As a secure termination point for all Ursalink devices, UrsalinkVPN offers a reliable, high-efficiency and secure solution for establishing connection between control stations and remote devices, and allows large scale deployment in bulk.
How to use UrsalinkVPN

Install UrsalinkVPN on the server as VPN server and connect your devices to Ursalink routers. As VPN clients, routers and control stations (laptops or other devices) establish connection with VPN server via UrsalinkVPN to enable control stations to access and configure your devices remotely. As a result, VPN real-time data transmission information can be checked on UrsalinkVPN platform.

Application Examples

Smart City
Retail
Industry
Transportation
Agriculture
Branch Office
Key Features

- Establish VPN tunnels quickly
- Secure access and configure devices remotely
- Support multiple control station connections
- A wide range of device management solutions with connected devices up to 1000
- Display real-time VPN connection status
- Simplify setup into a plug-and-go operation

Hardware Requirement

Your host hardware must meet the following minimum requirements:

For 500 devices
- CPU: 2 Cores, 2.0 GHz
- RAM: 16 GB
- Disk: 512 GB
- Bandwidth: ≥100MBps

For 1000 devices
- CPU: 8 Cores, 3.2 GHz
- RAM: 32 GB
- Disk: 1 TB
- Bandwidth: ≥100MBps

Software Requirement

- O/S: Ubuntu 16.04
- Installation package
- Browser: Chrome, Firefox