Askey, Unisys

User Guide

Remote Worker Kit
2326RWK

Welcome

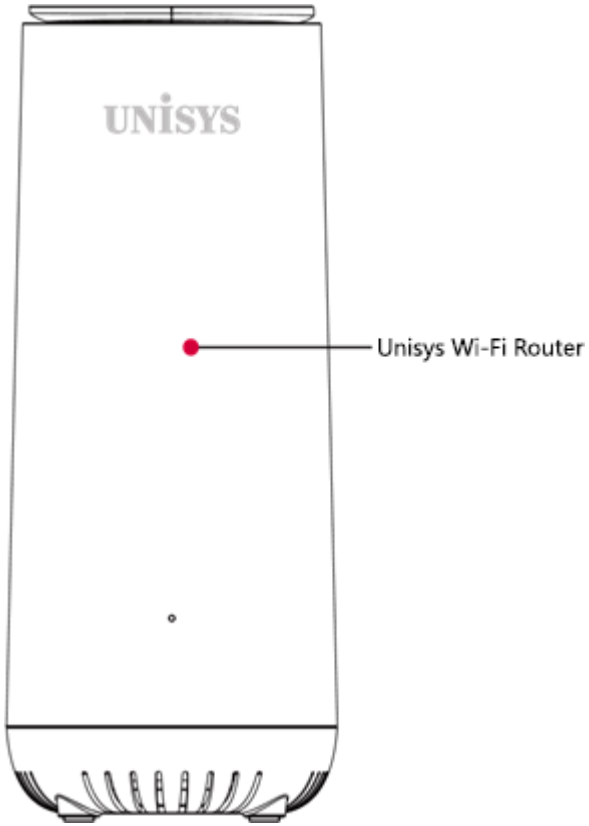
The Unisys Remote Worker Kit router is a sleek, multi-function, enterprise-grade Wi-Fi router. It packs all the functions needed for a residence or small office in one small form factor. The router has the latest Wi-Fi 6 technology and three Ethernet ports for WAN and LAN connections.

The router is small and light and provides great performance. It can be put on the countertop without occupying significant space.

1. Hardware Setup

1.1 Getting To Know Your Unisys RWK

1.1.1 Physical Hardware



Hardware Configuration

CPU	Qualcomm IPQ8072A Quad ARM Cortex A53 64bit @2.2GHz
DRAM	DDR4 DRAM : 1GB
Flash	eMMC : 8GB
Power Input	DC input: 12V
Dimensions	231 mm (H) x 150 mm (L) x 100mm (W)
Weight	900 g
Interfaces	3x100/1000 Base-T Ethernet, RJ-45
LED Indicator	1x Tri-Color LED Indicator: Power/Status
Buttons	ON/OFF, Reset ,WPS
Max. Power Consumption	20 W

Environmental Conditions	Operating Temperature: 0°C to 40°C Operating Humidity: 10% to 95% non-condensing Storage Temperature: -40°C to 80°C Storage Humidity: 5% to 95% non-condensing
Antenna type	4 x internal dual-band Wi-Fi antenna
Mounting	Desktop

Wireless Specifications

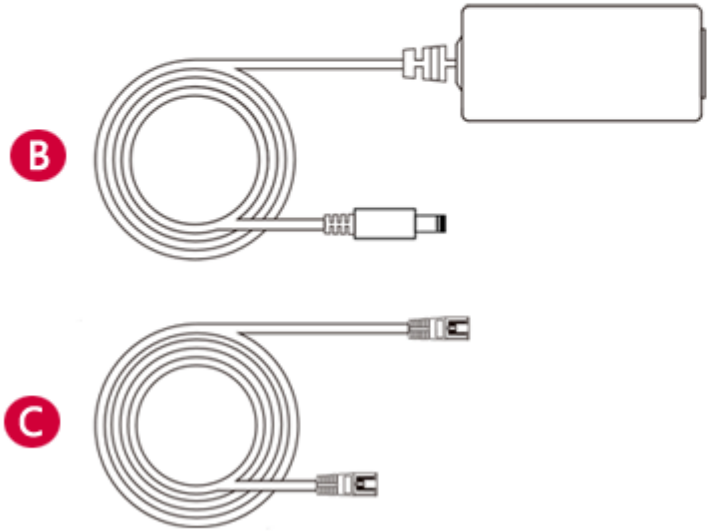
Standards	2.4GHz 802.11b/g/n/ax 5GHz 802.11a/n/ac/ax
Supported Rates	802.11ax: 4 to 2400 Mbps 802.11ac: 6.5 to 1732 Mbps 802.11n: 6.5 to 600 Mbps 802.11a: 6 to 54 Mbps 802.11g: 6 to 54 Mbps 802.11b: 1 to 11 Mbps
Radio Chains	4 x 4:4
Spatial Streams	4 for both SU-MIMO & MU-MIMO
Antenna	Up to 5.0 dBi
Max Phy Rate	2.4GHz: 1148 Mbps 5GHz: 2400 Mbps
Maximum transmit power	2.4 GHz: Up to 27dBm (combined power) 5 GHz: Up to 27dBm (combined power)
Minimum receiver sensitivity	2.4GHz HT20/VHT20/HE20: -93dBm @MCS0 2.4GHz HT40/VHT40/HE40: -94dBm @MCS0 • 5GHz VHT20/HE20: -95dBm @ MCS0 5GHz VHT40/HE40: -93dBm @ MCS0 5GHz VHT80/HE80: -89dBm @ MCS0
Max Number of Clients	Up to 128 per radio
SSIDs	Up to 4 per radio

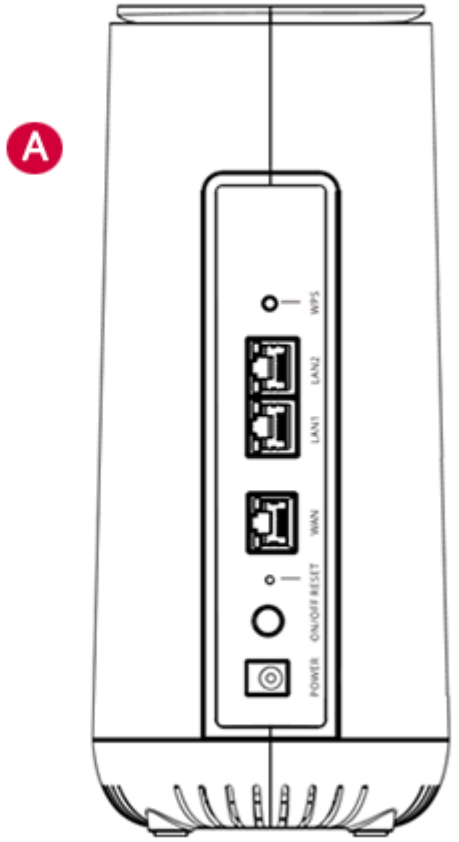
1.2 Unisys RWK's box

1.2.1 Package Contents

The Remote Worker Kit (RWK) contains the following:

- A RWK Device
- B Power Adapter and Cables
- C Ethernet Cable
- D Quick Start Guide



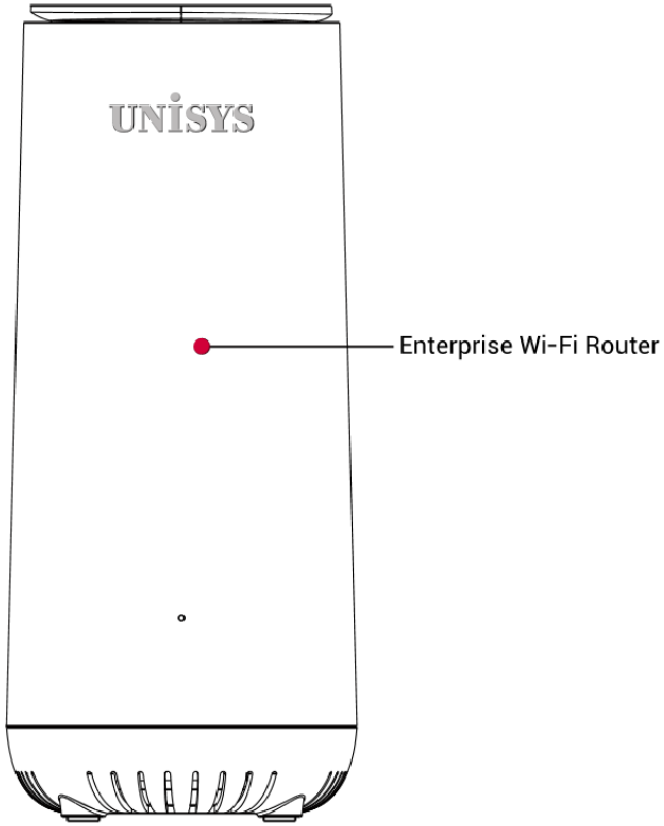


1.3 Hardware Features

Before configuring your router, it is important to familiarize yourself with the labels and functions visible on the router front and back panels. The LED status on the front of the router serves as a status indicator that enables you to quickly identify the status of the router's WAN (Internet) connection.

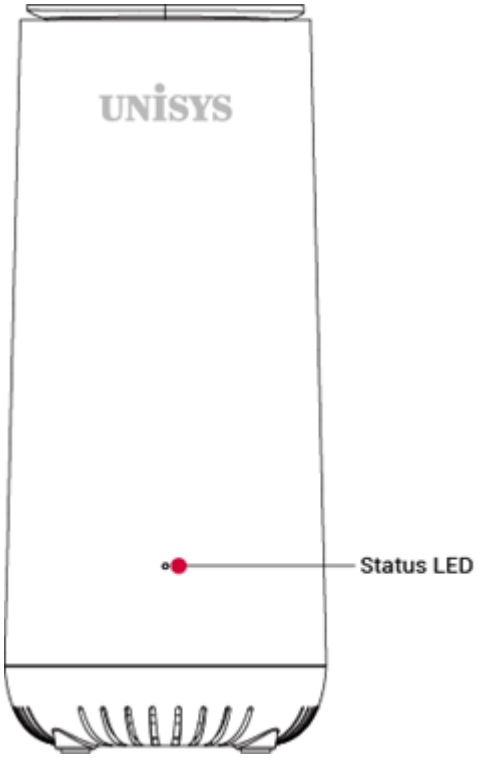
1.3.1 Front Panel

The front panel of the router features an LED light that provides you a visual indicator to easily determine the status of your router's network connection:



1.3.2 **LEDs**

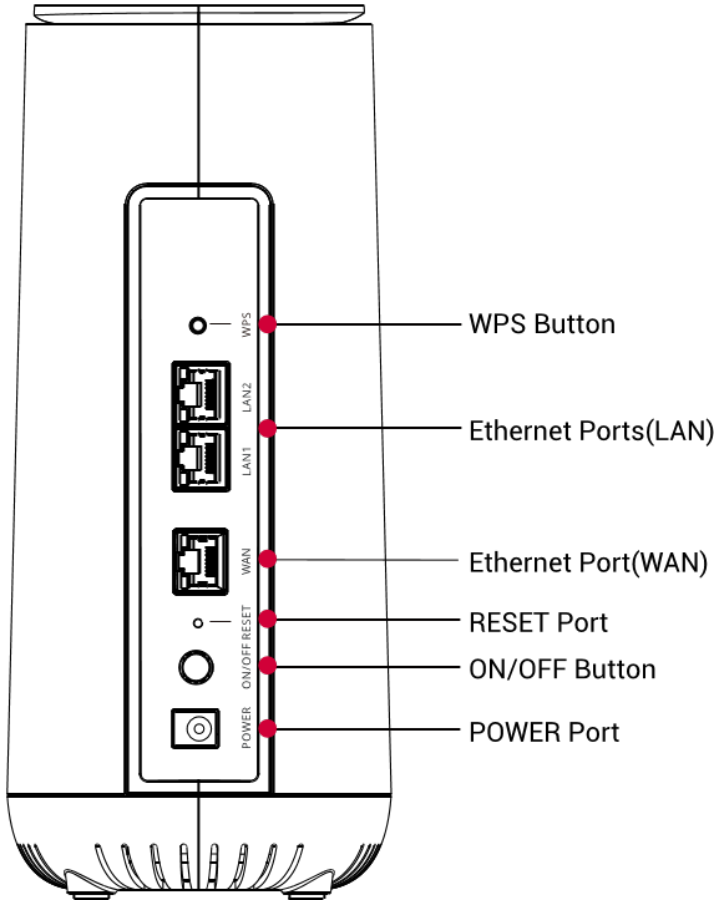
The LED status indicator identifies the status of your router's power and connection. The table below defines the possible status conditions:



LED	Activity	Description
	OFF	Device is not receiving power
Flashing	Cycling between BLUE and RED	Device is under firmware upgrading process
Flashing	Flashing GREEN	Device is under power on process
	Solid GREEN	Broadband connected
Flashing	Cycling between BLUE and GREEN	WPS station connecting
	Solid Red	No internet service

1.3.3 Rear Panel

The rear panel of your router includes multiple network ports and buttons as defined below:



Options	Description
WPS Button	This function is intentionally disabled . This feature is not supported for use with the Unisys RWK router.
Ethernet Ports (LAN)	Two ports providing physical local area network (LAN) access using CAT5/CAT6 network cables . For example: personal computer, printer, or document scanner.
Ethernet Port (WAN)	One port providing wide area network (WAN)/Internet access using a CAT5/CAT6 network cable.
RESET Port	Enables you to reset the Remote Worker Kit device.
ON/OFF Button	Applies or removes power to the Remote Worker Kit device.
POWER Port	This port is used to connect your router's power supply to an electrical outlet within your home or office.

1.4 Setting up the Hardware

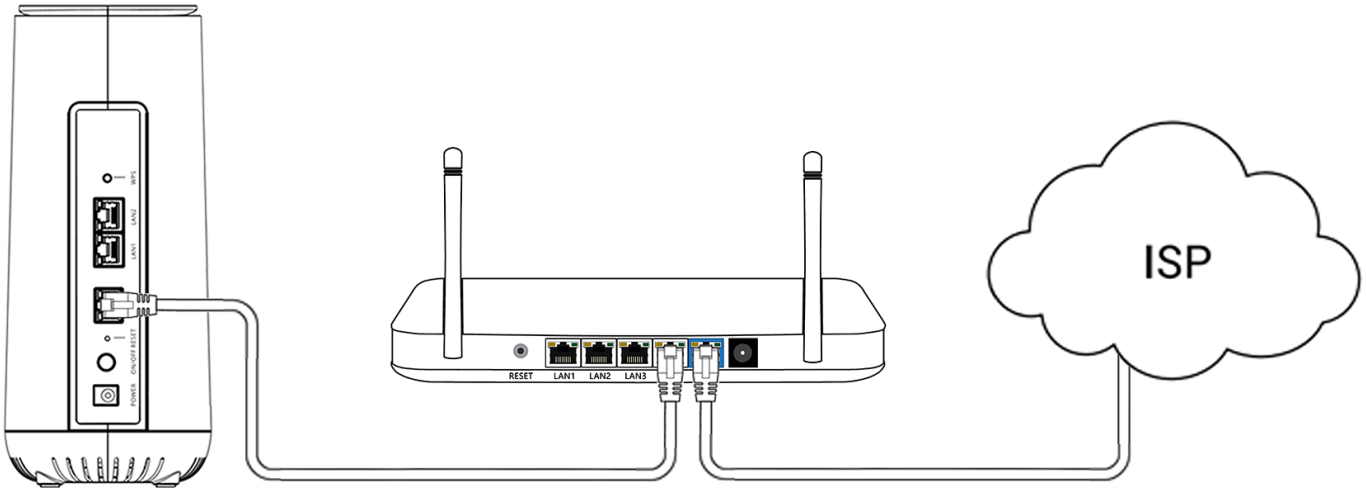
1.4.1 Before you Begin

Ensure you have the following: c

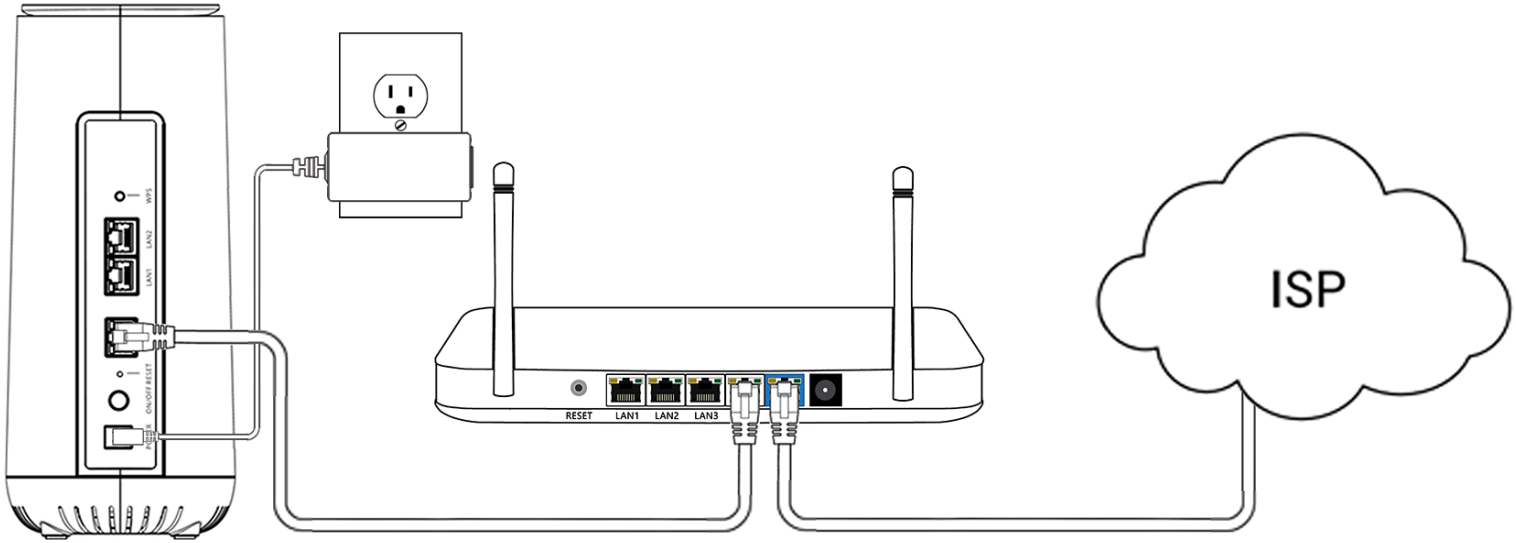
- An iOS or Android smartphone or tablet with the ability to:
  - Receive SMS (text) messages. (**Message and data rates may apply*)
  - Download and install mobile applications
- Access to the email from Unisys that contains a link to download the Unisys Remote Worker Kit mobile application

1.4.2 Setting up the Hardware

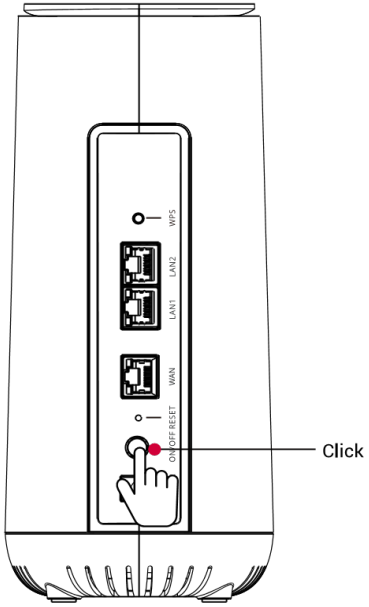
1. Use the supplied Ethernet cable to connect the WAN port of the Remote Worker Kit device to a LAN port on your home router or modem.



2. Use the supplied power adapter and cable to connect your Remote Worker Kit device to an electrical output.



3. Apply power to the Remote Worker Kit device, by pressing the Power switch on.



1.5 Positioning your Router

Identify the ideal location for your router by positioning your router to meet the following criteria:

- In an open space away from:
  - Walls or obstructions
  - Heavy-duty appliances or electronics, such as microwave ovens and baby monitors
  - Metal fixtures, enclosures, cabinets, reinforced concrete, or pipes
- Near a power outlet
- On an upper floor, where feasible, of the home -OR- at least 6 feet off the floor

1.6 Setup Requirements

To configure your wireless network, you need a computer, mobile phone, or tablet that meets the following system requirements:

- Ethernet RJ-45 (LAN) port -OR- IEEE 802.11a/b/g/n/ac/ax wireless capability
- An installed TCP/IP service
- Web browser such as Internet Explorer, Microsoft Edge, Firefox, Safari, or Google Chrome

2. Configuring the RWK Device

2.1 Installing the RWK Mobile Application

You must download and install the Unisys-supplied Remote Worker Kit mobile application on a smartphone running either an iOS or Android operating system.

Note: *The RWK Mobile Application should only be installed on a single device*

To download the Unisys Remote Worker Kit mobile application, perform the following steps:

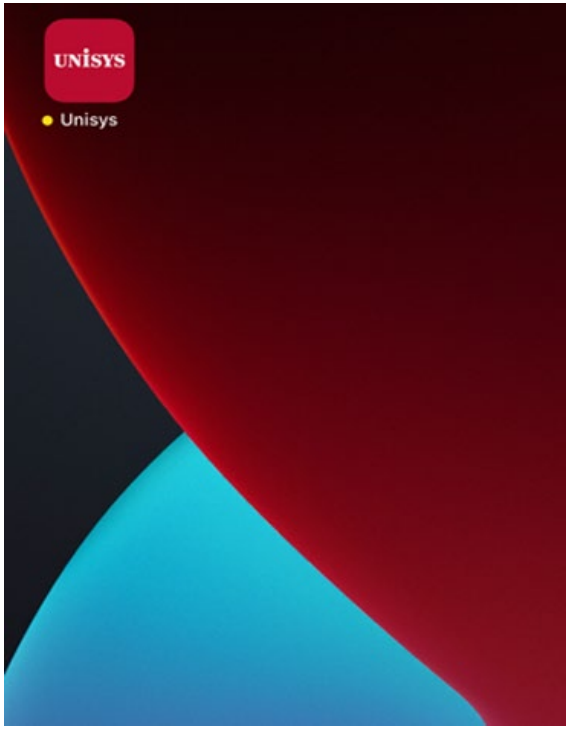
1. On your mobile device, access the email from Unisys that contains the link for downloading the mobile application.
2. Click the link corresponding to the operating system for your smartphone (iOS or Android).
3. Confirm the email address where you want Unisys to send instructions for downloading and installing the mobile application. An email will be sent to the specified email address.
4. Perform the steps as detailed within the email from Unisys to install the application on your smartphone.

2.1.1 For IOS Devices

1

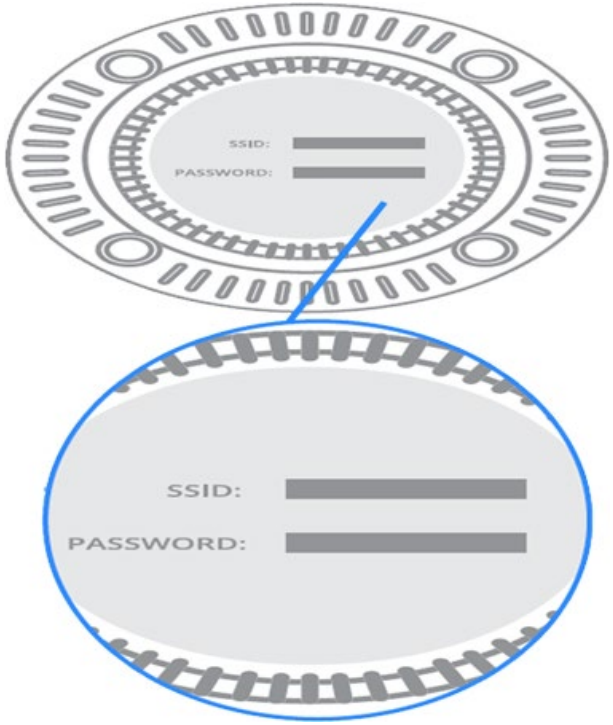
Download the Unisys Remote Worker Kit app from the app store

2



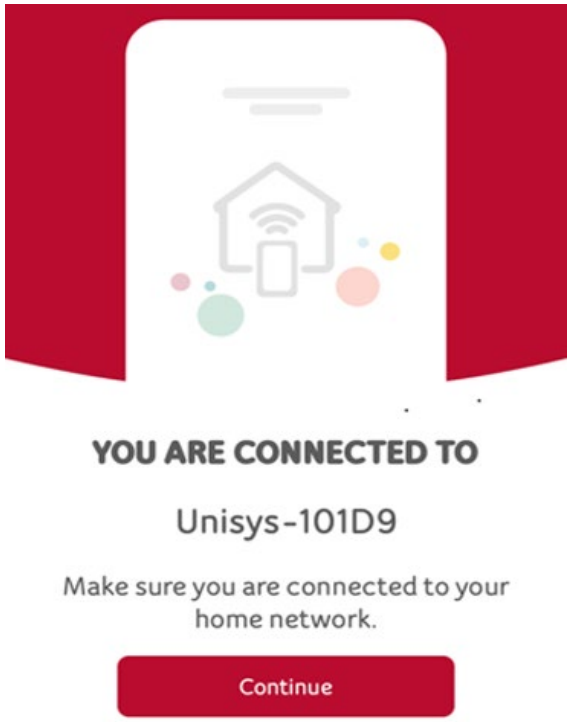
Once installed the Unisys app will be available on you home screen, Select the app to begin.

3



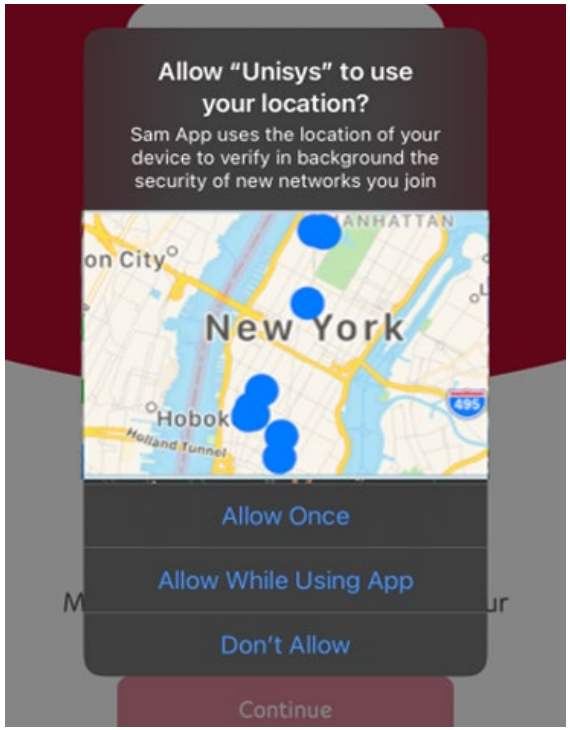
On your smartphone, access the Wi-Fi settings, and then connect to the Remote Worker Kit device using the SSID and password printed at the bottom of the device.

4



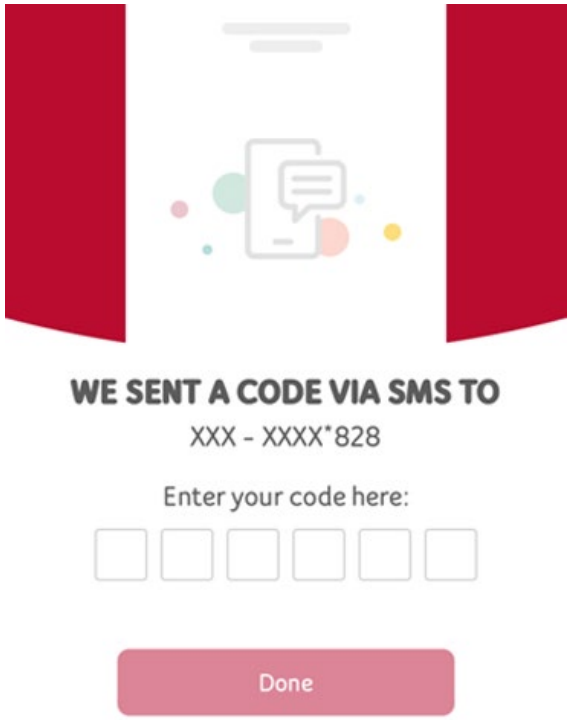
Unisys app will show that you are connected to the HWK wireless network. Select “Continue”.

5



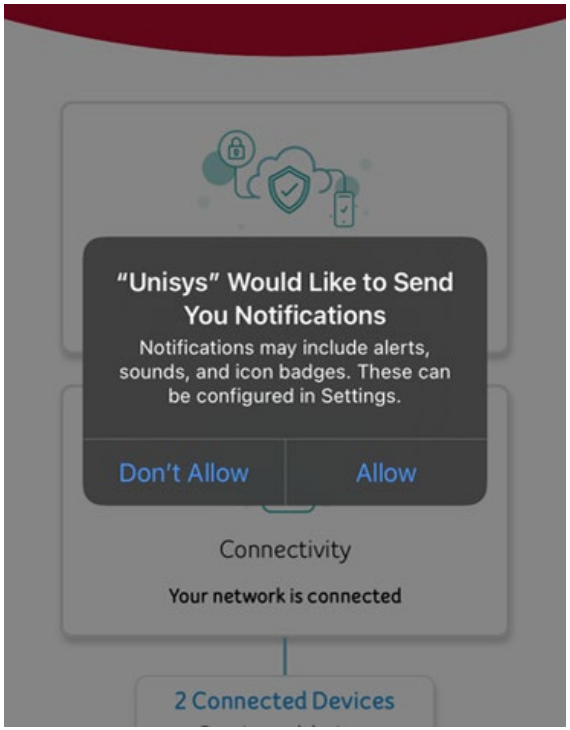
The Unisys app will ask to use location services, select “Allow While Using App”

6



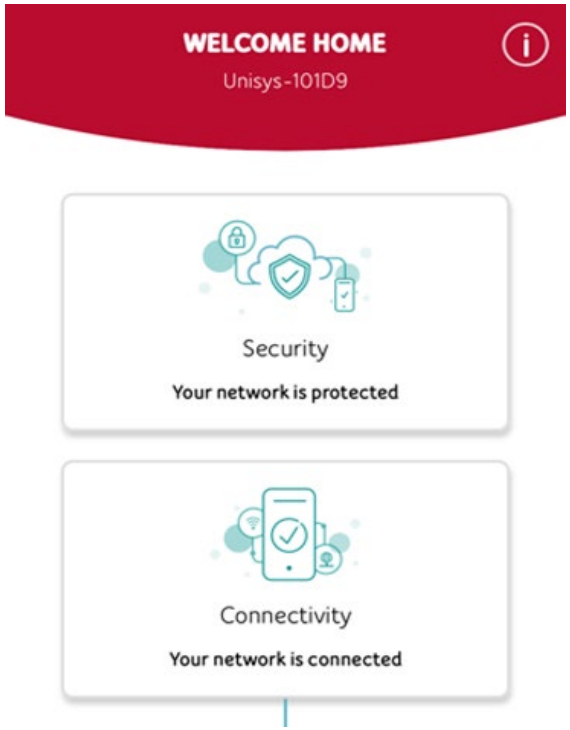
You will be prompted to enter a code sent via SMS to the number identified, enter the code that was sent to you and tap **Done**.

7



The Unisys app will request to send notifications, select "Allow".

8



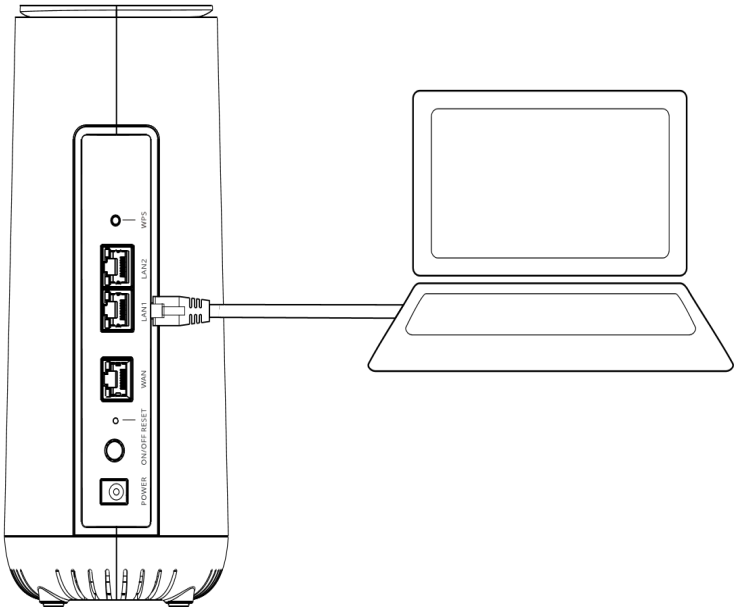
The Unisys app will display the welcome screen.

Note: *When setup completes successfully, the Remote Worker Kit mobile application Welcome Home screen indicates that your Unisys Remote Worker Kit device is connected to the network.*

2.2 Connecting Other Devices

To connect your company issued computer or any other devices, including printers, personal computers, or personal mobile phones/tablets, perform the following steps:

Note: *If you do not want to use a Wi-Fi connection or a device does not support wireless connectivity, you can use an Ethernet cable to connect up to two devices to the Remote Worker Kit router's LAN ports for wired connectivity.*

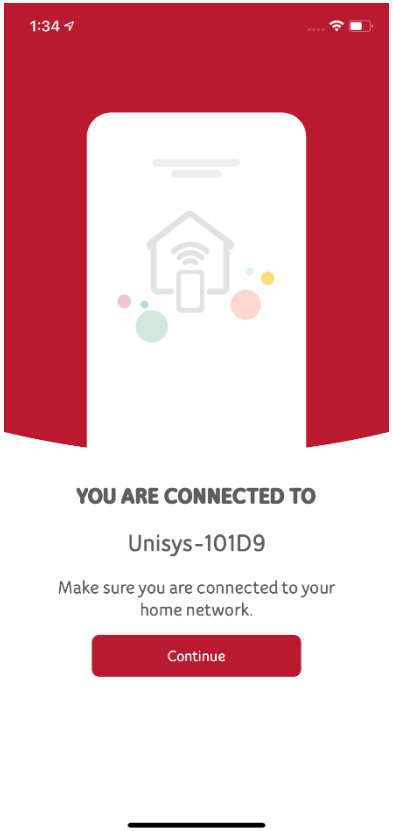


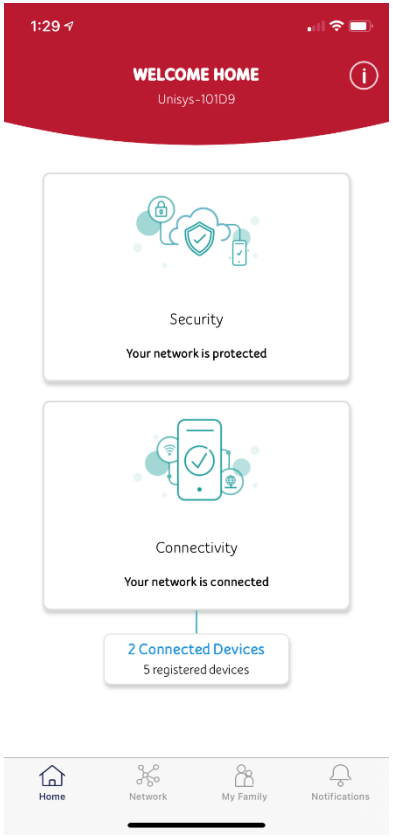
1. On your computer or mobile device, locate Wi-Fi Settings
2. Select the Wi-Fi Network Name (SSID) listed on the bottom of the RWK router
3. Enter the unique password found on the white sticker on the bottom of the RWK router

3. Managing your Wi-Fi Network Using the Mobile Application

3.1 Home page

Home





3.2 Managing the RWK Network

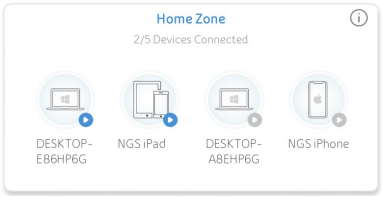
Network

The Network tab within the Remote Worker Kit mobile application enables you to monitor and manage all devices connected to your Remote Worker Kit router. In addition to adding and removing devices from the network, you can also restrict Internet access to select devices on your network at specified times, for example, disabling Internet access for a child's smartphone between 9 PM and 9 AM.

Depending on the MAC address of the device that is using the Remote Worker Kit router, the device is automatically placed within one of the following pre-defined zones:

Note: *By default, all unrecognized MAC addresses are placed within the Guest Zone. You can then move the device to the appropriate zone based on device type and the security permissions you want to apply for the device.*

Home Zone

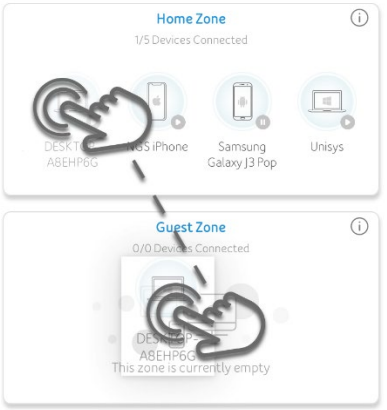


Guest Zone

IoT Zone

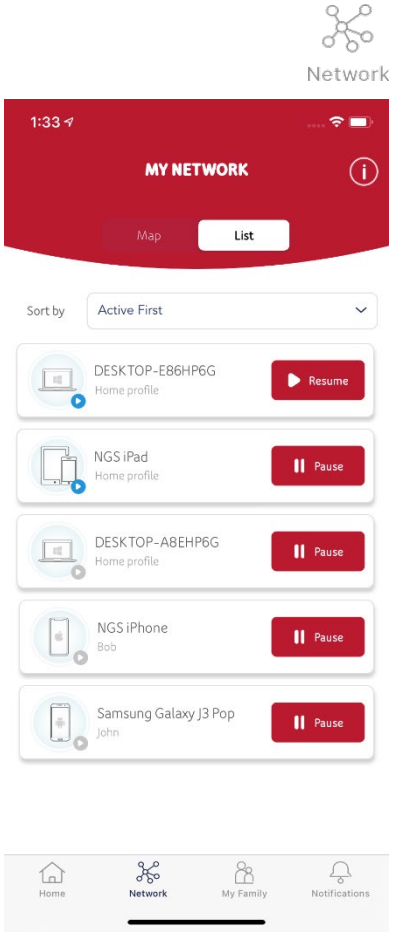
MyISP Zone

Blocked Zone



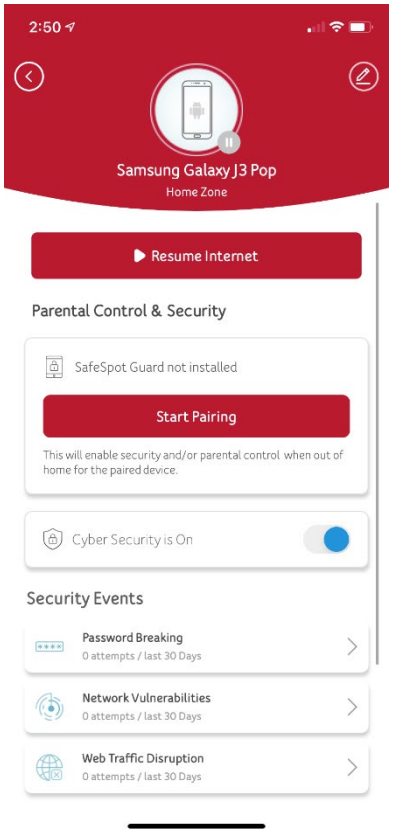
To move a device to a different zone simply touch the device and drag it to another zone.

3.3 Managing Devices on your Network



The "List" view under the network menu provides a list of the devices that are connected to the Remote Worker Kit router. This menu provides the capability to "Pause" and "Resume" Internet access for each device that is connected to the Remote Worker Kit. Clicking the device name for each of the connected devices opens the Parental Control & Security menu for each of the devices. This menu provides additional reports and controls which include:

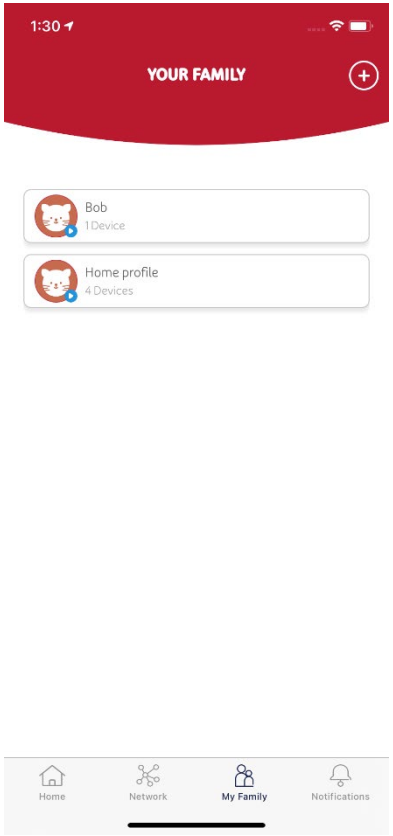
- Pause/Resume Internet access
- Pause/Resume Cyber Security rules
- Security Event Reporting:
  - Password Breaking
  - Network Vulnerabilities
  - Web Traffic Disruption
- Device Details Page

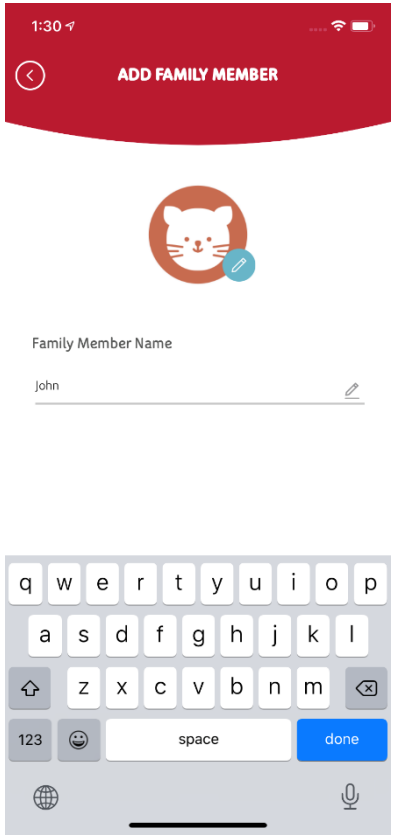


NOTE: Individual controls do not work on devices shared by multiple users.

3.4 Managing Family Members

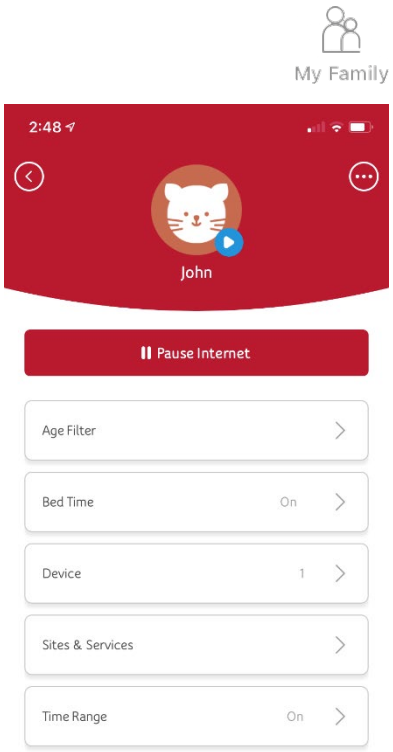
The “My Family” tab provides information on family members who have profiles on the Remote Worker Kit. Each family member who requires parental or general network controls is required to have a profile. To add a family profile, press the ⊕ button. This will provide a page for entering each family member’s name into the family profile page. Each name must be entered individually.





NOTE: Each device can only have one family member assigned to the device.

3.5 Family Member Properties



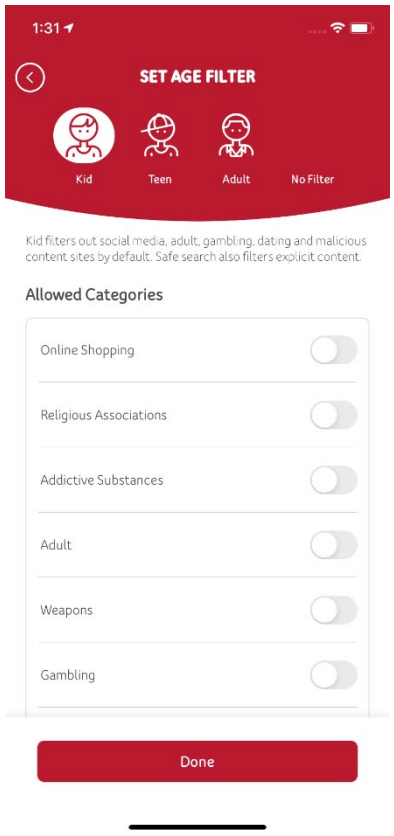
After entering the name of a family member, the properties page for the family member will appear. From this page options can be controlled to configure options for each family member. These options include the following management capabilities:

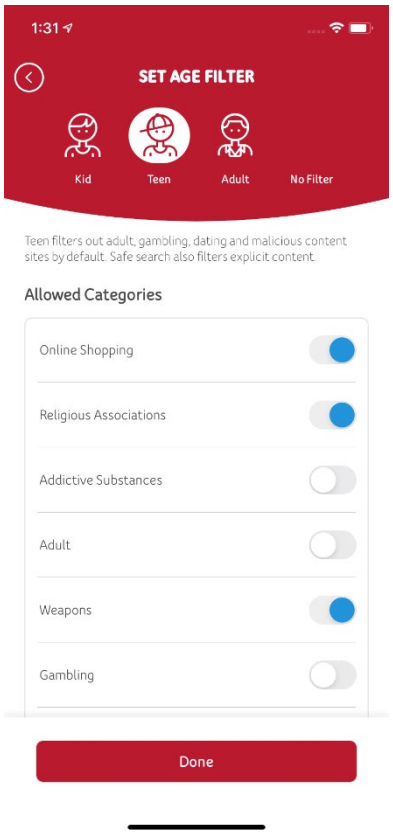
- Age Filter
- Bed Time
- Device Management
- Sites & services
- Time Range

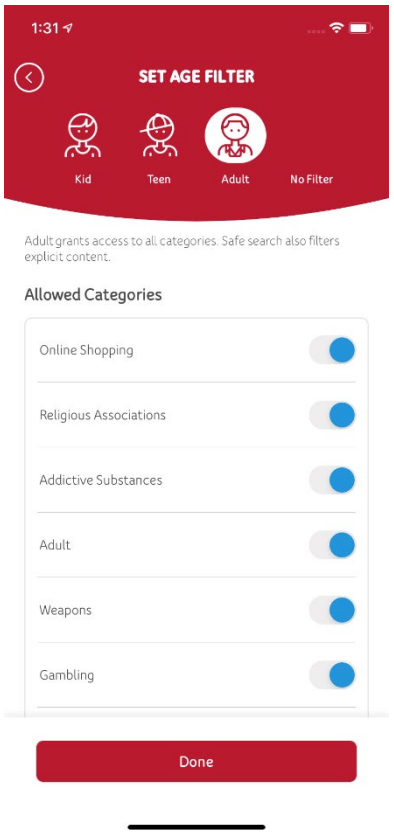
3.6 Set Age Filter

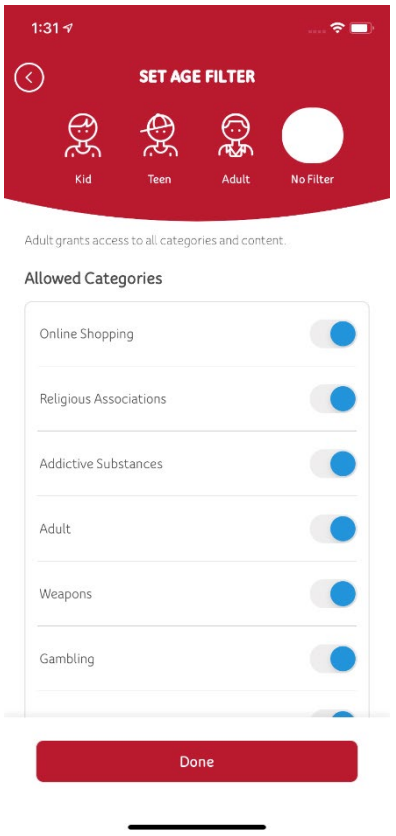
My Family

The age filter menu provides pre-configured allowed categories for different age groups in your household. Starting with children who have the largest number of pre-configured restrictions, each age group becomes progressively more lenient as you move to Teen, Adult, and then No Filter. Each tab allows customization of each category to allow or deny for each age group by clicking the toggle button.

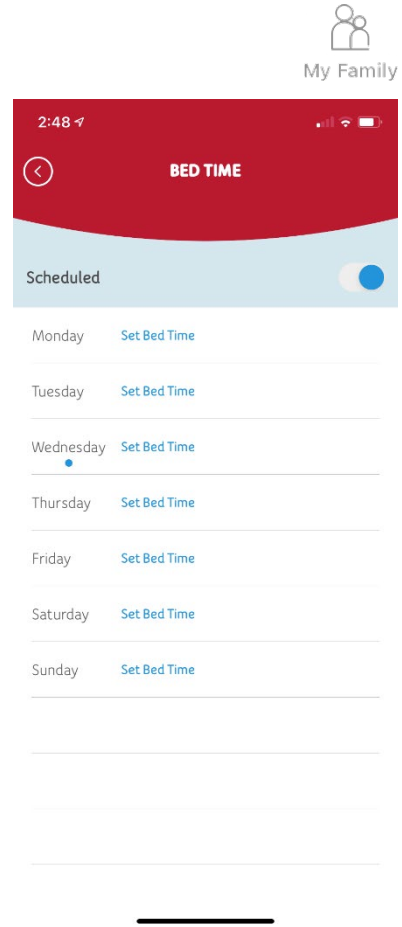






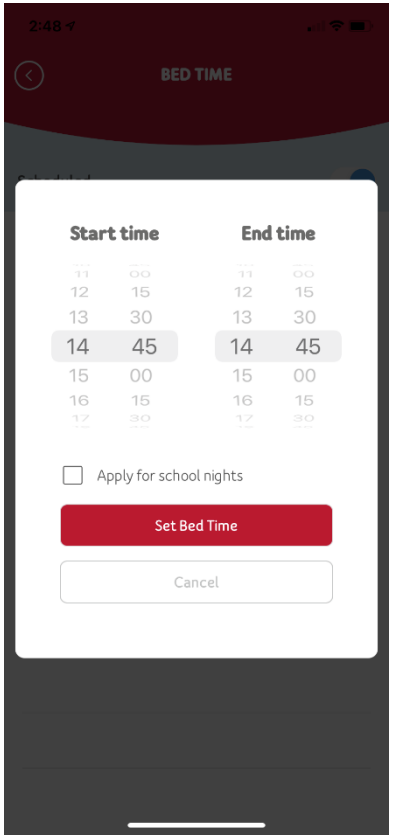


3.7 Bedtime Controls



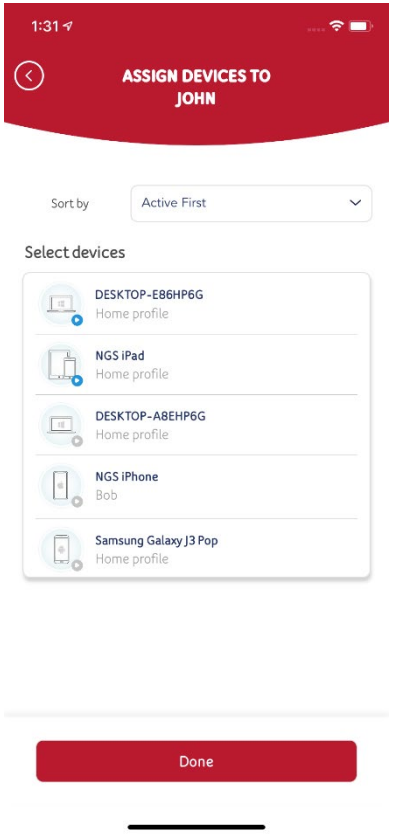
Controls for bedtimes are managed by the days of each week. Each day is provided with granular controls for restricting Internet access during times that are selected. This selection process starts by pressing “Set Bedtime”. When Set Bedtime is pressed a popup menu will appear for when bedtime should start. If bedtime is at 10PM then 20 00 will need to be assigned to the start time. If the family member restrictions end at 7AM then 07 00 will need to be selected to assign the End Time.

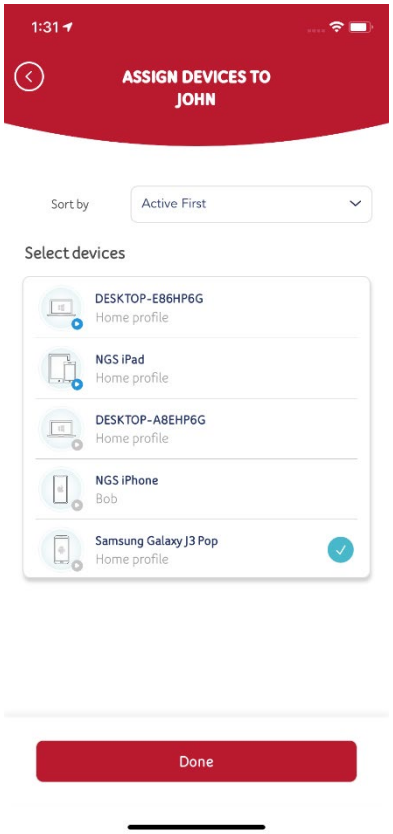
To apply the same setting to all school nights, check the box for “Apply for school nights”. This will start the bedtime settings to start on Sunday Evening and will end on Friday Morning.



3.8 Assign Devices to Family Profile

The option to assign devices to a family profile is performed by adding the device that is utilized by each family member. Each device will be listed in this profile and must be selected to assign the security controls to the proper user. By touching the device that is owned by the user a checkbox will appear next to the device on the list. Once all the devices that are used by the restricted user are selected, press “Done”.

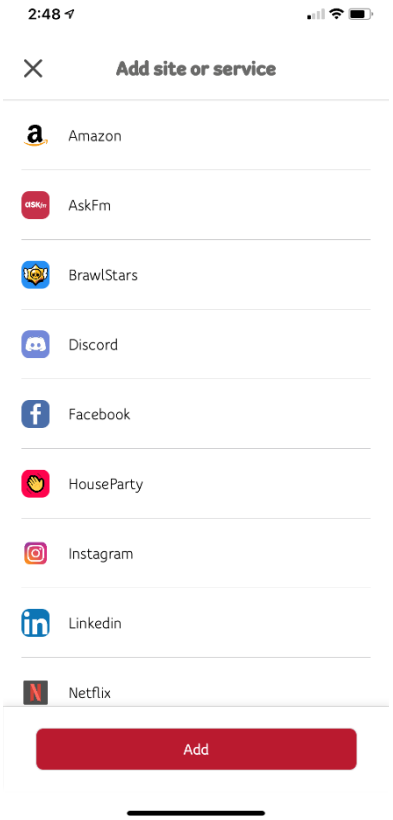




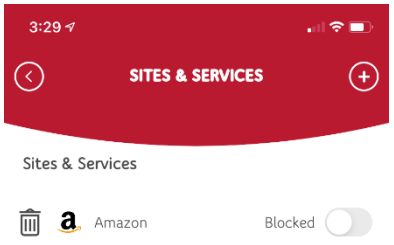
3.9 Sites & Services Management

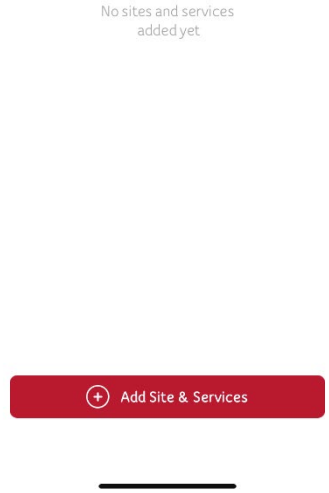
Adding sites & services will restrict the usage for the sites that are added to this list. To add sites to this list, click the ⊕ Add Site & Services button at the bottom of the page. A list of common sites will appear to add to the restrictions list.

Select the site/s to add restrictions for the family member and press the **Add** button.



Once added the sites will show up on the Sites & Services page for management control of the sites.

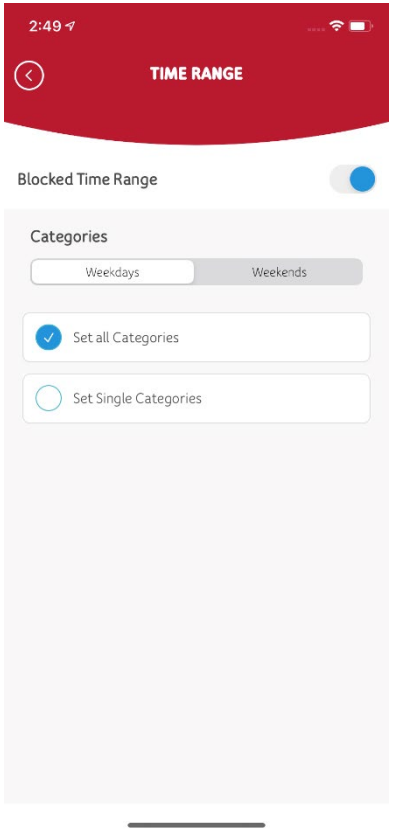


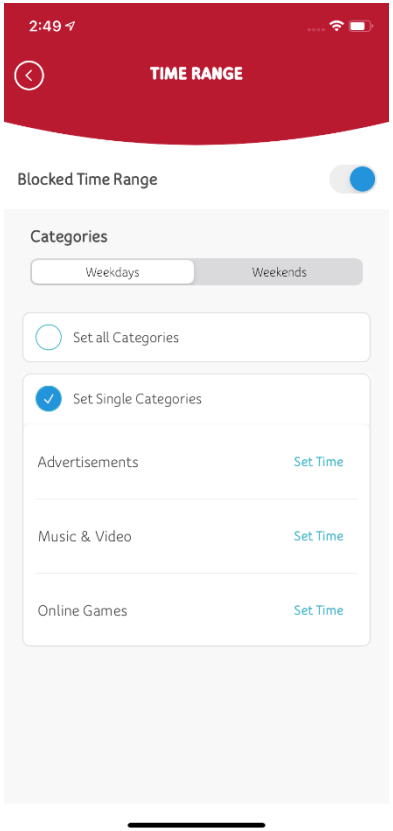


3.10 Blocked Time Management

My Family

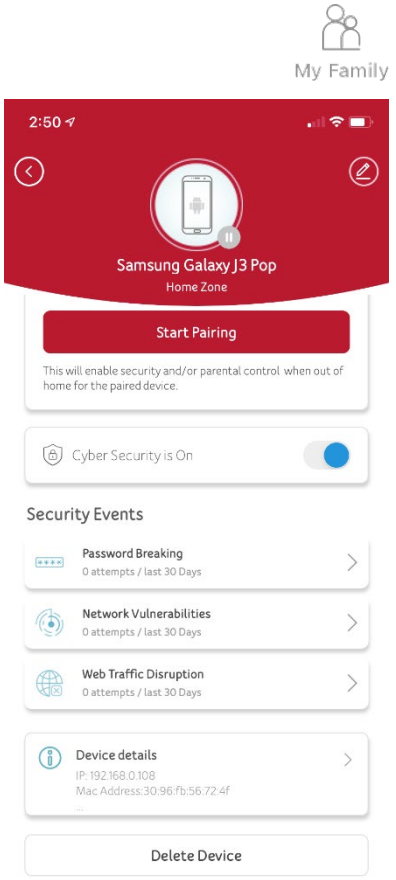
Time management to block website categories is managed through this option. The time management is separated between Weekdays and Weekends. Also, the category options are managed by selecting “Set all Categories” or “Set Single Categories”. The “Set all Categories” option will apply the same rules to all categories in the Age Filter. The “Set Single Categories” option allows controls to be applied individually to each website category.



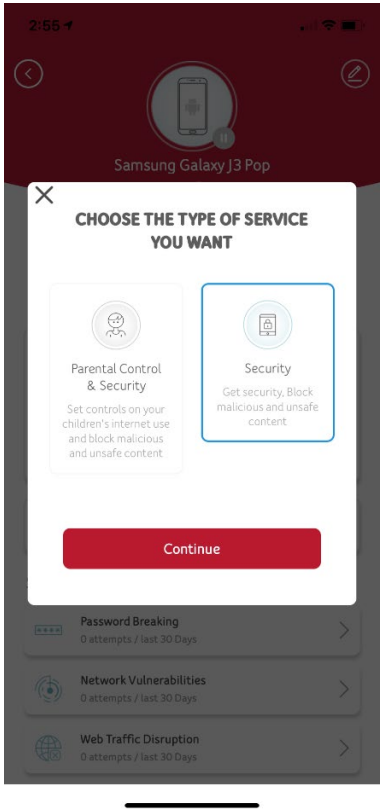


3.11 Managing Devices while not on your Network

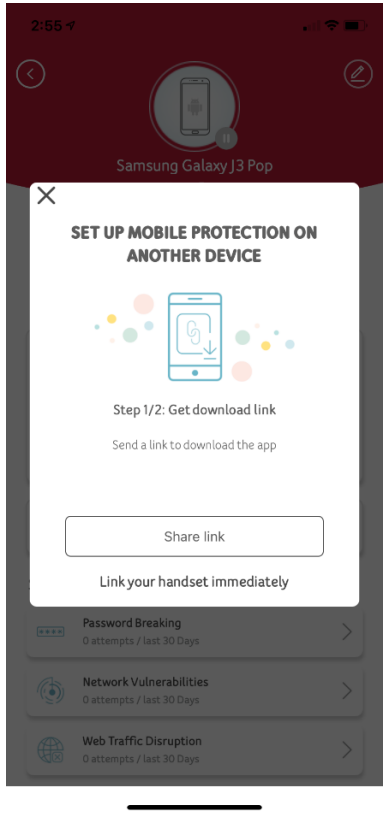
The Unisys Remote Worker Kit by default protects devices while they are connected to the RWK router. To enforce controls while devices are connected to other networks, e.g. a cellular network, go to the Network tab, select the device you want to manage away from your network, and select “Start Pairing”.



Select the service type you want to apply to the device while away from your network.

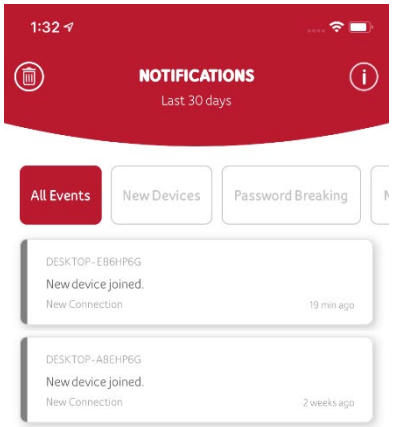


Select “Share link” to send the link to the device for downloading the App.



3.12 Notifications

Notifications alert you to real-time events on your Remote Worker Kit device such as when new devices connect to your network, the length of time a device has been connected to the network, as well as security related alerts pertaining to attempts on password breaking and other network vulnerabilities. Each event surfaced remains visible on the page for 30 days, and after 30 days the event is automatically deleted from the screen.



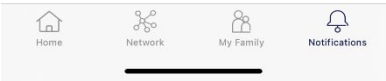
3.12.1 Accessing a Notification

To access notification, perform the following steps:

1. From the Home screen, tap **Notification**.

   The Notification screen appears.

   The tabs available in Notifications are as follows:



   - **All Events**: List of all the events that were logged by the Remote Worker Kit device during the last 30 days.
   - **New Devices**: List of new devices connected to the Remote Worker Kit device.
   - **Family**: List of family members connected to the device.
   - **Security**: List of devices that are under threat.
   - **Password Breaking**: List of devices breaking into your password-protected network.
   - **Network Vulnerabilities**: List of devices which has a flaw such as weak password, poor firewall configuration or unsecure email.
   - **Web Traffic Disruption**: List of devices with data disruption.

Tap ⓘ for more information on Notification.

3.12.2 Deleting a Notification

You can delete an event by swiping the event message to the left. You can also select all the events that you want to delete, and then tap **Delete**. A message, “Please confirm you would like to delete all notifications” appears. Tap **Delete** to delete the event messages or tap **Cancel** to retain the event messages.

3.13 Help

Tap the ⓘ icon in the upper-right corner of the screen for more details about the page you are on within the application. This information helps you in understanding the options available in the application.

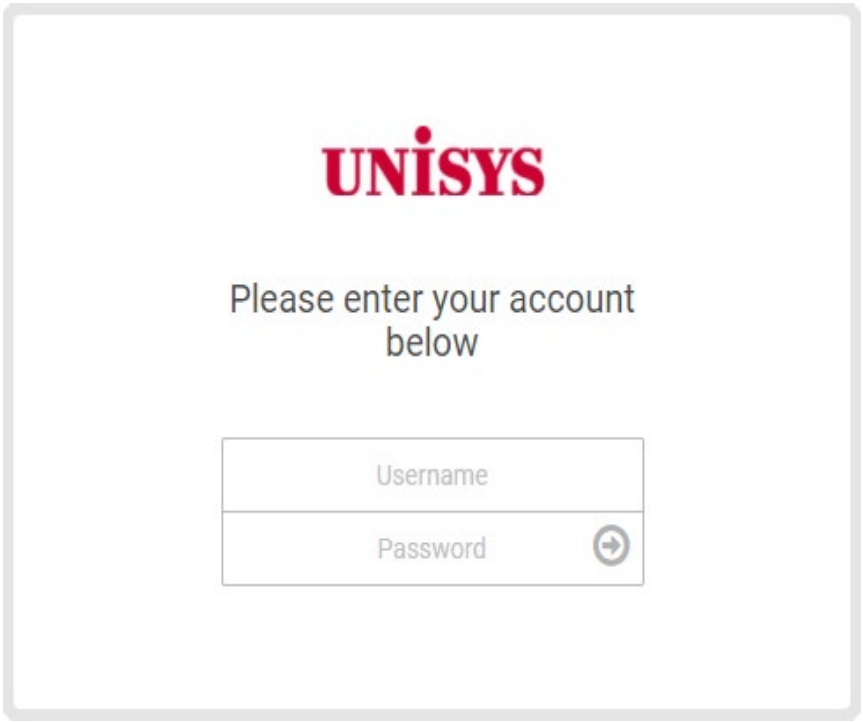
4. Accessing the RWK Management Console Web Interface

Accessing the RWK management console web interface is necessary for the modification of the network configuration, wireless settings, and passwords as well as troubleshooting the device. You can configure your router's network settings by using either your smartphone, tablet, or your computer to access the Remote Worker Kit Router Management Console Web interface.

To access the Management Console interface, perform the following steps:

1. Open a web browser and enter the router's default address **http://192.168.0.1** in the address bar.

2. Log into the Web UI using the default username: **admin** and password (Located on bottom of your Router).



4.1 Changing the Wi-Fi Password for the RWK Router

It is recommended that you change the default Management Console Web interface password after initial login.

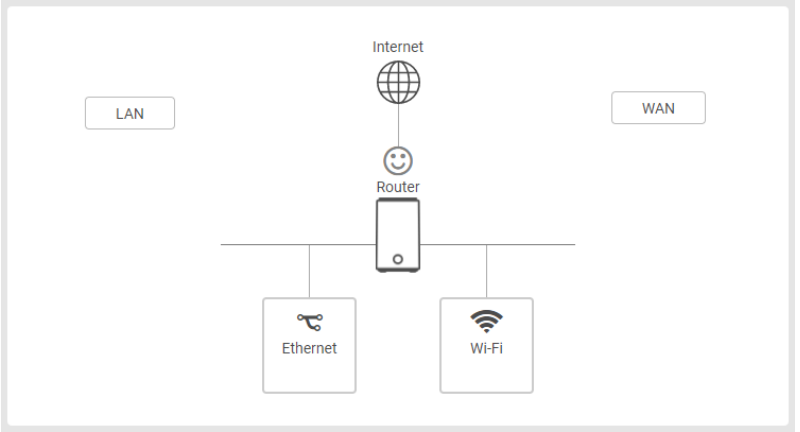
To change the Wi-Fi password associated with the Remote Worker Kit device, perform the following steps:

1. From the Home page of the Management Console Web interface**.**
2. Tap **Network**, then tap **Wi-Fi**.
3. Type your new password in the W-Fi Password field, and tap **Save**.

4.2 Network

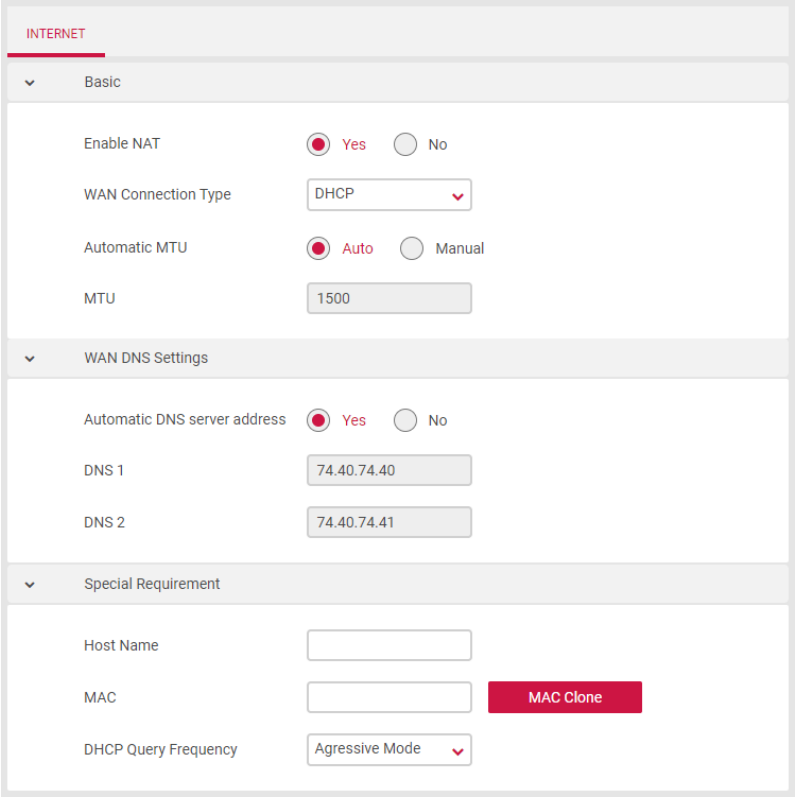
4.2.1 Network > Status

The network status map provides an overview of the network configuration with links to the settings page for each option.



4.2.2 Network > WAN > Internet

Internet connection settings between the Remote Worker Kit and the Internet Service Provider (ISP). The connection settings should be provided by your ISP to implement a proper connection between your device and the Internet.

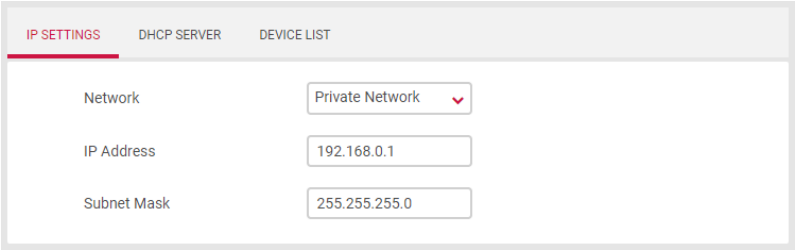


Basic	
Enable NAT	Enable NAT translation
WAN Connection Type	Select DHCP for automatically obtaining IP address or Static for manual entry. Static IP address requires the following information provided by the ISP. IP Address Subnet Mask Default Gateway Primary DNS Secondary DNS
Automatic MTU	Automatic or Manual MTU
MTU	Maximum packet transmission size

WAN DNS Settings	
Automatic DNS server address	Use ISP provided DNS or provide manual entry
DNS 1	Primary DNS Address
DNS 2	Secondary DNS Address
Special Requirement	
Host Name	Host name to assign to the Remote Worker Kit
MAC	Use the pre-configured MAC address for the router or provide a unique MAC address.
DHCP Query Frequency	Change the frequency the device provides a DHCP request.

4.2.3 Network > LAN > IP Settings

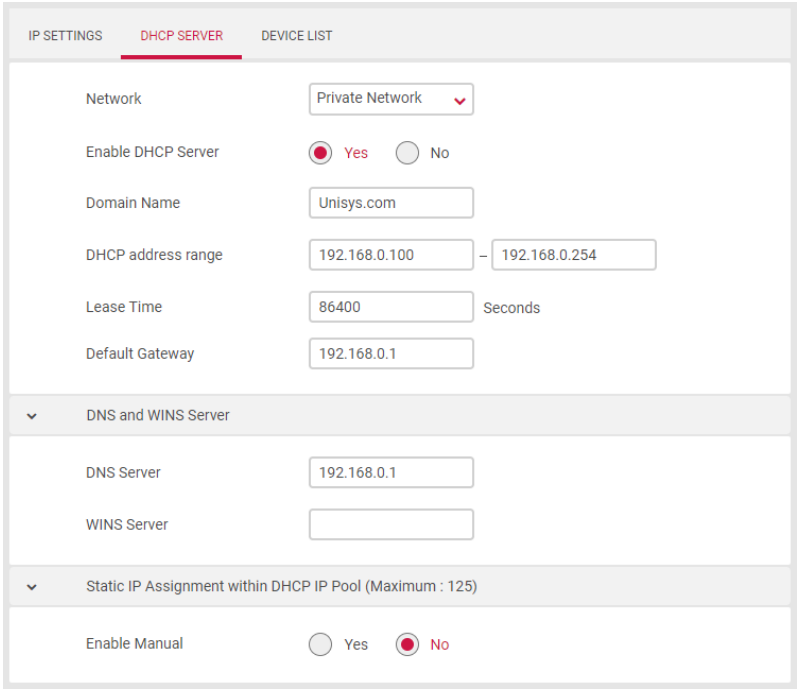
This page allows you to configure your gateway on your LAN.



IP Settings	
IP Address	The IP address in this field assigns the address to the RWK. Changing this value will change the IP address of the RWK.
Subnet Mask	Subnet Mask value in this field applies to the local network which is created by the RWK. Default is 255.255.255.0

4.2.4 Network > LAN > DHCP Server

This page allows you to configure your router as a DHCP server to assign IP addresses to other devices on your LAN.

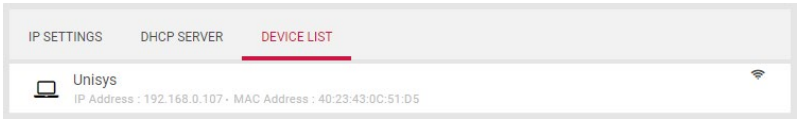


DHCP Server	
Network	Select one of the networks as DHCP server network.
Enable DHCP Server	Enables the local DHCP server to automatically assign IP addresses. This allows devices to connect without manual IP configuration.
Domain Name	Assigned domain name for the RWK.
DHCP Address Range	Allowed address range for IP address distribution.
Lease Time	Enter an address lease time in seconds. IP addresses will be assigned for this period of time before being reassigned.
Default Gateway	Default IP

DNS and WINS Server	
DNS Server	Enter a Domain Name Server address.
WINS Server	Enter a Windows Internet Name Service address.
Static IP Assignment within DHCP IP Pool	
Enable Manual	Toggle the switch to enable or disable Static IP Assignment.

4.2.5 Network > LAN > Device List

This page displays all devices (clients) connected to your router, by Ethernet (LAN) or Wi-Fi (wireless) e.g. laptops, smartphones. The device name, MAC address and IP address are listed for each device.

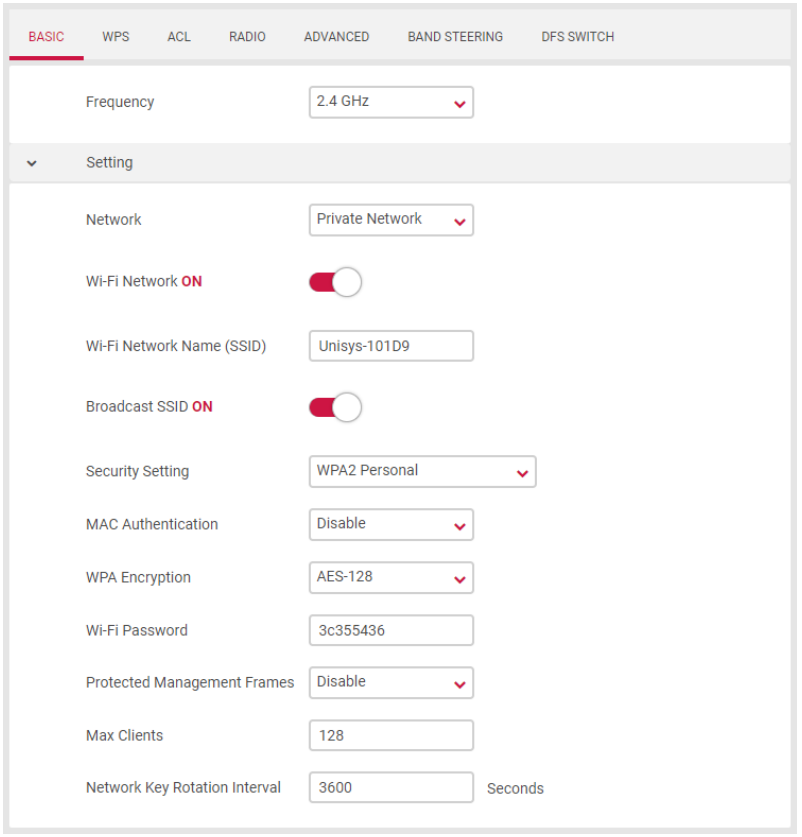


4.2.6 Network > Wi-Fi > Basic

Your router comes with an intuitive Web User Interface (Web UI) that allows you to manage your router's network Wi-Fi settings.

Note: *While many of the required Wi-Fi settings are pre-configured by default, it is recommended that you change the default Wi-Fi password that is associated with your Remote Worker Kit device.*

The **Wi-Fi** screen displays basic settings for your router's Wi-Fi. Your router is dual-band and uses two Wi-Fi frequencies (2.4GHz & 5GHz) for better wireless performance on your devices. You can edit advanced settings for 2.4GHz or 5GHz frequency bands by selecting the respective tab.

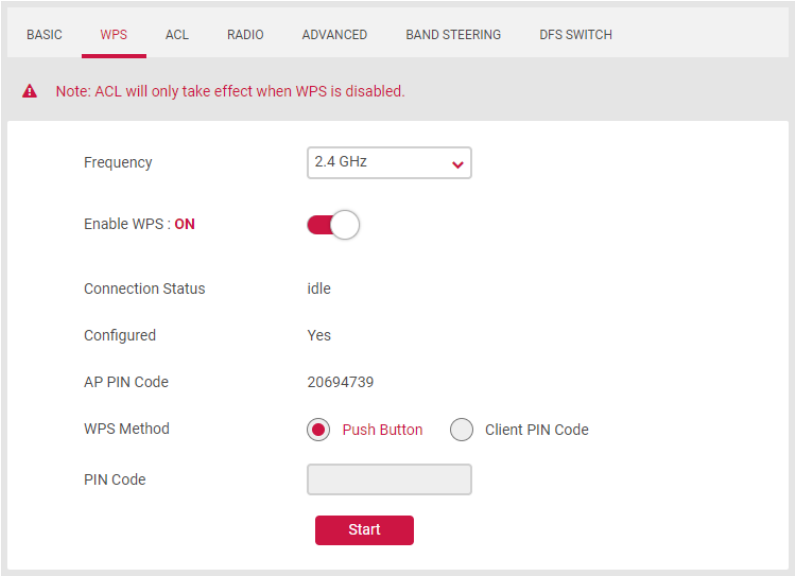


Basic	
Frequency	Select 2.4 GHz or 5 GHz. Default is 2.4 GHz.

Settings	
Network	Select between Private Network (default).
Wi-Fi Network <ON or OFF>	Toggle to enable or disable this Wi-Fi band.
Wi-Fi Network Name (SSID)	This is the name of your Wi-Fi network for identification, also sometimes referred to as "SSID". The SSID can consist of any combination of up to 32 alphanumerical characters.
Broadcast SSID <ON or OFF>	Enables visibility of the router's SSID in a mobile device list of available Wi-Fi networks. To improve security of your device, it is recommended that you disable this setting to prevent your Remote Worker Kit SSID from being broadcast as an available network to other devices.
Security Setting	Select a Wi-Fi security type from the drop-down menu. WPA2 personal is the default setting and the most secure.
WPA Encryption	Displays encryption type. This field must remain set to AES-128.
Wi-Fi Password	Enter your Wi-Fi password. It is strongly recommended that you change your password after initial login. **The Wi-Fi password must be 8 characters or longer.**
Protected Management Frames	If desired, you can enhance the security of your Wi-Fi connection, by enabling protected management frames. By default, this feature is disabled.
Max Clients	Identifies the number of clients that can be simultaneously connected to the Remote Worker Kit router. The default is 128.
Network Key Rotation Interval	Identifies the number of seconds…. The default is 3600 seconds.

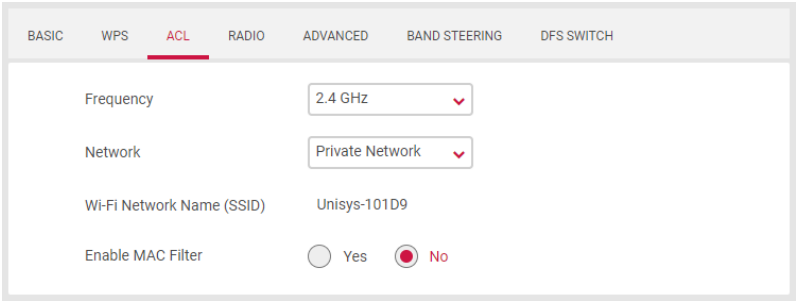
4.2.7 Network > Wi-Fi > WPS

The WPS feature is not supported on the Unisys Remote Worker Kit router.



4.2.8 Network > Wi-Fi > ACL

Access control list can allow or deny devices with one or more specified MAC addresses to connect to the wireless network.

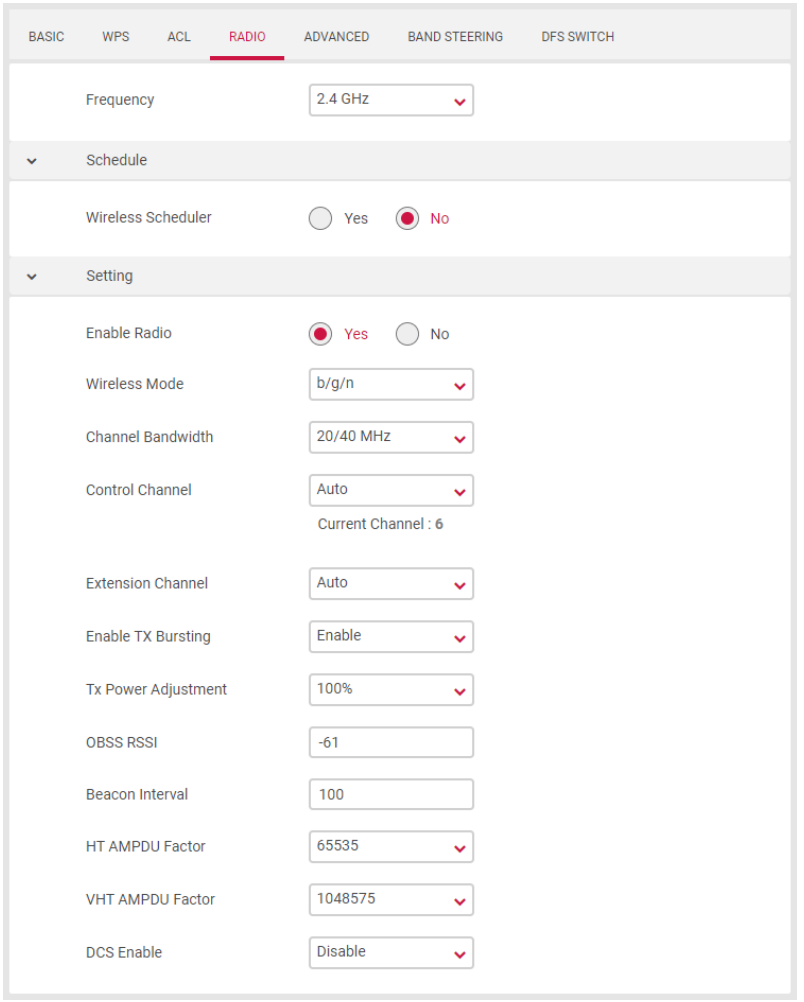


1. Enable ACL, select frequency and network.
2. Select MAC Filter Mode to Accept/Reject.
3. Add a rule, type a MAC address.
4. PC or smart phone with matched MAC address can or deny access to wireless network.

4.2.9 Network > Wi-Fi > Radio

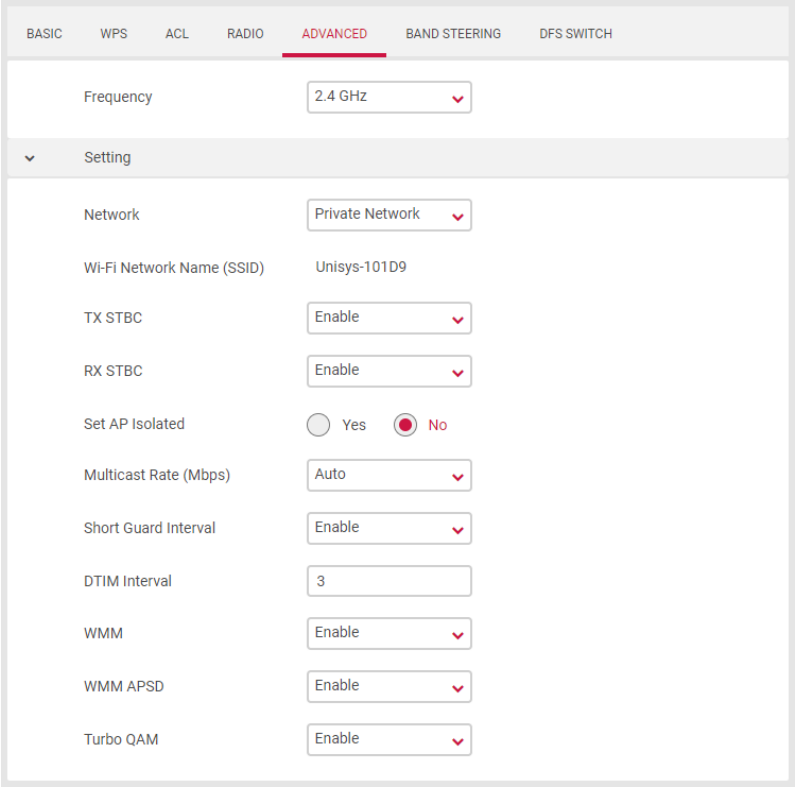
The Wi-Fi screen displays radio settings for your router's Wi-Fi. You can edit radio settings for 2.4GHz or 5GHz frequency bands by selecting the respective tab.

2.4 / 5 GHz Channel Settings	
Wireless Mode	2.4GHz: Select the wireless mode used for the router's Wi-Fi. Include **g/n, n, ax/n/g/b.** 5GHz: Select the wireless mode used for the router's Wi-Fi. Include **a, n/a, ac, ac/n/a, ax/ac/n/a.**
Control Channel	Select a wireless radio channel or use the default "Auto" setting from the drop-down menu. Changing radio channel can improve Wi-Fi signal depending on how crowded the channel is with other radio signals and interference.
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference), 40MHz (better performance but likely more interference), 80MHz (better performance but likely more interference), or Auto (automatically select based on interference level).



4.2.10 Network > Wi-Fi > Advanced

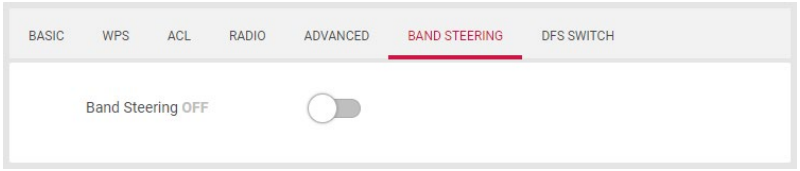
The Wi-Fi screen displays advanced settings for your router's Wi-Fi. You can edit radio settings for 2.4GHz or 5GHz frequency bands by selecting the respective tab.



2.4 / 5 GHz Advanced Settings	
Set AP Isolated	After it is enabled, all connected computers cannot be accessed by each other, and play a role of isolation to protect data security between different users.
TX STBC	Transmit rate.
RX STBC	Receive rate.
DTIM Interval	DTIM indicates the beacon interval that the AP will use to cache the package for the Station (for example, when the Station is sleeping).

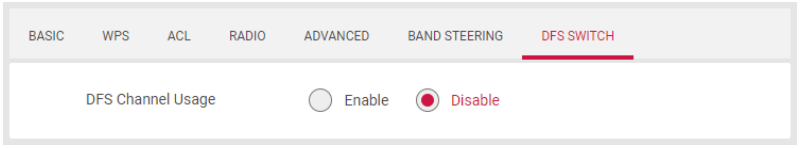
4.2.11 Network > Wi-Fi > Band Steering

Band Steering is a feature that encourages dual-band capable wireless clients to connect to the faster 5GHz Wi-Fi and leave the 2.4GHz Wi-Fi less-crowded for those clients who support 2.4GHz only; therefore, to improve Wi-Fi performance for all the clients.



4.2.12 Network > Wi-Fi > DFS Switch

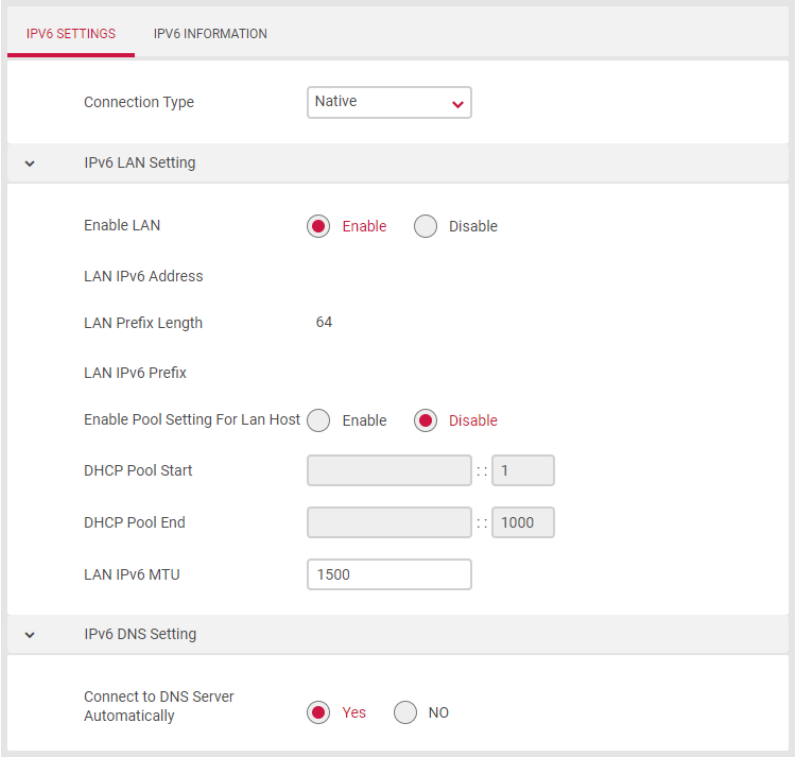
DFS Channel (Dynamic Frequency Selection) is an extension of the 802.11 protocol, allowing 5G channels to use radio system channels.



This mechanism defines that when using this 5G channel, it will not interfere with the normal operation of the normal radar. When these channels are detected, it is necessary to actively avoid them. It will be available after a while.

4.2.13 Network > IPv6 > IPv6 Settings

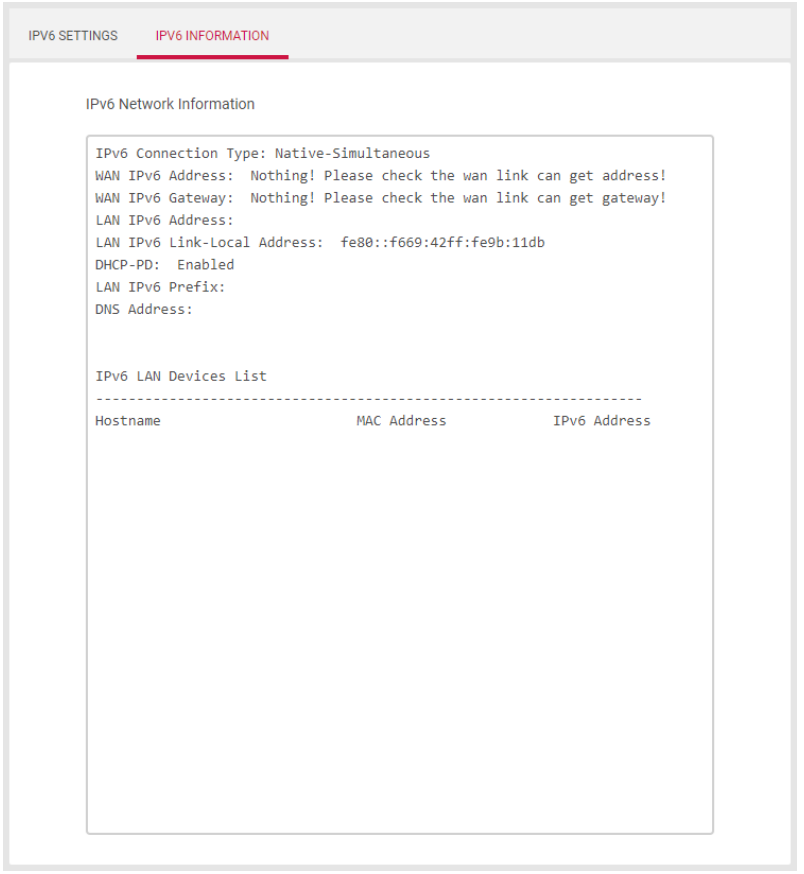
IPv6 (Internet Protocol Version 6) is a next-generation IP protocol designed by the IETF (Internet Engineering Task Force) to replace the current version of the IP protocol (IPv4). With the shortage of IPv4 resources, IPv6 will become the standard of the next generation of Internet addresses in the near future. Compared with IPv4, IPv6 has rich IP address resources.



IPv6 Settings	
Connection Type	Native.
IPv6 LAN Setting	
Enable LAN	Toggle the switch to enable or disable IPv6 LAN.
LAN IPv6 Address	Internet Protocol Version 6 (IPv6) is a network layer protocol that enables data communications over a packet switched network.
LAN Prefix Length	IPv6 Prefix Length is used to identify how many bits of a Global Unicast IPv6 Address are there in a network packet.
LAN IPv6 Prefix	The leftmost fields of the IPv6 address along with the network bits length represented in CIDR format is known as the network prefix.
Enable Pool Setting	Toggle the switch to enable or disable IPv6 LAN DHCP Pool.
DHCP Pool Start	Enter the start IPv6 address of the DHCP Pool.
DHCP Pool End	Enter the end IPv6 address of the DHCP Pool.
LAN IPv6 MTU	MTU (Maximum Transmission Unit) is the single largest frame or packet of data that can be transmitted across a network.
IPv6 DNS Setting	
Connect to DNS Server Automatically	Toggle the switch to connect to DNS server or not.
IPv6 DNS Server 1	Enter a DNS Server address manually.
IPv6 DNS Server 2	Enter a second DNS Server address manually.

4.2.14 Network > IPv6 > IPv6 Information

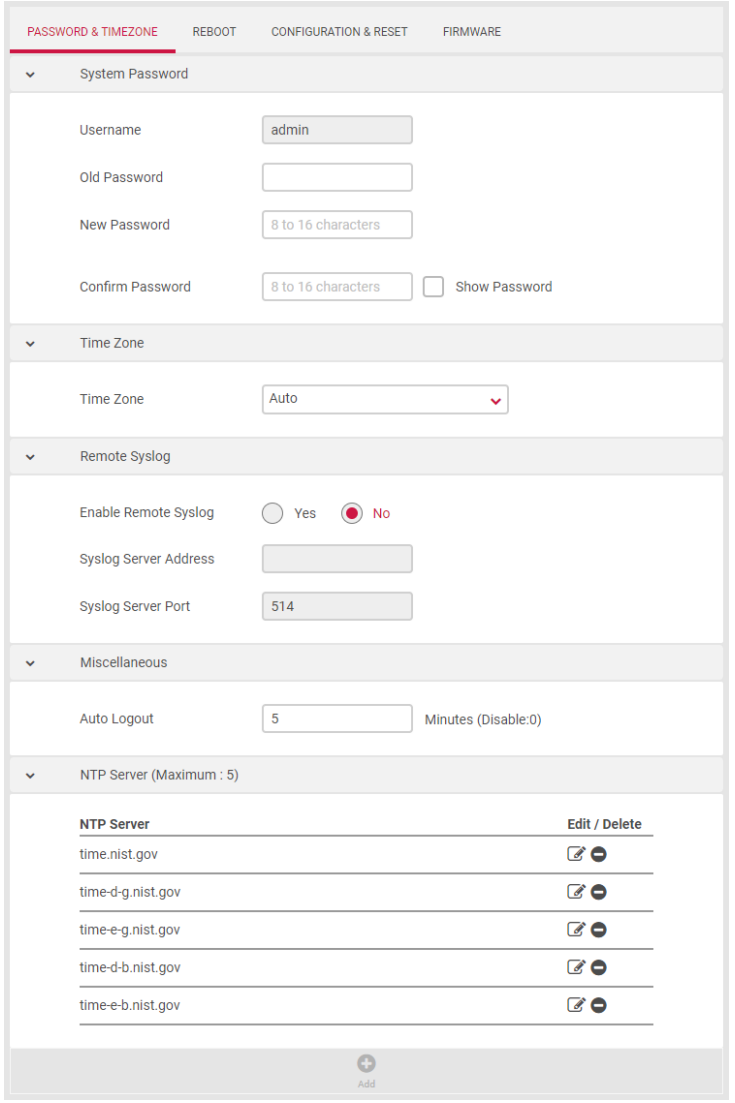
The IPv6 status displayed on the right:



4.3 System Settings

4.3.1 System Settings > Password & Timezone

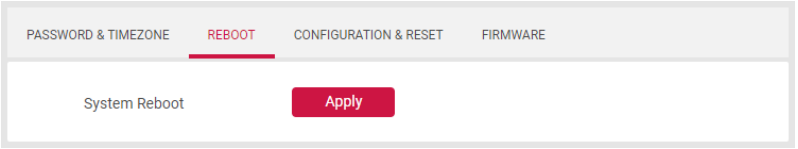
This page allows you to configure device login password and time settings.



PASSWORD & TIMEZONE	
Old Password	Old Password
New Password	A string used for log in authentication. Its length ranges from 8 to 16 characters - a combination of letters, digits, and special characters.
Time Zone	Default time-zone is Auto
Syslog Server Address	IP address of a syslog server which log messages will be sent to.
Auto Logout	Auto sign out time in minutes. Set 0 will disable auto logout function.
NTP Server	A network time server to synchronize the clocks of devices over a network.

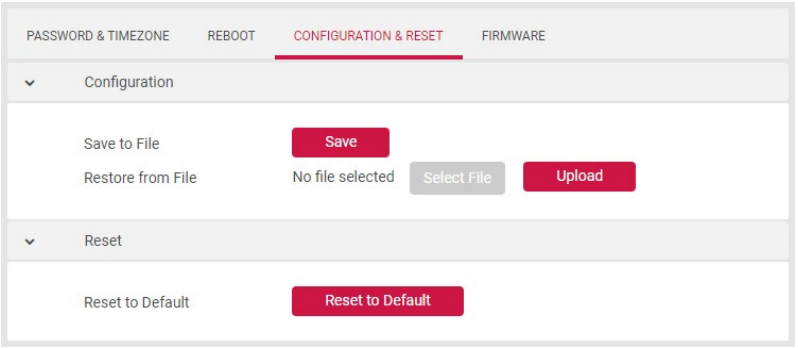
4.3.2 System Settings > Reboot

Restarting the router can be performed by pressing the Apply button. The router should be back online within 120 seconds.



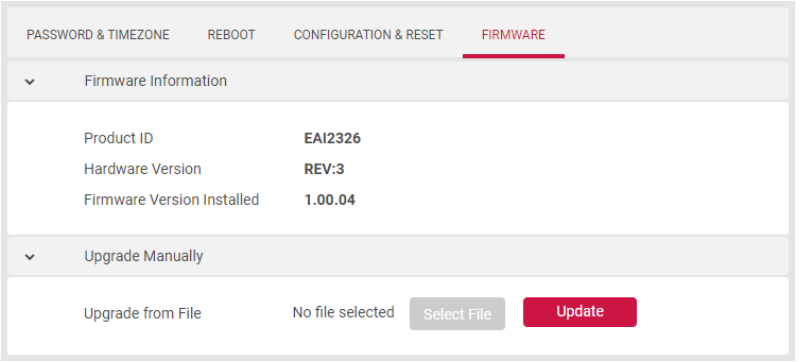
4.3.3 System Settings > Configuration & Reset

The Configuration & Reset page enables you to save/upload the router's current settings as a file to your local computer or upload your router to previously saved settings by loading a backed-up file. You can also reset the router back to factory default settings. If the router malfunctions or is not responding, then it is recommended that you first **reboot the device** (press the reset button for 1 second), and if still experiencing problems **reset the device back to its factory default settings**. You can reset the router back to its default settings using the Reset button on the back of the router (press and hold for 5+ seconds).



4.3.4 System Settings > Firmware

The Firmware page displays your router's firmware version and hardware version information. It can also upload images to your router and update router's firmware.



5. FCC Statement

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the 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 in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and 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/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device operates in the 2.4GHz and 5GHz frequency and is restricted for indoor use.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 21 cm between the radiator & your body.

ASKEY INTERNATIONAL CORPORATION (AIC)

- 4017 Clipper Court,Fremont CA 94538,USA **TEL：**+1-510-573-1259