IPsonar 6.0 QuickStart

Get started quickly by deploying a Lumeta IPsonar 6.0 virtual Report Server (RSN) on a VMware ESXi server. Then contact your Lumeta technical consultant to initiate the license-fulfillment process.

This deployment process assumes the following:

1. Use VMware vSphere as your client
2. Have 300GB of disk space on your VMware ESXi server
3. Have 16GB of memory on your VMware ESXi server
4. Know the IP, subnet mask, and gateway for your host

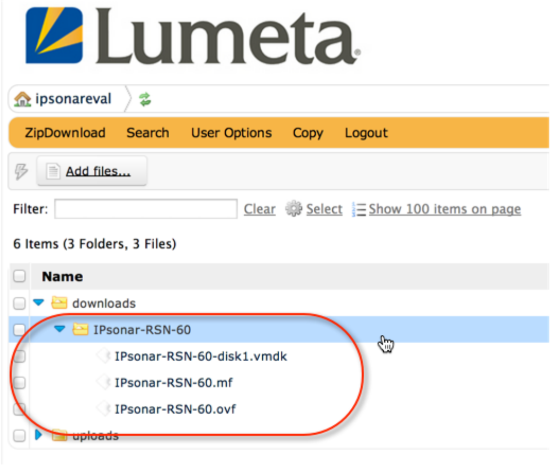
Download a Virtual RSN

Lumeta provides the virtual RSN image on our SFTP support site. The virtual RSN image may also be installed from media. If installing from media such as a DVD, skip to Check Available Space.

Download the Virtual RSN image as follows:

1. Browse to https://sftp.lumeta.com.
2. Enter your credentials and click Login.

   Contact us if you need this information or other login assistance.
3. Browse the Downloads directory for the virtual install directory for the IPsonar 6.0 release.



6 Items (3 Folders, 3 Files)

- downloads
  - IPsonar-RSN-60
    - IPsonar-RSN-60-disk1.vmdk
    - IPsonar-RSN-60.mf
    - IPsonar-RSN-60.ovf
- uploads

Check Available Space

If you don't have enough space on your virtual server, you'll need to reallocate resources (i.e., delete or stop them from running, or switch to another virtual machine that have more available resources)

1. Launch the VMware vSphere client.
2. Go to the Summary tab and view your disk space and memory.
3. Ensure that your VMware host has resources to accommodate a virtual configured with 16GB RAM, a virtual CPU with 1 virtual socket and 2 cores per socket, and a 300GB virtual disk.

Deploy the Virtual RSN

Install the virtual RSN image to your EXSi server. In vSphere, that RSN image is referred to as the *OVF Template*.

1. On the File menu, select **Deploy OVF Template** and follow the onscreen prompts.
2. Step through the process of browsing to and then opening the OVF package you downloaded from Lumeta.
3. Click Next to accept and proceed through two pages of default options.
4. On the Name and Location page, you may rename your RSN or accept the default.
5. On the Disk Format page, select **Thick Provision Lazy Zeroes** and click Finish.
   The OVF package downloads. It should take approximately 4 minutes to complete.
   The virtual machine deploys, and you will soon see the name of your new virtual RSN displayed among the inventory of virtual machines listed on the left-hand side of your page.

Configure the Virtual RSN

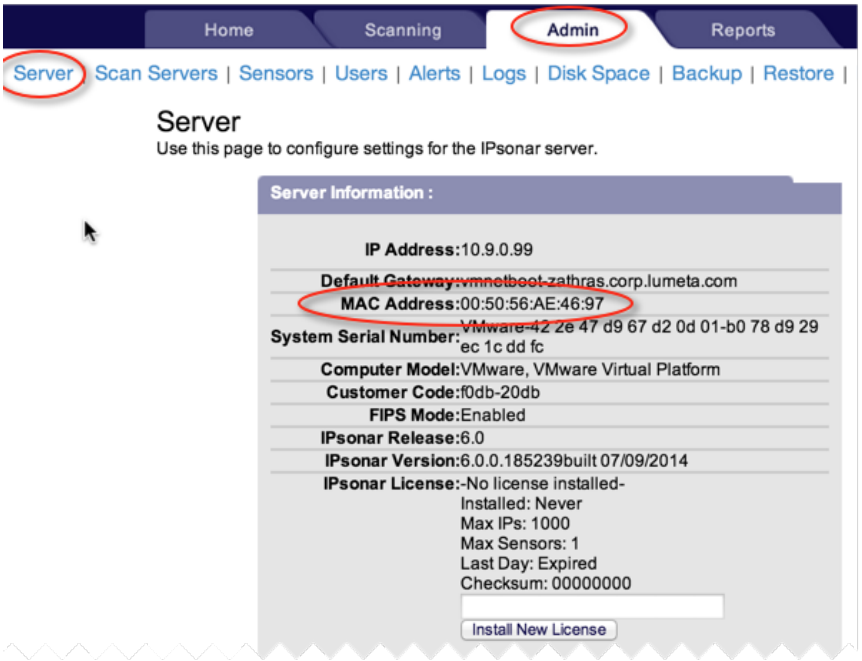
Set up the virtual RSN to operate on your networks.

1. Right-click the name of your virtual RSN and from the Main Menu, click **Power > Power On.**
2. Select the Console tab to ensure the RSN is booting. The boot completes and a Login prompt displays.

3. Log in as **serverconfig** and configure the network settings and other key features of IPsonar as follows:
    - Stop the IPsonar services (Option 62).
    - Set the date and time (Option 32).
    - Configure the interface options (Option 33).
    - Set an interface speed and indicate whether the RSN should respond to pings (Option 34)
    - OPTIONAL: Name the RSN (Option 37).
    - OPTIONAL: Configure the NTP server (Option 3262).
    - OPTIONAL: Set the common scan server and interval server password (Option 38).
4. Reboot the virtual RSN to activate this configuration (Option 72).

Install a License

1. Log in to IPsonar.
2. Contact your Lumeta technical consultant to request a license key. Provide the technical consultant with your virtual RSN's MAC Address.


Home
Scanning
Admin
Reports
Server | Scan Servers | Sensors | Users | Alerts | Logs | Disk Space | Backup | Restore |

Server

Use this page to configure settings for the IPsonar server.

Server Information :

IP Address:10.9.0.99

Default Gateway:vmnetboot-zathras.corp.lumeta.com

MAC Address:00:50:56:AE:46:97

System Serial Number:VMware-42 2e 47 d9 67 d2 0d 01-b0 78 d9 29 ec 1c dd fc

Computer Model:VMware, VMware Virtual Platform

Customer Code:f0db-20db

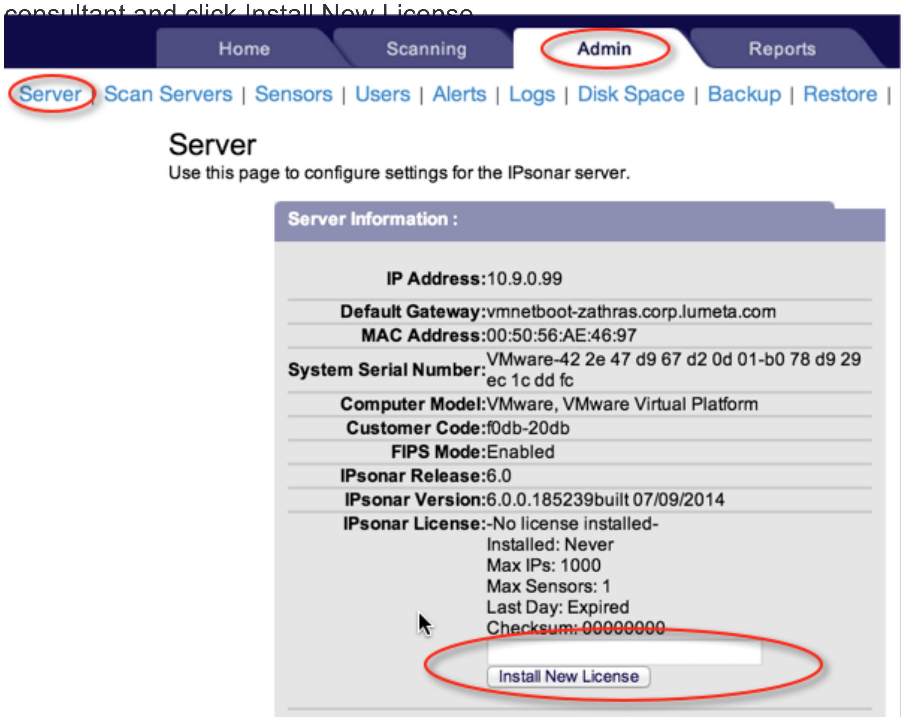
FIPS Mode: Enabled

IPsonar Release:6.0

IPsonar Version:6.0.0.185239built 07/09/2014

IPsonar License:-No license installed-
Installed: Never
Max IPs: 1000
Max Sensors: 1
Last Day: Expired
Checksum: 00000000

3. On the Admin > Server page, enter the license key you received from your technical consultant and click Install New License.


Home
Scanning
Admin
Reports
Server | Scan Servers | Sensors | Users | Alerts | Logs | Disk Space | Backup | Restore |
Install New License

Server

Use this page to configure settings for the IPsonar server.

Server Information :

IP Address:10.9.0.99
Default Gateway:vmnetboot-zathras.corp.lumeta.com
MAC Address:00:50:56:AE:46:97
System Serial Number:VMware-42 2e 47 d9 67 d2 0d 01-b0 78 d9 29 ec 1c dd fc
Computer Model:VMware, VMware Virtual Platform
Customer Code:f0db-20db
FIPS Mode:Enabled
IPsonar Release:6.0
IPsonar Version:6.0.0.185239built 07/09/2014
IPsonar License:-No license installed-
Installed: Never
Max IPs: 1000
Max Sensors: 1
Last Day: Expired
Checksum: 00000000

Congratulations! With this, your installation is complete and you are ready to use Lumeta IPsonar 6.0.

Log In to Lumeta IPsonar

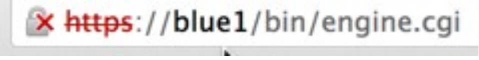
Lumeta supports the two most-recent releases of the Chrome and Firefox browsers. Log in as follows:

1. Using a supported browser, go to `https:/<your IPsonar server>`.

   For example:

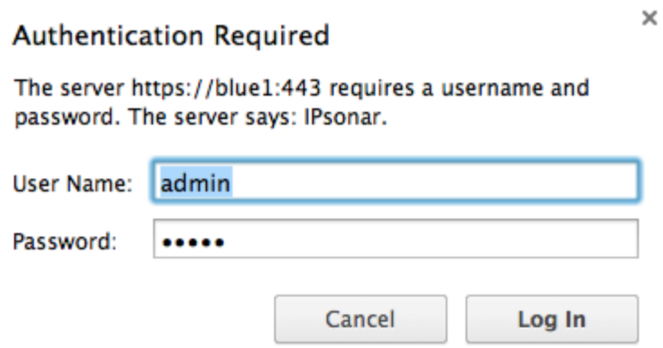
https://blue1

   or



~~https~~://blue1/bin/engine.cgi

2. Enter your User Name and Password.
   The default User Name is **admin**; the default Password is **admin**.



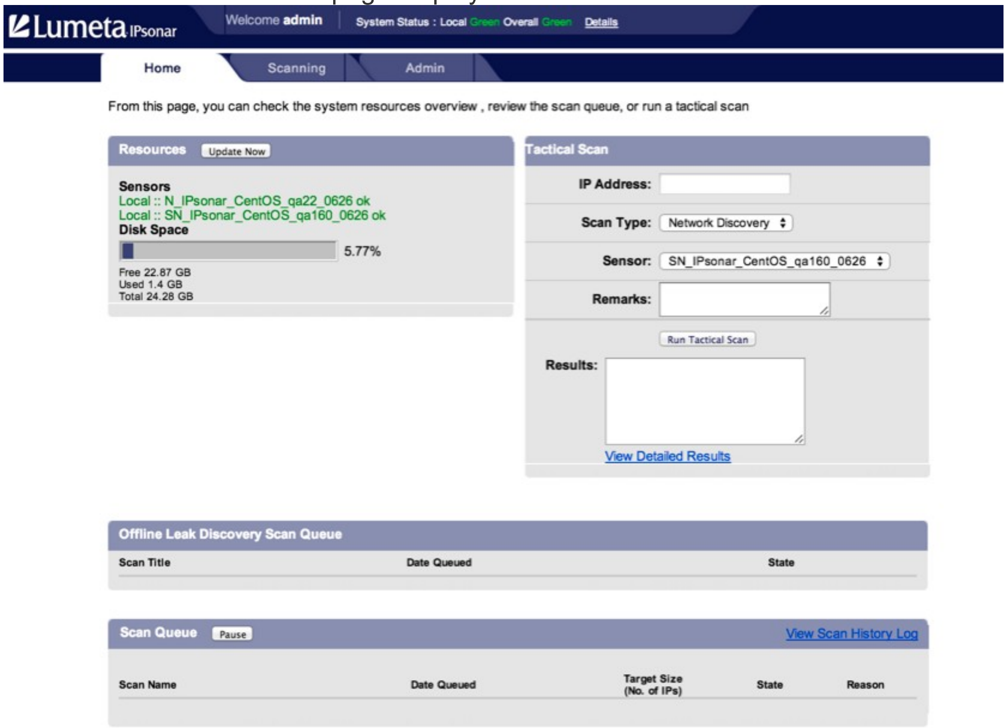
Authentication Required

The server https://blue1:443 requires a username and password. The server says: IPsonar.

User Name: admin

Password: •••••

The Lumeta IPsonar Home page displays:



Welcome admin | System Status : Local Green Overall Green

From this page, you can check the system resources overview , review the scan queue, or run a tactical scan

Resources

Sensors
Local :: N_IPsonar_CentOS_qa22_0626 ok
Local :: SN_IPsonar_CentOS_qa160_0626 ok

Disk Space

5.77%

Free 22.87 GB
Used 1.4 GB
Total 24.28 GB

Tactical Scan

IP Address:

Scan Type: Network Discovery

Sensor: SN_IPsonar_CentOS_qa160_0626

Remarks:

Results:

Offline Leak Discovery Scan Queue

Scan Title	Date Queued	State

Scan Queue

Scan Name	Date Queued	Target Size (No. of IPs)	State	Reason

Congratulations! You've logged in successfully!

If for any reason you had trouble logging in, please contact Lumeta Support (support@lumeta.com) for assistance.

Perform a First Scan

Use the Scan Wizard to experience your first scan as though it were magic. The Scan Wizard is a tool that queries your network for information and applies optimal general scan configuration settings. It is designed to remove hurdles, enabling you to generate scan results quickly.

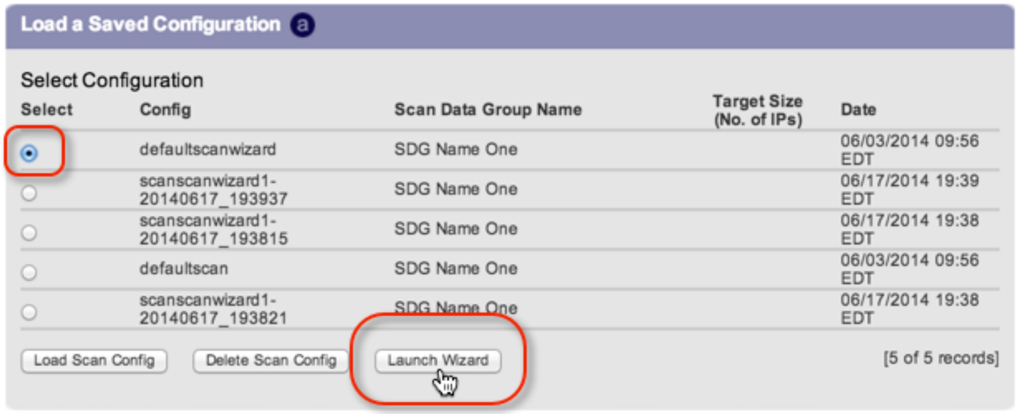
The Scan Wizard integrates the following characteristics:

- Network Discovery has been enabled (config attribute networkDiscovery).
- The option to skip BGP router has been disabled (snmpscanskipBgpRouters).
- The option to perform Network Discovery (ND) looping has been enabled (snmpScanLoop).
- The option to perform SNMP stitch has been disabled (snmpStitch).

When you complete the steps of the Scan Wizard, you'll have a saved scan configuration file with the filename <`scanwizard1-`*`yyyymmdd_hhmmss`*`.cfg`>. Scanning will begin immediately with the newly-created Scan Wizard file running in conjunction with the `defaultreport` report configuration file.

1. At the top of any page, click **Admin** > **Scanning.**

2. Select the **Defaultscanwizard** radio button and then click **Launch Wizard**.

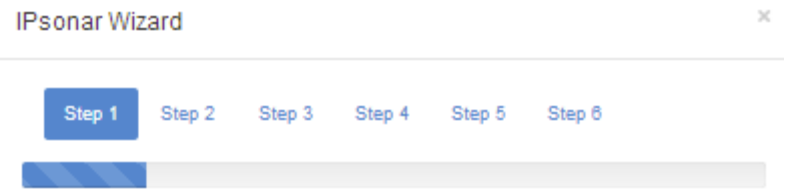


Load a Saved Configuration

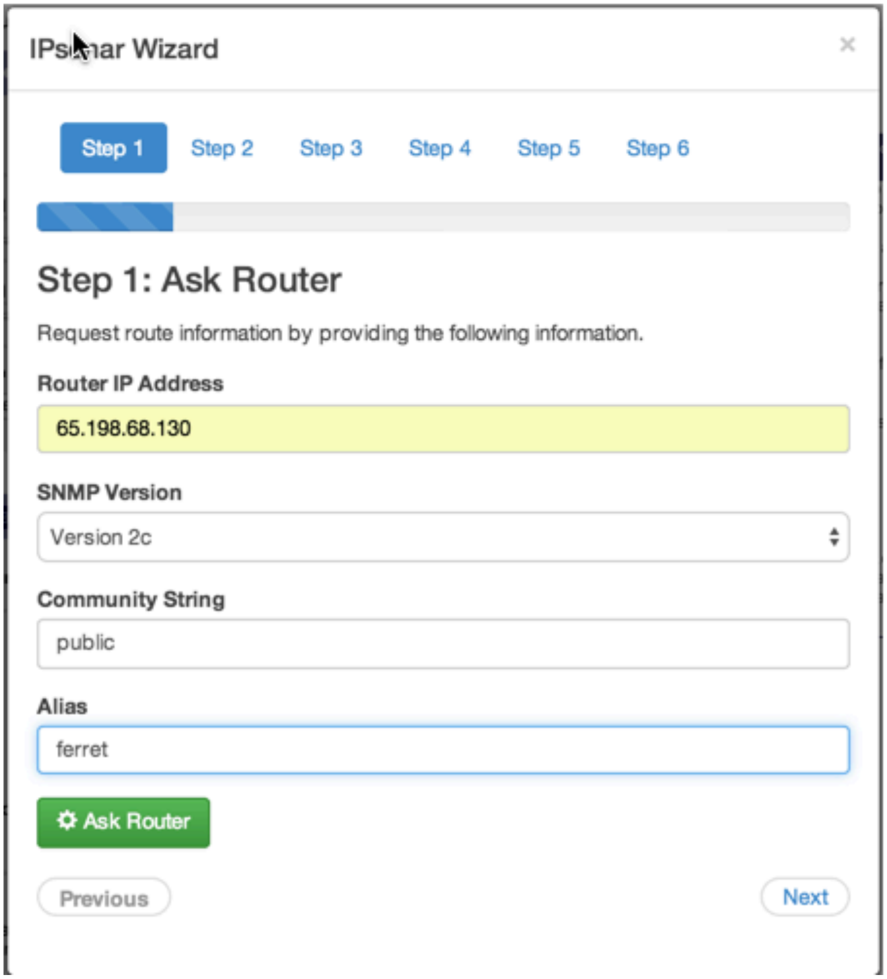
Select Configuration

Select	Config	Scan Data Group Name	Target Size (No. of IPs)	Date
●	defaultscanwizard	SDG Name One		06/03/2014 09:56 EDT
○	scanscanwizard1-20140617_193937	SDG Name One		06/17/2014 19:39 EDT
○	scanscanwizard1-20140617_193815	SDG Name One		06/17/2014 19:38 EDT
○	defaultscan	SDG Name One		06/03/2014 09:56 EDT
○	scanscanwizard1-20140617_193821	SDG Name One		06/17/2014 19:38 EDT

3. Although you'll progress through the steps in order, this screen provides flexibility to complete or revisit any step in the process.



4. In this Scan Wizard first step, we ask one router on your network to disclose the information it has stored in its route tables. Authenticate to the router by completing the form.



Step 1: Ask Router

Request route information by providing the following information.

Router IP Address: 65.198.68.130

SNMP Version: Version 2c

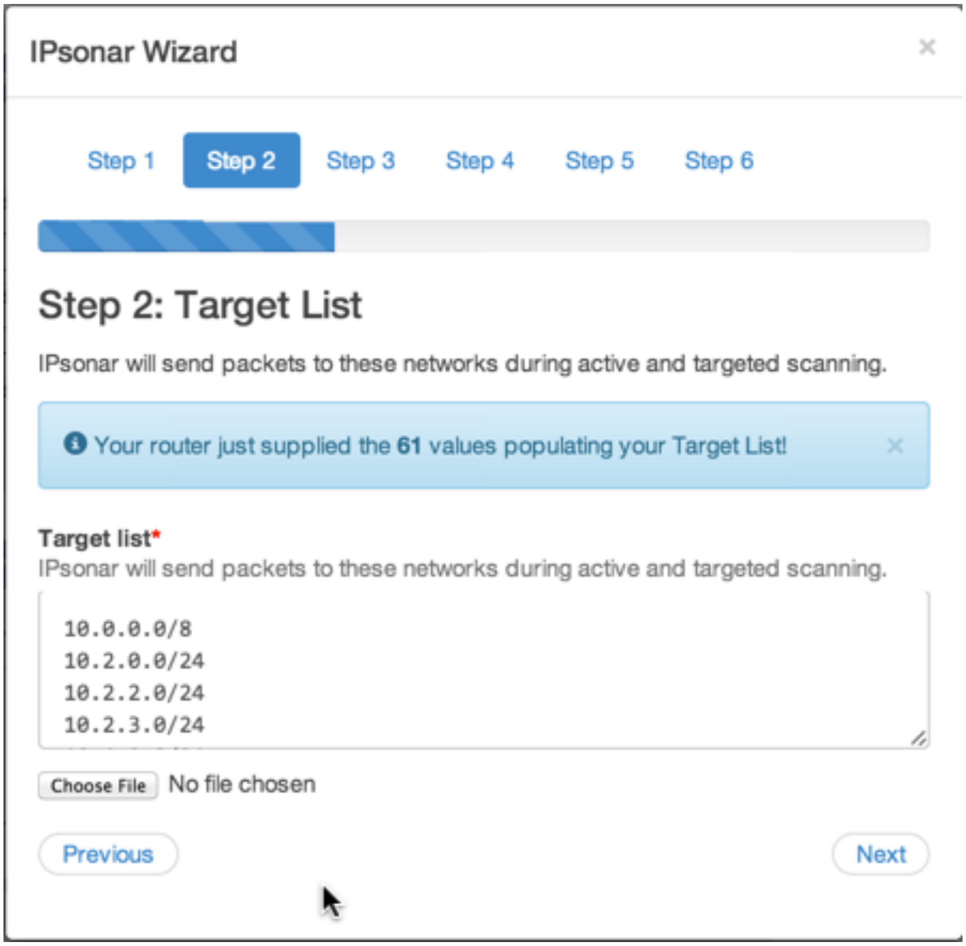
Community String: public

Alias: ferret

5. Indicate which IPs Lumeta IPsonar must target during the scan. The Target list governs where IPsonar sends packets during active and targeted discovery.

   Notice that the router you queried in Step 1 has already populated the Target list in Step 2.

To avoid typing, you can append to the content in the Target box by uploading a CSV-formatted file of IP address ranges. Click Choose File to browse to your CSV file and then select it.



IPsonar Wizard

Step 2: Target List

IPsonar will send packets to these networks during active and targeted scanning.

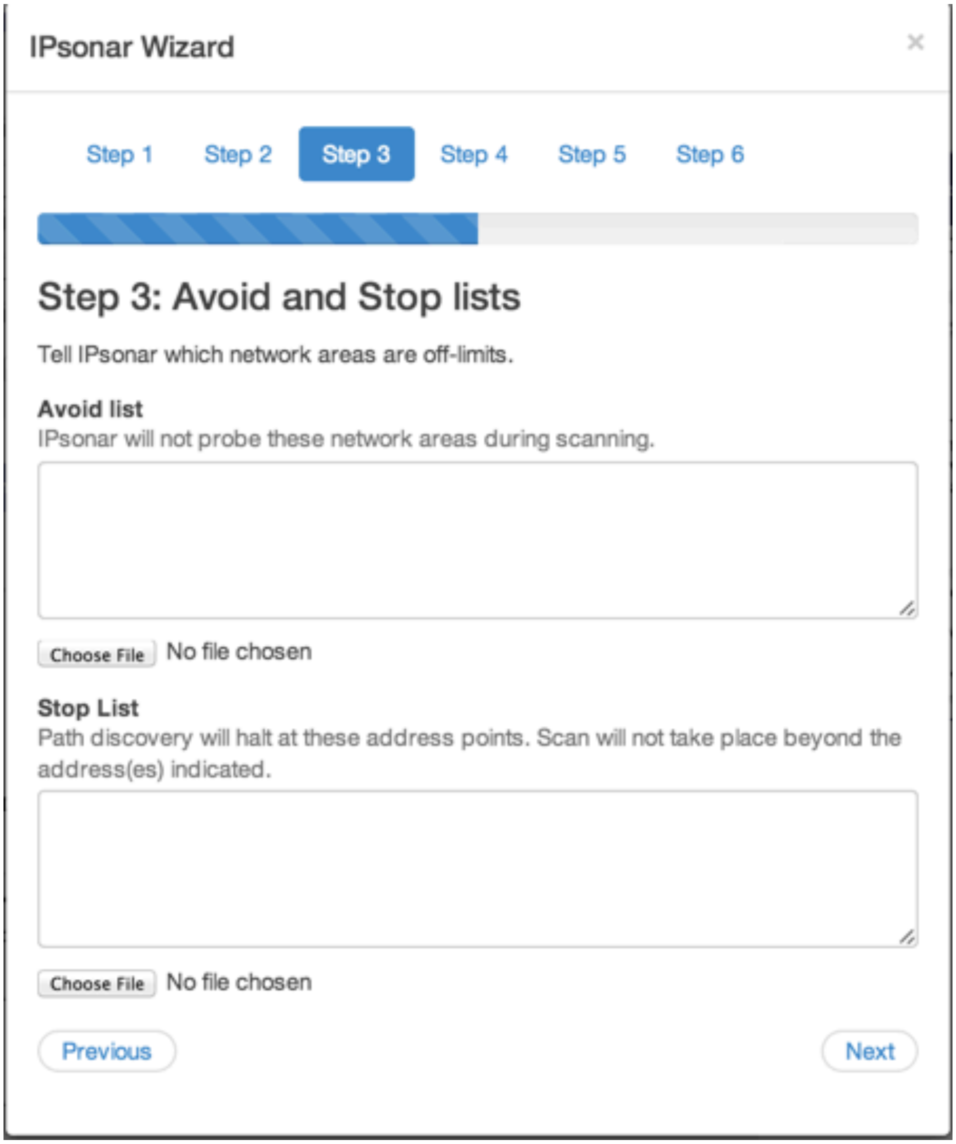
Your router just supplied the **61** values populating your Target List!

Target list*
IPsonar will send packets to these networks during active and targeted scanning.

```
10.0.0.0/8
10.2.0.0/24
10.2.2.0/24
10.2.3.0/24
```

Choose File No file chosen

6. Indicate which network locations Lumeta IPsonar must not scan.



IPsonar Wizard

Step 3: Avoid and Stop lists

Tell IPsonar which network areas are off-limits.

Avoid list

IPsonar will not probe these network areas during scanning.

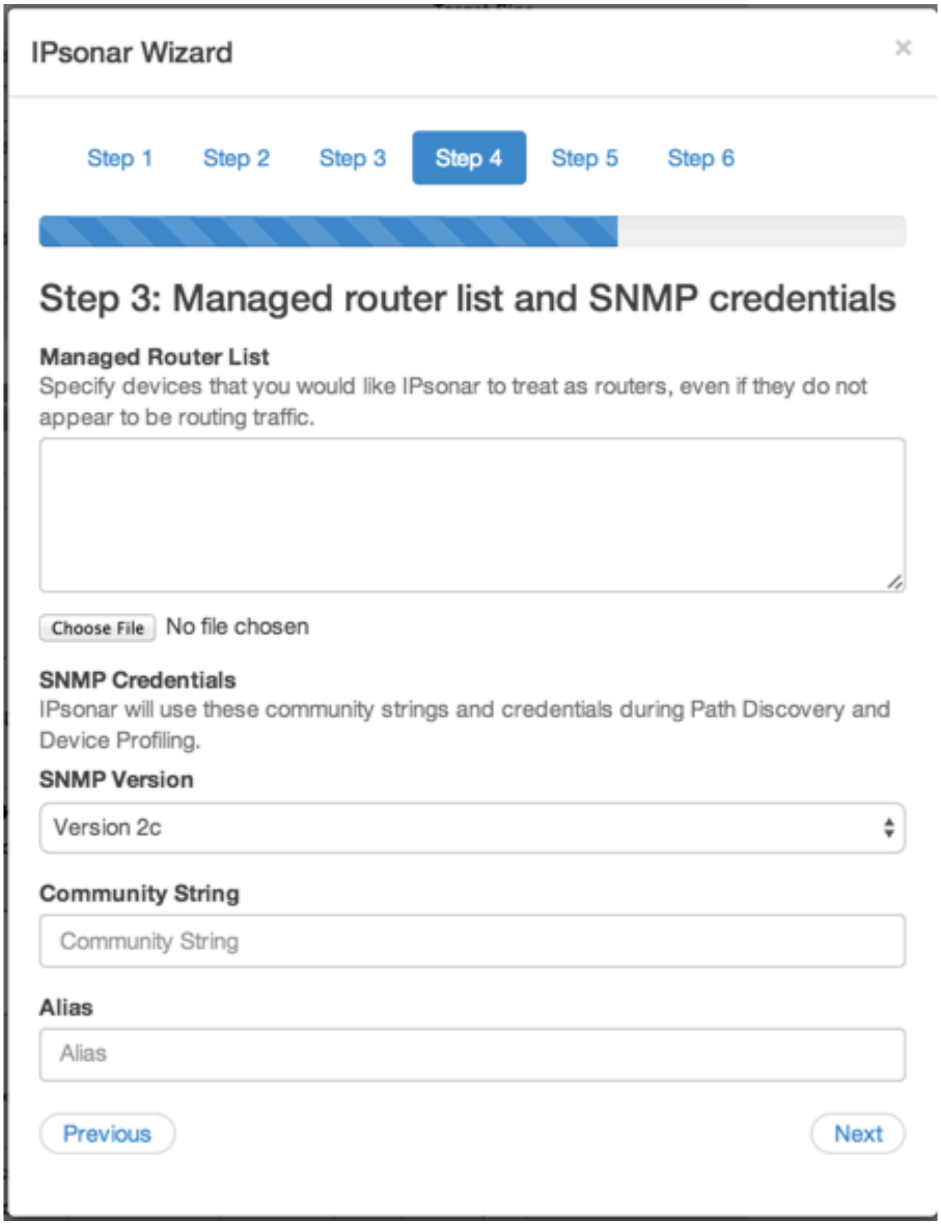
Choose File No file chosen

Stop List

Path discovery will halt at these address points. Scan will not take place beyond the address(es) indicated.

Choose File No file chosen

7. Tell IPsonar which routers you manage and provide SNMP with authentication information to them.



Step 3: Managed router list and SNMP credentials

Managed Router List

Specify devices that you would like IPsonar to treat as routers, even if they do not appear to be routing traffic.

No file chosen

SNMP Credentials

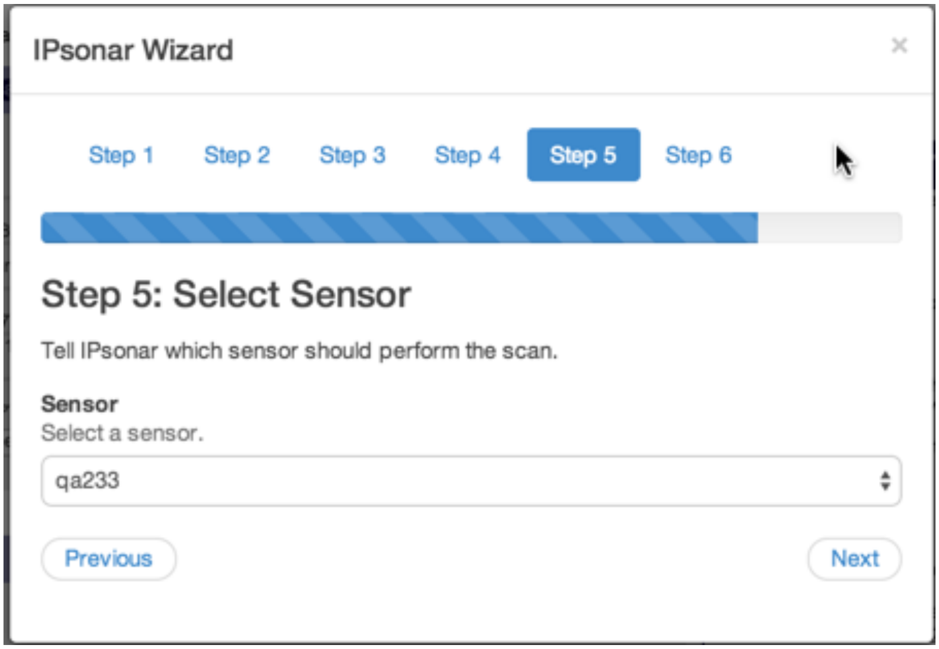
IPsonar will use these community strings and credentials during Path Discovery and Device Profiling.

SNMP Version: Version 2c

Community String: Community String

Alias: Alias

8. Tell IPsonar which sensor should perform the scan. You can select from all available sensors.



IPsonar Wizard

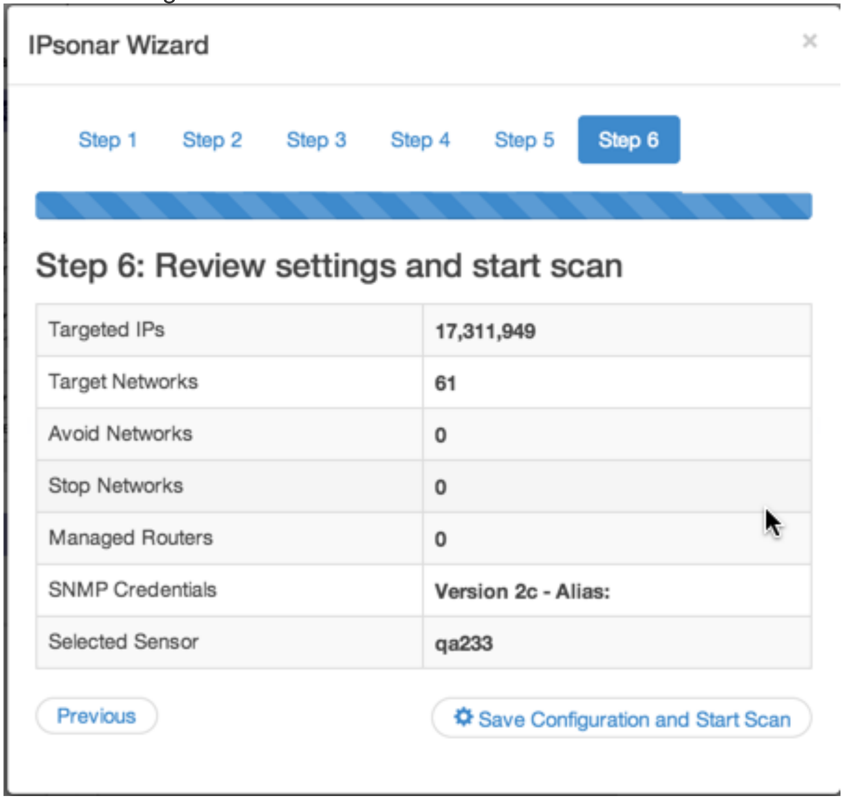
Step 5: Select Sensor

Tell IPsonar which sensor should perform the scan.

Sensor
Select a sensor.

qa233

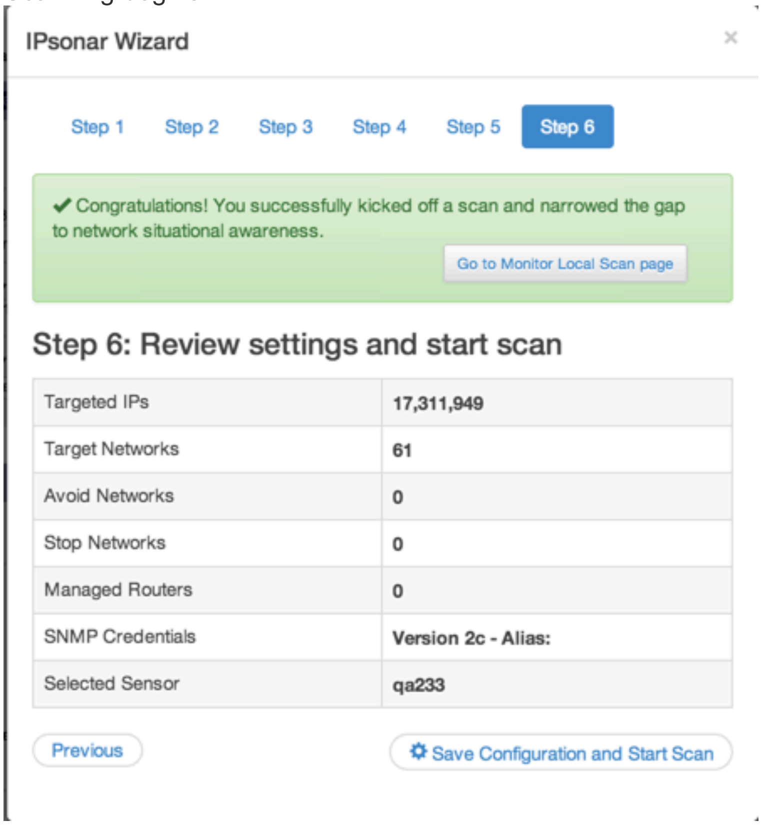
9. Review settings and start the scan.



Step 6: Review settings and start scan

Targeted IPs	17,311,949
Target Networks	61
Avoid Networks	0
Stop Networks	0
Managed Routers	0
SNMP Credentials	Version 2c - Alias:
Selected Sensor	qa233

10. Scanning begins.



IPsonar Wizard

×
Step 1
Step 2
Step 3
Step 4
Step 5
Step 6

✓ Congratulations! You successfully kicked off a scan and narrowed the gap to network situational awareness.

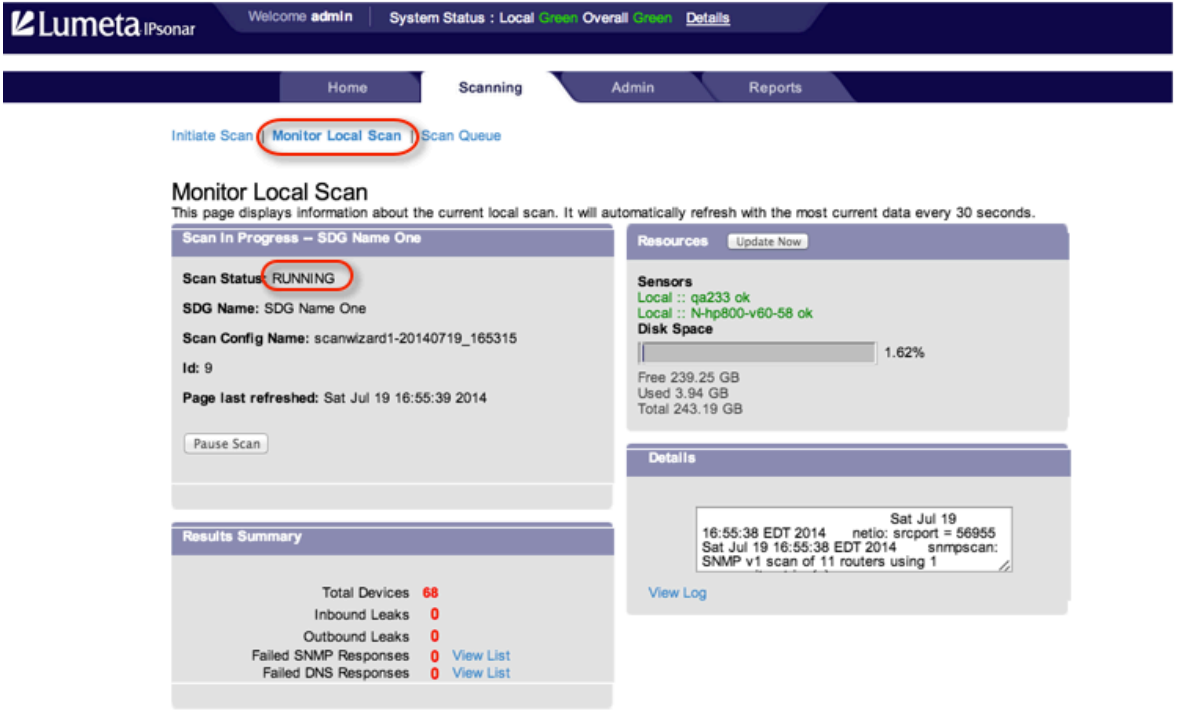
Go to Monitor Local Scan page

Step 6: Review settings and start scan

Targeted IPs	**17,311,949**
Target Networks	**61**
Avoid Networks	**0**
Stop Networks	**0**
Managed Routers	**0**
SNMP Credentials	**Version 2c - Alias:**
Selected Sensor	**qa233**

Previous
Save Configuration and Start Scan

Monitor the scan's progress on the Monitor Local Scan page.



Monitor Local Scan

This page displays information about the current local scan. It will automatically refresh with the most current data every 30 seconds.

Scan In Progress -- SDG Name One

Scan Status: RUNNING

SDG Name: SDG Name One

Scan Config Name: scanwizard1-20140719_165315

Id: 9

Page last refreshed: Sat Jul 19 16:55:39 2014

Results Summary

Total Devices	68
Inbound Leaks	0
Outbound Leaks	0
Failed SNMP Responses	0
Failed DNS Responses	0

Resources

Sensors
Local :: qa233 ok
Local :: N-hp800-v60-58 ok

Disk Space
1.62%
Free 239.25 GB
Used 3.94 GB
Total 243.19 GB

Details

```
                                  Sat Jul 19
16:55:38 EDT 2014      netio: srcport = 56955
Sat Jul 19 16:55:38 EDT 2014       snmpscan:
SNMP v1 scan of 11 routers using 1
```

You have completed your first scan successfully!

To learn how to read and interpret the results generated by this first scan, refer to the Review Your Scan Report page in All Things IPsonar.