



Scudo

hybrid firewall for macOS

Version 1.0 [public beta 3](#)

Welcome to Scudo

Scudo is a hybrid firewall app for macOS with a very simple interface aimed at all Mac users. It does not require any specific knowledge or skill. Its usage is very simple: Scudo automatically runs at user login and enables the firewall. To stop the firewall just quit Scudo. All options are grouped in a single window and everything is done using simple controls.

Scudo: Two Firewalls

Scudo combines both a *network-layer* and an *application-layer* firewall. Its purpose is to give all Mac user a compact, easy, reliable and affordable way to:

- protect shared documents and services from unwanted connections from remote computers
- improve privacy and security detecting apps connections attempts and allowing you to choose which app is allowed to connect to the network
- throttle upload and/or download bandwidth usage for each service/app independently

Scudo is a graphic user interface for an *inbound network layer packet filter* based on *PF* and an *outbound application layer socket filter* based on *AFW*.

Additionally, Scudo automatically monitors your Mac for active network services and applications so you are always aware of all network activities.

Scudo can be configured as a silent firewall that never requires interaction or maintenance, or can be configured as interactive, requesting your attention when it needs it. Your choice.

Scudo does not pollute your system: you can run it only when you need it, and when you quit Scudo your firewalls are instantly disabled. To configure and control Scudo click the Scudo icon in macOS menu bar, near the clock, and select "Firewall configuration".

Requirements

Scudo requires **macOS 10.11.6** or later. This release has been tested on 10.11, 10.12, 10.13 and 10.14.


If you installed Vallum then you must uninstall it using the correct uninstaller.

To uninstall Vallum 2 use Vallum Uninstaller found in Vallum 2 DMG.

To uninstall Vallum 3 use Vallum Uninstaller found in Vallum 3 DMG.

Installing Scudo

To install Scudo you need to provide administrator password. Installing Scudo requires a system restart.

On macOS 10.13 and later Scudo may require you to explicitly approve its execution. This is a new feature called "**Secure Kernel Extensions Loading**" introduced by Apple in order to secure your Mac allowing installation only of trusted software, like Scudo. If you are requested to approve it then just open System Preferences from  menu, then select Security and click :

"Allow system software from Davide Feroldi".

After installation is finished (and software approved) you need to restart your Mac.

Uninstalling Scudo

To uninstall Scudo please use the provided Scudo Uninstaller found in Scudo DMG.

Interaction with other firewalls

Scudo is an alternative to both **Murus** and **Vallum**.

Scudo is a front end for *AFW*, a socket filter firewall so you must uninstall Vallum using the correct Vallum Uninstaller before installing Scudo.

Scudo is also a front end for the macOS built-in *PF* packet filter. Other *PF* firewall front ends like Murus can interfere with Scudo. Do not run Murus when using Scudo.

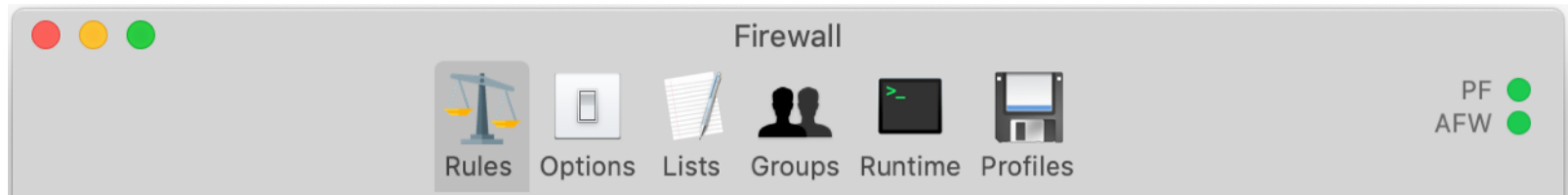
Please uninstall Murus Boot Scripts before using Scudo. You can do that running Murus and selecting Murus "Firewall" menu in macOS menu bar.

The macOS System Preferences Firewall

ALF is the built-in macOS **inbound** application-layer firewall. It can be enabled and configured from macOS *System Preferences* -> *Security* panel. Scudo (and its *AFW* core) are designed to work seamlessly with ALF. Using both firewalls gives you the opportunity to block both inbound (ALF) and outbound (*AFW*) connections at application layer.

Scudo interface

Scudo window is the place where you configure and control the firewall. Click the Scudo menulet icon near the macOS clock and select “*Firewall Configuration*” to open Scudo window. From the window toolbar you can access all Scudo configuration panels. By default the “*Rules*” panel is selected. This is the most important one as it contains both inbound and outbound rules.



Starting Scudo

When you start Scudo for the first time your firewalls will be enabled with a default configuration:

- *inbound policy: Pass*
- *outbound policy: Pass*

WARNING

Default configuration does not protect your Mac against unwanted access or data leak, as everything is set to pass by default.

Please carefully read this manual then decide how to configure your firewall.

The most typical usage of Scudo is to set both policies to “Ask”, but there are also other options. It’s up to you to decide which one suites your needs. All configuration changes are immediately active, and it’s always possible to restore default settings from Scudo “*Profiles*” panel, activating the first profile.

“*Rules*” panel is the place where you define firewall rules.

The first time you run Scudo both inbound and outbound policies will be set as “*Pass*”, left size of “*Rules*” panel will list all currently active network services, and they will be set as passed. All inbound connections to your shared documents and services are allowed.

Right size of “*Rules*” panel displays an empty list at the beginning, but this list will be quickly populated by app icons as soon as they connect to the network. Apps will be set as passed. System apps and root processes will not be shown as they are passed by default and ignored by the interface. You can change this setting in *Options* -> *Outbound*.

Both inbound and outbound policies can be set, independently, as “*Pass*”, “*Block*” or “*Ask*”. Changes take effect immediately, however already listed services and apps will keep their current rule. You can always switch services and apps rules using their corresponding popup button. Changes take effect immediately at runtime.

Changing policies has an immediate effect, however already managed apps (and services) will retain their rules.

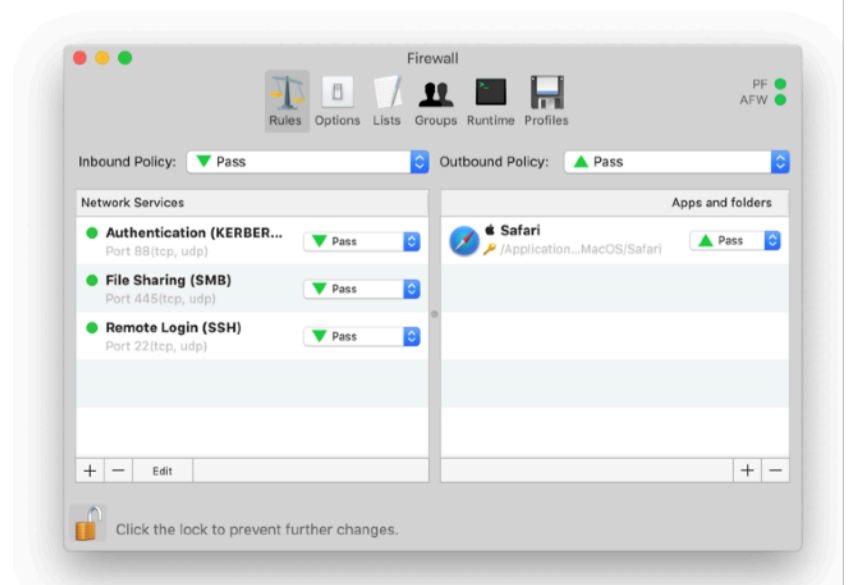
The most effective configuration is setting both policies as “Ask”: Scudo constantly monitors shared services and apps connections. At the beginning you will be requested to answer a bunch of inbound/outbound notifications, but your choices will be recorded and will be restored next time you start Scudo.

Firewall Rules

Both inbound and outbound rules are created managing lists of objects. Click the “*Rules*” toolbar button to display the Rules View. This view is divided into two subviews: **left for inbound rules** and **right for outbound rules**. All changes to firewall rules and options are immediately active at runtime.

When you run Scudo for the first time both sides of this window may be empty, specially the right side, and the default policies are set as “*Pass*”.

Use buttons and controls in this panel to set main firewall policies and to add, remove or edit firewall rules.



Inbound Rules

Main window's left side is used to secure local network services defining a policy for accessing your shared documents and resources. Additionally, it is possible to limit bandwidth for inbound connections to managed service, each service using its own independent dummynet pipe.

So if you enabled document sharing, screen sharing, printer sharing or other network services then this is the place where you can apply filters in order to block unwanted connections from remote hosts to your Mac.

This is achieved enabling a set of runtime *PF* rules to filter inbound connections. This is hidden under the hood and is transparent to the user. Runtime *PF* rules can be monitored clicking the "Runtime" button in Scudo toolbar and selecting the "Network layer" tab.

From a user perspective Scudo's inbound rules are represented by a table that lists all managed network services, each one featuring one single pass or block rule. A service is represented by a unique name, a list of ports, a protocol (*tcp*, *udp* or both) and a firewall rule.

To block a specific port simply manage the corresponding service then set it as blocked.

If you don't find any suitable service then create your own choosing from a list of predefined services or creating your own.

Inbound Policy

Scudo inbound policy can be set as inclusive, exclusive or interactive. Click the popup button on top to choose between two different policies:

- Pass (*silent*)

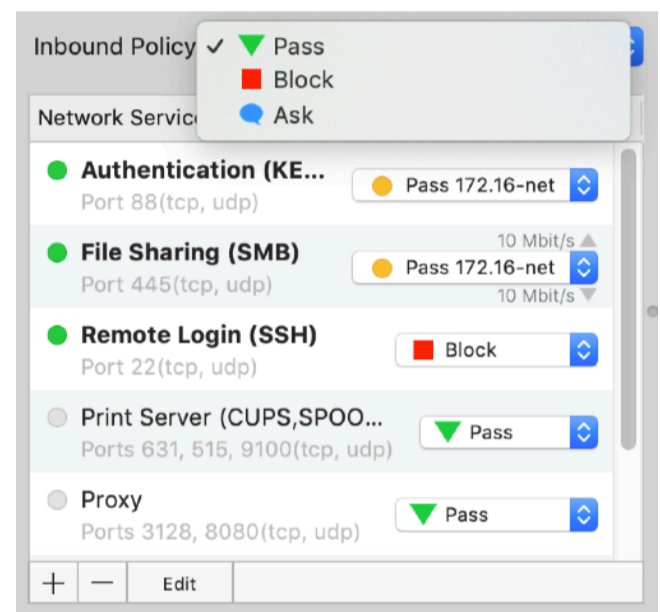
This option passes all inbound network connections by default. To block a service you need to manage it then set it as blocked. In case a new network service (listening *tcp* port) is detected Scudo will automatically add a new corresponding managed service and will set it as passed.

- Block (*silent*)

This option blocks all inbound network connections by default. To pass a service you need to manage it then set it as passed. In case a new service (listening *tcp* port) is detected Scudo will automatically add a new corresponding managed service and will set it as blocked.

- Ask (*interactive*)

When a new local network service (a new listening port) is detected Scudo **displays a notification alert**. This alert allows you to assign a pass/block rule to this service. Once done service will be added to the list of managed network services.



Inbound policy defines your firewall attitude and the behavior when a new listening network service is detected.

Set it as "Pass" if your Mac is connected to a safe and trusted network and you don't mind if someone on that network is able to access your shared documents, screens, and so on. Should you enable a new service, this will be available to everyone. This is the default setting when running Scudo for the first time.

Set it as "Block" for maximum security when your Mac is connected to an untrusted or public network. In this case you have to carefully check also managed services. Each service can be set as passed or blocked. Should you enable a new service, this will be automatically set as blocked.

Set it as "Ask" if you want Scudo to display an alert every time a new network service is detected. Doing so you will always be aware of which systems are active.

Ports Monitor

By default Scudo constantly monitors your Mac for local services listening on *privileged* or *registered* *tcp* ports (1-49151), automatically updating the services list in case new services are activated.

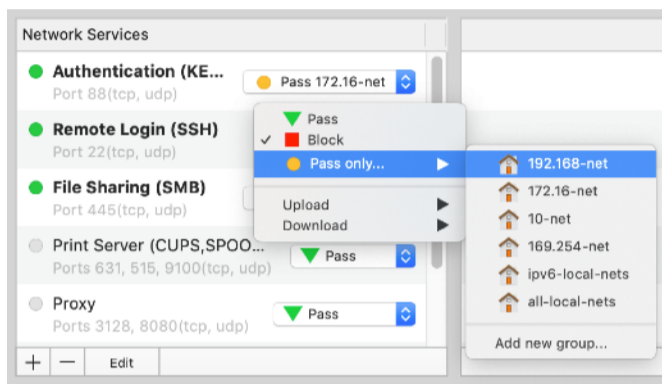
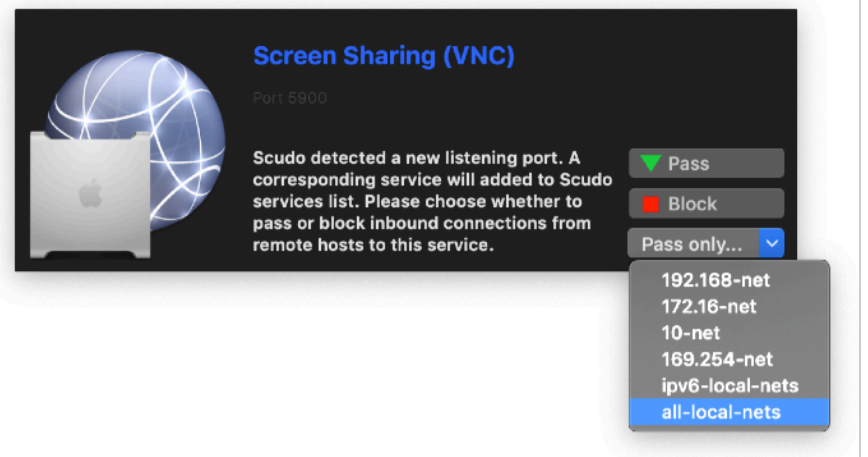
If a new listening port is detected then Scudo automatically adds the corresponding network service to the list and sets its rule according to current Inbound Policy. If current inbound policy is set to "Ask" Scudo displays a notification popup alert where the user can choose whether to pass or block inbound connections to that port. Rules are immediately applied at runtime.

Scudo ports monitor is enabled by default. It can be disabled in *Scudo Options* -> *Inbound*.

Please note that inbound policy can be set as "Ask" only if ports monitor is enabled.

Inbound notifications

If inbound policy is set to “Ask” then Scudo will popup a notification alert every time it detects a new active network service (listening tcp port). Click ‘Pass’, ‘Block’ or choose an option from the ‘Pass only...’ menu to decide whether to pass or block connections from remote hosts to that service. Once done the corresponding Scudo Service will be added to the list of managed network services. Rules are immediately applied at runtime.



Edit Inbound Rules

Use the corresponding popup button on the right to change a service rule choosing from three options: "Pass", "Block", "Pass only...". If you choose "pass only" you need also to select a *group* from the popup menu.

Services can be reordered dragging their icons. If two services has overlapping ports then services order matters: last matching rule wins, so services on the bottom always override services on top.

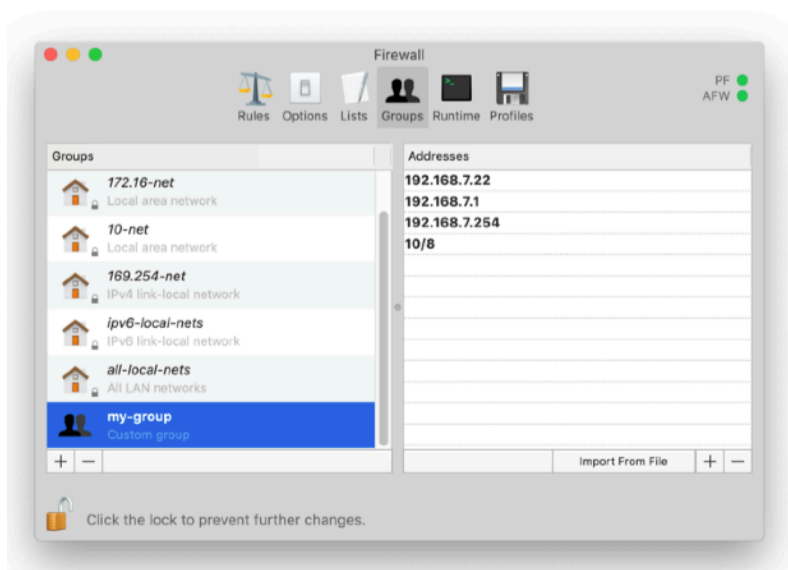
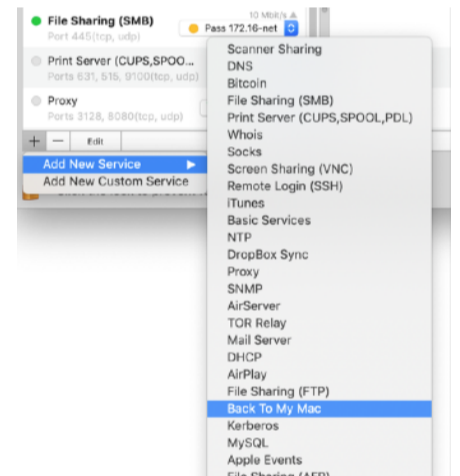
Changes to services policy are immediately active.

The PF network-layer firewall is automatically enabled every time you run Scudo and is automatically disabled when you quit Scudo.

Add new services

To manually add a network service click the “+” button. You can choose from a list of predefined network services or create a custom service.

Additionally, it is possible to automatically manage six default predefined network services, which correspond to the services you can manually enable/disable in macOS *System Preferences* -> *Sharing*. To do so select the "Always manage common services" checkbox in Scudo Options tab.



Groups

Click the "Groups" toolbar button to display Groups view. This view displays all Scudo groups. By default it includes only a bunch of predefined groups, but you can add as many custom groups as you need. Click the “+” button on the left to create a new group, then select it and click the “+” button on the right to add a new *address*. Addresses can be IPv4 or IPv6 IP addresses or CIDR network addresses. When adding addresses you can also use hostnames, however please note that they will be resolved into one or more IPv4/IPv6 addresses before being added to the list. Changes to Scudo groups are immediately active at runtime. Groups are translated into PF runtime tables.

Outbound Rules

Main window's right side is used to increase your security and privacy intercepting apps connections to the network or setting bandwidth limits for each app.

This is achieved enabling a set of runtime *AFW* rules to pass, block or intercept and hold apps connections. This is hidden under the hood and is transparent to the user. Runtime *AFW* rules can be monitored clicking the "Runtime" button in Scudo toolbar and selecting the "Application layer" tab.

Outbound rules are represented by a list of managed apps, and/or folders. Each one can be set as "Pass" or "Block". Scudo Apps and Folders view lists all managed apps and folders.

An app (or folder) is represented by a unique name, an icon, an absolute path and a rule. Each app can be set as passed or blocked independently.

At the beginning Scudo apps list is empty. It will be populated by apps icons as soon as they try to connect to the network.

It is also possible to manually add apps and folders to the list: simply drag their icons from the macOS Finder to Scudo window right side or click the "+" button. Apps and folders can be removed from the right-click contextual menu or clicking "-".

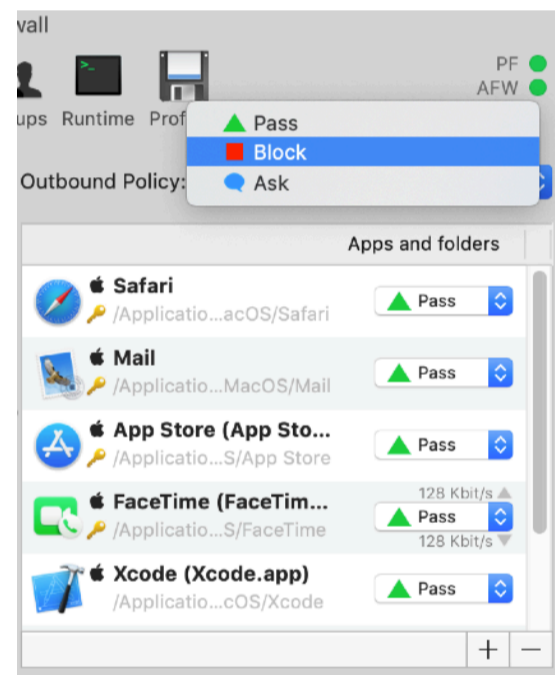
Double click an app icon to display its signature information popover.

Outbound Policy

Scudo outbound policy can be set as **silent** or **interactive**. Click the popup button on top to choose between three different policies.

If policy is set as "Pass" or "Block" then app list will be automatically populated by apps icons as soon as they try to connect to the network. Firewall will be silent, no interaction will be required.

If policy is set as "Ask" Scudo displays a notification alert every time a non-managed app tries to connect to the network. The connection is held until you choose whether to pass or block all connections by this app. Once the choice is taken the new app icon appears in apps list. When answering a notification it is possible to generate temporary rules. When a rule expires the corresponding app icon is removed from the list. Should this app try to connect to the network, a new notification alert will be displayed.



Outbound policy can be set as:

- **Pass** (*silent*)

The first option passes all apps by default. Apps list will be populated by apps icons as soon as they connect to the network. Connections will be passed.

- **Block** (*silent*)

The second option blocks all apps by default. Apps list will be populated by apps icons as soon as they try to connect to the network. Connections will be blocked.

- **Ask** (*interactive*)

The third option enables Scudo interactivity. Scudo will display a notification popup alert as soon as an app tries to connect to the network. Connection is intercepted and held until the user chooses whether to pass or block it.

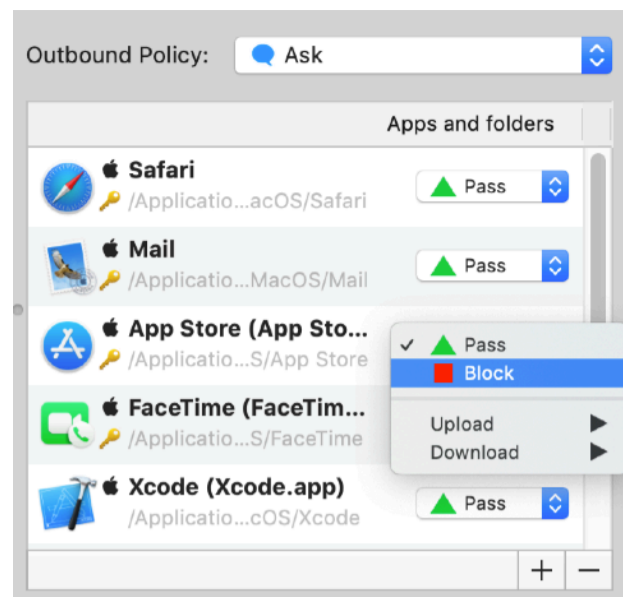
Edit Outbound Rules

To change an app or a folder rule use the popup button on the right. Each app or folder can be set as passed or blocked selecting "Pass" or "Block" from the popup button.

When an app is set as passed all connections are allowed, when it is set as blocked all connections to the network will be blocked.

By default Scudo excludes LAN from blocks. All blocked apps will be allowed to connect to local LAN addresses. The same applies to folders. This option can be disabled in Scudo Options -> Outbound.

If you add folders to the list please consider that all processes and apps included in the folder and its subfolders will heritage parent's folder rule. Please consider that order matters: if you manage a folder a one of its subfolders assigning conflicting rules, last rules wins. So the folder managed at bottom will override rule defined on top.



Changes to apps and folders policy and rules are immediately active.

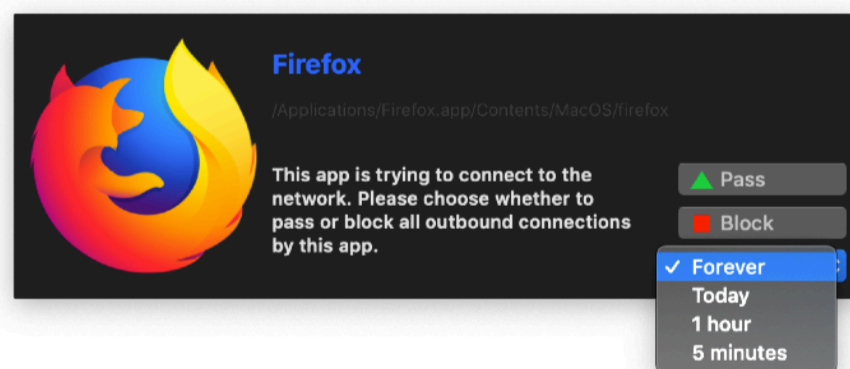
The AFW application-layer firewall is automatically enabled every time you run Scudo and is automatically disabled when you quit Scudo.

Outbound Notifications

If outbound policy is set to "Ask" then Scudo will monitor for apps connections. If an app tries to connect to the network Scudo displays a popup notification. App connection is held until you choose whether to pass or block connections by this app. Once done, the corresponding app will be added to the list of Scudo managed apps and folders. When answering notifications it is possible to choose whether to create a temporary or a fixed rule. Choose "Forever" if you want to create a fixed rule, and you want Scudo to remember your choice. Choose a different option if you want Scudo to forget your choice after some time. Once an app is managed Scudo will never show any more notifications by this app.

Notification window may **display a warning** in case:

- Process is **not signed**
- Process **signature is not valid**
- Signature **mismatch**: process path corresponds to the path of an already managed app. A managed app is not supposed to generate a new notification so this means that the signature has changed. This may occur after an update (very rare) or when an app has been tampered with or modified.



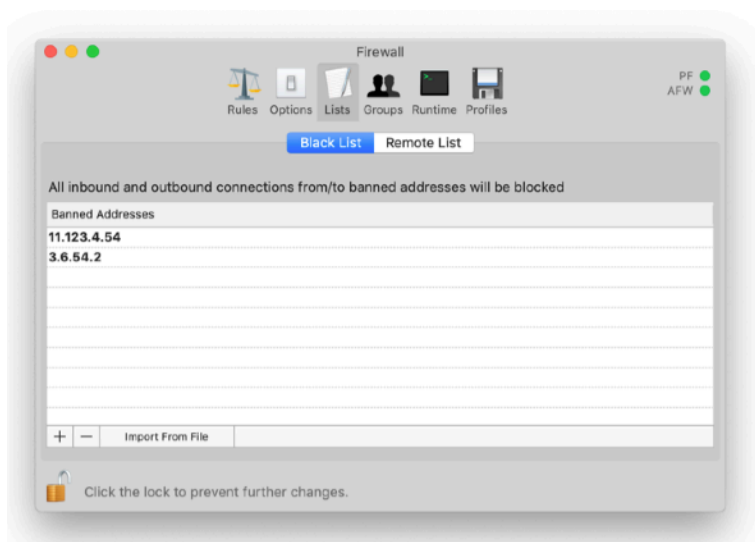
🔑 SIP: System Integrity Protection

System Integrity Protection (SIP) is a security system built into macOS and enabled by default on all genuine Macs.

This system prevents some specific files/directories from being deleted/moved/modified, even by the root user. By default SIP is applied to system folders (like /System and /usr/libexec among others) and preinstalled apps (including Safari, Mail, FaceTime).

SIP ensures that protected apps and processes are legit and genuine, and they have not been hacked or modified in any way. Being protected by SIP or not can be an important factor when deciding to pass or block a process, specially if we don't know what this process is and why it is connecting to the network.

Scudo display a key-shaped icon near SIP-protected processes and apps in order to easily identify them.



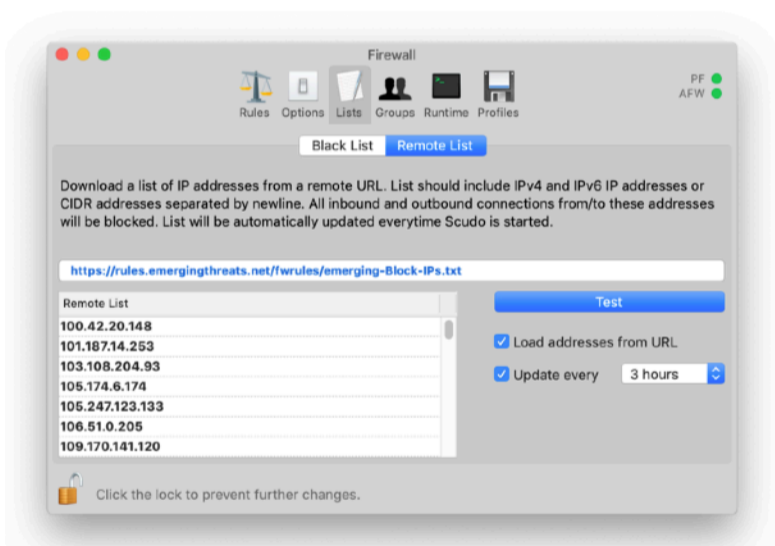
Black List

Click the “*Lists*” toolbar button to displays Lists View then select the “*Black List*” tab. Click the “+” button to add addresses to the black list, click “-“ to remove them.

Addresses can be IPv4 or IPv6 IP addressed or CIDR network addresses or hostnames. Hostnames will be resolved into one or more IP addresses.

All inbound and outbound connections from/to blacklisted addresses are blocked at network layer. Changes to the list take effect immediately.

It is also possible to add addresses to the list importing from file.



Remote Black List

Click the “*Remote List*” tab to enable Scudo remote black list. IP addresses will be downloaded from the remote server and placed in a dedicated *PF* anchor.

These addresses are hidden to the user and will be automatically updated in background every time you start Scudo.

All inbound and outbound connections from/to remote list’s addresses are blocked at network layer.

To verify if Scudo is able to read the remote IP list please type the URL then click “*Test*”. If the test is successful then you can enable Remote Black List.

Check the “*Load addresses from URL*” option to enable Remote Black List.

Scudo loads the remote IP list every time it starts. Additionally, check “*Update every*” to automatically update the list every hour, every 3 hours or every 6 hours.

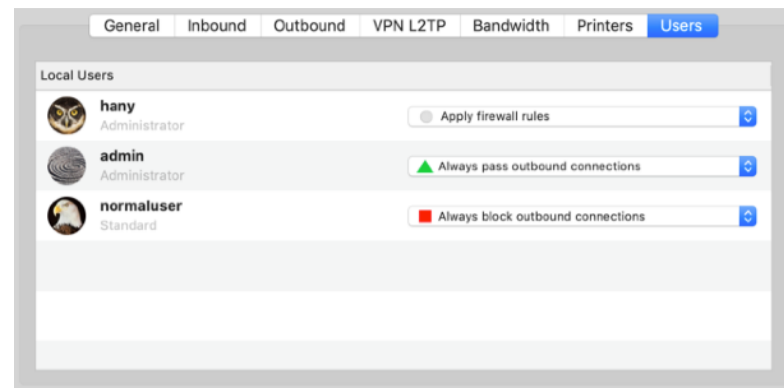
Users Management

Click the “Options” toolbar icon and select “Users” tab to display Scudo Users Management view.

This view lists all local Mac users. Users management allows the firewall administrator to assign different rules policy to users.

Each user can be set as:

- **Apply Firewall Rules:** user is subject to firewall rules defined in Scudo (default choice)
- **Always pass:** user's outbound connections are always passed, despite firewall configuration
- **Always blocked:** user's outbound connections are always blocked, despite firewall configuration



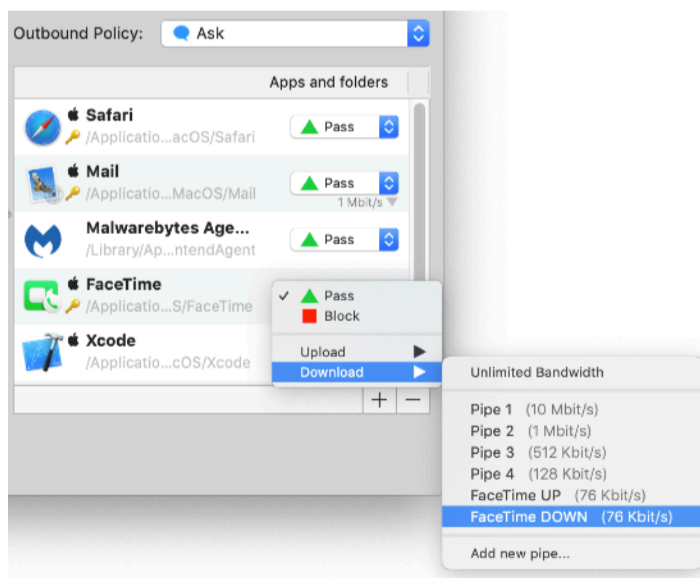
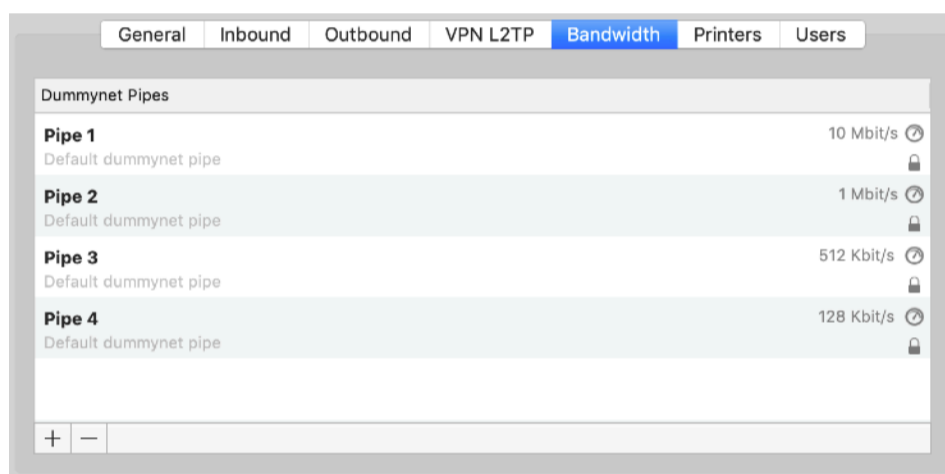
Bandwidth Management

Click the “Options” toolbar icon the select the “Bandwidth” tab to display Scudo Bandwidth Management view.

Scudo allows you to define download and/or upload bandwidth limits for both services inbound connections and apps outbound connections. This is achieved assigning **dummynet** pipes to services and apps.

Dummynet pipes are objects defined by an arbitrary name and a bandwidth value expressed in Kbit/s or Mbit/s. Dummynet is a macOS built-in kernel-level module used for traffic shaping.

By default Scudo pipes list is populated by 4 hardcoded pipes. You can add as many custom pipes as you need.



To assign a bandwidth limit to an app or a service click the popup button next to its name, select “Upload” or “Download” then select a dummynet pipe from the list. To remove a pipe from an app or service simply set it as “Unlimited bandwidth”

How to correctly apply bandwidth limits

The best results are always obtained when using different pipes for upload and download.

For example if you want to limit both download and upload bandwidth for FaceTime calls then you must assign a pipe for upload and a pipe for download. You can use the very same pipe

for both directions, but this is not the best practice.

The best solution is to create two pipes to simulate a full-duplex connection, one being used for download, the other one for upload. If you limit more apps you can assign the same pipe to different apps, however please note that the overall pipe bandwidth will be shared between those apps.

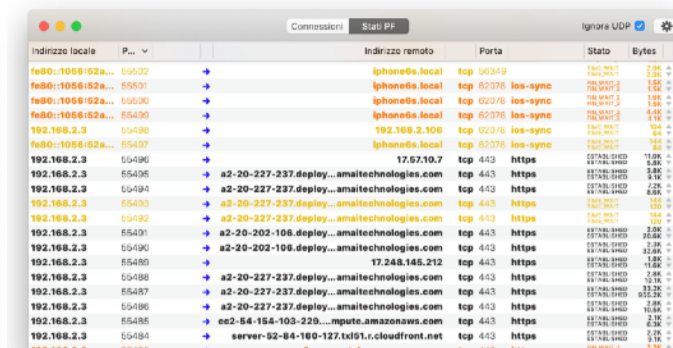
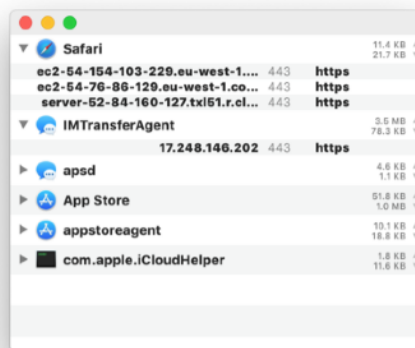
Network Monitor

Select "Network Monitor" in Scudo menulet to display *Scudo Network Monitor* window.

This view displays both current apps connections and current *PF* states.

Both **Connections** and **PF states** lists are automatically updated when a new state or connection is changed.

Connections tab displays a per-app list of connected IP addresses and ports.



PF States tab displays all pf states. A state defines a specific connection path with a flow status and traffic counters. To sort states table click table headers. Please note that this beta release of Scudo does not allow to kill pf states.

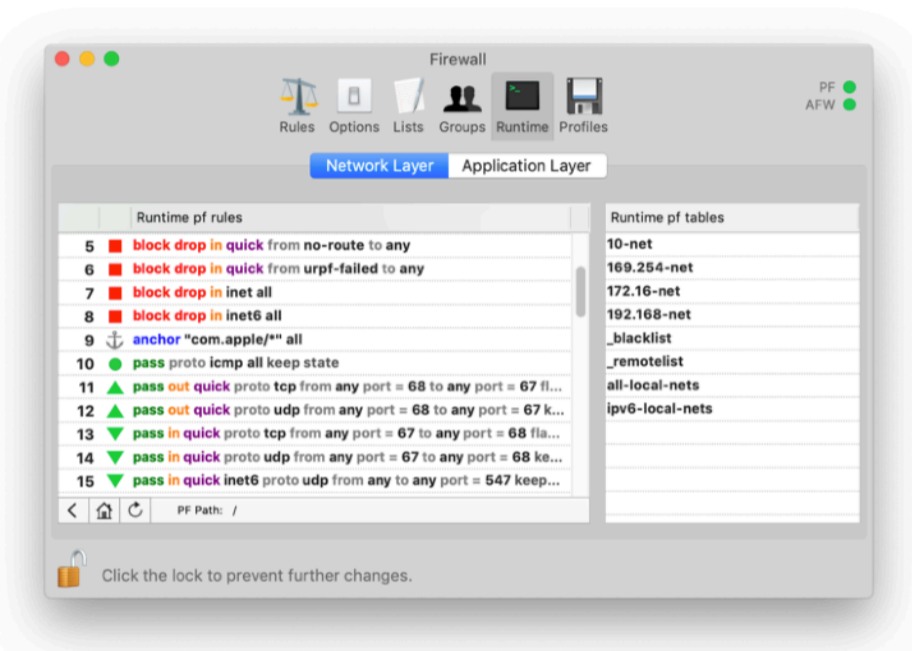
Runtime rule browsers

Click the "Browser" toolbar button to display runtime rule browsers view.

Select the "Network layer" tab to display *PF* runtime rules. This view displays *PF* runtime rules. By default it displays *PF* root anchor. Double click an anchor to browse it, click the "<" button on table footer to go back to parent anchor, click the "HOME" button to go to root anchor.

Click the "update" button in table footer to update runtime *PF* rules.

Select the "Application layer" tab to display *AFW* runtime rules. This view displays *AFW* runtime rules. When *AFW* runtime ruleset changes browser is updated automatically.



Shell terminal commands

It is possible to monitor both *PF* and *AFW* rules using the shell terminal.

To display *AFW* rules please type:

```
sudo afwctl -sr
```

To display *PF* filtering rules in root anchor please type:

```
sudo pfctl -sr
```

To display *PF* dummysnet rules in dummysnet anchor please type:

```
sudo pfctl -a /scudo.bw -sd
```

Both shell commands require root privileges.

WARNING

You should NEVER modify runtime *AFW* and *PF* rules using *afwctl* or *pfctl* while Scudo is running. This may lead to unexpected behaviors at least. Additionally, Scudo restores runtime rules every time a change is made, and everytime a background event occurs (for example a temporary rule expires or a remote black list is updated), so your runtime changes will be lost soon or later. Future releases of Scudo may include a alert system to notify if someone or something is trying to modify runtime rules outside Scudo. This limitations do not apply to system processes that add/remove rules from pf anchor */com.apple*.

Printers

Click the “Printers” toolbar button to display network printers view.

Some network printers require special firewall rules in order to be able to monitor printers queues and jobs. This view allows you to automatically manage network printers firewall rules.

Check the button in this view to automatically enable network printers spools control at network layer. Scudo automatically detects network printers on your LAN. Each time a new printer is found the corresponding firewall rules are added at runtime.

Scudo Options

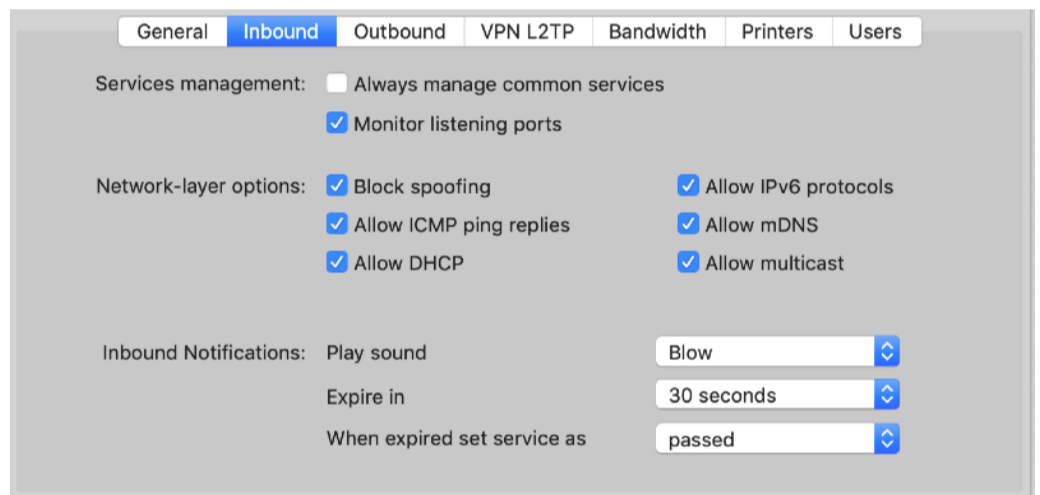
Click the “Options” toolbar button to display Scudo options view.

From this panel it is possible to set very important options that affects how your firewall works.

Inbound Options

Select the “Inbound” panel to display inbound options.

This view displays some options related to the network-layer *PF* packet filter which is used by Scudo to filter inbound connections.



- **Always manage common services**

this option is disabled by default. Enable it to automatically manage 6 well known network services, the same you enable in macOS System Preferences Sharing panel.

- **Monitor listening ports**

this option is enabled by default. Scudo constantly monitors for new listening privileged or registered tcp port.

- **Network-layer options**

this options affects the *PF* network-layer packet filter. By default all options are checked.

- **Inbound Notifications**

popup notifications are displayed if inbound policy is set to “Ask” and if a new listening port is detected and this port does not correspond to any managed service. Here you can set some very basic options for these popup notifications.

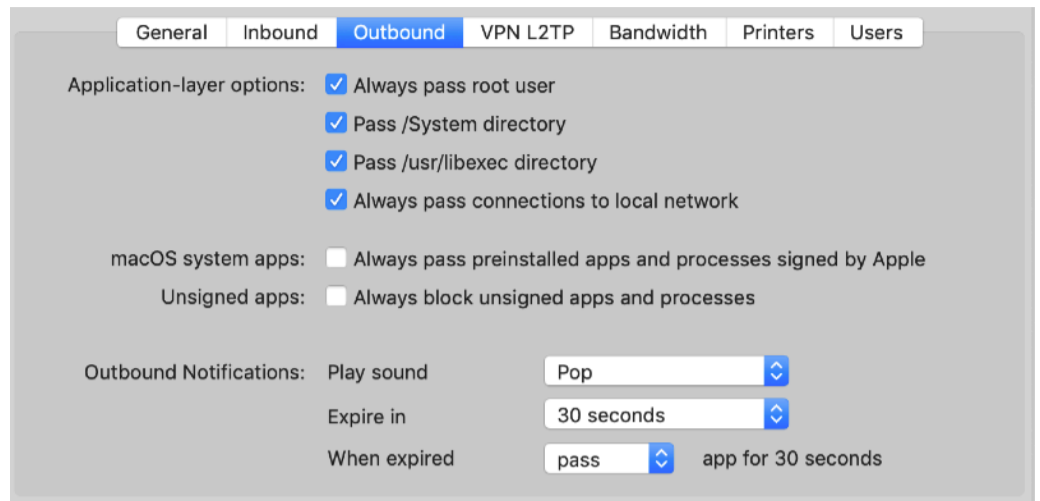
Outbound Options

Select the “Outbound” panel to display outbound options.

This view displays some options that affect the application-layer AFW outbound firewall which is used by Scudo to monitor and block applications connections.

Passing all root user connections is the safest choice, please do not change this option unless you know what you are doing.

Passing /System and /usr/libexec folders is useful in order to reduce firewall verbosity.



By default all apps are always allowed to connect to local (LAN) addresses. However to increase your security you may want to uncheck the “**Always pass connections to local network**” option.

Additionally, it is possible to set some very basic notifications options like sound, expire time and expire action.

Scudo always reads and **validates apps signatures** and warns in case an app or process is not signed or has an invalid signature.

All apps and processes installed by Apple on macOS are signed. All apps purchased on the Mac App Store are signed. Most apps distributed by third party developers on their web sites are signed. Each signature features a list of parameters used to identify the author and the app. Unsigned apps and processes should not be trusted, specially if they try to connect to the network.

In order to always block all connection attempts from unsigned apps and process check the “**Always block unsigned apps and processes**” option.

Additionally, if you trust all Apple preinstalled software and you want to be warned only in case of third-party app network activities then check the “**Always pass preinstalled apps and processes signed by Apple**”.

Match by name, by path or by signature

Scudo uses three ways to identify an app or process: by **name**, by **path** or by **signature**. It always apply the best possible approach automatically and this is transparent to the user. However it is possible to inspect runtime rules using Scudo rules browser. The general rule used by Scudo is:

- If a process is signed it is always matched by signature.
- If a process is not signed it is matched by path when passed and matched by name when blocked.

Match by signature is achieved using **AFW stamps**. Each signed app features a unique AFW stamp, a fingerprint generated by AFW combining some signature parameters. Double-click an app icon to display the signature information popover. This view includes the AFW stamp for signed processes and apps.

Additionally it is possible to generate an AFW stamp using the shell terminal command: (requires root privileges)

```
afwctl -stamp /path/to/app
```

Please note that an AFW stamp is not a hash. While a hash changes when app is updated, the AFW stamp is supposed to be consistent over updates. However some exceptions are possible so it’s up to you to verify app authenticity in case Scudo warns you about a signature mismatch.

VPN options

Select the “VPN L2TP” panel to display VPN options.

This option allows you to force all your traffic through a VPN. In order for this feature to work you must use a plain L2TP vpn setup configured using macOS tools like System Preferences or the Terminal.

Most VPN services based on proprietary clients will not work because the client itself needs a clean http connection to authenticate before opening the VPN channel. Enabling this option in Scudo blocks proprietary VPN clients authentication.

Technical information

Scudo is designed to automatically start at user login. *PF* and *AFW* firewalls are enabled as soon as Scudo is launched and is disabled as soon as Scudo is quitted.

PF is the kernel-level network-layer packet filter. Scudo uses *PF* to filter inbound connections, to throttle bandwidth and to display *PF* states. **PF is built into the macOS kernel, is part of the operating system.**

AFW is the kernel level application-layer socket filter. Scudo uses *AFW* to filter outbound connections from apps and to manage users. *AFW* is also the core of *Vallum*, a much more sophisticated application-layer firewall front end. **AFW has been developed by The Murus Team and first appeared in Vallum 3.0.**

Dummynet is a macOS built-in *PF* module, it is used by *PF* for traffic shaping. Scudo uses *dummynet pipes* to define download and/or upload bandwidth limits. Services limits are defined by dummynet rules created by Scudo. Apps limits are defined by dummynet rules created dynamically by *scudodummynetd* and featuring a dedicated label used to identify the app. All dummynet rules are stored in a dedicated *PF* anchor named *scudo.bw*.

Scudo Monitor.app is an independent app and is stored inside Scudo app bundle. *Scudo Monitor.app* uses its own privileged helper *scudomonitord* in order to perform privileged operations. *Scudo Monitor.app* will request administrator password to install its helper the first time you run it, or in case it needs to update an old helper. *Scudo Monitor.app* runs when you click “*Network Monitor*” from Scudo menulet. *Scudo Monitor.app* does not display any icon in the dock or in command-tab apps list. The process will quit when its last window is closed.

File List

This release of Scudo installs these files on the system:

<i>/Library/Extensions/afw.kext</i>	• <i>AFW</i> Network Kernel Extension
<i>/Library/PrivilegedHelperTools/it.murus.afw.helper</i>	• <i>AFW</i> privileged helper
<i>/Library/Application Support/Scudo/Scudo.app</i>	• Scudo app bundle
- <i>scudodummynetd</i>	• Dummynet management daemon, included in Scudo app bundle
- <i>Scudo Monitor.app</i>	• Network monitor app, included in Scudo app bundle
<i>/Library/PrivilegedHelperTools/scudomonitord</i>	• Network monitor privileged helper
<i>/Library/LaunchDaemons/it.murus.afw.core.plist</i>	• script to load <i>AFW</i> kext at boot
<i>/Library/LaunchDaemons/it.murus.afw.helper.plist</i>	• script to load <i>AFW</i> helper at boot
<i>/Library/LaunchAgents/it.murus.scudo.plist</i>	• script to run Scudo at login
<i>/usr/local/bin/afwctl</i>	• shell terminal <i>AFW</i> frontend
<i>/etc/scudo.conf</i>	• Scudo configuration (saved on exit)

To uninstall Scudo we strongly suggest you to use the provided **Scudo Uninstaller** located in Scudo DMG.

For more information please contact info@murus.it

<https://www.murusfirewall.com/scudo>

