FIELD NOTES FROM A PRESALES SOLUTIONS ARCHITECT

AutoSSL Quietly Dropped the Mail Name — a Cloudflare-Only Origin and the Move to DNS-01

A field story about a cPanel certificate that renewed on time and still broke every Outlook client — the port 80 rule almost nobody connects to mail — and the DNS-01 setup I now use for any origin locked to Cloudflare.

Daanial Farrukh · 21 November 2026 · https://quabin.com/autossl-dropped-mail-hostname-cloudflare-dns-01/

The message came in the next morning.

"Outlook is showing a certificate warning on every laptop. Nothing changed on our side."

The customer's IT lead had already checked the website. Green padlock. Valid certificate. Renewed the evening before.

"So the certificate is fine," he said. "It renewed. Why is Outlook complaining?"

I asked one question: "Which names are on the new certificate?"

He opened it. The site name was there. The www name was there.

The mail name was not.

That's the trap. **A certificate renewal can succeed and still lose a name.** cPanel does not fail the renewal when one name cannot be validated. It issues the certificate for the names that passed and moves on. The website stays green, so nobody looks further.

What Actually Happened

On this server, the web names and the mail name take two different paths.

The web names are proxied through Cloudflare:

Visitor → Cloudflare → Origin

The mail name is DNS-only. It has to be. IMAP and SMTP clients connect straight to the server, because Cloudflare's normal proxy only carries web traffic:

Outlook → mail.example.com → Origin (993, 465, 587)

Now add one hardening rule we had put in place earlier: the virtualisation platform's distributed firewall allowed TCP 80 and 443 to this VM **only from Cloudflare's IP ranges**. That is a good rule. It stops anyone from going around Cloudflare's WAF and hitting the origin directly.

Here is the part that trips people up. AutoSSL uses Let's Encrypt with HTTP validation by default. For each name on the certificate, Let's Encrypt connects to that name on port 80 and fetches a token file.

- For example.com, Let's Encrypt connects to Cloudflare. Cloudflare passes the request to the origin. Allowed.
- For mail.example.com, DNS points straight at the origin IP. Let's Encrypt connects from its own servers, not from Cloudflare. The firewall drops it. Timeout.

So the renewal ran, the web names passed, the mail name timed out, and AutoSSL issued a certificate without it. Dovecot and Exim then had no certificate that matched mail.example.com, so they served the server's hostname certificate. Outlook compared the name it asked for with the name on the certificate and showed the warning the customer saw: the target principal name is incorrect.

Where this pattern is common:

- cPanel servers behind Cloudflare with an origin lockdown (firewall, security group or host rules that allow only Cloudflare ranges).
- Any server where the web names are proxied and the mail, FTP or control-panel names are DNS-only.
- Servers where someone "tightened port 80" months ago and the first renewal after that is the first time anyone notices.

Why Nobody Sees It in Testing

The hardening was tested. The website worked. Direct access to the origin was blocked, as designed. Every check passed.

The failure only shows up at renewal time, which with Let's Encrypt is weeks or months after the change. By then, nobody links "Outlook warning today" with "firewall rule last quarter".

And the usual check misses it, because the usual check is the browser padlock. The padlock looks at the web name. The web name was fine.

The Wrong First Fix

The customer's IT team did the reasonable thing first. They went into cPanel and reinstalled the old certificate, the one that still had the mail name on it.

The warnings stopped. For a little over two hours.

Then AutoSSL ran again. AutoSSL checks every few hours and renews when a certificate is within a few days of expiry. The reinstalled certificate was close to expiry, so AutoSSL replaced it with a fresh one — again without the mail name.

A manual reinstall does not hold against AutoSSL. AutoSSL owns that certificate slot. Whatever you install by hand, it will replace on its next run if it thinks it can do better.

How to Actually Fix This

Step 1: Confirm Which Names the Mail Ports Really Serve

Do not trust the website. Ask the mail port directly. This is read-only.

```
openssl s_client -connect mail.example.com:993 -servername mail.example.com </dev/null 2>/dev/
null | openssl x509 -noout -subject -ext subjectAltName -enddate
```

A healthy answer lists mail.example.com under the subject alternative names. A broken one lists only the server hostname, or only the web names. Repeat for 465 and 587 if you use them. The mail ports can serve different certificates, so check each one.

Step 2: Read the AutoSSL Log for the Missing Name

```
ls -t /var/cpanel/logs/autossl/ | head -3
```

Open the newest folder's txt file and search for the mail name. You are looking for the domain control validation (DCV) result. In this case the HTTP check for mail.example.com had timed out, while every proxied name passed.

Plain takeaway: a timeout on one name and success on the others points at the network, not at DNS or cPanel.

Step 3: Prove Where the Packets Stop

This is the step that turns a theory into a cause. On the origin, watch port 80 while someone outside tries to reach it directly:

```
tcpdump -ni any 'tcp port 80 and host 198.51.100.25'
```

Here 198.51.100.25 stands for the public IP of the test machine. Then, from that machine:

```
curl -m 10 -I http://203.0.113.10/
```

If curl times out (exit code 28) and tcpdump shows **zero packets**, the drop happens before the VM. In our case the host firewall was not the reason: UFW was inactive, there was no CSF, and nftables had no inbound drop rules. The block was upstream, in the platform's distributed firewall.

This step is where most tutorials stop and where mine starts. Zero packets on the VM is the proof. Without it, you are guessing between the host firewall, the provider and Let's Encrypt.

Step 4: Short-Term — Open Port 80, Renew, Verify

To get the mail name back the same day, the platform team opened TCP 80 from any source to the VM.

One detail matters. The first attempt opened port 80 to a list of sources, not to everyone. Let's Encrypt still timed out. Let's Encrypt validates from several networks around the world and does not publish a fixed list, so "some sources" is not enough. HTTP validation needs port 80 open to any source.

Then trigger AutoSSL for the account:

```
/usr/local/cpanel/bin/autossl_check --user=exampleuser
```

Re-run the Step 1 check on 993, 465 and 587. The new certificate listed the mail name and carried a full ninety-day validity.

That buys you ninety days. It does not fix the design. The moment port 80 goes back to Cloudflare-only, the next renewal drops the mail name again.

Step 5: Long-Term — Validate Over DNS, Not Port 80

DNS-01 validation does not connect to your server at all. The client creates a TXT record under _acme-challenge, Let's Encrypt reads it from DNS, and the record is removed. The firewall becomes irrelevant to certificates.

Since the zone was already on Cloudflare, I used acme.sh with the Cloudflare DNS plugin. Create a Cloudflare API token scoped to **Zone › DNS › Edit** for this zone only. Then, as root:

```
export CF_Token="<scoped-token>"
```

```
acme.sh --issue --server letsencrypt --dns dns_cf --keylength 2048 -d example.com -d www.
example.com -d mail.example.com -d webmail.example.com -d cpanel.example.com
```

acme.sh saves the token in /root/.acme.sh/account.conf (mode 600) for renewals. Delete any other copy you made, such as an env file. The token itself must stay active, or renewals will fail.

Step 6: Hand the Certificate to cPanel

acme.sh ships a cPanel deploy hook that installs the certificate through UAPI, and re-runs it on every renewal:

```
export DEPLOY_CPANEL_USER=exampleuser
```

```
acme.sh --deploy -d example.com --deploy-hook cpanel_uapi
```

acme.sh's own cron job checks for renewal every day; I run it four times a day so a failed attempt is retried quickly.

Step 7: Tell AutoSSL to Stay Away From These Names

If you skip this, AutoSSL and acme.sh will fight over the same slot. Exclude every name acme.sh now owns:

```
uapi --user=exampleuser SSL add_autossl_excluded_domains domains=example.com,www.example.com,
mail.example.com,webmail.example.com,cpanel.example.com
```

Then re-run the Step 1 check on 443, 993 and 465. All three should show the acme.sh certificate with the mail name on it.

Step 8: Put Port 80 Back — But Not Fully Shut

Now close port 80 back to Cloudflare-only. Not fully closed. Here is why.

The server's own hostname was also proxied through Cloudflare, and we kept it on cPanel AutoSSL. Its HTTP validation still needs port 80 — reached through Cloudflare. So the rule is: port 80 from Cloudflare ranges only.

Two checks prove the rule is right:

```
curl -m 10 -I http://203.0.113.10/
```

Direct to the origin must time out (exit code 28).

```
curl -sI http://server.example.com/.well-known/acme-challenge/test
```

Through Cloudflare, this must return a 404 **from the origin** with cf-cache-status: DYNAMIC. A 404 is the right answer here — there is no such token file. It shows that a real validation request would reach the server. This error is not a bug. It is the verification.

The Second Certificate Nobody Was Renewing

About a week later the server moved to a new operating system version. Afterwards I checked the mail ports again, and found a second gap.

Dovecot's SNI map now pointed mail.example.com at the **service certificate** — the one cPanel keeps for Dovecot, Exim, FTP and cPanel itself in /etc/dovecot/ssl/dovecot.crt — not at the acme.sh certificate. That service certificate was valid. But acme.sh did not renew it, and it was not in any AutoSSL log. Nothing known was renewing it.

So I issued a second DNS-01 certificate with acme.sh for the server hostname plus the mail name, and installed it as the service certificate on every renewal with a small reload script that calls:

```
whmapi1 install_service_ssl_certificate service=dovecot crt=... key=... cabundle=...
```

once each for dovecot, exim, ftp and cpanel.

One gotcha cost me time. The whmapi1 command line URL-decodes its arguments. A PEM certificate is base64, and base64 contains +. URL-decoding turns + into a space, and the call fails with "Invalid base64". The fix is to URL-encode each PEM before passing it — in the script I used Python's urllib.parse.quote. After that, the reload printed "Reload successful", and 993 showed the new certificate.

Plain takeaway: "the certificate" on a cPanel server is often several certificates. Check what each port serves, and know which tool renews each one.

The Checklist I Run Now

1. **Which names does each mail port serve?** openssl s_client ... | openssl x509 -noout -ext subjectAltName on 993, 465 and 587.
2. **Which names are DNS-only?** Any DNS-only name on an origin locked to Cloudflare cannot pass HTTP validation.
3. **Who renews each certificate?** acme.sh --list for acme.sh, the AutoSSL log for AutoSSL. A certificate in neither list will expire silently.
4. **Is AutoSSL excluded from the names acme.sh owns?** Otherwise they overwrite each other.
5. **Does port 80 through Cloudflare still reach the origin?** The /.well-known/acme-challenge/test 404 with cf-cache-status: DYNAMIC.
6. **Is direct port 80 blocked?** curl to the origin IP must time out.
7. **Is the first auto-renewal confirmed?** Put a calendar reminder a week after the expected renewal and check the new end date on every port.

What I Tell Every Customer Now

When a customer locks their origin to Cloudflare, I ask one more question before we close the change:

"Which names on this server are not behind Cloudflare, and how do their certificates renew?"

If the answer is "mail is on DNS-01, the rest go through Cloudflare", they're in good shape. If the answer is "AutoSSL handles it", we're not done yet — AutoSSL will handle it right up to the renewal that quietly leaves the mail name out.

I write about the questions I ask in real customer rooms — the ones that change architectures and surface the problems no one else noticed. If you found this useful, drop your email below and I'll send the next one when it's ready.

FAQs

Why did AutoSSL renew my certificate without the mail subdomain?

AutoSSL issues a certificate for the names that pass validation and leaves out the ones that fail. With HTTP validation, Let's Encrypt must reach each name on port 80. If the mail name is DNS-only and the origin accepts port 80 only from Cloudflare, that check times out and the mail name is dropped.

Why does Outlook say "the target principal name is incorrect" after a renewal?

Outlook connected to the mail name, but the server presented a certificate that does not list that name. On cPanel this usually means the mail name fell off the domain certificate, so Dovecot and Exim fell back to the server hostname certificate. Check the names on port 993 with openssl s_client.

Can I just reinstall the old certificate in cPanel?

It works only until the next AutoSSL run. AutoSSL checks every few hours and replaces a certificate that is close to expiry. Either fix the validation path or move the names to DNS-01 and exclude them from AutoSSL.

Do I need to open port 80 to everyone for Let's Encrypt?

For HTTP validation, yes: Let's Encrypt validates from several networks and does not publish a fixed list of addresses. Opening port 80 to a few sources is not enough. DNS-01 validation avoids the question, because it never connects to your server.

How do I use DNS-01 on a cPanel server with Cloudflare DNS?

Install acme.sh, create a Cloudflare API token limited to DNS edit on the zone, and issue with --dns dns_cf. Deploy with the cpanel_uapi hook so every renewal is installed, and add the names to the AutoSSL exclusion list with uapi SSL add_autossl_excluded_domains.

Should I close port 80 completely after moving to DNS-01?

Only if no remaining name uses HTTP validation. If the server hostname is still on AutoSSL through Cloudflare, keep port 80 open to Cloudflare ranges only, and confirm that a test path under /.well-known/acme-challenge/ returns an origin 404 through Cloudflare.

Read online: https://quabin.com/autossl-dropped-mail-hostname-cloudflare-dns-01/