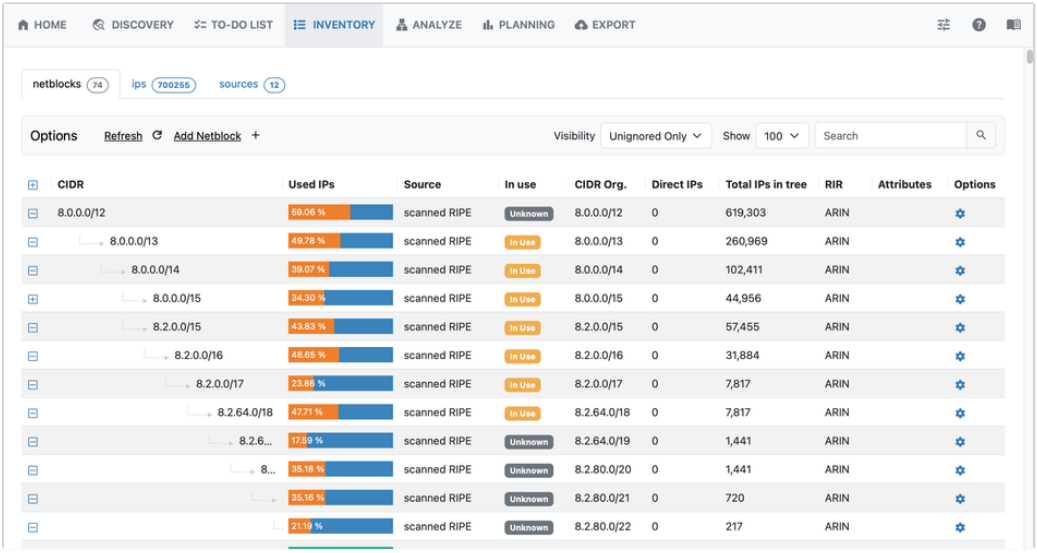
IPv4.GLOBAL

ReView: The User Guide

ReView

IPv4 Global / Hilco ReView 2
User Guide 4
Home Page & Getting Started 9
Discovery 11
To-Do List 21
Inventory 24
Analyze 32
Planning 39
Export 42

IPv4 Global / Hilco ReView



Overview

ReView is a powerful automated discovery and scanning tool that finds, catalogs, and analyzes your network topography. Using ReView, you can quickly find and view used and free IPs, giving your company the opportunity to efficiently consolidate used space and view the resulting potential market rate of your aggregated unused IP space.

Requirements and Installation

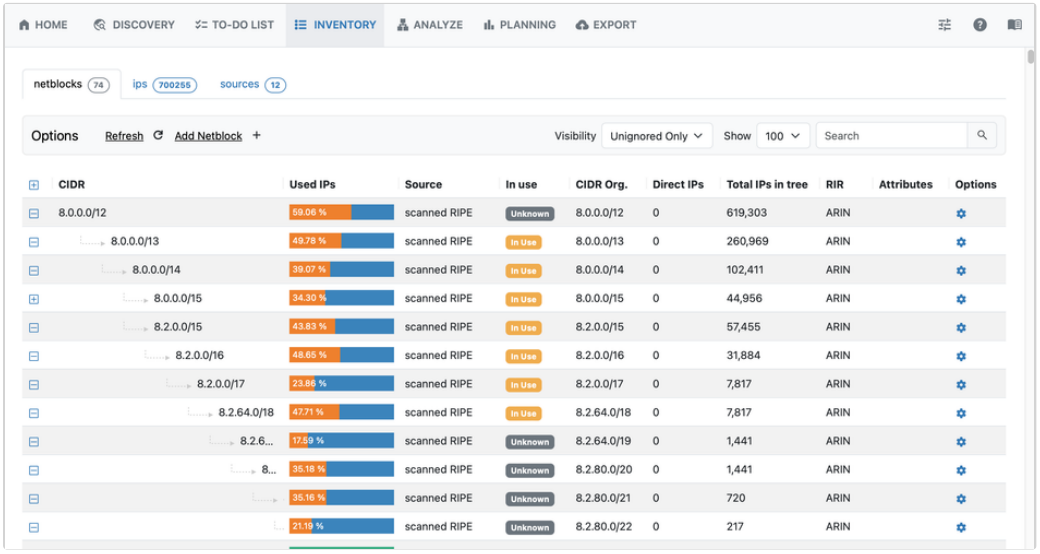
ReView is a locally downloaded tool with minimal system requirements. The hosting system must be connected to the internet for ReView to process scans.

To install, log in as the system administrator user (or select “run as administrator”) and download the provided build file for your OS (Windows, MacOS, and Linux are supported). Once downloaded, unzip the file and double click on the application name/icon in order to open.

For additional information, see the documentation sections below:

- User Guide
  - Home Page & Getting Started
  - Discovery
  - To-Do List
  - Inventory
  - Analyze
  - Planning
  - Export
- Release Notes
  - ReView 2.0.0

User Guide

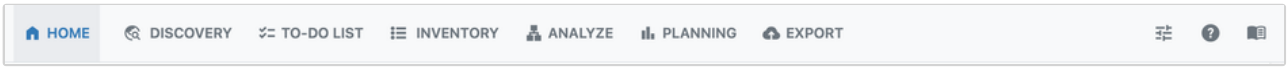


This User Guide provides details on navigation, application settings, and the tabs available in ReView.

- UI Overview
  - Navigation
  - Settings
    - General Settings
      - Appearance Options
      - Cache
    - Pricing
    - Logs
- Additional Information:

UI Overview

Navigation



To navigate through ReView, click the tabs and sub-tabs at the top of the application. The major tabs are:

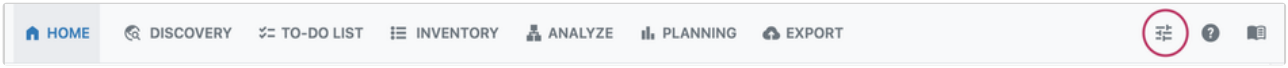
- Home - The Home page is the initial page displayed while in ReView. Tiles display current discovery progress, inventory, scan to-do list, and visualization tools for your network.
- Discovery - The Discovery tab is the first step to identifying network resources to add to your inventory. Here, you can use configuration files, paste text configs, or use automated scanning options to identify devices to use for Discovery. Available discovery / device identification options include: DHCP, DNS, Firewall, Generic Config, mDNS, Load Balancer, Ping Scan, RIR, Router Configs, SNMP, ARP, SSDP, and Cloud Providers.
- To-Do List - The To-Do list identifies and marks neighboring devices encountered during router discovery scanning, and lists them for future scanning.
- Inventory - The Inventory tab displays an organized list of all discovered netblocks, IPs, sources, and their associated metadata. Here, for each netblock you can view RIR, Source, CIDR, use status, IPs found, total IPs, IP utilization, and start/end address.

- Analyze - The Analyze tab interprets the IP inventory data found during Discovery, and determines valuation of free IPv4 space based on the current network structure.
- Planning - The Planning tab shows the potential value of saved plan strategies, and the configuration differences for each plan.
- Export - Export will prepare a report on the state of your network and email it to both you and to IPv4.Global/ Hilco. You may also download a PDF Report, or upload data into 6connect ProVision.

Additional helpful pages include:

- Settings (slider icon) - Set appearance theme, clear cache, or review pricing and log data.
- About (question icon) - Displays the EULA for ReView
- Documentation (book icon) - Provides a link to ReView's online documentation.

Settings

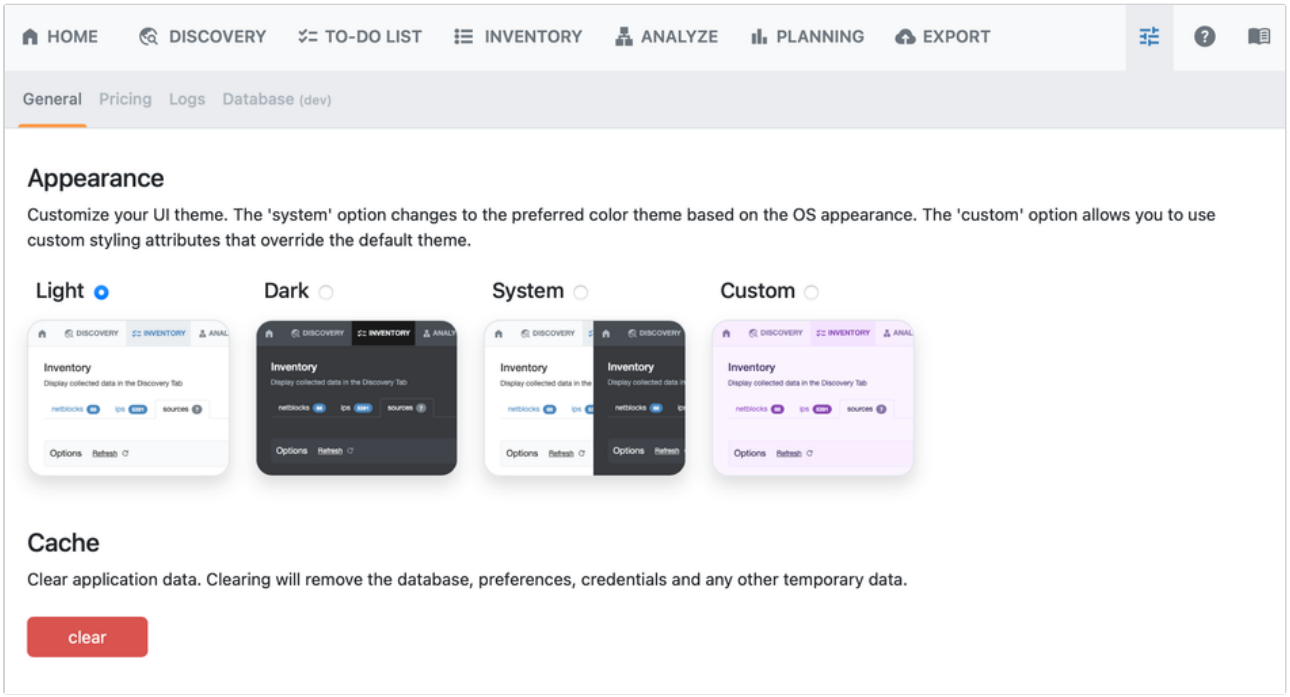


Click the settings icon at the top right of the navigation bar to open ReView settings.

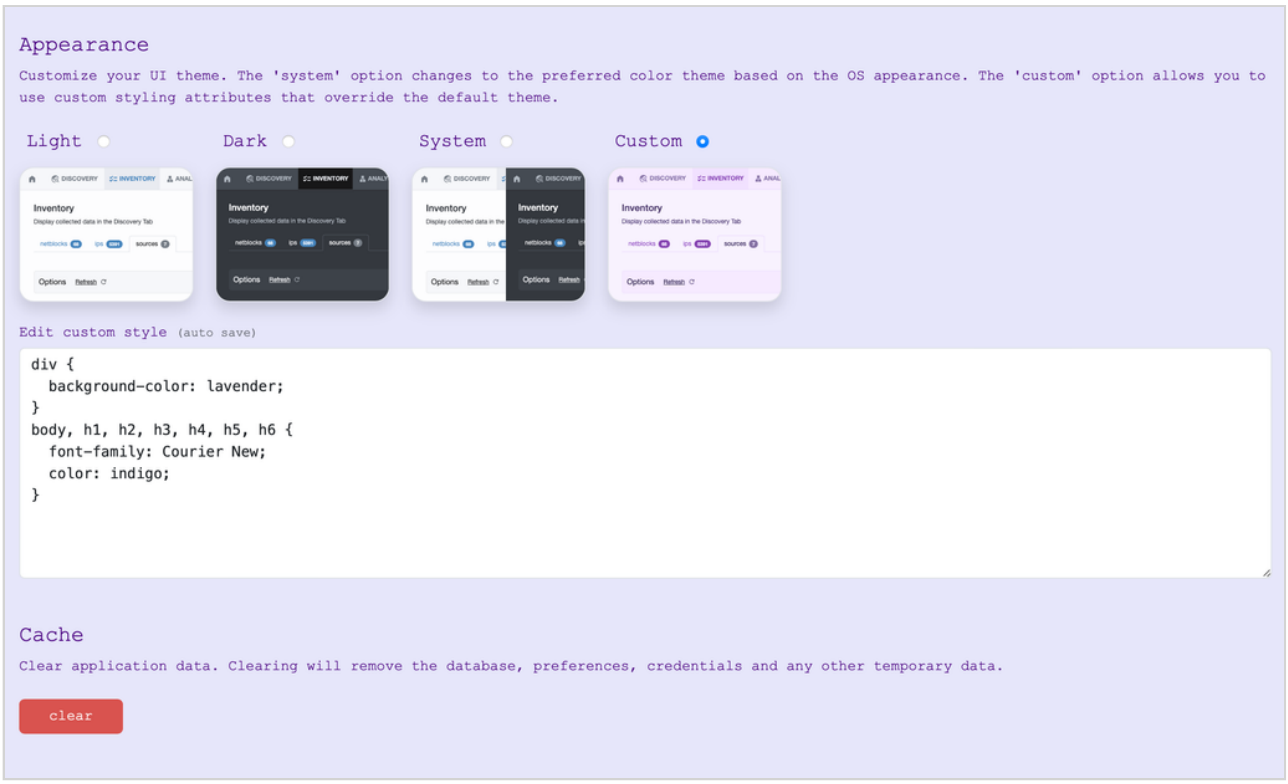
General Settings

Appearance Options

ReView supports light and dark themes according to your system settings. You may choose between light mode, dark mode, OS based, or custom appearance settings.



For custom settings, select "Custom" and then paste the desired custom CSS to override default attributes. Edits made to Custom Styles are saved automatically.



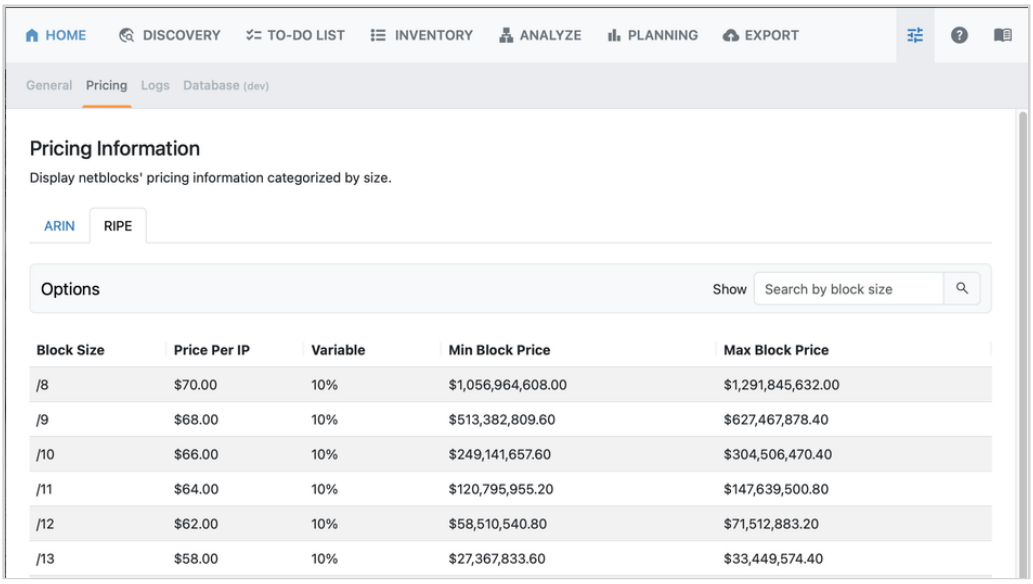
Cache

Clearing the cache clears all application data, including removing the database, preferences, credentials, and temporary data.

> ⚠ Clearing the cache should only be in circumstances where a full ‘reset’ is necessary. Use with caution.

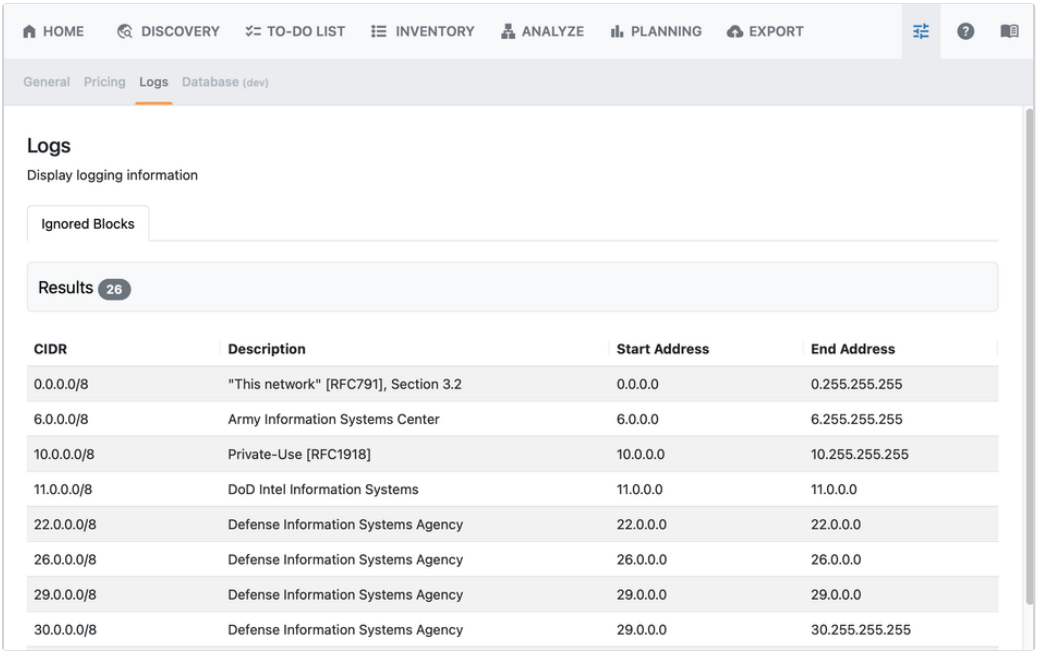
Pricing

The pricing data used for estimated values under the Analyze and Planning tabs is accessible under Settings → General → Pricing. Searchable price lists are available for both ARIN and RIPE.



Logs

The Logs tab displays logging information and ignored blocks.



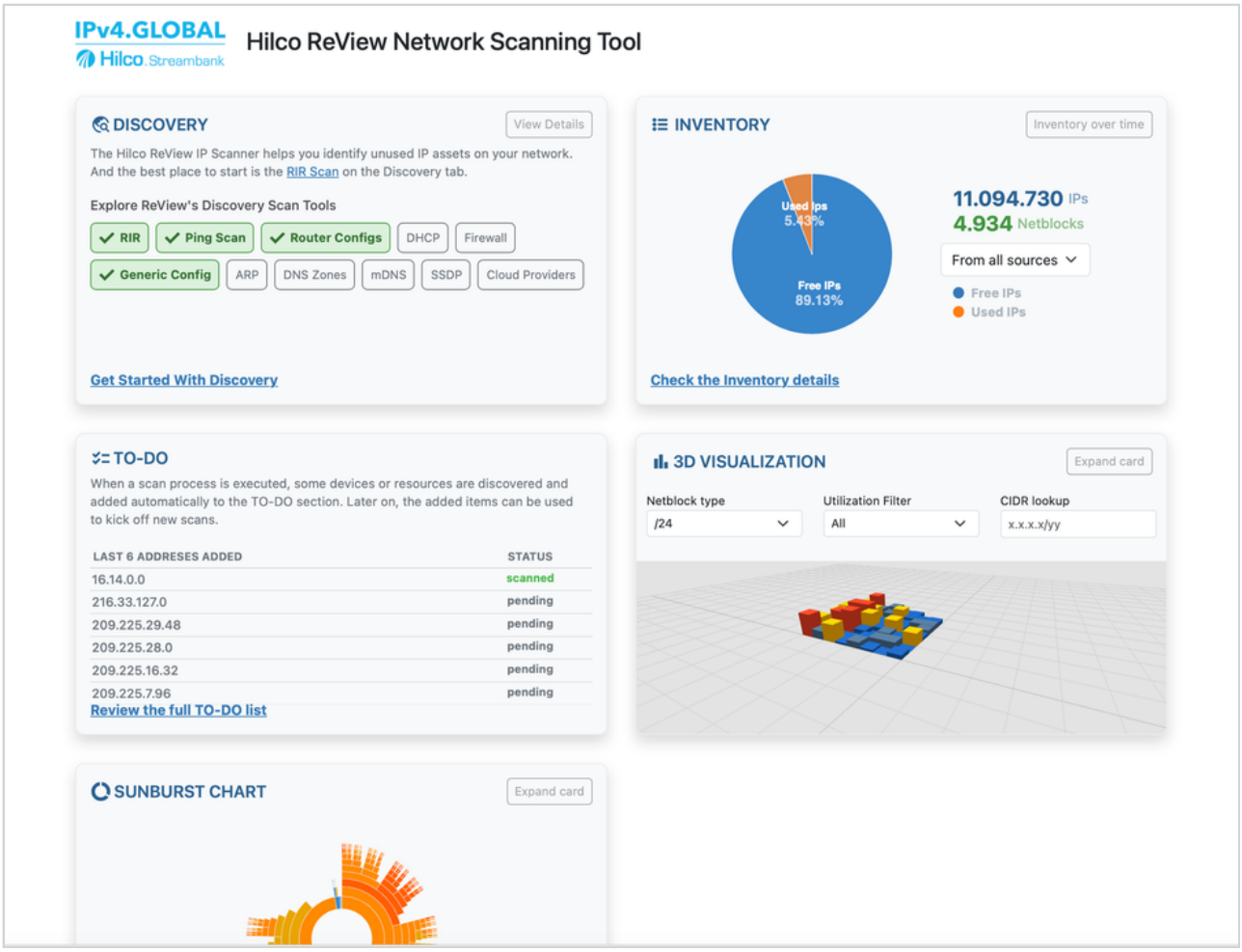
Additional Information:

See the following sections for details on working within ReView:

- Home Page & Getting Started
- Discovery
- To-Do List
- Inventory
- Analyze
- Planning
- Export

Home Page & Getting Started

ReView Home Page



The Home page is the initial page displayed while in ReView. Here, dashboard tiles show current discovery progress, inventory, scan to-do list, and visualization tools for your network. Links will be displayed to set up initial configuration and discovery steps to start using the scanning tool.

Getting Started

When you first open ReView, take a look at the links available on the Home page.

Demo data is available for you to explore the features and visualizations of ReView prior to importing your own network data.

If desired, open settings to customize your appearance to light mode, dark mode, or system-based.

Workflow:

When you are ready to start scanning, we recommend proceeding in the following order:

1) Network Discovery & Scans

Where: Home; Discovery Tab; To-Do List

- The best place to start is using the RIR Scan on the Discovery tab. Enter an IP (or use the default public IP found), click “scan”, and it and will query ARIN, RIPE, APNIC, LACNIC, and AFRINIC for officially allocated IP resources.
- Next, identify sub-blocks and hosts by supplying Router Configs or DNS Zones, or by scanning ARP tables or scanning DHCP leases files.
- Additional options under Discovery include items such as Firewalls, Load Balancers, SNMP, SSDP, and even a “Generic Config” option for other non-supported devices.
  - Data may be provided either by uploading config files (Note: Must be either .zip or .tar files) or by pasting the configuration text.
- Check the To-Do List to perform Ping Scans
  - If neighboring devices are encountered during an SNMP, SSH, Config, or Ping scan, they are added to the To-Do list and flagged for later user review and scanning to complete network segments.

2) Review and Update Inventory Status

Where: Inventory Tab

- During discovery scanning, found netblocks, ips and sources will be added to the Inventory page for review.
  - You may manually add additional blocks, update or change block status, add attributes, ignore blocks, or add sources from this area.
- Confirm the use status for the netblocks / IPs in inventory - the use status (unknown, in use, free, ignored) will determine whether the block is sellable and optimization strategy steps.

3) Analyze Inventory and Get Suggested Plans

Where: Analyze Tab

- After discovery scans and any necessary inventory review is complete, proceed to the Analyze tab. The tab will display an estimated value of your public IP space based on the current inventory. It can be used to identify areas where your network can be made more efficient. Suggested plans may be saved for later review.
  - If any change occurs in the data, click on "Reinitialize" to refresh the analysis.

4) Review Plans and Export

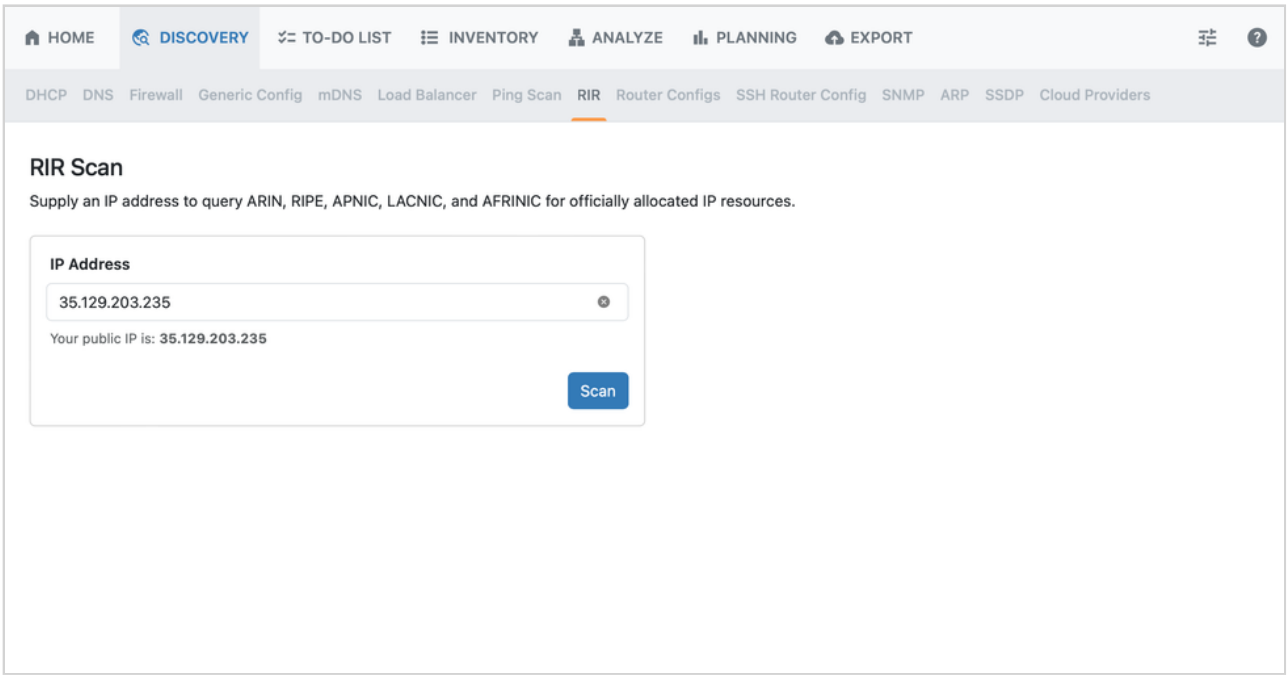
Where: Planning Tab; Export Tab

- The Planning tab shows the potential value of saved plan strategies, and the configuration differences for each plan.
- If desired, you may navigate to the Export tab to prepare a report on the state of your network and email it to both you and to IPv4Global. You may also download a PDF report, or upload your data into 6connect ProVision.

Next Steps:

Continue on to the Discovery section for to start scanning your network.

Discovery



The Discovery tab is first step to identifying network resources to add to your inventory. Here, you can use configuration files, paste text configs, or use automated scanning options to identify devices to use for discovery.

The Discovery tab allows the user to gather IP topography data via the following methods, organized as sub-tabs: DHCP, DNS, Firewall, Generic Config, mDNS, Load Balancer, Ping Scan, RIR, Router Configs, SSH Router Config, SNMP, ARP, and SSDP.

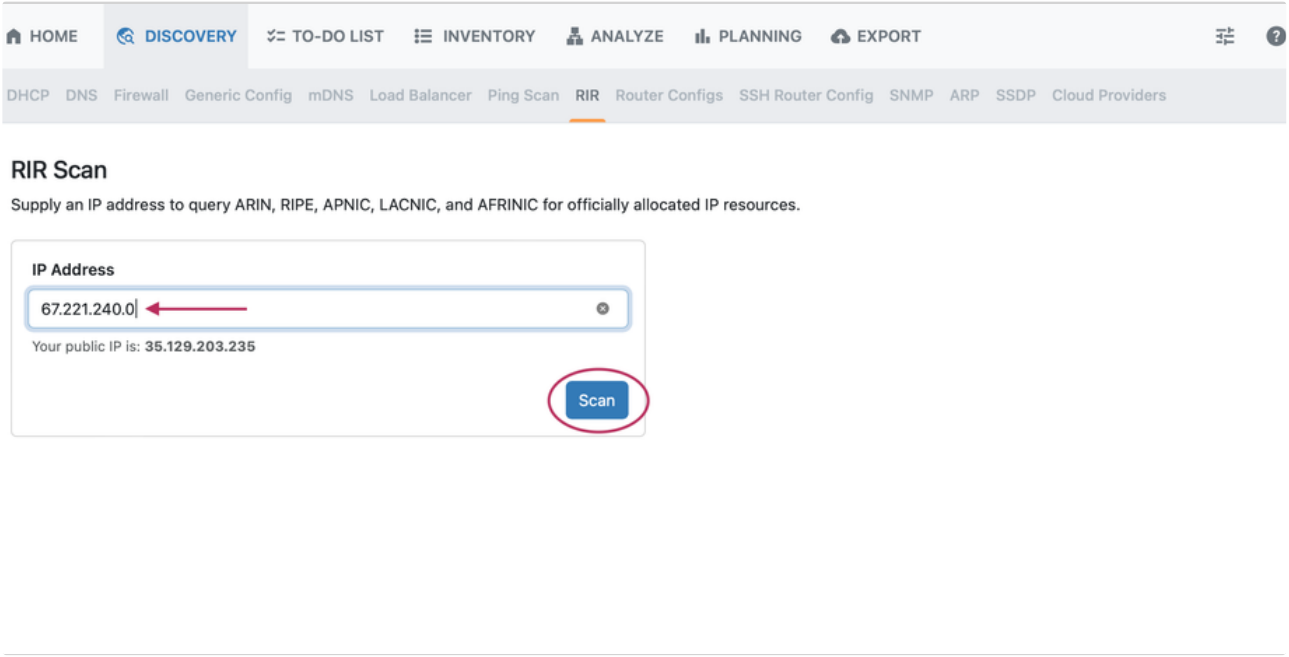
Discovery Tab Options

RIR

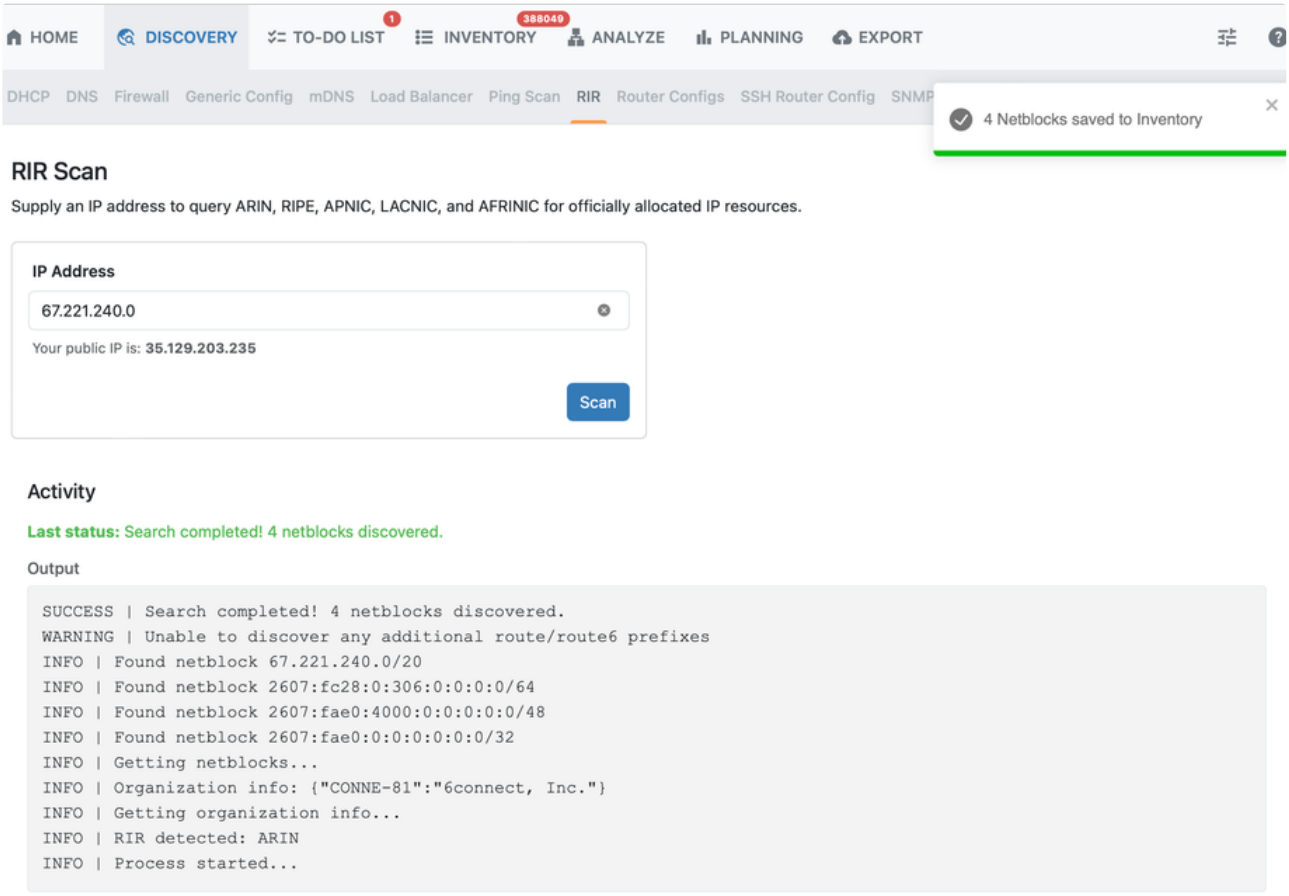
RIR Scan is the recommended first step in discovering your network assets.

RIR discovery establishes a baseline of public space. From here, ReView will use the current user's IP / provided IP, and then query the WHOIS system to find its ASN. From there, it queries again in order to discover netblock allocations.

When you open RIR Scan, your public IP is automatically populated, though you may also manually enter an IP.



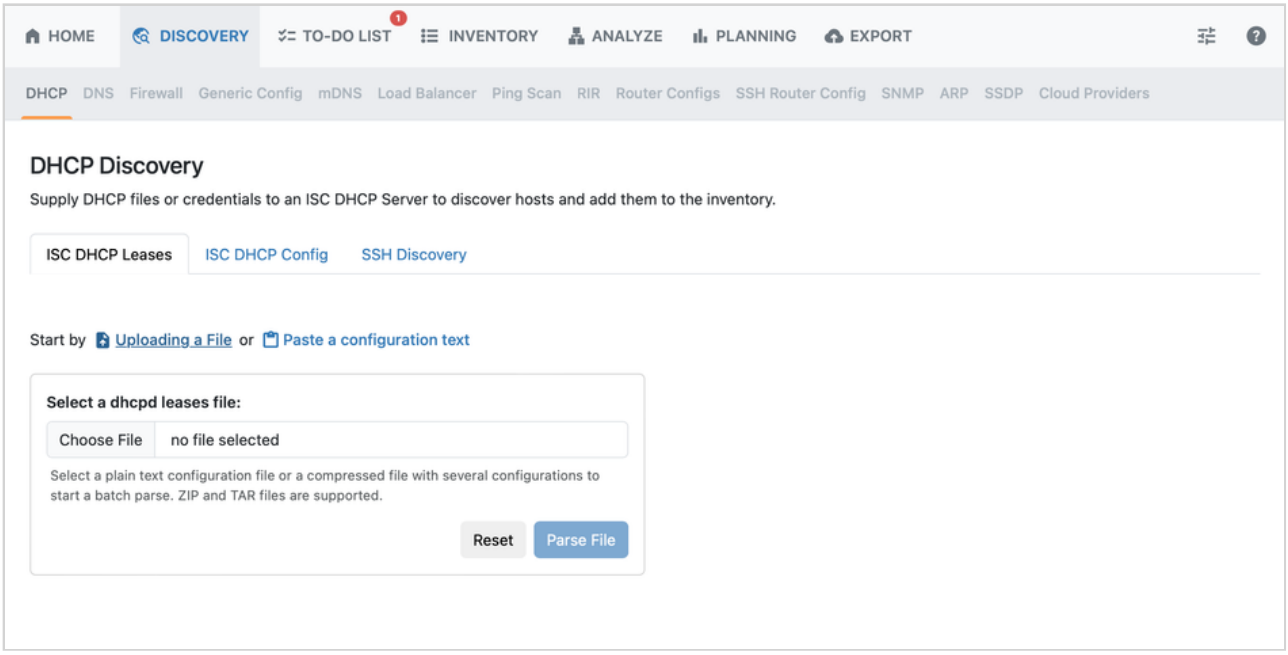
Enter the desired IP address and click “Scan”.



After a successful scan, flags will appear on the To-Do List and Inventory tabs to indicate pending actions.

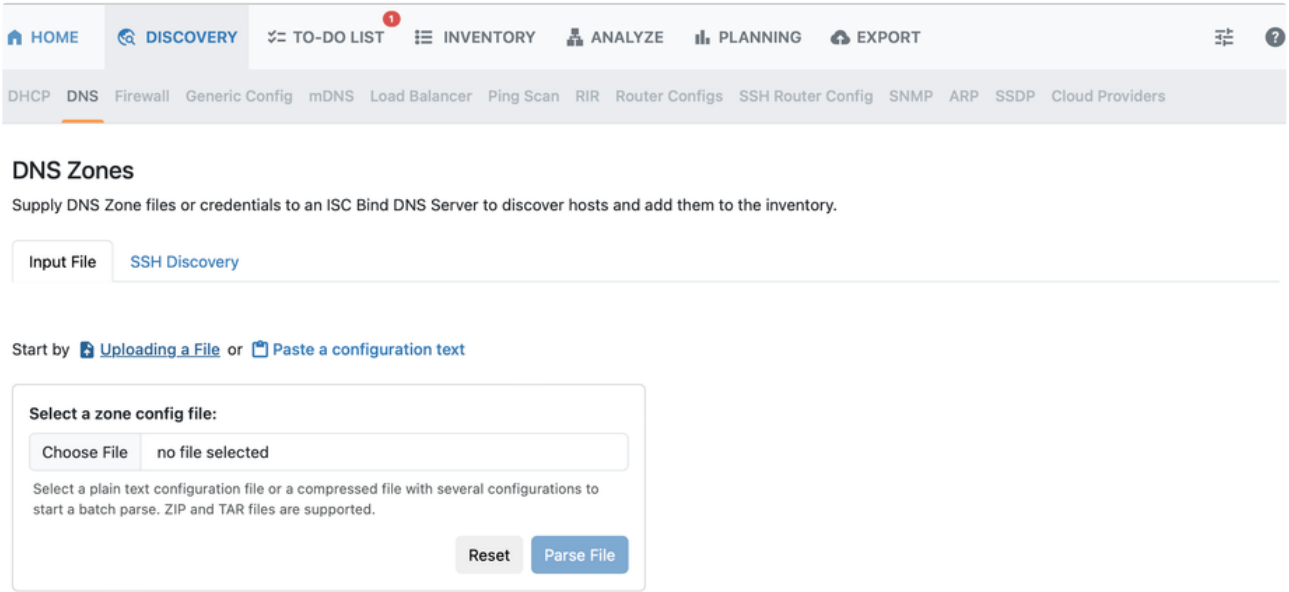
DHCP

Connects to DHCP usage logs. ReView uses this to determine whether allocated DHCP subnets can be shrunk. Currently supports ISC DHCP, though Microsoft support is expected in a future release.



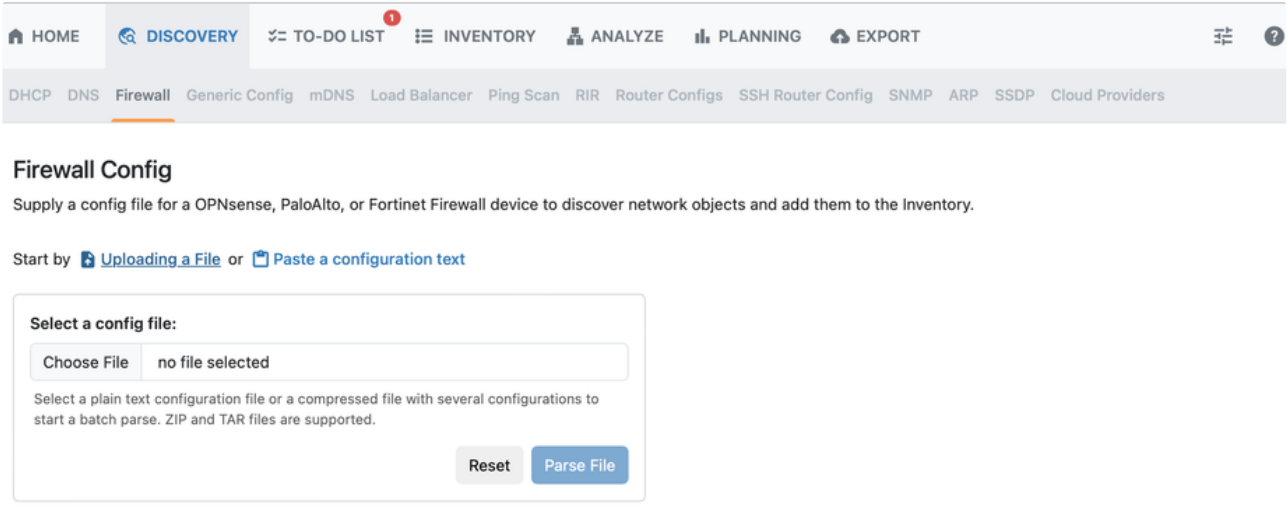
DNS

Supply DNS Zone files or credentials to an ISC Bind DNS Server to discover hosts. A config file may be uploaded or configuration text pasted directly into the text field.



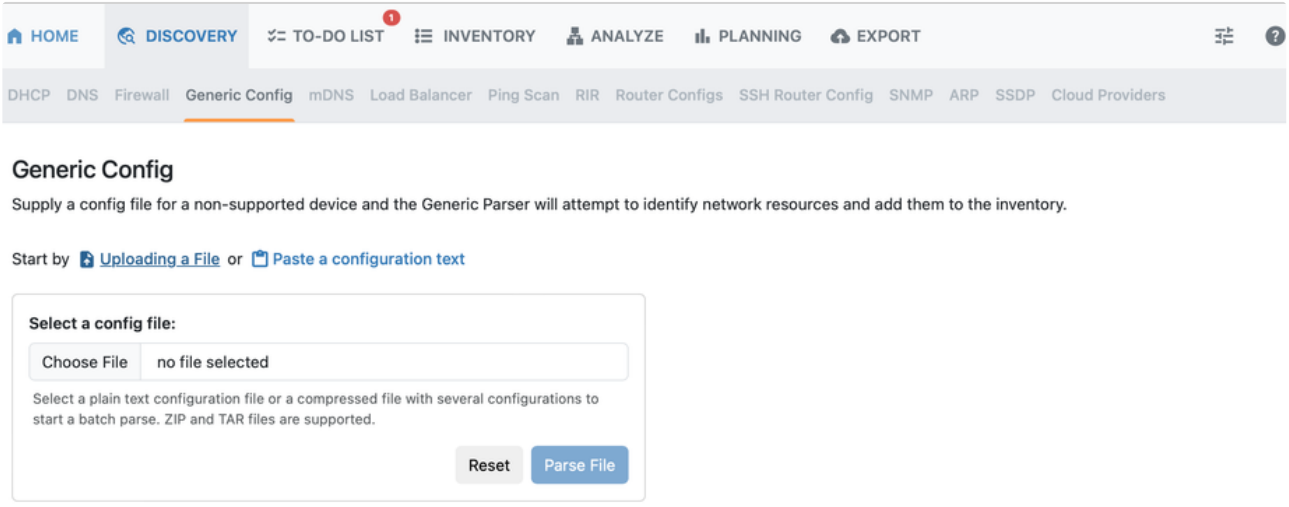
Firewall

Connects to Firewall configs (OPNsense, Palo Alto, Fortinet). A config file may be uploaded or configuration text pasted directly into the text field.



Generic Config

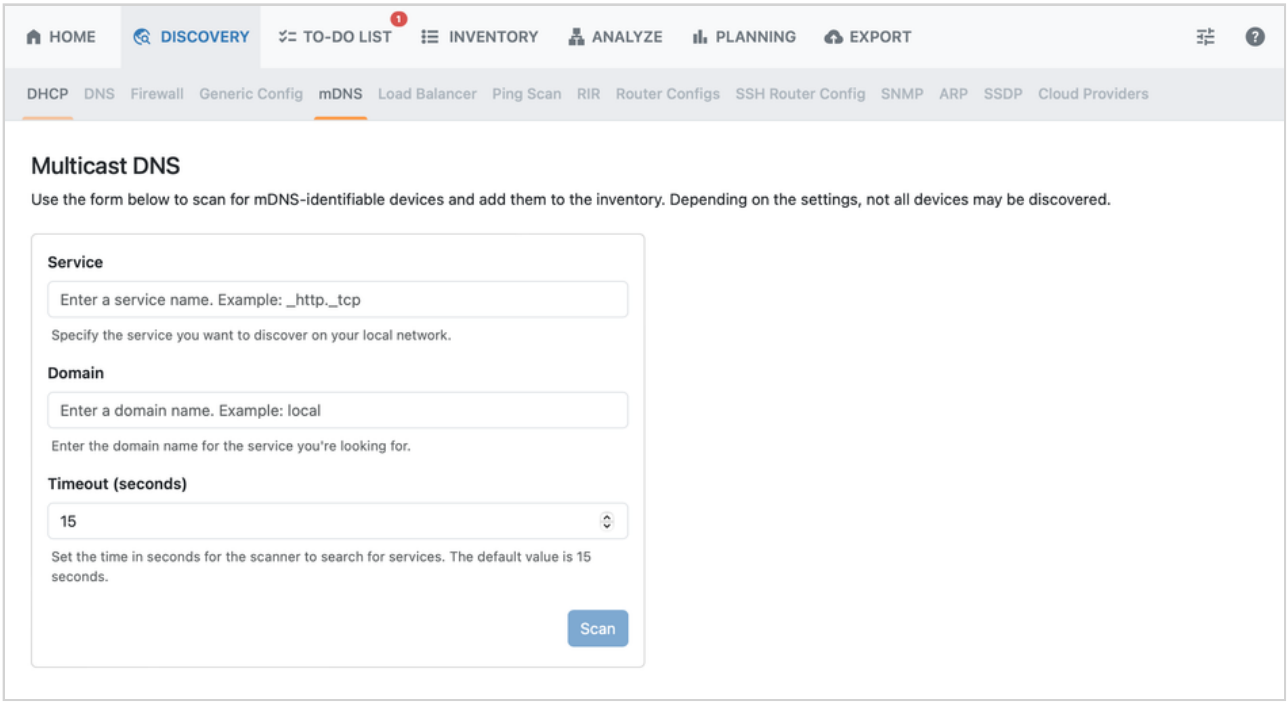
Attempts to parse non-supported devices via a config file in order to identify network resources and add them to the inventory.



---

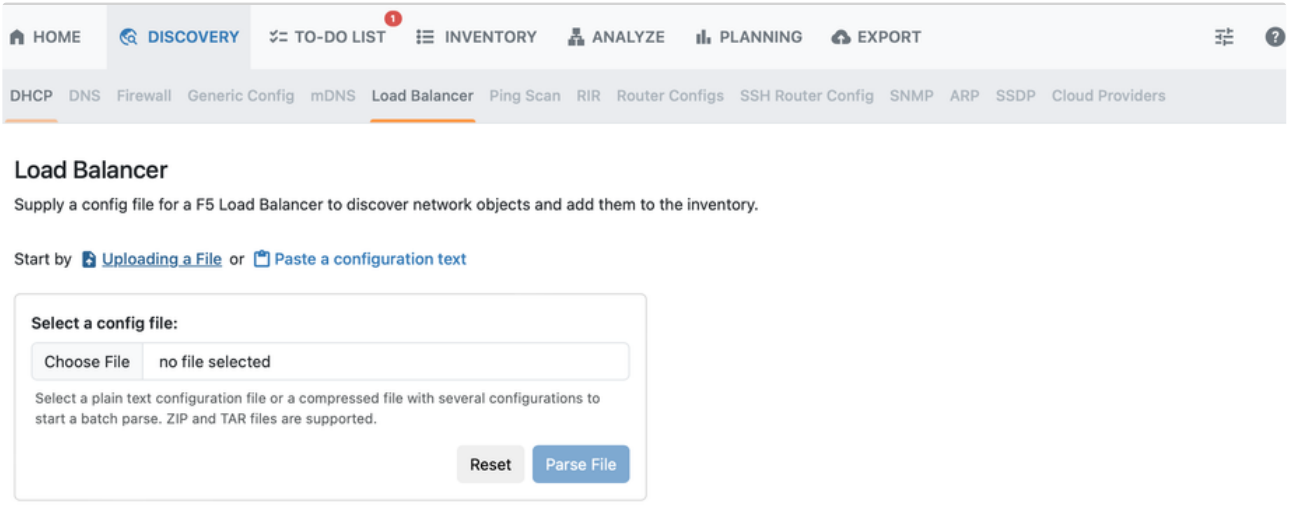
mDNS

Scans for Multicast DNS identifiable devices. Simply enter a service, domain, and a timeout (in seconds).



Load Balancer

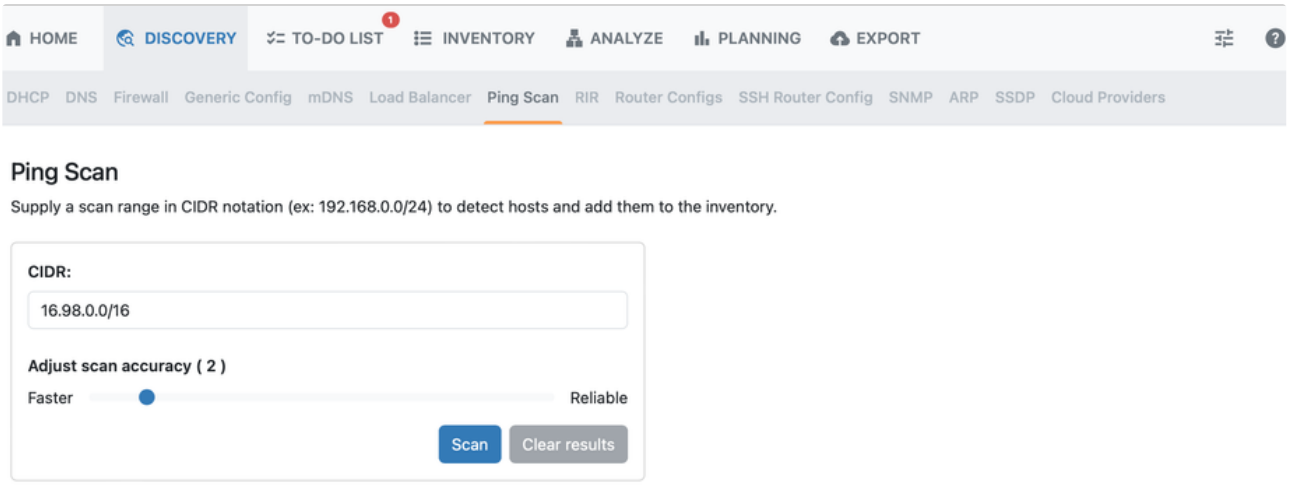
Connects to Load Balancer configs (F5). A config file may be uploaded or configuration text pasted directly into the text field.



Ping Scan

Enter a CIDR to detect hosts and add to the inventory. The scan can be adjusted via a slider to emphasize either speed or accuracy or balanced between the two options.

It is recommended to perform a ping scan after an RIR scan in order to discover individual hosts.



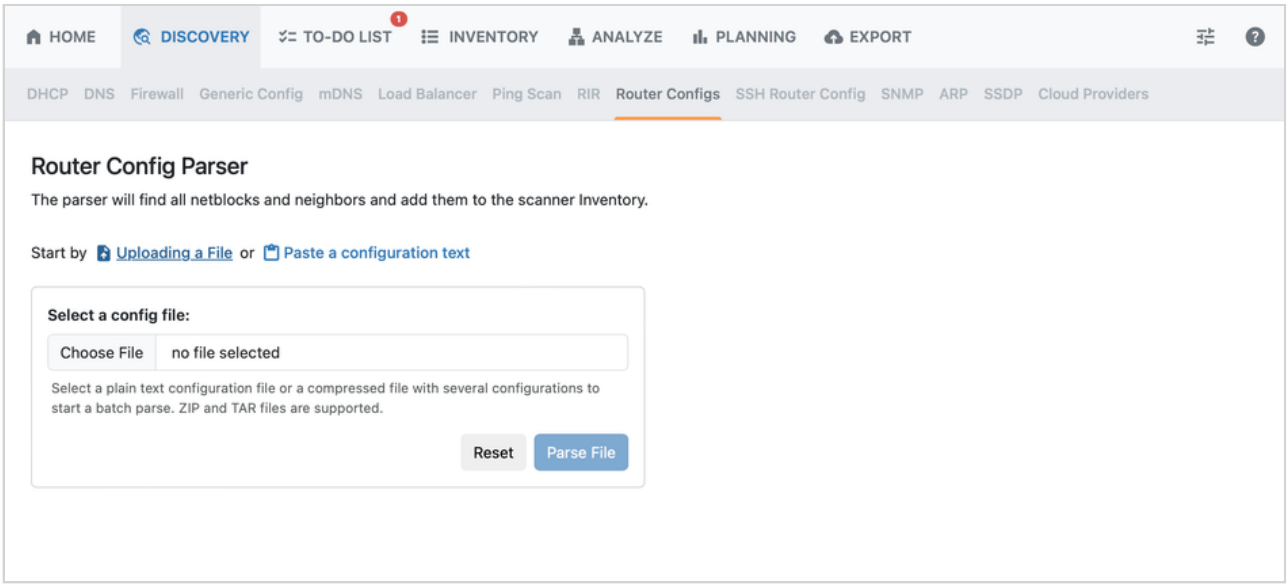
Router Configs

The Router Config page allows the user to either paste full router configs, upload a single config file, or provide an archive of files. ReView parses these configs for configured networks.

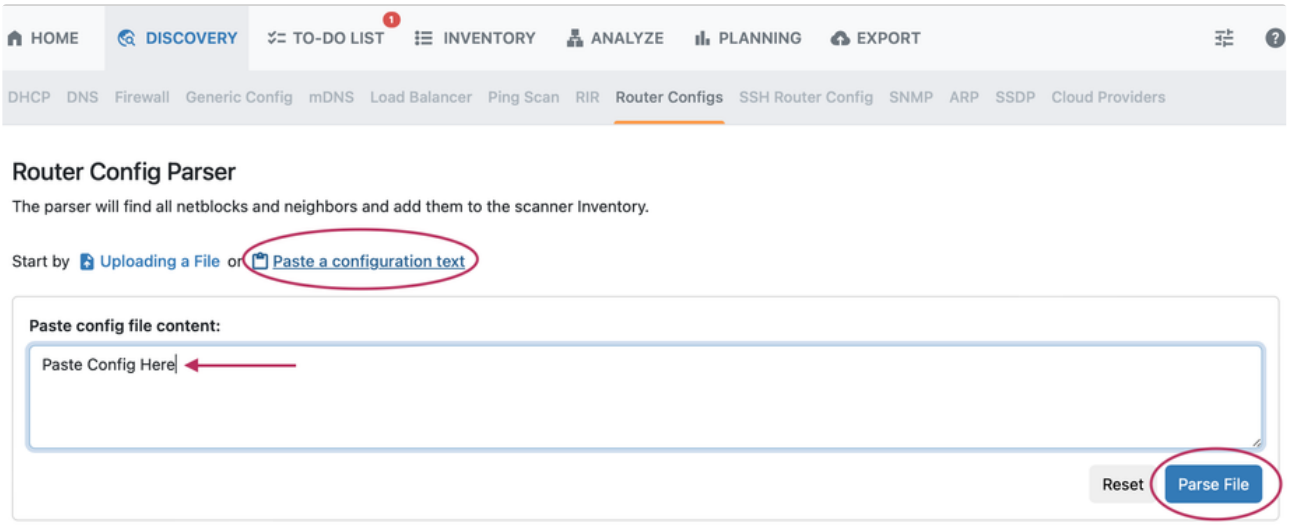
Currently supported router configs include the following:

- Cisco IOS
- Cisco IOS-XR
- Juniper
- Arista

To upload a config file, from the “Uploading a File” section; select a plain text configuration file or a compressed file with several configurations, and click “Parse File”.



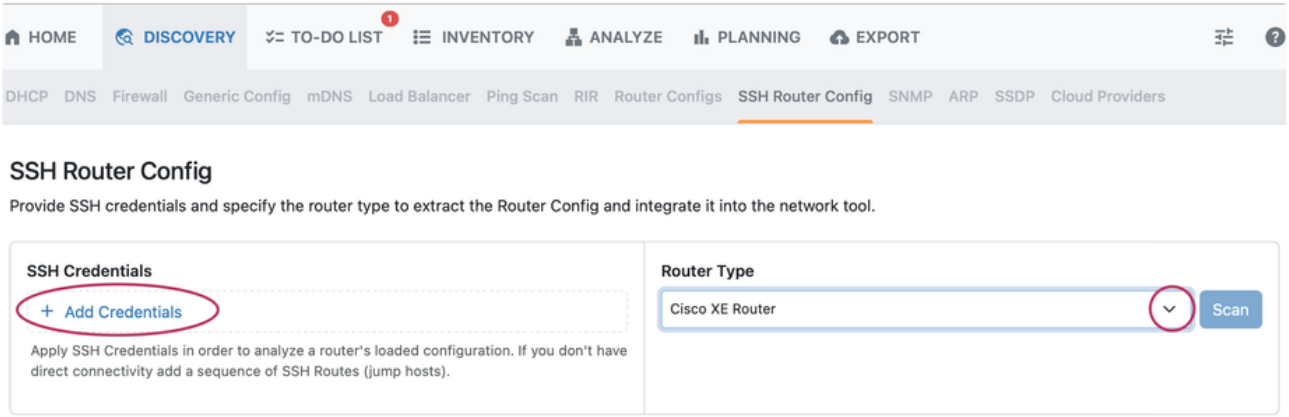
To paste a router config, select “Paste a configuration text”, paste your content, and click “Parse File”.



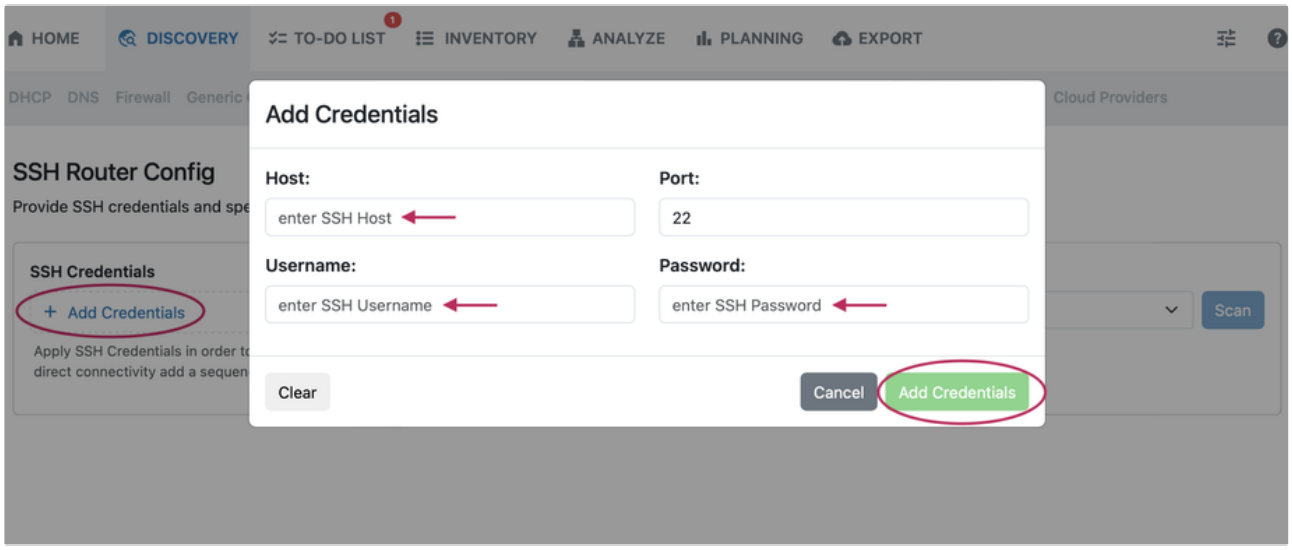
SSH Router Config

You may also provide credentials for a router, connect via SSH, and then extract the router config in order to integrate it into the tool.

Select a router type from the dropdown and then click “Add Credentials”.

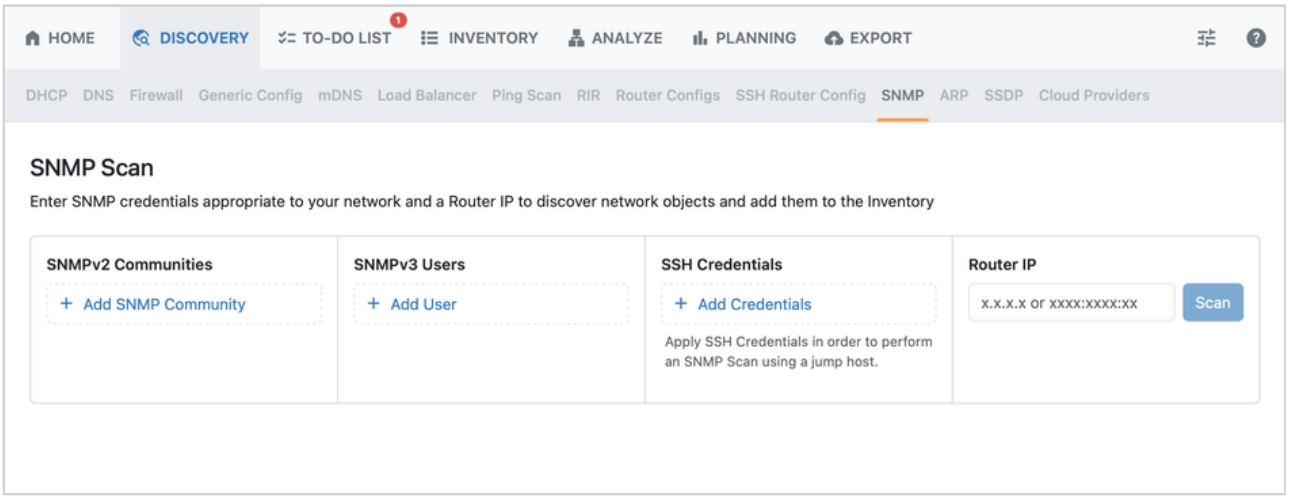


Enter SSH credentials in the resulting form and click the “Add” button.



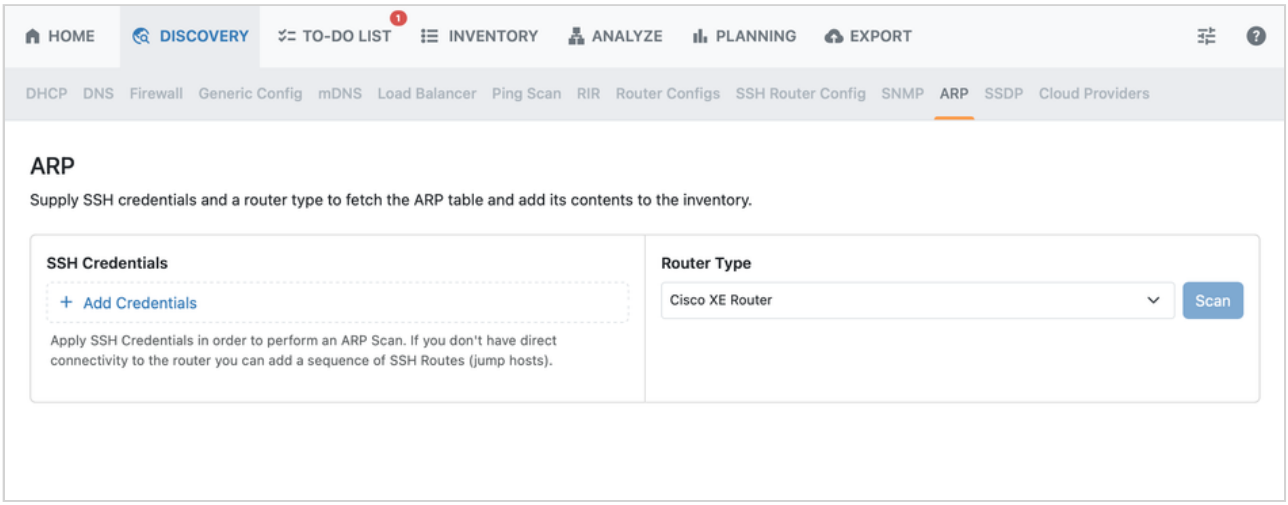
SNMP

To initiate an SNMP scan, enter credentials and a router IP.

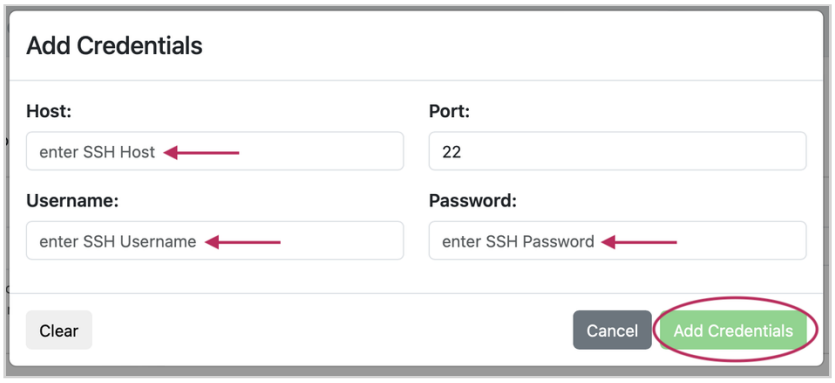


ARP

Supply SSH credentials and a router type to fetch the ARP table and add its contents to the inventory

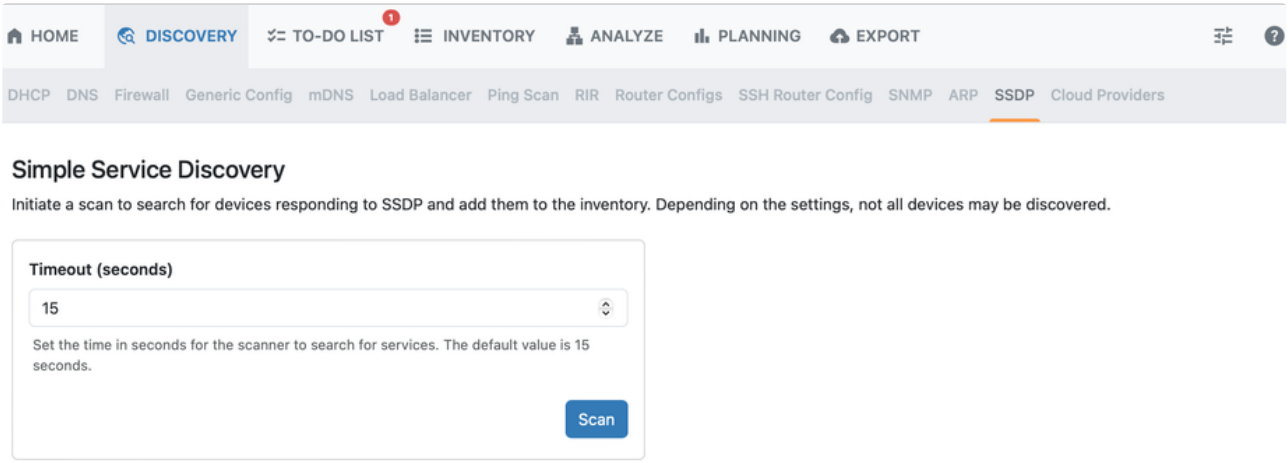


Select a router type and click “Add Credentials”. Enter credentials in the resulting form, and click the “Add” button.



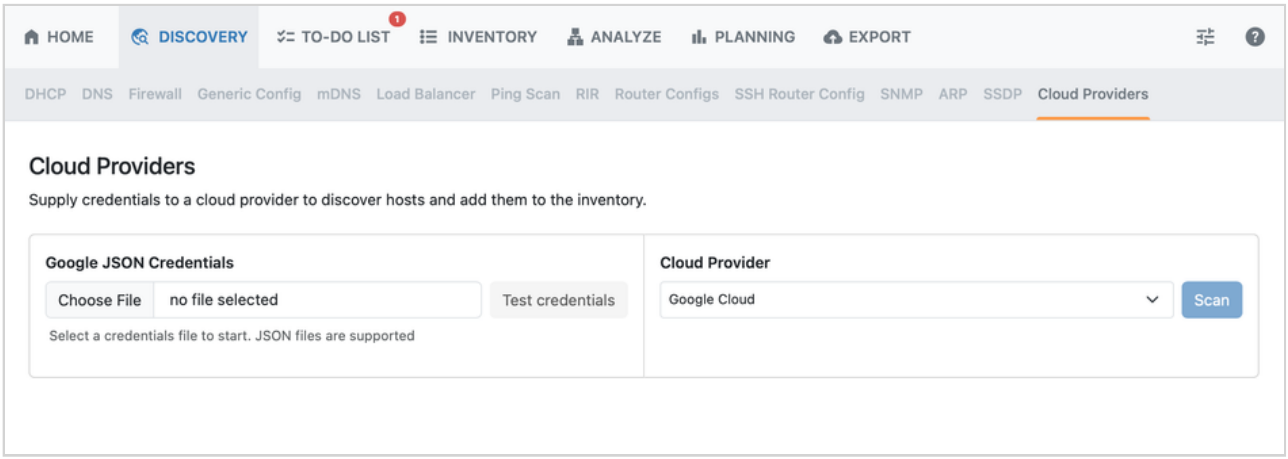
SSDP

Initiates a scan to search for devices responding to SSDP. The default timeout is 15 seconds.



Cloud Providers

Select a cloud provider and enter credentials to scan cloud provider hosts and add them to the inventory.

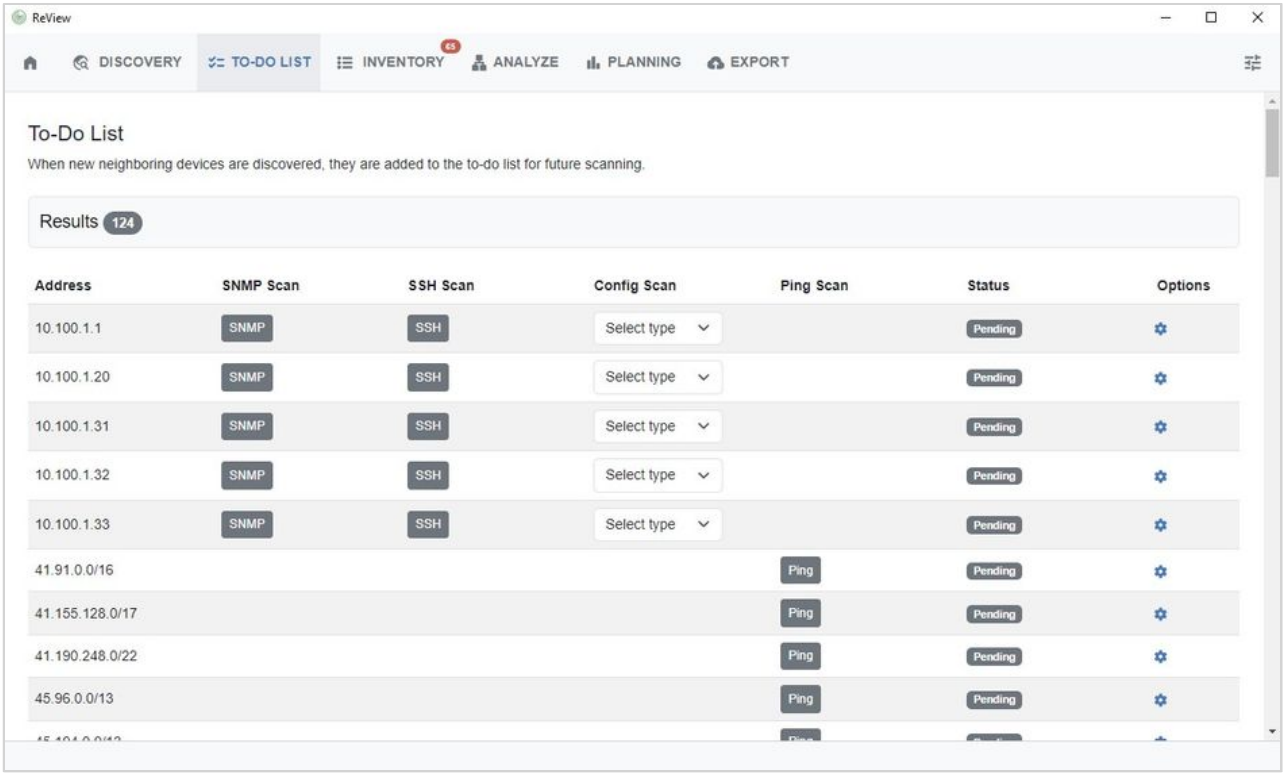


Next Steps

If neighboring devices have been discovered via the router config discovery option, those devices will be populated into the To Do List tab for further scanning.

Once one or more of the available Discovery modules has been processed, all found space will be loaded into the Inventory tab for display and auditing.

To-Do List

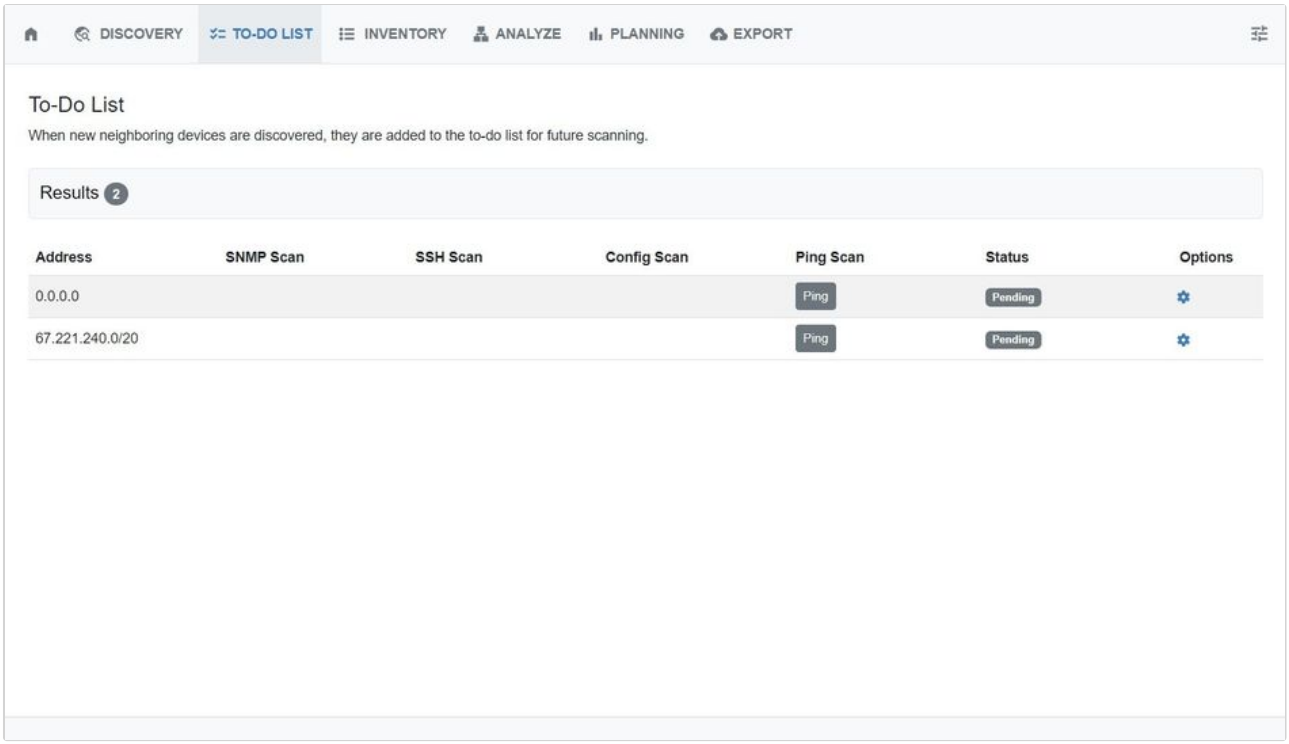


The To-Do list identifies and marks neighboring devices encountered during SNMP, SSH, router config, or ping discovery scanning. Users may then review, update the type of config scan, or mark with updated status flags.

Working with the To-Do List

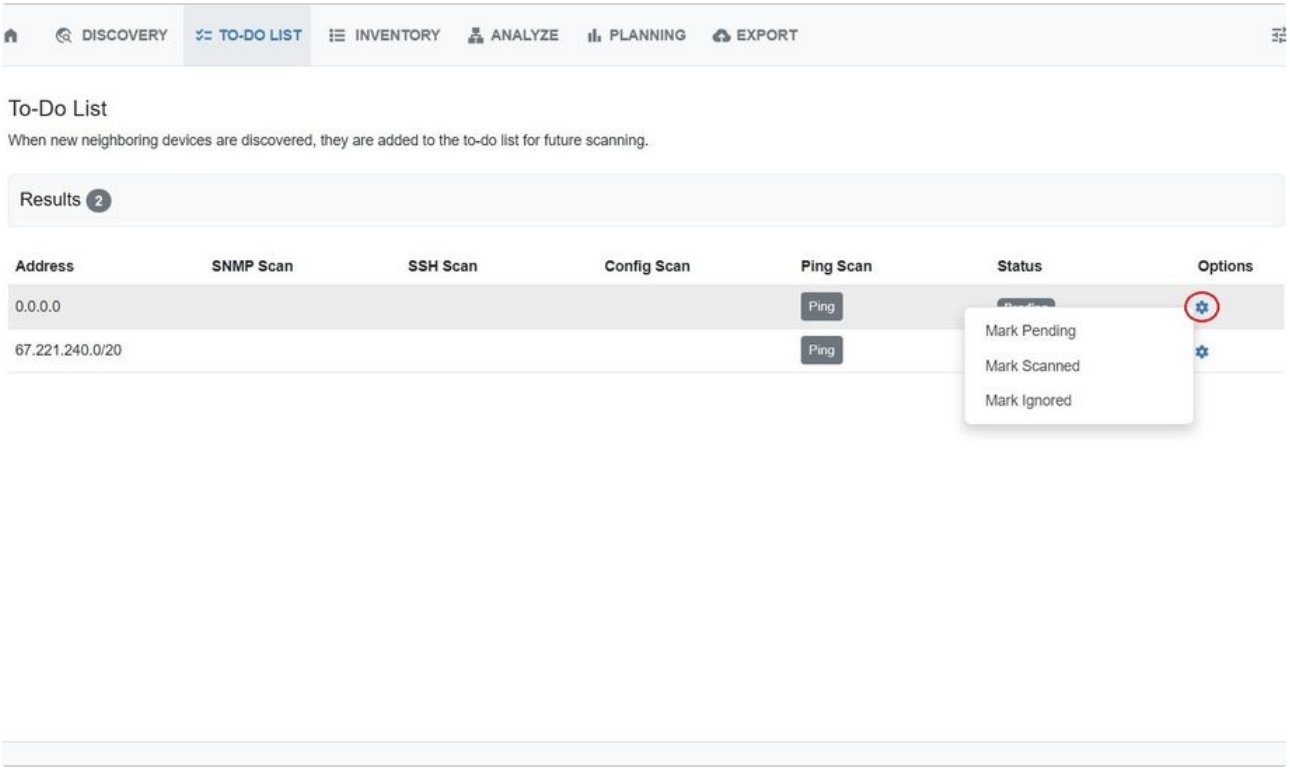
The To-Do list is only populated from discovery runs where SNMP, SSH, router config, or ping scans encounter new neighboring devices.

Once encountered, the address will be added to the list and the source marked (SNMP, SSH, Config, or Ping), so that users may return to the encountered devices to run additional scans, if needed.



Options

By default, the status of an encountered device is “pending”, serving as a reminder to review or scan the device. You may change the status at any time from the Options → Action menu (gear icon).

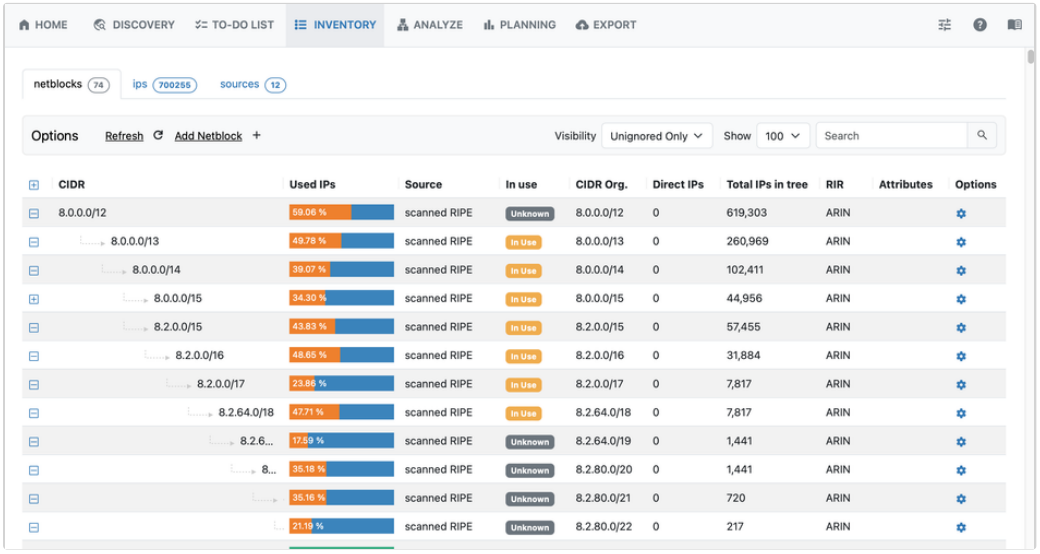


To mark the status of a device, right click anywhere on a row to open the Action Menu. You can choose from pending, scanned, or ignored.

Next Steps

Once the To-Do List items have been reviewed, scanned, or ignored as needed, proceed to the Inventory tab to review all netblocks, ips, and sources found during discovery.

Inventory

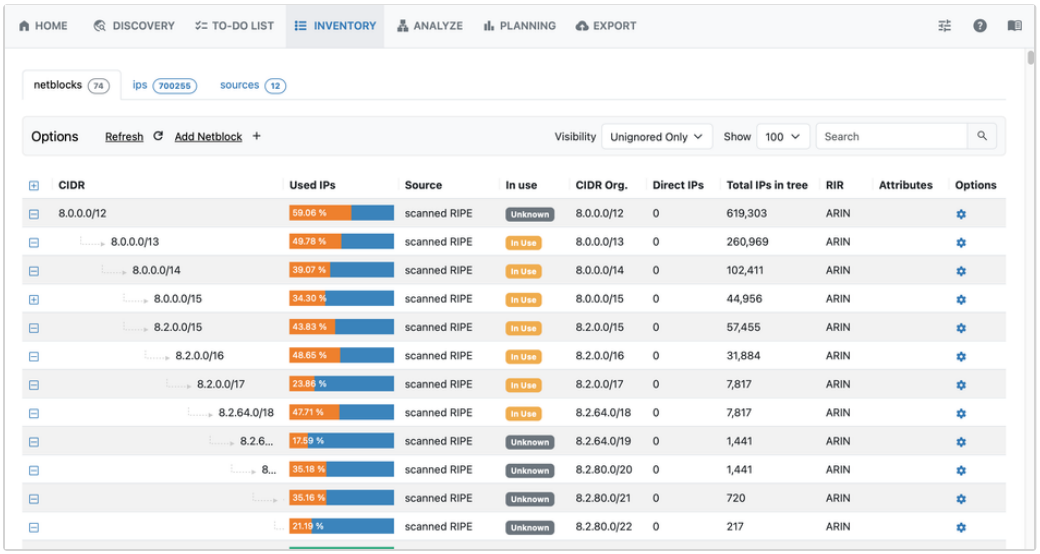


The Inventory tab displays an organized list of all discovered subnets, IPs, and associated metadata.

Here, for each netblock you can view RIR, Source, CIDR, use status, IPs found, total IPs, IP utilization, and start/end address.

Netblocks List:

Netblocks Tab



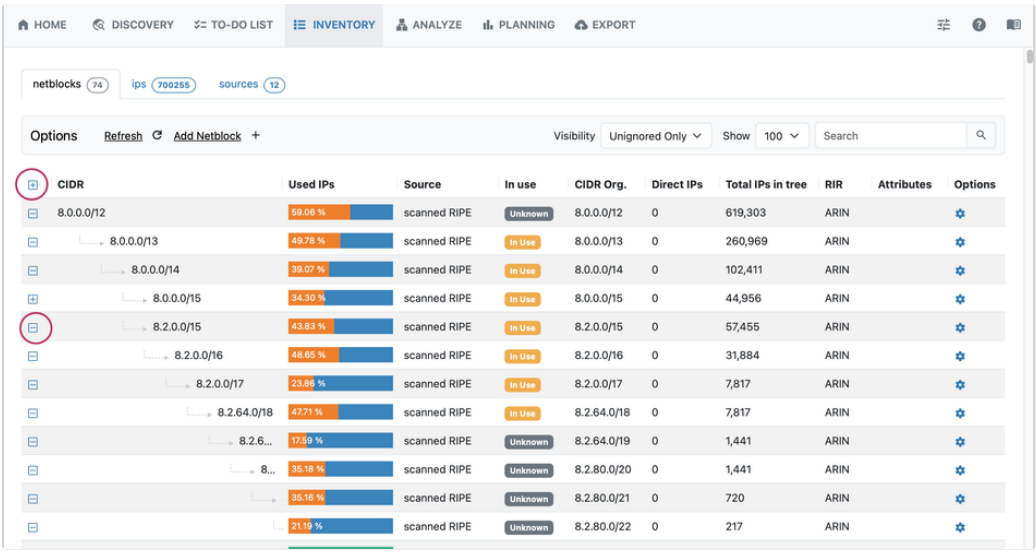
View Options:

The following view options are available in the Inventory list:

- Visibility: Select whether to view all netblocks/ips, ignored only, or unignored only.
- Show: Select the quantity of netblocks/ips to display per page.
- Search / Filter: Enter a CIDR or partial CIDR to filter to matching results.
- Column Resize: Column size may be manually adjusted by clicking and dragging on the vertical bar (pipe) between column headers.

Netblocks List Tree View:

Tree View shows child blocks in a hierarchy format. Click the +/- box next to the CIDR to expand or close the tree view hierarchy for the netblock.

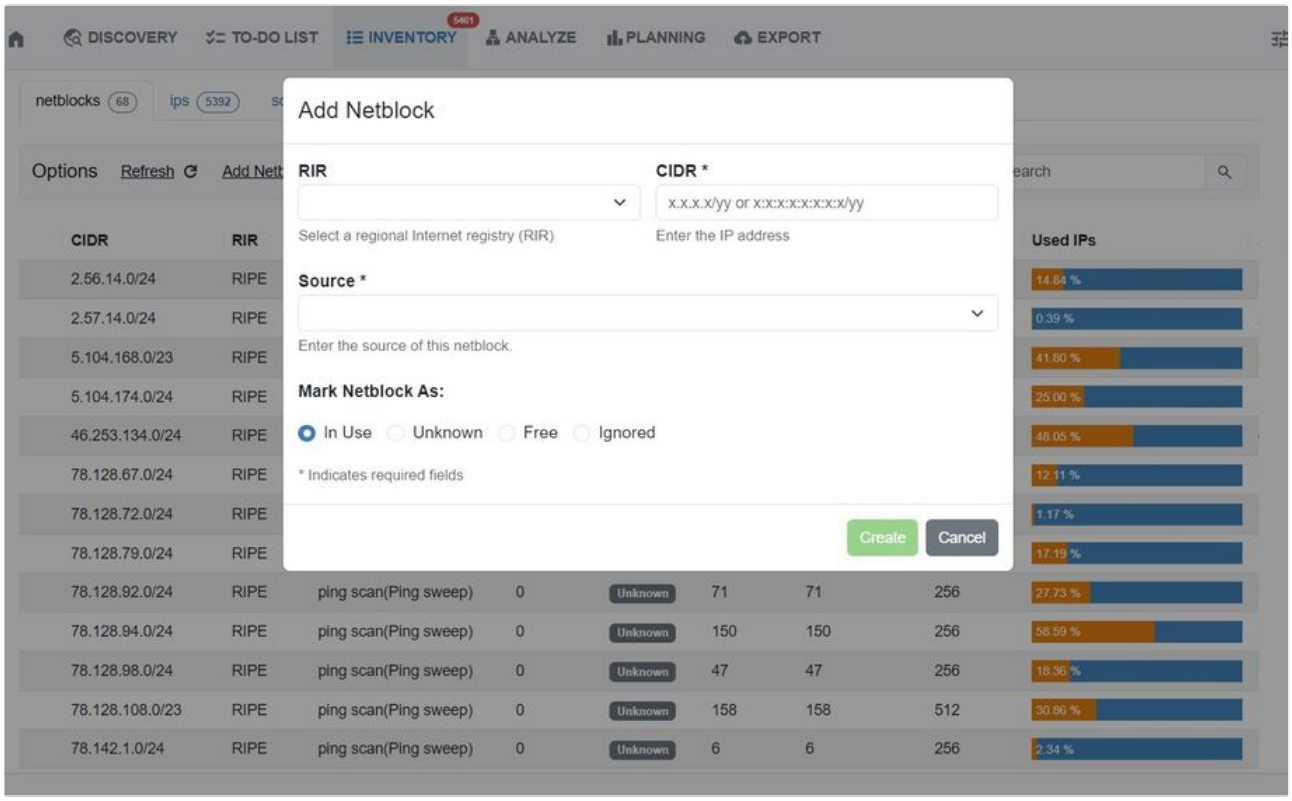


Refresh:

Click Refresh to check for updated data from the enabled sources.

Add Netblock:

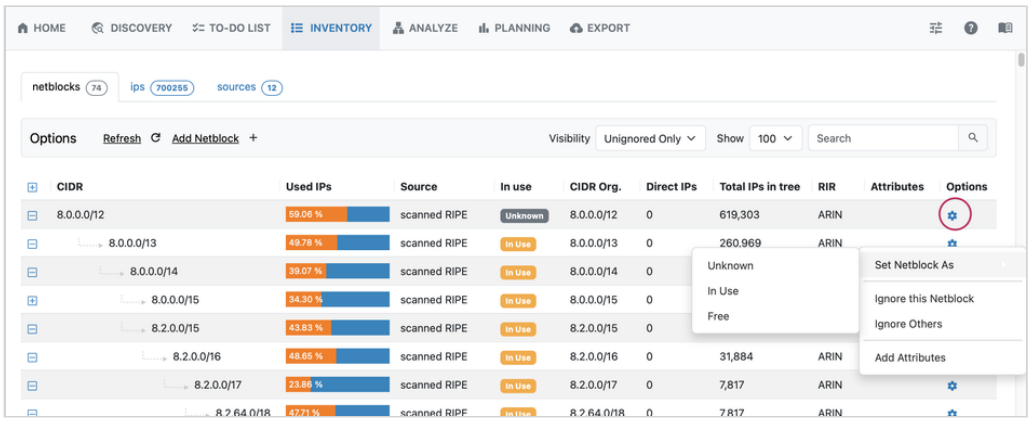
Click “Add Netblock” to manually add an undiscovered netblock to your inventory.



Select the RIR, enter the CIDR, and designate the source for the new netblock. If the netblock is known to be used, select the “In Use” radio to ensure that the proper status is associated with the netblock. You can also mark netblocks as Unknown, Free, or Ignored.

When done, click “Create”. The netblock will be added to inventory.

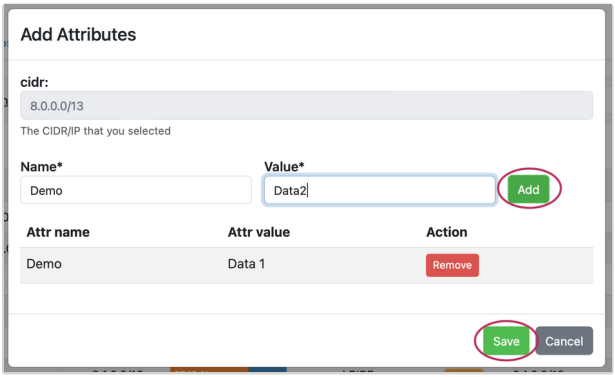
Netblock Options



For each netblock, the following options are available under Options → Action Menu (Gear Icon)

- Set status by selecting “Set Netblock As” and then choosing:
  - Unknown
  - In Use
  - Free
- Ignore this Netblock
- Ignore Others
- Add Attributes

- Add or edit attributes by selecting “Add Attributes”, entering the name-value pair, then click “Save”. You may also remove existing attributes by clicking “Remove” next to the desired attribute.

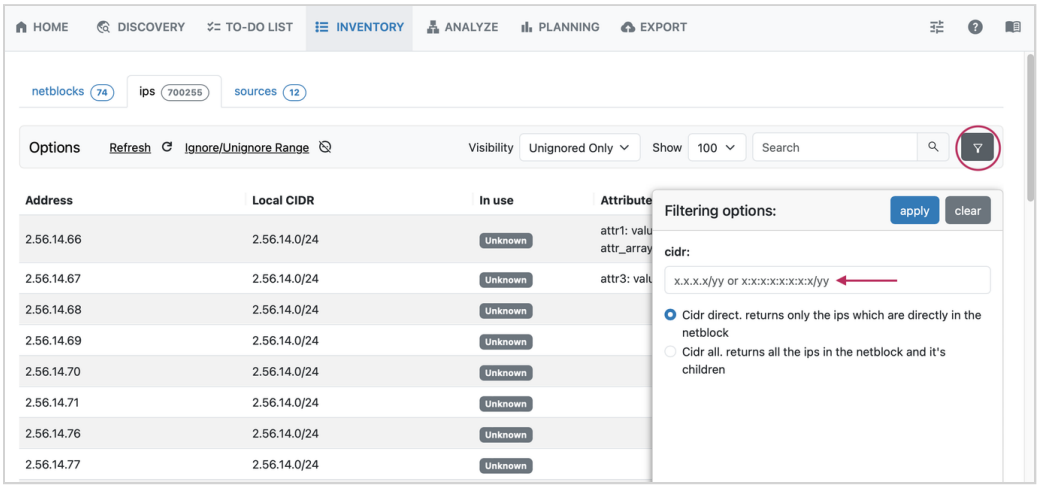


IPs Tab

View Options

The ips tab displays individual ip assets discovered during scanning, for user review. It contains the same view options as the netblocks tab - visibility, display count per page, and search/filter.

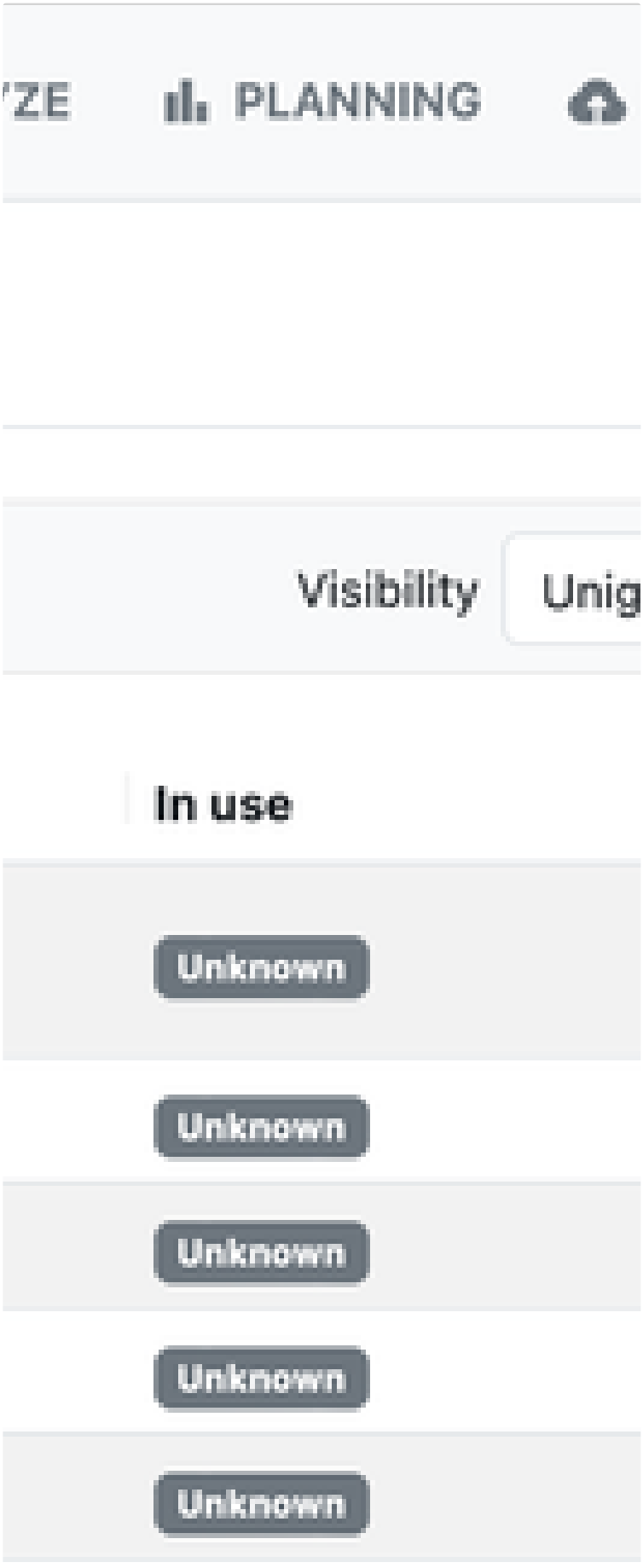
Additional CIDR-specific filtering options are available by clicking the filter icon next to the search box.



Enter the CIDR to filter to, and select one of the following options:

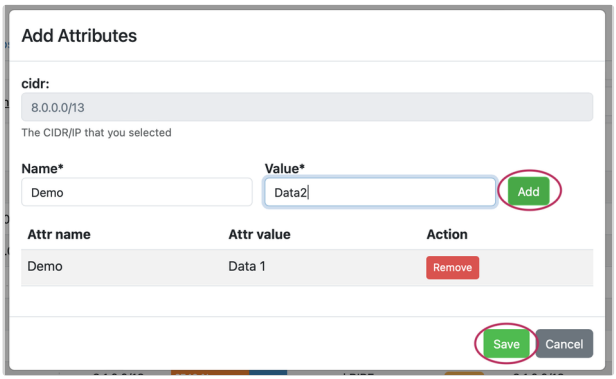
- CIDR direct: Returns only the ips which are directly in the netblock
- CIDR all: Returns all of the ips in the netblock, and its children

IP Options


'ZE
PLANNING
Visibility
Unig
In use
Unknown
Unknown
Unknown
Unknown
Unknown

To set the visibility status of an IP, right click anywhere on a row to open the Action Menu and select the desired option.

For each IP, the following options are available under Options → Action Menu (Gear Icon)

- Set visibility by selecting:
  - Ignore this IP
  - Ignore Others
  - Unignore Others
- Add Attributes
  - Add or edit attributes by selecting “Add Attributes”, entering the name-value pair, then click “Save”. You may also remove existing attributes by clicking “Remove” next to the desired attribute.
    - 

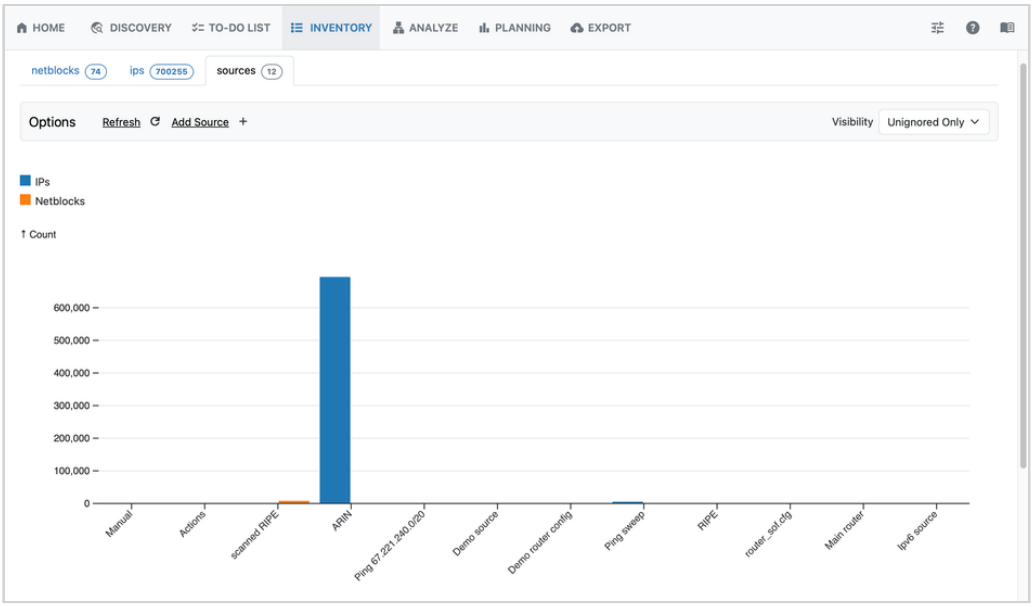
- Scan for Open Ports

Refresh

If data has changed due to additional scans, click “Refresh” to update the list.

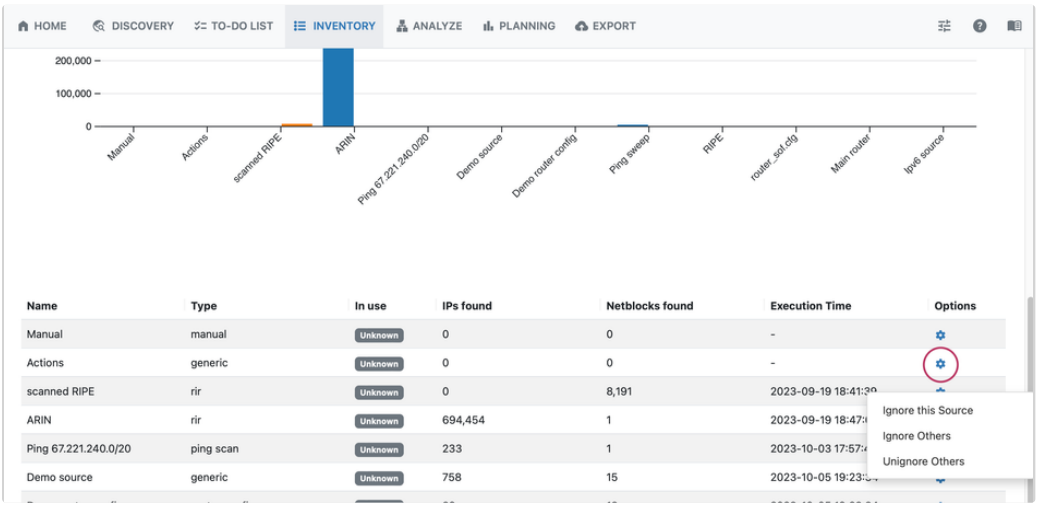
Sources Tab

The Sources tab displays a chart of the discovery tab configurations used to populate and update the inventory tab. Select which sources to view by visibility status via the dropdown at upper right.



Here, you may review sources and their associated count of netblocks found.

Scroll down to view the list of sources and associated data.



For each source, the following options are available under Options → Action Menu (Gear Icon)

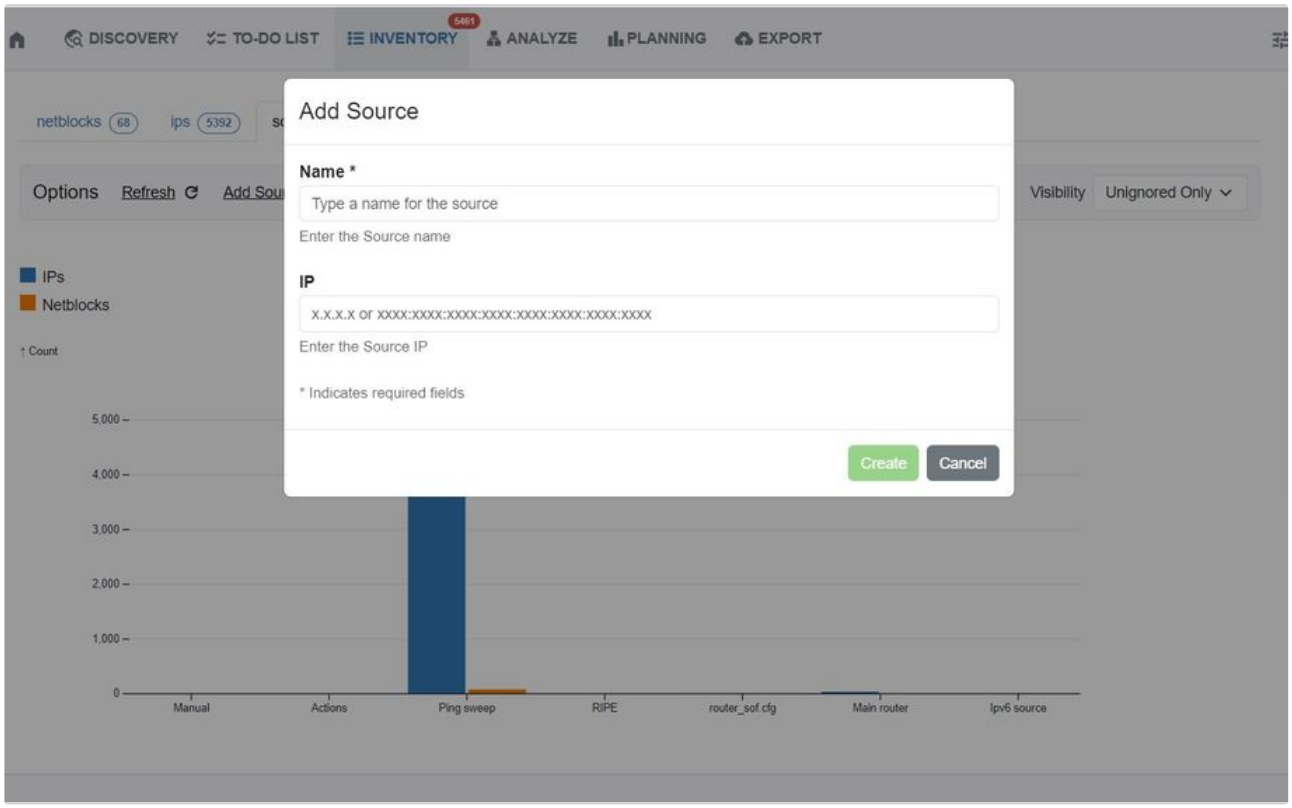
- Set visibility by selecting:
  - Ignore this Source
  - Ignore Others
  - Unignore Others

Add Source:

If needed, you may add additional sources not found during discovery scans.

Click “Add Source” to manually add a source.

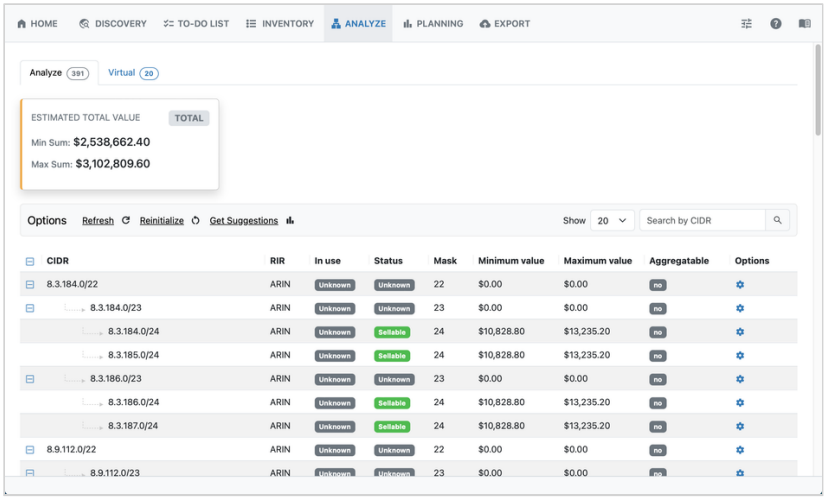
Enter the Name and IP, then click “Create”.



Next Steps

After reviewing and adjusting your inventory and sources as desired, proceed to the Analyze tab to view free space and valuation based on your current network.

Analyze



The Analyze tab interprets the IP inventory data found during Discovery, and determines valuation of free IPv4 space based on the current network structure.

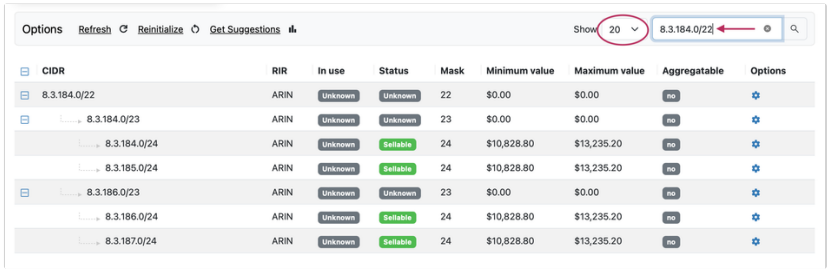
Analyze Blocks List

The Analyze tab Blocks List displays block inventory according to CIDR. It displays use status, sellable status, aggregatable status, and estimated min/max value of sellable space.

List Display options include the following:

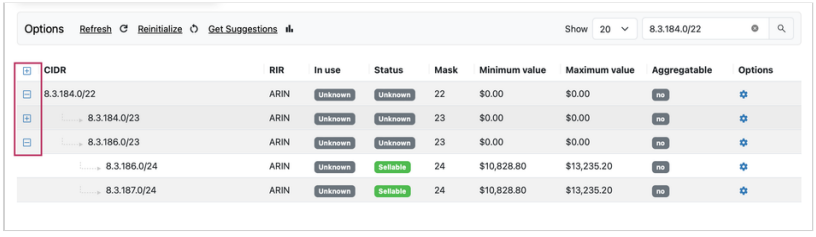
Filter / Search List:

At the top of the list, you can select the number of blocks to view per page (default is set to 20), and search/ filter for blocks.

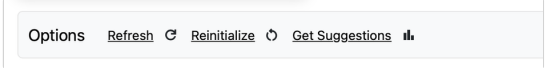


Tree View:

Tree View shows child blocks in a hierarchy format. Click the +/- box next to the CIDR to expand or close the tree view hierarchy for the netblock.



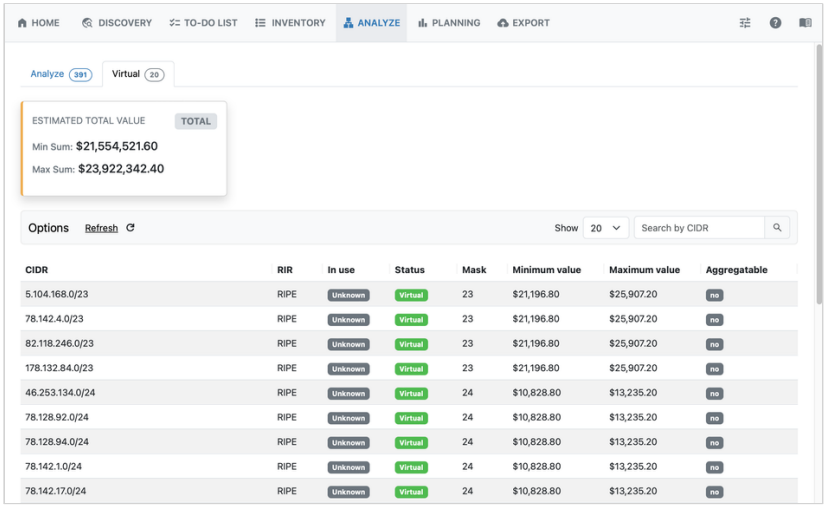
List Options



List management options are available in the top header of the analyze list view:

- Refresh: Refreshes the list data from the database.
- Reinitialize: Performs a more intensive re-analysis of data and status from provided sources - this may take some time, depending on the amount of blocks in inventory and sources.
- Get Suggestions: Provides optimization strategies based on the current use and status of the netblocks. Suggestions may be saved as a named optimization plan to compare against additional suggested plans under the Planning tab.

Virtual Blocks Tab



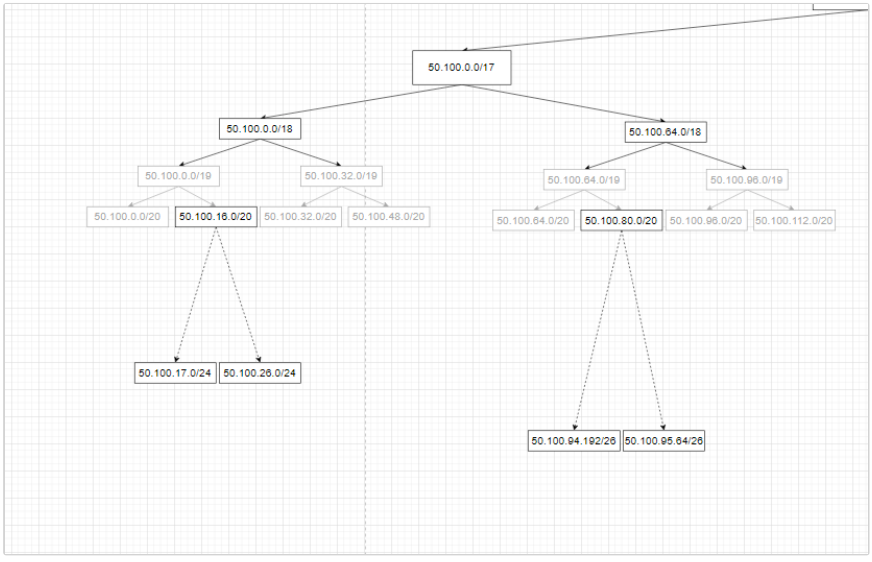
The Virtual tab displays blocks that are not directly created or in use, but are inherited subnets under the netblocks discovered by scans. These blocks have an estimated total value based on the full netblock mask being free. Virtual blocks which have real children are not sellable.

Virtual Blocks: Example

In this example, we use a /17 at the top of the block tree, split down to eight /20s, with one /20 split down into two /24s, and another into two /26s on the other side of the tree.

In this diagram, the “real” created netblocks are displayed in black - these are the netblocks that would be displayed in the Analyze tab - Blocks list. These blocks may or may not be sellable, depending on use status and whether IPs exist under them.

The lighter grey blocks - the /19s and remaining /20s - are virtual blocks. They have not been created as “real” blocks, but can be inferred based on the ownership of the parent /18s and tree structure.



Virtual Blocks vs Real Blocks example diagram

Virtual Blocks and Sellable Status

In our standard Blocks list tab, if our example /20 with the /24 from it contains 50 IPs, none of the real netblocks are considered sellable - the /20 is not a leaf and the /24 (although it is a leaf) has IPs in it. This would result in a $0 value estimation for the known existing blocks - which is not accurate when considering the entire tree structure. The /20 has many other netblocks under it which are not created or in use, and thus are free to be sold. These "not created" netblocks are displayed under the Virtual tab in ReView.

Virtual netblocks which have real children are not sellable, but those that are fully free without real children may be sellable. These show in the Virtual Blocks tab with an estimated value based on the full mask value being free.

Under our example parent block CIDR 50.100.16.0/20, the parent masks (/21, /22, /23) of our /24s - 50.100.17.0/24 and 50.100.26.0/24 - are not sellable, due to the /24s being real children. The same would apply to the parent blocks between our 50.100.80.0/20 and /26s on the other side of the tree. The remaining virtual blocks without real child blocks, however, would be sellable in this example.

Working with the Analyze Tab

Before You Begin

The Analyze tab interprets the netblock information gained from the Discovery and Inventory tabs and then combines that data with current available pricing estimations to provide an as-is valuation of free blocks.

Here are some steps that should be completed to ensure the Analyze tab has the best possible data available to determine pricing.

1. Ensure that Discovery steps are complete - double check that sources, devices, ping scans, etc have been comprehensively added to discovery and cover the desired extent of your network.
2. Go through the To-Do List tab and verify listed blocks have been scanned or ignored as needed.
3. Confirm blocks under the Inventory tab have the correct use status flags (in-use, free, unknown, ignored) assigned, and that any non-discoverable netblocks under consideration have been manually added to the Inventory List.

Once the data has been confirmed, you're ready to work under the Analyze tab!

Step 1: Review Netblock Status

The Analyze list is populated with netblocks which have been marked as unused or unknown, and are sellable or potentially sellable blocks.

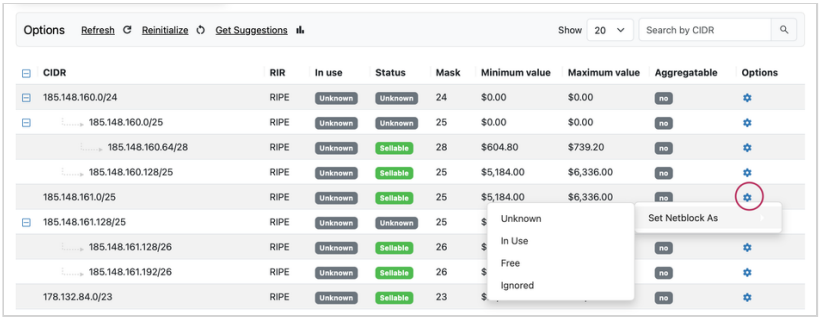
Sellable blocks: Blocks are considered "sellable" if they meet one of these conditions

- are marked as "Free"
- are leaf only netblocks with "Unknown" status, and no IPs in them

In this tab, it is best to review netblock status (in-use, free, unknown, ignored) to confirm the correct status was assigned under the Inventory list.

Update Netblock Use

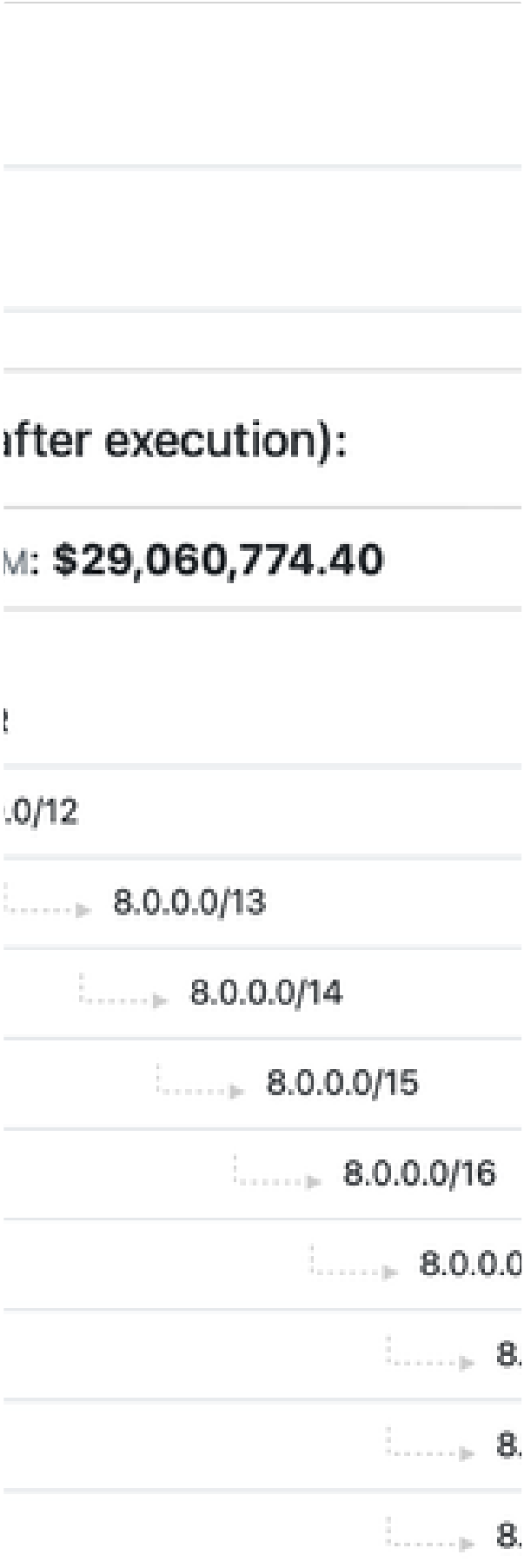
To make changes to the use status of a block, right click anywhere on a row to open the Action Menu and select to mark netblock use as unknown, in use, free, or ignored.



To make changes to the use status of a block, right click anywhere on a row to open the Action Menu and select to mark netblock use as unknown, in use, free, or ignored. The marked use will be considered when determining sellable status, valuation estimates, and optimization suggestions.

Step 2: Get Suggestions

Get Suggested Plan



Once netblock use status has been reviewed for accuracy, click “Get Suggestions” to see optimization strategies (Note: Depending on the size of netblock inventory, the suggested strategy may take a minute to load).

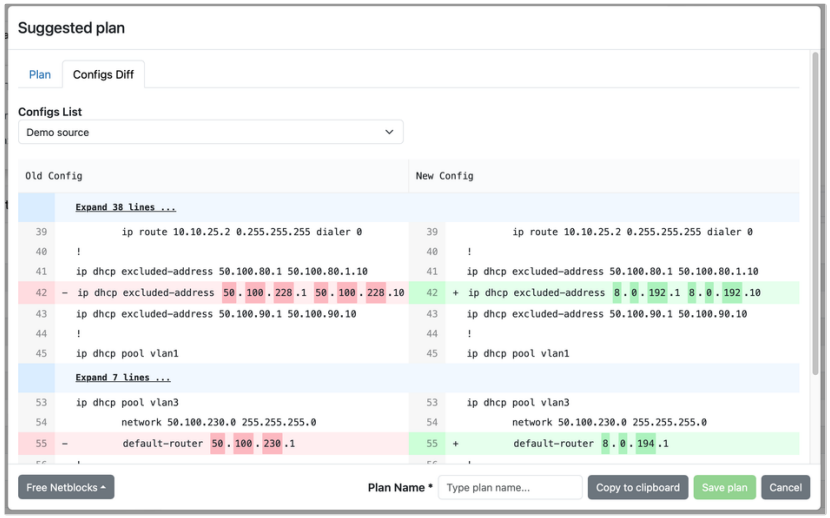
Get Suggestions displays three panels and their associated values:

- Network structure before plan - This shows the network structure as currently discovered, with pricing estimates based on keeping sellable blocks as-is at their current hierarchy location and size.
- Results (after execution) - This shows the network structure optimized to locate as many sellable blocks as possible contiguously, within the current structure strategy. This consolidates as many sellable blocks as possible, without otherwise making changes to the network structure.
  - The Optimization algorithm takes the following steps, generally:
    - Remove empty leaves
    - Shrink netblocks
    - Renumber netblocks, while preserving the number of levels as originally structured
  - If the structure - after removing empty leaves- was 4 levels, after optimization it will have 4 levels as well, with each parent containing exactly the same number of children.
  - This plan should be applicable to the existing network of the customer as we preserve parent-child relations.
- Minimal Structure - Minimal structure proposes the greatest possible consolidation of sellable blocks, including minimizing the existing network hierarchy and reallocating assignments to only use the fewest blocks needed. This allows for far greater availability of contiguous sellable blocks, larger masks, and higher profit potential, but may not be realistically applicable to some needs.
  - The Minimal Structure algorithm takes the following steps:
    - Get only the leaves with IPs in them
    - Remove all intermediary netblocks
    - Consolidate to a single parent

After getting the suggested plan, you may opt to review the Config Dif or the list of free netblocks.

Config Dif

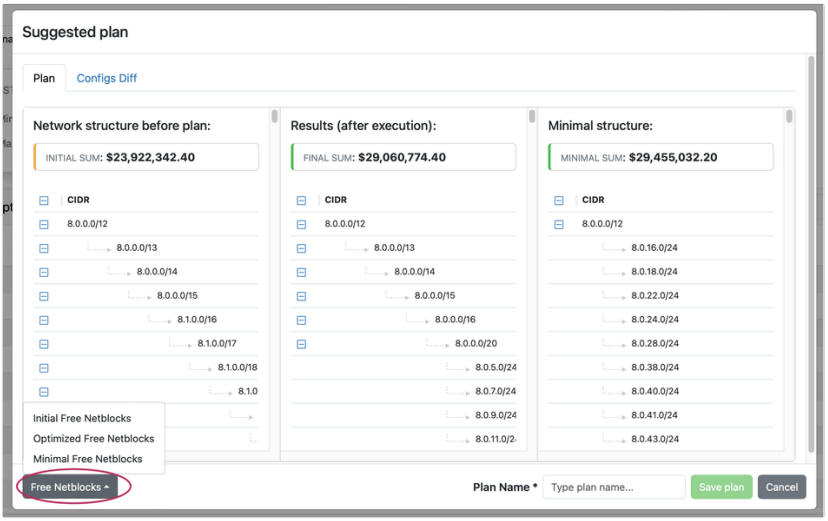
Click the “Config Dif” tab under Get Suggestions to review a detailed list of configuration differences between the current state and suggested plan. This will assist in implementing the suggested plan.



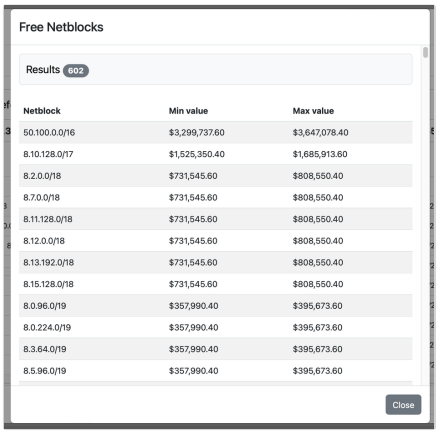
You may save the plan, copy it to clipboard, and view free netblocks.

Free Netblocks

Click on “Free Netblocks” and select a plan strategy to view a list of free netblocks under the plan.

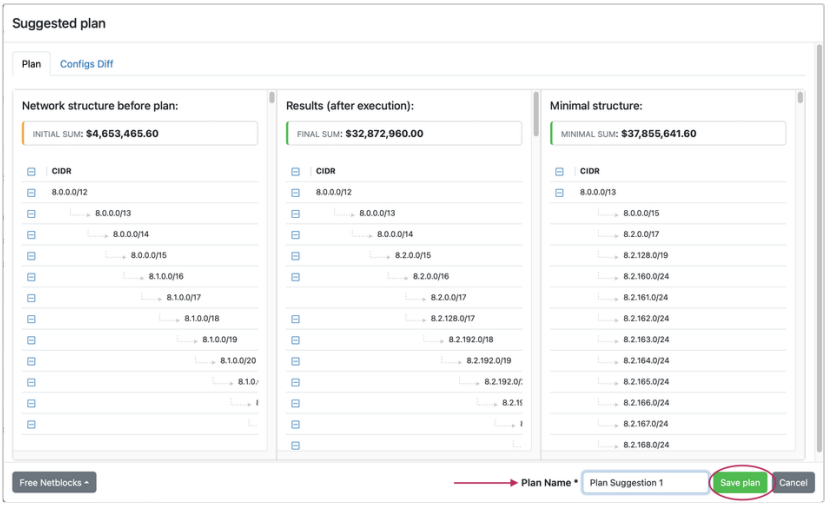


The Free Netblocks list will display with a list of CIDRS, and the estimated min/max values associated with them.



Save Suggested Plan(s)

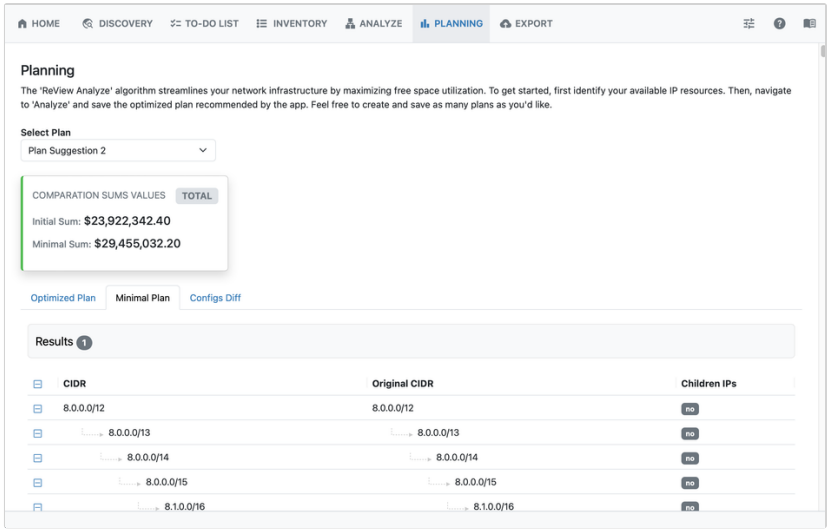
Save the suggested plan by entering a plan name and clicking “Save Plan”. Saved plans are available for review and comparison under the “Planning” Tab.



Next Steps

Next, proceed to the Planning tab to review and compare saved plans.

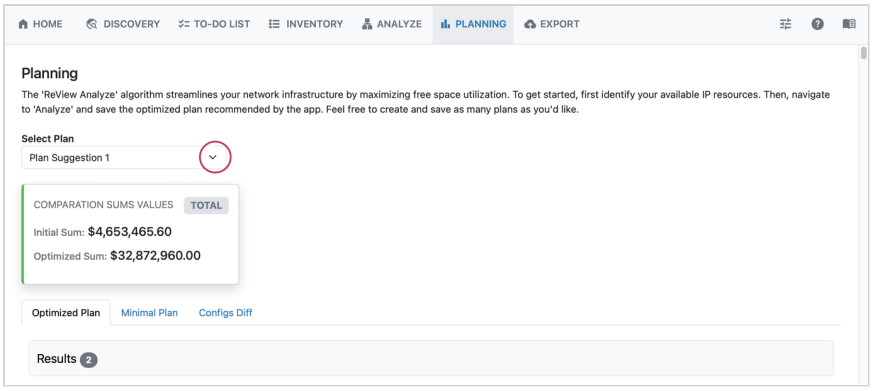
Planning



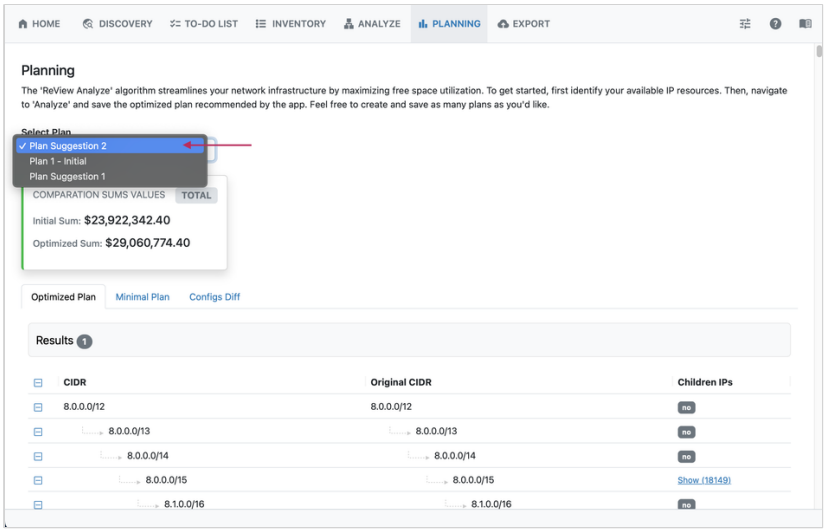
The Planning tab shows the potential value for plans saved under the Analyze tab. Here, you may view the Optimized Plan, Minimal Plan, and Configs Diff for each plan saved from the Analyze Tab - Get Suggestions step.

Select Plan

At the top of the page, click on “Select plan” to open the list of saved plans.



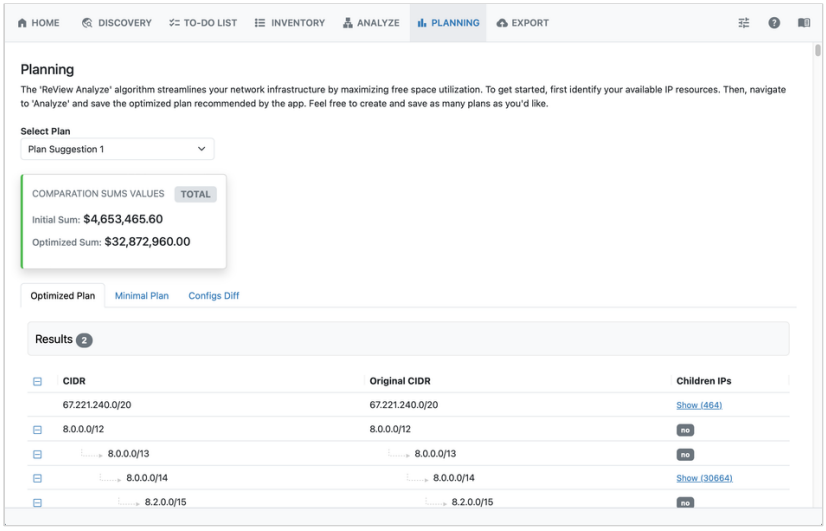
Then, select which saved plan to view.



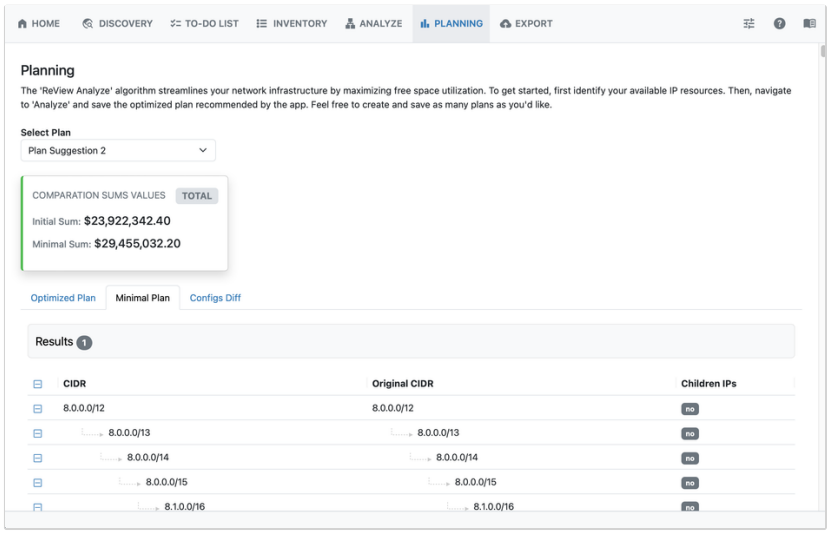
The plan will load organized into three subtabs: Optimized Plan, Minimal Plan, and Config Diff.

For each plan, the plan CIDR, original CIDR, and child IP status is displayed.

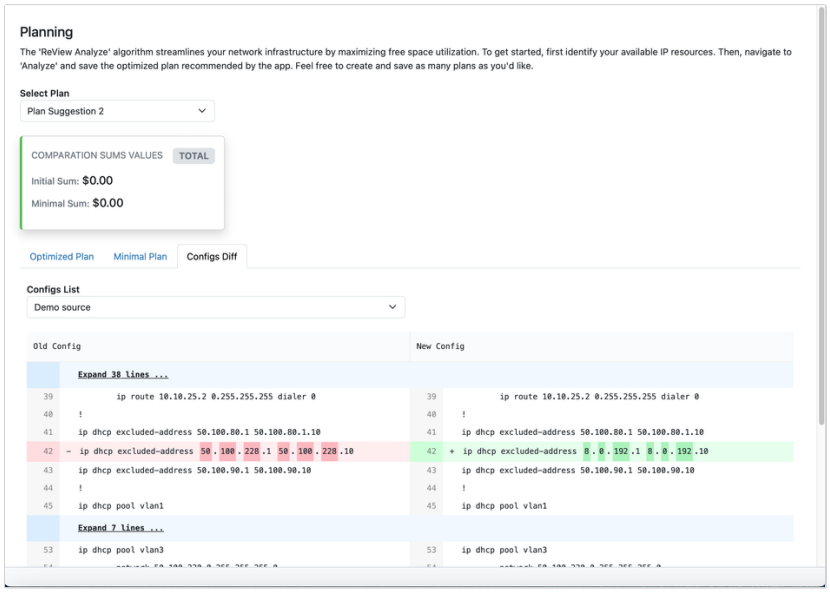
The **Optimized Plan** shows the optimal consolidation plan, keeping the current network structure and number of levels intact:



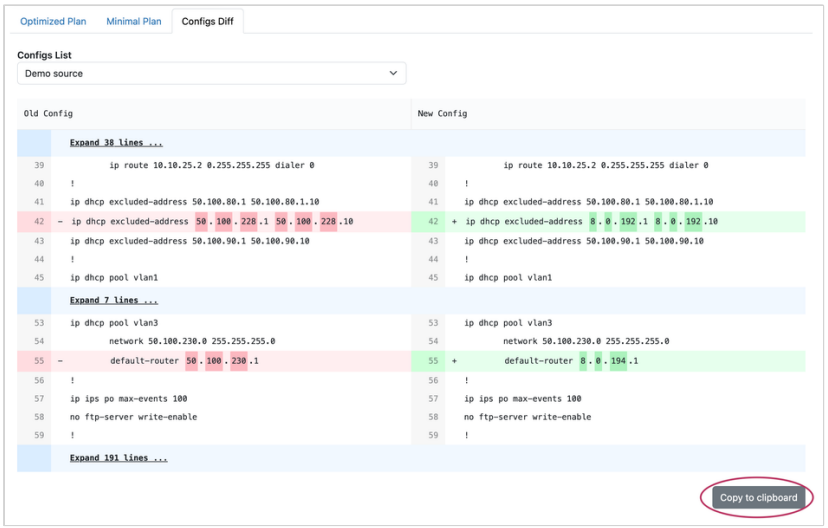
The **Minimal Plan** displays the highest value strategy to give the most free space, consolidating the structure into the fewest possible netblocks:



Configs Diff shows the side-by-side differences in the configuration for the plan implementation:



The Configs Diff files may be copied to clipboard to save to paste into a local file for later implementation.

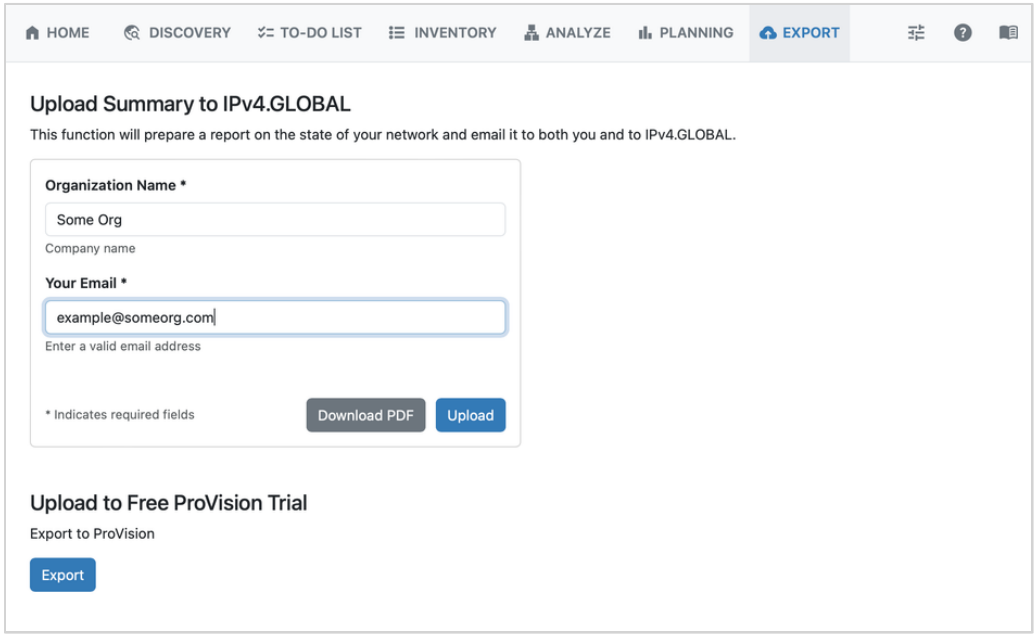


At this point, you may wish to review and compare multiple strategies for different plans, and decide on which version you may wish to implement.

Next Steps

After reviewing plans from the Planning tab, you may optionally select to proceed to the Export tab to generate a network status report.

Export



Upload Summary

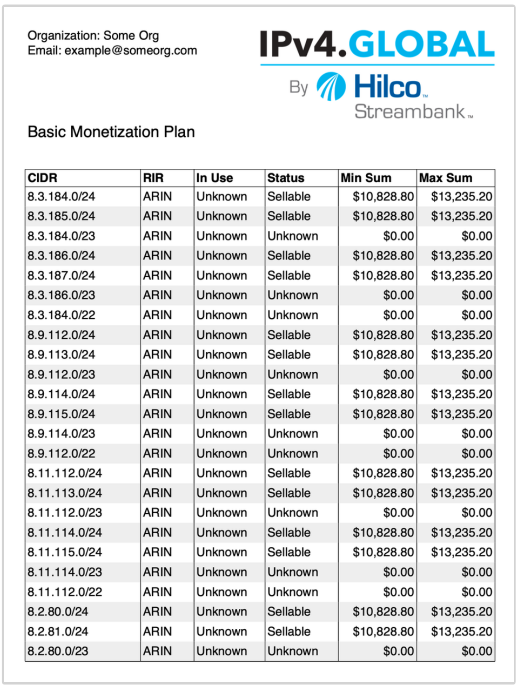
The Export tab will prepare a report on the state of your network and email it to both you and to Ipv4.GLOBAL.

Enter an Organization Name and an email address and click “Upload” to send the report.

Generate PDF

You may download a PDF of the report by clicking “Download PDF”.

The PDF format will be downloaded as a tabular montetization report, displaying CIDR, RIR, Use, Status, Min Sum, and Max Sum.



Organization: Some Org
Email: example@someorg.com

IPv4.GLOBAL
By Hilco Streambank

Basic Monetization Plan

CIDR	RIR	In Use	Status	Min Sum	Max Sum
8.3.184.0/24	ARIN	Unknown	Sellable	$10,828.80	$13,235.20
8.3.185.0/24	ARIN	Unknown	Sellable	$10,828.80	$13,235.20
8.3.184.0/23	ARIN	Unknown	Unknown	$0.00	$0.00
8.3.186.0/24	ARIN	Unknown	Sellable	$10,828.80	$13,235.20
8.3.187.0/24	ARIN	Unknown	Sellable	$10,828.80	$13,235.20
8.3.186.0/23	ARIN	Unknown	Unknown	$0.00	$0.00
8.3.184.0/22	ARIN	Unknown	Unknown	$0.00	$0.00
8.9.112.0/24	ARIN	Unknown	Sellable	$10,828.80	$13,235.20
8.9.113.0/24	ARIN	Unknown	Sellable	$10,828.80	$13,235.20
8.9.112.0/23	ARIN	Unknown	Unknown	$0.00	$0.00
8.9.114.0/24	ARIN	Unknown	Sellable	$10,828.80	$13,235.20
8.9.115.0/24	ARIN	Unknown	Sellable	$10,828.80	$13,235.20
8.9.114.0/23	ARIN	Unknown	Unknown	$0.00	$0.00
8.9.112.0/22	ARIN	Unknown	Unknown	$0.00	$0.00
8.11.112.0/24	ARIN	Unknown	Sellable	$10,828.80	$13,235.20
8.11.113.0/24	ARIN	Unknown	Sellable	$10,828.80	$13,235.20
8.11.112.0/23	ARIN	Unknown	Unknown	$0.00	$0.00
8.11.114.0/24	ARIN	Unknown	Sellable	$10,828.80	$13,235.20
8.11.115.0/24	ARIN	Unknown	Sellable	$10,828.80	$13,235.20
8.11.114.0/23	ARIN	Unknown	Unknown	$0.00	$0.00
8.11.112.0/22	ARIN	Unknown	Unknown	$0.00	$0.00
8.2.80.0/24	ARIN	Unknown	Sellable	$10,828.80	$13,235.20
8.2.81.0/24	ARIN	Unknown	Sellable	$10,828.80	$13,235.20
8.2.80.0/23	ARIN	Unknown	Unknown	$0.00	$0.00

Upload to ProVision

If you are a ProVision user, or wish to trial ProVision using the inventory discovered in ReView, click “Export” to export data into your ProVision instance.