

Deployment Guide



Table of Contents

1. [Pre-Deployment Information](#)

2. [On-site Prep](#)

3. [Installation Process](#)

4. [Configuration – Uplevel Portal](#)

5. [Service Checks](#)

6. [Setting a Static IP](#)

7. [Troubleshooting](#)



LAN IP schemes for each site

ISP static IP's at any of the sites

Resources currently onsite with Static IP's

- Servers
- Phone Systems
- Printers
- Other

VoIP configurations

- On Prem or Off Prem?
- Server IP's
- Phone IP's and VLAN's

Any DHCP servers onsite

Current configuration of deployed equipment

- VLAN's
- Subnets
- Port Forwarding

Pre deployment Speed Testing

Current Wi-Fi SSID's and Passwords

Plug in the gateway to allow all new firmware updates are complete



Surge protector

Power cable for gateway

PoE injector for Access Point

Ethernet cables

- 1 between ISP modem and Uplevel Gateway

- 1 between Uplevel Gateway and PoE injector

- 1 between PoE injector and access point

- Any other Ethernet cables for wired devices

Cisco Style Serial Cable (for static IP configuration)

Laptop with PuTTY and serial cable Drivers installed (for IP configuration)

Rack Mount shelf or other shelf mount (if applicable)

Access point Mount gear

Login Credentials for the Uplevel Dashboard



Perform a series of speed tests to determine the ISP reliability

This is especially important for VoIP services and QoS configurations

Survey of all existing devices on site

Note the LAN scheme of the ISP modem

Once all important information is noted in the Checklist unplug any existing infrastructure

Plug in the gateway power

Plug the gateway Port 1 into ISP modem LAN Port

Optional Set Static IP via Cisco Style Serial Cable (if needed) (see appendix for instructions)

NOTE the Uplevel Gateway does not require a static IP!

Plug 1 cable from the Uplevel gateway (any open port) to the PoE injector. Plug 1 cable from the PoE injector to the AP. Ensure the injector is also plugged into power.

If using an Uplevel PoE Switch simply plug the AP directly into the switch

Note the AP should be plugged directly into an Uplevel Switch or the Uplevel Gateway through a PoE injector (not into a 3rd party switch)

Wait at least 5 minutes for the gateway and AP to boot up

The Access Point will be the last thing to come online. This is normal!!

Log into the dashboard to watch the gateway come online (appear green)

If the gateway does not come up after at least 5 minutes proceed to the trouble shooting instructions located in the Appendix



Ensure connection to a physical port allows for connection to the internet

Keep in mind it will take about 5 minutes for the gateway to initially come online

It will take anywhere from 2-3 minutes for any configuration changes in the dashboard to get pushed down to the gateway

Proceed to <https://portal.uplevelsystems.com> and then the desired customers configuration page

To change the Customer Name proceed to Site Settings -> Edit Customer

This will change the customer's name in the dashboard as well as any alert emails

To change Internal DNS proceed to Site Settings -> Edit Customer

This is the internal DNS of the gateway. This should follow the form Customer.DomainName.com.

WARNING Inputting the customer website into this field will result in an unreachable website from within the LAN

To change the Site name proceed to Site Settings -> Edit Site

This will change the site name in the dashboard as well as any alert emails

To set the LAN IP scheme proceed to Site Settings -> IP DHCP

Here you can configure the scheme as well as LAN DHCP ranges previously recorded.

Ensure the ISP modem internal IP range does not conflict with the LAN scheme of the Uplevel Gateway. There should be 16 VLANs available for the Uplevel gateway. This means for a /20 network and the site set to 192.168.0.0 the ISP modem should be greater than 192.168.16.0 if it is not in bypass mode.

Setting the Employees network will auto configure the entire site and allow for a flat network configuration. To change this proceed to the advanced option.

Ensure DHCP ranges do not conflict with any existing Static IP's onsite

If you are deploying to multiple sites view the Multi Site option in the appendix to see specific multi site instructions

To create any new VLAN's proceed to the Overview page

Here ensure the Multiple Groups is enabled (located at the very bottom of the screen). From here you may add groups and assign resources to it which will create a VLAN and subnet. This IP scheme can be changed under Site Settings -> IP DHCP -> Advanced

To set any required port forwarding rules proceed to Firewall -> Port Blocking

Here you can add any rules which will punch a hole through the Stateful Port Blocking Firewall.

To configure Wi-Fi SSID's of the Uplevel Access Point proceed to Wi-Fi

To configure all SSID's and Passwords for the Corporate Network proceed to Create SSID's under the Corporate Network box
To configure a Guest Wi-Fi with password and bandwidth restrictions for the Guest Network proceed to Create a Guest SSID
Specify the power levels and channels by going to Wi-Fi-> Configure Access Point

To partition off part of the 1TB NAS by going to Storage -> Add a Drive

To configure backups for these particular drives proceed to Storage -> The Drive in question -> Configure Backup -> Both local and cloud backups can be found here

To configure a VoIP phone system proceed to VoIP -> Edit -> Enable

Here you can select from a predefined list the on prem or off prem service. This will allow the Uplevel to automatically configure the Firewall Rules. These firewall rules can be found under the Firewall tab.

You can also specify the Upload and Download speed limits gathered previously
This will configure a VoIP VLAN and define the QoS based on the input speeds

To configure Ethernet ports to already configured VLAN's proceed to Ethernet

By clicking Edit you can also enable and disable ports as you need
You will see all VLANs (including VoIP) in the drop down list to the right

To configure any Remote VPN Clients proceed to VPN -> Enable -> Add a VPN user

The will require you specify a username, password, and VLAN for the particular VPN Client

To configure Site to Site VPN proceed to Site to Site VPN

This will allow you to specify the VLAN's that you wish to have Site to Site VPN access

To configure Threat Scanning proceed to Firewall -> Threat Scanning -> Enable Threat Scanning

Here you can specify the initial alerting and dropping posture of the deep packet inspection firewall



Connect a device to a physical port on the gateway to ensure connectivity to the internet

Connect a device to an SSID created to ensure connectivity to the internet

Configure a VPN Client to connect remotely

Map a drive onto a machine on the network

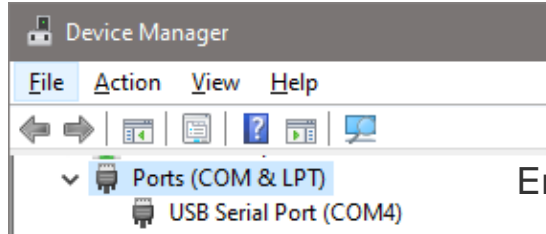
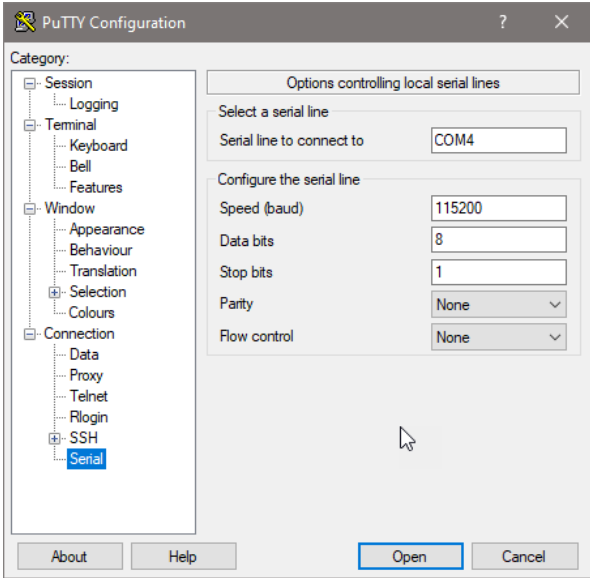
Add a folder to this drive

Ensure VoIP phones are operating as expected

Scan the network to ensure all devices are responding

Devices -> Ping Etc -> Scan Network

Microsoft Windows 10

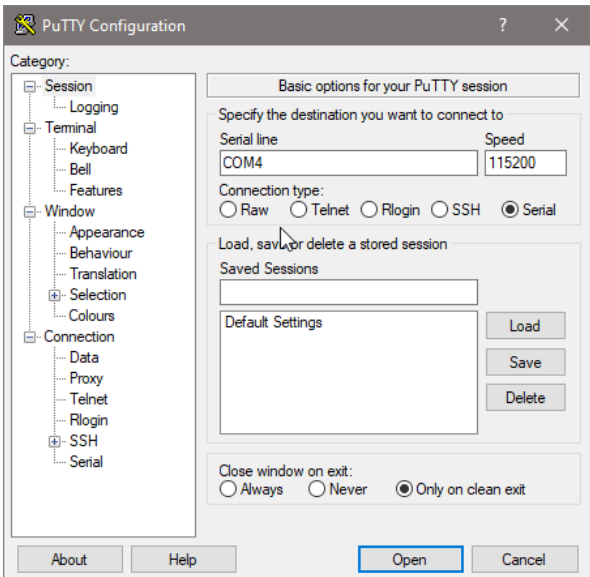


Ensure your computer has PuTTY downloaded (download at www.putty.org)

Ensure you have a Blue USB-to-Serial Port Console Cable

Ensure your computer also has the drivers installed. The Windows Driver is available as a direct download from the manufacturer (FTDICHIP.COM)

- Plug the serial cable into the console port of the gateway and connect to a computer
- Open PuTTY
- PuTTY configuration:
 - Select "Serial" as the Connection type
 - 115200 baud
 - No parity
 - 8 data bits
 - 1 stop bit
 - No hardware flow control
 - Input the serial line defined by your device - COM"X"
 - Open



To locate the COM Port: Device Manager > Ports (COM & LPT) > USB Serial Port (COM"X")

Tip: You can type “help” after any command to see the available options.

```

Please press Enter to activate this console.
Type 'help' for help. You need to reboot to put configuration changes into effect.
> help
Documented commands (type help <topic>):
=====
configure dhcp dig exit help login ping reboot show traceroute
> configure
>CONFIGURE> help
Documented commands (type help <topic>):
=====
exit help password primaryWAN secondaryWAN
>CONFIGURE> primaryWAN
>CONFIGURE>PRIMARY-WAN> help

Documented commands (type help <topic>):
=====
exit help ip

```


Tip: To set the AUX WAN use “secondaryWAN”

Tip: “mode dhcp” will wipe the Static IP on reboot.

Tip: Run “show config” to check your IP configuration

```

Please press Enter to activate this console.
Type 'help' for help. You need to reboot to put configuration changes into effect.
> help
Documented commands (type help <topic>):
=====
configure dhcp dig exit help login ping reboot show traceroute
> configure
>CONFIGURE> help
Documented commands (type help <topic>):
=====
exit help password primaryWAN secondaryWAN
>CONFIGURE> primaryWAN
>CONFIGURE>PRIMARY-WAN> help

Documented commands (type help <topic>):
=====
exit help ip

> configure
>CONFIGURE> primaryWAN

>CONFIGURE>PRIMARY-WAN> ip

>CONFIGURE>PRIMARY-WAN>IP> mode static
>CONFIGURE>PRIMARY-WAN>IP> address XXX.XXX.XXX.XXX
primary>ip>address successfully set to:XXX.XXX.XXX.XXX
>CONFIGURE>PRIMARY-WAN>IP> netmask XXX.XXX.XXX.XXX
primary>ip>netmask successfully set to:XXX.XXX.XXX.XXX
>CONFIGURE>PRIMARY-WAN>IP> gateway XXX.XXX.XXX.XXX
primary>ip>gateway successfully set to:XXX.XXX.XXX.XXX
>CONFIGURE>PRIMARY-WAN>IP> exit
>CONFIGURE>PRIMARY-WAN> exit
>CONFIGURE> exit
  
```

Tip: Run “show config” to view the subnet configuration of the Gateway.

```
> show config
{
  "secondary-ip": {
    "netmask": "0.0.0.0",
    "address": "0.0.0.0",
    "gateway": "0.0.0.0",
    "mode": "dhcp"
  },
  "ip": {
    "netmask": "XXX.XXX.XXX.XXX",
    "address": "XX.XXX.XX.XX",
    "gateway": "XX.XXX.XX.X
    "mode": "static"
  },
  "password": null
}
```



1: Is the status LED GREEN?

- Great! The gateway is online and connected up to the cloud. It may take 5 minutes for all of the services to fully enable. In the mean time breathe. Go check the online dashboard.

2: Is the status LED BLUE or PURPLE?

- All good! The gateway is interacting with the cloud server to pull updates and configurations. Just chill out for a bit until it goes green.

3: Is the status LED RED?

- Not good!
 - Check your ISP gateway and Unbox gateway configuration.
 - Use a laptop to verify that the ISP gateway is configured properly and can get Internet access.
 - Replace cables between the Unbox gateway and the Internet.
 - If none of that works then call support



1: Check the Dashboard... is the customer GREEN?

- Great! The gateway is online and connected up to the cloud. It may take 5 minutes for all of the services to fully enable but it is on!
- Is the AP reporting as Red?
 - That's okay. The AP is the last thing to come online so this will appear as red the longest.
 - If the AP does not come up after 5 minutes ensure that the cables are good and that the AP is connected either directly to the gateway through a PoE injector or an Uplevel switch. Using a 3rd party switch can cause AP connection issues so avoid this!

2: Is the Dashboard customer appearing as RED?

- Is the C' light Green?
 - The gateway is in **Recovery Mode**
 - Is the A' light also Green?
 - Don't worry the gateway has an IP address and is doing a firmware update. This will take about 30 minutes to complete however will come back up on its own afterward. Breathe. To avoid this in the future once the gateway is plugged in do not prematurely pull the power.
- Is the A' light OFF?
 - The gateway HAS NOT received a DHCP IP address.
 - This light will remain off if a static IP is set however if the Status light is also RED ensure that the static has been set correctly and the ISP modem is set into bypass mode. You can set the static IP using a serial cable (instructions on slide 10). After this is complete the gateway will begin booting up (keep in mind if it is also in recovery mode this will take about 30 minutes).
 - There are specific instructions for specific ISP modems. If you are experiencing difficulties please call Uplevel Support for more information about the specific ISP modem.
- Is the Status' light RED?
 - The gateway can not reach the internet. Ensure that the A' light is Green and has an IP address, if not see above.



3: Is the Dashboard appearing as **RED**? (Continued)

- Is the status LED **BLUE** or **PURPLE**?
 - All good! The gateway is interacting with the cloud server to pull down updates and configurations. Just chill out for a bit until it goes green.
- Is the status LED **GREEN**?
 - All good! The gateway is operating properly.
- Is the status LED **RED**?
 - Not good! The gateway does not have internet access. Double check that the gateway has been given a DHCP (Is the A light on?) or that the static IP has been set properly.

Mapping a Drive to a Device



Ensure you are connected to the network either by physical port or SSID and that that connection has access to the drive.

For PC's

Proceed to the File Explorer icon

Select Network

Ensure that Network Sharing is enabled *it may take a minute or two to load all of the devices*

Select the Site desired (by default this will appear as Site 1)

From here you should be able to view all Drives configured on the site

Keep in mind it does take up to 5 minutes for these configurations to work through the system so if it does not automatically appear right away give it a few more minutes.

Once you have ensured that the drive is fully configured on the network proceed to "This PC" seen in the left hand panel

Select Map Drive at the top of the window

From here you can either browse for the device or input the share path.

The share path can be either;

\\VLAN IP\Drive name (this will be displaced under storage on the Uplevel dashboard)

\\Site name\Drive name

For Mac's

Select GO under Finder

Select "Connect to Server"

Input the path of "smb://VLAN IP/Drive name" the VLAN IP can be found under storage of the Uplevel Dashboard

Our Howto for Client VPN (L2TP-IPSEC and SSTP with MFA) is located at our website > Partners > Partner Resources.

[Direct Link](#)



Ensure that the IP Schemes of each LAN do not conflict

The gateway requires a 16 block for each site to account for 9 possible VLAN's so if there are 2 sites it is imperative that their LAN IP's be 16 blocks apart. For example: Site 1: 192.168.0.0 and Site 2: 192.168.16.0

Each site will be configured separately

There are several things that will simultaneously configure across customers:

- VLAN's will configure across the entire customer

- Wi-Fi SSID's and passwords configure across the entire customer

- Threat Scanning Firewall Rules will configure across the entire customer

- VoIP settings will configure across the entire customer