

## Squid General Settings

**Enable Squid Proxy**  Check to enable the Squid proxy.  
**Important: If unchecked, ALL Squid services will be disabled and stopped.**

**Keep Settings/Data**  If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.  
**Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.**

**Proxy Interface(s)**

LAN  
WAN  
loopback

The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.

**Proxy Port**

3128

This is the port the proxy server will listen on. Default: 3128

**ICP Port**

This is the port the proxy server will send and receive ICP queries to and from neighbor caches.

Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.

**Allow Users on Interface**

If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy.

There will be no need to add the interface's subnet to the list of allowed subnets.

**Patch Captive Portal**

**This feature was removed** - see Bug #5594 for details!

**Resolve DNS IPv4 First**

Enable this to force DNS IPv4 lookup first.  
This option is very useful if you have problems accessing HTTPS sites.

**Disable ICMP**

Check this to disable Squid ICMP pinger helper.

**Use Alternate DNS Servers for the Proxy Server**

To use DNS servers other than those configured in System > General Setup, enter the IP(s) here. Separate entries by semi-colons (;)

### Transparent Proxy Settings

**Transparent HTTP Proxy**

Enable transparent mode to forward all requests for destination port 80 to the proxy server.



Transparent proxy mode works without any additional configuration being necessary on clients.

**Important:** Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below.

**Hint:** In order to proxy both HTTP and HTTPS protocols **without intercepting SSL connections**, configure WPAD/PAC options on your DNS/DHCP servers.

**Transparent Proxy Interface(s)**

The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.

**Bypass Proxy for Private Address Destination**

Do not forward traffic to Private Address Space (RFC 1918) destinations.  
Destinations in Private Address Space (RFC 1918) are passed directly through the firewall, not through the proxy server.

**Bypass Proxy  
for These  
Source IPs**

Do not forward traffic from these **source** IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall.

**Applies only to transparent mode.** Separate entries by semi-colons (;)

**Bypass Proxy  
for These  
Destination  
IPs**

Do not proxy traffic going to these **destination** IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall.

**Applies only to transparent mode.** Separate entries by semi-colons (;)


### SSL Man In the Middle Filtering

**HTTPS/SSL  
Interception**

Enable SSL filtering.

**SSL/MITM  
Mode**

The SSL/MITM mode determines how SSL interception is treated when 'SSL Man In the Middle Filtering' is enabled.

Default: Splice Whitelist, Bump Otherwise. **Click Info for details.** 

**SSL Intercept  
Interface(s)**

The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.

**SSL Proxy  
Port**

This is the port the proxy server will listen on to intercept SSL while using transparent proxy.

Default: 3129

**SSL Proxy  
Compatibility  
Mode**

The compatibility mode determines which cipher suites and TLS versions are supported.


Default: Modern. **Click Info for details.** 

**DHParams  
Key Size**

DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.

CA

none

Select Certificate Authority to use when SSL interception is enabled. 

SSL  
Certificate  
Daemon  
Children

This is the number of SSL certificate daemon children to start. May need to be increased in busy environments. Default: 5

Remote Cert  
Checks

Accept remote server certificate with errors  
Do not verify remote certificate

Select remote SSL certificate checks to perform. Use CTRL + click to select multiple options.

Certificate  
Adapt

Sets the "Not After" (setValidAfter)  
Sets the "Not Before" (setValidBefore)  
Sets CN property (setCommonName)

See `sslproxy_cert_adapt` directive documentation and Mimic original SSL server certificate wiki article for details.

## Logging Settings

Enable Access  
Logging

This will enable the access log.

**Warning:** Do NOT enable if available disk space is low.

Log Store  
Directory

/var/squid/logs

The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs

**Important:** Do NOT include the trailing / when setting a custom location.

Rotate Logs

Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

Log Pages  
Denied by  
SquidGuard

Makes it possible for SquidGuard denied log to be included on Squid logs.

Click Info for detailed instructions. 

## Headers Handling, Language and Other Customizations

**Visible  
Hostname**

This is the hostname to be displayed in proxy server error messages.

**Administrator's  
Email**

This is the email address displayed in error messages to the users.

**Error  
Language**

Select the language in which the proxy server will display error messages to users.


**X-Forwarded  
Header Mode**

Choose how to handle X-Forwarded-For headers. Default: on 

**Disable VIA  
Header**

If not set, Squid will include a Via header in requests and replies as required by RFC2616.

**URI  
Whitespace  
Characters  
Handling**

Choose how to handle whitespace characters in URL. Default: strip 

**Suppress  
Squid Version**

Suppresses Squid version string info in HTTP headers and HTML error pages if enabled.



Save



Show Advanced Options