# User Manual

## IronKey Keypad 200

Find the language and latest documentation here.

# KEYPAD 200

## User Manual


Remember to save your PIN in a safe place. If lost or forgotten, there is no way to access the Kingston® IronKey™ Keypad 200.

If you are having difficulty, please refer to this complete user manual loaded on your Keypad 200 (KP200) which is also available at: www.kingston.com/IKKP200

# Table of Contents

# Introduction

Note: The KP200 rechargeable battery is not fully charged, we recommend the battery be charged prior to first use. Please plug in the KP200 to a powered USB port for 30-60 minutes to fully charge the battery.

Thank you for purchasing the IronKey KP200, an ultra-secure and easy to use, hardware encrypted USB 3.2 Gen 1 PIN activated flash drive.

The KP200 is designed to be FIPS 140-3 Level 3 (certification pending). This is a high-level US government accreditation and means the product has passed numerous tests relating to the encryption algorithm and tamper-evidence as well as to thwart attacks directed at the Critical Security Parameters.

The KP200 uses military grade AES-XTS 256-bit hardware encryption, which encrypts all data stored on the drive in real-time. The KP200 requires no software and is OS and host independent.

The KP200 incorporates a rechargeable battery allowing the user to enter a 8-15 digit PIN (Personal Identification Number) onto the on-board keypad before connecting the drive to a USB port.

Should the drive be lost or stolen, the user can rest assured that all data held on the KP200 is safe and cannot be accessed by any unauthorized person.

The KP200 can be configured with both a User and Admin PIN, making it perfect for corporate and government deployment. As the KP200 is unlocked via the onboard keypad and not a host computer, it is not vulnerable to software/hardware based keyloggers or brute force attacks.

## 1. KP200 Layout


1. Protective sleeve.
2. Keyring- Unscrew to add to keyring.
3. LED lights- RED- Locked. GREEN- Unlocked. BLUE- Connected to the computer/data transfer/ Admin PIN indicator/User PIN change.
4. Polymer coated, wear resistant, alphanumeric keypad.
5. Epoxy coated- All critical components are covered by a layer of super tough epoxy resin.
6. On-device crypto chip.
7. Key button.

## 2. LED Indicators and Their Actions

| LED | LED State | Description | LED | LED State | Description |
|---|---|---|---|---|---|
| | Solid RED and blinking GREEN and BLUE | Initial shipment state, first time User PIN creation. | | Solid RED and blinking GREEN | Reset Drive awaiting User PIN configuration |
| | Red- fade Out | Locking down/incorrect PIN entry | | Red and Green blinking alternately | Factory reset/deleting files in Admin mode |
| | Red blinking | Locked and awaiting User PIN entry | | Red and Green flickering together | Awaiting Admin PIN entry |
| | Green solid | Drive is unlocked in User mode | | Green and Blue blinking together | User settings mode |
| | Green blinking | When connected to a USB port if Green Led blinks every 2 seconds this indicates the drive has been set as 'Read-Only' | | Green and Blue flickering together | Admin settings mode |
| | Green flickering | KP200 is unlocked in Admin mode | | Red and Blue blinking together | When not connected to a USB port indicates that both User and Admin PINs have been set on the KP200 |
| | BLUE blinking every 5 seconds | Battery is charging when drive is locked and connected to a USB port | | Red and Blue flickering together | Awaiting Admin PIN change |
| | Blue blinking | Data exchange with host or when not connected to a USB port indicates an Admin PIN exists | | Blinking Blue | Awaiting User PIN change |

## 3. How to Use the KP200 for The First Time

The KP200 is supplied in the **'Initial Shipment State' with no pre-set PIN**. An **8-15** digit **User PIN** must be configured before the drive can be used. Once a User PIN has been successfully configured, it will then not be possible to revert the drive back to the 'Initial Shipment State'.

PIN requirements:

- Must be between 8-15 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3-3)
- Must not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7-8), (7-8-9-0-1-2-3-4), (8-7-6-5-4-3-2-1)

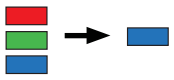
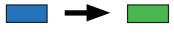
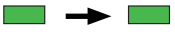
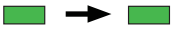
**Password Tip**: You can create a memorable word, name, phrase or any other Alphanumerical PIN combination by simply pressing the key with the corresponding letters on it.

**Examples of these types of Alphanumerical PINs are:**

- For "**Password**" you would press the following keys:
  **7** (pqrs) **2** (abc) **7** (pqrs) **7** (pqrs) **9** (wxyz) **6** (mno) **7** (pqrs) **3** (def)
- For "**IronKey1**" you would press:
  **4** (ghi) **7** (pqrs) **6** (mno) **6** (mno) **5** (jkl) **3** (def) **9** (wxyx) and then **1**

Using this method, long and easy to remember PIN's can be created.

To create a User PIN, proceed with the following steps.

| Instructions | LED | LED State |
|---|---|---|
| 1. Press **KEY** button once |  | Red, Green & Blue LEDs will flash together once and then switch to a solid Red LED and blinking Green and Blue LEDs |
| 2. Press the **KEY** button **twice** (double-click) |  | Solid Red LED and blinking Green and Blue LEDs will switch to a blinking Blue LED |
| 3. Enter your new 8-15 digit **User PIN** |  | Blue LED will continue to blink |
| 4. Press **KEY** button **twice** (double-click) |  | Blinking Blue LED will switch to a blinking Green LED |
| 5. Re-enter your new **User PIN** |  | Green LED continues to blink |
| 6. Press **KEY** button **twice** (double-click) |  | Blinking Green LED will change to solid Red LED and then switch to a solid Green LED indicating that the User PIN was successfully created |

**Note**: Once the KP200 has been successfully unlocked, the Green LED will remain on and in a solid state for 30 seconds only, during which time the KP200 needs to be connected to a powered USB port. It can be locked down immediately (if not connected to a USB port) by pressing and holding down the KEY button for 3 seconds, or by clicking the 'Safely Remove Hardware/Eject' icon within your operating system when connected to a USB port. When the KP200 is unlocked and connected to a USB port, it will not accept further instructions via the keypad.

## 4. How to Change the User PIN in User Mode

PIN requirements:

- Must be between 8-15 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3-3)
- Must not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7-8), (7-8-9-0-1-2-3-4), (8-7-6-5-4-3-2-1)

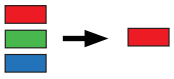
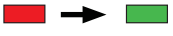
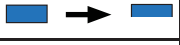
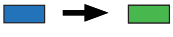
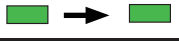
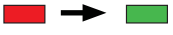
**Password Tip**: You can create a memorable word, name, phrase or any other Alphanumerical PIN combination by simply pressing the key with the corresponding letters on it.

**Examples of these types of Alphanumerical PINs are:**

- For "**Password**" you would press the following keys:
  **7** (pqrs) **2** (abc) **7** (pqrs) **7** (pqrs) **9** (wxyz) **6** (mno) **7** (pqrs) **3** (def)
- For "**IronKey1**" you would press:
  **4** (ghi) **7** (pqrs) **6** (mno) **6** (mno) **5** (jkl) **3** (def) **9** (wxyx) and then **1**

Using this method, long and easy to remember PINs can be created.

To change the User PIN, proceed with the following steps.

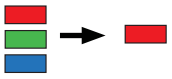
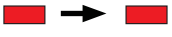
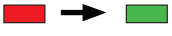
| Instructions | LED | LED State |
|---|---|---|
| 1. Press **KEY** button once |  | Red, Green & Blue LEDs will flash together once and then the Red LED will continue to blink |
| 2. Enter your current User PIN |  | Red LED will continue to blink |
| 3. Press the **KEY** button once |  | Solid Red LED switches to a solid Green LED indicating successful User PIN entry |
| 4. Press **KEY** button **twice** (double-click) |  | Solid Green LED switches to a blinking Blue LED |
| 5. Enter your new User PIN |  | Blue LED continues to blink |
| 6. Press **KEY** button **twice** (double-click) |  | Blinking Blue LED switches to a blinking Green LED |
| 7. Re-enter your new User PIN |  | Green LED continues to blink |
| 8. Press **KEY** button **twice** (double-click) |  | Solid Red LED changing to Green solid LED indicating successful User PIN change |

**Note:** The User PIN can also be changed by the Administrator using the Admin PIN if one exists, refer to section 14 'How to change the User PIN in Admin mode'. If a mistake was made while defining a new User PIN or the procedure was not completed, the drive will retain the old User PIN.

## 5. How to Access Drive Settings in User Mode

The drive settings mode will allow the user to perform different functions such as creating an Admin PIN, enabling and disabling the KP200 as Read-Only, setting a Timeout lock and determining the device version number.

The table below illustrates how to access the drive settings mode, sections 6-11 describe how to perform the various functions.

| Instructions | LED | LED State |
|---|---|---|
| 1. Press **KEY** button once |  | Red, Green & Blue LEDs will flash together once and then the Red LED will continue to blink. (**Note:** Both RED and Blue LEDs will blink together if an Admin PIN also exists.) |
| 2. Enter your current User PIN |  | Red LED will continue to blink |
| 3. Press the **KEY** button once |  | Solid Red LED switches to a solid Green LED indicating successful User PIN entry |
| 4. Press the **KEY** button **three** times- (triple-click) |  | Solid Green LED switches to blinking Green and Blue LEDs, indicating the drive is awaiting new user defined drive settings |

## 6. How to Enable Read-Only as User

To set the KP200 to Read-Only in User mode, proceed with the following steps.

| Instructions | LED | LED State |
|---|---|---|
| 1. Unlock the KP200 with your **User PIN** |  | Green LED will be solid indicating successful User PIN entry |
| 2. Press the **KEY** button **three** times- (triple-click) |  | Solid Green LED switches to blinking Green and Blue LEDs indicating the drive is awaiting new user defined settings |
| 3. Press button number **7** followed by the number **6** button - (**76**) |  | Green and Blue LEDs will continue to blink |
| 4. Press the **KEY** button once |  | Green and Blue LEDs will change to a solid Red LED before switching to a solid Green LED indicating successful Read-Only configuration |

**Note:** Once activated, drive access is limited to Read-Only. When KP200 is unlocked and inserted into a USB port the Green LED blinks every two seconds indicating the drive is in Read-Only Mode. Admin can override User Read/Write settings by enabling/disabling Read/Write in Admin mode.

## 7. How to Enable Read/Write as User

To set the KP200 to Read/Write in User mode, proceed with the following steps.

| Instructions | LED | LED State |
|---|---|---|
| 1. Unlock the KP200 with your **User PIN** |  | Green LED will be solid indicating successful User PIN entry |
| 2. Press the **KEY** button **three** times- (triple-click) |  | Solid Green LED switches to blinking Green and Blue LEDs indicating the drive is awaiting new user defined settings |
| 3. Press button number **7** followed by the number **9** button - (**79**) |  | Green and Blue LEDs will continue to blink |
| 4. Press the **KEY** button once |  | Green and Blue LEDs will change to a solid Red LED before switching to a Green LED indicating successful Read/Write configuration |

**Note:** Once activated, drive access is restored to the default Read/Write state. Admin can override User settings by enabling/disabling Read/Write in Admin mode.

## 8. How to Set the Timeout Lock in User Mode

To protect against unauthorized access in the event, the KP200 is connected to a host and left unattended, the KP200 can be set to automatically lock after a pre-set duration of time.

In its default state, the KP200 Timeout Lock feature is turned off. The Timeout Lock feature can be set to activate (lock) an idle drive anywhere between 1 and 99 minutes.

To set the Timeout Lock, please follow steps in the table below.

| Instructions | LED | LED State |
|---|---|---|
| 1. Unlock the KP200 with your **User PIN** | | Green LED will be solid indicating successful User PIN entry |
| 2. Press the **KEY** button **three** times- (triple-click) | | Solid Green LED switches to blinking Green and Blue LEDs indicating the drive is awaiting new user defined settings |
| 3. Press button number **8** followed by the number **5** button - (**85**) | | Green and Blue LEDs will continue to blink |
| 4. Press the **KEY** button once | | Green and Blue LEDs will switch to a blinking Green LED |
| 5. Enter the length of User Timeout:<br>0 = 0 minutes (default)<br>5 = 5 minutes<br>15 = 15 minutes<br>99 = 99 minutes etc | | Green LED continues to blink |
| 6. Press the **Key** button once | | Red solid LED will switch to a Green solid LED indicating the Auto-Lock time out has been successfully configured |

**Note:** If the Timeout Lock feature has been set by the user in '**User Mode**', the Administrator is able to change the user setting in Admin mode. If the Administrator set the Timeout Lock feature in '**Admin Mode**', the user is disabled from making any change to the Timeout feature in User Mode.

## 9. How to Disable the Timeout Lock in User Mode

To disable the Timeout Lock, please follow steps in the table below.

| Instructions | LED | LED State |
|---|---|---|
| 1. Unlock the KP200 with your **User PIN** | | Green LED will be solid indicating successful User PIN entry |
| 2. Press the **KEY** button **three** times- (triple-click) | | Solid Green LED switches to blinking Green and Blue LEDs indicating the drive is awaiting new user defined settings |
| 3. Press button number **8** followed by the number **5** button - (**85**) | | Green and Blue LEDs will continue to blink |
| 4. Press the **KEY** button once | | Green and Blue LEDs will switch to a blinking Green LED |
| 5. To disable the Timeout Lock, press button number **0** | | Green LED continues to blink |
| 6. Press the **Key** button once | | Red solid LED will switch to a Green solid LED indicating the Auto-Lock time out has been successfully disabled |

**Note:** If the Timeout Lock feature has been set by the user in '**User Mode**', the Administrator is able to change the user setting in Admin mode. If the Administrator set the Timeout Lock feature in '**Admin Mode**', the user is disabled from making any change to the Timeout feature in User Mode.

## 10. How to Determine the Device Version Number in User Mode

To display the device Version Number of the KP200 do the following.

| Instructions | LED | LED State |
|---|---|---|
| 1. Unlock the KP200 your **User PIN** |  | Green LED will be solid indicating successful User PIN entry |
| 2. Press the **KEY** button **three** times- (triple-click)  |  | Solid Green LED switches to blinking Green and Blue LEDs indicating the drive is awaiting new user defined settings |
| 3. Press button number **8** followed by the number **6** button - (**86**) |  | Green and Blue LEDs will continue to blink |
| 4. Press the **KEY** button once and the following happens;<br><br>a. All LEDs (RED, GREEN & BLUE) will flash together once.<br>b. RED LED blinks indicating the integral part of the firmware revision number.<br>c. GREEN LED blinks indicating the fractional part.<br>d BLUE LED blinks indicating the last digit of the firmware revision number<br>e. All LEDs (RED, GREEN & BLUE) become solid for 1 second.<br>f. RED, GREEN & BLUE LEDs switch to a solid Green LED | | |
| For example, if the revision number is '**1.12.3**', the Red LED will blink once (**1**) and the Green LED will blink twelve (**12**) times and the Blue LED will blink three (**3**) times. Once the sequence has ended the Red, Green & Blue LEDs will blink together once and then to solid Green. | | |

## 11. How to Create an Admin PIN in User Mode

If no Admin PIN exists, the user is able to create an Admin PIN by following the instructions in the table below.

The Admin PIN is a useful feature for corporate deployment, for example:

- Recovering data from a drive and configuring a new User PIN in the event an employee has forgotten their PIN
- Retrieving data from a drive if an employee leaves the company
- Setting Admin defined user policies
- The Admin PIN can be used to override all user settings

PIN requirements:

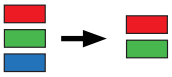
- Must be between 8-15 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3-3)
- Must not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7-8), (7-8-9-0-1-2-3-4), (8-7-6-5-4-3-2-1)

To create an Admin PIN in User mode, proceed with the following steps.

| Instructions | LED | LED State |
|---|---|---|
| 1. Unlock the KP200 with your **User PIN** |  | Green LED will be solid indicating successful User PIN entry |
| 2. Press and hold down the number **1** button and press the **KEY** button **twice** (double click) (**1** & 🔑 🔑) |  | Solid Green LED will switch to flickering Red and Blue LEDs |
| 3. Enter your new 8-15 digit **Admin PIN** |  | Red and Blue LEDs will continue to flicker together |
| 4. Press **KEY** button **twice** (double click) 🔑 🔑 |  | Red and Blue LEDs will switch to a blinking Green LED |
| 5. Re-enter your new **Admin PIN** |  | Green LED will continue to blink |
| 6. Press **KEY** button **twice** (double click) 🔑 🔑 |  | Blinking Green LED will change to a solid Red LED before switching to a solid Green LED indicating the Admin PIN has been successfully configured |

## 12. How to Unlock the KP200 as Admin

**Caution**: Entering the Admin PIN to access a locked drive will clear (delete) the User PIN.

| Instructions | LED | LED State |
|---|---|---|
| 1. Press and hold down the number **1** button and press the **KEY** button once (**1** & 🔑) |  | Red, Green & Blue LEDs will flash together once and then Red and Green LEDs flicker together |
| 2. Enter your **Admin PIN** |  | Red and Green LEDs continue to flicker together |
| 3. Press the **KEY** button once 🔑 |  | Flickering Red and Green LEDs will change to a solid Red LED and then switch to a flickering Green LED indicating successful Admin PIN entry- drive unlocked as Admin |

**Note**: Once the KP200 has been successfully unlocked, the Green LED will remain on and blinking for 30 seconds only, during which time the KP200 needs to be connected to a powered USB port. It can be locked down immediately (if not connected to a USB port) by pressing and holding down the KEY button 🔑 for 3 seconds, or by clicking the 'Safely Remove Hardware/Eject' icon within your operating system when connected to a USB port.

When the KP200 is unlocked and connected to a USB port, it will not accept further instructions via the keypad.

## 13. How to Create a New User PIN in Admin Mode

Creating a new User PIN in Admin mode will become necessary if the KP200 has been unlocked for any reason with the Admin PIN, as this will automatically clear (delete) the User PIN. To create a new User PIN in Admin mode please follow the instructions below.

**Admin PIN requirements:**

- Must be between 8-15 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3-3)
- Must not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7-8), (7-8-9-0-1-2-3-4), (8-7-6-5-4-3-2-1)

| Instructions | LED | LED State |
|---|---|---|
| 1. Unlock the KP200 with your **Admin PIN** | | Green LED will flicker indicating successful Admin PIN entry |
| 2. Press the **KEY** button **twice** (double-click) | → | Flickering Green LED switches to a blinking Blue LED ready to receive a new User PIN |
| 3. Enter your new 8-15 digit **User PIN** | → | Blue LED continues to blink |
| 4. Press **KEY** button **twice** (double-click) | → | Blinking Blue LED switches to a blinking Green LED |
| 5. Re-enter your new **User PIN** | → | Green LED continues to blink |
| 6. Press **KEY** button **twice** (double-click) | → OFF | Blinking Green LED switches to a Red LED and then quickly fades out (off) to indicate successful creation of a new User PIN |

## 14. How to Change the User PIN in Admin Mode

To change the User PIN in Admin mode please follow the instructions below.

| Instructions | LED | LED State |
|---|---|---|
| 1. Unlock the KP200 with your **Admin PIN** | | Green LED will flicker indicating successful Admin PIN entry |
| 2. Press the **KEY** button **twice** (double-click) | → | Flickering Green LED switches to a blinking Blue LED ready to receive a new User PIN |
| 3. Enter your new 8-15 digit **User PIN** | → | Blue LED continues to blink |
| 4. Press **KEY** button **twice** (double-click) | → | Blinking Blue LED switches to a blinking Green LED |
| 5. Re-enter your new **User PIN** | → | Green LED continues to blink |
| 6. Press **KEY** button **twice** (double-click) | → OFF | Blinking Green LED switches to a Red LED and then quickly fades out (off) to indicate the User PIN was successfully changed |

## 15. How to Verify Whether an Admin/User PIN Has Been Set Up

The following table illustrates how to determine which PINs, User and/or Admin, have been set up.
With the KP200 in a locked state (all LEDs off), press the KEY button once.

| | | |
|---|---|---|
| 1. Press KEY button once Red, Green & Blue LEDs will flash together once, then one of the following states occurs. | | |
| Only **User** PIN exists |  | Red LED blinks |
| Only **Admin** PIN exists |  | Blue LED blinks |
| Both **User** and **Admin** PINs exist |  | Red and Blue LEDs blink together |

## 16. How to Change the Admin PIN

Once an Admin PIN has been created, the KP200 needs to be unlocked in Admin mode in order to change the Admin PIN. The Admin PIN cannot be changed from the User mode.

**Caution**: Entering the Admin PIN to access a locked drive will clear (delete) the User PIN.

**Admin PIN requirements:**

- Must be between 8-15 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3-3)
- Must not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7-8), (7-8-9-0-1-2-3-4), (8-7-6-5-4-3-2-1)

| Instructions | LED | LED State |
|---|---|---|
| 1. Unlock the KP200 with existing **Admin PIN** |  | Green LED will flicker indicating successful Admin PIN entry |
| 2. Press and hold down the number **1** button and press the **KEY** button **twice** (double-click) (**1** & ) |  | Flickering Green LED switches to Red and Blue LEDs flickering together ready to receive new Admin PIN |
| 3. Enter your new 8-15 digit **Admin PIN** |  | Red and Blue LEDs continue to flicker together |
| 4. Press **KEY** button **twice** (double-click) |  | Red and Blue LEDs switch to a blinking Green LED |
| 5. Re-enter your new **Admin PIN** |  | Green LED continues to blink |
| 6. Press **KEY** button **twice** (double-click) |  | Solid Red LED switches to a flickering Green LED indicating successful Admin PIN change |

**Note:** If a mistake was made while defining a new Admin PIN or the procedure was not completed, the drive will retain the old Admin PIN.

## 17. How to Enable Read-Only in Admin Mode

When Admin writes content to the KP200 and restricts access to read-only, the User cannot change this setting in User mode.

To set the KP200 to Read-Only, please follow the steps below.

**Caution**: Entering the Admin PIN to access a locked drive will clear (delete) the User PIN.

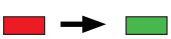
| Instructions | LED | LED State |
|---|---|---|
| 1. Unlock the KP200 with your **Admin PIN** |  | Green LED will flicker indicating successful Admin PIN entry |
| 2. Press the **KEY** button **three** times (triple-click) |  | Green and Blue LEDs flicker together |
| 3. Press the number **7** button followed by the number **6** button (**76**) |  | Green and Blue LEDs continue to flicker together |
| 4. Press **KEY** button once |  | Green and Blue LEDs change to a solid Red LED and then switches to a flickering Green LED. When the KP200 is inserted into a USB port the Green LED blinks every two seconds indicating the KP200 is in Read-Only mode |

## 18. How to Enable Read/Write in Admin Mode

Admin can override User set Read-Only by enabling Read/Write using the Admin PIN.

To set the KP200 to Read/Write, please follow the steps below.

**Caution**: Entering the Admin PIN to access a locked drive will clear (delete) the User PIN.

| Instructions | LED | LED State |
|---|---|---|
| 1. Unlock the KP200 with your **Admin PIN** |  | Green LED will flicker indicating successful Admin PIN entry |
| 2. Press the **KEY** button **three** times (triple-click) |  | Green and Blue LEDs flicker together |
| 3. Press the number **7** button followed by the number **9** button (**79**) |  | Green and Blue LEDs continue to flicker together |
| 4. Press **KEY** button once |  | Green and Blue LEDs change to a solid Red LED and then switches to a flickering Green LED. When the KP200 is inserted into a USB port the Green LED is solid indicating the KP200 is Read/Write enabled |

## 19. How to Determine the Device Version Number in Admin Mode

To display the device Version Number of the KP200 do the following.

**Caution**: Entering the Admin PIN to access a locked drive will clear (delete) the User PIN.

| Instructions | LED | LED State |
|---|---|---|
| 1. Unlock the KP200 with **Admin PIN** |  | Green LED will flicker indicating successful Admin PIN entry |
| 2. Press the **KEY** button **three** times- (triple-click) |  | Green and Blue LEDs flicker together |
| 3. Press button number **8** followed by the number **6** button - (**86**) |  | Green and Blue LEDs continue to flicker together |
| 4. Press the **KEY** button once and the following happens;<br><br>a. All LEDs (RED, GREEN & BLUE) will flash together once.<br>b. RED LED blinks indicating the integral part of the firmware revision number.<br>c. GREEN LED blinks indicating the fractional part.<br>d BLUE LED blinks indicating the last digit of the firmware revision number<br>e. All LEDs (RED, GREEN & BLUE) become solid for 1 second.<br>f. RED, GREEN & BLUE LEDs switch to a flickering Green LED | | |
| For example, if the revision number is '**1.12.3**', the Red LED will blink once (**1**) and the Green LED will blink twelve (**12**) times and the Blue LED will blink three (**3**) times. Once the sequence has ended the Red, Green & Blue LEDs will blink together once and will then switch to a flickering Green LED. | | |

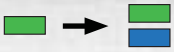
## 20. How to Set the Timeout Lock in Admin Mode

To protect against unauthorized access in the event the KP200 is connected to a host and left unattended, the KP200 can be set to automatically lock after a pre-set duration of time.

In its default state, the KP200 Timeout Lock feature is turned off. The Timeout Lock feature can be set to activate (lock) an idle drive anywhere between 1 and 99 minutes. Admin Timeout Lock settings will override User settings.

To set the Timeout Lock, please follow steps in the next table.

**Caution**: Entering the Admin PIN to access a locked drive will clear (delete) the User PIN.

| Instructions | LED | LED State |
|---|---|---|
| 1. Unlock the KP200 with the **Admin PIN** |  | Green LED will flicker indicating successful Admin PIN entry |
| 2. Press the **KEY** button **three** times- (triple-click) |  | Green and Blue LEDs flicker together |
| 3. Press button number **8** followed by the number **5** button - (**85**) |  | Green and Blue LEDs continue to flicker together |
| 4. Press the **KEY** button once |  | Green and Blue LEDs will switch to a blinking Green LED |
| 5. Enter the length of User Timeout:<br>0 = 0 minutes (default)<br>5 = 5 minutes<br>15 = 15 minutes<br>99 = 99 minutes etc |  | Green LED continues to blink |
| 6. Press the **Key** button once |  | Solid Red LED will switch to a flickering Green LED indicating the Auto-Lock time out has been successfully configured |

## 21. How to Disable the Timeout Lock in Admin Mode

To disable the Timeout Lock, please follow steps in the table below.

| Instructions | LED | LED State |
|---|---|---|
| 1. Unlock the KP200 with the **Admin PIN** |  | Green LED will flicker indicating successful Admin PIN entry |
| 2. Press the **KEY** button **three** times- (triple-click) |  | Green and Blue LEDs flicker together |
| 3. Press button number **8** followed by the number **5** button - (**85**) |  | Green and Blue LEDs continue to flicker together |
| 4. Press the **KEY** button once |  | Green and Blue LEDs will switch to a blinking Green LED |
| 5. To disable the Timeout Lock, press button number **0** |  | Green LED continues to blink |
| 6. Press the **Key** button once |  | Solid Red LED will switch to a flickering Green LED indicating the Auto-Lock time out has been successfully disabled |

## 22. How to Delete All Data in Admin Mode

To delete all data stored on the KP200, please follow the instructions below. All Admin settings will remain on the KP200 but all data will be deleted and cannot be retrieved and the KP200 will have to be reformatted (see sections 28, 29 or 30).

**Caution**: Entering the Admin PIN to access a locked drive will clear (delete) the User PIN.

| Instructions | LED | LED State |
|---|---|---|
| 1. Unlock the KP200 with the **Admin PIN** |  | Green LED will flicker indicating successful Admin PIN entry |
| 2. Press the **KEY** button **three** times- (triple-click) |  | Green and Blue LEDs flicker together |
| 3. Press button number **3** followed by the number **2** button - (**32**) |  | Green and Blue LEDs continue to flicker together |
| 4. Press the **KEY** button once |  | Green and Blue LEDs will switch to Red and Green LEDs alternating on and off |
| 5. Enter your **Admin PIN** |  | Red and Green LED continue to alternate on and off |
| 6. Press the **Key** button once |  | Alternating Red and Green LEDs switch to solid Red and Green LEDs and finally to a flickering Green LED indicating that all data has been deleted |

## 23. Brute Force Hacking Detection

If both Admin and User PINs have been created and a User enters an incorrect User PIN ten (10) consecutive times, the KP200's brute force mechanism will trigger and the User PIN will be deleted. All data will remain on the KP200 and can only be accessed by the Admin entering the correct Admin PIN.

If Admin enters an incorrect Admin PIN ten (10) consecutive times, then both the User and Admin PINs, the encryption key and all data will be deleted and lost forever.

The table below illustrates the different PIN set-up states and what happens when entering an incorrect Admin or User PIN incorrectly ten (10) consecutive times.

| PINs Set-up on KP200 | PIN used to unlock KP200 | What happens after 10 consecutive incorrect PIN entries? |
|---|---|---|
| Admin & User PINs | User PIN | The KP200's brute force mechanism will trigger and the User PIN will be deleted.<br>All data will remain on the KP200 and can only be accessed by the Admin entering the correct Admin PIN. |
| Admin & User PINs | Admin PIN | The KP200's brute force mechanism will trigger and both the User and Admin PINs, the encryption key and all data will be deleted and lost forever. |
| User PIN Only | User PIN | The KP200's brute force mechanism will trigger and the User PIN, the encryption key along with all data will be deleted and lost forever. |
| Admin PIN Only | Admin PIN | The KP200's brute force mechanism will trigger and the Admin PIN, the encryption key along with all data will be deleted and lost forever. |

**Note:** To use the drive after a Brute Force attack, the user must create either a new **User PIN** or a new **Admin PIN** as described in sections:

25. How to create a **User PIN** after a Brute Force attack or Reset.
26. How to create an **Admin PIN** after a Brute Force attack or Reset.

The KP200, unlike other similar drives, incorporates a random number generator, once the drive is reset a new encryption key is randomly generated and the drive will need to be reformatted (see sections 28, 29 or 30).

## 24. How to Reset the KP200

**Caution:** Resetting the KP200 will delete all PINs, the encryption key and all data stored on the drive.

In the event both the Admin and User PINs have been forgotten, the drive will need to be reset before creating a new User/Admin PIN. To reset the KP200, please follow the instructions below.

| Instructions | LED | LED State |
|---|---|---|
| 1. Press and hold down number **7** (seven) button and then press the **KEY** button and then release buttons (**7** & 🔑) |  | Red and Green LEDs alternate on and off |
| 2. Press the number **9** button **three** times (triple-click) (**999**) |  | Red and Green LEDs continue to alternate on and off |
| 3. Press and hold down number **7** (seven) button and then press the **KEY** button and then release buttons (**7** & 🔑) |  OFF | Alternating Red and Green LEDs switch to solid Red and Green LEDs, then the Green LED switches off and the Red LED fades out to complete the reset process |

**Note:** The reset process will clear all cryptographic parameters including both User and Admin PINs. To use the drive after a reset, the user must create either a new **User PIN** or a new **Admin PIN** as described in sections:

25. How to create a **User PIN** after a Brute Force attack or Reset.
26. How to create an **Admin PIN** after a Brute Force attack or Reset.

The KP200, unlike other similar drives, incorporates a random number generator, once the drive is reset a new encryption key is randomly generated and the drive will need to be reformatted (see sections 28, 29 or 30).

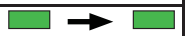
## 25. How to Create a User PIN After a Brute Force Attack or Reset

It will be necessary after a Brute Force attack or when the KP200 has been reset to create a new User PIN and format the drive before it can be used. To create an Admin PIN instead of a User PIN, refer to section 26.

**PIN Requirements:**

- Must be between 8-15 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3-3)
- Must not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7-8), (7-8-9-0-1-2-3-4), (8-7-6-5-4-3-2-1)

To create a User PIN after a Brute Force attack or Reset, proceed with the following steps.

| Instructions | LED | LED State |
|---|---|---|
| 1. Press **KEY** button once |  | Red, Green & Blue LEDs will flash together once and then switch to a solid Red LED and a blinking Green LED |
| 2. Press the **KEY** button **twice** (double-click) |  | Solid Red LED and blinking Green LED will switch to a blinking Blue LED |
| 3. Enter your new 8-15 digit **User PIN** |  | Blue LED will continue to blink |
| 4. Press **KEY** button **twice** (double-click) |  | Blinking Blue LED will switch to a blinking Green LED |
| 5. Re-enter your new **User PIN** |  | Green LED continues to blink |
| 6. Press **KEY** button **twice** (double-click) |  | Blinking Green LED will change to solid Red LED and then switch to a solid Green LED indicating that the User PIN was successfully created |

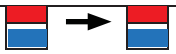
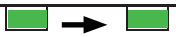
## 26. How to Create an Admin PIN After a Brute Force Attack or Reset

It will be necessary after a Brute Force attack or when the KP200 has been reset to create a new Admin PIN and format the drive before it can be used. To create a User PIN instead of an Admin PIN, refer to section 25.

**PIN Requirements:**

- Must be between 8-15 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3-3)
- Must not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7-8), (7-8-9-0-1-2-3-4), (8-7-6-5-4-3-2-1)

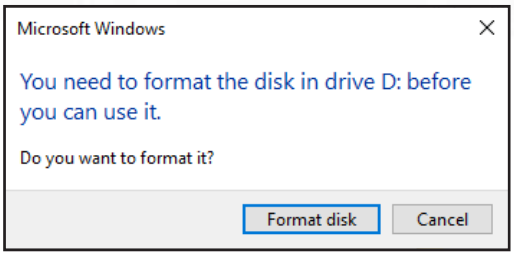
To create a Admin PIN after a Brute Force attack or Reset, proceed with the following steps.

| Instructions | LED | LED State |
|---|---|---|
| 1. Press **KEY** button once |  | Red, Green & Blue LEDs will flash together once and then switch to a solid Red LED and a blinking Green LED |
| 2. Press and hold down the number **1** button and press the **KEY** button **twice** (double click) (**1** & ) |  | Solid Red LED and blinking Green LED will switch to flickering Red and Blue LEDs |
| 3. Enter your new 8-15 digit **Admin PIN** |  | Red and Blue LEDs will continue to flicker |
| 4. Press **KEY** button **twice** (double-click) |  | Flickering Red and Blue LEDs will switch to a blinking Green LED |
| 5. Re-enter your new **Admin PIN** |  | Green LED continues to blink |
| 6. Press **KEY** button **twice** (double-click) |  | Blinking Green LED will change to solid Red LED and then switch to a flickering Green LED indicating that the Admin PIN was successfully created |

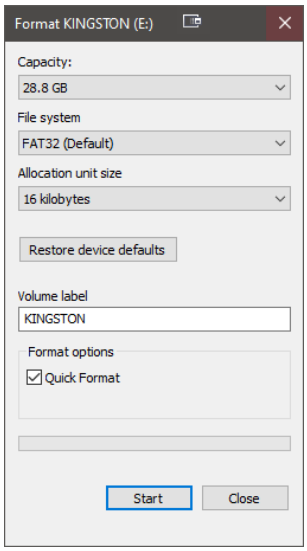
# 27. How to Format KP200 for Windows

To format your KP200 for Windows, please follow the steps below:

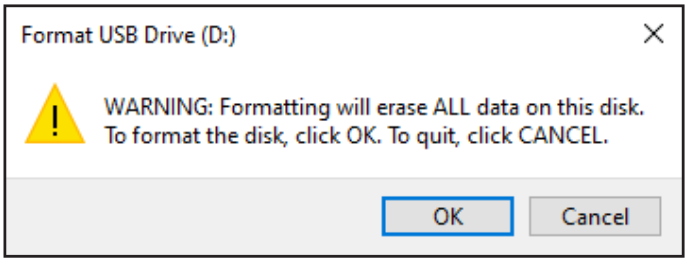
1. Unlock and attach the KP200 to the Windows machine.
2. The system will prompt you with the Format window.




3. Press Format disk and Format USB drive window will open.




4. Enter a name for the drive on the Volume label. The name of the drive will eventually appear on the Desktop. The File System dropdown menu lists the available drive formats for windows. Select NTFS for Windows or select FAT32 or exFAT for cross-platform compatibility, which includes macOS.
5. Click OK to continue with formatting the drive.



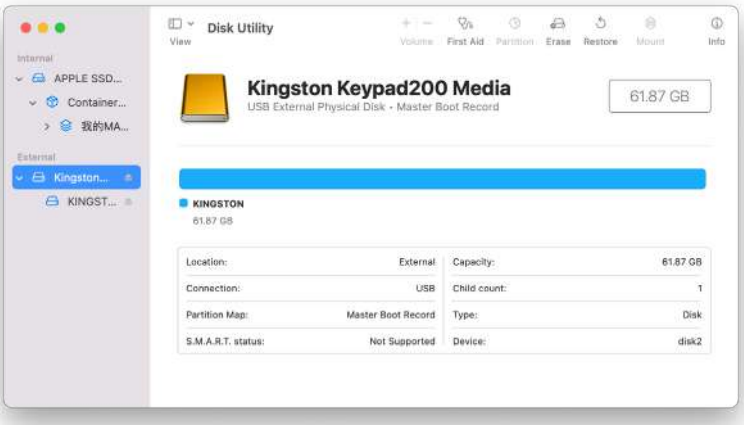

6. The procedure will finish formatting the drive with confirmation that formatting has been completed.

## 28. How to Format KP200 for macOS

To format your KP200 on macOS, please follow the steps below:

1. Unlock and attach the KP200 to your macOS machine.
2. A warning message will pop up. Press “Initialize”.


3. Select the external volume labeled “Kingston Keypad 200…” and press “Erase”.



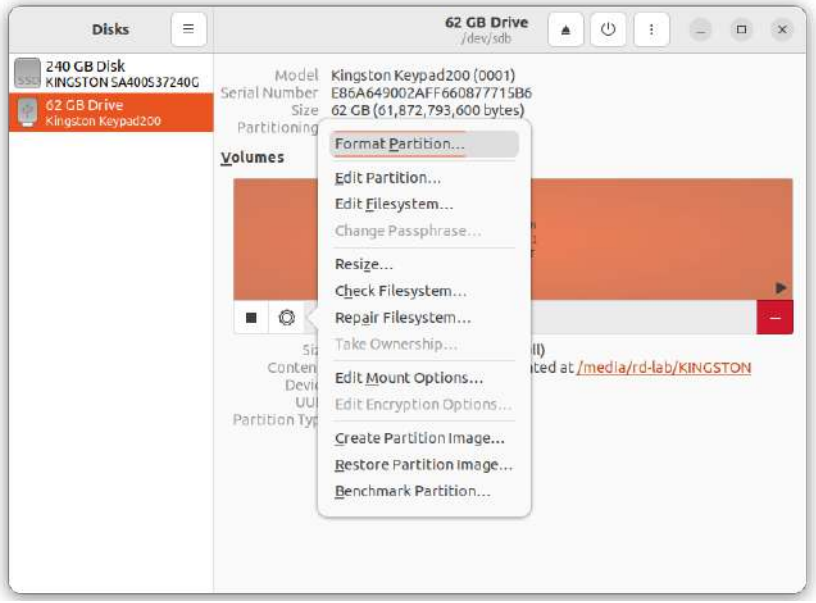

4. Enter a name for the drive. The name of the drive will eventually appear on the Desktop. The Volume Format dropdown menu lists the available drive formats that macOS supports. The recommended format type is macOS Extended for macOS and MS-DOS or exFAT for cross platform including windows. Select Scheme as GUID Partition Map.
5. Click Erase.
6. The formatted drive will appear in the Disk Utility window and will mount onto the desktop.

## 29. How to Format KP200 for Linux

To format your KP200 on Linux, please follow the below steps:

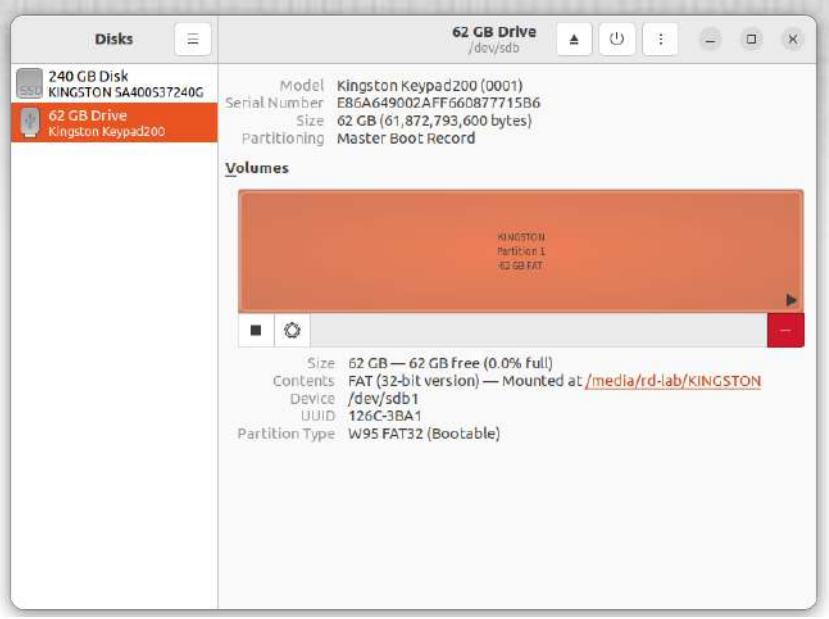
1. Unlock and attach the KP200 to the Linux machine.
2. Open 'Show Application' and type 'Disks' in the search box. Click on the 'Disks' utility when displayed.

3. Click to select the drive under 'Devices'. Next, click on the gear icon under 'Volumes' and then click on 'Format Partitions'.




4. Enter a name for the drive and select 'For use in all systems and devices (FAT)' for the 'Type' option. e.g.: KP200
5. Then, click the 'Format' button.

6. After the format process is finished, click ▶ to mount the drive to Linux.




7. Now the drive should be mounted to Linux and ready to use.

## 30. Technical Support

Kingston IronKey provides the following helpful resources for you:

Website:
https://www.kingston.com/IKKP200