

CKYC HTTP Proxy Setup Guide

Client-run installation instructions for the realtime API proxy script hosted on the SignCare CDN.

Document ID	SC-CKYC-HTTP-PROXY-GUIDE	Version	1.0
Published	2 June 2026	Script URL	https://cdn.signcare.io/ckyc/scripts/configure-http-proxy.sh
Script SHA-256	b67e32f388354affe72f5a37726c2d717965670d4b29824bd30adbcca0822bde		
Applies to	Ubuntu/Debian servers used for CKYC realtime API egress		

Purpose

This guide explains how a client infrastructure team can install the SignCare CKYC realtime HTTP proxy on a whitelisted or soon-to-be-whitelisted Linux server. The proxy allows CKYC realtime API traffic to leave from the approved server IP while requiring basic authentication for access.

Important: This setup is only for realtime HTTP/HTTPS API connectivity. Restrict access to the proxy port to the source IP/CIDR values provided by your SignCare onboarding contact.

What the Script Does

- Installs Squid and required authentication utilities.
- Creates a proxy username and password, or uses the values supplied during execution.
- Backs up any existing Squid configuration and user file before replacing them.
- Writes a controlled authenticated forward-proxy configuration on port 3128 by default.
- Blocks access to localhost, private networks, link-local ranges, and common metadata endpoints.
- Disables caching so realtime API traffic is not stored by the proxy.
- Validates the Squid configuration before activating it.
- Runs a local proxy test and prints one machine-readable RESULT line.

Operating system	Ubuntu 22.04, Ubuntu 24.04, or Debian 12 preferred.	The script uses apt packages and has been tested on these distributions.
Privileges	Run as root through sudo.	Package installation and Squid configuration require root access.
Internet access	Outbound HTTPS to the SignCare CDN and OS package repositories.	The server must fetch the setup script and install packages.
Inbound firewall	Allow TCP/3128 only from source IP/CIDR values provided by SignCare.	This prevents the proxy from being publicly reachable.
Outbound firewall	Allow outbound HTTPS/443 to CKYC/CERSAI realtime API endpoints as advised.	Realtime API calls must be able to leave from this server.

Run the Setup

Use the standard command when you want the script to generate a secure proxy password automatically. The generated credentials appear only in the final RESULT line.

```
curl -fsSL https://cdn.signcare.io/ckyc/scripts/configure-http-proxy.sh | sudo bash
```

To supply a specific username and password, pass them after --. Use only letters, numbers, dot, underscore, or hyphen.

```
curl -fsSL https://cdn.signcare.io/ckyc/scripts/configure-http-proxy.sh | sudo bash -s -- <username> <password>
```

To run on a non-default port, set PROXY_PORT. Port 3128 is the default and recommended value unless SignCare has advised otherwise.

```
curl -fsSL https://cdn.signcare.io/ckyc/scripts/configure-http-proxy.sh | sudo env PROXY_PORT=3128 bash -s -- <username> <password>
```

SignCare onboarding team.

```
STEP install_packages
STEP backup
STEP create_user
STEP write_config
STEP validate_config
STEP restart_service
STEP test_proxy
RESULT {
  "status": "ok",
  "host": "203.0.113.10",
  "port": 3128,
  "username": "proxyuser",
  "password": "generated-or-provided-password",
  "proxy_url": "http://proxyuser:<password>@203.0.113.10:3128",
  "test_command": "curl -x http://proxyuser:<password>@203.0.113.10:3128 https://api.ipify.org"
}
```

Handle the RESULT line as confidential. It contains the proxy credentials needed by SignCare to configure CKYC realtime API routing.

Validate After Installation

From the proxy server, run the test command printed in the RESULT output. It should return the public IP of the proxy server.

```
curl -x http://<username>:<password>@127.0.0.1:3128 https://api.ipify.org
```

From an allowed source IP or a mutually agreed test machine, verify remote reachability:

```
curl -x http://<username>:<password>@<proxy-server-public-ip>:3128 https://api.ipify.org
```

Final RESULT line	Yes	Required. Contains proxy URL and credentials.
Server public IP	Yes	Usually present in RESULT.host; confirm if NAT or firewall changes apply.
Firewall confirmation	Yes	Confirm TCP/3128 is allowed only from SignCare-provided source IP/CIDR values.
Server SSH credentials	No	Do not share server login credentials unless a separate support process explicitly requires it.

Troubleshooting

Symptom	Likely cause	Action
RESULT says run as root	The command was not run with sudo/root.	Run the setup command again with sudo.
unsupported system: apt-get not found	The server is not Debian/Ubuntu based.	Use Ubuntu/Debian or contact SignCare for a distribution-specific setup path.
install_packages failed	Package repository or outbound internet access issue.	Allow outbound package repository access, then rerun the same command.
squid config validation failed	Squid rejected the generated configuration.	Share the RESULT line with SignCare. The script restores previous config backups when validation fails.
local proxy test failed	Squid did not start correctly or outbound HTTPS is blocked.	Check service status and outbound HTTPS/443, then rerun.
SignCare cannot reach proxy remotely	Firewall/security group does not allow inbound TCP/3128 from SignCare source IPs.	Update inbound firewall rules to allow only the SignCare-provided source IP/CIDR values.

provided source IP/CIDR values.

- Do not reuse the generated proxy password for any other system.
- Do not paste the RESULT line in public tickets or shared channels. It contains credentials.
- The script replaces the local Squid proxy configuration after taking timestamped backups under /etc/squid/.
- The proxy is configured for HTTP/HTTPS forwarding and blocks private, localhost, link-local, and common cloud metadata destinations.
- Rerunning the script is supported. If validation fails, previous files are restored before the failed RESULT line. For password rotation, rerun with a new password and share the new RESULT line.