MIDCO BUSINESS®

# Midco Wi-Fi Pro Guide

Get the most out of Midco Business® Wi-Fi Pro with our all-encompassing instructions on using, managing and customizing your business Wi-Fi system through the Midco Business Wi-Fi Pro app.

# Initial Setup and Configuration

# The right connection for your business.

Thank you for choosing Midco® for your business Wi-Fi service. Your Midco Business Wi-Fi Pro is set up and ready to go!

We hope this comprehensive guide is a helpful resource. Inside you will find step-by-step instructions, troubleshooting solutions, advanced setting information, answers to frequently asked questions and so much more.

Your experience matters to us. We are available 24/7. If you have additional questions or need further assistance, contact our business support team at **1.800.888.1300** or **Midco.com/Business/Contact**.

# Midco Business Wi-Fi Pro App

The Midco Business Wi-Fi Pro app is key for managing, using and gaining insights into your Midco Business Wi-Fi Pro system. With your Midco Business internet, strategically placed pods and the app, you can optimize, control and protect your small business.

**Pods**

- Add more pods to your network.
- Remove pods from your network.
- Rename your pods.
- View the connection status and health of your pods.

**Network**

- Adjust Shield features for your network.
- Manage your network from anywhere you have internet.
- Run network speed tests.
- See a dynamic view of your Wi-Fi Pro network topology.

**Users and Devices**

- Change and share your network names and passwords.
- Create and manage user profiles.
- Create your Secure, Guest and Employee zones.
- Manage devices connected to the Secure and Employee zones.
- Pause internet access for your employees or guests.
- Rename connected devices and assign them to employees.
- Set content filters for your employees.
- View the number and data usage of connected devices on your Secure, Guest or Employee zones.
- View when employees return or leave through Keycard.
- View Keycard and Concierge analytics.

**Advanced Settings**

- Manage IP reservations, port forwarding and other router settings.

## Downloading the App

The Wi-Fi Pro app is currently available on the App Store and Google Play.

## Compatibility and Updates

Compatible with most iPhone and Android smartphones. App not working? Make sure you have the latest version installed on your phone, as it is frequently updated. Use the app to set up, access and manage your Midco Business Wi-Fi Pro network.

## Web App

Need to manage your Wi-Fi Pro system on a computer or device without the Wi-Fi Pro app? Visit https://web.workpass.plume.com/.

**Signing in**

Use your initial setup credentials for the web app. The Magic link can also be used if a password was not created.

**Web App Limitations**

- Co-admins (created by the admin) cannot access the web app.
- Not all Wi-Fi Pro mobile app features are available.
- You cannot use the web app to create a new account or location.

# App Features

**Keycard**
This workforce dashboard supports your employees and drives productivity. You can create custom profiles, manage devices, review usage and more.

**Link**
Self-optimizing Wi-Fi technology delivers powerful, reliable connectivity in every workspace and on every device.

**Shield**
Advanced AI security protects your business from cyberthreats with 24/7 network monitoring and autoblocking of malicious content.

**Flow**
Transform motion into valuable business insights. See staff and customer traffic during business hours and get alerts if motion is detected when your business is closed.

**Concierge**
Use guest analytics to improve your customer experience, boost revenue, understand trends, expand touchpoints and predict demand.

**Topology**
Get a dynamic view of your network connections.

- Green globe: Connected to the gateway router, or by Ethernet and acts as the gateway.
- White: Online and has client devices connected to the internet through it.
- Gray: Online but no devices are connected to it.
- Red: Pod is offline.

**In-app Customer Support**
Contact our team from the app!

1. Navigate to the **Settings page**.
2. Tap **Contact us** to send an email, or tap **Call us** to call or send a text.

# Initial Setup and Configuration

## Setting Up Midco Business Wi-Fi Pro

Midco Business Wi-Fi Pro is professionally installed by a Midco technician. But if an issue comes up where you need to reset Midco Business Wi-Fi Pro after initial installation, contact our team. We can send a technician to your business, or you can get more immediate assistance from a business support representative over the phone.

## Creating Your Account and Location

1. Download and open the **Midco Business Wi-Fi Pro app**.
2. Tap on **Set up Plume**.
3. Review the **Terms and Conditions**. Select **Accept**.
4. Enter your **Full Name** and the **Location Name** of your business.
5. Enter your email. Entering a password is optional.
   - If you already have Midco Wi-Fi for your home, you will need to use a different email for your Midco Business Wi-Fi Pro account.
   - You can use the **Magic Link** instead of a password. The Magic Link sends a link to your email every time you need to log into the Midco Business Wi-Fi Pro app.
6. Tap on **Next**. A verification email or Magic Link will be sent.
7. Open the email and tap on **Verify email link**. Open the **Midco Business Wi-Fi Pro app**.

## Connecting the First Pod

Set up varies slightly depending on your network setup and equipment.

1. Plug a pod into your modem, optical network unit (ONU) or router using the included Ethernet cable.
   - This pod will be the gateway pod of your network.
   - Use the Ethernet port marked with a globe to connect to your data access device. This port supports up to a 2.5 Gigabit WAN connection.
2. Plug the pod into an active power outlet. The LED should start to slowly pulse as it finds its connection to the cloud.
3. Restart the modem, ONU or fixed wireless adapter.
   - If you are connecting the pod directly to a modem, ONU or fixed wireless adapter, you will have to disconnect it from power for at least 30 seconds. Once 30 seconds have passed, connect it to power to ensure the pod receives an IP address.
   - Usually, restarting the modem, ONU or fixed wireless adapter again is not necessary when a pod is connected directly into it.

## Setting Up Your Wi-Fi Zones (SSIDs)

SSID stands for service set identifier and is the name of a Wi-Fi network.

1. Enter the **Secure Wi-Fi zone name** and **password**.
   - This zone will be used for anything you want to keep separate from the rest of the network, such as security cameras, point-of-sale systems and file servers.
2. Enter the **Employee Wi-Fi zone name** and **password**.
   - This zone will be used for you and your employees' devices.
3. Enter the **Guest Wi-Fi zone name**. Toggle **Enable Guest Wi-Fi** depending on if you want to offer a guest network.
   - This zone is for your guests and only has Internet access.
   - You can also limit internet usage for your guests.
   - The Guest portal is created after initial setup.

## Connecting All Remaining Pods

1. Place the remaining pods throughout your workspace.
   - Pods should be placed no more than 30 to 40 feet apart.
   - Avoid placing them in areas where they can be easily accessed by your guests.
   - Once a pod is plugged into an outlet, the LED light will slowly pulse while it finds a connection. Stay near the pod until the Midco Business Wi-Fi Pro app confirms the pod has been found.
   - Once successfully connected, the LED will turn off.
2. Tap **All Done** once all pods are active.
3. The pods will download and install any available firmware updates and then reboot. Tap on **Next** to continue.
4. Choose whether you will allow the Midco Business Wi-Fi Pro app to send you notifications. These can be changed later in your phone settings.
5. You will be prompted to join the network.

## Turning Off Your Old Wi-Fi

Remember to turn off your old Wi-Fi to ensure the best performance. If your previous SSID (Wi-Fi network) name and password were used for either the Secure or Employee zones, the devices should connect automatically as soon as the previous Wi-Fi is turned off.

During set up, the app will ask if you turned off your old Wi-Fi network. If you did, you could mark this as **Yes**. If not, it will provide instructions on how to turn it off.

## Additional Configurations

Once initial setup is complete, you can configure the additional features:

- Guest Portal
- Employee Profiles
- Device sharing with employees
- Local DNS server

# Setup FAQs

## How do I turn off the parallel network?

Turning off the Wi-Fi on your existing wireless router will help improve the performance of your Midco Business Wi-Fi Pro network by reducing channel utilization. Turning the old Wi-Fi off will also avoid confusing your devices.

Make sure you are turning off the radios and not just the SSID broadcast.

On some routers and modem-router combination units, there may be a physical switch or button to turn off the Wi-Fi.

1. From a device connected to your non-Midco Business Wi-Fi Pro network, open a web browser and go to your router's web interface.
2. Log in with your username and password. Use the default one provided by the manufacturer or check on the bottom or back of the unit.
3. From the web interface, look for wireless settings. You should have the ability to turn off Wi-Fi radios on the device. This may be required a second or third time – one for each of the radios.
4. After the change has been saved or applied, your router should restart.
5. After disabling Wi-Fi on your other router, your devices should automatically connect to Midco Business Wi-Fi Pro.

If you have any issues, please search the web for instructions for your router.

## How do I set up Midco Business Wi-Fi Pro with my PPPoE connection?

Native support for PPPoE, VLAN or fixed IP is available for pods and pods with Wi-Fi 6 running firmware version 3.4.1.98 or later.

Please contact the Midco support team if you need this option.

Pods must have all configurations removed and you must enter an advanced configuration after the pods are wiped.

## How do I configure PPPoE, VLAN or fixed IP?

During the initial setup process, you can configure pods for PPPoE, VLAN or fixed IP types of connections by using the advanced onboarding flow during setup:

1. Complete the step for Creating Your Account and Location (See page 9).
2. When the Midco Business Wi-Fi Pro app provides instructions for connecting the first pod, select **Other setup options**... (located above the **Next** button).
3. Select **Advanced configuration**.
4. Touch the pod connected to your modem with your phone.
5. Tap on **Set up advanced configuration**.
6. Select the type of connection your ISP supports: **Fixed IP, PPPoE or VLAN**.
7. Enter the required parameters. Contact us if you don't know them.
8. Next you will pair the pod:
   - iOS users will have to **Copy the Bluetooth pin** and enter it in the field located on the following screen.
   - Click on Pair will first check the Bluetooth connection. Then, as the second step, parameters for fixed IP, PPPoE or VLAN settings will be pushed on the Gateway pod.

# Guest Portal Setup

## Guest Portal Requirements

The captive Guest Portal only takes a few minutes to set up, provided you already have a few assets readily available. Here's what you'll need before starting:

- An image or your business logo
    - Less than 1 MB size
    - Less than 100KB and 400x200 to 400x400 pixel size recommended for .png images
    - .gifs, .png and .jpg images permitted
- A text file of the ***Terms and conditions*** for your guest access
- The Midco Business Wi-Fi Pro app
- Optional: Company website
- Optional: HTML color codes for your test and background.

## Setting Up Your Guest Portal

1. Navigate to the **Settings page**.
2. Tap on the **Guest Wi-Fi**.
3. Enter the **Guest Wi-Fi name**, **enable Guest access** and set a **Guest speed limit**.
4. Tap on **Set up guest login portal**.
5. Tap on the **Business info** button.
6. Under **Logo**, use the **Upload** button to upload an image from your phone. If you have a company website, you can use the **Scan website URL** option to automatically search your website for an appropriate photo. Then, use the slider to resize the image.
7. Tap on the fields to enter your **Business name** and **Footer text**.
8. Open the file with your Terms & Conditions copy and paste it into the **Terms & Conditions** field.
9. Scroll up and tap on the **< Back** button. Do not tap on the **Done** button in your browser bar. This will close the browser without saving your changes.
10. Tap on **Login options** and choose the methods you want to be used by your guest(s) when logging into the guest network:
    - **Enable Free Wi-Fi**: Allows guests to log in without providing any information.
    - **Email**: Requires the guest to provide an email address.
    - **Connect with Facebook**: Requires the customer to log in using Facebook Connect.
11. Tap on **Advanced** to change your text color, background color and set a redirect URL.
12. When finished with these options, tap on the **< Back** button.
13. Use the **Preview** button to give your guest portal a try. If satisfied with your selections, tap on the **Publish** button to activate the Guest portal or use the **< Back** button to continue making changes.

## Do guests need a password to log in to the guest network?

Unlike the Secure Wi-Fi zone and Employee Wi-Fi zone, the Guest Wi-Fi zone does not use a password. Guests use a captive portal. When connecting to the guest network for the first time, a guest will be required to accept your Terms and Conditions and choose their email marketing preference before gaining access.

## What do I do if I get a blank screen when trying to set up the Guest Portal?

When setting up the Guest Portal, a new window in your device's default browser should open so you can complete setup. If you are getting a blank screen, go to your browser's settings and clear all the browser data.

## Why can't I upload an image for my Guest Portal?

There are a few possible reasons why an image is not being accepted when creating your Guest Wi-Fi portal.

The file may be too large:

1. Make sure the file you are using is less than 1MB in size.
   - .png images recommended at less than 100KB and 400x200-400x400 pixels in size.
2. The file type is not compatible. The following file types are acceptable: .gif, .jpeg, .png and .x-png.
3. Check if there is a double extension in the filename (e.g., ImageName.jpg.jpg).

# Login and Account Management

## Changing Your Location Name

The Midco field tech will use your billing account number as your location name during installation. You can customize the location name any time after. It is recommended you change your location name before inviting admins to manage your Wi-Fi Pro system.

1. Navigate to the **Settings page**.
2. Scroll down and tap **Account**.
3. Tap on the ⋮ icon next to the location you want to rename.
4. Tap **Rename location**.
5. Enter the new location name and tap on **Save**.

## Signing In by Password or Magic Link

Passwords are not required to sign in. You can have a **Magic Link** sent to your email each time you or an account manager log in.

To use a password, select the small print that says you prefer to sign in by password on the login screen.

## Updating Your Login Password

1. From the login screen, select the small print that says you prefer to sign in by password.
2. Tap **Forgot password**.
3. Follow the instructions to update your password.

## Inviting a New Admin

You can easily invite other managers or supervisors to help you administer your Midco Business Wi-Fi Pro network – without needing to share your own credentials. They can view the status of the network, approve new device connections, restrict access to unrecognized devices, and help manage employees and guests.

1. Navigate to the **Settings page**.
2. Scroll down and tap on the **Account** section.
3. Tap on the **Invite new admin** under your desired location. The invite is to manage a single location only.
4. Enter the **first and last name** and **email** of the person you want to be your new admin. Tap on **Done**.
5. An email invitation will be sent to your new admin containing a single-use Magic Link. Until the invitation is accepted, the admin will be shown as **Invitation pending**.

Once the invitation is received, clicking on the link will prompt the user to download the Midco Business Wi-Fi Pro app if they do not already have it installed. They will also need to accept the terms and conditions to manage the network.

## Secondary Admin Limitations

- Secondary admins cannot invite other admins to manage the network, but they can manage nearly all the tasks needed for their assigned location.
- A secondary admin is not able to approve access or revoke access from other admins including the primary admin.
- Secondary admins must accept the invitation to manage the network. They do not have the ability to login to Midco Business Wi-Fi Pro with a password. If they change their mobile number, the invite will need to be resent.
- Admin access can be revoked by the primary admin at any time.
- The HomePass Web App cannot be accessed by secondary admin. Only the main account owner can access the web app.

# Pod Setup

## Naming Pods

1. Navigate to the Settings page.
2. Tap the ⋮ icon beside the pod you want to rename.
3. Enter your new pod name and tap **Save**.

## Adding Pods

Though this option is available in the app, you will need to contact Midco support to add pods.

1. Navigate to the **Settings page**.
2. Scroll down and select **Pods**.
3. From the Pod section, tap on **Set up new pods**.
4. While the app shows that it is “Looking for pods...”, plug in the other pod(s) or wait for them to connect if you already have them plugged in.
5. When the new pod is added, tap **All done**.

You can now see the new pod added in the **Topology view** of the app.

## Deleting Pods

Though this option is available in the app, you will need to contact Midco support to delete pods.

1. Navigate to the **Settings page**.
   – You can also go directly to the individual pod’s menu by clicking it from the Topology view.
2. Scroll down and select **Pods**.
3. Tap on the ⋮ icon beside the name of the pod you wish to remove.
4. Select **Delete Pod**... and then **Delete Pod** to confirm.

Note: You can add the pod back to your account later or to another Midco Business Wi-Fi Pro account after it has been deleted.

## Enabling or Disabling a Pod’s Ethernet Port

We recommend disabling the Ethernet ports for LAN connections if the pod is physically accessible to guests or employees. Why? Because Ethernet-connected devices are always connected to the Secure zone.

1. Tap the ⋮ icon beside the pod you want to enable or disable.
2. Move the toggle.
3. Select **Disable** or **Enable**.

# Pod Placement

## Placing Pods for Best Performance

When it comes to getting the best performance out of your Midco Business Wi-Fi Pro network, pod placement is everything! While every business has a unique size, shape and Wi-Fi environment, follow our guidelines to maximize your speeds.

We recommend starting with at least one pod for small businesses of 1,000 square feet or less, with an additional pod for every additional 500 square feet of space.

- Place one piece of hardware for every two rooms.
- Spread pods evenly throughout your workspace to maximize performance.
- If your office occupies multiple levels or has several separate, enclosed offices, consider additional coverage.
- Place pods about 30 to 40 feet apart through walls and 60 to 80 feet apart for large open spaces.
- Position pods in central locations along the interior walls of your business to ensure a strong backhaul connection between each other.

Our system measures the performance between each pod and creates the best pod-to-pod connections for you.

## Can I use pods outdoors?

We recommend that you keep your pods inside and away from rain or moisture. If you want to improve Wi-Fi coverage in your outdoor space, we suggest that you place a pod just inside your door.

Avoid placing pods in areas where it is difficult to supervise since any device that is plugged into an Ethernet port will be connected to the Secure zone.

# Pod Connectivity

## Are there tips for improving pod coverage and performance?

**Use your existing Ethernet infrastructure.**

- Your existing Ethernet wiring can provide a reliable connection for your pods. Follow our instructions below when connecting pods by Ethernet.

**Turn off additional Wi-Fi networks.**

- Parallel networks from an upstream router or additional access points increase interference, dramatically decreasing your network's performance.

- If your secondary network shares an SSID and password with your Midco Business Wi-Fi Pro network, devices will often become confused and hop between the two networks, hurting their connectivity.

**Steer clear of furniture.**

- Dense padding and metal and wood framing in furniture can inhibit your Wi-Fi performance. Try placing your pods in open, exposed areas to improve your signal.

- Like mirrors reflect light, they also reflect Wi-Fi signal, decreasing signal strength. Try to position pods to connect around large mirrors and windows rather than through.

**Avoid placement near appliances and equipment.**

- TVs, refrigerators, commercial equipment and other metal objects significantly affect Wi-Fi strength. Avoid placing pods too close to or behind these items.

- Devices like microwaves, cordless phones and industrial, medical or scientific equipment often share the same frequency as your Wi-Fi networks. This can create additional interference when placed too close to your pod.

**Work around the construction of your workplace.**

- Just like mirrors, energy-efficient windows can negatively impact your Wi-Fi signal.

- Metallic blinds and shades can also prevent your network from reaching outside areas.

- Avoid heavy metal doors directly in between your pods – it can severely impact performance.

- Reinforced concrete floors and HVAC ducting may prevent Wi-Fi signals from passing between floors in your workplace. Place pods near stairs where they might have a more direct line of sight between pods on other floors.

**Avoid making your pods physically accessibl to guests.**

- Keep pods out of guests reach or out of commonly used guest areas. Pods are easy to unplug from an outlet and may accidentally get unplugged by a guest looking for an outlet or out of simple curiosity.

- Use outlets that are out of your guests' immediate reach like those closer to the ceiling or behind a counter.

- Connecting a device to the Ethernet ports on a pod will connect that device to the Secure Zone.

## What happens when one of the pods loses power or is unplugged?

If one of the pods happens to lose connection or is unplugged, the system will reconfigure itself so you don't lose connectivity. Another path will be formed using your other pods to maintain coverage and network health. When the pod that lost a connection is restored, it is automatically placed back into the network. The system will self-optimize to incorporate the pod.

## Why are my pods offline?

There are various reasons why one or more of your pods would appear disconnected or offline.

**The entire network is offline.**
If you have received an alert from the app stating your network is offline, follow these steps to bring it back up:

1. Unplug the modem, ONU, or fixed wireless adapter from power for at least 30 seconds.
2. Unplug the Gateway pod from power and unplug anything connected to it by Ethernet.
3. Plug the Ethernet cables back into the Gateway pod and into the modem, ONU or fixed wireless adapter. Plug the Gateway pod back into power.
4. Plug the modem, ONU or fixed wireless adapter back into power and wait until it is fully restarted and its LEDs indicate there is an internet connection.
5. Wait at least two minutes until the Gateway pod's LED stops blinking.
6. If the Gateway pod's LED continues blinking and does not come back online, please contact Midco support.

**Single or a few pods are offline.**

1. The pod is unplugged or is not receiving any power.
   - Check if the outlet has power by plugging in another pod or any other appliance to confirm. When pods are first plugged in, the LED should always turn on solid briefly and then start to pulse slowly as it tries to connect to the cloud. Once connected, it will then turn off. By plugging it back in, you should see a pulse if there is power.
   - If the outlet is controlled by a switch, make sure no one else is turning it off by accident.
   - If the outlet is working and the pod's LED does not come on at all when it is first plugged in, this indicates there is something wrong with the pod. Contact Midco support for assistance.
2. The pod is too far away from any other connected pod.
   - When offline, the LED will slowly pulse as it tries to connect to the cloud. It will continue to do so if it cannot connect.
   - Move the pod closer to another pod or in the same location as a known working pod. The pod should connect, and the LED will turn off.
   - Use the pod health indicator to check signal quality. A poor signal is often the reason for pods intermittently going offline.
   - If it is a range issue, add another pod to your network by contacting Midco support.
3. There may be an unusual issue preventing your pod from connecting to the rest of the network. Contact Midco support if you suspect something unusual.
4. If there is no reason the pod cannot connect to another pod, the pod may be defective. Contact Midco support to confirm and set up getting a replacement.

# Hardwiring Pods and Network Performance

## Does Wi-Fi Pro support Ethernet backhaul?

Yes, you can set up multiple gateway pods by connecting them directly via Ethernet. This will deliver the fastest possible performance to your devices.

The backhaul is the connection between the pods going to your modem and is the core of your network. An Ethernet switch can also be used to further expand how many pods are connected by Ethernet.

## How does hardwiring pods improve the network?

Having Ethernet cabling in your business provides a large advantage in terms of the Wi-Fi speeds you can achieve. When Ethernet is not available, our pods use Wi-Fi to backhaul the network traffic between pods. However, if you have Ethernet in your business, you can connect the pods to the Ethernet jacks in your workplace and that backhaul traffic will travel over the Ethernet cable.

In addition to avoiding potential Wi-Fi signal strength issues between pods, this leaves more airtime available for the rest of the Wi-Fi network and devices for increased Wi-Fi speeds.

Because you are using the Ethernet to backhaul traffic instead of Wi-Fi, you may be able to space the pods a little further apart since their connection to each other is no longer over Wi-Fi. Just make sure you are not creating coverage gaps for your devices.

## Can pods be wired to each other (daisy-chained)?

Yes, you can wire pods to each other in a series of up to two pod-to-pod hops. You cannot wire pods to each other after a wireless hop, which will cause instability.

## What else can I use the Ethernet port for?

If you are not using the Ethernet port for backhaul connections, you can use the port for connections to your wired devices, like a printer or desktop PC. Even if your device is capable of both Wi-Fi and Ethernet, plugging a normally static device into the free Ethernet port of a convenient nearby pod will help free up more airtime for the Wi-Fi connections of other wireless-only devices.

An Ethernet switch can be connected to the pod's Ethernet port to further expand how many devices are hardwired to that pod.

Any device connected to an Ethernet port will always be connected to the Secure zone, so it is important that you place your pods in areas where your guests do not have easy access to them. If you cannot prevent physical access to the pods, it would be a good idea to block the Ethernet ports on the pods.

## What kind of Ethernet cable do you recommend?

You can use any quality Ethernet cable to hardwire your pods, although we recommend CAT 6 or CAT 7 to ensure Gigabit speeds over longer runs.

## Would it be better to connect devices into the pod Ethernet port or over Wi-Fi?

You will enjoy slightly faster speeds on your device when you hardwire them to a pod by an Ethernet cable. Connecting a device to a pod by Ethernet will not negatively impact your network performance. Midco Business Wi-Fi Pro supports Ethernet backhaul, meaning you can now create networks with multiple gateways and pod-to-pod Ethernet connections!

Please note that you may need to power cycle the pod you have connected to your device for Midco Business Wi-Fi Pro to properly recognize and add it to your network.

# Pod LEDs

| Color | LED State | Event | Explanation |
|---|---|---|---|
| Blue | Solid light, then slow pushing | Plugged in and looking to connect to the cloud | When initially plugging any pod into an outlet, the light should always turn solid for a moment. Then, the LED will slowly pulse while it is trying to connect to the cloud. Once connected to the cloud, the LED will turn off.<br><br>If there is no light at all when first plugging in the pod, check your outlet with another appliance or device to ensure it has power. If the outlet is working for other devices, there may be something wrong with the pod. Contact Midco support for assistance. This includes if you notice this behavior happening intermittently. |
| No LED | Off | N/A | There is no problem. The pod is connected, and the internet is working. |
| Green | Quick, repeating double blinking | Waiting for optimization to finish | You can see the “Optimizing your network” message in the app as well. Optimization usually takes two to three minutes, depending on how many pods are connected. Optimizations can be triggered by a change in your environment, such as high levels of interference, but will also happen overnight and immediately after initial setup. |
| | Quick double blinking | During pod naming or renaming | This will last for the duration of the naming process. |
| | Dim to bright slow, continuous pulsing/ breathing | Connecting with the cloud | It could mean:<br><br>– Everything is normal. This occurs after being powered on. The pod will pulse when trying to find a connection to the cloud and then the LED will turn off after it is connected.<br><br>– The pod is not added to your Midco Business Wi-Fi Pro network. The pod will continue to pulse indefinitely if it has not been added to the network.<br><br>– One Wi-Fi-connected pod is already added to your network. The pod is too far away from other pods and needs to be moved closer.<br><br>– The pod is already added to your network and all pods are in the same state. Do not unplug pods. Check the app to see if your pod is connected. You can also confirm there is internet connectivity at the modem or router level and ensure the pod near your router or modem has not been disconnected from the WAN. |
| | Dim to bright to dim pulsing cycle | Claimed by another account | Contact Midco for support. |
| Red | Continuous rapid blinking | Onboarding software issue or fan failure | Contact Midco for support. |
| | Solid or fast blinking | Fan failure | Contact Midco for support. |
| White | Dim to bright to dim pulsing cycle | Internet down or lost cloud connection | Contact Midco for support.<br><br>You can also confirm there is internet connectivity at the modem or router level or follow our instructions for checking your internet connection. Next, check the pod near your router or modem has not been disconnected from the WAN. |

# Router Settings

## Locating Advanced Settings

Advanced settings provide access to network and router features.

1. Navigate to the **Settings page**.
2. **Advanced Settings** can be found near the bottom of the page.

## Networking Mode

Auto is the default mode when you set up Midco Business Wi-Fi Pro. Auto chooses the best network mode for your setup (Router or Bridge).

Router mode will be chosen if the pod is connected directly to a modem, ONU or fixed wireless adapter or router and given a public internet IP. Bridge mode is selected if the pod is connected to a router and receives a private IP. Certain router settings are only visible in the Midco Business Wi-Fi Pro app when in Router mode:

- **DHCP IP Reservation:** Fixes an IP address to a particular client device, enabling you to run applications requiring a fixed IP to function. IP reservations are required to set up Port Forwarding rules.
- **Port Forwarding:** Permits connections from the internet to pass through to a particular IP address in your home network. You need to create a DHCP IP Reservation entry before you can set up Port Forwarding.
- **DNS Configuration:** Allows you to set a custom DNS so you can use a public DNS that is not provided by your ISP or a DNS that has built-in parental and security controls, such as OpenDNS.
- **UPnP:** Enables the devices in your network to be easily discoverable by other devices and applications for data sharing and communication purposes. This feature is on by default, but users may disable it through the app.
- **LAN IP Subnet Configuration:** Allows manual setting of the IP subnet range for the network. Only private IPv4 ranges are possible. These ranges include the following:
  - 10.0.0.x to 10.255.255.x
  - 172.16.0.x to 172.31.255.x
  - 192.168.0.x to 192.168.255.x

In Bridge mode, Midco Business Wi-Fi Pro handles your network's Wi-Fi, while your existing router continues to provide all router functions like DHCP.

**Note:** While you can switch the network mode from Auto to Router Only, forcing Midco Business Wi-Fi Pro to operate as a router when another router already exists can cause issues on your network.

**How does Midco Business Wi-Fi Pro choose what my network mode should be?**
When the network mode in the app is set to either Router Only or Auto (default), pods look at the different characteristics of the IP they are assigned.

In Auto (default setting), pods see if they are receiving a Public IP or Private IP from the equipment upstream to set the realized mode to either Bridge mode or Router mode.

In Router Only, pods look at whether they are getting a different subnet or same subnet from the modem, ONU or router upstream to the LAN IP subnet in the app.

This table shows what the realized network mode will be depending on the app setting in three different setups:

| Setup | Mode (app setting) | IP Range | Network Mode | |
|---|---|---|---|---|
| **Single gateway pod connected by Ethernet** | Router | Different subnet | Router | |
| | | Same subnet | Bridge | |
| | Auto | Public IP | Router | |
| | | Private IP | Bridge | |
| **Multiple gateway pods** | Router | Different subnet | Router (All gateway pods act as routers and have same LAN IP address) | |
| | | Same subnet | Bridge | |
| | Auto | Public IP | Router (All gateway pods act as routers and have same LAN IP address) | |
| | | Private IP | Bridge | |
| **Daisy-chained gateway pods** | | | **First pod** | **Additional pods** |
| | Router | Different subnet | Router | Bridge |
| | | Same subnet | Bridge | Bridge |
| | Auto | Public IP | Router | Bridge |
| | | Private IP | Bridge | Bridge |

This chart is created based on testing network modes on different types of setups.

**How can I set my business network to Bridge mode?**

Bridge mode should be used if there is an existing device that is already handling DHCP/NAT on your network. Pods default to Auto mode. If a pod detects an existing router handling DHCP/NAT, it will self-configure into (Auto) Bridge. If no DHCP is detected, it will switch to Auto (Router) mode.

When Midco Business Wi-Fi Pro is set in Router Only mode, your hardwired pod acts as a router and DHCP server. Multiple DHCP servers on the same network can cause duplicate IP assignments, leading to network instability and other issues.

Follow these steps to switch back to Auto (Bridge) if the networking mode was set to Router only.

1. Navigate to the **Settings page**.
2. Tap **Advanced settings** near the bottom of the page.
3. Tap **Networking mode**, which will display your network's current mode.
4. Tap **Auto (Router)** and then **OK** on the pop-up screen.
5. A prompt will tell you that your network is restarting. It may take up to 90 seconds for your network to come back up.

**Can I use a local DNS server with Midco Business Wi-Fi Pro?**
Yes, you can use a local DNS server with Midco Business Wi-Fi Pro. If the DNS server is upstream from your network, then it must be set in Router mode even if there already is a router upstream.

**How can I ensure all devices access the local DNS?**
Once you have set your Midco Business Wi-Fi Pro network in Router mode, you will also need to change the DNS servers in the Midco Business Wi-Fi Pro app to reflect your local DNS servers. All devices in all zones should now have access to the internet.

**How do I set a custom DNS?**
You can set up custom domain name system (DNS) settings using the Midco Business Wi-Fi Pro app if your network is operating in Router mode. If your network is operating in Bridge mode, you will have to set up a custom DNS using your router's configuration settings.

1. Navigate to the **Settings page**.
2. Scroll down and open **Advanced Settings**.
3. Under **DNS**, select **Custom DNS**.
4. In the DNS fields, enter the desired DNS in the Primary and Secondary server fields respectively.
5. Tap **Done**.

## UPnP

**What is UPnP?**
UPnP allows a device or service to automatically configure the needed port settings on the network address translation (NAT) required to communicate properly with other devices and servers. Without UPnP, port forwarding rules will have to be set on the router manually, which becomes tedious if you need rules for multiple devices and/or services.

**How do I enable UPnP?**
If you are running Midco Business Wi-Fi Pro in Bridge Mode and have a separate router, you can usually find the UPnP setting in the router's firewall or NAT settings. In Router mode, you can turn on the UPnP by:

1. Navigate to the **Settings page**.
2. Tap **Advanced Settings** towards the bottom of the page.
3. Scroll down and slide the UPnP toggle to the right.

## Port Forwarding

Port forwarding (opening ports) allows you to open specific ports in the router's firewall that are needed by some services to communicate to devices on your network. A port has an internal and external value called the port number. Multiple external hosts can use the same external port number, but each internal port must be different. This allows network address translation (NAT) to identify the destination for inbound traffic.

Port forwarding is necessary when you are having issues related to a restricted NAT.

**Where do I find Port Forwarding settings?**

UPnP allows services to automatically set up port forwarding rules, although you can also manually set up port forwarding. Manual setup can be tedious if you are setting rules for multiple services and multiple devices. You should not enable UPnP and set up port forwarding at the same time.

Because you are opening/forwarding ports in the firewall, this setting must be set in the router. If in Bridge mode, you will need to set up port forwarding rules in your router. If you are in Router mode, port forwarding can be set up in the Wi-Fi Pro app:

1. Navigate to the **Settings page**.
2. Tap **Advanced Settings** near the bottom of the page.
3. An IP reservation needs to be set for the device before ports can be opened. Tap **Reservations & Port Forwarding**. Complete the steps to create a New UP reservation if needed.
4. Once your IP reservation is created. From the IP reservation, tap on **Open Port**.
5. Enter a **name** for the rule. Each name needs to be unique.
6. Enter the **External port number** the service requires.
7. Enter the **Internal port number** to be used on the device.
   - Use the same number as the external port to open the port or another number to route the traffic to a different port.
8. Choose the required **Protocol**.
9. Tap on **Save**.
10. Repeat these steps for each rule needed.
    - If the external port has already been used for one service, it is not necessary to set it again for a different service on the same device
    - The external port number for each rule can be the same, but the internal port number must always be unique. This means you will need to choose another internal port number for each local device.

## Static IP

**What is a static IP?**

While most cases do not require a static IP, it is possible to reserve a static IP address for your devices in the Midco Business Wi-Fi Pro app.

By default, devices use dynamic IP addresses assigned by the network upon a connection that can change over time. In contrast, static IP addresses do not change. This can be useful when a device, website, application or service needs to remember the IP address of the device.

**How can I reserve a static IP for a device?**

Your network must be in Router mode to reserve an IP using the Midco Business Wi-Fi Pro App. If you are in Bridge mode, this feature must be configured through your router's settings.

1. Navigate to the **Settings page**.
2. Choose **Advanced Settings** towards the bottom of the screen.
3. Tap on **New IP Reservation**.
4. Select your desired device.
5. If desired, you can edit the name and IP address of the device or simply tap **Done**. Your device should now be assigned to the new static IP. If you want, you can now set up port forwarding.

## Static WAN IP

Pods are currently unable to be configured with a static WAN IP. For ISP connections that require a static WAN IP, you will need to keep your existing router and operate Midco Business Wi-Fi Pro in Bridge mode.

# Online Protection Through Shield

Enabling the Online Protection feature in Shield safeguards your devices from malware sites, botnets, spyware, spam, phishing, keyloggers, monitoring, proxy avoidance, anonymizer and other harmful attacks on your network.

## Turning On Online Protection

The Online Protection feature is enabled on all devices connected to your Midco Business Wi-Fi Pro network by default, but it can be customized on the device or employee level for a more individualized experience.

- When enabled for an employee, Online Protection is set automatically for all devices assigned to that person.
- Online protection can be controlled at the network level through the Shield feature, which is found in the Settings menu in the Midco Business Wi-Fi Pro app.
- Device and employee settings can be modified from within their respective detail screens. To provide online protection to guests, Online Protection must be enabled at the network level.

Content is restricted by our security feature whenever you see:

- HTTP sites: An on-screen message stating, “Access to this website is blocked.”
- HTTPS sites: An on-screen message with the browser’s default “can’t be reached” message.

## How Shield Protects Users and Guests

When Shield features, such as Online Protection and Content Access, are applied at the network level, all devices connected to your Midco Business Wi-Fi Pro network will be protected – including your guests. There is no way to provide protection to only your guests without applying the same protection to your Secure and Employee zone devices.

| Shield Feature | Network Level (Guest, Secure and Employee) | Employee Level | Device Level (Secure and Employee) |
|---|---|---|---|
| Content Access | ✓ | ✓ | ✓ |
| Online Protection | ✓ | ✓ | ✓ |
| Advanced IoT Protection | ✓ | | |
| Adblocking | ✓ | ✓ | ✓ |

## Applying Shield Settings at the Network Level

1. Navigate to the **Settings page**.
2. Scroll down to the **Shield section** and tap on the feature you wish to enable. – Any feature with **Custom** beside it has rules applied at either the device or employee level.
   - Anything displaying **On** is already enabled at the network level.
   - Advanced IoT protection is network level only.
3. Turn on the feature and tap on **Overwrite**.
4. It will now be displayed as **On**.

# Shield FAQs

## What kinds of sites are blocked by Content Access?

Content Access can be used to allow users to only view work-appropriate content. Enabling the Content Access feature prevents users from accessing domains that may add potential liability to your business.

The Content Access feature can be enabled at the network level, employee level or at the device level (Secure and Employee zones).

## What kinds of network activity does the Shield security features monitor?

Our security features have been designed with a privacy-first mentality, ensuring you have effective protection against today's threats while also respecting your users and their data privacy.

Since security-related features inherently require more information to protect your devices, users are in full control of enabling, disabling and customizing the features. Shield features monitor for device network metadata such as DNS, IP address and packet sizes. It does not inspect any data packets or break open any SSL-protected connections, meaning your privacy is preserved.

## How can I know Advanced IoT Protection is working?

If the feature is enabled, all your devices are being protected, even if you do not see any blocked events on your network! Advanced IoT Protection continually monitors and stops threats to your network. If a threat is detected, you are immediately notified.

# Access Zones

Midco Business Wi-Fi Pro has three different access zones to ensure the safety of all the devices connected to your network: Secure zone, Employee zone and Guest zone.

A separate service set identifier (SSID) is used to access each zone.

## Choosing the Best Access Zone for Each Device

All access zones provide internet access, although the local access requirements and your business needs determine which zone should be used for each device.

**Secure Zone**
The Secure zone is meant for devices that require the most protection. Devices connected to the Secure zone can access each other over the local network but cannot be accessed by devices connected to either the Employee zone or Guest zone by default.

All Ethernet-connected devices are also automatically placed in the Secure zone. This is ideal for devices that require extra protection, such as:

- Point of sale (POS)
- Security cameras, network servers and other security equipment
- IoT devices

Devices in the Secure zone can access each other over the local network; however, you can block new devices connecting to the Secure zone from all local access without manual authorization.

If you have resources on the network that you wish to share over the network with select employees, they can also be placed in the Secure zone.
This includes:

- Printers
- File servers and network-attached storage (NAS)
- Smart displays and other network-attached media devices

Secure zone devices can be grouped to make access sharing easier.

**Employee Zone**
The Employee zone is meant for your employees' devices. This allows you to manage their access to any shared resources on the Secure zone. And with Keycard, you can access device-usage analytics and review timecard data to help with future scheduling and increase workplace productivity.

**Devices to keep on the Employee zone:**

- Employee laptops
- Employee mobile phones
- Employee tablets and smart devices

All devices connected to the employee SSID (service set identifier) have local network access to each other.

Each employee can have customized local network access to specific Secure zone devices. Online Protection, Content Access and Adblocking can also be customized at the individual employee level.

You can also block all local network access to any new devices connecting to the Employee zone until you manually approve access.

**Guest Zone**
This zone is meant strictly for your guests. Your guests will use a custom guest portal when connecting to Guest Wi-Fi. The Guest Portal can be customized with your company name, image, terms and conditions to provide a branded experience. And multiple login options are available for the Guest Portal – so you do not have to worry about setting up a password.

All devices connected to the Guest zone only have internet access with no local network access. It is not possible to share any local network resources (like printers) with guests.

Only screen-enabled devices, such as mobile phones, tablets, and laptops, can connect to the Guest zone because they need to sign-in using the Guest captive portal, which is required every 24 hours.

You can also limit the internet speed for people on the Guest zone. That way you don't need to worry about guests slowing down your employees or the rest of your business.

Best of all, Concierge turns guest analytics into opportunities for your business. React to visit frequency, data usage, length of stay and more.

## Updating Access Zone Names

Navigate to the **Settings page**.

Tap the **>** icon next to the network you wish to edit (Secure Wi-Fi, Employee Wi-Fi or Guest Wi-Fi).

Tap on the **pencil** icon and enter the new name. The name used must be different from the Secure and Guest zones.

## Updating Access Zone Passwords

1. Navigate to the **Settings page**.
2. Tap the **>** icon next to the network you wish to edit (Secure Wi-Fi, Employee Wi-Fi or Guest Wi-Fi).
3. Tap the ⋮ icon next to Wi-Fi password.
4. Tap **Edit**.
5. Update the password and tap **Save**.

Any devices using the previous password will need to be updated with the new password. The **Copy** option lets you copy and paste the new password in an email for your employees.

# Secure Zone Support

## Device Groups

- Device groups make it easier to share local access to multiple devices in the Secure zone at the same time with your employee(s).
- Device groups in the Secure zone help organize devices but do not designate local network access within the zone.
- Once a device is blocked, all group assignments will have to be redone once it is unblocked.
- A device cannot be added to more than one group at a time. Although while in a group, a device can still be shared with employees as an individual device if needed.

## Creating Device Groups

1. Navigate to the **Secure zone**.
2. Tap on the **+** icon at the top right of the **Secure zone screen** and then select **Create a device group**.
   - You can also create the group directly from a device by tapping on the ⋮ icon next to the device and then selecting **New group**...
3. Enter the new name for the group and tap **Save**.
4. Tap on the ⋮ icon next to the device you want to add to the group and then tap **Change group**...
5. Choose a group and then tap the **<** icon to finish.
6. Repeat the last two steps as needed to add more devices to the group.

## Secure Zone Devices

- All devices connected to the Secure zone have local network access to each other unless they are in an unapproved state or are blocked.
- When **Limited access for new devices in the Secure zone** is enabled, unapproved and blocked devices will need to be approved before being shared.
- All Ethernet devices are added to the Secure zone automatically. If the pods and Ethernet ports are easily accessible by unauthorized people, it is imperative to enable **Limited access for new devices in the Secure zone**.
- Device groups in the Secure zone help organize devices but do not designate local network access within the zone.
- Devices connecting to the Secure zone are recognized based on their MAC addresses, so it is imperative that any devices you connect to the zone do not use a private address (random MAC address) to maintain their sharing settings.
- Secure zone devices or device groups can be shared with specific employees, providing local network access between Secure zone devices and designated employee devices. There is no way to share access with guests.

## Sharing Secure Zone Devices with Employees

1. Navigate to the **Secure zone**.
2. Tap on the ⋮ icon next to the **Device** or **Device group** you wish to share. Unapproved devices must be approved before being shared.
3. Tap on the **Share access**... option and then choose the employee or specific device you want to have access.
4. Tap **Done** to save.

## Limiting Network Access for New Devices in the Secure Zone

Midco Business Wi-Fi Pro can limit network access for any new devices that connect to the Secure zone. When enabled, this feature blocks local network access for all new devices until manually approved.

Unrecognized devices will still connect but only have access to the internet until approved. This protects your network if the password for the Secure zone SSID becomes compromised.

## Enabling Limited Network Access to New Devices

1. Navigate to the **Settings page**.
2. Tap on the **Secure Wi-Fi** to bring up the additional options.
3. Slide the **Limited network access for new devices** toggle to On.

## Blocking Devices

1. From the **Secure Zone**, navigate to the **Devices** section.
2. Tap **View all**. This will take you to a new screen.
3. Tap the ⋮ icon next to the device you want to block from the list.
4. Select **Block device** from the list. That device will move to your **Blocked Devices list**.

## Approving Blocked Devices

1. From the **Secure Zone**, navigate to the **Blocked devices** section.
2. Tap the ⋮ icon next to the device you want to approve.
3. Select **Approve device** from the list.

## Adding a Blocked Device Back to Its Group

When a **Secure Zone** device is blocked, it is automatically removed from its assigned group. Once the device is unblocked, it will need to be added back to its previous group to resume being shared with employees as part of the group.

1. From the Secure Zone, navigate to the **Blocked devices** section.
2. Tap on the ⋮ icon next to the device you wish to unblock and tap on **Approve device**.
3. Find the device in the **Approved devices** list and tap on the ⋮ icon next to the device.
4. Tap on **Change group...** and select the group.

Once back in the group, the device will be accessible again to employee devices that already have access to that group of devices.

# Employee Zone Support

## Adding an Employee

1. Navigate to the **Employee zone**.
2. Tap on the **+** icon in the top right corner of the **Employee zone detail screen**.
3. Select **Add employee**.
4. Type in the person's name.
5. You can choose a profile image or tap on the **camera** icon to take a photo or access your phone's photos.
6. By default, **Content access**, **Online Protection** and **Ad Blocking** settings will be inherited from the network-wide settings, although you can choose custom settings for the person and their assigned devices.
7. Under **Assign devices,** select the devices that belong to that person.
8. Tap on **Next** and then choose that person's **primary device**. The connection status of the primary device indicates when the employee is at work. That's why it's important to choose a device they keep on their person.

Once a device is assigned to an employee, it is automatically removed from the **Unapproved devices** list.

## Deleting an Employee

There's no need to change the Employee Wi-Fi password if an employee leaves. Midco Business Wi-Fi Pro makes it easy to manage a former employee's access without having to make major changes to the network to keep it secure.

1. Navigate to the **Employee zone**.
2. Tap on the employee you want to remove.
3. Tap on the ⋮ icon on the top-right of the employee detail page.
4. Tap on **Remove person**. A prompt will remind you that all historical data consumption for that person will be deleted.
5. Tap on **I understand** to confirm.
6. Another prompt will give you the following choices:
   - **Remove and don't block**: All previously assigned devices can still connect to the Employee zone, retain internet connectivity but will lose local access.
   - **Remove and block:** All previously assigned devices will have both local and internet access blocked.

In either case, once a person is deleted any previously shared devices will no longer be accessible even if they still have access to the Employee Wi-Fi password. If that person returns, their profile will have to be created again.

## Employees at Work Feature Not Working

The **Employees at work** feature needs your employees to have a primary device assigned to them.

If you have assigned a primary device to your employee, check for a duplicate of the device in the Employee zone. A duplicate of the device may be because the device is using a private address.

# Guest Zone Support

## Changing the Internet Speed for Guests

You can limit the internet speed available to your guests so they do not impact the internet bandwidth available for your critical business applications or your employees. Guests are allocated a percentage of the average internet speed measured during the last three system's speed tests.

1. Navigate to the **Settings page**.
1. Tap on the **>** icon next to the **Guest Wi-Fi.**
2. Tap on **Limit internet usage**.
3. Choose the **percentage** you wish to allocate for all your guests.
4. Confirm your choice by pressing **OK**.

## Guest Portal User Experience

1. Accept the Terms and Conditions.
   - If they do not accept, the process ends.
2. Choose their email marketing preference.
   - **YES**: The user continues to the login options configured.
1. - **NO**: The user is prompted to **Connect to Free WiFi**.
2. Log in using the available method.
3. They are then redirected based on options configured.

## Email Marketing Preferences

**Choosing yes.**

- Saves the user's email or the Facebook account name and email.
- Information saved in the last 30 days can be downloaded as a CSV through the WorkPass Web App for use in marketing or promotional emails.

**Choosing no.**

- The guest's email is not saved.
- The user is prompted to **Connect to Free WiF**i.

## Guest Portal Historical Data

The **Historical data** feature provides the email addresses, names (Facebook only) and device types for guests that have opted into marketing email during the last 30 days. This information can be downloaded as a CSV from the WorkPass Web App.

- The **Download historical data** button on the mobile app opens the WorkPass Web App in a new browser window.
- The name of the guest will only appear in the CSV if the user has logged in using Facebook Connect.
- Even when Facebook has been enabled, if email is not configured as a login option, you will be prompted to enable email when you attempt to download **Historical data** from the Web App.
- An email is also sent to the account owner with a link to download the data.

# Guest Analytics

## Guests Per Hour Feature

A **Guests per hour** bar graph showing how many guests have connected to your Guest network within the last 24 hours is available on the **Home screen** and **Guest zone**.

– Blue bars: Repeat guests

– Yellow bars: New guests

The device's MAC address is used to recognize a device type. If the random MAC feature is used, some device will show as a new device the second time and may not be typed.

## Popular Devices List

The Guest list found on the **Home and Guest zone** screens shows all current and recent guests who connected to your guest network in the last 24 hours. The most recent connected devices are shown. To see the full device list, tap the **View all** option.

– There is an option to **Download historical data**. On the mobile app, selecting the **Download on the web** button opens the web app in a new browser window.

– The **Popular devices** list displays the total number of devices and how much data has been consumed based on device type from the last 24 hours.

# Guest Zone FAQs

## How long does a guest's login last?

When a guest registers on your Guest Portal, their authentication token lasts for 24 hours. They do not have a session time limit. If the guest's device remembers the network, it will automatically reconnect within this 24-hour period. After 24 hours have passed, the person will need to register to the Guest Wi-Fi using the Guest Portal.

## Can I share network resources like a printer with my guests?

Guests do not have access to any devices on the local network. This means that you cannot share your printer with guests.

## Will guests slow down my employees' internet speeds?

You can limit the speed of your guests' internet connection to a percentage of your total internet speed to ensure you have enough bandwidth left over for your employees and other business needs. The percentage of bandwidth available to guests is based on a percentage of the average of the last three automatic speed tests run by Midco Business Wi-Fi Pro.

## Will my guests be able to access sensitive data or devices on my network?

No, the Guest network is segmented from the rest of your network to ensure your sensitive network is protected. Guests only have a connection to the internet and are not able to connect to any local devices connected to your Midco Business Wi-Fi Pro network.

# Device Issues

## Private (Random) MAC Addresses

Midco Business Wi-Fi Pro supports connections from devices that have enabled MAC address randomization (private address) in all zones.

Through our Advanced Device Typing feature, Midco Business Wi-Fi Pro will still be able to properly recognize devices with a random MAC and assign them to the proper device category and icon. The device brand, name and model should also still be displayed.

## Limitations When Using a Private (Random) MAC Address

Using a private (random) MAC address is a great way to improve privacy, particularly when connecting to guest networks like the one you created in Midco Business Wi-Fi Pro.

Certain features and policies rely on a consistent MAC address on the device to function, which you should keep in mind for devices connecting to both your Secure zone and Employee zone.

These include:

- Employee device assignments and any rules and Midco Business Wi-Fi Pro features associated with those assignments
- Secure device groupings
- Device-level and employee-level Content Access settings and Shield rules
- Sharing rules for devices in the Secure zone
- IP reservations and port forwarding
- Device approvals

In most cases, a device will use the same randomized MAC on saved networks. You can assign devices using a private (random) MAC to employees and set rules without issue.

There could be issues if the MAC changes. Every time a device changes its MAC address, the device will appear as new in Midco Business Wi-Fi Pro. These rules and configurations will need to be applied to the device again. Depending on how often devices rotate their MAC address, it can make maintain the rules you've set a challenge.

| Device Type | Default New Network Connection | Same random MAC used on saved networks? | When does the private (random) MAC rotate? |
|---|---|---|---|
| iOS 14 or later | Random (Private) MAC | Yes | Stays the same even when the network is forgotten |
| WatchOS 14 or later | Random (Private) MAC | Yes | Stays the same even when the network is forgotten |
| iPadOS 9 or later | Random (Private) MAC | Yes | Stays the same even when the network is forgotten |
| Android 10 or later | Random (Private) MAC | Yes | Stays the same even when the network is forgotten |
| Windows 10 | Device MAC | Yes | Changes when network is forgotten or can change every 24 hours (optional) |

## Limiting the Impact of Private (Random) MAC Addresses

- **Set up your rules and assignments based on both the device MAC and private (random) MAC.** Since most devices will use the same private (random) MAC on a network, you can apply the same settings and assignments for both MAC addresses that may be used for the device. Managing devices belonging to your business is particularly easy. The biggest limitation is that there can only be one primary device assigned to an employee.

- **Turn on the Limited network access for new devices feature in both the Secure zone and Employee zone.** This blocks local network access for all devices with an unrecognized MAC that connect to either the Secure zone or Employee zone until approved by you. When asked for approval by your employee, assign the new device MAC to the employee's profile or ask them to use the device MAC address to connect to the network. This feature should always be enabled anyways in case your Wi-Fi passwords are compromised.

- **Have Content Access and Shield rules set up at the network level to ensure the security of all devices connecting to your network.** These rules are set using the Midco Business Wi-Fi Pro app only when operating in Router mode. When operating in Bridge mode, these will set on the router, but an unrecognized MAC address will be the same. IP assignments and port forwarding rules will have to be done again if the device's MAC changes. Other features on your router like MAC filtering will also have issues with unrecognized MAC addresses.

## Disabling Private (Random) Wi-Fi Addresses

Devices using a private (random) Wi-Fi address will connect to your network. To get the best experience and guarantee device-level security and controls, we recommend turning off private Wi-Fi addresses for your home network. Turning off this setting is only for your network and does not impact the use of a private Wi-Fi address on other networks.

# Device FAQs

## What do I do if my device won't connect?

**Wi-Fi Devices**

1. Make sure Wi-Fi on your device is on and that you can see your Wi-Fi network name on your device. If you can't find your Wi-Fi network name, open your Midco Business Wi-Fi Pro app and verify your Wi-Fi network name.
2. Make sure you enter the correct Wi-Fi password if prompted.
3. Check that your gateway pod is connected and functioning. Make sure your pods are online.
4. Turn the Wi-Fi on your device off and then back on. This will force the device to scan for available networks.
5. Restart your device. Some always-on devices, such as thermostats and doorbells, may not connect to the new network without a reboot.
6. Check with your device manufacturer for any special requirements. For example, some devices will not connect to a network if the SSID and/or password have special characters.
7. Reset network settings or forget the old network on your device. If your old Wi-Fi is still broadcasting, your device may be switching between networks.
8. Check whether other devices can connect to the Wi-Fi network. If not, contact Midco support or log in to My Account to see if there are any internet outages.
9. Always make sure that the Wi-Fi on your old router has been turned off. Your device may have difficulty connecting to your Midco Business Wi-Fi Pro network if the old network is still broadcasting. Turning off the old Wi-Fi will also remove a potential source of interference from the environment.

**Ethernet-Connected Devices**

1. If your wired device is not connecting to the network, try power cycling the pod while the device is still connected by Ethernet.
2. Try another Ethernet cable. Ethernet cables can fail, causing poor or unstable connections.

**Settings**

1. Check your router settings. MAC filtering prevents new devices from connecting to your network.
2. Check the dynamic host configuration protocol (DHCP) settings on your router, particularly for limitations. You may not have enough available IP addresses for all your devices and pods.

## What if I cannot find my Wi-Fi Pro network in the Wi-Fi network list on my device?

All network lists on your devices are ordered alphabetically. If you cannot find your network, please check your Midco Business Wi-Fi Pro app and verify your Wi-Fi network name.

Still having issues? Try adding your SSID manually through Wi-Fi settings on the device.

The system currently does not support hiding its SSID. If you still cannot find the network from your device, contact Midco support for further assistance.

## My wireless device did not connect to my Wi-Fi Pro network. What do I do?

**All devices are not connecting.**

1. Use the app to check that your new zone SSID matches your previous SSID.
2. Check that the password also matches what was previously used.
3. Check that the old Wi-Fi on your router or modem-router combination disabled. If not, follow our instructions for disconnecting your old Wi-Fi in the Setup and Configurations section of this guide.
4. If you did not use the same SSID and password of your previous network:
   - Ensure your device settings match what has been set up in the Midco Business Wi-Fi Pro app.
   - Double check your old Wi-Fi is disabled.
   - Check every device has forgotten the old network or you can instead double check your old Wi-Fi is disabled.

**A group of devices is not connecting.**

There are some common reasons that a group of devices may not connect after setup:

1. You previously had separate 2.4 and 5 GHz networks (SSIDs) on your old wireless router.
   - Since you previously had two separate SSIDs, you'll have to check that all your devices have the updated Wi-Fi credentials. If you reused the credentials of one of these SSIDs, devices using the other will need to be updated with new credentials. This is because Midco Business Wi-Fi Pro utilizes a single SSID for both bands in each zone.
   - Likewise, you will need to disable both 2.4 GHz and 5 GHz radios; otherwise, devices will not disconnect from the old network.
2. Certain 2.4 GHz-only IoT (smart home) devices are not connecting to the new Wi-Fi even though the SSID and password match the previous router.
   - There are some smart home devices that use a control app running on mobile for setup, that have an issue connecting to Wi-Fi networks that use a single SSID for both bands like Wi-Fi Pro.
   - These 2.4 GHz-only devices use the BSSID to connect instead of the SSID. Because of this, even if you set up Midco Business Wi-Fi Pro's SSID and password to match the old 2.4 GHz network's password, these devices will not be able to immediately connect.
3. If you are still using your old router, check the dynamic host configuration protocol (DHCP) settings.
   - If there is a limit set on the IP address pool, it will need to increase to accommodate the IPs required for your new pods.

## Why is there a duplicate in my device list?

Individual devices are identified based on the unique MAC address of their network hardware, which normally never changes. However, there are a few possible reasons this MAC address can change.

- **A Different Connection Type**
  Laptops, desktops and other devices that have more than one connection type available actually have multiple hardware MAC addresses. Connecting your laptop by Ethernet and later by Wi-Fi will result in two different MAC addresses being seen by the network. Replacing the network interface card (NIC) will also change the hardware MAC address.

– **A Private (Random) MAC Address**
Android, iOS, Windows 10 and other devices can use a random MAC address (private Wi-Fi) instead of the hardware MAC on the device. Every time the MAC address randomizes and connects to your network, a different device is recognized. Depending on how often the MAC address randomizes, several duplicates of the same device can end up in your devices list.

## Should I remove the duplicate device?

If the duplicate device is the result of a different connection type, then you should keep the device in your list and assign it to the same person. This ensures that all Midco Business Wi-Fi Pro features that rely on the MAC address continue to function as intended regardless of how the device connects to the network.

If the duplicate is the result of a random MAC address, the old instance(s) can be safely removed since it is unlikely the exact same MAC address will be used again. It is recommended that you disable the random MAC address feature (private Wi-Fi) on the device to ensure the best experience and proper enforcement of Midco Business Wi-Fi Pro features.

## How do I remove duplicate devices from my device list?

Devices that are not assigned to a person will automatically disappear from the device list 14 days after their last connection. To manually remove a device from the list that is not assigned and not connected, simply swipe left on the device in the device list.

## How do I disable the private (random) MAC or Wi-Fi address on my device?

Devices using a private Wi-Fi address will connect to your Midco Business Wi-Fi Pro network. To get the best experience and guarantee device-level security and controls, we recommend you turn off private Wi-Fi addresses and revert to your original address when connecting to your work network.

**Android 10 and Later**

1. Connect to your Wi-Fi Pro network.
2. Navigate to **Settings** or the **Settings app** on your device.
3. Tap **Network & Internet/Connections** and then **Wi-Fi**.
4. Tap the **Gear** icon associated with your network.
5. Tap **Advanced** and then **Privacy**.
6. Tap **Use Device MAC**.

**Samsung Galaxy Android 10 and Later**

1. Connect to your Wi-Fi Pro network.
2. Navigate to **Settings** or the **Settings app** on your Samsung Galaxy device.
3. Tap **Connections** and then **Wi-Fi**.
4. Tap the **Gear** icon next to the appropriate network.
5. Tap **MAC address type**.
6. Choose **Phone MAC** from the dropdown options.

**iOS14 and Later**

1. Connect to your Wi-Fi Pro network.
2. Open the **Settings app** on your iPad. Then tap on **Wi-Fi**.
3. Tap on the **Information** button next to your network name.
4. Slide the **Private Address** toggle to turn it off. A message will pop up to rejoin the network.
5. The iPad will briefly disconnect and then reconnect using the original Wi-Fi address.

**Windows 10**

1. Connect to your Wi-Fi Pro network.
2. In your computer taskbar, right click on the **Wi-Fi** icon and then **Properties**.
3. Under the **Random Hardware Addresses** section, change the setting to **Off**.
4. Turn off the Wi-Fi on your device and turn it back on to reconnect to your Wi-Fi Pro network using the original Wi-Fi MAC address.

**Apple Watch watchOS 7 and Later**

1. Open the **Settings app** on your Apple watch, then tap on **Wi-Fi**.
2. Tap on your Wi-Fi Pro network.
3. Tap the **Private Address** toggle to turn it off.
4. To switch to the original Wi-Fi address, turn off Wi-Fi on the device and turn it back on.

Once connected to your network using the original Wi-Fi address, any of the previously personalized device- or employee-level features, such as Online Protection, Content Access controls and Employee Timecards, will be restored.

**Note:** These settings will only be saved for your Midco Business Wi-Fi Pro network. Your device will continue to protect your privacy by using a private (random) Wi-Fi address when connecting to other networks.

## What do I do if a device shows a duplicate SSID (Wi-Fi network name)?

Our pods are each broadcasting a copy of the Wi-Fi network name (SSID), and most Wi-Fi devices, such as your phone and computer, are smart enough to understand that this is the same SSID and only show it once.

Occasionally, a device lacks the networking intelligence to understand when multiple access points offer the same Wi-Fi network name (SSID). These devices will sometimes display multiple copies of the same network name (SSID).

Check with the device manufacturer for firmware or driver updates. If a signal strength indicator is shown, select the Wi-Fi name with the highest signal. Otherwise, select any of the Wi-Fi network names to connect your device to the network.

Some known devices with this issue:

– Wemo

– Dish Hopper

– Amcrest IP2M-841

– Foscam F19821

## What do I do when a device is only 2.4 GHz-network compatible?

Many devices state they are only compatible with 2.4 GHz networks or may prevent you from connecting them if your mobile is currently connected on 5 GHz. Usually, these devices tend to be IoT devices that require you to use their app to set up the Wi-Fi connection for the device.

Most of these devices will connect without issue. However, since Midco Business Wi-Fi Pro SSIDs broadcast on both 2.4 GHz and 5 GHz simultaneously, you may run into a situation where some of these devices are unable to join your network because of their simplified Wi-Fi implementation.

## What are some workarounds for 2.4-GHz network compatible devices?

| | |
|---|---|
| Contact Midco Support by phone. | We may be able to force your mobile device to connect on 2.4 GHz temporarily, so you can complete the IoT device setup. Depending on how many of these devices you intend to connect, the process may take a bit of time and cannot be completed over email. |
| Use a 2.4 GHz-only mobile device to run the device's app and complete setup. | Since your mobile device is connected on 2.4 GHz, this can sometimes allow the app to continue with the setup process. Once set up, you can usually continue to operate the device using your regular mobile.<br><br>**Android users can force the device to connect at 2.4 GHz**. Once connected at 2.4 GHz, you can set up the device.<br><br>Android 7 or higher:<br><br>1. Download and install Wifi Analyzer by Farproc to the Android device.<br><br>2. Forget the Midco Business Wi-Fi Pro network on the Android device.<br><br>3. Open the **Wifi Analyzer app** and swipe right until you get to the **AP List page** or use the ***VIEW*** button on the top of the screen. Then select the **AP List**.<br><br>4. Move closer to the IoT device being installed.<br><br>5. You will see several pods broadcasting on different bands.<br><br>6. Tap on the signal with the Midco Business Wi-Fi Pro network name.<br><br>7. This will display a list with all the AP and channels available to connect. Connect on the strongest one broadcasting on a 2.4 GHz channel (1,6,11). Choose **Connect**.<br><br>8. Enter the Wi-Fi password. The phone will connect to that pod on 2.4 GHz.<br><br>9. Use the IoT device app to set up the device.<br><br>10. Once the devices are connected, forget the network on your Android device.<br><br>11. Repeat steps 3-9 if there are other devices that need to be connected through your business. If no other devices need to be connected, proceed to step 12.<br><br>12. Once all devices are installed, forget the network once again and connect the device back to the Midco Business Wi-Fi Pro network using the Wi-Fi settings on the phone.<br>– If this last step is not followed, the mobile will always stay connected to the same BSSID and will not roam.<br><br>13. Because the IoT software uses the BSSID to connect, each device will always connect to their respective assigned pod. Keep this in mind when moving these devices and pods around. |

| | |
|---|---|
| Set up a twin network. | A twin network can be set up using a Windows computer, an Android phone or an old wireless router. The device can learn the network information to connect automatically later. You must use the exact same SSID (network name) and password. Then configure this hotspot on 2.4 GHz.<br><br>**Windows Computer Mobile Hotspot Configuration**<br><br>1. Select the **Start** button, then select **Settings > Network & Internet > Mobile hotspot**.<br><br>2. Go to the **Edit** button.<br><br>3. On the **Network name**, add the same name as the one being used for your Wi-Fi Pro network zone.<br><br>4. On the **Network password**, add the same password as the one being used for the correct zone.<br><br>**5.** **Network band** should be set to 2.4 GHz and then click **Save**.<br><br>6. Turn on the **Mobile Hotspot**.<br><br>**Android Mobile Hotspot Configuration**<br><br>1. Swipe down from the top of the screen.<br><br>2. Look for the **Hotspot** option. If you don't find Hotspot, tap **Edit** or the **Pencil** icon at the bottom and drag **Hotspot** into your **Quick Settings**.<br><br>3. Long press over the **Hotspot** icon to access the settings.<br><br>4. Once on the **Hotspot & Tethering** menu, you can access the **Wi-Fi hotspot** section. From this menu, you should edit hotspot information:<br>– **Hotspot name:** Exact same name as the Plume network zone<br>– **Security:** WPA2 PSK<br>– **Hotspot password:** Exact same password used for the zone of the Wi-Fi Pro network<br><br>5. Click on **Advanced**.<br><br>6. Make sure the AP Band has been set to 2.4 GHz.<br><br>7. Turn on the **Hotspot**. |

| | |
|---|---|
| Set up a twin network (continued). | **Wi-Fi Router Configuration**<br><br>1. Access your router GUI (graphic user interface). This is usually done by typing the IP address of the router on a web browser.<br><br>2. Configure the SSID (network name) using the exact same name as your Wi-Fi Pro network zone. Then enter the password.<br><br>3. Go to the Wi-Fi or Wireless section and disable the 5 GHz frequency leaving only the 2.4 GHz frequency enabled. Make sure the network is now up.<br><br>**Note:** This configuration will vary depending on the model and brand of the router. You can check the router manufacturer manual for further information on how to perform the configuration. |

**Once the twin network is up and running:**

1. Go to the **Wi-Fi Pro app**. You will need to add one extra character to the network name (usually adding a number 1 after the network name works). Then click **Done**.
   – **Important note:** Once you save the changes, this will cause all the devices connected to the Wi-Fi Pro network to disconnect from it and then automatically connect to the twin network.

2. Confirm that the phone with the IoT device app installed on it has successfully connected to the twin network.

3. Proceed with the onboarding of the IoT device.

1. Once the IoT device has been successfully configured, go back to the **Midco Business Wi-Fi Pro app** and then change the network name back to how it was before the change. Then click **Done**.

1. Turn off the **Hotspot**. This will cause the devices to automatically disconnect from the twin network and connect back to the Wi-Fi Pro network, including the IoT device that was just configured.

# Connectivity and Performance Issues

## Slow Wi-Fi Connection

1. One or more pods are too far away from another pod.
   - Pods should be no more than 40 feet from each other.
   - Ensure that you have a strong core network in your business, keeping most pods in the center and not on exterior walls.
2. Not enough pods are connected to your Midco Business Wi-Fi Pro network.
   - If your signal is constantly weak, this is a good indicator.
   - Additional pods can always be added to your network by contacting Midco support.
3. One of your pods may be offline.
   - Check if any of the LEDs of the pods are slowly pulsing, which means it is disconnected.
   - If one or more pods are offline, follow the steps to resolve the issue.
4. Modem issues.
   - Restart your modem while keeping your pods plugged in to fix certain connection issues.
5. Internet down.
   - Contact Midco support or log on the Midco Business My Account to check if there is an outage.
6. A parallel network may be using all the available airtime.
   - Make sure your old Wi-Fi is disabled on your router. Follow our instructions on disabling your Wi-Fi on your router to eliminate interference.
7. Multiple Wi-Fi networks are running in your area.
   - Try moving your pods away from the outside walls to avoid additional interference and promote a stronger core network.
8. Look for interference from other sources.
   - This can include cordless phones, baby monitors, video senders, microwave ovens, medical and industrial equipment and other electronics. Many of these devices use the same bands as your Wi-Fi and cause interference.

## Lost Internet Connection.

1. Verify that your device is connected to the network by going to your device's Wi-Fi connection settings.
2. Check to see if you can connect to other sites. Open your device browser and go to any website. If you can access it, there must be something wrong with the site or app that you were trying to access.
3. If you are unable to visit any website with your device, try to access the internet with another device, your computer or tablet. If other devices connect to the Wi-Fi network, restart your device and try to connect to the Wi-Fi network. Should you still not be able to connect your device to the network, contact us for help.
4. Unable to connect all devices to the internet via a Wi-Fi connection? Connect your computer directly to the modem via Ethernet. You may need to reboot your modem, which you can do by contacting our support team or logging on to Midco Business My Account. If you are unable to connect to the internet, contact our support team.
5. If you are able to connect your computer to the internet via Ethernet, verify that your service is working.

# Speed Test Issues

If you have a multi-gigabit symmetrical internet connection and a pod as your gateway pod, you may notice that the uploads on your speed test results in the app are currently limited to around 1.5 Gbps. This is a known limitation on the pod.

While the WAN Ethernet port on a pod is fully capable of 2.5 Gbps throughput in both directions, the software onboard is currently unable to generate the data needed to saturate the upload during an ISP speed test. Because of this limitation, the speed test in the app will be limited to reporting about 1.5 Gbps for the upload. There is no issue reporting the download speed available since it is the speed test server generating the data downloaded for the speed test.

The 1.5 Gbps upload limitation only applies when traffic is being generated by the pod and does not apply when the data passes through during actual use. In other words, even though the reported upload speed test result is limited to 1.5 Gbps, the actual throughput will be higher if available and there will be no actual performance impact on the network.

## What To Do When Receiving Poor Speed Test Results

The built-in speed test measures the speed of the link from your gateway pod to your ISP using Ookla's speed test servers. If those results are not close to our advertised speed, these tests will help you find the cause.

**Ethernet Connection**

The Ethernet connection between the gateway pod and the modem/router should always be checked first if the speed test result is slower than 100 Mbps when the expected speed test download speed is greater than 125 Mbps.

1. Make sure the Ethernet connection on the gateway pod is secure and run a speed test in the app to get a baseline. If securing the connection fixes the issue, you can stop here.
2. If the gateway pod is plugged into a router, combination modem-router or network switch, change the ports being used for the pod and run the speed test from the app. If the results have improved and now match your expected speed, there may be an issue with your router, the gateway pod or the switch.
3. Swap the Ethernet port being used on the pod. Then, perform the speed test again in the app. If the results have improved, the port on the pod may have an issue. Contact Midco support for next steps.
4. There may be an issue with the Ethernet cable itself. Swap the Ethernet cable with a known working cable and run the speed test again.

If the results do not improve, the issue is not the Ethernet connection. You should continue troubleshooting based on your network setup.

**Direct Modem or Optical Network Terminal (ONT) Connection**

1. Power cycle your modem for 30 seconds while keeping the gateway pod attached via Ethernet. Run the speed test in the app once again to get a baseline. If this result is fine, the issue may have been a temporary slowdown of your internet connection.

2. Unplug the pod from the modem or ONT and plug in a laptop or computer via Ethernet. You will need to power cycle the modem again. Wait until the internet has come online.
   - Open a web browser and run a speed test at **Midco.com/SpeedTest**.
   - Compare this to the results on the app, which should be very similar.
   - If the test results are still poor, the issue may be with the modem, your internet connection or wiring to the ONT. Contact Midco support for assistance.

**Connected to a Separate Router**

1. Disconnect all other Ethernet-connected devices from the router.
2. Run a speed test in the app once again to get a baseline. If this result matches your expected speeds, the issue may be that the device(s) previously connected to the router were using bandwidth during the automated speed test performed by Midco Business Wi-Fi Pro.
3. Disconnect the router and plug the pod directly into the modem or ONT. The modem will need to be power cycled.
4. Run a speed test in the app. If the results are good, the issue may be with the router.
5. If the results are still poor, the issue may be with your modem or internet connection. Contact Midco support for assistance.

**Connected to a Midco-Provided Combination Modem-Router**

1. Disconnect all other Ethernet-connected devices from the combination modem-router.
2. Run the speed test in the app to get a baseline. If this result is fine and matches your expected speeds, the issue may be that the device(s) previously connected directly to the combination modem-router were using bandwidth during the automated speed test.
3. Plug in a laptop or another computer to the router via Ethernet.
   - Open a web browser and run a speed test at Midco.com/SpeedTest.
   - Compare this to the results on the app, which should be very similar.
   - If the test results are still poor, the issue may be with the combination modem-router or your internet connection. Contact Midco support for assistance.

## Router or Combination Modem-Router Issues Affecting Speed

**QoS settings:** If you have QoS enabled, make sure that all pods or their ports are set to the highest priority. This will ensure that devices are properly prioritized, too.

**Firmware:** Firmware on routers needs to be updated on a regular basis. Check with the manufacturer or Midco support for updates.

**Security, other settings or defective equipment:** Check with the manufacturer or Midco support to see if there are any other settings that could potentially slow down your pods or to confirm if the unit is no longer working properly.

## Upstream Devices Using Bandwidth

Midco Business Wi-Fi Pro will automatically run a speed test every six hours if the network is idle. However, the activity of devices connected upstream from the network, like the devices directly connected to the router, is not monitored. This means that the automatic speed tests will run even while those upstream devices are using the internet and the speed test results will reflect this.

# Security and Privacy

There are four main measures taken to keep data secure and reduce vulnerability to DDoS attacks.

1. **Access to the Pods**
   Local access to your pods is shut down completely to prevent access except from the cloud. SSH, Telnet, HTTP/S and other entry ports are disabled for all shipped products. This prevents hackers from trying to gain access to the device and exploit it for attacks.

2. **Encrypted Transmission to Cloud**
   Data sent from the pod to the cloud is encrypted via transport layer security (TLS). Each pod has a unique TLS connection with the cloud to prevent access in route.

3. **Access to Data in the Cloud**
   The cloud database is separated from the customer-facing application programming interface (API) server with a virtual private network (VPN) connection, making it more difficult for anyone to access the data.

4. **Reliability in Failover**
   Our application programming interface (API) and pod control server is largely protected from distribution denial of services (DDoS) attacks. However, they can still occur, which was seen last year when several national websites were down temporarily. While operating in Router mode, if the pods lose connection to the cloud, they will operate in their last known state. The Wi-Fi will operate normally, but it will not have the ability to adapt to changes. New devices can join, traffic will flow normally and so on. However, if a new pod is plugged in, it must wait for the cloud to initialize it to join the network. If operating in Bridge mode and the outage lasts longer than ten minutes, Wi-Fi connectivity will be lost until the pods can reconnect to the cloud.

## Privacy Requests

Business owners can make a request for a copy of or the removal of their business location data at any time. This includes information such as their Midco Business Wi-Fi Pro account, network settings and device information.

Guests can also make similar requests regarding their email or social account ID and device information used when accessing a Midco Business Wi-Fi Pro Guest network.

The different types of privacy requests that can be made are found at **Midco.com/Legal**.

# Online Resources

Your experience with Midco matters to us. We want to help you get the most out of your services. We offer many resources at **Midco.com/Business**.

**Midco.com/Business/Support**
Visit our online library of helpful tools and information. Get step-by-step instructions, advanced setting information, common troubleshooting solutions, equipment support, answers to frequently asked questions and more.

**My Account and Bill Pay**
Midco.com/Business/MyAccount

– View your current and past bills online.

– Set up auto pay or make a one-time payment.

– Enroll in paperless billing.

**Policies**
Midco provides Midco Business Wi-Fi Pro service to our customers subject to policies established for the protection of our users, our company and our communities. Visit **Midco.com/Legal** for our:

– Acceptable Use Policy

– Internet Service Terms and Conditions

– Cable, Internet and Phone Subscriber Privacy Notice

– Online Privacy Policy

**24/7 Support**
Have a question? Contact our team.
**Midco.com/Business/Contact**
**1.800.888.1300**


MIDCO
BUSINESS®