# IntelliShun 10G™

/ ADVANCED SHUNNING

## Getting Started Guide

# Getting started guide

Model: **IntelliShun10G**

### About this guide

Thank you for protecting your network with IntelliShun10G.

Please read this guide and follow the steps to set up and register your IntelliShun10G device.

If you need further assistance beyond what this guide provides, email us at **support@riskanalytics.com** or call us at **1.855.639.4427**

# Contents

## About your IntelliShun10G device

The IntelliShun10G device is a network security appliance that uses a stateless bridge to block or allow traffic bidirectionally by IP address. The device is bridged between your edge router and your firewall. The device has three interfaces: Bridge, LAN and Service.

Your IntelliShun10G device uses its LAN interface to report statistics and retrieve updates. The device "heartbeats" over the Internet to an API server at RiskAnalytics. The device is fed by ShadowNet™, a stream of global threat intel generated by RiskAnalytics. Once activated, your device will receive updates to ShadowNet every few minutes, while posting its shun statistics and device status to your Web interface.

ShadowNet is an intelligent and vetted list of known malicious threats, including but not limited to malware distribution, crimeware and botnets. The intel is continually updated and maintained by RiskAnalytics security experts. You can whitelist IP addresses that are critical to business operations.

IntelliShun10G prevents attacks by malicious entities and prohibits existing compromised workstations from communicating with command and control systems managed by malicious users. IntelliShun10G's underlying technology allows devices on your network to access the Internet while being protected from cybercriminals.

***Pre-configure your IntelliShun10G before connecting to your network.***

## Required setup information

Your IntelliShun10G device must be activated before it can be deployed. Before you begin, be sure to have the following information at hand.

## Activation credentials

On subscribing to IntelliShun10G, your company received emails with a License Key, your device’s serial number, and the username and URL for your Web interface. If you are missing any of this information, please email us at support@riskanalytics.com.

License Key:______________________________________________________________

URL: ______________________________________________________________

Username: ______________________________________________________________

## Network configuration information

The device’s LAN interface must have access to the Internet at all times.
The interface is set to DHCP by default, but you can assign it a static IP address instead.

IP address: ______________________________________________________________

Netmask: ______________________________________________________________

Default gateway: ______________________________________________________________

DNS servers: ______________________________________________________________

## Speed and duplex settings

The IntelliShun 10G supports either 1 Gigbit SFP+ or 10 Gigabit SFP+,
neither of these two configurations support customization of duplex settings.

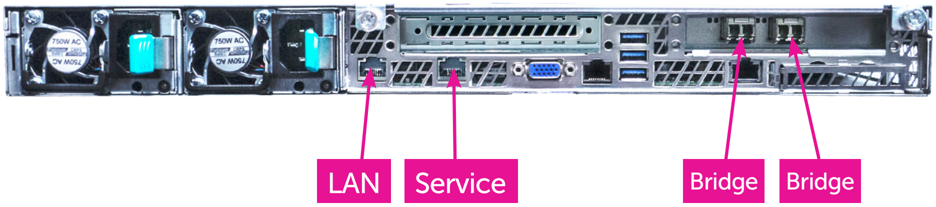
*Pre-configure your IntelliShun10G before connecting to your network.*

The following pages will guide you through the IntelliShun10G device configuration. Once you complete the initial configuration, you can go back and make changes to individual configuration elements. This permits pre-configuring the IntelliShun10G device for later deployment.

## Basic Setup and Registration

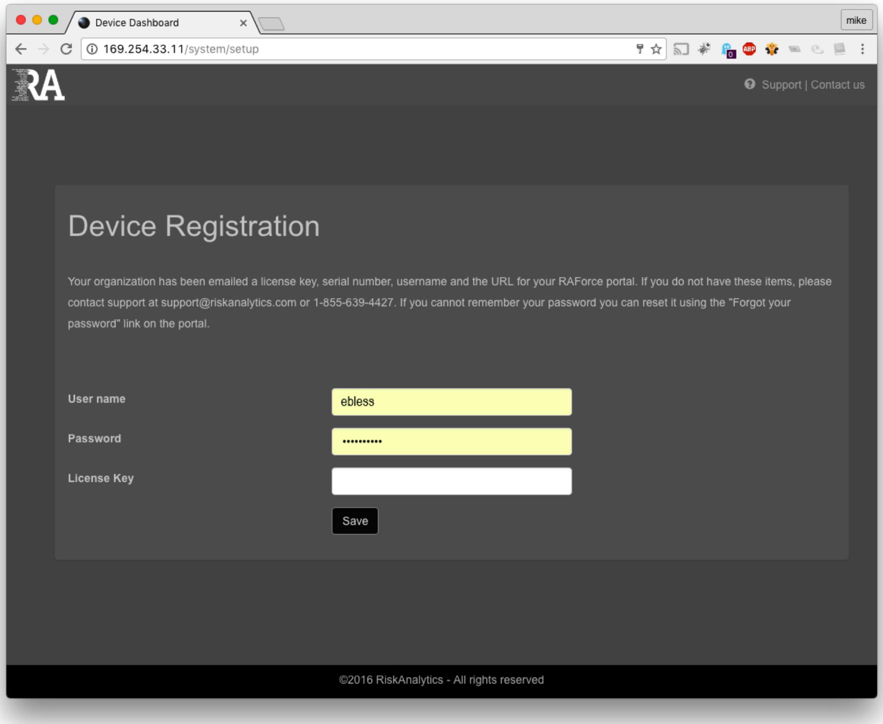
1 Connect power to the device. The device power automatically. Please wait approximately 5 minutes for service to load up.

2 Direct connect a workstation or laptop to the “Service” port



3 Either wait for your device to self-assign an IP address or configure your workstation’s network interface to use an IP address in the 169.254.0.0/16 range.

4 Connect the IntelliShun10G’s LAN port to your internal network. This cable will need to be continuously connected for the device to function properly. The IntelliShun10G will attempt to obtain a DHCP address, failing that you will need to configure a static IP address.



Device Registration

Your organization has been emailed a license key, serial number, username and the URL for your RAForce portal. If you do not have these items, please contact support at support@riskanalytics.com or 1-855-639-4427. If you cannot remember your password you can reset it using the "Forgot your password" link on the portal.

| | |
|---|---|
| User name | ebless |
| Password | ••••••••••• |
| License Key | |

©2016 RiskAnalytics - All rights reserved

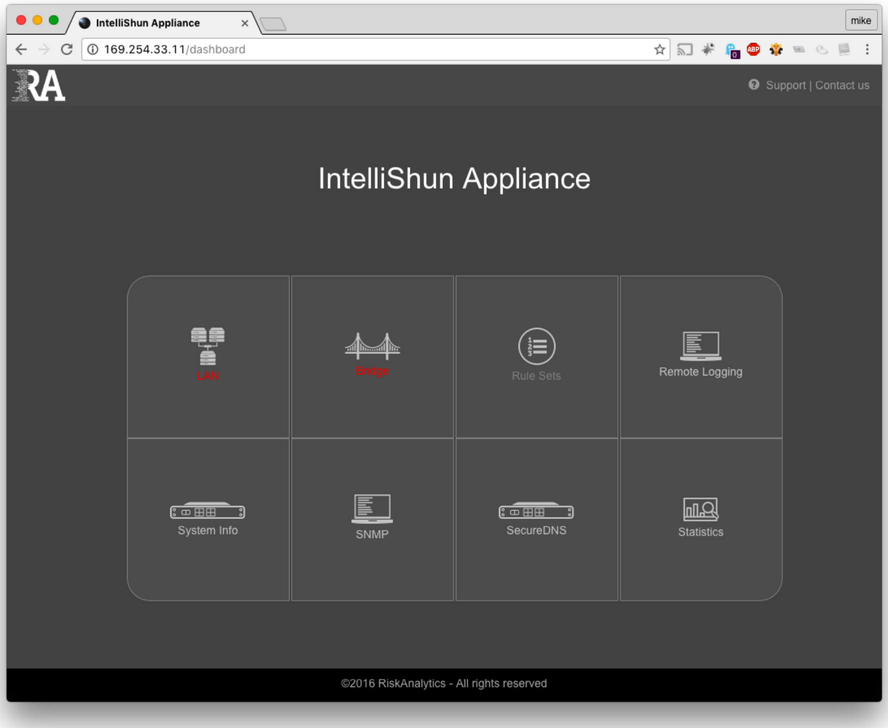
5 Open a web browser on the connected computer and connect to http://169.254.33.11

6 If the IntelliShun10G was able to get a valid DHCP address and connect to RiskAnalytics the device setup screen on your web browser should proceed to the registration page.

7 To configure a static IP Address, the LAN setup button is shown on the screen. Configure the LAN port to correspond with your network policies. If no cable was connected to the LAN, return to Step 4, and refresh the page.

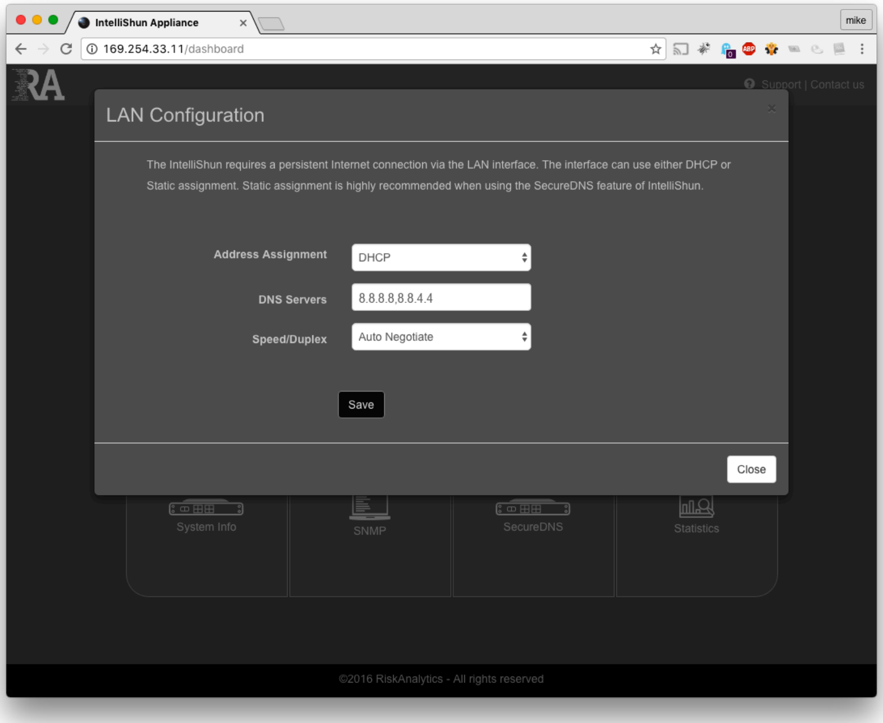
8 Input the activation credentials, license key emailed to you at the time of purchase. This will register and activate the device with RiskAnalytics.

9 The device is now configured for communication with RiskAnalytics. In your RAForce system, the device will now show as 'Green light' on RA Force "Service" page. The other configurable functions are available from the main screen on the device.



## DHCP LAN Setup:

1 Select either DHCP or Static .



LAN Configuration

The IntelliShun requires a persistent Internet connection via the LAN interface. The interface can use either DHCP or Static assignment. Static assignment is highly recommended when using the SecureDNS feature of IntelliShun.

Address Assignment: DHCP

DNS Servers: 8.8.8.8,8.8.4.4

Speed/Duplex: Auto Negotiate

2 If you chose DHCP, you may optionally specify a DNS server if you choose to not use the values provided by your DHCP server. Multiple DNS servers are separated with a single comma. For example "8.8.8.8,8.8.4.4"

3 If your network infrastructure does not support auto negotiation, you may specify the speed and duplex settings of the LAN port.

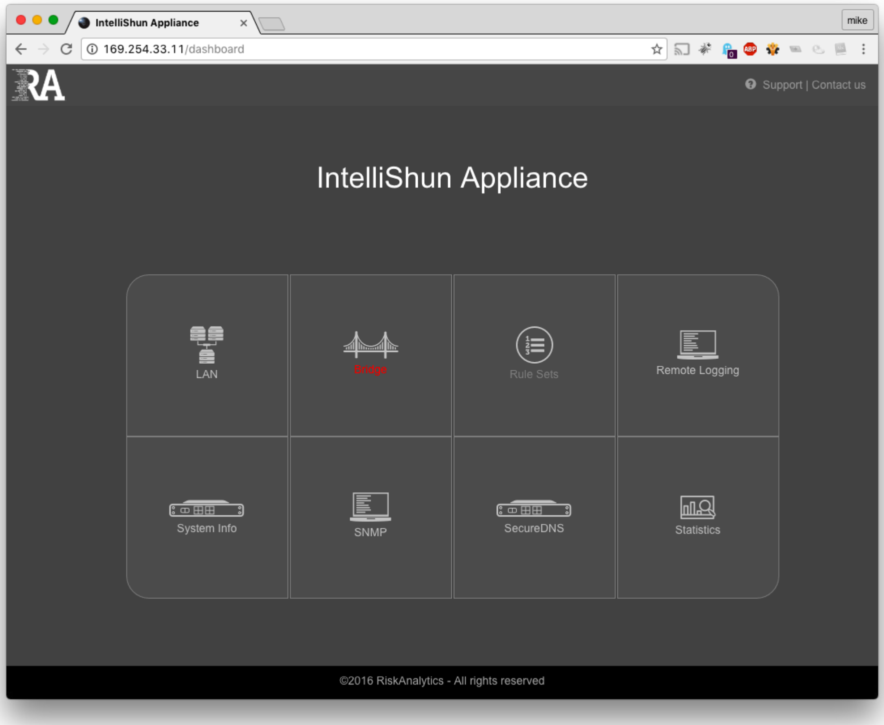
## Static LAN Setup:

1 Complete the fields on the form, all fields are required to save the configuration. Multiple dns servers are separated with a single comma. For example “8.8.8.8,8.8.4.4”

2 If your network infrastructure does not support auto negotiation, you may specify the speed and duplex settings of the LAN port.

## Bridge Setup:

1 The supported SFP & SFP+ modules in the IntelliShun10G operate at 1 Gigabit or 10 Gigabit only, there are no negotiation settings beyond “Auto”.



## RiskAnalytics API Addresses and ports required for IntelliShun

Certain customers are using web filtering proxies and/or restricted firewall egress rules on their networks. The IntelliShun appliance needs to be able to access our APIs in order to function properly.

**The following URLs need to be added to your webfilter whitelist:**

- iplist.device.riskanalytics.io
- heartbeat.device.riskanalytics.io
- ipscore.device.riskanalytics.io
- remote.device.riskanalytics.io
- async.device.riskanalytics.io
- api.riskanalytics.com
- hosted.riskanalytics.com
- mirror.riskanalytics.com
- myraforce.com
- risktool.com

**The following ports should be whitelisted on your egress filter:**

- TCP 80 and 443
- UDP 53 and 1776

**The following IPs should be whitelisted on your egress filter:**

- 52.21.143.192
- 139.146.167.0/24

You can also go to RiskAnalytics Support for more information.

| | Problem | Solution |
|---|---|---|
| 1 | I can't reach http://169.254.33.11 after plugging the Ethernet cable into the IntelliShun10G device's Service port. | After plugging in the Ethernet cable from your workstation to the service port of the IntelliShun10G device, your workstation will assign itself an address in the 169.254.0.0/16 range. This may take up to 30 seconds and is done automatically if your workstation is configured for DHCP. If you have configured your workstation with a static IP address that is not in the 169.254.0.0/16 range, you must reconfigure your workstation with an IP address in that range or set it to obtain an address via DHCP. |
| 2 | My IntelliShun10G device is displaying green on my Web interface, but my users are still able to get to websites that should be blocked. | There may be more than one path to the Internet from your network, or the device may not be wired between the edge router and the firewall. Verify that the device's Bridge ports are correctly connected between your Internet router and switch/firewall. Double-check by physically tracing the cables if necessary, since most network cables look identical. |

| | Problem | Solution |
|---|---|---|
| 3 | The IntelliShun10G device is unable to detect packets passing over the bridge. | IntelliShun10G tries two tests to determine whether the Bridge is working correctly. First, it sends a special “magic packet” and watches for the magic packet to pass over the Bridge.<br>If IntelliShun10G sees its own magic packet, it then declares that the Bridge is ready for operation. If it is unable to see its magic packet, it tries to detect any packets passing over the Bridge at all.<br>Scenario 1:<br>No packets are passing over the Bridge at all. If no packets at all are detected over the Bridge, then either the Bridge is not inline with the perimeter circuit or the Bridge is inline on an inactive circuit. If your network has multiple Internet circuits in an active-passive setting, the Bridge might be on the inactive circuit. If this is how you intend the Bridge to be deployed or if you wish to rearrange the deployment later, click “ignore” to acknowledge that you don’t expect packets to be passing over the Bridge yet. Note that this will cause an “untested bridge configuration” alert message to display on the Web interface until you rearrange the Bridge deployment.<br>Scenario 2:<br>Packets are passing over the bridge, but the IntelliShun10G device didn’t detect the magic packet because the device cabling is bridging two internal segments. If the magic packet is not detected but other non-broadcast TCP traffic is detected, then the Bridge may not be connected at the perimeter. We call this the “fax machine” scenario, because the Bridge is cabled in such a way that it is bridging two internal LAN segments. If you think this might be the case, you should verify that the Bridge is cabled correctly and click “retry.” Clicking “accept” or “ignore” will end the test.<br>Scenario 3:<br>Packets are passing over the bridge, but the IntelliShun10G device didn’t detect the magic packet because of egress filters. Some network managers or firewall administrators use egress filters or proxy servers to block unauthorized Internet traffic from leaving the network. In this case, the magic packet may have been discarded by the firewall or the proxy server. The magic packet is a UDP packet with a destination address of api.riskanalytics.com and a destination port of 1776. If you have egress filters or a proxy server, you can check their logs to see if they are discarding the magic packet. If so, whitelist api.riskanalytics.com and retry. If you are certain that the cabling is correct and the magic packet is being dropped on purpose, you can click “accept” or “ignore” to end the test. |

RiskAnalytics™

THE ART OF SECURITY™

Visit us at RiskAnalytics.com or call us at 1.855.639.4427