KNOWLEDGE BASE TECHALERT

TECHALERT DEVICE FORWARDING TECHNICIAN GUIDE

VERSION 1.11.0 | EFFECTIVE DATE: NOVEMBER 17, 2026 | LAST REVISED: NOVEMBER 19, 2026

TABLE OF CONTENTS

1. Purpose 1
2. Update Notes 1
3. What Is Device Forwarding 1
4. Requirements 2
5. Limits 2
6. Known Issues 2
7. How to Use Device Forwarding 3
8. Troubleshooting 4
9. Enable Device Forwarding on Windows and Linux Hosts 4
10. Device Buttons for Administrators 6

1. PURPOSE

This guide explains what Device Forwarding is and how to use it in TechAlert. Device Forwarding lets you open the web page of equipment that sits behind a TechAlert host, such as a power relay, camera or network switch inside a trailer, without traveling to the site and without connecting a laptop to its network.

It is written for technicians who use the Tech Connect page. The sections Enable Device Forwarding on Windows and Linux Hosts and Device Buttons for Administrators are for the people who install TechAlert hosts and manage TechAlert templates.

2. UPDATE NOTES

- 1.11.0: Update: Connect row layout
  - The button is now named **Device Forwarding** (it was Forward…).
  - Each host row shows **Quick Connect**, **Device Forwarding** and an **Other connections** menu.
- 1.10.1: Fix: Start page for device buttons
  - A device button can open on a specific page of the equipment. This fixes the Victron Cerbo GX, which lost its connection when it redirected to its own start page.
- 1.10.0: Feature: Device buttons
  - One-click buttons for the equipment behind a host, set up once by an administrator.
- 1.9.0: Feature: Device Forwarding
  - First release. Open the web page of any device on a host's local network by typing its address.

3. WHAT IS DEVICE FORWARDING

Every TechAlert host has a Tech-Connect agent installed on it. A normal connection, such as Connect in browser or Quick Connect, opens the screen of that host itself.

© 2026 Vetted Security Solutions. All Rights Reserved.

Device Forwarding goes one step further. The host passes your connection on to another device on its own local network. You see that device's web page in your browser as if you were plugged into the same network.

Example: A trailer has a TechAlert host, a Victron Cerbo GX power relay and two cameras. With Device Forwarding you can open the Cerbo GX web page from your office, through the trailer's host.

	Quick Connect	Device Forwarding
What you reach	The TechAlert host itself	Another device on the host's local network
What opens	The host's screen	That device's web page
What you need to know	Nothing; one click	Nothing if a device button exists; otherwise the device's local address

4. REQUIREMENTS

- A TechAlert account with access to the host. Hosts you can only see through a map do not offer Device Forwarding.
- The host must be online in Tech-Connect. Its status on the Tech Connect page must read **Ready** or **In use**.
- A Windows or Linux host must first be enabled for Device Forwarding by an administrator (see Enable Device Forwarding on Windows and Linux Hosts). Camera hosts running the Tech-Connect ACAP version 0.1.8 or later are enabled as installed.
- The equipment you want to reach must be switched on and connected to the same local network as the host.
- The equipment must have a web page (HTTP or HTTPS).
- To log in to the equipment, you need its username and password.
- A current web browser that allows TechAlert to open a new tab.

> **NOTE** Cameras without the Tech-Connect ACAP do not support Device Forwarding until it is installed. The latest ACAP is available from the PXE server at 192.168.240.5.

5. LIMITS

- Web pages only (HTTP and HTTPS). Other connection types, such as SSH or video streams, are not supported yet.
- Local network addresses only, on the networks and ports below. Names and public internet addresses are not accepted.

Network	Addresses	Ports
`192.168.0.0/16`	192.168.x.x	80, 443
`10.0.0.0/8`	10.x.x.x	80, 443
`172.16.0.0/12`	172.16.x.x to 172.31.x.x	80, 443

- A connection closes by itself after 5 minutes without use. Open it again when you need it.
- A connection only works from the network you opened it on. If you change network, for example by switching to a phone hotspot or turning a VPN on or off, open it again.
- Up to 12 device buttons are shown per host.

6. KNOWN ISSUES

- Some equipment sends the browser to a different address after its page loads, and the connection is lost. The browser then shows an address without the number after tech-connect.ai. Ask your administrator to add a start page to that device's button (see Device Buttons for Administrators).
- Equipment that only answers on HTTPS does not load when opened as HTTP, and the other way round. If a page does not load, try the other type.

© 2026 Vetted Security Solutions. All Rights Reserved.

7. HOW TO USE DEVICE FORWARDING

OPEN THE DEVICE FORWARDING PANEL

1. Log in to TechAlert.
2. Open the **Tech Connect** page from the main menu.
3. Find the host. You can type part of its name in the search box at the top of the list.
4. Check the host's status. It must read **Ready** or **In use**.
5. Click **Device Forwarding** on that host's row. A panel opens inside the row (see Figure 1).

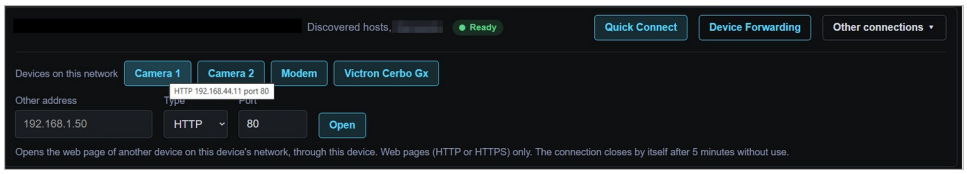


Figure 1. A host row on the Tech Connect page

Shortcut: You can also click a host's name on a dashboard or map and choose **Connection Options** from the device card. TechAlert opens the Tech Connect page with the panel already open for that host (see Figure 2).

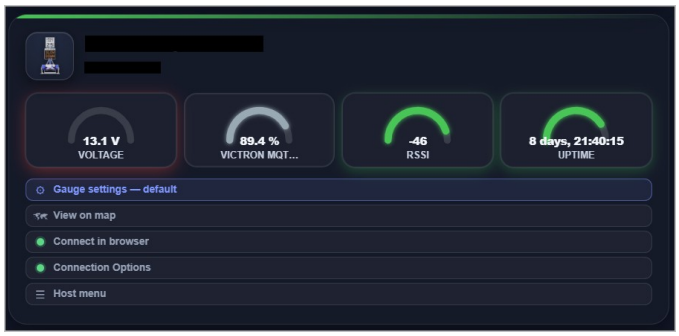


Figure 2. Connection Options from the Dashboard

CONNECT WITH A DEVICE BUTTON

If your administrator has set up device buttons for this host, they appear at the top of the panel under **Devices on this network** (see Figure 1). This is the quickest way to connect.

1. Click the button named after the equipment, for example **Cerbo GX**.
2. Wait a few seconds. The row shows "Opening the connection…".
3. The equipment's web page opens in a new browser tab.
4. Log in to the equipment as you normally would. TechAlert does not store or enter its password.

Tip: Hold the mouse over a device button to see the address, port and type it will open.

CONNECT TO ANOTHER ADDRESS

Use the fields in the panel when the equipment has no button. You need the equipment's local address, for example from the site's network diagram.

1. In **Other address**, type the local address of the equipment, for example 192.168.44.50. On a host without device buttons this field is named **Address on the device's network**.
2. In **Type**, choose **HTTP** or **HTTPS**.
3. In **Port**, keep the suggested port (80 for HTTP, 443 for HTTPS) unless the equipment uses a different one.
4. Click **Open**.
5. The equipment's web page opens in a new browser tab.

© 2026 Vetted Security Solutions. All Rights Reserved.

WHAT TO EXPECT AFTER CONNECTING

- The row shows the address that was opened and a link. If your browser blocked the new tab, click the link.
- The connection stays open while you use it and closes by itself after 5 minutes without use.
- Opening the same address again within that time reuses the same connection.
- You can have several forwards open at once, and they do not close your other connections to the host.
- Every Device Forwarding attempt is recorded in the TechAlert audit log with your user name, the host and the address opened.

8. TROUBLESHOOTING

When a connection cannot be made, TechAlert shows a short message and a reference such as TC-7F4AD1. Give that reference to support; it identifies the full reason in the audit log.

What you see	What it means	What to do
The **Device Forwarding** button is missing	You reach this host through a map only, or Device Forwarding is not set up on this server.	Ask your administrator for access to the host.
The **Device Forwarding** button is grayed out	The host is offline or not enrolled in Tech-Connect.	Check the host's power and internet connection, then reload the page.
"That address did not answer from this device."	The host could not reach the equipment at that address and port.	Check the address, the port and the type. Confirm the equipment is powered and connected.
"This device does not allow connections to that address."	The host's Tech-Connect agent is set to refuse that address.	On a Windows or Linux host, ask an administrator to enable Device Forwarding on it (see Enable Device Forwarding on Windows and Linux Hosts). Otherwise contact support with the reference.
"This device could not be found in Tech-Connect."	The host is not enrolled in Tech-Connect under its TechAlert name.	Contact support with the reference.
"The connection to this device could not be made."	Any other failure.	Try again once. If it repeats, contact support with the reference.
"Only addresses on a private network can be opened…"	The address typed is not a local network address.	Use the equipment's local address (see Limits).
The new tab shows "[403] … Access rejected by ACL"	You are on a different network from the one you opened the connection on.	Open the connection again from your current network.
The new tab does not load, or shows an address without a number after tech-connect.ai	The connection closed after 5 minutes without use, or the equipment redirected the browser.	Open it again. If it happens every time, see Known Issues.
No new tab opens	The browser blocked the pop-up.	Click the link shown in the row, and allow pop-ups for TechAlert.

9. ENABLE DEVICE FORWARDING ON WINDOWS AND LINUX HOSTS

IMPORTANT Device Forwarding on Windows and Linux hosts is not in production yet.

This section is for TechAlert administrators and installers. Camera hosts that run the Tech-Connect camera application (ACAP) version 0.1.8 or later can use Device Forwarding as installed. Windows and Linux hosts cannot: their Tech-Connect agent (RPort) is installed so

© 2026 Vetted Security Solutions. All Rights Reserved.

that it only connects to the host itself. Until the agent's configuration file is changed, a Device Forwarding attempt through one of these hosts is refused with "This device does not allow connections to that address."

Enabling a host has two parts. This section covers the first, which is done once on each Windows or Linux host. The second, device buttons, is optional and is covered in Device Buttons for Administrators.

THE SETTING

The agent's configuration file has a setting named `tunnel_allowed` in its `[client]` section. It lists the addresses and ports the host is allowed to connect to. A Windows or Linux host is installed with this line:

```
tunnel_allowed = ['127.0.0.1:5901', '127.0.0.1:3389', '127.0.0.1:22']
```

Change it to the line below. It keeps the three entries the host already has and adds six local network entries:

```
tunnel_allowed = ['127.0.0.1:5901', '127.0.0.1:3389', '127.0.0.1:22', '192.168.0.0/16:80',
'10.0.0.0/8:80', '172.16.0.0/12:80', '192.168.0.0/16:443', '10.0.0.0/8:443',
'172.16.0.0/12:443']
```

Entry	What it allows
`127.0.0.1:5901`, `127.0.0.1:3389`, `127.0.0.1:22`	The host itself: Quick Connect, VNC, RDP and SSH. Already present. Keep them.
`192.168.0.0/16:80`, `192.168.0.0/16:443`	Web pages (HTTP and HTTPS) on equipment with a 192.168.x.x address.
`10.0.0.0/8:80`, `10.0.0.0/8:443`	Web pages (HTTP and HTTPS) on equipment with a 10.x.x.x address.
`172.16.0.0/12:80`, `172.16.0.0/12:443`	Web pages (HTTP and HTTPS) on equipment with a 172.16.x.x to 172.31.x.x address.

IMPORTANT Add the six new entries to the host's existing line. Do not copy the camera's whole line onto a Windows or Linux host. The camera's line does not contain the 5901, 3389 and 22 entries, so Quick Connect, VNC, RDP and SSH would stop working on that host.

WHERE THE CONFIGURATION FILE IS

Host type	Configuration file
Linux	`/etc/rport/rport.conf`
Windows	`C:\TechAlertScripts\RPort\rport.conf`

Check the path on the device: These are the locations used by the current TechAlert installers. A host installed with an older installer, or by hand, may keep the file somewhere else. Confirm the file exists before you edit it.

ENABLE A LINUX HOST

1. Open a terminal on the host with an account that can use sudo.
2. Make a backup copy of the file: `sudo cp -p /etc/rport/rport.conf /etc/rport/rport.conf.bak`
3. Open the file in an editor: `sudo nano /etc/rport/rport.conf`
4. In the `[client]` section, find the line that starts with `tunnel_allowed`. Ignore lines that start with `#`; they are examples.
5. Replace that line with the new line shown under The Setting. If there is no such line, add the new line directly under `[client]`.
6. Save the file and restart the agent: `sudo systemctl restart rport`
7. Open the Tech Connect page in TechAlert. The host goes offline for a few seconds, then its status returns to **Ready**.
8. Click **Device Forwarding** on the host's row and open a device on its network to confirm.

© 2026 Vetted Security Solutions. All Rights Reserved.

ENABLE A WINDOWS HOST

1. Log in to the host with an administrator account.
2. In File Explorer, copy `C:\TechAlertScripts\RPort\rport.conf` to `rport.conf.bak` in the same folder as a backup.
3. Start Notepad with **Run as administrator** and open `C:\TechAlertScripts\RPort\rport.conf`.
4. In the `[client]` section, find the line that starts with `tunnel_allowed`. Ignore lines that start with `#`; they are examples.
5. Replace that line with the new line shown under The Setting. If there is no such line, add the new line directly under `[client]`.
6. Save the file. Open PowerShell with **Run as administrator** and restart the agent: `Restart-Service rport`
7. Open the Tech Connect page in TechAlert. The host goes offline for a few seconds, then its status returns to **Ready**.
8. Click **Device Forwarding** on the host's row and open a device on its network to confirm.

IMPORTANT NOTES

- Keep exactly one `tunnel_allowed` line in the `[client]` section. The agent does not start if the setting appears twice. If the host does not come back online, restore the backup copy and restart the agent.
- Every entry needs an address before the colon. An entry written as `:80` allows port 80 on every address the host can reach.
- Do not delete the line or leave the list empty. The agent then allows connections to any address the host can reach.
- The new line opens ports 80 and 443 only, on 192.168.x.x, 10.x.x.x and 172.16.x.x to 172.31.x.x addresses only. Equipment on another port needs its own entry, for example `192.168.0.0/16:8080`. The same applies to camera hosts.
- Running the TechAlert installer or the Lockdown script on the host again puts the original line back. Repeat these steps afterwards, or set the `RPORT_TUNNEL_ALLOWED` variable to the full list before running the script.
- If you restart the agent through Tech-Connect itself, the session you are using is cut off. The host reconnects within about a minute. If it does not, restart the agent on the device.
- This setting lets every TechAlert user with access to the host open web pages on that site's local network. Enable it only on hosts where that is intended.

10. DEVICE BUTTONS FOR ADMINISTRATORS

This section is for TechAlert administrators. Device buttons are created with macros on templates, so every host that uses a template gets the buttons for its equipment automatically. Users need no extra setup.

THE MACRO

One macro creates one button. The text in quotes is the button's name, and the value is the address to open:

```
{$TC.FORWARD:"Cerbo GX"} = https://192.168.44.10:443/gui-v2/
```

Part	Example	Rules
Button name	Cerbo GX	Up to 40 characters. Each name is a separate button.
Type	`https`	`http` or `https`.
Address	`192.168.44.10`	A local network address in numbers. No names.
Port	`443`	Required. Must be a port the host allows, currently `80` or `443` only.
Start page (optional)	`/gui-v2/`	The page to open on. Letters, numbers and `.` `_` `~` `/` `-` only, up to 100 characters.

ADD A BUTTON TO A TEMPLATE

1. Go to **Data collection** → **Templates** and open the template for that equipment, for example the Victron Cerbo GX template.
2. Open the **Macros** tab and click **Add**.

© 2026 Vetted Security Solutions. All Rights Reserved.

3. In **Macro**, enter `{$TC.FORWARD:"Cerbo GX"}` with the name you want on the button.
4. In **Value**, enter the address, for example `https://192.168.44.10:443/gui-v2/`. Leave the type as **Text** (see Figure 3).
5. Click **Update**.
6. Reload the Tech Connect page. Every host that uses the template now shows the button.

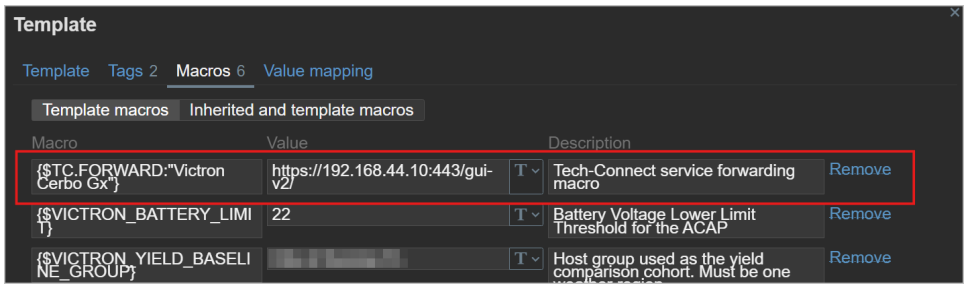


Figure 3. A device button macro on a template

ONE HOST WITH A DIFFERENT ADDRESS

Add the same macro on the host itself (**Data collection** → **Hosts** → **the host** → **Macros**) with that host's address. The host's value replaces the template's value for that host only.

REMOVE A BUTTON FROM ONE HOST

Add the same macro on the host with the value `-` (a single dash). That host no longer shows the button, and other hosts are not affected (see Figure 4).

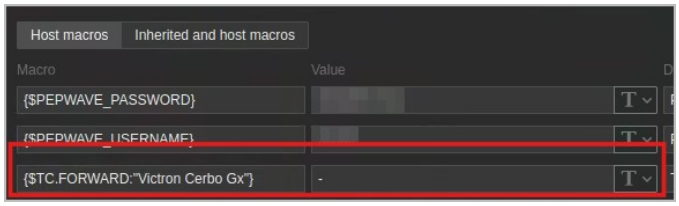


Figure 4. Removing the device button by changing the macro's value

HOW TECHALERT CHOOSES THE VALUE

Where the macro is set	Result
On the host	Used first. Replaces any template value.
On a template the host uses	Used when the host has no macro of that name. With templates inside templates, the closest one to the host is used.
On the host, with the value `-`	The button is removed for that host.
As a global macro	Not used. Device buttons come from hosts and templates only.

IMPORTANT NOTES

- Use **Text** macros. Secret and vault macros are ignored.
- A value that breaks the rules above produces no button and no error message. If a button does not appear, check the value first.
- Write the start page exactly as the equipment ends up on, including the final /. For the Victron Cerbo GX this is `/gui-v2/`.
- Define each device's macro in one template only. If two templates at the same level set the same name, TechAlert picks one of them consistently, but which one is not obvious.
- Buttons are sorted by name and limited to 12 per host.
- To check what a host will show, open the host's **Macros** tab and select **Inherited and host macros**.

© 2026 Vetted Security Solutions. All Rights Reserved.

EXAMPLES

Equipment	Macro	Value
Victron Cerbo GX	`{$TC.FORWARD:"Cerbo GX"}`	`https://192.168.44.10:443/gui-v2/`
Camera	`{$TC.FORWARD:"Camera 1"}`	`http://192.168.44.11:80`
Aetek switch	`{$TC.FORWARD:"Aetek Switch"}`	`http://192.168.44.8:80`

The addresses above are examples. Use the addresses of your own equipment.

© 2026 Vetted Security Solutions. All Rights Reserved.