Documentation

Little Snitch 3
Learn more about networking basics, how to configure the network filter with rules and how to switch sets of rules quickly with profiles.
Network Basics

We all know the experience of surfing the Internet with a web browser, receiving and sending emails etc., but what happens under the hood? We’ll try to explain some of that here. At least enough to understand the terms and concepts used by Little Snitch.

A simple example:

Let’s see what happens when we open a web page in a browser and watch the steps as they occur one after the other.

1. You enter http://www.obdev.at/index.html into the address field of a web browser and type Enter.

2. The browser dissects the URL into a schema (http://), a hostname (www.obdev.at) and a document path (index.html).

3. The browser resolves the hostname www.obdev.at to an Internet address (IP address). It uses the Domain Name System (DNS) for this purpose. We have dedicated a section of its own to DNS. All we need to know here is that it returns an IP address for the name, e.g. 78.46.114.187.

4. From the schema, the web browser knows that we want to connect to the http service. This is a well known service and the Internet Assigned Numbers Authority (IANA) has assigned the port number 80 to this service. Learn more about ports...

5. The web browser has obtained a remote IP address and remote port number now. That’s enough to establish a connection. The operating system supplements this information with your computer’s IP address and a random local port number and establishes a Transmission Control Protocol (TCP) connection. Learn more about connections...

6. The remote computer (server) accepts the connection.

7. The web browser sends the string GET /index.html HTTP/1.0 to the server. (Our example uses a very old web browser for simplicity. Today’s web browsers use HTTP 1.1 requests.)

8. The server responds with the page content on the same connection.

9. The server closes the connection.

10. Your web browser can now render the page and repeat the procedure for resources referenced by the page such as images.

You may have noticed a similarity to phone calls: A connection is established by one of the two parties, the other accepts the connection and then they exchange data until one of the two hangs up. We’ll use this analogy throughout the rest of this chapter.
The Domain Name System

The protocols mentioned so far work with numeric addresses only. Since humans prefer to use (hierarchical) names, there must be a service that translates between names and numeric addresses, similar to a phone book. This service, the Domain Name System (DNS) is a distributed database available via UDP and TCP port 53 (and 5353 for automatically assigned addresses in the local network).

Your computer sends queries to your Internet provider’s name servers, which in turn query the servers responsible for the requested domain and cache the result.

The Domain Name System primarily resolves names to addresses. One name can resolve to multiple addresses and the addresses can change over time. If you want to experiment with DNS, try the host Unix command in Terminal. It takes one parameter: the name to resolve. There’s a second database available in the DNS, the database of reverse mappings. You can query this database with numeric addresses and receive exactly one hostname for the address. The host Unix command does a reverse lookup if the parameter is a numeric address.

There is one important fact to note: The reverse lookup name of an IP address is rarely the hostname you used to look up the address in the first place.

For instance:
$ host books.google.com
books.google.com is an alias for www3.l.google.com.
www3.l.google.com has address 209.85.148.113
www3.l.google.com has address 209.85.148.138
www3.l.google.com has address 209.85.148.139
www3.l.google.com has address 209.85.148.100
www3.l.google.com has address 209.85.148.101
www3.l.google.com has address 209.85.148.102
www3.l.google.com has IPv6 address 2a00:1450:4001:c01::64

$ host 209.85.148.113
113.148.85.209.in-addr.arpa domain name pointer
rfra07s07-in-f113.1e100.net.

As you can see, Google returns a totally cryptic name when we query an IP address obtained for books.google.com.

Another important fact to note is that multiple names can resolve to the same address or have an overlapping set of addresses:

$ host maps.google.com
maps.google.com is an alias for maps.l.google.com.
maps.l.google.com has address 209.85.148.101
maps.l.google.com has address 209.85.148.102
maps.l.google.com has address 209.85.148.113
maps.l.google.com has address 209.85.148.138
maps.l.google.com has address 209.85.148.139
maps.l.google.com has address 209.85.148.100
maps.l.google.com has IPv6 address 2a00:1450:4001:c01::64

Both, maps.google.com and books.google.com use the same servers. If you repeat the query later, you may receive a different set of addresses.

You now know that IP addresses and hostnames have a somewhat weak correspondence. This has important consequences for Little Snitch.

Learn more about how Little Snitch copes with multiple names for an address...
Terms and Concepts used in Networking

After looking at the basic step by step procedure of a network request we now present the details and explain the terms used there.

Internet Address

In the metaphor of a phone call, an IP address is the phone number of a computer. You must know the computer’s IP address in order to send any information to it.

In version 4 of the Internet Protocol (IPv4), each computer connected to the Internet is identified by a worldwide unique 32 bit number between 0 and ca. 4 billion, its IP address. Version 6 of this protocol (IPv6) allows an even much, much higher number of computers.

For readability, IP addresses are written in groups of digits. IPv4 addresses are written as 4 groups of up to 3 digits each, separated by a dot (e.g. 78.46.114.187). Each group has a valid numeric range of 0-255. IPv6 uses 8 groups of up to 4 hexadecimal digits each, separated by a colon (e.g. 2a00:1450:4016:801::1013).

Since these addresses are long, there are ways to abbreviate. A range consisting of zeros only can be written as double-colon. The address in the previous example would then be: 2a00:1450:4016:801::1013. The address 0000:0000:0000:0000:0000:0000:0000:0001 can simply be written as ::1, or an address consisting of zeros only can be written as ::.

Port Number

Since a computer can be responsible for more than one task, its IP address is not sufficient to address all services it provides. Processes on the server can acquire a port (identified by a 16 bit number in the range 0-65535) and provide a service on that port. In the metaphor of a phone call, the IP address is the phone number of a big company and the port number is the extension to dial directly to a particular person.

Well known services, such as HTTP (web sites), HTTPS (secure web sites), SMTP (sending email), SSH (secure shell), etc. use well known port numbers. The Internet Assigned Numbers Authority (IANA) maintains a long list of well known services and their assigned port numbers.

Protocol

A protocol is a convention how data is transferred from one computer to another. The protocol specification says what an address looks like (e.g. 32 bit IP address plus 16 bit port number), what other information is added, in which order the components are sent over the wire, and so on. We distinguish connection-oriented protocols (such as TCP) from connectionless protocols (such as UDP).

A connection-oriented protocol is analogous to a phone call. There’s one computer which initiates the connection (= starts the phone call by dialing a number) and another one which accepts it (= picks up the phone). The connection lasts until one of the participants closes it (= hangs up the phone). While the connection is up, each computer can send data to the other (= speak) at any time. The computers may use any format or sub-protocol (= language) they like, as long as they agree on something.

A connectionless protocol is similar to postal mail. Data is sent in packets to the remote address. The remote address may or may not exist and the protocol may provide some feedback whether the data has been delivered.
or not. A data packet (a letter) is always unidirectional. The remote computer may respond with another packet directed to the sender, or it may not.

Note: Little Snitch cannot delay incoming connectionless data, because that would not stop the sender from sending more packets and an indefinite amount of data could pile up. It therefore can't display a Connection Alert which would cause an unpredictable delay. Even if Little Snitch would store an unlimited amount of data during the alert, the data would be outdated as UDP is usually used for real-time information where speed matters. Little Snitch allows incoming connectionless data, but creates rule suggestions.

Connection

For a phone call, a connection is completely identified by the phone number which calls and the phone number which was called. In TCP, addresses consist of an IP address and a port number. Connections are therefore completely identified by the IP address and port number of the computer initiating the connection and the IP address and port number of the computer accepting it.

IP addresses are assigned by Internet Providers. When you connect to the Internet, your computer automatically receives an IP address. The remote port number is determined by the service you want to reach (e.g. port 80 for HTTP). But what determines the port number on the caller’s side? The operating system chooses a random free port number (usually above a certain minimum, often above 48,000). This random port number has no particular importance (other than identifying the connection) and is never displayed by Little Snitch.

Internet Protocol (IP)

Protocols are layered (OSI model). Each layer builds on the services provided by the layers below it. The lowest layer we deal with is the Internet Protocol (IP) layer. The Internet is IP only. The Internet Protocol defines what IP addresses look like (see above) and how data packets are sent from one computer to another. IP requires another protocol layer on top of it, it cannot be used by itself.

Transmission Control Protocol (TCP)

TCP is a protocol layered on top of IP and offers ports and connection oriented bidirectional transfer of data streams. It ensures delivery even if IP data packets are lost between sender and recipient (by doing retries) and it ensures that all data is delivered in order (no part of the data can overtake other parts). These features make it the favorite for almost all services on the Internet. It is used for serving web pages, delivering email, file sharing, etc.

User Datagram Protocol (UDP)

UDP is the minimum addition to IP to make it useful for applications. It adds ports to IP, but neither guarantees delivery of packets nor delivery in order. UDP is used for real-time multimedia content such as Voice-Over-IP or other applications where it’s better to lose a packet than wait for a retry.

Internet Control Message Protocol (ICMP)

This protocol is also a minimum addition to IP. Contrary to UDP it does not add a port number to the address and is rarely used by applications. Most of ICMP is used by the operating system kernel itself (the IP stack) to administer data transmission in other protocols (e.g. destination port unreachable messages etc.). However, there’s one exception to this rule: The ping Unix command, which sends an ICMP request to the remote computer and listens for a response. It then dumps the requests sent and responses received. This information is useful for network debugging.
How Little Snitch does its work

Why is Little Snitch different?

Little Snitch works differently from conventional firewalls. A conventional firewall intercepts at a logical layer close to the network adapter. It therefore can filter based on all parameters in the protocol headers, usually source and destination addresses, protocol and port numbers.

Learn more about protocols, addresses and port numbers...

Little Snitch, on the other hand, intercepts at a logical layer very close to the application. The data has not been assembled into protocol packets at this layer and many of the protocol parameters (local port number, which network interface is used, packet size) are not yet available. However, instead of these parameters, Little Snitch knows the process which sends or receives data, and that is very valuable! Filtering rules can be based on process paths, not just protocol parameters. And Little Snitch can ask the user as if it was part of the application.

How is it implemented?

Little Snitch intercepts close to the application layer, but does not modify processes in any way (it does no code injection of any kind). Instead, it registers a Kernel Extension utilizing standard API calls provided by Apple. No hacks, no undocumented features, no reverse engineering. At the kernel level, however, remote computers are referenced by IP address only. The hostname used to obtain the IP address is not available in the kernel. This has important consequences for Little Snitch.

Learn how Little Snitch copes with multiple names for an address...
Rules

The filtering behavior of Little Snitch is defined by a set of rules. A rule consists of four parts:

- **Condition**
- **Action**
- **Lifetime**
- **Annotations**

If a connection attempt meets the condition of a rule, the rule's action will be performed. If more than one rule matches a particular connection attempt, the one with the highest precedence defines the action to be taken. The precedence of a rule is derived directly from its properties.

**Condition**

A rule matches a connection attempt if all of the following properties match:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection direction</td>
<td>Incoming or outgoing connection</td>
</tr>
<tr>
<td>Process</td>
<td>Applications like Safari or Mail, or Unix processes like storeagent, ntpd, etc.</td>
</tr>
<tr>
<td>Process owner</td>
<td>The user who started the process</td>
</tr>
</tbody>
</table>

**Action**

A rule's action can be one of the following:

- **Allow** – The connection is allowed in the same way as if Little Snitch were not installed.
- **Deny** – The connection is denied. The process attempting the connection receives an error, similar to a network failure.
- **Ask** – Little Snitch shows a Connection Alert and asks the user what to do. That’s also the default action if no rule matches.

**Lifetime**

Little Snitch rules can expire at a certain point in time when the rule's lifetime is over. When a rule expires, it is deleted and a rule suggestion for the expired rule is created. Rule lifetime options are:
• **Forever** – The rule never expires.

• **Until Quit** – The rule expires when the last instance of the process that matches the rule terminates.

• **Until Logout** – The rule expires when the user who created the rule logs out.

• **Until Restart** – The rule expires when the computer is restarted.

• **Lifetime in Minutes** – The rule expires a certain amount of time after it was created.

• **Once** – The connection is allowed or denied exactly once. No rule is created and as soon as another connection is attempted, Little Snitch shows a new connection alert. This option is only available in the Connection Alert, it can never be a property of a rule.

**Annotations**

Rules have properties which have no effect on the network filter. They are for maintenance and information purposes only. These properties are:

• **Protected** – Protected rules are part of the factory rule set. They are crucial for your system to work properly and hence cannot be deleted. You can still disable them, if you know what you are doing. Little Snitch Configuration uses a lock icon to tag these rules.

• **Unapproved** – Rules created automatically are marked as unapproved. As a preferences option (preferences section Advanced”), rules created from the Connection Alert can also be set to unapproved. To approve a rule, right-click it and choose Approve from the context menu. If the preferences option Approve rules automatically (also in the Advanced section) is on, rules are approved by selecting them.

• **Creation Date** – Little Snitch Configuration displays the date and time when a rule was created in the right sidebar (Info bar) close to the bottom edge.

• **Notes** – Rules can have comments. All rules shipped with the factory rule set have a comment describing their purpose. Rules created from a connection alert contain the information presented in the connection alert in their notes. You can edit the notes at any time.

Note that rule editing can be disabled for particular users in Little Snitch Configuration > Preferences > Security. This affects all rules (not only protected rules) and prevents them from being created, edited, enabled, disabled or deleted.

**Rule precedence**

We have already mentioned above that of all matching rules, the one with the highest precedence determines the action taken. But how is the precedence computed?

The general concept is that more specific rules take precedence over (they override) more general rules. If a profile is activated, rules in this profile take precedence over all rules not assigned to a profile.

**Sort by precedence**

Within the context of a single process, the rules are always sorted by precedence. If you want to get the entire list of rules sorted by precedence, do one of the following:

• Choose View > Sort By > Precedence

• Click the header of the “Rule” column in the rule list

Rules with higher precedence (overriding others) are listed first, so the first matching rule (from top to bottom) determines the action. Rules with equal precedence are sorted alphabetically by process name.
How rules are matched against connections

If all of the following properties match their respective connection parameters, a rule matches:

**Enabled**

Rules can be enabled or disabled. Disabled rules never match, they behave as if they had been deleted. However, the information stored in the rule is not lost, the rule can be re-enabled at any time. This property is particularly useful for protected rules (they cannot be deleted) or if you want to test what effect it would have if a particular rule were deleted.

**Connect Direction**

A rule can match either outgoing or incoming connections. An outgoing connection is when a process on your computer initiates a connection to somewhere else. In the metaphor of the phone call, your computer dials phone number to call somebody else. An incoming connection, on the other hand, is when a remote computer initiates a connection to a process on your computer. Your computer acts as a server in this case. In the metaphor of a phone call, this is when your phone is ringing.

**Process**

A process is an Application (an “App”) with user interface, a background process (Unix daemon) needed by the system to perform certain tasks (e.g. sync your data to the cloud) or a Unix command with no graphic user interface. Processes are matched by their file system path (where they are stored on your disk).

Applications may execute Unix commands to do things on their behalf. If Little Snitch encounters a Unix command which has been started by an Application, it shows both, the Unix command and the Application, e.g. "Terminal via ping". Rules matching the Application will match this combination as well. However, you can also create rules which match a particular combination of Application and Unix command only (Via-Rules).

**Process Owner**

Processes have an owner. The owner is usually the user who started the process. This user can also be the operating system (denoted as “System” by Little Snitch). Processes started by a user can gain system privileges by asking for an admin login.

Processes owned by the system are often of particular importance because they provide services for all users on the computer, not just for you. Rules matching processes owned by the system are therefore global, they are shared by all users. When Little Snitch shows a Connection Alert for a system process, it prepends the process name with a gear wheel icon:
The same icon is used to flag rules matching system processes only.

In addition to matching processes owned by the current user (“me”) and the system, Little Snitch rules can also match processes owned by anyone. These rules show up in all users’ rule sets (they are global) and also match processes owned by the system. Since rules of this type have an effect on all users, the permission to create them must be enabled in Little Snitch Configuration. Open Little Snitch Configuration > Preferences > Security & Privacy and turn on Allow Global Rule Editing.

Server

This property eventually defines a set of Internet addresses. The rule matches, if the remote address is in the set of Internet addresses. Addresses can be specified numerically, by providing a list of DNS hostnames resolving to addresses or as special placeholder for Internet addresses obtained elsewhere.

- **Numeric Sets** – Addresses can be entered as single IP address (e.g. 10.0.0.1), a range of addresses (e.g. 10.0.0.1-10.0.0.9), a range in CIDR notation (e.g. 192.168.0.0/16) or a comma separated list of addresses and ranges. Learn more about internet addresses...

- **DNS Hostnames** – A comma separated list of one or more hostnames, e.g. www.apple.com, store.apple.com. The rule property matches all connections where the remote IP address was obtained by resolving one of the names in the list. This type can be used for outgoing connections only, since no name to address resolving occurs for incoming connections. Learn more about rule matching by hostname...

- **DNS Domains** – A comma separated list of one or more DNS domains, e.g. apple.com. Similar to matching DNS hostnames described above, but matches all remote IP addresses which were obtained by resolving a hostname in one of the domains or the hostname is equivalent to one of the domains.

- **Local Network** – This placeholder represents IP addresses of all computers which you can reach without going through a router. In practice, these are usually all computers in your home or office or in the same Internet Cafe.

- **Broadcast and Bonjour Addresses** – These are special addresses in the local network. They are used for automatic detection of services.

- **Multicast Addresses** – These are similar to broadcast addresses, but not necessarily local to your network. They are used for automatic service detection and (not yet) used for efficient content delivery.

Port

A destination for an outgoing connection is defined by an IP address, a protocol and a port number. For outgoing connections, the rule matches if its port matches the connection’s remote port. For incoming connections, the rule’s port must match the local port where the connection is accepted.

Rules can match either a single port or a range of port numbers (e.g. 137-139) or any port.

Learn more about internet addresses, protocols and ports...

Protocol

A rule can match on particular protocols only (usually TCP, UDP or ICMP), or on any protocol.

Learn more about protocols...
Rule Suggestions

**What’s the difference between rules and suggestions?**

While rules define how traffic should be filtered, suggestions have no effect whatsoever on the network filter. Rule suggestions have the same set of properties as rules, but they usually don’t have an action.

Suggestions can be converted into rules easily. They are displayed in special sections of Little Snitch Configuration’s sidebar:

**How are rule suggestions created?**

When Little Snitch has to allow or deny a connection automatically, when no rule matches and no Connection Alert can be shown, or when a rule is automatically deleted because it expired, a rule suggestion is created from the connection or deleted rule.

Suggestions are displayed in groups in Little Snitch Configuration, representing the type of event that led to the suggestion:

- **Login Connections** – While no user is logged in or a login is in progress, Little Snitch cannot display Connection Alerts. It therefore creates suggestions for all connection attempts it sees.

- **Incoming Connectionless** – Since Little Snitch cannot show a Connection Alert for incoming data packets in a connectionless protocol such as UDP or ICMP, it allows these packets when there is no matching rule, but creates a rule suggestion for each new set of connection parameters encountered.

- **Silent Mode Connections** – In Silent Mode, instead of showing a Connection Alert, Little Snitch either allows or denies (depending on the type of Silent Mode) all traffic that is not covered by a rule. A suggestion is created for each new set of connection parameters encountered.

- **FullScreen Apps** – When a running application is circumventing the Window Server by using the graphics adapter directly (e.g. a game), Little Snitch is not able to show a Connection Alert. It therefore automatically denies any connection attempt from the full screen application (it creates a temporary deny-rule), speaks a notification through audio output and converts the temporary rule into a suggestion when the application quits.

- **Alert Timeout** – Little Snitch can be configured to automatically answer Connection Alerts after a timeout (Confirm connection alert automatically preferences setting). Alerts answered this way create an “Until Quit” rule, which is converted into a rule suggestion when it expires.
• **Expired Temporary Rules** – When a temporary rule expires, it is converted into a rule suggestion.

• **Invalid Rules** – This section actually contains rules, not suggestions. However, these rules cannot have an effect because the process they refer to has been deleted or moved. You may want to change the rule’s process path or delete the rule.

• **Redundant Rules** – This section also contains rules and not suggestions, but the rules have no effect because they are overruled by a higher precedence rule. These rules can safely be deleted, unless you plan to delete or disable the overriding rule. As an option selectable in the top bar, the overriding rule can be displayed as well, distinguishable with a “Priority Road” traffic sign.

**What can be done with rule suggestions?**

The purpose of rule suggestions is that they can be converted into rules conveniently. It is easy to browse over a handful of suggestions and decide which of them should be turned into rules and what detail level they should have (whether the rule should be for any process, any server or a particular domain etc.).

However, if there are hundreds of suggestions in a section (e.g. after running Little Snitch in Silent Mode for a while), you’ll find yourself asking for help. Little Snitch provides the following: Depending on the detail level you have chosen for the Connection Alert, suggestions are automatically grouped by the hidden properties. For instance, if you hide both, port and protocol, all suggestions for the same process and server will be shown in one line, regardless of the port and protocol used in all the connections that occurred.

Little Snitch can do even more than that. It can group by any of the remaining properties. Let’s look at an example. Say you have disabled or deleted any rules for Safari and entered Silent Allow Mode. Now you browse the web a while and look at the suggestions. For this example we assume that you configured the Connection Alert to show the port number, but not the protocol. Little Snitch Configuration now shows lots of suggestions in “Silent Mode Connections”. You will see all web sites you visited, but you’ll very likely also see sites collecting statistics, sites delivering ads and so on. We browse the list and watch out for names which contain the word “ad” or similar. We can simply create deny-rules for these sites by clicking the “Deny” button in the top bar.

When we are done with all the advertising sites, there’s still a whole bunch of other entries. We try the Group by Host option in the top bar. This reduces the number slightly, as secure and non-secure requests to the same server are collapsed into one line. Not what we want. We now try Group by Domain. This option collapses all requests to different hosts in the same domain into one line. www.apple.com, lists.apple.com and shop.apple.com are now all collapsed into apple.com. Better, but still too much to cope with each suggestion individually. Then we try Group by Port. We are left with a hand full of lines, usually two: Connections to port 80 and connections to port 443. We see that web browsing uses primarily these two ports. If we want to be restrictive but still allow browsing to any site, we allow these two ports. If we are permissive, we may allow Safari any Internet connection.

If we had done the same analysis for a different application, we might have found good results when grouping by host or domain.
Profiles

Profiles are a means to switch between rule sets easily. When rules are matched against a connection attempt, all rules in the current profile are considered first. If no match is found in the profile, all rules not assigned to any profile are taken into account. The applications of this simple concept are manifold:

Profiles for different types of network

This is obvious, but still very handy:

- **Public Network** – If you are in a public network, e.g. an Internet Cafe, you want to forbid incoming connections from everywhere (including local network) to all the handy sharing services you have enabled for your friends. You may even want to deny mDNS (port 5353) so that others can’t even see your computer’s name. If you still use mail accounts with plain text password authentication, you probably want to forbid these as well.

- **Expensive Network** – Sometimes your computer connects to a network with horrendous prices per gigabyte, e.g. 3G or other mobile networks. It’s not the best idea to update iTunes, download podcasts or perform a backup of your computer over the net while in one of these networks. Simply deny Internet access for all of these services while in an expensive network.

Little Snitch can switch profiles automatically when particular networks are joined, see Automatic Profile Switching.

Profiles for different types of work

Certain types of work may not admit distraction by Connection Alerts. If you give a presentation on a beamer, you probably don’t want any Connection Alerts to interrupt. On the other hand, if you test a suspicious piece of software, you may want to be super-careful and allow nothing which is not absolutely required for proper system operation.

Profiles for particular situations

When you suspect that something went wrong and some malware is already trying to send the file with all your passwords out to the Internet, you want a way to stop it quickly. This can easily be achieved with a profile containing one rule for outgoing connections by any process, owned by anyone, to any server, any port and any protocol and one rule for incoming connections with the same properties.
Automatic Profile Switching allows you to associate different networks (for example your Wi-Fi network at home, a public hotspot, etc.) with certain profiles in Little Snitch. Whenever you join one of these networks, Little Snitch detects the network change and switches to the associated profile automatically.

This allows you to automatically apply different sets of filter rules depending on the network you are currently connected to. You can for example use a rather restrictive ruleset in an Internet Cafe, a more permissive set of rules at home or when connected to a VPN, or rules that block software updates while using your mobile phone’s expensive data connection via tethering.

When you join a network for the first time, Little Snitch shows an alert window allowing you to choose the desired profile. Alternatively, you can configure a default profile that will be used for all unknown networks.

The mappings between profiles and networks can be reviewed and edited later in Little Snitch Configuration, either in the profiles section of the sidebar, or in the Known Networks Window (⌘K).

**How does Automatic Profile Switching work?**

Whenever you join a Wi-Fi network, connect to the Internet using your mobile phone’s data connection or plug in an Ethernet cable, your computer’s network configuration changes. Little Snitch observes these changes and checks if the new configuration matches an already known network. If it does, a previously configured action is taken:

- Activate a profile that’s associated with this network.
- Deactivate the currently active profile.
- Do nothing, thus ignore the network change.

Whenever Little Snitch changes or deactivates the currently active profile automatically, a notification alert is shown in the upper-right of your screen.

**Enable Automatic Profile Switching**

Automatic Profile Switching is disabled by default. It can be enabled in Little Snitch Configuration > Preferences > Automatic Profile Switching.

For dealing with unknown networks that you haven’t joined before, you can choose between two modes of operation:

- **Ask** – Shows the Profile Switching Alert where you can decide how to proceed, and where you can map the network to one of your profiles. This mode is recommended if you join new networks only occasionally.
- **Activate a profile** – In this mode a configurable default profile is activated whenever an unknown network is joined. This may be preferable if you travel a lot, joining many different networks, but each of them only once.
If the Save geolocations of networks option is enabled, Little Snitch stores the geographic coordinates of the network’s location when you join it. You can then later display the locations of all networks that you’ve joined in the map view of the Known Networks Window.

**The Profile Switching Alert**

When you join a yet unknown network, Little Snitch pauses all network traffic to prevent your computer from sending any information into a potentially insecure network. The Profile Switching Alert appears and only after you have dealt with it network traffic is resumed.
The alert window lets you decide how to deal with this network now and in the future:

- **Do Nothing** – Does not activate or deactivate any profile.
- **Deactivate Active Profile** – Deactivates the currently active profile.
- **Activate Profile** – Activates one of your existing profiles.
- **New Profile** – Creates and activates a new profile.

Alternatively, you can dismiss the alert by clicking Decide Later. The currently active profile will then remain unchanged, and the next time you join this network Little Snitch will show the Profile Switching Alert again.

By clicking the network’s name, you can enter an alternative, custom name that will be used for this network throughout Little Snitch.

All the choices made here in the Profile Switching Alert (mapping to profile, custom network name, etc.) can be reviewed and modified later in Little Snitch Configuration.

### The Default Profile

If you prefer not to be interrupted by an alert dialog when joining an unknown network, you can configure a default profile in Little Snitch Configuration > Preferences. The configured profile will then be activated immediately without any user interaction. Only a notification will be shown in the upper-right corner of your screen.

You can review and edit the mappings between profiles and networks in Little Snitch Configuration, either in the profiles section of the sidebar, or in the Known Networks Window.

- The sidebar shows a small button next to those profiles, that have any networks assigned to them. Click this button to open a popover that lists the networks that are currently mapped to this particular profile.
- To assign a network to a different profile, drag it from the popover onto another profile in the sidebar.
- To quickly assign the current network to a profile, click the gear wheel icon in the upper-right corner of the popover and choose *Assign Current Network* from the menu.
- To rename a network, double-click its name in the popover.

---

**Profile Activated**

“Deny Any Connection”
Connected to unknown network
The Known Networks Window

The Known Networks Window shows a complete list of all networks currently known to Little Snitch along with their associated profile switching action. To open this window, do one of the following:

• Choose Window > Known Networks from the menu bar of Little Snitch Configuration.

• Press the ⌘ K menu shortcut.

The action taken when a network is joined can be edited in the Action When Joined column.

In the lower half of the window you find details for the selected network, including a map of the location where the network was first joined.

In the toolbar you can switch from list view to map view. The map view displays a larger map showing all known networks at once.
Learn more about Little Snitch’s Connection Alert and how to decide whether to allow or deny a connection attempt.
Allow or Deny Connections

Connection Alert

When Little Snitch encounters a connection attempt that is not yet covered by an existing rule, it shows a Connection Alert, allowing you to decide whether to allow or deny the connection. It also lets you create a rule declaring how to handle future, similar connections.

Learn more about rule lifetime...

Connection Summary

The connection summary provides a brief description of the connection attempt, including the names of involved processes and servers as well as protocol and port information.

- If an application utilizes a helper tool to establish the connection, the name of this tool is shown next to the application name (e.g. “Safari via WebProcess”).
- If more than one hostname is known for the remote server’s IP address, you can hover the hostname with the mouse to reveal a pop-up menu showing those alternative names. The name which is selected in the menu will be used as server or domain name for rule creation. Learn more about Little Snitch and multiple hostnames...
- The display of the connection protocol and the port number of the destination server depends on your detail level setting. Learn more about protocols and port numbers...
Show Details

Click the *Show Details* button to get a comprehensive list of connection details.

![Image 2.1 Connection Alert - Show Details](image)

This turns the alert into full detail view and reveals information such as process ID, process owner, IP address, reverse DNS name, and more.

Rule Options

To prevent the Connection Alert from being shown again for similar connections from the same process, you can create a *rule* declaring how to handle those future connection attempts.

You can choose from one of these rule options to define how specific the rule shall be:

- **Any Connection** – The rule matches any future connection attempt for this process.
- **Only port** – The rule matches only for connections to the same port.
- **Only server** – The rule matches only for connections with the same remote server.
- **Only server and port** – The rule matches only for connections to both the same server and the same port.

*Note:* The port specific rule options (*Only port, Only server and port*) are only visible if the detail level is configured to show port details.

Domain Rules

If you wish to create a rule that matches not only a particular server but an entire domain, you can hover the hostname with the mouse and then choose the domain from a pop-up menu.

![Image 2.2 Connection Alert - Choose Domain](image)

Rule Lifetime

The rule lifetime lets you specify whether the connection shall be allowed or denied permanently (by selecting *Forever*) or just temporarily (by selecting one of the temporary options from the pop-up menu).

Learn more about rule lifetime...

![Image 2.3 Connection Alert - Rule Lifetime](image)

Action

Here you determine whether the connection is allowed or denied. If a rule is created, you also determine whether it is an allow or a deny rule.
Help Button

The Help button triggers a query to an online database maintained by Objective Development. This database contains information about processes and servers and may guide you in your decision whether to allow or deny a particular connection.

Learn more about the Research Assistant...

Keyboard Shortcuts

Most actions in the Connection Alert can also be triggered via keyboard shortcuts:

<table>
<thead>
<tr>
<th>Action</th>
<th>Shortcut</th>
</tr>
</thead>
<tbody>
<tr>
<td>Toggle display of details</td>
<td>D or I</td>
</tr>
<tr>
<td>Select rule lifetime “Forever”</td>
<td>1 or F</td>
</tr>
<tr>
<td>Select next rule lifetime</td>
<td>2</td>
</tr>
<tr>
<td>Select previous rule lifetime</td>
<td>3</td>
</tr>
<tr>
<td>Select rule lifetime “For 15 Minutes”</td>
<td>0</td>
</tr>
<tr>
<td>Select rule lifetime “Until Quit”</td>
<td>Q</td>
</tr>
<tr>
<td>Select rule lifetime “Until Restart”</td>
<td>R</td>
</tr>
<tr>
<td>Select rule lifetime “Until Logout”</td>
<td>L</td>
</tr>
<tr>
<td>Select rule lifetime “Once” (no rule is created)</td>
<td>O or hold ⇧  (shift key)</td>
</tr>
<tr>
<td>Select rule lifetime “Forever”</td>
<td>F or hold ⇧  (shift key)</td>
</tr>
<tr>
<td>Select rule option “Any Connection”</td>
<td>A</td>
</tr>
<tr>
<td>Cycle through server specific rule options</td>
<td>S</td>
</tr>
<tr>
<td>Deny</td>
<td>Esc or ←-Return</td>
</tr>
<tr>
<td>Allow</td>
<td>Return</td>
</tr>
</tbody>
</table>
Rule Matching by Hostname

Little Snitch’s filter engine is implemented in the operating system’s kernel. It works on Internet addresses (IP addresses), not hostnames. When a connection is attempted, Little Snitch only receives the numeric IP address, not the hostname. Since we want to present a meaningful computer name to the user (e.g. in a connection alert), we must somehow translate this numeric address to a name.

How hostnames are determined

Little Snitch wants to show the hostname recently entered by the user or used by a process, not the reverse lookup name returned by the Domain Name System (DNS) because the reverse lookup name is often very cryptic. It therefore watches all DNS requests and responses on UDP and TCP ports 53 and 5353, and remembers the names which led to a particular IP address.

Learn more about TCP, UDP and port numbers...

If there are multiple names which resolve to a given address, it guesses the “best” name (usually the last one used) to present to the user. In the Connection Alert and in Little Snitch Network Monitor’s connection list, you can view the other names by clicking the hostname.

Rules for incoming connections

The mechanism described above does not work for incoming connections, though. Since they are not initiated by a local process, there is no name lookup leading to the IP address. The IP address occurs spontaneously — it comes from outside. We therefore only allow numeric addresses for incoming connections. We do not use reverse DNS lookup to obtain a hostname for the address because the reverse lookup names are usually cryptic and are under the control of the IP address owner. The owner can set any name he or she likes, even from domains owned by somebody else. An attacker could map his or her IP address to something in the domain apple.com to make the access look more trustworthy.

For rule matching, all hostnames resolving to the IP address in question are taken into account. Among all rules that match any of the hostnames, the one with the highest precedence determines the action taken.
If you have been using Little Snitch before, you probably know the situation: A connection alert asks you whether to allow or deny a connection, but you have no idea what that process is good for. Is this process part of the system? Is it a third party software component? Why does it want to connect to this particular server? Be relieved, you’re not alone. In many cases we, too, did not know until we did some research.

To spare our users this tedious task at least to a certain extent, we are making our findings available for Little Snitch users in an online database. The data contains primarily descriptions of processes and what they are good for.

Open the Research Assistant

When a connection alert pops up, you can click the Research button in the bottom left corner to open the Research Assistant window and to trigger a query for the current connection:

Note: Before the assistant can be used, a rule allowing access to an obdev.at server must be created. The first time you attempt to query our research database, Little Snitch will ask you whether to enable the service and to create the rule. If you later want to revoke the permission for the component of Little Snitch to access the server, simply click on Turn off Research Assistant to disable the rule.

Query Results

- The result window shows the name of the process, whether or not it has a valid code signature and who signed it.
- If no information is available for a process or you think the information we provide is incorrect or incomplete, please click on Improve information.
It opens a window where you can provide additional information regarding the current connection.

How does it work?

When you click the Research button to query our database, a URL request (a GET request) to port 80 of our database server is sent. We purposely use an unencrypted protocol so that you can verify which information is sent by using a network sniffer. The request contains all connection parameters so that the information we provide can be as specific as possible:

<table>
<thead>
<tr>
<th>Info</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac OS Version</td>
<td>Version of your Mac OS X installation. Some system daemons behave differently on different versions of the operating system, so it may be useful to have specific information available.</td>
</tr>
<tr>
<td>Bundle Identifier</td>
<td>If the process is an application, it has a bundle identifier which uniquely identifies it. This field is empty for non-application processes.</td>
</tr>
<tr>
<td>Executable Path</td>
<td>The full path of the process executable in the file system.</td>
</tr>
<tr>
<td>Localized Name</td>
<td>For applications, the app name localized to your language. We don’t use this for matching database entries, but may need it when we research a frequently requested app.</td>
</tr>
<tr>
<td>Via-Path</td>
<td>If an application performs the request via a Unix command, the full file system path of the Unix command.</td>
</tr>
<tr>
<td>Server</td>
<td>The server’s DNS name (if available) or IP address (otherwise).</td>
</tr>
<tr>
<td>Port</td>
<td>The connection’s destination port number for TCP and UDP, 0 for other protocols.</td>
</tr>
<tr>
<td>Signature</td>
<td>A short signature. Timestamp and signature are there to sort out invalid requests before any database query is done. This is a first level of protection from online attacks.</td>
</tr>
</tbody>
</table>

The response is the database entry in XML format, prefixed with a signature.
Which information about queries is stored?

We (Objective Development Software GmbH) collect statistics about which connection is requested frequently, so we can add information for those records. We do not store any information that could identify you in our database. In fact, requests with the same set of parameters (except timestamp and signature) are merged into a single database record. Your IP address is only stored in standard web server logs, which are rotated regularly.
Allow or Deny Connections

Detail Level

When Little Snitch presents a Connection Alert, it is often hard to find the relevant information quickly. Especially if you are new to the technical concepts of Internet networking, you may want to hide the less relevant details like protocol and port number.

To this end, Little Snitch offers the “Detail Level” preferences option.

Although this option has been originally designed for technically inexperienced users, it turned out that experts like it as well: It’s much easier and faster to find the most frequently used options in a simpler alert. In the rare case when you want to choose one of the hidden options, simply click the “Show Details” button and the full set of available options is back.

The more details you hide, the simpler becomes the Connection Alert and the less options you have. The example below is for “Hide Protocol and Port Details”:

![Image 2.7 Preferences – Detail Level](image)

![Image 2.8 Simplified Connection Alert](image)

**Image 2.7 Preferences – Detail Level**

**Image 2.8 Simplified Connection Alert**
Silent Mode

Silent Mode is a way to completely silence Little Snitch. You will not be bothered with Connection Alerts while this mode is active. There is a Silent Allow Mode and a Silent Deny Mode. In all cases where an alert would be shown, Silent Allow Mode lets the connection pass and Silent Deny Mode blocks it.

What is it good for?

Since all connections are allowed or denied, you may wonder what advantage Little Snitch brings in this mode. Well, not all connections are allowed or denied while this mode is active. Those which match an existing rule are handled according to the rule’s action. And in addition to allowing or denying connections, rule suggestions are created for all connections that did not match an existing rule.

So, imagine you run Little Snitch in Silent Allow Mode for the first week after installation. Yes, Little Snitch won’t protect you during this time, but that’s just one more week. You have not been protected all the years before. Then, after this week, take some time and review the Silent Mode Rule Suggestions. Try the grouping options to find the best types of rules, or consider an Allow Any or Deny Any rule for processes that are using many different connection parameters. Once you are done, you should have a rule set that matches your requirements, handling most of the connection requests occurring on your system. Then turn off Silent Mode and, depending on how you configured your rule set, you should see Connection Alerts only in rare cases.

Activate Silent Mode

Silent Mode can be activated and deactivated from Little Snitch’s Status Menu Item.

Or it can be configured in Little Snitch Configuration’s General Preferences.
Analyze Traffic

Learn more about Little Snitch Network Monitor and how to use it to analyze past connections, search for particular connections or permanently store the connection history or a traffic capture to disk.
Network Monitor

Little Snitch Network Monitor complements Little Snitch's rule based network filter by a powerful retroactive analyzer. If you want to check whether the filter rules perform as you had planned, if a software does not work as expected and you suspect that it interferes with a deny-rule, or if you are concerned that a process has just connected to the Internet although it should not, then Little Snitch Network Monitor is your tool of choice.

Components of Little Snitch Network Monitor

- **Network Monitor Menu** lets you change filtering and sorting options, manage snapshots and open Preferences.
- **Floating Window**
  - **Connection Inspector**
  - **Search**
  - The Network Monitor Menu lets you change filtering and sorting options, manage snapshots and open Preferences.
  - Change the visibility of the **Traffic Diagram**.
• Open the **Connection Inspector** for details about the selected connection.
• Narrow down the connection list by entering search terms into the **Search Field**.
• Click the Floating Button to make the Network Monitor window float on top of other windows and visible on all spaces.

**Connection List**

The connection list is the primary window of Little Snitch Network Monitor. Here is an example with default settings (connections grouped by process and sorted by last activity):

The **Server column** shows the name of the server with the most recent activity. If a server has multiple names, you can hover the name with the mouse and click to see all alternative names.

Servers in red have never been contacted because connections were denied. Servers in white are currently connected.

If the process did connect to more than one server, the number of additional connections is shown next to the hostname. You can click the number to reveal these additional connections.

The **traffic meters** display the current traffic rate of a process or an individual connection. The green bars represent the download while the red bars show the upload rate.

If the list is sorted by total traffic amounts (which can be chosen in the Network Monitor Menu), the traffic meters are replaced with horizontal bars representing the total number of bytes received and transmitted.

**Tips and Tricks**

*Sort by Traffic Amounts* – When you’ve selected the Sort by Traffic Amounts option from the Network Monitor Menu, the traffic meters are replaced with bars displaying total traffic amounts in red and green for upload and download. When you have also selected the Group by Process option, and you expand an item to show the details, total amount bars for the details show the percentage of the summary’s total amounts and are therefore not related to the size of summary bars. The first detail item always shows a 100% bar.

*Delete connections* – Connections can be deleted from the connection list either via context menu or via keyboard shortcut ⌘⌫. You may want to delete some connections from a snapshot before you send it to somebody else, or you may want to delete an entire process’ history to reset the statistics.
*Show only recent activity* – The list of connections can be limited to connections with recent activity. See *Show only Last* in the pop-up menu. This keeps the list short and clear.

*Show local network activity* – By default, all connections in the local network are suppressed because they are not so relevant from a security point of view, but generate a lot of activity. If you debug a problem in the local network, e.g. a network printer or similar, choose *Show Local Network* in the pop-up menu.
The connection inspector shows all the technical details recorded for a connection or a summary of connections. Select a connection in the list and open the inspector.

The following information is displayed:

- The connection summary from the list is repeated in the window header.
- The file system path of the process and the user name of the process owner.
- All names currently known to resolve to one of the IP addresses of the server.
- All IP addresses currently known for the server (including reverse lookup names, if available).
- Protocols and port numbers used to communicate with the server.
- The total amount of data sent and received via the connection.
- Whether the connection is currently established (connection-oriented protocols only).
- At what time the first activity was encountered and when the last.
- How often the connection was successfully established and how often it was blocked by Little Snitch.

Some of the infos are clickable. When you click on the roll-over button, the info is used as search term in the connection list.

### Tips and Tricks

**Ports and protocols** – The connection list, traffic diagram and inspector show details for process and server, but only summaries for protocols and ports. If you want to filter on a particular port or protocol, click the port or protocol in the inspector to add a filter in the connection list. All information shown is now narrowed down the the particular port or protocol.

**Absolute dates** – Dates are often given as relative times (e.g. 25 minutes ago) or in ISO format. Hold the Option-key while the inspector window is active to show them as absolute dates in your preferred localized format.
Traffic Diagram

The traffic diagram provides a graphical representation of your computer’s recent network activity. It lets you view and analyze total traffic amounts, peak and average traffic rates, as well as related system events such as application launches or system sleep. It covers one hour of computer up-time, and you can zoom in on a portion of the graph down to a one minute time-frame.

• You can hover the diagram with the mouse to get an overlay with upload and download data rates for any point of time within the graph.

• The Total Amounts display shows the total amounts of received and sent data within the selected range. You can hold down the Option-key (⌥) to see average data rates instead (averaged over the entire selection).

• The Zoom slider lets you select a zoom level from one hour down to one minute. Alternatively, you can zoom in by selecting an area in the diagram with the mouse (auto-zoom) or with a pinch to zoom gesture on a trackpad.

• The gear wheel menu in the bottom left corner lets you choose between linear and logarithmic data rate display, turn auto-zoom on/off, and it provides a couple of fixed zoom presets. This menu can also be accessed via right-click into the diagram.

System Events

[Image 3.2 Traffic Diagram – Events Indication]
System events such as launch or termination of applications, fast user switching etc. are marked with yellow diamonds. You can hover them with the mouse to see a description of the event.

**System Sleep**

Those times where your computer was in sleep mode are marked with thick, gray vertical lines within the diagram. Those sleep times do not count up to the total of 60 minutes recorded in the traffic diagram.

You can hover the gray line with the mouse to get the duration of the system sleep displayed.

**Tips and Tricks**

*Who has sent that byte?* When you select a time range in the traffic diagram, the connection list focuses on connections that actually had any traffic during that time. If you see a traffic peak in the diagram, you can select it to see which process caused it. Note that limiting the time range in this way temporarily overrides any time limit (*Show only Last*) currently set in the connection list.

*Moving average* – The selected time range can be moved by holding down the Command key and dragging it with the mouse. Statistics in the Total Amounts display are updated in real-time. Hence, when you select a one minute time range and drag it over a download with the Command and Option keys held down, you can inspect the one minute average download rates over time.
Search the Connection List

The connection list can be searched by typing a search term into the search field. Search terms without a prefix are searched in:
- Process names.
- All server names, even those not currently shown.
- IP addresses displayed for a connection, even if hidden in a summary.

If you type multiple search terms separated by a space character, only connections matching all of the terms are displayed. If you want to search a term which contains spaces literally, surround it with quotes. Searching is not case-sensitive and also matches if the term is just part of a word (e.g. "Dev" finds "www.obdev.at").

Search in particular properties

The search can be restricted to particular properties of connections. Click on the search field's menu to see a list of properties that can be searched. When you choose a property, a search prefix is written into the search field and you can append your search term to it. If you know the prefix, you can also type it instead of selecting it from the menu. The following properties can be searched:

- **Process** – The name (not the file system path) of the process, as displayed in the connection list, is searched.
- **Hostname** – All forward-lookup names, even those not shown in connections, are searched.
- **IP Address** – All IP addresses are searched textually. You can search for parts of IP addresses, for instance 123.5
- **Protocol** – The protocol names of all connections are searched. Protocol names are TCP, UDP, ICMP, etc.
- **Port** – The destination port is searched numerically. This means that 12 matches port 12, but not 120 or 512.
- **Status** – Searches for connections with a particular status. Valid status keywords are “denied”, “allowed”, “connected” and “disconnected”.

If you add multiple search terms with or without prefix, only connections matching all of them are displayed. Again, you can add terms containing spaces by including them in quotes.

Tips and Tricks

Find blocked connections – If an application behaves in an unexpected way and you suspect that a deny-rule might cause the problem, search for “status:denied” and inspect recently denied connections. Note that the problem may be caused by denying a different process and your application depends on it. When you find a connection and don't know why it was denied, right-click it and choose Show Corresponding Rules from the context menu.
Sometimes you want to preserve something for the future. You might have found a situation you want to share with our support, or you just want to take some time to analyze the data without fear that information might be lost.

**Create and save snapshots**

Little Snitch Network Monitor can make snapshots of the history currently stored, and the connection list built from this history. Choose “Make Snapshot” from the connection list window’s pop-up menu or hit ⌘D while the connection list is in front. This duplicates the current status of the connection list and you can edit it, if you like (delete connections), and save it to disk.

Alternatively, you can save a snapshot directly to disk with the menu option *Save Snapshot As...* or ⌘S.

**Open snapshots**

Snapshots can be opened by double-click or by choosing the menu item *Open Snapshot...*. You can then view the data in the connection list, traffic diagram and inspector, and you can even edit it (delete connections) and re-save it.

Note that some things are displayed differently in snapshots than in live views: Relative dates are given with respect to the snapshot date and the connected/disconnected status is not available.
Capture Network Traffic

Little Snitch is able to capture and store any process’ network traffic. The recorded data is stored in PCAP format so that it can easily be opened with third-party tools like Wireshark (a powerful analyzer which can read almost any protocol known on earth) or Cocoa Packet Analyzer.

Start and Stop a Capture

To start capturing traffic of a certain process, right-click any connection of this process in Little Snitch Network Monitor’s connection list and choose Capture Traffic of... from the context menu. Little Snitch starts capturing immediately while you choose a name for the file. Little Snitch can run any number of simultaneous traffic captures.

To stop a running capture, you can either click Little Snitch’s status menu item (which blinks a red recording indicator) and choose the capture from the menu, or right-click the connection being captured in the connection list and choose Stop Capture from the context menu.

Interpret Captured Data

In order to understand the results of a traffic capture, you must know that Little Snitch intercepts traffic at the application layer. This is what distinguishes Little Snitch from conventional firewalls: Decisions can be made based on which application sends or receives the data. At this layer, however, it is not yet known via which network interface the data will be routed (which sender IP address will be used) and sometimes it is not known which sender port number will be used. It is also not known whether and how the data will be fragmented into packets. However, all this information is required in order to write a valid PCAP file. Little Snitch simply makes up the missing information. It fakes TCP, UDP, ICMP, IP and even Ethernet protocol headers. Missing information is replaced as follows:

- **Ethernet (MAC) address** – Sender and recipient address are both set to
- **Local IP (v4 or v6) address** – Numeric Process-ID of process.
- **Local TCP/UDP port number** – Kernel’s socket identification number.
- Packets are always generated as large as the protocol allows (not as large as the network would allow).

Since all network protocol headers are made up, it is not possible to debug network problems (such as lost packets, retries) with these traffic captures. If you need to debug at the protocol header level, use the tcpdump Unix command or Wireshark instead.
Organize Rules

Learn more about Little Snitch Configuration: How to manage, inspect and analyze rules, create profiles or work with rule suggestions.
Little Snitch Configuration is the interface for managing rules and profiles. It’s also the central hub for editing preferences of all components of Little Snitch.

- **Rules List** – The list of rules or rule suggestions. Rules define how network traffic is filtered.
- **Sidebar** – The sections in the sidebar define which rules or rule suggestions are listed. You can filter the rule set by various criteria, or view suggestions for rules you might want to create. In addition to filtering, profiles are also destinations for drag operations. Drag a rule on a profile to make it effective in only that profile.
- **Info Pane** – This part of the window contains all detail information about the currently selected rule or suggestion. This is the place where a rule’s notes can be edited.
- **Toolbar** – Customizable toolbar with shortcuts for frequently used actions.
Manage Rules

Rules are at the core of how Little Snitch filters network traffic. Whenever you manually create, modify or duplicate a rule, the rule editor, will be opened, allowing you to specify the conditions and actions for that rule.

Note that rule editing can be disabled entirely in Little Snitch Configuration > Preferences > Security.

Learn more about Rules...

Creating new rules

Most of your rules will be created automatically when you answer a Little Snitch Connection Alert with “Allow” or “Deny”. As discussed in the Connection Alert chapter, any lifetime option other than Once will result in a rule.

... using Little Snitch Configuration
• Press ⌘N or click New Rule in the toolbar to create a new rule from scratch.
• Press ⌘⌥N or right-click on a rule, then select New Rule for “Process” to create another rule for the clicked process.
• Drag an application or another executable from the Finder onto the rules table to create a rule for that process.
• Drag an application onto Little Snitch Configuration’s Dock icon or onto its application icon in Finder.

... using the Menu Bar Item
If you don’t have Little Snitch Configuration handily available in the dock or in an open Finder window, you can also drag an app or any executable onto the Menu Bar Item. This will open the rule editor in Little Snitch Configuration, pre-filled with the corresponding process information.

... using Little Snitch Network Monitor
If you see an established connection in Little Snitch Network Monitor that should be blocked (or vice versa - a blocked connection that should be allowed), then you simply can create a rule with the opposite action from within Little Snitch Network Monitor. Just right-click on the connection in the list and select Create Rule... from the context menu. This will fill in Little Snitch Configuration’s rule editor with the appropriate information.

Duplicating rules

If an existing rule matches almost exactly what you want, that rule can be duplicated, which allows you do edit a copy of the rule. To duplicate one or more selected rules, do one of the following:
• Choose Rules > Duplicate... from the menu bar.
• Right-click on the selected rules and choose Duplicate from the contextual menu.
• Press ⌘D
• Press ⌘C and ⌘V to copy & paste the rules.

Delete rules

To delete one or more selected rules, do one of the following:
• Choose Edit > Delete from the menu bar.
• Click the Delete button in the menu bar.
• Right-click on the selected rules and choose *Delete* from the contextual menu.
• Press ᴡ

Note that protected rules cannot be deleted. You can disable them instead if you need to.

### Disabling / Enabling rules

Disabling rules is an alternative to deleting them. It allows you to keep them available and reenable them later, and it also works for protected rules. To disable (or enable) one or more selected rules, do one of the following:

• Choose *Edit > Disable* (or *Enable*) from the menu bar.
• Right-click on the selected rules and choose *Disable* or *Enable* from the contextual menu.
• Click the checkbox in the “On” column of the rules list.
• Press the space bar to toggle the selected rules between enabled and disabled.

Disabled rules are greyed out and can be hidden from the list by clicking the *Hide Disabled* button in the toolbar.
The rule editor is used to create new rules or edit existing ones. To create a new rule, click (+) in the main window’s bottom bar or New in the toolbar. To edit an existing rule, double-click it. The rule editor is responsible for editing the rule’s action and properties used in matching.

Learn more about rule actions and matching...

- **Action** – This is the action taken when the rule matches. Actions are Allow connections, Deny connections, or Ask. When a rule is created, a second pop-up menu, next to the action, defines whether this is a rule matching incoming or outgoing connections. When editing temporary rules, there is an indication of the validity period next to the action menu and you can turn these rules into permanent rules.

- **Process Condition** – Matching properties related to process. Click the app icon for options related to the process (e.g. choose a different process). The process owner can be Me, System or Anyone. Learn more about process owners...

- **Server Condition** – Matching properties related to remote server. Learn more about IP addresses, ports and protocols...

If the rule matches incoming connections, the server section precedes the process section (sections are exchanged).
Manage Profiles

Profiles are a means to switch between rule sets easily. Profile editing can be disabled entirely in Little Snitch Configuration > Preferences > Security.

Learn more about Profiles...

Create new profiles

To create a new profile in Little Snitch Configuration, do one of the following:
- Choose Rules > New Profile... from the menu bar
- Click the (+) button in the bottom left corner of the rules window
- Press ⌘N

Add rules to a profile

- To add existing rules to a profile, drag them from the rules list onto the desired profile in the left sidebar.
- When creating rules in Little Snitch Configuration, the new rules are automatically added to the currently active profile, or if a profile is selected in the left sidebar, new rules are added to the selected profile.
- New rules created from a connection alert are automatically added to the currently active profile

Rename a profile

To rename an existing profile in Little Snitch Configuration, do one of the following:
- Right-click on the profile in the left sidebar and choose Rename from the contextual menu.
- Single-click on an already highlighted profile in the sidebar.
- Select the profile in the sidebar and press ⌘

Delete a profile

To delete an existing profile in Little Snitch Configuration, do one of the following:
- Right-click on the profile in the left sidebar and choose Delete from the contextual menu.
- Select the profile in the sidebar and press ⌡

If the selected profile has rules assigned to it, Little Snitch will ask what should be done with these rules. You can either choose to delete those rules or keep them and they will appear as unapproved, disabled rules not assigned to any profile.

Activate a profile

To activate a profile, do one of the following:
- Right-click on the profile in the left sidebar of Little Snitch Configuration and choose Activate from the contextual menu.
- Double-click the profile in the sidebar.
- Open the Little Snitch menu bar item, and choose the desired profile from the Profiles submenu.
Deactivate a profile

To deactivate a currently active profile, do one of the following:

• Right-click on the active profile in the left sidebar of Little Snitch Configuration and choose *Deactivate* from the contextual menu.

• Double-click the active profile in the sidebar.

• Double-click the *Effective in all profiles* item in the sidebar.

• Open the Little Snitch menu bar item, and choose *No Profile* from the *Profiles* submenu.

Automatically activate a profile in particular networks

When *Automatic Profile Switching* is enabled, Little Snitch can automatically activate a profile when a particular network is joined. The mapping between networks and profiles can be edited in the *Known Networks Window*, or it can be changed directly in the profiles section of the sidebar.

Profiles which are participating in Automatic Profile Switching are shown with a small arrow button in the sidebar. Click on that button to open a popover that lists the networks that are currently assigned to this profile. You can drag networks from there onto another profile, or click on a network’s (x) button to delete it.

For profiles which are not assigned to any network yet the arrow button is only shown when the mouse cursor hovers that area. Click on that button to open a popover that allows you to assign the current network to the profile.
Sidebar

The sidebar provides convenient access to rules, suggestions and profiles.

The Rules section contains various smart filters focusing on different types of rules. The Suggestions section contains various filters focusing on rules you might want to add (suggestions) or delete (invalid or redundant rules). The Profiles section contains filters focusing on rules assigned to particular profiles. Furthermore, each of these lists can be searched textually.

Rules

This section contains various filters working on non-textual rule properties.

Learn more about rules...

Suggestions

Rule suggestions can be filtered by the type of event that created the suggestion. Lists of suggestions always have a top bar which allows quick creation of rules from the suggestions.

Learn more about rule suggestions...

Profiles

The profiles section is slightly different from other filters: In addition to filtering the rules by the profiles in which they are active, they can be used to assign rules to profiles (drag rule on profile), activate a profile (double-click it) or rename a profile (single-click into name).

The top bar in this section offers an option whether to show all rules which are effective in the profile (i.e. also show rules that are effective in all profiles), or rules effective in only in this profile.

Learn more about profiles...
Sort Rules

Rules can be sorted alphabetically (by process name), by precedence, or by creation date. These options are available in the “View” menu or by clicking the table header “Process” for alphabetical order, “Rule” for precedence, and “bullet” for creation date.

Sort by precedence

While the result of sorting alphabetically or by creation date are pretty obvious, sorting by precedence can be quite enlightening. If multiple rules match a connection attempt, the rule action is taken from the one with the highest precedence. Since ordering is by decreasing precedence, more important rules are at the top of the list. Rules that can never match for the same connection (i.e. they are orthogonal, for instance because they match two different processes) and thus can have the same precedence, are sub-sorted alphabetically by process.

Tips and Tricks

If you wonder why a particular connection was allowed or denied, right-click the process attempting the connection in the rule list and choose Focus on Rules Affecting... This sets the process name as search term, sets the search scope to Process (exact match) and sorts rules by precedence. The result is a list where you see only rules affecting the process with decreasing precedence. Step through the list from the top to the bottom. The first rule matching your connection defines the action.

You can also right-click the connection in Little Snitch Network Monitor and choose Show Corresponding Rule to see the rule responsible for allowing or denying the connection, but you won’t have the insight why exactly this rule had the highest precedence.
Organize Rules

Search Rules

Enter a search term in the toolbar's search field to focus only on rules containing the search term. By default (search scope “All”), the term is searched in

• the process name,
• the full file system path of the process' executable,
• the bundle identifier of the process (if any),
• the textual representation of the rule's properties as displayed in the rule list (this includes the server name or address),
• the rule’s notes.

The search scope can be limited to any of these properties in the search field's menu.

The search term is split into words (separated by spaces) and a rule matches if it contains all words in the selected search scope.

In the search scope Process (exact match), the search term is not split into words. It is used as-is, including spaces and the entire process name must match the search term. In addition to rules for processes which match the term exactly, Any Process rules match as well. The search scope therefore finds all rules which have an effect on network filtering for the given process.
Top Bars

In some filters of the sidebar, the rule list is supplemented by a top bar above the list header, providing direct access to frequently used actions:

Top Bar for temporary rules

… for unapproved rules

… for rule suggestions

Suggestions can directly be converted into allow or deny rules, or the rule can be edited before it is created. The grouping options offer a powerful mechanism to cover multiple suggestions by a more general rule. Learn more about rule suggestions...

… for invalid rules

… for redundant rules

Redundant rules can be shown in the context of those overriding them. Choose this option to see redundant rules in context or turn it off to see the redundant rules only.

… for profiles

Profile filters can either show only rules that are effective when the profile is active (suppress rules not assigned to a profile), or show all rules effective when the profile is active. The latter is useful to see the entire rule set that is actually effective when the profile is active.
Everything Else

Further explanations, uninstalling Little Snitch and more.
This page explains the various icons used in Little Snitch.

- **Unapproved Rule** – Rules are tagged as unapproved if they were created outside of Little Snitch Configuration.

  Rules Annotations, Connection Alert

- **Temporary Rule** – Depending on how a rule was created, it can expire automatically, e.g. if a Connection Alert was answered with Until Quit.

  Rules Annotations, Connection Alert

- **Process Owner System** – The process was started by a system user, mainly root.

  Rule Lifetime, Lifetime of Rules Created Using Connection Alert

- **Process Owner Anyone** – Rules for anyone match processes started by any user, including system users.

  Rule Condition

- **Allow Action** – The action of a rule or the Silent Mode is to allow connections.

  Rule Condition

- **Deny Action** – The action of a rule or the Silent Mode is to deny connections.

  Rule Action, Rule Matching

- **Ask Action** – The action of a rule is to show a Connection Attempt.

  Rule Action, Rule Matching

- **Covering Rule** – This rule covers other rules, making them redundant.

  Sorting rules by precedence, How are rule suggestions created?, Rule Matching

- **Redundant Rule** – This rule is redundant and therefore never matches a Connection Attempt.

  Sorting rules by precedence, Rule Matching

- **Incoming Connection** – Indicates rules or connections that a process accepts from peers, in contrast to a process establishing an outgoing connection to a remote server.

  Rules, Connection Alert
Invalid Rule – This rule is invalid because the process path is not valid.

Icons in the Menu Bar Item

⚠️ *Network Filter off* – Little Snitch is inactive because the network filter was stopped, the demo period expired or an internal error prevents Little Snitch from working. If it was disabled, it can be enabled again using the Little Snitch Menu Bar Item or Little Snitch Configuration’s preferences.

_traffic |_| |_|* Traffic Capture running* – Little Snitch currently is capturing network traffic.

Capture network traffic

❌ *Blocked Connection* – Little Snitch blocked a connection attempt due to a deny rule.
Menu Bar Item

With one glance at the Little Snitch Menu Bar Item you can quickly get information not only about Little Snitch’s own status but also about your system’s current network activity.

Depending on your settings you will be able to see the current network throughput for both, upload and download, and whenever you need more information about what app is communicating with which server right now, Little Snitch can be configured to bring up the Network Monitor by simply hovering the mouse cursor above the area the menu bar item occupies.

You can also create rules quickly by dragging & dropping an app or any other executable on the menu item. This will open Little Snitch Configuration with the appropriate information in the rule editor already filled in.

Configuration options

The menu bar item can be configured in Little Snitch Configuration’s preferences as follows:

• **No menu bar item** – Item will be hidden unless it is set to display an inactivity warning and the network filter is off
• **Traffic meters off** – Do not show network activity
• **Show traffic meters** – In color or monochrome
• **Show traffic meters & data rates as numerical values** – In color or monochrome

Status Information

Depending on Little Snitch’s state, the menu bar icon will provide additional information:

• **Network filter off** – A yellow triangle (caution sign)
• **Traffic capture running** – A red, blinking recording icon
• **Silent Mode active** – Background shaded in green (Silent Allow Mode), or red (Silent Deny Mode)

Whenever Little Snitch blocks a connection attempt due to a deny-rule, a red “X” appears and fades out on top of the traffic meters (if enabled).
Permissive Mode

Why be permissive?

While no user is logged in or a login is in progress, Little Snitch cannot display Connection Alerts. Normally, suggestions are created for all connection attempts not covered by rules, but the connection attempt itself is denied. This can cause problems if a network connection is required for the login to succeed, e.g. if a network user account is used. This is what Permissive Mode is for.

In Permissive Mode, everything works as written above, except that connection attempts that would normally be denied are allowed instead, thus circumventing problems with network user accounts. You still get suggestions for connection attempts, which you can turn into permanent rules to eliminate the need for Permissive Mode.

When to enable Permissive Mode

Permissive Mode is enabled for the first start of your computer after you install Little Snitch to prevent the problem outlined above. If you ever need to restart your computer in Permissive Mode, you can do so in Little Snitch Configuration’s menu: Little Snitch Configuration > Restart in Permissive Mode...

Some applications may need to connect to the internet before a user logs in. The reasons for why they do depend on the applications. For example, an anti-virus software may want to check for updates as soon as the computer starts and not only after the first user logs in.

Little Snitch shows a message right after you log in if connection attempts happened during login and offers to show them in Little Snitch Configuration. You can find suggestions for these connection attempts in the “Login Connections” section in Little Snitch Configuration.
Uninstall

In order to perform its duty, Little Snitch needs to add components to a very low level of the operating system, which also need to be registered and unregistered with the system. Hence, it is not sufficient to drag Little Snitch’s application bundles to the trash for uninstallation.

Little Snitch Uninstaller

The Little Snitch Uninstaller can be found in the Little Snitch .dmg disk image file, next to the Installer. If you don’t have the disk image to hand, you can always download the current version from our website.

The uninstallation process itself is straight forward, with only one option to choose: Whether you want to remove your rules and settings, or not. After the process is finished, you will have to restart your computer.

If you enable the option to remove rules and settings, the Uninstaller will delete all your system-wide configuration and rules files (also any Little Snitch 2 files), including the file that stores your license information, as well as the configuration and rules files for the user executing the Uninstaller.

List of Files

If you have the need to remove a single configuration file, here is a list:

/Library/Application Support/Objective Development/Little Snitch/configuration.xpl
~/.Library/Application Support/Little Snitch/configuration.user.xpl
~/.Library/Preferences/at.obdev.LittleSnitchConfiguration.plist
~/.Library/Preferences/at.obdev.LittleSnitchNetworkMonitor.plist
~/.Library/Preferences/at.obdev.LittleSnitchInstaller.plist

The “~” (tilde) sign refers to your user’s home folder.

Please note that the Uninstaller does more than moving the application bundles to the trash and deleting the configuration files. If you really want to remove Little Snitch completely from your system it is highly recommended to use the provided uninstallation application.
If you have any further questions or comments about our products, please contact our support.

Copyright © 2013 Objective Development Software GmbH

Apple, Bonjour, Mac OS X and Safari are trademarks of Apple Inc., registered in the U.S. and other countries.