Copyright and Publication Information

This manual is copyrighted and Icon Laboratories, Inc. reserves all rights. No part of this publication may be reproduced, transmitted, stored in a retrieval system, modified, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise without written permission by Icon Laboratories, Inc.

Copyright © 2016 Icon Laboratories, Inc.
All Rights Reserved
Revision: B
Publication Date: May 2016

Trademarks

Floodgate Defender is a trademark of Icon Laboratories, Inc. All other product names and services identified throughout this manual are trademarks or registered trademarks of their respective companies. They are used throughout this manual in editorial fashion only. No such use, or the use of any trade name, is intended to convey endorsement or other affiliation with the manual.

Disclaimer

Icon Laboratories, Inc. makes a genuine attempt to ensure the accuracy and quality of the content described herein; however, Icon Labs makes no warranty, express or implied, with respect to the quality, reliability, accuracy, or freedom from error of this document or the products it describes. Icon Labs makes no representation or warranty with respect to the contents hereof and specifically disclaims any implied warranties of fitness for any particular purpose. Icon Labs disclaims all liability for any direct, indirect, incidental or consequential, special or exemplary damages resulting from the use of the information in this document or from the use of any products described in this document. Mention of any product or organization does not constitute an endorsement by Icon Labs of that product or corporation. Data used in examples and labs is intended to be fictional even if actual data is used or accessed. Any resemblance to, or use of, real persons or organizations should be treated as entirely coincidental.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTENTS</td>
<td>2</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>3</td>
</tr>
<tr>
<td>PRODUCT COMPONENTS AND HARDWARE SPECIFICATION</td>
<td>3</td>
</tr>
<tr>
<td>FEATURES</td>
<td>4</td>
</tr>
<tr>
<td>FLOODGATE DEFENDER USAGE</td>
<td>4</td>
</tr>
<tr>
<td>POWER CONNECTION</td>
<td>5</td>
</tr>
<tr>
<td>DIN RAIL ATTACHMENT (OPTIONAL)</td>
<td>5</td>
</tr>
<tr>
<td>INITIAL CONFIGURATION</td>
<td>5</td>
</tr>
<tr>
<td>ATTACHING TO THE NETWORK</td>
<td>5</td>
</tr>
<tr>
<td>FLOODGATE DEFENDER FILTERING OVERVIEW</td>
<td>6</td>
</tr>
<tr>
<td>MANAGEMENT WITH THE FLOODGATE SECURITY MANAGER</td>
<td>6</td>
</tr>
<tr>
<td>MANAGEMENT WITH THE LOCAL WEB INTERFACE</td>
<td>7</td>
</tr>
<tr>
<td>Login Screen</td>
<td>8</td>
</tr>
<tr>
<td>Network Configuration</td>
<td>9</td>
</tr>
<tr>
<td>Time Configuration</td>
<td>10</td>
</tr>
<tr>
<td>Filter Configuration</td>
<td>11</td>
</tr>
<tr>
<td>Show Filtering Rules</td>
<td>12</td>
</tr>
<tr>
<td>Add Filtering Rule</td>
<td>13</td>
</tr>
<tr>
<td>Delete User</td>
<td>15</td>
</tr>
<tr>
<td>Version</td>
<td>16</td>
</tr>
<tr>
<td>Event Log Viewer</td>
<td>17</td>
</tr>
<tr>
<td>Log Viewer After Start</td>
<td>18</td>
</tr>
<tr>
<td>Download Full Log</td>
<td>19</td>
</tr>
<tr>
<td>QUESTIONS AND ANSWERS</td>
<td>20</td>
</tr>
<tr>
<td>What is Floodgate Defender?</td>
<td>20</td>
</tr>
<tr>
<td>Why should I purchase Floodgate Defender?</td>
<td>20</td>
</tr>
<tr>
<td>Trouble Shooting</td>
<td>20</td>
</tr>
<tr>
<td>What is Icon Labs’ support policy?</td>
<td>20</td>
</tr>
<tr>
<td>Product Warranty</td>
<td>20</td>
</tr>
<tr>
<td>How do I purchase Floodgate Defender?</td>
<td>20</td>
</tr>
<tr>
<td>WARRANTY INFORMATION</td>
<td>21</td>
</tr>
</tbody>
</table>
Introduction

This manual describes Floodgate Defender Mark III™, a compact firewall appliance providing drop-in protection for networked devices or computers. It is designed, implemented, and supported by Icon Laboratories, Inc. of West Des Moines, Iowa.

Product components and hardware specification

Floodgate Defender is shipped with the firewall appliance, power supply and an Ethernet cable. Hardware specifications are:

- Size: 4" x 3.75" x 1.25"
- Weight: 13 oz.
- Operating temperature: 0–70 C
- Power input: 24 VDC
- Power usage: 8W full load, 1W standby, 6W low load
- 2 x 10/100 Ethernet RJ-45 ports
Features

Floodgate Defender is a compact firewall appliance providing drop-in protection for networked embedded devices. Installation and configuration can be done in minutes, providing instant protection against cyber-attacks from hackers, denial of service attacks, cyber-sabotage attacks, automated hacking bots, and any other Internet-based threats. Floodgate Defender provides:

- Flexible packet filtering rules allowing filtering by:
  - LAN IP address
  - WAN IP address
  - IP protocol
  - UDP port
  - TCP port
- Stateful packet inspection.
- Web interface for configuration.
- Protection from common attacks such as SYN flood (denial of service) attacks.
- Bi-directional filtering, providing complete control of incoming and outgoing packets for the target device.
- Event logging. Maintains a log of all packets that violate the configured communication policies.
- Works with any TCP/IP network configuration.

Floodgate Defender usage

Floodgate Defender can be used to protect any target device attached to the Internet or any other TCP/IP network. Floodgate Defender is installed between the target device and the Internet or corporate network and operates transparently; no modifications are required to either the network or to the target device. Floodgate will work with any network configuration.

Floodgate Defender was designed to provide protection for embedded or industrial devices that lack security and cannot be easily upgraded. These devices include industrial control equipment, printers, SCADA networks and similar devices. However, Floodgate Defender can also be used as an additional layer of security to any device that connects to a TCP/IP based network.

NOTE: In this document we will use the term target device to refer to the device protected by Floodgate Defender. The target device may be an embedded device such as an industrial, communications, SCADA, military or medical device. Less likely, but it may also be a PC or laptop computer.
Power connection

Make certain you know where the 24V line and GND line is before powering up the Defender. 24VDC and Ground terminals are marked on the case. Power the board with 24V and connect the ground return on the middle terminal.

Earth ground is also marked on the case, but is only needed for three-wire terminal supplies that have earth ground.

For lab use, we recommend CUI’s power supply EPSA240100U available from the digikey.com web site. Digi-Key’s part number is T1074-P5RP-ND and is found on this page: http://www.digikey.com/product-detail/en/EPSA240100U-P5RP-SZ/T1074-P5RP-ND/2235266?WT.srch=1&gclid=CPrErN7D5ssCFQiQoQdZbYMaw

You’ll also need this gator clip adapter, part number 839-1219-ND, also from Digi-Key: http://www.digikey.com/product-detail/en/tensility-international-corp/10-01597/839-1219-ND/4502384

DIN rail attachment (optional)

The Defender can be attached to a DIN rail with this adapter from the Digi-Key website: http://www.digikey.com/product-detail/en/TSH%2035-2/902-1087-ND/2164012

The Digi-Key part number is 902-1087-ND.

You will need two (2) 11mm machine screws to attach the Defender to the adapter. Do not overtighten the screws.

Initial configuration

Before installing the Defender on your network you must configure the Defender’s networking properties using its local web interface. All Floodgate Defenders are assigned a static IP address of https://192.168.0.201 when shipped. The Floodgate Defender provides a web interface allowing filtering management, and system configuration. For maximum security, the initial configuration should be performed with a PC attached to the Defender with either a crossover cable or with the PC and Defender attached to a network hub with no other devices attached to that same hub. If you attach the Defender to the network where you intend to ultimately use it, instead of using a crossover or hub, for initial configuration, you may have difficulty connecting to the Defender’s web-based setup. Make the initial connection to https://192.168.0.201. It is likely you will need to assign a static IP address to your PC. Go here if you need a tutorial to set a static IP: http://www.howtogeek.com/howto/19249/how-to-assign-a-static-ip-address-in-xp-vista-or-windows-7/

Configuration of the Defender is described in this document in the section titled “Management with the local web interface”.
Attaching to the network

Without Floodgate Defender, your system looks like this:

![Diagram](Image1)

**Figure 2 – Without Floodgate Defender**

To install Floodgate Defender, unplug the target device’s CAT5 lead from the Internet or corporate network and plug that CAT5 cable into Floodgate Defender port Eth0. Plug another CAT5 cable into the target device and into Floodgate Defender port Eth1. Once installed, the system will look like this:

![Diagram](Image2)

**Figure 3 – With Floodgate Defender installed**

Once the Floodgate Defender is connected to the network and booted, it will be operational on your network, but not yet protecting the target device. The following section will step you through initial configuration.

**Floodgate Defender Filtering Overview**

Before starting configuration, it is important to understand how Floodgate Defender implements filtering.
Stateful Packet Inspection
A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

Floodgate Defender provides stateful packet inspection to project against SYN flood attacks and to support applications and protocols using dynamic port allocation. For example, if Floodgate Defender is protecting a device with a web browser, the web browser may open several TCP/IP sessions at one time to a given web server. Each of these connections will use a different port. Stateful packet inspection allows use of these dynamically allocated ports, even if these ports would be blocked otherwise. No configuration is required for stateful packet inspection.

Enable Ping
By default, the Floodgate Defender ignores ping messages sent to the Floodgate Defender itself. Depending on the user configured selection, Floodgate Defender will either block pings directed at the target device, or allow them.

Static Filtering
Floodgate Defender provides static filtering based on user defined rules. Filtering rules allow specification of rule direction (inbound or outbound), LAN IP address, WAN IP address, IP protocol, TCP port number and UDP port number and Rule Action (Allow, Block or Log).

Bidirectional filtering
The Floodgate Defender performs bidirectional filtering. This means the Floodgate Defender will filter both inbound packets (sent from the WAN to the LAN) and outbound packets (sent from the LAN to the WAN) allowing control over both traffic sent to the protected device(s) and traffic sent by the protected device(s).

There are two common scenarios when bidirectional filtering is important. One is to quarantine a target device suspected of being infected with malware or that otherwise needs to be isolated. Floodgate Defender can block all communication until further remediation is possible.

The second scenario controls communication from the target device. For example, the target device may only need to communicate with a known set of other machines. Floodgate Defender can enforce this limitation.

Management with the Floodgate Security Manager
The Floodgate Defender is initially managed using the local web interface. The local web interface must be used for the initial configuration of the device’s networking properties.

Once the initial networking properties have been configured, ongoing management of the Floodgate Defender can be done using the local web interface or using the Floodgate Security Manager, a separate advanced management system available from Icon Labs. Once configured, the Floodgate Defender should be auto-discovered by the Floodgate Manager. If this does not happen, you can add the Floodgate Defender to the Agent List on the “Settings->Agent Settings” page of the Floodgate Security Manager manual.
See the Floodgate Security Manager Manual for more information.

Management with the local web interface

When you first browse to the web interface you will be presented with the login screen. Instructions for logging into the web interface and managing the device are provided in the following sections of this document.

Login Screen

![Login Screen](image)

The first time a computer connects to the Floodgate Defender, the Defender’s Web Administrator login screen is presented. You will enter a new password (minimum 10 characters) which must contain an uppercase letter, lowercase letter, number, and one special character. You’ll be asked to confirm the password. Once you’re logged in, you’ll see the Device Configuration page.

You may get a certificate error in your web browser the first time you connect to the Defender. Each browser has a short procedure to override the error, which you’ll need to do. Your browser may offer to remember user name and password. We recommend you not allow the browser to save this information.

Subsequent pages include a New User link allowing you to create additional user accounts if needed. Note, you will need to provide the administrative password to create a new user account. Only the admin account can set time, network configuration, and filtering rules. Other users are limited to viewing documentation and viewing filtering rules.
Network Configuration

The Network Configuration page is used to control the networking characteristics of Floodgate Defender. If DHCP is enabled, the Static IP configuration fields can be left blank. If DHCP is not enabled, the user must configure the Device IP Address, and Subnet. Gateway and Name Server field(s) are optional when using static IP addresses.

Changing the host name field is required.

Make note of the host name and IP address so you can reconnect in the future if you need to change any of the Defender’s settings.

Changes in the settings on this page must be committed using the Submit button. The system will reboot and will typically be available within 20 seconds. If you changed the Defender’s IP address, you will need to reflect that change when you re-access the web management pages.
Time Configuration

Figure 6 – Time Configuration Screen

The Time Configuration page is used to set the Defender’s clock. The time should be set to approximately the same time as the target device. Note: NTP and UTC are not supported in this release. In future releases, NTP and UTC will be supported.

Changes in the settings on this page must be committed using the Submit button.
Filter Configuration

Floodgate Defender Firewall Appliance
Ping and Inbound/Outbound Traffic Configuration

The **Ping and Inbound/Outbound Traffic Configuration** page is used to control the basic filtering behavior of the Floodgate Defender. This page allows the user to set the default Inbound and outbound traffic rules. The drop-down list presents the options **Allow**, **Block** or **Log**. The default rules define the handling for any packets that do not match any configured filtering rules. (i.e., if the default Inbound rule is BLOCK, then any inbound traffic not explicitly allowed by another configuration rule is dropped).

**Allow** – Packet is processed and no log entry is created.
**Block** – Will not process the packet. A log entry is created.
**Log** - Packet is processed and a log entry is created.

For the ping to work for a specific IP address, add outbound rule (on the **Filtering Rules** page) for that IP address to allow protocol 1. Which looks like this:

<table>
<thead>
<tr>
<th>Direction</th>
<th>Lan IP</th>
<th>WAN IP</th>
<th>Action</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound</td>
<td>192.168.0.17</td>
<td></td>
<td>Allow</td>
<td>1</td>
</tr>
</tbody>
</table>

With the above rule only the IP address (192.168.0.17) will be able to ping the target device whereas other devices will not be able to ping. This applies even if the ping is enabled in the **Ping Configuration** page. If every device needs to ping the target, add the above rule by leaving the IP address field as blank.

Changes in the settings on this page must be committed using the **Submit** button.
The Show Filtering Rules page shows the filtering rules that have been configured. For each rule, the following fields are displayed:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direction</td>
<td>Inbound/Outbound. Specifies if the rule applies to inbound traffic (from the WAN) or outbound traffic (to the WAN).</td>
</tr>
<tr>
<td>WAN IP</td>
<td>IP address of the machine on the WAN</td>
</tr>
<tr>
<td>LAN IP</td>
<td>IP address of the machine on the LAN</td>
</tr>
<tr>
<td>Action</td>
<td>Specifies the handling of packets that match this rule. Values are Allow (allow the packet but do not log), Block (block the packet and log to iptables.log) or Log (allow the packet but log to iptables.log)</td>
</tr>
<tr>
<td>Protocol</td>
<td>IP protocol number</td>
</tr>
<tr>
<td>TCP Port</td>
<td>TCP Port number</td>
</tr>
<tr>
<td>UDP Port</td>
<td>UDP Port number</td>
</tr>
</tbody>
</table>

The Add Rule button appearing at the top of the table can be used to navigate to another page on which a new rule can be added. The Delete button in the last column can be used to delete a row from the table.
Add Filtering Rule

Figure 9 – Ethernet Frame Filtering

The Add Filtering Rule page allows a new rule to be created. Fields left blank will have a value of ALL.

As with all configuration pages, the changes must be committed by using the Submit button.

The IP Protocol, TCP Port and UDP Port values are specified as a numeric value. Common IP Protocol numbers are:

<table>
<thead>
<tr>
<th>Value</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ICMP</td>
</tr>
<tr>
<td>2</td>
<td>IGMP</td>
</tr>
<tr>
<td>6</td>
<td>TCP</td>
</tr>
<tr>
<td>17</td>
<td>UDP</td>
</tr>
</tbody>
</table>

More information on IP protocol numbers can be found at: http://en.wikipedia.org/wiki/List_of_IP_protocol_numbers
Common TCP Port numbers are:

<table>
<thead>
<tr>
<th>Value</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>20, 21</td>
<td>FTP</td>
</tr>
<tr>
<td>22</td>
<td>SSH</td>
</tr>
<tr>
<td>23</td>
<td>telnet</td>
</tr>
<tr>
<td>25</td>
<td>SMTP</td>
</tr>
<tr>
<td>80</td>
<td>HTTP</td>
</tr>
</tbody>
</table>

More information on TCP Port numbers can be found at:

Common UDP Port numbers are:

<table>
<thead>
<tr>
<th>Value</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>67, 68</td>
<td>BOOTP</td>
</tr>
<tr>
<td>69</td>
<td>TFTP</td>
</tr>
<tr>
<td>161, 162</td>
<td>SNMP</td>
</tr>
</tbody>
</table>

More information on UDP Port numbers can be found at:

For the ping to work for a specific IP address, add outbound rule (on the Filtering Rules page) for that IP address to allow protocol 1. Which looks like this:

<table>
<thead>
<tr>
<th>Direction</th>
<th>Lan IP</th>
<th>WAN IP</th>
<th>Action</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound</td>
<td>192.168.0.17</td>
<td></td>
<td>Allow</td>
<td>1</td>
</tr>
</tbody>
</table>

With the above rule only the IP address (192.168.0.17) will be able to ping the target device whereas other devices will not be able to ping. This applies even if the ping is enabled in the Ping Configuration page. If every device needs to ping the target, add the above rule by leaving the IP address field as blank.
Delete User

Figure 9 – Ethernet Frame Filtering

Enter the user name you wish to delete in the *Delete user* field or select from the dropdown. Removing a user is an administrative function, so you will need to enter the administrator’s password in the *Administrative Password* field.

The administrator’s password cannot be deleted.
The Version page displays the current Floodgate version and technical support contact information.
The Event Log Viewer page allows examination of a log file. The “Start Log” and “Stop Log” allow viewing of current log file entries as they are created. At the bottom of the page, you can select type by IP Tables, Debug Log, Events Log, and Packets Log in the Select log type link.

The Download Full Log link downloads the entire log as ASCII text for viewing offline (described below).
Log Viewer After Start

The Event Log Viewer page, once viewing has started, displays current log file entries. There is a link at the bottom of the page that initiates a download of the log. A sample log appears on the following page.
The **Download Full Log** option allows the full log file to be downloaded as ASCII text for archive or offline viewing.
Questions and Answers

What is Floodgate Defender?

Floodgate Defender is a compact firewall appliance that provides drop-in protection for networked industrial devices.

Why should I purchase Floodgate Defender?

Floodgate Defender can be used to add protection to legacy networked devices without modifying the legacy system.

Trouble Shooting

The IPTables log can be viewed via the administrative interface as described in the Log Viewer section above. If the target device is unable to communicate, set all filtering configuration drop down options to NONE. This should open the firewall to all traffic that is not pre-configured by the factory.

It may take up to 30 seconds after initial boot up for Floodgate Defender to begin passing traffic to the target device.

If the target device does not have an IP address, it may be necessary to perform a DHCP renewal on the target device or manually set a static IP address.

What is Icon Labs' support policy?

Icon Labs provides 90 days of technical support from the date of purchase. If you need support after this period, you can purchase a technical support contract by contacting info@iconlabs.com. Bug fixes and enhancement releases are provided at no charge if you have a valid support contract.

Product Warranty

Icon Labs provides a 1 year limited warranty on Floodgate Defender. See the appendix below for warranty information. Direct all questions regarding product warranties to info@iconlabs.com.

How do I purchase Floodgate Defender?

To purchase Floodgate Defender, contact

   Icon Labs
   Sales Department
   3636 Westown Parkway, Suite 203
   West Des Moines, IA 50266
   Phone: 1-515-226-3443
   Toll Free: 1-888-235-3443

   info@iconlabs.com
   www.iconlabs.com

www.iconlabs.com
Warranty Information

Appendix A
Limited Warranty Statement

Icon Labs' warranty obligations are limited to the terms set forth below.

Please note that Icon Labs reserves the right to update from time to time the warranty terms provided for new purchases of Icon Labs products, and to establish the effective date of those updated warranty terms. Please refer to www.iconlabs.com for the then current form of Limited Warranty Statement for Icon Labs brand products.

Please note that Icon Labs products are distributed through local authorized distributors and resellers ("Resellers"). These Resellers generally offer a consumer warranty, and associated warranty services, to consumer purchasers. Icon Labs recommends that consumers first contact the Reseller from whom they purchased the Icon Labs product for all issues with regard to product defects and the applicable product warranty.

Icon Labs warrants to the original consumer purchaser ("you") that new Icon Labs Floodgate Defender products ("New Products") will be free from defects in material and workmanship for the Standard Warranty Period for the relevant New Product. The Standard Warranty Period for the various New Products marketed by Icon Labs is twelve (12) months from date of purchase.

The warranty period on replacements for New Products is the remainder of the warranty on the original New Product or 90 days from the date of shipment of the replacement product, whichever is longer.

The start of the Warranty Period is the documented date of your purchase of the Product from Icon Labs or Icon Labs' authorized reseller. In the absence of a documented purchase date, the start of the Warranty Period will be deemed the date of original shipment by Icon Labs to Icon Labs' customer.

The Products are manufactured from parts and components that are new or equivalent to new in accordance with industry standards.

If you discover a defect in material or workmanship during the Warranty Period, and Icon Labs agrees that the defect exists, Icon Labs will, at its option, repair or replace the Product at no charge to you, provided it is returned during the applicable Warranty Period, with transportation charges prepaid, to the facility designated by Icon Labs. The Product must be properly packaged in Icon Labs or Icon Labs-approved packaging, with the Return Material Authorization clearly displayed on the outside of the packaging, to obtain warranty service. Products that fail within the first 30 days after purchase will be replaced with a new Product. Icon Labs may require proper proof of purchase documentation prior to issuing the replacement Product.

If Icon Labs elects to repair a Product, Icon Labs owns all parts removed from the repaired Product. Icon Labs uses new and used parts made by various manufacturers in conjunction with warranty repairs and replacement Products. Repair parts or replacement Products may, at Icon Labs' option, include an equal or better model or features. Icon Labs has no responsibility whatsoever with regard to any content or data on returned Products.
To request warranty service and before returning a Product to Icon Labs, please contact Icon Labs at info@iconlabs.com or 866-235-3443. Once the Icon Labs determines that a repair is required, Icon Labs will issue an RMA number. A copy of your receipt or bill of sale bearing the name and location of Icon Labs’ authorized reseller and the Icon Labs serial number and model number of the Product in which the defect has been reported may be required as a proof of your purchase for warranty service.

You are responsible for saving or backing up data contained in any Product returned to Icon Labs in conjunction with warranty or any other services. Icon Labs shall have no responsibility for such data whatsoever and shall have no liability arising out of any damage to, or loss or disclosure of, such data.

This limited warranty applies only to the Icon Labs products that can be identified by the original, unaltered Icon Labs trademark, trade name or logo affixed to them. Icon Labs does not warrant any product that is not manufactured by, for, or with permission from Icon Labs, or which is not otherwise distributed by Icon Labs under the Icon Labs brand.

This warranty does not cover any of the following conditions:

- Abuse, unreasonable use, mistreatment, or neglect
- Unusual physical or electrical stress or power fluctuations
- Damage caused during installation of the Product
- Damage or capacity/performance/operational resetting caused by the equipment or system with which the Product is used
- Damage caused by modification or repair not made or authorized by Icon Labs
- Products whose Icon Labs Serial Number and/or Material Number label have been removed, torn or defaced
- Damage caused by use of non-Icon Labs packaging
- Damage caused by improper or improperly used packaging
- Damage caused by lack of ESD protection
- Products that are determined to be stolen.

Further, this limited warranty is void if the Product cover, or any label or seal on the Product, is removed or damaged.

Icon Labs owns all parts removed from the repaired Products. Icon Labs uses new and reconditioned parts in performing warranty repairs and building replacement products.

FAILURE TO COMPLETE AND RETURN ANY ICON LABS PRODUCT REGISTRATION FORM WILL NOT DIMINISH YOUR WARRANTY RIGHTS.

Certain Products include software or firmware as a component (“Software”). Icon Labs or its suppliers retain all rights of ownership in such Software and any use of the Software is subject to the license agreement provided by Icon Labs accompanying such Software. If no license is provided by Icon Labs, you are granted the limited right to use the Software as required for the operation of the Product and no other rights are granted whatsoever. EXCEPT AS OTHERWISE PROVIDED BY Icon Labs IN A WRITTEN LICENSE AGREEMENT, SOFTWARE IS OFFERED “AS IS” AND ICON LABS GRANTS NO WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, BY STATUTE, COMMUNICATIONS OR OTHERWISE WITH REGARD TO THE
SOFTWARE. ICON LABS SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT WITH RESPECT TO THE SOFTWARE.

TO THE MAXIMUM EXTENT PERMITTED BY LAW, THIS WARRANTY AND THE REMEDIES SET FORTH ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHERS, WHETHER ORAL OR WRITTEN, EXPRESSED, IMPLIED OR STATUTORY. OTHER THAN AS EXPRESSLY SET FORTH HEREIN, ICON LABS SPECIFICALLY DISCLAIMS TO THE MAXIMUM EXTENT PERMITTED BY LAW ANY AND ALL IMPLIED REPRESENTATIONS, WARRANTIES AND CONDITIONS AS TO THE PRODUCTS, SERVICES, OR ANY OTHER MATTER WHATSOEVER. IN PARTICULAR, BUT WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, ICON LABS SPECIFICALLY DISCLAIMS ANY AND ALL IMPLIED OR DEEMED WARRANTIES AND CONDITIONS OF SATISFACTORY QUALITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, PERFORMANCE IN A SKILLFUL AND WORKMANLIKE MANNER, AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS OR ANY OTHER WARRANTY ARISING FROM A COURSE OF DEALING OR USAGE OF TRADE. THIS LIMITED WARRANTY DOES NOT APPLY TO, AND ICON LABS MAKES NO WARRANTY TO YOU WITH REGARD TO, PRODUCTS ORIGINALLY SOLD AS AN INTEGRATED COMPONENT OF A SYSTEM NOT SUPPLIED BY ICON LABS, OR PRODUCTS PROVIDED UNDER A THIRD PARTY LEASING OR SERVICE ARRANGEMENT. No Icon Labs distributor, reseller, dealer, agent or employee is authorized to make any modification, extension or addition to this warranty.

ICON LABS IS NOT RESPONSIBLE OR LIABLE FOR ANY INDIRECT, UNFORESEEABLE, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES HOWEVER CAUSED AND WHETHER OR NOT ICON LABS WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, INCLUDING BUT NOT LIMITED TO, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS, LOSS OF DATA OR PROGRAMS, LOST PROFITS, DOWNTIME, GOODWILL, DAMAGE OR REPLACEMENT OF EQUIPMENT AND PROPERTY, AND ANY COSTS OF RECOVERING, PROGRAMMING OR REPRODUCING ANY PROGRAM OR DATA STORED IN OR USED WITH ICON LABS PRODUCTS OR ANY OTHER DAMAGES ARISING OUT OF THE PURCHASE, USE OR PERFORMANCE OF THE PRODUCT. Icon Labs is not, and cannot be, responsible for any losses or damages arising out of any loss of, or any inability to access, data as a result from the failure of a Product, and accordingly you bear this risk. The allocation of risk under this limitation of liability is reflected in the purchase price of the Product. This limitation of liability, however, will not apply to claims for death or personal injury caused by the negligence of Icon Labs or its associated companies, officers, representatives or agents.

Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages or exclusions of implied or deemed conditions or warranties, so the above limitations or exclusions may not apply to you. This warranty gives you specific legal rights, and you may also have other rights that vary from jurisdiction to jurisdiction.

Please note that you are expressly not permitted to use the Products in conjunction with the operation of nuclear facilities, aircraft navigation, aircraft communication, aircraft flight control, aircraft air traffic control systems, weapons devices or systems, or in any devices or systems in which a malfunction (including, without limitation, software related delay or failure) would result in foreseeable risk of injury or death to the operator of the device or system, or to others.

This Statement of Limited Warranty shall be exclusively interpreted in accordance with the English language with the meaning of its terms. Should any provisions of this Limited Warranty be declared invalid by any court of competent jurisdiction, the balance of this Limited Warranty will remain in full force and affect. In addition should a translation of this Limited Warranty deviate from the English language version, only the English language version shall apply and be binding.