Monero Application
User Guide

Cédric Mesnil (cedric@ledger.fr)

March 16, 2018

Contents

Chapter 1

License

Author: Cedric Mesnil <cedric@ledger.fr>

License:

Copyright 2018 Cedric Mesnil <cedric@ledger.fr>, Ledger SAS

Licensed under the Apache License, Version 2.0 (the “License”);
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an “AS IS” BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND,
either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

Chapter 2

Introduction

Monero application for Ledger Blue and Nano S

Chapter 3

How to install Monero Application

3.1 Nano S / Blue

For both, source and binary installation, use the most recent tag.

3.1.1 From Binary

Use the "Ledger Manager" Chrome App. See https://www.ledgerwallet.com/apps/manager for details.

As the "Monero" application is still in beta stage the application is in developer section: click on "Show developers items" on the bottom right corner to see it.

- Launch the Ledger Manager. See Ledger Manager and https://ledger.groovehq.com/knowledge_base/topics/ledger-manager for details about installing and using the manager;
- Connect your Nano S or your Blue, enter your PIN, and stay on the dashboard;
- Click on *show developer items* on the bottom right corner;
- Click on the green bottom arrow icon near the Ledger *Monero* logo;
- Confirm the installation when required on your device by pressing the right button above the checkmark;
- Quit the Ledger Manager

The application is ready to use!

3.1.2 From source

Building from sources requires the the Nano S SDK 1.4.1+ on firmware 1.4.1+.
See https://github.com/LedgerHQ/nanos-secure-sdk

Refer to the SDK documentation for the compiling/loading...

3.2 System Configuration

3.2.1 Linux

The following packages must be installed: pcsc-tools pcscd libpcsclite1:amd64 .

You have to have to add the NanoS to /etc/libccid_Info.plist

> In <key>ifdVendorID</key> add the entry <string>0x2C97</string>
> In <key>ifdProductID</key> add the entry <string>0x0001</string>
> In <key>ifdFriendlyName</key> add the entry <string>Ledger Token</string>

These 3 entries must be added at the end of each list.

3.2.2 MAC

The SmartCard service must be installed. See https://smartcardservices.github.io/

1. First it is necessary to [disable SIP](https://developer.apple.com/library/mac/documentation/Security/Conceptual/System_Integrity_Protection_Guide/ConfiguringSystemIntegrityProtection/ConfiguringSystemIntegrityProtection.html) That doesn't allow the editing of files in /usr/.
2. You have to add the Nano S to /usr/libexec/SmartCardServices/drivers/ifd-ccid.bundle/Contents/Info.plist

   > In <key>ifdVendorID</key> add the entry <string>0x2C97</string>
   > In <key>ifdProductID</key> add the entry <string>0x0001</string>
   > In <key>ifdFriendlyName</key> add the entry <string>Ledger Token</string>

   This 3 entries must be added at the end of each list.
3. [Enable SIP](https://developer.apple.com/library/content/documentation/Security/Conceptual/System_Integrity_Protection_Guide/ConfiguringSystemIntegrityProtection/ConfiguringSystemIntegrityProtection.html)

3.2.3 Windows

SmartCard service should be already installed. Maybe you have to start it.

Chapter 4

Nano S Monero application explained

4.1 Menu Overview

The full menu layout is :

Device Info
Settings
    Change Network
        It will reset the device
        Abort
        Test Network
        Stage Network
        Main Network
    Reset
About
    Monero
    (c) Ledger SAS
    Spec 3.0
    App 1.0.1

Emphasis entries are not selectable and just provide information.
A "#" after the entry label means default value on reset.
A "+" after the entry label means current value.

4.2 Device Info

The *Device Info* provides current user and slot information. The format is:

<Monero: public key >

4.3 Settings

4.3.1 Change Network

Change the network pairing of the application. Some version maybe locked to Test or Stage network.

4.3.2 Reset

Selecting the menu will erase all Monero Application data and will reset the application in its '*just installed*' state.

Chapter 5

Nano-S Monero Card application usage

5.1 Monero

The Monero application is intended to be used with monero-wallet-cli 0.12 on v7 network (March 2018 fork) Previous network are not supported and will be not. Next network version will be added on time.

Today, the following feature are supported:

- Creating
- Restoring wallet
- Send Funds
- Receive Funds
- Sub-address

So the following commands are NOT supported:

- **specific send:** – submit_transfer
  – transfer_original
- **import/export:** – import_key_images
  – export_key_images
  – import_outputs
  – export_outputs
- **multi-sig:** – make_multisig
  – prepare_multisig
  – export_raw_multisig_tx
  – sign_multisig
  – finalize_multisig

  - import_multisig_info
  - export_multisig_info
  - submit_multisig

- **proof generation** – get_reserve_proof
  - get_spend_proof
  - get_tx_proof

- **misc** – get_tx_key
  - sign
  - sign_transfer
  - verify

Those command are planned to be added in future versions

5.1.1 Creating/Restoring Wallet

Creating or Restoring a wallet in done in the same manner as key comes from the Device.

The basic command is `monero-wallet-cli --generate-from-device </path/to/wallet/directory>`

In practice, you never do this! Why? Because Monero is a special network in which all transactions are fully encrypted. That means the only way to know if a block contains a transaction for you is to decrypt that transaction. This implies decrypting the whole blockchain on the device. Impossible: TOO LONG!

So the best solution is to use the `--restore-height <height>` option.

When creating a new wallet you can just pass the last mined block height. As it is a new wallet, there nothing for you until that block.

When restoring a wallet you should pass the block containing your first input transaction or the one used at creation time.

Finally there a last option that should be used: `--subaddress-lookahead <Major:minor>`. By default when creating a wallet, the client pre-computes the first 200 addresses for the first 50 accounts 50:200. This setup take around 25 minutes. You can drastically reduce this time by using something like 10:50,

Finnally a suggested creation wallet is :

monero-wallet-cli –generate-from-device </path/to/wallet/directory> –restore-height <height> –subaddress-lookahead 10:50

5.1.2 Sending Funds

Use transfer normally and check your device to accept/reject fee, amount and destination.

Screenshots to come ...

Chapter 6

Annexes

6.1 References