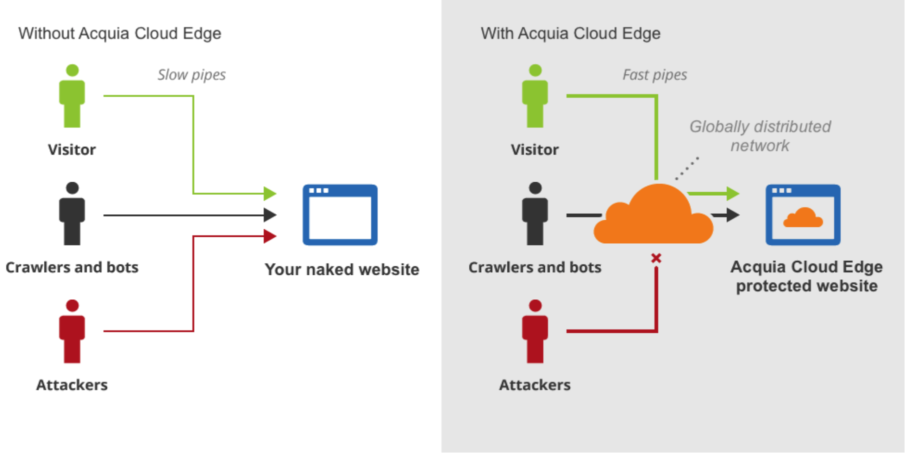
Acquia Cloud Edge Onboarding Guide

Acquia Cloud Edge at a Glance

The Acquia Cloud Edge product family extends the security and performance advantages of the Acquia Platform to the edge of the distribution network. Edge Protect mitigates a range of online threats before they can affect the delivery of your site. Edge CDN ensures that global visitors interact with your site at the fastest possible speeds for the best experience with your brand.



Acquia Cloud Edge Protect

Acquia Cloud Edge Protect enables you to deliver the highest levels of site availability and security by mitigating distributed denial-of-service (DDoS) and other online attacks. With Edge Protect, attack traffic that would otherwise directly hit your web servers is automatically routed to Edge Protect's global network of 100 data centers, which filter and absorb the flood of attack traffic at the edge through a web application firewall (WAF) and advanced DDoS protection system. This ensures that only legitimate network traffic reaches your web servers, enabling you to deliver an optimal digital experience to your visitors.

Acquia Cloud Edge CDN

Acquia Cloud Edge CDN drastically reduces site response times so you can deliver exceptional experiences. Edge CDN speeds up your sites by caching static content across a global content delivery network (CDN). When visitors go to your site, Edge CDN automatically optimizes the delivery of your web content so your visitors get the fastest page load times and best performance from wherever they are around the world. Edge CDN is powered by a global network of 100 data centers which use modern, SSD-based hardware without the legacy of the last 15 years. Edge CDN can reduce page load times by up to 50 percent, decrease the number of requests hitting your origin web servers and decrease bandwidth utilization, ensuring that your visitors experience your digital experience the way it was meant to be experienced.

Getting Started - Four Things to Consider

1. Who should have access to manage Acquia Cloud Edge?

Acquia Cloud Edge supports a delegated administration model that allows you to assign different roles to different users so they can control the various Edge CDN and/or Protect settings. Administration membership is controlled at the "organization" level. An organization is a container of one or more domains managed by one or many administrators. All members within an organization have access to all domains with that organization, with access to the Edge features governed by their assigned role(s). It is not possible to restrict an individual member's access to a specific domain within a multi-user organization, so keep this in mind as you provide access to the members of your team(s).
The Edge roles available to your team members are the following:

Role	Responsibility
Analytics Administrator	Restricted to the Analytics tab; member allowed to view analytics data for a domain. Analytics data includes number of cached vs. uncached requests to the domain, amount of bandwidth delivered through the CDN, etc.
Cache Purge	Restricted to the Caching tab; member allowed to clear the global CDN cache for the domain. This role applies to **Edge CDN customers only.**
Crypto, Caching, Performance, Page Rules, and Customization	Restricted to the Crypto, Caching, Speed, Page Rules and Customize tabs; member allowed to manage the SSL certificate, caching and performance settings, page rule configuration, and custom error pages for the domain. This role has all of the permissions required to manage the CDN-specific settings for the domain.
DNS Administrator	Restricted to the DNS tab; member allowed to make DNS-related configuration changes for the domain.
Firewall Administrator	Restricted to the Firewall and Traffic tabs; member allowed to change website's security level, enable WAF and IP Firewall as well as see when IP Firewall and WAF events were triggered. This role applies to **Edge Protect customers only.**
Raw Logs Access	Not granted explicit administrator console UX access; member allowed to call an API endpoint to download Edge CDN web logs for processing by Splunk, Sumologic, or other third-party log analytics services.

2. Which domains do you want to protect and/or accelerate?

You will manage one or more domain accounts within each organization. A domain account is created for each second-level domain (e.g. domain.com, school.edu, etc.) that you want to manage through Acquia Cloud Edge. Domain accounts are the actual accounts accessed by Edge administrators to control the Edge settings for a specific domain. Once the second-level domain is added to Edge, you can enable the necessary settings and also add subdomains. The Acquia Ready team will be able to assist you with this step.

3. What DNS approach will you use?

DNS changes are required to route traffic to your site(s) through the Acquia Cloud Edge network. Acquia Ready can set up your domain accounts on Cloud Edge using one of two DNS configuration approaches, with Edge providing full authoritative DNS or using a partial CNAME configuration. Choose the approach that works best for your needs.

Full (authoritative) DNS setup

With this approach, Acquia Cloud Edge becomes the authoritative DNS for your domain. This mode requires you to move all of your DNS records for a domain to Acquia Cloud Edge. Cloud Edge's DNS service is one of the fastest, largest, and most secure in the world, supporting millions of domains and delivering fast name resolution times (www.dnsperf.com).

Using Cloud Edge as your authoritative DNS makes the Edge set-up and management process easier. The Cloud Edge default SAN certificate is automatically issued with this approach, and you are able to accelerate and/or protect the bare domain as well.

To take advantage of the Edge authoritative DNS service, you will need to point to the Cloud Edge nameservers in order to activate this set-up.

If you are a Cloud Edge Protect customer, Acquia Ready recommends to utilize the Full Authoritative DNS setup as this affords the highest protection level available.

Advantages

- Cloud Edge DNS provides fast, reliable, and secure global DNS services.
- DNS setup is simpler, as you have only one DNS service to manage.
- If you are using SSL then you can protect the bare domain with an SSL certificate.
- The bare domain and DNS are fully covered with DDoS and WAF protection.

Disadvantages

- You must be prepared to move all of your DNS to Acquia Cloud Edge. If you wish to protect only a single subdomain, or if your current provider hosts DNS for domains that are not part of your Edge subscription, then you may need to keep your DNS where it is and consider the second option, described below.

Partial (CNAME) DNS setup

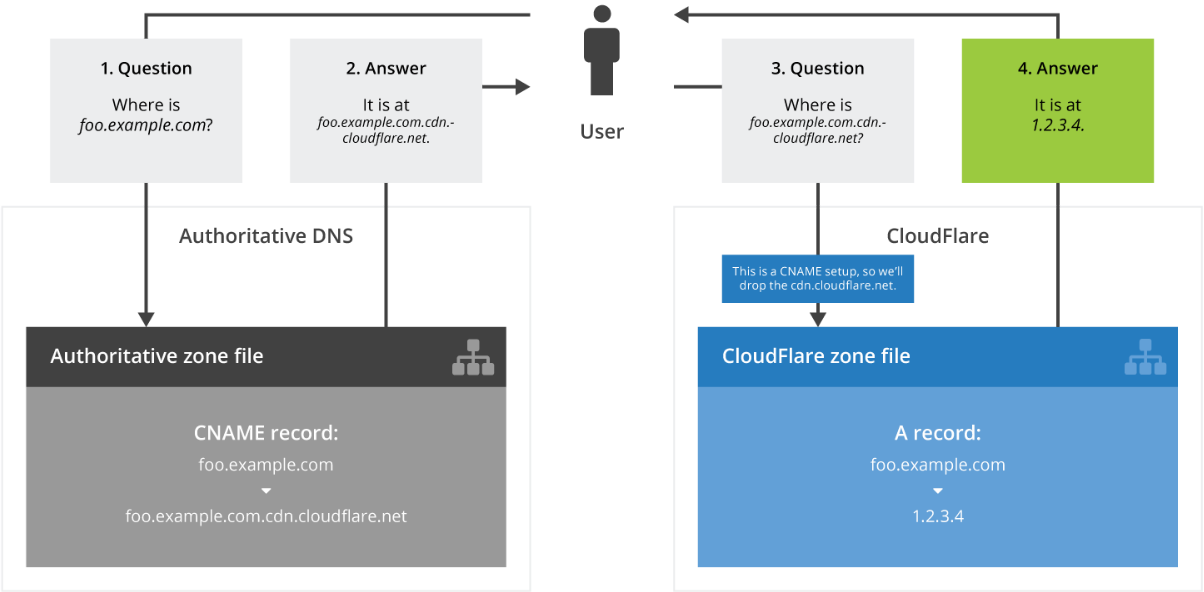
With this approach, you manage DNS records through your current authoritative DNS, and only direct requests to the site (via a subdomain) through the Cloud Edge network. This mode offers greater flexibility, allowing you to control which of your sites, or which parts of your sites, are served through Edge using a CNAME record (e.g. www.example.com can be CNAME'd to www.example.com.cdn.cloudflare.net). Please see the image below for more information about the CNAME process. With this implementation you will manage DNS through your current authoritative DNS and the Edge DNS services. Note that the bare domain cannot be proxied through the Edge network in this setup unless your DNS supports "ANAME" records. If you wish all traffic to be encrypted, you must implement a redirect from the bare domain to a subdomain (e.g. www).

Your Authoritative DNS

CNAME	www.yourdomain.com	www.yourdomain.com.cdn.cloudflare.net

Acquia Cloud Edge DNS

CNAME	www.yourdomain.com	origin.yourdomain.com
A	origin.yourdomain.com	123.456.543.210


1. Question
Where is *foo.example.com?*
2. Answer
It is at *foo.example.com.cdn.-cloudflare.net.*
User
3. Question
Where is *foo.example.com.cdn.-cloudflare.net?*
4. Answer
It is at *1.2.3.4.*
Authoritative DNS
Authoritative zone file
CNAME record:
foo.example.com
foo.example.com.cdn.cloudflare.net
CloudFlare
This is a CNAME setup, so we'll drop the cdn.cloudflare.net.
CloudFlare zone file
A record:
foo.example.com
1.2.3.4

Source: https://support.cloudflare.com/hc/en-us/articles/200168706-How-do-I-do-CNAME-setup-

If you choose the partial CNAME setup, you will be asked to add a TXT record (provided by Acquia Ready) to your authoritative DNS to validate ownership of the domain. This validation is an important security measure to prevent the possibility of domain hijacking. It ensures the party who claims ownership of the domain also has the ability to make DNS configuration changes for it.

Additionally, if you use the Edge default SAN certificate for SSL, you will be required to add three CNAME records to your authoritative DNS to authorize and issue the certificate.

Advantages

- Offers greater flexibility, allowing you control which of your sites, or which parts of your sites, are served through the CDN.

Disadvantages

- Your Cloud Edge DNS implementation will require changes to both your authoritative DNS and the Edge DNS, increasing the effort required to maintain it.
- You are unable to protect the bare domain with an SSL certificate. If you wish all traffic to be encrypted then you must implement a redirect from the bare domain to a subdomain (e.g., www).
- Your DNS infrastructure and bare domain will not be protected from DDoS or malicious traffic.

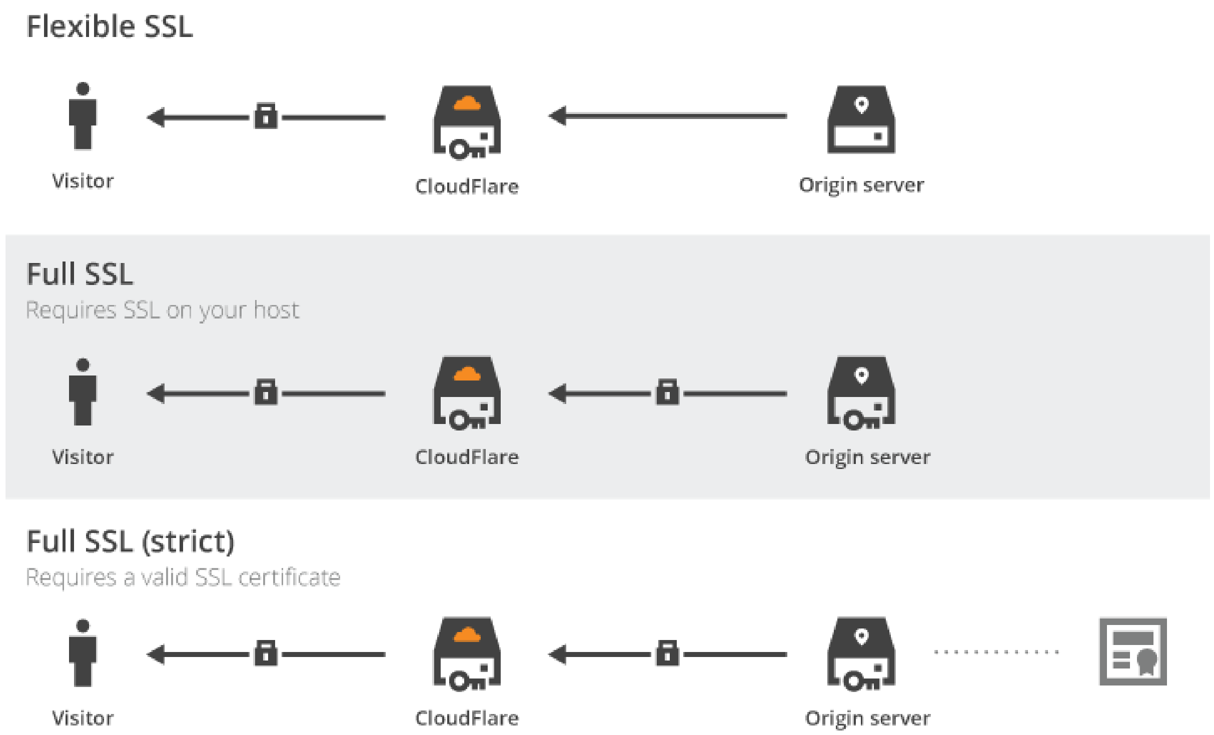
If you wish to protect only a single subdomain, or if your current provider hosts DNS for domains that are not part of your Edge subscription, or if your organization mandates the use of a specific DNS service or provider, then you may need to keep your DNS where it is and consider the Partial CNAME option.

The Acquia Ready team is available to provide additional consultation on the differences and things to consider when choosing one or the other option.

4. Consider SSL Certificates

As an Edge customer you can utilize Cloud Edge's default SAN certificate to provide SSL encryption on your websites. We recommend the use of this certificate whenever possible as it is automatically included as part of Acquia Cloud Edge, enables you to deliver a secure visitor experience if required, and reduces the level of effort required to maintain and manage the certificate going forward. The SAN certificate is automatically renewed and updated for you upon expiration without any involvement from your employees.

There are three SSL settings that you can choose from and enable for each of the top-level domains separately: Flexible SSL, Full SSL, Full (strict) SSL.



The Acquia Ready team recommends enabling the Full SSL mode as it encrypts the connection between your visitors and Edge, and from Edge to origin. Full (strict) SSL should be considered if the highest levels of encryption are required.

If you have chosen the Partial CNAME DNS approach and want to use the default SAN certificate, Acquia Ready will provide you with SSL authorization CNAME records that need to be added to your authoritative DNS to validate the issuance of the Cloud Edge SAN certificate that covers your domain.

The CNAME entry provided by Acquia will look similar to this:

```
A6B19DA764460FE4C941DA85A029186B.domain1.com CNAME
E8BB4748A5A758C2878363390ED1940E24A0D518.comodoca.com
```

The default SAN certificate issued by Cloud Edge covers the bare domain and wildcard support for second level subdomains (e.g. example.com and *.example.com) at the Edge data centers, supporting encrypted communication between the visitor’s browser and the Edge data centers. If you need to encrypt traffic to deeper-level subdomains, you will need to use your own custom SSL certificate.

Your Edge subscription allows you to upload your own SSL certificate should you not wish to use the default one. The number of custom SSL certificates that you can upload depends on the package that you have purchased. If you plan to upload your own custom SSL certificate, you will not need to add the CNAME record to validate the Acquia Cloud Edge-issued SAN certificate.

Acquia Cloud Edge QuickStart - what to expect from your onboarding

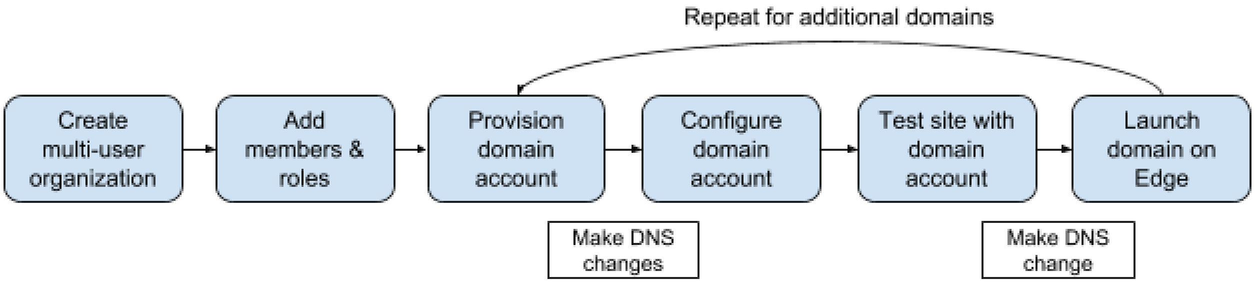
As part of your Acquia Cloud Edge Quick Start our Acquia Ready team will be able to provide initial guidance and support to make sure you and your team are fully enabled on using Edge going forward. Our activities are performed over the course of **two weeks** and include:

- Cloud Edge initial account provisioning of a multi-user organization and up to 11 initial domain accounts;
- initial configuration;
- introduction and guided walkthrough of the Edge administration dashboard;
- additional advice on implementing Cloud Edge, including such topics as: page rules, SSL, DNS approach etc.

Your Acquia Ready Customer Onboarding Manager will engage with you to discuss the full onboarding process.

Cloud Edge Provisioning Process

When you purchase an Edge subscription, a number of synchronized configuration steps are performed by both Acquia and yourself to provide the necessary access to a per-domain Edge account through which you will manage that domain's DNS, SSL, and CDN or Security configurations. One or more domain accounts will be provisioned for you depending on the number of domains for which you purchased Edge. The provisioning process is shown below:



Acquia Ready will provision the organization, invite assigned members, and assign the desired roles to members. Note that all members within a multi-user organization will have access to all domains within that organization, with access governed by their assigned role(s).

Technical Considerations & Best Practices

Here is a list of steps that we consider essential for ensuring you are making the most use of your Edge subscription.

Choose an SSL mode

- You can use the flexible mode regardless of whether you already own a certificate or not. Choose the full mode if you have a self-signed certificate and if you own a certificate signed by a valid Certificate Authority, choose the Full(Strict) option.
- If you want to use HTTPS only on your website, your Acquia Ready team will be able to guide you on how you can redirect all visitors to HTTPS. They will also be able to help you upload your custom SSL certificate.

Validate your DNS settings

- When configuring the TXT and CNAME records during the domain provisioning process, you can validate that the DNS records have been properly configured and have fully propagated by using the propagation validation service at https://www.whatsmydns.net.
- Navigate to the URL in a browser and enter the name of the TXT or CNAME record you want to check. If the value has propagated, the validation service will identify the value of the name and report its availability across the world. If the value has successfully propagated, you will be ready to move to the next step of the domain provisioning process.

Review your performance settings (Edge CDN customers)

- You can customize your performance settings in your CloudFlare Dashboard under the “Speed” and “Caching” apps along the top navigation menu.
  - Acquia Cloud Edge is an “intermediate” cache that stands between any application level caching (i.e., memcache, Drupal database caching) and browser caching. Within Drupal, there are settings that control how content is cached, and there are modules available to communicate these settings to external caches so that they can act in accordance with these settings.
  - On Acquia’s own stack, Varnish is an intermediate cache that respects the standard cache control headers. In particular, Acquia Cloud Edge will respect the following headers:
    - Cache-Control:private
    - Expires
    - max-age & s-max-age
  - Your Customer Onboarding Engineer can provide you with guidance and best practices on your caching strategy.

Review your security settings (Edge Protect customers)

- By default, your security settings are set to Medium. You can change your security settings by clicking on the Firewall app in your Cloud Edge Dashboard. The Security Level you choose will determine which visitors will be presented with a Challenge Page.
- Depending on your needs and requirements, your Acquia Ready team can provide guidance on additional security measures that you can benefit from.