GL·iNet



User Manual

GL-RMQ1 / Comet Q

All-in-One USB Remote KVM

Firmware Version 1.8.1

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 Compatibility 11

1.4 Package Contents 12

Chapter 2 Hardware Connection 13

Chapter 3 Local Access 16

3.1 Domain 17

3.2 IP Address 19

Chapter 4 Remote Access 21

4.1 Cloud Service 22

4.2 GLKVM App 26

4.3 Tailscale 32

4.4 ZeroTier 38

4.5 NetBird 46

Chapter 5 Settings 52

5.1 Video 53

5.2 Audio&Keyboard&Mouse 55

5.3 System 58

5.4 Network 59

Chapter 6 Toolbox 60

6.1 Clipboard 61

6.2 Shortcut 61

6.3 Terminal 62

Chapter 7 Virtual Media 63

7.1 File Sharing 64

7.2 Format Disk 69

Chapter 8 Apps Center 70

8.1 Tailscale 71

8.2 ZeroTier 72

8.3 NetBird 73

Chapter 9 System Tools 74
9.1 Help Center 75
9.2 Collapse 76
9.3 Fullscreen 77
9.4 Upgrade 78
9.5 Cloud Service 79
9.6 Security 80
Frequently Asked Questions 82
Regulatory Statement 86

Chapter 1

Get To Know Your Device

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

1.1 Product Overview

Comet Q is a palm-sized device that can plug into mobile phones, Mac mini, or any laptop via USB-C. Once connected, you may open a browser to gain full control of the target device, with no extra software installation or complex configuration required. Its built-in 1.8 inches touchscreen enables quick setup, status checks, and on-device action triggers directly from the unit. It is the world's first KVM that can controls smart phones from a browser remotely — a feature previously unavailable.

1.1.1 Appearance







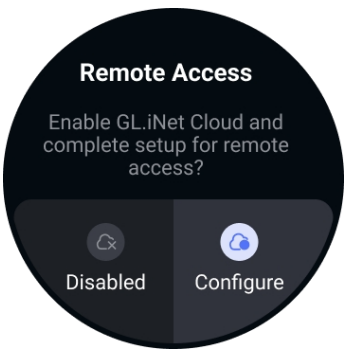


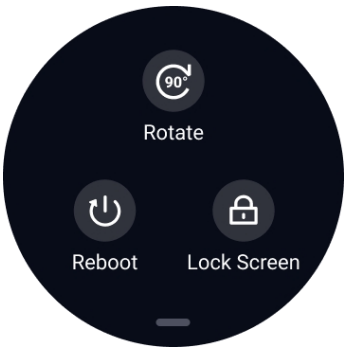
1.1.2 Interface and Dimension



Item	Description
USB Type-C Port	This port supports Power Passthrough. Connect it to a power adapter if needed.
USB Type-C Cable	This cable supports DP Alt Mode. Connect it to the controlled device.
Reset Pinhole	Insert a pin into the pinhole, hold for **8 seconds** and then release to factory reset.

1.1.3 Touchscreen

Screen Display	Description
	**Starting up** Plug Comet Q's integrated USB-C cable (attached to the bottom and can be bent out) into the target device, or connect Comet Q to an external power adapter to power it on. 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 4-digit screen password for your Comet Q to protect your privacy.
	**Set up network** Connect Comet Q to a 2.4 GHz or 5 GHz Wi-Fi network. You can configure now or skip this step to set it up later.
	**Cloud access** Enable Cloud service for remote access. You can configure now or skip this step to set it up later.

	**Home screen** **Top**: Wi-Fi connectivity status, cloud service status and system time. **Middle**: Comet Q's IP address (shown only when internet is connected). **Bottom**: Keyboard & mouse signal, session status, and video streaming signal.
	**Basic settings** On the home screen, swipe left from the right to access basic settings, including **Session**, **Wi-Fi**, **Cloud**, and **Display**.
	**System Menu** On the home screen, swipe down from the top to access system menu, including **Rotate**, **Lock Screen** and **Reboot**.
	**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 Type-C (power passthrough) 1 x USB Type-C Cable (DP Alt Mode supported)
Operating System	Buildroot
CPU	ARM Cortex, quad-core
Memory / Storage	LPDDR4 512 MB / NAND 512 MB
Display Screen	1.8 inches touchscreen
Wi-Fi Standard	IEEE 802.11 a/b/g/n/ac/ax
Wi-Fi Speed	5 GHz: 286 Mbps 2.4 GHz: 286 Mbps
Antennas	1 x internal Wi-Fi antenna
Resolution	2K QHD@60FPS
Power Input	Type-C PD, 5V/3A
Other Tools	Datasheet / Firmware / App / Unboxing / Tutorials

1.3 Compatibility

Comet Q works with any device whose USB-C port supports DisplayPort Alt Mode for video output. This includes, but is not limited to:

- **iPhones**: iPhone 15 and newer (excluding iPhone 16e, 17e and iPhone Air)
- **iPads**: All iPad Pro (2018 and newer), iPad Air (4th generation and newer), iPad mini (6th generation and newer), and iPad (10th generation and newer)
- **Android phones** (Samsung as example): Samsung Galaxy S8 and newer, Galaxy Note 8 and newer, Galaxy Z Fold/Flip series, and Galaxy Tab S series
- **Laptops & mini PCs**: Most models with a USB-C port that supports video output, including MacBooks, Mac mini, and most modern Windows laptops

1.4 Package Contents

The package includes:

- 1 x Comet Q (GL-RMQ1)
- 1 x User Guide (Quick Setup Guide)
- 1 x Thank You Card
- 1 x Silicone Case



User Guide x1



Comet Q x1



Thank You Card x1



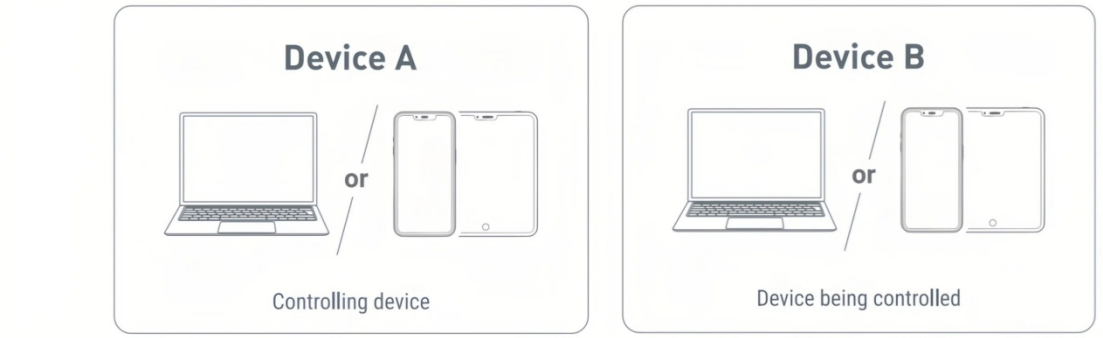
Silicon Case x1

Chapter 2

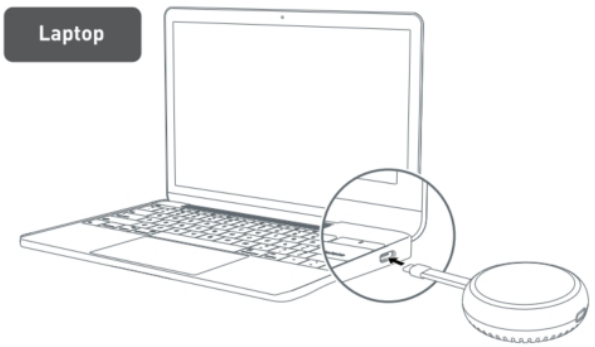
Hardware Connection

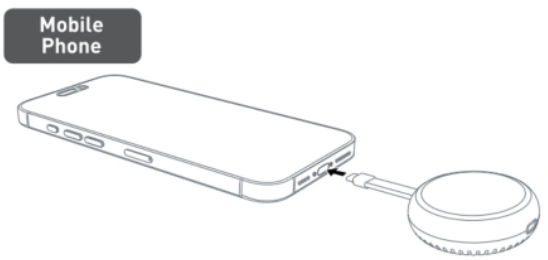
This chapter introduces the basic steps to connect the KVM and related devices.

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

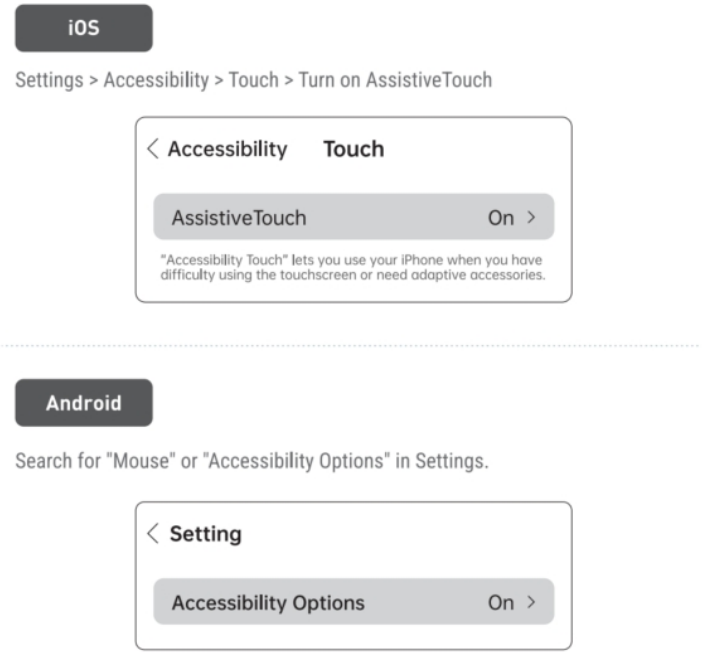


1. Connect the Comet Q's Type-C cable to the Type-C port on Device B.





2. If Device B is a touchscreen mobile device such as a smartphone or tablet, enable accessibility controls first. This allows Comet Q to operate the touchscreen.
   - iOS: **Settings** > **Accessibility** > **Touch** > **Enable AssistiveTouch**.
   - Android: Search for **Mouse** or **Accessibility** in Settings. Menu paths vary by device brand and model.



3. Follow the on-screen instructions to complete the initial setup. See 1.1.3 Touchscreen for details.
4. Device initialization is complete. Now you can access the Comet Q locally or remotely.

Chapter 3

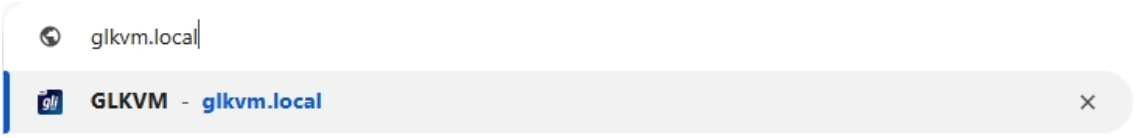
Local Access

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

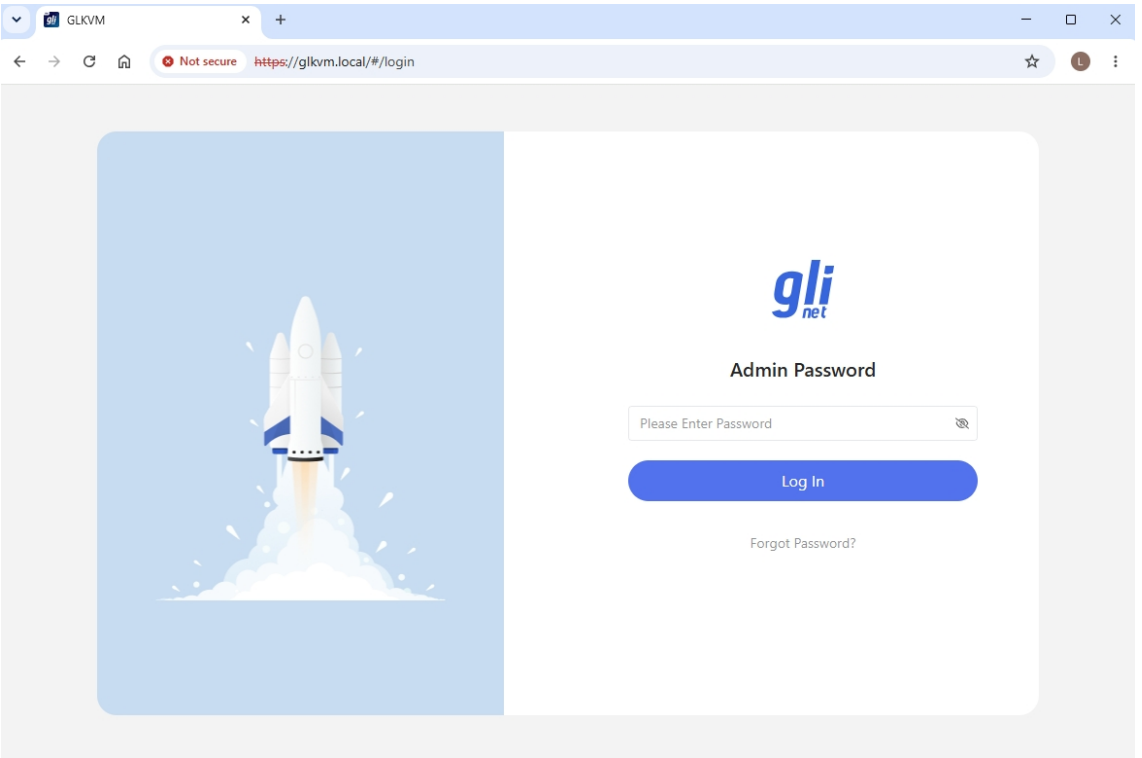
You can access your Comet Q on the local network via a domain name or an IP address.

3.1 Domain

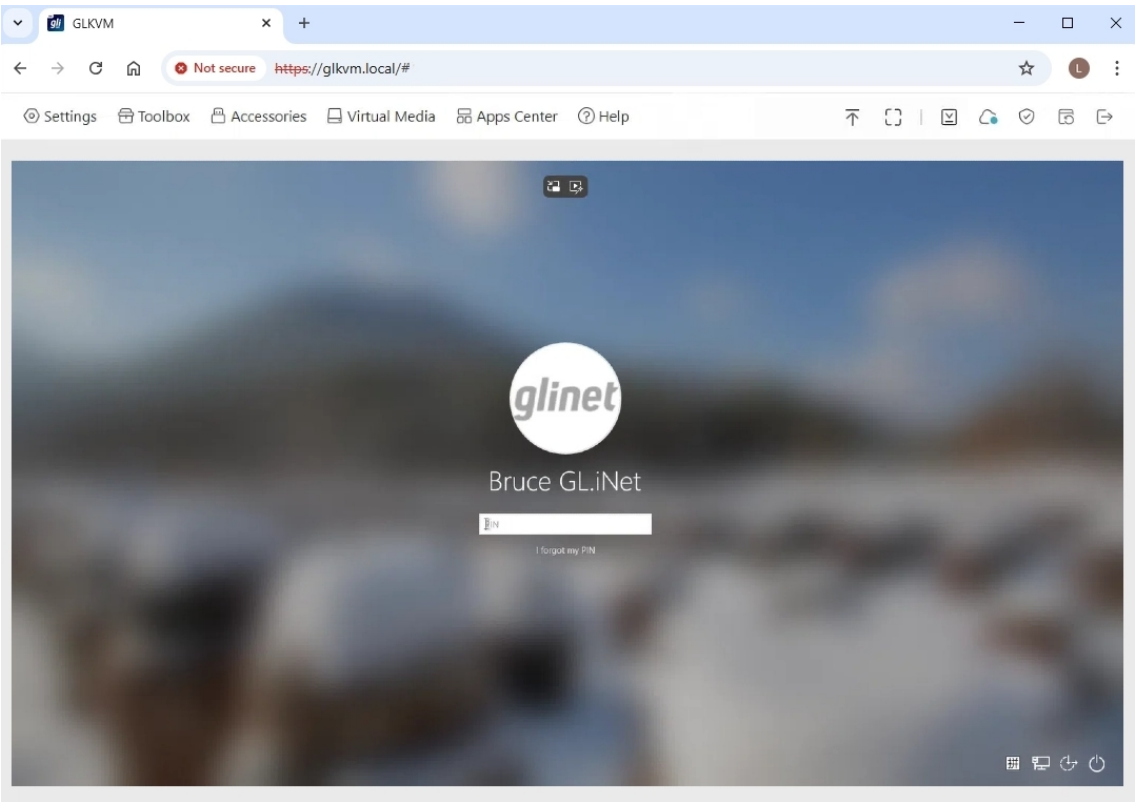
1. Ensure your controlling device is on the same LAN as Comet Q.
2. Launch a browser on the controlling device. Chrome or Edge is recommended for better compatibility.
3. Enter ***glkvm.local*** in the address bar.



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.

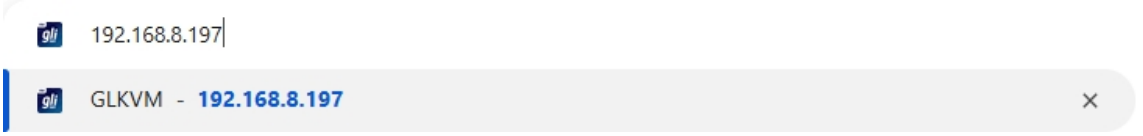


5. You will then access the Comet Q's console locally and gain access to the controlled device.

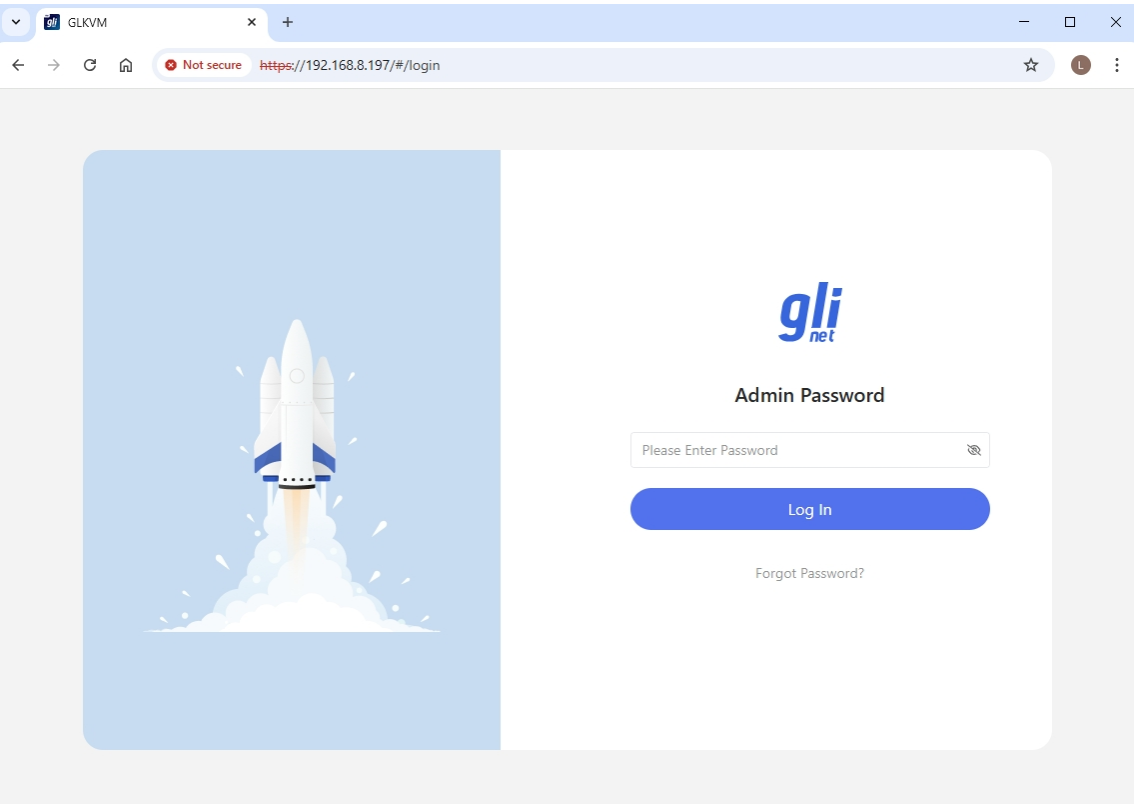

GLKVM
Not secure
https://glkvm.local/#
Settings
Toolbox
Accessories
Virtual Media
Apps Center
Help
glinet
Bruce GL.iNet
PIN
I forgot my PIN

3.2 IP Address

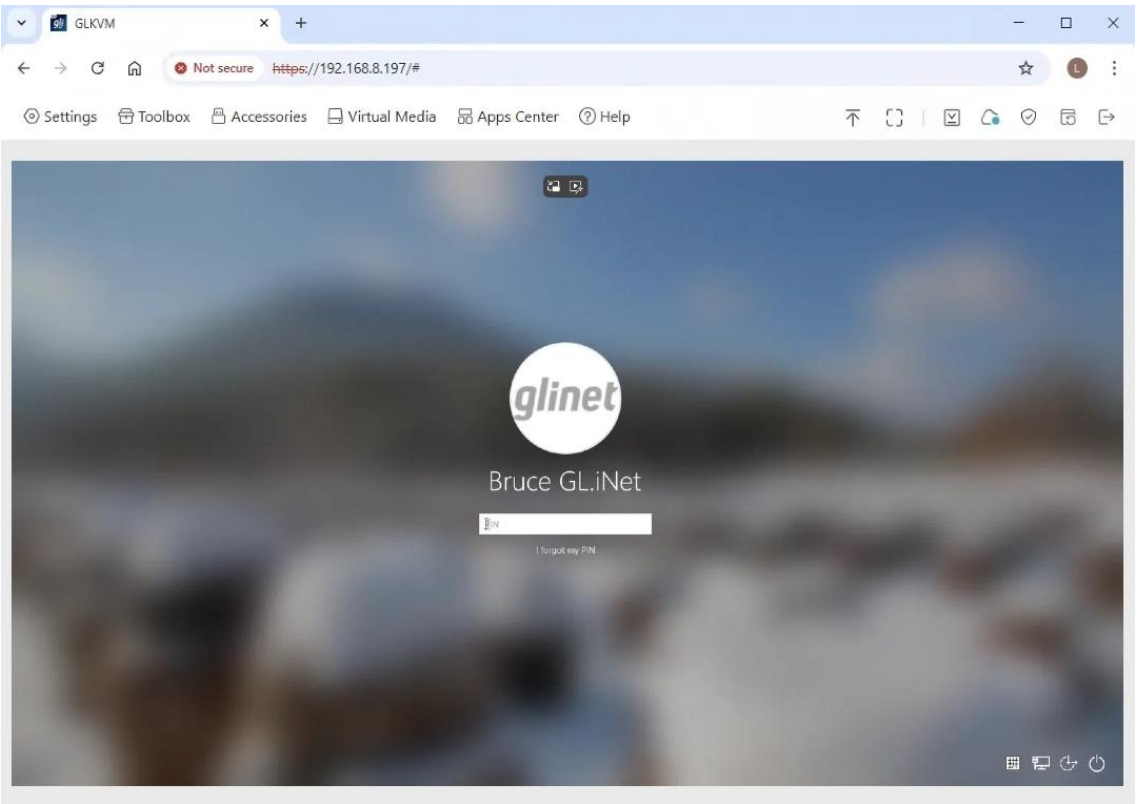
1. Ensure your controlling device is on the same LAN as Comet Q.
2. Connect Comet Q to a Wi-Fi network and find its IP address on the touchscreen. In this example, the Comet Q's IP address is *192.168.8.197*.
3. Launch a browser and enter this IP in the address bar..



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 Q's console locally and gain access to the controlled device.


GLKVM
Not secure
https://192.168.8.197/#
Settings
Toolbox
Accessories
Virtual Media
Apps Center
Help
glinet
Bruce GL.iNet
PIN
I forgot my PIN

Chapter 4

Remote Access

This chapter introduces multiple ways to access your KVM remotely.

4.1 Cloud Service

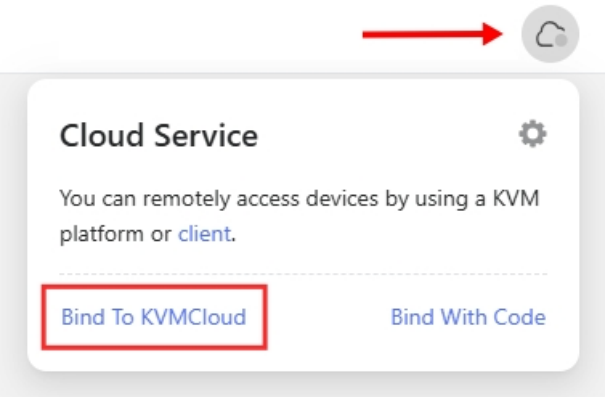
4.1.1 Bind Device

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

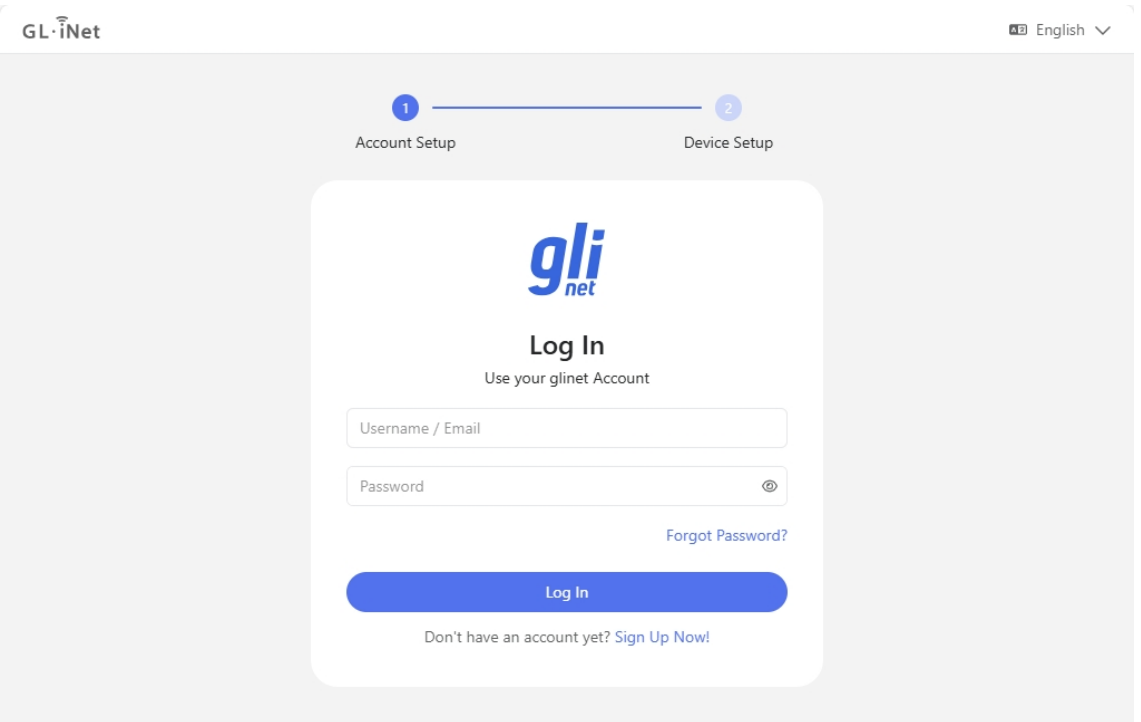
You can bind your KVM to the Cloud via regular steps or via dynamic code.

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

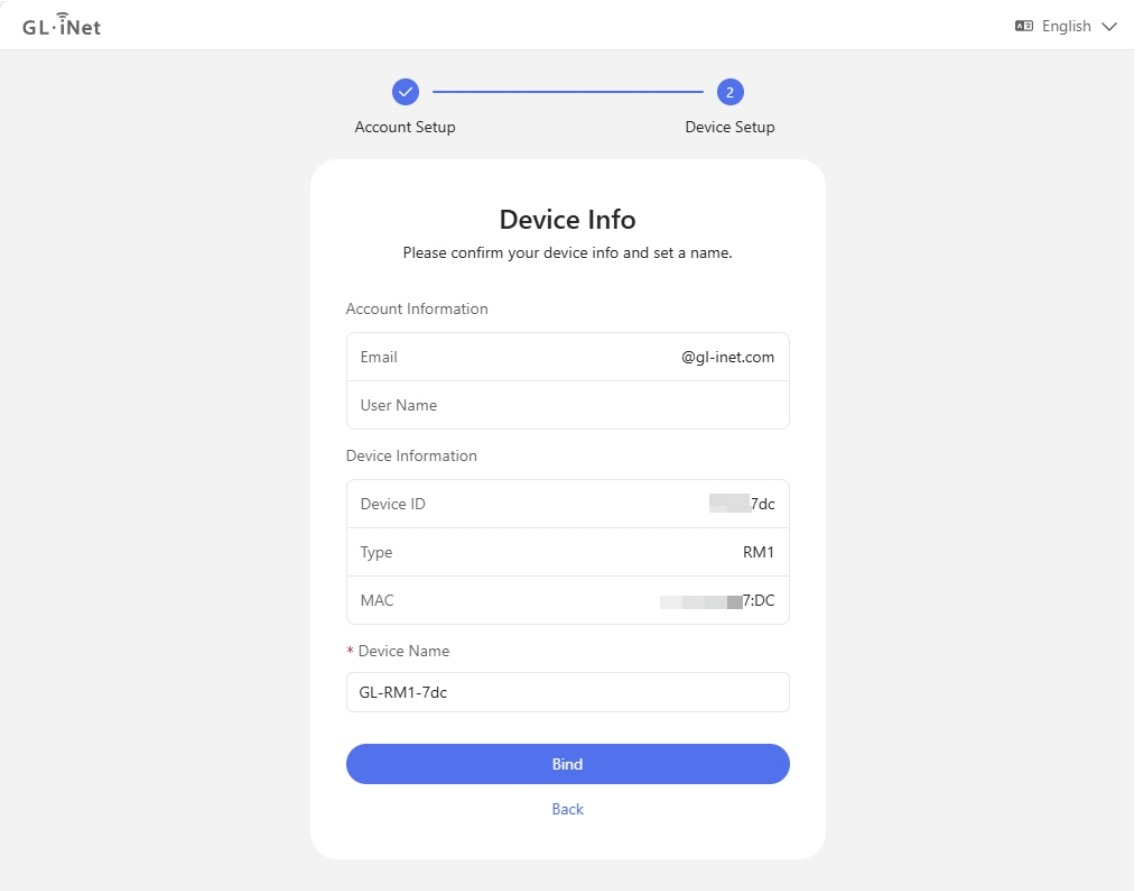
1. Log in to your KVM console locally and navigate to **Cloud Service** in the upper right corner. Click **Bind To Cloud**.



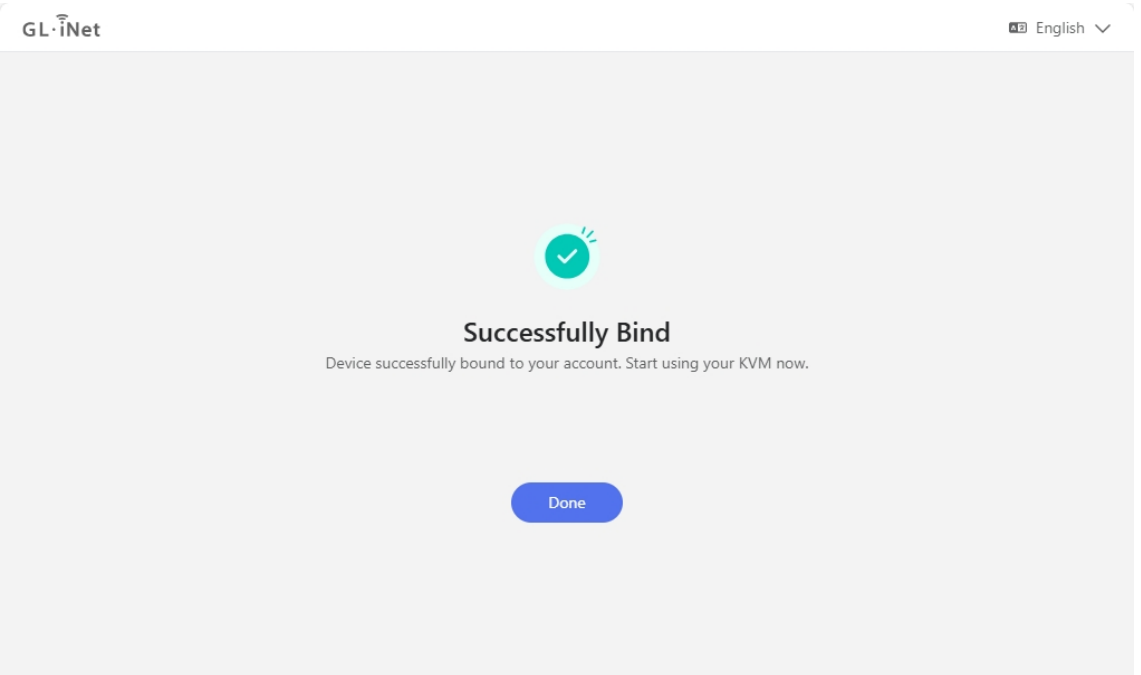
2. You will be redirected to a login page. Log in with your glinet cloud account.



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

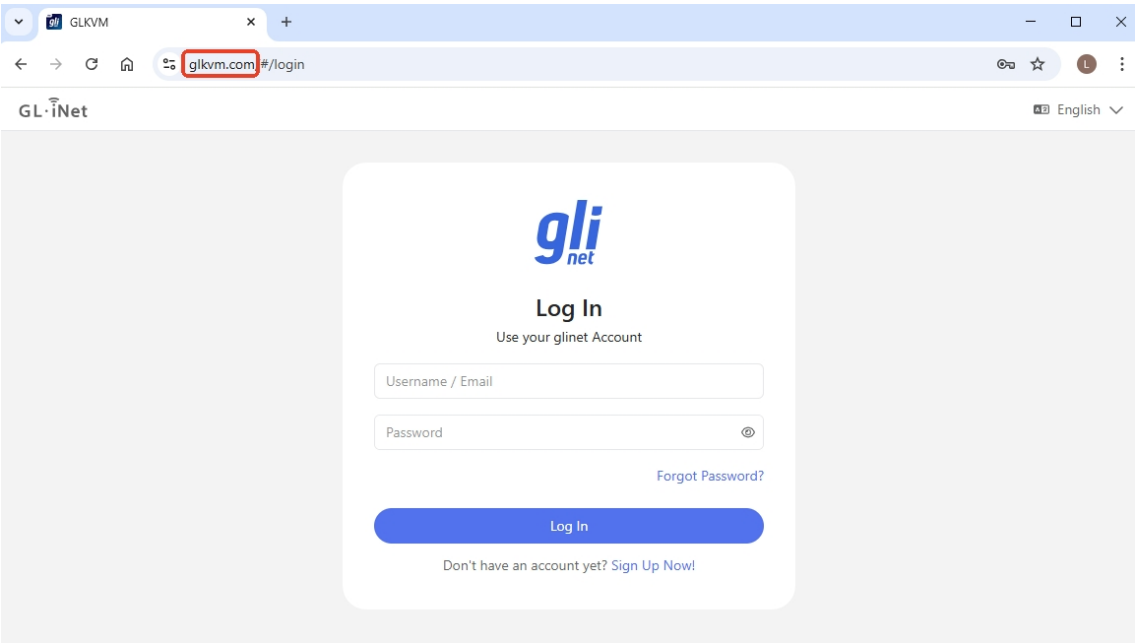


4. Wait a second and your device will be bound to your account successfully.

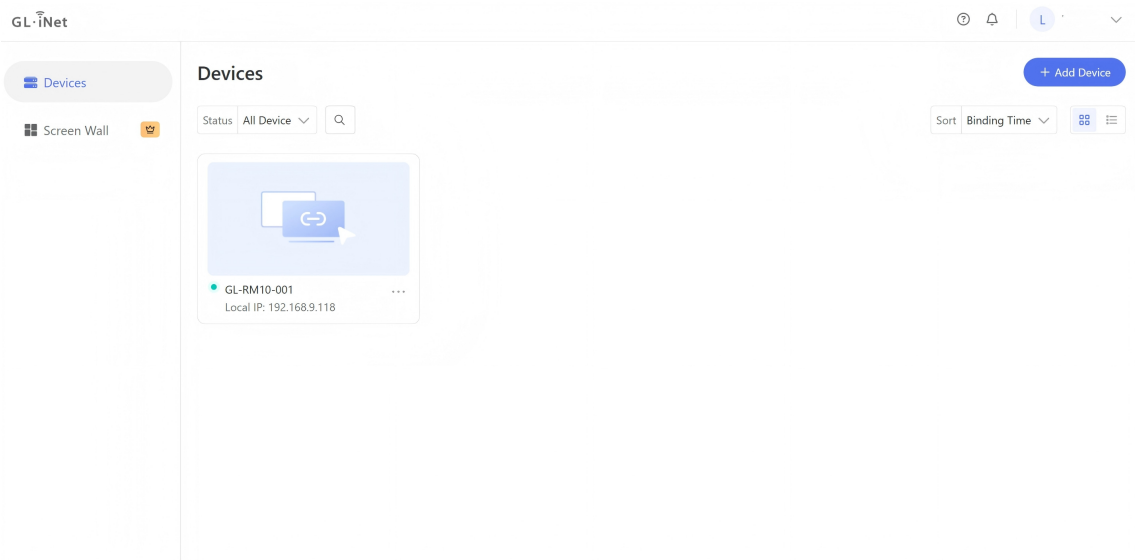


4.1.2 Remote Access via Cloud

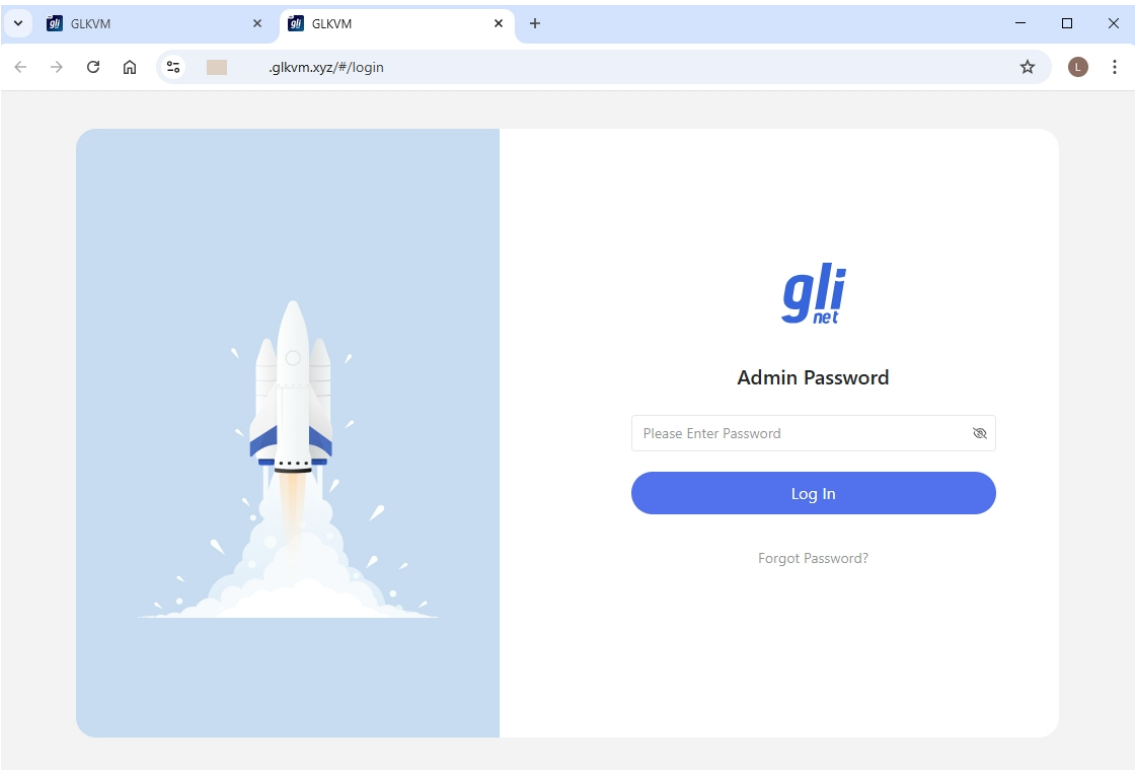
1. Open a browser (take Google Chrome as an example), and enter *glkvm.com* in the address bar. You will see a login page. Use your glinet account to log in.



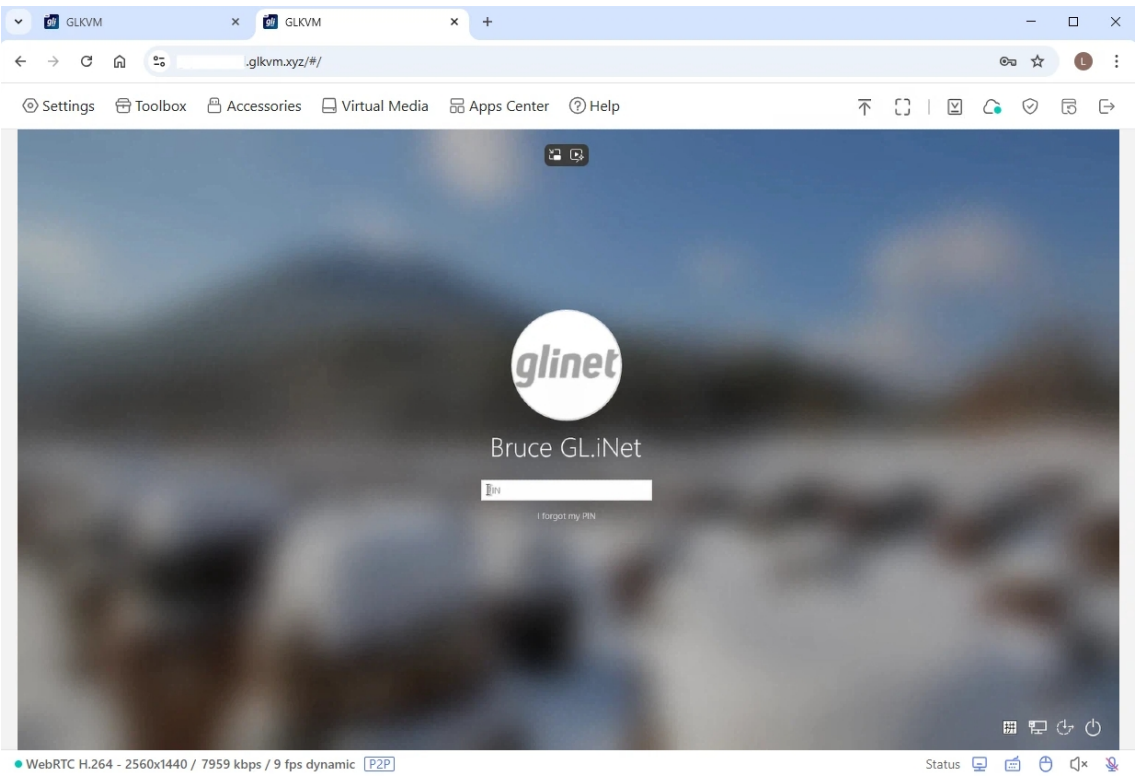
2. After login, you will see the devices bound to your account. Click on the device you want to remotely access.



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



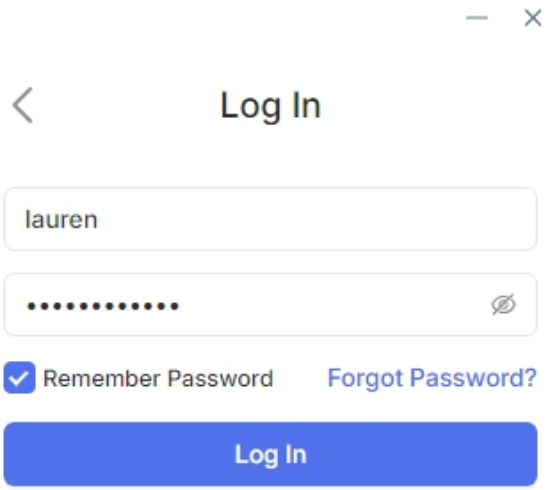
4. You will then be able to remotely access the KVM and the controlled device via Cloud, without installing the app.



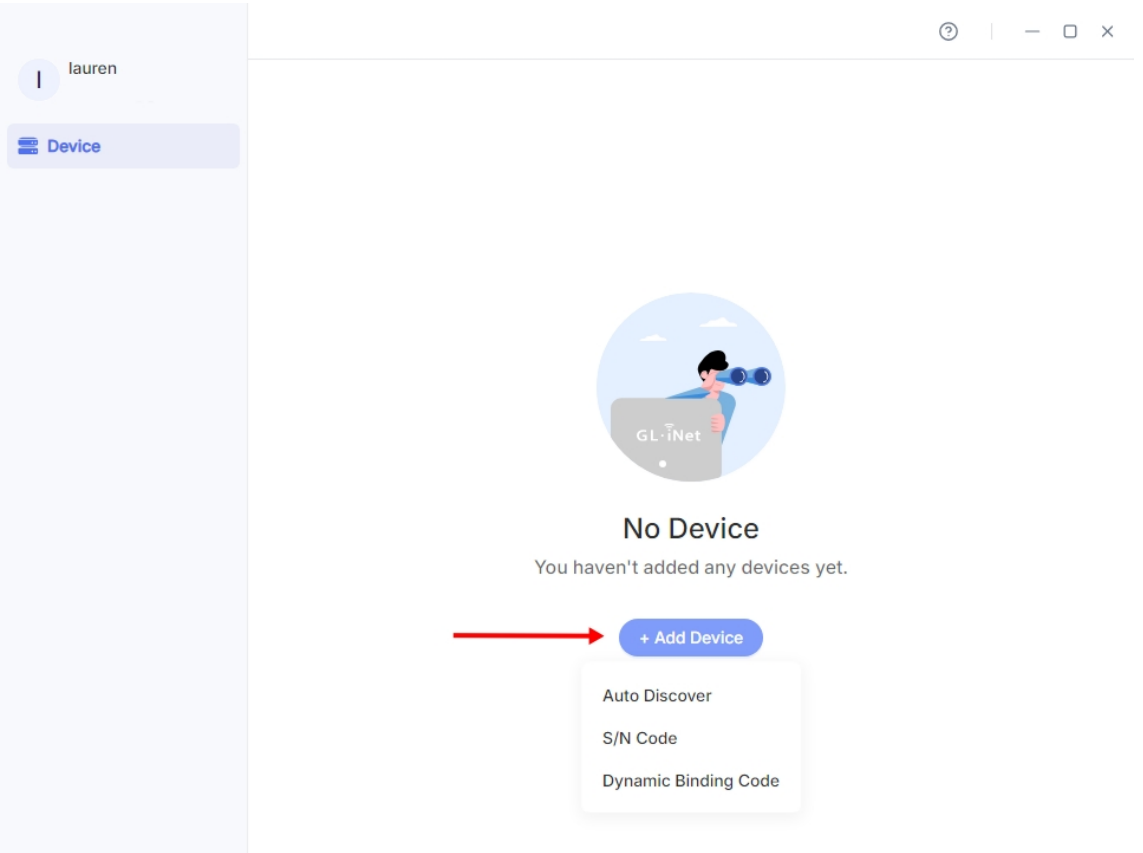
4.2 GLKVM App

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**.

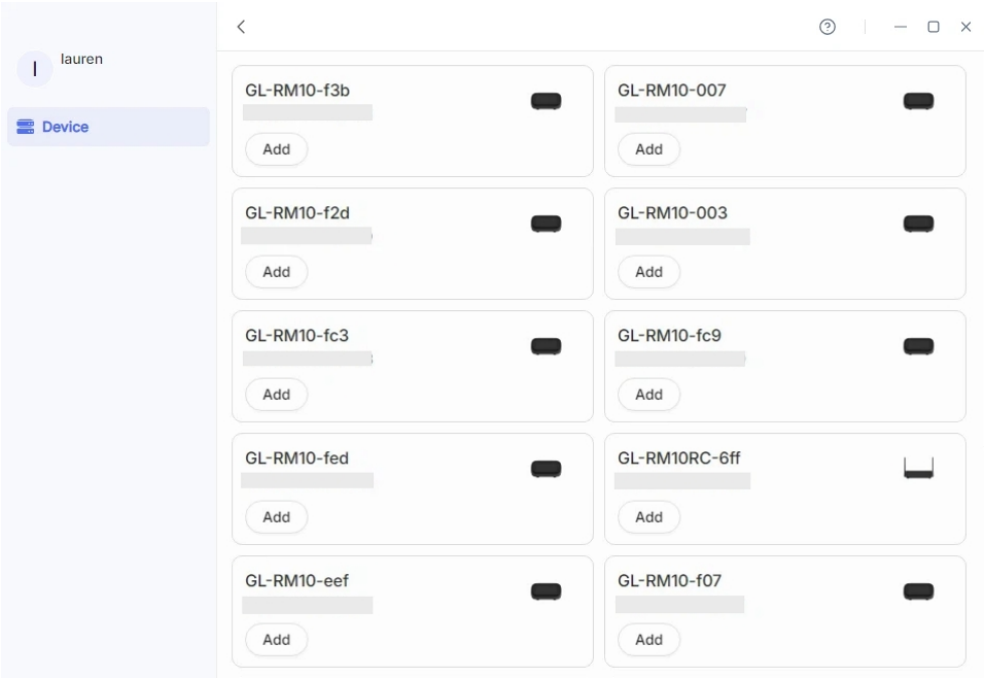


4. Bind your device in three ways: Auto Discover, S/N Code, and Dynamic Binding Code.

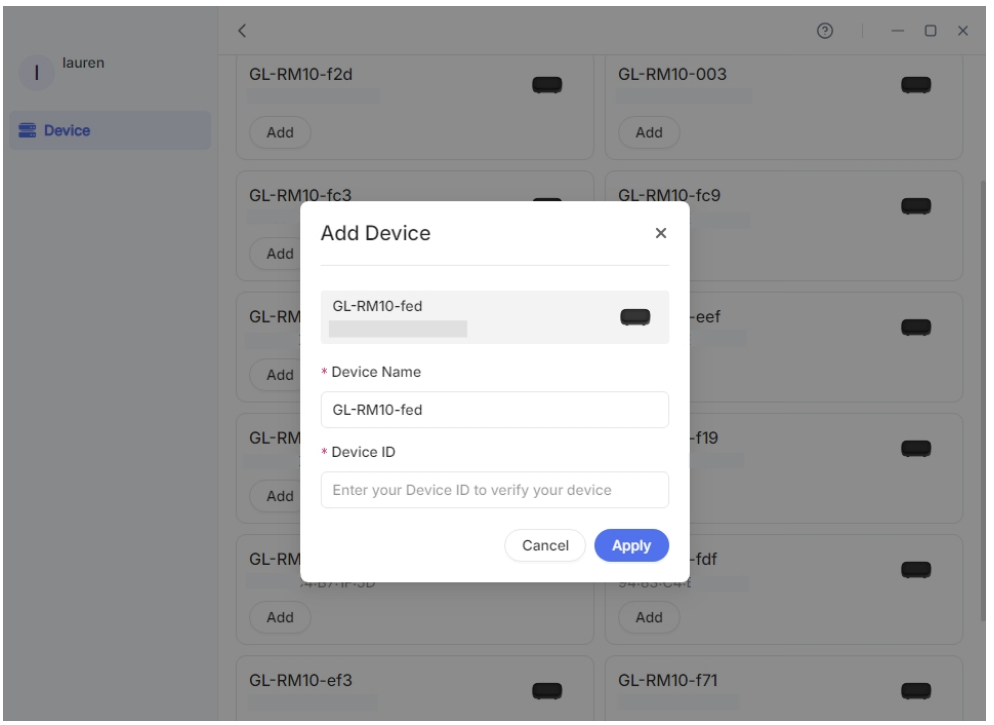
   (1) **Auto Discover**

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

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



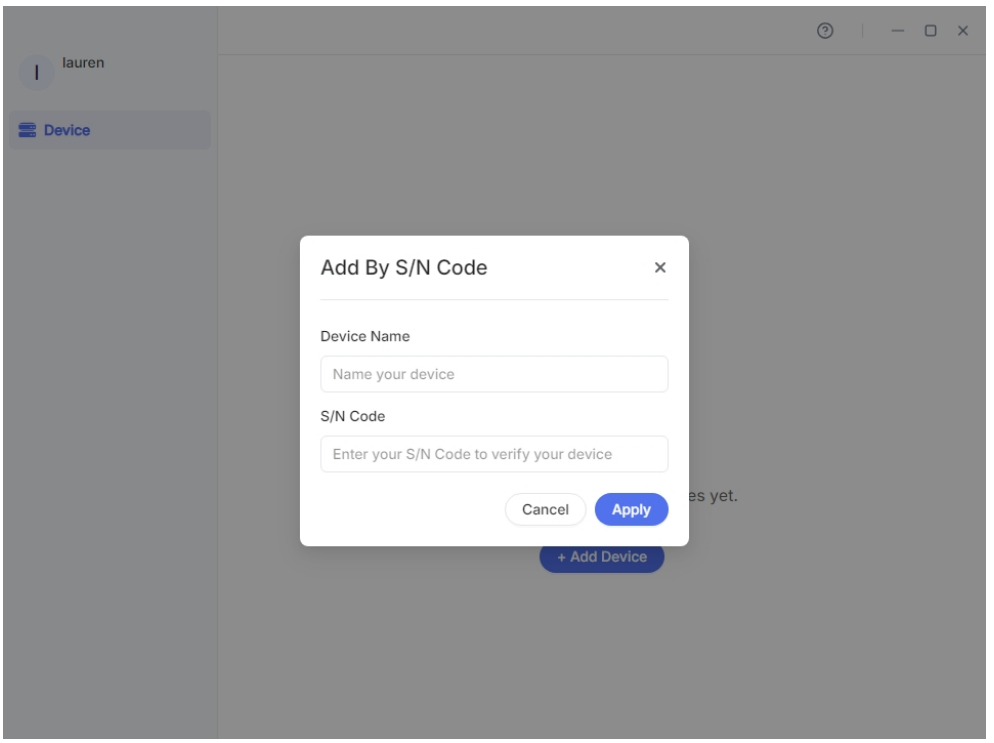
   Find your KVM and enter its **Device ID** to bind it to your account.



(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).

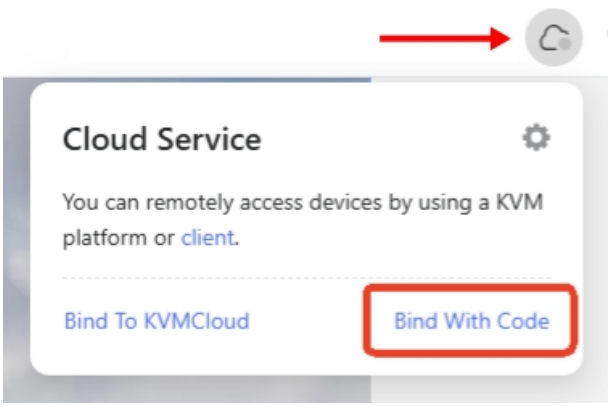
Click **S/N Code**. In the pop-up window, customize the device name and enter the S/N, which is printed on the label bottom of your KVM device.



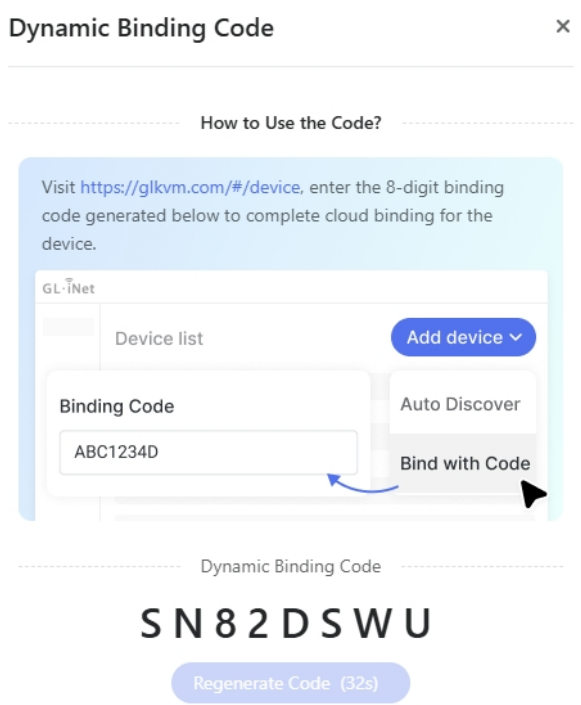
(3) **Dynamic Binding Code**

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

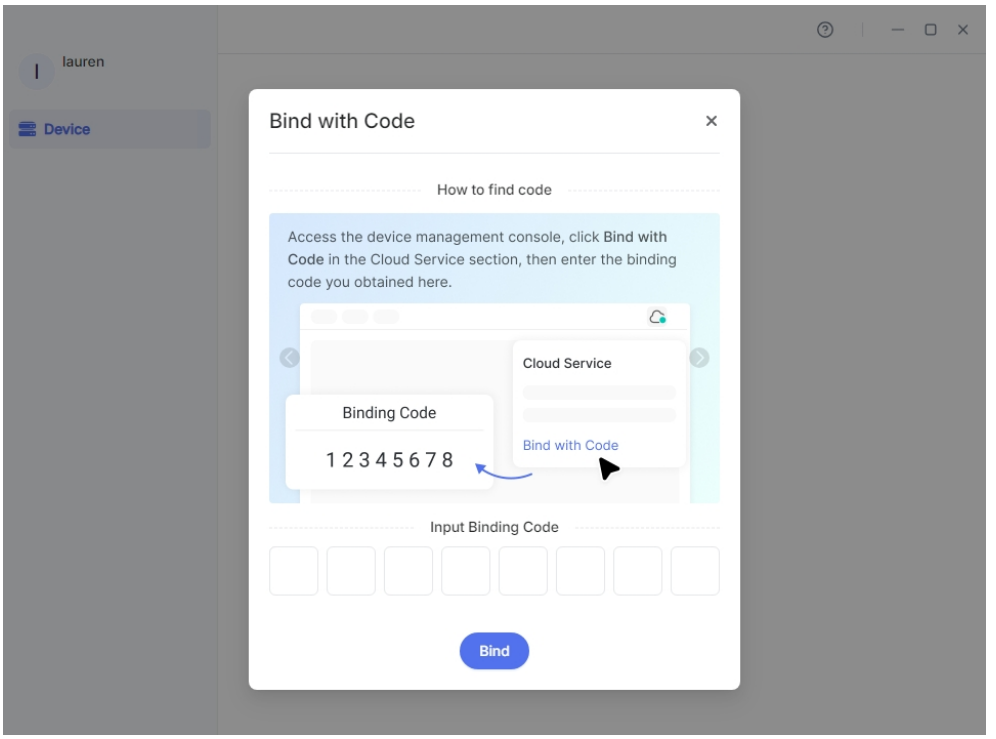
a. Log in to your KVM locally using domain or IP address, and navigate to **Cloud Service** in the upper-right corner. Click **Bind With Code**.



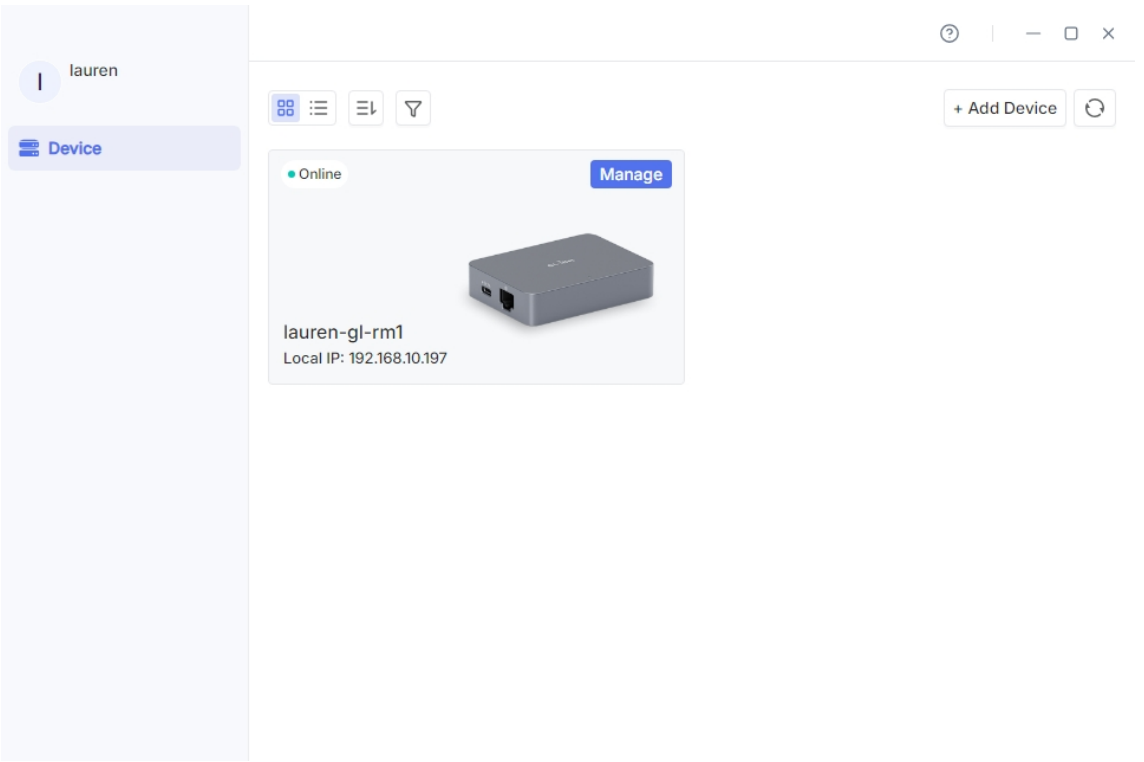
b. It will generate **an 8-digit dynamic code** randomly for device binding, valid for 60 seconds. Copy this code.



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

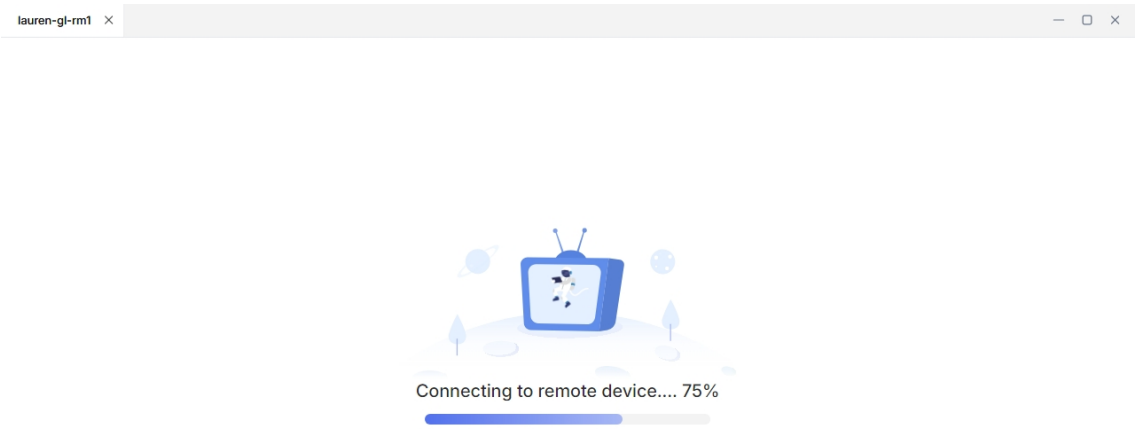


5. Once your KVM device is bound to your account, it will show "Online" in the app.

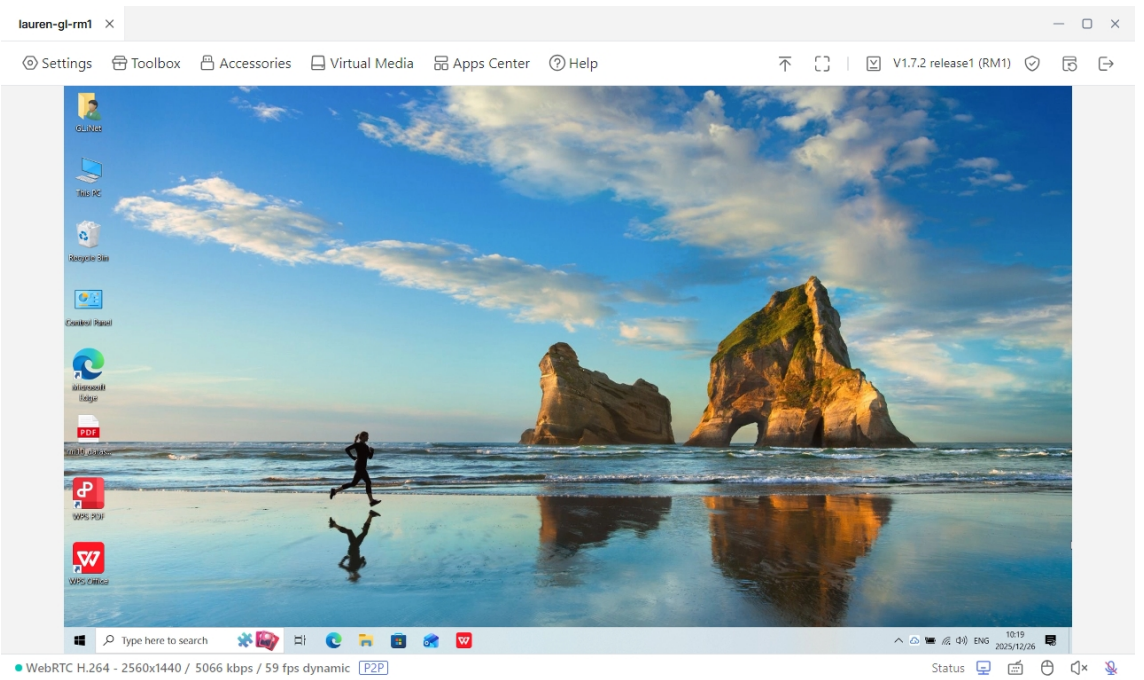

lauren
Device
+ Add Device
Online
Manage
lauren-gl-rm1
Local IP: 192.168.10.197

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.

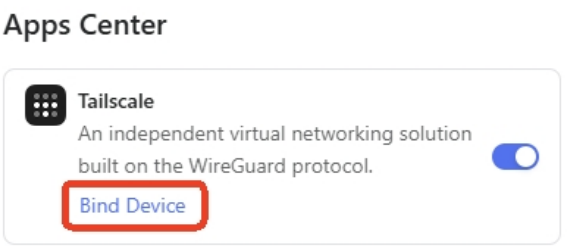


4.3 Tailscale

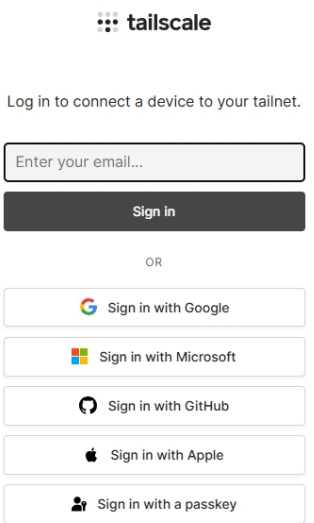
GL.iNet KVM integrates Tailscale®, allowing you to bind it to the Tailscale virtual network for remote access — no need to install the GLKVM app or use the cloud service. This is useful when your controlling device does not run Windows, macOS, Android, or iOS (and thus cannot install the GLKVM app),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

4.3.1 Bind KVM

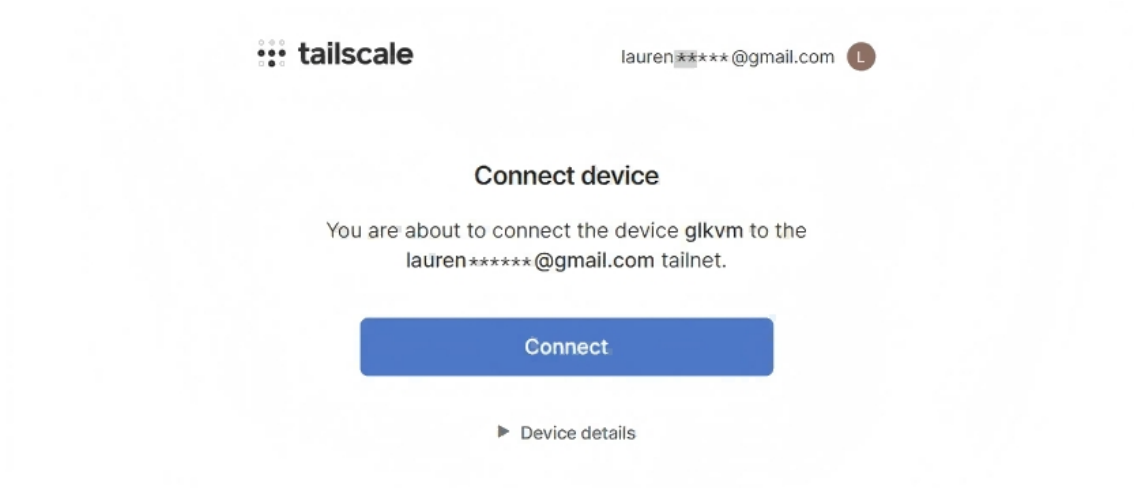
1. Connect your KVM and the controlling device to the same local network.
2. On the controlling device, log in to your KVM console locally via its domain or IP address, then go to **Apps Center** > **Tailscale**. Enable Tailscale and click **Bind Device**.



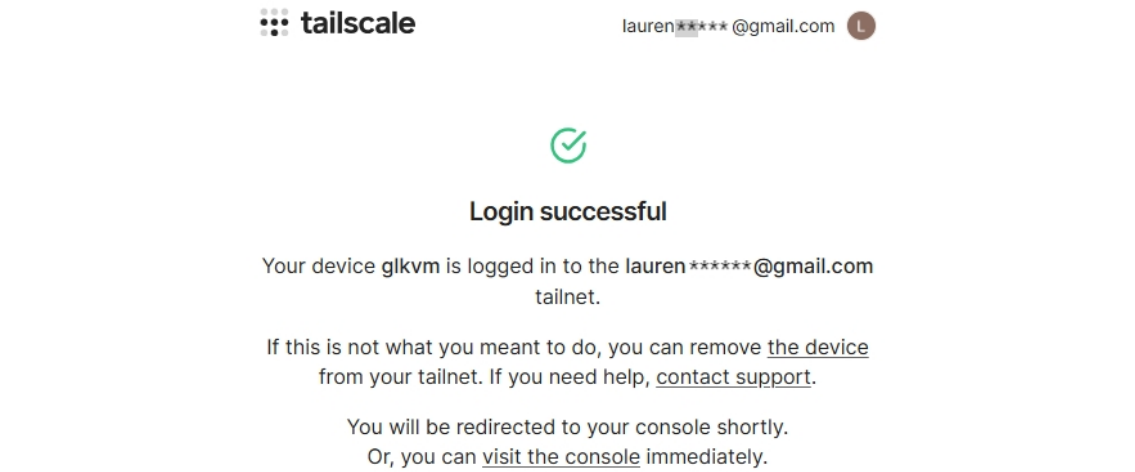
3. You will be directed to the Tailscale login page. Enter your email to log in.



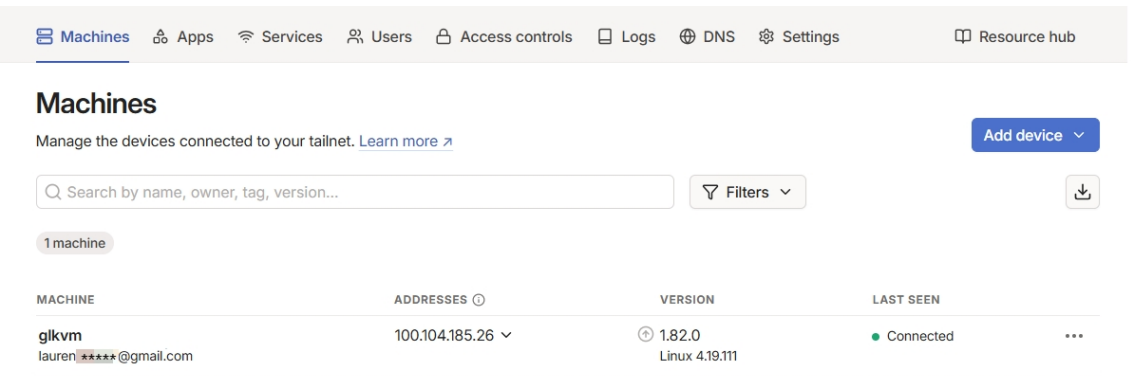
4. After logging in, the page prompts that you are about to connect the device glkvm to your Tailnet. Click **Connect**.



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



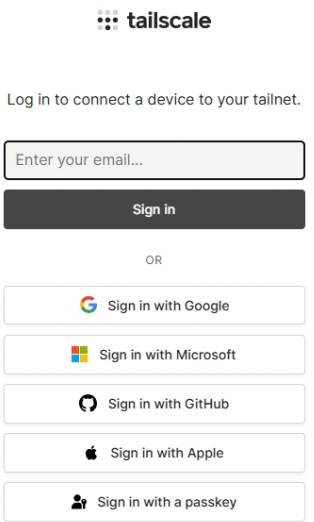
6. You will be redirected to your Tailscale console, where a device **glkvm** is displayed under **Machines**.



4.3.2 Bind Controlling Device

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

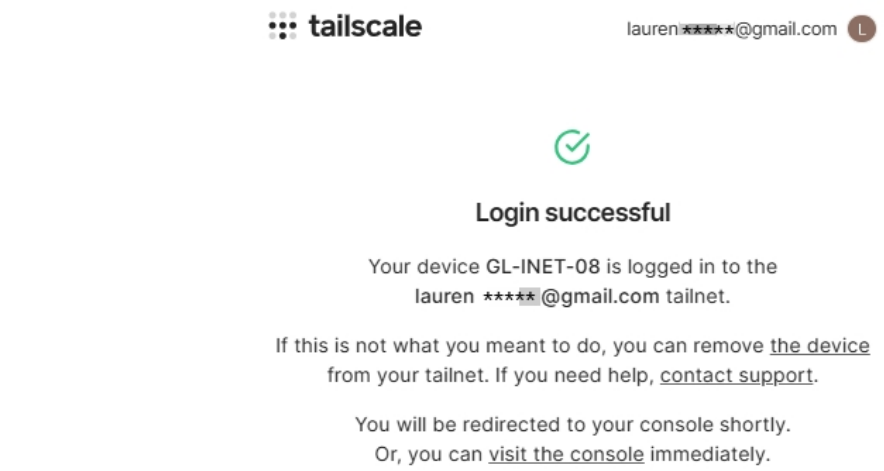
1. Install Tailscale on your laptop from here.
2. Run Tailscale on the laptop and log in with the same email.



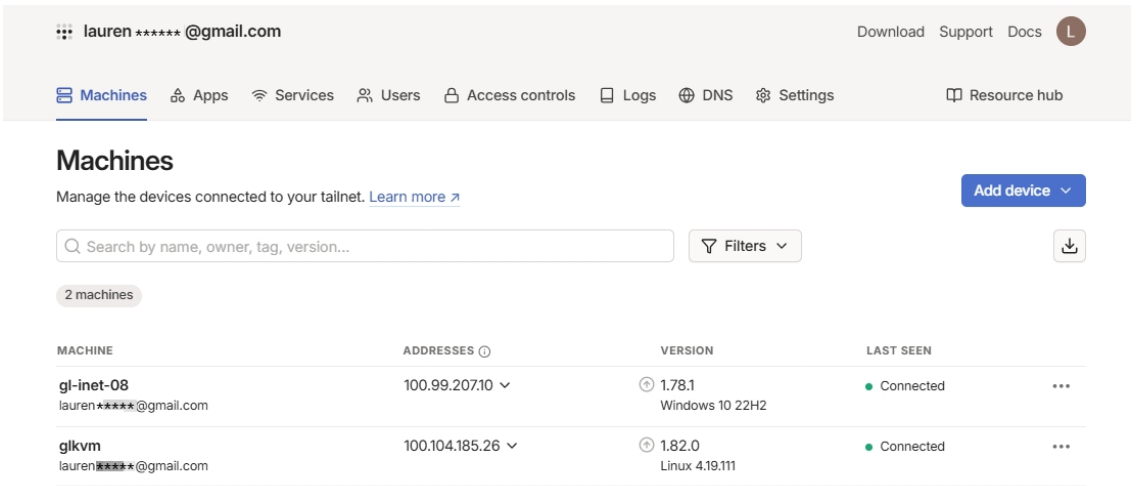
3. After logging in, the page prompts that you are about to connect the laptop (e.g. the controlling device) to your Tailnet. Click **Connect**.



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

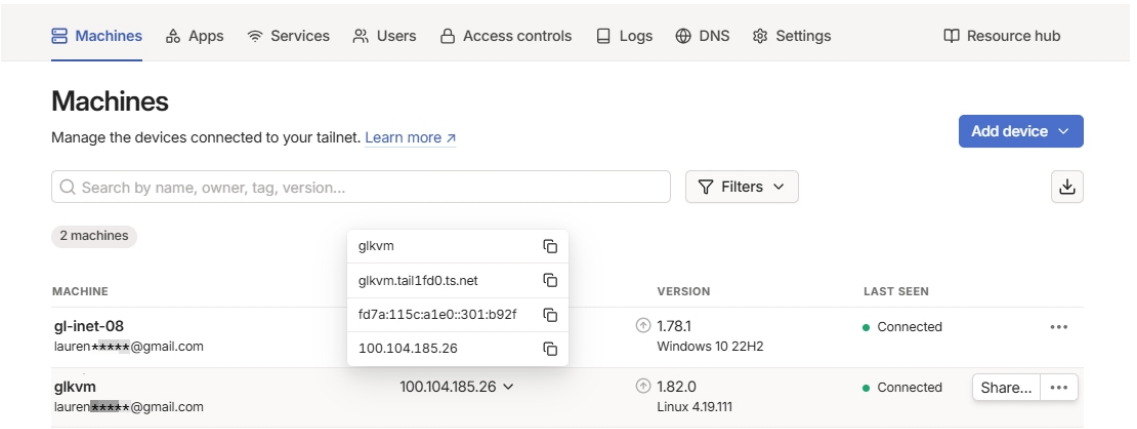


5. You will be redirected to your Tailscale console, where the controlling device is also displayed under **Machines**.

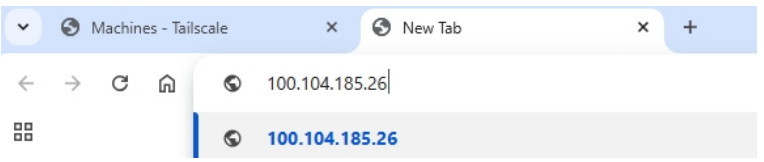


4.3.3 Remote Access via Tailscale

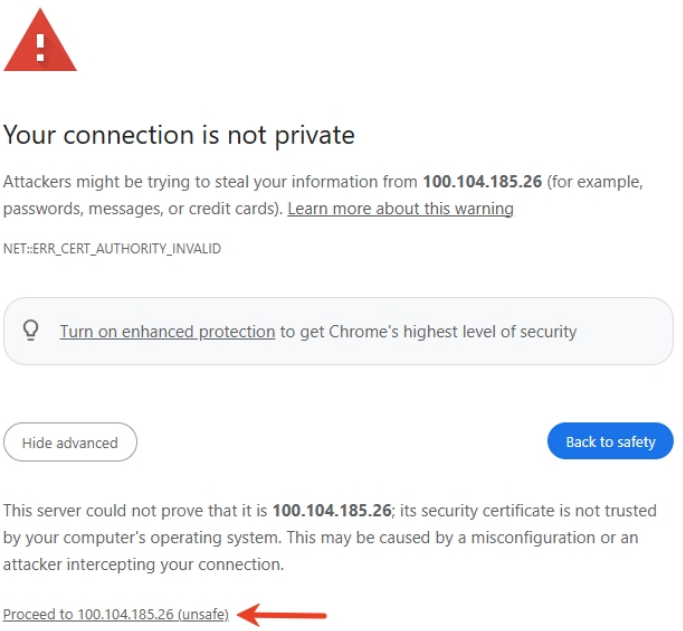
1. In the Tailscale console, click the **glkvm's Address** (100.104.185.26 in this example).



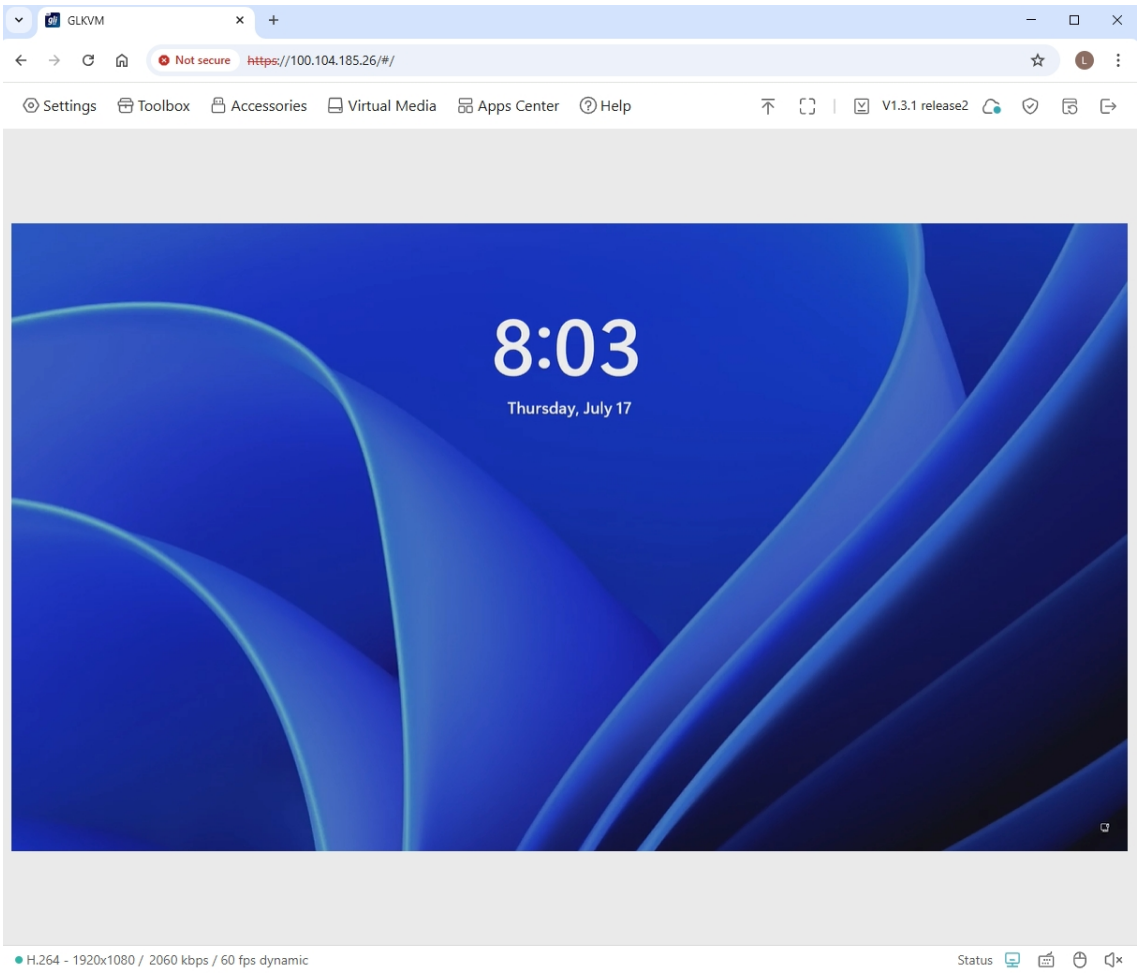
2. You will see four values, which are assigned by Tailscale for device identification and virtual network communication. You can remotely access your KVM using any of them.
3. Take the virtual IPv4 as an example. Copy the virtual IPv4 address of your KVM device, then open a new tab and enter the IP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

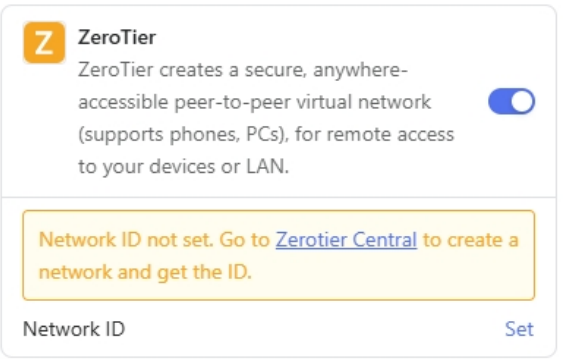


4.4 ZeroTier

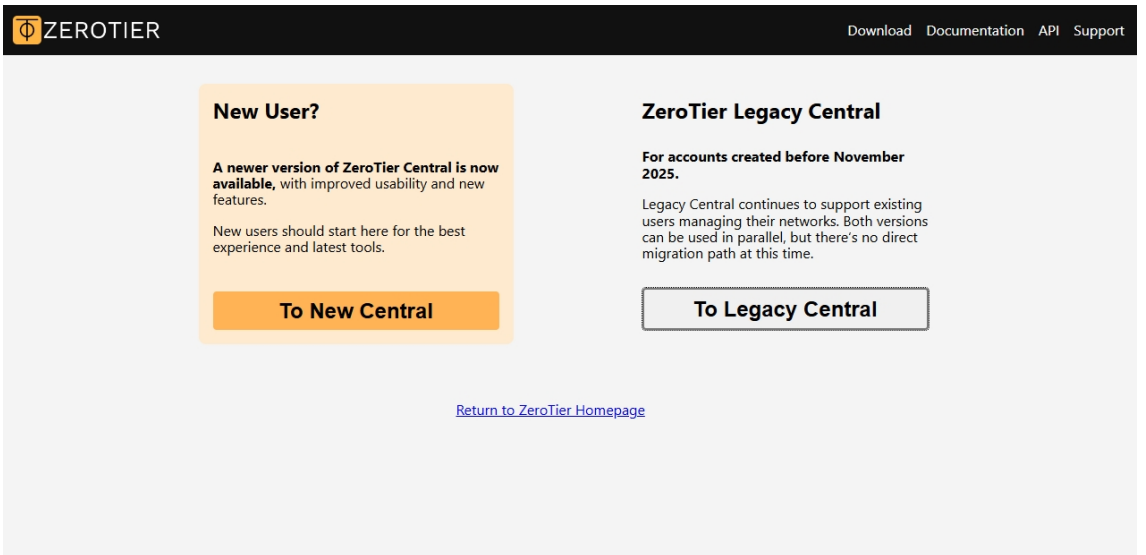
GL.iNet KVM integrates ZeroTier, allowing you to bind it to the ZeroTier network for remote access — no need to install the GLKVM app or use the cloud service.

4.4.1 Bind KVM

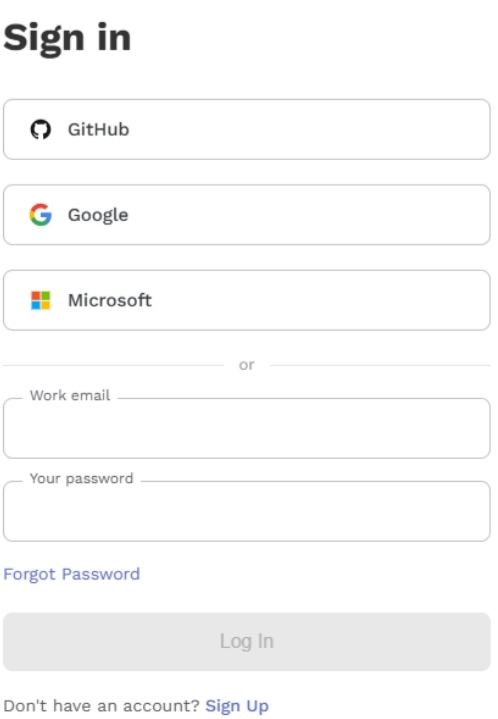
1. Connect your KVM and the controlling device to the same local network.
2. On the controlling device, log in to your KVM console locally via its domain or IP address, then go to **Apps Center** > **ZeroTier**. Enable ZeroTier, and you will see a yellow prompt as shown below. Click the hyperlink or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



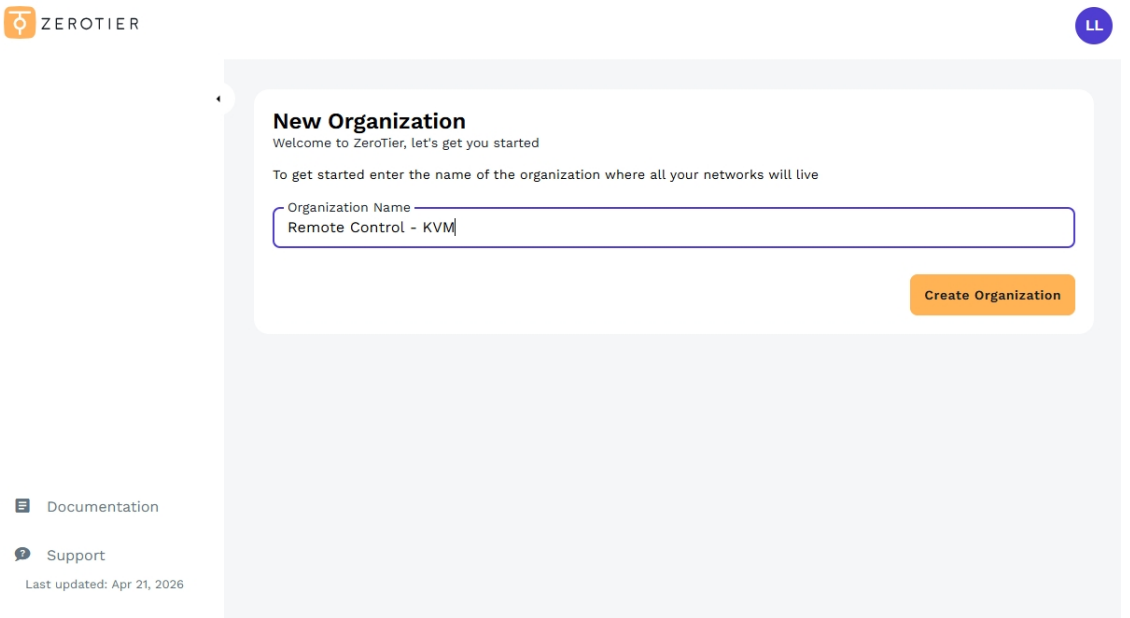
3. When signing in to ZeroTier for the first time, you may be asked to select between **New Central** and **Legacy Central**. Select the appropriate version to proceed.



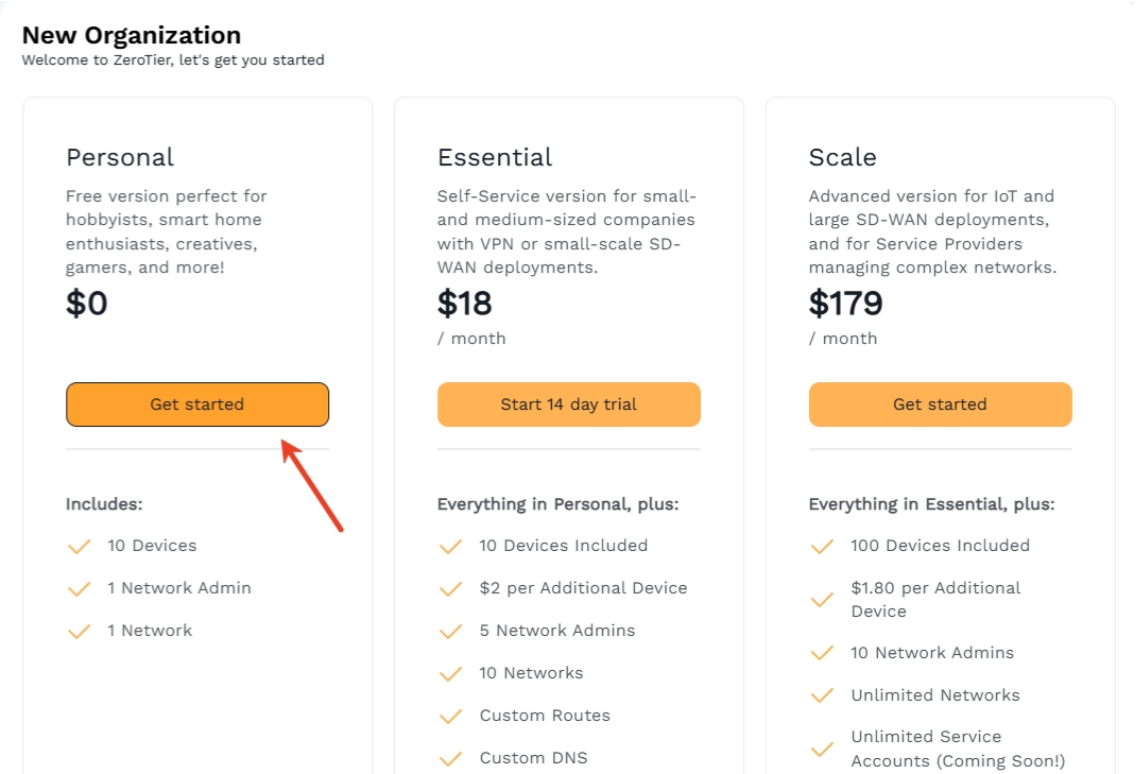
4. Take New Central as an example. Sign in with your email and password. If you don't have an account, sign up first.



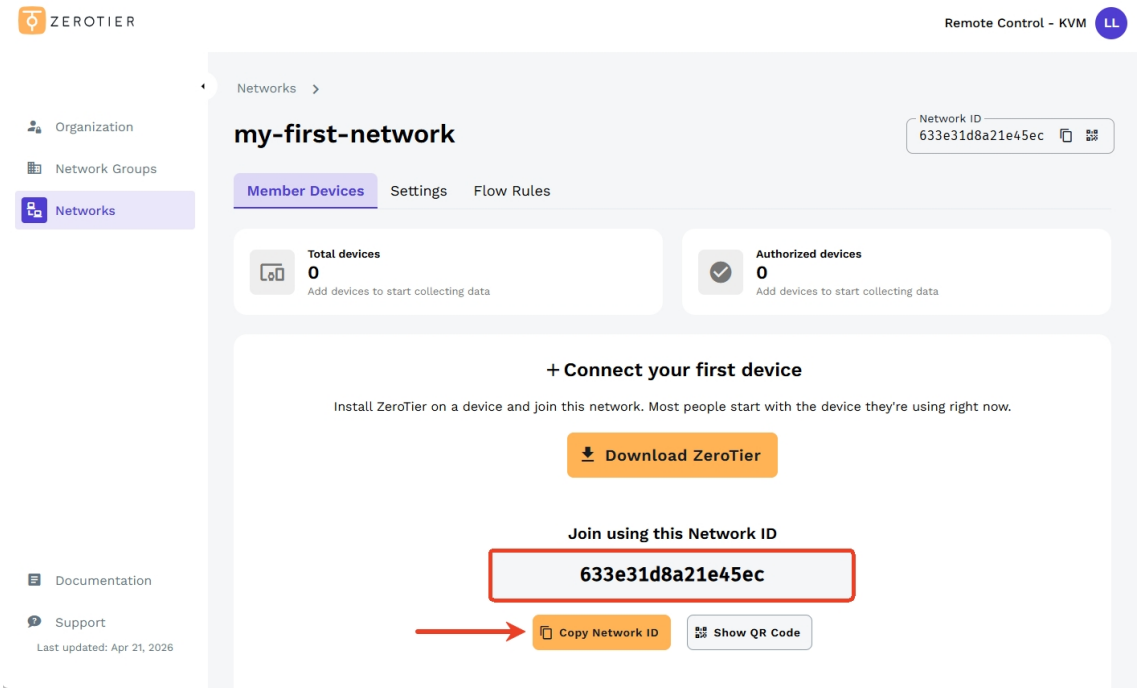
5. After signing in, create an organization.



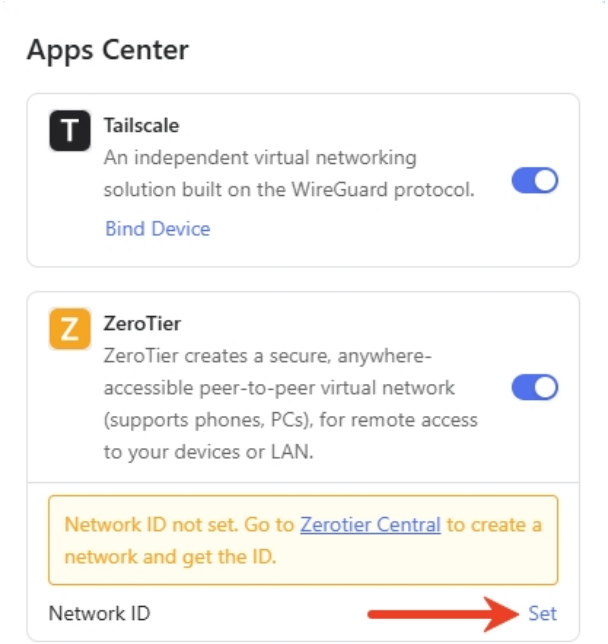
6. Select a plan. Here we choose **Personal plan** as an example, which includes 10 devices, 1 network admin, and 1 network. If you need to create more networks, add more devices, or add custom routes and DNS, choose **Essential** or **Scale plan**.



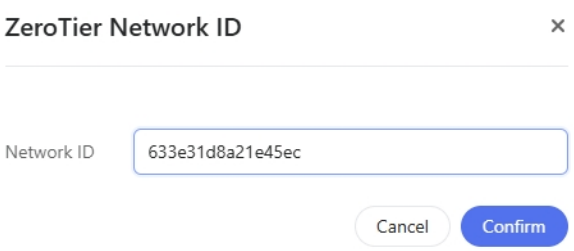
7. Now your ZeroTier network has been created. Copy the **Network ID**, which is **a 16-character alphanumeric string**. You will need it later when adding devices to your ZeroTier network. Keep this tab open.



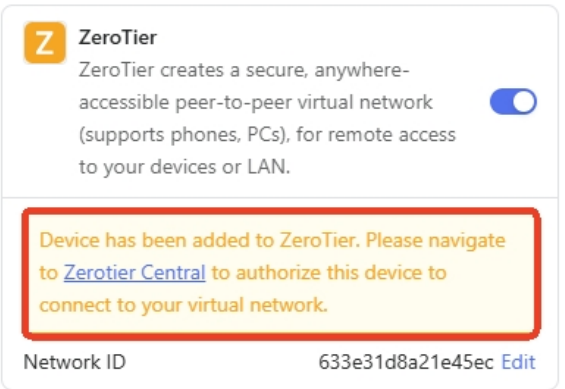
8. Go back to your KVM console and navigate to **Apps Center** > **ZeroTier**. Click **Set**.



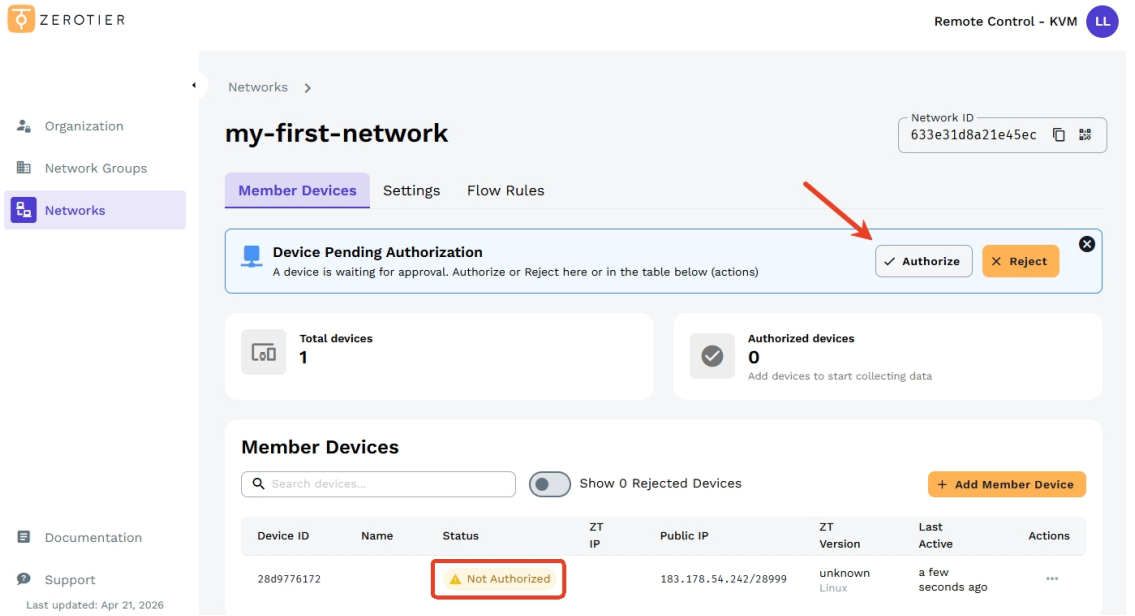
9. In the pop-up window, paste the **Network ID** and click **Confirm**.



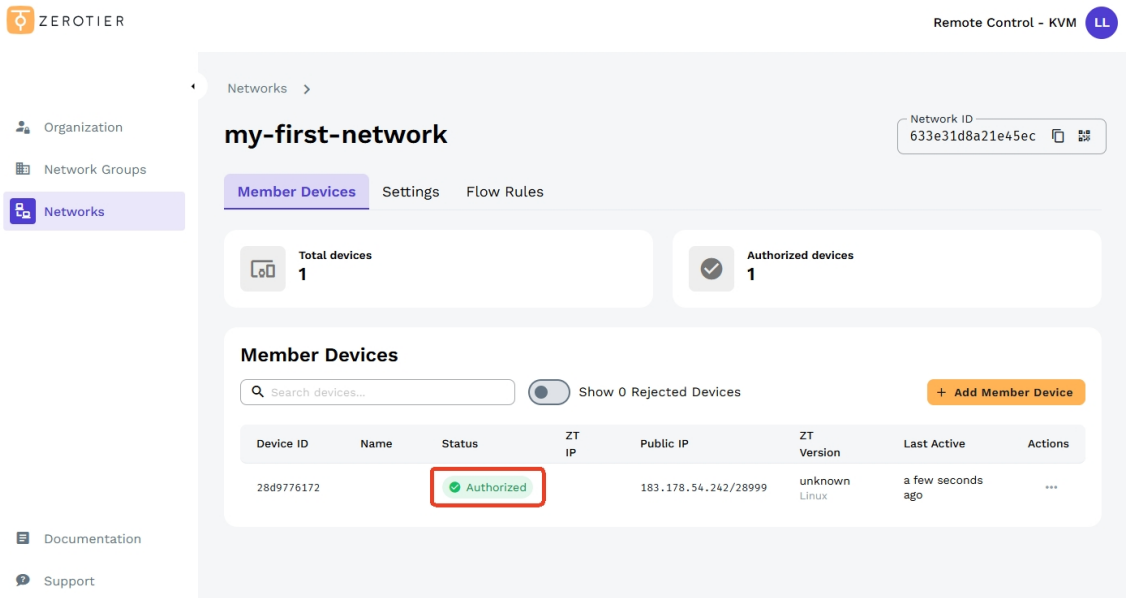
10. A prompt appears on the console, indicating that this device needs to be authorized.



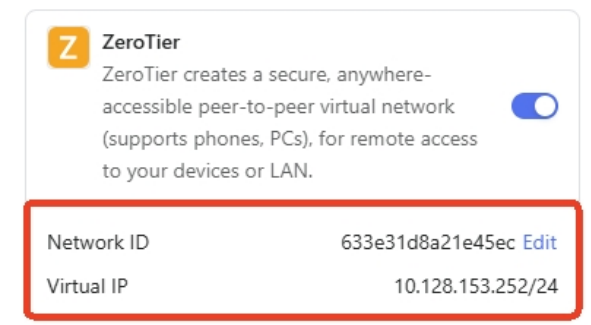
11. Go back to ZeroTier Central. You will see a device (your KVM) waiting for approval. Click **Authorize**.



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.



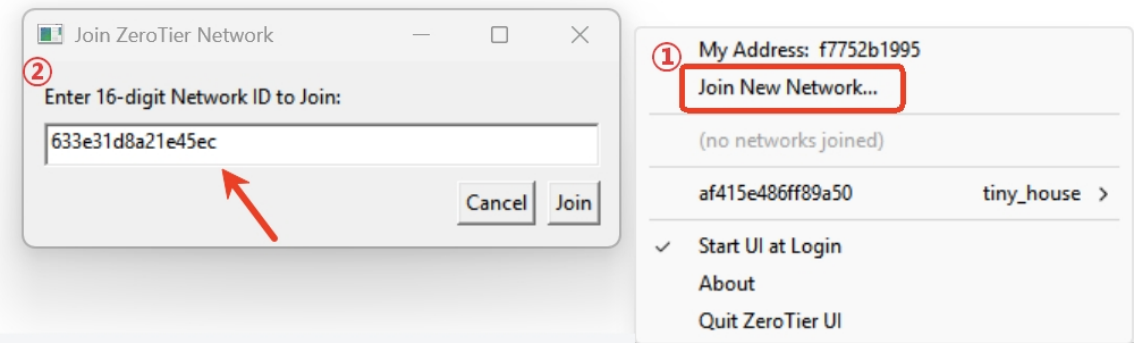
4.4.2 Bind Controlling Device

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

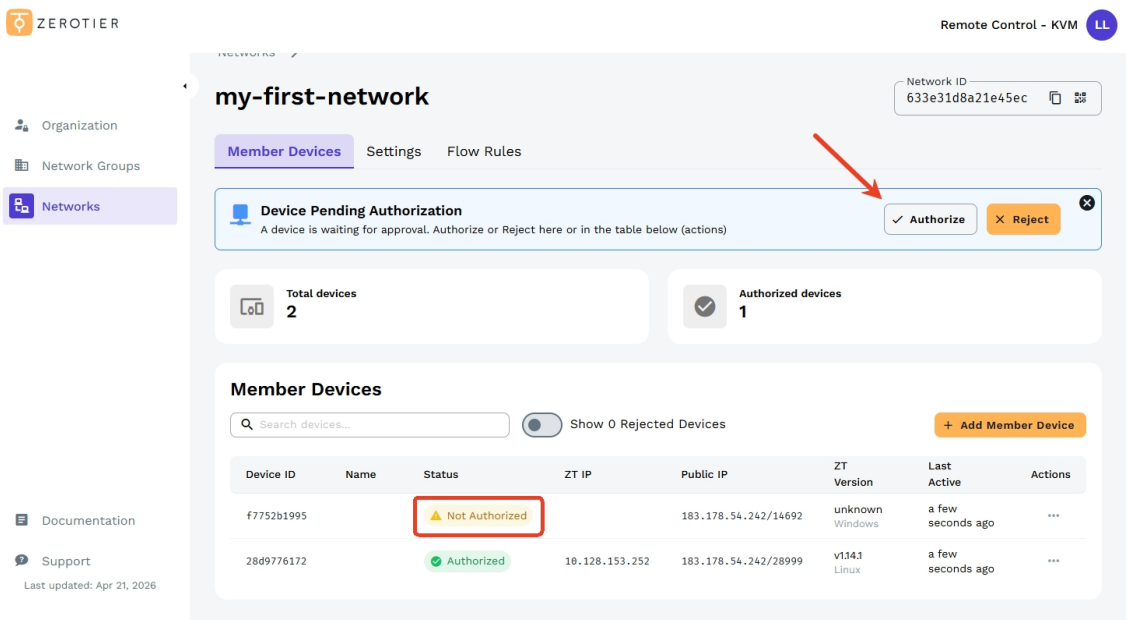
1. Install ZeroTier on your laptop from here.
2. Run ZeroTier on the laptop and add it to the same ZeroTier network.

   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.

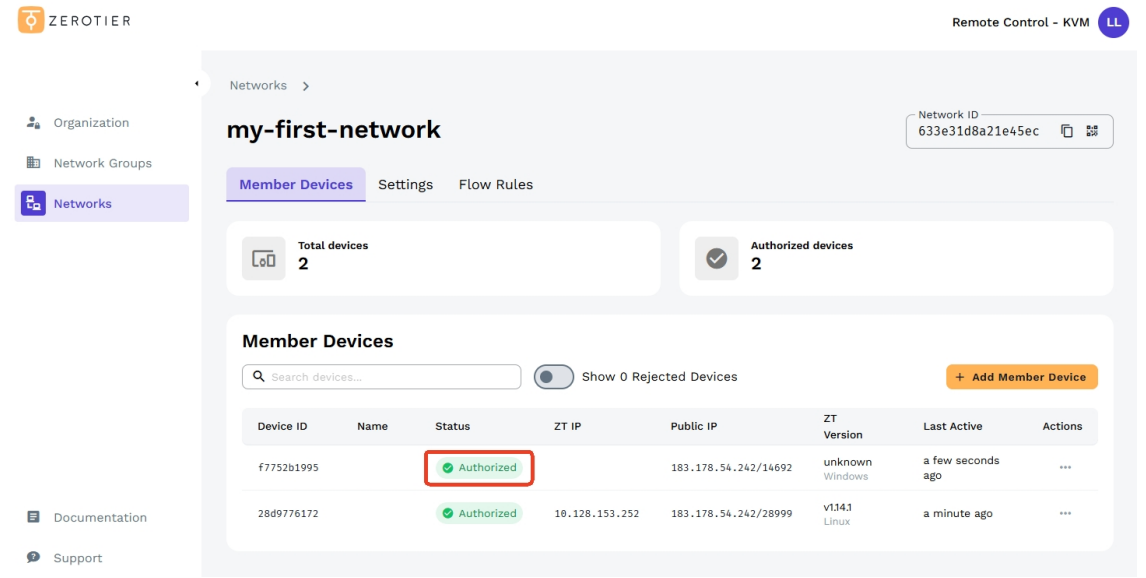
   Right click the ZeroTier icon, and click **Join New Network**. In the pop-up window, enter the same **Network ID** to add this PC to the same ZeroTier network.



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.

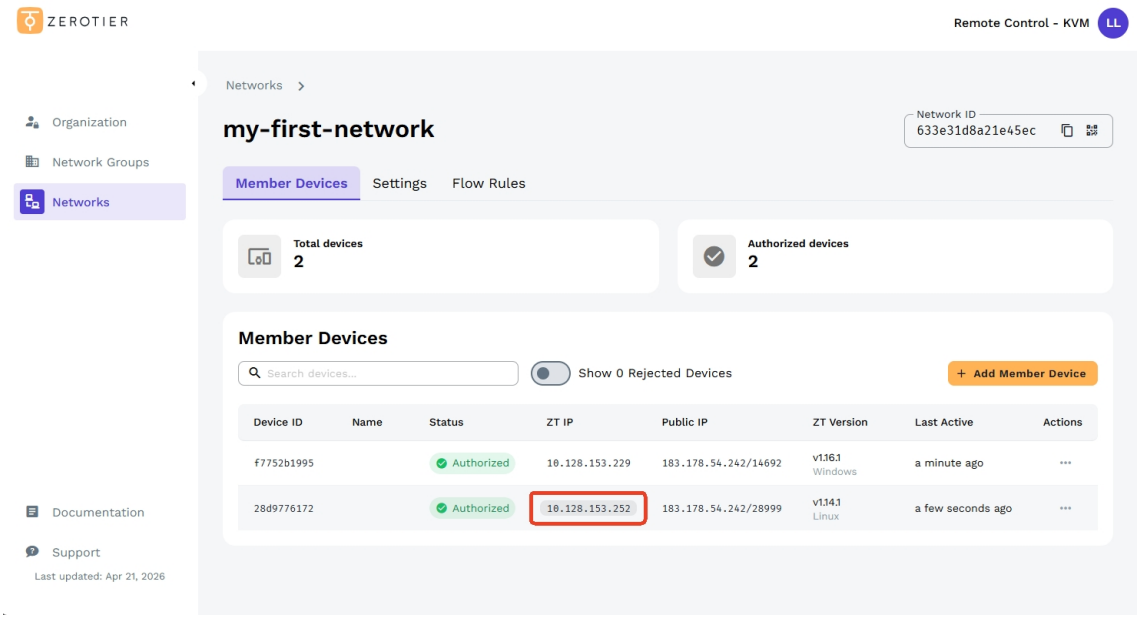


Now your KVM and the laptop are both added into the same ZeroTier network.

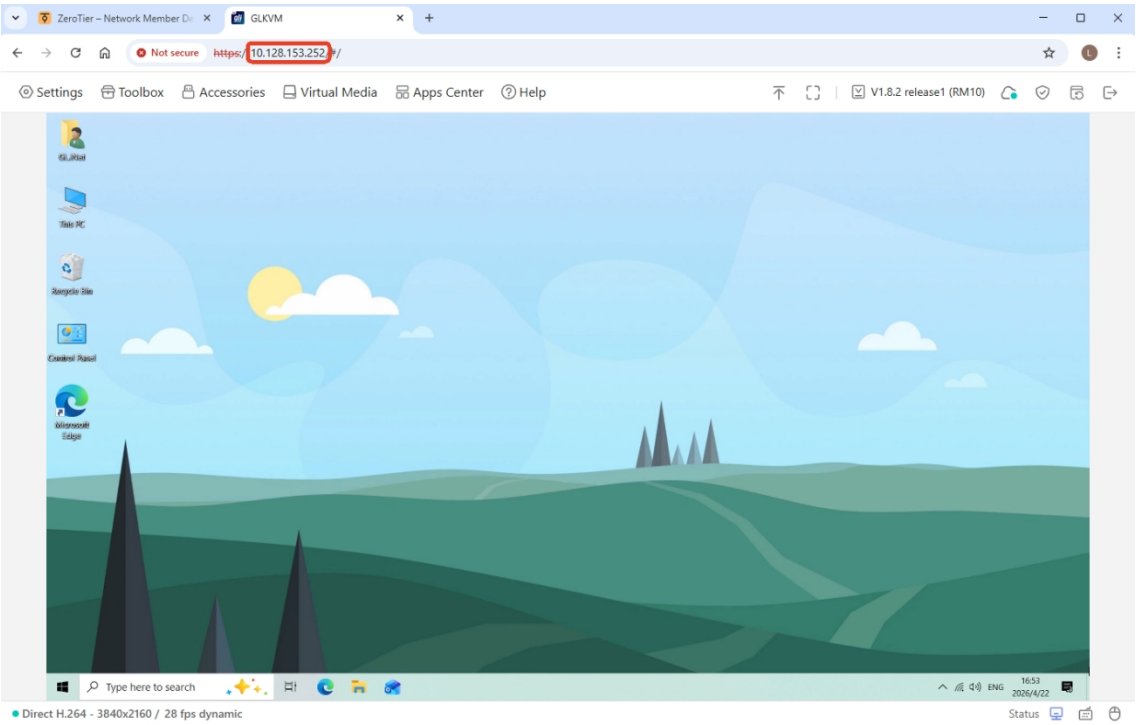
4.4.3 Remote Access via ZeroTier

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.



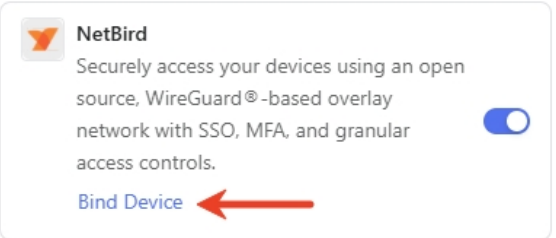
Tip: A privacy error may appear when accessing this ZeroTier IP for the first time. Simply click **Advanced** > **Proceed** to continue. See here for details.

4.5 NetBird

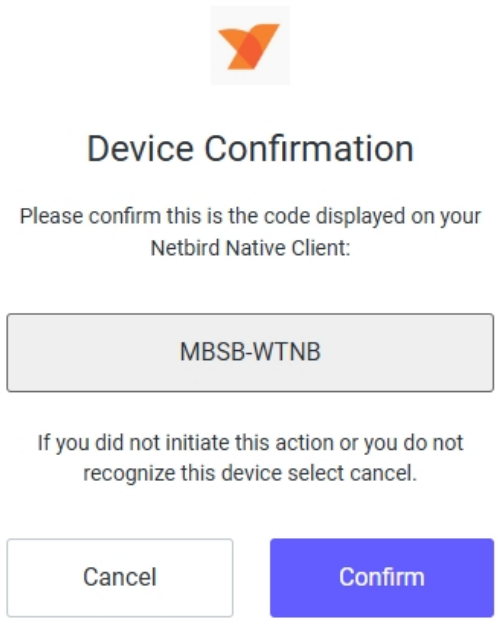
NetBird is an open-source zero trust networking platform that lets you build secure private networks for home and business use. As a WireGuard®-based overlay network, NetBird enables secure access to your devices anytime and anywhere. GL.iNet KVM integrates NetBird, allowing you to bind it to the NetBird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

4.5.1 Bind KVM

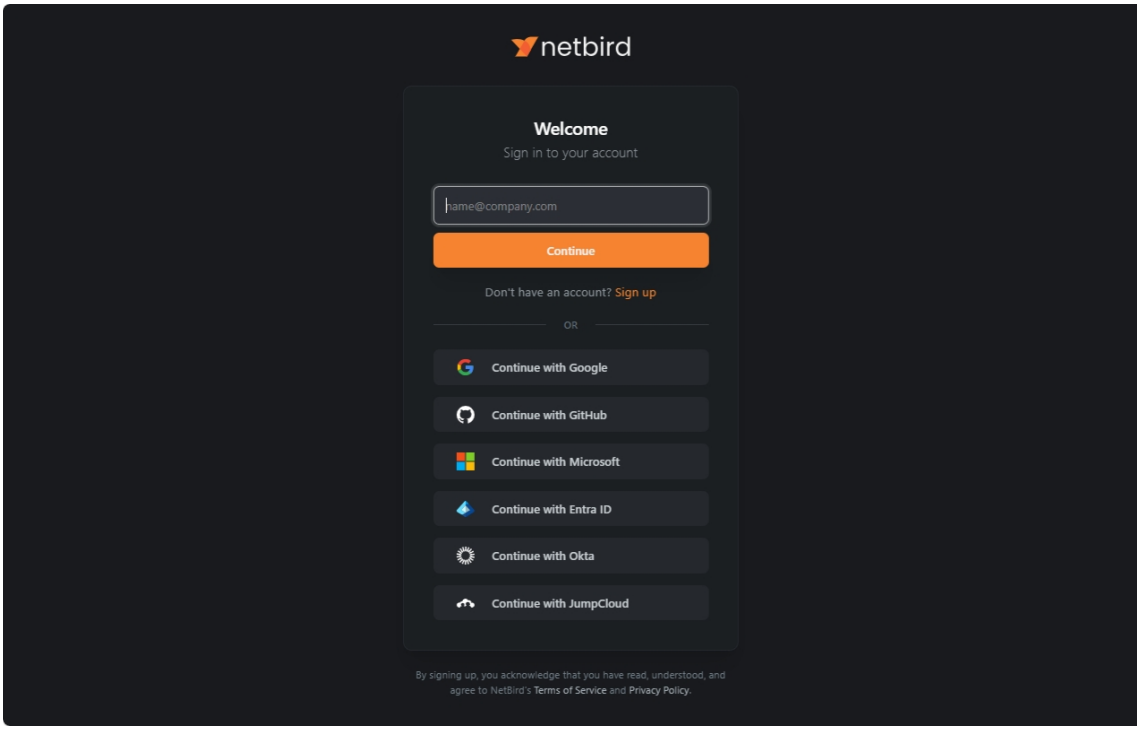
1. Connect your KVM and the controlling device to the same local network.
2. On the controlling device, log in to your KVM console locally via its domain or IP address, then go to **Apps Center** > **NetBird**. Enable NetBird and click **Bind Device**.



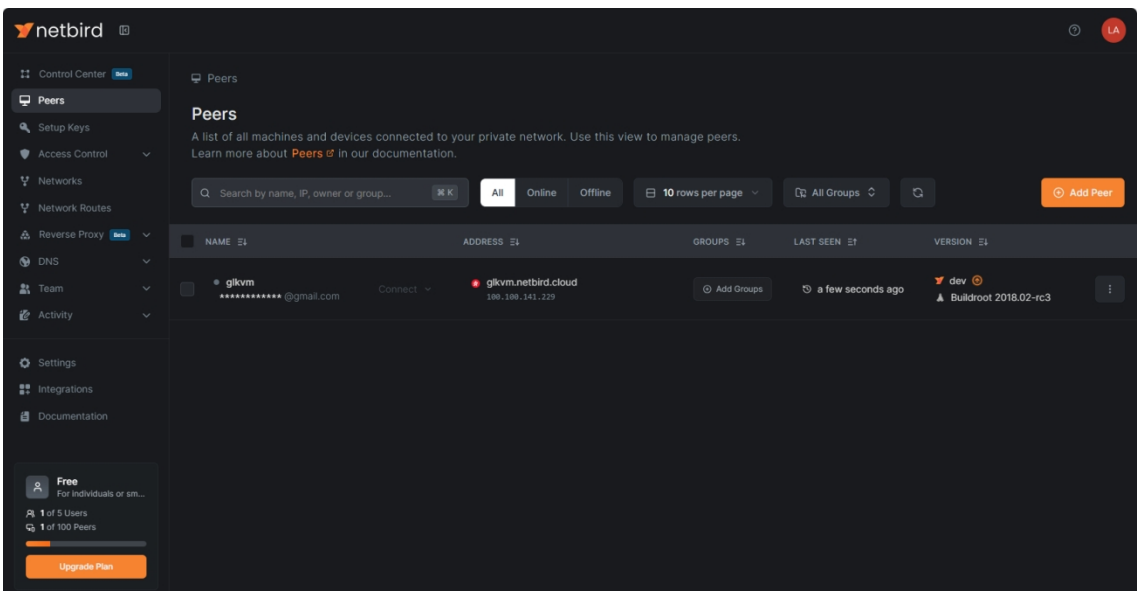
3. You will be redirected to the device confirmation page. Click **Confirm**.



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



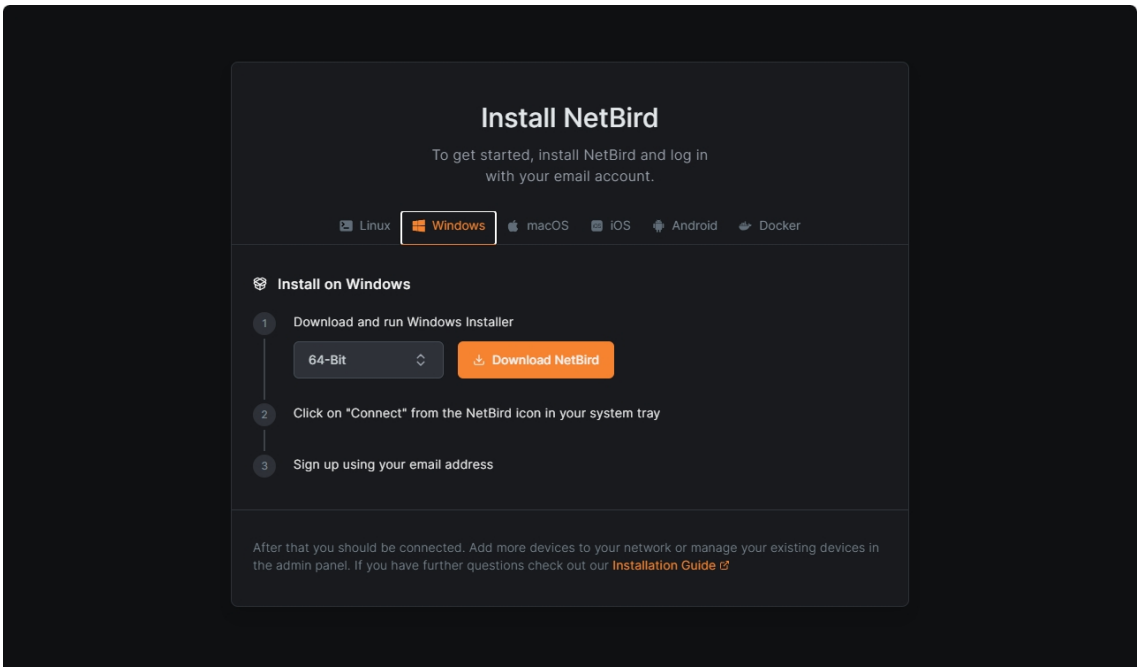
5. After signing in, the KVM device will be automatically bound to your account. On the NetBird dashboard, you will see your KVM listed on the **Peers** page.



4.5.2 Bind Controlling Device

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

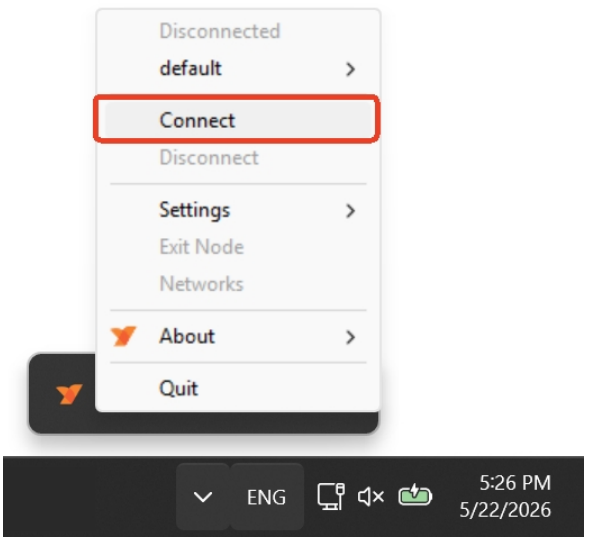
1. Install NetBird on your laptop from here.



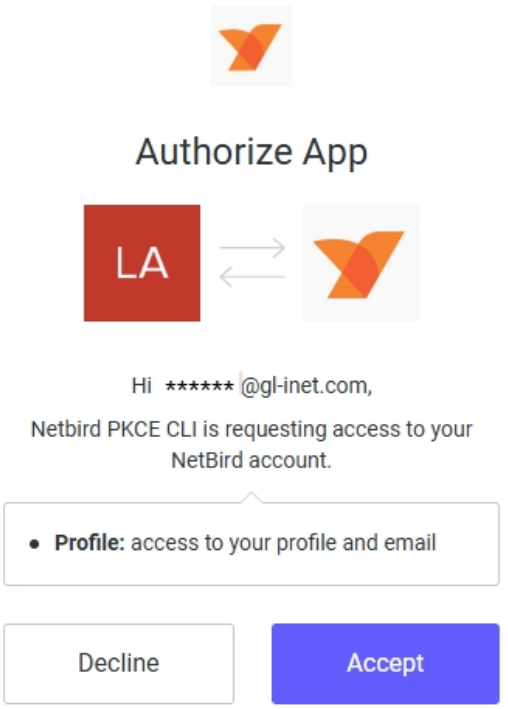
2. Run NetBird on the laptop and add it to the same NetBird network.

   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.

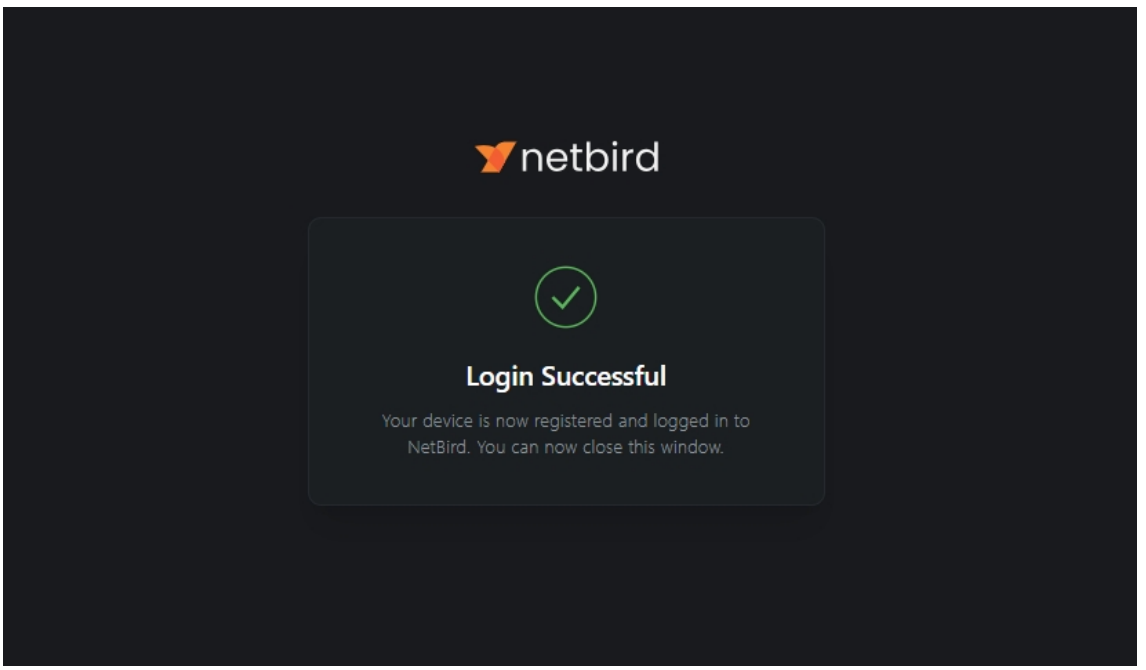
   Right click the NetBird icon, and click **Connect**.



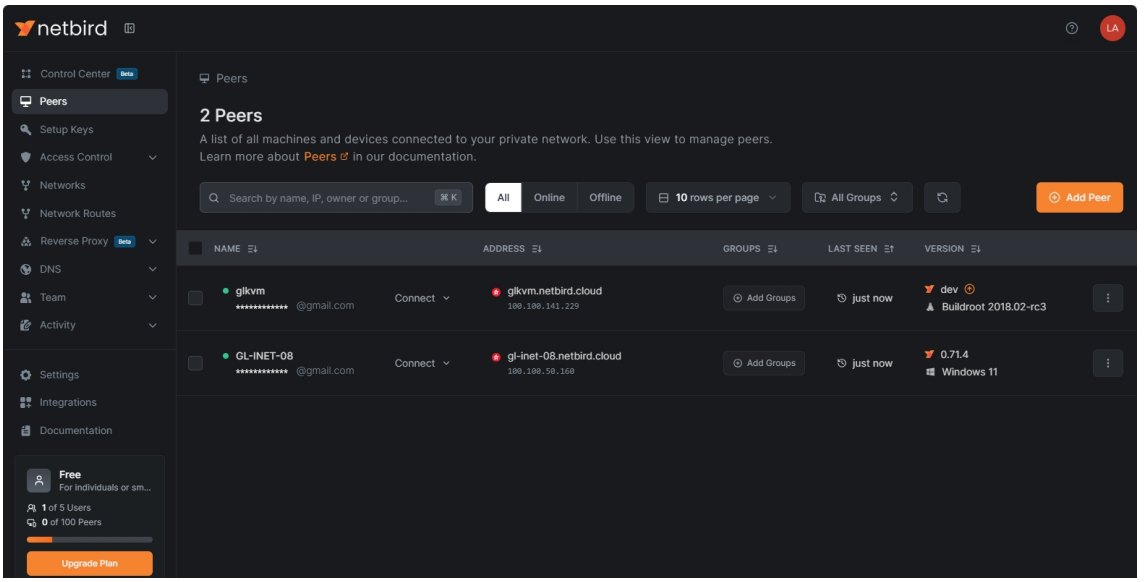
3. In the pop-up window, click **Accept** to authorize.



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



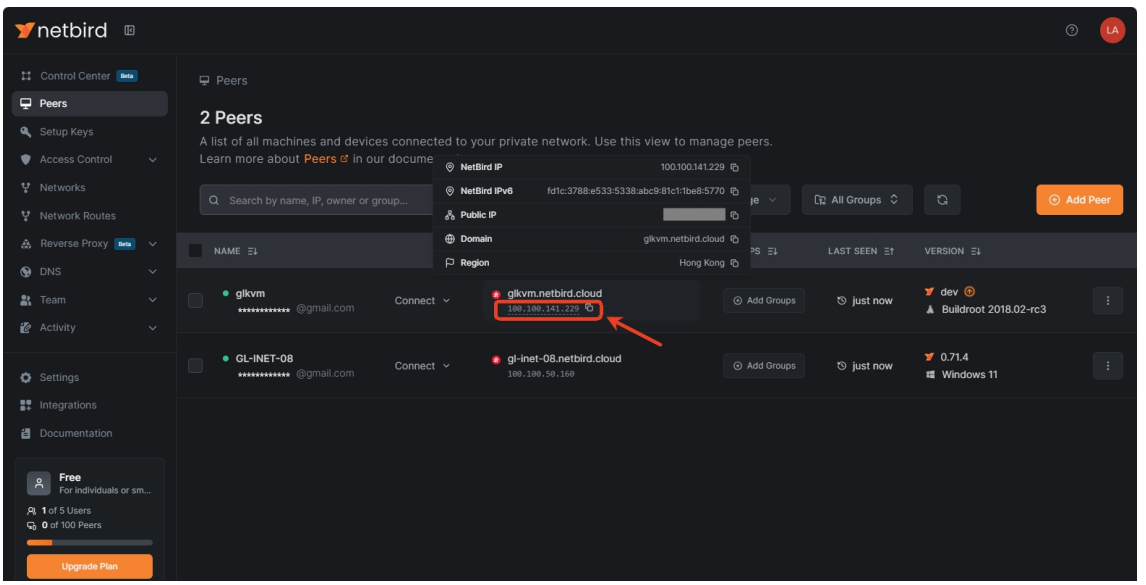
5. On the NetBird dashboard, there are two devices on the **Peers** page: your KVM and the controlling laptop.



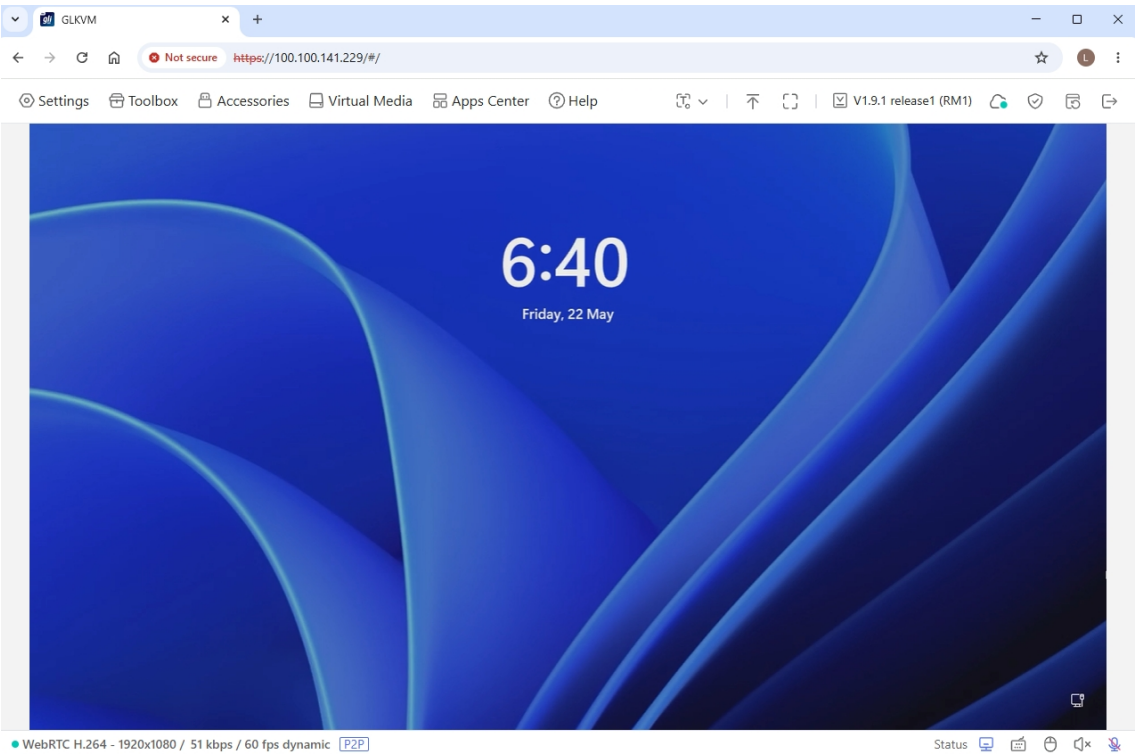
4.5.3 Remote Access via NetBird

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.

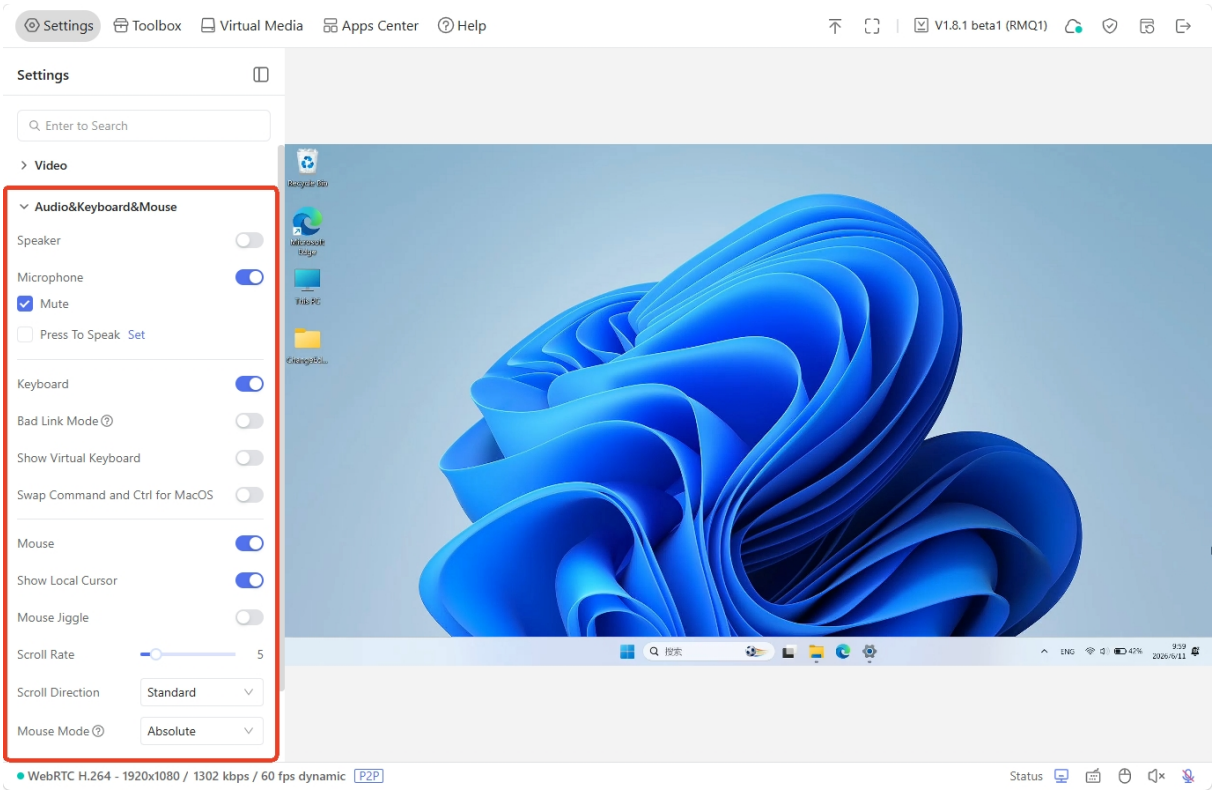


- **Type**: Select your controlled device type.
  The system automatically applies the recommended mouse mode and EDID settings to deliver the best display aspect ratio and control accuracy. Switch this option if the device is not recognized correctly or you need to use a custom type.
- **EDID**: Short 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.
- **Mode**: Switch between Smart and Normal mode as needed. Smart mode helps reduce bandwidth consumption, especially in weak networks.
- **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.

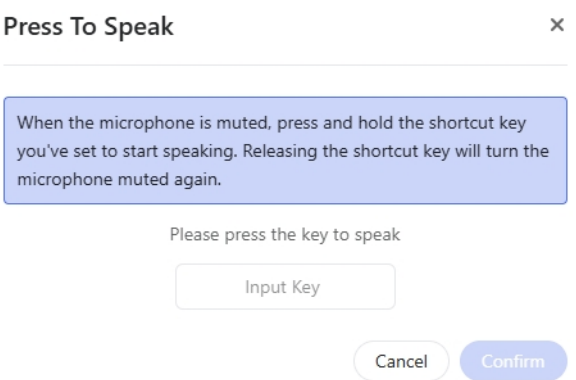
    - **Direct**: Provides the lowest latency and lossless video quality, but does not support audio transmission.
- **Orientation**: Adjust the console's rotation angle to 0°/90°/180°/270°.
- **View**: This setting determines screen scaling when resizing the browser window. Available options: Adaptive, Best Picture Quality, Original Pixel.

5.2 Audio&Keyboard&Mouse

You can adjust relevant settings of the audio, keyboard, and mouse..

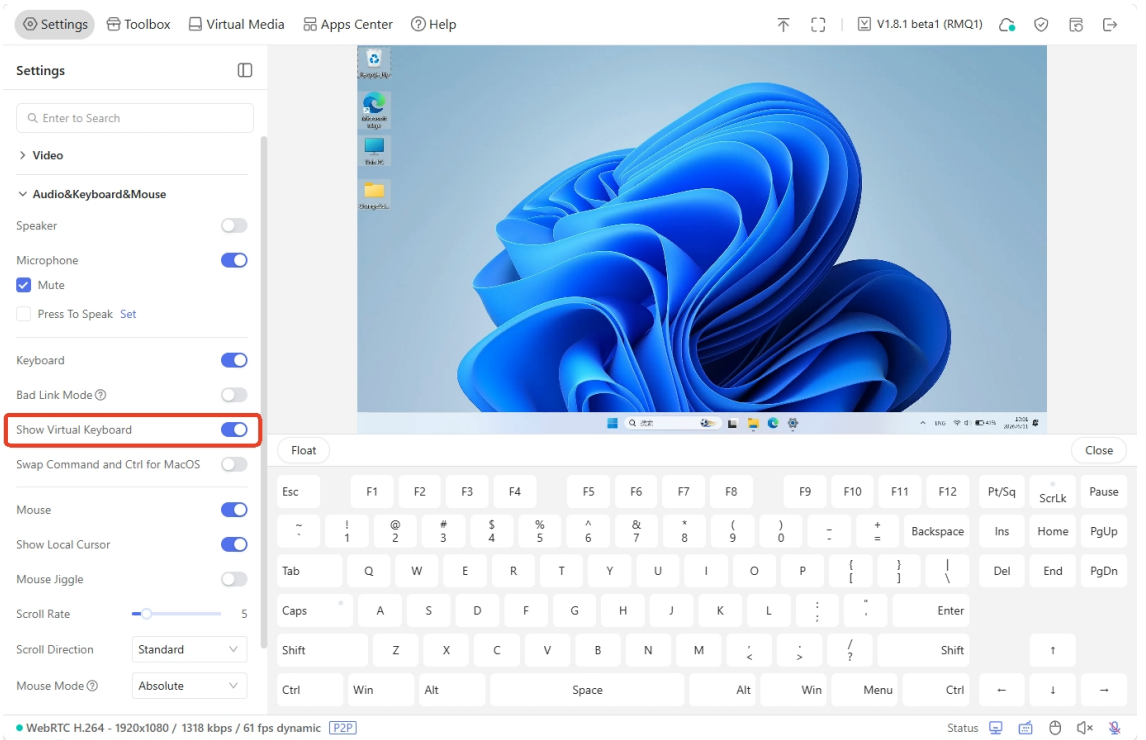


- **Speaker**: Control audio output from the controlled device (e.g., system sounds, video audio).
- **Microphone**: Transmit local audio (e.g., your voice) from the controlling device to the remote end. It supports one-click mute, and a long-press shortcut to activate the microphone (i.e., Press To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

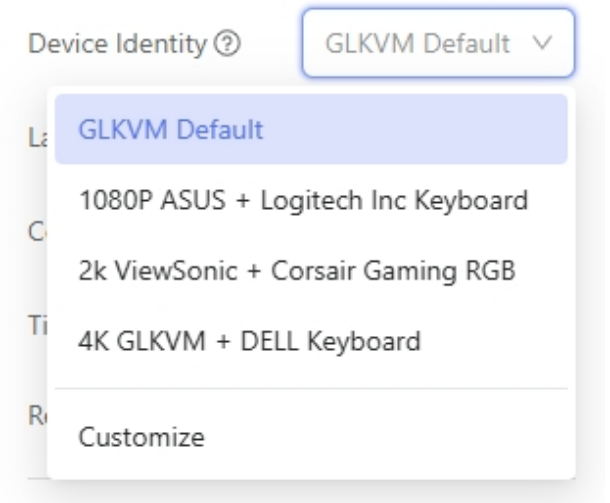
- **Relative Sensitivity**: It is available when the Mouse Mode is Relative.

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.



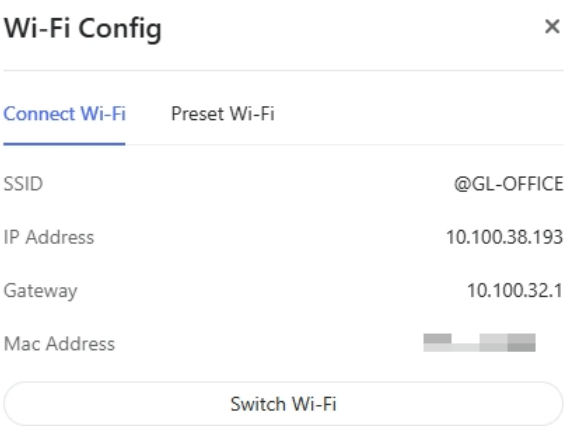
- **Language**: Set the console's language to Chinese or English.
- **Color Mode**: Customize the theme color to Light or Dark mode.
- **Time Zone**: Customize the time zone of the KVM console.
- **Reset KVM**: Factory reset your KVM with just one click.

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.
- **Wi-Fi**: Comet Q's Wi-Fi IP address will be displayed here when it connects to a Wi-Fi network. Click the Wi-Fi SSID or the right arrow to view the Wi-Fi details, including the SSID, assigned IP address, gateway, and the MAC address your Comet Q uses to connect to.



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

Chapter 6

Toolbox

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

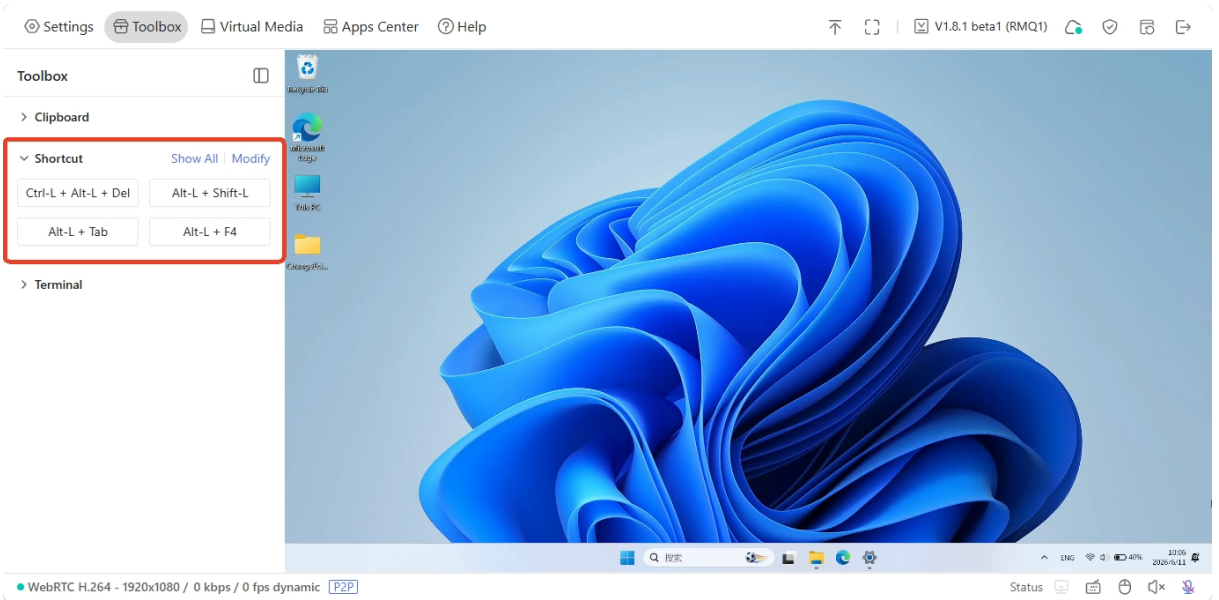
6.1 Clipboard

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. Some common shortcuts are available on this page, and you can click **Modify** to adjust the shortcuts options if needed.



6.3 Terminal

You can access the Comet Q's terminal to perform advanced settings. Click **Access**.



You will be redirected to the GLKVM terminal.



Chapter 7

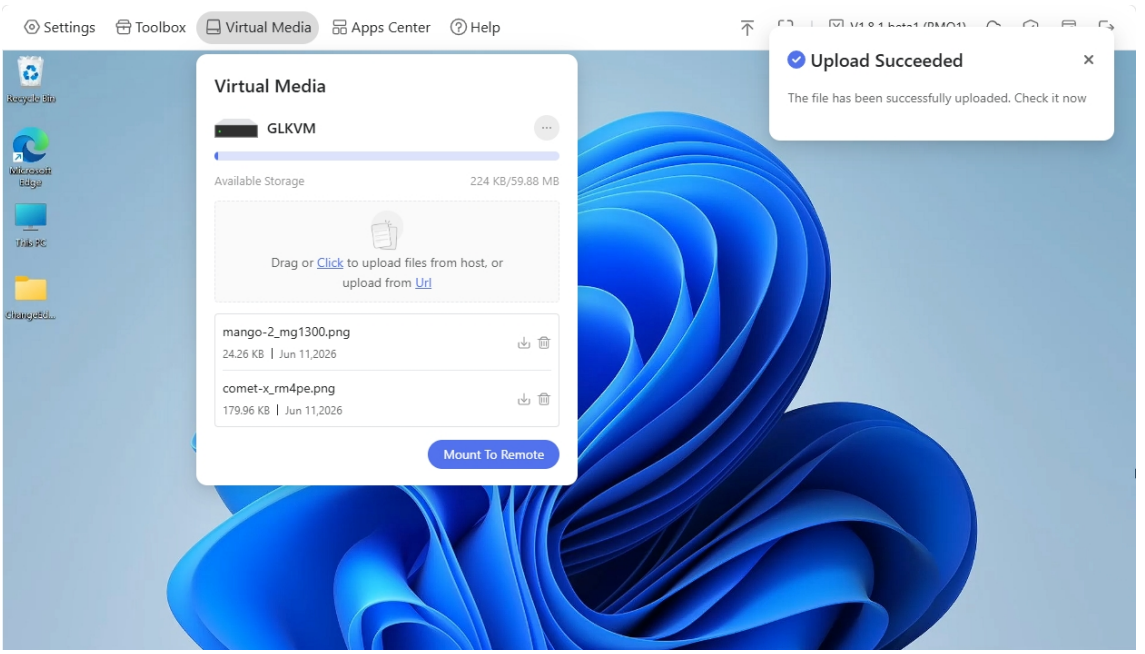
Virtual Media

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

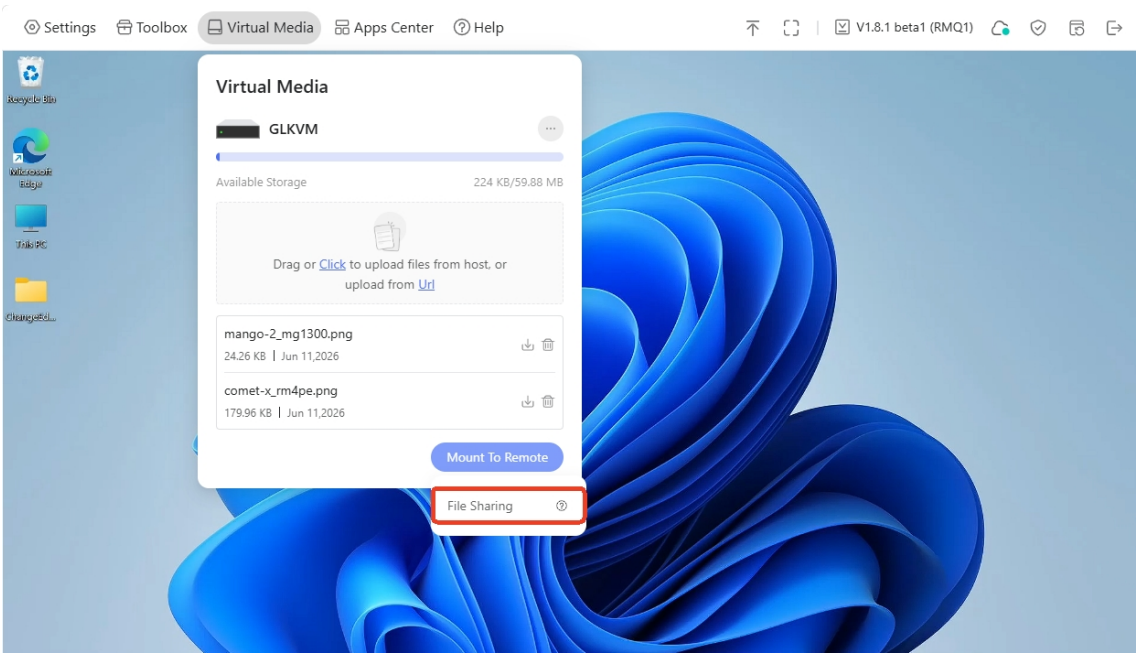
7.1 File Sharing

Comet Q 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.

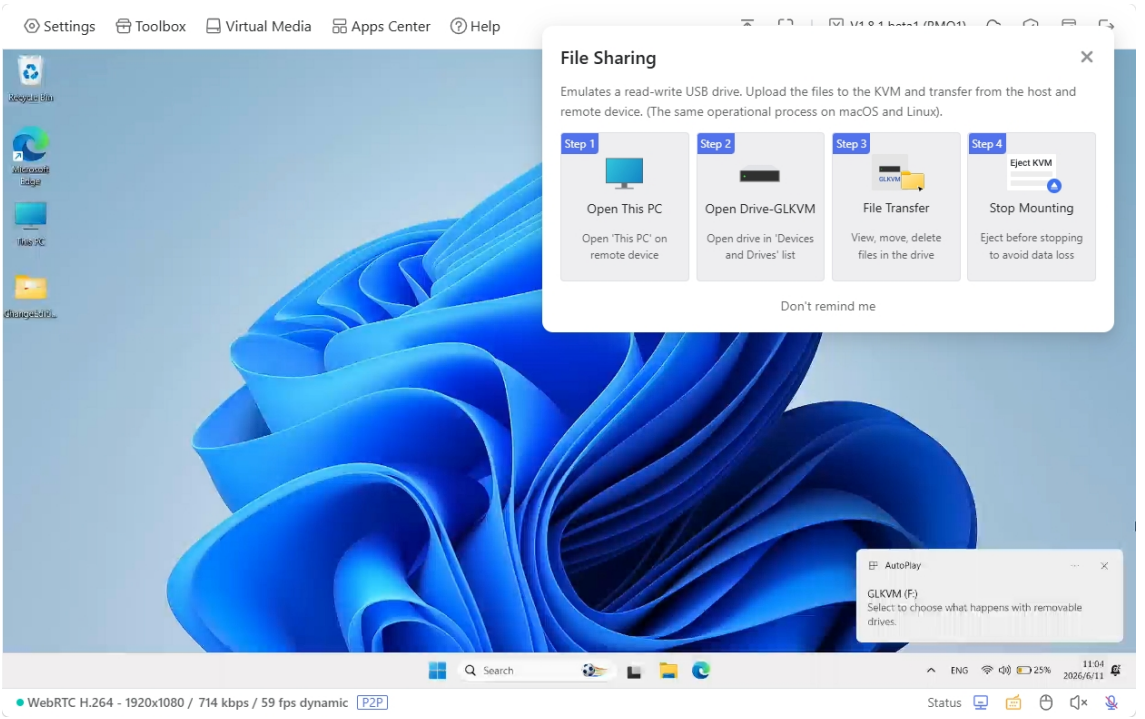
1. On your controlling device, log in to the KVM Web console and navigate to **Virtual Media**. Drag or click the box to upload files.



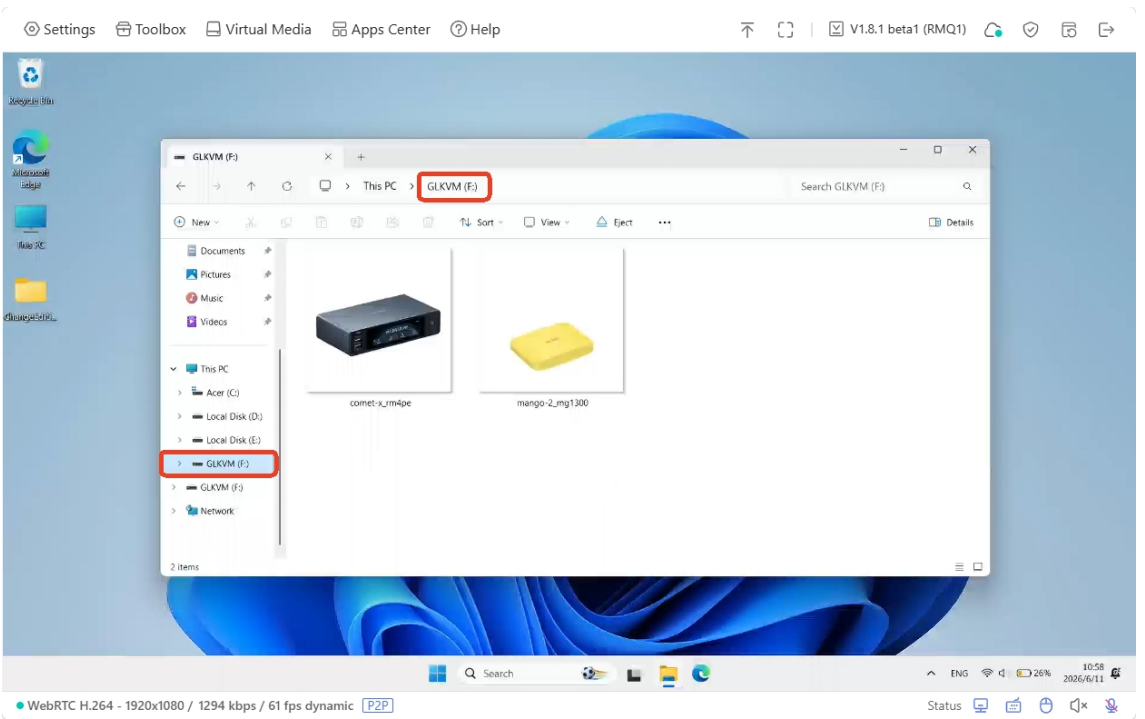
2. Click **Mount To Remote** > **File Sharing**.



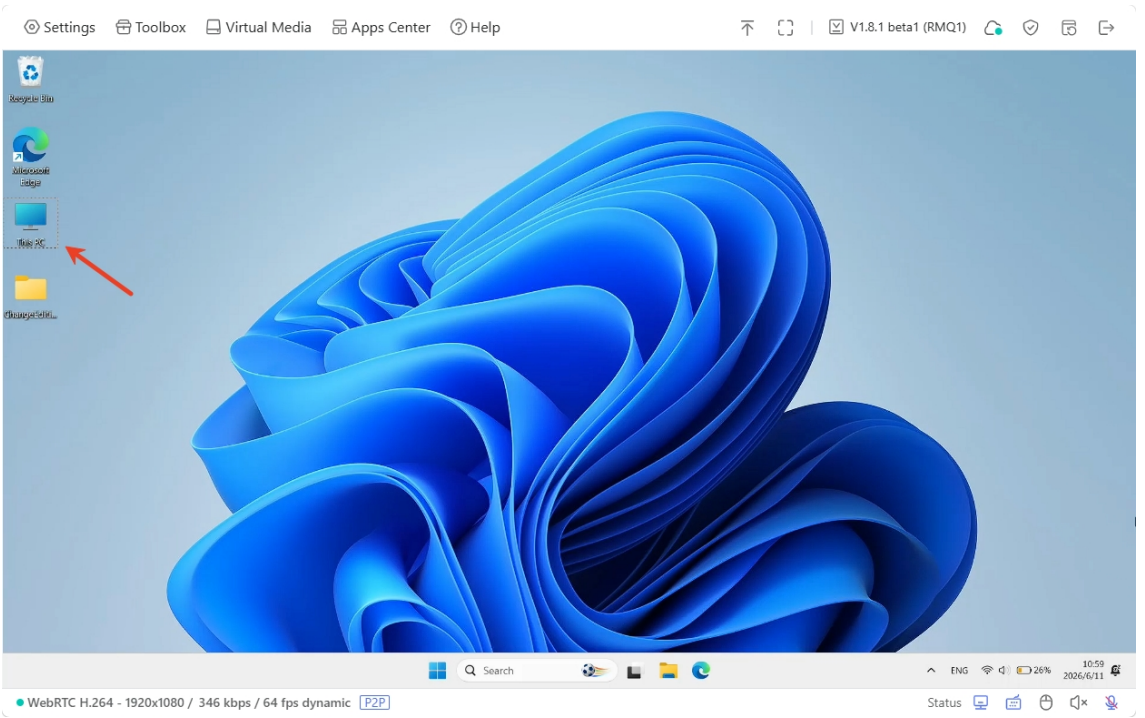
3. A window will pop up on the console indicating the file sharing steps, as shown below.



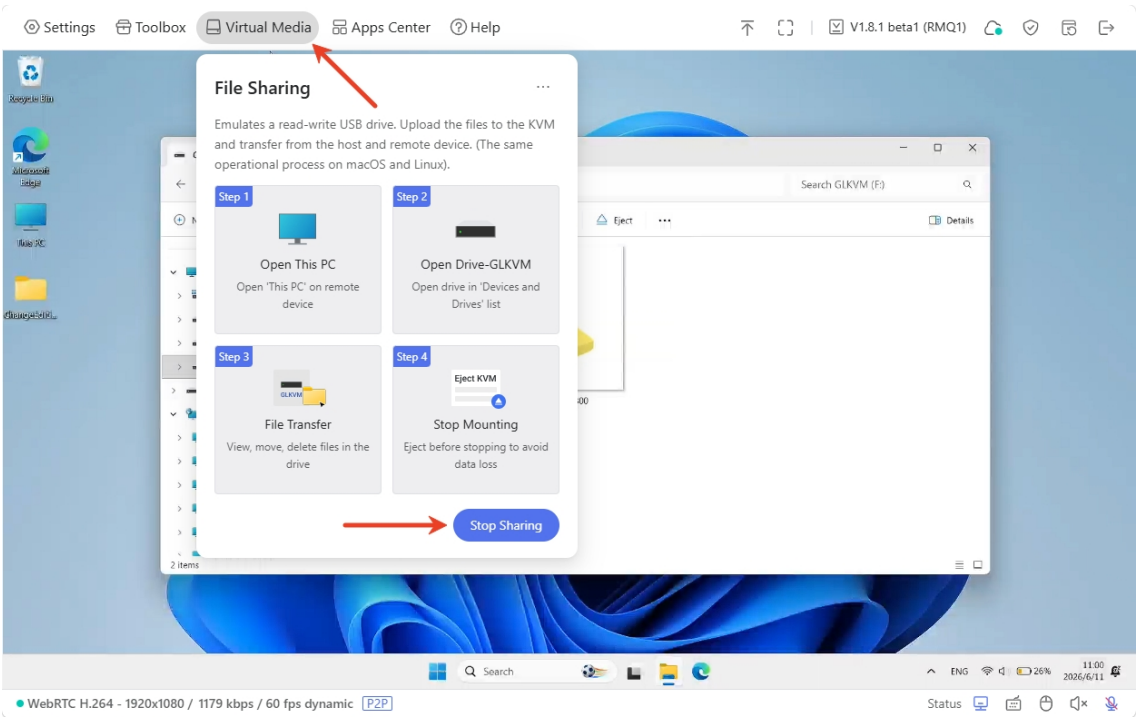
4. Wait a second, and a drive named "GLKVM" will pop up on the screen automatically. You will then see the files you previously uploaded from the controlling device to Comet Q have been shared to the controlled device. Now you can view, move or delete the files in this drive on the controlled device.



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.

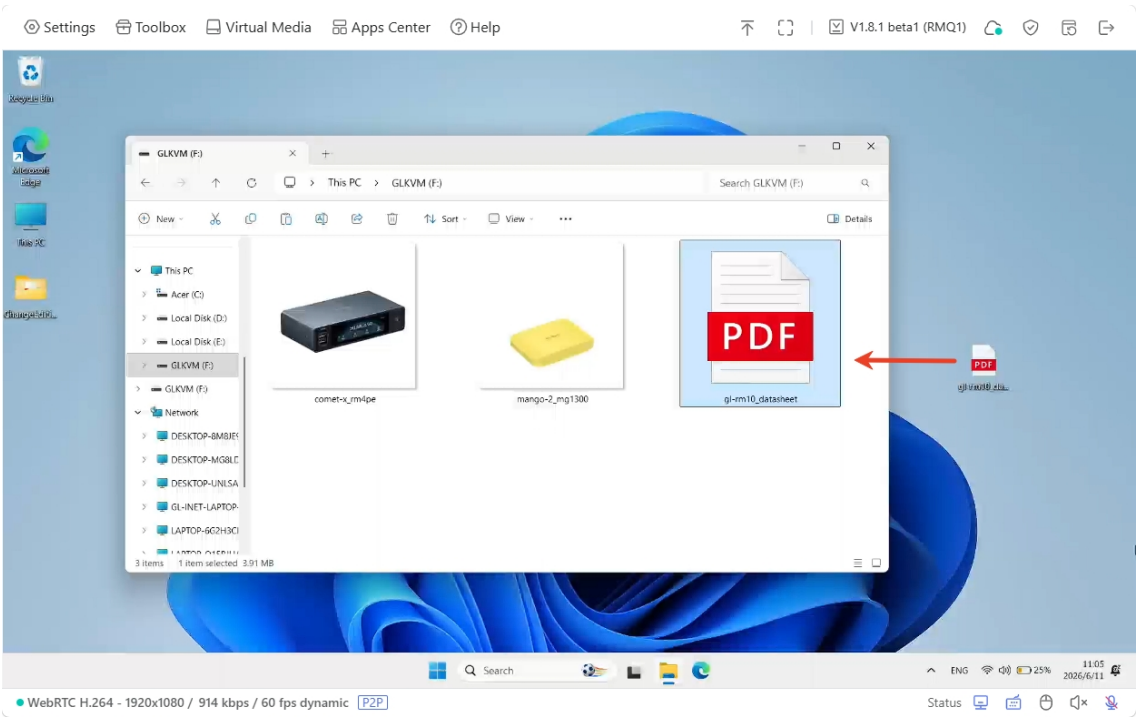


5. If you want to stop sharing, click **Virtual Media** in the toolbar and click **Stop Sharing**.

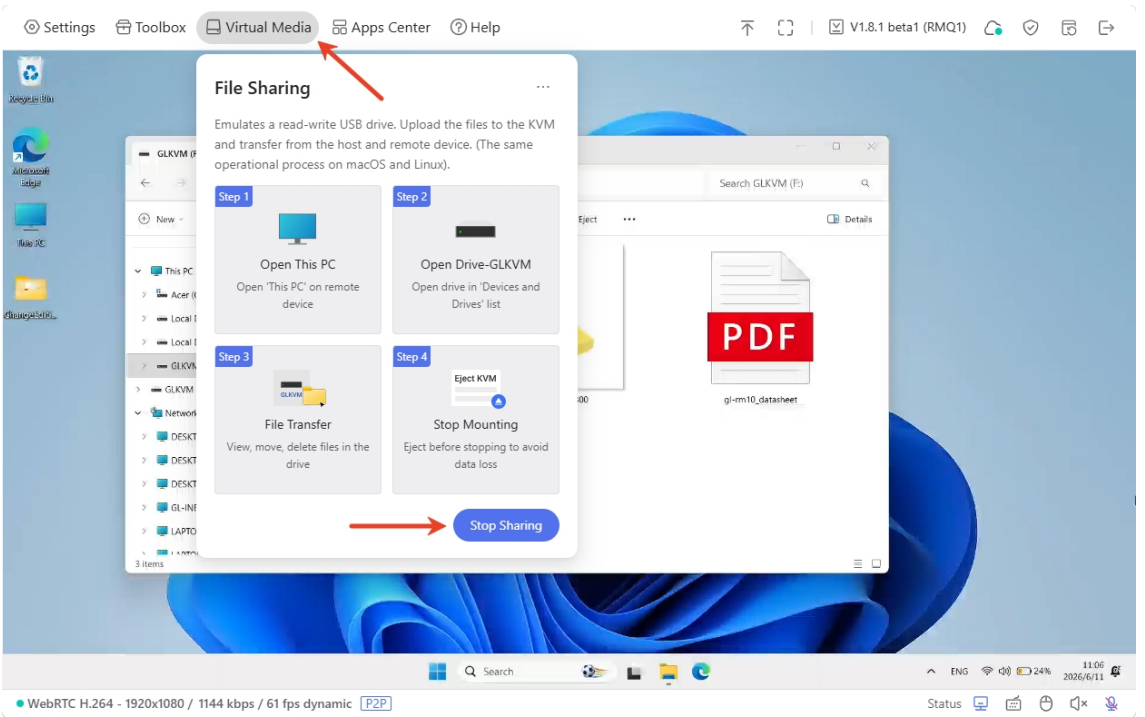


6. To share files from the controlled device to the controlling one, move or copy the files you want to share from the controlled device into the drive **GLKVM**. For example, a PDF file

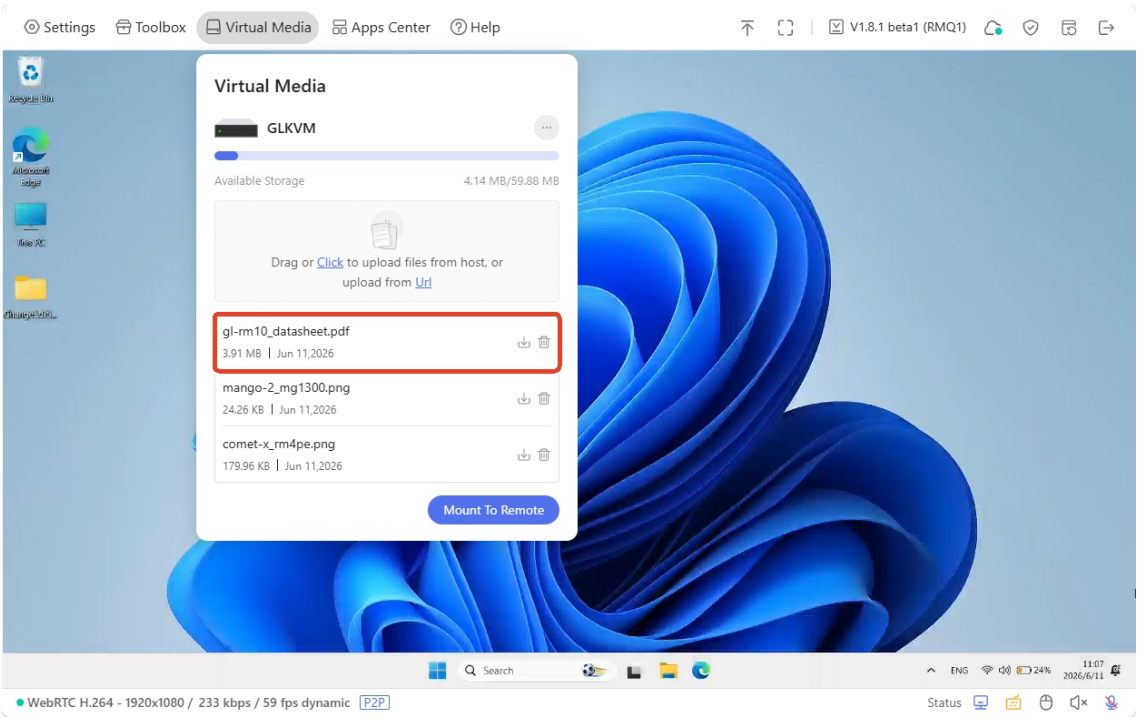
named "gl-rm10_datasheet" has been copied from the controlled device's Desktop into the disk GLKVM.



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

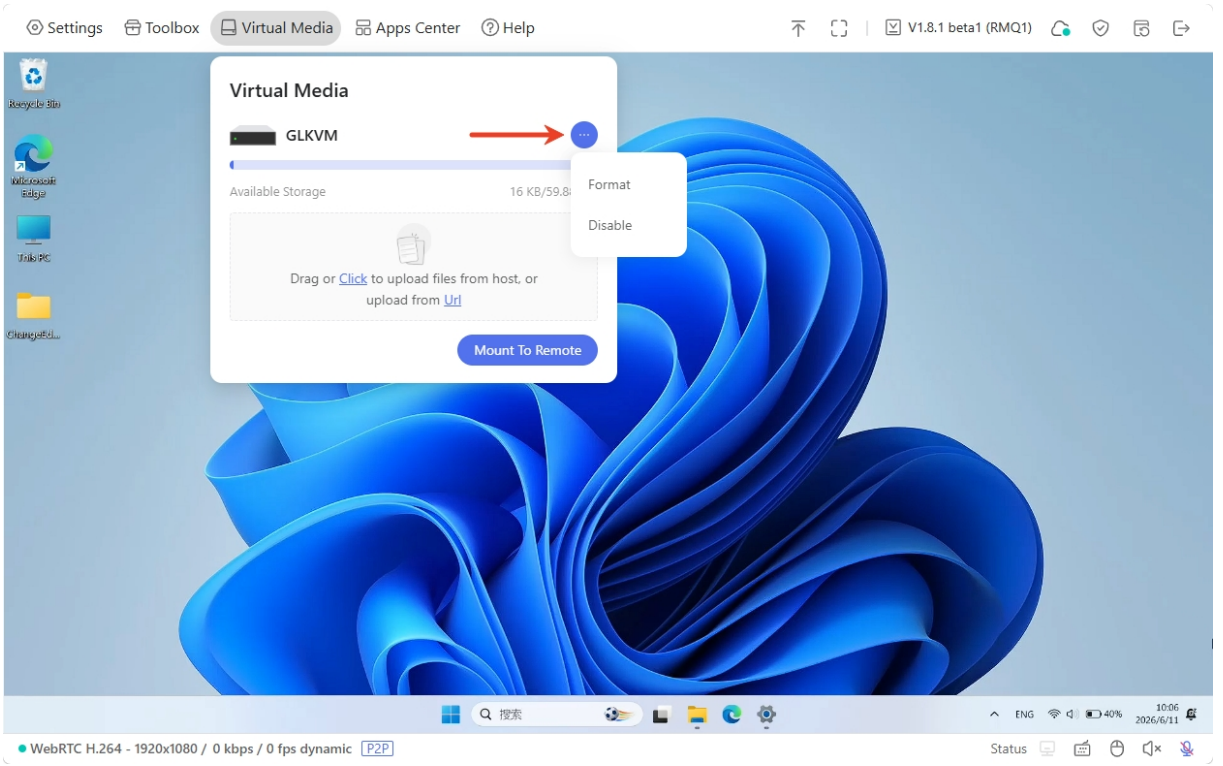


8. This file will then be displayed under the **Virtual Media**, as shown below. Now you can download this file from Comet Q to your controlling device.


Settings
Toolbox
Virtual Media
Apps Center
Help
V1.8.1 beta1 (RMQ1)
Virtual Media
GLKVM
Available Storage
4.14 MB/59.88 MB
Drag or Click to upload files from host, or upload from Url
gl-rm10_datasheet.pdf
3.91 MB | Jun 11,2026
mango-2_mg1300.png
24.26 KB | Jun 11,2026
comet-x_rm4pe.png
179.96 KB | Jun 11,2026
Mount To Remote
Search
ENG
24%
11:07
2026/6/11
WebRTC H.264 - 1920x1080 / 233 kbps / 59 fps dynamic
P2P
Status

7.2 Format Disk

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



- **Format**: Erase all data on the disk and reinitialize its file system structure.
- **Disable**: Disable the virtual media will immediately reboot the KVM device.

Chapter 8

Apps Center

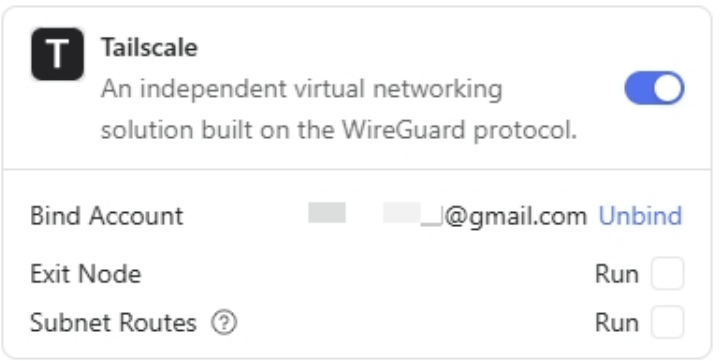
This chapter introduces some applications integrated in GL.iNet KVM console.

8.1 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 Q integrates with Tailscale, allowing you to remotely access it through Tailscale virtual network. Simply bind Comet Q and your controlling device to the same Tailscale account, then you can remotely access your Comet Q 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.

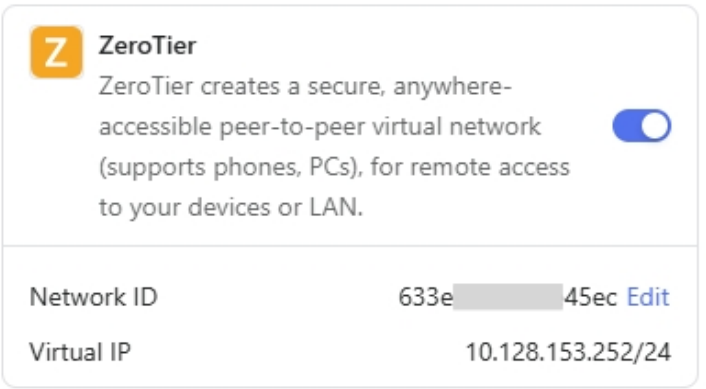


8.2 ZeroTier

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

Comet Q integrates with ZeroTier, allowing you to remotely access it through ZeroTier virtual network. Simply join Comet Q and your controlling device to the same ZeroTier network, then you can remotely access your Comet Q 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.

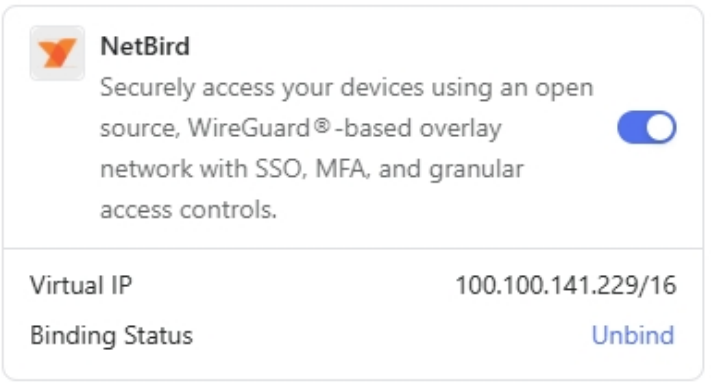


8.3 NetBird

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 Q 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.



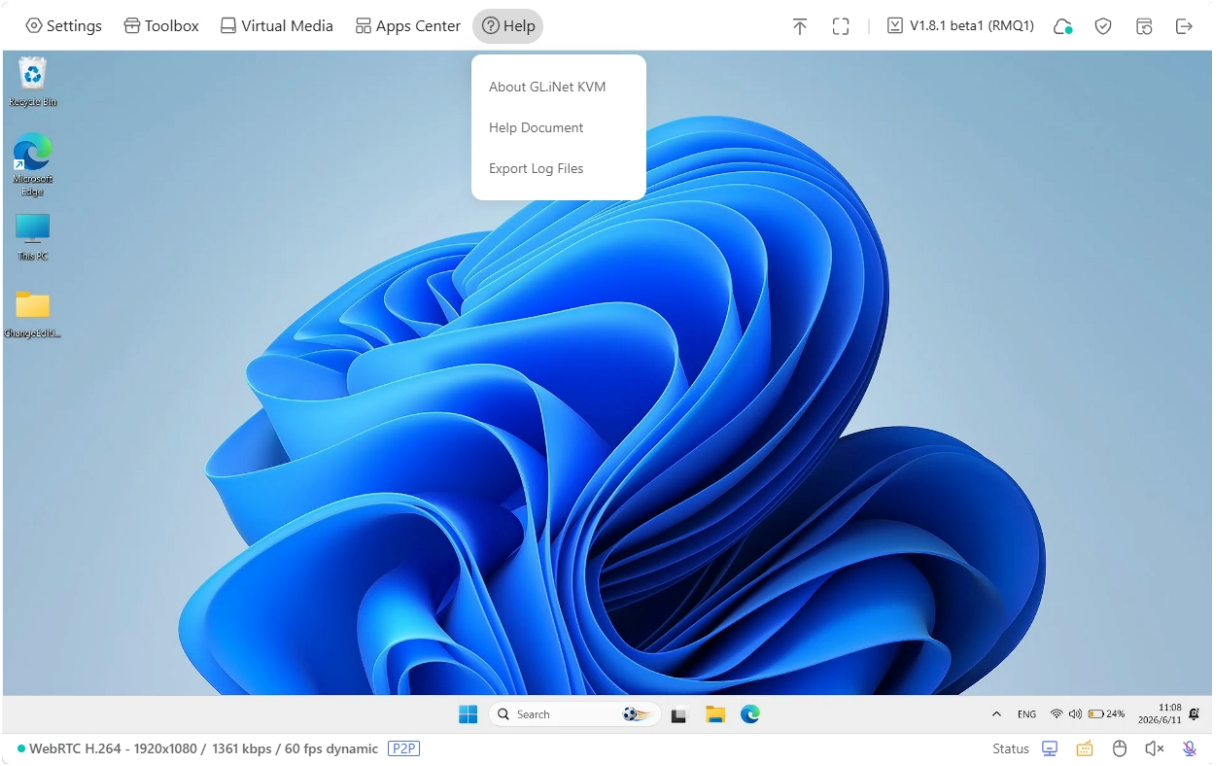
Chapter 9

System Tools

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

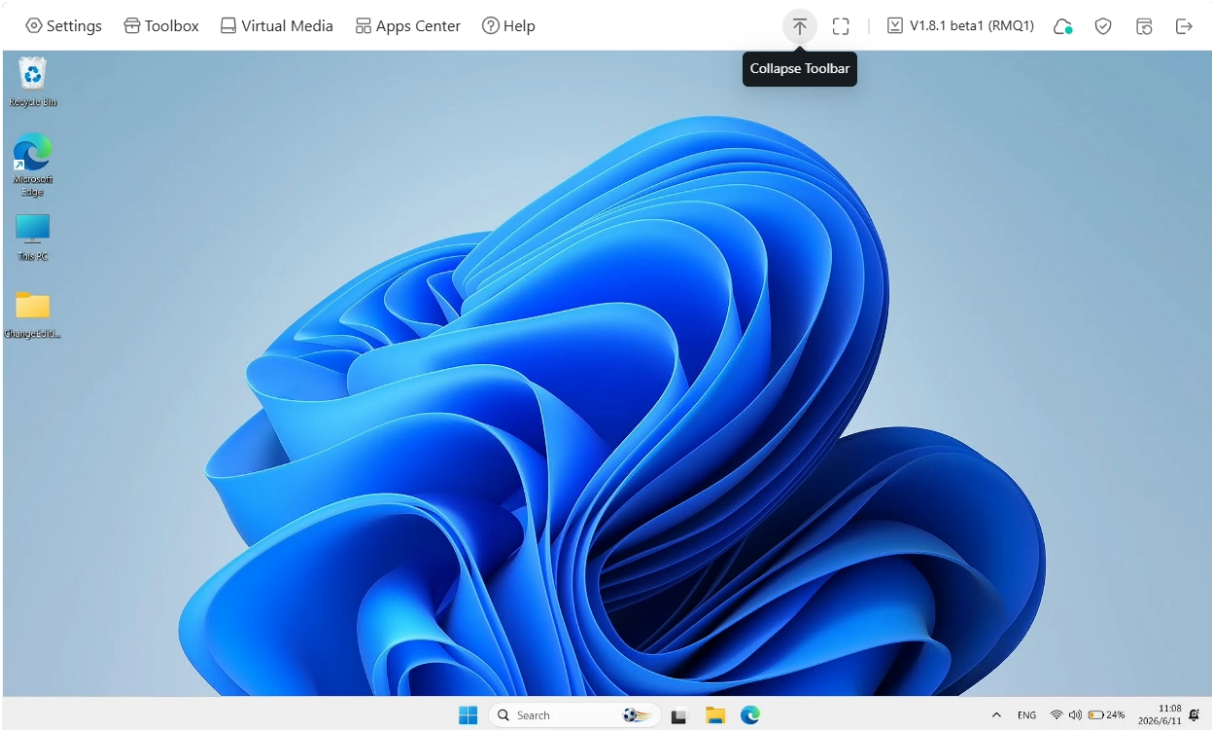
9.1 Help Center

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.



9.2 Collapse

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

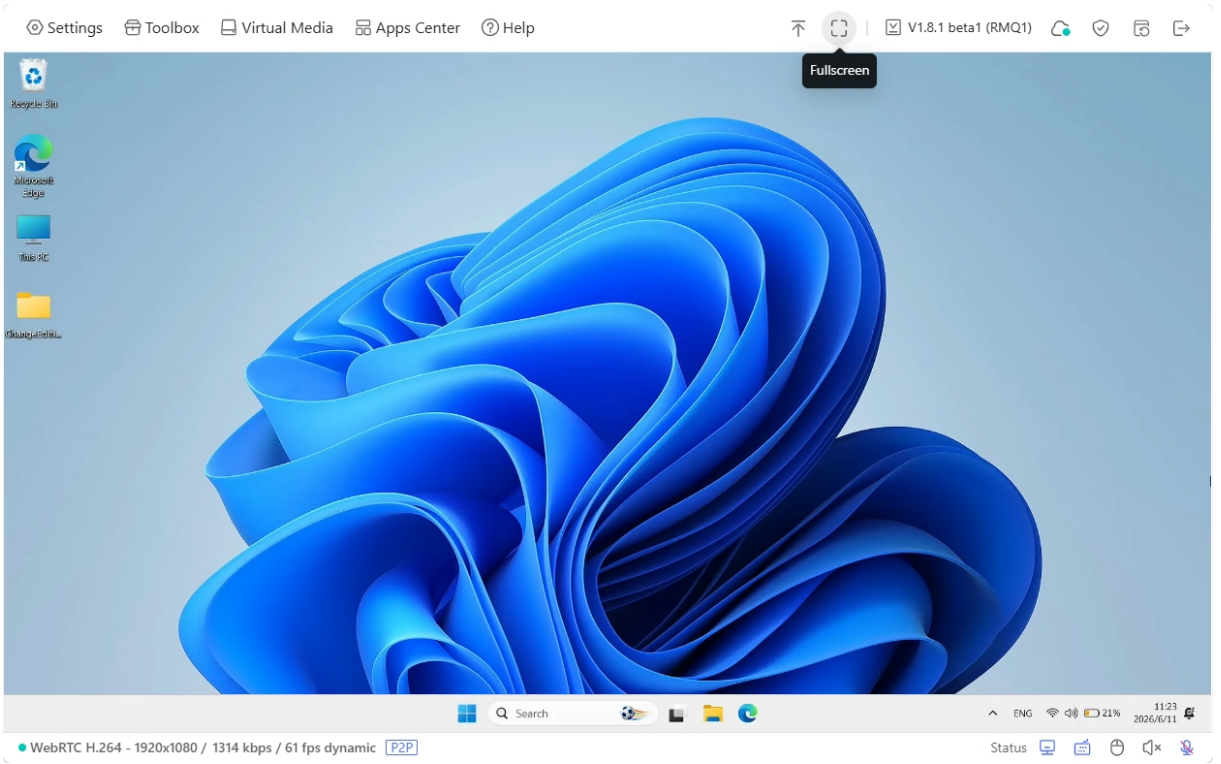


When the toolbar is folded, click the downward arrow icon at the top to expand it.

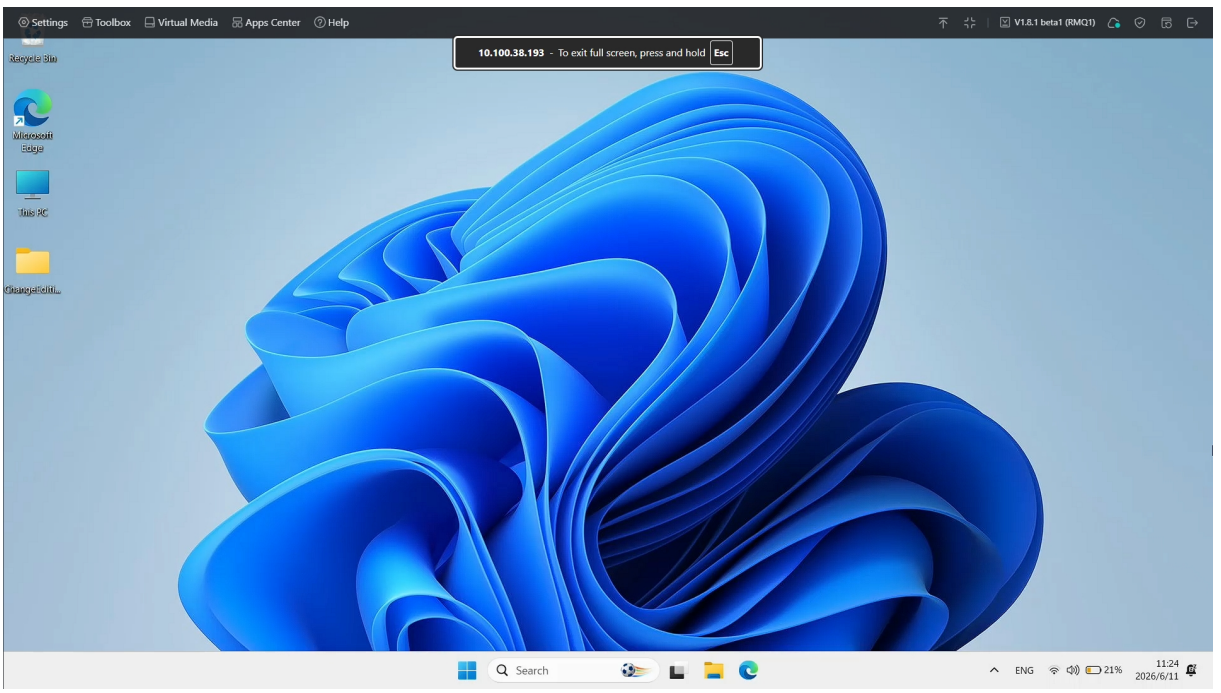


9.3 Fullscreen

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

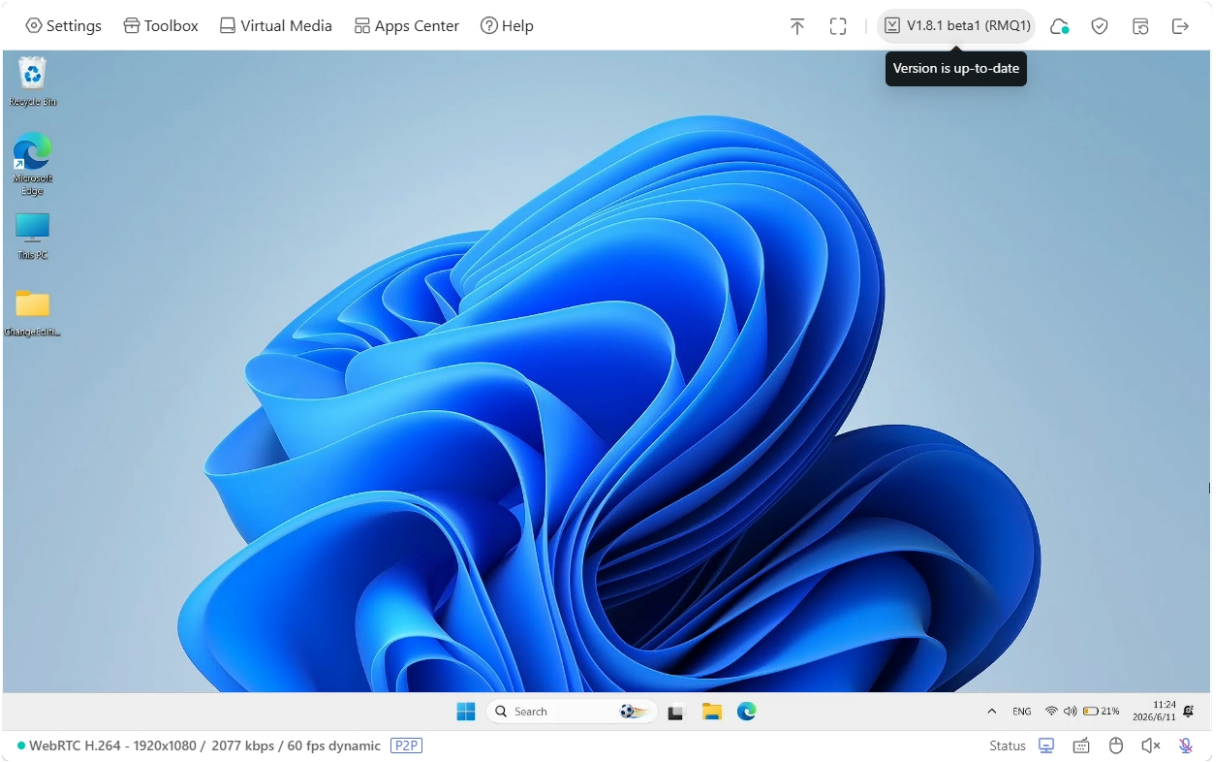


To exit fullscreen, press and hold the **Esc** key, or click the exit fullscreen icon (grid-shaped) in the upper right corner.



9.4 Upgrade

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

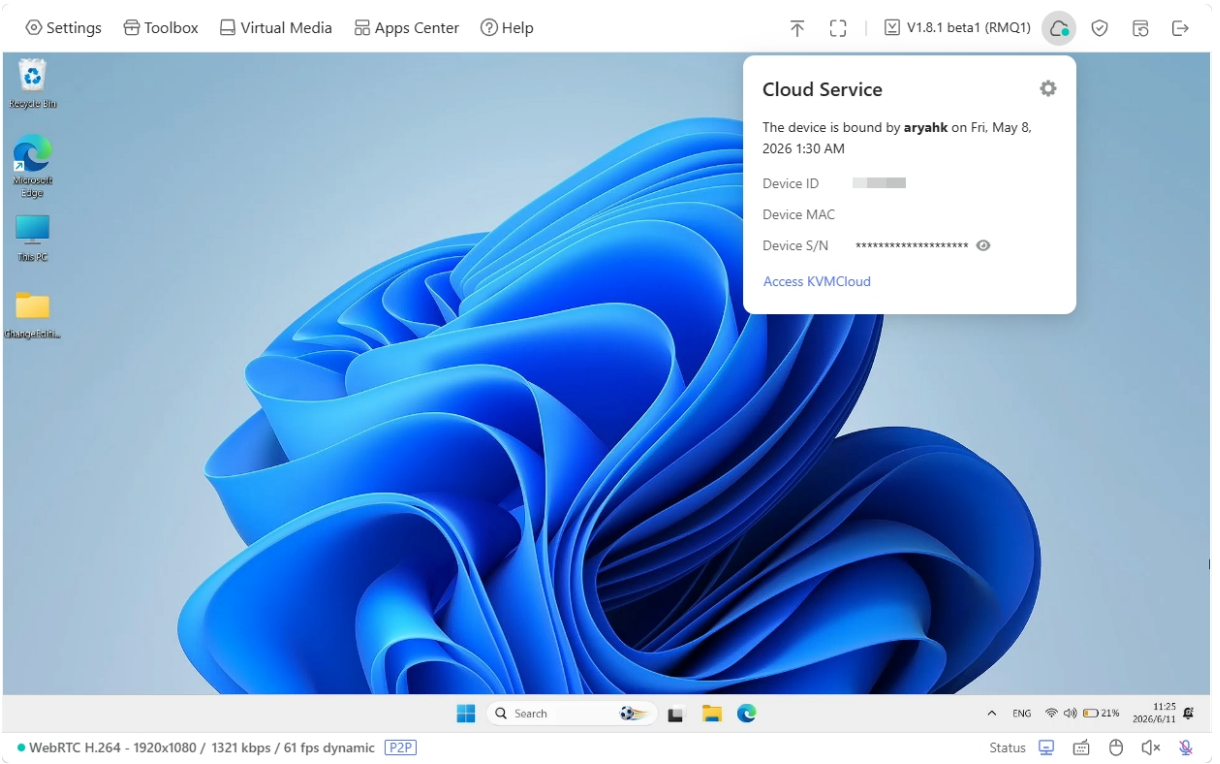


In the pop-up window, you can perform an online upgrade if newer firmware is available. Alternatively, download the latest firmware from the Firmware Download Center before performing a local upgrade.

9.5 Cloud Service

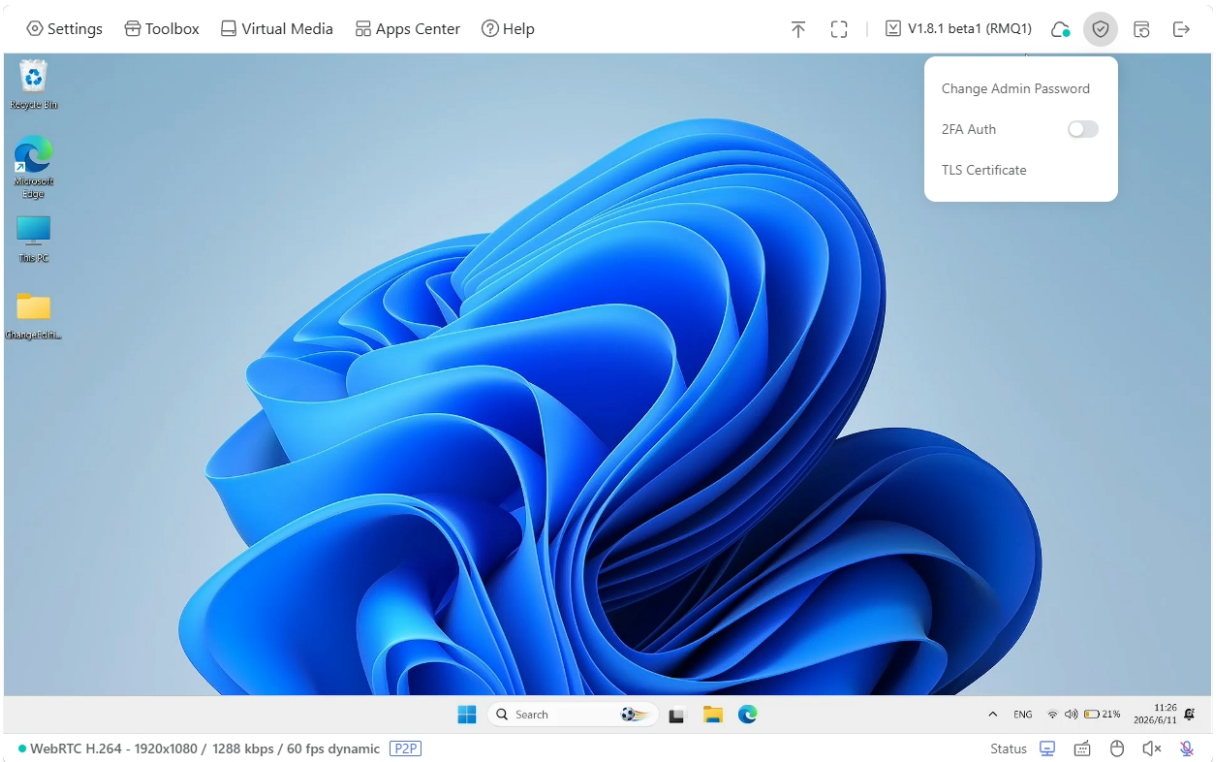
GL.iNet KVM Cloud allows you to access the controlled device remotely. See 4.1 Cloud Service for details.

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

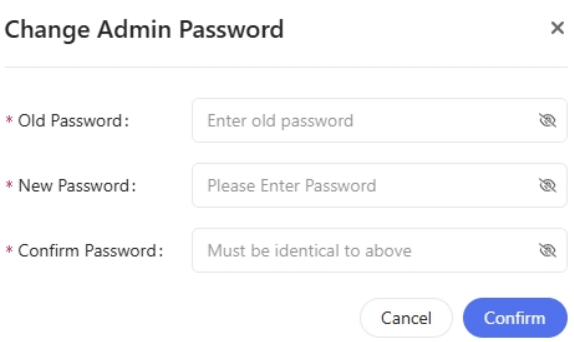


9.6 Security

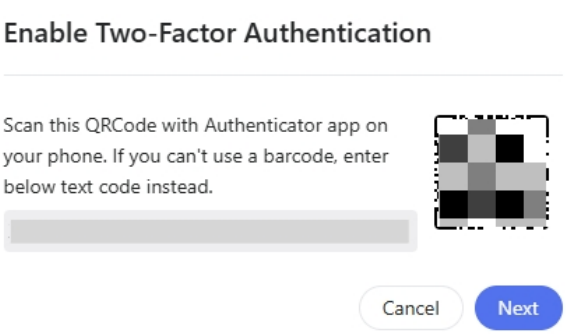
The security allows you to change admin password, enable two-factor authentication, and customize TLS certificate.



- **Change Admin Password**

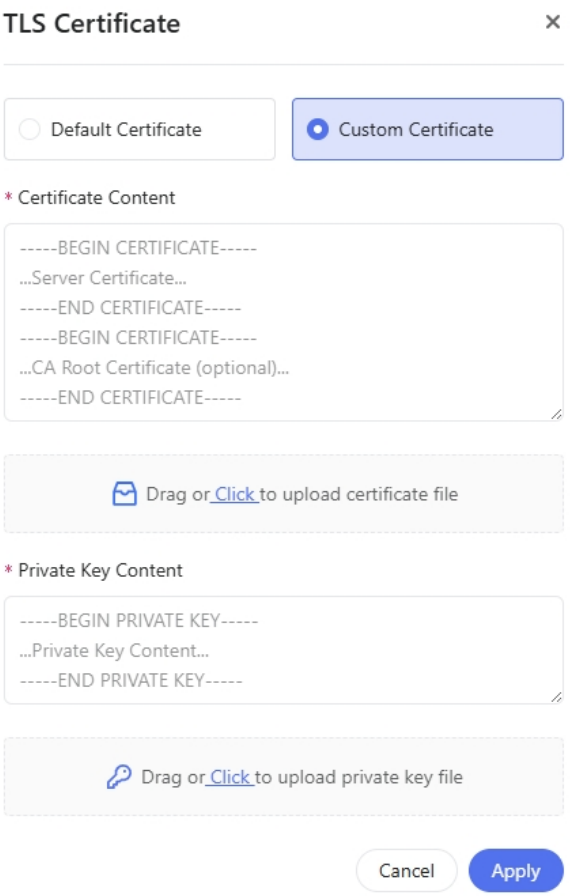


- **2FA**: Enable two-factor authentication to protect your account.



- **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.



Frequently Asked Questions

General

1. **What should I do if the KVM control screen shows "Unable to Display" when Comet Q connects to the controlled device?**
   This is because your controlled device does not support USB-C DisplayPort Alt Mode, which prevents video stream output. See How to check if your device supports DisplayPort Alt Mode.

2. **Why is the controlling device unable to display the password input keyboard when the controlled device's screen is locked?**
   Due to iOS/Android security restrictions, the system blocks the password entry page during screen mirroring or remote control. You may directly enter the unlock password from the controlling end to unlock your device.

3. **Why can't the sound be transmitted to the controlling device when the controlled device is making a voice call?**
   This problem commonly occurs on iPhones and some Android devices. When voice interaction software (e.g., WhatsApp, Microsoft Teams) is running on the controlled device for voice calls, due to iOS/Android system restrictions, audio can only be output through local speakers on the controlled device and cannot be transmitted to the controlling end through KVM.

   Tip: Media audio (videos, music, games, etc.) can be normally transmitted to the controlling end via KVM when voice interaction apps are inactive.

iOS

1. **Why can't I adjust the system volume on iOS devices after connecting to Comet Q?**
   Restricted by the iOS system, once an iPhone/iPad connects to a screen mirroring device such as GL.iNet KVM, which has been set as the audio output, the native system volume control becomes unavailable.

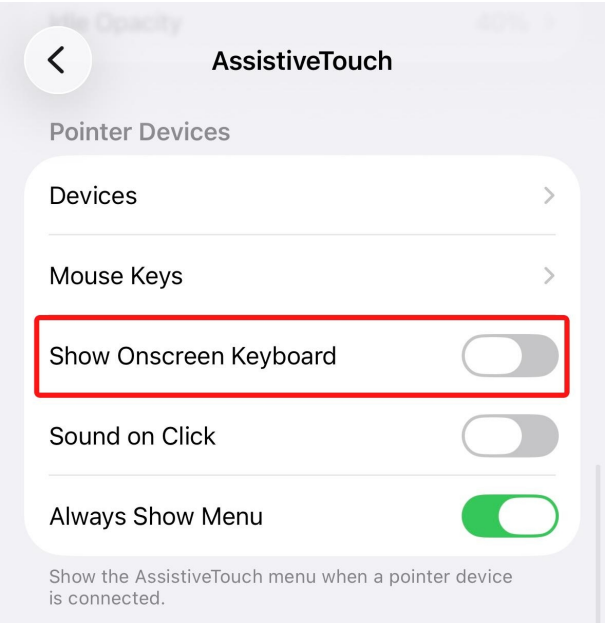
2. **Why does the iOS device show no local video frame when streaming videos via video apps?**

   When an iOS device connects to a screen mirroring device such as GL.iNet KVM, some video apps (e.g., YouTube, Netflix) default to outputting video via AirPlay, thus the iOS device does not show local video frame. This behavior cannot be disabled at the system level. If you want the controlled device to play videos locally when being mirrored, please play the videos through a web browser instead.

3. **What should I do if the on-screen keyboard disappears from iOS device after connected to Comet Q?**

   This is likely that iOS recognizes Comet Q as an external physical keyboard and automatically hides the native on-screen keyboard. In that case, please use the keyboard on the controlling device, or the virtual keyboard embedded in the KVM console.

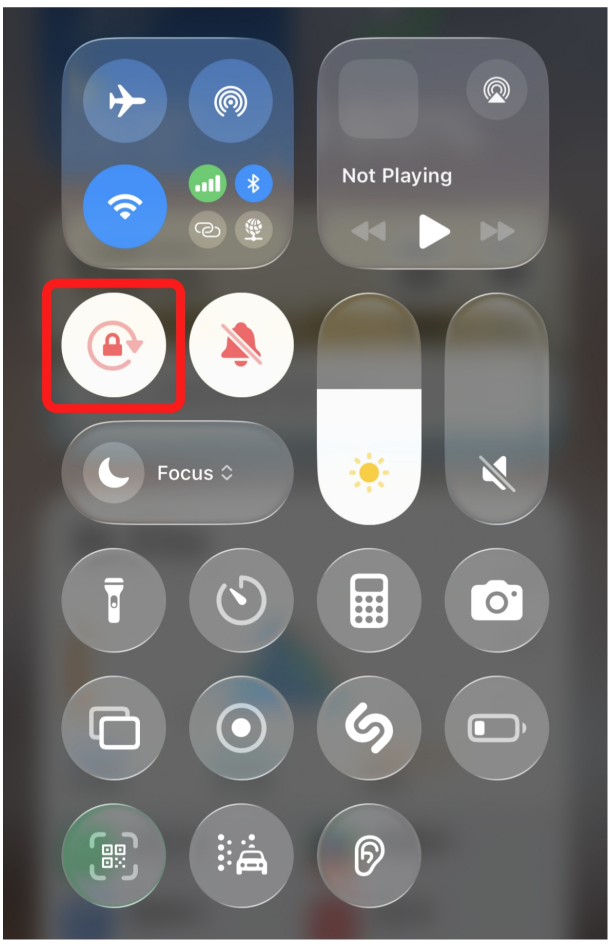
   If you still need to use the iOS on-screen keyboard, navigate to **Settings** > **Accessibility** > **Touch** > **AssistiveTouch**, then enable **Show Onscreen Keyboard**.



4. **When mirroring an iPhone/iPad in portrait/landscape orientation, the mouse on the controlling end still drifts out of alignment even after adjusting screen orientation in the KVM console. What should I do?**

Precise cursor tracking on iPhone or iPad requires perfect alignment between the device's gyroscope orientation and the displayed screen orientation. During remote control, the system may fail to correctly detect the current gyroscope state, causing mouse offset.

To fix this, turn on the **Portrait Orientation Lock / Rotation Lock** on your iPhone/iPad to guarantee accurate cursor tracking.



5. Why does the keyboard not work properly on iOS devices, with some keys not working or the mouse pointer drifting?
   This issue is usually caused by the **Mouse Keys** feature being enabled on the iOS device. Mouse Keys allows users to move the mouse pointer using a keyboard or numeric keypad. To resolve the issue, navigate to **Settings** > **Accessibility** > **AssistiveTouch** > **Mouse Keys** and turn off Mouse Keys.

Android

1. **Why can't I control the device in absolute mouse mode?**
   Restricted by the Android operating system, Android devices can only be controlled in relative mouse mode.
   When controlling via the glkvm mobile APP, fully cover the mouse pointer with your finger to execute operations.

2. **What should I do if the screen displayed on the controlling end is not synchronized with the screen displayed on the controlled Android phone?**
   Some Android phones identify Comet Q as an extended display rather than a mirrored screen. To fix this, please modify the display setting on your phone to Screen Mirroring mode.
   Take Samsung S Series as an example: Go to **Settings** > **Device Connections** > **Samsung DeX** > **Connected Display**, then select **Screen Mirroring** mode.

Regulatory Statement

FCC ID: 2AFIW-RMQ1

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 and SAR Statements

The device has been tested for body-worn Specific Absorption Rate (SAR) compliance.
The FCC/IC has established detailed SAR requirements and has established that these requirements.

RF Exposure Information
The radio module has been evaluated under FCC Bulletin C95.1 and IEEE 1528 and found to be compliant to RF Exposure from radio frequency devices.
This model meets the applicable government requirements for exposure to radio frequency waves.
The highest reported SAR level for usage near the body (0mm) is 0.834 W/kg.

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.
1) Do not cover ventilation openings, this equipment is not intended to be used on soft support.
2) The marking information is located at the bottom of apparatus.

Declaration of Conformity

Hereby, GL TECHNOLOGIES (HONG KONG) LIMITED declares that the radio equipment type [Remote KVM, GL-RMQ1] is in compliance with 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:
CE: ≤20dBm EIRP (2.4GHz); ≤23dBm EIRP (5.15GHz~5.35GHz); ≤30dBm EIRP (5.47GHz~5.725GHz); ≤13.98dBm (5.725GHz~5.85GHz)