



Objective-See
a non-profit 501(c)(3) foundation.



tools



blog

Support Us!

LuLu



↓ [download](#)

In today's connected world, it is rare to find an application or piece of malware that *doesn't* communicate with a remote server.

LuLu is the free, open-source firewall that aims to block unknown outgoing connections, protecting your privacy and your Mac!



Supported OS: macOS 10.15+



Current version: 2.5.1 ([change log](#))



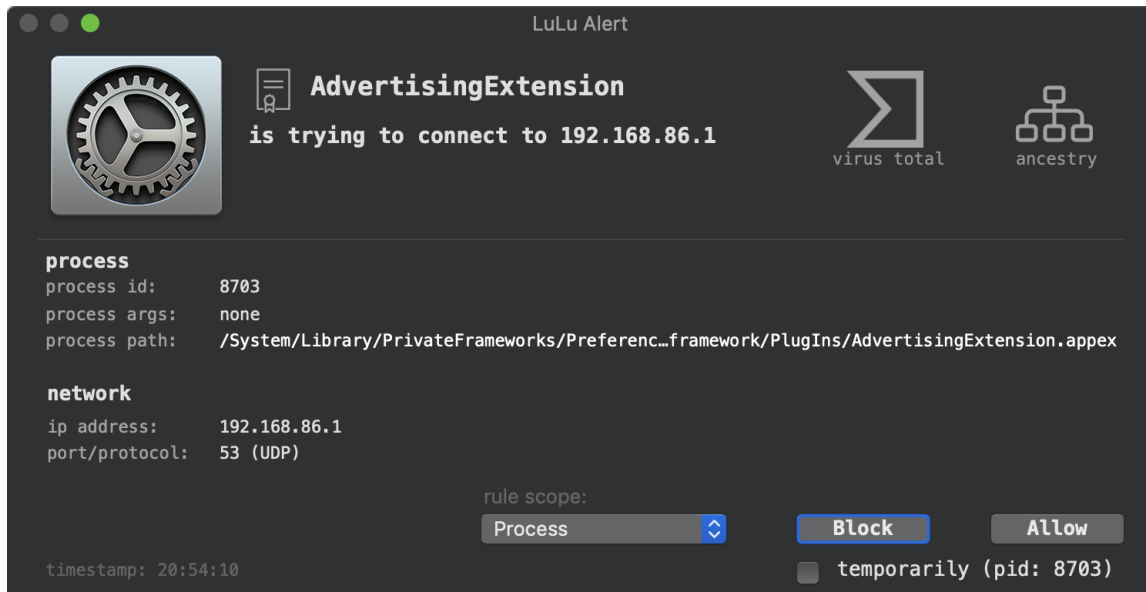
DMG's SHA-1: 161F90B4C8A8A0604B99980F8EAC1C352ED78D8B



Source Code: [LuLu](#)

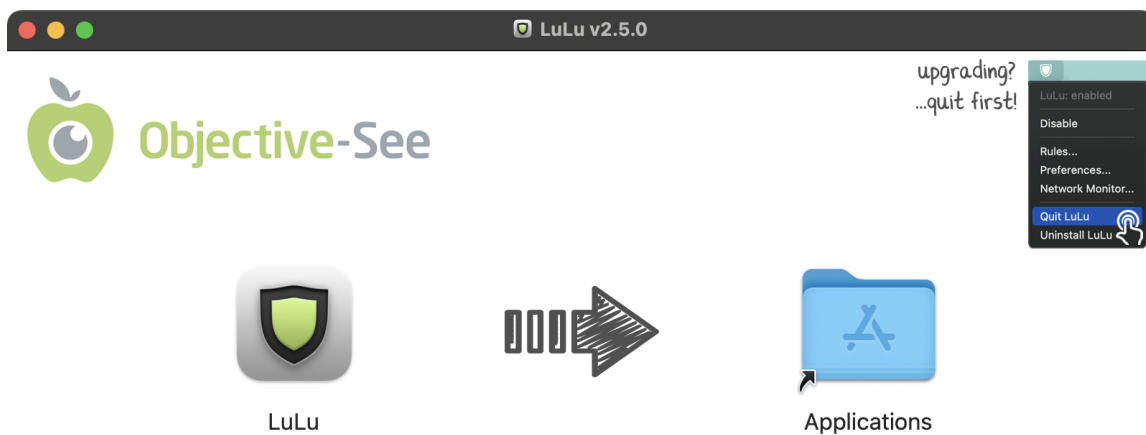
 LuLu leverages Apple's new Network Extension framework.

As Apple continues to improve the stability of this framework, it is recommended you upgrade to the latest version of macOS, before installing LuLu!



INSTALLING LuLu

To install LuLu, first **download** the disk archive containing the application. Then double-click `LuLu.dmg` and drag `LuLu.app` into the `Applications` folder:

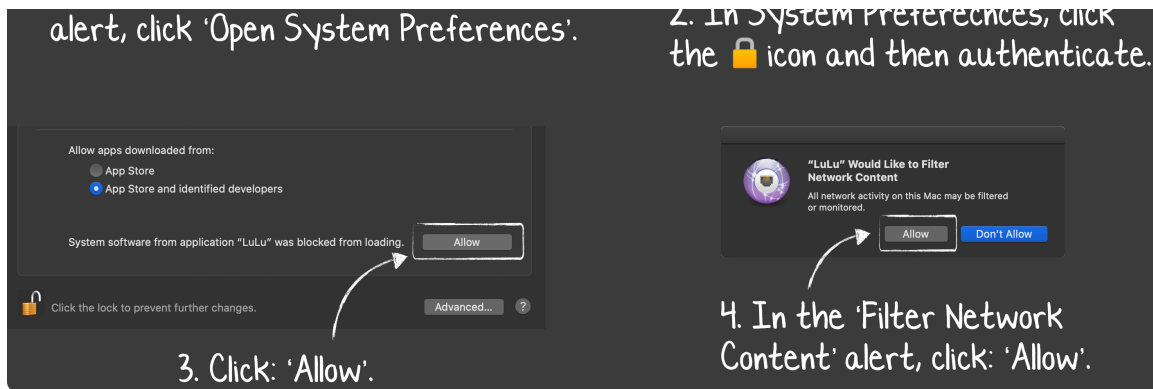


LuLu v2.5.0

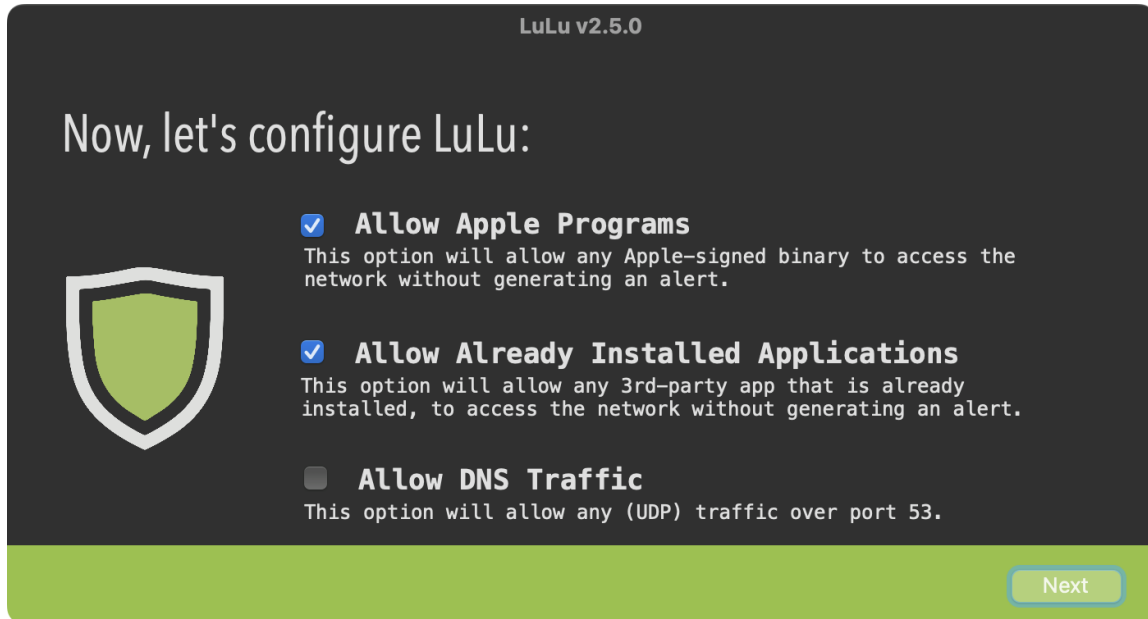
If you're upgrading LuLu and receive a "*LuLu.app is in use*" error message, exit the currently running instance of LuLu (via "Quit LuLu" in the status bar menu).

After copying `LuLu.app` to the `Applications` folder, launch it to continue its installation. On a fresh install, LuLu will walk you thru various installation steps, the most important being the manual approval of its System Extension and Network Filter:

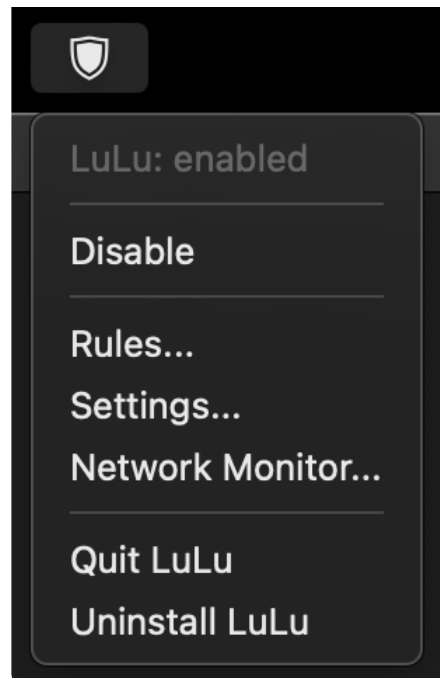


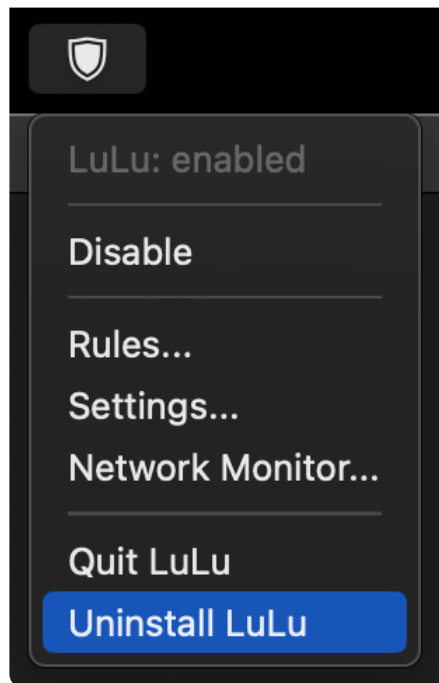


Once you have granted LuLu the required approvals, LuLu will display several initial configuration options. It is recommend you leave the default options selected which will allow Apple and already installed programs to (keep) accessing the network without alerting you:

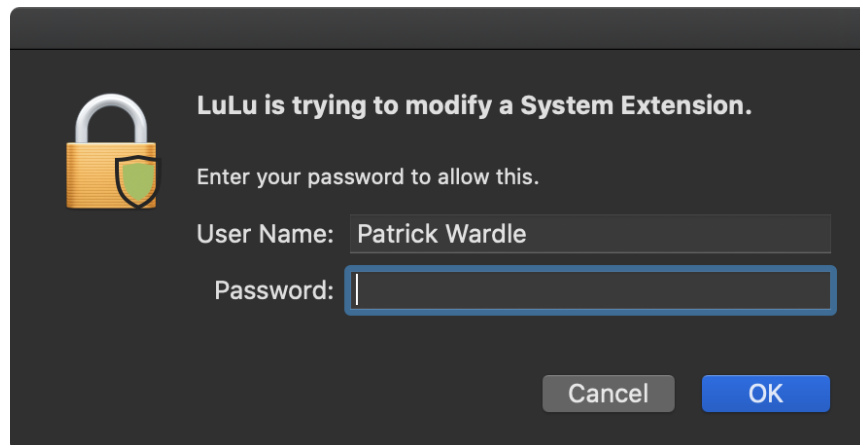


Now that LuLu is configured and installed, it will be running and set to automatically start each time you log in. It will appear in the status bar (unless configured otherwise):





...and authenticate, to fully remove the application and all its components:

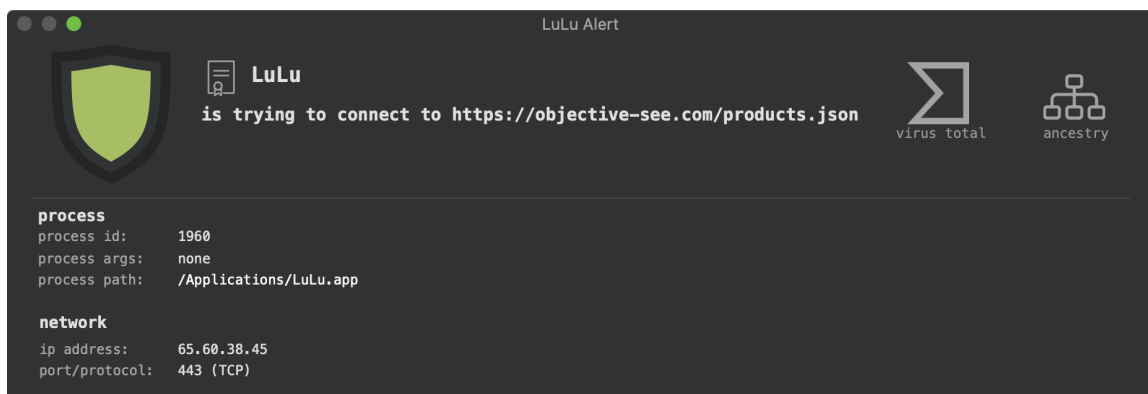


To uninstall an older version (v1.*), first download [LuLu \(v1.2.3\)](https://objective-see.org/products/lulu.html) ...then launch it and click "Uninstall".

USING LULU (ALERTS)

Once LuLu is installed, it aims to alert you anytime a new or unauthorized outgoing network connection is created.

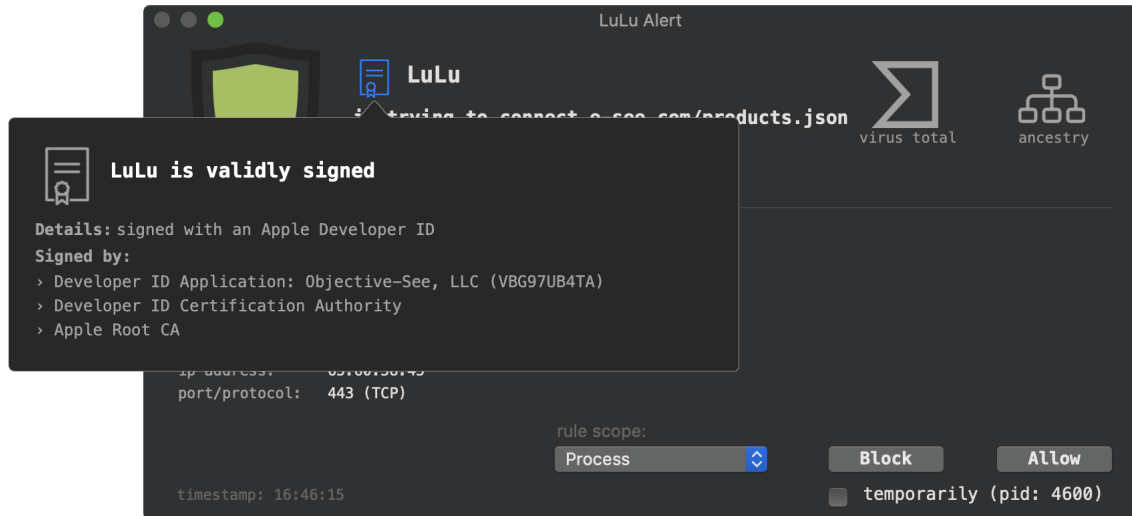
Here's a LuLu alert, displayed when LuLu checks for an update (by requesting the remote `products.json` file):



This website uses cookies to improve your experience.

The alert contains information about the process attempting the connection, as well as information about the connection's destination.

Various elements of the alert are click-able, such as a button to display the process's code signing information:

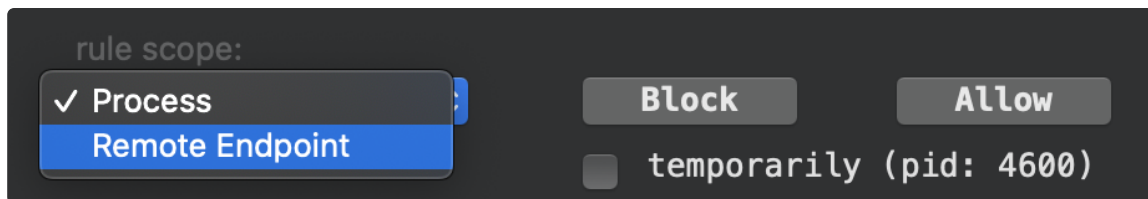


Other elements include of the alert, that once clicked provide more information, include:

- **Virus Total Information:**
Contains an anti-virus detection ratio for process that is attempting to create the outgoing connection.
- **Process Hierarchy:**
Display the hierarchy (ancestry) for the process that is attempting to create the outgoing connection.

To approve the outgoing connection, simply click "Allow" ...or click "Block" to prevent it. Unless you click the "temporarily" button, a persistent rule will be created to remember your decision.

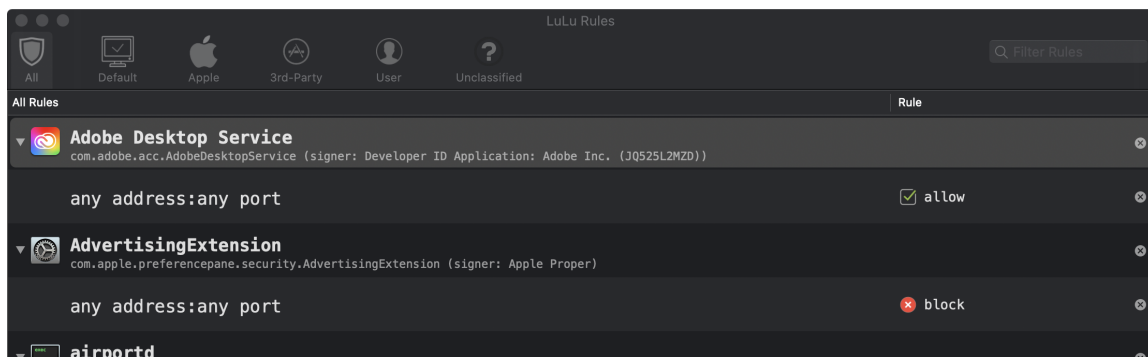
By default, your decision (block or allow) applies to the entire process. That is to say, your decision will be applied to subsequent connections (regardless of their destination) for this process, and any other instances. However, if you select the "Remote Endpoint" option, your decision will be scoped, and only will be applied subsequent connections that match the same (remote) destination:



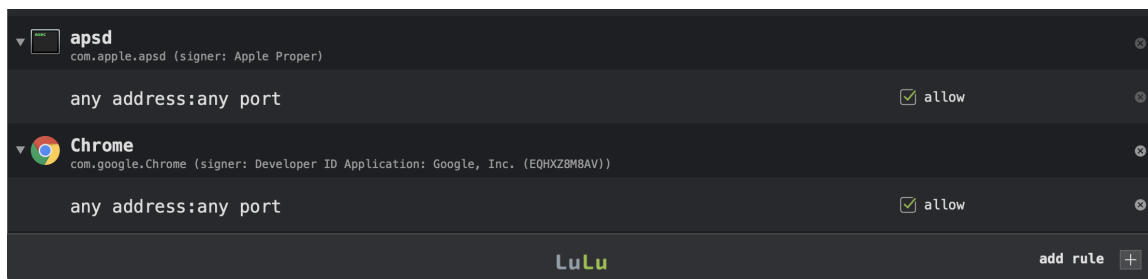
Via the Rules window (described below), you can further customize rules, for example by leveraging regular expressions.

1. USING LuLu (RULES)

Process or connections are either allowed to access the network, or blocked, based on LuLu's rules. The 'Rules' window displays these rules:



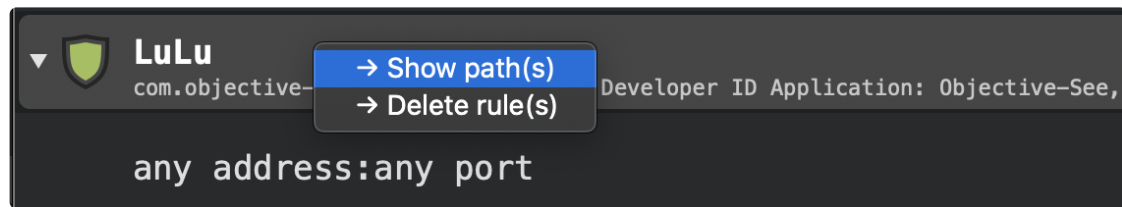
This website uses cookies to improve your experience.



If signed, a program is identified in the Rules window by name and its code signing (bundle) identifier (e.g. `com.objective-see.lulu`).

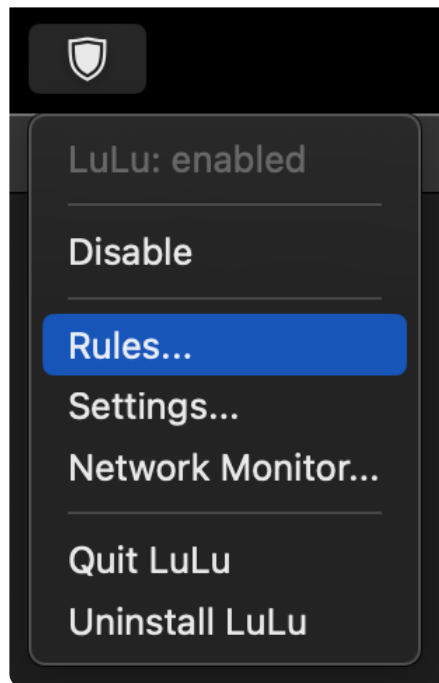
Using a code signing identifier (vs. a path), allows the rule to be applied even if the program is moved, or updated.

Want to view a program's path(s)? Simply double click (or \wedge +click and select "→ Show Path(s)") on any program in the Rules window:

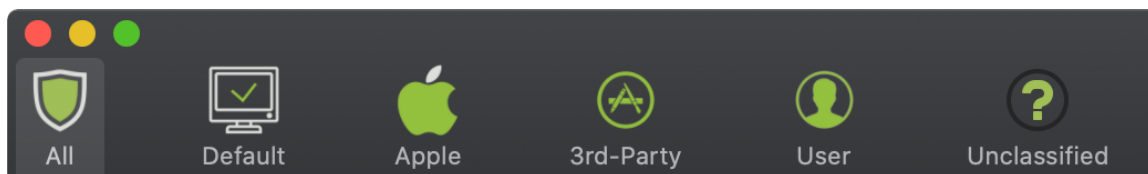


The Rules Window

The Rules window can be accessed either by launching LuLu's application (`/Applications/LuLu.app`), or by clicking on 'Rules...' in LuLu's status bar menu:



There are several tabs in the rules window, aimed at organizing the rules:



▪ All Rules:

The first tab shows all of LuLu's rules. In other words, it is a combination of the default, apple, baseline, user, and unclassified rules

The second tab shows LuLu's default or system rules. These rules are for Apple/macOS processes that must be allowed to access to the network in order to preserve system functionality.

- **Apple Rules:**

When the 'Allow Apple Programs' option has been selected (either during installation, or via LuLu's preferences), any process that is signed by Apple proper will be automatically allowed to connect to the network. Also, an 'Allow' rule will be created, and will show up under this tab.

- **3rd-Party Program Rules:**

When the 'Allow Installed Programs' option has been selected (either during installation, or via LuLu's preferences), any applications or program that was (pre)installed will be automatically allowed to connect to the network. Also, an 'Allow' rule will be created, and will show up under under this tab.

- **User Rules:**

This tab shows rules the user has created, either manually via the 'add rule' button, or by clicking 'Block' or 'Allow' in a LuLu alert window.

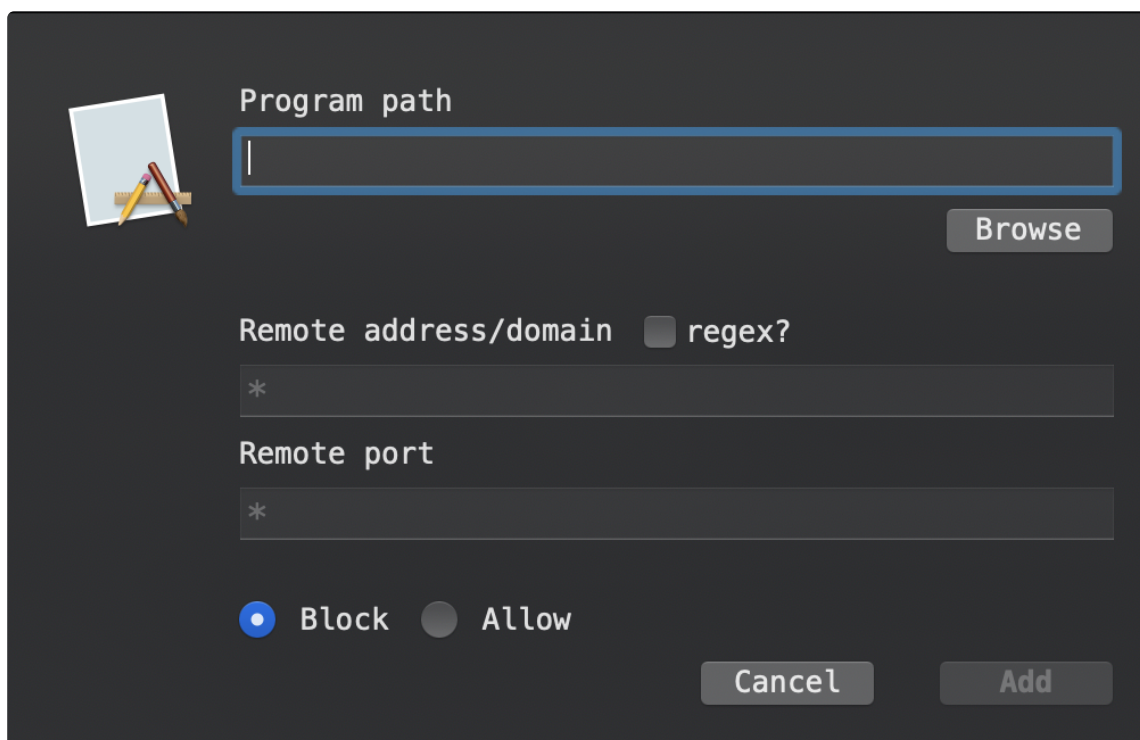
- **Unclassified Rules:**

If you are not logged in, and a process attempts to access the network will be automatically allowed. Also, an 'Allow' rule will be created, and will show up under under this tab.

Adding Rules

Generally rules are created in response to an alert (unless the user has selected the "temporarily" button).

To manually add a rule, click on the 'add rule' button at the bottom of the rules window. This will bring up an 'Add Rule' dialog box:



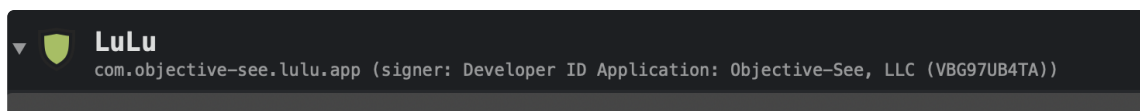
In this dialog box, enter the path to the program (or click 'Browse' to open a file chooser window). Then, enter the remote address or domain, remote port, and finally select 'Block' or 'Allow'. Click 'Add' to add the rule, which will be persistently saved, and show up as a 'User' rule.

Enter * for "any" (e.g. a program path of * will globally match all programs).

The rule's remote address/domain can also be a regular expression (though make sure to select the "regex" checkbox if this is the case).

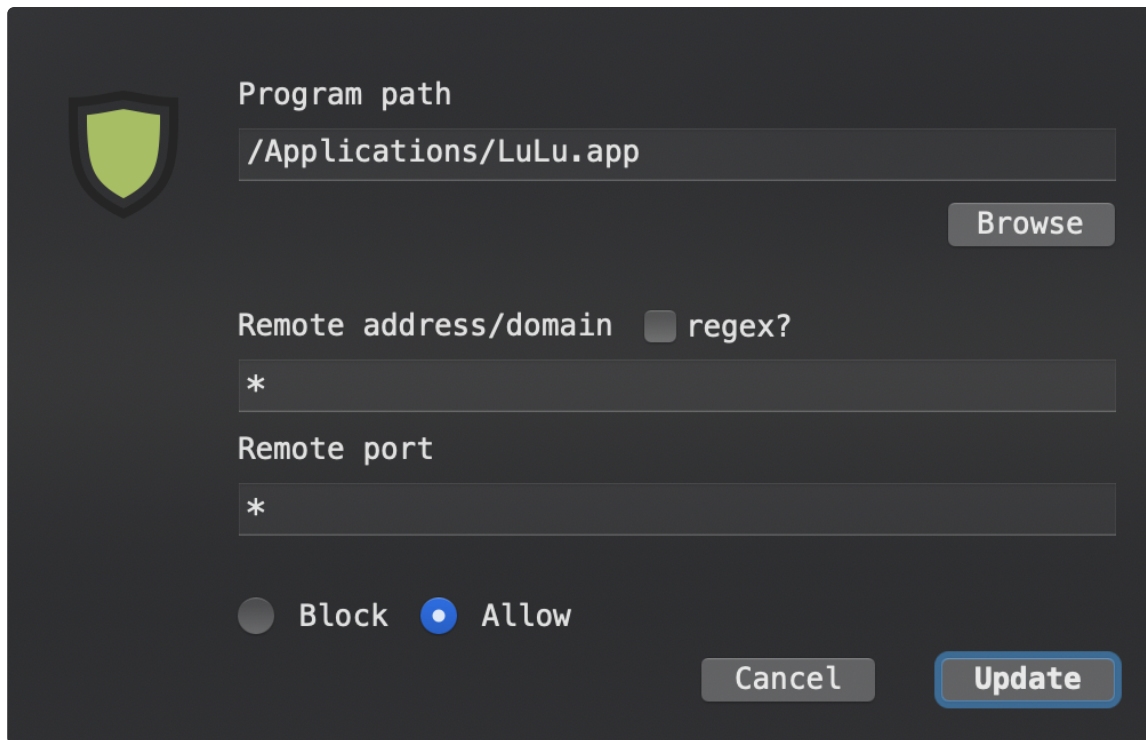
Editing (Updating) Rules

To change a rule, either double click on a rule, or ^+click and select " → Edit Rule":



→ Delete Rule

This will bring up the "Edit Rule" window. Here you can edit any aspect of the rule:



Program path
/Applications/LuLu.app Browse

Remote address/domain ☐ regex?
*

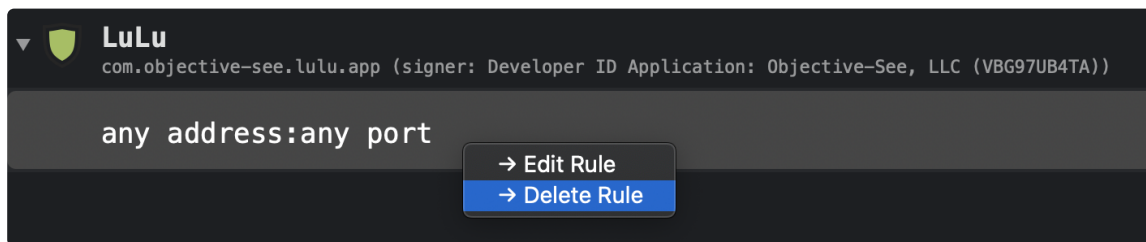
Remote port
*

☐ Block ☒ Allow

Cancel Update

Deleting Rules

There are several ways to delete a rule. With the rule selected, simply press the "delete" on your keyboard or, ^+click and select " → Delete Rule":



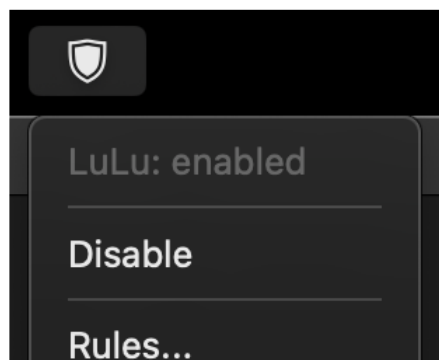
...or simply click the 'x' button on the right hand side of the rule.

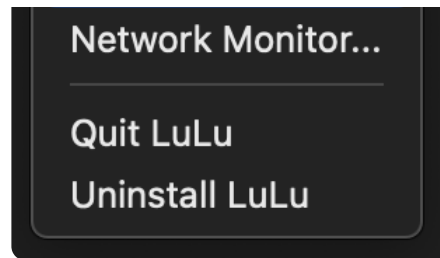
Deleting a row that contains program information, will, as expected also remove all its rules.

Also note that default (system) rules cannot be deleted (via the Rules window).

USING LuLU (SETTINGS)

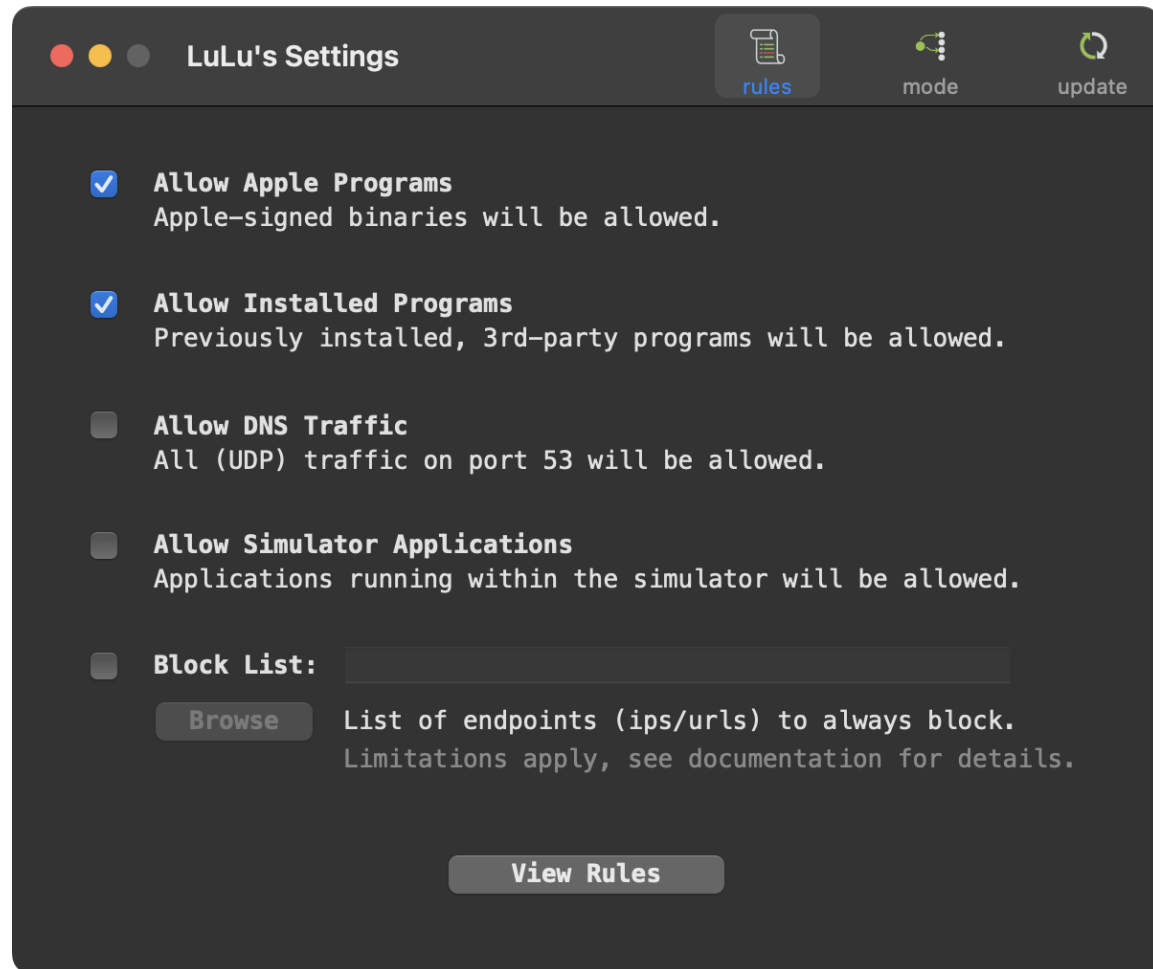
LuLu can be configured via its settings pane. To open this pane, either in the main LuLu application (/Applications/LuLu.app), or via LuLu's status bar menu, click on 'Settings...'





The preference pane has three tabs: **rules**, **mode**, and **update**.

The **rules** tab, allows one to configure how LuLu will (automatically) generate rules, as well as other rule-related settings:



- **'Allow Apple Programs'**
When this option is selected any process that is signed by Apple proper will be automatically allowed to connect to the network. Also, an 'allow' rule will be created, and will show up in the Rules window, under 'Apple Rules'.
- **'Allow Installed Applications'**
When this option is selected any applications (and their components) that were (pre)installed will be automatically allowed to connect to the network. Also, an 'allow' rule will be created, and will show up in the Rules window, under 'Baseline Rules'.
- **'Allow DNS Traffic'**
When this option is selected any UDP traffic over port 53 will be allowed.
- **'Allow Simulator Applications'**
When this option is selected, traffic any applications running within a simulator will be allowed. This is useful if you are developing applications and testing them within (iOS/iPad) simulator.
- **'Block List'**
When this option is selected, LuLu will automatically block any connection that matches any items in specified block list. The block list can be a local file, or remote url (e.g.

This website uses cookies to improve your experience.

The block list file should contain a (newline-separated) list of url hosts and/or ip addresses to block.

Items in the block listed are matched and applied regardless of the process creating the connection, or any other rules.

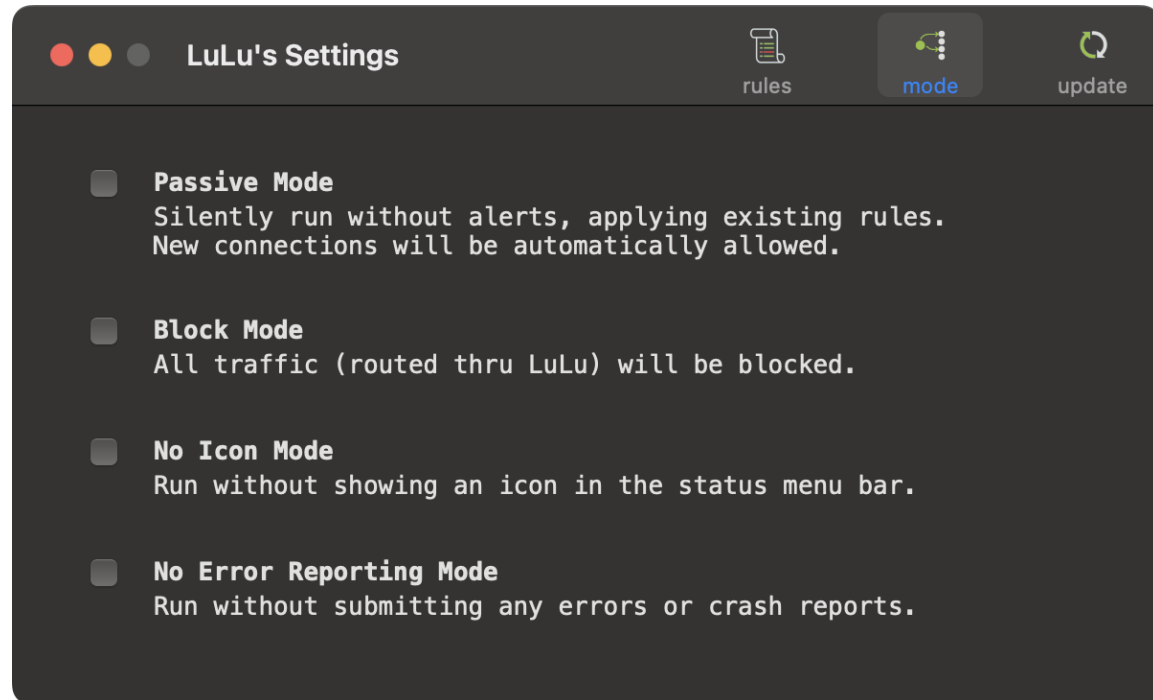
For a free (privacy focused) block list, see: [blockyouxlist](#).

Due to limitations of macOS, blocking via host name is only applicable to (as Apple notes) *"Network.framework or NSURLSession connections"*.

As such, for browsers (such as Chrome), that do not leverage these frameworks, only ip address based blocking is supported.

...as Safari and Firefox leverage such frameworks, they are not subject to this limitation.

The **mode** tab, allows one to configure LuLu to run in various modes:

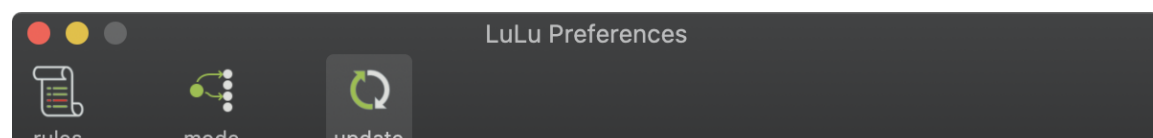


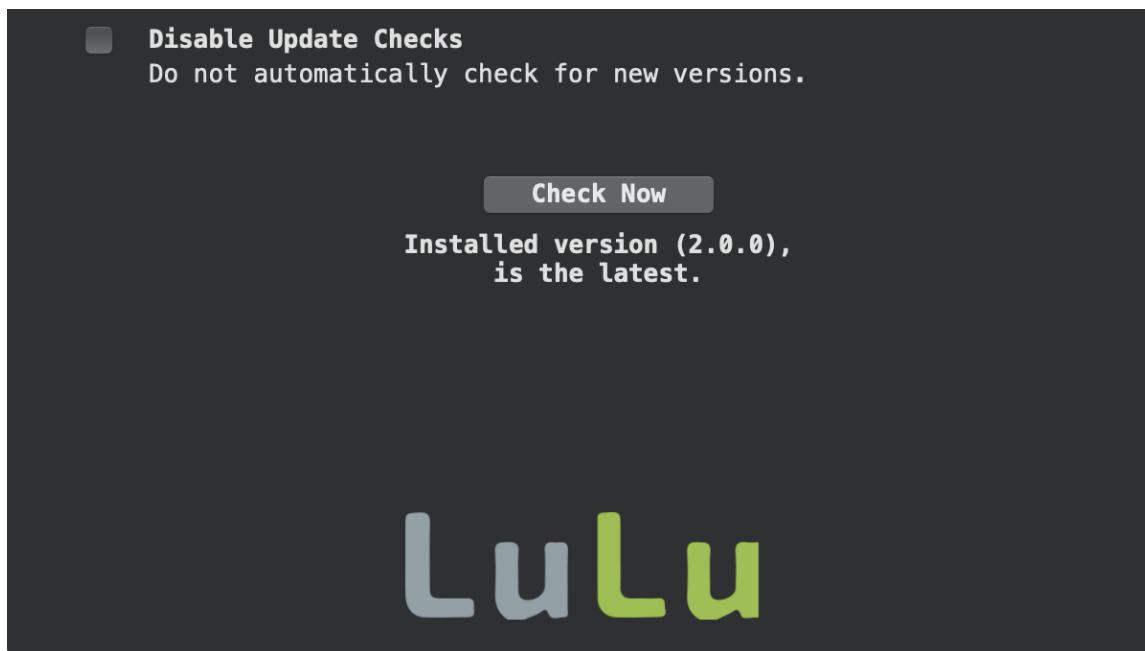
- **'Passive Mode'**
When this option is selected, LuLu will run silently without alerts. Existing rules will be applied, and new connections will be automatically allowed.
- **'Block Mode'**
When this option is selected, all traffic (that is routed thru LuLu) will be blocked.

The OS does not route all traffic through Network Extensions (such as LuLu). As such, such traffic is never seen by LuLu, and be cannot be blocked.

- **'No Icon Mode'**
When this option is selected, LuLu will run without an icon in the status bar.
You can always manually run `/Applications/LuLu.app` to disable this preference if you'd like the status bar icon back!
- **'No Error Reporting Mode'**
When this option is selected, LuLu will not submit (anonymized) crash reports.

The **update** tab, allows one to check for new versions, as well as disable the automatic check for new versions of LuLu:





FAQs

Q: Why is LuLu called LuLu?

A: In Hawaiian, the word 'LuLu' means protection, shield, or peace. As this tool aims to instill peace, by providing a protective shield, it seemed the fitting name. And as LuLu, (along with all of Objective-See's tools) are coded with aloha on the lovely island of Maui, it's the perfect name!

Q: Do I need LuLu if I've turned on the built-in macOS firewall?

A: Yes! Apple's built-in firewall only blocks incoming connections. LuLu is designed to detect and block outgoing connections, such as those generated by malware when the malware attempts to connect to its command & control server for tasking, or exfiltrates data.

Q: Does LuLu conflict with other (paid) macOS firewalls or security products?

A: Although at this point testing has been limited, LuLu appears to play nice with other tools :)

Q: I found a bug (or issue) with LuLu. Can you fix it?

A: For sure! If you encounter any issues, create a bug report via [GitHub](#).

Q: Why does LuLu try to access the network? **A:** When LuLu is started, it connects to [Objective-See.com](#) to check if there is a new version of the product. Specifically, it reads the file `products.json`, which contains the latest version number of LuLu. No user or product information is collected nor transmitted.

LuLu may generate network traffic related to its integration with [VirusTotal](#). As described above, when a user clicks the 'virus total' button in the alert window, this will send generate a request which contains the file's path, name, and hash. Note that the automated version checking can be disabled via the 'disable update checks' option in LuLu's preferences.

Finally, LuLu also utilizes [Sentry.io](#) for crash detection which may generate network traffic related to crash reporting.

Looking for an older version (compatible with older versions of macOS)?

Download: [LuLu \(v1.2.3\)](#).