

Blentity Data Protector with FIDO2 User Manual

Version 1.1 | Release in 2024.01



DOCUMENT CHANGE HISTORY

Date	Version	Change Description	Remark
2024.01.10	v1.0	First release	
2024.01.12	v1.1	Update the URLs	

Table of Contents

Preface

1. Product Information

- 1-1. Product Specifications
- 1-2. Partitions and "Blentity Manager"
- 1-3. Supported Environments
- 1-4. Names of Parts
- 1-5. Status LED List

2. How to Use

- 2-1. Precautions
- 2-2. FIDO-only Mode and Operation Mode
- 2-3. Install "Blentity Manager"
- 2-4. Initialization
 - 2-4-1. PIN
 - 2-4-2. Passphrase
 - 2-4-3. Initialization Steps
- 2-5. Passwordless Authentication
- 2-6. Partition Setup
- 2-7. Open Secure partition
- 2-8. Other Features of Blentity Manager
 - 2-8-1. Chang PIN
 - 2-8-2. Operation Mode Setup
 - 2-8-3. Factory Reset
 - 2-8-4. Language Setup
 - 2-8-5. Update

3. Troubleshooting

4. FAQ

5. Technical Support

Preface

Thank you for purchasing Blentity (known as SAMURAI Key in Japan). This document provides detailed usage instructions for the product. Before using Blentity, please read this document (please check for the latest version at https://wisecure-tech.jp/samurai_key/support) and the [Terms of Use](#) thoroughly to ensure proper and safe usage.

The contents of this document may change without prior notice. The most current version can always be found at https://wisecure-tech.jp/samurai_key/support. For updates or corrections, please consult this link. Should you identify any errors in this document, we encourage you to contact our support center.

Blentity and SAMURAI Key are trademarks of WiSECURE Technologies Corporation. Other company and product names mentioned here may be trademarks or registered trademarks of their respective owners.

Please note that the illustrations in this document may not exactly match the actual product. We continuously strive to improve our products, which may result in changes to their specifications without notice.

WiSECURE is not liable for damages resulting from improper use of Blentity, non-compliance with instructions in this guide, or repairs and modifications performed by unauthorized third parties.

This product adheres to the FIDO standard and functions as an authenticator for passwordless and multifactor authentication. Its compatibility with various services following the FIDO standard may differ and is subject to change.

Be aware that if you forget your PIN and Passphrase, access to stored data will be impossible. WiSECURE does not offer data recovery services, so we strongly recommend backing up important data regularly.

WiSECURE cannot assure uninterrupted or error-free operation of Blentity. Users bear the risk of non-compliance with product instructions or using the product with incompatible devices.

As Blentity does not connect to WiSECURE's device network, WiSECURE is unable to access or decrypt data encrypted or stored with this product, including authentication keys. Consequently, WiSECURE bears no responsibility for user actions with Blentity or for any loss or damage of data.

[Back to top](#)

Product Information

1-1. Product Specifications

Main Unit Specifications

Product Name	Blentity Data protector with FIDO2 (SAMURAI Key)
Compliance	FIDO2 Level 2, VCCI, CE, FCC
Interface	USB 3.2 Gen1
USB Connector Shape	Type C
Read/Write Speed (Maximum)	Read: 140MB/s Write: 45MB/s
Capacity	128GB
Format Type	exFAT, NTFS(Windows only)
Encryption Algorithm	Hardware-based AES XTS 256
Case Material	Plastic
External Dimensions	76 x 20.5 x 10 mm
Weight	13.6g

Adapter Specifications

Interface	USB 3.2 Gen1
Input Shape	Type C
Output Shape	Type A
Case Material	Plastic
External Dimensions	37.5 x 20.5 x 10 mm
Weight	5.6g

Note:

- Part of the storage capacity of this product is allocated for system use; therefore, the advertised storage capacity does not reflect the total usable space available to the user.
- The stated maximum transfer speed is based on tests conducted in our company's controlled environment. Actual speeds may vary depending on your specific setup and operating conditions.
- Please note that both the specifications and the physical appearance of the product are subject to change without prior notification.

[Back to top](#)

1-2. Partitions and Blentity Manager

The product has a total storage capacity of 128GB, divided into three main parts: the system partition, secure partition, and plaintext partition.

System Partition

Default configuration, only read is supported.

Contents include:

- Blentity Manager: A full-featured management tool that requires installation. For initialization, refer to "Install Blentity Manager".
- Blentity Manager Lite: A lite version of Blentity Manager that does not require installation and can be quickly accessed on non-personal computers.
- User Manual (PDF): Provides detailed product guidelines and instructions.

Secure Partition and Plaintext Partition

After initialization, users can configure the capacity of these two partitions and format them using Blentity Manager. Refer to "Partition Setup" for setup.

Secure partition: Provides hardware-based data encryption (AES 256 XTS) for securing sensitive data, accessible only after successful PIN verification in Blentity Manager.

Plaintext Partition: Suitable for general data storage and quick access, accessible in easy mode based on operational mode.



Warning

Configuring partitions will delete all data and cannot be restored. Ensure you back up important data before transferring or formatting.

The system partition does not support writing; do not attempt to change its contents.

The two management tools cannot be used simultaneously.

[Back to top](#)

1-3. Supported Environments

Partitions and Management Tool Execution Environment:

Recommended Computer Specifications

- Computers with USB 3.0 interfaces
- Minimum 8GB of RAM

Supported Operating Systems

Windows	Windows 10 (ver 21H2) and later
macOS	Ventura and later

Caution

- Operations via USB 3.0 cards or USB hubs are not guaranteed.
- Please use the latest version of each host controller driver.
- Windows RT, Starter Edition, Embedded, and Mobile are not supported.
- Due to the nature of the product, we cannot guarantee operation in all environments and device combinations.

FIDO Authentication Function Execution Environment

The authentication services provided by this product require the following FIDO2 supported browsers: Microsoft Edge, Mozilla Firefox, Google Chrome, Apple Safari. For the latest supported list, please visit the [FIDO Alliance official website](#).

Recommended Execution Environment:

Windows	Chrome, Edge
Linux	Firefox
macOS	Safari

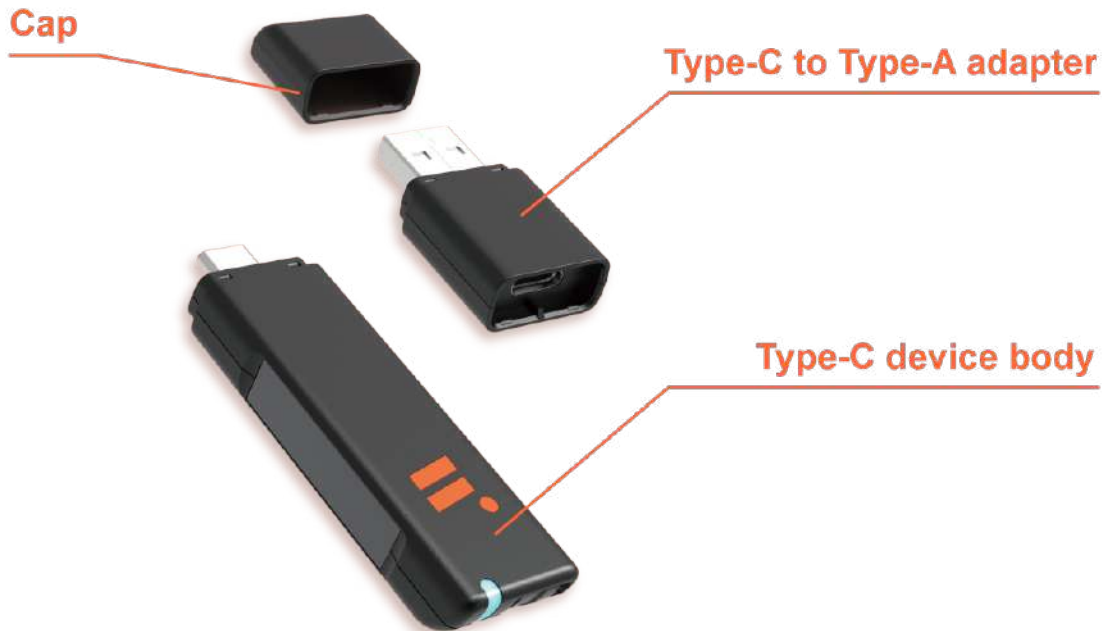
Caution

- Before using the FIDO authentication function, please complete the [initialization](#) process.
- When using FIDO functions on a Mac, please close all the Blentity Manager. This will ensure the function operates correctly.

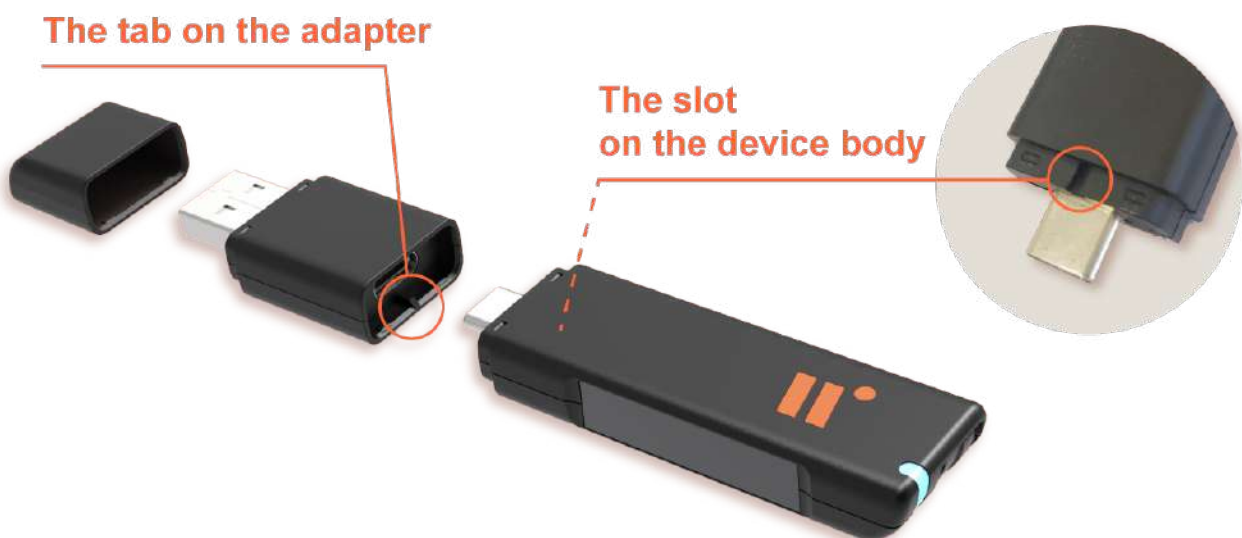
[Back to top](#)

1-4. Names of Parts

Main Components



This product supports USB 3.0 data transfer speeds for efficient operation. To maintain these speeds, it is essential that the main body of the device and the adapter are connected in the correct orientation. Please carefully align the notch on the adapter with the groove on the device body to ensure a proper fit. An incorrect orientation will not allow a successful connection and may impede the device's performance.





① Touch area

The metal areas on both sides of the body are equipped with touch sensors. When logging in, gently touch these metal areas with your finger as instructed to ensure that the authentication is being performed by a real person, not remotely or by a robot. This mechanism is not fingerprint recognition and does not record any biometric data.

② Status LED

Various device statuses, such as locking and unlocking the secure partition, are indicated through LED signals. Refer to the [1-5. Status LED List](#) for more details.

③ Bottom slide switch

When the switch is on (orange color visible), the disk operation mode (Operation mode) is activated. In this state, based on the relevant settings, you can directly operate the device to access partitions.

When the switch is off, the device enters the FIDO-only mode. For more details, refer to the sections on [2-2. FIDO-only mode and Operation Mode](#).

④ Lanyard Hole

To prevent loss of the device, it can be carried using a lanyard.

[Back to top](#)

1-5. Status LED List

The following is ordered from highest to lowest priority according to the status indicators.

LED Status	Product Status
Solid White	Device is powered on
Solid Red	Not initialized, PIN locked, or device error
Red Blinking	Partition opening or waiting for touch
Solid Green	Secure partition is unlocked
Green Blinking	File access within the secure partition is in progress
Blue Blinking	Normal standby state (when no partitions are open)
Purple Blinking	Normal standby state (other partitions except for the secure partition are open)

Handling Solid Red Light Status

- If the device has not been initialized, please refer to [2-4. Initialization](#) to learn more.
- If the PIN is locked, open Blentity Manager and follow the guide at the top of the homepage to enter your Passphrase and reset the PIN.
- If the red light remains solid after excluding these two factors, it indicates a device malfunction. Please refer to other troubleshooting methods or contact the support center for assistance.

[Back to top](#)

2. How to Use

2-1. Precautions

Please read the following carefully before use.

The following cautions and warnings include information to prevent harm to users and third parties, as well as property damage.

Please understand and follow instructions.

Warning

This item indicates that if the content in this category is ignored and mishandled, there is a risk of death or serious injury.

Do not use if smoking, odor, or unusual sounds occur

If smoking, emitting odors, or making unusual sounds, immediately remove the product from the computer.

Using it under abnormal conditions may result in malfunctions, fires, electric shocks, and damage to the connected computer.

Do Not Disassemble Or Modify

Do not disassemble or modify the device, as it may cause malfunctions, electric shocks, fires, and damage to the connected computer. If inspection, adjustment, or repair is needed, please contact our support center.

Avoid Device Contact With Water

If water enters the device, promptly remove it from the computer.

Using it in wet conditions may result in malfunctions, fires, electric shocks, and damage to the connected computer.

Avoid Use In Specific USB Ports

Avoid using in USB ports that support power banks or fast charging, as it may cause malfunctions and damage to the connected device.

This Product Contains Precision Parts; Please Be Mindful Of The Following:

- Avoid dropping or applying heavy impact.
- Do not eat, smoke, etc., near the product during use.
- Do not forcibly bend, twist, bind, or clamp the interface.
- Do not place heavy objects or the device body on the interface.
- Do not damage the interface with staples, nails, etc.
- Do not forcefully insert into incompatible sockets or interfaces.
- Do not place the product where it may be stepped on may cause injury.

Do Not Touch The Device With Wet Hands

Avoid touching the device interface with wet hands, as it may result in electric shock, malfunctions, or damage to the connected computer host.

Stop using if you experience any abnormal conditions

If your body experiences any abnormal reaction, please immediately cease using this product and consult a doctor.

Depending on the plastic materials used in the device, it may cause itching and allergic reactions.

Do not allow children or pets to use

Keep children and pets away from this device.

Ingesting small parts could lead to injury.

 **Caution**

This item indicates that if the content in this category is ignored and mishandled, there is a risk of injury or property damage.

Regarding Product Placement, do not store or use this product in the following locations:

- Places subject to vibration or impact
- Areas exposed to direct sunlight
- Humid or dusty environments
- Areas with significant temperature variations
- Proximity to heat-emitting objects (such as stoves, heaters, etc.)
- Near objects emitting strong magnetic waves
- (such as magnets, displays, speakers, radio transceivers, etc.)
- Humid locations (kitchens, bathrooms, etc.)
- Areas with corrosive gases in the atmosphere
- (Cl₂, H₂S, NH₃, SO₂, NO_x, etc.)
- Locations with severe static electricity interference

Storage Method For Long Periods Of Non-use

When not using this product for an extended period, please remove it from the computer and cover it with the cap for proper storage.

When Moving Inserted Devices

When inserted into a device, such as a computer, please remove this product from the computer. It may cause malfunctions while plugged into a moving device.

Please Be Aware Of Static Electricity

Exercise caution regarding static electricity when in contact with this product. This product is a precision electronic device, and applying static electricity may result in product malfunctions.

[Back to top](#)

2-2. FIDO-only mode and Operation Mode

This product can switch between the following two modes via the Bottom slide switch:

Operation Mode

The mode as the bottom slide switch is on (showing orange color)

In this mode, you can open System Partition and Plaintext Partition after operating the device according to [the settings of Operation Mode](#).

FIDO-only mode

The mode as the bottom slide switch is off.

In this mode, any operation on the device (inserting into a computer, long-pressing the Touch area, etc.) will not open the partitions. This prevents partitions from popping up during authentication, which could interfere with the login process.

After switching modes, please unplug and replug the device for the new mode to take effect.



Both modes require Blentity Manager to [open the secure partition](#).

[Back to top](#)

2-3. Install "Blentity Manager"

For first-time use, please follow the steps below to install Blentity Manager in the system partition to proceed with the initialization process.

The steps for first-time use are as follows:

1. Confirm that the Bottom slide switch on the product is turned on (orange visible).
2. Insert into computer, press and hold the Metal areas on both sides of the device for about 3 seconds to bring up the system partition.
3. Install Blentity Manager from the partition. Upon opening, it will automatically guide you through the initialization process.

Installation file paths in the system partition named BLENTITY:

For Windows user:

Windows > Manager Installer.exe

For Mac user:

Mac > Manager Installer.pkg

[Back to top](#)

2-4. Initialization

Before initializing, please install Blentity Manager. After opening Blentity Manager, follow the guide to create a PIN and a Passphrase.

2-4-1. PIN

PIN is a protective mechanism for this product. Even if the device is lost or stolen, it cannot be used without PIN.

Setting PIN

You can set a PIN of 8 to 63 characters, including upper and lower case letters, numbers, and symbols.

Using PIN

You will need to enter your PIN to perform FIDO authentication, unlock the secure partition, and use certain features of Blentity Manager.

Changing PIN

You can change it at any time through "Settings > Change PIN" in Blentity Manager (full version).

Locking and Unlocking PIN

If the PIN is entered incorrectly 8 times, or if an attempt is made to change the PIN using a non-official management tool for this product, the PIN will automatically lock. In this case, the status LED will show a solid red light. Please open the Blentity Manager, use the Passphrase to unlock and reset the PIN.

2-4-2. Passphrase

The Passphrase is a mechanism widely adopted in encrypted asset wallets, based on the industry standard "BIP39." During the initialization of this product, 12 random English words are generated as the Passphrase, used for the secure recovery of the master key of the device.

When would you use the Passphrase?

To unlock and reset PIN

If PIN entry exceeds the limit or is locked, you can enter this Passphrase to unlock and reset PIN.

To restore encrypted backup files (this feature will be available in the future)

If the device is lost, you can use this Passphrase on a new device to recover your master key (the key that can derive encryption keys), making it easy to restore your encrypted backup files on another device.



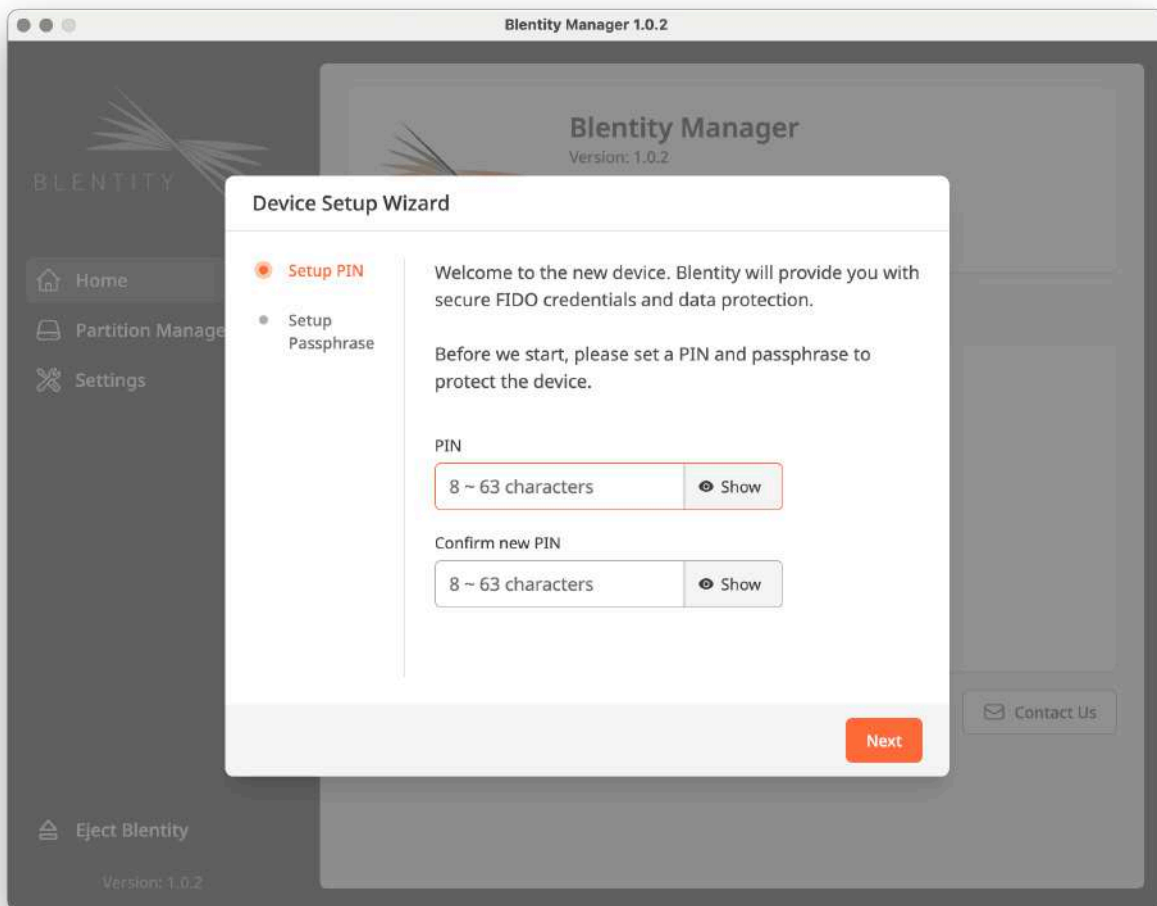
Warning

- Please remember or securely store your Passphrase (a writable paper card is included in the product packaging).
- If the wrong Passphrase is entered 8 consecutive times, **the device will be forcibly restored to factory settings, and all data will be deleted.**
- If you forget your Passphrase, it is recommended to back up your data first, then restore the device to factory settings and establish a new Passphrase.

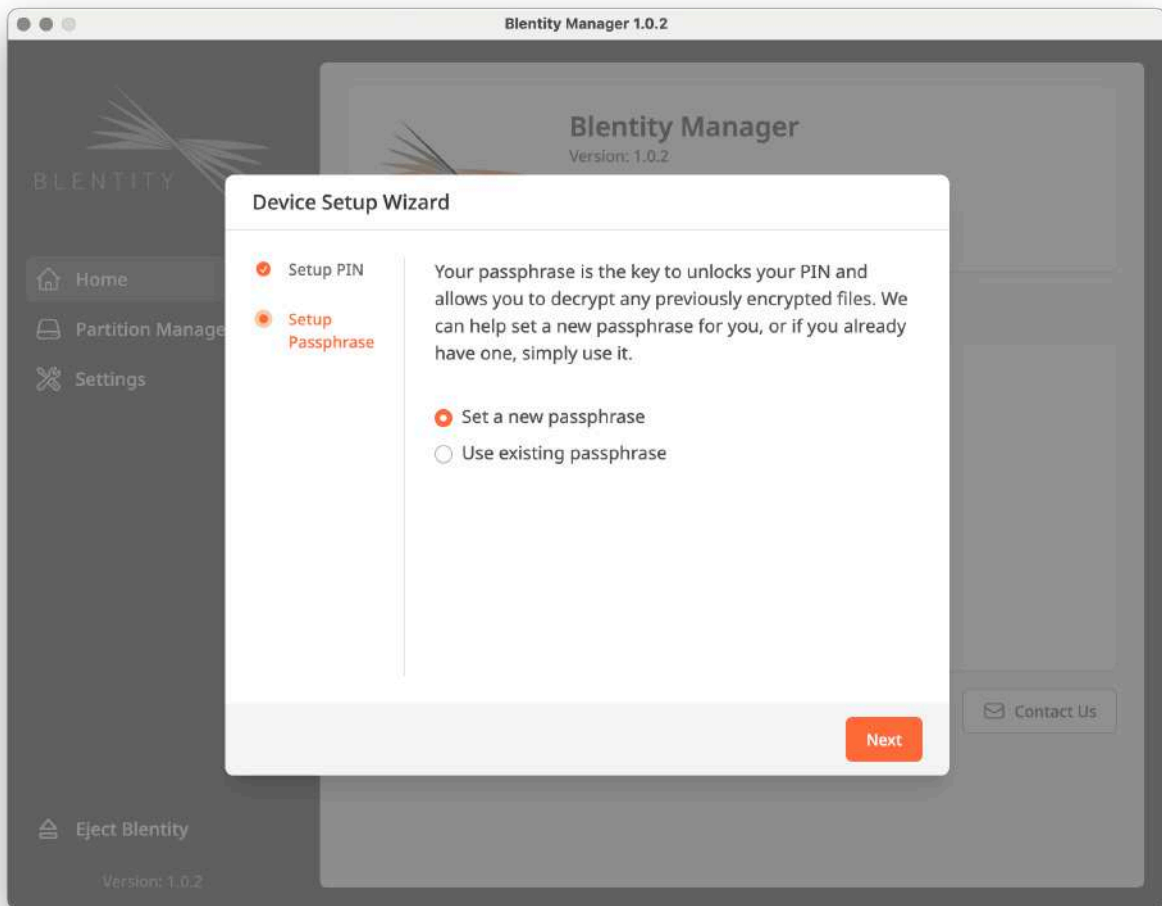
2-4-3. Initialization Steps

Before initializing, please install the management tool “Blentity Manager”. During initialization, Blentity Manager will automatically guide you through setting up PIN and Passphrase. Below is the reference process.

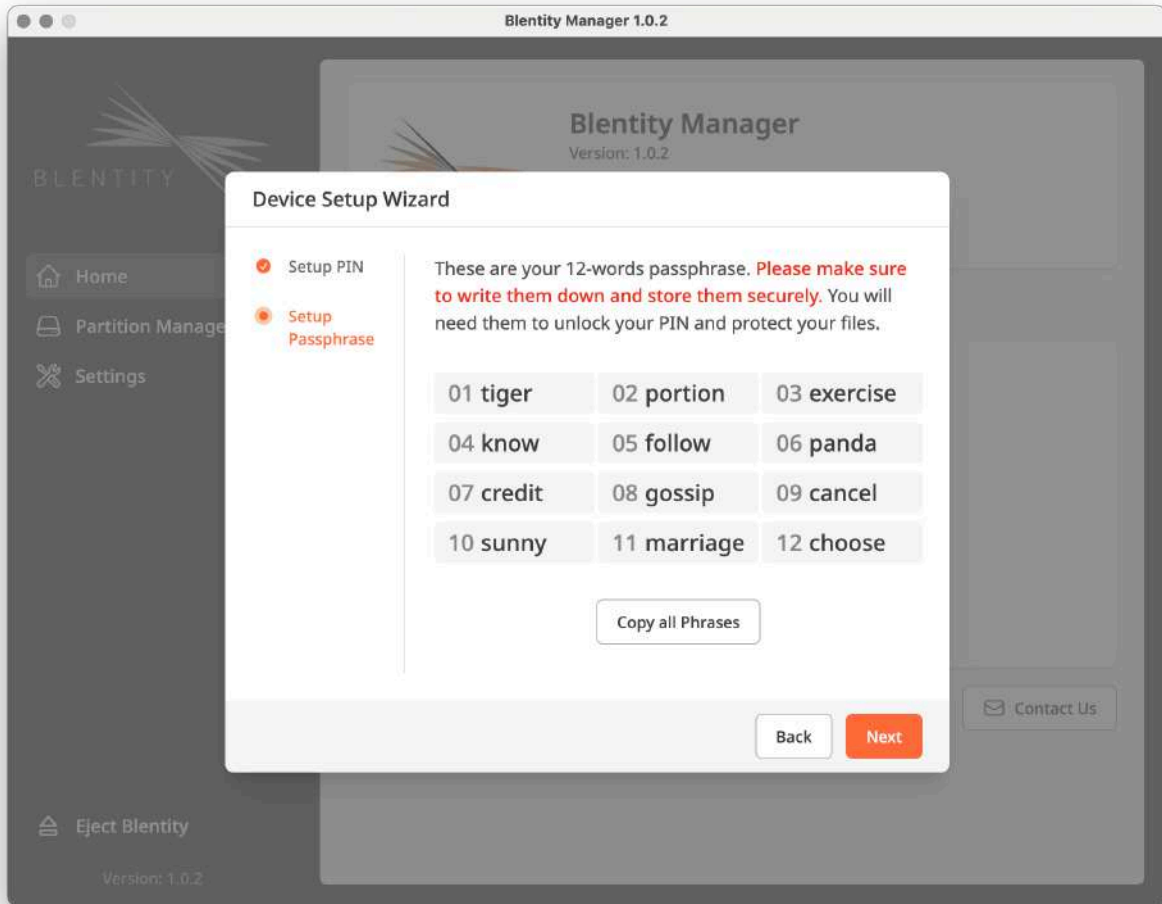
1. As mentioned on the following page, please start by creating a PIN.



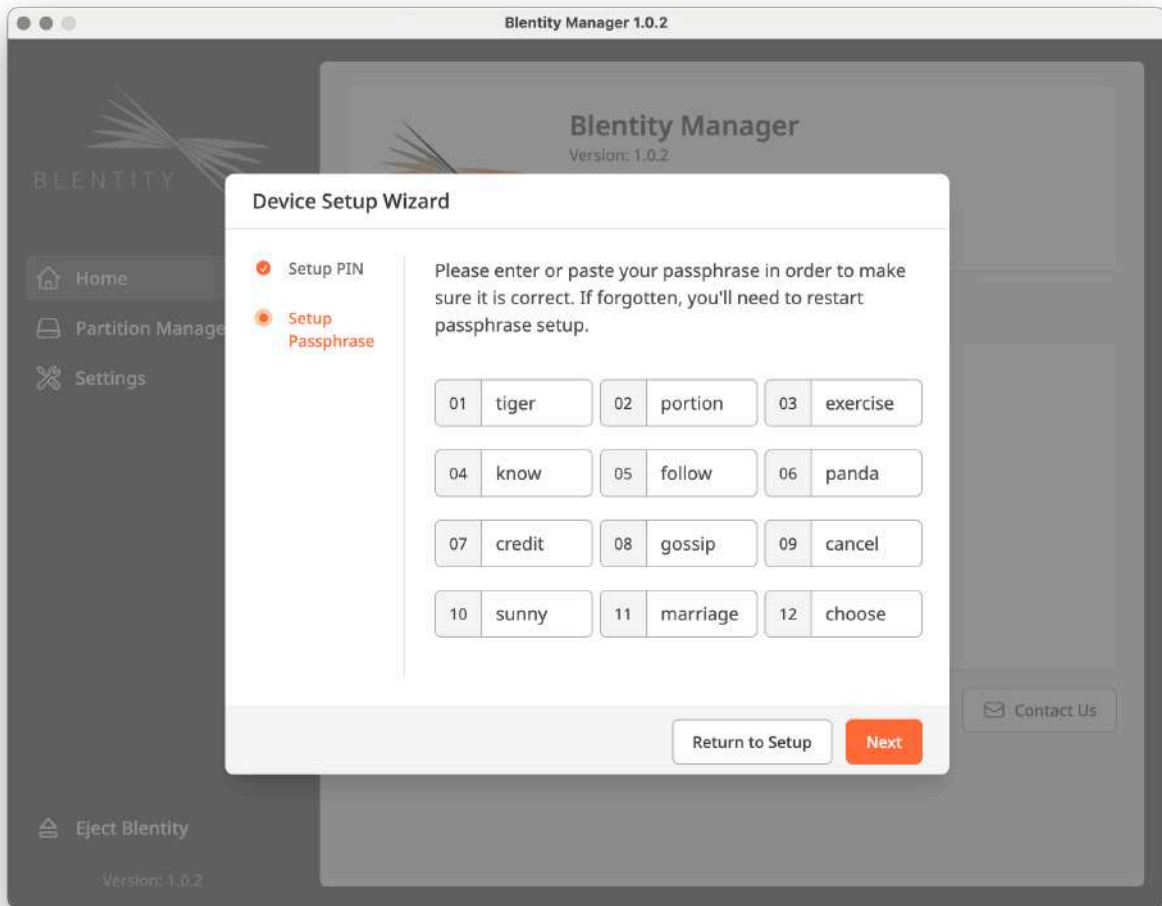
2. After creating PIN, click on the next step, where you will choose to obtain a new Passphrase or use a previously backed-up Passphrase.



3. After choosing to obtain a new Passphrase, a 12-word Passphrase will be automatically generated. Remember, copy, or write this down and keep it in a safe place. On the next page, you will need to enter the Passphrase in the correct order to confirm; you can also copy and paste it directly from this page.



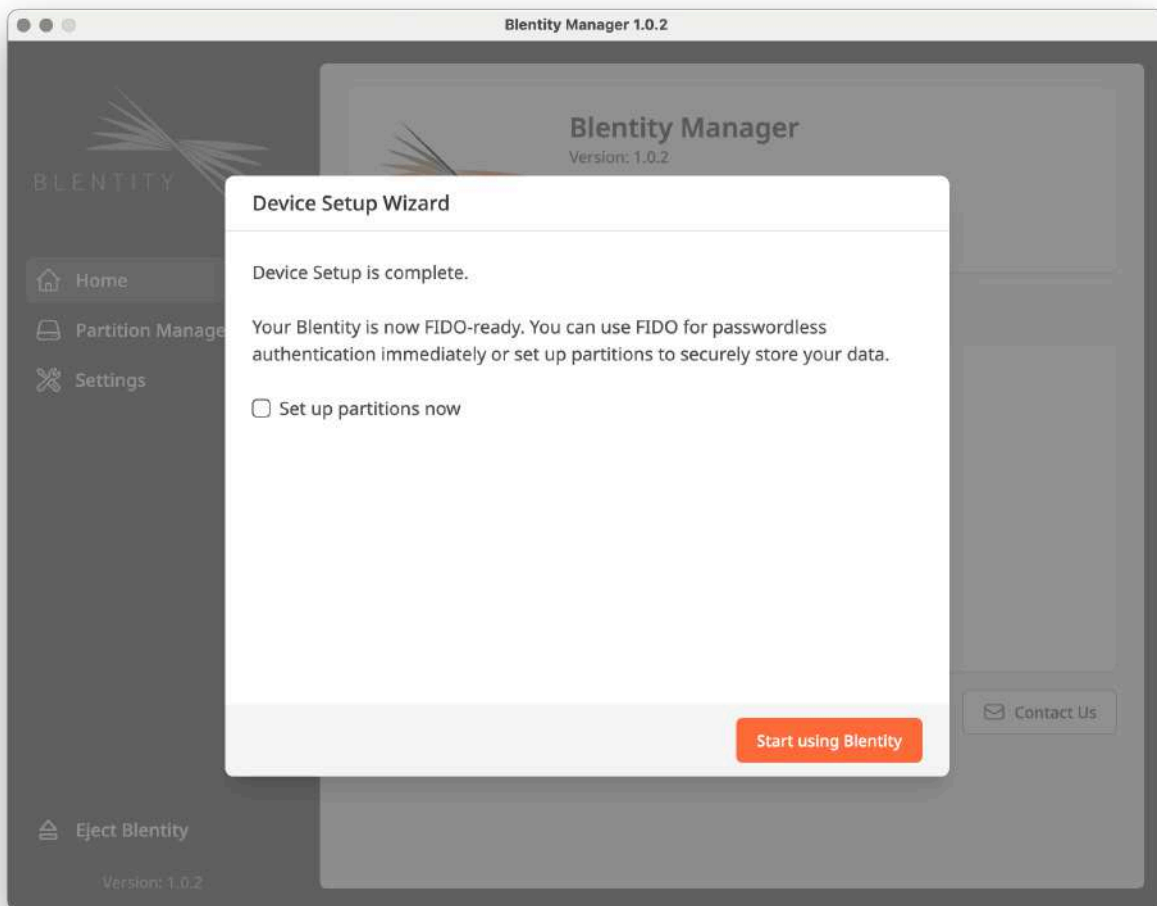
4. On this confirmation page, past or enter the Passphrase and then click on the next step to begin the generation of the keys. Once the keys are generated, the initialization process is complete.



After initialization, you can perform the following operations:

Start Using FIDO Authentication Features

After the initial setup, you can start using the FIDO authentication feature of this product to achieve more secure and simple account protection in services that support FIDO. Please refer to "[2-5. Passwordless Authentication.](#)"



Set up partitions

Once the initial setup is complete, you can choose to immediately proceed with setting up the partitions. After configuring the capacity and format of the encrypted and plaintext partitions, you can begin using the data storage function.



Caution

If the disk partition has not been configured, it remains unformatted. Therefore, even if you click the "Open Encrypted Partition" button and enter the correct PIN, the encrypted partition will not be visible. Please go to "Partition Management > Partition Setup" to set it up.

2-5. Passwordless Authentication

The authentication services provided by this product require the following FIDO2 supported browsers: Microsoft Edge, Mozilla Firefox, Google Chrome, Apple Safari. For the latest supported list, please visit the [FIDO Alliance official website](#).

Recommended Execution Environment:

Windows	Chrome, Edge
Linux	Firefox
macOS	Safari



Caution

- Before using the FIDO authentication function, please complete the [initialization](#) process.
- When using FIDO functions on a Mac, please close Blentity Manager. This will ensure the function operates correctly.

After registering and binding the security key, you can sign in more securely using the designated PIN and physical security key. Please refer to the operating instructions for various services that support FIDO2.

Example: To add a security key as a sign in method for your Microsoft account

1. Go to the [Microsoft account page](#) and sign in as you normally would.
2. Select [Security] > [More security options].
3. Select [Add a new way] to sign in or verify.
4. Select [Use a security key].
5. Identify what type of key [USB] and select [Next].
6. You will be redirected to the setup experience where you will insert or tap your Blentity.
7. Enter an existing PIN (if you haven't created one, please [initial your device](#) by Blentity Manager first).
8. Touch the touch area of Blentity.
9. Name your Blentity so that you can distinguish it from other keys.
10. Sign out and open Microsoft Edge, select Use Windows Hello or security key instead, and sign in by inserting or tapping your key.

To learn more about managing and deleting a security key on Microsoft, please visit the [Microsoft official support site](#).

[Back to top](#)

2-6. Partition Setup

Before using the data storage function of this product, capacity allocation and formatting must be done through Blentity Manager in "Partition Management > Partition Setup". Both the encrypted partition and the plaintext partition can be configured.



Caution:

This operation requires administrator rights on the computer.



Warning:

This operation **will erase all data** within the partition, and it is irreversible. Be sure to back up your data beforehand.

Instructions:

1. Go to "Partition Management > Partition Setup".
2. Allocate capacity for the encrypted partition and the general plaintext partition.
3. Set the partition name. This setting is limited to uppercase letters; you can change the partition name at any time in your computer's file manager (such as Windows' "File Explorer" or Mac's "Finder").
4. Choose the file system format. This product supports exFat and NTFS (Windows-only).
5. If a warning appears about the disk being unreadable, choose [Ignore].
6. Follow the system prompts to enter the administrator password for the computer.
7. Once the Partition Setup is complete, **remove the device and then reinsert it.**

How to Use the Partition:

Please refer to "[2-7. Open Secure Partition](#)" and "[2-8-2. Set Operation Mode](#)".

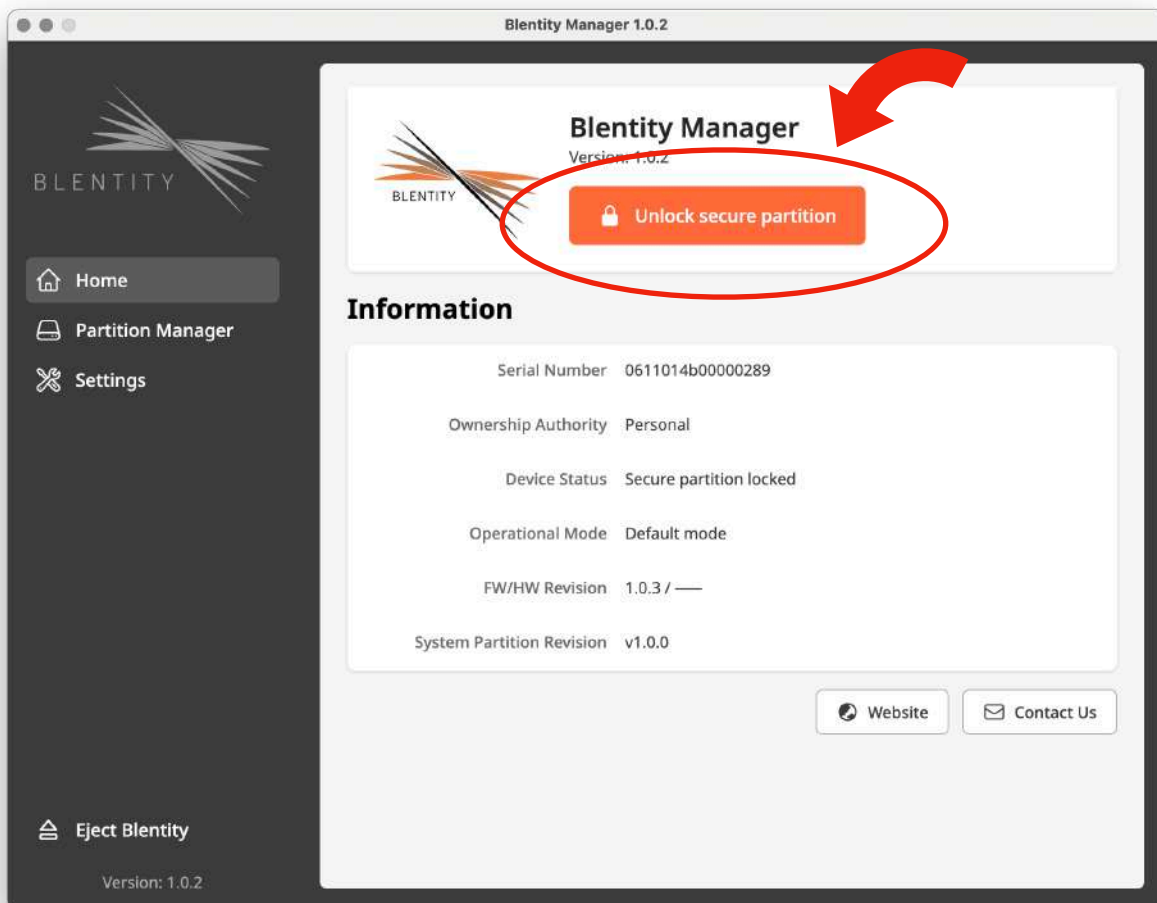
[Back to top](#)

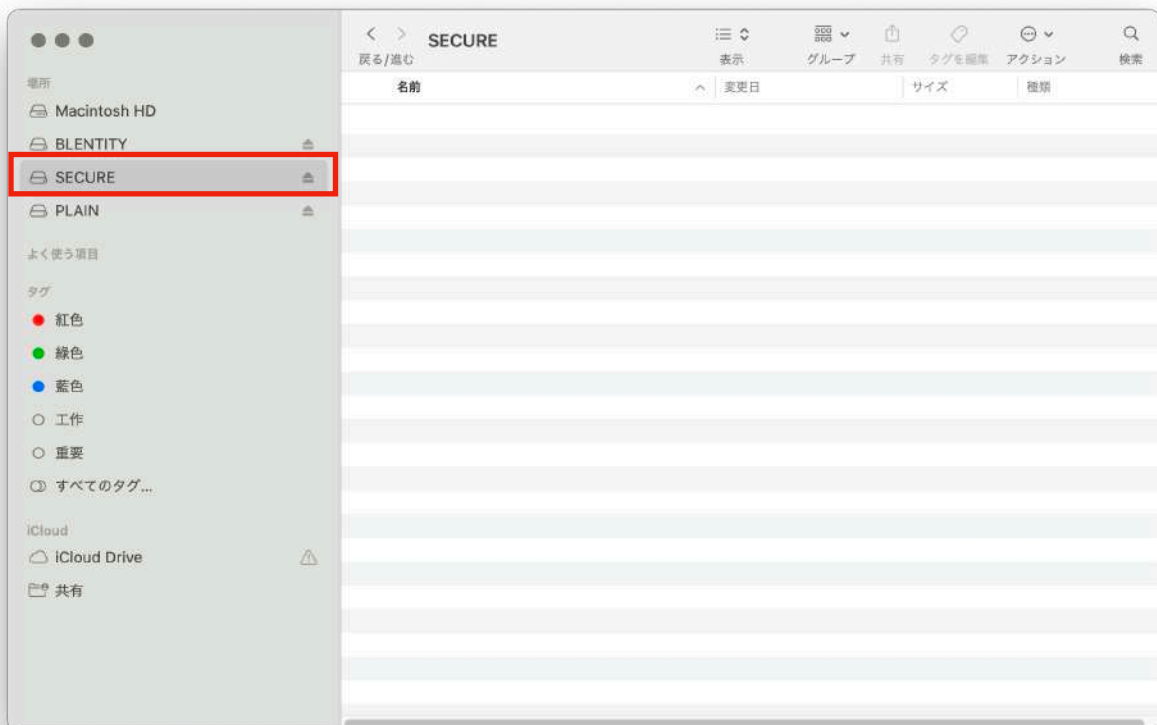
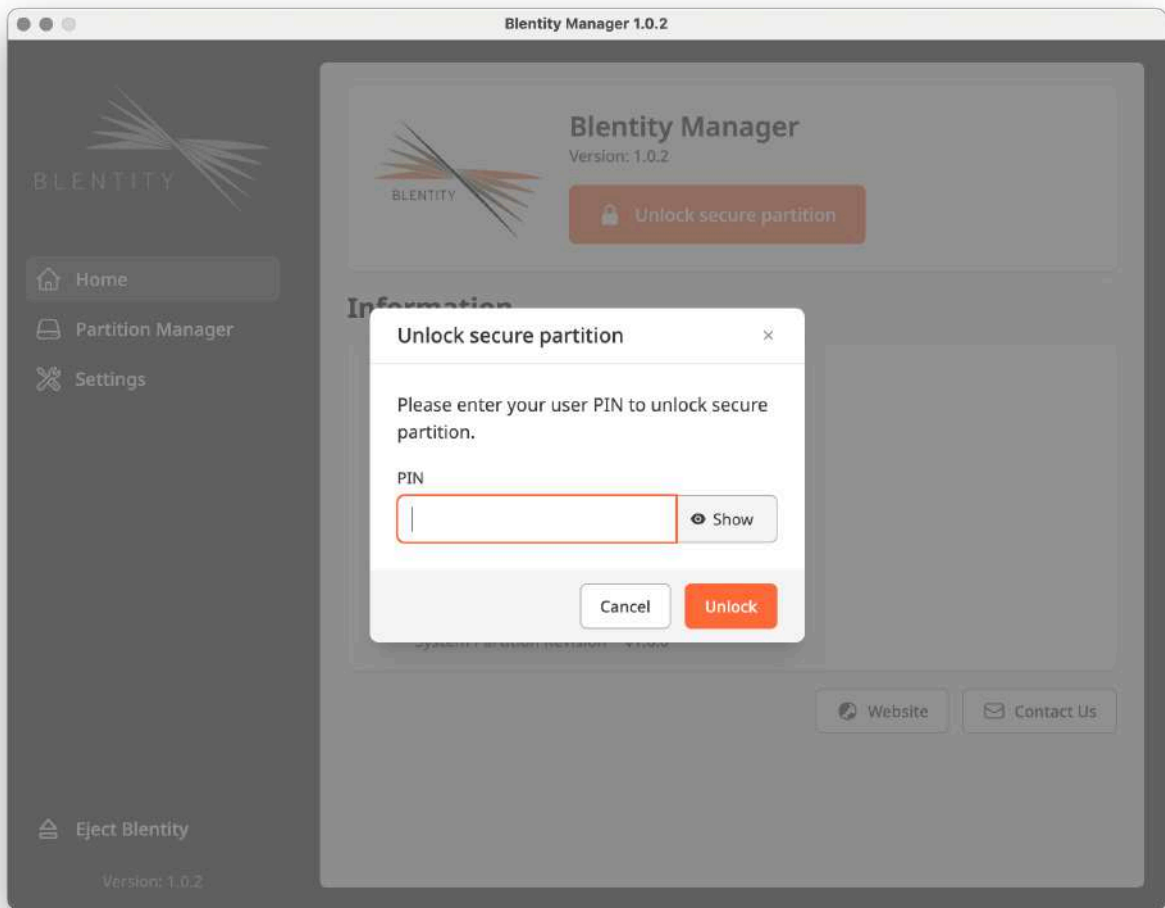
2-7. Open Secure partition

Blentity provides the following two methods to access the secure partition:

Using Blentity Manager

Click [Unlock secure partition] on the homepage of Blentity Manager (full version). After entering PIN, the secure partition will be opened.

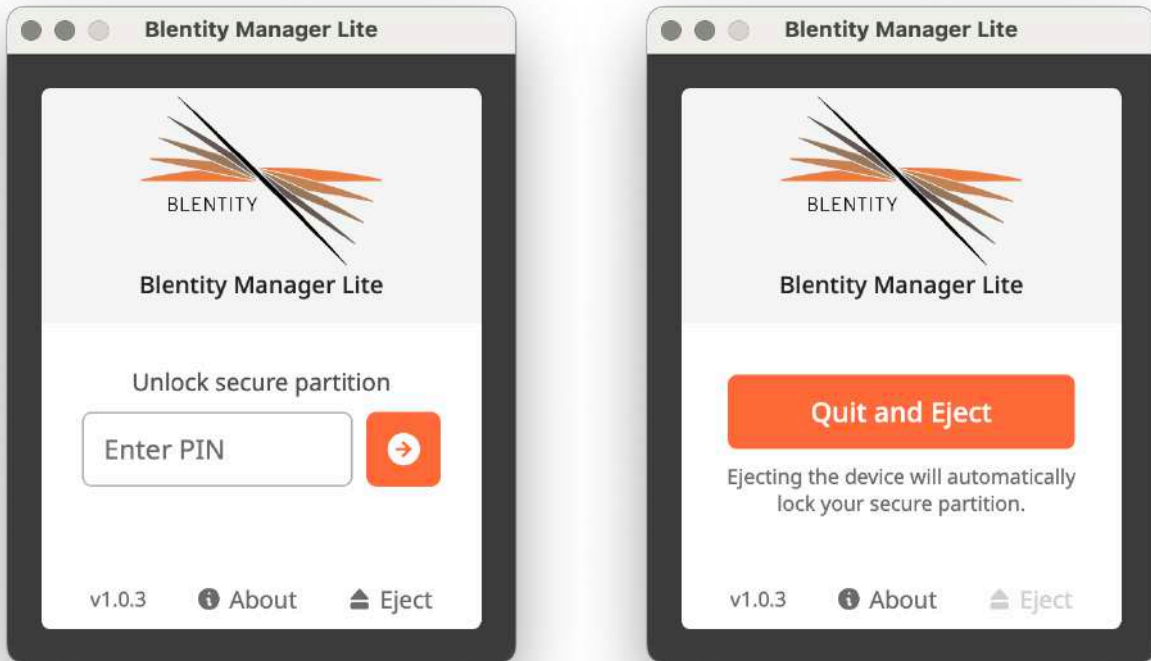




Using Blentity Manager Lite

In operation mode, open the system partition, click on Blentity Manager Lite and directly enter PIN to open the secure partition.

After using the secure partition, you can click [Quit and Eject]. The secure partition will be locked, the device will be safely ejected, and the program will end.



[Back to top](#)

2-8. Other Features of Blentity Manger

2-8-1. Chang PIN

Change PIN under "Settings > Change PIN".



Caution

If you change PIN using a third-party tool other than Blentity Manager, your PIN would be locked. You must reset PIN by the passphrase through Blentity Manager.

2-8-2. Operation Mode Setup

When the Bottom slide switch is on (showing orange color), the product enters "Operation Mode," where you can operate and access the system partition and the plaintext partition. Set this under "Settings > Operation Mode Settings".

Blentity offers the following three operation modes:

Default Mode

No partitions will open when the device is connected. Hold the Touch area on the sides of the device for about 3 seconds to open "System Partition and Plaintext Partition." Hold for another 3 seconds to close all partitions.

System-only Mode

The "System Partition" opens automatically when the device is connected.

Easy Mode

The "System Partition and Plaintext Partition" opens automatically when the device is connected.

	System Partition (RO)	Plaintext Partition (RW)	Secure Partition (RW)
Default Mode	Closed by default; opened when held for 3 seconds*.	Closed by default; opened when held for 3 seconds.	Closed by default; opened upon app authentication
System-only Mode	Opened by default*.	Always closed.	
Easy Mode	Opened by default.	Opened by default*	

Operation mode for partitions

*means the bottom slide switch must be on

RW : Read / Write

RO : Read Only

2-8-3. Language Setup

The product offers interfaces in Chinese, English, and Japanese. Adjust this in "Settings > Language Setup".

2-8-4. Factory Reset

This function will reset the product to its factory uninitialized state. Perform this operation under "Settings > Factory Reset".



Warning

This operation will **clear PIN, Passphrase, all credentials, authentication information, and data, and cannot be reversed**. Please be sure to back up your data beforehand.

2-8-5. Update

The product can be updated through Blentity Manager to ensure the best quality and experience.

Preparation Before Update

- Make sure the network connection is normal.
- Be sure to back up your data beforehand.



Warning

This operation **may clear all data within the partition and cannot be reversed**. Make sure to back up your data beforehand.

Update Steps

1. Insert the device into a computer that meets the specifications.
2. Open Blentity Manager(full version) and wait about ten minutes for the update file to be retrieved. Removing the device during this process will interrupt the retrieval.
3. Once retrieved, the Manager will display an update button at the bottom of the homepage or under "Settings > Update". Click to complete the update.

[Back to top](#)

3. Troubleshooting

If you encounter any of the following problems, please refer to the corresponding solutions.

Device Not Recognized by Computer

Connect the device directly to the computer's USB port, not through a USB hub.

After connecting, check if the status LED lights up.

Ensure the USB 3.0 port is securely connected and undamaged.

If the USB 3.0 interface card driver is outdated, please update it to the latest version.

Files Corrupted After Resuming from Sleep, Standby, or Hibernate Mode

Before entering sleep, standby, or hibernate mode in Windows or Mac, save your files and unplug the device to avoid corruption of files being accessed.

Forgotten PIN or Unable to Verify Successfully

- First, check for typing errors.
- If PIN is forgotten or entered incorrectly more times than the limit, it will be locked. In this case, use the Passphrase generated during initialization to reset PIN.
- If you have changed the FIDO PIN using a non-Blentity Manager tool, the PIN will be locked. If this occurs, open Blentity Manager and follow the instructions to reset PIN.

Encrypted Partition Not Found in Slot

Please ensure that initialization and formatting of the encrypted partition are complete.

After initialization, if formatting is not done, the encrypted partition will not be visible in the slot even after the correct unlock operation. Kindly go to 'Partition Management > Partition Setup' to allocate and format the space.

Screen Stops When Unlocking PIN with Passphrase

The key derivation process after entering the Passphrase takes about 10 seconds, which may vary depending on your computer. Please wait patiently. If the wait exceeds one minute, please contact the support center.

[Back to top](#)

4. FAQ

Q: Is mobile device support, Windows Server, or Linux OS available?

A: These operating systems are not within our support range. If you use this product with these systems, you do so at your own risk. For supported operating systems and browsers, please refer to "[1-3. Supported Environments](#)."

Q: Is software installation required?

A: Installation of the full-featured management tool is necessary for initialization. After initialization, the secure partition can be accessed through the Blentity Manager Lite. The product can be used on computers where the tool is not installed.

Q: What should I do if I forget my PIN?

A: If you forget the PIN, you can unlock it using the 12-word Passphrase generated during initialization. If the Passphrase is also lost, data loss will result, so it's very important to back up data regularly and store the Passphrase securely.

Q: What happens if I enter the wrong PIN repeatedly?

A: If the wrong PIN is entered 8 consecutive times, it will automatically lock, and you will need to use the Passphrase to unlock it. After successful unlocking, you can use it normally again.

Q: Can I change the PIN?

A: Yes, you can change the PIN in [settings > change PIN] without affecting the data already stored.

Q: Will the device automatically lock if not operated for a certain time?

A: This product does not have an auto-lock feature. When leaving, please unplug the device or unmount the secure partition.

Q: If used with Azure AD, will Windows automatically lock when the device is removed from the PC?

A: It will not automatically lock. You only need to use the device during login and can safely remove it afterward.

Q: Why is the number set different from the number displayed?

A: The disk space set may be "larger" than the space displayed on the security partition. This is because 1GB equals 1024MB, and if your set value is not divisible by 1024, this remainder will not be accounted for during the setting but will eventually be allocated to the secure partition. Therefore, the secure partition will be larger than the set value after configuration.

Q: Is it a concern that Blentity is categorized as Passkeys in certain browsers when utilized as sign in method for a Google account?

A: When registering Blentity on Edge and Chrome, it is identified as Passkeys, while on Firefox, it is recognized as a FIDO2 security key. However, you can successfully sign in

regardless of the browser used for registration. User experience remains consistent across all platforms.

For more FAQs, please refer to the product support page:

<https://wisecure-tech.jp/products/samurai-key/support/>

[Back to top](#)

5. Technical Support

Warranty

This product comes with a 1-year warranty service starting from the date of purchase. Warranty service cannot be provided for damages and malfunctions caused by abnormal use. If the product is damaged upon arrival, please contact us immediately for a replacement (excluding damaged packaging).

To assert your rights, please visit <https://wisecure-tech.jp/warranty>

Technical Support

Please submit problems through the "Contact Us" within Blentity Manager; the mail will automatically include the product serial number and version information. If it is beyond the warranty period, a quote will be provided based on the repair needs. Additionally, your authentication information and data may be at risk of deletion during repair and inspection, so please back up in advance.

Support Center

WiSECURE Technologies Corporation

Product Support Page: <https://wisecure-tech.jp/products/samurai-key/support/>

Customer Service Email: info@wisecure-tech.jp (Please contact us through the "Contact Us" feature within Blentity Manager to ensure we can quickly access your device information.)

Office Hours: 10:00—17:00, Monday to Friday (excluding holidays)

[Back to top](#)

Blentity Data Protector with FIDO2

User Manual

Version 1.1 | Release in 2024.01

S