hour.
Once the synchronization process is finished, you can use Electrum normally.

Sending a transaction

When you want to sign a transaction, you must validate it on your Ledger Nano S.



Important archlinux user note
installation of python2-btchip is required to detect the Ledger Nano S.

Important Ubuntu user note
These additional steps are required on Ubuntu 16.04:
- apt-get install libusb-1.0-0-dev
- apt-get install libudev-dev
- ln -s /lib/x86_64-linux-gnu/libudev.so.1 /lib/x86_64-linux-gnu/libudev.so
- pip install btchip-python

Set up your device with EtherDelta

Ledger does not do customer support for EtherDelta, if you have issues with your transactions from or to EtherDelta you need to contact them (https://www.reddit.com/r/EtherDelta/comments/7dpqz2/etherdelta_support_chat_guides_for_new_users/).

Close all programs on your computer, go to EtherDelta.com and follow this procedure:

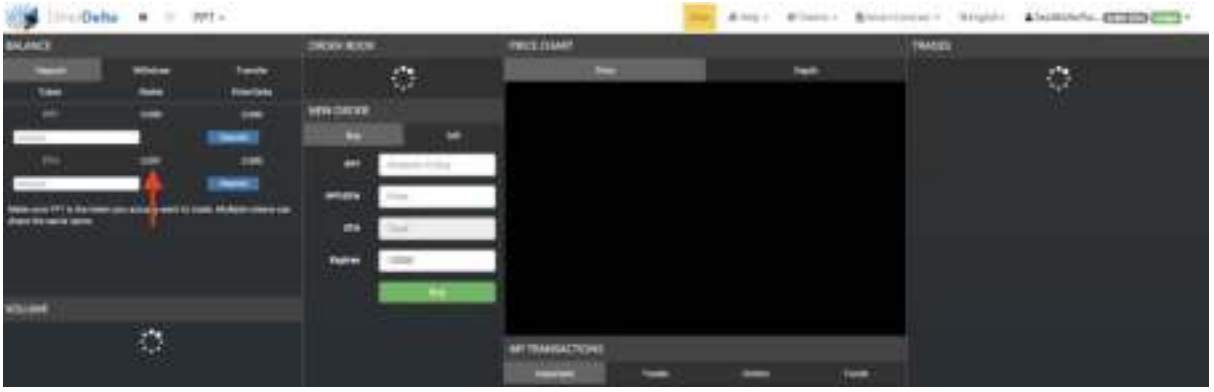
- On the top right corner of the screen click on “Select Account”.

- Choose “Ledger Nano S”.

- Follow the instructions on your computer screen. In your Ledger Nano S you need to go to the settings of the Ethereum application on your Ledger device and set "Browser Support" and "Contract Data" to "Yes".

- Once plugged in you will see your Ethereum public address, with your ETH balance, and the name "Ledger" on the top right corner of your computer screen.
Important notice: EtherDelta does not access your Ledger private keys, it does not have the ability to do so. Your Ledger private keys allow you to sign transactions.

- On the left side of your computer screen you will see your Ethereum and token balances.



- If you unplug the device while you are connected to EtherDelta you will be able to see your balance but you will not be able to make transactions.

Connect with Radar Relay

Radar Relay maintains a Øx order book and provides a simple interface to facilitate signing, finding, and filling Øx orders via browser interface.

To know how to connect your Ledger Nano S to Radar Relay please follow this link.

More Features

Check the firmware version

A new Ledger Nano S

1. Press and hold the right button. The right button is the one far away from the USB connector, closest to the swivel hole.
2. Insert the USB cable while holding the right button until *Recovery* is displayed.
3. Press the right button to select to the settings menu and press both buttons to enter.
4. Navigate to *Settings* > *Device* > *Firmware.*
5. The firmware version is displayed under *Secure Element*.
6. The micro controller version is displayed under *MCU.*

A Ledger Nano S in use

1. Insert the USB cable to switch on the device.
2. Enter your PIN code to unlock the device.
3. Press the right button to select to the settings menu and press both buttons to enter.
4. Navigate to *Settings* > *Device* > *Firmware.*
5. The firmware version is displayed under *Secure Element*.
6. The micro controller version is displayed under *MCU.*

Update the firmware

Follow the step by step instructions in the update guide to upgrade the firmware.


Device


Firmware


Secure Element
1.4.1

Change the PIN code

- Make sure firmware version 1.3.1 or higher is installed on the Ledger Nano S.
- Refer to this article if you do not know how to check the firmware version.
- Check the update guide to learn how to upgrade the firmware version.
- Turn on the Ledger Nano S by inserting the USB-cable.
- Unlock the device with your PIN code.
- From the dashboard, navigate to *Settings* > *Security* > *Change PIN*.
- Choose a new PIN code.
- Confirm the new PIN code by entering it again.
- Enter your old PIN code.
- The PIN code is now successfully changed.

Hide accounts with a passphrase

Warning: this tutorial is for advanced users.

Firmware compatibility:
1.3.1 (+): These options are available directly under the Settings menu on the Ledger Nano S.
1.0 to 1.2: Update your Ledger Nano S or contact us for advanced developer tools.

What is a hidden passphrase?
The hidden passphrase is a 25th word on top of your 24 word recovery phrase, but one that you need to remember and never write down. It generates a new identity: there is no right or wrong passphrase.

The hidden passphrase is used for two reasons

1. Protection of your 24 words recovery phrase if your accounts are behind a passphrase then you are protected.
2. "Plausible deniability" is a security feature that combats the risk of being threatened and/or forced to enter your PIN code. With this option, you can manage two PIN codes, unlocking two separate accounts:
- Your first PIN code provides access to your main wallet, like a basic account, with low amounts used for daily payments and small transactions.
- Second PIN code, linked to a specific passphrase you need to set up, opens an hidden account, to save large amounts, which will only be used occasionally. With this option, in case you are forced to recover a wallet from your 24-word backup, only the main wallet will be displayed, and the second account will remain hidden, as long as you don't reveal the attached passphrase.

Note that all applications on your Ledger device (Bitcoin, Ethereum, FIDO…) are affected by the passphrase identity change.

How to create a hidden passphrase and its PIN code
On your Ledger Nano S:

"Settings" > "Security" > "Passphrase" > "Attach to a PIN"
1. Enter a second and new PIN code
2. Confirm this new code
3. Enter and confirm a secret passphrase (100 characters max)
4. Enter your first main PIN code to validate

During the rest of your session, until the Ledger Nano S is disconnected, you will run a hidden wallet. Next time you use your Ledger Nano S, you will choose which PIN code you want to enter, main one (main wallet) or second one (hidden wallet). You can't set a third PIN code. If you ever set a new PIN code attached to a passphrase, it would erase the first one and the assets held by it.

How to best use the passphrase feature: our recommendation is to use your current PIN for your day to day accounts, and your alternate PIN for your savings account, holding a larger amount of assets. This way, not only will your backup seed be protected by the passphrase, but your “duress” PIN code will in fact be a real account with real transactions. This would be much more effective for a plausible deniability scenario.

Temporary Passphrase
With this feature, you can create, open or manage an hidden wallet, accessible only in this setting path. As long as your session will be open with this passphrase, you will be able to access it. When you disconnect your Nano S or when you quit the standby mode, this passphrase will be overwritten.

You can create and manage as many temporary passphrases as you want, but only one by one - you can't open two or more temporary passphrases in the same session:

"Settings" > "Security" > "Passphrase" > "Set temporary"
1. Enter and confirm your secret passphrase (100 characters max)
2. Enter your PIN code to validate
Then during the rest of your session until the Nano S is disconnected, you will run a new wallet attached to this passphrase. Next time you will enter your PIN code, you will open your main wallet, not this hidden account.

How to recover your hidden wallet(s) on a Ledger Nano S
On your Ledger Nano S you need to recover your 24 words and set your previous hidden passphrase as a temporary passphrase or as a hidden wallet attached to a PIN code.

If you want to attach it to a passphrase:

1. on your Nano S you must run the 24 words you previously ran when you set your passphrase. If you don't, reset your device and import the correct 24 words
2. go to "Settings" > "Security" > "Passphrase" > "Attach to a PIN"
3. choose a second PIN code and confirm it (you don't have to choose the same one as the previous one you set with the passphrase)
4. set the exact passphrase you want to recover and confirm it
5. validate by entering your first PIN code

If you want to set it as temporary passphrase:

1. on your Nano S you must run the 24 words you previously ran when you set your passphrase. If you don't, reset your device and import the correct 24 words
2. go to "Settings" > "Security" > "Passphrase" > "Set temporary"
3. set the exact passphrase you want to recover and confirm it
4. validate the passphrase by entering your current PIN code

How to recover your hidden wallet(s) on a compatible wallets
If you ever lose your Ledger Nano S, you can restore your main wallets and hidden wallets by importing your 24 words backup and your hidden passphrase, using any compatible wallet that supports BIP39 passphrases, or on another Ledger Nano S hardware wallet.

You can also manually export your private keys using an online tool for advanced users.

Advanced Passphrase options

This feature is not available for the Ledger Blue device.

Since the Nano S 1.3 update, you'll find an ADVANCED security mode in your Nano S to manage different passphrases in the same wallet. This feature is sometimes called "Plausible deniability".
To update to Nano S 1.3, read this guide
These settings are useful to have 1 main account and 2 or several hidden accounts from the same wallet, with the same 24-word seed. But take care, these plausible deniability features are delicate to manage, as you are the only one to know a multitude of codes. if you ever lose them, Ledger nor anyone will be able to recover them for you. Do not activate this option if you are not absolutely sure to understand it.

WHAT IS PLAUSIBLE DENIABILITY?
In Nano S, "Plausible deniability" is a security feature to face the risk of being threatened and/or forced to give your PIN code. With this option, you will manage 2 PIN codes:

1. First PIN code gives access to your main wallet, like a basic account with low amounts, to check daily payments.
2. Second PIN code, linked to a specific passphrase you need to set up, opens an hidden account, for example to save large amounts, which will be used once in a while.

With this option, in case you are forced to recover a wallet from your 24-word backup, only the main wallet will be displayed, and the second account will remain hidden, as long as you don't reveal the attached passphrase. No one can know you have 2 PIN codes attached to your wallet, so you can reveal the first PIN code giving access to your daily wallet, to avoid having your savings stolen from your second wallet.

As each PIN is using its own independent counter and PIN comparison is constantly done, it is highly unlikely for an unsuspecting sophisticated attacker to guess that a second PIN is enabled, providing that you give the first PIN to the attacker, and not possible to brute force one PIN knowing another one.

PASSPHRASE ATTACHED TO A PIN
In your Nano S, go to SETTINGS > Security > Passphrase > Attach to a PIN
With this feature, you can create, open and manage a second (and hidden) wallet attached to a specific passphrase, wallet accessible when you connect your Nano S with another PIN code. As long as your session will be open with this PIN code, you will be able to access it. When you disconnect your Nano S or when you quit the standby mode, you will be asked a PIN code, then you can choose to reopen this one or enter the main PIN code.

1. Open the "Settings" of the Nano S
2. Select "Security"
3. Select "Passphrase"
4. Select "Attach to a PIN"
5. Enter a second and new PIN code
6. Confirm this new code
7. Enter and confirm a secret passphrase (100 characters max)
8. Enter your first main PIN code to validate

Then during the rest of your session until the Nano S is disconnected, you will run an hidden wallet. Next time you will enter your PIN code, you will choose which PIN code you want to enter, main one or second one.
You can't set a third PIN code. If you ever set a new PIN code attached to a passphrase, it would erase the first one. To manage more than 1 hidden wallet you need to use the "temporary passphrase" option.

How to best use the passphrase feature

Our recommendation is to use your current PIN for your day to day accounts, holding reasonable assets, and your alternate PIN for your savings account, holding higher value assets. This way, not only will your backup seed be protected by the passphrase, but your “duress” PIN will in fact be a real account with real transactions. This would be much more effective in a plausible deniability scenario.

Temporary Passphrase

In your Nano S, go to SETTINGS > Security > Passphrase > Set Temporary
With this feature, you can create, open or manage an hidden wallet, accessible only in this setting path. As long as your session will be open with this passphrase, you will be able to access it. When you disconnect your Nano S or when you quit the standby mode, this passphrase will be overwritten. You can create and manage as many temporary passphrases as you want, but only one by one - you can't open 2 or more temporary passphrases in the same session.

1. Open the "Settings" of the Nano S
2. Select "Security"
3. Select "Passphrase"
4. Select "Set temporary"
5. Enter and confirm your secret passphrase (100 characters max)
6. Enter your PIN code to validate

Then during the rest of your session until the Nano S is disconnected, you will run a new wallet attached to this passphrase. Next time you will enter your PIN code, you will open your main wallet, not this hiden account.

How to recover your hidden wallet(s) on a Ledger Nano S
On your Nano S, just recover your 24 words and set your previous hidden passphrase as a temporary passphrase or as a hidden wallet attached to a PIN code.
if you want to attach it to a passphrase:
- on your Nano S you must run the 24 words you previously ran when you set your passphrase. If you don't, reset your device and import the correct 24 words
- go to Settings > Security > Passphrase > Attach to a PIN
- choose a second PIN code and confirm it (you don't have to choose the same one as the previous one you set with the passphrase)
- set the exact passphrase you want to recover and confirm it
- validate by entering your first PIN code

if you want to set it as temporary:

- on your Nano S you must run the 24 words you previously ran when you set your passphrase. If you don't, reset your device and import the correct 24 words
- go to Settings > Security > Passphrase > Set temporary
- set the exact passphrase you want to recover and confirm it
- validate by entering your current PIN code

HOW TO RECOVER YOUR HIDDEN WALLET(S) ON A COMPATIBLE WALLET
If you ever lose your Ledger Nano S, you can restore your wallets and hidden wallets by importing your 24 words backup + your hidden passphrase, using any compatible wallet supporting BIP39 passphrases, on another Nano S, or on Trezor hardware wallet.
You can also manually export your private keys using an online tool for advanced users.

Export your accounts

Accounts generated by a Ledger Nano S device can be recovered on any (third-party) hardware or software wallet that supports the same standards as Ledger (BIP39/BIP44).

Before you begin

- Note that your 24-word recovery phrase provides full access to your accounts. Entering your recovery phrase on a computer or smartphone may be insecure. Avoid doing so if possible.
- Carefully select a (third-party) hardware or software wallet. Protecting your accounts remains your own responsibility.
- Contact Ledger Support when in doubt.

Use your recovery phrase

1. Carefully select a BIP39/BIP44 compatible hardware or software wallet that you trust.
2. Get your 24-word recovery phrase.
3. Follow the manual of the selected device or service to import your recovery phrase.

Compatible Ledger devices

- Ledger Nano S
- Ledger Blue
- Ledger Nano
- Ledger HW.1

Arbitrary list of thirdartp-party software wallets

- Mycelium (smartphone)
- Bither (smartphone/desktop)
- Coinomi (smartphone)

- MyEtherWallet
- MyCrypto

Generate private keys (advanced)

Advanced users can manually generate all private keys using Ian Coleman's BIP39 tool. This tool is best downloaded for offline use, as instructed below.

Generate your private keys

1. Download the BIP39 tool at the bottom of this article or view the source on GitHub.
2. Double-click the downloaded file to open it in a browser.
3. Type your 24-word recovery phrase in the field *BIP39 Mnemonic*. Use lowercase only.
4. Type your passphrase if you set one in your Ledger hardware wallet.
5. Select a cryptocurrency.
6. Leave the field Internal/External at 0.

Import your private keys

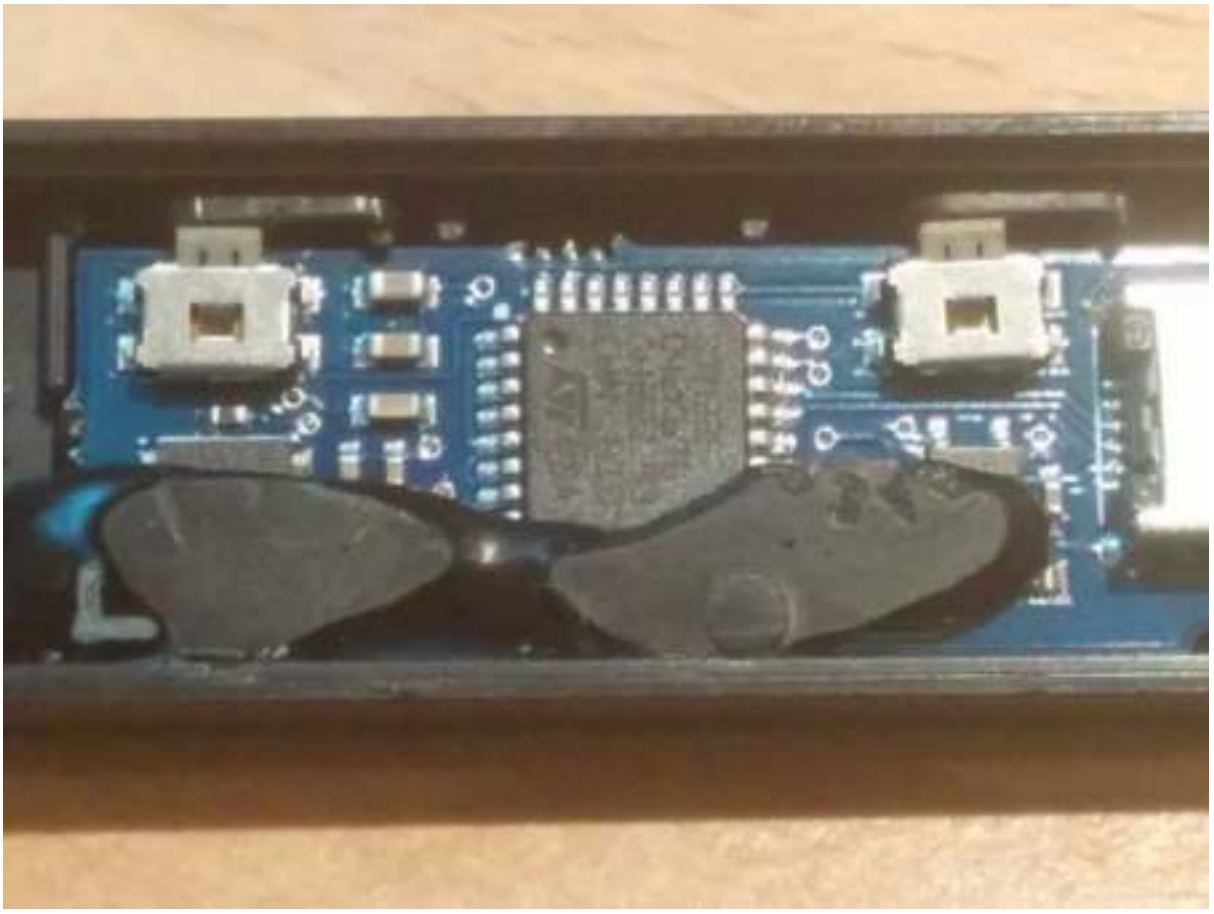
1. Copy the list of generated private keys from the *Derived Addresses* section. Use the controls below the list to show more rows or start at a certain index.
2. Import your private keys in a third-party wallet that supports this, such as Armory.
3. Set the field Internal/External to 1 to generate the private keys of your change addresses.
4. Import the private keys associated with your change addresses in the third-party wallet.

Check hardware integrity

IMPORTANT NOTICE
For advanced hardware savvy users only.
Please handle with high care the Nano S while you proceed with this verification. Be aware that once opened, your device will not be refundable or exchangeable.

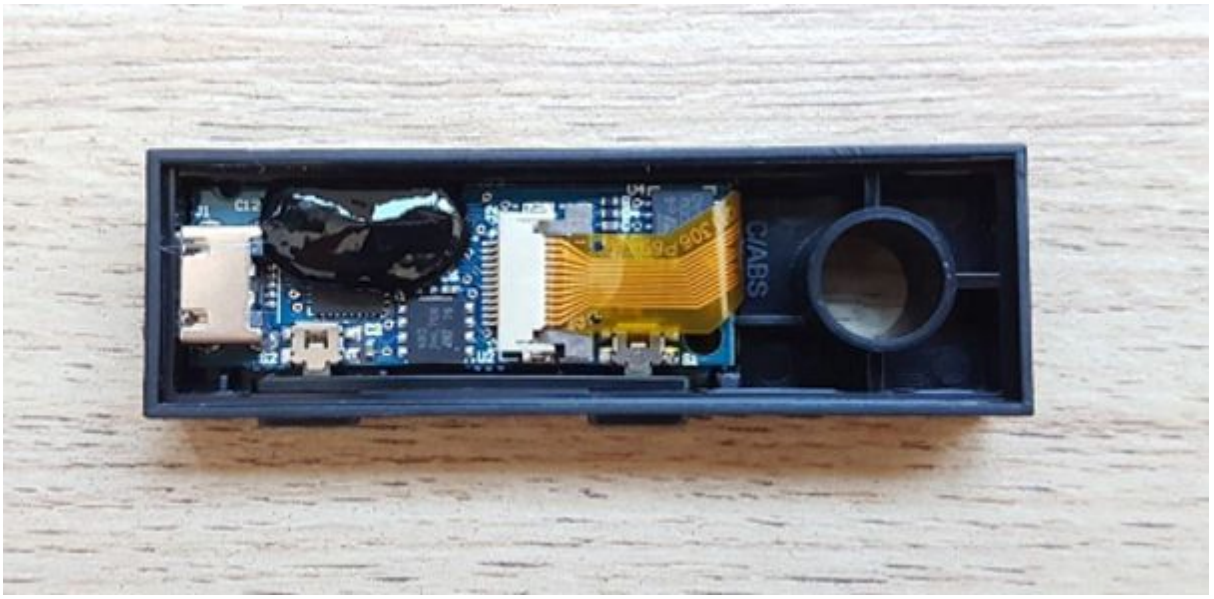
On the hardware side, if you want to check that the Nano S has not been tampered with, or the applications running are the official apps, here are a few things that you might need to know:
1) The Secure Element checks the full microcontroller flash at boot (this is described in our blog post). If it 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 (referring to the attached picture) and that the MCU is an stm2f042k6 (with 32 Kb flash, as a bigger flash could contain code fooling the Secure Element validation). Markings on the chip can vary but you should see the string "042K6".

Revision 1 (blue PCB, black glue):

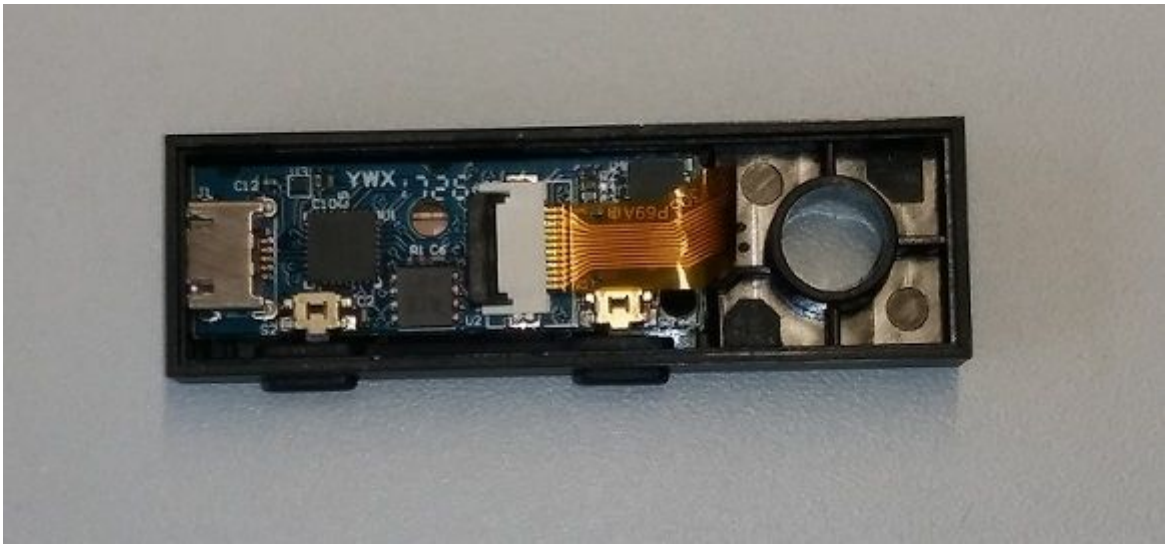


Revision 2 (green PCB, black or transparent glue [not pictured] depending on the batch):

Revision 3 (blue PCB, black glue)

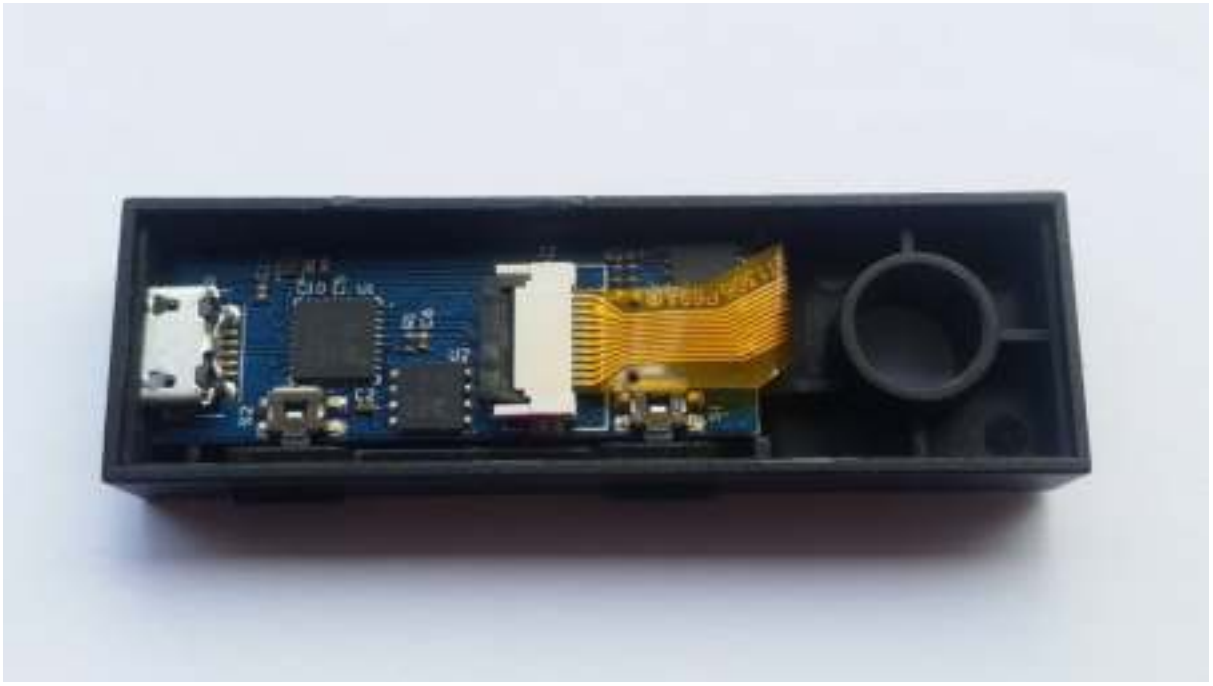


Revision 4 (blue PCB + hole)



Revision 5 (blue PCB)

Revision 5 bis (blue PCB)



Revision 6

2) The Secure Element itself is personalized at factory with an attestation proving that it has been created by us. You can verify it by running
pip install --no-cache-dir ledgerblue
Then on firmware 1.3.1 or below
python -m ledgerblue.checkGenuine --targetId 0x31100002
Or on firmware 1.4.1 and above
python -m ledgerblue.checkGenuine --targetId 0x31100003

The source code is available here.

3) Each individual application will display a "Non Genuine" warning if not signed when opened. A modified User Interface (as found in https://github.com/LedgerHQ/nanos-ui) will also display a warning message on boot.

4) The root of trust for the current batch is the following secp256k1 public key : 0490f5c9d15a0134bb019d2afd0bf297149738459706e7ac5be4abc350a1f818057224fce12ec9a65de18ec34d6e8c24db927835ea1692b14c32e9836a75dad609 - as checked here Genuine.py

Troubleshooting

Firmware Update - FAQ

How can I update my Nano S?
Please refer to our update guide for step by step instructions.
What if my Ledger Nano S displays *MCU firmware is not genuine*?
Try disconnecting and reconnecting the USB cable to continue. If the USB cable is not fully inserted, the authenticity check of the MCU will return this particular error during the startup process of the device.
What to do if I am stuck somewhere in the update?
Please carefully read the step by step instructions. Still having issues?

1. Close Chrome and all other applications *(crypto wallets, Geth, Parity, Mist, Bitcoin Core, etc).*
2. Turn OFF VPN and anti-virus.
3. Quit, reinstall and restart the Ledger Manager.
4. Change the USB-cable if possible.
5. Restart the computer.
6. Windows 7 users: please check the solutions at the bottom of this page.
7. Try another computer.

Is it mandatory to update my Nano S firmware?
Updating your Nano S to firmware 1.4 is strongly recommended, but there is no mechanism to force you to upgrade.
What will happen if I do not update my Nano S?
We strongly recommend updating the firmware of your Nano S. However, there are no significant consequences if you do not update your device at once. The Ledger Wallet applications will notify you to update your device, but you are free to ignore them and the device will continue to work normally.
What is this update for?
The update to firmware version 1.4.2 introduces user experience as well as minor security improvements. For more information regarding the specific changes, please refer to the blog post dedicated to this firmware release.
Do I have to upgrade my Nano S if I am not using it?
There is no necessity to install the firmware update immediately. It is no problem if you do not have immediate access to your device or if you do not plan to use it in the short term. You will always be able to update to the firmware later, whenever you decide to use your device.
What exactly are the security vulnerabilities discovered? Should I be concerned?
Please refer to our blog post concerning the release of firmware version 1.4.2.
Is it possible to downgrade from 1.4 to 1.3.1?
No. For security reasons, it is not possible to downgrade the firmware of your Nano S.
How can I enter my PIN code after the update?
If your PIN code includes less than 8 digits, please type in your PIN code as usual, and use the right / left button until you reach a check mark (✓). Then, confirm your PIN code pressing both buttons.
Why didn't my Ledger Nano S prompt to check the Identifier?

As explained in step 5 of the update guide, the Ledger Nano S shows three screens after each other in a slider. If the right button is pressed before the other screens are shown, the firmware update will be installed before you could have checked the version number or the identifier. Please check that firmware version 1.4.2 and MCU version 1.5 are correctly installed.

How many applications can I have on my Nano S with 1.4?

One of the user experience gains of the 1.4 firmware update is the possibility to install many more applications on the Nano S. The global limitation is related to the small amount of memory available on the device. The new firmware does not expand the memory, but optimizes the size of Bitcoin related applications.

Many cryptocurrency projects are clones of the Bitcoin blockchain that share most of the signature code (such as Bitcoin, Bitcoin Cash, Bitcoin Gold, Litecoin, Dogecoin, Dash, Zcash, Komodo, Stratis, Posw, Pivx, Viacoin, Vertcoin, Stealthcoin, Digibyte, Qtum, Hcash...). By refactoring all common codes in a library, hosted in the Bitcoin app, we were able to significantly reduce the size of the other apps. This enables the installation of up to 18 applications that share this library.

However, installing applications with a completely different code base will still limit the amount of apps to 4 or 5, for instance: Bitcoin, Ethereum, Ripple, FIDO U2F and Password Manager.

So, the types of applications installed lead to varying capacities. Most users may expect to see a capacity of 10 to 12 applications.

Will I need my 24 word seed during the update?

Most users do not need to restore their Nano S after the update, and thus do not require access to their 24 word seed. The seed will only be wiped when updating a Nano S that currently has firmware version 1.2 or lower installed. You can check the current firmware version on your device before updating to 1.4.2.

However, make sure your 24 recovery words are properly backed-up and securely stored before starting the update.

Could I lose my funds during this update?

Funds will not be at risk as long as the 24 word seed is properly backed-up and securely stored. Carefully follow the steps in the update guide.

Only users updating from firmware version 1.2 or lower will have their seed wiped during the process and will need to restore their 24 word seed after the update.

Always make sure your 24 recovery words are properly backed-up and securely stored before starting the update.

Is this firmware version compatible with Nano / Unplugged / HW.1?

No, this update only applies to Ledger Nano S devices.

Is this new version compatible with Ledger Blue?

No, this update only applies to Ledger Nano S devices.

What if I am stuck on the *Update* message on my Nano S?

If your Nano S stays stuck displaying *Update*, and the Ledger Manager shows the message *To begin, connect your Ledger Wallet*, then:

1. Disconnect your Ledger Nano S
2. Quit and relaunch the Ledger Manager
3. Reconnect the Ledger Nano S and unlock it by entering your PIN code
4. Go to Step 4 of the update guide.

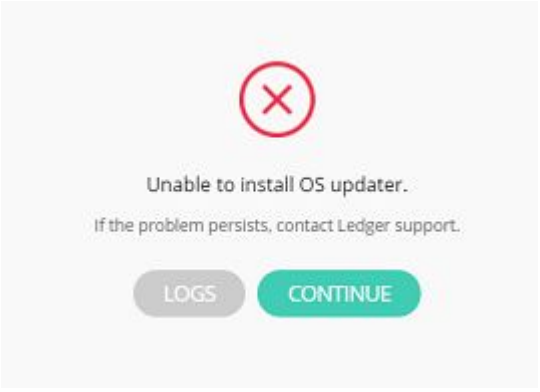
What to do with issues on Windows?

1. Open the Device Manager from the Control Panel.
2. Find the USB-device that has a yellow warning sign and right-click on it to select *Update driver*.
3. After the driver has been updated, you can close and open Chrome browser, open Ledger Manager, connect your device and just wait.

If you are using Windows 7, you will have to finalize the update on another computer (not running Windows 7). We are working on a fix, but meanwhile this is the only option.
On other systems (Mac/Linux), if you are having trouble then the only solution is to try again.
The update server processes the download requests in a queue. The best is to wait when nothing seems to be happening. If it fails, then retry a few moments later. We thank you for your patience.
If you are still having a hard time updating, make sure that no other applications are running on your computer (such as Parity, other crypto wallets or a firewall app).
I have an issue that is not described neither in the update guide, nor in this FAQ article
Please contact our support team and describe your problem in as much detail as possible.

Unable to install OS Updater

This guide suits for Ledger Nano S only. If you have a special edition Nano S (orange casing), you can not update your device.
If this message appears on your Ledger Manager when you want to update your firmware: "Unable to install OS updater"



check on the "FIRMWARES" tab of the Ledger Manager the latest available release and compare it with yours. To know which firmware you currently run on your Ledger Nano S, open the Settings on the Nano S itself, and go to Settings > Device > Firmware.

- If you already have the latest firmware, you do not need and can't update as you have the latest one.
- If you do not have the latest firmware,
    - temporary remove all your applications from your Nano S to install the OS updater. Click here to know how to uninstall apps. Don't worry, you'll be able to reinstall the apps you need after the update, and they will synchronize all your past operations. Even if you uninstall your applications, your coins won't be lost or erased, your balances and operations will be synchronized as soon as you reinstall them and open your wallets.
    - Then you will be able to install the OS updater, and to go through the update procedure.

If the problem persists despite of the complete uninstallation of your applications:

- click on the "LOGS" grey button
- save the Logs folder on your computer
- send it to the customer support below with a message explaining the context of your issue.

Connection issues with Windows or Linux

Windows
Please try with another USB cable. If possible, please try on a Mac computer to verify that your Ledger Nano S is not faulty.

Linux
You need to create a set of udev rules to allow access to the device on Linux. This can be done easily by running the following command:

```
wget -q -O - https://raw.githubusercontent.com/LedgerHQ/udev-rules/master/add_udev_rules.sh | sudo bash
```

For more information, please refer to https://developer.chrome.com/apps/app_usb#caveats.

If you still cannot access the Ledger Wallet, your user might not belong to the "plugdev" group - in this case, modify the above /etc/udev/rules.d/20-hw1.rules rule to match your group or add a OWNER="username" parameter to each line, username being your Linux user name.

For Arch Linux, here are the following rules to use:
/etc/udev/rules.d/20-hw1.rules

```
SUBSYSTEMS=="usb", ATTRS{idVendor}=="2581", ATTRS{idProduct}=="1b7c", MODE="0660", TAG+="uaccess", TAG+="udev-acl"
SUBSYSTEMS=="usb", ATTRS{idVendor}=="2581", ATTRS{idProduct}=="2b7c", MODE="0660", TAG+="uaccess", TAG+="udev-acl"
SUBSYSTEMS=="usb", ATTRS{idVendor}=="2581", ATTRS{idProduct}=="3b7c", MODE="0660", TAG+="uaccess", TAG+="udev-acl"
SUBSYSTEMS=="usb", ATTRS{idVendor}=="2581", ATTRS{idProduct}=="4b7c", MODE="0660", TAG+="uaccess", TAG+="udev-acl"
SUBSYSTEMS=="usb", ATTRS{idVendor}=="2581", ATTRS{idProduct}=="1807", MODE="0660", TAG+="uaccess", TAG+="udev-acl"
SUBSYSTEMS=="usb", ATTRS{idVendor}=="2581", ATTRS{idProduct}=="1808", MODE="0660", TAG+="uaccess", TAG+="udev-acl"
SUBSYSTEMS=="usb", ATTRS{idVendor}=="2c97", ATTRS{idProduct}=="0000", MODE="0660", TAG+="uaccess", TAG+="udev-acl"
SUBSYSTEMS=="usb", ATTRS{idVendor}=="2c97", ATTRS{idProduct}=="0001", MODE="0660", TAG+="uaccess", TAG+="udev-acl”
```

If this still doesn't work you may need to add these rules:

```
KERNEL=="hidraw*", SUBSYSTEM=="hidraw", MODE="0660", GROUP="plugdev", ATTRS{idVendor}=="2c97"
KERNEL=="hidraw*", SUBSYSTEM=="hidraw", MODE="0660", GROUP="plugdev", ATTRS{idVendor}=="2581"
```

Lost device, PIN code or recovery phrase

Ledger Wallet

In case of the loss, theft, or destruction of your Ledger Wallet - or at any time - you can restore your entire balance either on another Ledger Wallet or on any BIP39 compatible software wallet such as Myceliumthanks to the 24 words you copied on the Recovery Sheet.

These 24 words are paramount, they insure you are the owner of your coins. You must never reveal them, and never lose them. Without the PIN code and the 24 words a thief cannot access your coins.

Watch this video to learn how to restore your wallets.

You can recover your wallet from any wallet supporting the 24-words recovery phrase, compatible with BIP39 wordlist, BIP32, BIP44. List of compatible wallets to import your Ledger wallet backup:
- Ledger Nano
- Ledger HW.1
- Ledger Nano S
- Ledger Blue
- Mycelium (smartphone)
- Bither (smartphone and desktop)
- Coinomi (smartphone)
- MyEtherWallet

If you forget your PIN code
After three invalid attempts, the wallet will reset itself to factory condition, wiping your 24 words recovery phrase (see next section below). You will need to restore your wallet using these 24 words recovery phrase.

Recovery Phrase
It is extremely important not to lose your recovery sheet: you must keep it in a very safe location. If anyone gets access to it (and understands what it is), they can steal all your cryptocurrencies (without the need for your PIN or security card, if you own a Nano/HW.1).
However, if you were to lose your recovery sheet, you need to immediately transfer your entire balance to a temporary wallet. Then reset the Nano and create a new seed. Once done, transfer back your balance to your Ledger Wallet.

Browser support

Enable browser support to use your Ledger device with a third-party application, like MyEtherWallet. This is required for

Ledger Nano S

Enable browser support to use your Ledger Nano S with:
- Ledger Ethereum Wallet
- Ledger Ripple (XRP) Wallets
- Third-party services, like Electrum and Mycelium

Step by step instructions

1. Connect your Ledger Nano S to your computer

2. Open the Ripple or Ethereum app on your Ledger Nano S by pressing both buttons
3. Disable browser support from the settings within the app.
4. Press the right button to find *Settings*
5. Press both buttons to open *Settings*
6. Press the right button to select *Browser support*
7. Press both buttons to open it *Browser support.*
8. Select *Yes* and press both buttons to confirm.

Troubleshoot hardware issues

If you have issues with your buttons (stuck buttons, broken buttons…), damaged screen or pixelated screen, or a loose USB port, then please fill out this form. There is no guarantee of a refund or exchange, but this form must be filled out in order to begin the process.

What to do if your Ledger Nano S is stuck displaying “Update”
This means that something - probably a network failure - blocked the update procedure before it was completed.
Please follow this guide to fix your issue:

1. In your Chrome browser go to “chrome://extensions”
2. Click on the bin beside the Ledger Manager to uninstall it
3. Go to “github/Ledger”
4. Download the “chrome-app.zip” file and extract it
5. Restart the Chrome browser
6. In “chrome://extensions/” , activate the "Developer mode" in the top right corner
7. When it appears, click on "Load unpacked extension"
8. Download the extracted "chrome-app" folder
9. Once installed, launch this new application
10. Connect your Nano S
11. Once this new Ledger Manager has been launched, go to "Firmwares"
12. Then click on the grey "Firmware" button
13. Follow the instructions on the device to complete the update
14. Once everything is done, uninstall this custom application on Chrome extensions and deactivate the Developer mode
15. Re-install the Ledger Manager application on Chrome.

What to do if your Ledger Nano S only displays the “Settings” menu
If you can only access the Settings menu of your Ledger Nano S, you probably have recently reset or updated your Ledger Nano S.

Once your update or reset is complete, your Nano S will be entirely wiped, which is why you can only access the “Settings” menu of your device. You will not have any other applications installed on your Nano S following the update or reset, so now you must reinstall all of your applications from the Ledger Manager using this tutorial.

Please note that your private keys are not erased since they are linked to your 24 word recovery phrase.

What to do if your Ledger Nano S screen is not responsive

If the screen of your Ledger Nano S is stuck on the same menu and you can not scroll up or down do the following procedure:

1. Download the Ledger Manager
2. Launch it
3. Do not plug or unplug your Ledger Nano S
4. Press and hold the left button for at least 5 seconds (the button near the micro USB port)
5. Plug in your Ledger Nano S
6. The screen will display "Bootloader"
7. Release the left button
8. The Ledger Manager will start loading