insee**go**

SKYUS 300
IP Rated Gigabit LTE Router

insee**go**

INSEEGO COPYRIGHT STATEMENT

INSEEGO TRADEMARKS AND SERVICE MARKS

Document Number: MKT-00070 Rev 6

Contents

1

Introduction

Overview

Description

Indicator LEDs

Overview

The Skyus 300 is a full-featured router that provides high-speed cellular connectivity. It provides Cat-18 (4G LTE-A Pro) and future external 5G support for ultra-fast internet access and to optimize your business needs in fixed or mobile applications.

Skyus 300 features multiple Ethernet ports, Wi-Fi 5, GPS, Bluetooth 5.0[*], aGNSS location based services as well as enterprise-grade security and routing features.

Key Features

- IP64 Rating (Dust Proof, Water Resistant)

- MIL-STD 810G and SAE J1455 Testing

- High-Speed Cellular Connectivity

- Dual Concurrent High-Speed 2.4 GHz and 5 GHz Wi-Fi; Access Point and Client Mode

- Standalone and Assisted GPS/GNSS; GPS Reporting to Local Ports, Remote Servers, and NetMotion Mobility Client

- IPsec VPN and Standard Routing Features (Firewall, Filtering, Forwarding, DHCP, etc.)

- Cloud Connectivity for Device Management, GPS Tracking, and Smart Rules/Alerts

---

[*] For future release

Description

Inside the box, you will find a Skyus 300 router, a Quick Start Guide, and a DC power + I/O cable. Below is an overview of the physical interfaces of the device.

Front View
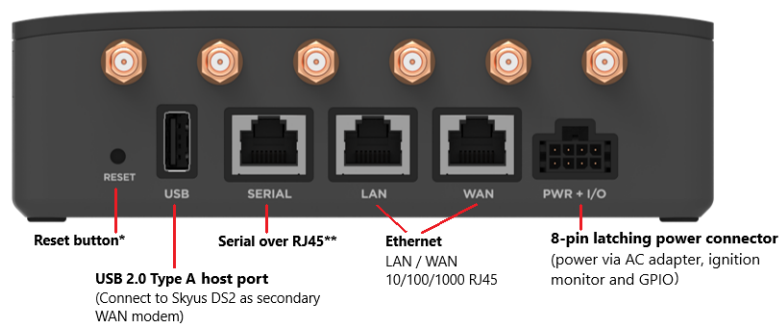
Device Health
USB
Cellular
WiFi
Bluetooth*
GPS

*For future use

Back View

Reset button*
USB 2.0 Type A host port
(Connect to Skyus DS2 as secondary WAN modem)

Serial over RJ45**

Ethernet
LAN / WAN
10/100/1000 RJ45

8-pin latching power connector
(power via AC adapter, ignition monitor and GPIO)

*Press quickly to turn the router off and on again.
CAUTION: Pressing for 15 seconds or longer resets settings to factory default values.
**For future release.

Indicator LEDs

The Skyus 300 has six indicator LEDs. These indicators change colors and either blink or glow solid to communicate current states for the device.

LED	LED Color	Operation	Meaning
Device Health[*]			
USB*			
Cellular	**Orange**	Solid	No SIM
		Slow Blink	Inactive SIM
	Red	Solid	Cellular Error
	Blue	Solid	Great Signal
		Fast Blink	Excellent Signal with Traffic
	Green	Solid	Good Signal
		Fast Blink	Great Signal with Traffic
	Yellow	Solid	OK Signal
		Fast Blink	Good Signal with Traffic
	Magenta	Solid	Poor Signal
		Fast Blink	Poor Signal with Traffic
Wi-Fi	**Off**	Off	Off
	Red	Solid	Wi-Fi Error
	Orange	Solid	On with no Connected Devices
	Green	Solid	On with Connected Devices
		Fast Blink	Wi-Fi Traffic
	Blue	Solid	Wi-Fi as WAN Mode Active
Bluetooth*			
GPS	**Off**	Off	Off
	Red	Solid	GPS Error
	Orange	Slow Blink	Searching/Acquiring
	Yellow	Solid	Standalone GPS/GNSS Active; Location Acquired
	Green	Solid	Assisted GPS/GNSS Active, Location Acquired

---

[*] For future release

	Blue	Solid	Dead Reckoning Active, Location Acquired

The WAN/LAN connector ports also have indicator LEDs.

LED	LED Color	Operation	Meaning
LAN	Green		Indicates Ethernet connection speed
		Solid	1000 Mbps (Gigabit)
		Off	10/100 Mbps
	Amber		Indicates link status
		Solid	Link
		Blinking	Activity
		Off	No link

2

Installation and Getting Started

Installation Overview

This chapter provides instructions for installing and getting your Skyus 300 up and running, as well as reset and support information.

The installation process consists of the following steps:

- Installing SIM Cards

- Installing and Connecting Power (for Vehicle Applications)

- Connecting I/O Devices

- Connecting Antennas

- Powering your Router

- Connecting to the Web UI

- Initial Configuration and Setup

- Connecting to a Mobile Network

- Connecting Additional Devices

Installing SIM Cards

If you are using cellular service, insert SIM cards into the slots on the left side of the router with the SIM contacts facing up.

SIM Slot (insert with contacts facing up)

Installing and Connecting Power (for Vehicle Applications)

NOTE: Follow your vehicle manufacturer's guidelines for connecting electrical accessories and use only UL Listed components.

WARNING: Electrical installations can be hazardous and should be performed only by licensed professionals.

Consider the following when installing your Skyus 300 in a vehicle:

- Do not install the device in an area of a vehicle where it will distract the driver.

- The power supply cable, which will connect to the vehicle's fuse box, must be installed along the vehicle wall, inside the cab, and must not cross the vehicle's firewall protection. NOTE: The power supply must be sourced from Inseego or an Inseego approved supplier.

- Ensure easy access for connecting cables.

- Ensure minimum bend radius for cables.

- Avoid sharp edges or existing wiring.

- Avoid proximity to high amperages or extreme temperatures.

- Avoid direct exposure to harmful elements such as water, dust, and heat.

Installing and Grounding

To install and ground your device:

1. Use the two installation holes to secure the device in place using M3 or M3.5 (#4 or #6) screws (16+1.8mm).
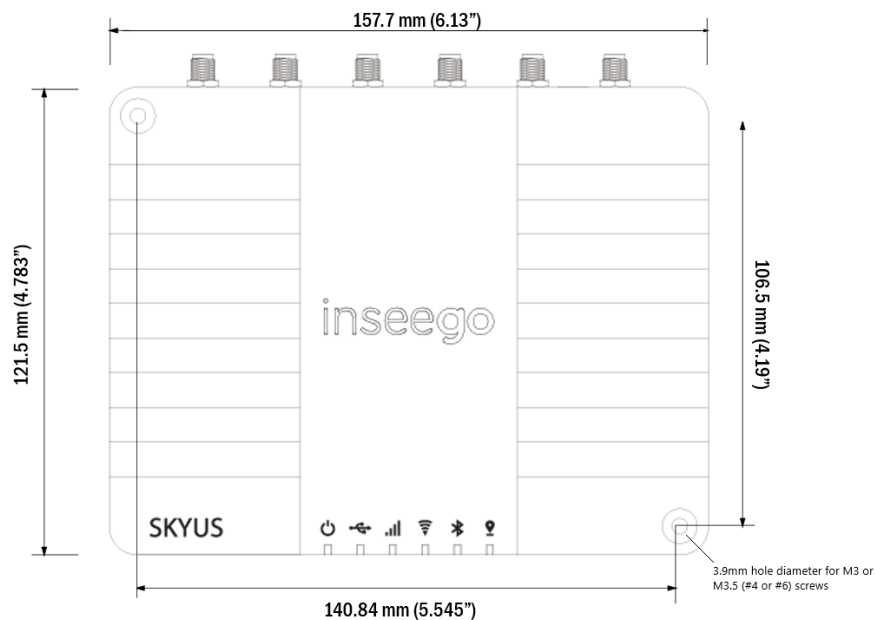
2. Ground the device by drilling into a grounded metallic surface using the integrated holes.

3. If you are installing in a high vibration setting, use cable strain relief to reduce the effects of vibration. Install the strain relief to the same surface as the Skyus 300, within eight inches of the device. This allows the router and cable to vibrate together. Ensure the cable is not pulling on the power connection.

Connecting to Vehicle Electrical System

Your Skyus 300 cable harness includes power and I/O pins, including an ignition monitor, four configurable digital General Purpose Input/Output (GPIO) pins[*], and a 1-Wire I/O pin[†].

1 - Ignition Monitor
2 - GPIO*
3 - 1-Wire Input
4 - Ground
5 - Voltage In (Power)
6 - GPIO
7 - GPIO
8 - GPIO*
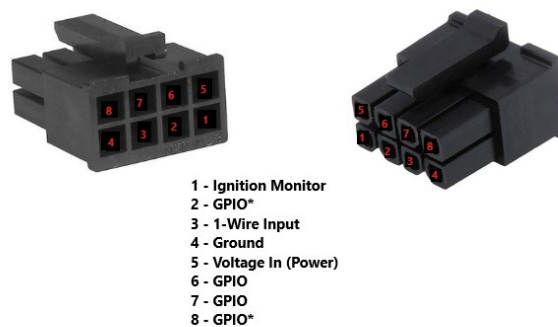
*For future release

To connect your Skyus 300 to the vehicle's electrical system:

1. Turn the vehicle off and remove the key from the ignition.

2. Disconnect the vehicle's battery by disconnecting the negative terminal first and then the positive terminal.

3. Connect the black (ground) wire on the DC power cable to the vehicle chassis.

4. Ensure the Skyus 300 device is also grounded.

---

[*] Two available in future release
[†] For future release

5. Fuse the red power wire on the DC power cable to the power source through the vehicle's fuse box.
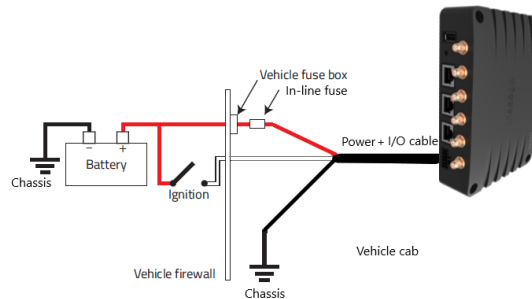
6. Connect the ignition monitor wire on the DC power cable to the ignition switch on the vehicle.

   NOTE: The ignition monitor ensures a controlled shutdown of the router when the vehicle is turned off. You can configure a delay between the time the ignition shuts off and when the Skyus 300 shuts off. See the I/O Settings Page on page 54.

7. Connect the DC power cable to the Skyus 300.

8. Reconnect the vehicle's battery, connecting the positive terminal first and then the negative terminal.

Connecting I/O Devices

You can use the configurable digital GPIO pins to provide on/off data and functionality. Page 14 shows the placement of GPIO pins in the Skyus 300 cable harness.

I/O inputs convey information to the router about the state of an external device or system; for example, that a siren is on.

I/O outputs are used for the Skyus 300 to tell a device or system to turn on or off; for example, an ignition lock.

Connecting Antennas

There are two possible antenna configurations, depending on whether your device is mobile or fixed.

Finger tighten the appropriate antennas for your desired configuration.

NOTE: Recommended torque is 5 in-lbs (56 N-cm).

Mobile Antenna Configuration

Wi-Fi
(2.4 GHz; 5 GHz)

Primary LTE
(690-960 MHz; 1700-2700 MHz)

Bluetooth*
(2.4 GHz)

GPS **
(1570-1580 MHz)

Diversity (Aux) LTE
(690-960 MHz; 1700-2700 MHz)

RESET   USB   SERIAL   LAN   WAN   PWR + I/O
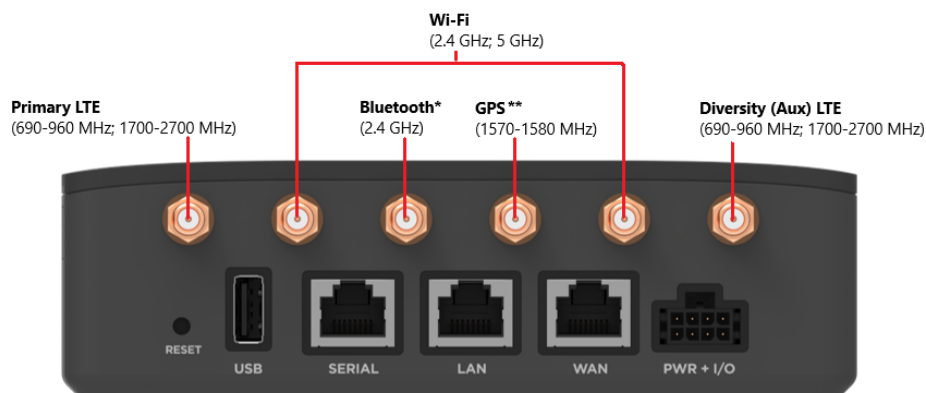
Mobile Antenna Configuration

*For future release
**Ensure the GPS antenna has clear access to satellites.

NOTE: In the mobile antenna configuration, LTE and GPS ports are SMA, Wi-Fi and Bluetooth ports are RP- SMA.

Fixed Antenna Configuration

LTE 1   UHB 1   LTE 3   LTE 4   UHB 2   LTE 2

RESET   USB   SERIAL   LAN   WAN   PWR + I/O
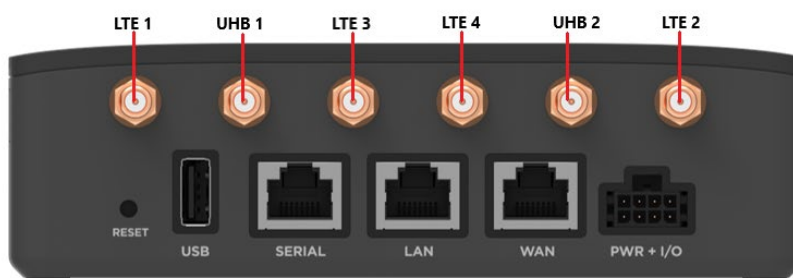
Fixed Antenna Configuration

NOTE: All ports in the fixed antenna configuration are SMA.

Powering your Router

Connect the power cord (9-32 VDC input range) to the applicable power source. If in a mobile setting, refer to Installing and Connecting Power (for Vehicle Applications) on page 13. If in a fixed environment, connect to the appropriate power source using the DC cable or the AC adapter as needed. NOTE: AC power supply/AC Adapter must be installed in a location where the ambient temperature is below 40 °C.

Connect the end of an Ethernet cable one of the Ethernet ports and the other end of the cable into the Ethernet port of the device you wish to connect.

It is recommended to only use the power supply/adapter or connection accessory provided by Inseego. Contact insidesalesus@inseego.com for more information about the power supply/adapter.

Reset button*

USB 2.0 Type A host port
(Connect to Skyus DS2 as secondary WAN modem)

Serial over RJ45**

Ethernet
LAN / WAN
10/100/1000 RJ45

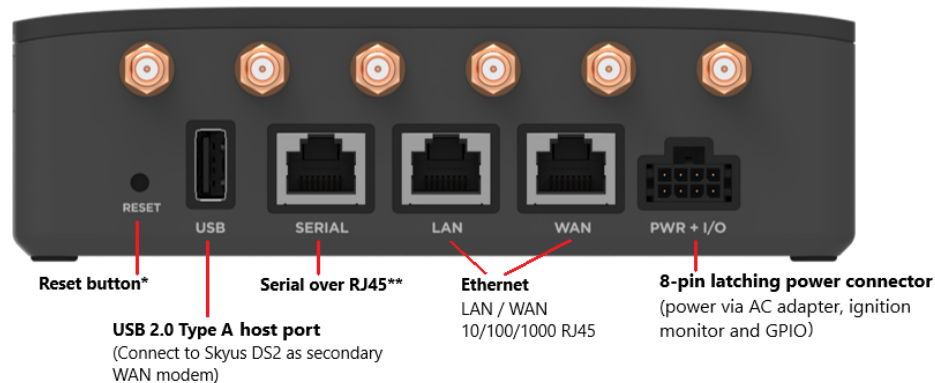**8-pin latching power connector**
(power via AC adapter, ignition monitor and GPIO)

*Press quickly to turn the router off and on again.
  CAUTION: Pressing for 15 seconds or longer resets settings to factory default values.
**For future release.

Connecting to the Web UI

On the device connected to your Skyus 300, open any web browser and go to http://my.router or http://192.168.0.1.

Select Sign In (in the top-right corner of the screen), and enter the password printed on the bottom of your router.

Initial Configuration and Setup

There are some initial steps you may want to take before connecting more devices to your Skyus 300.

NOTE: It is strongly recommended to change both your Wi-Fi passwords and your device Admin password for increased security.

1. Set up Primary network name, security, and password on the **Wi-Fi** > **Wi-Fi Primary Network** tab. You can also set up a Guest network on the **Wi-Fi** > **Wi-Fi Guest Network** tab.

2. Change the Admin password for the Web UI. Click the down arrow next to **Sign Out** in the top-right corner of any Web Interface page and select **Change Password**. Select **Help > Admin Password** for more information.

3. To set an Access Point Name (APN) for your network to communicate with the Skyus 300, go to **Settings > Advanced > Network** tab.

Connecting to a Mobile Network

To activate a SIM card, contact your carrier representative. Please note, after activation is complete, it may take a few minutes for the SIM card to activate and connect to the mobile network. When the cellular LED is magenta, yellow, green or blue (depending on connection strength), the connection is successful. Orange indicates no SIM card. Blinking orange indicates an inactive SIM card. Red means there is a cellular error. See Indicator LEDs on page 9.

Connecting Additional Devices

You can connect up to 128 client devices to your Skyus 300 via Wi-Fi and hundreds of devices via Ethernet using DHCP. **NOTE:** Higher client counts will affect throughput.

Connecting via Wi-Fi

To wirelessly connect a Wi-Fi-capable device to your Skyus 300 for the first time:

On the device you want to connect to the Internet, open the Wi-Fi application or controls and in the displayed list of available networks, find the network name for your Skyus 300.

Click **Connect** or otherwise select the network name.

When prompted, enter the password.

NOTE: The Wi-Fi name and password are displayed in the Wi-Fi panel of the Home screen.

Connecting via Ethernet

To connect a wired device to your Skyus 300, plug the end of an Ethernet cable into one of the Ethernet ports.

NOTE: If you are connecting several devices via Ethernet using your Skyus 300 as a Dynamic Host Configuration Protocol (DHCP) server on a switch, select **Setting> Advanced > LAN** to view and configure DHCP settings.

Resetting Skyus 300

You can restart your Skyus 300, or restore settings to the factory defaults. You can do this using the Web UI at **Settings > Backup and Restore**, or by clicking the Sign Out drop-down in the top-right corner of any Web Interface page and selecting **Restart**.

Alternately, you can use the **RESET** button on the device:

To restart the Skyus 300: Press the **RESET** button quickly. This turns your router off and on again and does not affect settings.

To restore Skyus 300 to factory default settings: Press and hold the **RESET** button for 15 seconds or longer. This resets all settings to their factory default values.

CAUTION: This initiates a restart and may change the current Wi-Fi settings, breaking all existing connections to this router and disconnecting you from the Web UI.

Getting Support

Documentation for your Skyus 300 is available online. Go to www.inseego.com/support-documentation.

For additional information and technical support, email Technical Support at technicalsupportus@inseego.com or call Customer Support (Toll Free) at **1-877-698-6481**.

3

Software Configuration

Overview

On the device connected to your Skyus 300, open any web browser and go to http://my.router or http://192.168.0.1.

Home Page

The Skyus 300 Home page is the local gateway to configuring and managing your router. It displays current router status, lists currently connected devices, and offers links to other pages with option settings and help.

Click > in the bottom-right corner of a panel to access subscreens with further information and options.

Skyus 300

Sign Out

Wi-Fi

Primary Network (ON)

2.4 GHz Network Name (SSID):

Skyus-300-751E

Password: ••••••••   👁

Guest Network (OFF)

Settings

Port Filtering (OFF)

Port filtering allows you to select which applications can access the internet.

System Update

Last system update: Never

Connected Devices

Device	Network
Laptop	Primary

About

Internet Status: Not Connected

Network name: None

Time connected:

Help

Overview
Setup
Support

Device Support Page
User Guide

Side Menu

Each subscreen in the Skyus 300 Web Interface includes a menu on the left, which you can use to return to the Home page or jump to other screens. The current screen is indicated by a red bar.

The side menu includes items that are not visible from the Home page, including **Access Control**, **GPS**, **I/O Settings**, **VPN**, and **Remote Management**. Access a subscreen from the Home page to choose these additional options from the Side Menu.

Home

Wi-Fi

Connected Devices

Access Control

Settings

GPS

VPN

I/O Settings

Remote
Management

About
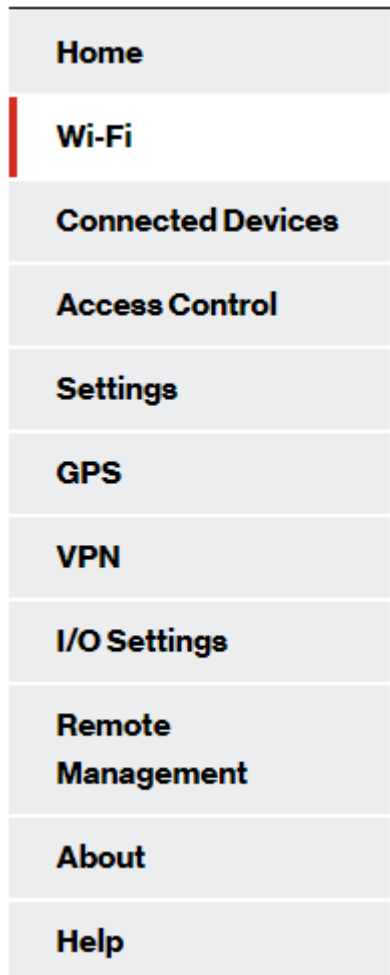
Help

Getting Help

Select the question mark (?) in the upper right hand corner of a page to view Help on that topic.

Admin Password

The Admin password is what you use to sign into the Skyus 300 Web Interface. Initially, it is the same as the default password for your router's Primary network and is printed on the bottom of the router.

NOTE: You can set up separate Wi-Fi passwords both Primary and Guest networks in **Wi-Fi**, but these are different from the Admin password, which is for this Web Interface.

Important: It is critical that you change the Admin password from the default to keep the device and your network secure.

To change the Admin password:

1. Click the down arrow next to **Sign Out** in the top-right corner of any Web Interface page and select **Change Password**.

2. Enter your current Admin password, then enter a new password and confirm it.

3. Select a security question from the drop-down list and type an answer to question in the **Answer** field. **NOTE:** Answers are case-sensitive.

4. Click **Save Changes**.

The next time you sign in to the Skyus 300 Web Interface, use the new Admin password. If you cannot remember the password, click **I forgot the Admin password**. After you correctly answer the security question you set up, the current password is displayed.

Managing Wi-Fi Settings

Your Skyus 300 offers primary and guest networks for accessing the Internet over Wi-Fi, as well as Wi-Fi as WAN. Each network can be accessed over two bands: 2.4 GHz and 5 GHz:

- The 2.4 GHz band is supported by all devices with Wi-Fi and should be used by devices that are a few years old or older. This band passes through walls better, so it may have a longer range.

- The 5 GHz band is best for newer devices, it offers better throughput and reduced interference, but does not pass through walls as well as 2.4 Ghz.

On the Web UI Home page, the Wi-Fi panel shows the current name (SSID) and state of primary and guest networks. Click the eye icon to view the current passwords for each.

Skyus 300

Wi-Fi

Primary Network (ON)

2.4 GHz Network Name (SSID):
  Password: ••••••• 👁
5 GHz Network Name (SSID):
  Password: ••••••• 👁

Guest Network (OFF)

                                          >

Settings

Port Filtering (OFF)

Port filtering allows you to select which
applications can access the internet.

System Update

Last system update: Never

                                          >

Connected Devices

Device	Network
Jane's Work	Primary

About

Internet Status: Connected

Network name: WAN

Technology: Ethernet

Time connected: 3:03:27:43 (dd:hh:mm:ss)

                                          >

Help

Overview
Setup
Tips

Device Support Page ⧉
User Guide ⧉

                                          >

                                          >

inseego © 2018 All rights reserved.

www.inseego.com

To manage settings for these networks, select **>** from the Home page Wi-Fi panel (or select **Wi-Fi** from the Web UI side menu).

The Wi-Fi page includes four tabs:

- Wi-Fi Settings Tab

- Wi-Fi Primary Network Tab

- Wi-Fi Guest Network Tab

- Wi-Fi as WAN Tab

Wi-Fi Settings Tab

You can use the default values as they appear on this tab, or can adjust them for your environment.

Wi-Fi

Use the **Allow Wi-Fi devices to connect to this Router** ON/OFF slider to turn Wi-Fi on or off. This selection affects Primary and Guest networks.

When Wi-Fi is turned off, the only way to connect to the router (and to the Admin website) is with Ethernet cable.

Band Selection

Each network can be accessed over two bands: 2.4 GHz and 5 GHz:

- The 2.4 GHz band is supported by all devices with Wi-Fi and should be used by devices that are a few years old or older. This band passes through walls better, so it may have a longer range.

- The 5 GHz band is best for newer devices. It offers better throughput and reduced interference, but does not pass through walls as well as the 2.4 GHz band.

NOTE: The Guest Network must be assigned at least one band before it can be turned on.

2.4 GHz Band Selection

This section displays the 802.11 Mode in use when the 2.4 GHz band is active and allows you to select a Channel.

NOTE: Leave the Channel set to **Automatic** unless you need to choose a particular channel for your environment.

5 GHz Band Selection

This section displays the 802.11 Mode in use when the 5 GHz band is active and allows you to select a Bandwidth and Channel.

NOTE: Leave the Bandwidth at the default setting unless you experience interference with other Wi-Fi devices. If you experience interference, try lowering the Bandwidth setting to reduce the interference.

NOTE: Leave the Channel set to **Automatic** unless you need to choose a particular channel for your environment.

Select **Save Changes** to store new settings.

Wi-Fi Primary Network Tab

Use these settings to connect initially to the Primary Wi-Fi network or change Primary network information. Connected devices must use the Wi-Fi settings shown on this screen.

NOTE: If you change these settings, existing connected devices may lose their connection.

Settings

Primary network name (SSID): Enter a Primary network name (SSID) to set up or change the Primary network name. The name can be up to 28 characters long.

Security: Select an option for Wi-Fi security:

- **WPA2 Personal** is the most secure method of Wi-Fi Protected Access and should be used if possible.

- **WPA/WPA2 Personal** can be used if some of your older devices do not support WPA2.

- **WPA/WPA2 Enterprise** is designed for organizations and includes enterprise-grade authentication. **NOTE:** This method provides administrative control over access to your Wi-Fi network, so that administrators assign, modify and revoke login credentials for users. A Remote Authentication Dial-In User Service (RADIUS) server is required and must be configured for this option.

- **None** allows others to monitor your Wi-Fi traffic and use your data plan to access the Internet. **NOTE:** Avoid using this option.

Password: Enter a Wi-Fi password, *or* you can use the Generate new password button.

Important: It is critical that you change the password from the default and use a different password from your Admin password to keep the device and your network secure.

Generate new password: This button inserts a strong random password in the Password field.

You can click the eye icon to view the password.

Options

Broadcast primary network name (SSID): Check this box to allow Wi-Fi devices in the area to see the Wi-Fi Primary network name (SSID) on their list of available networks. If not selected, the network name will need to be manually entered for devices to connect to the network.

Select **Save Changes** to store new settings.

Wi-Fi Guest Network Tab

The Wi-Fi Guest network allows you to segregate traffic to a separate network rather than share access to your Wi-Fi Primary network. Use settings on this tab to set up or change Wi-Fi Guest network information. Connected devices must use the Wi-Fi settings shown on this screen to connect to the Guest Wi-Fi network.

NOTE: To turn the Wi-Fi Guest network on, you must select at least one band for Guest Network under **Band Selection** on the **Wi-Fi Settings** tab and then select **Save Changes**.

Settings

Guest network name (SSID): Enter a Guest network name (SSID) to set up or change the Guest network name. The name can be up to 28 characters long.

Security: Select an option for Wi-Fi security:

- **WPA2 Personal** is the most secure method of Wi-Fi Protected Access and should be used if possible.

- **WPA/WPA2 Personal** can be used if some of your older devices do not support WPA2.

- **WPA/WPA2 Enterprise** is designed for organizations and includes enterprise-grade authentication. **NOTE:** This method provides administrative control over access to your Wi-Fi network, so that administrators assign, modify and revoke login credentials for users. A Remote Authentication Dial-In User Service (RADIUS) server is required and must be configured for this option.

- **None** allows others to monitor your Wi-Fi traffic and use your data plan to access the Internet. **NOTE:** Avoid using this option.

Password: Enter a Wi-Fi password, *or* you can use the Generate new password button.

Important: It is critical that you change the password from the default and use a different password from your Admin or Primary network password to keep the device and your network secure.

Generate new password: This button inserts a strong random password in the Password field.

You can click the eye icon to view the password.

Options

Broadcast guest network name (SSID): Check this box to allow Wi-Fi devices in the area to see the Wi-Fi Guest network name (SSID) on their list of available networks. If not selected, the network name will need to be manually entered for devices to connect to the network.

Select **Save Changes** to store new settings.

Use settings on this tab to set options for using an external Wi-Fi network to access the Internet.

NOTE: To enable Wi-Fi as WAN, you must go to the **Wi-Fi Settings** tab and in **Band Selection**, select a band for **Wi-Fi as WAN.** Then select **Save Changes**.

Important: Only one station/network from either the 2.4GHz or 5GHz band can be enabled at a time. If you change a radio band to client mode (Wi-Fi as WAN), all clients connected to that radio band will be disconnected.

Once you have enabled Wi-Fi as WAN on the Wi-Fi Settings tab, return to the **Wi-Fi as WAN** tab. The band you enabled is displayed.

Access Points

By default, one access point is listed initially.

Add Access Point: Use this button to add a hidden network. The Add new access point dialog displays. Enter an **SSID**, choose a security level from the **Security** drop-down, and enter a password if prompted. Select **Save Changes**.

Once connected, the new access point appears in the Access Points list.

Scan: Use this button to see a list of available access points and add an access point. The Scan Results dialog displays, listing available access points. Click **Add** to add an access point. The **Add new access point** dialog displays. Choose a security level from the **Security** drop-down and enter a **Passphrase**. Select **Save Changes**.

Once connected, the new access point appears in the Access Points list.

When there is at least one Access Point in the Access Points list, you can set the following:

- **Enabled:** Enable or disable an access point.

- **Priority:** Use the Up and Down buttons to set the priority for each access point.
  If an access point is enabled and available, and has highest priority among the enabled access points (is first in the list), the Skyus 300 connects to that access point and displays its details in the **Connected Access Point** area below, including:

  - **SSID:** The SSID (network name) of the connected access point.

  - **MAC Address:** The MAC Address (unique network identifier).

  - **Freq:** The frequency used by the connected access point.

  - **Security:** The security level.

  - **WPA State:** The Wi-Fi Protected Access state.

- **Edit:** Change the SSID, security setting, or password for an access point. **NOTE:** The SSID and password must match the access point. Only change these fields to match changes in the actual access point information.

- **Delete:** Delete an access point from the list.

Managing Connected Devices

On the Web UI Home page, the Connected Devices panel lists all devices currently connected to your Skyus 300, along with the network they are using.

To manage connected devices, select **>** from the Home page Connected Devices panel (or select **Connected Devices** from the Web UI side menu). The Connected Devices page appears.

Connected Devices Page

This page provides details about each device connected to the Skyus 300 and allows you to edit how device names appear in the Web UI. You can also block or unblock a device from Internet access.

Connected

This table lists all devices connected to the Skyus 300:

> **Connection:** An icon indicates the connection type (Wi-Fi or Ethernet) for each device. (You can hover over the icon to read the type of connection.)

> **Device:** This is usually the hostname set on the connected device. In rare cases, the hostname may be unavailable.

> You can change the name of a device as it appears in the Skyus 300 Web UI by clicking in the **Device** field and editing the name. **NOTE:** This only changes the how the device name appears in the Skyus 300 Web UI.

> **Network:** Indicates whether the device is connected to the Primary or Guest network.

Block: Select this box to disconnect a device and prevent it from reconnecting. Select **Save Changes**. The device is removed from the **Connected** list and appears in the **Blocked** list below. **NOTE:** This option is available for each device connected through Wi-Fi, but is not available for your own device or devices connected via Ethernet.

To view details on a device, click the **plus icon** (**+**) on the right to expand the device row. The following information appears:

- **IPv4**: The IP address of the connected device.

- **MAC Address**: The MAC Address (unique network identifier for this connected device).

- **Link Local:** The Link-Local IPv6 address if the connected device supports IPv6.

Click the **minus icon** (-) to collapse a row.

Blocked

This section lists all devices blocked from connecting to the Skyus 300.

NOTE: Since blocked devices are not currently connected, they do not have an IP address. Instead, they are identified by their name and MAC address.

To unblock a blocked device, click the **Unblock** button and select **Save Changes**. The device is removed from the **Blocked** list and appears in the **Connected** list above.

Managing Access Control

Access controls in the Web UI allow you to control access to specific devices. You can set up multiple schedules for access and apply them to individual connected devices. To manage access controls, select **>** from any Home page panel and then select **Access Control** from the Web UI side menu.

The Access Control page includes two tabs:

- Devices Tab

- Schedules Tab

Devices Tab

Access controls in the Skyus 300 Web UI allow you to control Internet access to specific devices. You can set up multiple schedules for Internet access on the Schedules tab and apply them to individual connected devices on the Devices tab.

NOTE: You must first create schedules on the **Schedules** tab for device and schedule information to display on the **Devices** tab.

This tab lists all currently connected devices and any applied schedules. (**No access controls** indicates that no schedule is applied to a device, and Internet access is unrestricted.)

To apply a schedule to a device, select a schedule from the drop-down list. Select **Save Changes**.

Schedules Tab

Access controls in the Skyus 300 Web UI allow you to control Internet access to specific devices. You can set up multiple schedules for Internet access on the Schedules tab and apply them to individual connected devices on the Devices tab.

Use this tab to manage schedules for when devices can access the Internet through the Skyus 300.

Create new schedule: Select this button to create a new schedule. The Create new schedule dialog box appears.

Create New Schedule   ✕

Schedule Name: [_____]

Description:

[   ]
[   ]
[   ]
[   ]
[   ]
[   ]

Access: [Allow ∨]

| Mon | Tue | Wed | Thu | Fri | Sat | Sun | Start Time | End Time |
| ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | [hh:mn] [AM ∨] | [hh:mn] [AM ∨] |

                                              [Cancel]   [Save schedule]

Enter a **Schedule Name** and **Description**.

In the **Access** section:

- Determine if you want **Allow** access during the specified days/times or if you want to **Block** access during the specified days/times.

- Set a range of time for allowing or blocking Internet access:

  o Select the days of the week you want the range to apply to.

  o Enter start and end times for the range.

Select **Save schedule** to close the dialog box and return to the Schedules page. The new schedule is now listed.

Use the **View**, **Edit**, and **Delete** buttons to view, edit, or delete (unapplied schedules only) listed schedules.

Use the **Devices** tab to apply schedules to devices.

Managing Settings

On the Web UI Home page, the Settings panel shows the current Port Filtering setting (On/Off) and the date and time of the last system update.

To change system settings, select **>** from the Home page Settings panel (or select **Settings** from the Web UI side menu).

The Settings page includes four tabs:

- Preferences Tab

- Software Update Tab

- Backup and Restore Tab

- Advanced Tab

Preferences Tab

This tab allows you to change how dates, time, and numbers are displayed in the Skyus 300 Web UI. **NOTE:** These preferences affect packets sent to remote servers. For example, if you select a 24 hour time format, the Web UI, and any packets reporting time somewhere else, will display time in 24 hour format.

Date: Select the date format to be used throughout the Web UI and remote servers (mm/dd/yyyy or dd/mm/yyyy).

Time: Select the time format to be used throughout the Web UI and remote servers (12 or 24 hour).

Number format: Choose the format for decimal numbers displayed in the Web UI and remote servers (using a period or comma as the decimal point).

Select your display choices from the drop-down menus and click **Save Changes** to update settings.

Software Update Tab

Software updates are delivered to the Skyus 300 automatically over the mobile network. This tab displays your current software version, last system update information, and allows you to check for new software updates.

Current Software

Software version: The version of the software currently installed on your Skyus 300.

Check for New System Update

Checked for update: The date and time the Skyus 300 last checked to see if an update was available.

Update status: This is area is usually blank. If you check for an update, the result of that check, or the download progress of an update displays.

Check for update: Click this button to manually check for available software updates.

- If a new software update is available, click **Download now** to install it.

- If a new system update is available, you are given an option to install it now or later.

- If a configuration update is available, it is installed automatically.

Last System Update

This section displays details about the last software update, including the date and time of the last update, and the name, source, package version and size of the update.

System Update History

This section displays details of the last updates that have been downloaded and installed to this device. If this section is blank, no updates have been installed.

Use this tab to back up current Skyus 300 settings to a file on your computer, restore (upload) a previously-saved configuration file, reset the router to factory defaults, or restart the router.

Backup

To back up current Skyus 300 settings to a file on your computer, enter your Admin password in the **Admin password** field.

The default Admin password is printed on the bottom of the router. If you have changed the Admin password and don't remember it, select **Sign Out** in the top-right corner of the Home page, click **I forgot the Admin password**, and answer the displayed security question. The current Admin password will be displayed.

NOTE: If you enter an incorrect password five times in a row, you will be locked out of the Web UI. To unlock it, restart the router.

Click the **Download** button. The file is automatically downloaded to your Downloads folder. This configuration file contains all settings for the device, router and system functions. It does not contain any modem settings or data.

NOTE: The backup file cannot be edited or viewed on the downloaded system or on any other device. This file can only be restored for this model of Skyus 300, and settings can only be viewed or changed using the Web UI.

Restore Settings

CAUTION: Restoring settings (uploading a configuration file) changes ALL of the existing settings to match the configuration file. This may change the current Wi-Fi settings, breaking all existing connections to this router and disconnecting you from the Web UI.

To restore system settings from a backup settings file, enter your Admin password in the **Admin password** field.

In the **Select a file** field, click **Browse** and choose a backup settings file to restore.

NOTE: You can only restore a file that was created for this model of Skyus 300.

Click the **Restore Now** button.

Restore to Factory Defaults

Restore factory defaults: This button resets all settings to their factory default values.

CAUTION: This initiates a restart and may change the current Wi-Fi settings, breaking all existing connections to this router and disconnecting you from the Web UI.

Restart Router

Restart: This button turns your router off and on again.

Advanced Tab

Advanced settings are intended only for users with advanced technical knowledge. For information about the Advanced Settings page, go to Chapter 4, "Advanced Settings" on page 66.

Configuring GPS

The Skyus 300 incorporates a GPS receiver. The GPS receiver can determine your current location, often even indoors. Current location information can be shared with connected devices by using the Local Streaming feature on the Local tab.

To configure GPS, select **>** from any Home page panel and then select **GPS** from the Web UI side menu.

The GPS page includes three tabs:

- Status Tab

- Local Tab

- Remote Tab

Status Tab

Use settings on this tab to enable or disable GPS and to view the current status of your GPS connection.

Enable GPS receiver

This setting enables or disables the GPS radio on your device. When the **ON/OFF** slider is **ON**, the device acquires GPS and makes the data available to applications running on the device. A GPS Agreement appears, click **Confirm** to proceed. When **OFF**, no GPS data is available.

Status: The current status of your GPS connection. When searching, the device is making the connection to satellites in order to populate GPS data.

Latitude: Latitude for the last location fix.

Longitude: Longitude for the last location fix.

Speed: Speed the device is traveling at.

Altitude: Altitude for the last location fix.

Accuracy: A measure of the accuracy of the horizontal position obtained by the GPS receiver.

Direction: Direction the device is traveling relative to North.

Local Tab

GPS data is provided by the Skyus 300 in the form of a National Marine Electronics Association (NMEA) text stream. Using a NMEA (GPS) port is a standard method for applications to access a GPS data stream in Windows and other computing platforms.

To create this port, you must download and install the GPS over Wi-Fi driver for your platform. This driver will create the NMEA port, obtain GPS data from the Skyus 300, and make this GPS data available to NMEA-aware applications.

Once you have created the port, use this tab to turn on Local GPS.

Turn on local GPS: Check this box to turn on local GPS.

Port number: The port number used by the driver software on your computer to establish a connection to the Skyus 300 and obtain GPS data. Unless there is a good reason to do so, you should not change the port number. Acceptable port values are between 1024 and 65535.

Click **Save Changes** to update settings.

Remote Tab

Use this tab to configure the system to stream GPS data to remote servers. **NOTE:** These servers are not IoT Connect. Use the **Remote Management** page to configure IoT Connect remote servers.

Global device ID: The 4-digit unique ID specific to your Skyus 300 that is inserted into your GPS packet for routing to remote servers.

GPS Remote Server Configurations

Add remote server: Use this button to add a remote server. The **Add GPS Remote Server** dialog appears with the following options:

- **Server name** — Enter a name for the GPS remote server.

- **Odometer value** — To utilize this feature, input the current Odometer reading from your vehicle. Once set, the Skyus 300 will monitor distance traveled and add to this value. For example, if you set this to 0 and you drive 10 miles, the value will be 10; if you set this to 100 and drive 10 miles, the value will be 110. **NOTE:** You can only set one odometer value, which will serve as the value for all GPS remote servers.

- **Report current odometer value** — You have the option to track this data, but not report it to remote servers in order to save data usage. If this box is un-checked, the device will not report the odometer value to remote servers.

GPS Report Server

- **Reporting** — To begin streaming GPS data from your Skyus 300 to the remote server, check this box.

- **Store & forward** — If there is an interruption in the WAN interface, the system can store packets and forward them once the WAN interface connection returns. Check this box if you want the system to store and forward packets.

- **Server address** — Enter the address for the remote server to which you would like to route packets.

- **Port number** — Enter the port for the remote server to which you would like to route packets. Acceptable port values are between 1024 and 65535.

- **Network protocol** — Select the protocol to use for routing packets to your remote serve from the drop-down (TCP or UDP).

NMEA/TAIP Reporting

The Skyus 300 is capable of routing NMEA or TAIP sentences to the remote server.

Select **NMEA** or **TAIP**. The available options for your selection are displayed. Select or de-select any option. All options that are checked will be part of the packet routed to the remote server.

Reporting Triggers

- **Time interval** — You can set a time interval to trigger when packets will be routed to the remote server. For example, if you select 15 minutes, a GPS packet will be sent to the remote server 15 every minutes.

  Check the box if you want to use the time interval and enter a value between 5 and 60 minutes.

- **Distance interval** — You can set a distance interval to trigger when packets will be routed to the remote server. For example, if you select 1000 feet, a GPS packet will be sent to the remote server every time your device moves 1000 feet.

  Check the box if you want to use the distance interval and enter a value between 130 and 215009 feet.

  NOTE: You can choose both Time and Distance as your interval specification. The device will route packets based on which event occurs first.

- **Stationary Timer** — You can set a stationary timer that monitors for movement and only route packets if the Skyus 300 is continuously moving within the time range. For example, if you set this value to 1 minute and your router has not moved within 1 minute, a packet will not be routed. Once your device begins registering GPS movement again, packet routing will resume.

Check the box if you want to use the stationary timer and enter a value between 60 and 15300 seconds.

Click **Save Changes** to implement your settings or **Cancel** to cancel. You return to the Remote page. The new remote server is now listed.

Use the **View**, **Edit**, and **Delete** buttons to view, edit, or delete listed remote servers.

Managing VPN

The Skyus 300 allows you to create IPSEC VPNs to establish secure connections to remote networks over a public network.

To configure VPN, select **>** from any Home page panel and then select **VPN** from the Web UI side menu. The VPN page appears.

VPN Page

VPN Service

This setting enables or disables IPSEC VPN service on your device. When the **ON/OFF** slider is **ON**, VPN is enabled. When **OFF**, VPN service is not available.

VPN Tunnel Configurations

Once such a tunnel is added, the page would display the list of tunnel configurations. Administrator can delete, edit, view, change priorities of the tunnel configurations.

Add new VPN tunnel: Use this button to add a new VPN tunnel. The Add New VPN Tunnel Dialog appears:

Add New VPN Tunnel: Step 1 out of 5

General Settings

- **Start tunnel** — Select whether to start the tunnel automatically upon start up or manually.

- **Enable tunnel** —Check this box to enable the tunnel.

- **Tunnel name** — Enter a unique name to identify this VPN.

- **Local identity** — Enter a unique name to identify the local point of the tunnel.

- **Remote identity** — Enter a unique name to identify the remote point of the tunnel.

- **Local Authentication** — Select **Pre-shared Key** from the drop-down list. This is currently the only form of authentication available with Skyus 300.

- **Pre-shared key —** Enter a password used to authenticate to your end of the tunnel (usually matches the remote password.)

- **Remote Authentication** — Select **Pre-shared Key** from the drop-down list. This is currently the only form of authentication available with Skyus 300.

- **Pre-shared key —** Enter a password used to authenticate the remote end of the tunnel (usually matches the local password).

Add New VPN Tunnel: Step 2 out of 5

Local Network

- **Local IP** — Enter the WAN IP address of local device. **NOTE:** This should be a static IP that you are able to reach from remote device (no NAT).

- **Local Subnet Mask** — Enter the subnet mask of the local device, for example: If your local IP is 192.168.0.100 and your subnet mask is 255.255.255.0 this should be **192.168.0.0/24**. **NOTE:** This should mirror what the subnet displays in the local device, for example: 192.168.0.0 / 255.255.255.0. **NOTE:** The local device should be on a different subnet from remote, for example: If the Remote Subnet Mask is **192.168.1.0/24**, the Local Subnet Mask might be **192.168.0.0/24**. This is usually based off the DHCP settings of the devices.

Remote Network

- **Remote IP** — Enter the WAN IP address of remote device. **NOTE:** This should be a static IP that you are able to reach from local device (no NAT).

- **Remote Subnet Mask** — Enter the subnet mask of the remote device, for example: If your remote IP is 192.168.0.100 and your subnet mask is 255.255.255.0 this should be **192.168.0.0/24**. **NOTE:** This should mirror what the subnet displays in the local device, for example: 192.168.0.0 / 255.255.255.0. **NOTE:** The remote device should be on a different subnet from local, for example: If the Local Subnet Mask is **192.168.1.0/24**, the Remote Subnet Mask might be **192.168.0.0/24**. This is usually based off the DHCP settings of the devices.

Add New VPN Tunnel: Step 3 out of 5

IKE Phase 1

Select desired items from each column.

NOTE: Each phase should support at least one matching option in each column. For example, if Phase 1 on this page is configured to support Hash SHA2 512, SHA2 384, and SHA2 256, then at least one of those selections must be selected in Phase 2 on the next page in order for there to be a common Hash.

Add New VPN Tunnel: Step 4 out of 5

IKE Phase 2

Select desired items from each column.

NOTE: Each phase should support at least one matching option in each column. For example, if Phase 1 on the previous page is configured to support Hash SHA2 512, SHA2 384, and SHA2 256, then at least one of those selections must be selected in Phase 2 on the this page in order for there to be a common Hash.

Add New VPN Tunnel: Step 5 out of 5

Dead Peer Detection (DPD) is a keep-alive method that ensures the tunnel is up and will take action if it is not able to reach the remote side of the tunnel, depending on what DPD action you select. You can use the default values, if desired.

Dead Peer Detection

Enable: Check this box to enable DPD.

DPD Action: Use the drop-down to select a DPD action.

DPD Delay: The number of seconds between DPD packets.

DPD Timeout: The number of seconds the router will allow an IPsec session to be idle before beginning to send DPD packets to the peer machine.

Managing I/O Settings

The Skyus 300 includes I/O pins, including an ignition monitor and configurable digital General Purpose Input Output (GPIO) pins. Page 14 shows the placement of GPIO pins in the Skyus 300 cable harness.

To configure I/O settings, select **>** from any Home page panel and then select **I/O Settings** from the Web UI side menu. The I/O Setting page appears.
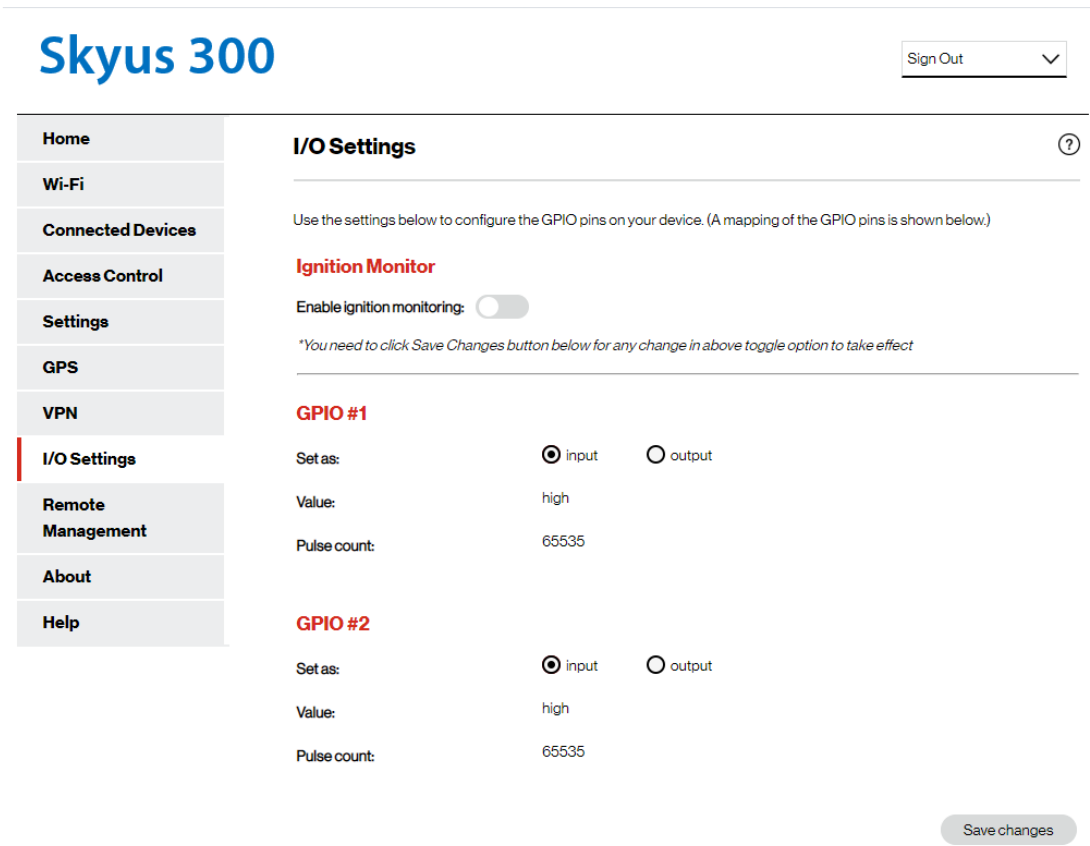
I/O Settings Page

Use settings on this tab to enable or disable the ignition monitor and view or configure pin settings.

NOTE: When using Skyus 300 in vehicles, enable the ignition monitor to ensure a controlled shutdown of the router when the vehicle is turned off.

Ignition Monitor

Enable ignition monitoring: This setting enables or disables the ignition monitor on your device. When the ON/OFF slider is **ON**, the Skyus 300 turns on and off (with time delay) with the ignition. When **OFF**, the ignition monitor is not available.

If ignition monitor is enabled, you can set the amount of time (in seconds) you want the router to remain on after the ignition is turned off.

GPIO #1

Set as: Select **input** or **output**.

NOTE: Input is used to tell the Skyus 300 the state of an external device or system. Output is used to turn another device or system on (low) or off.

If you select input:

Value: The current state of the pin: Low or High.

Pulse Count (visible for INPUT): Displays the number of times the Value field has moved from Low to High or High to Low. **NOTE:** To reset the pulse count to zero, reset the device to the factory default settings.

If you select output:

Set output: Select **off** or **low**.

GPIO #2

Set as: Select input or output.

If you select input:

Value: The current state of the pin: Low or High.

Pulse Count (visible for INPUT): Displays the number of times the Value field has moved from Low to High or High to Low. **NOTE:** To reset the pulse count to zero, reset the device to the factory default settings.

If you select output:

Set output: Select **off** or **low**.

Click **Save Changes**.

Configuring Remote Management

Remote management allows you to enable server reporting with IoT Connect™. IoT Connect is a cloud platform product that provides 360 degree visibility and secure accessibility into your deployment from a single platform. You must have IoT Connect installed to use the Remote Management feature.

To configure remote management, select **>** from any Home page panel and then select **Remote Management** from the Web UI side menu. The Remote Management page appears.
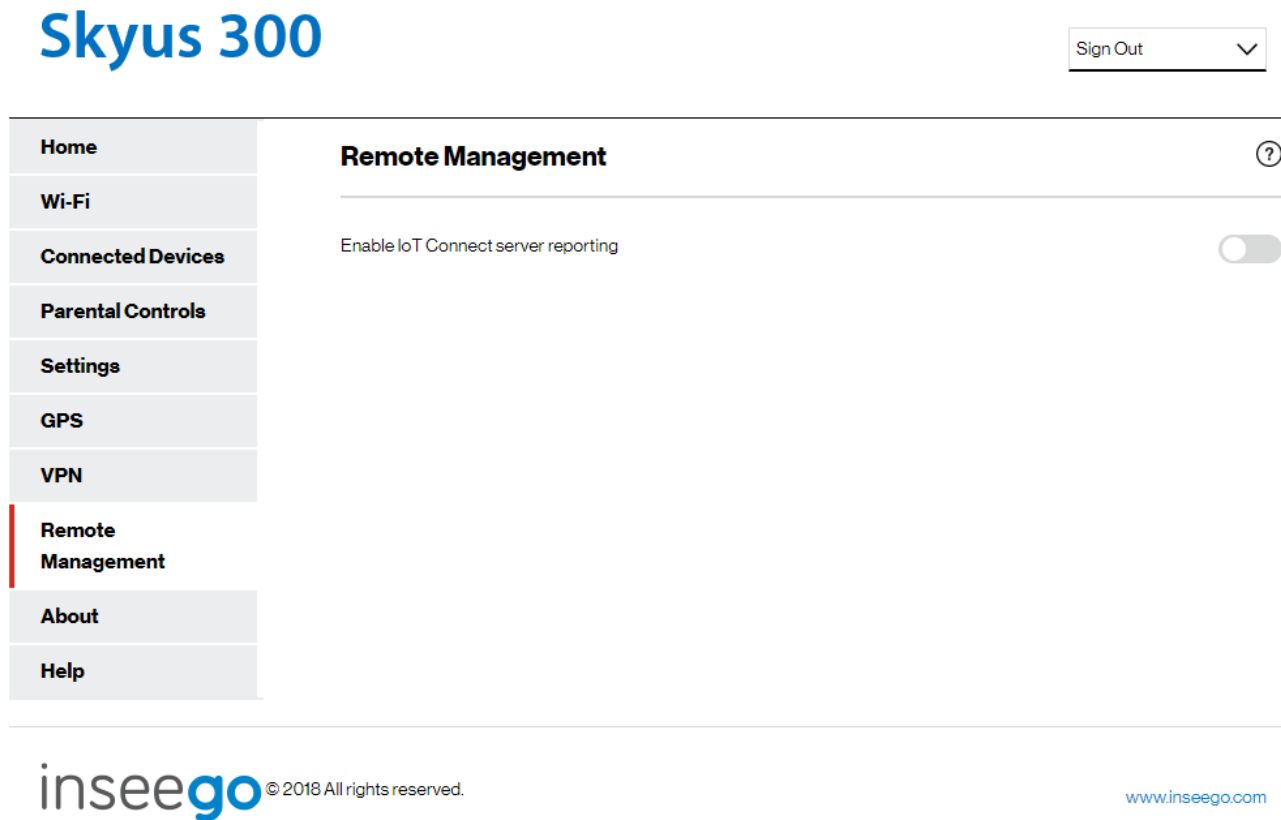
Remote Management Page

Enable IoT Connect server reporting: This setting enables or disables server reporting with IoT Connect on your device.

Remote Server

Connection State: A report on your router's connection to the IoT Connect server. **Up** indicates Skyus 300 is communicating with IoT Servers. **Down** means Skyus 300 is not communicating with IoT Connect servers.

Last reported: The time when your router last sent a packet to the IoT Connect servers.

Configurations

NOTE: You can change the configuration information by clicking the **Change Configuration** button.

Verbose reporting: Check this box to utilize verbose reporting. This enlarges the size of the packets your router sends to IoT Connect and can slow down performance. You will still be able to use Connection Up or Down, data usage measurements, alarms, and commands.

Name: This static value shows that this server configuration is for IoT Connect services. **NOTE:** Editing this field can affect your ability to utilize IoT Connect services.

Server URL: The server your router is communicating with. This must be the URL where your router is registered.

Server port: This static value is provided to show which port your router is using for communication with IoT Connect.

Server Password: The password that was used to register your Skyus 300. **NOTE:** Editing this field can affect your ability to utilize IoT Connect services.

Traffic type: This static value is provided to show that the router is communicating via Inseego's protocol.

Exclude GPS: Check this box if you do not want the Skyus 300 to send GPS information to the IoT Connect server.

Reporting interval: This is the interval at which your device will send packets into the IoT Connect server. **NOTE:** A shorter interval means more data usage.

Reset credentials: This button clears credentials and resets all your remote server configurations back to the default (IoT Connect) settings.

Change configuration: This button brings up the **Change Remote Server Configuration** dialog, where you can change the configuration information shown on this page.

Viewing Info About the Router

On the Web UI Home page, the About panel shows current Internet status (Connected or Not Connected or Dormant), the name of the network to which the router is connected, and time connected.

To view more detailed information about your router and its use, select **>** from the Home page About panel (or select **About** from the Web UI side menu).

The About page includes five tabs:

- General Status Tab

- Primary WAN Tab

- Ethernet WAN Tab

- Wi-Fi as WAN Tab

- System Status Tab

General Status Tab

Use the General Status tab to view general Internet connection and system information.

General

- **Connection Status:** Indicates whether your router is connected to WAN.

- **Session Connection Time:** The amount of time that has elapsed since the connection for the current Internet session was established.

- **Active Interface**: The WAN interface that is active (Ethernet WAN, Primary WAN, Wi-Fi as WAN, or None).

- **Session Data Tx:** The amount of data transmitted for the current Internet session. This counter starts at zero when the connection is established.

- **Session Data Rx:** The amount of data received for the current Internet session. This counter starts at zero when the connection is established.

System

- **Manufacturer:** The manufacturer of this router.

- **Model Name**: The model name for this device.

- **Model Number**: The model number for this device.

- **Model Version**: For the 4G modem component, this is the version of the firmware (software) currently installed.

- **System Version**: The version of currently installed software.

Primary WAN Tab

Use this tab to view details about your Primary WAN connection.

General

- **Radio Access Technology:** Indicates the current cellular data connection, for example, LTE.

- **IMEI:** The International Mobile Equipment Identity (IMEI) for this device. This is a 15 or 17 digit code used to uniquely identify an individual mobile station on a LTE network. The IMEI does not change when the SIM is changed.

- **SIM Status:** The status of the SIM card. If the SIM card is missing, or this field indicates some form of SIM error, connection to the mobile network is not possible.

- **ICCID:** The unique ID number assigned to the SIM card. This field is blank if there is no SIM card installed, or a SIM error condition exists.

IP Address and Signal

- **IPv4 Address:** The Internet IP address assigned to the router.

- **IPv6 Address:** The global IPv6 address for the router. This will be blank if IPv6 is turned off or is not supported by the current network connection or carrier.

- **Signal Strength:** The strength of the LTE signal, measured in dBm. Higher absolute values indicate a stronger signal, for example: -80 dBm is a stronger signal than -90 dBm. **NOTE:** LTE signal strength is typically lower than 3G signal strength.

Use this tab to view details about your Ethernet WAN connection.

IP4

- **IPv4 Address:** The Internet IP address assigned to the Skyus 300.

- **IPv4 Subnet Mask:** The network mask associated with the IPv4 address.

- **IPv4 Gateway:** The gateway IP address associated with the IPv4 address.

- **IPv4 DNS:** The Domain Name Server currently used by this device.

IP6

- **IPv6 Address:** The global IPv6 address for the Skyus 300. If IPv6 is turned off, or is not supported by the current network connection, this appears blank.

- **IPv6 Subnet Mask:** The network mask associated with the IPv6 address.

- **IPv6 Gateway:** The gateway IP address associated with the IPv6 address.

- **IPv6 DNS:** The Domain Name Server currently used by this device.

Wi-Fi as WAN Tab

Use this tab to view details about your Wi-Fi as WAN connection.

General

- **SSID:** The network name of Wi-Fi network.

- **BSSID:** The MAC address of Wi-Fi network.

- **Security:** The security type of the Wi-Fi network.

IP Address and Signal

- **Signal Strength:** The received signal strength indicator (RSSI) value.

- **Mode:** The mode setting of the Wi-Fi network connection.

- **Channel:** The channel setting of the Wi-Fi network connection.

- **IP Address:** The IP address assigned to the router.

Use this tab to view details about your system status.

General

- **Ethernet Clients:** The number of clients connected by Ethernet.

- **GHz Clients:** The number of clients connected at 2.4 GHz band.

- **5 GHz Clients:** The number of clients connected at 5 GHz band.

4

Advanced Settings

Overview

The Advanced Settings pages are intended for users with technical expertise in the area of telecommunication and networking.

WARNING! Changing the Advanced settings may be harmful to the stability, performance, and security of the Skyus 300.

When you select the **Advanced** tab on the Settings page, a warning message appears. If you click **Continue**, the LAN tab of the Advanced Settings page appears.

The Advanced Settings page includes eight tabs:

- LAN

- Manual DNS

- Network

- Firewall

- MAC Filter

- Port Filtering

- Port Forwarding

- WAN Configuration

LAN

This tab provides settings and information about the Skyus 300's local area network (LAN). For this device, the LAN consists of this device and all Wi-Fi and Ethernet connected devices.

IPv4

IP address: The IP address for this device, as seen from the local network. Normally, you can use the default value.

Subnet mask: The subnet mask network setting for the Skyus 300. The default value 255.255.255.0 is standard for small (class "C") networks. If you change the LAN IP Address, make sure to use the correct Subnet Mask for the IP address range of the LAN IP address.

MAC address: (read-only) The Media Access Controller (MAC) Address for the Wi-Fi interface on this device. The MAC address is a unique network identifier assigned when a network device is manufactured.

Turn on DHCP server: This checkbox turns the DHCP Server feature on or off. This should be left checked. The DHCP server allocates an IP address to each connected device. **NOTE:** If the DHCP Server is turned off, each connected device must be assigned a fixed IP address.

DHCP lease time: The number of minutes in which connected devices must renew the IP address assigned to them by the DHCP server. Normally, this can be left at the default value, but if you have special requirements, you can change this value.

Start DHCP address range at: The start of the IP address range used by the DHCP server. If the IP is set on the client device, use an IP address outside of this DHCP range; if the IP address is set using an IP reservation, it will usually be inside this range. **NOTE:** Only expert users should change this setting.

End DHCP address range at: The end of the IP address range used by the DHCP server. If the IP is set on the client device, use an IP address outside of this DHCP range; if the IP address is set using an IP reservation, it will usually be inside this range. **NOTE:** Only expert users should change this setting.

Use Reserved IP Addresses: This allows you to ensure that a connected device will always be allocated the same IP Address by the Skyus 300. To use this feature, click the **Reserve specific IP addresses for selected devices** link. A list of devices with their MAC Address, Current IP Address, and a field to enter a Reserved IP Address appears.

Click **Save Changes** to activate and save new settings.

Manual DNS

The Skyus 300 automatically selects a Domain Name Server (DNS). This tab allows you to manually assign up to two DNS IP addresses.

Turn on manual DNS: Check this box to manually select a DNS.

DNS 1 IP address: Enter the IP address for the primary DNS. This address is required to use the Manual DNS feature.

DNS 2 IP address: Enter the IP address for the secondary (backup) DNS. This address is optional and may be left blank if desired.

Click **Save Changes**.

Network

In most configurations, the Skyus 300 is used with a dynamic IP and SIM and the Access Point Name (APN) is available from the network, for example: *vzwinternet*. However, if you are on a private network, you may need to set the APN on this tab for the network to communicate with the Skyus 300, for example: we01.*vzwstatic*.

APN

Internal Modem: Enter the APN for your private network.

CAUTION: Changing the internal modem APN may cause a loss of data connectivity and disconnect you from the Web UI.

Click **Save APN Changes**. The router will reboot for changes to take effect.

External Modem: This option is configurable if you have a Skyus DS2 connected to the external USB port of your Skyus 300. In this case, enter the APN for your private network.

CAUTION: Changing the external modem APN may cause a loss of data connectivity and disconnect you from the Web UI.

Click **Save APN Changes**. The router will reboot for changes to take effect.

Firewall

The Skyus 300 firewall determines which Internet traffic is allowed to pass between the router and connected devices and protects your connected devices from malicious incoming traffic from the Internet. The firewall cannot be turned off.

Use the Firewall tab to adjust the general security level of the firewall, designate a specific device to receive all traffic, and set up specific firewall rules.

Security Level

You can select from three general security levels to block traffic into and through the Skyus 300. The default Security Level is Medium.

- **Low** — allows inbound traffic to services with open ports matching the inbound request port. Outbound traffic is allowed to any service.

- **Medium** — Rejects inbound traffic. Outbound traffic is allowed for any service.

- **High** — Rejects inbound traffic. Outbound traffic is allowed only for TELNET (port 23), FTP (port 21), HTTP (port 21), HTTP (port 80), HTTPS (port 443), SMTP (port 25), DNS (port 53), POP3 (port 110), and IMAP (port 143).

Click **Save Changes**.

DMZ

DMZ allows the connected device specified as the DMZ IP address (the DMZ destination) to receive all traffic that would otherwise be blocked by the firewall.

NOTE: Allowing DMZ may assist some troublesome network applications to function properly, but the DMZ device should have its own firewall to protect itself against malicious traffic.

Allow DMZ: Check this box to allow DMZ.

Destination IP Address: Enter the IP address of the connected device you wish to become the DMZ device (the DMZ destination). **NOTE:** You can check the IP address of each connected device on the Connected Devices screen.

Click **Save Changes**.

Firewall Rules

You can define one or more specific rules for the firewall to follow. Use the fields to set up a rule, and click **Add New Rule**. New rules are added to the bottom of the list. Use **Up** and **Down** to reposition rules on the list.

NOTE: For **Src. IP** and **Dest. IP**, enter a specific IP address or the keyword **any**.

MAC Filter

The MAC filter allows only selected devices to access the Skyus 300's Primary Wi-Fi network. By default, MAC filter is turned OFF.

Use this tab to turn the MAC Filter ON and specify device access.

NOTE: The MAC filter has no effect on devices connected to the Guest Wi-Fi network or connected via Ethernet.

MAC Filter

To use the MAC filter, select the device(s) from the device list that you want to be allowed to connect to the Primary network and move the **ON/OFF** slider to **ON**.

CAUTION: Turning on MAC filtering immediately disconnects all devices that are not included in the filter from the Primary network.

Device List

This list includes all devices currently connected to the Skyus 300, except those connected via Ethernet.

Add New Device: Use this button to add a device to the device list, then enter the device name, MAC address, choose whether to select the MAC Address Filter checkbox, and click **Save Changes**.

To delete a device from the list, select its **Delete** checkbox and click **Save Changes**.

To discard any unsaved changes and refresh the list, click **Refresh List**.

Notes on Blocking Devices

There are two ways to block devices from connecting to the Skyus 300:

- **Temporarily block a device from connecting to the router via the Primary and Guest networks and via Ethernet.**

  To use this method, go to the **Connected Devices** page and click the **Block** button next to the device.

- **Permanently block a device from connecting to your router's Primary network only.**

  Use the **MAC Filter**.

When blocking devices, the following information applies:

- Devices blocked with **Connected Devices > Block** are blocked from the Wi-Fi network, even if the **MAC Filter** is ON and the device is enabled for the MAC Filter.

- If the **MAC Filter** is ON, and a device is blocked with **Connected Devices > Block**, and is not enabled for the MAC Filter, then it will not be able to connect. Both the MAC Filter and the Block prevent connection.

- If the **MAC Filter** is ON, and a device is enabled for the MAC Filter, then the device will be able to connect. However, it can still be blocked using **Connected Devices > Block** or by disabling the **MAC Filter**.

Port Filtering

Port Filtering allows you to block outgoing Internet connections and permit only selected applications to access the Internet. Traffic is identified by port numbers. Some applications are pre-defined. You can define additional applications if you know the details of the traffic used and generated by the applications.

NOTE: You can also view the current Port Filtering setting (ON/OFF) in the Settings panel on the Web UI Home page.

Port Filtering

To turn on port filtering, move the **ON/OFF** slider to **ON**.

To turn off port filtering, so that any application can connect to the Internet, move the slider to **OFF**.

Applications

Select the applications you want to be able to access the Internet and click **Save Changes**.

The following table provides port numbers and protocol information for each port filtering application listed.

Application Name	Port	TCP*	STCP*	UDP*
Email				
POP3	110	Yes	No	Assigned
POP3S	995	Yes	No	Yes
IMAP	143	Yes	No	Assigned
IMAPS	993	Yes	No	Assigned
SMTP	25	Yes	No	Assigned
SecureSMTP	465	Yes	No	No
FTP control (command)	21	Yes	Yes	Assigned
FTP data transfer	20	Yes	Yes	Assigned
HTTP	80	Yes	Yes	Assigned
HTTPS	443	Yes	Yes	Assigned
Telnet	23	Yes	No	Assigned

---

* **Yes** indicates the protocol is standardized for the port number.
No indicates the protocol is standardized for the port number.
Assigned indicates the port number is assigned by IANA (Internet Assigned Numbers Authority) for protocol use, but may not be standardized.

Custom Applications

You can define up to ten custom applications.

Add custom application: Use this button to add a new row to the custom application list.

- **On:** Check this box if you want the new application to be able to access the Internet.

- **Application Name**: Enter a name for the custom application.

- **Start Port:** Enter the beginning of the range of port numbers used by outgoing traffic for the custom application being added.

- **End Port:** Enter the end of the range of port numbers used by the application.

- **NOTE:** If the application uses a single port instead of a range, type the same value for both the **Start Port** and the **End Port**.

- **Protocol:** Select the protocol used by the port range from the drop-down list (TCP, UDP, or both).

- **Delete:** Check this box to delete a custom application. **NOTE:** Click on the Port Filtering tab again to remove deleted custom applications from view on the screen.

Click **Save Changes** to save any changes made to the custom applications.

Port Forwarding

Port Forwarding allows incoming traffic from the Internet to be forwarded to a particular computer or device on your Wi-Fi network. Normally, the built-in firewall blocks incoming traffic from the Internet. Port forwarding allows Internet users to access any server you are running on your computer, such as a Web, FTP, or Email server. For some online games, port forwarding must be used in order for the games to function correctly.

IMPORTANT: Port forwarding creates a security risk and should not be turned on unless it is required.

Some mobile networks provide you with an IP address on their own network rather than an Internet IP address. In this case, Port Forwarding cannot be used, because Internet users cannot reach your IP address.

Port Forwarding

To turn on port forwarding, move the **ON/OFF** slider to **ON**.

To turn off port forwarding, so that any application can connect to the Internet, move the slider to **OFF**.

Port Forwarding Applications

Check the box next to each Port Forwarding application that you want to allow.

If you want to limit service for an application to a single connected device, enter the IP address of the target device in the application's **IP Address** field.

Click **Save Changes**.

The following table provides port numbers and protocol information for each port forwarding application listed.

Application Name	Port	TCP*	STCP*	UDP*
DNS	53	Yes	No	Yes
FTP control (command)	21	Yes	Yes	Assigned
FTP data transfer	20	Yes	Yes	Assigned
HTTP	80	Yes	Yes	Assigned
HTTPS	443	Yes	Yes	Assigned
NNTP	119	Yes	No	Assigned
POP3	110	Yes	No	Assigned
POP3S	995	Yes	No	Yes
SMTP	25	Yes	No	Assigned
SecureSMTP	465	Yes	No	No
SNMP	161	Assigned	No	Yes
Telnet	23	Yes	No	Assigned
TFTP	69	Assigned	No	Yes

---

* **Yes** indicates the protocol is standardized for the port number.
No indicates the protocol is standardized for the port number.
Assigned indicates the port number is assigned by IANA (Internet Assigned Numbers Authority) for protocol use, but may not be standardized.

Custom Applications

You can add up to ten custom applications. Once defined, these applications can be turned on and off the same way as pre-defined applications.

Add Custom Application: Use this button to add a new row to the custom applications list.

- **On:** Check this box if you want the application to be able to access the Internet (enabling port forwarding).

- **Application Name:** Enter a name for the custom application.

- **IP Address:** If you want to limit service for the application to a single connected device, enter the IP address of the target device. To find the IP address of a device, go to the Connected Devices page. **NOTE:** To ensure the device you are forwarding to does not have a different IP address after a reboot, either statically assign the IP address on the client device, or set up a DHCP reservation.

- **Port Type:** Select Range or Translate from the drop-down list.

- **Port Numbers:** Use the **From** and **To** fields to specify the range of port numbers to be forwarded. **NOTE:** If the application uses a single port instead of a range, type the same value in both the **From** and **To** fields.

- For translate ports, use the **Ext.** and **Int.** to specify ports. **NOTE:** Forwarding takes inbound traffic on a port to the same port on a client device. Use translate ports to send traffic to a different port on the client device. For example, instead of having inbound traffic on port 1234 forward to port 1234 of the client device, you can have it forward to port 5678.

- **Protocol**: Select the protocol used by the port range from the drop-down list (TCP, UDP, or both).

- **Delete:** Check this box to delete a custom application. **NOTE:** Click on the Port Forwarding tab again to remove deleted custom applications from view on the screen.

Click **Save Changes** to save any changes made to the custom applications.

WAN Configuration

Use this tab to configure and set the priority of each available WAN interface.

Active WAN Interface

This section displays current active WAN interfaces.

Priority Listing of the Available WAN Interfaces

Use the drop-downs to reset the priorities you wish for WAN interfaces.

WAN Settings

Use the tabs to set the following for each WAN interface.

- **WAN interval** — How often the router verifies a connection on this interface, in minutes. **NOTE:** A shorter interval will use more router resources and more data, while a longer interval may delay detection of issues.

- **WAN ICMP host 1** — The IP address of the host. This must be a stable Internet address.

- **WAN ICMP host 2** — The IP address of the host. This must be a stable Internet address.

- **WAN ICMP host 3** — The IP address of the host. This must be a stable Internet address.

- **WAN timeout** — The amount of time the router waits between verification attempts, in minutes, before determining the verification has failed. **NOTE:** A shorter amount of time may create false positive results, while a longer amount of time may delay detection of issues.

- **WAN retries** — The number of times the router attempts to verify the connection on this interface before the connection is considered failed. **NOTE:** A smaller value may create false positive results, while a larger value may delay detection of issues.

- **WAN recovery retries** — The number of successful checks a failed connection requires before it is considered active again.

5

Product Specifications and Regulatory Information

Product Specifications

Regulatory Information

Wireless Communications

Limited Warranty and Liability

Safety Hazards

Installation and Operating Instructions

Product Specifications

Device

Name:	Skyus 300
Model Number:	SKR3MD8800
Marketing Name/Model Name	SK300V
Carrier Support:	Verizon
Cellular Certification:	GCF
Housing:	Ruggedized Aircraft Grade Aluminum
Dimensions:	121.5 x 155.7 x 47.1 mm (4.783 x 6.13 x 1.85 in)
Weight:	1.2 kg (2.65 lbs)
Installation:	Integrated holes; 3.9mm hole diameter for M3 or M3.5 (#4 or #6) screws (16+1.8mm)

Environmental

Operating Temperature:	-40 – 70 °C (-40 – 158 °F)
Ambient Temperature:	-40 - 70 °C (-40 – 158 °F)
Storage Temperature:	-40 – 85 °C (-40 – 185 °F)
Temperature Code:	T4
Ingress Protection:	IP64 Dust Proof Water Resistant

Device Certifications / Standards

Regulatory	FCC, ISED
Device Testing	SAE J1455 (Shock, Vibration, Electrical), MIL-STD 810G (Shock, Vibration, Thermal Shock, Humidity), RoHS2 Green, REACH, WEEE, UL 60950 Safety, Wi-Fi Alliance
Class 1 Division 2 (C1D2) Rating	9-32V, 3A

Cellular

LTE Cat-18 (1.2 Gbps downlink, 150 Mbps uplink); up to five Carrier Aggregation and 256 QAM	
NA Coverage	LTE: B2, B3, B4, B5, B7, B13, B14, B20, B46 (TD), B48 (TD), B66, 3G (WCDMA): B1, B2, B5, B8, 2G (CDMA): BC0, BC1, BC10
Unlicensed Band Coverage	LTE: B46 (TD LTE-LAA), B48 (TD CBRS 3600)
Carrier Acceptance	Verizon

Wi-Fi

802.11 a/b/g/n/ac WAVE2

2 x .2.4 GHz Radio

2 x 5 GHz Radio

Dual concurrent (Mobile SKU only)

Access Point/Client Mode

Positioning

aGPS and aGNSS (Standalone and Assisted)

Dead Reckoning[*]

Local/Remote Forwarding

Store and Forward (Mobile SKU only)

Dual Modem Support

Supports Skyus DS2 and Skyus SC USB WAN Modems

Supports Inseego 5G NR WAN Modems

Intelligent WAN Prioritization

Bluetooth*

BT5*, BLE Long Range

GATT, MESH, SPP

Store and Forward (Mobile SKU only)

Power

9 – 32 VDC, 3 A Input Voltage

12 VDC @ 3.75 A (45 W) Max Power Consumption

12 VDC @ 3 mA (36 mW) Min Power Consumption

Withstands 5V Engine Cranking and 5V Brownouts

Surge Protection From -600 – 200 VDC Spikes

Interfaces

2x RJ45 10/100/1000 Ethernet

1x RJ45 10/100 Serial over Ethernet

1x USB 2.0 Type A Host

---

[*] For future release

1x 8-Pin Molex Mini-Fit Latching Power and I/O	
2x Accessible 4FF Nano SIM Slots	

Antenna Connections

Mobile	2x SMA for LTE Cellular Multi-In Multi-Out (MIMO)
	2x RP-SMA for Wi-Fi MIMO
	1x RP-SMA for Bluetooth*
	1x SMA for GPS
Fixed	4x SMA for LTE Cellular Multi-In Multi-Out (MIMO)
	2x SMA for Ultra-High Band (CBRS/LAA) Cellular

SIM

2x Accessible 4FF Nano SIMs (1 available for this release)
Access on Side of Device Using T7 Torx Driver
SIM Slot 1 (Left) is Primary

USB Host

5V @ 1A (5W Supply)
Up to 480 Mbps from External USB Modem

LEDs

1x Device Health
1x Cellular Status and Signal Strength
1x Wi-Fi Status
1x GPS Status
1x BT Status
1x USB Status

Software

OS Compatibility	Windows 7 or Later, Linux 2.6 or Later, Ubuntu 12.04 or Later, Raspbian 2.0 or Later, Android Jelly Bean or Later, iOS8 or Later
Security	**IPsec VPN,** Port Filtering, MAC Filtering, IP Filtering, DMZ, Encrypted Log Files, Encrypted Configurations, WPA/WPA2 Authentication, Wi-Fi Privacy Separation
Networking	DHCP Server, Network Address Translation, WAN Failover, Port Forwarding, URL Filtering

---

* For future release

Remote Networking and Alerting	Inseego IoT Connect Cloud Platform
	Customizable Dashboard, Alerts, Alarms, and Actions Based on Smart Rules
	Secure Remote Visibility and Device Management, Remote Configuration and FOTA, MQTT Encryption with x.509 Certificates

Inputs/Outputs

1x Voltage In

1x Ground

1x Ignition monitor Input

1x 1-Wire Input

4x GPIO (2x available at launch)

Warranty and Services

Industry Leading Warranty, Inseego IoT Connect Options Available

Inseego Care Support and Advanced Replacement Options Available

Skyus Provisioning Available to Apply Custom Templates and Verify Device Activation Prior to Shipment

Regulatory Information

MODEL NUMBER: SKR3MD8800

FCCID: PKRISGSKR3MD8800

FEDERAL COMMUNICATIONS COMMISSION NOTICE (FCC - UNITED STATES)

Electronic devices, including computers and wireless modems, generate RF energy incidental to their intended function and are therefore subject to FCC rules and regulations.

This equipment has been tested to, and found to be within the acceptable limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment.

This equipment generates radio frequency energy and is designed for use in accordance with the manufacturer's user manual. However, there is no guarantee that interference will not occur in any particular installation. If this equipment causes harmful interference to radio or television reception, which can be determined by turning the equipment off and on, you are encouraged to try to correct the interference by one or more of the following measures.

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and the receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/television technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation of the device.

FCC RF Radiation Exposure Content:

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter, except in accordance with FCC multi-transmitter product procedures.

2. This equipment is authorized only for Fixed or Mobile applications and is required to be installed as such.

3. This equipment must be installed and operated with a minimum separation of 20 cm (8 in.) between the equipment and users/bystanders at all times.

Cellular External Antenna Considerations:

1. External Antenna(s) Included: There are no included external antennas.

2. To comply with FCC RF Exposure Requirements, the Maximum Cellular Antenna Gain Must Not Exceed 6 dBi.

INNOVATION, SCIENCE AND ECONOMIC DEVELOPMENT (ISED) CANADA STATEMENT

ISED RSS-Gen Notice:

This device complies with Industry Canada's licence-exempt RSSs. Operation is subject to the following two conditions:

1. This device may not cause interference; and

2. This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1. l'appareil ne doit pas produire de brouillage;

2. l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

ISED RF Exposure Guidance:

In order to comply with FCC/ISED RF Exposure requirements, this device must be installed to provide at least 20 cm separation from the human body at all times.

Afin de se conformer aux exigences d'exposition RF FCC / ISED, cet appareil doit être installé pour fournir au moins 20 cm de séparation du corps humain en tout temps.

ISED ICES-003 Notice: CAN ICES-3 (B)/NMB-3(B)

Wireless Communications

IMPORTANT: Due to the transmission and reception properties of wireless communications, data occasionally can be lost or delayed.

This can be due to the variation in radio signal strength that results from changes in the characteristics of the radio transmission path. Although data loss is rare, the environment where you operate the modem might adversely affect communications.

Variations in radio signal strength are referred to as fading. Fading is caused by several different factors including signal reflection, the ionosphere, and interference from other radio channels.

Inseego Corp. or its partners will not be held responsible for damages of any kind resulting from the delays or errors in data transmitted or received with the Skyus 300 device, or failure of the Skyus 300 device to transmit or receive such data.

Limited Warranty and Liability

Inseego Corp. warrants for the 12-month period immediately following receipt of the Product by Purchaser that the Product will be free from defects in material and workmanship under normal use. THESE WARRANTIES ARE EXPRESSLY IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The exclusive remedy for a claim under this warranty shall be limited to the repair or replacement, at Inseego's option, of defective or non-conforming materials, parts or components. The foregoing warranties do not extend to (I) non-conformities, defects or errors in the Products due to accident, abuse, misuse or negligent use of the Products or use in other than a normal and customary manner, environmental conditions not conforming to Inseego's specification, of failure to follow prescribed installation, operating and maintenance procedures, (II) defects, errors or nonconformities in the Product due to modifications, alterations, additions or changes not made in accordance with Inseego's specifications or authorized by Inseego, (III) normal wear and tear, (IV) damage caused by force of nature or act of any third person, (V) shipping damage, (VI) service or repair of Product by the purchaser without prior written consent from Inseego, (VII) products designated by Inseego as beta site test samples, experimental, developmental, reproduction, sample, incomplete or out of specification Products, or (VIII) returned products if the original identification marks have been removed or altered.

Safety Hazards

WARNING: This equipment is to be installed by qualified personnel only.

NOTE: This product is intended for restricted access whereby access is controlled through the use of a means of security (for example, key, lock, tool, badge access) and personnel authorized for access have been instructed on the reasons for the restrictions and any precautions that need to be taken.

This device is designed to be connected to a grounded power source. The socket (outlet) supplied with a grounded supply source, in order to maintain the security provided by a grounded power source to the device.

Do not operate the Skyus 300 in an environment that might be susceptible to radio interference resulting in danger, specifically:

Areas where prohibited by the law

Follow any special rules and regulations and obey all signs and notices. Always turn off the host device when instructed to do so, or when you suspect that it might cause interference or danger.

Where explosive atmospheres might be present

Do not operate your device in any area where a potentially explosive atmosphere might exist. Sparks in such areas could cause an explosion or fire resulting in bodily injury or even death. Be aware and comply with all signs and instructions.

Users are advised not to operate the device while at a refueling point or service station. Users are reminded to observe restrictions on the use of radio equipment in fuel depots (fuel storage and distribution areas), chemical plants or where blasting operations are in progress.

Areas with a potentially explosive atmosphere are often but not always clearly marked. Potential locations can include gas stations, below deck on boats, chemical transfer or storage facilities, vehicles using liquefied petroleum gas (such as propane or butane), areas where the air contains chemicals or particles, such as grain, dust or metal powders, and any other area where you would normally be advised to turn off your vehicle engine.

Near medical and life support equipment

Do not operate your device in any area where medical equipment, life support equipment, or near any equipment that might be susceptible to any form of radio interference. In such areas, the host communications device must be turned off. The device can transmit signals that could interfere with this equipment.

On an aircraft, either on the ground or airborne

In addition to FAA requirements, many airline regulations state that you must suspend wireless operations before boarding an airplane. Please ensure that the modem is turned off prior to boarding aircraft in order to comply with these regulations. The modem can transmit signals that could interfere with various onboard systems and controls.

While operating a vehicle

The driver or operator of any vehicle should not operate a wireless data device while in control of a vehicle. Doing so will detract from the driver or operator's control and operation of that vehicle. In some countries, operating such communications devices while in control of a vehicle is an offense.

Electrostatic Discharge (ESD)

Electrical and electronic devices are sensitive to electrostatic discharge (ESD). Macintosh native connection software might attempt to reinitialize the device should a substantial electrostatic discharge reset the device. If the software is not operational after an ESD occurrence, then restart your computer.

ROHS COMPLIANCE

As a part of Inseego's corporate policy of environmental protection, Inseego takes every step to ensure that devices are designed and manufactured to comply to the European Union Directive 2015/863 amending 2011/65/EU for the Restriction of Hazardous Substances (RoHS).

Installation and Operating Instructions

Temperature code, T4

SUITABLE FOR USE IN CLASS I, DIVISION 2, GROUPS A, B, C, D HAZARDOUS LOCATIONS, OR NONHAZARDOUS LOCATIONS ONLY.

THESE DEVICES ARE OPEN TYPE DEVICES THAT ARE INTENDED TO BE INSTALLED IN A TOOL-ONLY ACCESSIBLE ENCLOSURE THAT IS SUITABLE FOR THE ENVIRONMENT.

WARNING: EXPLOSION HAZARD – DO NOT DISCONNECT EQUIPMENT WHILE THE CIRCUIT IS LIVE OR UNLESS THE AREA IS KNOWN TO BE FREE OF IGNITABLE CONENTRATIONS

ANTENNAS INTENDED FOR USE IN CLASS I, DIVISION 2 HAZARDOUS LOCATIONS MUST BE INSTALLED WITHIN THE END USE ENCLOSURE. FOR REMOTE INSTALLATION IN AN UNCLASSIFIED LOCATION, ROUTING AND INSTALLATION OF THE ANTENNAS SHALL BE IN ACCORDANCE WITH NATIONAL ELECTRICAL CODE REQUIREMENTS (NEC/CEC).

The USB, Serial, ETH ports, and Reset button may only be accessed for equipment set-up, installation and maintenance within non-hazardous location. These ports and the associated interconnecting cable shall remain inaccessible within the hazardous location.

Power Adaptor (optionally provided with the product) shall not be used in the hazardous location.

The instructions shall stipulate that if a power adaptor is provided with the equipment, the adaptor and associated wiring harness may only be used in a non-hazardous (unclassified) location.

6

Glossary

Glossary

- **4G LTE**—Fourth Generation Long Term Evolution. LTE is a standard for wireless data communications technology and an evolution of the GSM/UMTS standards. The goal of LTE is to increase the capacity and speed of wireless data networks using new DSP (digital signal processing) techniques and modulations that were developed around the turn of the millennium. A further goal is the redesign and simplification of the network architecture to an IP-based system with significantly reduced transfer latency compared to the 3G architecture. The LTE wireless interface is incompatible with 2G and 3G networks, so that it must be operated on a separate wireless spectrum

- **802.11 (a, b, g, n, ac)** — A set of WLAN Wi-Fi communication standards in the 2.4 and 5 GHz frequency bands.

- **APN** — Access Point Name. The name of a gateway between a mobile network and another computer network, often the Internet.

- **bps** — Bits per second. The rate of data flow.

- **Broadband** — High-capacity high-speed transmission channel with a wider bandwidth than conventional modem lines. Broadband channels can carry video, voice, and data simultaneously.

- **DPD** — Dead Peer Detection. A method to detect the aliveness of an IPsec connection.

- **DHCP** — Dynamic Host Configuration Protocol. Software found in servers and routers that automatically assigns IP addresses and other configuration data to computers, tablets, printers, and other devices connection to the IP network.

- **DHCP Server** — A server or service with a server that assigns IP addresses.

- **DMZ** — demilitarized zone. A sub-network that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet.

- **DNS** — Domain Name System. A system for converting host names and domain names into IP addresses on the Internet or on local networks that use the TCP/IP protocol.

- **Firmware** — A computer program embedded in an electronic device. Firmware usually contains operating code for the device.

- **FTP** — File Transfer Protocol. A standard network protocol used to transfer computer files between a client and server.

- **GB** — Gigabyte. A multiple of the unit byte for digital information storage. Usage depends on context. When referring to disk capacities it usually means 10^9 bytes. It also applies to data transmission quantities over telecommunication circuits.

- **Gbps** — Gigabits per second. The rate of data flow.

- **Hotspot** — A Wi-Fi (802.11) access point or the area covered by an access point. Used for connecting to the Internet.

- **HTTP** —Hypertext Transfer Protocol. An application-level protocol for accessing the World Wide Web over the Internet.

- **IEEE** —Institute of Electrical and Electronics Engineers. An international technical/professional society that promotes standardization in technical disciplines.

- **IMAP** — Internet Message Access Protocol. An Internet standard protocol for accessing email from a remote server from email clients. IMAP allows access from multiple client devices.

- **IMEI** — International Mobile Equipment Identity. Used in LTE networks to identify the device. It is usually printed on the device and can often be retrieved using a USSD code.

- **IP** — Internet Protocol. The mechanism by which packets are routed between computers on a network.

- **IP Type** — The type of service provided over a network.

- **IP address** —Internet Protocol address. The address of a device attached to an IP network (TCP/IP network).

- **ISP** — Internet Service Provider. Also referred to as the service carrier, an ISP provides Internet connection service (*See* Network Operator).

- **Kbps** — Kilobits per second. The rate of data flow.

- **LAN** — Local Area Network. A type of network that lets a group of computers, all in close proximity (such as inside an office building), communicate with one another. It does not use common carrier circuits though it can have gateways or bridges to other public or private networks.

- **MAC Address** —Media Access Control. A number that uniquely identifies each network hardware device. MAC addresses are 12-digit hexadecimal numbers. This is also known as the physical or hardware address.

- **Mbps** — Megabits per second. The rate of data flow.

- **MSID** — Mobile Station IDentifier. A number for a mobile phone that identifies that phone to the network.

- **Network Operator** —The vendor that provides your wireless access. Known by different names in different regions, some examples are: wireless provider, network provider, or cellular carrier.

- **Network Technology** —The technology on which a particular network provider's system is built; such as LTE or GSM.

- **NMEA port** —National Marine Electronics Association port. The port through which applications can access a GPS data stream.

- **NNTP** — Network News Transfer Protocol. The primary protocol used to connect to Usenet servers and transfer news articles between systems over the Internet.

- **POP3** — Post Office Protocol 3. A protocol in which email is received and held for you by your Internet server until you download it.

- **Port** — A virtual data connection used by programs to exchange data. It is the endpoint in a logical connection. The port is specified by the port number.

- **Port Forwarding** — A process that allows remote devices to connect to a specific computer within a private LAN.

- **Port Number** — A 16-bit number used by the TCP and UDP protocols to direct traffic on a TCP/IP host. Certain port numbers are standard for common applications.

- **PRL** — Preferred Roaming List. A list that your wireless phone or device uses to determine which networks to connect with when you are roaming (Network operator specific).

- **Protocol** — A standard that enables connection, communication, and data transfer between computing endpoints.

- **Proxy** — A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it.

- **RADIUS** — Remote Authentication Dial-In User Service. A networking protocol, operating on port 1812, that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service.

- **Router** — A device that directs traffic from one network to another.

- **RP-SMA** — Reverse Polarity Sub-Miniature Version A. A connector interface with a screw-type coupling mechanism for coaxial cables.

- **RSSI** — Received signal strength indicator.

- **SIM** — Subscriber Identification Module. Found in LTE and GSM network technology, the SIM is a card containing identification information for the subscriber and their account. The SIM card can be moved to different devices.

- **SMA** — Sub-Miniature Version A. A variation of the SMA connector where the gender of the interface is reversed.

- **SMTP** — Simple Mail Transfer Protocol. The standard protocol for sending emails across the Internet.

- **SNMP** — Simple Network Management Protocol. An Internet protocol used to manage and monitor network devices and their functions.

- **SSID** — Service Set IDentifier. The name assigned to a Wi-Fi network.

- **TCP/IP** — Transmission Control Protocol/Internet Protocol. The set of communications protocols used for the Internet and other similar networks.

- **TFTP**—Trivial File Transfer Protocol. An Internet software utility for transferring files that is simpler to use than FTP, but does not provide user authentication and directory visibility supported by FTP.

- **Telnet** — A user command and underlying TCP/IP protocol that allows a user on one computer to log into another computer that is part of the same network.

- **TTY**—Text Telephones (TTY), also known as Telecommunications Device for the Deaf (TDD), are used by the deaf, hard–of–hearing, and individuals with speech impairments to communicate.

- **UDP** — User Datagram Protocol (UDP) is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP.

- **USB** — Universal Serial Bus. A connection type for computing device peripherals such as a printer, mobile modem, etc.

- **USB Port Types** — The USB ports on computers and hubs have a rectangular Type A socket, and peripheral devices have a cable with a Type A plug. Peripherals that do not have an attached cable have a square Type B socket on the device and a separate cable with a Type A and Type B plug. Ports and connectors are available in different sizes (for example, standard, mini, and micro).

- **USSD**— Unstructured Supplementary Service Data (USSD), also known as "Quick code" or "Feature code", is a communications protocol used to send data between a mobile device and network service provider.

- **VPN**—Virtual Private Network. A secure private network that runs over the public Internet. Commonly used to connect to an office network from elsewhere.

- **Wi-Fi**—Any system that uses the 802.11 standard developed and released in 1997 by the IEEE.

- **Wi-Fi 5**—The fifth generation of Wireless Fidelity, using 802.11ac on 5 GHz. This standard was developed and released in 2013.

- **Wi-Fi Client** — A wireless device that connects to the Internet via Wi-Fi

- **WPA/WPA2**— Wi-Fi Protected Access. A security protocol fir wireless 802.11 networks from the Wi-Fi Alliance.