GL·iNet



User Manual

GL-RM10RC / Comet 5G

Remote KVM over 5G RedCap

Firmware Version 1.9.1

About This Manual

This manual is your go-to resource for getting started with your device, covering basic product information, hardware connections, local and remote access, and detailed instructions for all software features in the Web console.

With this guide, you will be able to:

- Understand key product details
- Complete hardware connections step by step
- Access your KVM and the controlled device locally and remotely
- Understand all software features in the Web console

Format Conventions

These symbols/colors help you follow steps faster.

Convention	What It Means
Underlined teal text	Clickable link which can open a web page or a specific section
Bold text	Emphasize or mark some key information in this document, such as titles, hyperlinks, and exact menu/item names on the device's web interface
>	The path to load the corresponding page (e.g., System > Firmware)
Note	Key information for setup, operations, and safety. Ignoring this might result in setup failure, device malfunction or damage
Tips	Advice to help you use your device better

Note:

- Device features may vary by model and firmware version.
- Product availability is subject to regional differences or ISP specifications.
- All images, procedures, and descriptions in this guide are for illustrative purposes only and may differ from your actual usage experience.

Need More Help or Info?

- Firmware Update: GL.iNet download center
- Community: Discuss our products and share insights at GL.iNet Community Forum
- Technical Support: Contact our Technical Support at Contact page

Copyright © 2026 GL.iNet Technology (HK) Ltd. All rights reserved.
No part of this manual may be reproduced, transcribed, translated, or distributed in any form or by any means, without the prior written permission of GL.iNet Technology (HK) Ltd. GL.iNet is a registered trademark of GL.iNet Technology (Hong Kong) Ltd. in China and/or other countries and regions. All other brand and product names mentioned herein are trademarks or registered trademarks of their respective owners.
The content of this document is subject to change without notice due to product version upgrades or other reasons. Unless otherwise agreed, this document is provided for informational purposes only, and all statements, information, and recommendations contained herein do not constitute any form of warranty.

GL Tech (HK) Ltd: #601, 5W, Hong Kong Science Park, N.T. Hong Kong
GL Intelligence, Inc.: 10400 Eaton Place, Suite 215, Fairfax, VA 22030

Contents

Chapter 1 Get To Know Your Device 6

1.1 Product Overview 7

1.2 Specifications 11

1.3 Package Contents 12

Chapter 2 Hardware Connection 13

Chapter 3 Local Access 17

3.1 Domain 18

3.2 IP Address 20

Chapter 4 Remote Access 22

4.1 Cloud Service 23

4.2 GLKVM App 27

4.3 Tailscale 33

4.4 ZeroTier 39

4.5 NetBird 47

Chapter 5 Settings 53

5.1 Video 54

5.2 Remote Device Settings 56

5.3 System 59

5.4 Network 61

Chapter 6 Toolbox 65

6.1 Clipboard 66

6.2 Shortcut 66

6.3 Wake-on-Lan 67

6.4 Terminal 68

Chapter 7 Accessories 69

7.1 Fingerbot 70

7.2 ATX Board 71

Chapter 8 Virtual Media 72

8.1 File Sharing 73

8.2 Image Mounting 78

8.3 Replace Storage Drive 80

8.4 Format Disk 80
Chapter 9 Apps Center 81
9.1 Tailscale 82
9.2 ZeroTier 83
9.3 NetBird 84
Chapter 10 System Tools 85
10.1 Help Center 86
10.2 Text Recognition 86
10.3 Collapse 88
10.4 Fullscreen 89
10.5 Upgrade 90
10.6 Cloud Service 91
10.7 Security 92
Regulatory Statement 94

Chapter 1

Get To Know Your Device

This chapter covers the device overview, specifications, and package contents.

1.1 Product Overview

Comet 5G (GL-RM10RC) is a Wi-Fi 6 remote KVM that integrates cellular 5G RedCap connectivity to enhance deployment flexibility, even in areas without wired broadband access. Equipped with a touchscreen, it delivers a simple and efficient interface for daily operations. When being used with extensions such as an ATX Board or a Fingerbot, it enables remote power on and off control of connected equipment, making it well-suited for distributed management and field maintenance scenarios.

1.1.1 Appearance

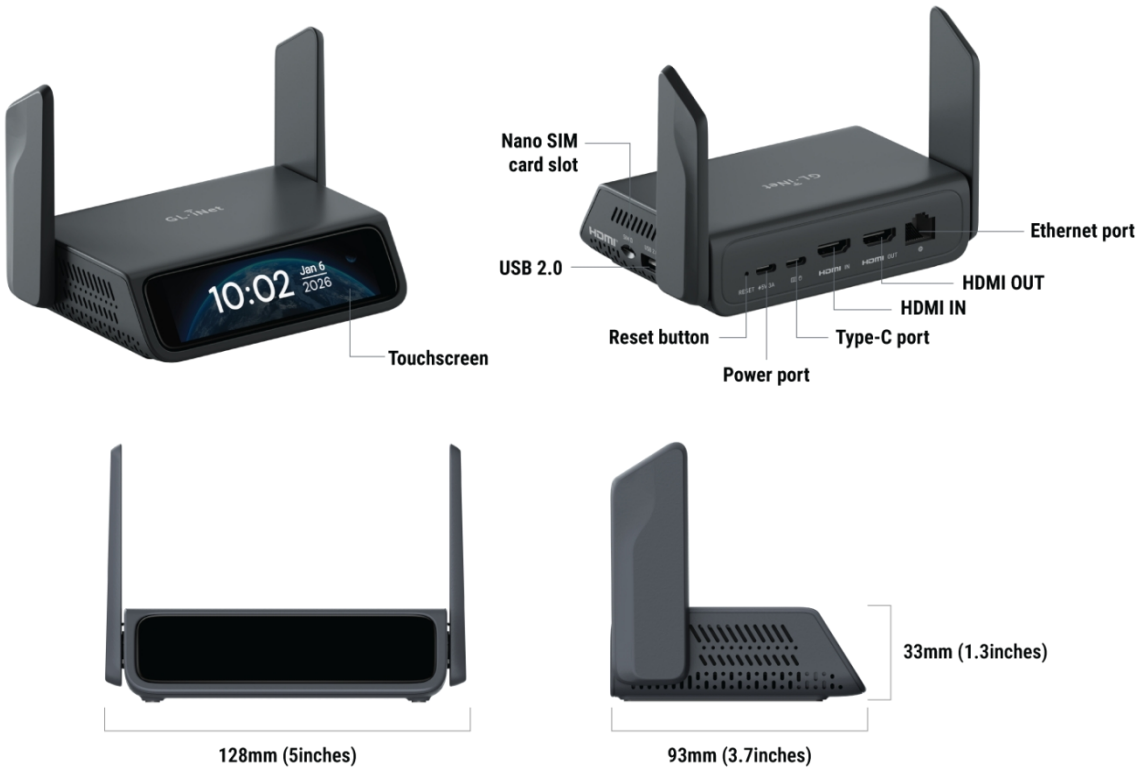








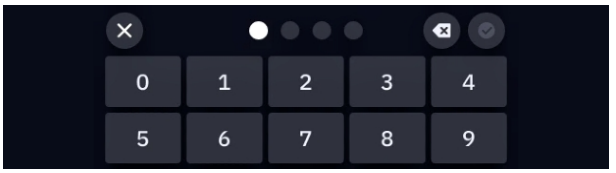
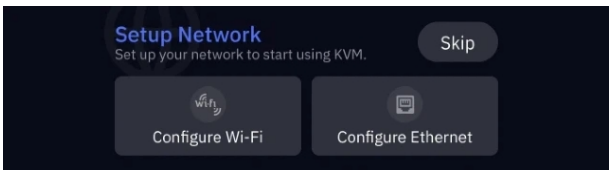
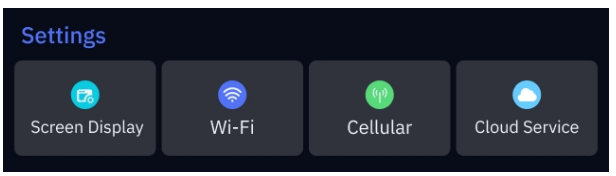
1.1.2 Interface and Dimension

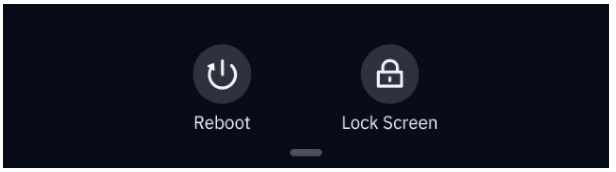
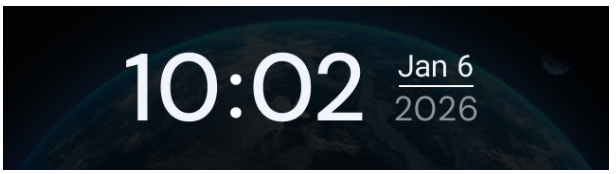
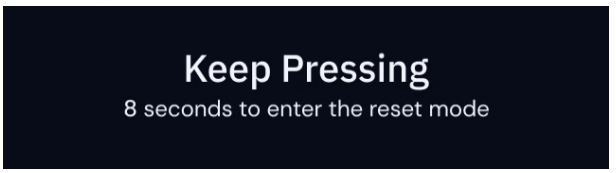


Item	Description
Power Port	Connects to a power adapter.
Ethernet Port	Connects to a network source, such as a router, a network switch, or an Ethernet outlet.
HDMI IN	Connects to the controlled device via an HDMI cable for video signal transmission.
HDMI OUT	(Optional) Connects to an external display of the controlled device if needed.
Type-C Port	Connects to the controlled device via a USB-C cable for keyboard & mouse signal transmission.
USB 2.0	Connects to an accessory (e.g., Fingerbot or ATX board) via a USB wireless receiver for remote power control.
Nano SIM Slot	Accepts a Nano-SIM card for 5G connectivity.

Reset Button	Press and hold for **10 seconds** and then release to reset the device to factory default.

1.1.3 Touchscreen

Screen Display	Description
	**Starting up** The GL.iNet logo appears, followed by a startup progress bar. Once the progress bar is fully loaded, the device startup is complete.
	**Set up screen password** Set a screen password for your Comet 5G to protect your privacy.
	**Set up network** Connect Comet 5G to 2.4GHz/5GHz Wi-Fi, or connect it to a network device (such as a router, network switch, or Ethernet jack) via Ethernet cable.
	**Home screen** **Top-left**: Network status. **Top-right**: Cloud status and system time. **Middle**: Device IP address. **Bottom**: Keyboard & mouse signal, HDMI signal, and USB connected status.
	**Settings** On the home screen, swipe left from the right to access basic settings, including Screen Display, Wi-Fi, Cellular, and Cloud

	Service.
	**System Menu** On the home screen, swipe down from the top to access system menu, including Reboot and Lock Screen.
	**Lock Screen** The lock screen displays the time and date.
	**Factory Reset** With the KVM powered on, insert a pin into the reset pinhole and hold for 8 seconds to factory reset. Release the pin within 8 seconds to cancel the reset.

1.2 Specifications

Interface	1 x USB 2.0 Type-C (Keyboard & Mouse) 1 x USB 2.0 Type-A 1 x Ethernet Port 1 x HDMI IN 1 x HDMI OUT 1 x Nano SIM Slot 1 x Reset Button
CPU	Quad-core ARM Cortex-A53
Memory / Storage	DDR3L 1GB / eMMC 64GB
Display Screen	3.69 inch, touchscreen
Wi-Fi Standard	IEEE 802.11 a/b/g/n/ac/ax
Wi-Fi Speed	286Mbps (2.4GHz), 286Mbps (5GHz)
Cellular	4G LTE & 5G RedCap
Frequency Bands	5G NR: 3GPP Release 17 RedCap, SA operation (Sub-6 GHz) n1 / n2 / n3 / n5 / n7 / n8 / n12 / n13 / n14 / n18 / n20 / n25 / n26 / n28 / n30 / n38 / n40 / n41 / n48 / n66 / n70 / n77 / n78 / n79 LTE FDD: B1 / B2 / B3 / B4 / B5 / B7 / B8 / B12 / B13 / B14 / B17 / B18 / B19 / B20 / B25 / B26 / B28 / B30 / B66 / B70 LTE TDD: B34 / B38 / B39 / B40 / B41 / B42 / B43 / B48
Ethernet Speed	10/100/1000Mbps
External Antenna	1 x Celluar, 1 x 2.4GHz & 5GHz
Internal Antenna	1 x Celluar
Resolution	4K@30fps
Power Input	1 x USB Type-C (5V/3A, PD-compatible)
Dimension / Weight	128 x 93 x 33mm / 285g
Other Tools	Datasheet / Firmware / App / Unboxing / Tutorials

1.3 Package Contents

The package includes:

- 1 x Comet 5G (GL-RM10RC)
- 1 x User manual
- 1 x Thank you card
- 1 x Ethernet cable
- 1 x HDMI cable
- 1 x USB cable (Type-A to Type-C)
- 1 x Power adapter
- Converter (Based on your shipping country)



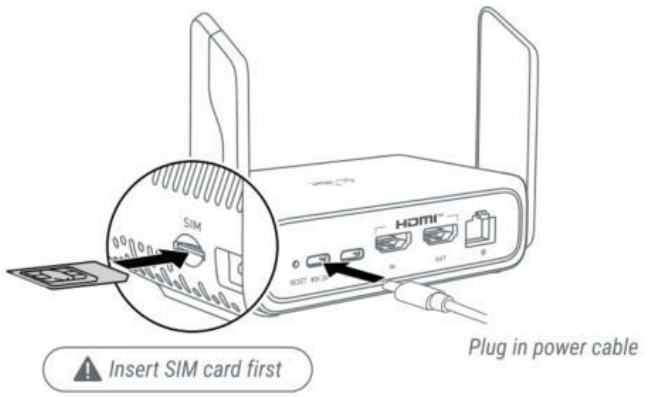
Chapter 2

Hardware Connection

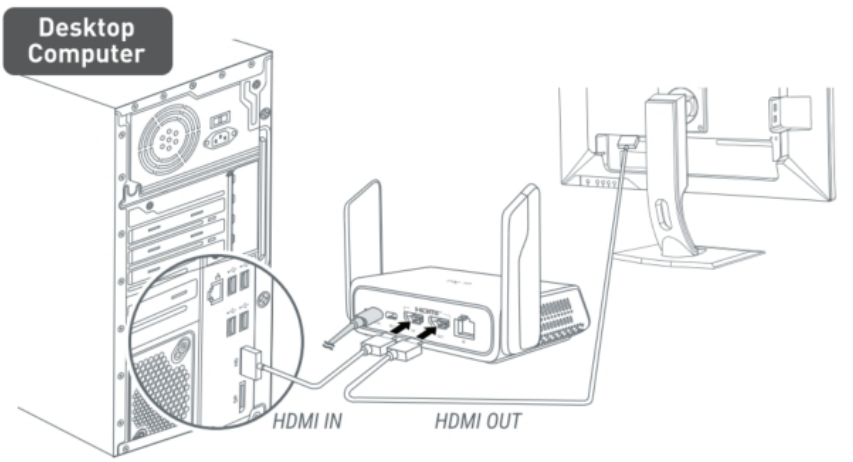
This chapter introduces the basic steps to connect the KVM and related devices.

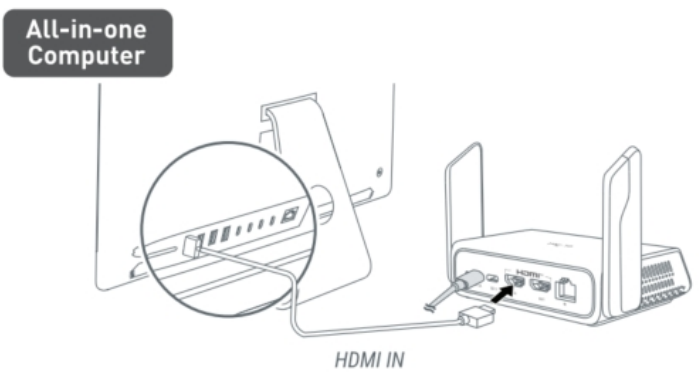
For clarity, Device A refers to the controlling device, and Device B the controlled device.

1. Insert a SIM card into your Comet 5G, and power it on.

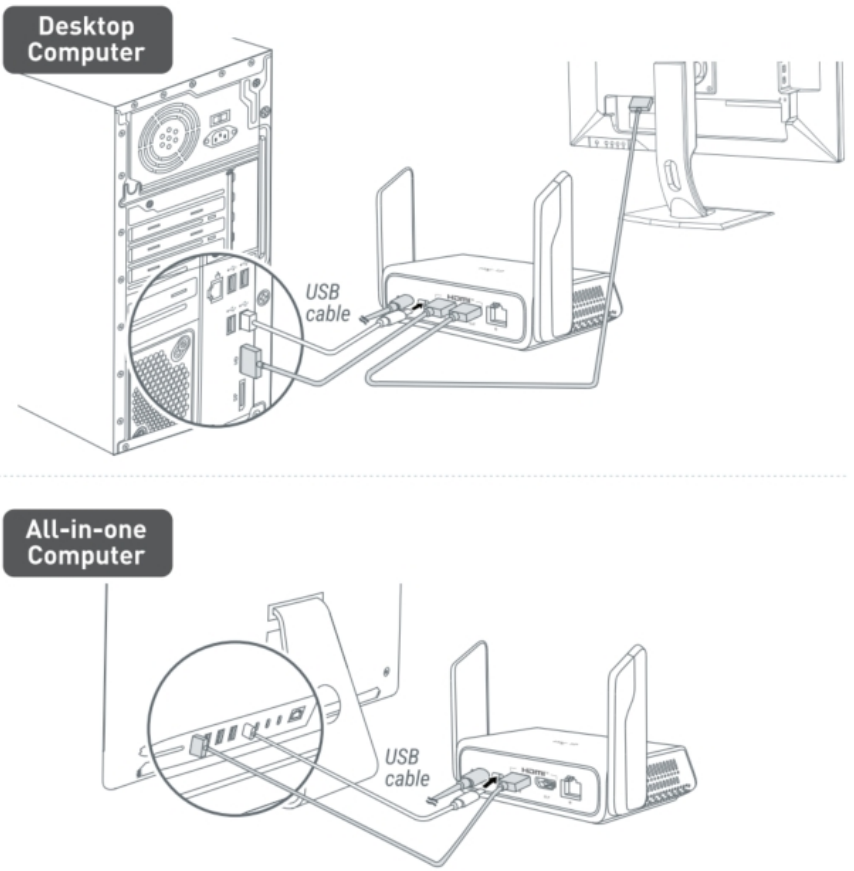


2. Connect Comet 5G's HDMI IN port to the Device B's HDMI port. Use another HDMI cable to connect Comet 5G's HDMI OUT port to an external monitor if necessary.

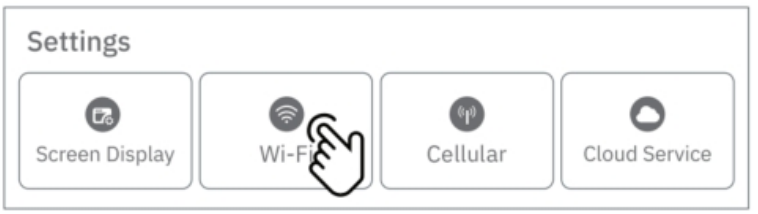




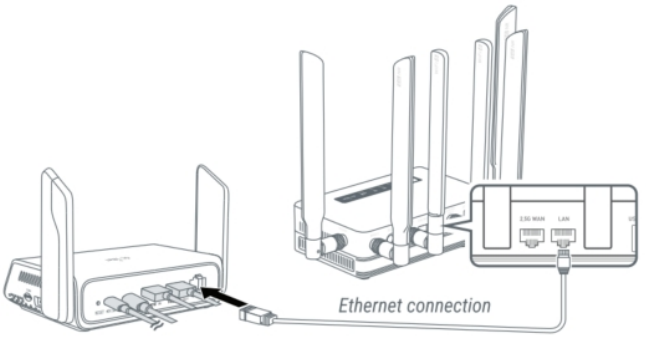
3. Connect Comet 5G's Type-C port to the Device B's Type-C interface using a USB-C cable.



4. Connect Comet 5G to a network source.
    - **5G**: With SIM card inserted, the 5G connection will be automatically established upon system startup.
    - **Wi-Fi**: Swipe left on the touchscreen, and connect Comet 5G to an existing Wi-Fi network (2.4G and 5G supported).



    - **Ethernet**: Connect the Comet 5G's Ethernet port to a network source.



Note: The connection priority is Ethernet > Wi-Fi > 5G. For the complete logic of WAN Network Detection and Failover, please see here.

5. Device connection is complete. Now you can access the Comet 5G's console via nearby control, local access, or remote access.

Chapter 3

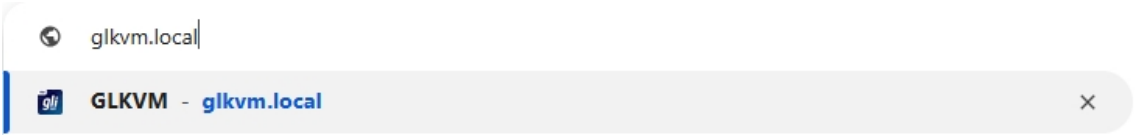
Local Access

This chapter guides you to access your KVM locally via a domain name or an IP address.

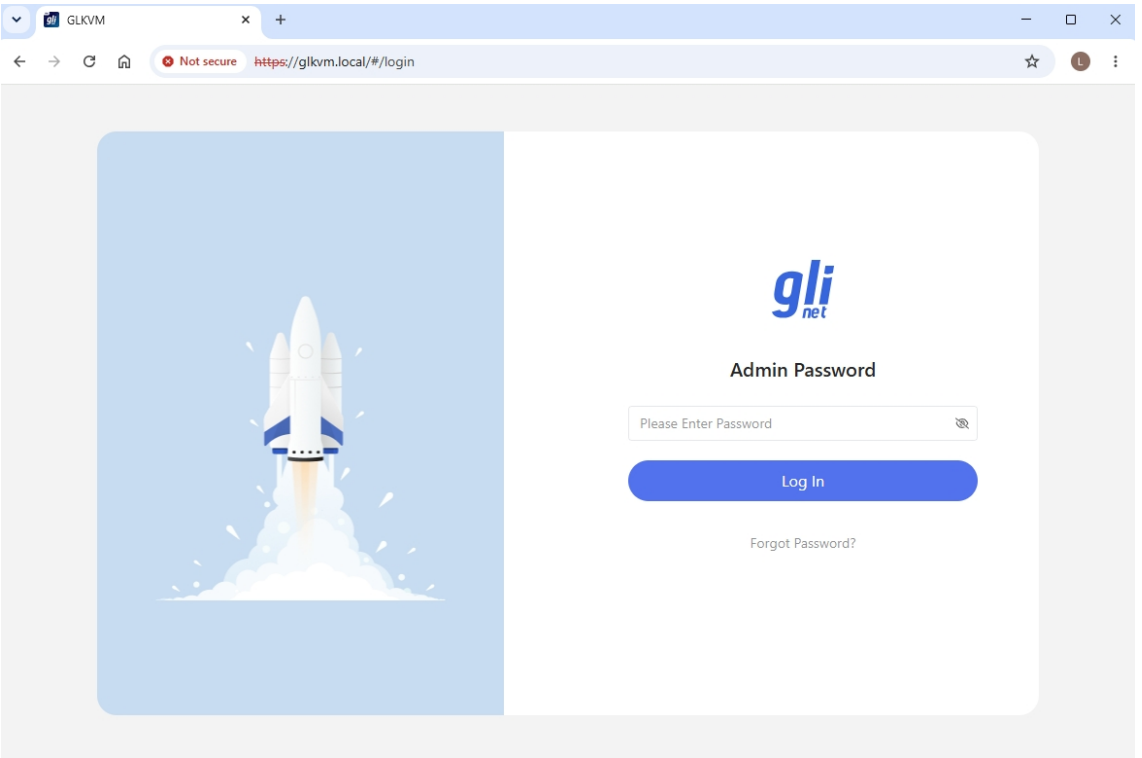
You can access your Comet 5G from the local network via a domain name or an IP address.

3.1 Domain

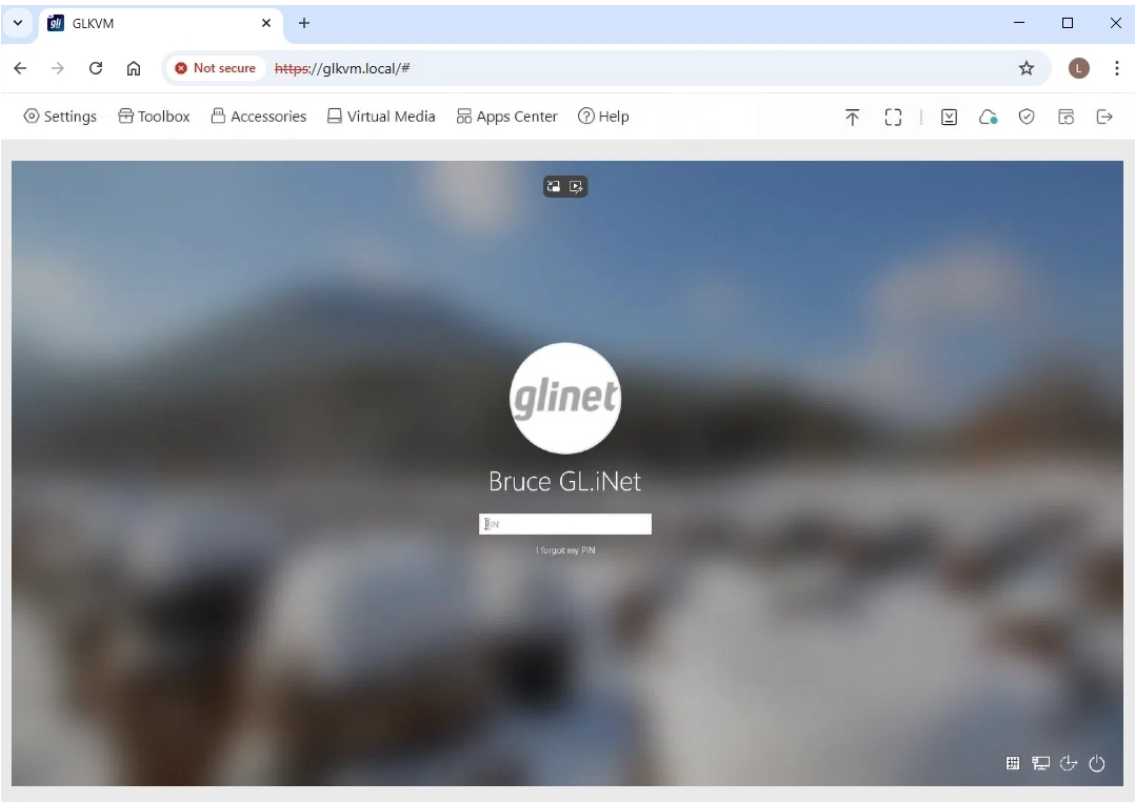
1. Ensure your controlling device is on the same LAN as Comet 5G.
2. Launch a browser on the controlling device. Chrome or Edge is recommended for better compatibility.
3. Enter *glkvm.local* in the address bar.



4. You will be directed to the GLKVM login page. Enter the admin password. You may set up your admin password when accessing for the first time.

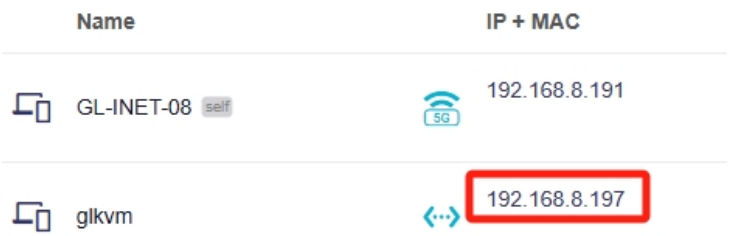


5. You will then access the Comet 5G's console locally and gain access to the controlled device.

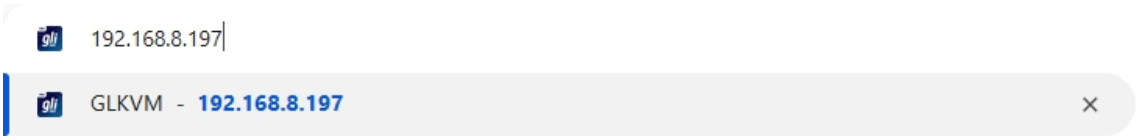

GLKVM
Not secure
https://glkvm.local/#
Settings
Toolbox
Accessories
Virtual Media
Apps Center
Help
glinet
Bruce GL.iNet
PIN
I forgot my PIN

3.2 IP Address

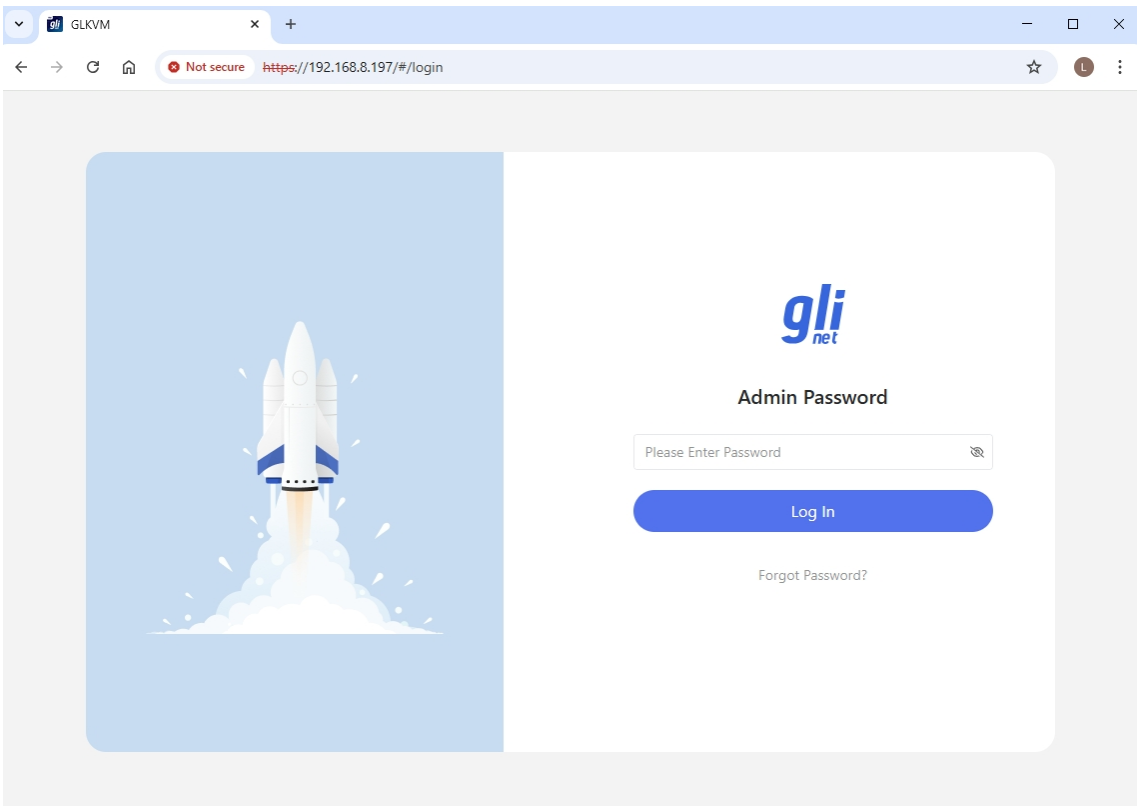
1. Ensure your controlling device is on the same LAN as Comet 5G.
2. Find Comet 5G's IP address in the upper router.
   For example, Comet 5G is connected to a GL.iNet router GL-AXT1800. Log in to the router's web admin panel, find Comet 5G's IP address in the Client list, as shown below.



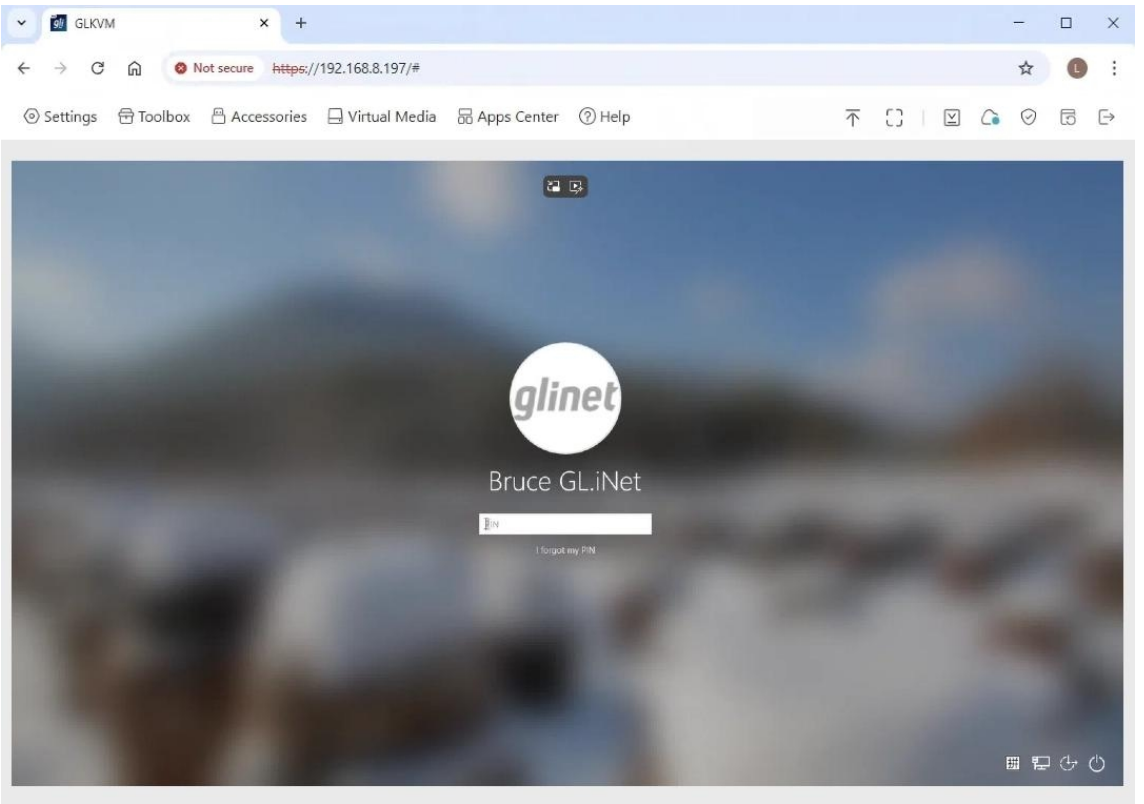
3. Open a new tab in the browser and enter the IP address.



4. You will be directed to the GLKVM login page. Enter the admin password. You may set up your admin password when accessing for the first time.



5. You will then access the Comet 5G's console locally and gain access to the controlled device.



Chapter 4

Remote Access

This chapter introduces multiple ways to access your KVM remotely.

4.1 Cloud Service

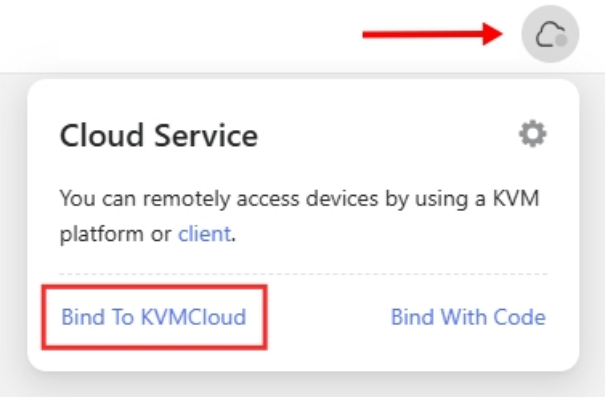
4.1.1 Bind Device

Bind your KVM device to the Cloud. **This needs to be done on the local network.**

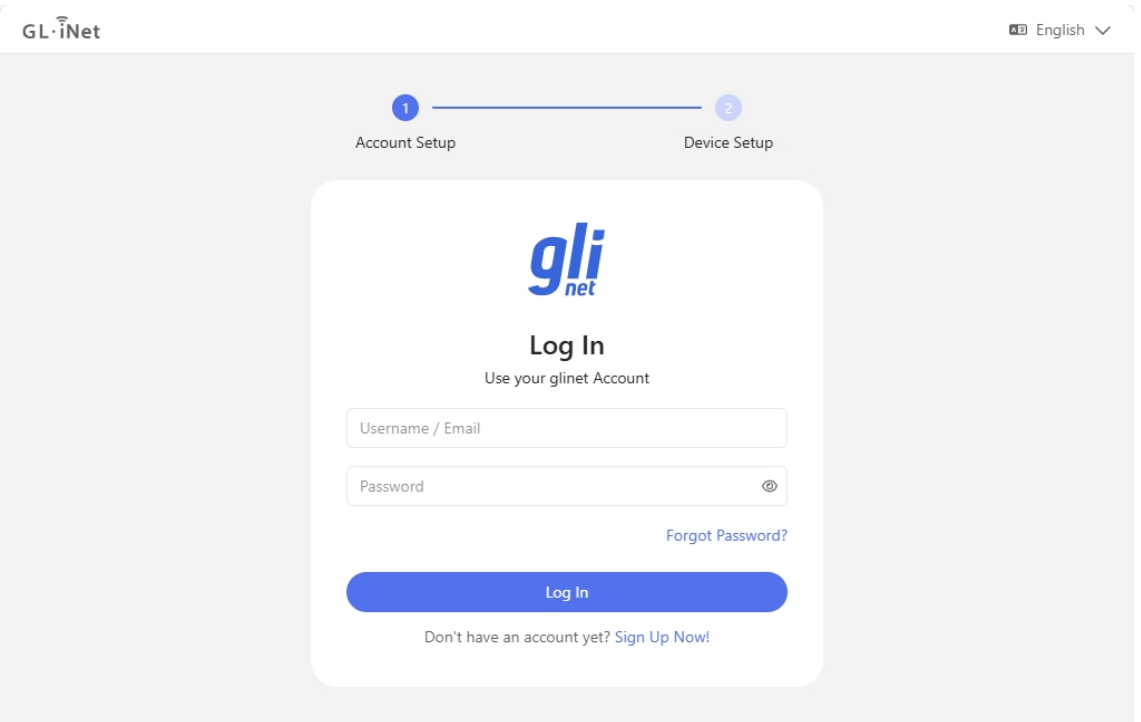
You can bind your KVM to the Cloud via regular steps or via dynamic code.

Here we take the regular steps as an example. If you prefer Dynamic Code Binding, click here for details.

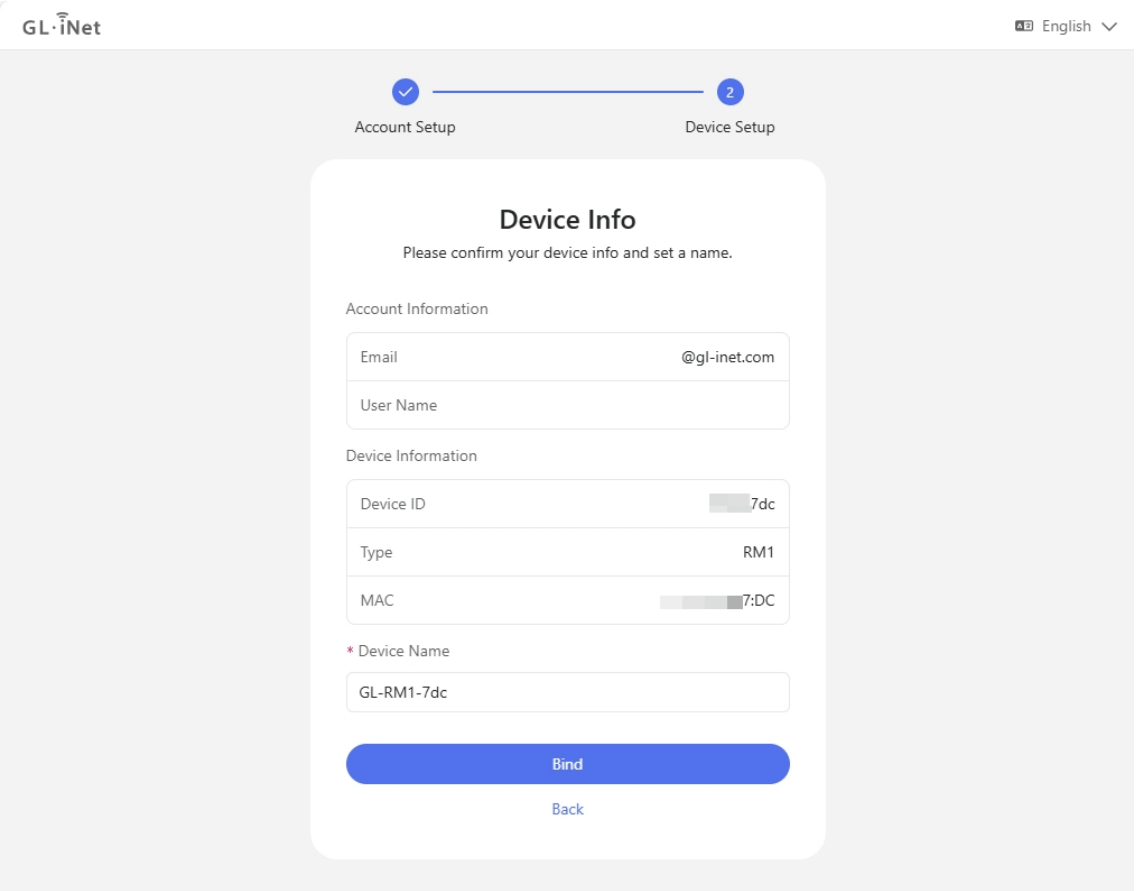
1. Log in to your KVM console locally and navigate to **Cloud Service** in the upper right corner. Click **Bind To Cloud**.



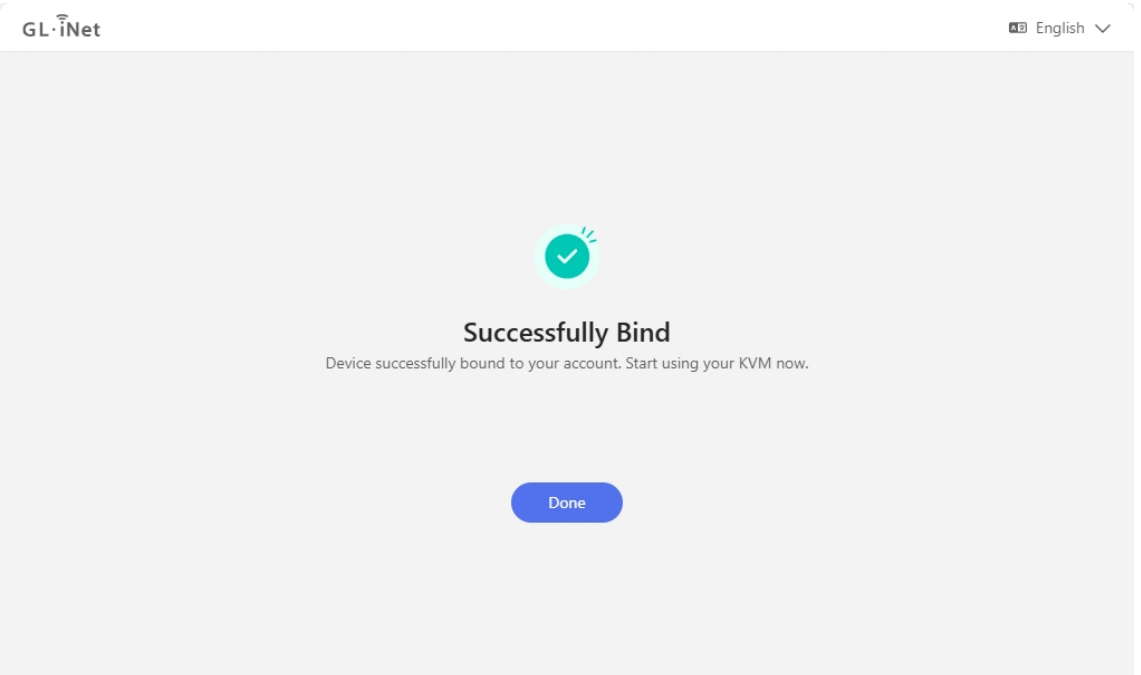
2. You will be redirected to a login page. Log in with your glinet cloud account.



3. Confirm your device info, and click **Bind**.

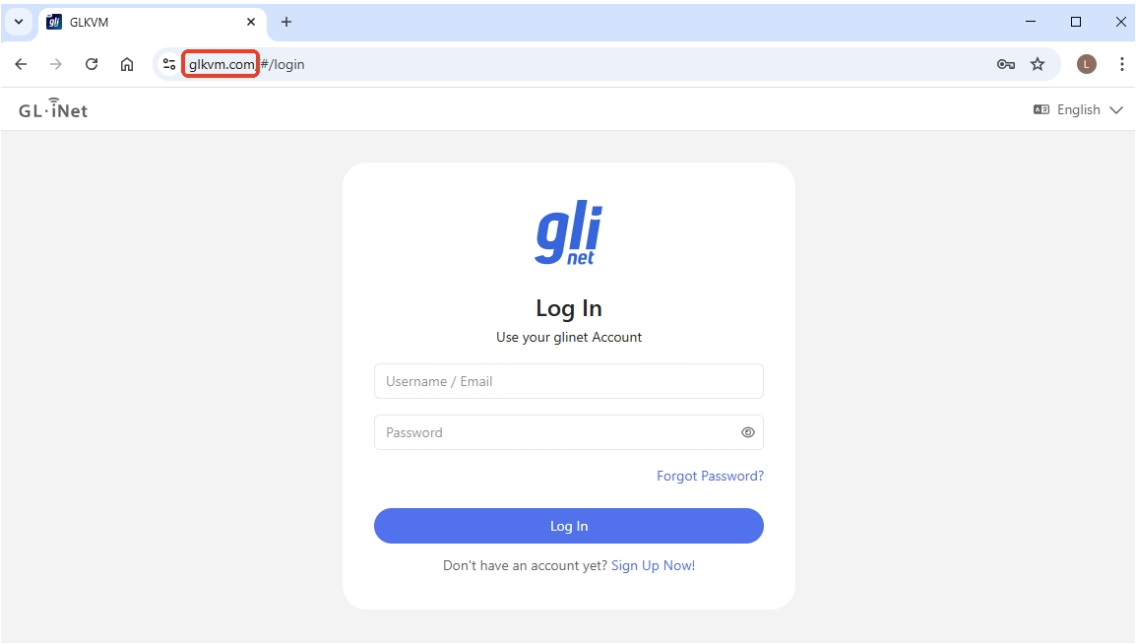


4. Wait a second and your device will be bound to your account successfully.

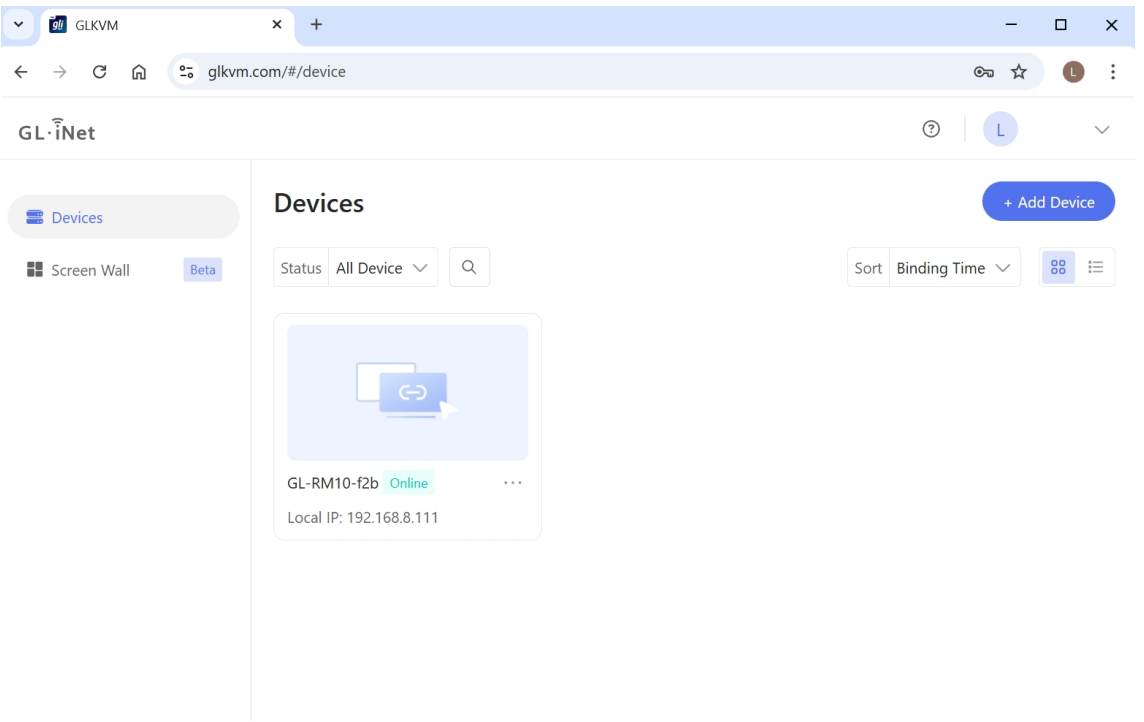


4.1.2 Remote Access via Cloud

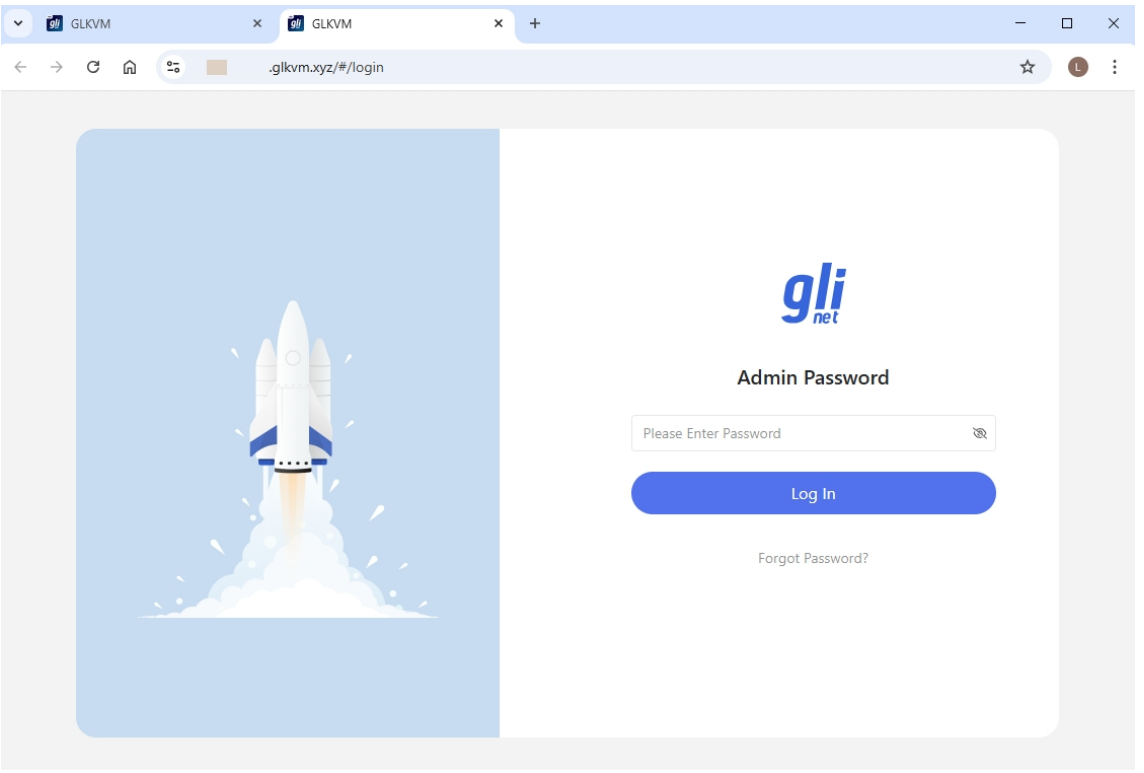
1. Open a browser (take Google Chrome as an example), and enter *glkvm.com* in the address bar. You will see a login page. Use your glinet account to log in.



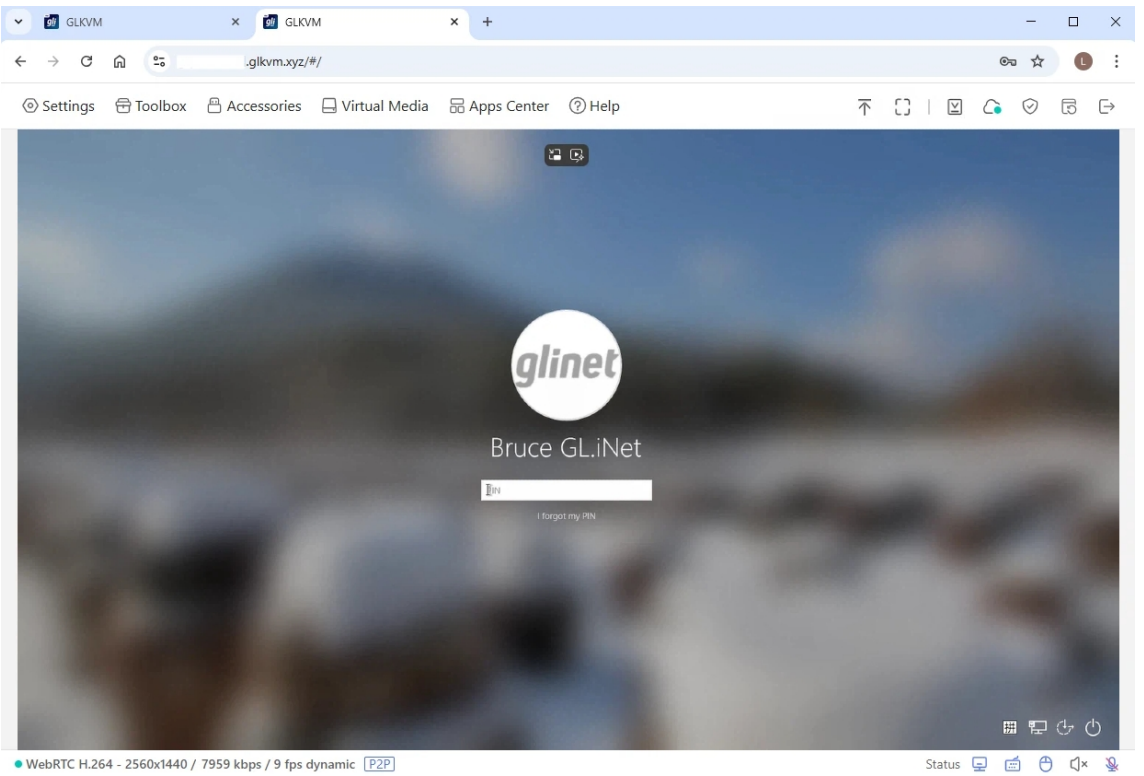
2. After login, you will see the devices bound to your account. Click on the device you want to remotely access.



3. In the newly opened webpage, enter your admin password to log in.



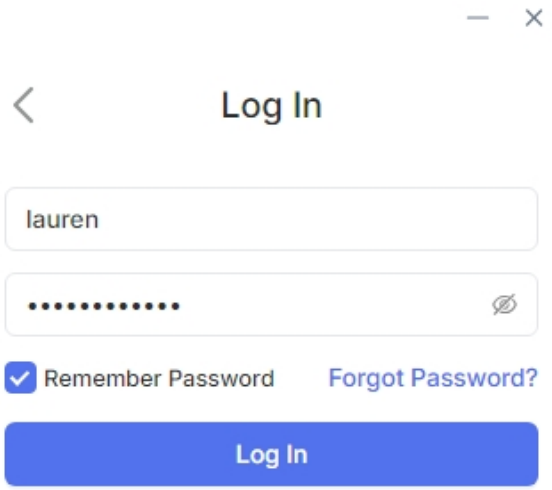
4. You will then be able to remotely access the KVM and the controlled device via Cloud, without installing the app.



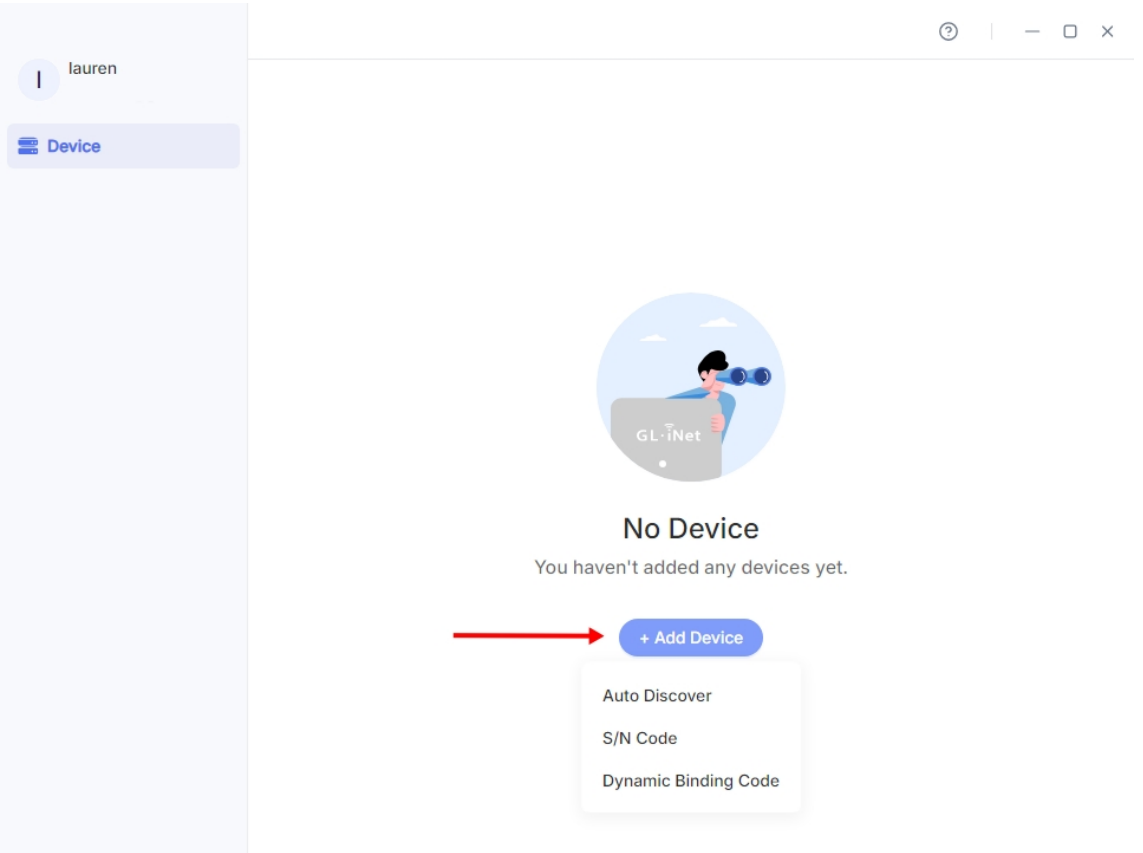
4.2 GLKVM App

4.2.1 Bind Device

1. Install the GLKVM App on your controlling device.
2. Log in with your GL.iNet account. If you don't have one, sign up first and log in.



3. After logging in, click **Add Device**.

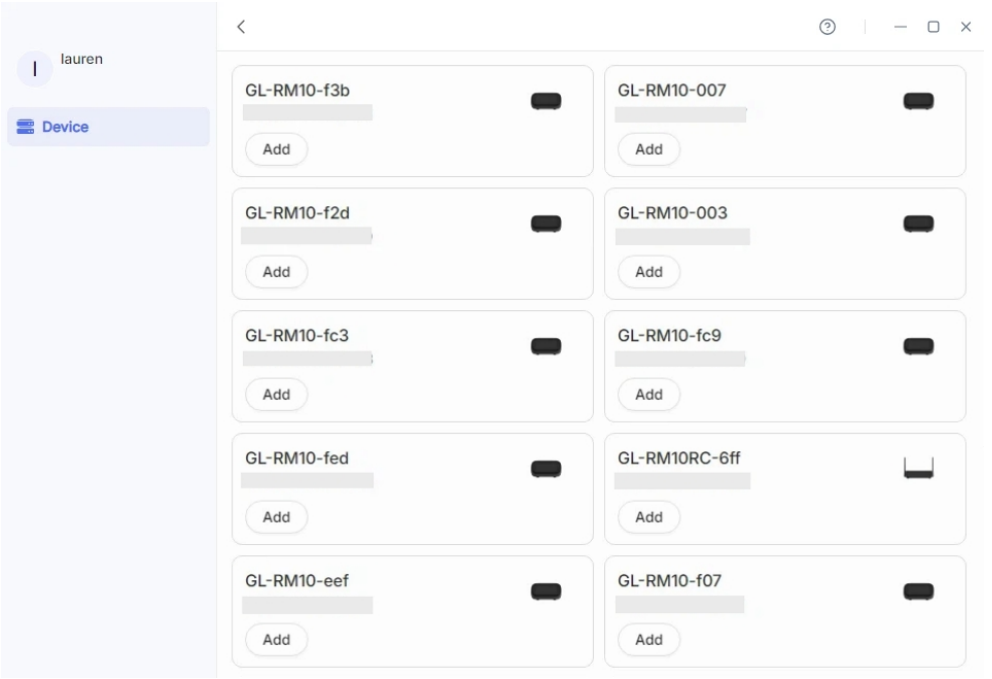


4. Bind your device in three ways: Auto Discover, S/N Code, and Dynamic Binding Code.

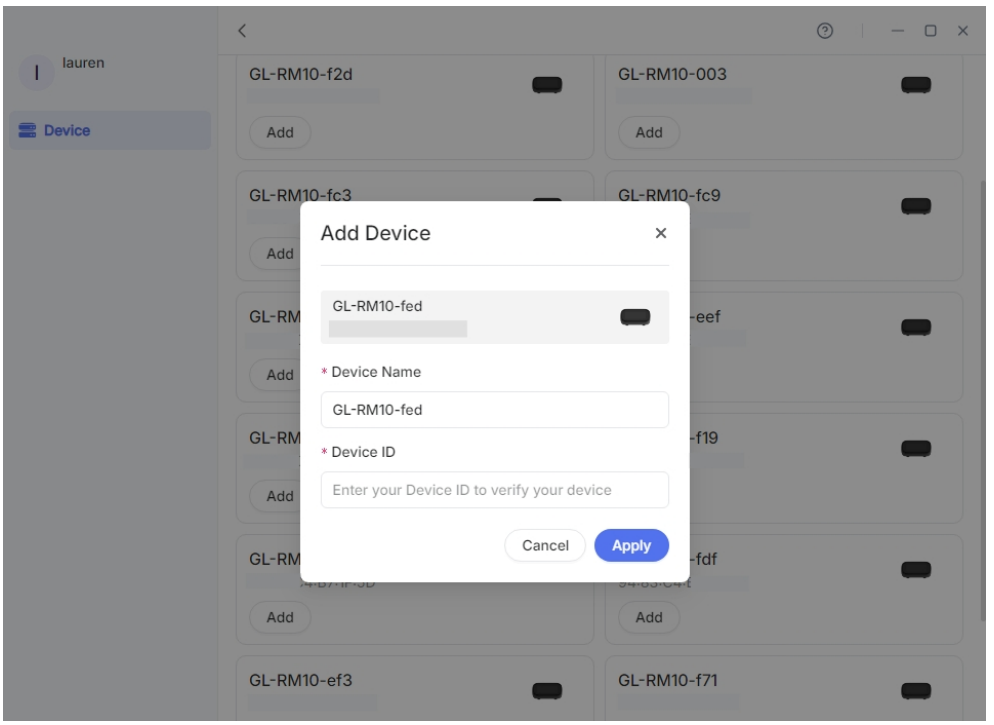
   (1) **Auto Discover**

   Ensure your controlling device is on the same LAN as Comet 5G.

   Click **Auto Discover**. It will start searching automatically.



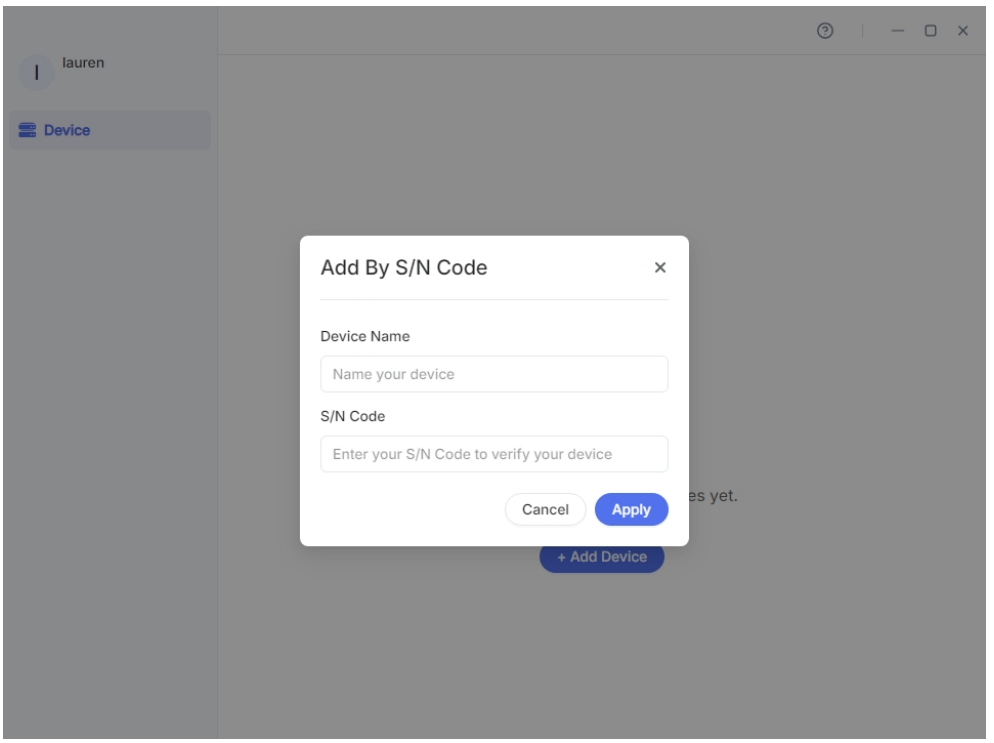
   Find your KVM and enter its **Device ID** to bind it to your account.



(2) **S/N Code**

This applies to the scenario where your KVM is not detected, or is not on the same LAN, but you have its serial number (S/N).

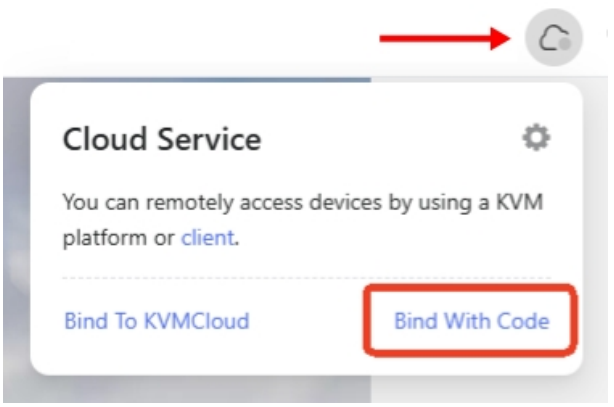
Click **S/N Code**. In the pop-up window, customize the device name and enter the S/N, which is printed on the label bottom of your KVM device.



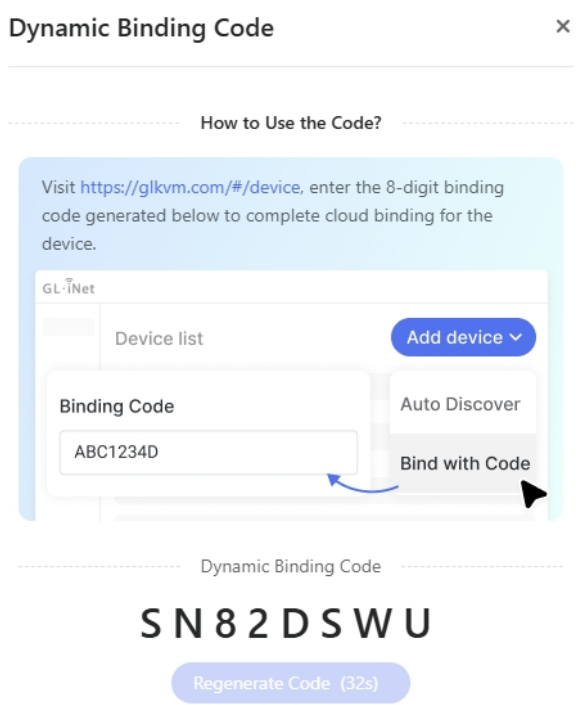
(3) **Dynamic Binding Code**

This needs to be done on the local network. Ensure your controlling device is on the same LAN as Comet 5G.

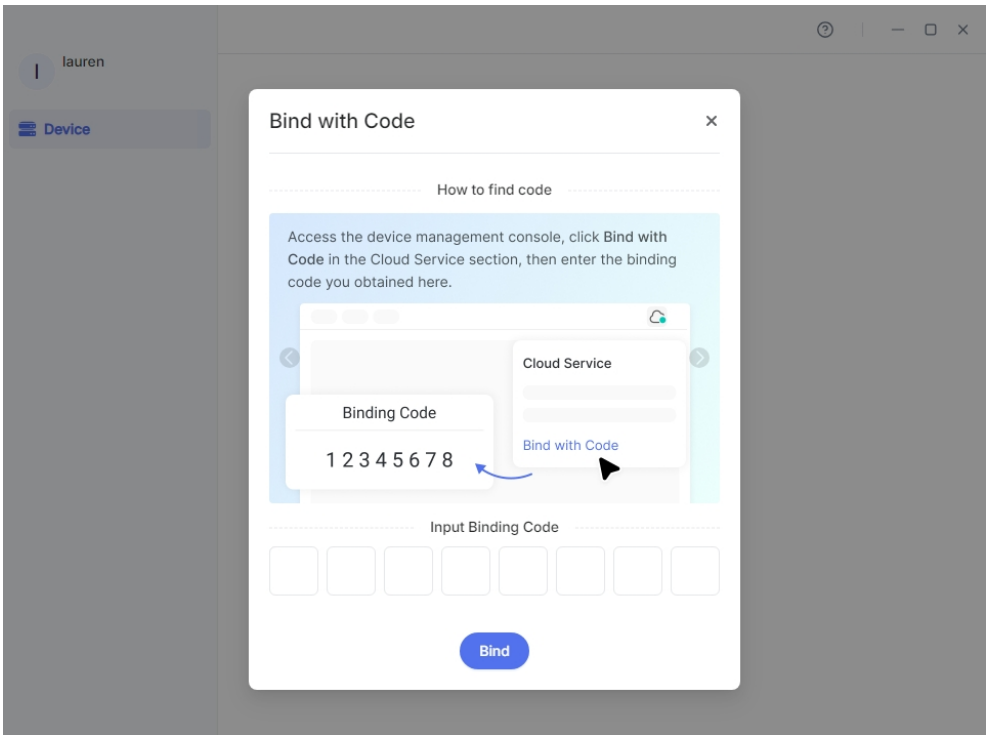
a. Log in to your KVM locally using domain or IP address, and navigate to **Cloud Service** in the upper-right corner. Click **Bind With Code**.



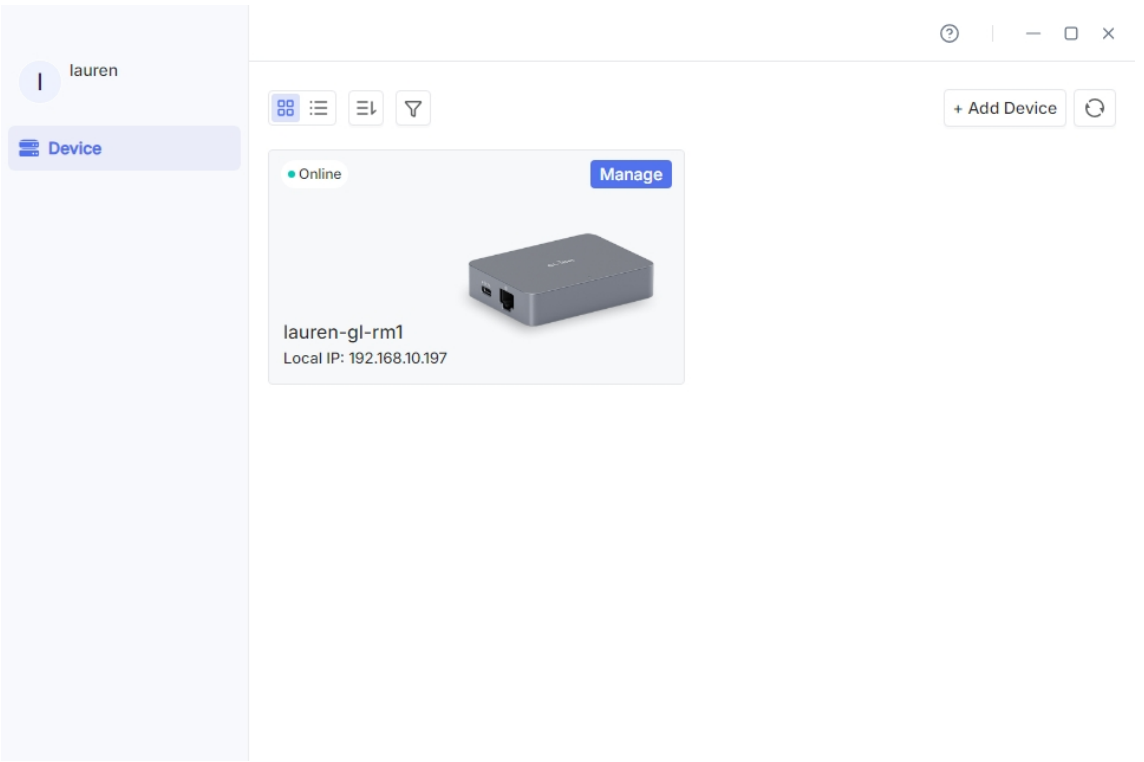
b. It will generate **an 8-digit dynamic code** randomly for device binding, valid for 60 seconds. Copy this code.



c. Back to the GLKVM app, enter the dynamic binding code and click **Bind**.

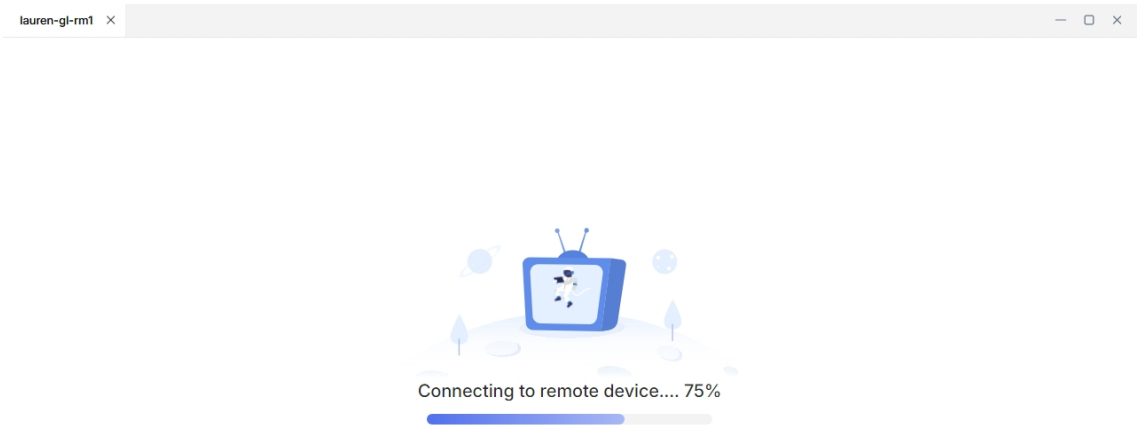


5. Once your KVM device is bound to your account, it will show "Online" in the app.

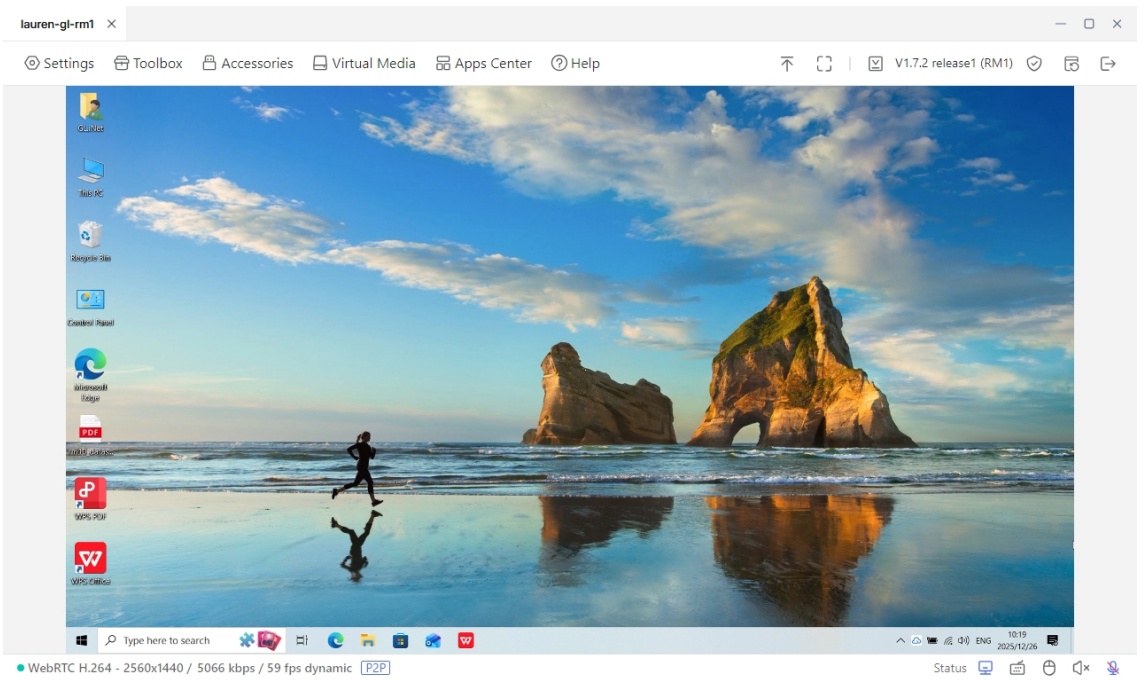

lauren
Device
+ Add Device
Online
Manage
lauren-gl-rm1
Local IP: 192.168.10.197

4.2.2 Remove Access via GLKVM App

1. Click your KVM device. It will open a new window and start connecting.



2. Once connected, enter the admin password to log in to your device.
3. You will then access the KVM and the controlled device remotely via GLKVM App.

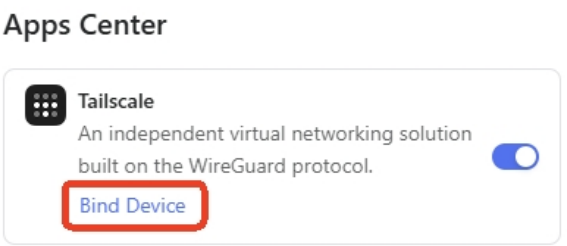


4.3 Tailscale

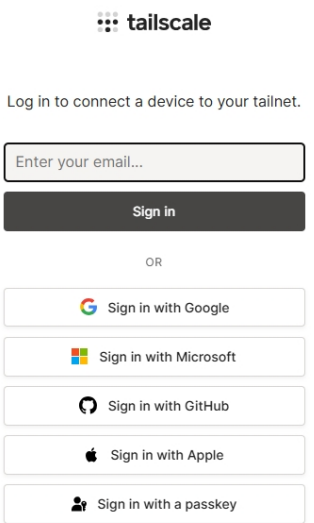
GL.iNet KVM integrates Tailscale®, allowing you to bind it to the Tailscale virtual network for remote access — no need to install the GLKVM app or use the cloud service. This is useful when your controlling device does not run Windows, macOS, Android, or iOS (and thus cannot install the GLKVM app), or when you do not want to use the GLKVM app or cloud service.

4.3.1 Bind KVM

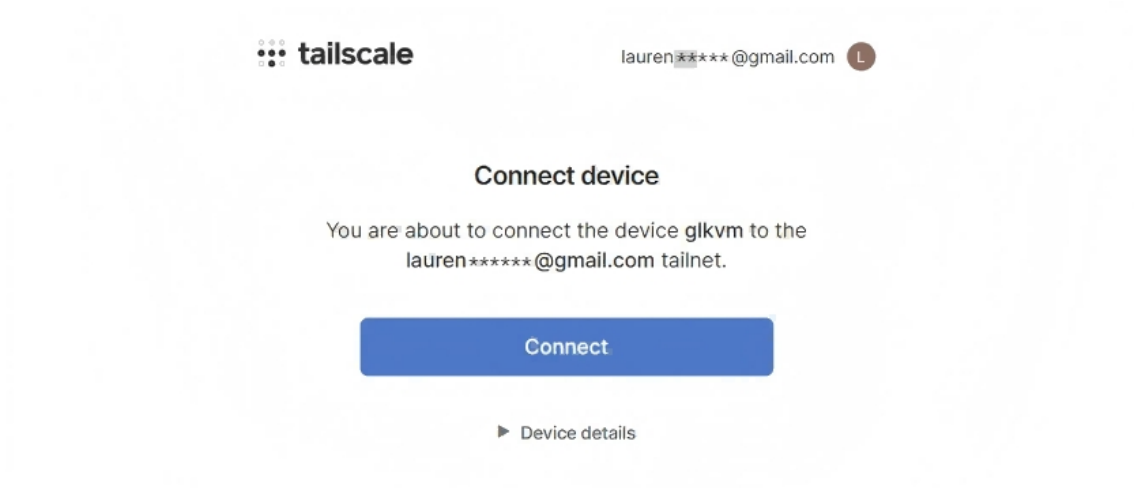
1. Connect your KVM and the controlling device to the same local network.
2. On the controlling device, log in to your KVM console locally via its domain or IP address, then go to **Apps Center** > **Tailscale**. Enable Tailscale and click **Bind Device**.



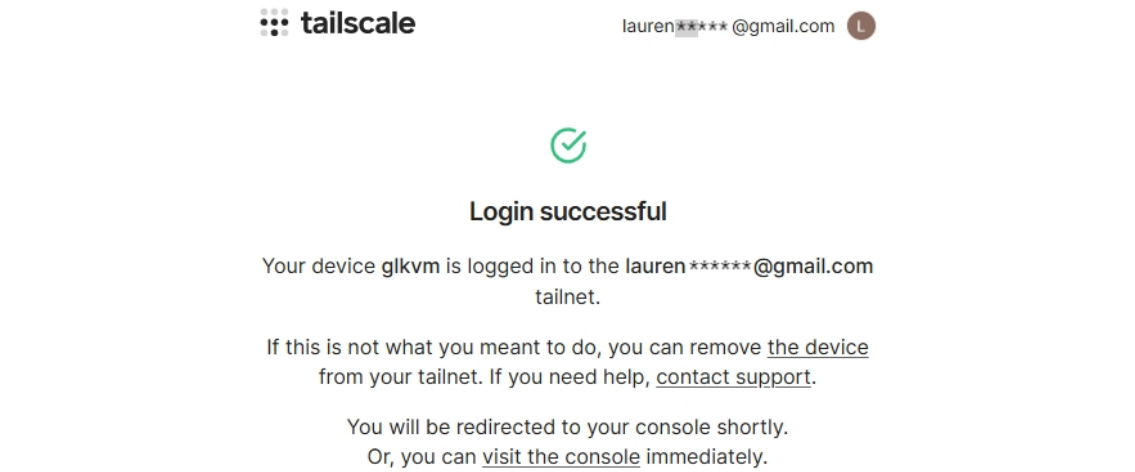
3. You will be directed to the Tailscale login page. Enter your email to log in.



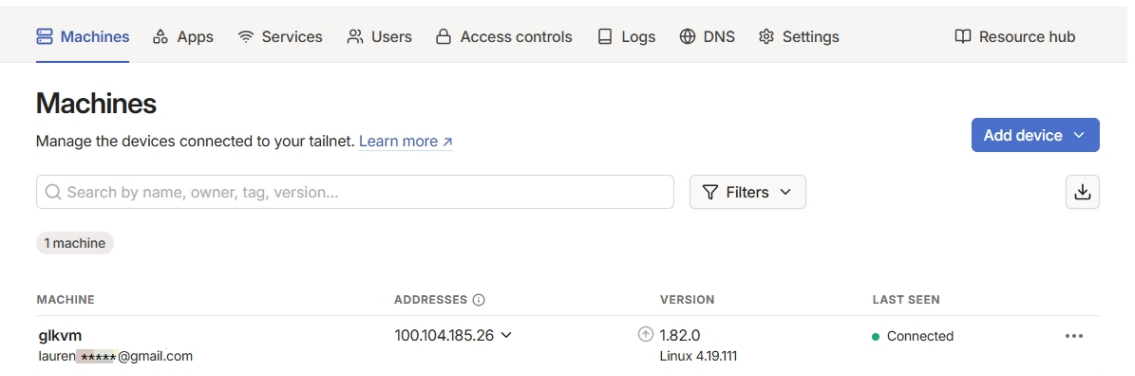
4. After logging in, the page prompts that you are about to connect the device glkvm to your Tailnet. Click **Connect**.



5. Your KVM device will then be bound to your tailnet successfully.



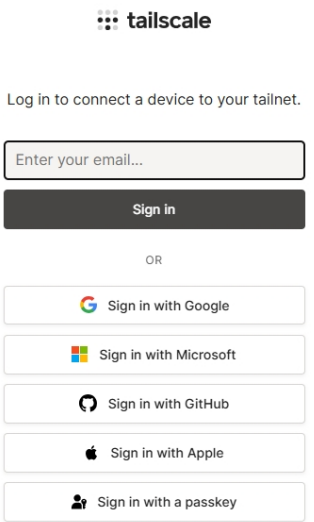
6. You will be redirected to your Tailscale console, where a device **glkvm** is displayed under **Machines**.



4.3.2 Bind Controlling Device

The example below demonstrates how to bind a Windows laptop (as the controlling device) to the Tailscale network.

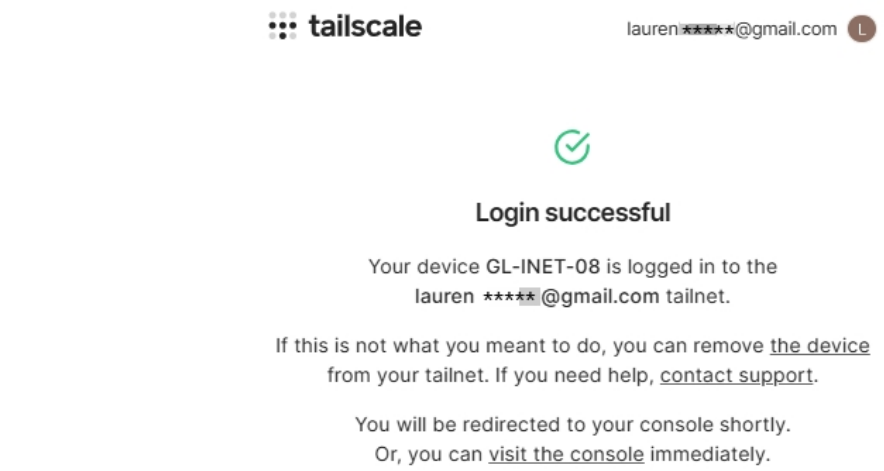
1. Install Tailscale on your laptop from Tailscale Download Center.
2. Run Tailscale on the laptop and log in with the same email.



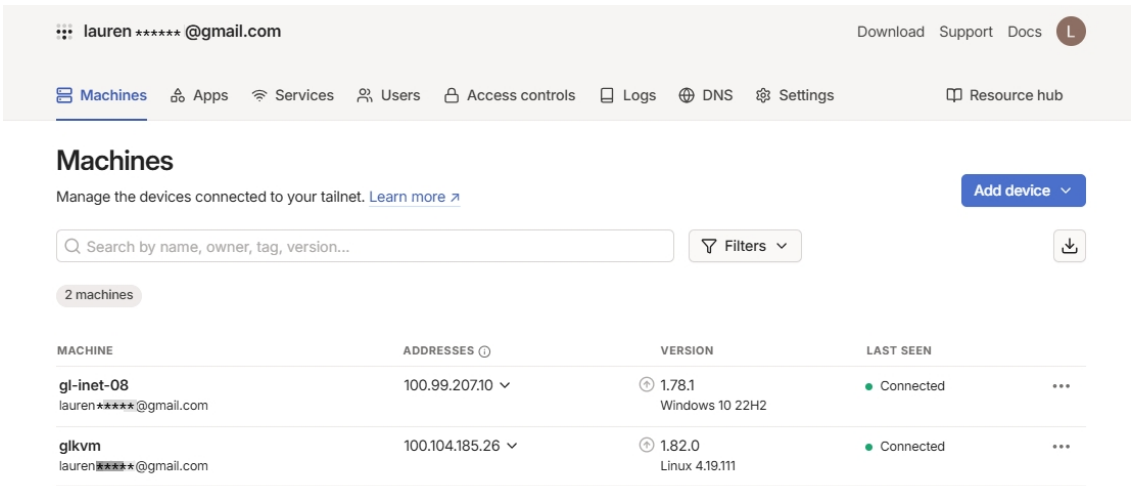
3. After logging in, the page prompts that you are about to connect the laptop (e.g. the controlling device) to your Tailnet. Click **Connect**.



4. Your laptop will then be bound to your tailnet successfully.

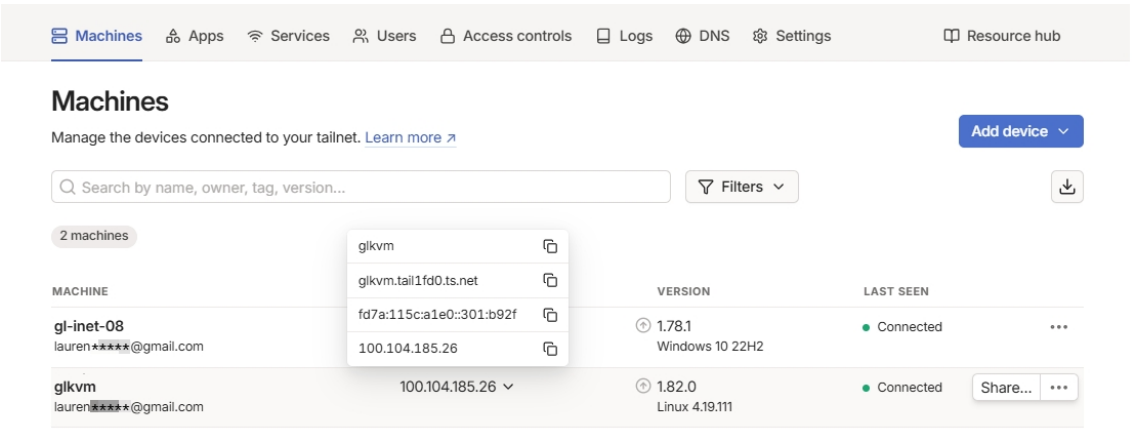


5. You will be redirected to your Tailscale console, where the controlling device is also displayed under **Machines**.

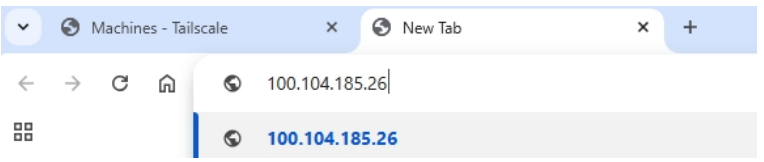


4.3.3 Remote Access via Tailscale

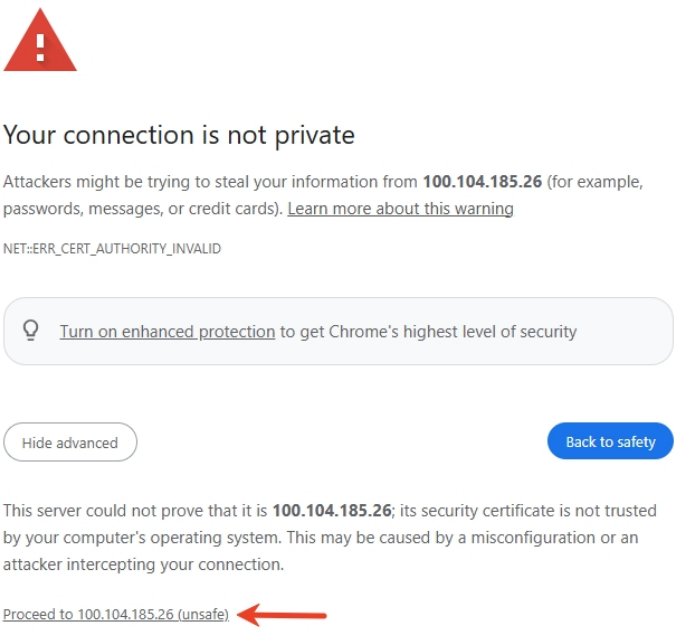
1. In the Tailscale console, click the **glkvm's Address** (100.104.185.26 in this example).



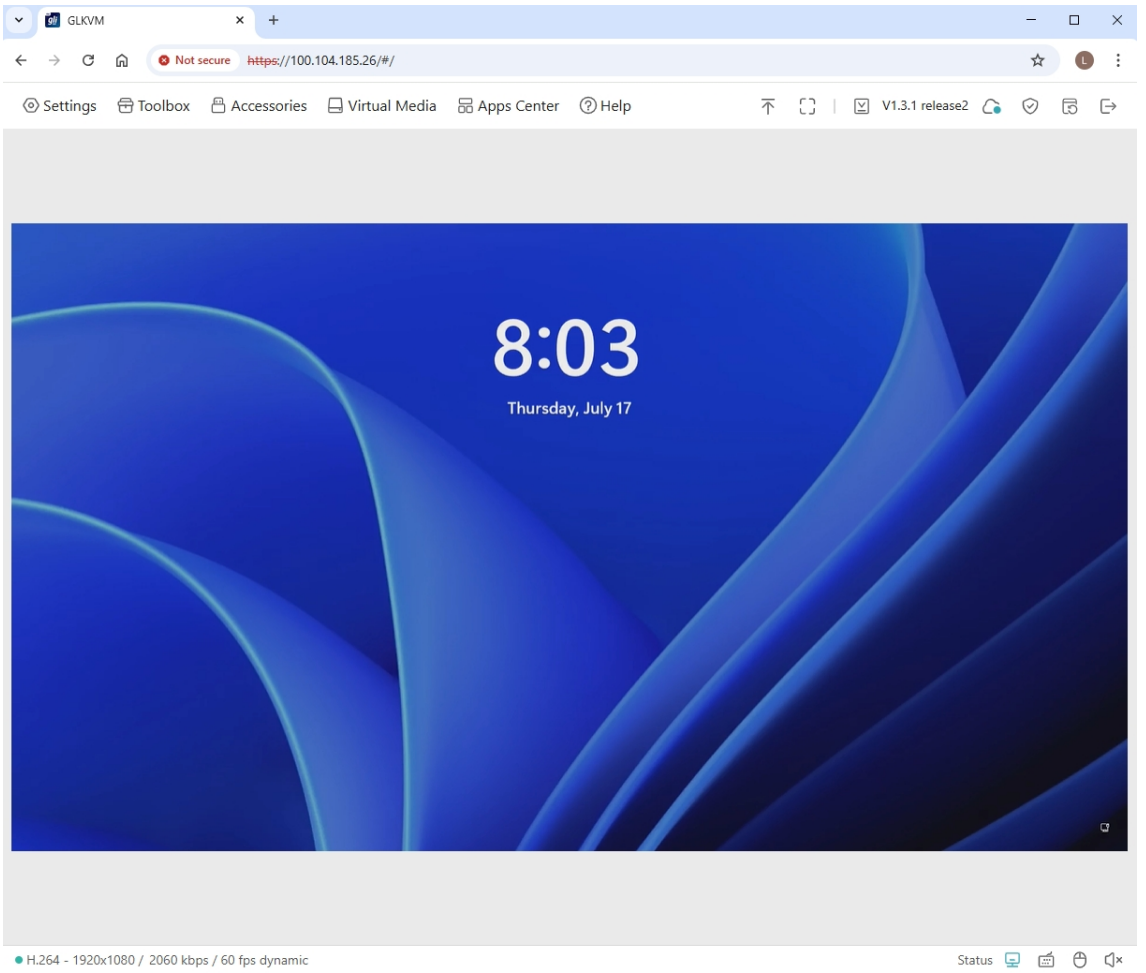
2. You will see four values, which are assigned by Tailscale for device identification and virtual network communication. You can remotely access your KVM using any of them.
3. Take the virtual IPv4 as an example. Copy the virtual IPv4 address of your KVM device, then open a new tab and enter the IP address into the address bar.



Tip: If a privacy error appears, click **Advanced**, then **Proceed to 100.104.185.26**. Click here for details about the privacy error.



4. You will be redirected to the GLKVM login page. Enter your admin password to log in.
5. Then you can access your KVM and the controlled device via the Tailscale virtual IP.

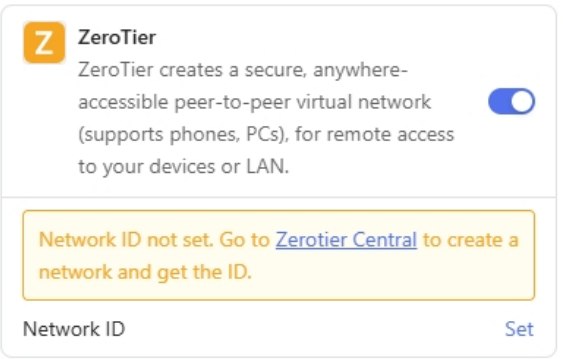


4.4 ZeroTier

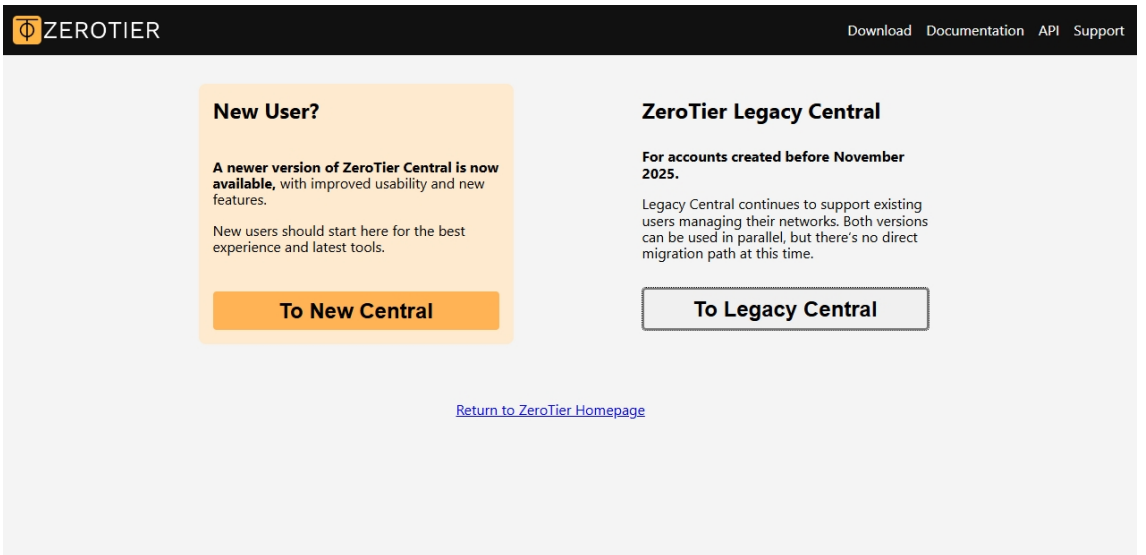
GL.iNet KVM integrates ZeroTier, allowing you to bind it to the ZeroTier network for remote access — no need to install the GLKVM app or use the cloud service.

4.4.1 Bind KVM

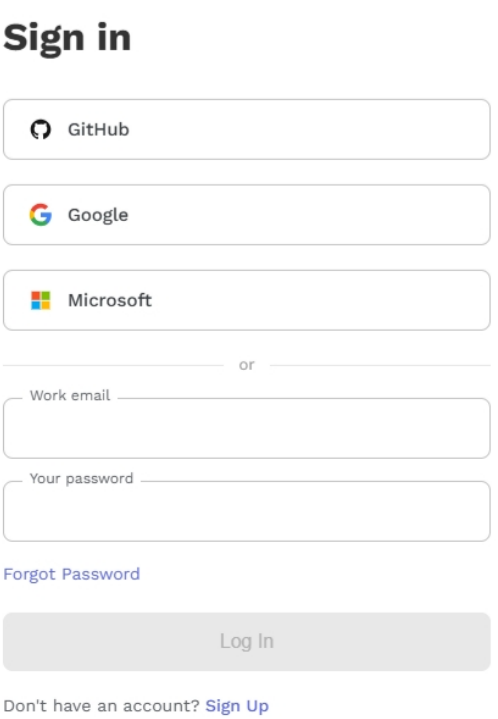
1. Connect your KVM and the controlling device to the same local network.
2. On the controlling device, log in to your KVM console locally via its domain or IP address, then go to **Apps Center** > **ZeroTier**. Enable ZeroTier, and you will see a yellow prompt as shown below. Click the hyperlink or here to sign in to ZeroTier Central.



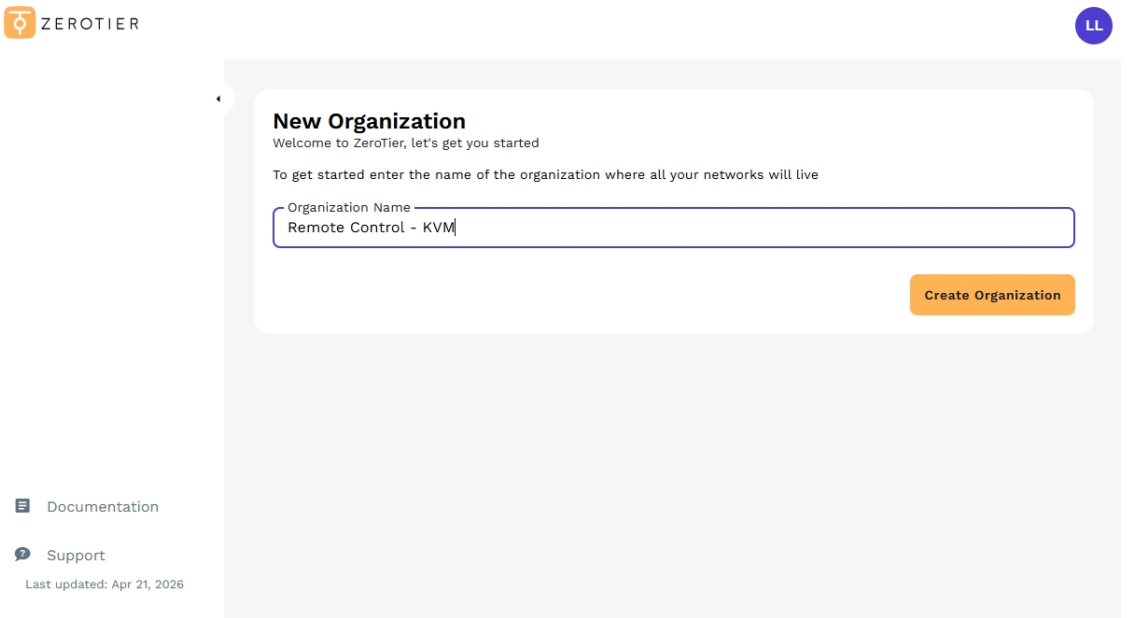
3. When signing in to ZeroTier for the first time, you may be asked to select between **New Central** and **Legacy Central**. Select the appropriate version to proceed.



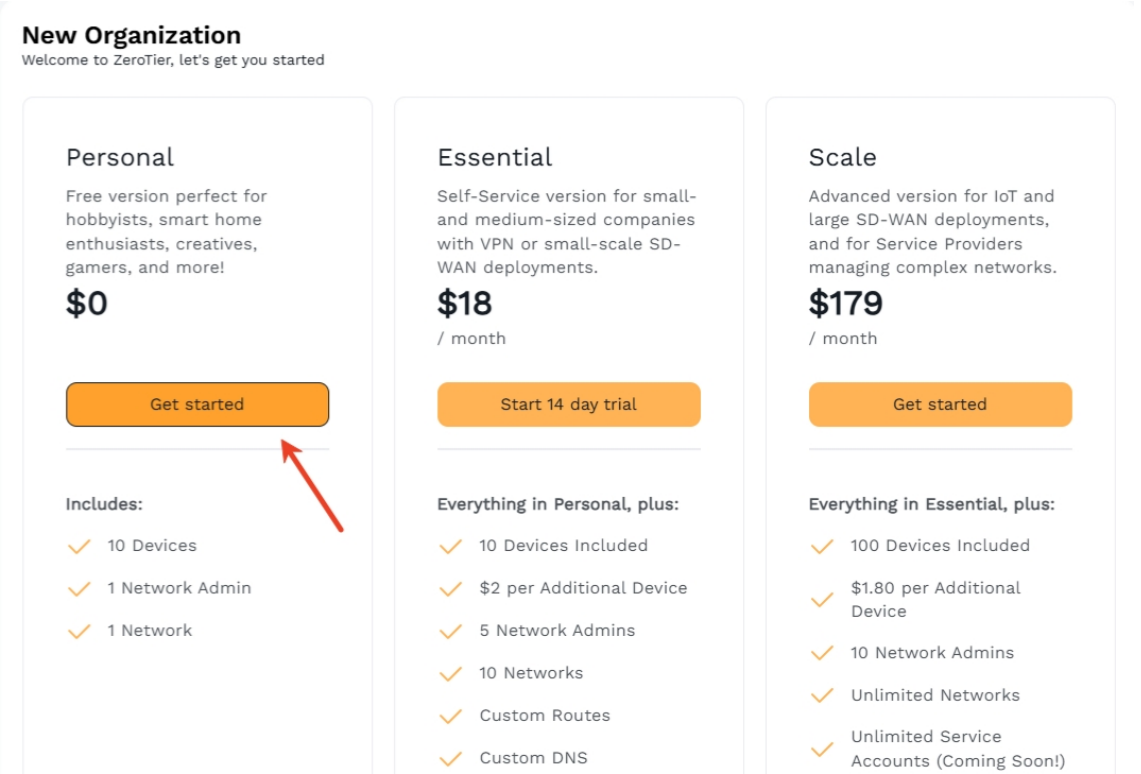
4. Take New Central as an example. Sign in with your email and password. If you don't have an account, sign up first.



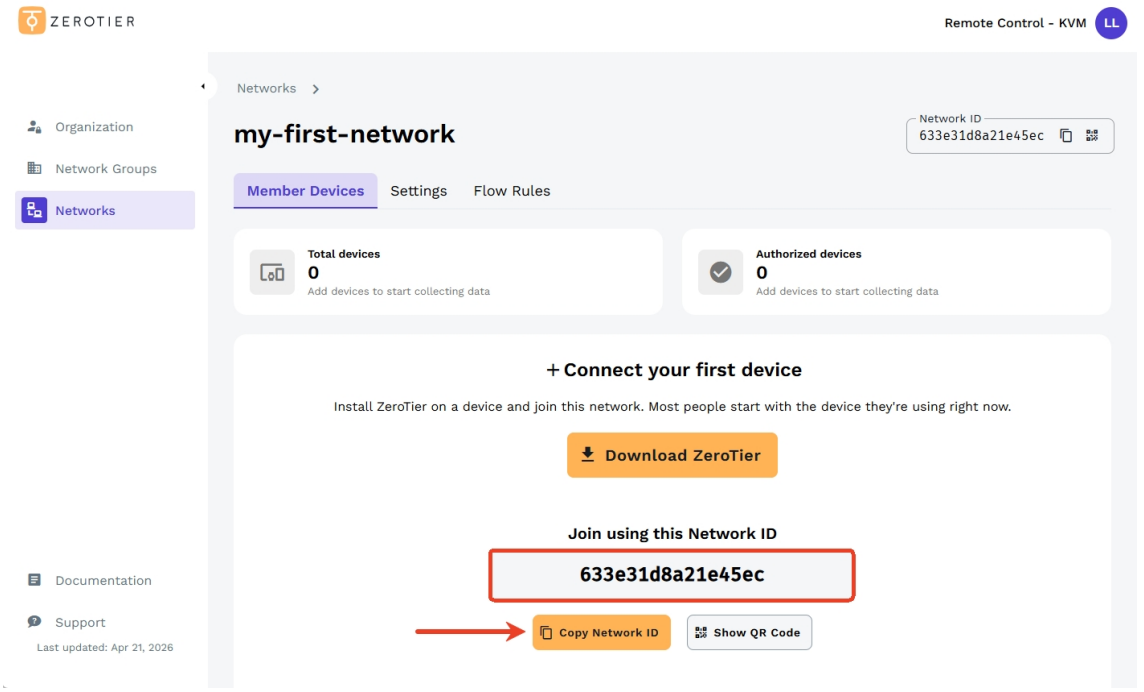
5. After signing in, create an organization.



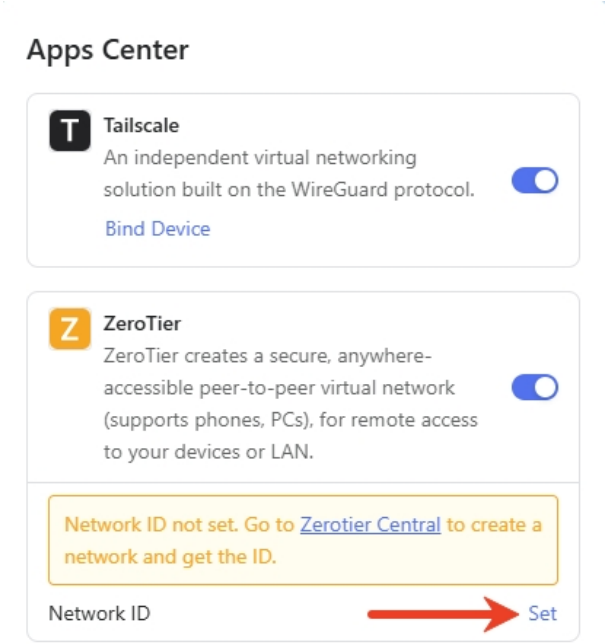
6. Select a plan. Here we choose **Personal plan** as an example, which includes 10 devices, 1 network admin, and 1 network. If you need to create more networks, add more devices, or add custom routes and DNS, choose **Essential** or **Scale plan**.



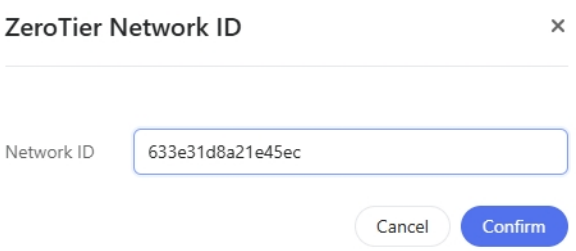
7. Now your ZeroTier network has been created. Copy the **Network ID**, which is **a 16-character alphanumeric string**. You will need it later when adding devices to your ZeroTier network. Keep this tab open.



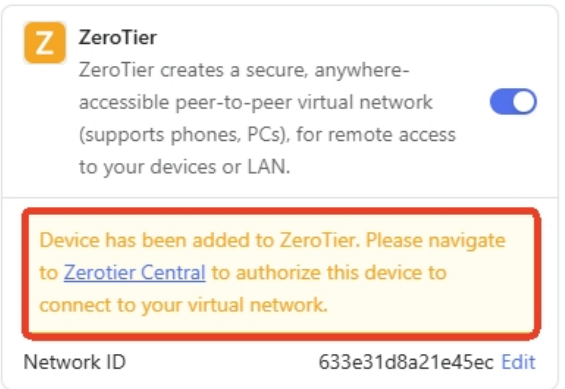
8. Go back to your KVM console and navigate to **Apps Center** > **ZeroTier**. Click **Set**.



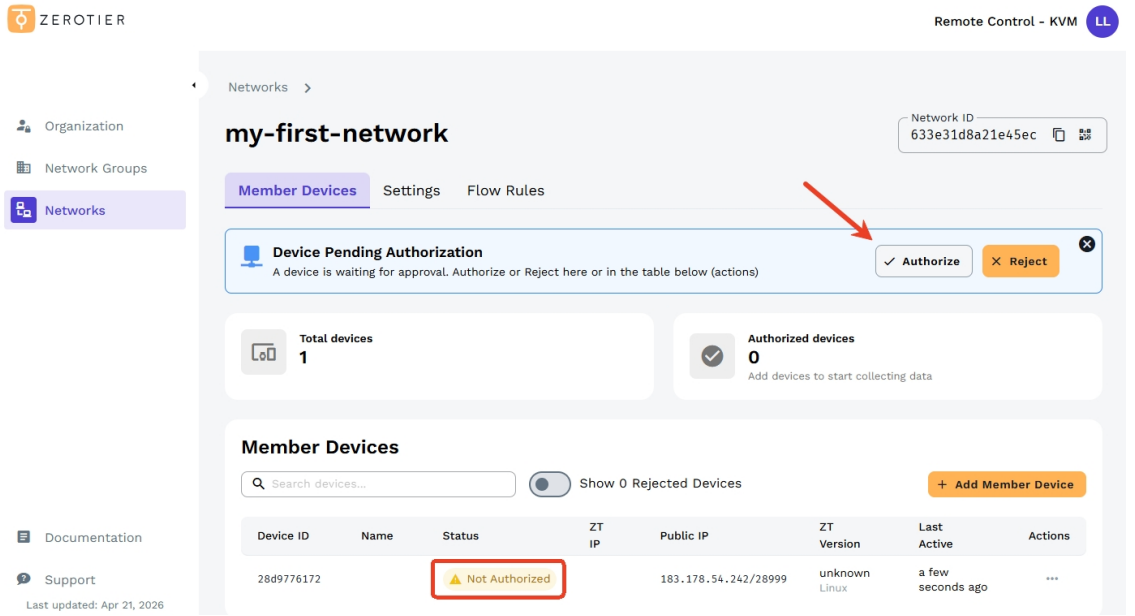
9. In the pop-up window, paste the **Network ID** and click **Confirm**.



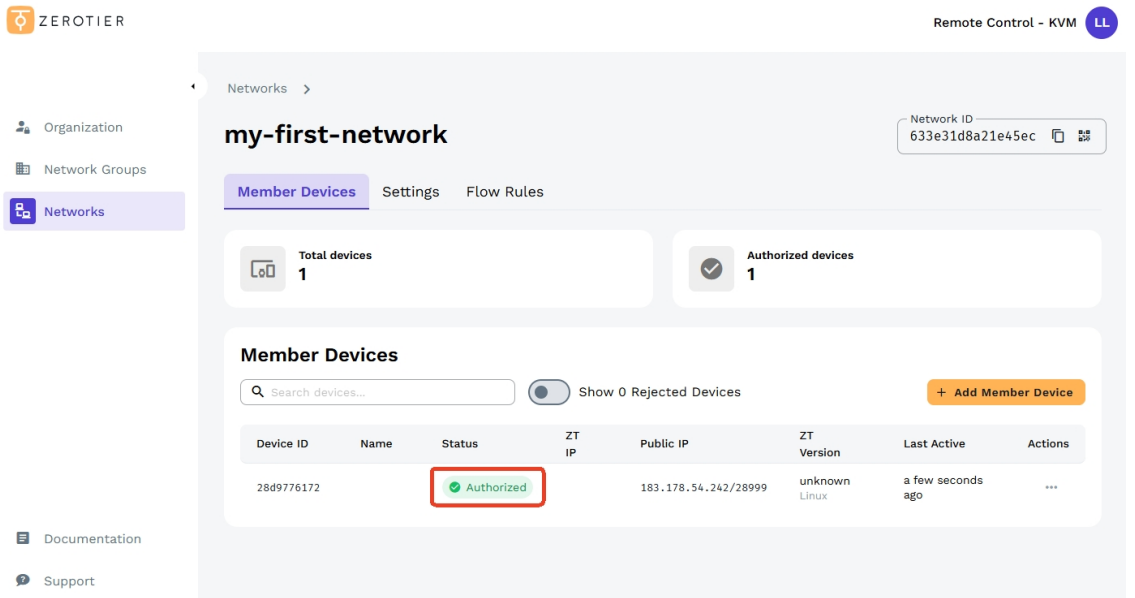
10. A prompt appears on the console, indicating that this device needs to be authorized.



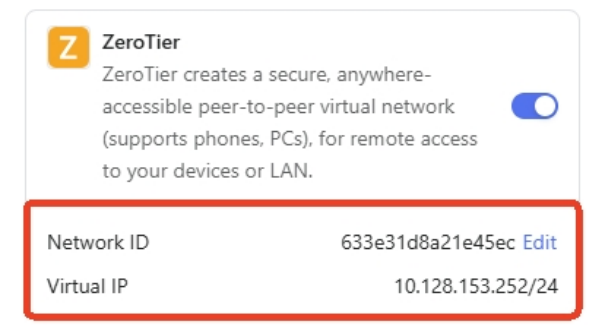
11. Go back to ZeroTier Central. You will see a device (your KVM) waiting for approval. Click **Authorize**.



12. Once authorized, the status will change to Authorized in green, as shown below.



13. On the KVM console, you can also view the **Network ID** and **Virtual IP**, as shown below.



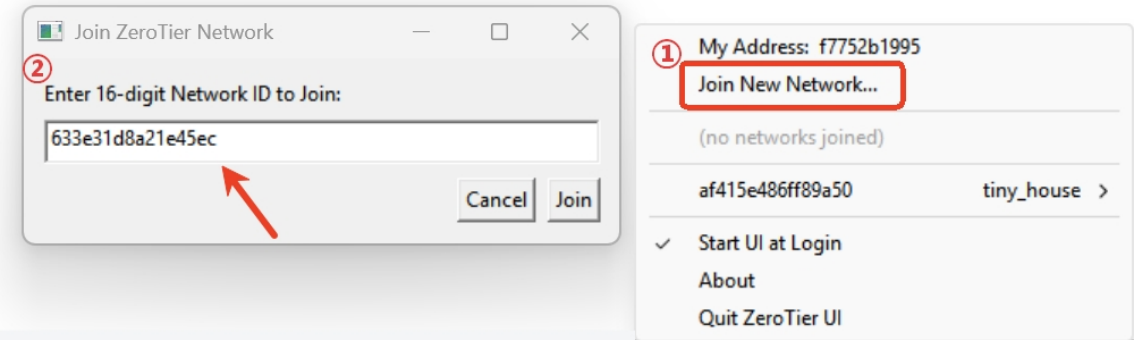
4.4.2 Bind Controlling Device

The example below demonstrates how to bind a Windows laptop (as the controlling device) to the ZeroTier network.

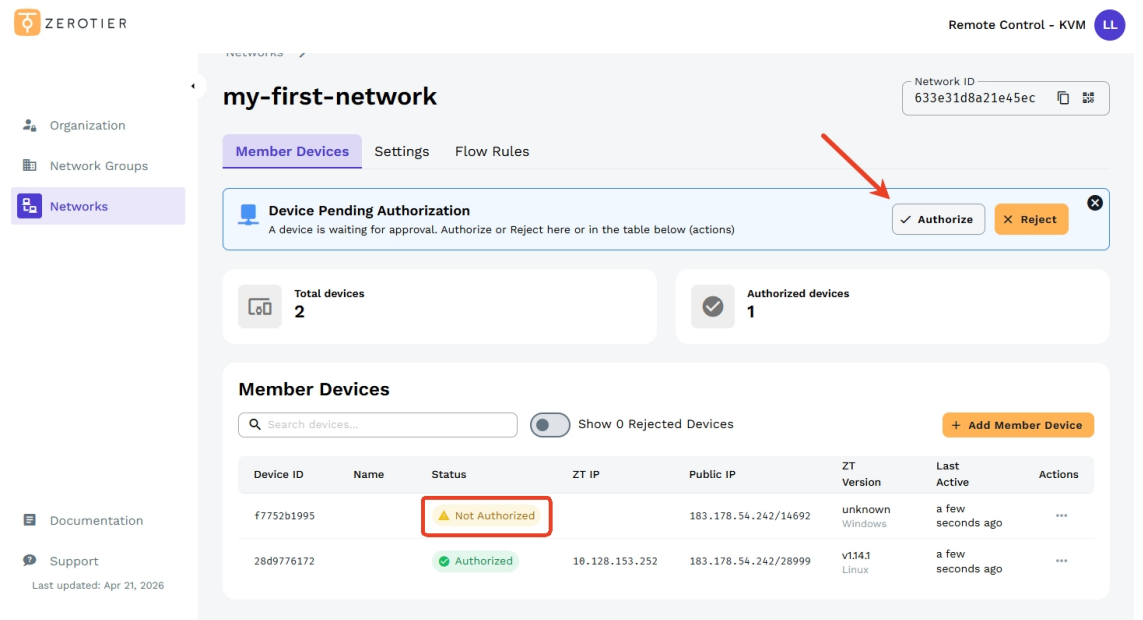
1. Install ZeroTier on your laptop from ZeroTier Download Center.
2. Run ZeroTier on the laptop and add it to the same ZeroTier network.

   Note: ZeroTier does not display a separate window/UI on the desktop; it only resides as an icon in the system tray (bottom-right corner). All operations are performed via the right-click menu.

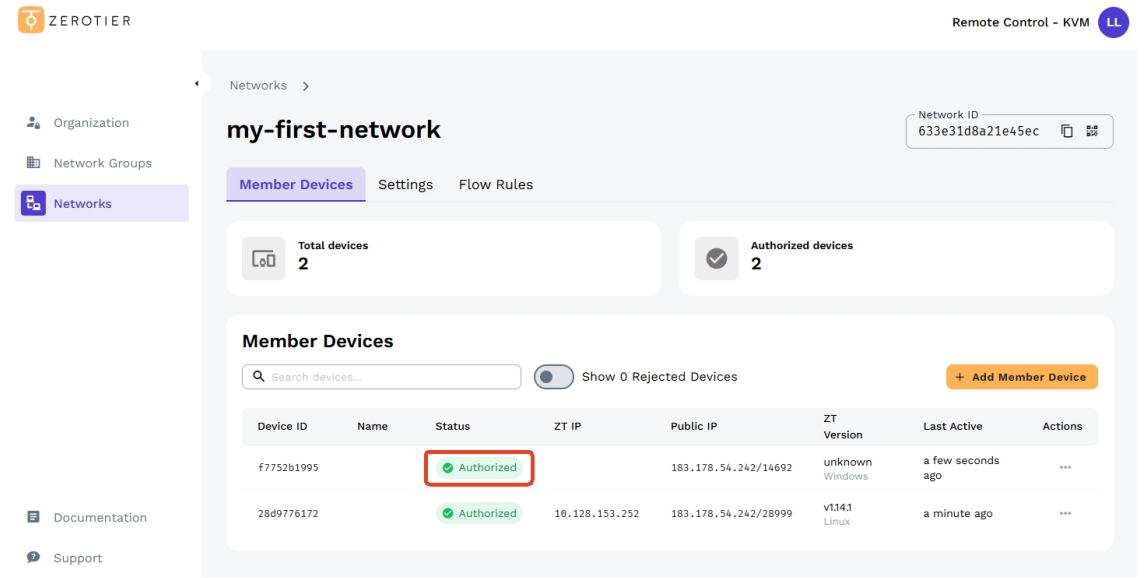
   Right click the ZeroTier icon, and click **Join New Network**. In the pop-up window, enter the same **Network ID** to add this PC to the same ZeroTier network.



Then go to ZeroTier Central, find the Pending device and authorize it.



3. Once authorized, the status will change to Authorized in green, as shown below.

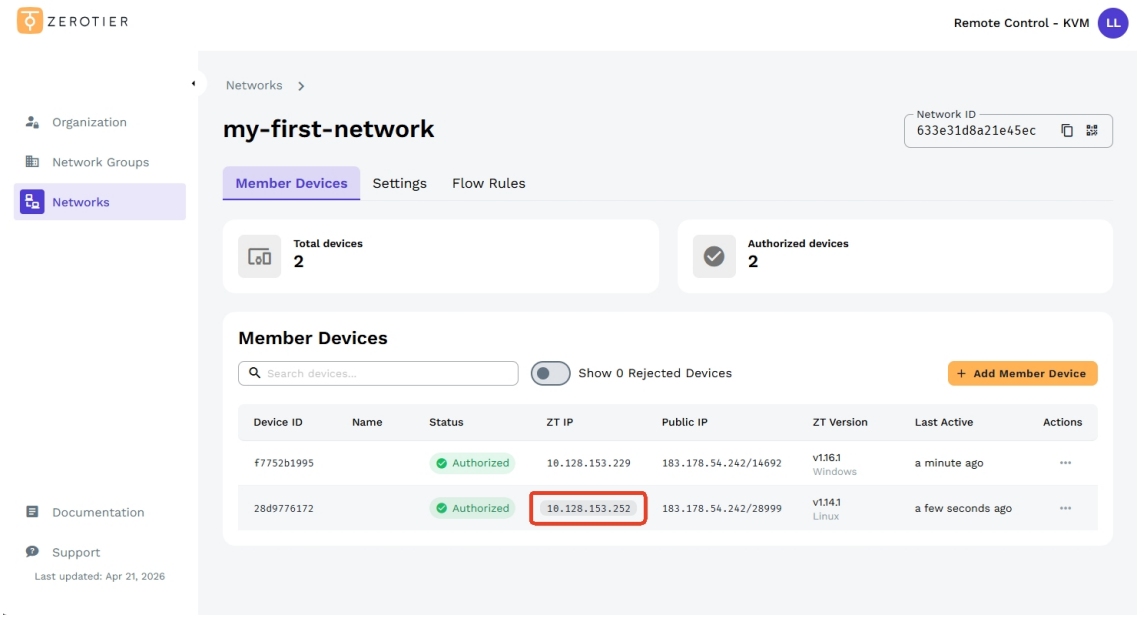


Now your KVM and the laptop are both added into the same ZeroTier network.

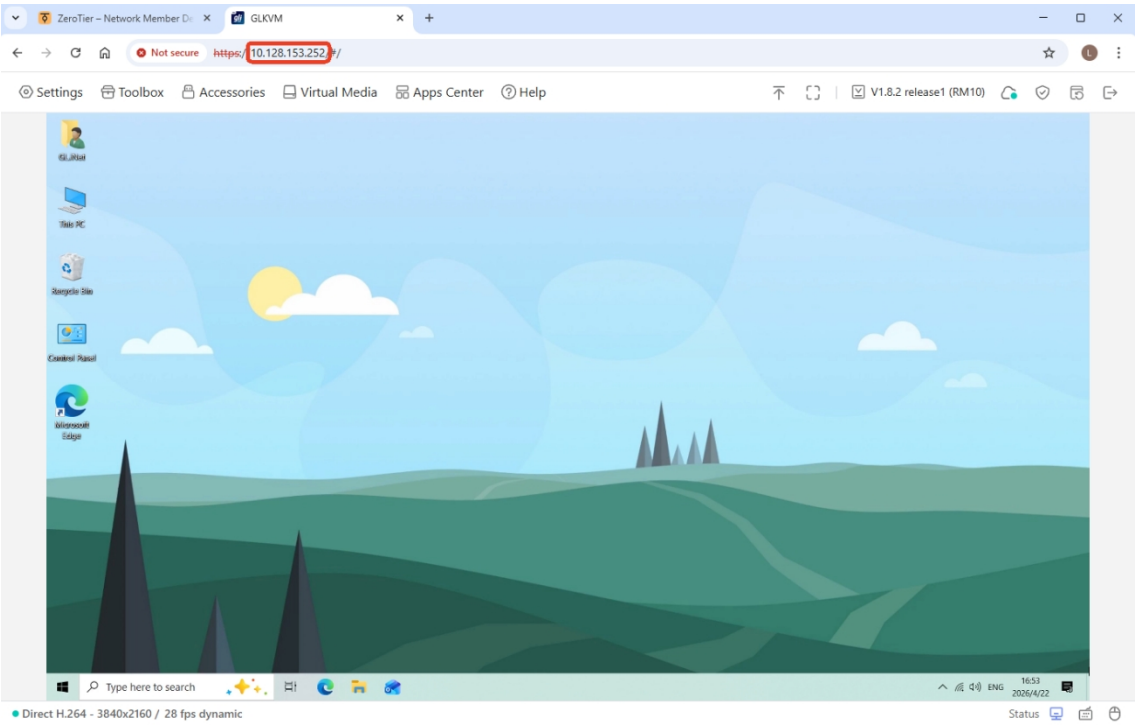
4.4.3 Remote Access via ZeroTier

The example below demonstrates how to remotely access the KVM console via the ZeroTier IP address.

1. On your laptop, sign in to ZeroTier Central with your account, find your KVM device, and click its **ZT IP** to copy it.



2. Open a new browser tab, enter the copied ZeroTier IP into the address bar, and you will be redirected to the GLKVM login page. Enter your admin password, then you can access your KVM and the controlled device via the ZeroTier IP.



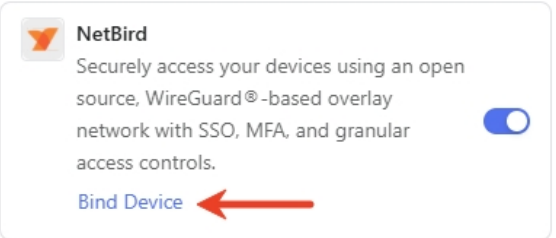
Tip: A privacy error may appear when accessing this ZeroTier IP for the first time. Simply click **Advanced** > **Proceed** to continue. See here for details.

4.5 NetBird

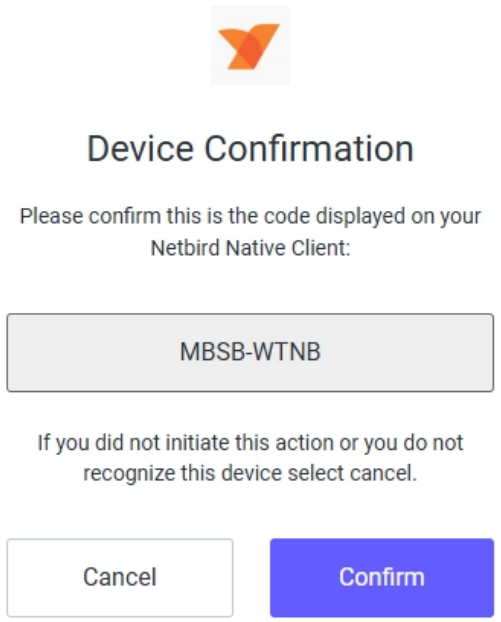
NetBird is an open-source zero trust networking platform that lets you build secure private networks for home and business use. As a WireGuard®-based overlay network, NetBird enables secure access to your devices anytime and anywhere. GL.iNet KVM integrates NetBird, allowing you to bind it to the NetBird virtual network for remote access — no need to install the GLKVM app or use the cloud service.

4.5.1 Bind KVM

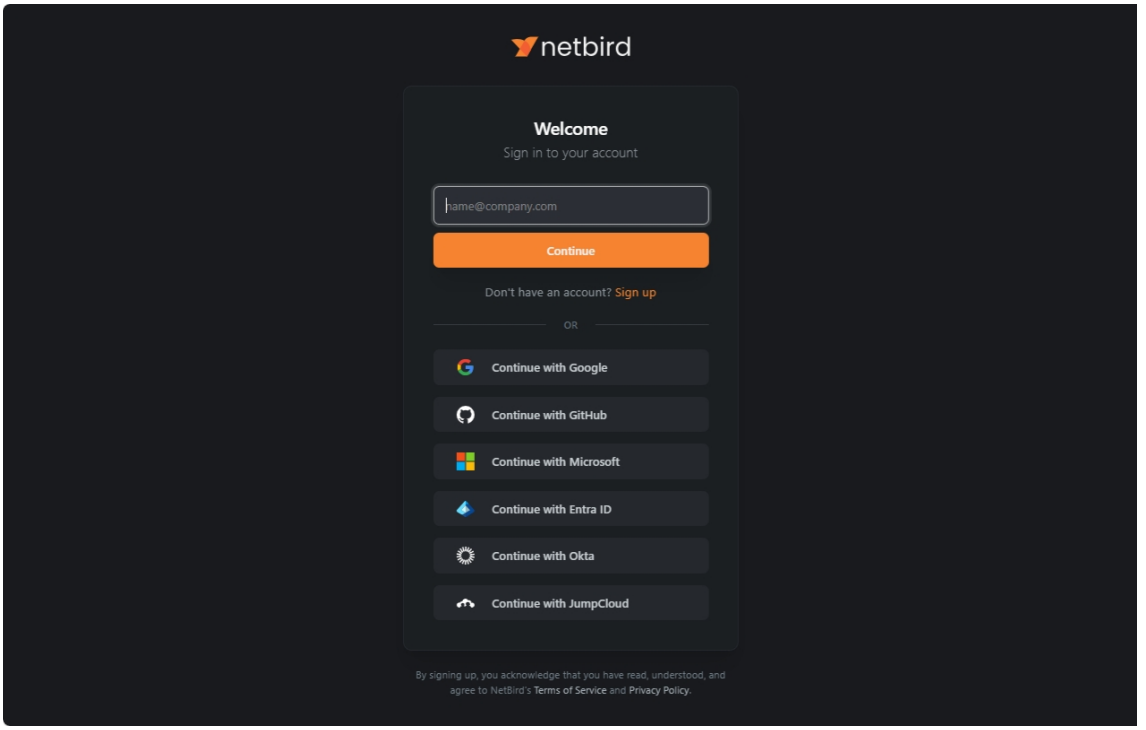
1. Connect your KVM and the controlling device to the same local network.
2. On the controlling device, log in to your KVM console locally via its domain or IP address, then go to **Apps Center** > **NetBird**. Enable NetBird and click **Bind Device**.



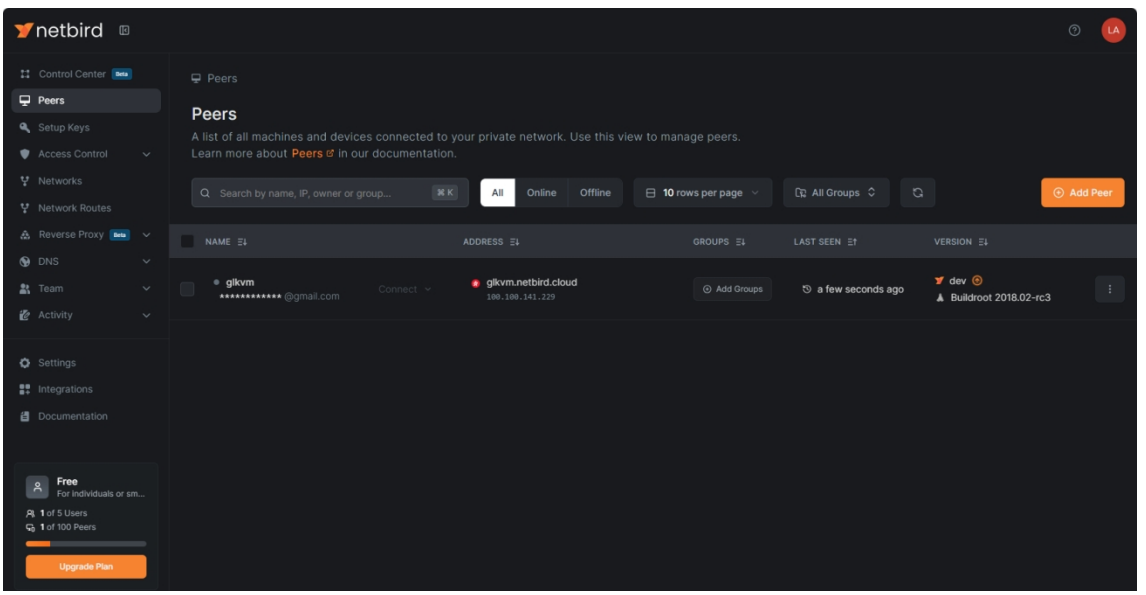
3. You will be redirected to the device confirmation page. Click **Confirm**.



4. Sign in to your NetBird account. If you don't have an account, sign up first.



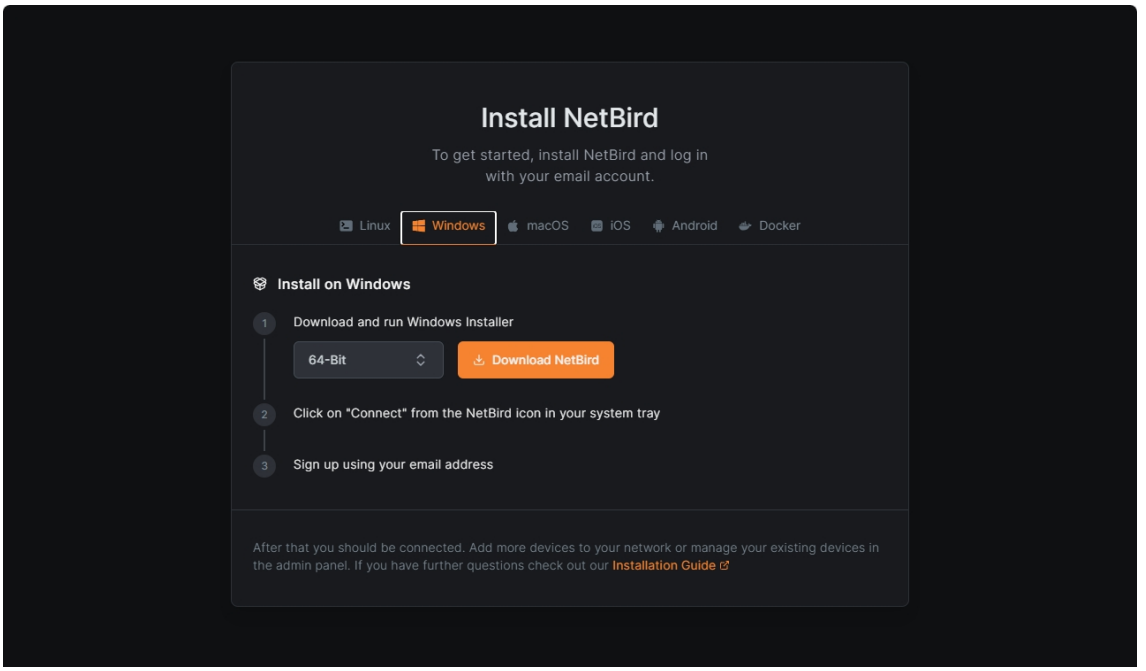
5. After signing in, the KVM device will be automatically bound to your account. On the NetBird dashboard, you will see your KVM listed on the **Peers** page.



4.5.2 Bind Controlling Device

The example below demonstrates how to bind a Windows laptop (as the controlling device) to the NetBird network.

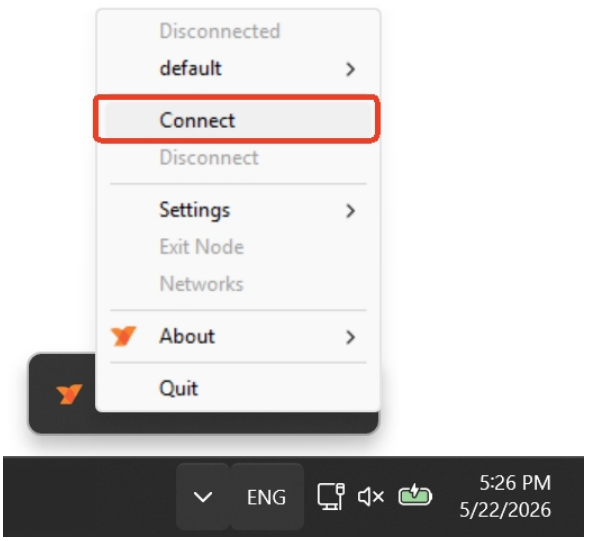
1. Install NetBird on your laptop from NetBird Download Center.



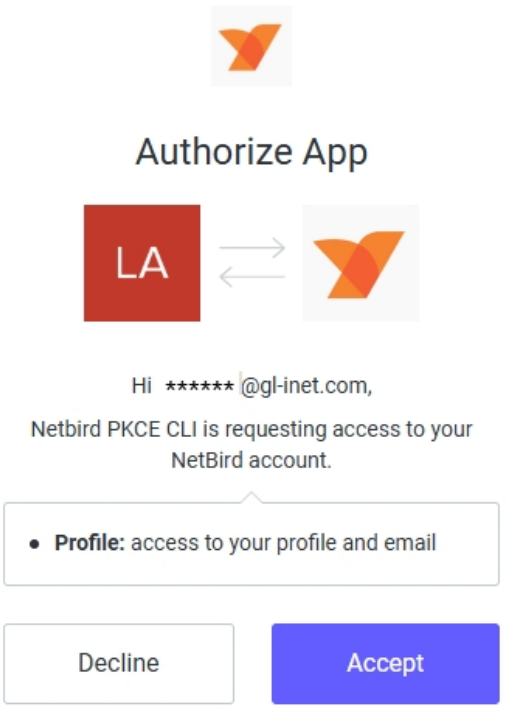
2. Run NetBird on the laptop and add it to the same NetBird network.

   Note: NetBird does not display a separate window/UI on the desktop; it only resides as an icon in the system tray (bottom-right corner). All operations are performed via the right-click menu.

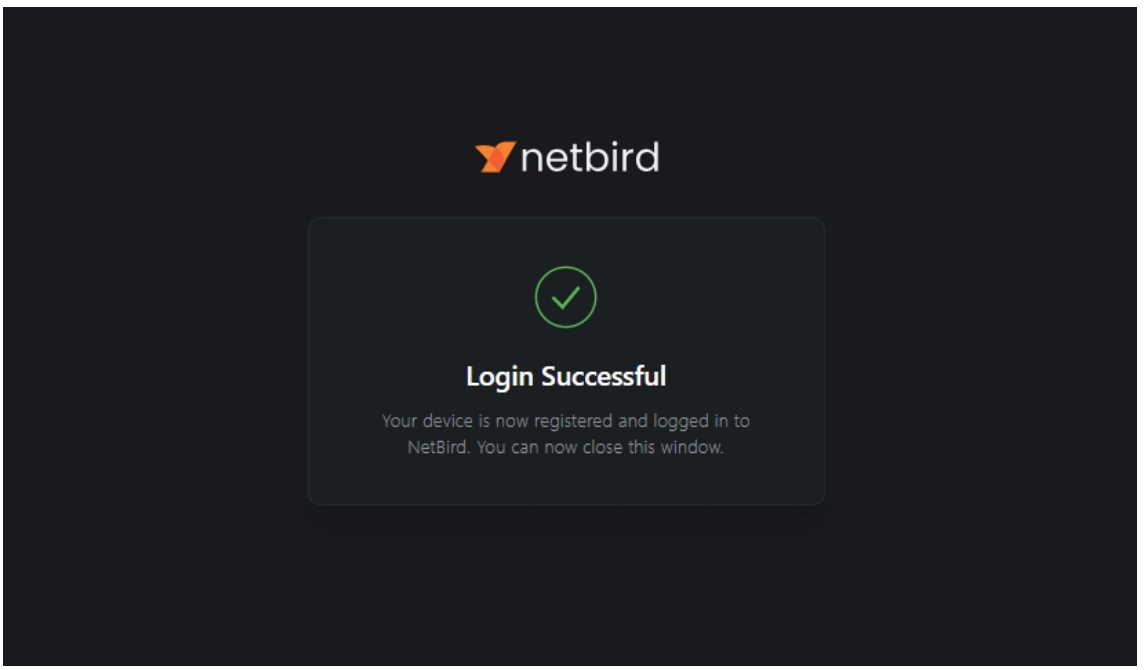
   Right click the NetBird icon, and click **Connect**.



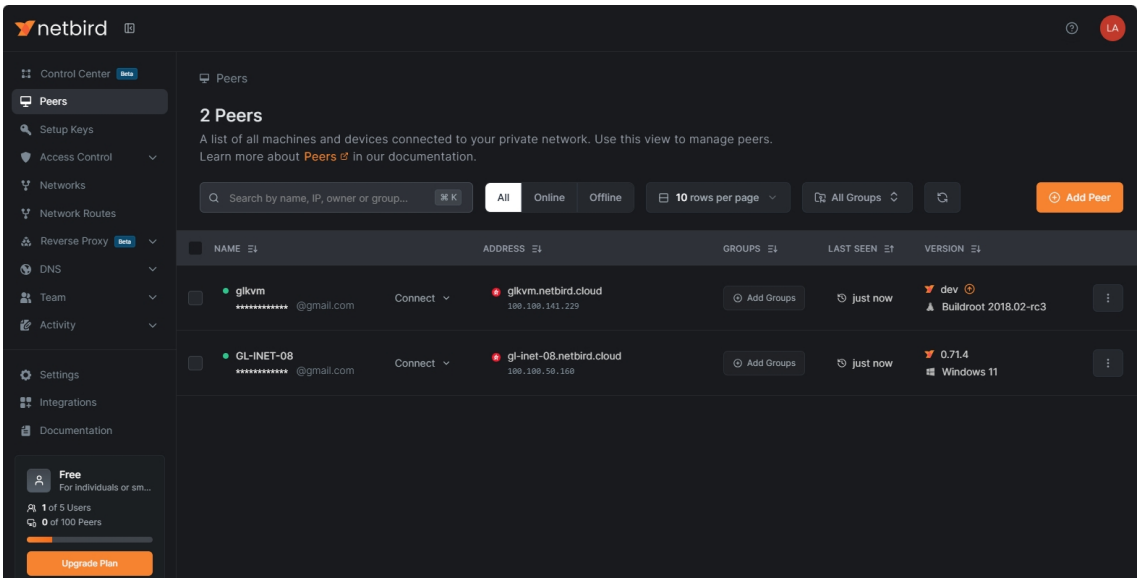
3. In the pop-up window, click **Accept** to authorize.



4. Your laptop will be automatically bound to your account and added to the same NetBird network.



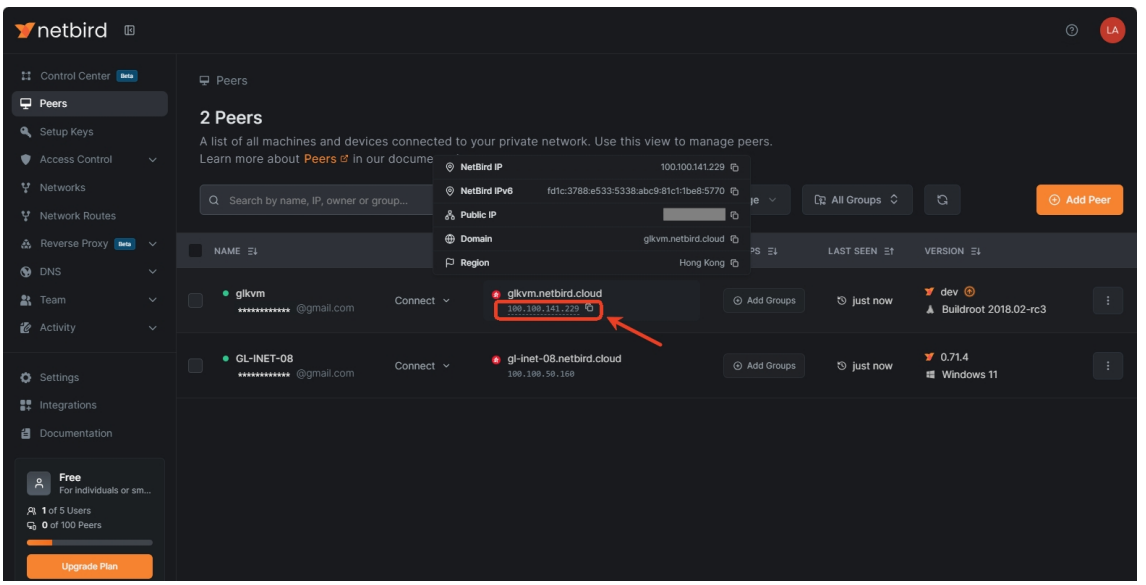
5. On the NetBird dashboard, there are two devices on the **Peers** page: your KVM and the controlling laptop.



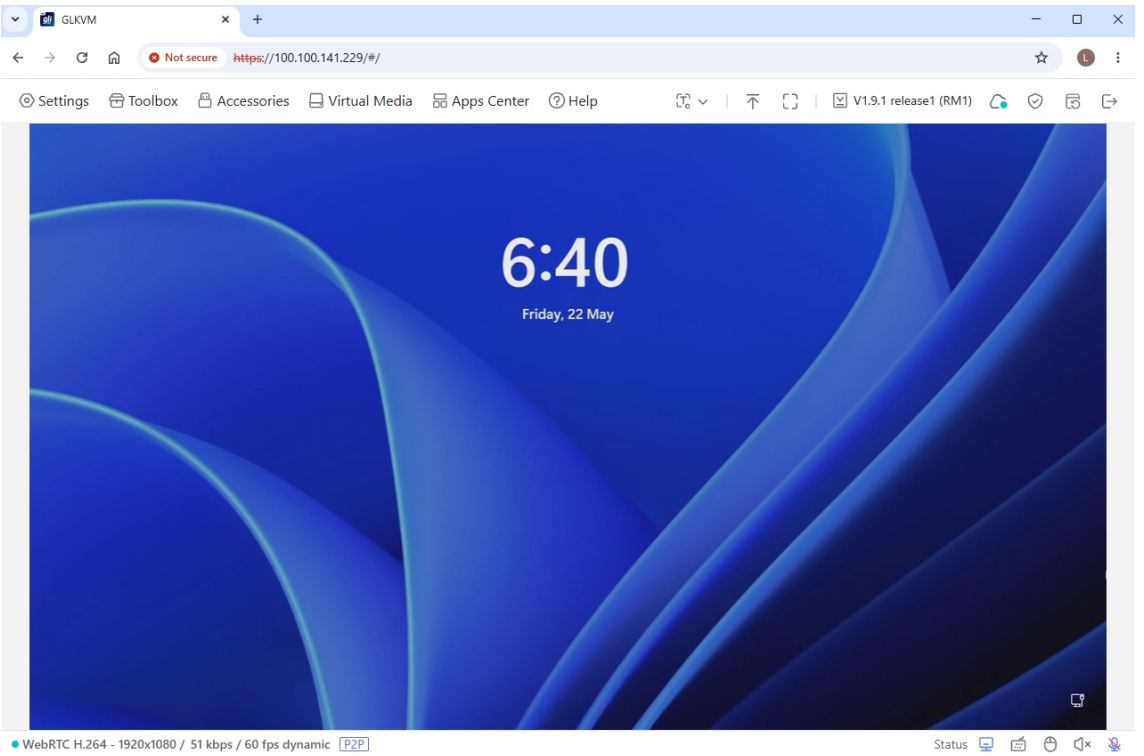
4.5.3 Remote Access via NetBird

The example below demonstrates how to remotely access the KVM console via the NetBird virtual IP address.

1. On your laptop, sign in to the NetBird dashboard and navigate to **Peers**.
2. Find your KVM device and click its **NetBird IP** (100.100.141.229 in this example) to copy the virtual IP.



3. Open a new browser tab, enter the copied NetBird IP into the address bar, and you will be redirected to the GLKVM login page. Enter your admin password, then you can access your KVM and the controlled device via the NetBird IP.



Tip: A privacy error may appear when accessing this NetBird IP for the first time. Simply click **Advanced** > **Proceed** to continue. See here for details.

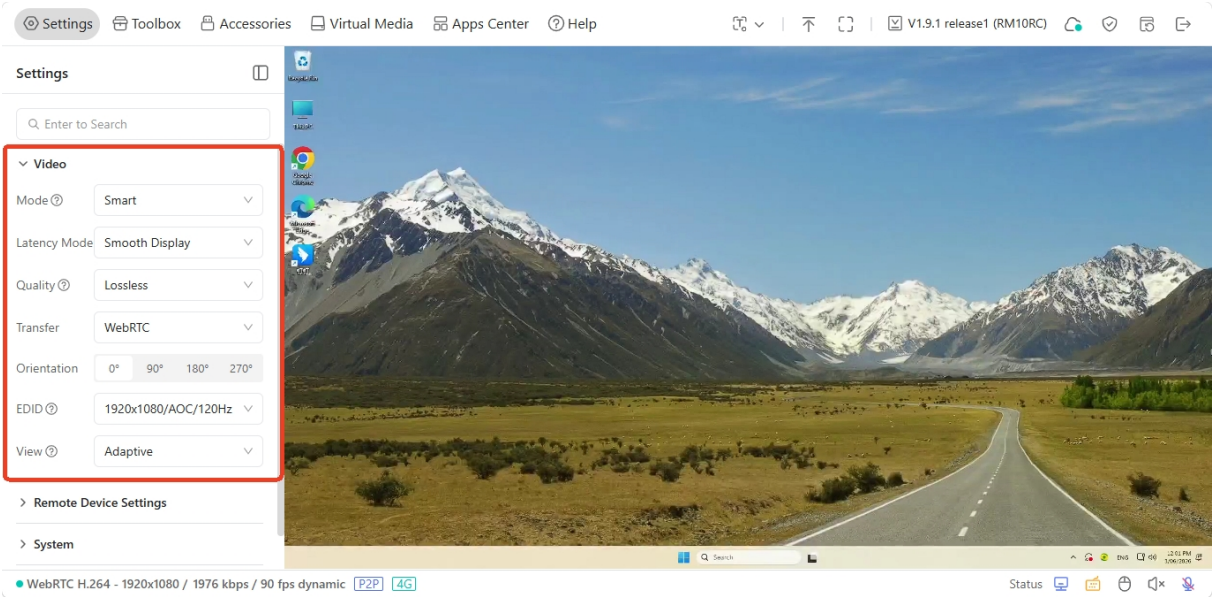
Chapter 5

Settings

This chapter introduces the Settings page on the KVM Web console.

5.1 Video

You can customize the video settings on the console, e.g., video quality, transmission, EDID.

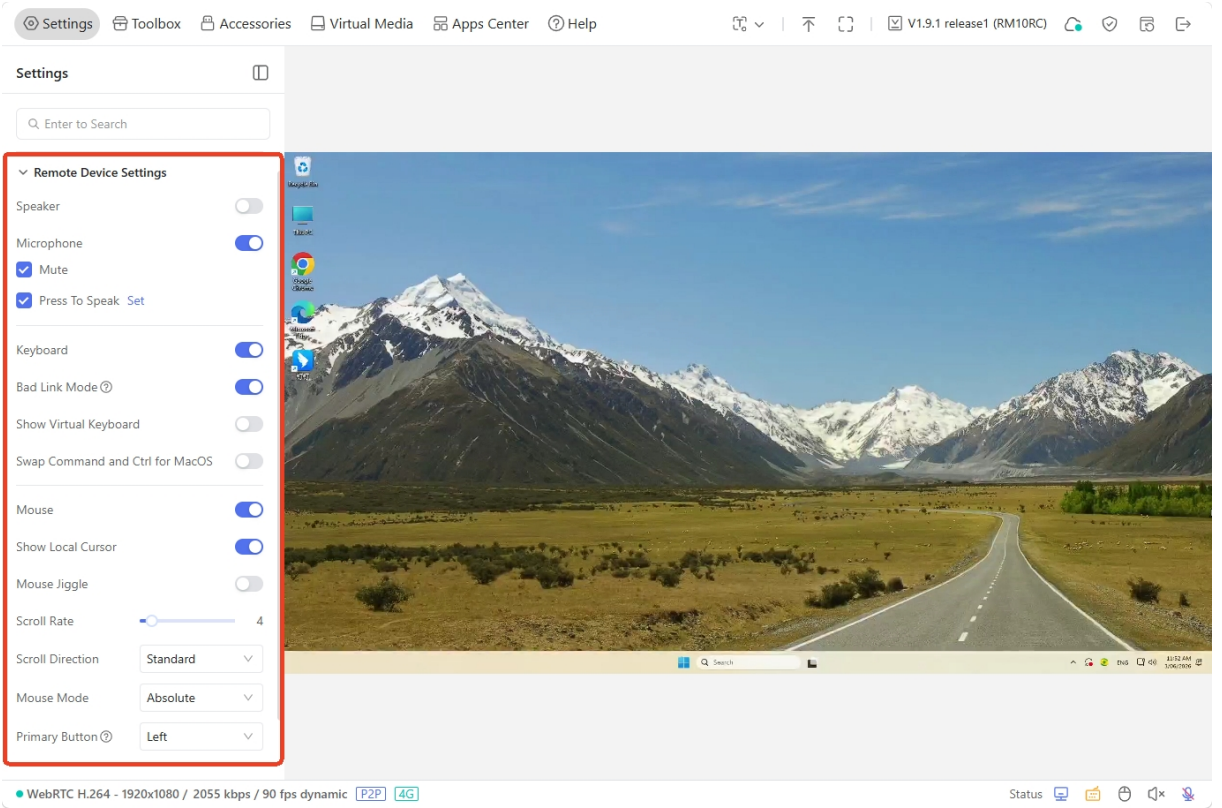


- **Mode**: Switch between Smart and Normal mode as needed. Smart mode helps reduce bandwidth consumption, especially in weak networks.
- **Latency Mode**: You can choose between Lowest Latency and Smooth Display for the device. This feature was introduced in firmware v1.9.0.
  - **Lowest Latency**: Minimizes input latency to deliver snappier keyboard and mouse response.
  - **Smooth Display**: Optimizes visual performance to eliminate stuttering and frame loss for steady playback.
- **Quality**: Adjust the video quality to Auto/Low/Medium/High/Ultra-high/Lossless according to your network environment and resolution requirements.
- **Transfer**: Switch the video transmission method between WebRTC, WebRTC (FEC), and Direct as needed. Note that the Direct transfer has no sound.
  - **WebRTC**: Balances smooth video and stable audio for real-time remote control.
  - **WebRTC (FEC)**: Adds forward error correction to improve connection stability under poor or unstable network conditions. When selected, it automatically repairs lost data packets by transmitting a small amount of redundant data, reducing screen flickering and lag.
  - **Direct**: Provides the lowest latency and lossless video quality, but does not support audio transmission.

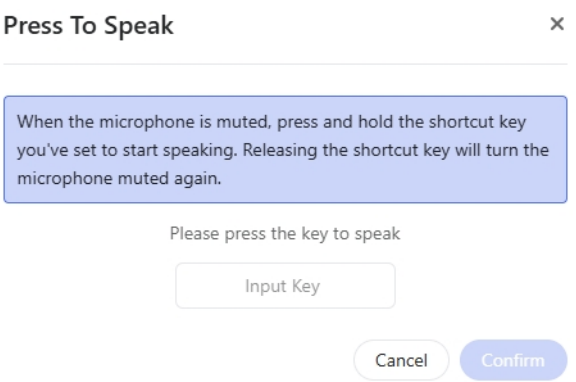
- **Orientation**: Adjust the console's rotation angle to 0°/90°/180°/270°.
- **EDID**: Short for Extended Display Identification Data, it automatically matches the optimal display parameters. The default setting applies to most scenarios and generally does not need to be modified. See here for details. If the screen does not refresh after EDID adjustment, restart the controlled device.
- **View**: This setting determines screen scaling when resizing the browser window. Available options: Adaptive, Best Picture Quality, Original Pixel. This feature was introduced in firmware v1.8.0.

5.2 Remote Device Settings

You can adjust the relevant settings of the controlled device.

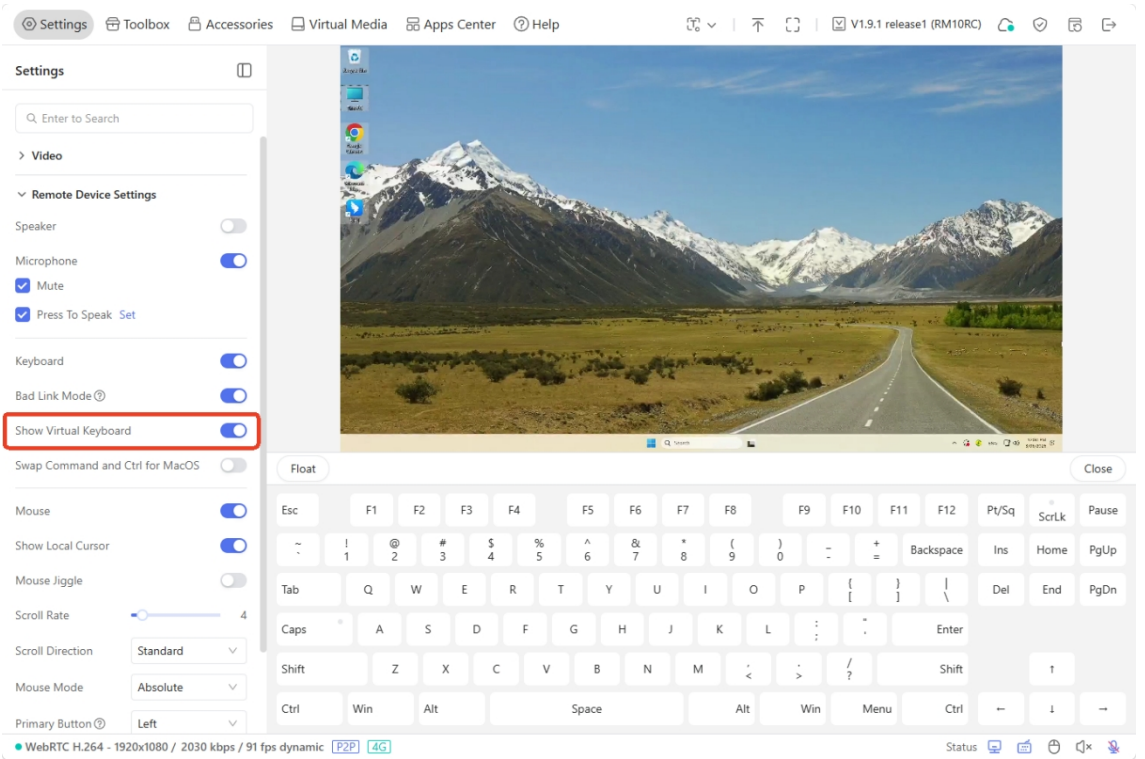


- **Speaker**: Control audio output from the controlled device (e.g., system sounds, video audio).
- **Microphone**: Transmit local audio (e.g., your voice) from the controlling device to the remote end. It supports one-click mute, and a long-press shortcut to activate the microphone (i.e., Press To Speak).



- **Keyboard**: Turn on or off the keyboard of the controlled device.

- **Bad Link Mode**: i.e. Release keys immediately. Each key press is sent as a single quick press-and-release action, preventing stuck keys or unintended repeated input during remote control.
- **Show Virtual Keyboard**: Show and use the virtual keyboard on the console.



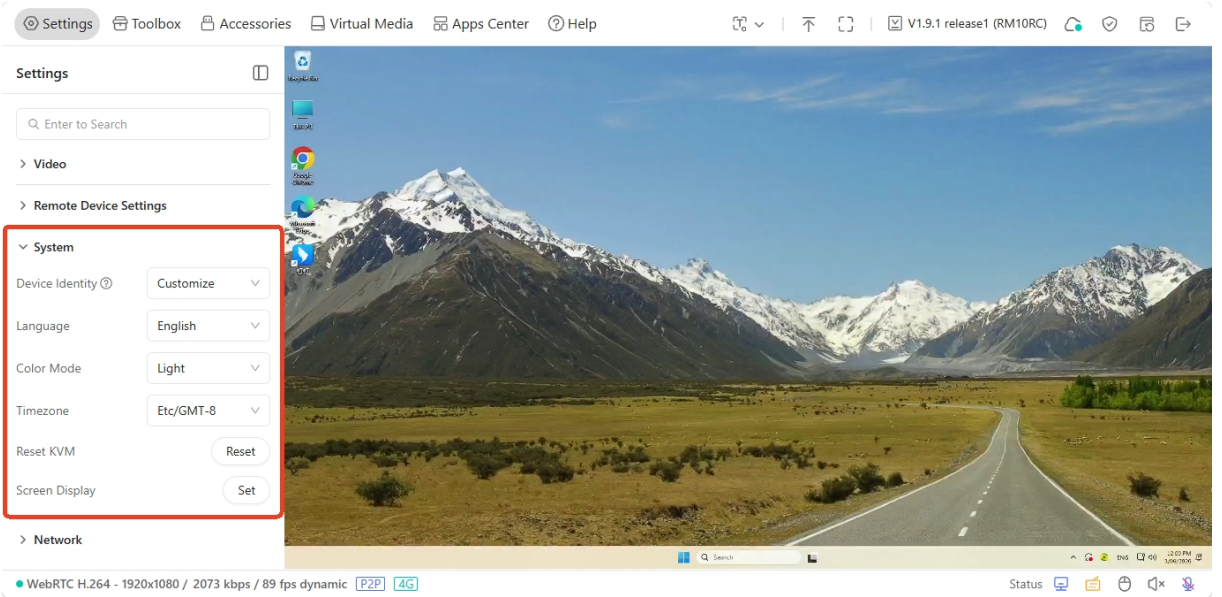
- **Swap Command and Ctrl for MacOS**: This feature swaps the Cmd and Ctrl keys to ensure keyboard compatibility across different operating systems.
- **Mouse**: Turn on or off the mouse of the controlled device.
- **Show Local Cursor**: Show the mouse of the controlling device on the screen.
- **Mouse Jiggle**: The Mouse Jiggle feature simulates subtle, periodic mouse movements to prevent the controlled device from going to sleep due to prolonged inactivity, such as during remote meetings and server management.
- **Scroll Rate**: It refers to the speed at which the mouse wheel scrolls or the number of lines/units scrolled per wheel rotation, affecting how quickly content moves on the remote.
- **Scroll Direction**: It determines whether scrolling the mouse wheel up/down moves content on the remote screen in the same direction (natural scrolling) or the opposite direction (traditional scrolling). Four direction modes are available: Standard, Vertical Invert, Horizontal Invert, and Both Invert.
- **Mouse Mode**: Allows switching between Absolute Mode and Relative Mode to ensure smooth and accurate cursor control in different remote control scenarios.

- **Relative Mode**: The mouse position is calculated based on movement rather than fixed screen coordinates. You must click inside the remote window to control the mouse. The cursor is locked within the remote screen and cannot move out smoothly. This mode provides better compatibility with BIOS, old systems, and embedded devices.
- **Absolute Mode**: The mouse position corresponds to exact screen coordinates. The remote cursor follows the local one smoothly and accurately, allowing seamless movement between your local screen and the remote screen. It is ideal for daily desktop control and precise operations, though a slight delay may occur due to network transmission.
- **Summary**: Use Absolute for smooth daily control; use Relative for BIOS access, some older devices that do not support absolute positioning, or to avoid accidental cursor movement.

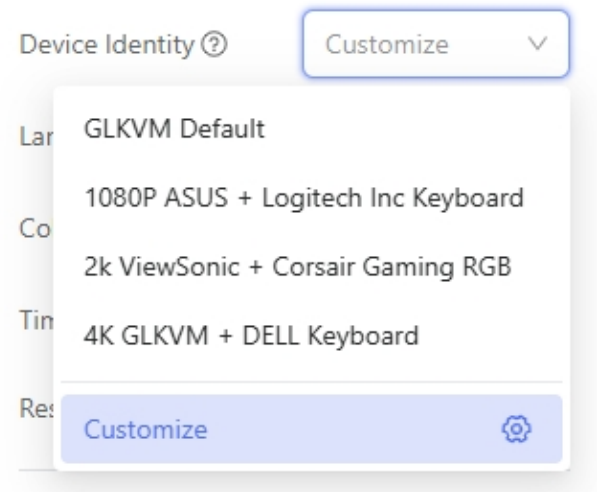
- **Relative Sensitivity**: It is available when the Mouse Mode is Relative.
- **Primary Button**: Select the left or right button as the primary click. This feature was introduced in firmware v1.9.0.

5.3 System

You can customize the system settings of the console, or reset the device with one click.



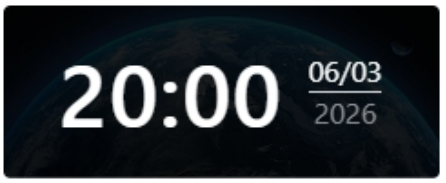
- **Device Identity**: Customize or modify the KVM's identity recognized by the controlled device. Note that EDID and device identification remain synchronized. Changing either one will automatically update the other to ensure correct device recognition.



- **Language**: Set the console's language to Chinese, English, or Japanese.
- **Color Mode**: Customize the theme color to Light or Dark mode.
- **Time Zone**: Customize the time zone of the KVM console.
- **Reset KVM**: Factory reset your KVM with just one click.
- **Screen Display**: You can customize the screen display as needed. This feature was introduced in firmware v1.9.1.

Preview

*Pictures are examples of displays



Settings

Lock Screen: World Clock

Time Format: 24-Hour | 12-Hour

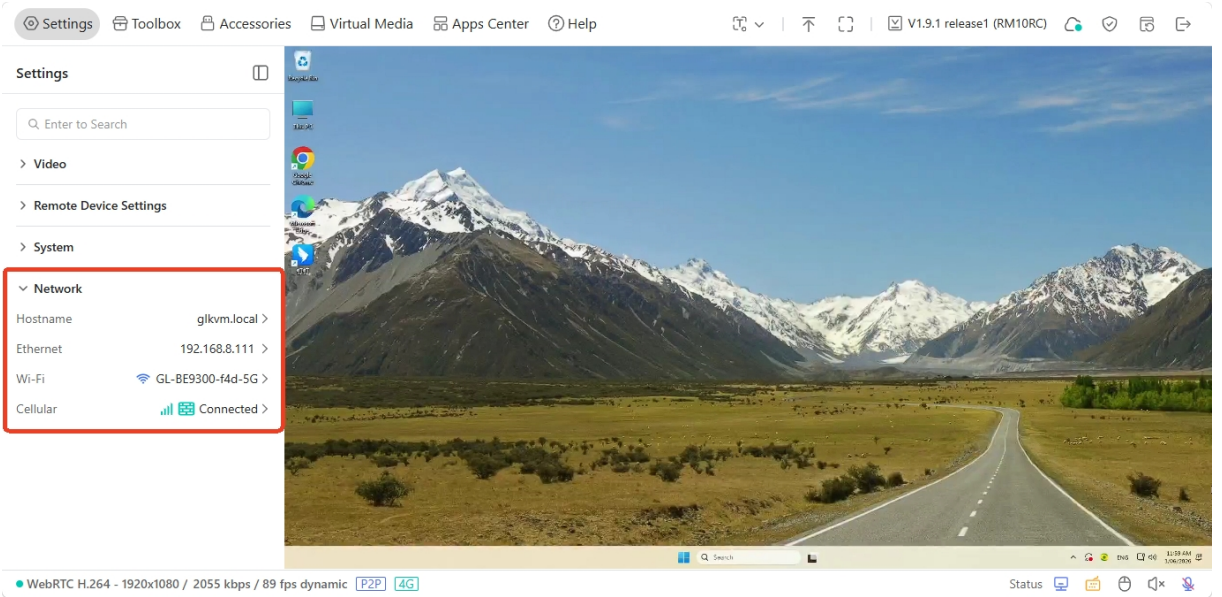
Date Format: 06/03 2026

Wallpaper:  Upload

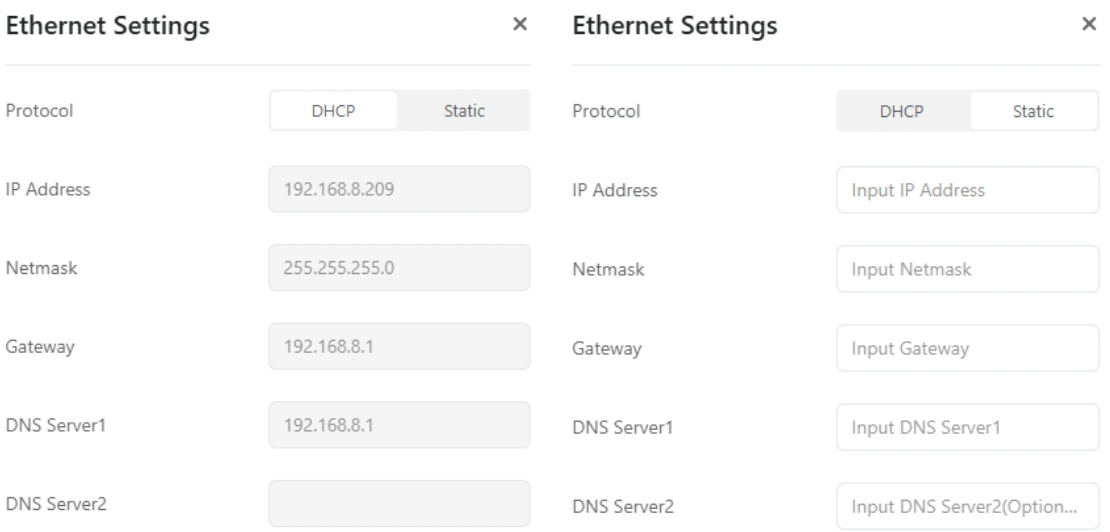
Cancel | Apply

5.4 Network

You can check network details of your device, such as hostname and IP address.



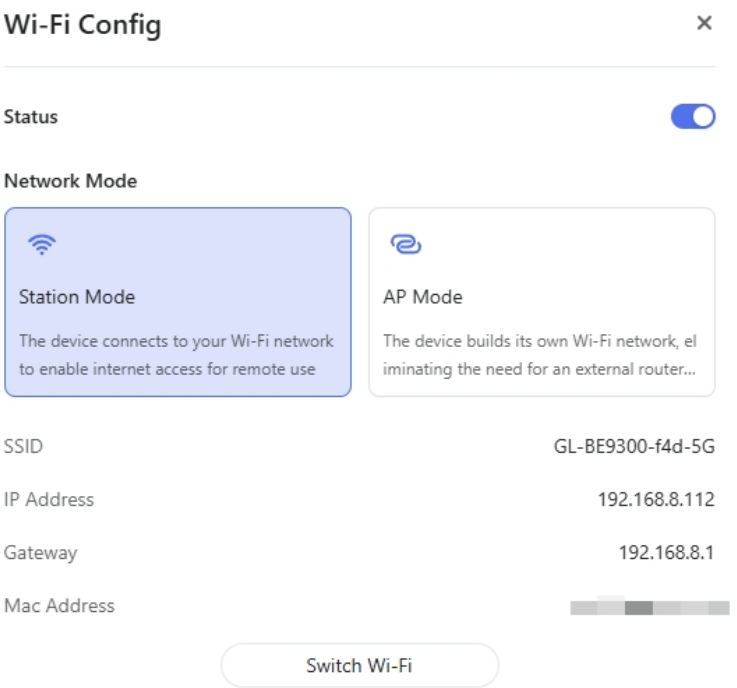
- **Hostname**: Modify the device hostname directly on the console if needed.
- **Ethernet**: When Comet 5G connects to an upstream network via an Ethernet cable, its Ethernet IP address will be displayed here. You can click the IP address or the right arrow to view the Ethernet details. If you want to set a static IP address, switch the protocol to Static and enter the required network parameters (e.g., IP address, netmask, gateway) accordingly.



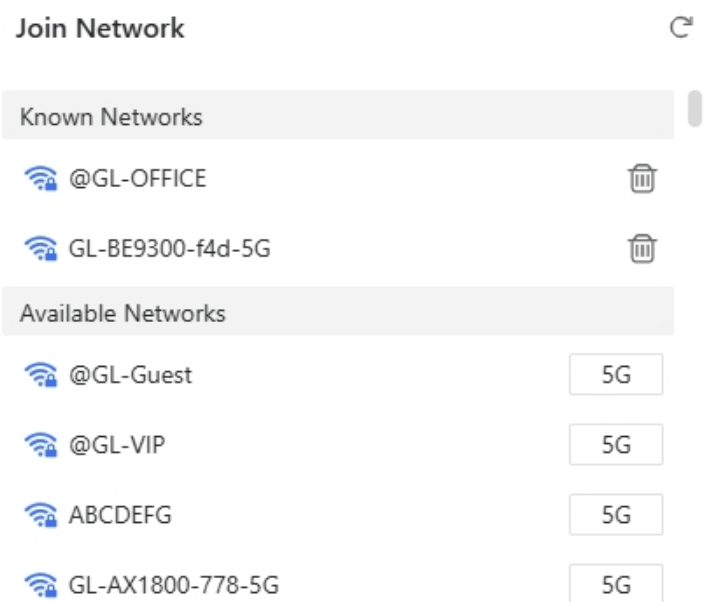
- **Wireless**: Comet 5G support two wireless working modes: Station Mode and AP Mode, catering to different network access requirements.

- **Station Mode**

  This mode is suitable for scenarios where an existing wireless network is available for your Comet 5G to connect to. In this mode, Comet 5G functions as a wireless client, which can scan for and connect to an upstream Wi-Fi hotspot (e.g., a router) to obtain network access.

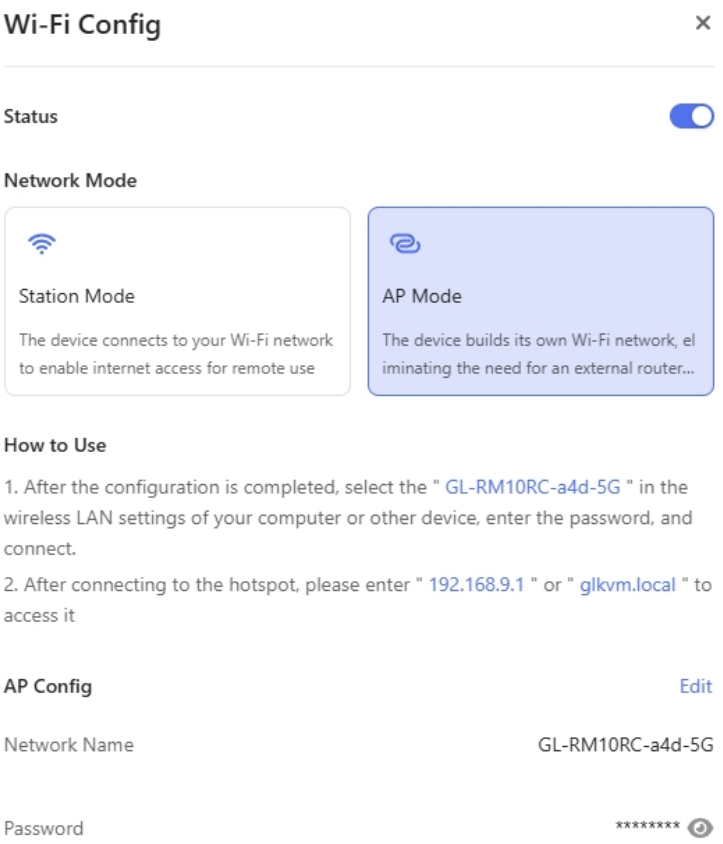


If you want to connect it to a different Wi-Fi network, click **Switch Wi-Fi** at the bottom, then select a Wi-Fi from the available network list.

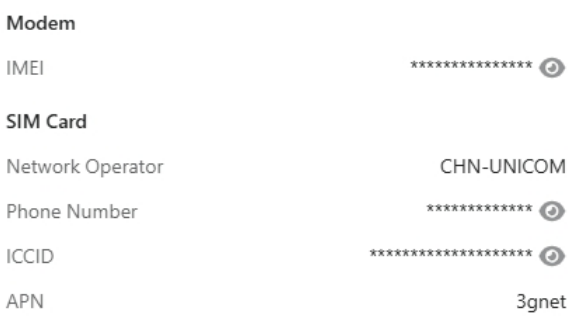


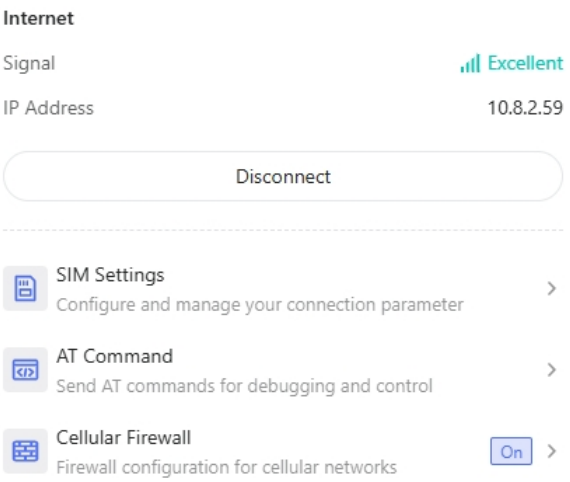
- **AP Mode**

  This mode is ideal for setting up a local area network, enabling offline close-range control of your KVM without requiring an external network. In this mode, Comet 5G functions as a Wi-Fi hotspot to broadcast signals for terminal devices such as smartphones and laptops to connect to. However, it cannot access the upstream network via Wi-Fi anymore.



- **Cellular**: Comet 5G comes with a built-in cellular module, enabling mobile network access via a SIM card. After inserting a SIM card, you can view cellular connection details (e.g., carrier information, phone number, ICCID, and current APN profile).





- **SIM Settings** allows you to manage your cellular configurations (e.g., adjust APN and MTU).
- **AT command** enables you to execute AT commands to retrieve modem-related outputs.
- **Cellular Firewall** is used to set up firewall rules for cellular networks.

In summary, the cellular connection serves as a robust backup network option when Ethernet or Wi-Fi connections are unavailable.

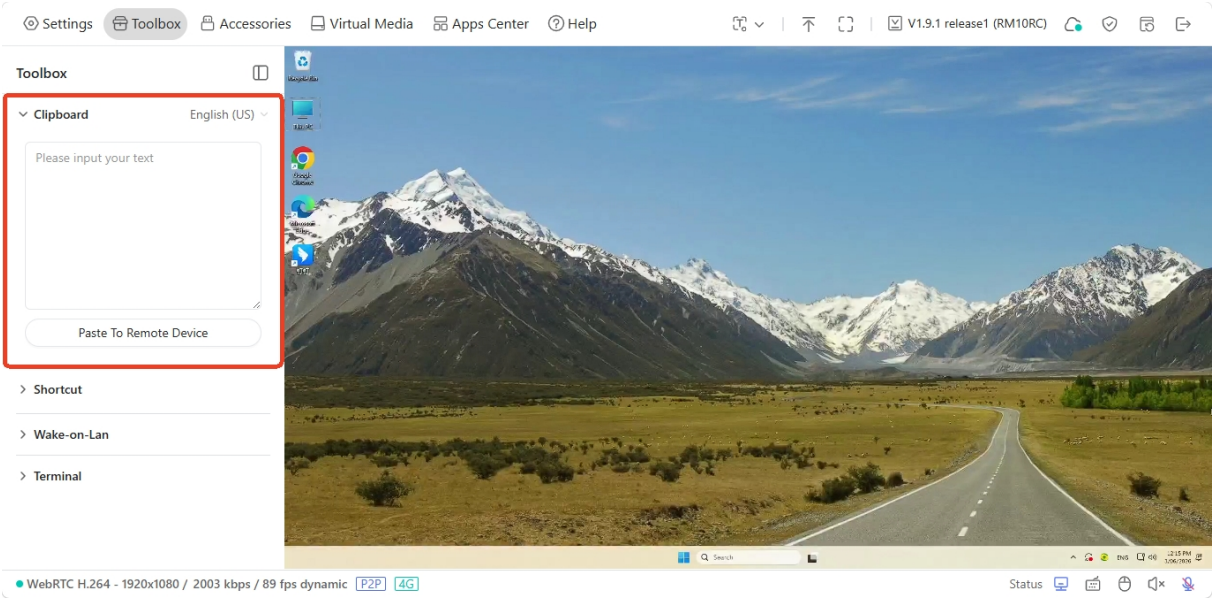
Chapter 6

Toolbox

This chapter introduces the Toolbox page on the KVM Web console.

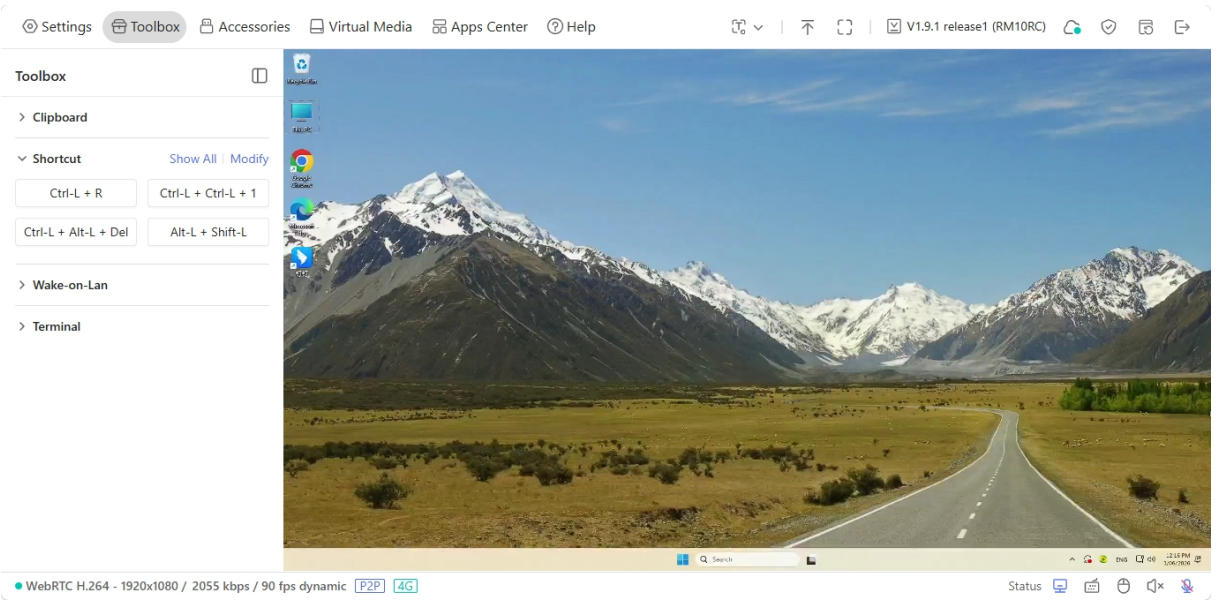
6.1 Clipboard

The clipboard allows you to paste text from the controlling device to the controlled device.



6.2 Shortcut

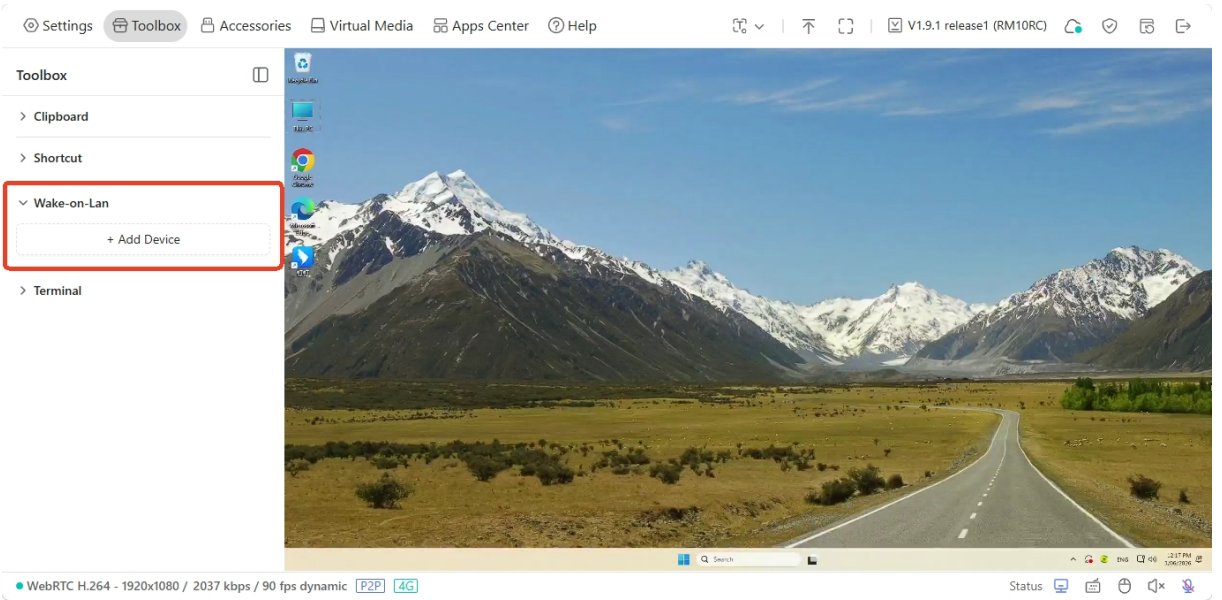
The shortcut let you perform actions faster without using the virtual keyboard, helping you work more efficiently and save time on daily tasks.



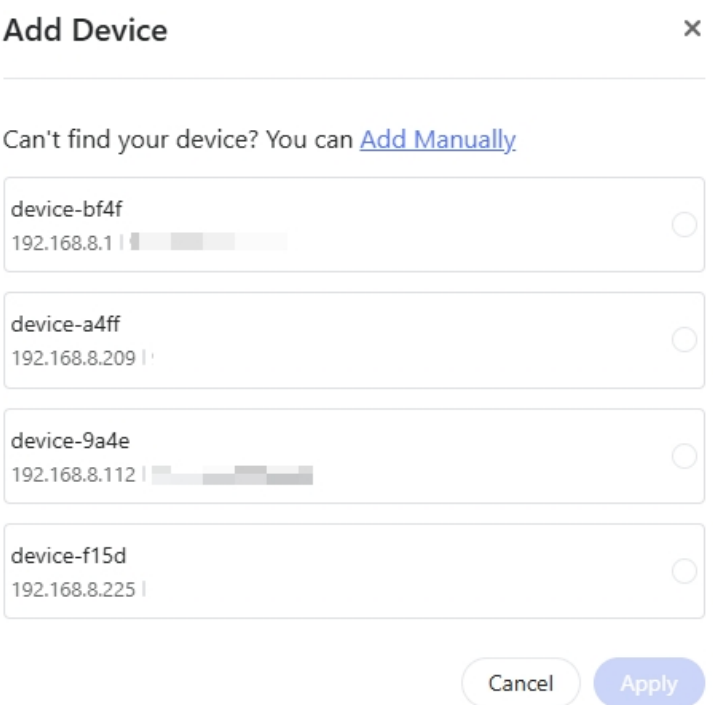
6.3 Wake-on-Lan

Wake-on-LAN (WOL) is a technology that allows the controlled device to be remotely powered on or awakened from a low-power state.

To set up Wake-on-LAN, click **Add Device**.

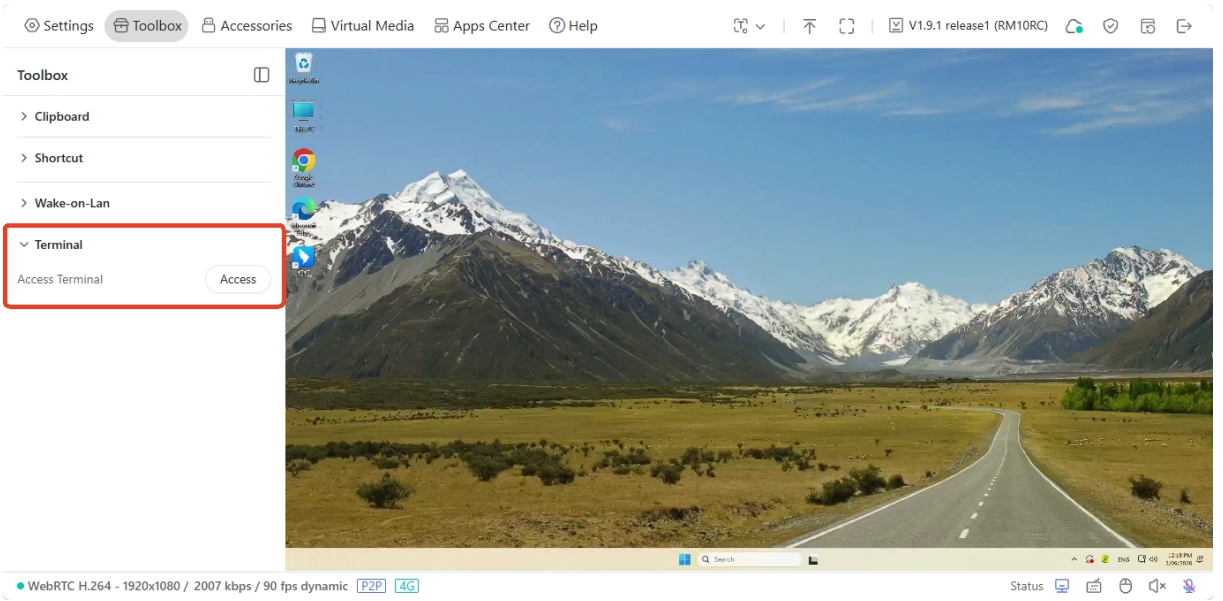


Choose a device from the same LAN, and click **Apply**. If the device you want to add is not in the list, click **Add Manually** and enter the device name and MAC address.



6.4 Terminal

You can access the terminal to perform advanced settings. Click **Access**.



You will be redirected to the GLKVM terminal.



Chapter 7

Accessories

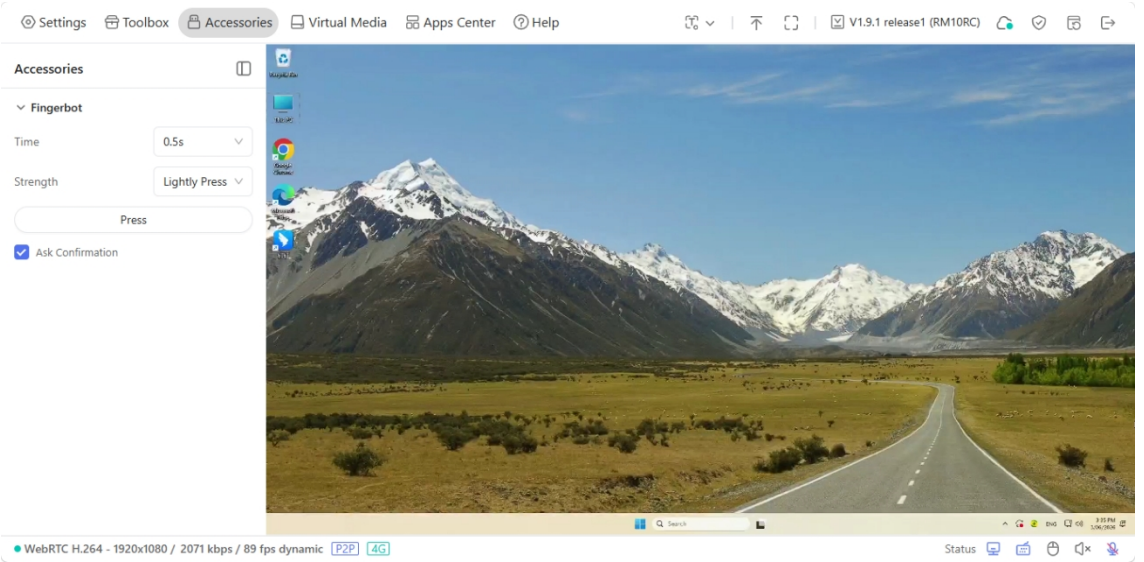
This chapter introduces the usage of two optional KVM accessories (not included): Fingerbot and ATX board.

7.1 Fingerbot

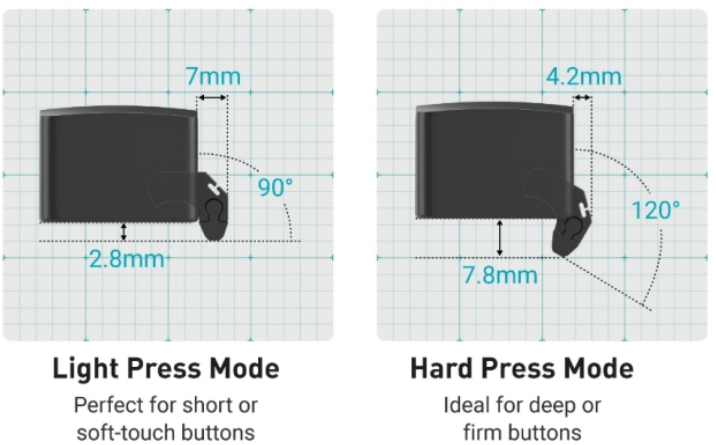
The Fingerbot is adhered to the physical power button of the controlled device, to achieve remote control of the controlled device's power supply.

Follow the steps below to install and set up your Fingerbot.

1. Refer to the setup video here to connect the Fingerbot to your controlled device.
2. Log in to the KVM console, and navigate to **Accessories**.



3. You can achieve different effects by adjusting the pressing duration and intensity.
   - **Time**: The press duration of the Fingerbot. You can set it to 0.5s/3s/8s.
   - **Strength**: There are two levels of pressing strength: Lightly Press and Firmly Press. Lightly Press is perfect for short or soft-touch buttons, while Firmly Press is ideal for deep or firm buttons.

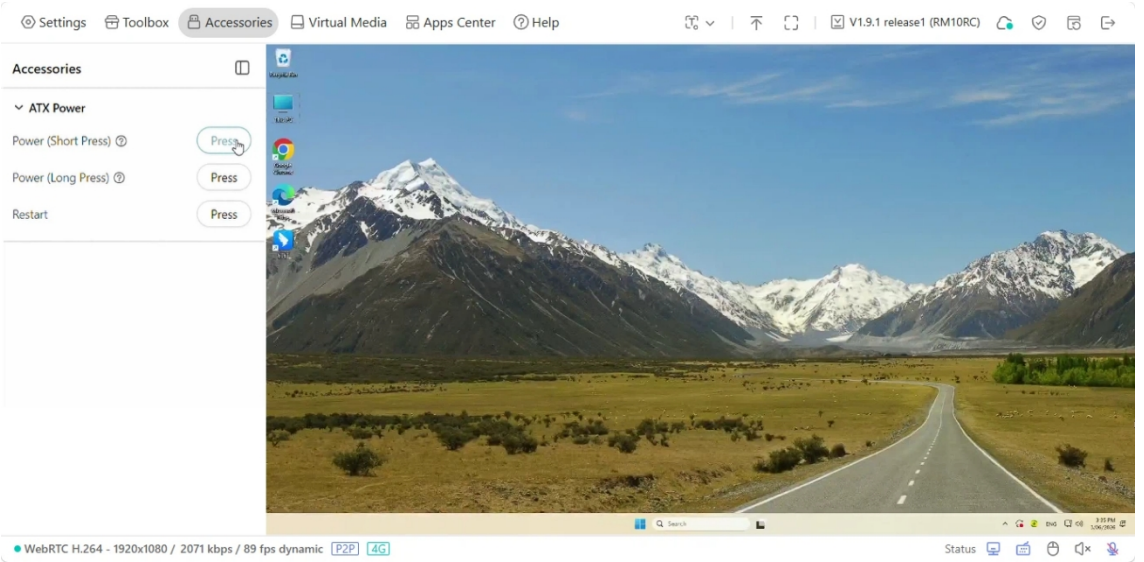


7.2 ATX Board

The ATX Board is installed in the computer case to remotely control the device's power on/off/reboot.

Follow the steps below to install and set up your Fingerbot.

1. Refer to the installation video here to install ATX board.
2. Log in to the KVM console, and navigate to **Accessories**.



3. The ATX board works according to the settings on the console.
    - **Power (Short Press)**: Used for regular power-on or system wake-up.
    - **Power (Long Press)**: Performs a forced shutdown operation.
    - **Restart**: Restart the device.

Chapter 8

Virtual Media

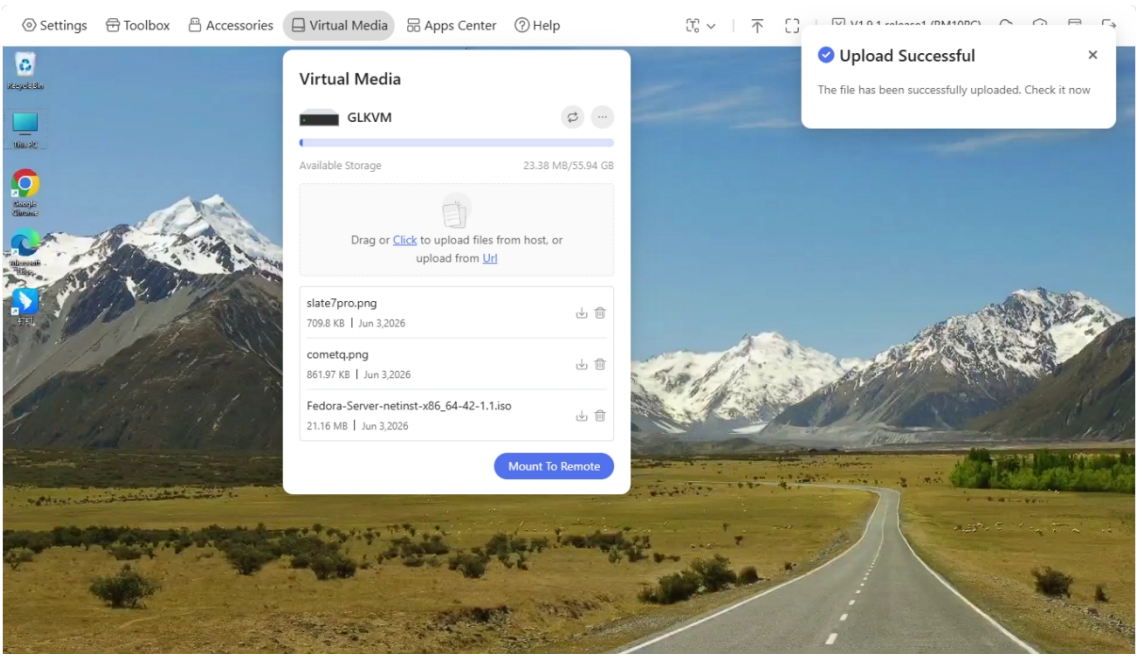
This chapter introduces the virtual media feature, allowing you to transfer files between the controlling and controlled device.

8.1 File Sharing

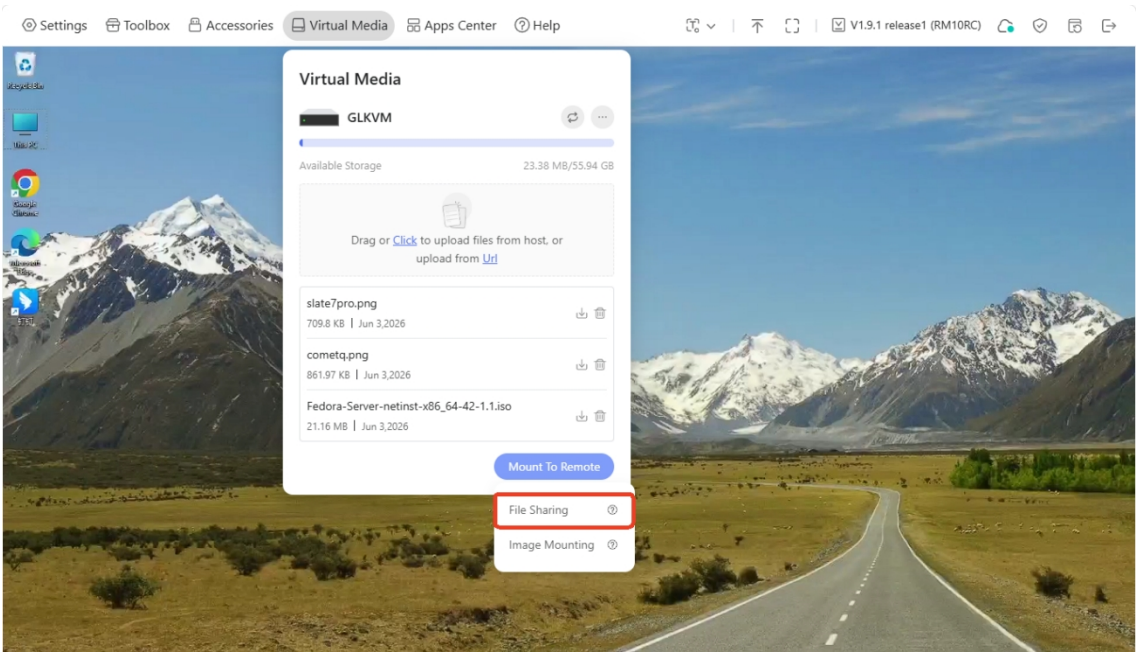
Comet 5G can emulate a read-write USB drive, allowing you to share and manage files between the controlling device and the controlled device.

Follow the steps below to share files between the controlling and controlled device.

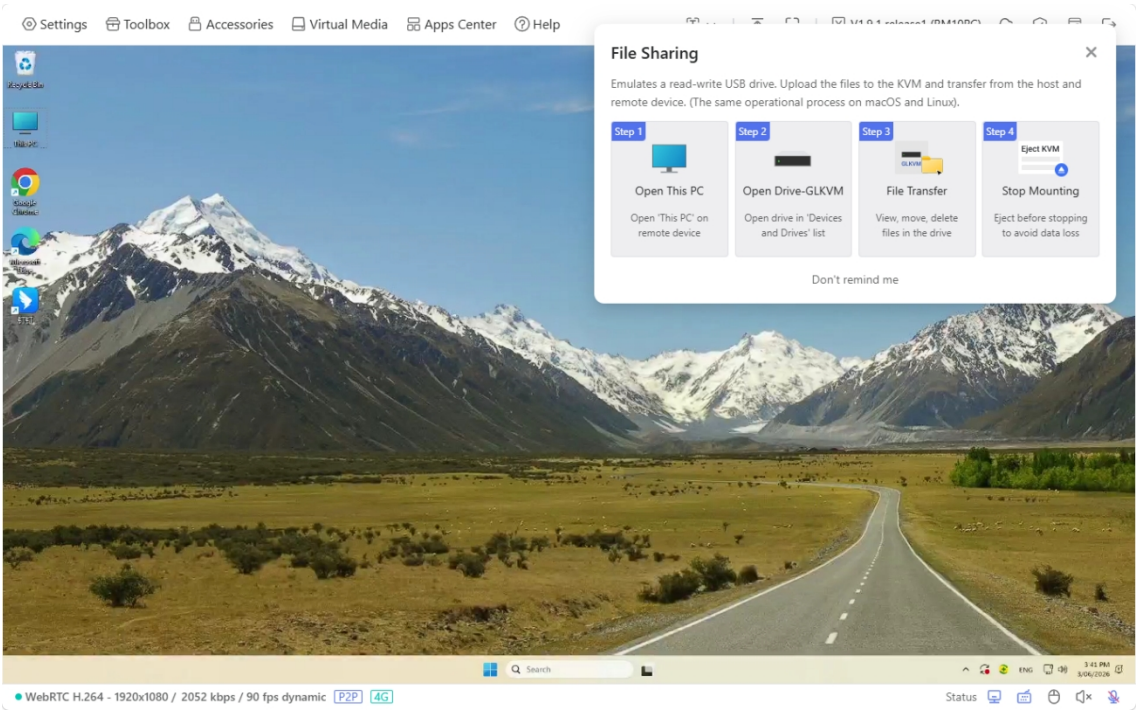
1. On your controlling device, log in to the KVM Web console and navigate to **Virtual Media**. Drag or click the box to upload files.



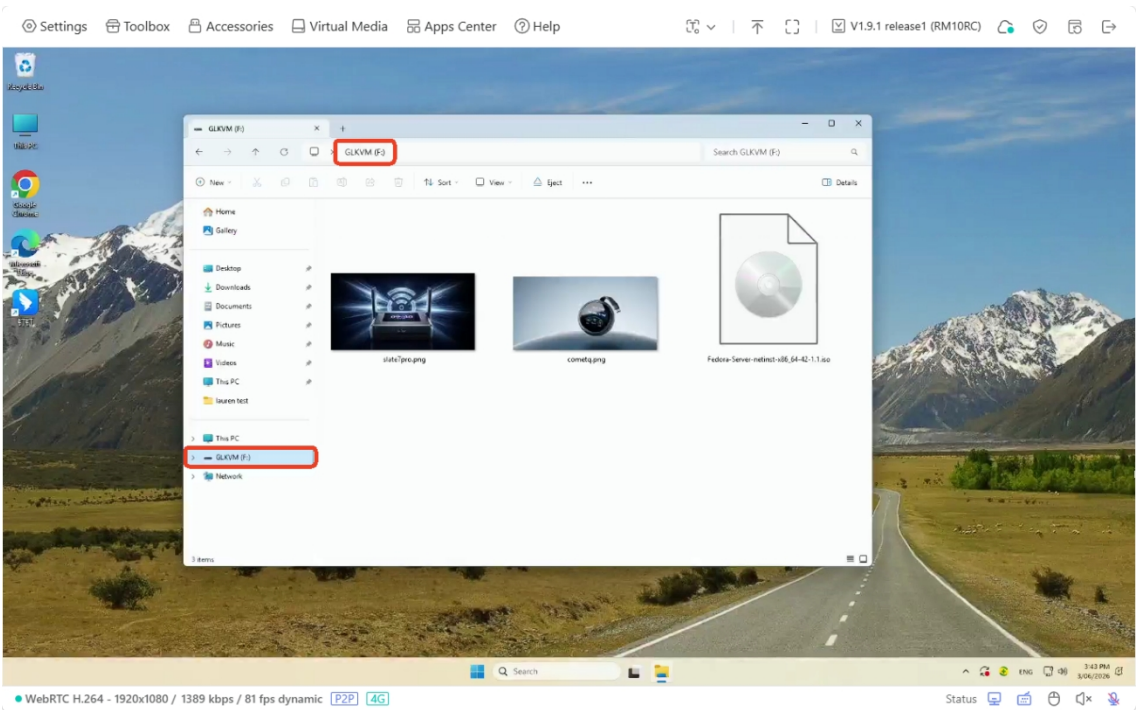
2. Click **Mount To Remote** > **File Sharing**.



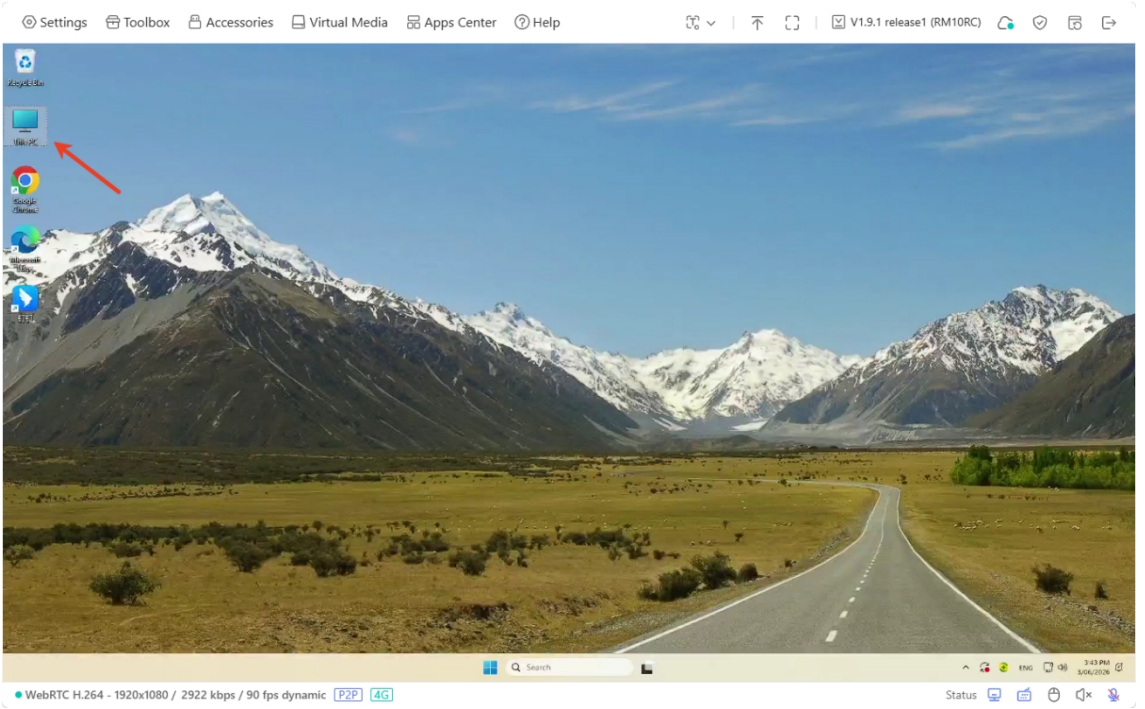
3. A window will pop up on the console indicating the file sharing steps, as shown below.



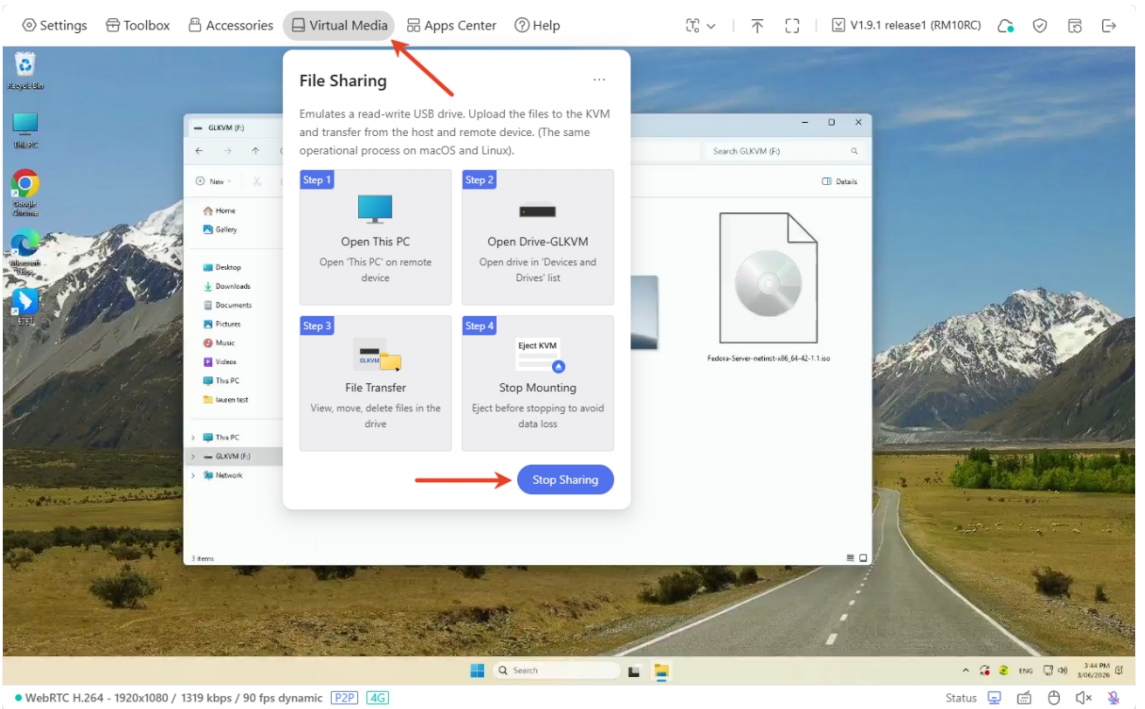
4. Wait a second, and a drive named "**GLKVM**" will pop up on the screen automatically. You will then see the files you previously uploaded from the controlling device to Comet 5G have been shared to the controlled device. Now you can view, move or delete the files in this drive on the controlled device.



Tip: If the drive does not pop up automatically, go to **This PC** of your controlled device and find a drive named GLKVM. Then you can view, move or delete the files in this drive.

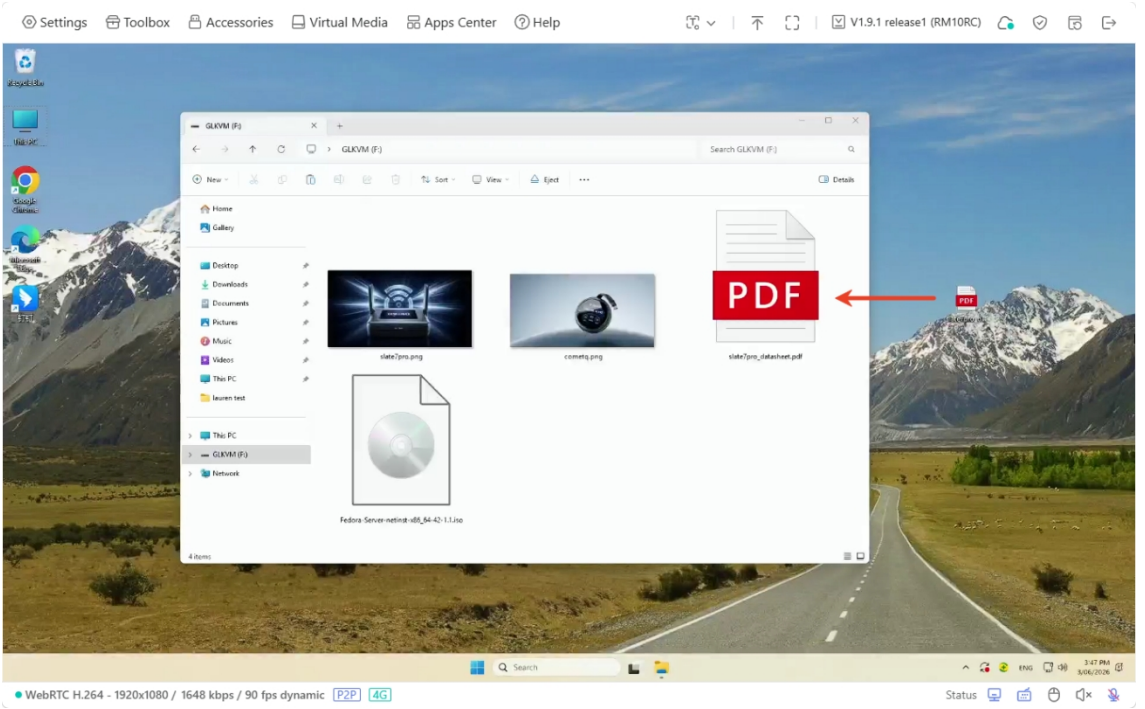


5. If you want to stop sharing, click **Virtual Media** in the toolbar and click **Stop Sharing**.

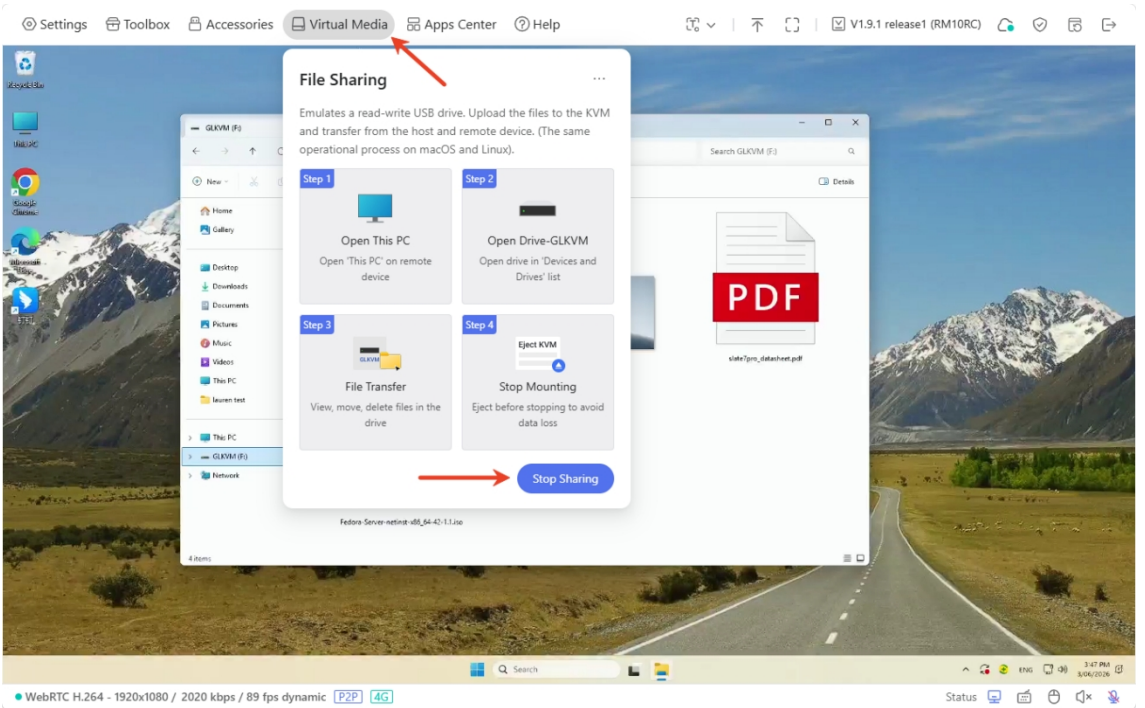


6. To share files from the controlled device to the controlling one, move or copy the files you want to share from the controlled device into the drive **GLKVM**. For example, a PDF file

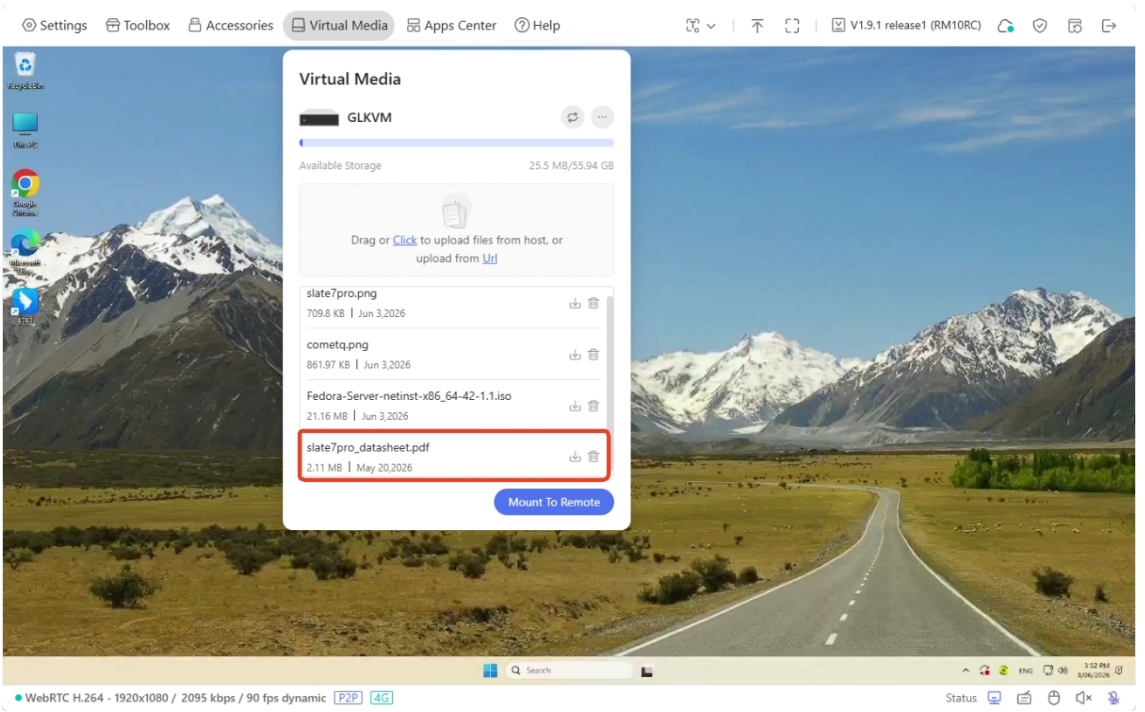
named "slate7pro_datasheet" has been copied from the controlled device's Desktop into the disk GLKVM.



7. Turn to the Comet 5G's console, click **Virtual Media** in the toolbar and click **Stop Sharing**.



8. This file will then be displayed under the **Virtual Media**, as shown below. Now you can download this file from Comet 5G to your controlling device.

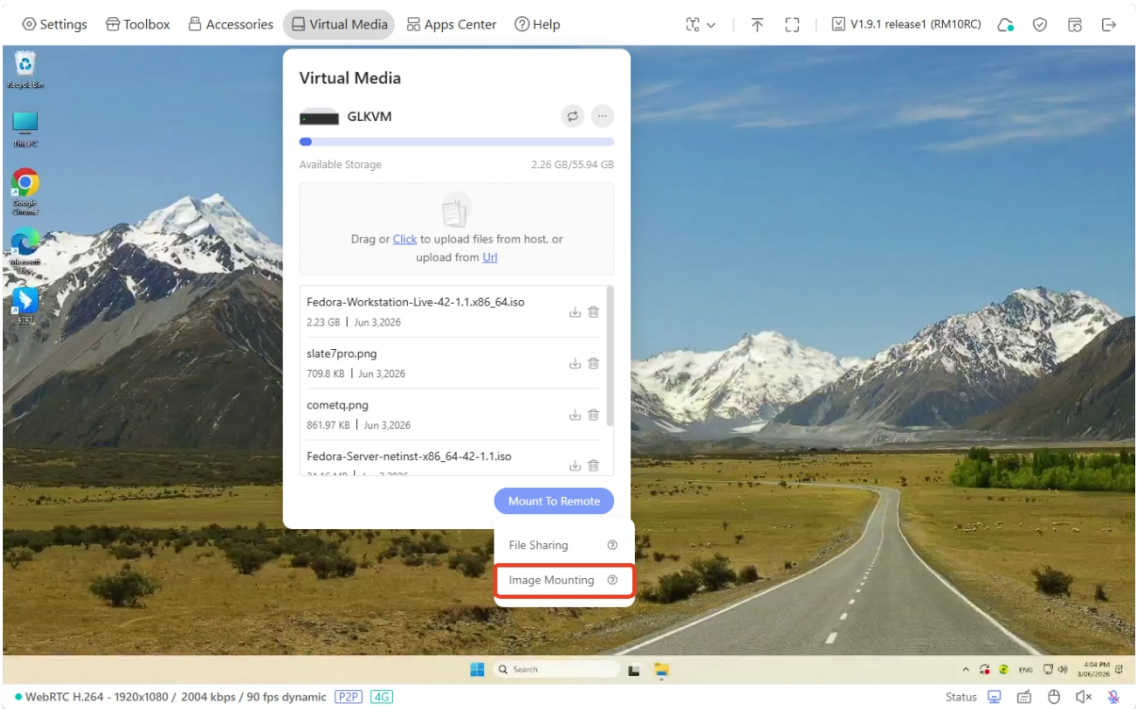


8.2 Image Mounting

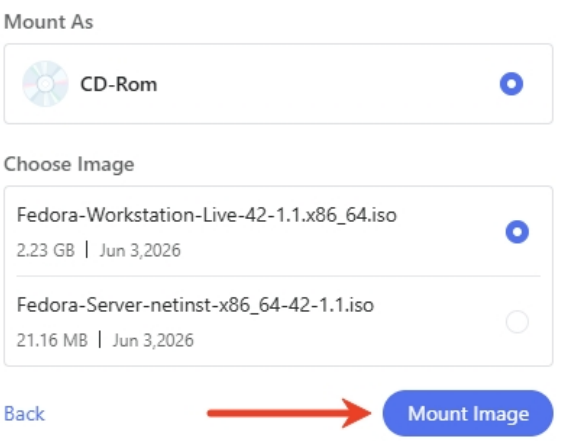
Comet 5G can simulate a read-only virtual CD/DVD or disk drive on the device being controlled. You can access this drive during the BIOS or UEFI startup process. This function can help you reinstall the operating system or mount an ISO to install applications on the device being controlled, or perform other tasks.

Follow the steps below to mount image.

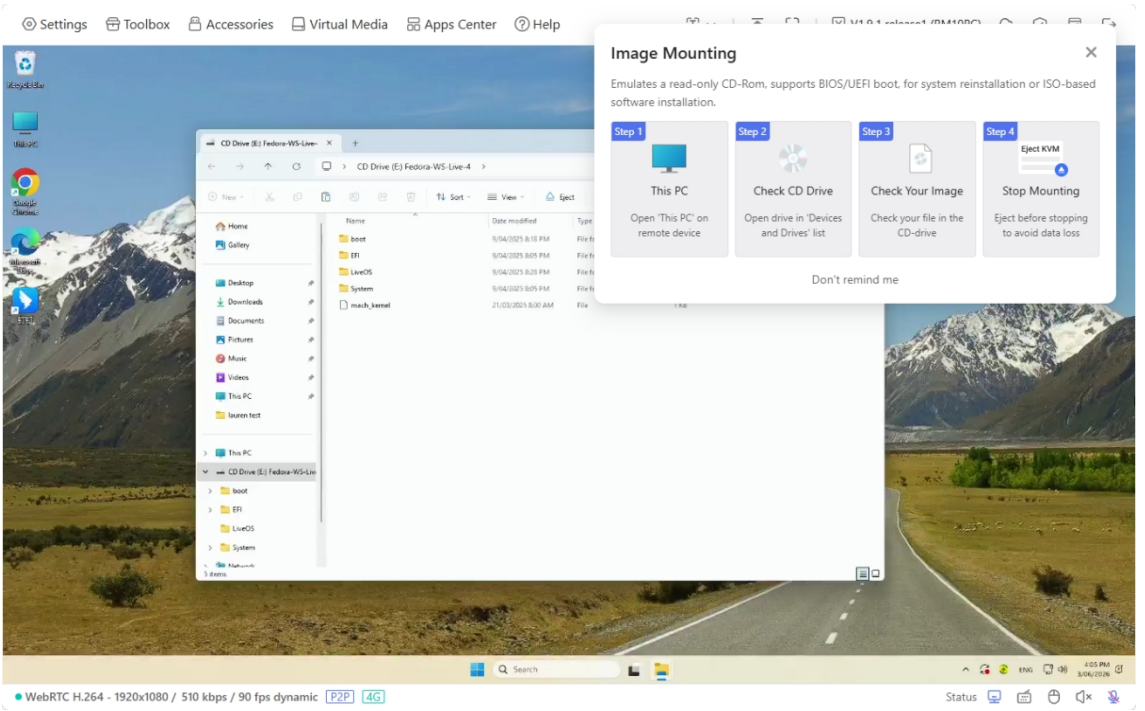
1. Drag or click the box to upload files. **Ensure this file can be mounted as an iso format.**
2. Click **Mount To Remote** > **Image Mounting**.



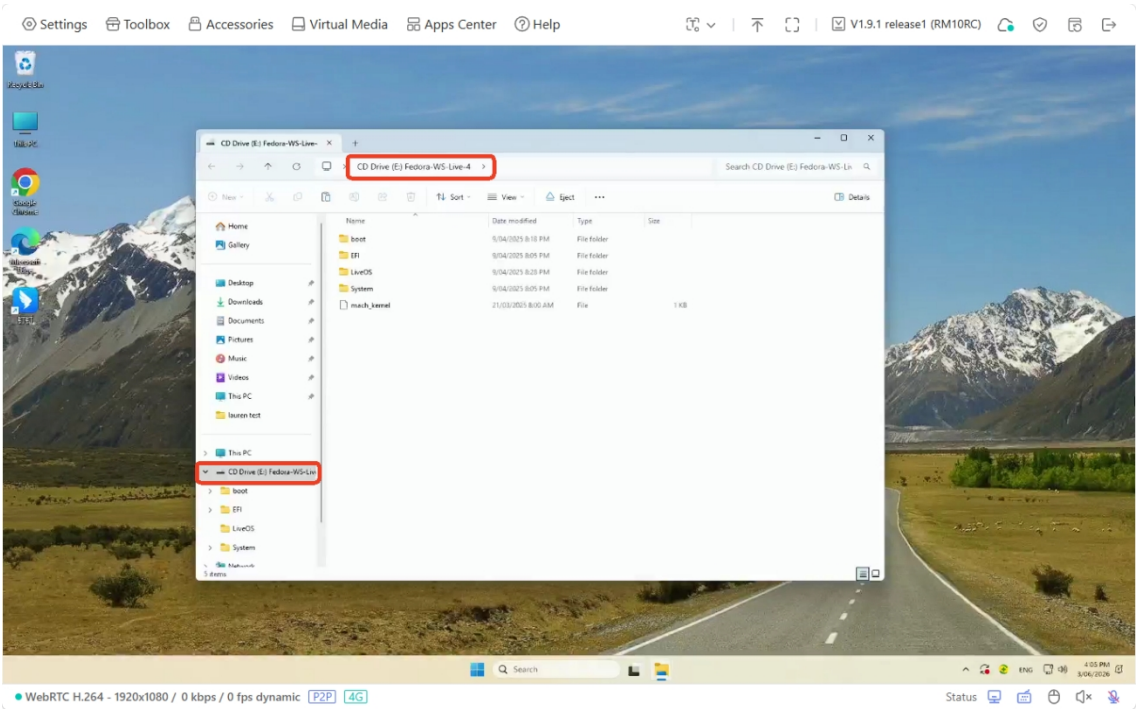
3. Select the file and click **Mount Image**.



4. A window will pop up on the console indicating the mounting steps, as shown below.

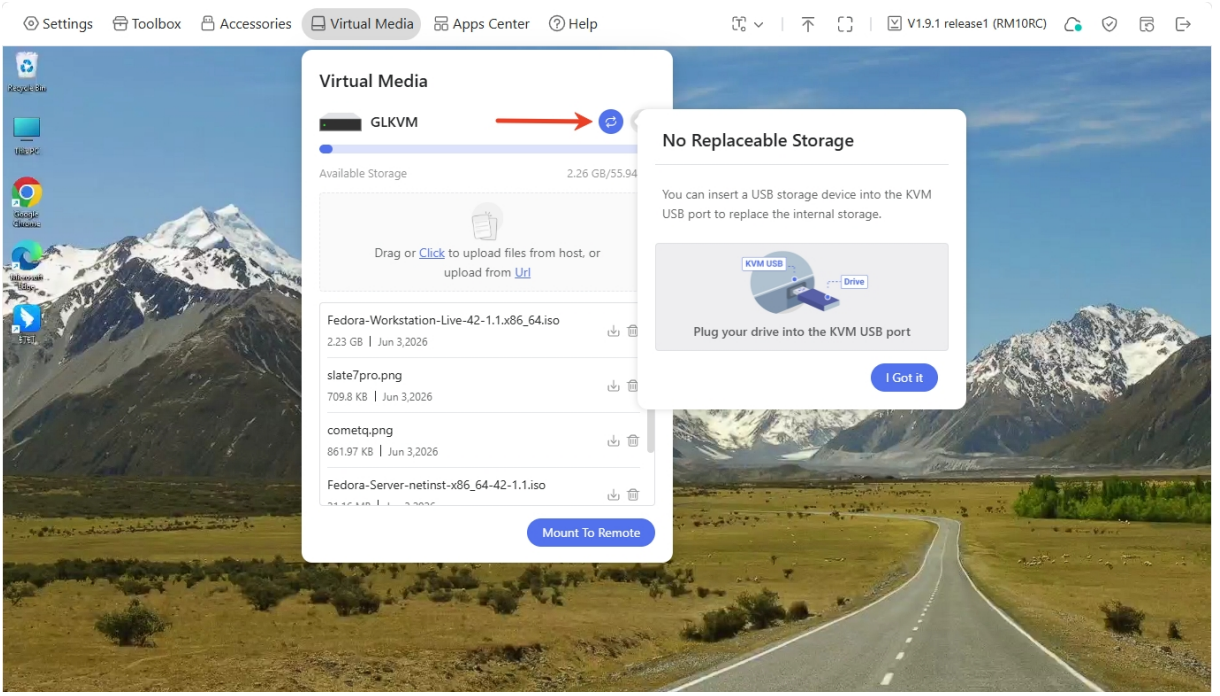


5. Now you can use this file from the CD drive on the controlled device.



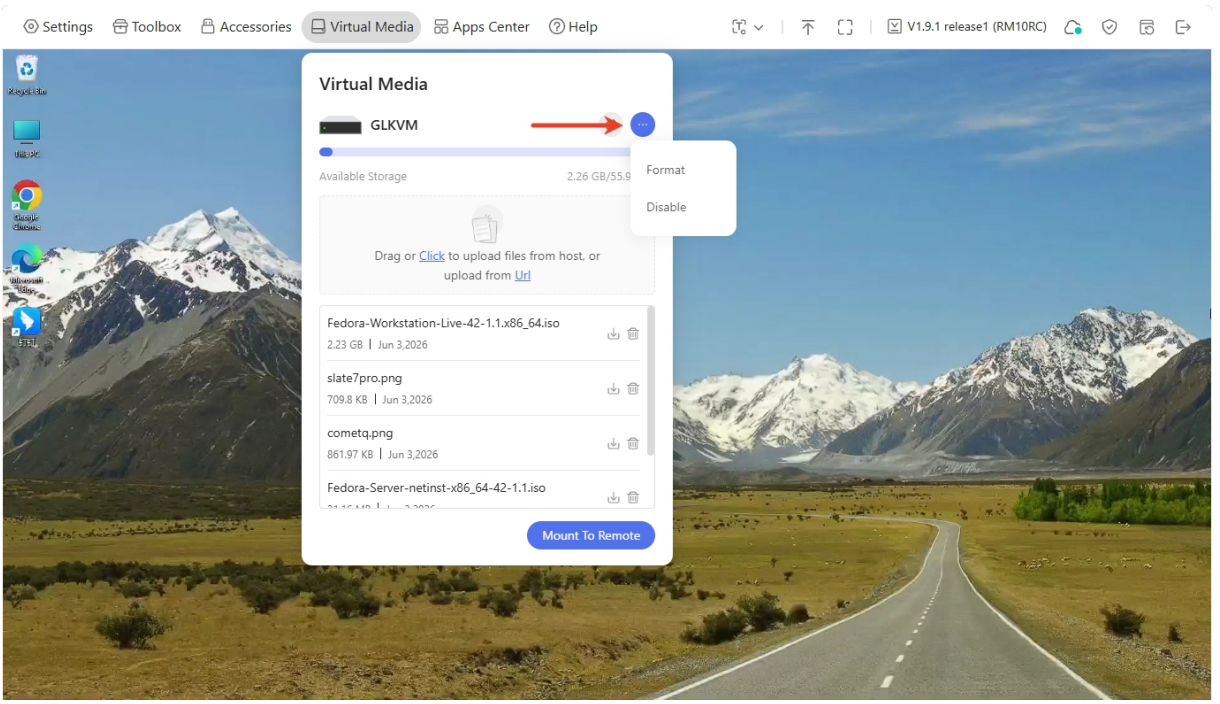
8.3 Replace Storage Drive

You can insert a USB storage device into the KVM USB port to replace the internal storage.



8.4 Format Disk

You can format the disk or disable the virtual media with one click.



Chapter 9

Apps Center

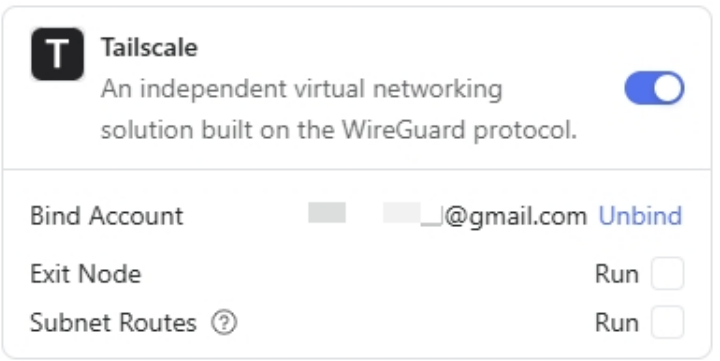
This chapter introduces some applications integrated in GL.iNet KVM console.

9.1 Tailscale

Tailscale is a WireGuard®-based mesh VPN service that builds encrypted peer-to-peer private networks across devices without port forwarding or complex firewall setup.

Comet 5G integrates with Tailscale, allowing you to remotely access it through Tailscale virtual network. Simply bind Comet 5G and your controlling device to the same Tailscale account, then you can remotely access your Comet 5G by entering its Tailscale virtual IP in a web browser on the controlling device, without installing the GLKVM app. See 4.3 Tailscale for details.

After binding, the console displays the linked Tailscale account and unlocks some advanced features including Exit Node and Subnet Routes.

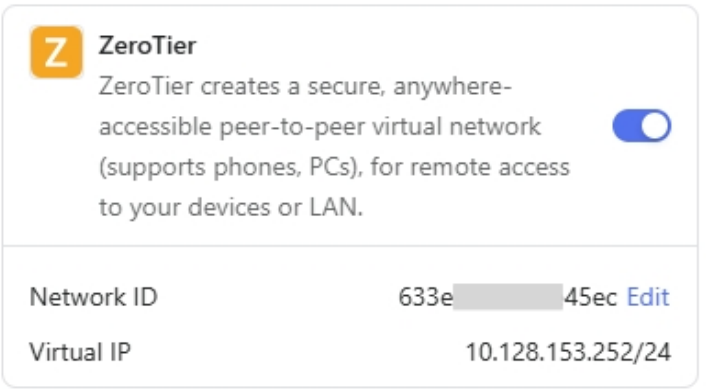


9.2 ZeroTier

ZeroTier creates encrypted overlay virtual networks to connect scattered devices globally as if they are inside the same local area network.

Comet 5G integrates with ZeroTier, allowing you to remotely access it through ZeroTier virtual network. Simply join Comet 5G and your controlling device to the same ZeroTier network, then you can remotely access your Comet 5G by entering its ZeroTier IP in a web browser on the controlling device, without installing the GLKVM app. See 4.4 ZeroTier for details.

After binding, the console displays the ZeroTier Network ID and Virtual IP.

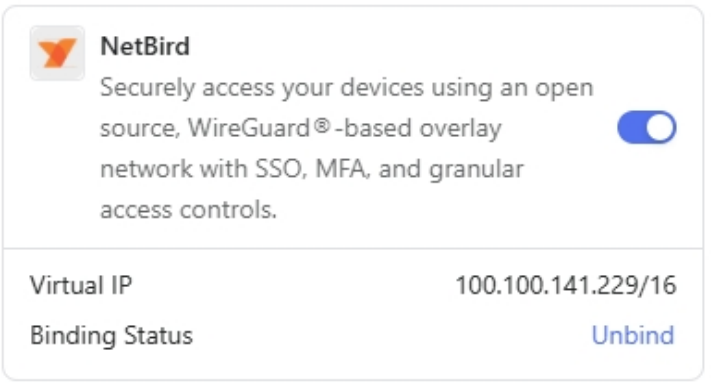


9.3 NetBird

NetBird is an open-source zero trust networking platform that lets you build secure private networks for home and business use. As a WireGuard®-based overlay network, NetBird enables secure access to your devices anytime and anywhere.

Comet 5G integrates with NetBird, allowing you to remotely access it through NetBird virtual network. See 4.5 NetBird for details.

After binding, the console displays the NetBird Virtual IP.



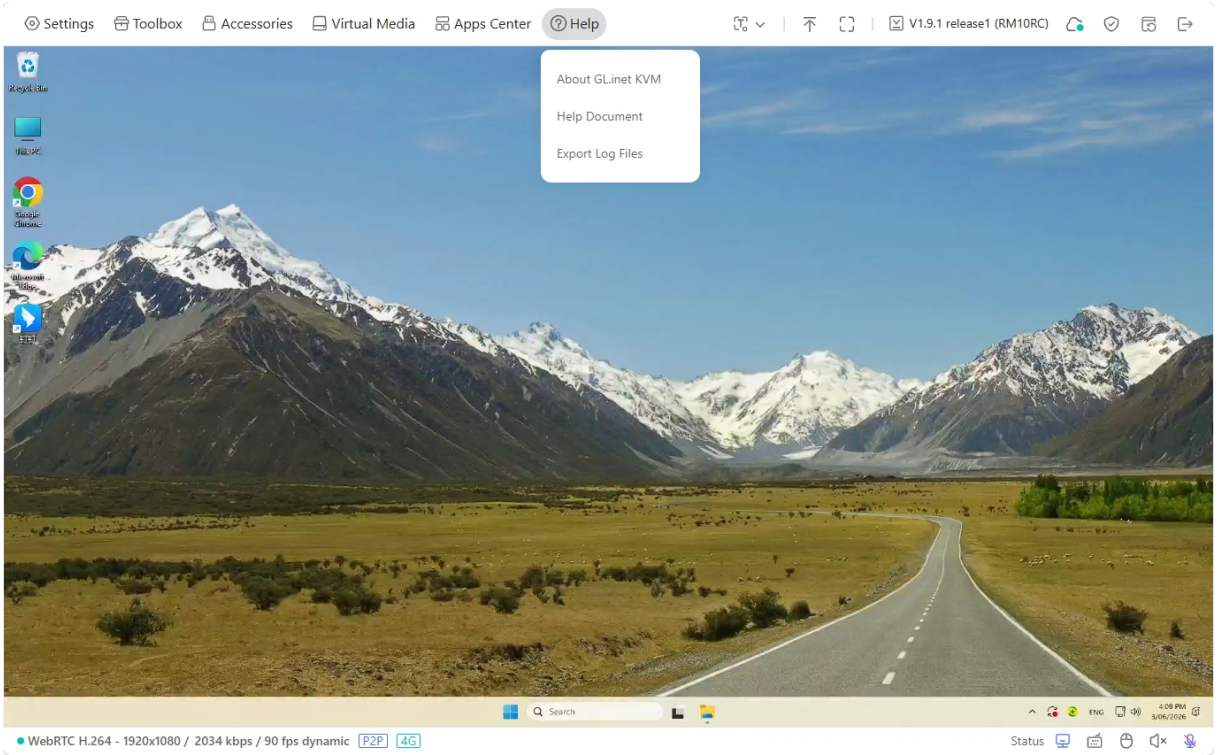
Chapter 10

System Tools

This chapter describes the system tools on the top menu bar of the KVM Web console.

10.1 Help Center

Log in to the KVM Web console and navigate to **Help**. You can find more information about GL.iNet KVM and help documentation, as well as export logs for troubleshooting.

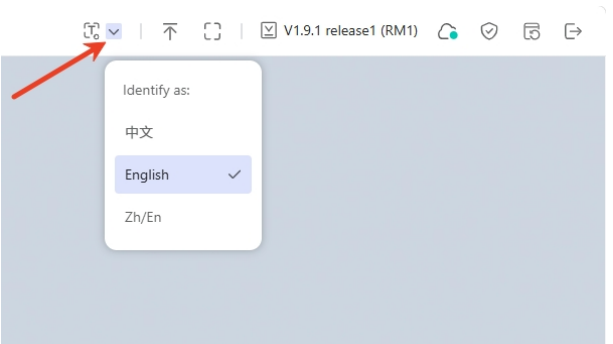


10.2 Text Recognition

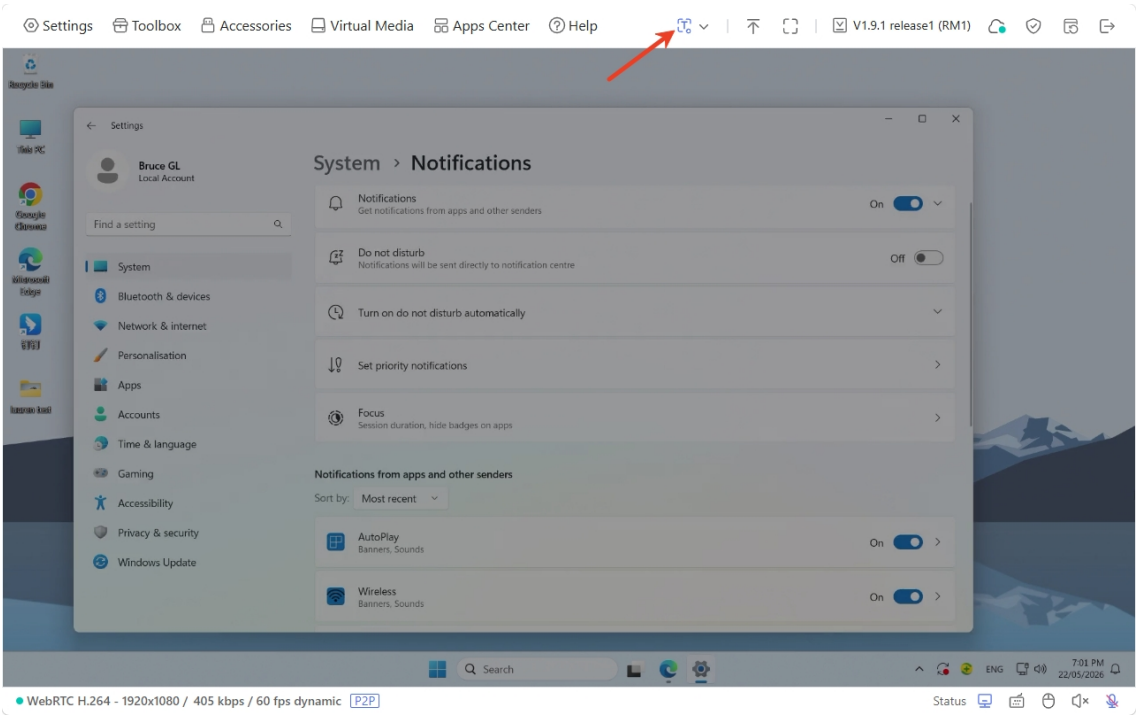
The Text Recognition feature is driven by Optical Character Recognition (OCR) technology and was introduced in firmware v1.9.0. With this feature, you can easily capture text from the remote screen (i.e., the controlled device) and copy it to the controlling device.

Follow the steps below to capture text.

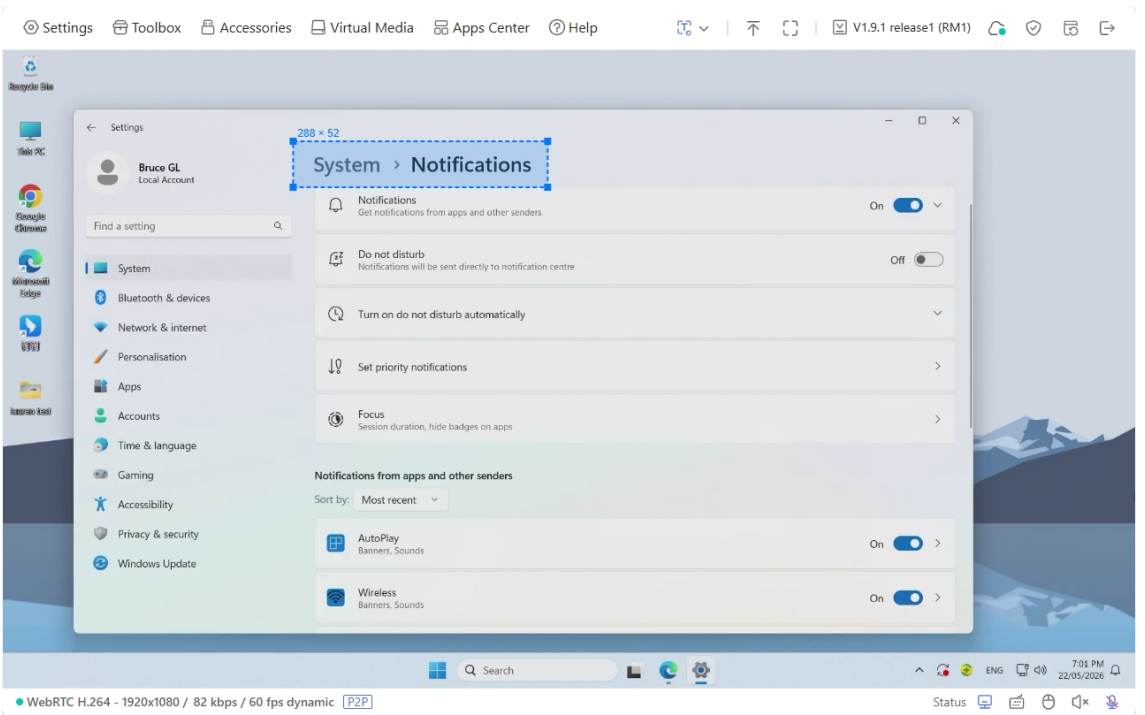
1. Log in to your KVM console. Click the downward arrow at the top menu to select your preferred recognition language, such as Chinese, English, or bilingual (Zh/En).



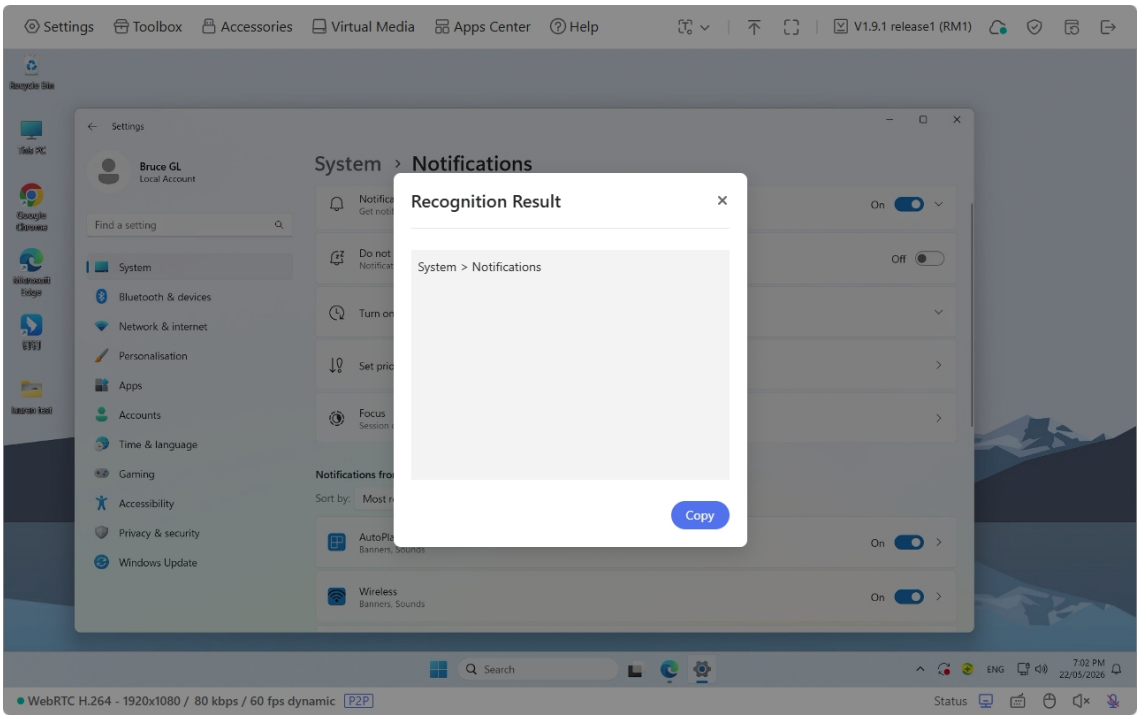
2. Click the "**T**" icon at the top center of the toolbar, and the remote screen will dim.



3. Draw a box around the text you want to extract, as shown below.

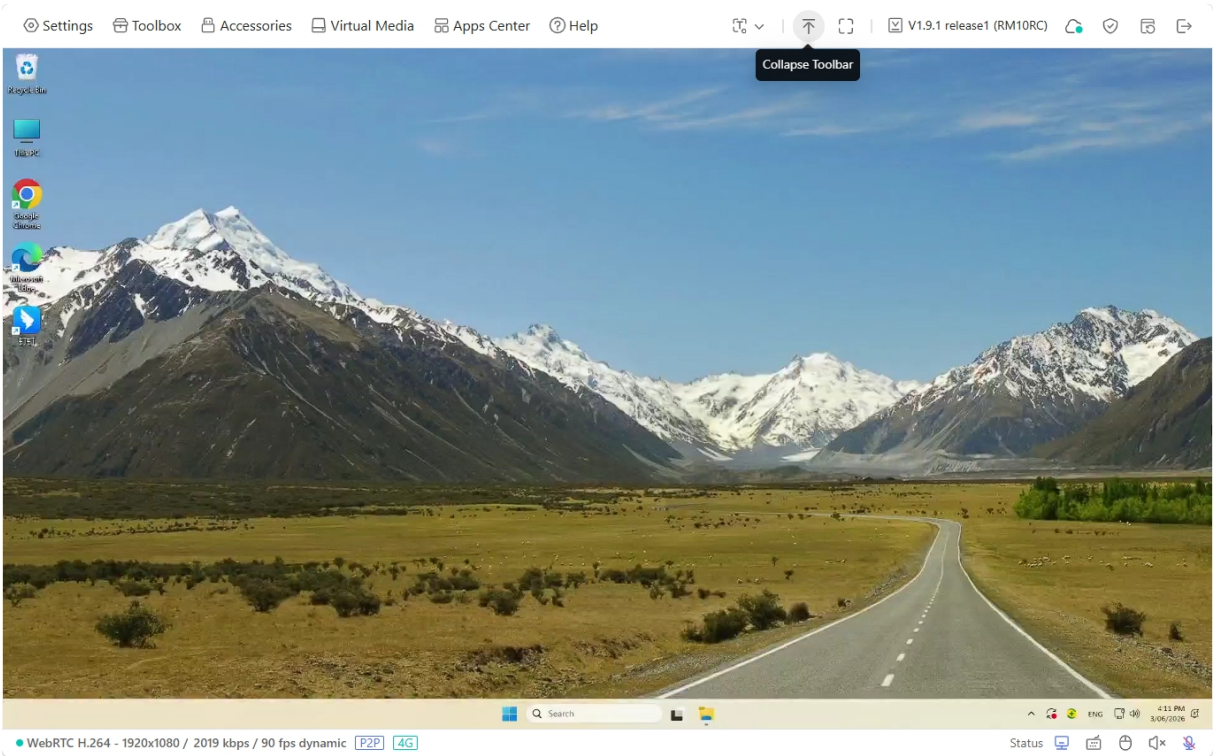


4. The system will identify the text within the selected area automatically. You can then copy the recognized text as needed.

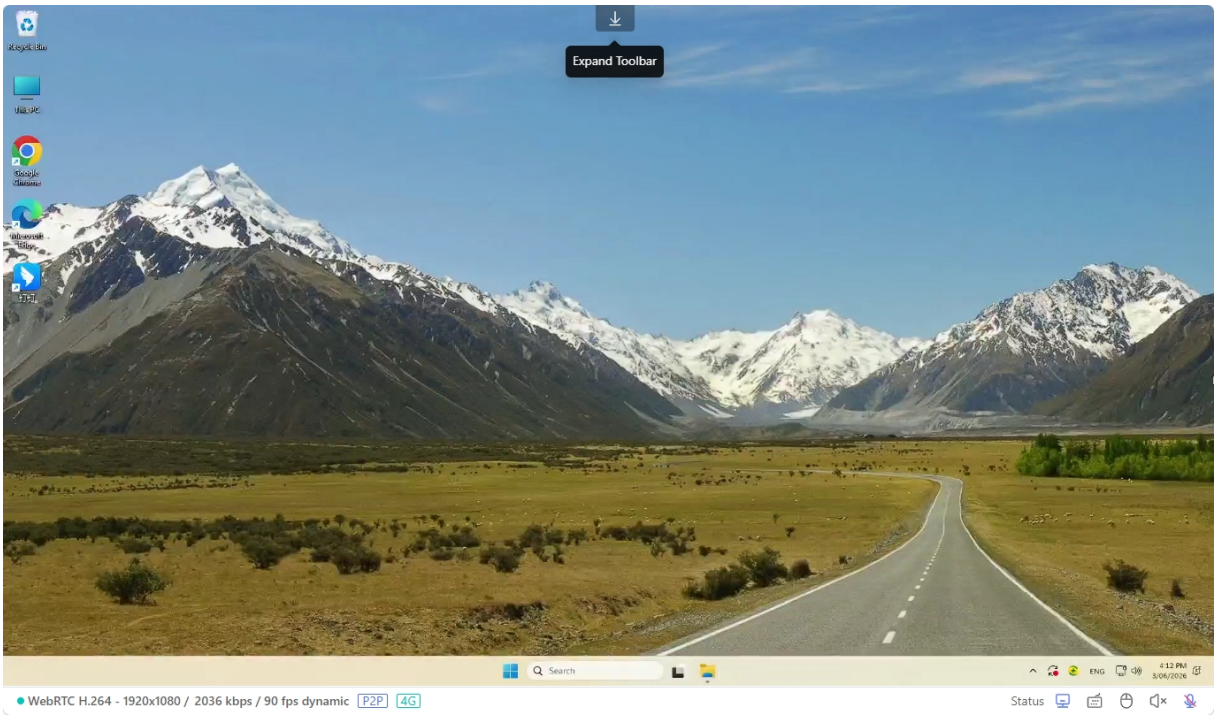


10.3 Collapse

Click the upward arrow icon in the top right corner to collapse the toolbar.

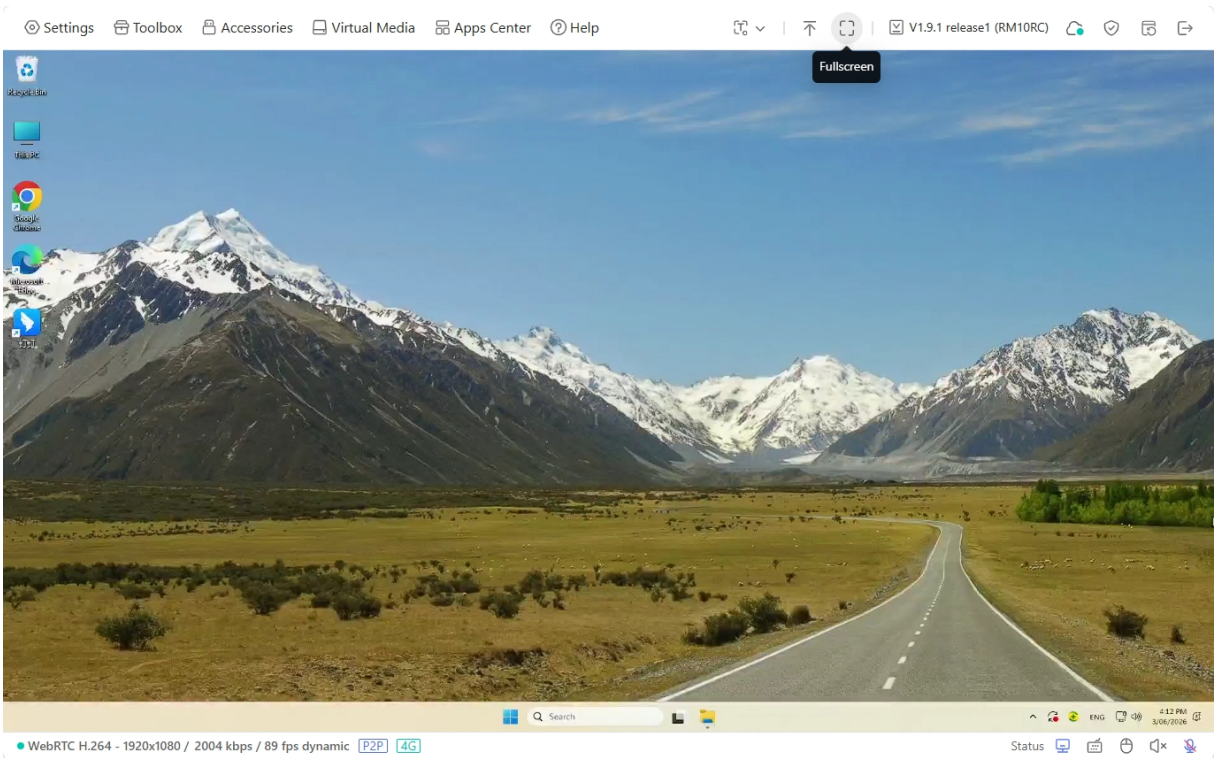


When the toolbar is folded, click the downward arrow icon at the top to expand it.

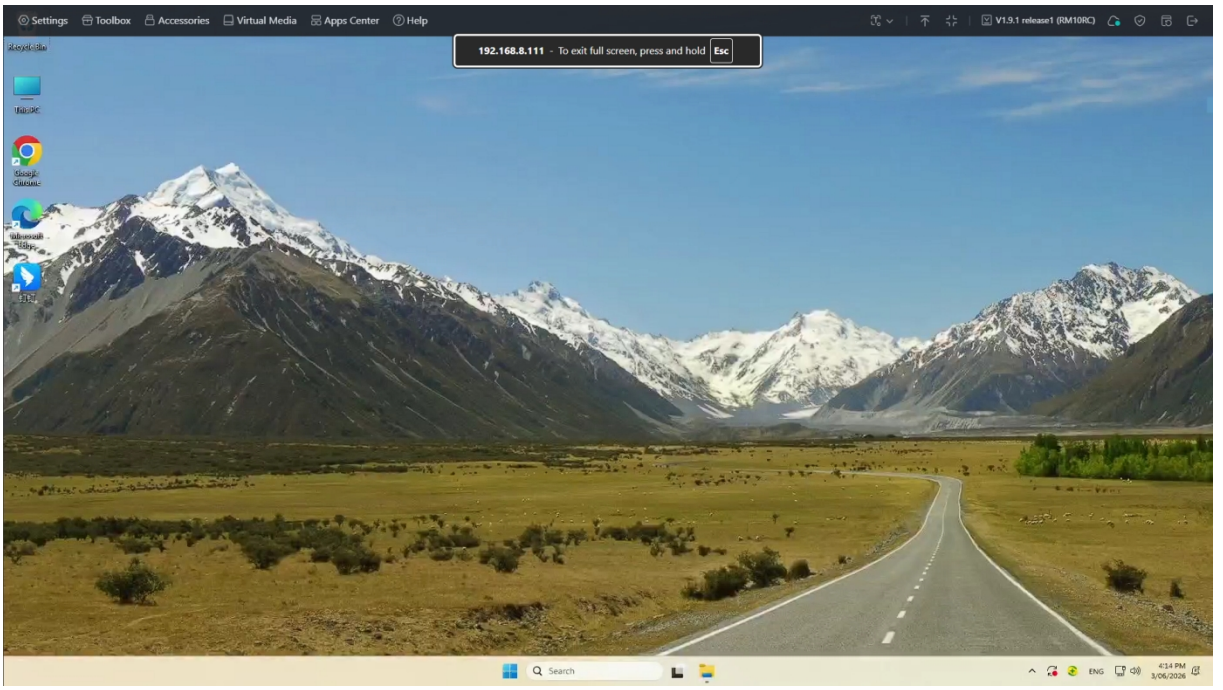


10.4 Fullscreen

Click the fullscreen icon (square-shaped) in the top right corner to switch to fullscreen mode.

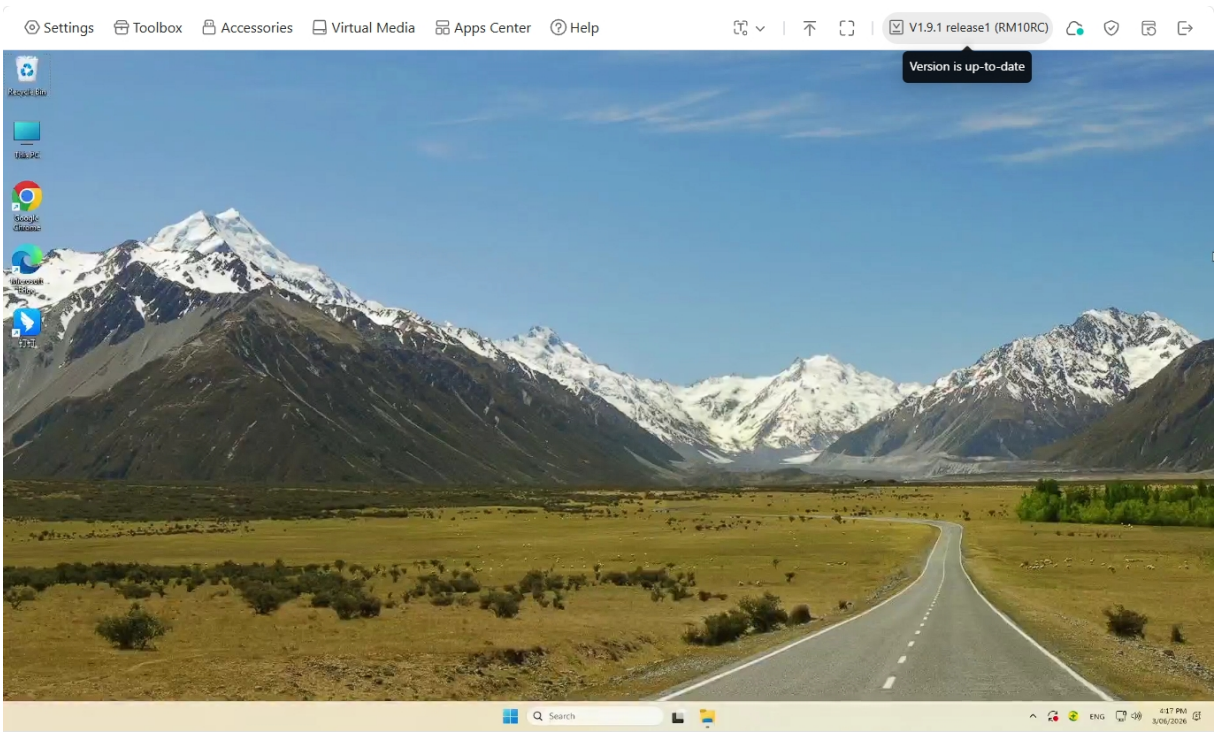


To exit fullscreen, press and hold the **Esc** key, or click the exit fullscreen icon (grid-shaped) in the upper right corner.

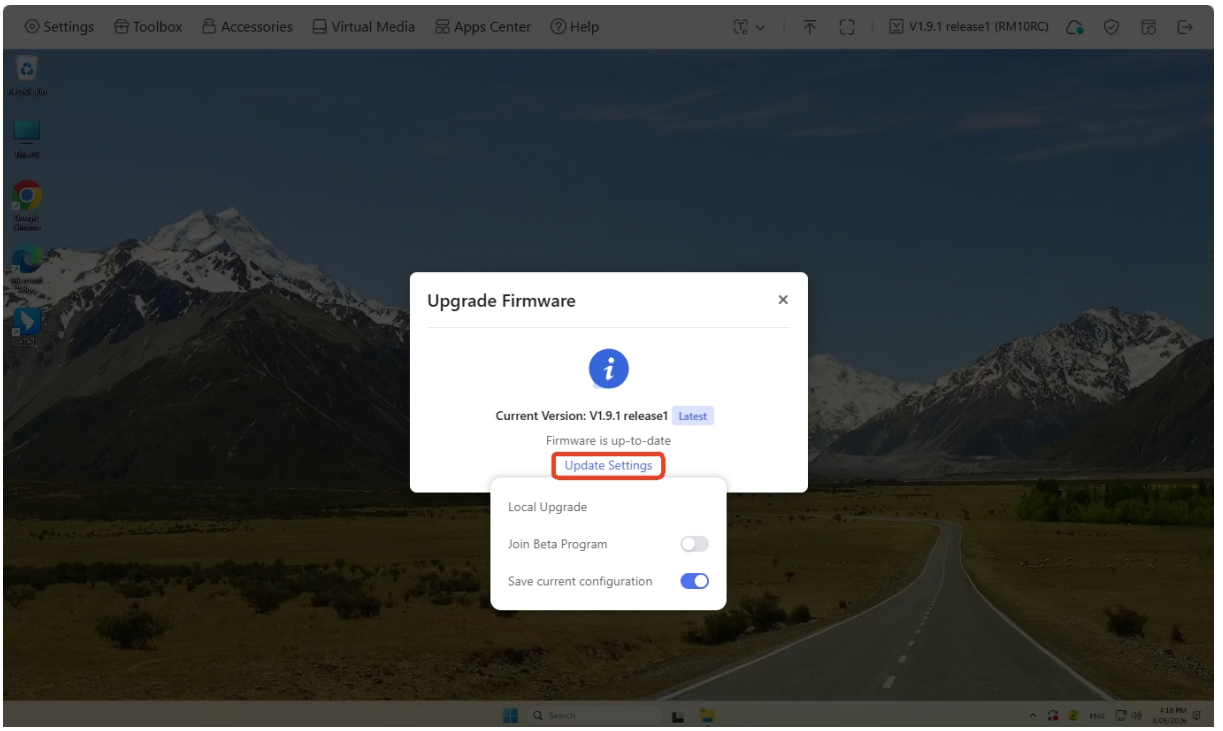


10.5 Upgrade

Click the firmware version in the upper right corner to check for updates.



In the pop-up window, you can click **Update Settings** to perform a local upgrade, join Beta program, or save current configuration.

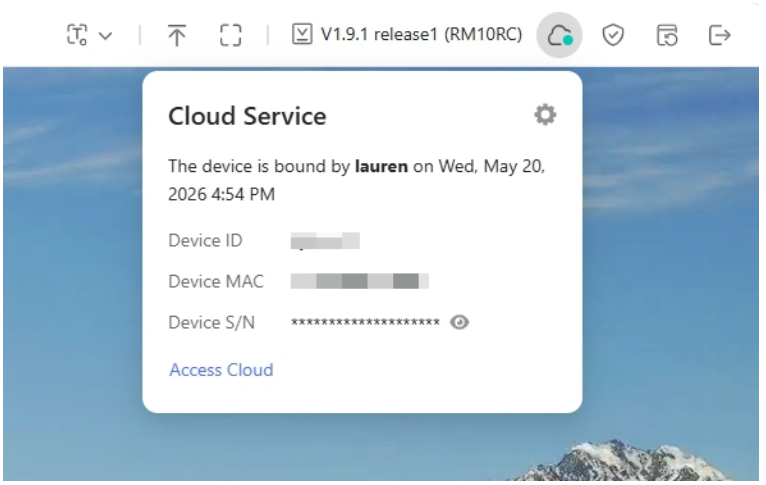


Tip: Download the latest firmware from the Firmware Download Center before performing a local upgrade.

10.6 Cloud Service

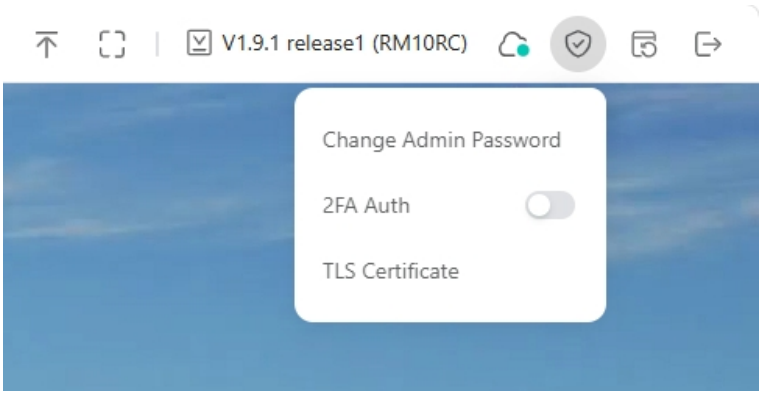
GL.iNet KVM Cloud allows you to access the controlled device remotely. See 4.1 Cloud Service for details.

Once your Comet is bound to the Cloud, the console will display the cloud status as follows.

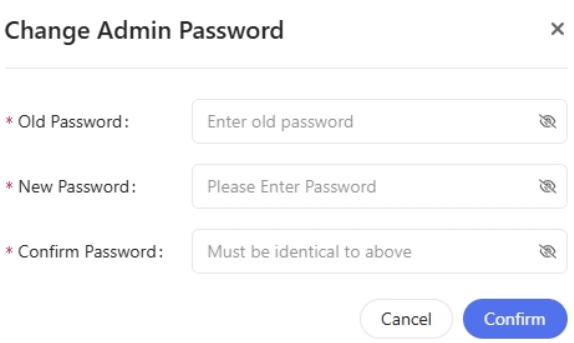


10.7 Security

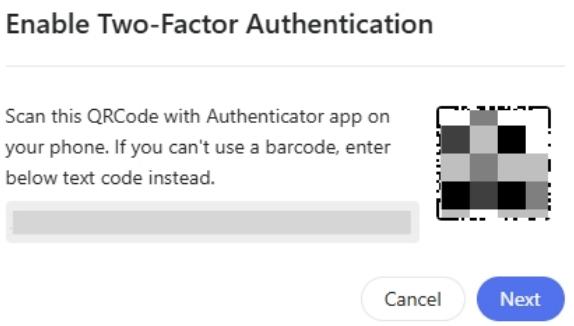
The security allows you to change admin password, enable two-factor authentication, and customize TLS certificate.



- **Change Admin Password**

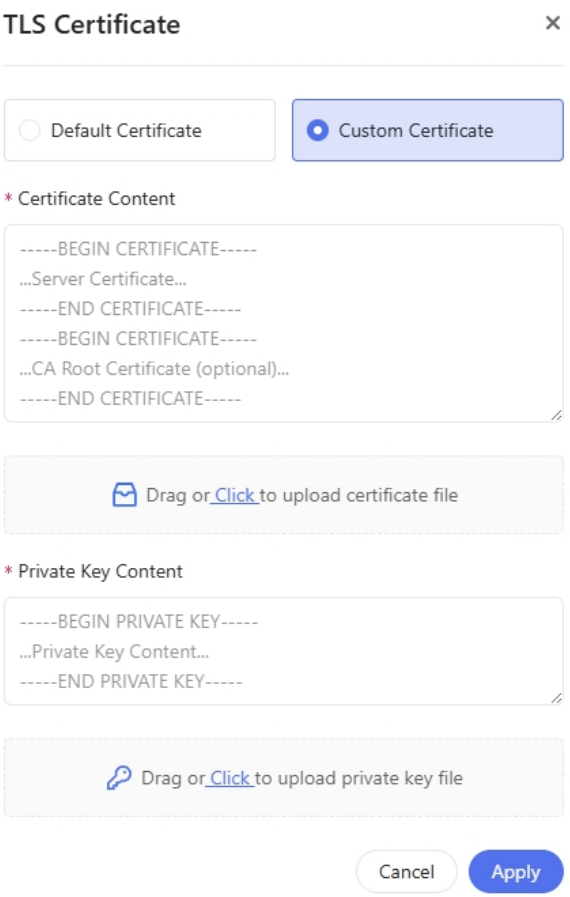


- **2FA**: Enable two-factor authentication to protect your account.



- **TLS Certificate**

  The system will use the pre-installed default certificate for browser access. If you want to customize the TLS certificate for web browser access, click TLS Certificate in the upper right corner of the console, select Custom Certificate, then upload your certificate file & private key file.


TLS Certificate
Default Certificate
Custom Certificate
* Certificate Content
-----BEGIN CERTIFICATE-----
...Server Certificate...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
...CA Root Certificate (optional)...
-----END CERTIFICATE-----
Drag or Click to upload certificate file
* Private Key Content
-----BEGIN PRIVATE KEY-----
...Private Key Content...
-----END PRIVATE KEY-----
Drag or Click to upload private key file
Cancel
Apply

Regulatory Statement

FCC ID: 2AFIW-RM10RC

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

IC Caution

This device complies with Innovation, Science, and Economic Development Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) This device may not cause interference, and

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d' Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

(1) l'appareil ne doit pas produire de brouillage, et
(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

The user manual for LE-LAN devices shall contain instructions related to the restrictions mentioned in the above sections, namely that:
i. the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;
i. le dispositif utilisé dans la bande 5150-5250 MHz est réservé à une utilisation en intérieur afin de réduire le risque de brouillage préjudiciable aux systèmes mobiles par satellite dans le même canal.

FCC/IC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator& your body.
L'appareil est conforme aux limites d'exposition aux rayonnements spécifiées par la FCC/ISED pour les environnements non contrôlés. La distance entre le radiateur et le corps doit être d'au moins 20 cm lors de l'installation et du fonctionnement de l'appareil.

Frequency band: 5150 - 5250 MHz:
Indoor use: Inside buildings only. Installations and use inside road vehicles and train carriages are not permitted.
Limited outdoor use: If used outdoors, equipment shall not be attached to a fixed installation or to the external body of road vehicles, a fixed infrastructure or a fixed outdoor antenna. Use by unmanned aircraft systems (UAS) is limited to within the 5170 - 5250 MHz band.

Frequency band: 5250 - 5350 MHz:
Indoor use: Inside buildings only. Installations and use in road vehicles, trains and aircraft are not permitted. Outdoor use is not permitted.

Frequency band: 5470 - 5725 MHz:
Installations and use in road vehicles, trains and aircraft and use for unmanned aircraft systems (UAS) are not permitted.

Declaration of Conformity

Hereby, GL TECHNOLOGIES (HONG KONG) LIMITED declares that this product type [Remote KVM, GL-RM10RC] is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU, 2014/30/EU and 2011/65/EU. The full text of the EU declaration of conformity is available at https://www.gl-inet.com/products/certificate.

Wi-Fi Transmission Power:
FCC: ≤30dBm (2.4 GHz), ≤30dBm (5 GHz)
CE: ≤20dBm EIRP (2.4GHz); ≤23dBm EIRP (5.15GHz~5.35GHz); ≤30dBm EIRP (5.47GHz~5.725GHz); ≤13.98dBm (5.725GHz~5.85GHz)
Power supply: ICP20-050-3000D

Cellular Data Transmission Power:
CE:
LTE Band 1/3/5/7/8/20/28/B34: 25dBm; Band 38/40/41/42/43: 28dBm;
5G NR SA Band n1/3/5/7/8/20/28: 25dBm
5G NR SA Band 38/40/41/77/78: 28dBm
FCC, IC:
LTE Band 2/4/5/7/12/13/14/17/25/26/48/66/70/71: 25dBm; Band 30: 24dBm; B38/41/42/43: 28dBm;
5G NR SA Band n2/5/7/12/13/14/25/26/66/70/71: 25dBm; n30: 24dBm; n38/41/77/78: 28dBm