
PRODUCT SUPPORT

AnyConnect

Updated May 19, 2026



Download data from your connected device/s across a secure, private 4G or LAN network by downloading the AnyConnect App and using the details supplied with every IoT Router.

Latest information

<https://www.csl-group.com/support/any-connect/>

Quick Guide

Downloading and logging into Cisco AnyConnect on a PC

- Open the Microsoft Store and search for “AnyConnect.”
- Download and install the AnyConnect application on your PC.
- After installation, go to Settings → Network & Internet → VPN. Select “Add VPN.”
 - Choose AnyConnect as the VPN provider.
 - Enter a connection name of your choice (e.g. CSL AnyConnect).
 - Enter the server address: <https://remote.cslm2m.com/vpn>
 - Save the configuration.
- Connect to the VPN you just created.
- Enter the username and password as provided on the information sheet accompanying your IoT router.
- The Cisco AnyConnect VPN will then be connected and running in the background on your PC.
- You will have 10 minutes, as standard, before this disconnects.
 - This can be extended, to a maximum of 1 hour, by sending a written request to iotsupport@csl-group.com.

Downloading and logging into Cisco AnyConnect on a Mobile Device

- Go to the Apple App Store or the Google Play Store and download **Cisco Secure Client**.
 - **(iOS)** (<https://apps.apple.com/us/app/cisco-secure-client/id1135064690>)
 - **(Android)** (https://play.google.com/store/apps/details?id=com.cisco.anyconnect.vpn.android.avf&hl=en_GB&gl=US)
- Open the app, click on **Connections** and select: **Add VPN connection**.
- Add a description to help you identify the site.
- Ensure the server address is: **<https://remote.cslm2m.com/vpn>**
 - Or the server address specified on the information sheet provided with the router.
- Go back to the front of the app.

- Click on the white button that says **AnyConnect VPN**, and this will slide to the right.
 - Enter the username and password as specified on the information sheet provided with the router.
 - The VPN connection will then be made, and this will run in the background.
 - Access your device connected to the router as below.
-

Remotely accessing a device via your CSL Router (PC or a Mobile Device)

- Use a browser such as Chrome.
 - Once you are logged into Cisco AnyConnect and running in the background, enter the IP address of the router, followed by a colon, and then the port needed to access the device connected to the router.
 - There are default port forwarding rules on each router, which means all ports are open to 192.168.100.2. Set your device to:
 - IP 192.168.100.2
 - Subnet Mask to 255.255.255.0
 - Gateway to 192.168.100.1
 - You need to know the port that the device needs to use. Use it after the IP address of the router and a colon when you try to access the device via a browser:
 - e.g. 10.xxx.xxx.xxx:80
-

Important Notes

- All ARC-connected routers will need port forwarding set up. However, if you set your device to **192.168.100.2**, all ports are always open by default, so no port forwarding request would need to be made.
- For cloud/P2P devices, no port forwarding will be needed (unless ARC-connected), and you would use the app/service provided with your IoT device.
- Please note that the information sheet provided with the router may say different numbers for those IP, subnet mask and gateway details.
- If your IoT device is not programmed to **192.168.100.2** as the IP, or you need to reach any additional devices on the router, port forwarding rules will need to be set up for those additional devices.
- To request port forwarding amendments or additions, email iotsupport@csl-group.com requesting those to be set up for a specific:

- External port
 - Internal port
 - The IP address of your IoT device.
 - You can access it by logging into AnyConnect, having it running in the background, and using:
 - The IP address of the router.
 - Colon
 - The external port that the additional device is using. E.g. 10.xxx.xxx.xxx:81.
 - You can request a different external port to go to the same internal port that another device connected to the router is using.
 - You may wish to request to alter the LAN range of the router, and/or the “all-ports-open” rule to your referred IP range. If so:
 - Please email: iotsupport@csl-group.com.
 - Additionally, please ensure the router’s default **192.168.100.x** range does not clash with a different network connected to the CSL router. You may wish to request that CSL change the LAN range of the router in these instances.
 - Devices on the router must always use the LAN range, the subnet mask and the gateway of the router (**default 192.168.100.x**) and not another network’s details.
-

IoT Routers

CSL Router

[\(https://www.csl-group.com/support/csl-router/\)](https://www.csl-group.com/support/csl-router/)

CSL Router Pro

[\(https://www.csl-group.com/support/router-pro/\)](https://www.csl-group.com/support/router-pro/)

CSL Router Pro – Industrial Grade

[\(https://www.csl-group.com/support/csl-industrial-router/\)](https://www.csl-group.com/support/csl-industrial-router/)

CSL Router Pro – Wired Only

[\(https://www.csl-group.com/support/router-pro-wired-only/\)](https://www.csl-group.com/support/router-pro-wired-only/)

IoT Router – 4G

[\(https://www.csl-group.com/support/4g/\)](https://www.csl-group.com/support/4g/)

IoT Router – 5G

[\(https://www.csl-group.com/support/5g/\)](https://www.csl-group.com/support/5g/)
