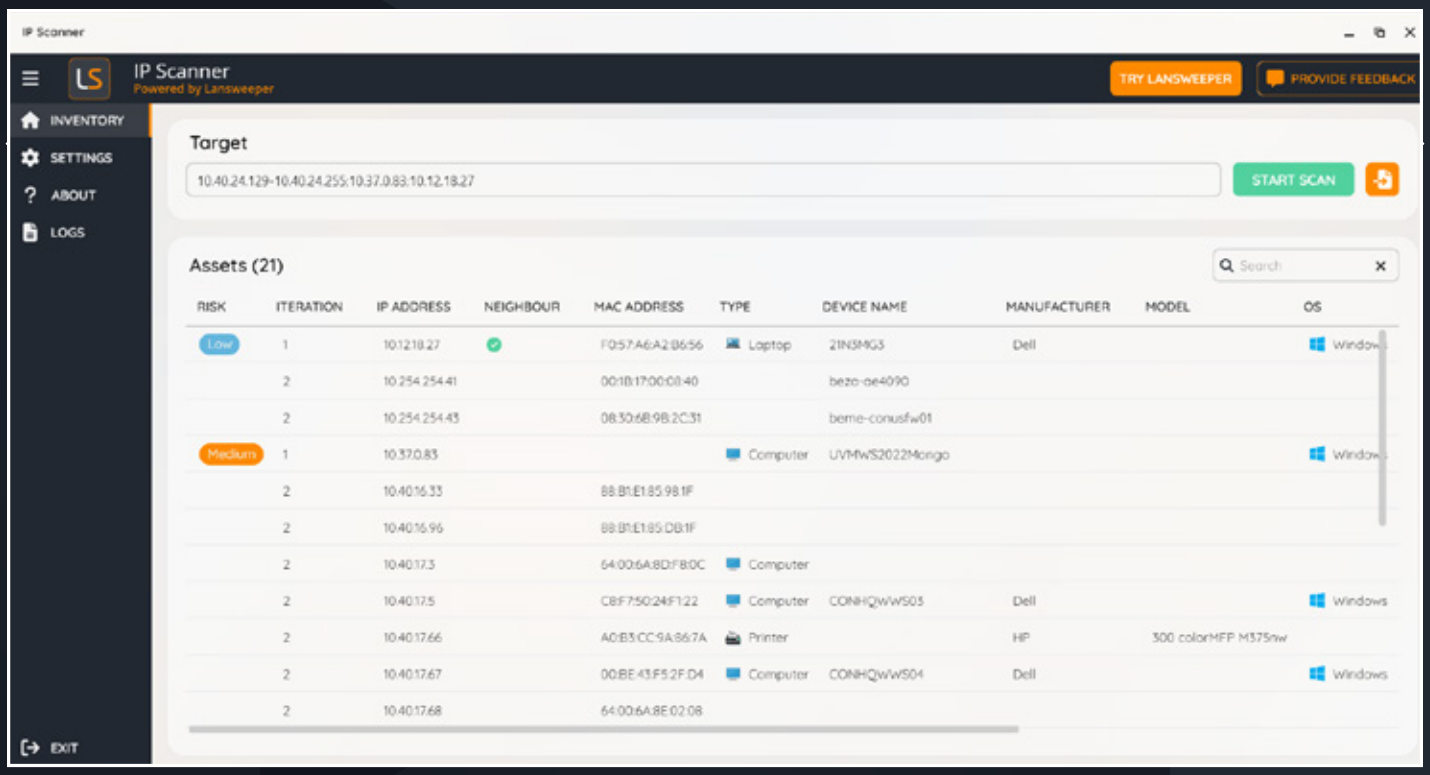
Lansweeper

# Using the IP Scanner




## Scan entire IP ranges to identify and analyze network devices, open ports, and security risks with customizable settings.

When the IP Scanner scans entire IP ranges simultaneously, the tool displays basic information about all the assets it discovers in a concise overview. You can also drill down into individual assets to learn more.

To keep scans efficient, the tool only scans the most commonly used ports by default. However, you can customize the settings if you want to scan specific ports or all ports.

Use the IP Scanner tool to identify devices with open ports, assess risks such as open RDP ports, detect end-of-support (EOS) or end-of-life (EOL) statuses for operating systems and hardware, and discover any hidden or public shared folders without authentication.

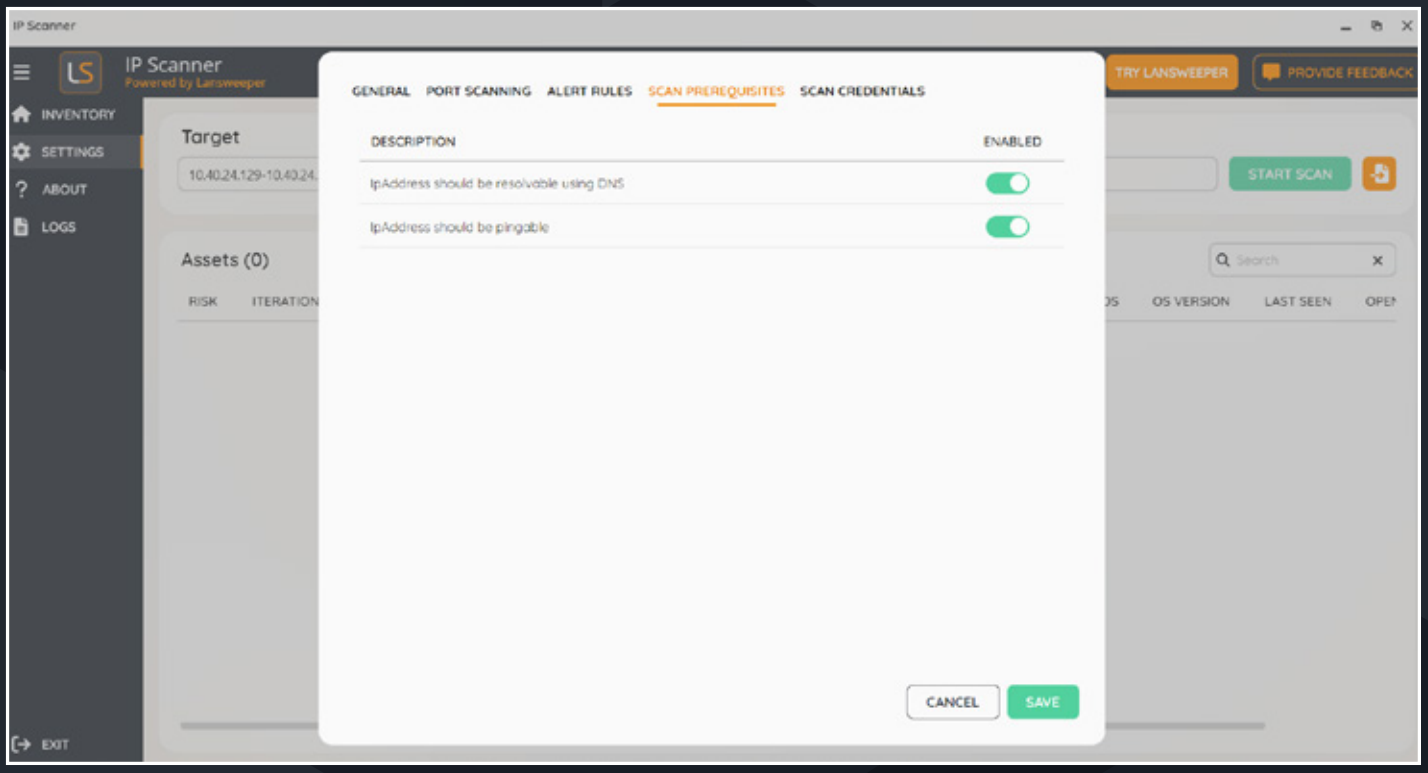
# I. Prerequisites

## → Operating systems:

Windows or macOS.

## → Network requirements:

The local machine must be able to successfully ping the target or resolve it using DNS. If your network devices don't respond to ping or are not registered in DNS, you can disable these settings in Settings > Scan Prerequisites.



## II. Specify the IP Range

1. Open the Lansweeper IP Scanner tool.

2. Specify the range of IP addresses. The target can be in any of the following formats:

   x.x.x.x (e.g. 10.0.0.1)

   x.x.x.x-x.x.x.x (e.g. 10.0.0.1-10.0.0.127)

   x.x.x.x/y (e.g. 10.0.0.0/24 a.k.a. CIDR)

   localhost (a shortcut for 127.0.0.1)

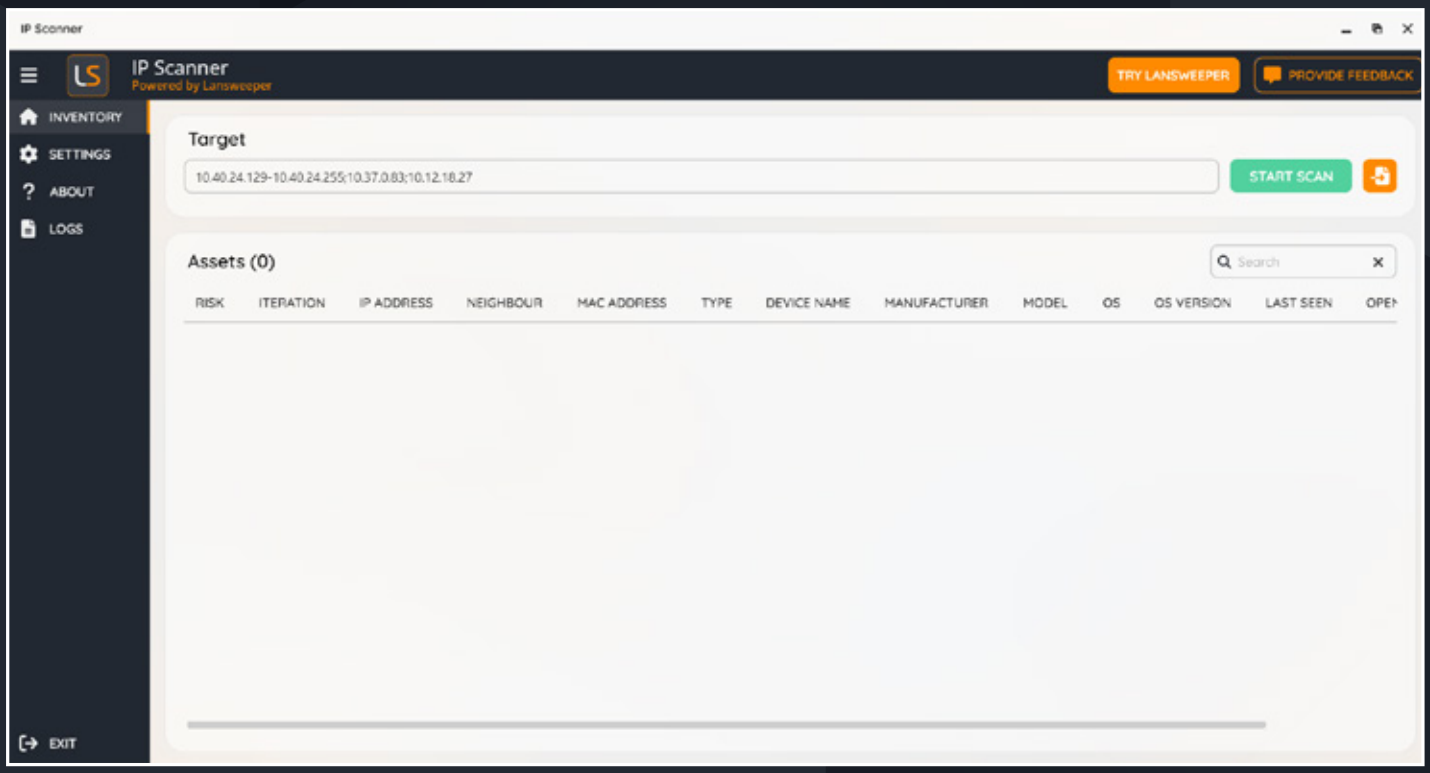
   or any combination using ';' as a separator, e.g.

   10.0.0.1-10.0.0.127;192.168.1.1;localhost

By default, an IP range based on your current IP address and subnet is displayed.

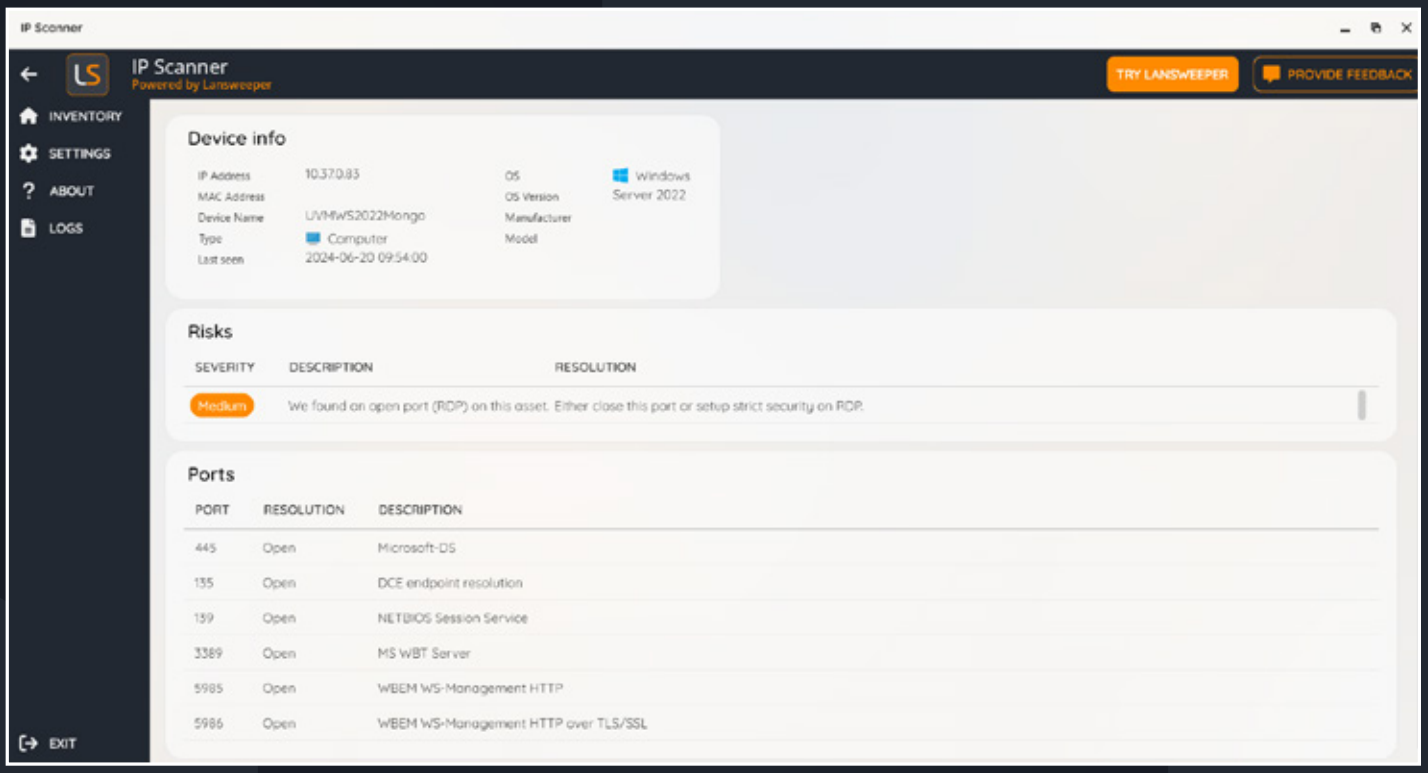
3. Select **Start scan**.

The tool will start scanning the IP range.



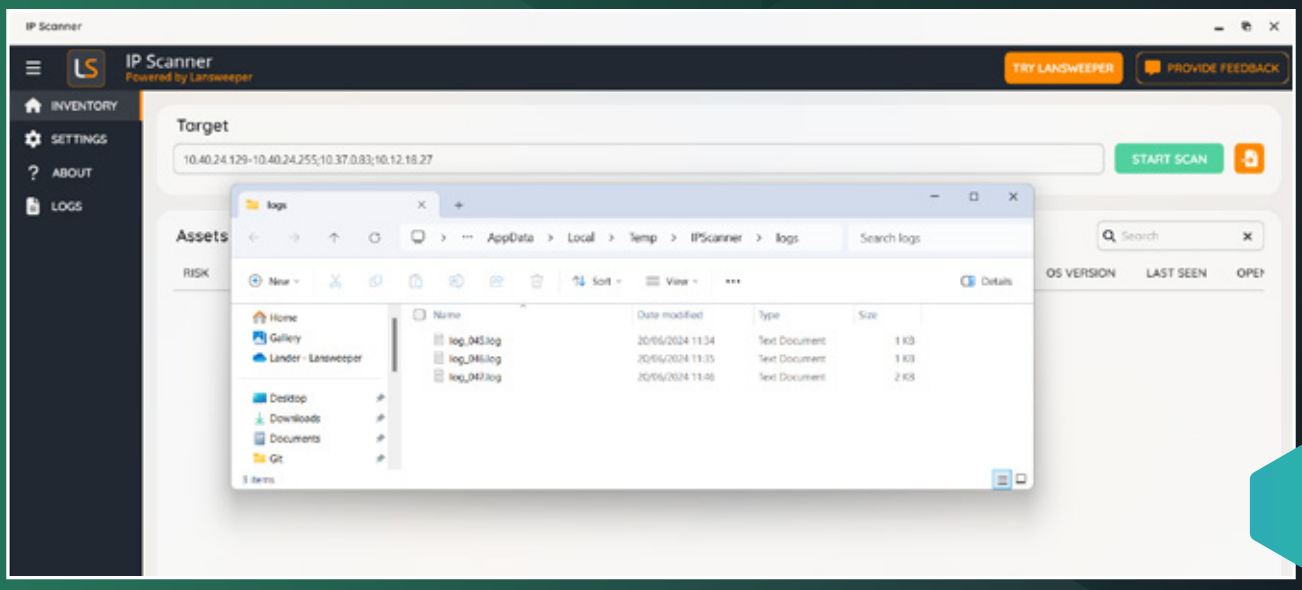
## III. Analyze the Results

After the scan has completed, select any result in the Assets list to view more detailed information. Next to relevant device information, the tool will show you any open ports, and any detected security risks.




For scanned switches, additional details are available such as interfaces, the IP routing table, interface stacking, and neighbor information (using OSPF, EGP, or BGP).

A log of the scan will be saved in: C:\Users\USERNAME\AppData\Local\Temp\IPScanner\logs on Windows. For MacOS, the exact location depends on various factors, so we recommend Mac users click the 'logs' button in the app rather than navigating manually.

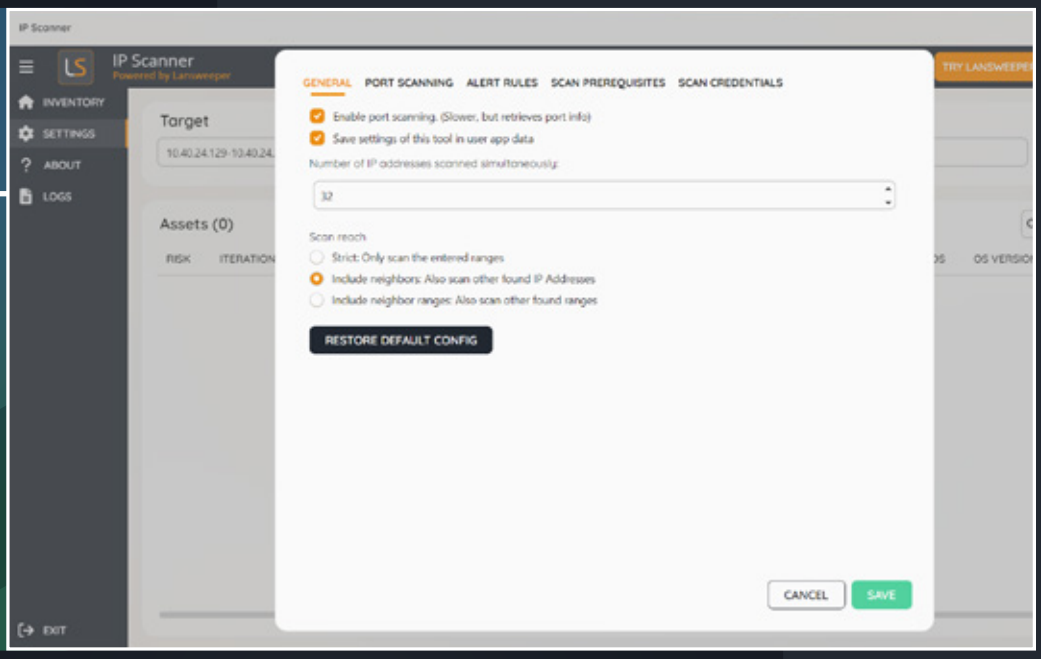


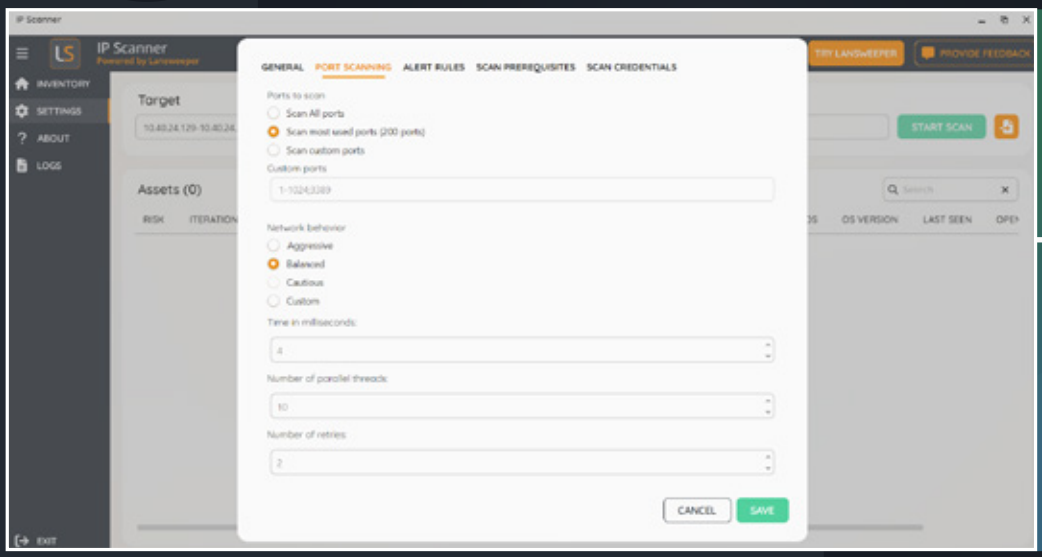
## IV. Configure the Settings

Customize your IP scans by navigating to Settings.

**General:** Enable port scanning and select the reach of your scans.

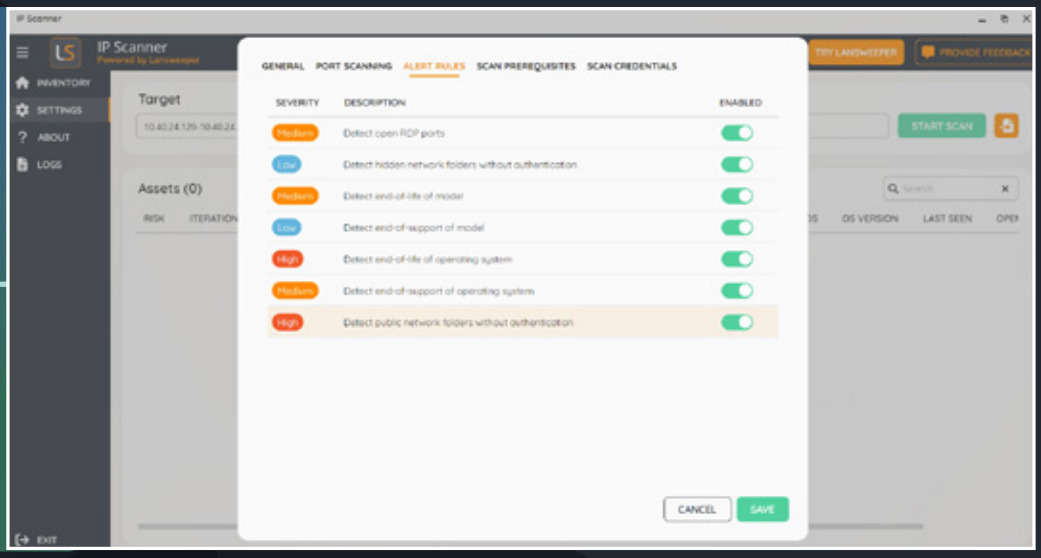
When enabled, the tool can scan outside of the given IP range if it detects neighboring devices. For example, if a switch is scanned, and the tool has detected a connected device, it will scan those connected devices as well.

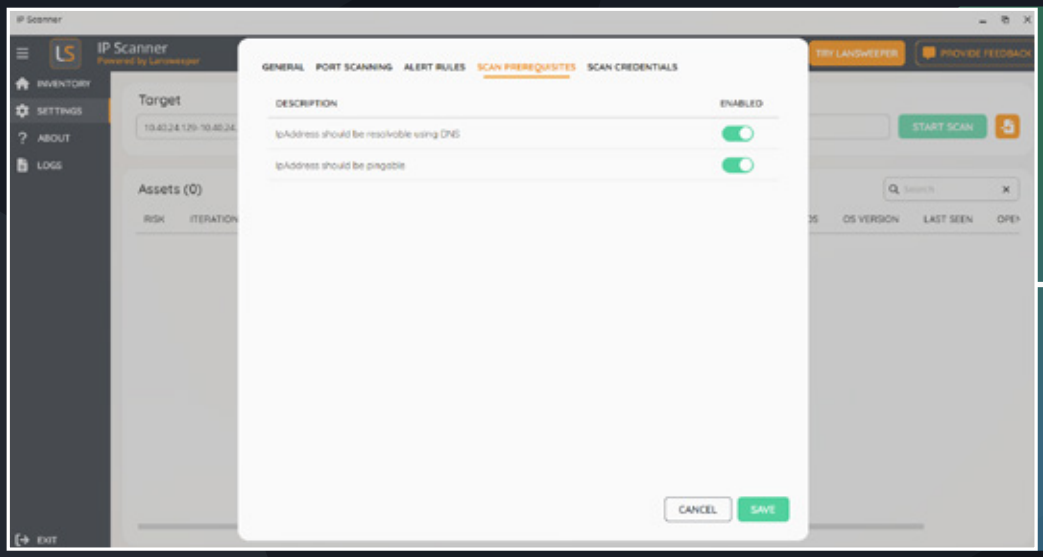



**Port Scanning:** Select which ports to scan and choose the aggressiveness of port scans.

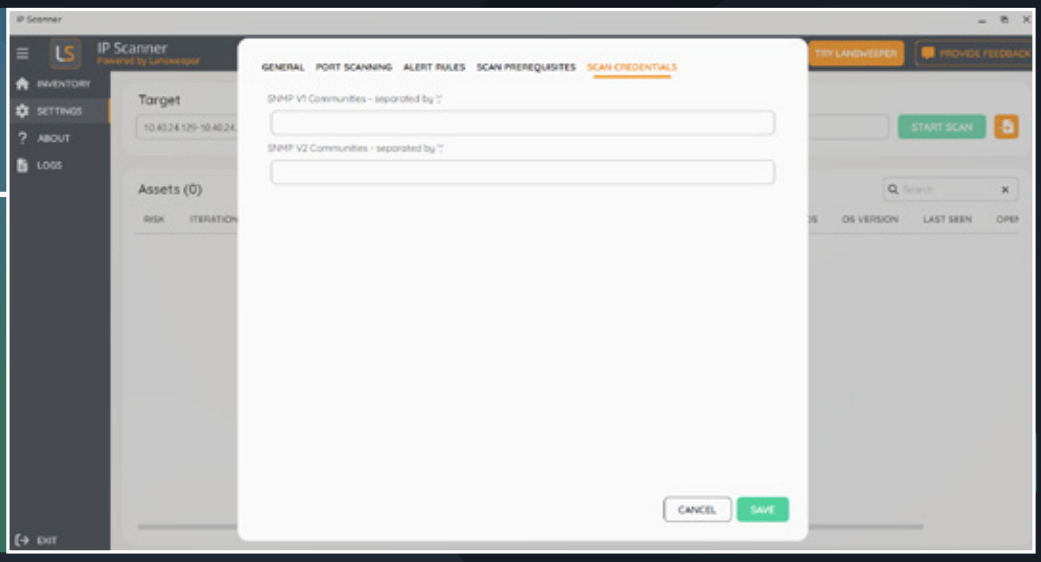
**Alert Rules:** Set up any rules for scanning, such as identifying open RDP ports and checking for EOL information.




**Scan Prerequisites:** Select whether the IP address must be ping-able, or resolvable using DNS.

**Scan Credentials:** Enter SNMP V1 and V2 community strings.



## V. Provide Feedback

If you'd like to share your experience or suggestions, select Provide feedback to open up the feedback form.