Blog

We've Issued Our First IP Address Certificate

By Aaron Gable · July 1, 2025

Since Let's Encrypt started issuing certificates in 2015, people have repeatedly requested the ability to get certificates for IP addresses, an option that only a few certificate authorities have offered. Until now, they've had to look elsewhere, because we haven't provided that feature.

Today, we've issued our first certificate for an IP address, as we announced we would in January. As with other new certificate features on our engineering roadmap, we'll now start gradually rolling out this option to more and more of our subscribers.

Some Background on IP Address Certs

IP addresses are the underlying numerical addresses used on the Internet. Every device on the Internet has one (though, in modern practice, it might be shared with other devices, like when an entire home network shares a single public IP address). The Internet infrastructure uses them to route communications to their proper destination. IP addresses come in two forms, IPv4 and IPv6, and generally look like 54.215.62.21 (IPv4) or 2600:1f1c:446:4900::65 (IPv6).

Most Internet users rarely see or refer to IP addresses directly. Instead, they almost always use domain names like letsencrypt.org to refer to Internet services. The domain name system (DNS) is a part of the Internet infrastructure that's responsible for allowing software to find the IP addresses associated with a particular domain name. For instance, your web browser can use DNS to find out that the service https://letsencrypt.org/ (Let's Encrypt's own website) is provided from the IP addresses 54.215.62.21 and 2600:1f1c:446:4900::65, among several others. This probably happened behind the scenes before you started reading this article! Your web browser needed to know our IP address in order to actually connect to our site and fetch this article.

Because we overwhelmingly tend to think and talk about Internet services in terms of domain names, those are the identifiers that are normally listed in certificates like those that Let's Encrypt provides to our subscribers. Since you know us as "letsencrypt.org" and not as, say, "54.215.62.21," it makes the most sense for our domain name to be on our certificate. After all, that's what you'll want your web browser to check against. This also gives Internet services more flexibility to be hosted in multiple locations, or to change where they're hosted, without necessarily needing separate certificates for each server.

In principle, there's no reason that a certificate couldn't be issued for an IP address rather than a domain name, and in fact the technical and policy standards for certificates have always allowed this, with a handful of certificate authorities offering this service on a small scale. In Let's Encrypt's case, we've preferred to wait until some other pieces, like short-lived certs, were in place before we made this option available for our subscribers.

Why IP Address Certs Are Less Common

First and foremost, it's because Internet users usually know services by domain names, not by IP addresses, and because IP addresses can easily change "behind the scenes" with no prior notice. For instance, a popular site could switch from one cloud hosting company to a different one, and update its DNS records to point at the new host. Most users wouldn't ever notice the change at all, even though the site's underlying IP addresses would be completely different.

Second, because IP addresses can change so easily, the sense of "ownership" one might have for them—or that a certificate authority might be able to attest to—tends to be weaker than for a domain name. If you're hosting something in your house on a residential broadband connection, your Internet service provider most likely doesn't guarantee that your IP address will stay the same over time. (That is, most home Internet users have a "dynamic IP address" from their ISPs, rather than a "static IP address.") In that case, you have to contend with the possibility that that address may change often, possibly without warning, and that your old address may be assigned to somebody else.

Third, most Internet service operators don't expect that end users will ever intentionally connect to their sites directly by IP address. In some cases, when an IP address is shared by different websites or different devices, connecting by IP address alone wouldn't even work properly. In that case, there's not much benefit to obtaining a certificate for the IP address!

How Let's Encrypt Subscribers May Use IP Address Certs

Most current subscribers should be fine with their existing domain name certs and won't need IP address certs. Subscribers who have a use for an IP address cert are typically already aware of that. A few use cases that we're aware of include:

- A default page for hosting providers, in case someone pastes a server's IP address into a browser instead of an individual site name (right now, this normally produces an error in the browser).
- A way to access your website if you don't have a domain name at all (at some cost in reliability and convenience compared to getting a domain name).
- Securing DNS over HTTPS (DoH) or other infrastructure services. Having a certificate makes it much easier for DoH servers to prove their identities to clients. That could make it more feasible for DoH users or clients to enforce a requirement for a valid publicly-trusted certificate when connecting to DoH servers.
- Securing remote access to some home devices (like network-attached storage servers and Internet-of-things devices) even without a domain name.
- Securing ephemeral connections within cloud hosting infrastructure, like connections between one back-end cloud server and another, or ephemeral connections to administer new or short-lived back-end servers via HTTPS—as long as those servers have at least one public IP address available.

How To Get an IP Address Cert

IP address certificates are available right now in Staging. They should be generally available in Prod later in 2025, at the same time that short-lived certificates become generally available. Prior to general availability we may allow list issuance for a limited number of partners who can provide us with feedback.

Many Let's Encrypt client applications should already be able to request certificates for IP addresses, although there can be minor technical changes required to support this in some client software.

As a matter of policy, Let's Encrypt certificates that cover IP addresses must be short-lived certs, valid for only about six days. As such, your ACME client must support the draft ACME Profiles specification, and you must configure it to request the `shortlived` profile. And, probably not surprisingly, you can't use the DNS challenge method to prove your control over an IP address; only the http-01 and tls-alpn-01 methods can be used.

If your client software requests an IP address cert with details that aren't compatible with these policies, the order will be rejected by the ACME server. In this case, your client application may need to be updated or reconfigured. Feel free to ask for help on the Let's Encrypt community forum if you encounter any problems, either as a client application developer or as an end user.

LEGAL ADDRESS
548 Market St,
PMB 77519
San Francisco, CA
94104-5401
USA

SEND ALL MAIL OR INQUIRIES TO:
PO Box 18666
Minneapolis, MN
55418-0666
USA

Email

- [ ] Brighter Bytes: the ISRG Newsletter
- [ ] Let’s Encrypt Technical Updates
- [ ] Let’s Encrypt Service Statistics
- [ ] Prossimo: Updates about our memory safety project
- [ ] Divvi Up: Updates about our privacy-respecting metrics project

Sign Up

Note: You can opt-out at any time. See our Privacy Policy.