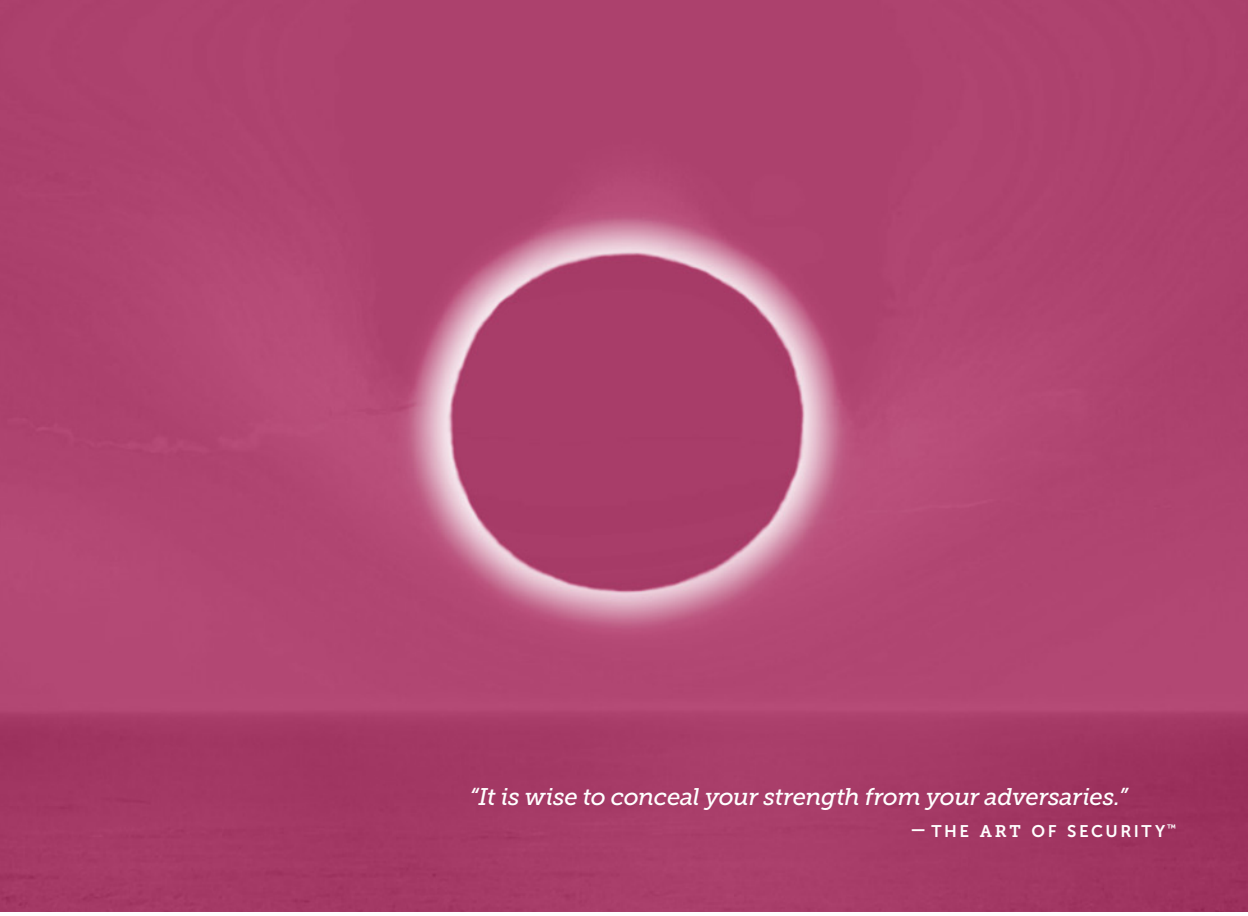


"It is wise to conceal your strength from your adversaries."
— THE ART OF SECURITY™

RA IntelliShun™

/ ADVANCED SHUNNING

Getting started guide v3.0

Model: **IntelliShun RAF21G** *(formerly known as SkyCoal)*

RiskAnalytics™
/ THE ART OF SECURITY™

RA IntelliShun™

ADVANCED SHUNNING

Getting started guide v3.0

Model: **IntelliShun RAF21G** *(formerly known as SkyCoal)*

About this guide

Thank you for protecting your network with IntelliShun.

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

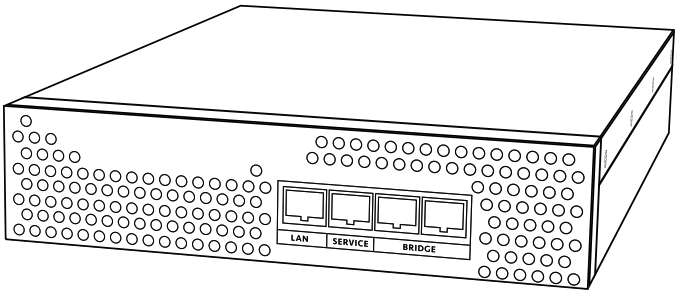
If you need further assistance beyond what this guide provides, email us at **support@riskanalytics.com**.

RiskAnalytics™

THE ART OF SECURITY™

Contents

The IntelliShun 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.



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.

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

Your IntelliShun 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 IntelliShun, 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

Your IntelliShun device uses its LAN interface to report statistics and retrieve updates. 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

Your IntelliShun device shipped with the Bridge ports' speed and duplex set to AutoNegotiate. Verify the existing speed and duplex settings of your edge router and next-in-line perimeter device (typically a firewall). If these devices are not set to AutoNegotiate, change your IntelliShun device's speed and duplex to match the settings of the existing devices. Mismatched speed and duplex settings will result in degraded network speed or malfunction.

Perimeter devices' link speed setting: _____

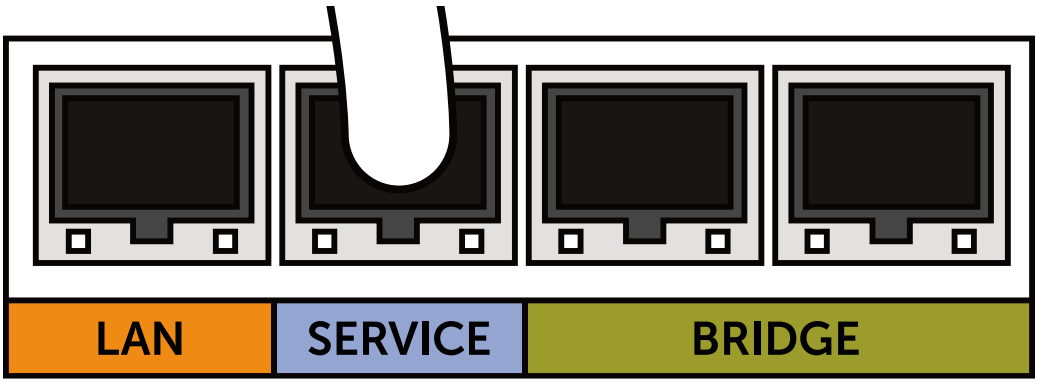
Perimeter devices' duplex setting: _____

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

1 Connect the IntelliShun device's power cord to the device and plug it in to the power outlet. Note that there is no power switch on the device; it is always on while plugged in.

2 Connect the device to your workstation:

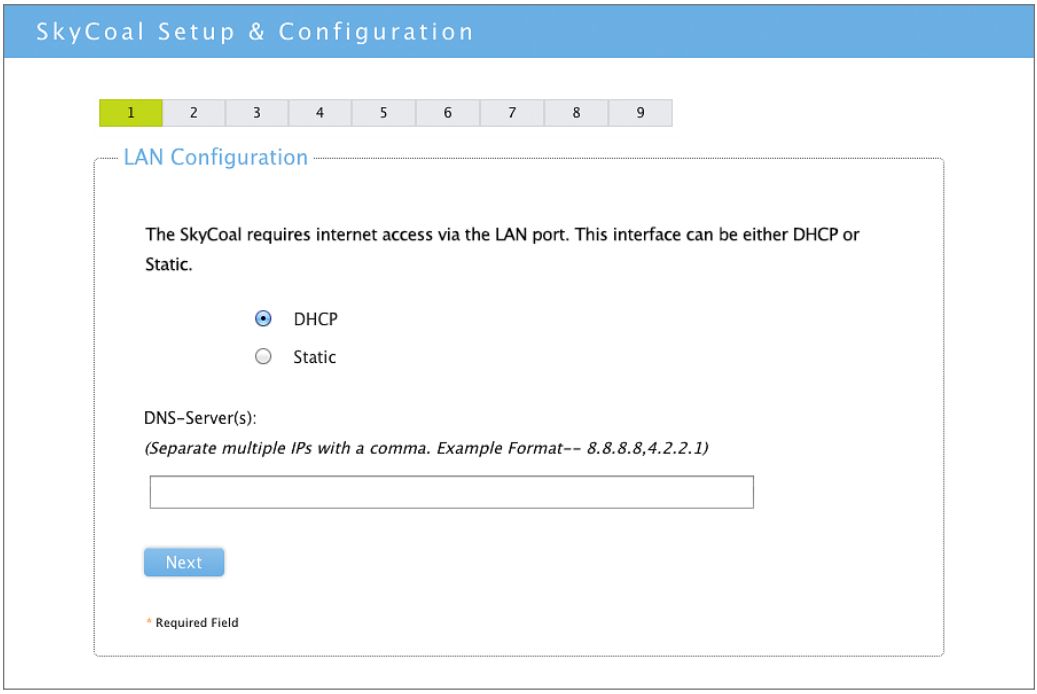
- Connect an Ethernet cable to the device's Service port, as shown here.



- Connect the other end of the Ethernet cable to your workstation's Ethernet port.

3 Wait a few seconds, and then open a Web browser on your workstation and navigate to: http://169.254.33.11

/ The Setup & Configuration wizard will launch, as shown here:



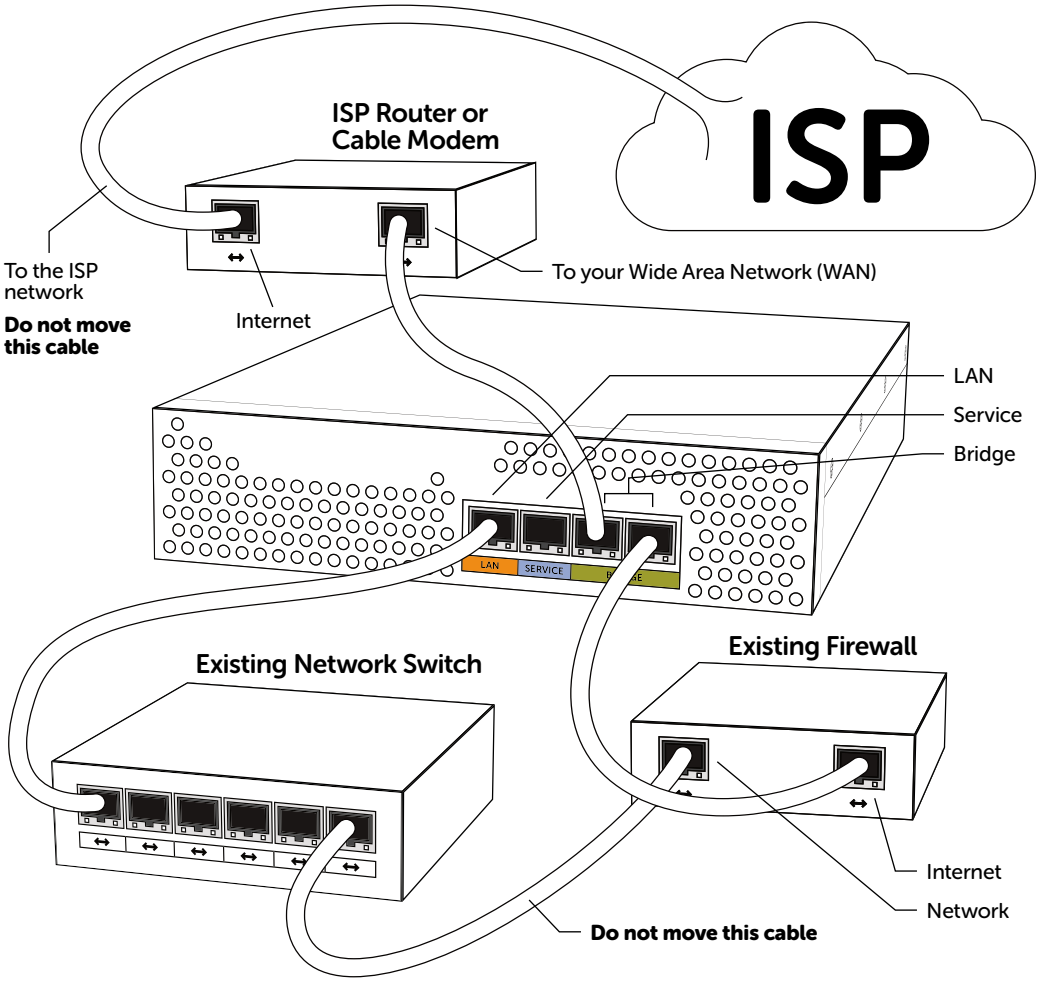
/ At this point, you can remove the stickers covering the other ports on the IntelliShun device.

/ Follow the onscreen instructions to activate your device.

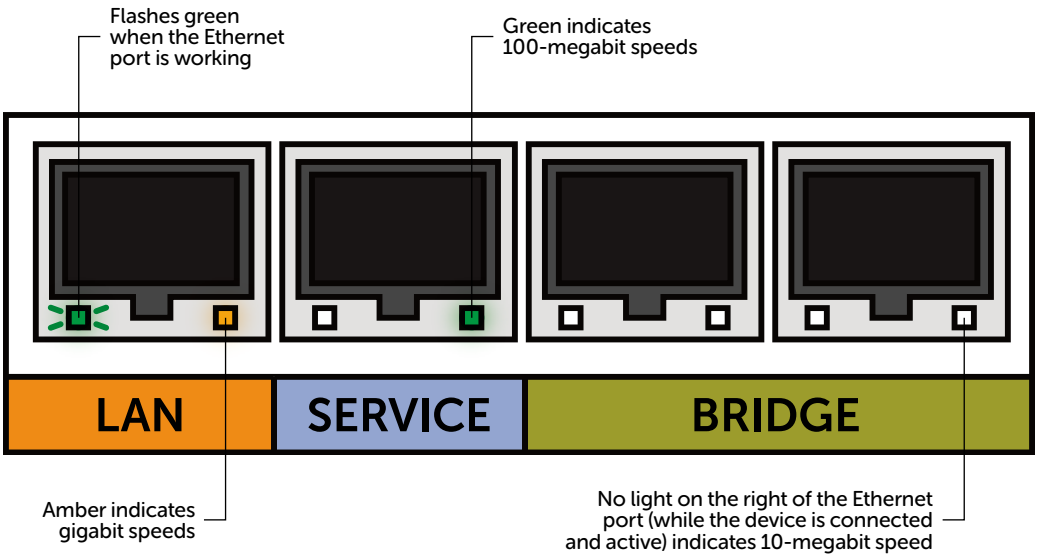
4 At the end of the setup process, the setup wizard will prompt you to unplug the device's power cord from the power port. After you unplug it, wait at least five seconds, and then plug it back in. This will require a brief temporary outage of your Internet circuit.

5 You can verify your device is receiving the ShadowNet intel feed by visiting: http://riskanalytics.com/skycoaltest/

After completing the Setup & Configuration wizard, unplugging your IntelliShun device from the power outlet, and plugging it back in, connect the device to your network as shown here.



NOTE: For most modern network equipment, the IntelliShun device will not need a crossover cable. However, it may require a crossover cable if you have host-to-host port hookup. Setting Speed/Duplex to anything other than AutoNegotiate disables the MDI-X, so you may need a crossover cable for this scenario as well. If you hook up the Bridge interface and there are no lights on the Bridge ports, try a crossover cable.



Special configurations

Deploying the IntelliShun device into a failover environment

There are many different ways to address redundancy for your Internet connection. Please discuss your specific architecture with RiskAnalytics support staff before installation. One of the more common questions we encounter is how many IntelliShun devices a network needs. This can vary depending on factors like multiple ISP circuits, multiple firewalls and multiple switches. If the circuit is available in one point after the edge router but you have multiple firewalls, you can place a single IntelliShun device in front of these firewalls.

Using your Internet circuit distribution switch to hook up the bridge

If you have an Internet circuit distribution switch and you already use VLANs for the router and firewall connections, you can create a new VLAN for the IntelliShun device's bridge interfaces. You need to know the VLAN number for your existing signal path of your edge router physical port and firewall physical port. Create a new VLAN and place one of the bridge interface ports in that VLAN. The other bridge interface port must be connected to the existing VLAN. To place the device in line, you must move the router port of the existing VLAN into the new VLAN you have created. To go out of line, reverse the operation.

	Problem	Solution
1	I can't reach http://169.254.33.11 after plugging the Ethernet cable into the IntelliShun device's Service port.	After plugging in the Ethernet cable from your workstation to the service port of the IntelliShun device, your workstation will assign itself an address in the 168.254.0.0/16 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 168.254.0.0/16 range, you must reconfigure your workstation with an IP address in that range or set it to obtain an address via DHCP.
2	My IntelliShun 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.
3	Our Internet traffic seems slower after installing the IntelliShun device.	This could indicate a speed/duplex problem. The device ships with the Bridge ports interface configured to auto-negotiate for speed and duplex. Log in to your edge router and firewall devices and verify the existing speed and duplex settings. The IntelliShun device's Bridge will need to be configured to match these settings. It is a good idea to run a speed test with the IntelliShun device not inline, and then again with it inline. If performance is degraded by greater than 5%, you may have a speed/duplex mismatch. The IntelliShun device is rated for a sustained speed of 960 megabits/second. Consult your Internet service provider if you are unsure of your network speed.
4	Our central printer stopped working after the IntelliShun device was activated.	Your DHCP server may have assigned the IntelliShun device an IP address that was already assigned statically to your central printer. By default, the IntelliShun device uses DHCP to obtain an IP address to communicate with RiskAnalytics. Most networks have a pool of IP addresses reserved for DHCP. Some devices that do not change very often (such as a printer) may be assigned a static or hard-coded IP address; if that address is within the range of pool addresses and the DHCP server assigns your IntelliShun device the same address, there will be a conflict. Contact a network administrator to repair the DHCP setting, or use the Web interface to assign the IntelliShun device a static IP address outside the DHCP range.
5	My reports show inbound traffic only. Or My external traffic is VLAN tagged.	You may have external VLAN tagging on or 802.1Q traffic outside your firewall. The IntelliShun device supports VLAN tagged traffic; however, reports in your Web interface will not display bidirectional traffic. You will see zero reported hits for one direction on the reports.

Problem	Solution
6 The IntelliShun device is unable to detect packets passing over the bridge.	IntelliShun 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. If IntelliShun 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. **Scenario 1:** **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. **Scenario 2:** **Packets are passing over the bridge, but the IntelliShun 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. **Scenario 3:** **Packets are passing over the bridge, but the IntelliShun 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.


RA
RiskAnalytics™
THE ART OF SECURITY™