# Table of Contents

Getting Started................................................................................................................................ 5

Connecting a Recon Sentinel .......................................................... 5
Creating or Login to an Account.................................................... 6
Registering a Recon Sentinel......................................................... 8

Main Menu.......................................................................................... 9

About................................................................................................. 9

Toggle Help Mode ............................................................................ 12
Send Us Feedback ............................................................................ 13
Sign Out............................................................................................. 13

Console.............................................................................................. 14

Connected Recon Sentinels ......................................................... 14
Add New Recon Sentinel ............................................................... 15
Device Status Legends................................................................. 16
  Active Defense Countermeasures (ADC) ................................... 16
  Health Status Legend ................................................................. 16

Home................................................................................................. 17

Message Center .............................................................................. 17
  Critical ......................................................................................... 17
  Warning ....................................................................................... 17
  Messages ..................................................................................... 17
  Online .......................................................................................... 17

Turn On/Turn Off ADC ................................................................. 18
Subscription ..................................................................................... 18
Fix Wizard ....................................................................................... 18

Status.............................................................................................. 22

Critical ............................................................................................ 23
  Unknown Devices ...................................................................... 23
  Attacks ....................................................................................... 26
  Warning ...................................................................................... 27

Informational .................................................................................. 28
  New Services .............................................................................. 28
  Trusted ....................................................................................... 29
Messages ............................................................................................................................... 33
Online Devices .......................................................................................................................... 35
Offline Devices .......................................................................................................................... 35
Live Status .................................................................................................................................. 36
Settings .......................................................................................................................................... 37
Configure ................................................................................................................................... 37
Set Name ....................................................................................................................................... 38
Turn On/Turn Off ADC ............................................................................................................... 39
Turn Off/Turn On Screen ............................................................................................................ 40
Control ....................................................................................................................................... 41
Factory Reset ............................................................................................................................... 41
Reboot ....................................................................................................................................... 42
Shut Down .................................................................................................................................. 43
Profile ........................................................................................................................................... 44
User Information ......................................................................................................................... 45
Subscription Information ............................................................................................................ 48
LIMITED WARRANTY RECON SENTINEL ......................................................................................... 49

**NOTE:** Pictures shown below may be different than the current version of the App and/or Website
Congratulations!

Hackers are now using home networks and IoT devices to steal personal data, attack others and more. With new threats and vulnerabilities discovered daily, current products are DIFFICULT to install, configure for use, don’t work with existing equipment, and are expensive.

Cybersecurity Defense Solutions (CDS) is proud to introduce Recon Sentinel™ Essential. A cybersecurity device designed to add a layer of detection and protection above and beyond traditional anti-virus, anti-malware and firewall solutions.

Recon Sentinel was designed for ease of use and works with all routers, firewalls and wireless access points without slowing down Internet connectivity. It is the perfect complement to existing antivirus and anti-malware solutions, and provides automatic updating of the device’s firmware to ensure you always have the best protection possible.

Recon Sentinel sits on your network like a trusted soldier, constantly looking for signs of cybercriminal reconnaissance, intrusion or other nefarious activity.

Once detected, Recon Sentinel will take actions to disrupt the communications of the attacking device, stopping the cybercriminal in their tracks and alerting you to their presence.
Getting Started
Getting started with a new Recon Sentinel is easily done in a few quick steps!

Connecting a Recon Sentinel
After taking the Recon Sentinel out of the box, connect the Ethernet cable into the Recon Sentinel and any open Ethernet port of your router/modem.

*NOTE: USB Ports are disabled for future development.*

Plug the power adapter into an outlet and the Recon Sentinel.

The Recon Sentinel will now power on and once running, will display its Device ID. The next step is to create an account.
Creating or Login to an Account
To Create an Account, go to www.reconsentinel.com, or download the Recon Sentinel App from the Apple App Store or Google Play Store. From within the App or Website, select the ‘Register User’ button.

After completing the registration form, the ‘Register’ button should be selected to submit and finalize your new account.

**NOTE:** Creating a new account can be skipped if you already have an existing account. Simply login with your ‘Username/Email’ and ‘Password’ associated with your existing account.
The ‘Forgot Password’ button can be selected if you don’t remember your password and find yourself locked out of your account. The Username is used to lookup your account information for resetting the password.

A verification code is sent via email from no-reply@reconsentinel.com. Once you have entered the Verification Code and your New Password, select the ‘Submit’ button to reset the password for your account.
After successfully resetting your password, you can return to the login screen to login with your new password.

Registering a Recon Sentinel
Registering a Recon Sentinel to your account can be done by selecting the ‘Add New Recon Sentinel’ button from the Console panel along with the Device ID displayed on the Recon Sentinel LCD screen. For more information, see the Add New Recon Sentinel section.
Main Menu

The Main Menu can be opened by selecting the menu icon in the upper right corner of every main page.

Language Selection

The website and app can be set to display messages in English, Spanish, or French. The default language selection is English.
Selecting the displayed language from the Main Menu will provide you with the Language Options Menu. Select the desired language from the list, and then select ‘OK’ to change the displayed messages.
About

Selecting ‘About’ from the Main Menu will provide you with an ‘About this App’ section, as well as an ‘About Recon Sentinel’ section.

The ‘About this App’ section will detail the current and previous versions, while also listing the new features and bug fixes released with each version.
The ‘About Recon Sentinel’ section provides a quick overview of what Recon Sentinel does, while detailing key protection features offered by the device.

### About Recon Sentinel

#### What is a Recon Sentinel?

The Recon Sentinel is a small, inconspicuous cyber security device designed to add a layer of detection and protection above and beyond traditional anti-virus, anti-malware and firewall solutions.

- Works with all routers, firewalls and wireless access points.

#### Key Features

- Real Time Network Inventory
- Online/Offline Status
- Trusted/Unknown Devices
- Active Defense Countermeasures (ADC)

### Toggle Help Mode

The ‘Toggle Help Mode’ switch will toggle the information displayed across the various sections of each page within the App/Website. If Help Mode is enabled, each section will have a quick description. These descriptions are hidden when Help Mode is disabled. By default, Help Mode is disabled.
Send Us Feedback
Selecting ‘Send Us Feedback’ from the Main Menu provides you with a way to report a problem, suggest a new feature, or leave a comment about the App/Website or Recon Sentinel device.

Sign Out
Selecting ‘Sign Out’ from the Main Menu will sign you out of the App/Website. You are prompted with a confirmation to sign out before being signed out.
Console
The Console page displays the status of all Recon Sentinel devices registered to your account.

Connected Recon Sentinels
The status for all of your Recon Sentinels can be quickly viewed in the Console page. The Health Status, Device Name, Device ID, and Active Defense Countermeasures (ADC) statuses are shown for each Recon Sentinel device.

Selecting a Recon Sentinel device button from the Console page will direct you to that Recon Sentinel’s Home page and provide more information about the current device status.
Add New Recon Sentinel

The ‘Add New Recon Sentinel’ button will step you through the process of registering a new Recon Sentinel device to your account. There is no limit to the number of Recon Sentinel devices registered to your account. This comes in handy for business users as a system administrator can monitor and interact with many devices at one time.

Make sure you select the Vendor where you purchased your Recon Sentinel when entering the New Device Information during the Add New Device process.
Device Status Legends

Active Defense Countermeasures (ADC)
Active Defense Countermeasures (ADC) allow the Recon Sentinel to “disrupt or block” internet access to a device. When enabled, blocking is automatically performed for unknown devices detected on your network or trusted devices that exhibit dangerous behavior. To protect your network, the blocked devices will not have access to the internet until you resolve the issue with the device.

Below is a table illustrating the various connection permissions allowed for all devices detected to your network:

<table>
<thead>
<tr>
<th>Device Type</th>
<th>ADC Status</th>
<th>Block Button Status</th>
<th>Is Device Blocked??</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown Device</td>
<td>Enabled</td>
<td>Blocked</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unblocked</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
<td>Blocked</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unblocked</td>
<td>No</td>
</tr>
<tr>
<td>Trusted Device (Attacking)</td>
<td>Enabled</td>
<td>Blocked</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unblocked</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
<td>Blocked</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unblocked</td>
<td>No</td>
</tr>
<tr>
<td>Trusted Device (Not Attacking)</td>
<td>Enabled</td>
<td>Blocked</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unblocked</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
<td>Blocked</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unblocked</td>
<td>No</td>
</tr>
</tbody>
</table>

Health Status Legend
The Health Status Legend shows the various icons used for each status that a Recon Sentinel device may be in:

- The **Critical** icon 🔄 is used to show that a critical event has occurred, such as new devices and/or attacks that are detected
- The **Warning** icon 🚨 is used to show that potentially dangerous activity was detected, such as Network Scans
- The **OK** icon ✓ is used to show that no issues have been detected and that the network is currently protected
- The **Offline** icon 🌍 is used to show that the Recon Sentinel is offline due to no Internet connectivity or no power
- The **Busy** icon 🥊 is used to show that the Recon Sentinel is processing a user-issued command, such as completing registration, rebooting, or finding a device using SONAR

www.reconsentinel.com
Home
The Home page provides you with a status overview for the selected Recon Sentinel, as pictured below.

![Home Page Screenshot]

Message Center
The message center provides you with the number of alerts reported by Recon Sentinel. The alerts are displayed in various categories based on importance.

Critical
Critical messages are high priority alerts that may have a critical impact to your network. These alerts cover new unknown devices that have connected to your network, as well as possibly malicious attacks performed by devices currently connected to your network.

Warning
Warning messages are important alerts that you should review to ensure that they don’t pose any risk to your network. These alerts cover Network Scans that appear from devices connected to the network.

Messages
Messages are used for information alerts from your Recon Sentinel that may include New Services, update notifications, upcoming sales, or other important events.

Online
Online messages will show you which trusted and unknown devices are actively connected to your network.
**Turn On/Turn Off ADC**

The ‘Turn On ADC’ button will enable Active Defense Countermeasures (ADC) for your network by actively blocking unknown devices or trusted devices that are performing attacks on your network.

When ADC is enabled, the button will toggle to ‘Turn Off ADC’ for disabling of ADC.

**Subscription**

The Subscription section displays the current subscription status of your Recon Sentinel. Selecting the ‘Subscription’ button will redirect you to a website where you can manage your subscription.

**Fix Wizard**

If issues are detected with your network by Recon Sentinel, a Fix Wizard is displayed to help quickly fix issues in order of importance. To use the Fix Wizard, select the Status icon from the Home page. The wizard will open and then provide each task one at a time, that require your attention.

The tasks will begin by addressing Unknown Device Alerts. For each unknown device, you will have the ability to ‘Find’ the device, ‘Trust’ the device, ‘Remove’ the device from the Unknown Devices List, or ‘Block’ the device. If you don’t wish to perform a fix for the task, you can select the ‘Skip’ button to move on to the next task. For more information about Unknown Device Alerts, see the Unknown Devices section.

---

**Fix Wizard**

Unknown Device Alert Tasks (part 1)

---

**Fix Wizard**

Unknown Device Alert Tasks (part 2)
The next set of tasks address Attack Alerts. For each attack, you can ‘Accept’ to acknowledge and clear the alert or ‘Ignore’ the alert. If you don’t wish to perform a fix for the task, then you can select the ‘Skip’ button to move on to the next task. For more information about Attack Alerts, see the Attacks section.
The final set of tasks address Network Scan Alerts. For each network scan, you can ‘Accept’ to acknowledge and clear the alert or ‘Ignore’ the alert. If you don’t wish to perform a fix for the task, then you can select the ‘Skip’ button to move on to the next task. For more information about Network Scan Alerts, see the Network Scans section.
If the Recon Sentinel reports no issues with your network, selecting the Status icon from the Home page will display tasks for all Network Service Messages. For each network service, you can ‘Accept’ to acknowledge and clear the message or ‘Ignore’ the message. If you don’t wish to perform a fix for the task, then they can select the ‘Skip’ button to move on to the next task. For more information about Network Service Messages, see the New Services section.

If no Network Service Messages are available for your Recon Sentinel, then you will be directed to the Live Status page. For more information about Live Status Monitoring, see the Live Status section.
After all tasks have been addressed within the Fix Wizard, you will see a confirmation screen that will return you to the Home page.

**Status**
The Status page displays the various alerts available to you based on their importance level: Critical, Warning, and Informational.
**Critical**
The Critical section contains alerts that may have a critical impact on your network. Alerts of this type may be serious and require your attention.

**Unknown Devices**
An Unknown Device is a device connected to your network (phone, computer, tablet, IoT device, etc.) that you have not trusted. New devices to the network will show up as unknown and will remain this way until you trust the device for use on your network.

Selecting the ‘Unknown Devices’ button in the Critical section will provide detailed information for all detected Unknown Devices.

All unknown devices can be trusted using the ‘Trust All’ button. If you don’t want to trust all unknown devices, then each device can be individually trusted using the ‘Trust’ button displayed for each device.

The ‘Include Offline Devices’ switch will toggle offline devices from being displayed in the Unknown Devices List. Online devices are those that are actively connected to your network, while offline devices are those that were previously connected but are not currently using your network.

The Search field allows you to search for devices based on keywords such as Name, Operating System, Manufacturer, etc. All keyword searches are not case-sensitive.

Each unknown device can be removed from the Unknown Devices List by selecting the ‘Remove’ button displayed for each device. If the device is Online, then the Recon Sentinel will place the
device back in the list upon performing the next scheduled device scan. If the device is Offline, it will remain out of the list until the next time it connects to the network as an Online device.

The button can be used to edit the device name within the Unknown Devices List.

Each unknown device has a ‘More Info’ button to display additional information. This can be useful when attempting to identify the device. The ‘Less Info’ button will appear when all available device information is being displayed and allows you to hide the expanded informational view.

![Unknown Devices (More Info)](image)

The button will expand to display all network services running on this device.
You can block a device from connecting to the internet by selecting the ‘Block’ button. Upon selecting the block button for the device, you will be prompted to confirm blocking the selected device.

Blocking a device may take a few minutes. Some devices attempt to gain a new IP address when their initial IP address has been blocked. Blocking unknown devices happens automatically if ADC is enabled. Selecting the ‘Block’ or ‘Unblock’ buttons while ADC is enabled can also be used to set the connection permissions for a device if ADC is disabled at a later time.
Locating a device on your network can be done using the Simple ONline Active Reconnaissance or ‘SONAR’ feature of Recon Sentinel by following these steps:

1. Select the ‘Find’ button for the device you wish to locate
2. Once SONAR is running, begin disconnecting devices from your network one device at a time by powering off the device, turning on Airplane Mode, Turning Off WiFi, or disconnecting the Ethernet cable from the device
   
   **NOTE: You should disconnect 1 device at a time, rather than disconnecting a group of devices together.**

3. If SONAR doesn’t report “Found It!” after disconnecting a device from the network, then repeat Step 2 for each different device until Recon Sentinel reports “Found It!”
4. Once you find the device, make sure you name it in your Recon Sentinel

A device can be shown as Online or Offline based on its connectivity to your network. Each device will display the status in the bottom right of the device information.

**Attacks**
Attacks occur when a device purposely targets special ‘traps’ controlled by the Recon Sentinel. Devices that are found to be attacking your network, typically are doing so with malicious intent.

Some attacks are passive in nature, which means that they are used to monitor information on the network. Other attacks are considered active, meaning that information is altered with intent to corrupt or destroy data.
Selecting the ‘Attacks’ button in the Critical section will provide detailed information for all detected network attacks.

The ‘View Host’ button provides information about the host device that was used to issue the attack.

**Warning**
The Warning section contains alerts that should be reviewed to make sure they don’t pose any risk to your network.

**Network Scans**
Network Scans occur when a device performs an analysis of open network ports. This is a common tactic used by hackers, but it may also be used by legitimate software for a variety of reasons.
Selecting the ‘Network Scan’ button in the Warning section will provide detailed information for all detected network scans from connected devices.

**Informational**
The Information section contains alerts that are not considered a threat to the security of the network and may include update notifications, important events, and more.

**New Services**
New Services are network services found by the Recon Sentinel. A network service is typically an application that runs in the background and provides some type of service for the computer or network. An example would be a fax service that allows you to send and receive faxes without having to start a program each time. Hackers may use services to gain control of a network, however legitimate software may also use services.
Selecting the ‘New Service’ button in the Informational section will provide detailed information for all detected network services from connected devices.

**Trusted**

Trusted Devices will display any device on your network (phone, computer, tablet, IoT device, etc.) that was previously considered a safe device.
Selecting the ‘Trusted’ button in the Informational section will provide detailed information for all detected Trusted Devices.

All trusted devices can be untrusted using the ‘Untrust All’ button. If you don’t want to untrust all trusted devices, then each device can be individually untrusted using the ‘Untrust’ button displayed for each device.

The ‘Include Offline Devices’ switch will toggle offline devices from being displayed in the Trusted Devices List. Online devices are those that are actively connected to your network, while offline devices are those that were previously connected but are not currently using your network.

The Search field allows you to search for devices based on keywords such as Name, Operating System, Manufacturer, etc. All keyword searches are not case-sensitive.

Each trusted device can be removed from the Trusted Devices List by selecting the ‘Remove’ button displayed for each device. If the device is Online, then the Recon Sentinel will place the device back in the list upon performing the next scheduled device scan. If the device is Offline, it will remain out of the list until the next time it connects to the network as an Online device.

The button can be used to edit the device name within the Trusted Devices List.
Each trusted device has a ‘More Info’ button to display additional information that can be useful when attempting to identify the device. The ‘Less Info’ button will appear when all available device information is being displayed and allows you to hide the expanded informational view.

The 👀 button will expand to display all network services running on this device.
You can block a device from all network activity by selecting the ‘Block’ button. Blocking a trusted device is useful for a variety of reasons, such as limiting a person’s Internet access or turning off devices that aren’t frequently used while using a streaming device (i.e. watching Netflix® with a Smart TV, Roku®, etc.). Upon selecting the button for a given device, you will be prompted to confirm blocking the selected device.

Blocking a device may take a few minutes because some devices attempt to gain a new IP address when their initial IP address has been blocked.
Locating a device on your network can easily be done using the SONAR feature of Recon Sentinel! Using SONAR is easily done by following the below steps:

1. Select the ‘Find’ button for the device you wish to locate
2. Once SONAR is shown as running, begin disconnecting devices from your network one device at a time by powering off the device, turning on Airplane Mode, Turning Off WiFi, or disconnecting the Ethernet cable from the device
   
   **NOTE: You should disconnect 1 device at a time, rather than disconnecting a group of devices together.**

3. If SONAR doesn’t report “Found It!” after disconnecting a device from the network, then repeat Step 2 for a different device until Recon Sentinel reports “Found It!”
4. Once you find the device, make sure you name it in your Recon Sentinel

A device can be shown as Online or Offline based on its connectivity to your network. Each device will display the status in the bottom right of the device information.

**Messages**

Messages are used for informational alerts about update notifications, upcoming sales, or other important events.
Selecting the ‘Messages’ button in the Informational section will provide detailed information for all messages in the Message List.

The ‘Accept All’ button will acknowledge and clear all messages from the Message List. If you don’t wish to acknowledge all messages as once, then the ‘Accept’ button for each individual message can be selected to acknowledge them individually.
**Online Devices**
Selecting ‘Online Devices’ will display all devices that are actively connected to your network. The devices shown may be a combination of unknown and trusted devices.

![Online Devices](image)

**Offline Devices**
Selecting ‘Offline Devices’ will display all devices that are not actively connected to your network, but were at a previous time. The devices shown may be a combination of unknown and trusted devices.

![Offline Devices](image)
Live Status
Selecting ‘Live Status’ will provide you with the current status of your Recon Sentinel.

The current status and up to the previous 100 status updates will be displayed to you from the time that the Live Status page was entered.

Live Status updates are provided anytime that a new status update is available. New status updates can be from a variety of things, such as new alerts, new command being executed, periodic device check-in, and more.
Settings
The Settings page provides you access to customizing or controlling various features of your Recon Sentinel.

Configure
The Configure section contains commands used to configure various settings for your Recon Sentinel.
Set Name
Selecting the ‘Set Name’ button allows you to rename the Recon Sentinel device.

Once the new device name has been entered, the ‘Save’ button will save the new name for your Recon Sentinel. The ‘Cancel’ button will discard any changes to the name and will continue using the current name for your Recon Sentinel.
**Turn On/Turn Off ADC**

The ‘Turn On ADC’ button will enable Active Defense Countermeasures (ADC) for your network by actively blocking unknown devices or devices that are performing attacks on your network.

When ADC is enabled, the button will toggle to ‘Turn Off ADC’ for disabling of ADC.
**Turn Off/Turn On Screen**

The ‘Turn Off Screen’ button will disable the LCD screen on the Recon Sentinel device. If disabled, you will not see any messages displayed on the LCD screen until the screen has been enabled using the ‘Turn On Screen’ button or the device has been rebooted/power cycled. The LCD screen will automatically turn back on if a new alert is available and will remain on until you re-select the ‘Turn Off Screen’ button.
Control
The Control section contains commands for controlling your Recon Sentinel.

Factory Reset
The ‘Factory Reset’ button will reset the Recon Sentinel device back to factory defaults. Resetting the device to factory defaults will clear all pending alerts/messages, clear all unknown and trusted device lists, and clear all Recon Sentinel configuration options. The process of a Factory Reset is similar to re-installing the operating system on your computer. After resetting the device to factory defaults, the device is unregistered from your account.

Factory Reset Confirmation
Factory Reset In Progress
Factory Reset Complete
**Reboot**

The ‘Reboot’ button will instruct the Recon Sentinel to go through a clean reboot process, much like restarting a computer.

During the restart procedure, your network will not be protected by Recon Sentinel.
Shut Down

The ‘Shut Down’ button will instruct the Recon Sentinel to shut down. While the Recon Sentinel is shut down, your network will not be protected by Recon Sentinel.

Because the Recon Sentinel is not meant to be powered off, there is no power button. To reboot the Recon Sentinel after a shut down, you should remove and re-insert the power cable to the device.
Profile
The Profile page provides you with tools to edit your account information, as well as Recon Sentinel device subscriptions.
User Information

The User Information section provides you with a way to update your contact information, account password, and notification settings.

Selecting the ‘Edit User Info’ button displays the ‘Contact Info’ tab within the Edit/View User page. This tab provides you with the ability to update all contact information such as Email Address, Name, Address, and Phone Number.
Selecting the ‘Password’ tab at the top of the Edit/View User page allows you to change your account password. To change a password, you will be required to enter the old password.
Selecting the ‘Alert Settings’ tab at the top of the Edit/View User page allows you to customize the types of alerts that you wish to receive. Each alert method can be enabled for the 3 alert types (Critical, Warning, and Info) by selecting the appropriate checkbox. Alerts can be delivered as Email Alerts or Mobile Alerts (App Push Notifications).
Subscription Information
The Subscription Information section displays the current subscription status of every Recon Sentinel device registered to your account. The Recon Sentinel service is a subscription-based service that is billed annually. Once the subscription expires, the Recon Sentinel will no longer be protecting your network. Selecting a specific Recon Sentinel from the list will redirect you to a webpage to manage the subscription renewal.
LIMITED WARRANTY RECON SENTINEL

Who provides this Limited Warranty: This warranty is provided by Cybersecurity Defense Solutions, (“CDS”).

What this Limited Warranty covers and how long it lasts: CDS warrants the Recon Sentinel device ("Device") against defects in materials and workmanship under ordinary consumer use in accordance with the Device documentation for one year from the date of Device activation. Please note, CDS may consider the Device to be activated in certain circumstances following purchase, even if you do not take direct action to activate the Device, as further described in the documentation.

The warranties in this paragraph are collectively referred to as CDS’ “Limited Warranty”. What CDS will do to correct problems covered under this Limited Warranty: During this warranty period, if a defect arises in the Device, and you follow the instructions for returning the Device, CDS will at its option, to the extent permitted by law, in its sole discretion (i) repair the Device using either new or refurbished parts, (ii) replace the Device with a new or refurbished Device that is functionally at least equivalent to the Device to be replaced, or (iii) refund to you all or part of the purchase price of the Device in exchange for your return of the Device. This Limited Warranty applies, to the extent permitted by law, to any repair, replacement part or replacement device for the remainder of the original warranty period or for ninety days, whichever period is longer. All replaced parts and Devices for which you receive a refund will become CDS’ property.

What this Limited Warranty does not cover: The Limited Warranty will apply only if you purchased your Device from CDS or its authorized resellers. This Limited Warranty only applies to hardware components of the Device (and not any associated software), and this Limited Warranty does not apply to damage caused by shipment, accident, misuse, neglect, disassembly, alterations, repair, fire or other external causes, normal wear and tear or commercial or other non-consumer use.

TO THE EXTENT PERMITTED BY LAW, THE WARRANTY AND REMEDIES SET FORTH ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES AND REMEDIES, AND CDS SPECIFICALLY DISCLAIMS ALL STATUTORY AND IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND AGAINST HIDDEN OR LATENT DEFECTS. IF CDS CANNOT LAWFULLY DISCLAIM STATUTORY OR IMPLIED WARRANTIES, THEN TO THE EXTENT PERMITTED BY LAW, ALL SUCH WARRANTIES SHALL BE LIMITED IN DURATION TO THE DURATION OF THIS EXPRESS LIMITED WARRANTY AND TO REPAIR OR REPLACEMENT SERVICE. Some states, provinces, countries and jurisdictions do not allow limitations on how long a statutory or implied warranty lasts, so the above limitation may not apply to you.
CDS IS NOT RESPONSIBLE FOR DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM ANY BREACH OF WARRANTY OR UNDER ANY OTHER LEGAL THEORY. IN SOME JURISDICTIONS THE FOREGOING LIMITATION DOES NOT APPLY TO DEATH OR PERSONAL INJURY CLAIMS, OR ANY STATUTORY LIABILITY FOR INTENTIONAL AND GROSS NEGLIGENT ACTS AND/OR OMISSIONS, SO THE ABOVE EXCLUSION OR LIMITATION MAY NOT APPLY TO YOU. Some states, provinces, countries and jurisdictions do not allow the exclusion or limitation of direct, incidental or consequential damages, so the above exclusion or limitation may not apply to you. No vendor, seller, authorized reseller, employee or representative of CDS or any third party is authorized to make any modification, extension or addition to this Limited Warranty. If any term of this Limited Warranty is held to be illegal or unenforceable, the remaining terms of this Limited Warranty will remain in full force and effect.

How you can receive service: For specific instructions and information regarding how to obtain warranty service for your Device, please contact Customer Support at https://www.reconsentinel.com/support. In general, you will need to deliver your Device in either its original packaging or in equally protective packaging to the address specified to you by Customer Support. Before you deliver your Device for warranty service, it is your responsibility to remove any information entered in conjunction with your use of the device. CDS will not be responsible for any loss of such information. This Limited Warranty is provided to you by Cybersecurity Defense Solutions LLC. 2211 Widman Way #150, Fort Myers, FL 33901.

How the law in certain jurisdictions relates to this Limited Warranty: This Limited Warranty gives you specific rights, and you may have other rights that vary from state to state, or jurisdiction to jurisdiction. This Limited Warranty does not change any such rights.

Warranty / Recon Sentinel / 6-17