

ProxyCap Help

© 2018 Proxy Labs

Table of contents

- [Configuring ProxyCap](#)
 - ◆ [The Ruleset panel](#)
 - ◇ [Loading and saving rulesets](#)
 - ◇ [Delegating ruleset management](#)
 - ◆ [The Proxies panel](#)
 - ◇ [The proxy list view](#)
 - ◇ [Adding, removing and modifying proxies](#)
 - ◇ [Proxy server properties](#)
 - [Setting the proxy type](#)
 - [Host name and port](#)
 - [Authentication](#)
 - [Preferred cipher \(SSH only\)](#)
 - [Host key verification \(SSH only\)](#)
 - ◇ [Checking a proxy](#)
 - ◇ [Setting the default proxy](#)
 - ◆ [The Chains panel](#)
 - ◇ [The chain list view](#)
 - ◇ [Adding, removing and modifying chains](#)
 - ◇ [Proxy chain properties](#)
 - ◇ [Checking a chain](#)
 - ◆ [The Rules panel](#)
 - ◇ [The rule list view](#)
 - ◇ [Adding, removing and modifying rules](#)
 - ◇ [The Quick Add Rule dialog box](#)
 - ◇ [Routing rule properties](#)
 - [Rule Action](#)
 - [Programs](#)
 - [Destination Ports](#)
 - [Destination IP Addresses](#)
 - [Destination Hostnames](#)
 - [Transports](#)
 - ◇ [Prioritizing rules](#)
 - ◇ [Disabling a rule](#)
 - ◇ [Predefined rules](#)
 - ◆ [The DNS panel](#)
 - ◆ [The Miscellaneous panel](#)
 - ◇ [Controlling product updates notifications](#)
 - ◇ [Controlling error logging](#)
 - ◇ [Controlling crash reporting](#)
- [Enabling or disabling ProxyCap](#)
- [Viewing status and logs](#)
 - ◆ [The Connections screen](#)
 - ◆ [The SSH Tunnels screen](#)
 - ◆ [The Error Log screen](#)

Configuring ProxyCap

This chapter describes all the configuration options in ProxyCap.

ProxyCap is configured using the ProxyCap Configuration dialog box that comes up if you right-click on the ProxyCap tray icon and choose “Configuration”. All settings can be changed at any time. Changes are saved and applied when you close the ProxyCap Configuration dialog box by pressing the OK button. To configure ProxyCap, you must be a member of the “Administrators” or “ProxyCap Admins” groups on the local computer.

- [The Ruleset panel](#)
- [The Proxies panel](#)
- [The Chains panel](#)
- [The Rules panel](#)
- [The DNS panel](#)
- [The Miscellaneous panel](#)

The Ruleset panel

The Ruleset panel allows you to perform some tasks on your proxies, routing rules and DNS settings as a whole.

- [Loading and saving rulesets](#)
- [Delegating ruleset management](#)

Loading and saving rulesets

You can store your proxies, routing rules and DNS settings in a single file in the PRS format. PRS is a binary file format designed to be understood by ProxyCap only.

To load a ruleset from a PRS file,

1. Press the Load button. The Load Ruleset dialog box will come up.
2. Select the PRS file you want to load the ruleset from, then press the Open button.

To save your ruleset to a PRS file,

1. Press the Save As button. The Save Ruleset dialog box will come up.
2. Type a file name in the File name box, then press the Save button.

Delegating ruleset management

The Ruleset management delegation feature allows you to delegate the task of defining and subsequently modifying your proxies, routing rules and DNS settings to your network administrators.

When the delegation is turned on, ProxyCap periodically checks for an updated ruleset, and automatically performs updates. You are not allowed to change your proxies, routing rules and DNS settings, unless you turn the delegation off. ProxyCap enforces the above restriction by disabling the corresponding features.

To delegate ruleset management,

1. Tick the “Delegate ruleset management to a trusted provider” box.
2. In the Location field, specify the URL of the [PRS](#) file. Note: HTTP and HTTPS URLs are supported.

The Proxies panel

The Proxies panel allows you to define your proxies. In order for ProxyCap to work, you must specify at least one working proxy.

- [The proxy list view](#)
- [Adding, removing and modifying proxies](#)
- [Proxy server properties](#)

- [Setting the default proxy](#)

The proxy list view


The proxy list view displays your proxies in a details view. Each row represents a proxy.


- The “Name” column shows the display name of the proxy.
- The “Type” column shows the type of the proxy.
- The “Hostname” column shows the name, or the IP address, of the server the proxy is running on.
- The “Port” column shows the port number on the server to connect to.
- The “Attribute” column indicates whether the proxy is the default proxy.


You can show and hide list view columns. To show or hide a column, right-click the list header, then select or unselect the name of the column you wish to show or hide.

If you double-click a row, [the Proxy Server Properties dialog box](#) will come up.

Adding, removing and modifying proxies

To add a proxy, press the New Proxy Server  button on the toolbar. [The New Proxy Server dialog box](#) will come up.

To remove a proxy, select the proxy from the list, then press the Remove  button on the toolbar.

To change settings for a proxy, select the proxy from the list, then press the Properties  button on the toolbar. [The Proxy Server Properties dialog box](#) will come up.

Proxy server properties

The New Proxy Server dialog box allows you to define a new proxy. The Proxy Server Properties dialog box allows you to change settings for an already defined proxy.

- [Setting the proxy type](#)
- [Host name and port](#)
- [Authentication](#)
- [Preferred cipher \(SSH only\)](#)
- [Host key verification \(SSH only\)](#)

Setting the proxy type

The “Type” combo box allows you to specify the type of the proxy.

- Selecting “HTTP” allows you to redirect HTTP connections made by an application through a HTTP proxy.
- Selecting “HTTPS” allows you to tunnel applications through a HTTP proxy supporting the CONNECT command, as documented in the “Upgrading to TLS Within HTTP/1.1” RFC.
- Selecting “SOCKS4” allows you to tunnel applications through a SOCKS4 proxy server. The original SOCKS4 protocol does not support proxy-side DNS. If you enable proxy-side DNS, ProxyCap will use SOCKS4A - a protocol extension to SOCKS4 which does support proxy-side DNS. NOTE: Not all SOCKS4 proxy servers provide this extension.
- Selecting “SOCKS5” allows you to tunnel applications through a SOCKS5 proxy server. SOCKS5 is the only proxy type that allows you to proxy UDP.
- Selecting “SSH” allows you to tunnel applications through a SSH server. All traffic between your computer and the SSH server is encrypted.

Host name and port

- The “Hostname” box is where you type the name, or the IP address, of the server the proxy is running on.
- The “Port” box lets you specify which port number on the server to connect to.

Authentication

If your proxy requires authentication, you should tick the corresponding box and either provide logon credentials or use the built-in single sign-on (SSO) functionality. In the latter case, the program will try to use the currently logged on credentials to authenticate against the proxy.

The authentication methods supported vary depending on the proxy type:

- With SOCKS5, ProxyCap supports the username/password and GSSAPI authentication methods. The GSSAPI method is implemented using SSPI Kerberos.
- SOCKS4 can use the “Username” field, but does not support passwords.
- With HTTP and HTTPS proxying, ProxyCap supports the Negotiate, NTLM, Digest and Basic authentication schemes. ProxyCap will try to use the most secure authentication method from the list of methods supported on the proxy server. For Negotiate and NTLM, it is assumed that the user belongs to the domain on the target system. You can explicitly specify the domain using the format “domain\user”. To authenticate using the logged on credentials, tick the “Use integrated Windows authentication” box.
- With SSH, ProxyCap supports the password, public key and GSSAPI (“gssapi-with-mic”) authentication methods. If you specify a password, and password authentication is disabled on the SSH server, the program may try to simulate keyboard-interactive authentication. The GSSAPI method is implemented using SSPI Kerberos. For public key authentication, you must import your private key from a key file in the OpenSSH format. Please refer to the documentation of your SSH client application on how to export your private key to the OpenSSH format.

Preferred cipher (SSH only)

ProxyCap supports a variety of different encryption algorithms, and, with SSH2, allows you to choose which one you prefer to use. This setting has no effect for SSH1. Note that ProxyCap uses SSH2 whenever possible.

Host key verification (SSH only)

Host key verification is designed to protect you against IP address spoofing.

To enable host key verification, tick the “Verify server's host key” box, and then import the server's public host key from a key file in the OpenSSH format. Some SSH servers have more than one host key of different types and for different versions of the SSH protocol. You can use any of them with ProxyCap provided the server is configured to support the corresponding version of the SSH protocol. OpenSSH stores its public host key files at the following paths:


- /etc/ssh/ssh_host_rsa_key.pub (SSH2 RSA)
- /etc/ssh/ssh_host_dsa_key.pub (SSH2 DSA)
- /etc/ssh/ssh_host_key.pub (SSH1 RSA)

If host key verification fails, ProxyCap will disconnect from the server and will log the error to the Session Error Log.

Checking a proxy or chain

ProxyCap includes an integrated proxy checker that allows you to perform a number of tests on a selected proxy or proxy chain. Depending on the type of the test, you can check the following:


- availability of the proxy service at the given address
- validity of the authentication credentials
- reachability of the given destination host/port
- connect delay (how long it took to establish the connection)
- download speed
- UDP round-trip time

To invoke the proxy checker, select an item from the list, then press the Check  button on the toolbar.

Setting the default proxy

The purpose of the default proxy setting is to allow you to switch proxies with a single click of your mouse. To put it in use, whenever you add a redirect routing rule, select the “(default)” alias from the drop-down list of proxy servers.

You cannot change the default proxy from SOCKS5 to a proxy of a different type if the UDP protocol is selected in a redirect rule.

To set a proxy as the default proxy, select a proxy from the list, then press the Set as Default  button on the toolbar.

The Chains panel

The Chains panel allows you to create proxy chains.

- [The chain list view](#)
- [Adding, removing and modifying chains](#)
- [Proxy chain properties](#)

The chain list view


The chain list view displays your proxy chains in a details view. Each row represents a proxy chain.


- The “Name” column shows the display name of the proxy chain.
- The “Proxies” column shows the proxies the chain consists of, in connection order.


You can show and hide list view columns. To show or hide a column, right-click the list header, then select or unselect the name of the column you wish to show or hide.

If you double-click a row, [the Proxy Chain Properties dialog box](#) will come up.

Adding, removing and modifying chains

To add a chain, press the New Proxy Chain  button on the toolbar. [The New Proxy Chain dialog box](#) will come up.

To remove a chain, select the chain from the list, then press the Remove  button on the toolbar.

To change settings for a chain, select the chain from the list, then press the Properties  button on the toolbar. The [Proxy Chain Properties dialog box](#) will come up.

Proxy chain properties

The New Proxy Chain dialog box allows you to define a new chain. The Proxy Chain Properties dialog box allows you to change settings for an already defined chain.


A proxy chain must contain at least two proxies. The proxies must be positioned in connection order.

A proxy chain cannot contain more than one HTTP proxy. A HTTP proxy must be the last in the chain.

Checking a proxy or chain

ProxyCap includes an integrated proxy checker that allows you to perform a number of tests on a selected proxy or proxy chain. Depending on the type of the test, you can check the following:

- availability of the proxy service at the given address
- validity of the authentication credentials
- reachability of the given destination host/port
- connect delay (how long it took to establish the connection)
- download speed
- UDP round-trip time

To invoke the proxy checker, select an item from the list, then press the Check  button on the toolbar.

The Rules panel

The Rules panel allows you to specify which applications will connect to the Internet through a proxy and under what circumstances. By default, all programs connect directly.

Rules are examined in ascending order (from top to bottom). If the rule does not match, the next rule in the chain is examined; if it does match, then all following rules are ignored.

- [The rule list view](#)
- [Adding, removing and modifying rules](#)
- [Routing rule properties](#)
- [Prioritizing rules](#)
- [Disabling a rule](#)
- [Predefined rules](#)

The rule list view

The rule list view displays your routing rules in a details view. Each row represents a rule.


- The “Name” column shows the display name of the rule.
- The “Programs” column shows the programs to which the rule applies. The special value “(all)” means that the rule applies to all programs.
- The “IP Addresses” column shows the destination IP addresses to which the rule applies. The special value “(all)” means that the rule applies to all destination IP addresses.
- The “Hostnames” column shows the destination hostnames to which the rule applies. The special value “(all)” means that the rule applies to all destination hostnames.
- The “Ports” column shows the destination port numbers to which the rule applies. The special value “(all)” means that the rule applies to all destination port numbers.


- The “Transports” column shows the TCP/IP transport protocol to which the rule applies. The special value “(all)” means that the rule applies both to TCP and UDP.
- The “Action” column contains the rule action and, if the rule action is “Redirect through proxy”, the name of the proxy.


You can show and hide list view columns. To show or hide a column, right-click the list header, then select or unselect the name of the column you wish to show or hide.


If you double-click a row, [the Routing Rule Properties dialog box](#) will come up.

Adding, removing and modifying rules

To add a rule with minimum mouse clicks, press the Quick Add Rule  button on the toolbar. [The Quick Add Rule dialog box](#) will come up.

The Quick Add Rule dialog box exposes only a subset of the features available. It doesn't allow you to define proxy chains, specify multiple programs, etc. To add a rule that utilizes these advanced features, press the New Rule Wizard  button on the toolbar. [The New Routing Rule wizard](#) will come up.

To remove a rule, select the rule from the list, then press the Remove  button on the toolbar.

To modify a rule, select the rule from the list, then press the Properties  button on the toolbar. [The Routing Rule Properties dialog box](#) will come up.

The Quick Add Rule dialog box

The Quick Add Rule dialog box allows you to add a new routing rule with minimum mouse clicks.

Rule Action

A routing rule can be assigned one of the following actions:

- “Redirect through proxy” means to redirect this connection through a specific proxy. You must select the proxy from the dropdown list of proxies. Instead of specifying the proxy explicitly, you can choose the special value “(default)”. Please see [Setting the default proxy](#) for more information.

If you check the “Resolve names remotely” checkbox, ProxyCap will force proxy-side DNS. NOTE: If you are doing DNS at the proxy side, you should make sure that your routing rules do not depend on knowing the IP address of a host. If the name is passed on to the proxy, ProxyCap will never know the IP address and cannot check it against your routing rules.

The original SOCKS4 protocol does not support proxy-side DNS. If you enable proxy-side DNS, ProxyCap will use SOCKS4A - a protocol extension to SOCKS4 which does support proxy-side DNS. NOTE: Not all SOCKS4 proxy servers provide this extension.

- “Force direct connection” means to not redirect this connection through a proxy.
- “Block” means to block this connection.

The icon on the right represents the selected rule action. The same icons are used in [the rule list view](#) to indicate the rule action.

Program

The Program section allows you to specify the program to which the rule applies.

If you want the rule to apply to a specific program, choose Specify, then press the Browse button on the right of the edit box. The Select Program dialog box will come up. Select the executable of the program you want

the rule to apply to, then press the Open button.

Transports

The Transports section lets you control which TCP/IP transport protocols the rule applies to. You must enable at least one protocol. SOCKS5 is the only proxy type that allows you to proxy UDP. If the rule action is “Redirect through proxy” and the specified proxy is not of the type SOCKS5, the UDP checkbox is grayed out. “TCP” is then the only available option.

Destination Port Range

The Destination Port Range section lets you specify which destination ports the rule applies to.

You can specify either a single port or an inclusive port range.

Destination IP Range

The Destination IP Range section lets you specify which destination IP range the rule applies to.

Address must be a plain IP address. The mask is a plain number, specifying the number of 1’s (bits) at the left side of the network mask. Thus, a mask of 24 is equivalent to 255.255.255.0 for IPv4 and FFFF:FF00:: for IPv6. When the mask is omitted, single IP assumed.

Note that if you enabled proxy-side DNS, the hostname is passed on to the proxy without being resolved. As a result, ProxyCap will never know the IP address and cannot check it against your routing rules.

Destination Hostname

The Destination Hostname section lets you specify which destination hostname the rule applies to.

A hostname must be a fully-qualified domain name. Wildcards are allowed. The asterisk character (*) substitutes for any zero or more characters, and the question mark (?) substitutes for any one character.

NOTE: The Quick Add Rule dialog box exposes only a subset of the features available. It doesn't allow you to define proxy chains, specify multiple programs, etc. To add a rule that utilizes these advanced features, use the New Routing Rule wizard.

Routing rule properties

The New Routing Rule wizard allows you to add a new routing rule. The Routing Rule Properties dialog box allows you modify an existing routing rule.

- [Rule Action](#)
- [Programs](#)
- [Destination Ports](#)
- [Destination IP Addresses](#)
- [Destination Hostnames](#)
- [Transports](#)

Rule Action

A routing rule can be assigned one of the following actions:


- “Redirect through proxy” means to redirect this connection through a proxy. You can specify more than one proxy. In this case, the program will pick a proxy for each connection randomly from the list. Instead of specifying the proxy explicitly, you can choose the special value “(default)”. Please see

[Setting the default proxy](#) for more information.

If you check the `&"temp0023.html">` the rule list view to indicate the rule action.

Programs

The Programs screen allows you to specify the programs to which the rule applies.

To add a program, press the Add  button on the toolbar. The Select Program dialog box will come up. Select the executable of the program you want to add, then press the Open button.

Destination Ports

The Destination Ports section lets you specify which destination ports the rule applies to.

You can specify either single ports or inclusive port ranges.

Destination IP Addresses

The Destination IP Addresses screen lets you specify which destination IP addresses the rule applies to.

You can specify either single IP addresses or inclusive IP address ranges.

Note that if you enabled proxy-side DNS, the hostname is passed on to the proxy without being resolved. As a result, ProxyCap will never know the IP address and cannot check it against your routing rules.

Destination Hostnames


The Destination Hostnames screen lets you specify which destination hostnames the rule applies to.


A hostname must be a fully-qualified domain name. Wildcards are allowed. The asterisk character (*) substitutes for any zero or more characters, and the question mark (?) substitutes for any one character.

Transports

The Transports screen lets you control which TCP/IP transport protocols the rule applies to. You must enable at least one protocol. SOCKS5 is the only proxy type that allows you to proxy UDP. If the rule action is “Redirect through proxy” and one or more of the specified proxies are not of the type SOCKS5, the UDP checkbox is grayed out. “TCP” is then the only available option.

Prioritizing rules

To raise the priority of a rule, click the rule and the up arrow  button until the rule is in the correct priority.

To lower the priority of a rule, click the rule and the down arrow  button until the rule is in the correct priority.

Disabling a rule

You can disable a rule instead of removing it.

To disable a rule, uncheck the check box on the left of the rule.

Predefined rules

ProxyCap has the following predefined routing rules that are checked before user-defined rules. If a predefined rule matches, then all user-defined rules are ignored.

Programs	IP Addresses	Hostnames	Ports	Transports	Action
(all)	127.0.0.0-127.255.255.255	(all)	(all)	(all)	Force direct connection
(all)	::1	(all)	(all)	(all)	Force direct connection

The DNS panel

The DNS panel allows you to specify which names must always be resolved locally.

A hostname must be a fully-qualified domain name. Wildcards are allowed. The asterisk character (*) substitutes for any zero or more characters, and the question mark (?) substitutes for any one character.

ProxyCap ensures that the following names and name groups are always resolved locally:

- “Localhost”
- The name of your computer
- Names defined in the “system_root\system32\drivers\etc\hosts” file

The Miscellaneous panel

The Miscellaneous panel allows you to control options that are not part of the ruleset.

- [Controlling product updates notifications](#)
- [Controlling error logging](#)
- [Controlling crash reporting](#)

Controlling product updates notifications

By default, ProxyCap is configured to automatically check for updates for itself and notify you when one is available. When prompted, just click the balloon and the ProxyCap Update wizard will come up. You will be given a brief description of the update and three options: Download, Decide later and Skip update. If you select the Download option, the new version will be downloaded and the ProxyCap installer will come up.

If you do not want to be notified when an update is available, untick the “Notify me when a new version of ProxyCap is available” box.

Controlling error logging

By default, ProxyCap logs proxy connection errors to a temporary log available through the Error Log tab of the ProxyCap Status and Logs dialog box. See [The Error Log screen](#) for more information.

If you do not want proxy connection errors to be saved, untick the “Enable error logging” box.

Controlling crash reporting

Software is complex and, like most complex things, is not perfect. Proxy Labs constantly strives to improve the reliability of the program. As part of that effort, Proxy Labs can gather information from your computer in the form of a report when ProxyCap experiences a serious error aka “crash”. The crash-reporting information enables the developers of ProxyCap to identify bugs. So, if crash reporting is turned on when a crash occurs,

there is a better chance that the bug that caused the crash will be fixed in the near future.

Crash reports include the following information:

- **Windows version information.** Includes the operating system version.
- **Date and time.** Indicates when the error occurred.
- **Software information.** Includes the name of the process where the error occurred and the list of loaded modules (DLLs).
- **Error information.** Includes the information the system recorded about the error.
- **Winsock configuration.** Contains information about the configuration of Windows sockets when the error occurred.

If you do not want crash reports to be sent to Proxy Labs, untick the “Submit crash reports” box.

Enabling or disabling ProxyCap

To disable ProxyCap, right-click on the ProxyCap tray icon and choose “Disable ProxyCap”. The grayed-out tray icon indicates that ProxyCap is disabled. Open connections that had been redirected through the proxies prior to ProxyCap being disabled are NOT interrupted.

To enable ProxyCap back, right-click on the ProxyCap tray icon and choose “Enable ProxyCap”

ProxyCap may disable itself if it encounters an error that prevents it from functioning properly. When you try to enable ProxyCap, it displays one of the following error messages:

Error message: “Not all ProxyCap components are loaded.”

Cause: The ProxyCap Service is not running.

Solution: Start the ProxyCap Service or restart Windows. If the error persists, contact support.

Error message: “Your system configuration is no longer compatible with ProxyCap.”

Cause: The Winsock configuration was modified by a program or user in such a way that ProxyCap cannot continue to function properly.

Solution: Reinstall ProxyCap. If the error persists, then there is a conflict between ProxyCap and some other program installed on your PC. If you have no idea which program it is, contact support.

Viewing status and logs

ProxyCap enables you to keep track of traffic and events through the ProxyCap Status and Logs dialog box that comes up if you right-click on the ProxyCap tray icon and choose “Status and Logs”.

- [The Connections screen](#)
- [The SSH Tunnels screen](#)
- [The Error Log screen](#)

The amounts of tunneled traffic in each direction and the number of active proxied connections are displayed in the bottom of the dialog box. The traffic figures apply to the current Windows session.

The Connections screen

The Connections screen lists open connections that were redirected through the proxies. The list includes the following information about each connection:

- The “Time” column shows how long the connection is open.
- The “Program” column shows the name of the executable for the program which initiated the connection.

- The “Proxy” column shows the name of the proxy.
- The “Transport” column shows the TCP/IP transport protocol.
- The “Destination” column shows the hostname (or IP address) and the port number of the destination.
- The “Sent” column shows the amount of data sent through this connection so far.
- The “Received” column shows the amount of data received through this connection so far.

The “Transports” column shows the TCP/IP transport protocol to which the rule applies.

You can show and hide list view columns. To show or hide a column, right-click the list header, then select or unselect the name of the column you wish to show or hide.

The SSH Tunnels screen

The SSH Tunnels screen lists established SSH tunnels. The list contains the following information about each tunnel:

- The “Time” column shows how long the tunnel is connected.
- The “SSH Server” column shows the display name of the SSH server.
- The “Via” column shows the display name(s) of the intermediate proxy server(s).
- The “Encryption” column shows the name of the encryption algorithm used to encrypt the data.
- The “Channels” column shows the number of open channels on the tunnel. Each channel corresponds to a tunneled connection.
- The “Sent” column shows the amount of data sent through this connection so far.
- The “Received” column shows the amount of data received through this connection so far.
- The “Connection” column indicates whether the tunnel connection is permanent or a disconnect was scheduled (see below).

Once a tunnel is established, it stays connected even when there are no open channels on the tunnel.

The “Schedule disconnect” command causes ProxyCap to disconnect from the SSH server after a delay. Once the command is issued, ProxyCap waits until there are no open channels on the tunnel. After that, the disconnection is delayed for additional 30 seconds. If no new channels are opened during this period, ProxyCap takes the tunnel down. If a proxied application tries to make a connection after the termination of the tunnel then a new tunnel is created.

To issue the “Schedule disconnect” command for an SSH tunnel, right-click on the row that represents the tunnel, then choose “Schedule disconnect” from the context menu.

You can show and hide list view columns. To show or hide a column, right-click the list header, then select or unselect the name of the column you wish to show or hide.