Fastly Products Archive

Generated: Fri, 28 May 2021

Products

Deliver

These articles provide information about Fastly products that accelerate content delivery with control from an edge cloud platform.

https://docs.fastly.com/products/product-deliver

Application Programming Interface (API)

https://docs.fastly.com/products/application-programming-interface

The Fastly Application Programming Interface (API) allows you to integrate your applications and services with the Fastly platform.

Our API is presented using a REST model. It uses standard HTTP response codes and verbs to allow you to programmatically control all the same features that are available through the Fastly web interface. Our web interface is a client of our public API.

Documentation

The Fastly API provides a variety of endpoints that we document in our API reference documentation. The endpoint documentation for each API call shows the method, path, authentication type, resource, and parameters that must be combined with the base URL to form a request.

Client libraries

To make coding against the Fastly API easier, we maintain a list of client libraries in a variety of languages. Our client list provides more information about each of the client libraries in our list, including third-party tools and integrations in other languages created by the Fastly community.

Base URL and endpoints

With one exception, all API calls referenced in our documentation start with a base URL:

```
https://api.fastly.com/
```

The base URL for the real-time analytics API is:

https://rt.fastly.com

Authentication

Nearly all API requests require authentication using an API token. You can limit the capabilities of those tokens using a scope. Our authentication page provides more information about the API tokens you must use to authenticate. Our guide to Using API tokens provides more information about managing these tokens via the web interface depending on the role your organization has assigned to your account.

NOTE: Fastly accounts created before May 15th, 2017 may have used one or more API keys to authenticate API requests. See our note on legacy API keys for more information.

Errors

Fastly uses standardized HTTP response codes to indicate the success or failure of an API request. Codes in the 2xx range indicate success and confirm a request worked as expected. Codes in the 4xx range indicate an error and provide both an error code and a brief explanation.

Rate limiting

Unless otherwise stated in the API reference documentation for individual endpoints, API access is limited to 1,000 non-read requests per hour, per user account. If more than one API token is associated with one user, all that user's tokens share the same limit. Information about rate limit consumption and remaining credit is available in an HTTP response header, examples of which can also be found in our API reference documentation.

TLS version requirement

The Fastly API requires TLS 1.2. Because of the PCI Security Standards Council mandate, TLS versions 1.0 and 1.1 are no longer supported for accessing Fastly's API.

Dedicated IP addresses

https://docs.fastly.com/products/dedicated-ip-addresses

Fastly's Dedicated Internet Protocol (IP) addresses provide you with a pool of IPv4 and IPv6 addresses, maintained and managed by us, across Fastly's global Edge Cloud. They can be used to support TLS certificate management for non-SNI clients, to support custom cipher suites or IP-to-service pinning, or to help manage zero-rated billing endpoints or security allowlisting.

NOTE: Purchase of Fastly's Platform TLS product requires you to also have purchased Dedicated IP addresses.

TLS non-SNI client support

Dedicated IP addresses can be used to host customer certificates for non-SNI client support. Fastly can install customer-provided or Fastly-managed certificates at a dedicated set of IP addresses identified via customer-managed DNS records. These DNS records can be set up to use three possible network routing options (sometimes referred to as network maps or domain maps) that allow you to choose which parts of the Fastly network to use. See Fastly's TLS offerings for a more detailed description of the supported TLS options at Fastly.

Custom cipher suites

Fastly supports a number of standard cipher suites. Should you require more personalized control, Fastly supports the creation of custom cipher suites by providing you with dedicated IP addresses that support these custom sets.

IP-to-service pinning

IP-to-service pinning uses dedicated IP addresses to map customer services to specific endpoint IP addresses and direct an end user's request to a specific service based on the requested endpoint IP address.

Zero-rated IP addresses

Zero-rated IP addresses (ZRIPs) allow you to use dedicated IP addresses within Fastly's global Edge Cloud to identify traffic for special treatment. For example, if you need to waive billing charges going to or from specific web pages, ZRIPs can help you to identify traffic for zero billing.

Security allowlisting

Security allowlisting uses dedicated IP addresses to control the set of Fastly global IP addresses seen by third parties. You can incorporate dedicated IPs into access control lists (ACLs) to tighten security between a customer and a third party.

Fastly's Full-Site Delivery

https://docs.fastly.com/products/fastlys-full-site-delivery

Fastly's Full-Site Delivery allows you to speed up websites and mobile applications by pushing content closer to users, providing improved and secure experiences across the world. Full-Site Delivery includes the following features.

Content serving, caching, and control

Full-Site Delivery uses Fastly's global content delivery capabilities to cache and accelerate the delivery of your HTTP-based file content such as video, images, CSS, Javascript files, as well as HTML and API responses. Specifically:

- **HTTP header controls.** Full-Site Delivery obeys standard HTTP caching headers and support forwarding, adding, removing, and modifying the HTTP headers we receive from your origin servers and send to end users, allowing you to send one set of instructions to your Fastly services and another set of instructions to downstream caches, proxies or browsers.
- **Time to Live controls.** Content expiration is controlled via Time to Live (TTL) settings you configure that work as timers on your cached content. You have the option of configuring a global default TTL to control cached content which, when set, will cache objects in a consistent manner even if you have multiple origins or server applications with inconsistent TTL settings.
- **Request collapsing.** When your content expires, the fetch and refresh process from your origin may take one second or more. During that time, your Full-Site Delivery may receive dozens or hundreds of end-user requests for that content. Fastly's request collapsing feature groups those requests and fulfills them together when it receives the refreshed content from your origin. Request collapsing decreases load on your origin servers by keeping your Fastly services from sending duplicate requests for the same expired content to them. Request collapsing is enabled by default.
- **Grace mode (Serving stale content).** If your origin servers become unavailable for any reason, grace mode can instruct your Fastly services to continue to serve stale or expired (but likely still valid) content to end users for a set amount of time. This allows you some extra time to return your unavailable servers to normal operations while still serving content instead of error messages to end users. Grace mode is not configured by default. To enable it, you must specifically configure your services to serve stale content.
- **Purging.** For dynamic or event-based content that doesn't lend itself to predetermined TTL-based content expiration, you can proactively remove or invalidate your content within milliseconds with Fastly's purging features. We limit purging to an average of 100K purges per hour per customer account, inclusive of all services within that account.

Edge logic and advanced content delivery control

Fastly's content delivery capabilities are based on a heavily extended version of the Varnish caching software. Varnish software gives you direct access to content delivery, control and edge logic capabilities, via the expressive HTTP inspection and modification scripting language, Varnish Configuration Language (VCL).

Streaming content delivery

Fastly's Streaming Delivery allows you to stream live and video-on-demand streaming content by leveraging Fastly's native support of common streaming formats. Fastly streaming format support includes HTTP Live Streaming (HLS), HTTP Dynamic Streaming (HDS), Dynamic Adaptive Streaming over HTTP (MPEG-DASH) and HTTP Smooth Streaming.

Precision Path

Precision Path traffic routing proactively identifies network congestion and poorly performing paths and automatically switches your traffic over to better performing alternatives. This improves service availability and resilience. Provisioned at strategic locations across our global fleet, this feature is available to all Fastly customers as part of our platform.

Origin shielding

You can designate a Fastly point of presence (POP) to serve as a shield for your origin servers, thus enabling increased cache hit rates for your Fastly services and potentially protecting your origin servers from unexpected spikes in requests for content. You can optimize this shielding geographically by configuring different shield POPs for different origin server locations. Origin shielding is not enabled by default. To use it, you must specifically enable it.

Load balancing

Services configured with multiple origin servers will automatically distribute requests to those servers evenly. You can modify this default load balancing behavior with a variety of conditions and load balancing rules.

Health checks

The health of your origin servers can be monitored with configurable health checks to help ensure only responsive origin servers are being sent requests.

Fastly web interface

All Fastly accounts have access to Fastly's web interface, allowing it to be managed by multiple users within your organization. You can control each user's role, as well as control the scope of their service access and their specific permission levels. Fastly services can be created, monitored, and managed through the Fastly Web Interface via any standard, modern web browser.

Application programming interface (API)

Fastly provides an application programming interface (API), accessible via HTTPS, through which Fastly services can be created and configured, and customers can access account information and analytics.

Real-time log streaming

To help you tune the performance of your Fastly services, we support real-time log streaming to a variety of locations, including third-party services, for storage and analysis. You can find our supported logging endpoints in our list of streaming log guides. We limit real-time log usage to a monthly average of two log statements per request, per service. If you require a higher volume of logs, Fastly offers High Volume Logging.

Transport Layer Security

Fastly supports a variety of Transport Layer Security (TLS) services that allow websites and applications to serve traffic over HTTP Secure (HTTPS), providing added privacy and data security for your services and end users. All Fastly services have access to our free shared domain option, plus a variety of additional paid TLS services to meet your TLS business and technical needs.

Always-on DDoS mitigation

Fastly's globally distributed network was built to absorb Distributed Denial of Service (DDoS) attacks. As part of Fastly's standard, Full Site Delivery, all customers receive access to a combination of features inherent in Fastly Edge Cloud network capabilities that help protect the availability of your content from DDoS threats.

Pricing and billing

Full-Site Delivery prices are based on the volume of content delivered to your end users and the location of the POPs from which that content was served. Fastly billing is done in arrears based on actual usage with month-to-date usage being available via both our web interface and APIs.

> **NOTE:** Fastly maintains partnerships with Google and Microsoft that may provide discounts on outbound data transfer traffic to customers who qualify and configure their Fastly services correctly. See our integrations guides for additional details.

Fastly's Streaming Delivery

https://docs.fastly.com/products/fastlys-streaming-delivery

Fastly's Streaming Delivery allows you to scale your streaming content delivery when you will not be using your Fastly services for any of the other HTTP content formats supported by Fastly's Full Site Delivery.

> **NOTE:** Fastly's Streaming Delivery is a subset of Fastly's Full-Site Delivery and it must be configured in an account separate from other Fastly accounts to allow for separate billing and invoices.

If you have your own video packaging infrastructure, Fastly can act as a globally distributed HTTP streaming network to improve quality of service and increase viewer capacity for both your live and Video On Demand (VOD) content. When a manifest or video segment is requested by an end user's player, your Fastly Streaming Delivery will pull the requested content from your origin media servers and subsequent requests for that stream will be served from Fastly's POPs instead of your origin servers.

Fastly's Streaming Delivery supports the following HTTP-based media streaming protocols:

- HTTP Live Streaming (HLS)
- HTTP Dynamic Streaming (HDS)
- HTTP Smooth Streaming (HSS)
- Dynamic Adaptive Streaming over HTTP (MPEG-DASH)

You can also use Fastly's Full Site Delivery to configure and control live streaming and VOD caching.

> **NOTE:** Fastly maintains partnerships with Google and Microsoft that may provide discounts on outbound data transfer traffic to customers who qualify and configure their Fastly services correctly. See our integrations guides for additional details.

Origin Connect

https://docs.fastly.com/products/origin-connect

Origin Connect provides you with a direct fiber connection between your origin servers and a Fastly shield POP thus reducing the number of organizations (and by association, the number of servers) handling your data.

Prerequisites

To be considered for Origin Connect, you need to:

- have at least one Fastly shield POP configured
- have servers in the same data center as the selected Fastly shield POP (e.g., BWI, DCA, AMS, SJC)
- be interviewed by Fastly so we can identify your customer-specific business needs
- have Enterprise-level support
- have a publicly routed Autonomous System Number (ASN)

If you are approved for Origin Connect, we'll issue you with a Letter of Authorization and Connecting Facility Assignment (LOA-CFA) that the data center provider will need when you order your cross-network connection (or cross connect). You will need to pay for the cross connect with your facility provider.

For each cross connect, you, as subscriber, will need to provide Fastly with:

- a minimum of a globally unique (non RFC-1918) /31 IPv4 network prefix
- a minimum of a /127 IPv6 network prefix
- a 10G port (we recommend two and will accept up to 4x 10G ports for redundancy)

Both you, as the subscriber, and Fastly will each need to:

- provide the ASN intended for Border Gateway Protocol (BGP) peering use
- provision BGP peering on each interconnect
- provide a BGP prefix filter list
- comply with any other reasonable request to technically provision the Origin Connect product

If the cross connect is not completed within 90 days, the authority granted by the LOA-CFA expires.

In the event of Origin Connect service degradation, congestion, or a failure of one of these interconnects, public internet transit will be used for origin connectivity, and the subscriber will prefer the carrier of Fastly's reasonable request. There is no Service Level Agreement (SLA) available for Origin Connect.

If your origin server is located within a cloud storage provider or your traffic doesn't meet our minimum threshold for Origin Connect, contact us at sales@fastly.com to discuss other options.

Platform TLS

https://docs.fastly.com/products/platform-tls

Fastly's Platform TLS product allows you to programmatically manage certificates and keys for Transport Layer Security (TLS) using a web API.

Consider this product if:

- you need to support thousands of individual X.509 certificates and their associated private keys.
- you own and generate your own certificates and private keys (typically obtained from a third-party certification authority such as Let's Encrypt).

For more information about this product, contact sales@fastly.com.

IMPORTANT: This information is part of a limited availability release. For more information, see our product and feature lifecycle descriptions.

How Platform TLS works

Platform TLS allows you to programmatically manage certificates and private keys on a special Fastly service provisioned for use with the Platform TLS API. Using the API, you can:

- deploy new X.509 certificates
- retrieve information about deployed certificates
- update and delete existing certificates
- deploy new private keys
- retrieve information about private keys
- delete private keys

You can support your entire certificate lifecycle by replacing expiring certificates with newly generated ones at any time and using the API to rotate your private keys to manage your key management requirements.

Initial setup and configuration

The Platform TLS product will be provisioned by Fastly staff on a dedicated IP address pool (which you purchase separately) in Fastly's infrastructure. We configure your service to skip domain lookups and instead route client requests directly to your service based on the destination IP address that a client is connecting to. Because multiple certificates are served off the same IP address pool, Server Name Indication (SNI) is required for this product to work properly. We then provide you with a custom DNS map to use in your CNAME records and the corresponding Anycast IP addresses (for use with any apex domains you serve through Fastly).

Once setup is complete, certificates you upload using the API will automatically be made available to your dedicated IP address pool. Browser clients initiating a TLS handshake will automatically receive the proper certificate based on the domain indicated in the TLS handshake.

Certificate and key uploads and renewals

Once setup and configuration are complete, you can upload TLS private keys and matching TLS certificates using the Platform TLS API. The Platform TLS product automatically matches certificates to previously uploaded keys. TLS certificates may be procured from the certification authority (CA) of your choice.

When renewing and replacing certificates nearing expiration, you must procure new ones from your CA and then use the Platform TLS API to upload their replacements. You may also rotate your private keys. Any time you decide to swap out your key with a new one, that new key would need to be uploaded first, and then all the certificates associated with the old key would need to be regenerated and uploaded.

Domain configuration

To begin serving traffic through Fastly with the Platform TLS product, you or your customers must modify DNS records for any web properties to point traffic to the IP address pool assigned for your service. Fastly will assign a DNS name for use with your DNS records that can support a CNAME record and the Anycast IPs that can be used with apex domains.

- **Using a CNAME record.** With this option, a CNAME record gets created with a DNS provider and points to a custom DNS map Fastly provides. This option should be used for subdomains or wildcard domains (e.g., `www.example.com` or `*.example.com`).
- **Using an A record.** With this option, an A record gets created with a DNS provider and points to an Anycast address that Fastly provides. This option should be used for apex domains (e.g., `example.com`). Map names and Anycast addresses will be provided during initial setup and configuration. To obtain this information again, contact support@fastly.com.

IMPORTANT: For each of your domains, a CNAME or an A record must have been created with a DNS provider *and* you must have activated a Fastly service for traffic to be properly directed through it.

How TLS is enforced when you have multiple certificates

Fastly will automatically choose the certificate to be delivered for a given request based on the Host requested. The certificate with the most specific matching hostname will be preferred over certificates with less specific hostnames. Fastly's TLS server will always prefer an exact match SAN entry to a wildcard match. For example, on a request for `api.example.com`, Fastly will serve a certificate with a SAN entry for `api.example.com` over a different certificate with a SAN entry for `*.example.com`.

Conditions and limitations

When using Platform TLS, you agree to the following conditions:

- You are responsible for procuring your own certificates from the CA of your choice. Fastly will not procure certificates on your behalf.

- You are responsible for updating certificates prior to expiration. Expired certificates will cause TLS handshake failures that most browsers will display as site errors.

When using Platform TLS, you agree to the following limitations:

- This product requires Server-Name Indication (SNI). Browsers that do not support SNI will not receive the correct certificate for the domain requested.
- This product requires a dedicated IP address pool on Fastly's infrastructure. If you've previously purchased a dedicated IP address pool from Fastly, Platform TLS may be enabled on it.
- The certificate deployment process is not instantaneous. It takes approximately 20 minutes on average to complete once a certificate is submitted, though the deployment may take as long as one hour.
- If two certificates are uploaded with identical hostnames, the most recently uploaded certificate will be chosen.
- By default certificates uploaded via the Platform API should not exceed one domain per certificate.

As with all API-based activities, standard API rate limits apply.

Subscriber Provided Prefix

https://docs.fastly.com/products/subscriber-provided-prefix

Fastly's Subscriber Provided Prefix product allows you to have your IP spaces announced, routed, and served by Fastly infrastructure for use with production services. When you purchase this product, you provide your own IP address space to Fastly rather than use Fastly IP addresses. You can then direct traffic to your own IP addresses, which are reachable via HTTP Anycast on Fastly's infrastructure.

We recommend this service for customers who want to control their address space by separating their network layer concerns from their content delivery concerns. By combining Fastly's Subscriber Provided Prefix service with our Origin Connect product and our DDoS Protection and Mitigation service, you can protect your origin servers by directing traffic through Fastly's global network.

For more information about this product, contact sales@fastly.com.

Prerequisites

To purchase Fastly's Subscriber Provided Prefix service you must also purchase Fastly's Enterprise Support package and our IP-to-Service Pinning Setup service.

When you sign up for this product, you'll need to provide Fastly with an executed Letter of Authorization (LOA), on a form we provide, that grants us permission to announce your prefixes. The LOA includes, at a minimum, the IP blocks to announce, the registry and object identifier, as well as the administrative, technical, and abuse contacts for those prefixes.

Using the Subscriber Provided Prefix product requires at least one /24 IPv4 or /48 IPv6 prefix for announcement purposes. Additional prefixes and larger prefixes may also be supported. These prefixes must not be originated from any autonomous system number (ASN) at the time Fastly announces them. They should also be dormant for a period of approximately three months prior to use by Fastly.

How the Subscriber Provided Prefix product works

Fastly will announce the designated prefixes identified in your LOA. Your prefixes will be announced along with existing Fastly prefixes and will be originated from the Fastly Autonomous System (AS) Number AS54113. The Subscriber Provided Prefix product supports HTTP and HTTPS traffic only and your prefixes will be terminated at Fastly for these two protocols. We make routing announcements on a global basis unless you request they be constrained to our defined North America and Europe region.

To enable specific IP addresses within your announced prefix, Fastly combines this Subscriber Provided Prefix product with our IP-to-Service Pinning feature, which must be purchased separately. IP addresses that are not service pinned will not serve your traffic.

After completing all the necessary routing announcements and setup within your CDN services, Fastly needs additional time to complete the setup. In general, you should allow for at least one month's lead time for us to set up routing announcements and CDN service. Your service order identifies the specific lead time Fastly needs for full operability.

You may provide Fastly notice at any time to withdraw your prefix announcement by opening a ticket at support@fastly.com. We need at least one month's notice to permanently remove routing announcements and CDN service for your designated prefixes. When we receive notice of your request for prefix withdrawal, we will provide you with a withdrawal process timeline. This process starts with us reconfiguring your service within the Fastly network. When that reconfiguration work completes, you must then point your DNS records at Fastly to ensure uninterrupted service. Once your traffic is moved from your prefix to a Fastly prefix, we will withdraw the announcement.

Conditions and limitations

When using Fastly's Subscriber Provided Prefix product you agree to the following limitations:

- Your purchase of the Subscriber Provided Prefix product entitles you to the announcement of the specified IP prefixes identified in your LOA. Any additional prefixes beyond your initial order will require an additional purchase of this product.
- Fastly does not provide termination or proxy services for non-HTTP and non-HTTPS protocols with this product.
- Fastly does not provide general network transit or peering services as part of this product.

When using Fastly's Subscriber Provided Prefix product you agree to the following conditions:

- Your IP addresses are your assets. They belong to you and are not a Fastly service. Fastly has no liability for your assets.
- You will pay additional fees if you withdraw your prefixes for the purpose of replacing or updating them.
- Your provided prefixes will not have any negative IP reputation associated with them as determined by us. Fastly will scan your prefixes against common IP reputation databases prior to announcement to ensure your IP reputation remains neutral or positive.
- You must maintain transit connectivity to Fastly for origin traffic. Prefixes provided to Fastly for this service must not overlap with IP addressing used by your origin servers.
- Fastly retains exclusive announcement rights for your prefixes. Conflicting announcements will disrupt or prevent traffic delivery.

To specifically mitigate DDoS attacks, you agree that:

- Prefix announcements Fastly makes for you may include regional capacity announcements.
- Fastly may prepend, remove, or blackhole routing announcements in the event of a DDoS attack.
- Fastly may de-aggregate your prefixes at our discretion to improve network reliability.
- Fastly may perform these actions even if you have not purchased the Fastly DDoS protection and mitigation service.

NOTE: For any IP addresses not pinned to a service but contained within your Subscriber Provided Prefix product, Fastly's Varnish servers will return a TCP reset or an HTTP 500 error response code.

TLS オプション

https://docs.fastly.com/products/tls-service-options-ja

Fastly は、Web サイトやアプリケーションがサービスのプラバシーとデーターセキュリティに必要となる HTTPS でトラフィックを配信できるようにする様々な TLS (Transport Layer Security) サービスを提供しています。Fastly から安全な HTTPS トラフィックを配信するには、Web サイトに一致する秘密鍵を持つ有効な TLS 証明書が必要です。これらの証明書は、お客様が生成してアップロードすることも、Fastly 側で代わりに作成することも可能です。

ヒント: Fastly の pricing ページ は、当社の TLS サービスの現在の料金の詳細を記載しています。

重要な検討事項

Let's Encrypt やその他の認証局が提供する証明書は、サードパーティーの技術です。利用者は、自分が正当な登録者であることに責任を持ち、代わりに手配された証明書に記載されているドメインを管理していることを証明する必要があります。

GlobalSign が提供する証明書は、https://www.globalsign.com/repository に記載された GlobalSign の利用規約に従うものとします。

Fastly の PCI 準拠キャッシング または HIPAA 準拠キャッシング を購入している場合、Fastly は PCI Security Standards Council が定めるコンプライアンス要件を満たすために、すべての接続に TLS 1.2 以上を適用します。

デフォルトでは、Server Name Indication (SNI) 拡張機能を使用します。最新のブラウザはすべて SNI をサポートしています。SNI をサポートしていないクライアント（Windows XP や Android 2.x 以前のクライアントなど）は、TLS ハンドシェイクのエラーが発生します。

Fastly は、RSA 公開鍵暗号化のために最小鍵長 2048 ビットの信頼された認証局によって署名された SHA-256 証明書をサポートしています。パフォーマンス上の理由から、それ以上の鍵長が必要ない場合には、2048 ビットの鍵長を使用することを強くお勧めします。

Fastly TLS

Fastly TLS では、有料アカウントのお客様は、Web コントロールパネルまたは API を使用してドメインごとに TLS 証明書を管理することができます（開発者向けトライアルアカウントでは、Fastly TLS を使用することはできません）。Fastly TLS では、お客様が TLS 証明書と秘密鍵を生成してアップロードする方法と、Fastly がサードパーティの認証局を介して TLS 証明書を代わりに生成して管理する方法があります。

設定・動作

お客様所有の証明書を利用する場合、Fastly の Web コントロールパネルまたは API を使用して TLS ファイルをアップロードすることができます。証明書をアップロードする前に、対応する秘密鍵を事前にアップロードしておく必要があります。

Fastly が管理する証明書を利用する場合、証明書の発行要求を完了させるには DNS レコードを変更することで、ドメインを管理できることを証明する必要があります。Fastlyはドメインごとに1つの証明書を生成します。

デフォルトでは、Fastly は TLS 証明書を共有 IP アドレスにインストールします。クライアントのリクエストが Fastly に送信されると、TLS の SNI 拡張機能を使用して正しい証明書を選択し、クライアントが TLS ハンドシェイクリクエストでホスト名を提示できるようにします。

重要: Fastly TLS の証明書は50までに制限されています。この制限を上げる方法については、sales@fastly.com までお問い合わせください。

課金方法

Fastly TLS は、月末に TLS が有効になっている FQDN (fully qualified domain names) (例: `example.com` や `www.example.com`) とワイルドカードドメイン(例: `*.example.com`)の数に基づいて課金されます。

コンシェルジュTLS

コンシェルジュ TLS は、エンタープライズサポート オプションのパッケージとして販売され、TLS に特化した高度な設定サポートを提供します。コンシェルジュ TLS は、Fastly TLS のドメイン追加の制限を50から100に増やし、、エンタープライズ向けの高度な TLS サポートと設定オプションを提供します。お客様がお持ちの証明書をご利用になる場合には、Domain Validated (DV)、Organization Validated (OV)、およびExtended Validation (EV) 証明書のサポートが可能となります。

エンタープライズサポートにコンシェルジュ TLS を加える場合には、sales@fastly.com までお問い合わせください。

その他のTLSオプション

Fastly TLS の他にも、共有証明書オプションや商用認証局から調達した証明書を使用するマネージドオプションなど、いくつかの TLS オプションをご用意しています。

重要: TLS1.2 向けの共有証明書の提供を2020年12月31で終了する予定です。新しい Fastly TLS のウェブインターフェイスおよび API は、共有証明書と同様の機能を提供します。当変更に関するお問い合わせは弊社のカスタマーサポートチーム fastlytlsupdates@fastly.com へご連絡ください。

Fastlyの共有ドメインを利用した無料 TLS

Fastly は無料の TLS オプションを提供しており、`example.global.ssl.fastly.net` のような Fastly の共有ドメインで HTTPS トラフィックを配信することができます。

このオプションを使用するには、ガイドの無料 TLS の設定の手順に従い、設定をはじめる前にの項目を確認してください。特定のトラフィックルーティング、ドメイン名や URL の要件がある場合は、Fastly の有料 TLS オプションを利用すると、より柔軟に対応できます。

Dedicated IPアドレス

Fastly は、お客様固有の DNS レコードで指定された Dedicated IP アドレス にお客様証明書をインストールすることができます。これらのDNSレコードは、3つのネットワークルーティングオプション（ネットワークマップまたはドメインマップと呼ばれることもあります）を使用するように設定することができ、Fastly ネットワークのどの部分を使用するかを選択することができます。

お客様がこのオプションの使用基準を満たしているかどうかを確認するには、sales@fastly.com までお問い合わせください。

TLS service options

https://docs.fastly.com/products/tls-service-options

Fastly provides a variety of Transport Layer Security (TLS) services that allow websites and applications to serve traffic over HTTPS, offering privacy and data security for services. To serve secure HTTPS traffic from Fastly, your website needs a valid TLS certificate with a matching private key. You can generate and upload these yourself or have Fastly do this automatically on your behalf.

> ★ **TIP:** Fastly's pricing page details the current rates for our TLS services.

Important considerations

Certificates provided by any certification authority (CA), whether they are non-profit or commercial providers, are third-party technologies. You are responsible for ensuring that you are the legitimate registrant and can demonstrate control of any domain that appears on a certificate procured on your behalf. Certificates provided by GlobalSign are subject to the terms of GlobalSign's Subscriber Agreement, which can be found at https://www.globalsign.com/repository.

For customers bringing their own certificates, both Fastly TLS and Concierge TLS service support Domain Validated (DV), Organization Validated (OV), and Extended Validation (EV) certificates. If Fastly manages your certificates, however, only DV and OV certificates can be used.

If you've purchased Fastly's PCI-compliant caching or HIPAA-compliant caching products, Fastly will enforce a minimum version of TLS 1.2 or higher for all connections to meet the compliance requirements mandated by the PCI Security Standards Council.

By default Fastly uses the Server Name Indication (SNI) extension. All modern browsers support SNI. Clients that do not support SNI (such as those on Windows XP and Android 2.x or earlier) will see a TLS handshake error.

Fastly supports SHA-256 certificates signed by publicly trusted certification authorities that have a minimum key size of 2048 bits for RSA public key encryption. For performance reasons, we strongly recommend using a 2048-bit key size for RSA when larger key sizes are not required for your application.

Fastly TLS

Fastly TLS allows paid account customers to manage TLS certificates on a domain-by-domain or multi-domain basis using our web interface or API (you can't use Fastly TLS with a developer trial). With Fastly TLS, you can either generate and upload your own TLS certificates and private keys or instruct Fastly to automatically generate and manage TLS certificates via a third-party, non-profit or commercial CA on your behalf.

How it works

If you bring your own certificates, you can use the Fastly web interface or API to upload TLS certificates and keys. You must ensure you upload the relevant private key first before uploading the matching certificate.

When Fastly manages your certificates, you use the Fastly web interface or API to select the CA from which Fastly should procure your TLS certificates. Fastly then procures DV certificates from the authority you've chosen. To complete a certificate request, you must prove that you control your domains by modifying DNS records.

> ★ **TIP:** To have Fastly procure organization validated certificates (OV) instead, contact sales@fastly.com.

By default, Fastly installs TLS certificates at a shared set of IP addresses. When client requests get sent to Fastly, we select the correct certificates using the SNI extension of TLS that allows clients to present a hostname in the TLS handshake request.

> ❗ **IMPORTANT:** Fastly TLS comes with a 50 certificate limit. To discuss how to raise this product's certificate limit, contact sales@fastly.com.

How we bill for it

Fastly TLS is billed based on the number of fully qualified domain names (e.g., `example.com` or `www.example.com`) and wildcard domains (e.g., `*.example.com`) that are TLS enabled at the end of the month for your account. All domains in an enabled state will be billed at the end of the month, regardless of certificate status (e.g., valid or expired).

Fastly TLS treats all entries on a certificate equally and each entry as its own item. On both certificates you manage and those that Fastly manages for you, an entry can be an apex domain, a subdomain, or a wildcard domain. Charges are based on the combined total of the domains on the certificates you manage as well as certificates that Fastly manages for you.

For Fastly-managed subscriptions, your charges may vary based on the CA you select. Specifically, there are pricing differences between Fastly TLS certificates provided by a commercial CA and those provided by a non-profit CA. Our pricing page provides specifics about these differences.

Concierge TLS

Concierge TLS provides TLS-specific advanced configuration support sold as a packaged addition to Fastly's Enterprise Support service option. Concierge TLS increases the Fastly TLS limit on domain additions from 50 to 100 and provides advanced TLS support and configuration options for Enterprises.

To add Concierge TLS to your Enterprise Support option, contact sales@fastly.com.

Other TLS options

In addition to Fastly TLS, we make several other TLS options available including shared certificate options and a managed option that uses a procured certificate from a commercial certification authority.

IMPORTANT: As part of our previously announced planned retirement of shared certificates and our previously announced planned retirement of our Certificate Procurement, Management, and Hosting Service, Fastly has begun working with customers to migrate certificates to Fastly TLS. Fastly TLS offers an associated web interface and API with similar functionality to the retired products. We will continue to support shared and procured certificates for existing customers during this migration. Our support team will contact you to schedule individual migrations and can be emailed at fastlytlsupdates@fastly.com for general questions.

Free TLS via the shared Fastly domain

Fastly offers a free TLS option that allows you to serve HTTPS traffic using an address like `example.global.ssl.fastly.net` via a shared Fastly domain.

To use this option, follow the instructions in our guide to setting up free TLS and pay close attention to the noted limitations. If you have specific traffic routing, domain naming, or URL requirements, one of Fastly's paid TLS options will provide you with more flexibility.

Dedicated IP addresses

Fastly can install customer-provided or Fastly-managed certificates at a dedicated set of IP addresses specified via customer-specific DNS records. These DNS records can be set up to use three possible network routing options (sometimes referred to as network maps or domain maps) that allow you to choose which parts of the Fastly network to use.

To see if your company meets the qualification criteria for this option, contact sales@fastly.com.

Varnish Configuration Language (VCL)

https://docs.fastly.com/products/varnish-configuration-language

Fastly Varnish Configuration Language (VCL) is a domain-specific language derived from the Varnish proxy cache, which is part of Fastly's platform architecture.

When you create and enable a VCL service via the web interface or the API, Fastly generates VCL code automatically for the functionality you've specified. You can refine and augment that functionality as needed to create customized configurations by defining your own VCL logic and combining it with the automatically generated VCL. Those configurations are then distributed to all Fastly caches worldwide, loaded, and activated without requiring maintenance windows or service downtimes.

Documentation

Fastly VCL provides a variety of language components, which we document in our VCL reference documentation. The documentation describes each component, including its syntax and structure where necessary. Where applicable, examples of each component's use are included.

Custom VCL

You can create a custom VCL configuration to augment or override the default VCL configuration for your service. To make using custom VCL easier, we maintain a VCL boilerplate that you can use as a starting point when including your own VCL logic. You can use the web interface to upload custom VCL files for your service as well as preview it prior to activation.

VCL Snippets

VCL Snippets are short blocks of VCL logic that can be included directly in your service configurations. They're specifically designed to allow you to add small sections of code when you don't need more complex, specialized configurations.

Perform

These articles provide information about Fastly products that focus on performance (speed), availability, and media.

https://docs.fastly.com/products/product-perform

Cloud Optimizer

https://docs.fastly.com/products/cloud-optimizer

IMPORTANT: This information is part of a limited availability release. For more information, see our product and feature lifecycle descriptions.

Fastly's Cloud Optimizer product allows customers using one or more non-Fastly content delivery networks (CDNs) to take advantage of Fastly's Full-Site Delivery features without migrating edge delivery traffic to Fastly. Cloud Optimizer works with your existing content delivery infrastructure by designating Fastly as the origin for all of your end-user-serving CDNs. Using Cloud Optimizer provides you with real-time visibility of origin traffic, granular load balancing for your origin infrastructure, and request collapsing to decrease traffic to origin.

To learn more about Fastly's Cloud Optimizer, contact your account manager or email sales@fastly.com for more details.

NOTE: Cloud Optimizer is not available for video streaming activities. Check out Media Shield for Live and Media Shield for VOD instead.

Fastly's On-the-Fly Packaging service

https://docs.fastly.com/products/fastlys-onthefly-packaging-service

Fastly offers an "on-the-fly," dynamic, video-on-demand content packaging service. Rather than requiring you to pre-package all protocols of a viewer-requested video, Fastly allows you to dynamically package video content in different HTTP streaming formats in real time, using source files. That video content then becomes immediately available to viewers.

IMPORTANT: Fastly's On-the-Fly Packager (OTFP) for On Demand Streaming service is an add-on service. Our Professional Services team will assist with configuration and testing. To enable OTFP and begin this process, contact your account manager or email sales@fastly.com for more details.

Supported on-the-fly packaging features

Fastly's OTFP service supports the following specific features:

Supported HTTP streaming formats and codecs

- **HDS, HLS, and MPEG-DASH packaging.** Fastly provides support for version 1 of the Adobe HTTP Dynamic Streaming (HDS) specification and support for the ISO/IEC 23009-1:2014 specification defining Dynamic Adaptive Streaming over HTTP (MPEG-DASH). We support all features included in up to version 3 (draft 6) of the HTTP Live Streaming (HLS) specification and popular features from later versions such as subtitle, trick play and media segmentation in fragmented MPEG-4 (fMP4) format (per ISO/IEC 14996-12:2015 specification).
- **Standard codecs.** Fastly supports Advanced Video Coding (H.264/AVC/MPEG-4 Part 10) and High Efficiency Video Coding (H.265/HEVC) video codecs. Fastly also supports Advanced Audio Coding (AAC, AAC-LC, HE-AAC), Dolby Digital (AC-3) and MPEG-1 Audio Layer III (MP3) audio codecs.
- **Source video container format.** Fastly supports the Progressive MP4 specification (specifically the .mp4, unencrypted .mov, and audio-only .m4a extensions) as source container format for packaging into all supported HTTP streaming formats.

Accessibility and user experience

- **HLS multi-language subtitles and closed captions.** Fastly provides support for both in-band (EIA-608 and CEA-708) and out-of-band (Web Video Text Tracks or WebVTT) subtitle and closed caption delivery.
- **HLS trick play.** Fastly supports trick play (also called trick mode), a feature that displays video scenes during fast-forwarding and rewinding. The HLS Authoring Specification requires this feature for distributing video on the Apple TV.

Content protection

- **Media encryption.** Fastly can encrypt videos packaged into HLS (supports both Envelope/AES-128 and SAMPLE-AES methods) and MPEG-DASH (ISO/IEC 23001-7, a common encryption in ISO base media file format file) streaming formats by generating a unique content encryption key for each video, enabling secure video delivery to viewers.
- **Multi-DRM.** Fastly can support multiple Digital Rights Management (DRM) technologies including Apple FairPlay for HLS and Microsoft PlayReady, Google Widevine and Marlin DRM for MPEG-DASH streaming formats. OTFP is integrated with Multi-DRM service providers that are responsible for content rights management and DRM license delivery.

Dynamic Ad Insertion (DAI) readiness

- **HLS timed metadata injection.** Fastly supports HLS time-based metadata, which allows you embed custom metadata or ad markers about a stream into video segments at specified time instances in ID3v2 format.
- **Content preconditioning.** Fastly can segment video at the intended break points, such as for ad markers via HLS and MPEG-DASH protocols. Fastly can also add any third-party service-specific cues or metadata into video manifests at those break points to implement server or client-side ad stitching.

Live-to-VOD transition

- **Clip creation (also known as "timeline trimming").** Fastly supports clip creation features for all supported packaging formats, allowing you to deliver sections of video without segmenting a longer, archived video.

Fastly also provides the following features as part of standard content delivery network services:

- Token-based validation for decreasing response time by placing validation at the edge
- Geolocation and device detection for content targeting
- Edge dictionaries for real-time business rules and decision making at the edge
- Remote log streaming for data aggregation and viewer diagnostics
- Transport Layer Security (TLS) for secure communications delivery

How the on-the-fly packaging service works

Fastly's OTFP service gets configured between our caching network and your origin storage (e.g., Amazon S3, Google Cloud Storage, or Rackspace Cloud Files).

When users request manifests or video segments, those requests initially come to Fastly caches instead of going to your origin storage. Fastly's edge caches deliver those objects if they are available and valid. If the objects don't already exist in the edge caches, the requests will be passed on to a designated shield cache to be delivered instead as long as the objects are available and valid. If neither the edge caches nor the shield cache can deliver the objects, the requests for those objects will go directly to and be fulfilled by the OTFP service which acts as an origin for Fastly's cache nodes.

The OTFP service will make the necessary request to your origin storage to fulfill the original request from the user. The OTFP service also maintains a small, local, in-memory cache for video metadata indexes. These indexes are created using mp4 moov atom (or movie atom) that provide information about the video file such as its timescale, duration, audio and video codec information, and video resolution (among other characteristics).

For adaptive bitrate playback, the OTFP service will cache indexes of each quality level requested. If a user requests a manifest, OTFP will look for the corresponding indexes and, if it is available and valid, OTFP will generate the manifest and deliver it to the user. Otherwise, OTFP will fetch the moov atom from origin storage to generate the corresponding index. If a user requests video segments, OTFP will look for the corresponding audio and video sample entries in the cached index, download those samples from origin storage, and package them in the format requested.

Image Optimizer

https://docs.fastly.com/products/image-optimizer

The Fastly Image Optimizer (Fastly IO) is a real-time image transformation and optimization service that caches and serves pixel-optimized, bandwidth-efficient images requested from your origin server. Fastly IO specifically supports a variety of input and output image formats.

Image transformation and optimization

When an image is requested from your origin server, Fastly IO can perform transformation tasks before serving and caching the optimized version. Image transformations can be applied programmatically and through dynamic URLs in real-time. You can make images responsive so they automatically adjust to fit the size of the screen viewing the content. As a result, image pre-processing can be offloaded to the edge. Multiple copies of the images, each appropriately sized for different devices, are served from cache instead, which allows you to reduce the number of requests to your origin.

Debugging and troubleshooting

To aid in debugging when serving images, special HTTP headers will be present in a response when an image is requested. The specific header included depends on the response's result. For successful transformations and optimizations, the HTTP header returned provides general information that allows you to compare image dimensions, file sizes, and formats. Additional HTTP headers are included for source image issues that aren't fatal enough to cause an error but could still be problematic, as well as transformations and optimizations that fail outright.

Billing

Billing for Fastly IO is based on the number of monthly image requests that are processed and delivered. When using the animated GIF to video functionality, each image frame delivered as video is counted as an optimized image request.

This article describes a product that may use third-party cloud infrastructure to process or store content or requests for content. For more information, see our cloud infrastructure security and compliance program.

Media Shield for Live

https://docs.fastly.com/products/media-shield-for-live

Fastly Media Shield for Live offers customers the ability to decrease origin traffic by reducing multiple CDN requests of live video events or live linear channels into a single request back to your origin. Media Shield for Live works with your existing architecture by making Fastly the origin to all of your end-user-serving CDNs. This also allows you to take advantage of Fastly's observability features like real-time analytics, historical stats, and real-time logging in a multi-CDN environment.

To learn more about Fastly's Media Shield for Live, contact your account manager or email sales@fastly.com for details.

Media Shield for VOD

https://docs.fastly.com/products/media-shield-for-vod

Fastly Media Shield for VOD offers video-on-demand customers the ability to decrease origin traffic by reducing multiple CDN requests into a single request back to your origin. Media Shield for VOD works with your existing architecture by making Fastly the origin to all of your end-user-serving CDNs. Fastly Media Shield for VOD is compatible with Fastly's On-the-Fly-Packaging (OTFP) service.

Media Shield for VOD allows you to take advantage of Fastly's observability features like real-time analytics, historical stats, and real-time logging in a multi-CDN environment.

To learn more about Fastly's Media Shield for VOD, contact your account manager or email sales@fastly.com for details.

Nearline Cache

https://docs.fastly.com/products/nearline-cache

IMPORTANT: This information is part of a limited availability release. For more information, see our product and feature lifecycle descriptions.

Fastly's Nearline Cache allows you to manually or automatically populate and store content in third-party cloud storage near a Fastly POP. In the event of a cache miss, content that has previously been written to Nearline Cache is fetched from the storage instead of your origin. Content not present in Nearline Cache will be fetched from your origin and, if configured for automatic migration, will be written to Nearline Cache asynchronously.

There is no charge for data transfer costs between the third-party cloud storage and Fastly. Availability and performance of Fastly's Nearline Cache depends upon the third-party cloud storage provider's services. You are responsible for purging or otherwise rendering inaccessible any stored content that you do not intend to serve to end users. Content in the third-party cloud storage will be programmatically deleted by Fastly after a specified period.

Billing

When purchasing Nearline Cache, you must also purchase Gold or Enterprise Support.

You will be charged for content in Nearline Cache based on the average amount of data in gigabytes (GB) in Nearline Cache during the billing period and for write operations as specified on your service order.

Secure

These articles provide information about Fastly products that deliver web application and API protection.

https://docs.fastly.com/products/product-secure

DDoS Protection and Mitigation Service and SLA

https://docs.fastly.com/products/ddos-protection-and-mitigation-service-and-sla

Fastly offers DDoS Protection and Mitigation Service to customers with a sustained DDoS threat risk or with short term and seasonal events to protect. While the DDoS Protection and Mitigation Service cannot prevent or eliminate attacks or guarantee the uptime of your origin servers, it offers the following resources to assist you with mitigating the service and financial impacts of DDoS and related attacks.

Fastly's DDoS Protection and Mitigation Service includes:

- Immediate onboarding - We will work directly with you to immediately transition you to Fastly's CDN service if you're not already a customer.
- Emergency configuration and deployment support - We will actively work with you to configure your service map and provide an initial filter policy to immediately block an attack.
- Ongoing attack mitigation support - We will work directly with you to write custom VCL filters to deal with changing attacks or new attacks. We'll also isolate malicious traffic on your behalf.
- Incident response plan - We will create a plan that identifies how communication and escalation will occur between you and your staff and Fastly if an attack occurs. The plan will also describe mitigation and defense details such as any DDoS filters that we can insert into VCL prior to or during an attack.

Using our knowledge of attacks against our network and our customers, we analyze all DDoS Attack vectors using VCL statements, network filters, bulk traffic filtering through regional sinks, or a combination of these techniques.

The following table summarizes what is provided under our DDoS Protection and Mitigation Service:

Support offering	Details
Online self-service help	Unlimited access.
Availability for general inquiries	24/7.

Support offering	Details
Availability for incident reports	24/7.
Initial response times	Attack notification response within 15 minutes. Service onboarding beginning within 60 minutes of threat notification.
Overage Insurance	Included.
Access to Fastly IP Space	Included.
Email support	Available.
Phone and chat support	Toll-free telephone available 24/7/365. Dedicated chat channel available during Fastly Business Hours.
Emergency escalation	Available via email and phone support.

Technical support

The following section applies to all Subscribers of the DDoS Protection and Mitigation Service.

Definitions

- **"Business Hours"** are 8AM-6PM during a Business Day in California, New York, London, or Tokyo.
- **"Business Days"** are Monday through Friday, excluding any day that is simultaneously a US, UK, and Japanese national or banking holiday.
- A "DDoS Attack" is a Denial of Service (DoS) event (including Distributed Denial of Service (DDoS) or Distributed Reflection Amplification Denial of Service (DRDoS) attacks) that includes both an increase of unwanted traffic beyond two (2) times the average traffic of any Fastly Service for the preceding two (2) month period and a simultaneous increase in error responses from origin sites configured for any Fastly service. Fastly captures and analyzes suspected or actual DDoS Attack traffic to improve and protect its services.
- A "Fastly IP Space" is a published API endpoint that allows Subscribers to download an updated list of all Fastly IPs globally and can be used to filter traffic and control communication between Fastly's caches and a Subscriber's origin. Fastly provides the Fastly IP Space to Subscribers in order to ensure known communication between the Fastly cache nodes and a Subscriber's origin data center.
- **"Fastly Control"** means elements entirely under Fastly's control and not a consequence of (a) a Subscriber's hardware or software failures, (b) a Subscriber's or end user's connectivity issues, (c) Subscriber operator errors, (d) Subscriber traffic amounts that exceed a Subscriber's Permitted Utilization as defined in the Terms and Conditions, (e) corrupted Subscriber content, (f) acts of god (any) or war, or earthquakes, or terrorist actions.

Subscriber responsibilities

As a Subscriber, you:

- must identify and maintain two points of contact to be used during an attack to communicate status, issues, and coordinate with Fastly to successfully protect services.
- must use common best practices for DDoS Attack defense including:
  - using updated white and black lists in the Fastly IP Space at the origin data center to protect against attack traffic bypassing Fastly's infrastructure.
  - limiting or eliminating your origin IP addresses from Domain Name System (DNS) records to avoid these addresses being used as attack targets.
- are responsible for using and configuring services according to the documentation available at https://docs.fastly.com.

Support requests

Subscribers may make support requests by submitting a support ticket which will trigger a system-generated acknowledgement within minutes containing the ticket number and a direct link to the ticket.

DDoS Attack reports should include at least:

- a determination of the severity of the attack.
- the size of the attack threatened or previously observed.

- the type and vector of attack traffic seen or threatened.
- any duration of previous attacks and vector behavior including major source IP addresses.
- attack history for the last 24 months.
- threat specifics including all details of any attacks that the protected services or sites have experienced in the past.

Communications and channels of support

Support tickets

Create support tickets by sending an email to support@fastly.com or calling our dedicated phone line. Filed tickets trigger Fastly's promised response time.

Tickets for communication between Fastly support engineers and a Subscriber's personnel are tracked using a ticketing application, which maintains a time-stamped transcript of communications, and sends emails to Subscriber and Fastly staff as tickets are updated.

Phone support

Subscribers to the DDoS Protection and Mitigation Service receive a dedicated phone number to contact Fastly support engineers. Fastly personnel can also establish audio and video conferencing (free app or browser plug-in required) for real-time voice and video communications.

Chat

To facilitate real-time communication, Subscribers to the DDoS Protection and Mitigation Service receive a dedicated chat channel for real-time communications during Business Hours or as needed by Fastly personnel. Though subject to change, Fastly's current chat provider is Slack (www.slack.com).

Attack traffic

Response time

Fastly commits to responding to DDoS Attack notifications from Subscribers within 15 minutes of notice and, as applicable, will begin on-boarding Subscribers to the DDoS Protection and Mitigation Service within 60 minutes of a DDoS Attack notification.

Related Invoice Credits

Fastly will waive all bandwidth and request charges associated with DDoS Attack traffic and will provide Invoice Credits or adjustments for the same.

Attack traffic credit terms

Subscribers must submit claims for waiver of DDoS Attack-related charges to billing@fastly.com within 30 days of the DDoS Attack.

DDoS Mitigation response SLA

If, during a DDoS Attack on a Subscriber with the DDoS Protection and Mitigation Service, there is a material delay in response time and the cause of the delay is within Fastly's control, a one-time credit of $500 per incident will be credited to that Subscriber's account.

SLA credit terms

- Requests for Invoice Credits must be made within 30 days of the DDoS Attack that triggered the service credit.
- All requests for Invoice Credits must be made to billing@fastly.com.
- In no event shall Invoice Credits exceed the fee for the DDoS Protection and Mitigation Service payable by a Subscriber for the month in which the Invoice Credits accrued.
- A pending Invoice Credit does not release a Subscriber from the Subscriber's obligation to pay Fastly's submitted invoices in full when due.
- Invoice Credits will be applied to the invoice within the month the credits were incurred.

Termination for SLA

For a Subscriber of the DDoS Protection and Mitigation Service with a Termed Contract, if in any three-month period where three (3) or more support response time objectives are not met and the failure to meet the objectives materially adversely impacted the Subscriber, the Subscriber will have 30 days to terminate the DDoS Protection and Mitigation Service subscription following the third response failure. Subscribers must notify Fastly of their intention to terminate the DDoS Protection and Mitigation Service subscription within 30 days of the triggering event.

HIPAA-Compliant Caching and Delivery

https://docs.fastly.com/products/hipaa-compliant-caching-and-delivery

You can configure the Fastly CDN service to cache and transmit protected health information (PHI) in keeping with Health Information Portability and Accountability Act (HIPAA) security requirements. Use the following features to ensure secure handling of cache data that contains PHI:

- Configure frontend and backend TLS to encrypt transmitted data from your origin to your end users.
- Add the `beresp.hipaa` variable to objects containing PHI to keep that data out of non-volatile disk storage at the edge.

Contact sales@fastly.com for more information on how to enable the `beresp.hipaa` feature for your account. For accounts that have this feature enabled, Fastly will enter into a HIPAA business associate agreement (BAA) as an addendum to our terms of service.

IMPORTANT: If you have purchased Fastly's PCI-compliant caching or HIPAA-compliant caching products Fastly will enforce a minimum version of TLS 1.2 or higher for all connections to meet the compliance requirements mandated by the PCI Security Standards Council.

NOTE: Fastly's security and technology compliance program includes safeguards for the entire Fastly CDN service, independent of using the `beresp.hipaa` variable. The Fastly security program and technology compliance guides provide more information about these safeguards.

PCI-Compliant Caching and Delivery

https://docs.fastly.com/products/pci-compliant-caching-and-delivery

We have designed Fastly's core CDN service with Payment Card Industry Data Security Standard (PCI DSS) compliance in mind. With proper authorization on your account, you can use Fastly's `beresp.pci` VCL variable to automatically cache content in a manner that satisfies PCI DSS requirements.

Adding the `beresp.pci` variable to an object prevents writing of that object to non-volatile disk storage on the edge. Combined with frontend and backend TLS, this feature allows you to cache and transmit flagged content through the Fastly network in compliance with our PCI certification.

Contact sales-ecommerce@fastly.com for more information on how to enable this product for your account.

IMPORTANT: If you have purchased Fastly's PCI-compliant caching or HIPAA-compliant caching products Fastly will enforce a minimum version of TLS 1.2 or higher for all connections to meet the compliance requirements mandated by the PCI Security Standards Council.

NOTE: Fastly's security and technology compliance program includes safeguards for the entire Fastly CDN Service, independent of using the `beresp.pci` variable. The Fastly security program and technology compliance guides provide more information about these safeguards.

WAF Quick Start Package

https://docs.fastly.com/products/waf-quick-start-package

Fastly's WAF Quick Start Package provides your organization with basic setup and provisioning of your WAF by Fastly. For more information about this package, contact support@fastly.com.

Prerequisites

To use the WAF Quick Start Package, you need to:

- purchase a paid account with a contract for Fastly's services

- purchase Fastly's WAF
- have logging enabled for at least one supported logging endpoint

NOTE: It's your responsibility to ensure you have a suitable logging service available and properly configured during the onboarding period.

How it works

Fastly Professional Services staff will guide you through the following stages:

- **Planning.** Professional Services staff will help you configure your WAF based on your security requirements. They will gather protection requirements, select from available WAF rules, and configure the WAF based on known or perceived risks to your application.
- **Deployment.** Professional Services staff help you configure your Fastly WAF VCL and add it to your Fastly service. They provide best-practice consulting for configuration of your WAF functionality within the Fastly service and will publish the policy to your Fastly service.
- **Hand-off.** Professional Services staff help you validate that your WAF policy is active and set up in logging only mode.

WAF Support and SLA

https://docs.fastly.com/products/waf-support-and-sla

IMPORTANT: No security product, such as a WAF or DDoS mitigation product, including those security services offered by Fastly, will detect or prevent all possible attacks or threats. As a subscriber, you should maintain appropriate security controls on all web applications and origins. The use of Fastly's security products do not relieve you of this obligation. As a subscriber, you should test and validate the effectiveness of Fastly's security services to the extent possible prior to deploying these services in production, continuously monitor their performance, and adjust these services as appropriate to address changes in your web applications, origin services, and configurations of the other aspects of your Fastly services.

Fastly WAF Support

Fastly WAF Support offers the following resources to assist you with mitigating the service impacts of unwanted or malicious requests:

- Onboarding - We will work with you to enable the initial setup and then do limited monitoring of the designated services for Fastly WAF.
- Initial configuration and deployment support - We will actively work with you to select your rules to block Attacks.
- Ongoing Attack mitigation support - We will work directly with you to configure and activate existing WAF rule filters to deal with changing Attacks or new Attacks.
- New standard rules - We will assist you with the configuration of any new, standard rules introduced in the Fastly WAF.

Definitions

- **"Business Hours"** are 8AM-6PM during a Business Day in California, New York, and London.
- **"Business Days"** are Monday through Friday, excluding any day that is a US national or UK banking holiday.
- An **"Attack"** is a request or requests intended to cause unwanted or error responses from origin sites configured for any Fastly service. Fastly captures and analyzes suspected or actual Attack traffic to improve and protect its services.
- **"Fastly Control"** means elements entirely under Fastly's control and not a consequence of (a) a Subscriber's hardware or software failures, (b) a Subscriber's or end user's connectivity issues, (c) Subscriber operator errors, (d) Subscriber traffic amounts that exceed a Subscriber's Permitted Utilization as defined in the Terms and Conditions, (e) corrupted Subscriber content, (f) acts of god (any) or war, or earthquakes, or terrorist actions.

Support channels and availability

The following table summarizes support channels and availability for Fastly WAF Support as determined by the support package purchased by a Subscriber:

Support offering	Gold Support	Enterprise Support

Support offering	Gold Support	Enterprise Support
Online self-service help	Unlimited access.	Unlimited access.
Availability for general inquiries	Business hours.	24/7/365.
Severity 1 incident report response	2 hours.	15 minutes.
Dedicated chat channel	Not available.	Business hours.
Web and email support	Available.	Available.
Phone support	Not available.	Toll-free telephone available 24/7/365.
Emergency escalation	Available via email.	Available via email and phone support.

Onboarding

As part of onboarding a subscriber service, Fastly support will:

- enable designated services for WAF functionality, providing access to our rule and filter libraries.
- work directly with you to determine the right set of rules and filters for your service.
- publish those rules or filters into your service in logging mode.
- monitor the behavior of those rules for a designated period starting when the rules are published to the service.

Note that false positive triage will resolve instances where legitimate requests have triggered a WAF rule or filter and either remove the rule from the policy or, where possible, modify the rule or policy to address the legitimate request properly.

Subscriber responsibilities

Subscribers must identify and maintain two points of contact to be used during an Attack to communicate status and issues and to coordinate with Fastly to successfully protect services. Subscribers are responsible for using and configuring CDN services according to the documentation available at https://docs.fastly.com.

Support requests

Subscribers may make support requests by submitting a support ticket, which will trigger a system-generated acknowledgement within minutes containing the ticket number and a direct link to the ticket.

In particular, when requesting support related to an Attack, Subscribers should include as much of the following information as available:

- a determination of the severity of the Attack.
- the size of the Attack threatened or previously observed.
- the type and vector of Attack traffic seen or threatened.
- any duration of previous Attacks and vector behavior including major source IP addresses.
- an Attack history for the last 24 months.
- threat specifics including all details of any Attacks that the protected services or sites have experienced in the past.

Communications and channels of support

Support tickets

Create support tickets by sending an email to support@fastly.com. Tickets for communication between Fastly support engineers and a Subscriber's personnel are tracked using a ticketing application, which maintains a time-stamped transcript of communications, and sends emails to Subscriber and Fastly staff as tickets are updated.

Phone support

Subscribers who also purchase Enterprise Support receive a dedicated phone number to contact Fastly support engineers. Fastly personnel can also establish audio and video conferencing (free app or browser plug-in required) for real-time voice and video communications.

Chat

To facilitate real-time communication, Subscribers receive a dedicated chat channel during Onboarding and, for Subscribers that also purchase Enterprise Support, for an Attack for real-time communications about WAF issues during Business Hours or as needed by Fastly personnel. Though subject to change, Fastly's current chat provider is Slack (www.slack.com).

Observational logging

Fastly may from time to time, including as part of initial onboarding and during any period where Subscriber purchases additional Fastly WAF Tuning Package or Fastly WAF Tuning Plus Package, collect and store a copy of logging information from the Fastly WAF (which will include IP addresses) to monitor ruleset behavior, including false positives, by establishing a logging endpoint in your service configuration which will securely collect logging information in a third-party storage provider. Subscriber instructs Fastly to access and use the logs exclusively for providing WAF services, providing support and performance management to Subscriber, monitoring or maintaining Subscriber's Services and the Fastly WAF, threat detection and in accordance with the Documentation. Logged data will be deleted on a rolling basis and in any event retained no longer than thirty (30) days unless otherwise agreed by Subscriber.

WAF Tuning Package

https://docs.fastly.com/products/waf-tuning-package

Fastly's WAF Tuning Package provides your organization with tuning of your WAF by Fastly. For more information about this package, contact support@fastly.com.

How it works

Fastly Professional Services staff will guide you through the following tuning stages:

- **Planning.** Professional Services staff help you gather protection requirements, define rules or filter policies, and develop policy structure.
- **Deployment.** Professional Services staff help you configure your Fastly WAF VCL and add it to your Fastly service. They provide best-practice consulting for configuration of your WAF functionality within the Fastly service and will publish the policy to your Fastly service.
- **Testing.** Professional Services staff help you validate that your WAF policy is active and set up testing for it.
- **Go-Live.** Professional Services staff monitor and address issues during final production testing and policy deployment.

Planning, deployment, testing, and go-live may involve some iterative cycles depending on the complexity of your policy.

Policy services

Some common tuning options we offer include:

- Initial setup and configuration
- Validation of policy match to origin systems
- Policy updates and maintenance

WAF Tuning Plus Package

https://docs.fastly.com/products/waf-tuning-plus-package

Fastly's WAF Tuning Plus Package provides your organization with enhanced professional maintenance of your WAF by Fastly. The WAF Tuning Plus Package also improves visibility into application layer threats and strengthens your overall security posture. The WAF Tuning Plus Package includes ongoing tuning and configuration services designed to help protect you against critical threats. To protect against WAF bypass attacks, it also includes authenticated TLS to origin.

For more information about the WAF Tuning Plus Package, contact support@fastly.com.

WAF Tuning Plus Package features

Fastly's WAF Tuning Plus Package is a service offering for the term of your contractual agreement. It includes the following features.

Ongoing tuning and configuration

At your request, Fastly will provide you with one report per service protected by the Fastly WAF. Fastly will schedule periodic calls with you to review the reports.

Up to once per quarter, at your request, Fastly will tune previously provisioned WAF services as follows:

- We'll update your original profile, created during your initial WAF tuning, to record any new changes to your application stack or new perceived security risks based on actual or attempted attacks.
- We'll update your WAF rule set to the latest available (if applicable).
- We'll enable, disable, or change new or existing WAF rules based on new traffic patterns or security risks not present in the initial tuning cycle.
- We'll make a set of final recommendations on OWASP thresholds and switch your WAF into blocking mode.

Up to three times per quarter, at your request, Fastly will provide on-demand rule enablement (if available) for critical vulnerabilities.

Proactive notifications

We may notify you of available Fastly rules to help address critical vulnerabilities that we identify.

Authenticated TLS to origin

To mitigate WAF bypass attacks, Fastly will configure client-authenticated connections to your origin server for each service running WAF. This is an additional layer of security on top of network-level ACLs. This service requires a customer-provided TLS certificate, matching private key, and CA certificate or certificate chain.

Fastly will update the certificate on your behalf prior to expiration. Here's how it works:

- Fastly must receive new certificates at least 15 business days prior to expiration.
- Fastly will update the private key on your behalf (with a 15 business day notice) should the key be revoked.
- If you don't have your own key and certificate, Fastly can help you generate the certificates and keys at an additional cost. For more information, contact sales@fastly.com.

Web Application Firewall (WAF)

https://docs.fastly.com/products/web-application-firewall

The Fastly WAF is a Web Application Firewall (WAF) security product that detects malicious request traffic sent over HTTP and HTTPS. Once properly configured and enabled for a service, the Fastly WAF can help protect against application-layer (layer 7) attacks such as SQL injection, cross-site scripting, and HTTP protocol violations.

Enabling Fastly WAF doesn't require modifications to your web application or origin servers. Contact our sales team to get started. Once you purchase the Fastly WAF, our customer support team will enable it with a default WAF policy for any service you've provided a service ID for. They will then work closely with you on additional configuration refinements. Once configured, you can then begin monitoring logs to determine which requests to your origin are legitimate and which you should consider blocking.

Limitations

All WAF products that exist today, including the Fastly WAF, have several limitations:

- **False positives.** Any WAF can mistake good traffic for bad. We strongly recommend you monitor your logs for a minimum of two weeks before blocking traffic. You don't want to start blocking traffic with rules that are generating false positives.
- **DNS configuration.** A WAF only works when traffic is directed through it. It cannot protect against malicious requests that are sent to domain names or IP addresses that are not specified in your WAF configuration.
- **Effective rules.** A WAF is only as effective as the provisioned and tuned rules. You can add, remove, or modify rule modes using rule management web interface or the API.
- **Custom application vulnerabilities.** If attackers discover a vulnerability unique to your application or the technologies you use, and if your WAF configuration does not have a rule to protect against exploits for that particular vulnerability, it will not be able to protect your application in that instance. You can add additional rules to help protect against these types of attacks. If you need more protection than the selected rules provide, customer support can work with you to create custom VCL to help block malicious requests.
- **Inspection of HTTP and HTTPS traffic only.** A WAF only inspects HTTP or HTTPS requests (layer 7). It will not process any TCP, UDP, or ICMP requests.

Security products note

IMPORTANT: To ensure your web application only receives traffic from your WAF-enabled Fastly service, we strongly recommend you configure TLS client authentication for that service and allowlist Fastly's assigned IP ranges.

No security product, such as a WAF or DDoS mitigation product, including those security services offered by Fastly, will detect or prevent all possible attacks or threats. As a subscriber, you should maintain appropriate security controls on all web applications and origins. The use of Fastly's security products do not relieve you of this obligation. As a subscriber, you should test and validate the effectiveness of Fastly's security services to the extent possible prior to deploying these services in production, continuously monitor their performance, and adjust these services as appropriate to address changes in your web applications, origin services, and configurations of the other aspects of your Fastly services.

Observe

These articles provide information about Fastly products that provide visibility and insights into traffic, security, and performance.

https://docs.fastly.com/products/product-observe

High Volume Logging

https://docs.fastly.com/products/high-volume-logging

Fastly's real-time log streaming features allow you to tune the performance of Fastly services, but are limited to a monthly average of two log statements per request, per service. For customers who need to increase this limit, Fastly offers High Volume Logging. Contact sales@fastly.com to learn more.

Billing

High Volume Logging is billed based on the cumulative log statements streamed in excess of the Fastly's Full-Site Delivery Real-Time Log Streaming limits. Usage is calculated using the average size of all log statements multiplied by the number of statements in excess of the limit. The size is measured in log GBs streamed, pre-compression.

Logging Insights Package

https://docs.fastly.com/products/logging-insights-package

Fastly's Logging Insights Package provides you with guidance and customization of dashboard graphs in your third-party logging endpoint. After we've interviewed you to identify your specific business needs, we'll write advanced queries and create customized dashboards for the logs stored in your logging endpoint. You can then analyze and correlate any aspect of HTTP and HTTPS requests and responses to gain visibility into your service, allowing you to make decisions and changes. We'll then answer your questions and incorporate feedback to further customize the dashboards.

Prerequisites

To use the Logging Insights Package, you need to:

- purchase a paid account with a contract for Fastly's services
- have logging enabled for at least one supported logging endpoint
- be interviewed by Fastly so we can identify your customer-specific business needs
- grant Fastly temporary access to your third-party logging endpoint so we can configure your account on your behalf

NOTE: It's your responsibility to grant and revoke Fastly's access to your third-party logging endpoint.

Logging Insights Package features

The Logging Insights Package for Sumo Logic provides you with customization of the following Sumo Logic dashboards:

- The **Overview dashboard** provides you with a high-level overview of your Fastly services, allowing you to identify potential problems within them.

- The **Origin Performance dashboard** allows you to focus on your origin performance to check for latencies, slow URLs, and error-causing URLs.
- The **Quality of Service dashboard** allows you to see where your Fastly service's download times, cache performance, and performance by geographic location are below minimum thresholds.
- The **Visitors dashboard** allows you to see where your traffic is coming from.

The Logging Insights Package supports the Sumo Logic App for Fastly. You'll need a Sumo Logic account with the appropriate license, and you'll need to enable the Sumo Logic logging endpoint. For additional information, contact sales@fastly.com.

Compute

These articles provide information about Fastly's serverless compute environment for building applications and executing at the edge.

https://docs.fastly.com/products/product-compute

Compute@Edge

https://docs.fastly.com/products/compute-at-edge

IMPORTANT: This information is part of a limited availability release. For more information, see our product and feature lifecycle descriptions.

The Compute@Edge platform helps you compile your custom code to WebAssembly and runs it at the Fastly edge using the WebAssembly System Interface for each compute request. Per-request isolation and lightweight sandboxing create an environment focused on performance and security.

Serverless isolation technology

Compute@Edge runs WebAssembly (Wasm) and leverages the Lucet compiler and runtime, which ahead-of-time compiles customer code to Wasm. When a compute request is received by Fastly, an instance is created and the serverless function is run, allowing developers to apply custom business logic on demand.

Global deployment

Deploying to a Compute@Edge service leverages Fastly's software-defined network and globally distributed points of presence. A single deploy action makes customer logic available across the Fastly network.

Available programming languages

By running Wasm on the Fastly network, Compute@Edge creates a serverless environment suitable for multiple programming languages. Fastly collaborates with the ByteCode Alliance and other open source communities to actively grow the number of supported languages. Resources per language are available on developer.fastly.com.

Logging endpoint compatibility

Compute@Edge supports sending user-specified logs to a variety of logging endpoints. These connections can be created and managed via manage.fastly.com and by using the log_fastly crate.

Continuous integration and deployment

Deployment to the Compute@Edge platform can be accomplished via manage.fastly.com, the Fastly API, and via Fastly's Terraform provider plugin. The Fastly CLI also provides a local toolchain with features for creating, debugging, and deploying to Wasm services. Some of those features, like those related to log tailing, are disabled by default. To learn more about them, contact your account manager or email sales@fastly.com for details.

Enable

These articles provide information about Fastly services and support solutions.

https://docs.fastly.com/products/product-enable

Assurance Services

https://docs.fastly.com/products/assurance-services

Subscribers who purchase Assurance Services will:

- have access to a library of third-party audit reports and certification attestations (most recent 12 months).
- have access to executive summary reports for penetration tests and network scans (most recent 12 months).
- have access to a library of security-related policies and procedures.
- have access to a library of executive summaries of annual risk assessments (most recent 12 months).
- have access to a library of historical Fastly Service Advisory (FSA) documents (most recent 12 months).
- be able to perform unlimited audits of Fastly's security and technology compliance programs, subject to Subscriber's purchase of Professional Services. Audits require advance notice of at least 10 business days and shall be performed by Subscriber (or a mutually acceptable third party) according to standard audit practices.
- have the ability to be added as an Additional Insured on Fastly's General Commercial Liability Insurance for an additional fee.

Subscribers who wish to purchase Assurance Services must also purchase Gold or Enterprise Support.

Designated Technical Specialist

https://docs.fastly.com/products/designated-technical-specialist

Fastly offers the ability to purchase the support of a Cloud Engineer to serve as a Designated Technical Specialist for your organization. These specialists help you optimize your use of Fastly's products and features by providing proactive check-ins and regular reviews to help you analyze your account's service configurations and their performance. Designated Technical Specialists also provide enhanced troubleshooting coordination with Fastly's support and professional services organizations.

Fastly offers three Designated Technical Specialist packages: Essentials, Premier, and Enterprise. A Designated Technical Specialist's available hours of service each month to your organization depend on the package you purchase and could include the following summarized activities:

Support Offering	Essentials	Premier	Enterprise
Total available hours	Up to 15 hours/month	Up to 80 hours/month	Up to 160 hours/month
VCL code configuration reviews	1 review/month	4 reviews/month	8 reviews/month
Architecture and configuration recommendations	Included	Included	Included
White glove escalation support	Included	Included	Included
Email support	Available	Available	Available
Private chat support	Available	Available	Available
Emergency phone support	Available	Available	Available
Availability for general inquiries	Business hours	Business hours	Business hours
Initial response time	Next business day	Next business day	Next business day
Proactive account management	Account Manager	Account Manager	Account Manager
Support coordination	Included	Included	Included

Support Offering	Essentials	Premier	Enterprise
Scheduled technical check-ins	Monthly	2x monthly	Weekly (as requested)
Account reporting	Monthly	Weekly	Weekly
Business reviews	Annually	Quarterly	Monthly
On-site travel for business reviews	Not included	Up to 2x annually (as requested)	Quarterly (as requested)
Custom reporting	Not included	Not included	By request
Early beta program access	Not included	Not included	Included

Definitions

- **"Business Hours"** are 8AM-6PM during a Business Day in California, New York, London, or Tokyo.
- **"Business Days"** are Monday through Friday, excluding any day that is simultaneously a US, UK, and Japanese national or banking holiday.

IMPORTANT: Designated Technical Specialists provide support during Fastly business hours to facilitate *non-urgent* discussions. They are not a 24×7 resource. Always rely on normal support communications channels for urgent issues and escalations.

Designated Technical Specialist packages

Each Designated Technical Specialist package includes Enterprise Support as well as the following core features:

- Email and private chat channel support during business hours between you and Fastly to facilitate quick questions and answers for general inquiries and communication.
- Regular guidance on topics like configuration analysis, account performance, infrastructure and company plans, and roadmap requests.
- Advice on best practices for implementing and using Fastly with your infrastructure.
- Priority engagement and coordination with appropriate support resources as necessary during normal Fastly business hours.
- Comprehensive documentation of your implementation of Fastly's services and requirements to enable better support by Fastly teams.
- Basic reports on utilization and performance of Fastly services.

For all Designated Technical Specialist packages, keep in mind that other than regularly scheduled business reviews on site (as applicable for your package) additional reviews or on site travel must be agreed upon in advance via a statement of work. Also, any unused hours or other scheduled availability does not carry forward to future months. You won't be entitled to any refunds or credits for unused hours or other scheduled availability for any one month.

NOTE: English is the primary language used by Designated Technical Specialists.

Essentials Designated Technical Specialist

In addition to the core features noted above, included hours could be used for:

- Monthly account reports with an overview of services, traffic, and tickets.
- An annual business review.

Premier Designated Technical Specialist

In addition to the core features noted above, included hours could be used for:

- Weekly account reports with an overview of services, traffic, and tickets.
- Scheduled check-ins via phone, 2x monthly.
- A quarterly business review (QBR), with onsite option, twice annually.

Enterprise Designated Technical Specialist

In addition to the core features noted above, included hours could be used for:

- Weekly account reports with an overview of services, traffic, and tickets.
- Weekly scheduled check-ins via phone (as requested).
- A monthly business review (QBR), with onsite option, quarterly as requested.
- Custom reporting upon reasonable request.
- Early access to beta programs.

Live Event Monitoring Service

https://docs.fastly.com/products/live-event-monitoring-service

With Fastly's Live Event Monitoring Service, our Customer Support engineers will monitor your scheduled event's performance and help troubleshoot issues with your Fastly service. We will also alert you as we detect issues with internet congestion and with upstream or downstream providers. We do this in real time throughout your event using a dedicated chat channel. This allows you to receive alerts and notifications as well as ask questions without losing time spent contacting support and recounting what the issue is. Fastly's Live Event Monitoring Service is performed from Fastly's offices and does not include support on-site at your facilities.

For additional information about this service, contact sales@fastly.com.

IMPORTANT: This information is part of a limited availability release. For more information, see our product and feature lifecycle descriptions.

Prerequisites

To use the Live Event Monitoring Service, you must purchase a paid account with a contract for Fastly's services.

You must schedule the start and end times of your event. These times will appear on your service order.

Event Monitoring service features

For the duration of your scheduled event, the Live Event Monitoring service reserves Fastly support staff who will perform the following:

Monitoring:

- Drops or spikes in bandwidth and request levels
- 5xx and 4xx errors
- Cache hit ratio
- Origin latency
- Upstream issues with origin
- Internet congestion events

Alerting and real-time communication:

- Kick-off call to define alerting thresholds
- Real-time notifications via instant messaging

Troubleshooting:

- Rapid response from personnel who know your configuration and have been monitoring the scheduled event
- Accelerated escalation to senior support teams

Observational logging

In the course of performing Live Event Monitoring services, Fastly may collect and store a copy of logging information from Fastly Services by establishing a logging endpoint in your service configuration that will securely collect logging information in a third-party storage provider. When you purchase Live Event Monitoring services, you allow Fastly to access and use the logs exclusively for providing performance management, monitoring, and troubleshooting of your Fastly services during the event and for analysis after the event. Logged data will be deleted on a rolling basis and in any event retained no longer than thirty (30) days unless otherwise agreed to by you.

Performance Optimization Package

https://docs.fastly.com/products/performance-optimization-package

Fastly's Performance Optimization Package allows you to take advantage of configuration expertise to analyze and tune the performance of your Fastly services. Fastly's Professional Services team can help you use real-time analytics to identify potential improvements for your site's performance.

Prerequisites

To use the Performance Optimization Package, you need to:

- purchase a paid account with a contract for Fastly's services
- provide Fastly with a batch of representative site URLs that Fastly will analyze for various performance-related factors and use to suggest changes to increase performance

Performance Optimization Package features

The Fastly Performance Optimization Package specifically includes the following analyses and recommendations by Fastly Professional Services staff:

- **Cache Hit Ratio, Shielding, and Clustering.** We'll review your existing configuration and service settings and recommend incremental performance improvements you can make to ensure you're taking advantage of Fastly's network architecture.
- **Gzip and Brotli (origin based) compression.** We'll suggest configuration changes needed to ensure requested objects have the proper compression for each content type.
- **HTTP/2 readiness.** We'll assess your site and suggest network protocol changes to support HTTP/2, and provide recommendations on how to optimize for it.
- **TCP/IP protocols.** We'll analyze how your Fastly services send data via TCP/IP to end users and suggest the configuration changes needed to maximize request throughput while reducing last mile latency.

As part of this package, we'll provide you with a written assessment of our recommendations. Implementation of those recommendations by Fastly's Professional Services team can be purchased at an additional cost. For more information, contact sales@fastly.com.

Professional Services

https://docs.fastly.com/products/professional-services

Fastly offers a range of Professional Services to help you begin using Fastly services. Choose between Service Implementation, Service Management, or Consulting Engagement Services, depending on your needs. For more information about any of our Professional Services packages, contact sales@fastly.com.

Service Implementation

How it works

Fastly Professional Services staff will personally guide you through the following stages:

- **Planning:** Professional Services staff help you with requirements gathering, solution design, documentation and resource allocation.
- **Implementation:** Professional Services staff help you with configuration of Fastly services and custom VCL development. They provide best-practice consulting for configuration of your origins.
- **Testing:** Professional Services staff help you validate configurations and set up testing.
- **Go-Live:** Professional Services staff monitor and address issues during final production testing and deployment.

Implementation, Testing, and Go-Live may involve some iterative cycles depending on the complexity of your configuration.

Implementation options

Some common implementation options we offer include:

- Initial setup and configuration

- End-to-end encryption setup
- Fine-tuning cache times
- Custom header logic
- Dynamic content delivery optimization
- Multi-tiered caching setup
- Lightweight web page hosting
- Custom purging and event-driven content management
- Geographic or localization detection
- Edge logic and device detection
- Stale content configuration and origin outage handling
- Edge authentication and authorization
- ESI (edge side includes)
- Streaming and video packaging
- Site performance analysis
- On-site Varnish and VCL training

Fastly offers two Service Implementation packages:

- **Standard:** Basic implementation for Fastly customers with simple content configurations.
- **Enterprise:** Advanced implementation for Fastly customers with complex, custom configurations.

Service Management

For customers who require ongoing configuration and technical assistance, Fastly offers Service Management that provide professional services to you and your staff on an as-needed basis. These hours may be used to supplement your existing Support Plan or Service Implementation.

Some common activities you may need assistance with:

- Site performance analysis
- Varnish and VCL training
- Service configuration
- End-to-end encryption setup
- Cache time fine-tuning
- Custom header logic creation
- Dynamic content delivery optimization
- Multi-tiered caching setup
- Lightweight web page hosting
- Custom purging and event-driven content management
- Geographic or localization detection
- Edge logic and device detection
- Stale content configuration and origin outage handling
- Edge authentication
- ESI (edge side includes) configuration
- Streaming and video packaging

Consulting Engagement Services

For customers who require in-house expertise or dedicated resources, Fastly's Support Engineers are available to provide a range of more technical professional services, including:

- Technical advisory services
- Translating configurations to VCL
- Optimization of website performance
- On-site Varnish and VCL training

- Non-Fastly related performance tuning
- Adapting Fastly features to a particular customer use case

Related offerings

https://docs.fastly.com/products/related-offerings

Fastly offers service level agreements to customers based on the nature of their agreement with Fastly and the Fastly products they have purchased. These service level agreements offered by Fastly provide information to customers based on the nature of their agreement with Fastly and the Fastly products they have purchased.

- Service availability SLA
- Support description and SLA

We understand that some customers may require more support from Fastly to meet their additional security and compliance needs. Customers with these needs may subscribe to packages that include our Assurance Services offering.

Service availability SLA

https://docs.fastly.com/products/service-availability-sla

Support availability and response times vary depending on the type of account you have and the level of support you have purchased.

Agreement Type	Unpaid Account	Month-to-Month Account	Termed Contract	Gold & Enterprise Support
Service Level Agreement	None	None	Termination Option	Invoice Credits + Termination Option

Definitions

"Degraded Performance" means the Services are experiencing Error Conditions that are (1) caused by issues under Fastly Control, (2) observable or reproducible by Subscriber or Fastly, (3) requiring Subscriber to redirect traffic off the Services. Degraded Performance does not include any reduction on availability of the Application User Interface or API due to maintenance.

"Error Condition" means the Services are (1) not responding to end user requests, (2) incorrectly sending end users error condition messages or (3) sending incorrect partial content to end users and these conditions are observable or reproducible by Subscriber or Fastly.

"Fastly Control" means elements entirely under Fastly's control and not a consequence of (a) Subscriber hardware or software failures, (b) Subscriber or end user connectivity issues, (c) Subscriber operator errors, (d) a Utilization spike (see below), (e) corrupted Subscriber content, or (f) acts of god (any) or war, or earthquakes, or terrorist actions.

Termination

Any Subscriber that has a contract with a term and a minimum commitment shall have thirty (30) days to terminate their subscription agreement following (1) a period of Degraded Performance longer than 7.2 hours in any one month, or (2) three contiguous months that have periods of Degraded performance longer than 43.8 minutes each.

Availability invoice credits

Subscribers who purchase Gold or Enterprise Support shall be entitled to Invoice Credits according to the following table.

Availability Percent	Period of Degraded Performance	Monthly Credit Percent
Below 100% - 99.99%	Up to 4.32 minutes	1%
Below 99.99% – 99.9%	Up to 43.8 minutes	5%
Below 99.9% – 99.0%	Up to 7.2 hours	10%
Below 99.0% - 98.0%	Up to 14.4 hours	25%
Below 98.0%	Greater than 864 minutes	50%

Invoice Credits for unavailability will accrue on a monthly basis. The Credit Amount for a month is equal to the monthly usage charge multiplied by Monthly Credit Percent.

Credit terms

- Requests for Invoice Credits for Degraded Performance must be made within 30 days of the period of Degraded Performance.
- The maximum amount of any credit is the Invoice Amount for the month the Degraded Performance occurred.
- A pending credit does not release Subscriber from its obligation to pay Fastly's submitted invoices in full when due.
- Credits will be applied to the Invoice two months following the month an invoice credit was incurred.

Utilization Spikes

Subscriber's bandwidth utilization, measured in megabits per second, will be sampled every five (5) minutes on a region-by-region basis each month (the "**Samples**"). Subscriber's "**Average Utilization**" for a region in a month will be the average of the Samples. Subscriber's "**Peak Utilization**" for a region in a month will be calculated by the 95th percentile method, according to which the Samples will then be ordered from highest to lowest, and the highest five percent (5%) of Samples will be discarded and the remaining highest Sample will be Subscriber's Peak Utilization for the region in that month. Subscriber's "**Permitted Utilization**" in a month for a region will be five (5) times Subscriber's Average Utilization in that month for that region. A "**Utilization Spike**" will occur if Subscriber's Peak Utilization exceeds its Permitted Utilization in a region. Utilization Spikes may interfere with or disrupt the integrity or performance of the Services. Subscribers should contact Support in advance of any planned utilization spike and respond immediately to any communications from Fastly regarding an actual or suspected Utilization Spike.

Support description and SLA

https://docs.fastly.com/products/support-description-and-sla

Support availability and response times vary depending on the type of account you have and the level of support you have purchased. The following table summarizes those offerings:

Support Offering	Standard Support	Gold Support	Enterprise Support
Online Self-Service Help	Unlimited access.	Unlimited access.	Unlimited access.
Availability for General Inquiries	Business hours.	Business hours.	24/7/365.
Availability for Incident Reports	Business hours, including weekends & holidays.	24/7/365.	24/7/365.
Initial Response Times	By the next business day.	Severity 1 Incidents within 2 hours. Severity 2 Incidents within same day. All other Incidents by the next business day.	Severity 1 Incidents within 15 minutes. Severity 2 Incidents within 2 hours. All other Incidents by the next business day.
Email support	Available.	Available, with priority over Standard Support.	Available, with priority over Standard and Gold Support.
Phone and chat support	Not available.	Not available.	Toll-free telephone available 24/7/365. Dedicated chat channel available during Fastly business hours.
Emergency Escalation	Not available.	Not available.	Available via email and phone.
Designated Technical Resource	Not available.	Not available.	Available with designated technical resource add-on package.

Support Offering	Standard Support	Gold Support	Enterprise Support
Discounted Professional Services	Not available.	Not available.	30% discount on Service Management packages. Does not apply to Signal Sciences service packages.
PCI and HIPAA configuration services	Not available.	Not available.	Available via email, phone, and chat support.
Enhanced compliance support (including GDPR)	Not available.	Not available.	Available via email, phone, and chat support.
Termination Option	Not available for unpaid and month-to-month customers. Only included for termed contracts.	Available with invoice credits.	Available with invoice credits.

Partner Support Services

For Fastly customers approved as Partners, additional partner support products become available. To be eligible as a Partner, customers must be classified and approved as such. Contact partners@fastly.com for details.

Partners will not be entitled to Standard Support that customers receive automatically on the platform. All Partners will be required to purchase either Partner Gold or Partner Enterprise support. The corresponding support availability and response times vary depending on the purchased support level.

In addition to the Gold and Enterprise support offerings, all Partners purchasing Partner Support receive access to a library of on-demand online training modules.

Technical support

The following section applies to all subscribers.

Definitions

- **"Business Hours"** are 8AM-6PM during a Business Day in California, New York, London, or Tokyo.
- **"Business Days"** are Monday through Friday, excluding any day that is simultaneously a US, UK, and Japanese national or banking holiday.
- An **"Incident"** is an occurrence during which end users' use of Subscriber's services is adversely impacted.
- A **"Severity 1 Incident"** is an incident resulting in a major service outage requiring Subscriber to redirect all traffic from Fastly to another CDN.
- A **"Severity 2 Incident"** is an incident resulting in minor or intermittent outage not requiring Subscriber to redirect traffic to another CDN.
- **"Fastly Control"** means elements entirely under Fastly's control and not a consequence of (a) a Subscriber's hardware or software failures, (b) a Subscriber's or end user's connectivity issues, (c) Subscriber operator errors, (d) Subscriber traffic amounts that exceed a Subscriber's Permitted Utilization as defined in the Terms and Conditions, (e) corrupted Subscriber content, (f) acts of god (any) or war, or earthquakes, or terrorist actions.

Subscriber responsibilities

Subscriber is responsible for using and configuring services according to the Documentation available at https://docs.fastly.com.

Support requests

Subscribers submit support requests by sending email to support@fastly.com. Subscribers receive a system-generated response within minutes containing the ticket number and a direct link to the ticket.

Reasons to contact us for incidents include:

- Services are not responding to end user requests.
- Services incorrectly send end users error condition messages.
- Services send incorrect or partial content to end users.

Incident reports should include all relevant information such as:

- Subscriber's determination of the Severity Level of the incident,
- Subscriber hardware failures,
- Subscriber operator errors,
- Services configuration errors made by Subscriber employees,
- A potential Utilization Spike (see the Service Availability SLA),
- Corrupted Subscriber content,
- DDOS attacks, and
- Relevant *force majeure* acts such as extreme weather, earthquakes, strikes or terrorist actions.

Communications

Tickets

Communications between Fastly support engineers and Subscriber personnel are conducted using a ticketing application that maintains a time-stamped transcript of communications and sends emails to Subscriber and Fastly staff as tickets are updated.

Chat

Subscribers to Enterprise Support receive a dedicated chat channel for real-time communications during Business Hours. Though subject to change, Fastly's current chat provider is Slack (www.slack.com).

Phone support

Subscribers to Enterprise Support receive a dedicated, toll-free phone number to contact Fastly support engineers. Fastly personnel can also establish audio and video conferencing (free app or browser plug-in required) for real-time voice and video communications.

Response time

Fastly shall use best efforts to respond in a timely fashion.

Termed contracts

The following applies to any subscriber that has a contract with a term and a minimum commitment.

Response times

Fastly commits to acknowledging receipt of a support ticket within the next Business Day following submission of a support request by a Subscriber with a Termed Contract.

Termination

In any three-month period where three (3) or more support Response Time objectives are not met and the failure to meet the objectives materially adversely impacted Subscriber, Subscribers with a Termed Contract, Gold Support, or Enterprise Support shall have thirty (30) days to terminate their subscription agreement following the third failure.

Incident response times

Incident reporting

Severity 1 Incidents: Fastly will provide Subscriber an Incident Support Email address for Subscriber to report Incidents. Subscriber should report Incidents promptly using the Incident Support email.

Severity 2 Incidents: Subscriber should report Severity 2 Incidents by submitting a Support Request.

Incident reporting and additional fees

For Severity 1 Incidents caused by factors within Subscriber's control, a flat fee of $1500 will be assessed, and any time spent beyond three (3) hours will be invoiced at Subscriber's undiscounted Professional Services rates. For Severity 2 Incidents caused by factors within Subscriber's control, Subscriber will be invoiced at Subscriber's undiscounted Professional Services Rates.

For all incidents:

- If the Incident-causing factors are within Fastly's control, there will be no hourly charges for Fastly engineering staff time.
- If the factors are within Subscriber's control, Subscriber agrees to pay Fastly its hourly charges for Fastly engineering staff time. If it appears likely the factors are within Subscriber's control, Subscriber may tell Fastly staff to stop working on troubleshooting the Incident (thereby stopping the hourly charges from being incurred). Subscriber agrees to tell Fastly to stop working on an Incident via an email sent to Fastly's Incident Support email address. The timestamp on the email will be the time charges cease to be incurred.

Gold Support

Fastly will respond to the report of an Incident by troubleshooting the causes of the Incident and resolve them if caused by factors within Fastly's control, or provide information to those who can resolve the factors if the factors are within others' control, as follows:

For a Severity 1 Incident:

- Fastly support staff will acknowledge receipt of the email within two hours.
- Fastly engineers will begin actively troubleshooting within the same day, will work on the Incident during the same day, and will provide status updates to Subscriber daily on each subsequent day.
- Fastly staff will work until (a) the incident is resolved or (b) the incident is believed to be outside of Fastly's control.

For a Severity 2 Incident:

- Fastly support staff will acknowledge receipt of the email within the same day.
- Fastly engineers will begin actively troubleshooting within the same day, will work on the Incident during the same day or next day, and will provide status updates to Subscriber daily on each subsequent day.

Enterprise Support

Fastly will respond to the report of an Incident by troubleshooting the cause(s) of the Incident and resolve them if caused by factors within Fastly's control, or provide information to those who can resolve the factors if the factors are within others' control, as follows.

For a Severity 1 Incident:

- Fastly support staff will acknowledge receipt of the email within 15 minutes.
- Fastly will start actively troubleshooting within 30 minutes of receipt of the email.
- Fastly will perform its tasks on a 24/7 basis.
- Fastly and Subscriber will immediately communicate upon learning new information that may be useful in troubleshooting the incident, and status updates between Fastly and Subscriber staff will take place no less frequently than every 30 minutes for the first two hours, and no less frequently than every hour thereafter.
- Fastly staff will work until (a) the incident is resolved or (b) the incident is believed to be outside of Fastly's control.

For a Severity 2 Incident:

- Fastly support staff will acknowledge receipt of the email within two hours.
- Fastly engineers will begin actively troubleshooting within the same day, will work on the Incident during the same day, and will provide status updates to Subscriber daily on each subsequent day.

Support invoice credits

In the event a Severity 1 Incident occurs, Subscriber has purchased Gold or Enterprise Support, the cause of the Incident is within Fastly's control, and any of the communication or response timeframes are materially not met, a one-time credit of $500 per incident will be credited to Subscriber's account.

Credit Terms:

- Requests for Invoice Credits must be made within 30 days of the incident which triggered the service credit.
- In no event shall Invoice Credits exceed the invoice value of the month in which they are accrued.
- A pending credit does not release Subscriber from its obligation to pay Fastly's submitted invoices in full when due.

- Credits will be applied to the invoice two months following the month an invoice credit was incurred.

NOTE: Fastly maintains support for its original Premium Support and Platinum Support plans. To convert your account to the current Gold and Enterprise Support plans, contact sales@fastly.com. If you have an agreement that requires the purchase of Platinum support, converting to Enterprise support satisfies that requirement.

Signal Sciences

These articles provide information about Fastly's Signal Sciences products.

https://docs.fastly.com/products/signal-sciences

Signal Sciences Cloud WAF

https://docs.fastly.com/products/signal-sciences-cloud-waf

The Signal Sciences Cloud WAF (Cloud WAF) is an application security monitoring system that monitors for suspicious and anomalous web traffic and protects against attacks directed at the applications and origin servers that you specify.

Cloud WAF

Cloud WAF analyzes inbound traffic to your applications and origin servers to detect and identify threats and attacks. When enough attacks are seen from an IP address, Cloud WAF determines whether to allow the request, block the request, tag the request with signals, flag the IP address, or rate limit the IP address. You can choose to enable or disable the blocking feature.

Enabling Cloud WAF doesn't require modifications to your applications or origin servers. In order to use Cloud WAF, you must upload a TLS certificate, add an origin server using the Signal Sciences Hosted Dashboard, and update your DNS records to point to the appropriate servers.

Threat Intelligence

As part of Cloud WAF, we may aggregate the attack data collected from Cloud WAF and combine it with data collected from security and other services offered as part of the Fastly platform, including for other subscribers. We use these data insights (Threat Intelligence) to analyze and detect potential future anomalies or attacks and to improve, secure, provide, and market Fastly services in a manner that does not associate the Threat Intelligence with or identify any subscriber. For example, you receive the benefits of this Threat Intelligence via the Network Learning Exchange (NLX) feature that adds a unique signal to information in the Hosted Dashboard and NLX alerts you to potential bad actors that have been identified elsewhere in the subscriber network.

Signal Sciences Cloud DDoS

Signal Sciences Cloud DDoS (Cloud DDoS) is an always-on service integrated in the Cloud WAF infrastructure that examines inbound traffic to detect and mitigate DDoS attacks before they reach the applications and origin servers that you specify. Cloud DDoS uses automated mitigation techniques to stop common network protocol-based floods including SYN floods and reflection attacks using UDP, DNS, NTP, and SSDP. Cloud DDoS requires no additional installation or maintenance.

Signal Sciences Hosted Dashboard

The Signal Sciences Hosted Dashboard (Hosted Dashboard) is a web interface that you can use to investigate anomalous web traffic and see what actions, if any, Cloud WAF performed in response to certain requests. You can also use the Hosted Dashboard to create Workspaces. A Workspace is a user-defined set of rules and settings for applications and origin servers. The Hosted Dashboard allows you to create multiple Workspaces to differentiate between one or more APIs, microservices, or web applications. For each Workspace, you can use the Hosted Dashboard to add rules for requests, configure site alert thresholds, and add integrations to other systems.

API

The Signal Sciences Application Programming Interface (API) allows you to integrate your applications and services with the Cloud WAF. It uses standard HTTP response codes and verbs to allow you to programmatically control all the same features that are available through the Hosted Dashboard. The Signal Sciences API provides a variety of endpoints that we document in our API

reference documentation.

Control over data sharing

Cloud WAF gives you control over data shared with Fastly. The Hosted Services (defined below) component of Cloud WAF does not create copies of or store your data as it passes through. The security components of Cloud WAF do not require transmission or collection of any sensitive or personally identifiable information to function other than IP addresses that are identified as the initiator of anomalous or suspicious requests and related metadata. The hosted agents and modules are designed to automatically redact other sensitive or personally identifiable information in fields that are known to commonly contain sensitive or personally identifiable information before transmission to Fastly. Also, the hosted agents and modules allow you to manually configure them via the Hosted Dashboard to redact any sensitive information or other information not needed to be transmitted to Fastly, other than the limited data required for the functionality of the security components of Cloud WAF. Together, the full data stream going through Cloud WAF is not copied or retained by Fastly, and, if properly configured, the portion of that data stream that is evaluated by the security components of Cloud WAF and shared with Fastly will not include your sensitive information other than the IP addresses identified as the initiator of anomalous or suspicious requests.

Documentation

We provide documentation for the Cloud WAF in the Signal Sciences Help Center.

Billing

We bill you as specified in your applicable ordering document, according to the number of Workspaces, the average requests per second (RPS) processed by the Cloud WAF, and the overall traffic flowing through the Hosted Services (defined below) in terabytes (TBs). We measure months according to Coordinated Universal Time (UTC).

Subscriber responsibilities

As a Subscriber, you can identify and maintain up to five points of contact for support communications. All support requests must be initiated from and communicated through the designated points of contact.

Support channels and response times

Fastly provides customer support via the support channels listed below.

Support tickets

Cloud WAF includes access to a support portal that allows you to submit requests for support online, update existing support tickets, and track the status of support tickets. As part of submitting a request via the support portal, you may designate a proposed severity level for the issue being reported, but the ultimate classification of a request will be determined by Fastly based on various factors including input you provide.

Email

Fastly's technical support staff can be contacted via support@signalsciences.com during standard business hours. All support tickets generated by email will be designated with a P2 severity level.

Response times

The following table summarizes the response times based on the severity of the reported issue.

Severity Level	Description	Response Time	Updates
P0	**Urgent - Critical Impact:** A Confirmed Error in a production environment makes the solution, its features, or its functionality completely unavailable to users.	60 minutes or less (24/7/365)	Every 2 hours (24/7/365)
P1	**High - Serious Impact:** A Confirmed Error in a production environment causes significant loss functionality for a primary feature of the solution that has notable impacts to customer business.	4 business hours	Every 12 business hours

Severity Level	Description	Response Time	Updates
P2	**Normal - Minor Impact:** A Confirmed Error in a production environment causes partial loss of functionality of a non-significant feature or a significant cosmetic issue with the web interface. Any errors in a non-production environment are identified.	1 business day	Every 4 business days
P3	**Low - Minor Impact:** Minor cosmetic issues with the web interface are identified. Also applicable to feature requests and general questions about functionality.	2 business days	Not applicable

Definitions

- **Business Hours** are 4 AM-7 PM Monday through Friday, Pacific Time.
- **Business Days** are Monday through Friday, except standard Fastly holidays.
- **Confirmed Error** is any failure of the Cloud WAF to meet Fastly's specifications outlined in the relevant documentation, found in production uses of Cloud WAF, and that can reasonably be reproduced by Fastly.

SLA

Fastly endeavors to maintain 99.9% availability of the Cloud WAF and the Hosted Dashboard.

SLA for Hosted Services

Subscribers experiencing unavailability of the hosted infrastructure component of Cloud WAF (Hosted Services) will be entitled to service credits according to the following table.

Monthly Availability of Hosted Services	Service Credit % of Pro-rated Monthly Cloud WAF Subscription Fees
<99.9-99.0	5%
<99.0%-98.5%	10%
<98.5%-98.0%	15%
<98.0%	20%

"Availability" of the Hosted Services is calculated as follows: ([# of minutes in month]-[# of minutes per month the Hosted Services is Unavailable]) / [# of minutes in month].

"Unavailable" with respect to the Hosted Services means the Hosted Services are not available to process traffic or communicate with Hosted Dashboard, excluding (a) unavailability caused by issues not under Fastly Control or (b) unavailability that does not last for a consecutive ten-minute period.

"Fastly Control" means elements entirely under Fastly's control and not a consequence of (a) Subscriber or third party hardware or software failures, (b) Subscriber or end user connectivity issues, (c) Subscriber operator errors, (d) alteration, modification, unauthorized or misuse of Fastly products, or use not in accordance with the documentation, (e) corrupted Subscriber content, or (f) acts of god (any) or war, or earthquakes, or terrorist actions.

SLA for Hosted Dashboard

Subscribers experiencing unavailability of the Hosted Dashboard will be entitled to service credits according to the following table.

Monthly Availability of Hosted Dashboard	Service Credit % of Pro-rated Monthly Cloud WAF Subscription Fees
<99.9-99.0	5%
<99.0%-98.5%	10%
<98.5%-98.0%	15%
<98.0%	20%

"Availability" of the Hosted Dashboard is calculated as follows: ([# of minutes in month]-[# of minutes per month the Hosted Dashboard is Unavailable]) / [# of minutes in month].

"Unavailable" with respect to the Hosted Dashboard means the Hosted Dashboard is not available for your access and use through your internet connection, excluding (a) unavailability of the Hosted Dashboard caused by issues not under Fastly Control or (b) unavailability that does not last for a consecutive ten-minute period.

Credit terms

- You must contact us within 15 days of experiencing unavailability to receive a service credit.
- For any given month, the maximum amount of any credit is 20%, regardless of the reason it is owed.
- A pending credit does not release Subscriber from its obligation to pay Fastly's submitted invoices in full when due.
- Credits will be applied to the invoice two months following the month an invoice credit was incurred.

Limitations

All WAF products that exist today, including the Cloud WAF, have several limitations:

- **False positives.** Any WAF can mistake good traffic for bad. We strongly recommend you monitor your traffic via the Hosted Dashboard for a minimum of two weeks before blocking traffic. You don't want to start blocking traffic with configurations that are generating false positives.
- **Custom application vulnerabilities.** If attackers discover a vulnerability unique to your application or the technologies you use, and if your WAF configuration does not have a rule to protect against exploits for that particular vulnerability, it will not be able to protect your application in that instance.
- **Inspection of HTTP and HTTPS traffic only.** A WAF only inspects HTTP or HTTPS requests (layer 7). It will not process any TCP, UDP, or ICMP requests.
- **Security products note.** No security product, such as a WAF or DDoS mitigation product, including those security services offered by Fastly, will detect or prevent all possible attacks or threats. Subscribers should maintain appropriate security controls on all web applications and origins, and the use of Fastly's security products do not relieve subscribers of this obligation. Subscribers should test and validate the effectiveness of Fastly's security services to the extent possible prior to deploying these services in production, and continuously monitor their performance and adjust these services as appropriate to address changes in the Subscriber's web applications, origin services, and configurations of the other aspects of the Subscriber's Fastly services.

This article describes a product that may use third-party cloud infrastructure to process or store content or requests for content. For more information, see the section on cloud infrastructure, data center, and physical security.

Signal Sciences Next-Gen WAF

https://docs.fastly.com/products/signal-sciences-next-gen-waf

The Signal Sciences Next-Gen WAF (Next-Gen WAF) is an application security monitoring system that monitors for suspicious and anomalous web traffic and protects against attacks directed at the applications and origin servers that you specify. The system is comprised of three components:

- a monitoring agent
- a web server integration module
- our cloud-hosted collection and analysis system (cloud analysis system)

The module and agent run on your web servers within your infrastructure, analyzing and acting on suspicious traffic in real-time. Anomalous request data is collected locally and uploaded to our cloud analysis system, allowing us to perform out-of-band analysis of inbound traffic.

Next-Gen WAF

The Next-Gen WAF requires modifications to your applications and origin servers. You must install the Signal Sciences Agent. We also recommend that you install the optional Signal Sciences Module, an architecture component that passes request data to the agent.

When the module and agent determine that an incoming request is anomalous, a snippet of that request is sent to the cloud analysis system. This system aggregates data from across all of your agents. When enough attacks are seen from an IP address, the cloud analysis system determines whether to allow the request, block the request, tag the request with signals, flag the IP address, or rate limit the IP address. You can choose to enable or disable the blocking feature.

Threat Intelligence

As part of Next-Gen WAF, we aggregate the attack data collected from your agents and combine it with data collected from security and other services offered as part of the Fastly platform, including for other subscribers. We use these data insights (Threat Intelligence) to analyze and detect potential future anomalies or attacks and to improve, secure, provide, and market Fastly services in a manner that does not associate the Threat Intelligence with or identify any subscriber. For example, you receive the benefits of this Threat Intelligence via the Network Learning Exchange (NLX) feature that adds a unique signal to information in the Hosted Dashboard and NLX alerts you to potential bad actors that have been identified elsewhere in the subscriber network.

Signal Sciences Agent

The Signal Sciences Agent is a required small daemon process that provides an interface between your web server and our cloud analysis system. The agent decides whether inbound requests should be permitted to continue or whether action should be taken. You are responsible for installing and maintaining the Signal Sciences Agent.

Signal Sciences Module

The Signal Sciences Module is an optional architecture component that passes request data to the agent. The module can exist as a plugin to your web server or a language or framework specific implementation. You can remove the module if you run the agent in reverse proxy mode. You are responsible for installing and maintaining the Signal Sciences Module.

Signal Sciences Hosted Dashboard

The Signal Sciences Hosted Dashboard (Hosted Dashboard) is a web interface that you can use to investigate anomalous web traffic and see what actions, if any, Next-Gen WAF performed in response to certain requests. You can also use the Hosted Dashboard to create Workspaces. A Workspace is a user-defined set of rules and settings for applications and origin servers. The Hosted Dashboard allows you to create multiple Workspaces to differentiate between one or more APIs, microservices, or web applications. For each Workspace, you can use the Hosted Dashboard to add rules for requests, configure site alert thresholds, and add integrations to other systems.

API

The Signal Sciences Application Programming Interface (API) allows you to integrate your applications and services with the Next-Gen WAF. It uses standard HTTP response codes and verbs to allow you to programmatically control all the same features that are available through the Hosted Dashboard. The Signal Sciences API provides a variety of endpoints that we document in our API reference documentation.

Control over data sharing

Next-Gen WAF gives you control over data shared with Fastly. Next-Gen WAF does not require transmission or collection of any sensitive or personally identifiable information to function other than IP addresses that are identified as the initiator of anomalous or suspicious requests and related metadata. The agents and modules are designed to automatically redact other sensitive or personally identifiable information in fields that are known to commonly contain sensitive or personally identifiable information before transmission to Fastly. Also, the agents and modules allow you to manually configure them via the Hosted Dashboard to redact any sensitive information or other information not needed to be transmitted to Fastly, other than the limited data required for the functionality of the Next-Gen WAF. If properly configured, none of your sensitive information other than the IP addresses identified as the initiator of anomalous or suspicious requests will be shared with Fastly.

Documentation

We provide documentation for the Next-Gen WAF in the Signal Sciences Help Center. Release notes for the agents and modules are also provided in the Signal Sciences Help Center.

Billing

We bill you as specified in your applicable ordering document, according to the number of Workspaces and the average requests per second (RPS) processed by Next-Gen WAF. We measure months according to Coordinated Universal Time (UTC).

Subscriber responsibilities

From time to time, we may provide error corrections, bug fixes, software updates, and software upgrades to the Signal Sciences Agent and/or the Signal Sciences Module (Updates). Notices about Updates are included in the Documentation and they are also described in the Release notes. You can also subscribe to receive emails from us when Updates are released, or subscribe to our

integrations with third-party tools (e.g., Slack or Microsoft Teams). It is your responsibility to ensure that you are using the most recent version of the Next-Gen WAF components.

As a Subscriber, you can identify and maintain up to five points of contact for support communications. All support requests must be initiated from and communicated through the designated points of contact.

Subject to the terms of any open source license applicable to any Fastly software installed in your environment (namely the agents and modules), your subscription for Next-Gen WAF does not include permission to modify the software or create derivative works based upon the software other than as set forth in the Documentation.

Support channels and response times

Fastly provides customer support via the support channels listed below.

Support tickets

Next-Gen WAF includes access to a support portal that allows you to submit requests for support online, update existing support tickets, and track the status of support tickets. As part of submitting a request via the support portal, you may designate a proposed severity level for the issue being reported, but the ultimate classification of a request will be determined by Fastly based on various factors including input you provide.

Email

Fastly's technical support staff can be contacted via support@signalsciences.com during standard business hours. All support tickets generated by email will be designated with a P2 severity level.

Response times

The following table summarizes the response times based on the severity of the reported issue.

Severity Level	Description	Response Time	Updates
P0	**Urgent - Critical Impact:** A Confirmed Error in a production environment makes the solution, its features, or its functionality completely unavailable to users.	60 minutes or less (24/7/365)	Every 2 hours (24/7/365)
P1	**High - Serious Impact:** A Confirmed Error in a production environment causes significant loss functionality for a primary feature of the solution that has notable impacts to customer business.	4 business hours	Every 12 business hours
P2	**Normal - Minor Impact:** A Confirmed Error in a production environment causes partial loss of functionality of a non-significant feature or a significant cosmetic issue with the web interface. Any errors in a non-production environment are identified.	1 business day	Every 4 business days
P3	**Low - Minor Impact:** Minor cosmetic issues with the web interface are identified. Also applicable to feature requests and general questions about functionality.	2 business days	Not applicable

Definitions

- **Business Hours** are 4 AM-7 PM Monday through Friday, Pacific Time.
- **Business Days** are Monday through Friday, except standard Fastly holidays.
- **Confirmed Error** is any failure of the Next-Gen WAF to meet Fastly's specifications outlined in the relevant documentation, found in production uses of Next-Gen WAF, and that can reasonably be reproduced by Fastly.

SLA

Fastly endeavors to maintain 99.9% availability of the Hosted Dashboard. Subscribers experiencing unavailability of the Hosted Dashboard will be entitled to service credits according to the following table.

Monthly Availability of Hosted Dashboard	Service Credit % of Pro-rated Monthly Next-Gen WAF Subscription Fees
<99.9-99.0	5%

Monthly Availability of Hosted Dashboard	Service Credit % of Pro-rated Monthly Next-Gen WAF Subscription Fees
<99.0%-98.5%	10%
<98.5%-98.0%	15%
<98.0%	20%

"Availability" of the Hosted Dashboard is calculated as follows: ([# of minutes in month]-[# of minutes per month the Hosted Dashboard is Unavailable]) / [# of minutes in month].

"Unavailable" with respect to the Hosted Dashboard means the Hosted Dashboard is not available for your access and use through your internet connection, excluding (a) unavailability of the Hosted Dashboard caused by issues not under Fastly Control or (b) unavailability that does not last for a consecutive ten-minute period.

"Fastly Control" means elements entirely under Fastly's control and not a consequence of (a) Subscriber or third party hardware or software failures, (b) Subscriber or end user connectivity issues, (c) Subscriber operator errors, (d) alteration, modification, unauthorized or misuse of Fastly products, or use not in accordance with the documentation, (e) corrupted Subscriber content, or (f) acts of god (any) or war, or earthquakes, or terrorist actions.

Credit terms

- You must contact us within 15 days of experiencing unavailability to receive a service credit.
- For any given month, the maximum amount of any credit is 20%, regardless of the reason it is owed.
- A pending credit does not release Subscriber from its obligation to pay Fastly's submitted invoices in full when due.
- Credits will be applied to the invoice two months following the month an invoice credit was incurred.

Limitations

All WAF products that exist today, including the Next-Gen WAF, have several limitations:

- **False positives.** Any WAF can mistake good traffic for bad. We strongly recommend you monitor your traffic via the Hosted Dashboard for a minimum of two weeks before blocking traffic. You don't want to start blocking traffic with configurations that are generating false positives.
- **Custom application vulnerabilities.** If attackers discover a vulnerability unique to your application or the technologies you use, and if your WAF configuration does not have a rule to protect against exploits for that particular vulnerability, it will not be able to protect your application in that instance.
- **Inspection of HTTP and HTTPS traffic only.** A WAF only inspects HTTP or HTTPS requests (layer 7). It will not process any TCP, UDP, or ICMP requests.
- **Security products note.** No security product, such as a WAF or DDoS mitigation product, including those security services offered by Fastly, will detect or prevent all possible attacks or threats. Subscribers should maintain appropriate security controls on all web applications and origins, and the use of Fastly's security products do not relieve subscribers of this obligation. Subscribers should test and validate the effectiveness of Fastly's security services to the extent possible prior to deploying these services in production, and continuously monitor their performance and adjust these services as appropriate to address changes in the Subscriber's web applications, origin services, and configurations of the other aspects of the Subscriber's Fastly services.

This article describes a product that may use third-party cloud infrastructure to process or store content or requests for content. For more information, see the section on cloud infrastructure, data center, and physical security.

Signal Sciences professional services

https://docs.fastly.com/products/signal-sciences-professional-services

Signal Sciences professional services provide your organization with training, implementation, and maintenance services for the Signal Sciences Cloud WAF and Next-Gen WAF. Depending on the service offerings you select, our team will provide training and work with you to plan, test, deploy, and maintain a solution to protect your applications and origin servers. All Signal Sciences professional services are designed to be delivered remotely and can be purchased a la carte or in bundles.

A la carte services

The following services can be purchased a la carte.

Implementation services

Fastly can help you implement a solution using the Cloud WAF or Next-Gen WAF. Implementation services include personalized meetings to help you plan and deploy a customized solution for your applications and origin servers. Fastly will help you test your configuration prior to deployment.

Training services

Fastly can provide two different types of training sessions for up to 15 people in your organization. The introductory session teaches skills for using Signal Sciences products and provides real-world examples. The advanced session teaches skills for using the Signal Sciences API and troubleshooting the Signal Sciences Agents and Modules.

Managed rules

Managed rules are rules created and managed by Fastly for your organization. Fastly will create and deploy managed rules for your organization after speaking with you about your organization's requirements. Managed rules are sold in packs of five.

Health checks

Fastly can perform a health check of your deployment of Cloud WAF or Next-Gen WAF to ensure that your deployment is in a "good" state and being fully utilized. At your request, our team will speak with you to understand how you currently use the Cloud WAF or Next-Gen WAF and then provide you with an assessment of your deployment with suggestions for improvement.

General services

General services is an hourly service offering (an eight hour minimum) that provides you with access to the Solutions Engineering team.

Essentials subscriptions

Essentials subscriptions are bundles of implementation services, training services, managed rules, and health checks. Depending on the subscription, you may receive access to our team of support engineers.

Continuity Essentials

Continuity Essentials is an annual service offering that provides introductory training and an onboarding call with our team. At your request, Fastly will provide a quarterly review of your implementation and an assessment of your deployment.

TAM Essentials

TAM Essentials is an annual service offering that provides you with access to Shared TAMs. Your organization will receive up to two training sessions and an onboarding call with our team. At your request, Fastly will provide a quarterly review of your implementation and an assessment of your deployment. Our team will also provide a roadmap session and review all of your organization’s open support cases, bugs, and feature requests.

Strategic TAM Essentials

Strategic TAM Essentials is an annual service offering that provides access to a designated TAM with access to the TAM enterprise team for additional support as needed. Your organization will receive up to four training sessions, including self-paced and instructor-led sessions, an onboarding call with our team, and a monthly check-in call. At your request, Fastly will provide a quarterly review of your implementation and an assessment of your deployment. Our team will also provide a roadmap session and review all of your organization’s open support cases, bugs, and feature requests.

Resources

These articles provide information about Fastly's product lifecycle and the products within it.

https://docs.fastly.com/products/product-resources

Fastly product lifecycle

https://docs.fastly.com/products/fastly-product-lifecycle

https://docs.fastly.com/products/fastly_product_lifecycle

Fastly releases or retires its products and features as detailed below.

Product and feature releases

We release our products and features in the following stages.

Beta

Beta products are initial releases of potential future products or features. We provide customers who participate in our Beta program the opportunity to test, validate, and provide feedback on future functionality. Feedback gathered during this phase helps us to determine which features and functionality provide the most value to our customers and helps us focus our efforts accordingly.

These guidelines apply to Fastly's Beta program:

- Customers can choose or elect to participate in a Beta program.
- Fastly does not make any promises on the features, functionality, or performance of our Beta products.
- We reserve the right to change the scope of or discontinue a Beta product or feature at any point in time.
- We do not charge our subscribers for using our Beta products or features.
- Beta products or features are not included in any existing support contracts or obligations.
- Fastly does not provide Beta customers with discounts on future purchases of any products or services.
- Fastly strongly advises against using production traffic for Beta products due to their dynamic nature.

Beta services are covered by Section 6 of our Terms of Service.

Limited Availability

Limited Availability products are ready to be released to the world, pending some fine tuning. Limited Availability allows us to test out a product or service with a limited number of customers, so we can closely monitor it and make any necessary adjustments before rolling it out more broadly. Our goal is to make it easy for customers to set up our products with their services and take advantage of the features that come along with them.

These guidelines apply to Fastly's Limited Availability program:

- Fastly may charge its Limited Availability customers and pricing may vary depending on features.
- Fastly does not make any promises on the features, functionality, or performance of our Limited Availability products.
- Fastly does not provide its Limited Availability customers with discounts on future purchases of any products or services.
- Fastly does provide limited product and customer engineering support and documentation for Limited Availability products.

General Availability

General Availability products released by Fastly are available for everyone's use. Fastly manages these products in accordance with Fastly's terms and conditions.

Product or feature retirement

The decision to retire or deprecate Limited Availability or General Availability features always follows a rigorous process including understanding the demand, use, impact of feature retirement and, most importantly, customers' feedback. Our goal is to always invest resources in areas that will add the most value for customers. When low-value functionality or less successful features compete for resources or create confusion, we may decide that retirement or deprecation is the best solution. In the most difficult of scenarios, feature retirement may cause temporary challenges for some customers. Focusing on the highest priorities of the greatest number of customers, however, allows us to continue to deliver a superior solution with the most benefit.

Fastly is committed to transparency in everything we do, particularly when that activity has implications on the functionality of our features or platform. In the interest of building trust and clarifying change, we have established a number of guidelines around communication of feature retirement, end-of-life, and deprecation.

When a decision to retire a feature is reached Fastly will strive to provide:

- **Advance notice:** We will provide notification proportional to feature criticality. For minor changes with improved functionality we will notify customers no less than three (3) months prior to deprecation, and for major changes we will notify no less than six (6) months in advance.
- **Alternative functionality:** We will include guidance and direction on new features in our services which replace retired or deprecated functionality. New features and functionality will always be provided in advance to ensure customers have time to understand and transition to new functionality prior to the retirement of previous functionality. In some cases this may be with partners or other approved third-party services.

- **Continuous support:** Fastly commits to providing continuous support for all features until the retirement date.
- **Considerate scheduling:** When planning significant changes, including feature or product retirement, we will align retirement as close to major updates or releases as possible to limit the scope of impact on your services.

In some extreme cases Fastly may need to accelerate the retirement of functionality timeline:

- Essential changes that are necessary or appropriate to protect the integrity of our service may occasionally be required. In these cases, it is important that those changes occur as quickly as possible. We will communicate with customers transparently with as much advance notice as possible in these situations.
- Integrated third-party software or services may need to be retired due to the third-party decision to change or retire their solution. In these situations, the pace of the retirement will be out of our control, although we remain committed to transparency and will strive to provide as much notice as possible.

For more information, contact customer support or your account team.

Summary product definitions

https://docs.fastly.com/products/summary-product-definitions

Fastly defines each of its products as follows. For more information about any of our products, contact sales@fastly.com.

Application Programming Interface

Fastly provides an application programming interface (API) that can be accessed via a number of popular interactive clients and allows you to manage Fastly services via remote procedure calls. These services include features such as authentication, configuration, historical stats, purging, and remote logging. In addition to being accessible via Fastly's API, Fastly services can also be accessed via a web interface for users with the appropriate access permissions; however, API features do not include customer account setup, which can only occur through the web interface controls.

Assurance Services

Assurance Services offers access to third-party audit reports, certification attestations, and unlimited audits of Fastly's security and technology compliance programs. In addition, it provides access to libraries with summary reports of penetration tests, risk assessments, and security policies, as well as an historical archive of security advisories.

Certificate Procurement, Management, and Hosting

Fastly's Certificate Procurement, Management, and Hosting service obtains dedicated Transport Layer Security (TLS) certificates for you. These certificates are serviced using Server Name Indication (SNI) technology, which allows multiple secure websites to be served off the same IP address without requiring those sites to use the same certificate.

Cloud Optimizer Limited Availability

Fastly's Cloud Optimizer product allows you to use Fastly's Full-Site Delivery features without migrating edge delivery traffic to Fastly by designating Fastly as the origin to one or more existing non-Fastly content delivery networks currently serving your infrastructure.

Compute@Edge Limited Availability

Fastly's Compute@Edge is a serverless compute environment that allows you to develop, deploy, and operate serverless applications using Fastly's edge cloud platform. You can use Compute@Edge to write new applications, move critical logic closer to end users, and bring enhanced security and performance to current workflows.

Concierge TLS Limited Availability

Concierge TLS is a packaged addition to Fastly's Enterprise Support service option that includes one hundred (100) TLS enabled domains, as well as advanced TLS support and configuration options for Enterprises.

Consulting Engagement Services

Fastly Consulting Engagement Services provide high levels of expert support and implementation assistance for customers who require in-house expertise or dedicated resources from our Professional Services and Senior Engineering teams.

Customer Support Services

Fastly Customer Support Services provide answers to questions about features of Fastly products and services. Each member of the Fastly support team provides technical support to resolve questions about account configuration, operation, and management. Support availability and response times vary depending on the level of support you have purchased.

Dedicated IP addresses

Fastly's Dedicated Internet Protocol (IP) addresses provide you with a pool of IP addresses across Fastly's global Edge Cloud.

Designated Technical Specialist

Fastly offers the ability to purchase the support of a Cloud Engineer to serve as a Designated Technical Specialist for your organization. These specialists help you optimize your use of Fastly's products and features and provide enhanced troubleshooting coordination with Fastly's support and professional services organizations.

DDoS Protection and Mitigation Service

Fastly's DDoS Protection and Mitigation Service helps protect against volumetric and targeted distributed denial of service attacks against origin servers. It provides overage insurance for unplanned or unexpected traffic patterns, immediate onboarding assistance, emergency configuration and deployment support, ongoing attack mitigation support, and an incident response plan.

Fastly TLS

Fastly TLS provides TLS management using either certificates that customers upload themselves or Fastly-managed certificates generated by a third-party Certification Authority.

Full-Site Delivery

Fastly's Full-Site Delivery uses Fastly's global content delivery capabilities to cache and accelerate the delivery of static, dynamic, and streaming HTTP-based file content. Full-Site Delivery allows you to tailor delivery of content using features like HTTP header manipulation, time-to-live (TTL) settings, purging, origin shielding, and the advanced edge logic capabilities provided via scripting with the Varnish Configuration Language (VCL). Transport Layer Security (TLS) and Always-on DDoS mitigation provide security for Fastly services, with real-time monitoring via the Fastly web interface. Log streaming to a variety of third-party endpoints provides observability. Comprehensive APIs power Fastly's web interface and provide programmatic access to Fastly's Full-Site Delivery features.

High Volume Logging

Fastly's High Volume Logging allows you to increase your real-time log streaming log limit beyond the monthly average of two log statements per request, per service.

HIPAA-Compliant Caching and Delivery

Fastly offers a HIPAA-CompliantCaching and Delivery product that allows you to transmit protected information like protected health information through Fastly's network.

Image Optimizer

Fastly's Image Optimizer product provides real-time image transformation that caches optimized images requested from your origin server. This product may use third-party cloud infrastructure to process or store content or requests for content.

Live Event Monitoring Limited Availability

Fastly's Live Event Monitoring service offers customers the ability to reserve Fastly customer support resources during their scheduled event's specified hours to proactively monitor key availability and performance metrics. It also offers a dedicated chat channel to communicate with Fastly customer support engineers in real-time.

Logging Insights Package

Fastly's Logging Insights Package helps you analyze and interpret your streaming log data. This professional services offering includes a guided customization of preconfigured third-party logging endpoint dashboards tailored to your specific business needs. Fastly assists with advanced queries, customizations, and best practices.

Media Shield for Live

Fastly's Media Shield for Live product offers the ability to decrease origin traffic of live video events or live linear channels by reducing multiple CDN requests into a single request per shield point of presence (POP) back to your origin. Media Shield for Live works with your existing architecture by making Fastly the origin to all of your end-user-serving CDNs.

Media Shield for VOD

Fastly's Media Shield for VOD product offers the ability to decrease origin traffic of video on demand by reducing multiple CDN requests into a single request per shield point of presence (POP) back to your origin. Media Shield for VOD works with your existing architecture by making Fastly the origin to all of your end-user-serving CDNs.

Nearline Cache Limited Availability

Fastly's Nearline Cache allows you to manually or automatically populate and store content in third-party cloud storage near a Fastly POP.

Origin Connect

Fastly's Origin Connect product offers a private network interconnect between your origin servers and your Fastly shield POP.

Partner Support Services

Fastly partners are required to purchase Partner Support Services. These services provide Fastly platform support benefits as well as a library of on-demand training modules.

PCI-Compliant Caching and Delivery

Fastly offers a PCI-Compliant Caching and Delivery product that allows you to transmit protected information like cardholder data through Fastly's network.

Performance Optimization Package

Fastly's Performance Optimization Package provides configuration expertise for analysis and tuning of Fastly services using real-time analytics to identify potential improvements for site performance. This professional services offering includes an assessment, followed by specific recommendations and implementation work.

Platform TLS Limited Availability

Fastly's Platform TLS product allows you to programmatically manage certificates and keys for Transport Layer Security (TLS) using a web API. Use this service if you need to upload thousands or hundreds of thousands of individual X.509 certificates and their associated private keys to Fastly.

Service Implementation

Fastly Service Implementation offers remote planning, customized configurations, testing, and go-live assistance from our Professional Services team for your initial Fastly service implementation and implementation of new Fastly products and services.

Service Management

Fastly Service Management offers ongoing configuration and advanced technical assistance from our Professional Services team on an as-needed basis.

Shared TLS Certificate

Fastly's Shared TLS Certificate service offers customers the option to use their own domains on a shared TLS certificate managed by Fastly. Customers provide one or more hostnames and Fastly administers them using the certificate's Subject Alternative Name (SAN) field.

Shared TLS Wildcard Certificate

Fastly's Shared TLS Wildcard Certificate service offers customers the option to use their own domains on a shared certificate. Customers provide Fastly with one or more wildcard domain entries and Fastly adds them to the certificate SAN field.

Streaming Delivery

Fastly's Streaming Delivery allows you to use Fastly as a globally distributed HTTP streaming network to improve quality of service and increase viewer capacity for both live and Video On Demand (VOD) content. Streaming Delivery provides all the capabilities of Fastly's Full-Site Delivery, but only for HTTP-based media streaming protocols including HTTP Live Streaming (HLS), HTTP Dynamic Streaming (HDS), HTTP Smooth Streaming (HSS), and Dynamic Adaptive Streaming over HTTP (MPEG-DASH). Fastly's Streaming Delivery must be configured in an account separate from other Fastly accounts.

Subscriber Provided Prefix

Fastly's Subscriber Provided Prefix product allows you to have your IP spaces announced, routed, and served by Fastly infrastructure for use with production services. When you purchase this product, you provide your own IP address space to Fastly rather than use Fastly IP addresses. You can then direct traffic to your own IP addresses, which are reachable via HTTP Anycast on Fastly's infrastructure.

Web Application Firewall (WAF)

Fastly's Web Application Firewall (WAF) product offers the ability to detect and block malicious traffic to your origin servers using predetermined rules.

Web Application Firewall (WAF) Quick Start Package

Fastly's WAF Quick Start Package provides you with assistance configuring the initial setup of the Fastly WAF. This professional services offering helps you set up a default policy and configure your WAF in logging mode.

Web Application Firewall (WAF) Tuning Package

Fastly's WAF Tuning Package provide tuning assistance with the configuration of the Fastly WAF. This professional services offering helps you plan your WAF policies and the configuration of the WAF VCL for your Fastly service.

Web Application Firewall (WAF) Tuning Plus Package

Fastly's WAF Tuning Plus Package provides ongoing enhanced professional maintenance of your WAF by Fastly. For each service running WAF, the WAF Tuning Plus Package includes ongoing tuning and configuration services as well as authenticated TLS to origin to help protect you against critical security threats. To purchase the WAF Tuning Plus Package, you must have already purchased and provisioned our WAF product. Once purchased, these professional services continue for the term of your WAF contract.

Legacy offerings

These articles provide information about Fastly's legacy offerings.

https://docs.fastly.com/products/legacy-offerings

Fastly's Legacy Full-site Delivery services

https://docs.fastly.com/products/fastlys-legacy-full-site-delivery-services

IMPORTANT: These terms apply to Subscribers who purchased Full-site Delivery on or before October 8, 2018. For more information about our current Full-Site Delivery, contact sales@fastly.com.

Fastly offers full-site delivery that allows you to speed up websites and mobile apps by pushing content closer to users, providing improved and secure experiences across the world.

HTTP request fulfillment

The Fastly CDN Service responds to HTTP GET requests initiated from end users' using your website, or from a program making calls to an internet-hosted API.

Header support

Fastly's CDN Service supports forwarding HTTP headers to end users when they are received from your origin server. Alternatively, headers can be added, removed, or modified using our edge scripting language either before or after caching a response from the origin. This includes the Cache-Control and Expires headers as well as the Surrogate-Control header. HTTP header support allows you to send one set of instructions to the Fastly cache servers and another set of instructions to downstream caches, such as proxies or browsers. In particular, the Surrogate-Control header allows you to specify how to forward and transform specific header types.

Time to Live support

Fastly has no set hard limit on how long objects will remain cached. Instead, Fastly supports the expiration of content via Time to Live (TTL) settings that you configure. TTL settings work as timers on your cached content. When content has resided in the cache for the entire TTL interval, that content is given the status of "expired." Before Fastly delivers requested content that is expired, the cache checks to see if the content is still valid by checking with your application server first.

If the application server says the content remains unchanged, the cache sets the content's status to "valid" and resets its TTL value. If the object has been changed, it is declared "invalid" because the content has expired. The application server delivers updated content. Fastly's CDN Service caches the updated content with the status of "valid," and its TTL timer begins to run.

The fetch and refresh process may take a second or more, and during that time, a Fastly cache may receive dozens or hundreds of end-user requests for that content. Fastly's request collapsing feature groups these requests and fulfills them at once when the application server response is received.

Fastly offers you the option of setting a global, default TTL for cached content control. When set, Fastly's CDN service caches objects in a consistent manner even when applications are inconsistent in doing so.

Origin shielding

When configuring Fastly's CDN Service during the self-provisioning process, you can designate a specific point of presence (POP) to serve as a shield for your origin servers. This server is referred to as a "shield" because it protects your application servers from continuous requests for content. By default, no origin shield is enabled for you. You must specifically enable shielding to use it.

If Fastly's caches do not have the content being requested, they fetch it from the shield server instead of your origin servers. Fastly caches fetch content from your origin server only when the shield server does not have the content being requested.

Load balancing

You can designate multiple servers as your origin servers. When two or more application servers are provisioned as origin servers, Fastly's CDN Service will distribute requests to fetch content across those application servers. This type of load balancing is enabled by default. You must explicitly disable it if you don't want to use it.

Request collapsing

Cached content sometimes must be refreshed when that content becomes "stale" or expires. When multiple end users request content that is in the process of being refreshed, request collapsing groups those requests to be satisfied together, as soon as the content is received. This accelerates content delivery by keeping Fastly's CDN Service from repeating duplicate requests to your origin server. Request collapsing is enabled by default.

Instant Purge support

Fastly supports an Instant Purge feature that allows you to actively invalidate content. Rather than requiring your network operations and application staff to guess how frequently each bit of content may change, Fastly allows you to generate an HTTP Purge method that is sent to the CDN Service whenever an application changes or deletes data in its database. The Fastly CDN Service invalidates the associated content throughout the service's cache network, causing a new version of that content to be retrieved from the application server the next time it is requested.

Fastly allows URL-based and key-based purging, as well as purging of all content at once via specific, configurable purging commands. Fastly currently supports Ruby, Python, PHP, and Perl libraries for instant purging.

When purging by URL or surrogate key, Fastly's CDN Service can process thousands of changes per second. The invalidation process takes less than 300 milliseconds, making it possible to deliver dynamic content that changes rapidly and unpredictably. Using Instant Purge, you can eliminate cache-to-origin HTTP traffic that all other CDN services generate to determine if expired objects are still valid.

Health checks

You have the option to configure Fastly's CDN Service to perform health checks on your application servers and measure their responsiveness. You can use health check responsiveness measurements to fine-tune the distribution of fetch requests. Health checks are not enabled by default. You must specifically enable them.

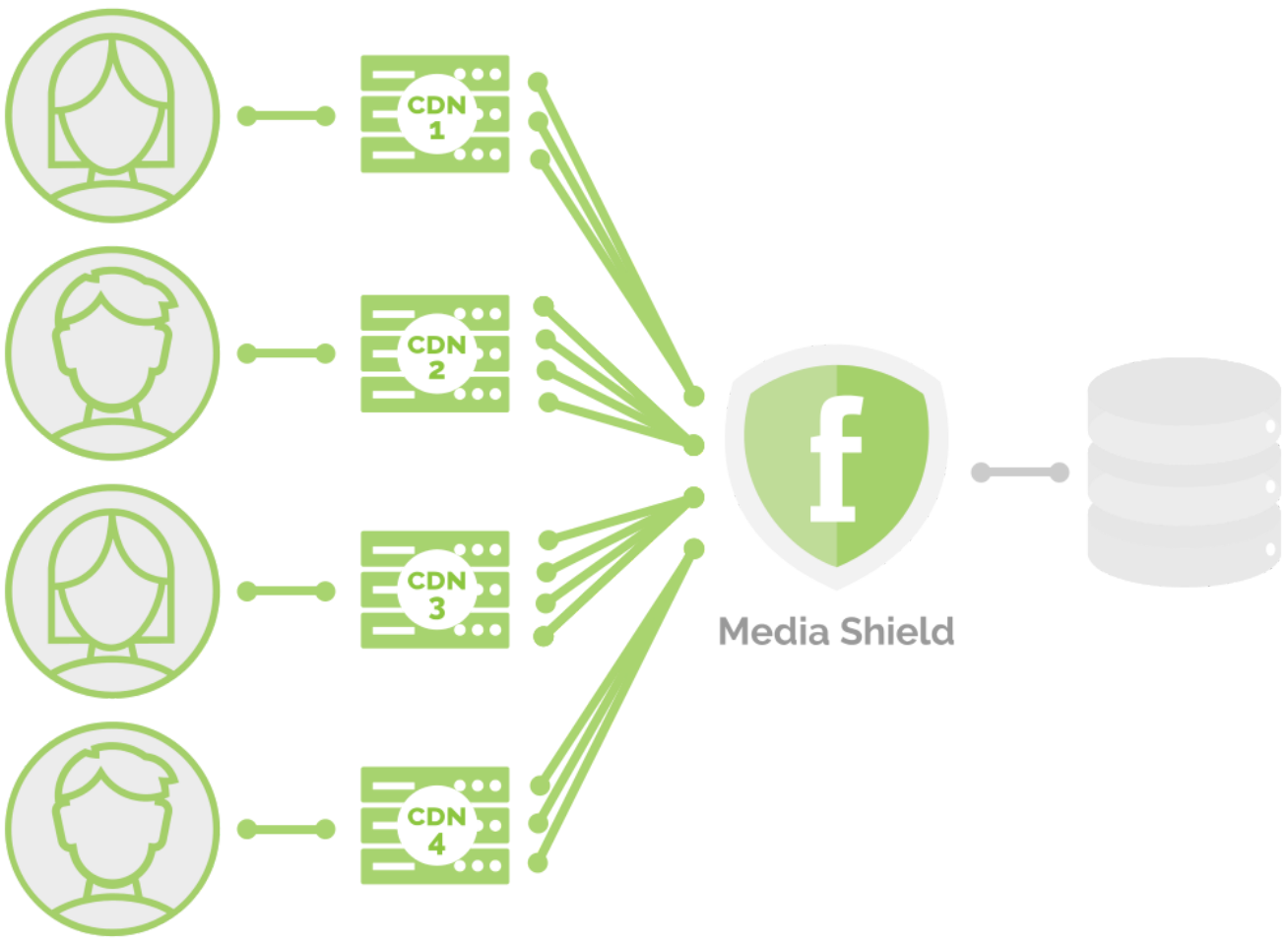
Grace mode support

When an application server becomes unavailable for any reason, end users will normally receive error messages indicating the content they've requested cannot be retrieved. When enabled, grace mode shields application servers by instructing Fastly's CDN Service to continue to serve stale or expired (but likely still valid) content to end users for a set amount of time. This allows you to return otherwise unavailable application servers to normal operations and still serve content rather than error messages to end users. By default, grace mode is not configured. You must specifically configure you service to serve stale content to use grace mode.

Fastly's Legacy Media Shield

https://docs.fastly.com/products/fastlys-legacy-media-shield

IMPORTANT: These terms apply to Subscribers who purchased Media Shield on or before September 12, 2019. For more information about our current Media Shield product, contact sales@fastly.com.



Fastly Media Shield offers customers the ability to decrease origin traffic by reducing multiple CDN requests into a single request back to your origin. Media Shield works with your existing architecture by making Fastly the origin to all of your end-user-serving CDNs.

To learn more about Fastly's Media Shield, contact your account manager or email sales@fastly.com for more details.

IMPORTANT: This information is part of a limited availability release. For more information, see our product and feature lifecycle descriptions.

Legacy Certificate Procurement, Management, and Hosting Service

https://docs.fastly.com/products/legacy-certificate-procurement-management-and-hosting-service

NOTE: Fastly maintains support for its original Certificate Procurement, Management, and Hosting Service. For more information about our current TLS service options, contact sales@fastly.com.

IMPORTANT: As part of our previously announced planned retirement of Certificate Procurement, Management, and Hosting Service, Fastly has begun working with customers to migrate procured certificates to Fastly TLS. Fastly TLS offers an associated web interface and API with similar functionality to the retired products. We will continue to support procured certificates for existing customers during this migration. Our support team will contact you to schedule individual migrations and can be emailed at fastlytlsupdates@fastly.com for general questions.

Fastly offers a Certificate Procurement, Management, and Hosting Service where we purchase dedicated TLS certificates on your behalf, then host and manage them for you. Specifically:

- Each certificate purchased will support 2,500 bytes of SAN entries up to a maximum of 150 SAN entries.
- When the limits on any purchased certificate are reached, Fastly will purchase an additional one for you with the same limits, managing and hosting it on your behalf.
- All certificates will be served using SNI technology.
- All new SAN entries require you to verify your control of the domains requested.
- You manage additions and removals of SAN entries using our web interface.

Legacy Customer-Provided TLS Certificate Hosting Service

https://docs.fastly.com/products/legacy-customer-provided-tls-certificate-hosting-service

NOTE: Fastly maintains support for its original Customer-Provided TLS Certificate Hosting Service. For more information about our current TLS service options, contact sales@fastly.com.

Fastly offers a Customer-Provided TLS Certificate Hosting Service where you provide TLS certificates and private keys which we then install at a shared set of IP addresses. Each are selected using the SNI extension of TLS that allows clients to present a hostname in the TLS handshake request. Choose this option if you have requirements that prevent you from using the Fastly TLS interface to upload your TLS certificates and private keys personally.

To purchase this option, contact sales@fastly.com.

Legacy Platinum Support and SLA

https://docs.fastly.com/products/legacy-platinum-support-and-sla

NOTE: Fastly maintains support for its original Platinum Support plan. For more information about our current Gold and Enterprise Support plans or for information about our Professional Services packages, contact sales@fastly.com.

Legacy Platinum Support description and SLA

Support availability and response times vary depending on the type of account you have and the level of support you have purchased. The following table summarizes those offerings:

Support Offering	Platinum Support
Online Self-Service Help	Unlimited access.
Availability for General Inquiries	24/7/365.
Availability for Incident Reports	24/7/365.
Initial Response Times	Severity 1 Incidents within 15 minutes. Severity 2 Incidents within 2 hours. All other Incidents by the next business day.
Email support	Available, with priority over Standard and Gold Support.
Phone and chat support	Toll-free telephone available 24/7/365. Dedicated chat channel available during Fastly business hours.
Emergency Escalation	Available via email and phone.

Support Offering	Platinum Support
Designated Customer Support Engineer	Available for large accounts on case-by-case basis.
Termination Option	Available with invoice credits.

Technical support

The following section applies to all subscribers.

Definitions

- **"Business Hours"** are 8AM-6PM during a Business Day in California, New York, London, or Tokyo.
- **"Business Days"** are Monday through Friday, excluding any day that is simultaneously a US, UK, and Japanese national or banking holiday.
- An **"Incident"** is an occurrence during which end users' use of Subscriber's services is adversely impacted.
- A **"Severity 1 Incident"** is an incident resulting in a major service outage requiring Subscriber to redirect all traffic from Fastly to another CDN.
- A **"Severity 2 Incident"** is an incident resulting in minor or intermittent outage not requiring Subscriber to redirect traffic to another CDN.
- **"Fastly Control"** means elements entirely under Fastly's control and not a consequence of (a) a Subscriber's hardware or software failures, (b) a Subscriber's or end user's connectivity issues, (c) Subscriber operator errors, (d) Subscriber traffic amounts that exceed a Subscriber's Permitted Utilization as defined in the Terms and Conditions, (e) corrupted Subscriber content, (f) acts of god (any) or war, or earthquakes, or terrorist actions.

Subscriber responsibilities

Subscriber is responsible using and configuring services according to the Documentation available at https://docs.fastly.com.

Support requests

Subscribers submit support requests by sending email to support@fastly.com. Subscribers receive a system-generated response within minutes containing the ticket number and a direct link to the ticket.

Incident reports should include at the least the following:

- Services are not responding to end user requests.
- Services incorrectly send end users error condition messages.
- Services send incorrect or partial content to end users.

Incident reports should include all relevant information such as:

- Subscriber's determination of the Severity Level of the incident,
- Subscriber hardware failures,
- Subscriber operator errors,
- Services configuration errors made by Subscriber employees,
- A potential Utilization Spike (see the Service Availability SLA),
- Corrupted Subscriber content,
- DDOS attacks, and
- Relevant *force majeure* acts such as extreme weather, earthquakes, strikes or terrorist actions.

Communications

Tickets

Communications between Fastly support engineers and Subscriber personnel are conducted using the ticketing application, which maintains a time-stamped transcript of communications, and sends emails to Subscriber and Fastly staff as tickets are updated.

Chat

Subscribers to Platinum Support receive a dedicated chat channel for real-time communications during Business Hours. Though subject to change, Fastly's current chat provider is Slack (www.slack.com).

Phone support

Subscribers to Platinum Support receive a dedicated phone number to contact Fastly support engineers. Fastly personnel can also establish audio and video conferencing (free app or browser plug-in required) for real-time voice and video communications.

Response time

Fastly shall use best efforts to respond in a timely fashion.

Termed contracts

The following applies to any subscriber that has a contract with a term and a minimum commitment.

Response times

Fastly commits to acknowledging receipt of a support ticket within the next Business Day following submission of a support request by a Subscriber with a Termed Contract.

Termination

In any three-month period where three (3) or more support Response Time objectives are not met and the failure to meet the objectives materially adversely impacted Subscriber, Subscribers with a Termed Contract, Platinum Support shall have thirty (30) days to terminate their subscription agreement following the third failure.

Incident response times

Incident reporting

Severity 1 Incidents: Fastly will provide Subscriber an Incident Support Email address for Subscriber to report Incidents. Subscriber should report Incidents promptly using the Incident Support email.

Severity 2 Incidents: Subscriber should report Severity 2 Incidents by submitting a Support Request.

Platinum Support

Fastly will respond to the report of an Incident by troubleshooting the cause(s) of the Incident and resolve them if caused by factors within Fastly's control, or provide information to those who can resolve the factors if the factors are within others' control, as follows:

For a Severity 1 Incident:

- Fastly support staff will acknowledge receipt of the email within 15 minutes.
- Fastly will start actively troubleshooting within 30 minutes of receipt of the email.
- Fastly will perform its tasks on a 24/7 basis.
- Fastly and Subscriber will immediately communicate upon learning new information that may be useful in troubleshooting the incident, and status updates between Fastly and Subscriber staff will take place no less frequently than every 30 minutes for the first two hours, and no less frequently than every hour thereafter.
- Fastly staff will work until (a) the incident is resolved or (b) the incident is believed to be outside of Fastly's control.

For a Severity 2 Incident:

- Fastly support staff will acknowledge receipt of the email within two hours.
- Fastly engineers will begin actively troubleshooting within the same day, will work on the Incident during the same day, and will provide status updates to Subscriber daily on each subsequent day.

Support invoice credits

In the event a Severity 1 Incident occurs, Subscriber has purchased Platinum Support, the cause of the Incident is within Fastly's control, and any of the communication or response timeframes are materially not met, a one-time credit of $500 per incident will be credited to Subscriber's account.

Credit Terms:

- Requests for Invoice Credits must be made within 30 days of the incident which triggered the service credit.
- In no event shall Invoice Credits exceed the invoice value of the month in which they are accrued.
- A pending credit does not release Subscriber from its obligation to pay Fastly's submitted invoices in full when due.
- Credits will be applied to the invoice two months following the month an invoice credit was incurred.

Legacy Service availability SLA

Support availability and response times vary depending on the type of account you have and the level of support you have purchased.

Agreement Type	Unpaid Account	Month-to-Month Account	Termed Contract	Platinum Support
Service Level Agreement	None	None	Termination Option	Invoice Credits + Termination Option

Definitions

"Degraded Performance" means the Services are experiencing Error Conditions that are (1) caused by issues under Fastly Control, (2) observable or reproducible by Subscriber or Fastly, (3) requiring Subscriber to redirect traffic off the Services. Degraded Performance does not include any reduction on availability of the Application User Interface or API due to maintenance.

"Error Condition" means the Services are (1) not responding to end user requests, (2) incorrectly sending end users error condition messages or (3) sending incorrect partial content to end users and these conditions are observable or reproducible by Subscriber or Fastly.

"Fastly Control" means elements entirely under Fastly's control and not a consequence of (a) Subscriber hardware or software failures, (b) Subscriber or end user connectivity issues, (c) Subscriber operator errors, (d) a Utilization spike (see below), (e) corrupted Subscriber content, (f) acts of god (any) or war, or earthquakes, or terrorist actions.

Termination

Any Subscriber that has a contract with a term and a minimum commitment shall have thirty (30) days to terminate their subscription agreement following (1) a period of Degraded Performance longer than 7.2 hours in any one month, or (b) three contiguous months that have periods of Degraded performance longer than 43.8 minutes each.

Availability invoice credits

Subscribers who purchase Platinum Support shall be entitled to Invoice Credits according to the following table.

Availability Percent	Period of Degraded Performance	Monthly Credit Percent
Below 100% - 99.99%	Up to 4.32 minutes	1%
99.99% – 99.9%	Up to 43.8 minutes	5%
99.89% – 99.0%	Up to 7.2 hours	10%
98.99% - 98.0%	Up to 14.4 hours	25%
Below 97.99%	Greater than 864 minutes	50%

Invoice Credits for unavailability will accrue on a monthly basis. The Credit Amount for a month is equal to the monthly usage charge multiplied by Monthly Credit Percent.

Credit terms

- Requests for Invoice Credits for Degraded Performance must be made within 30 days of the period of Degraded Performance.
- The maximum amount of any credit is the Invoice Amount for the month the Degraded Performance occurred.
- A pending credit does not release Subscriber from its obligation to pay Fastly's submitted invoices in full when due.
- Credits will be applied to the Invoice two months following the month an invoice credit was incurred.

Utilization Spikes

Subscriber's bandwidth utilization, measured in megabits per second, will be sampled every five (5) minutes on a region-by-region basis each month (the "**Samples**"). Subscriber's "**Average Utilization**" for a region in a month will be the average of the Samples. Subscriber's "**Peak Utilization**" for a region in a month will be calculated by the 95th percentile method, according to which the Samples will then be ordered from highest to lowest, and the highest five percent (5%) of Samples will be discarded and the remaining highest Sample will be Subscriber's Peak Utilization for the region in that month. Subscriber's "**Permitted Utilization**" in a month for a region will be five (5) times Subscriber's Average Utilization in that month for that region. A "**Utilization Spike**" will

occur if Subscriber's Peak Utilization exceeds its Permitted Utilization in a region. Utilization Spikes may interfere with or disrupt the integrity or performance of the Services. Subscribers should contact Support in advance of any planned utilization spike and respond immediately to any communications from Fastly regarding an actual or suspected Utilization Spike.

Legacy Premium Support and SLA

https://docs.fastly.com/products/legacy-premium-support-and-sla

NOTE: Fastly maintains support for its original Premium Support plan. For more information about our current Gold and Enterprise support plans or for information about our Professional Services packages, contact sales@fastly.com.

Legacy Premium Support description and SLA

Support availability and response times vary depending on the type of account you have and the level of support you have purchased. The following table summarizes those offerings:

Offering	Unpaid Account	Month-to-Month Account	Termed Contact	Premium Support
Online Forums	Yes	Yes	Yes	Yes
Email Support Response Time Commitment	Best Effort	Best Effort	Next Business Day	Severity 1 Incidents: 15 minutes*. All Others: Next Business Day
Severe Incident Response Email Address	No	No	No	Yes
Support SLA	None	None	Termination Option	Invoice Credits + Termination Option

Technical support

The following section applies to all Subscribers.

Definitions

- **"Business Hours"** are 8AM-6PM Monday through Friday, Pacific Time.
- **"Business Days"** are Monday through Friday excluding US and UK national and banking holidays.
- An **"Incident"** is an occurrence during which an end user's use of Subscriber's services is adversely impacted.
- A **"Severity 1 Incident"** is an Incident resulting in a major service outage requiring Subscriber to redirect all traffic from Fastly to another CDN.
- A **"Severity 2 Incident"** is an Incident resulting in minor or intermittent outage not requiring Subscriber to redirect traffic to another CDN.
- **"Fastly Control"** means elements entirely under Fastly's control and not a consequence of (a) Subscriber hardware or software failures, (b) Subscriber or end user connectivity issues, (c) Subscriber operator errors, (d) Subscriber traffic amounts that exceed Subscriber's Permitted Utilization as defined in the Terms and Conditions, (e) corrupted Subscriber content, (f) acts of god (any) or war, or earthquakes, or terrorist actions.

Subscriber responsibilities

Subscriber is responsible for using and configuring services according to the Documentation available at https://docs.fastly.com.

Support requests

Subscribers submit support requests by sending email to support@fastly.com. Subscribers receive a system-generated response within minutes containing the ticket number and a direct link to the ticket.

Incident reports should include at the least the following:

- Services not responding to end user requests.
- Services incorrectly sending end users error condition messages.
- Services sending incorrect or partial content to end-users.

Incident reports should include all relevant information, such as:

- Subscriber's determination of the Severity Level of the Incident,
- Subscriber hardware failures,
- Subscriber operator errors,
- Services configuration errors made by Subscriber employees,
- Potential Excess Utilization (as defined in the Terms of Use or master services agreement),
- Corrupted Subscriber content,
- DDOS attacks, and
- Relevant *force majeure* acts such as extreme weather, earthquakes, strikes or terrorist actions.

Communications

Communications between Fastly support engineers and Subscriber staff are conducted using the ticketing application, which maintains a time-stamped transcript of all communications, and sends emails to Subscriber and Fastly staff as tickets are updated.

Response time

Fastly shall use best efforts to respond in a timely fashion.

Termed contracts

The following applies to any Subscriber that has a contract with a term and a minimum commitment.

Response times

Fastly commits to acknowledging receipt of a support ticket within the next business day following submission of a support request.

Termination

In any three-month period where three (3) or more support Response Time objectives are not met and the failure to meet the objectives materially adversely impacted Subscriber, Subscriber shall have thirty (30) days to terminate their subscription agreement following the third failure.

Premium Support

The following applies to Subscribers who have purchased Premium Support.

Incident reporting

Severity 1 Incidents: Fastly will provide Subscriber an Incident Support Email address for Subscriber to report Incidents. Subscriber should report Incidents promptly using the Incident Support email.

Severity 2 Incidents: Subscriber should report Severity 2 Incidents by submitting a Support Request.

Response times

Fastly will respond to the report of an Incident by troubleshooting the cause(s) of the Incident and resolve them if caused by factors within Fastly's control, or provide information to those who can resolve the factors if the factors are within others' control, as follows:

For a Severity 1 Incident:

- Fastly support staff will acknowledge receipt of the email within 15 minutes.
- Fastly will start actively troubleshooting within 30 minutes of receipt of the email.
- Fastly will perform its tasks on a 24/7 basis.
- Fastly and Subscriber will immediately communicate upon learning new information that may be useful in troubleshooting the Incident, and status updates between Fastly and Subscriber staff will take place no less frequently than every 30 minutes for the first two hours, and no less frequently than every hour thereafter.
- Fastly staff will work until (a) the Incident is resolved or (b) the Incident is believed to be outside of Fastly's control.

For a Severity 2 Incident:

- During Business Hours, Fastly support staff will acknowledge receipt of the email within two hours or within two hours of the start of the next business day if the Incident does not come in during a Business Day.

- Fastly engineers will begin actively troubleshooting within one business day, will work on the Incident during Business Hours, and will provide status updates to Subscriber daily on each subsequent Business Day.

Charges for Incident Response

For Severity 1 Incidents caused by factors within Subscriber's control, a flat fee of $1500 will be assessed, and any time spent beyond three hours will be invoiced at Subscriber's undiscounted Professional Services rates.

For Severity 2 Incidents caused by factors within Subscriber's control, Subscriber will be invoiced at Subscriber's undiscounted Professional Services Rates.

For all Incidents:

- If the Incident-causing factors are within Fastly's control, there will be no hourly charges for Fastly engineering staff time.
- If the factors are within Subscriber's control, Subscriber agrees to pay Fastly its hourly charges for Fastly engineering staff time. If it appears likely the factors are within Subscriber's, Subscriber may tell Fastly staff to stop working on troubleshooting the Incident (thereby stopping the hourly charges from being incurred). Subscriber agrees to tell Fastly to stop working on an Incident via an email sent to Fastly's Incident Support email address. The timestamp on the email will be the time charges cease to be incurred.

Support Invoice Credits

In the event a Severity 1 Incident occurs, Subscriber has purchased Premium Support, the cause of the Incident is within Fastly's control, and any of the communication or response timeframes are materially not met, a one-time credit of $500 per Incident will be credited to Subscriber's account.

Credit Terms:

- Requests for Invoice Credits must be made within 30 days of the Incident which triggered the service credit.
- In no event shall Invoice Credits exceed the invoice value of the month in which they are accrued.
- A pending credit does not release Subscriber from its obligation to pay Fastly's submitted invoices in full when due.
- Credits will be applied to the invoice two months following the month an invoice credit was incurred.

Legacy Service availability SLA

Support availability and response times vary depending on the type of account you have and the level of support you have purchased.

Agreement Type	Unpaid Account	Month-to-Month Account	Termed Contract	Premium Support
Service Level Agreement	None	None	Termination Option	Invoice Credits + Termination Option

Definitions

"Degraded Performance" for the Services means the Services are experiencing Error Conditions that are (1) caused by issues under Fastly Control, (2) observable or reproducible by Subscriber or Fastly, (3) requiring Subscriber to redirect traffic off the Services. Degraded Performance does not include any reduction on availability of the Application User Interface or API due to planned maintenance.

"Error Condition" means the Services are (1) not responding to end user requests, (2) incorrectly sending end users error condition messages or (3) sending incorrect partial content to end users and these conditions are observable or reproducible by Subscriber or Fastly.

"Fastly Control" means elements entirely under Fastly's control and not a consequence of (a) Subscriber hardware or software failures, (b) Subscriber or end user connectivity issues, (c) Subscriber operator errors, (d) Subscriber traffic amounts that exceed Subscriber's Permitted Utilization, (e) corrupted Subscriber content, (f) acts of god (any) or war, or earthquakes, or terrorist actions.

Termination

Any Subscriber that has a contract with a term and a minimum commitment shall have thirty (30) days to terminate their subscription agreement if the Services experience Degraded Performance (a) for longer than 7.2 hours in any one month, or (b) for longer than 43.8 minutes each month in any three contiguous months. Subscriber shall have thirty (30) days to terminate their contract following the third failure.

Availability of invoice credits

Subscribers who purchase Premium Support shall be entitled to Invoice Credits according to the following table.

Availability Percent	Period of Degraded Performance	Monthly Credit Percent
Below 100% - 99.99%	Up to 4.32 minutes	1%
99.99% – 99.9%	Up to 43.8 minutes	5%
99.89% – 99.0%	Up to 7.2 hours	10%
98.99% - 98.0%	Up to 14.4 hours	25%
Below 97.99%	Greater than 864 minutes	50%

Invoice Credits for unavailability will accrue on a monthly basis. The Credit Amount for a month is equal to the monthly usage charge multiplied by Monthly Credit Percent.

Credit terms

- Requests for Invoice Credits for Degraded Performance must be made within 30 days of the period of Degraded Performance.
- The maximum amount of any credit is the Invoice Amount for the month the Degraded Performance occurred.
- A pending credit does not release Subscriber from its obligation to pay Fastly's submitted invoices in full when due.
- Credits will be applied to the Invoice two months following the month an invoice credit was incurred.

Legacy Shared TLS and Shared TLS Wildcard Certificate Services

https://docs.fastly.com/products/legacy-shared-tls-and-tls-wildcard-certificates-services

NOTE: Fastly maintains support for its original Shared TLS and Shared TLS Wildcard Certificate Services. For more information about our current TLS service options, contact sales@fastly.com.

IMPORTANT: As part of our previously announced planned retirement of shared certificates, Fastly has begun working with customers to migrate shared certificates to Fastly TLS. Fastly TLS offers an associated web interface and API with similar functionality to the retired products. We will continue to support shared certificates for existing customers during this migration. Our support team will contact you to schedule individual migrations and can be emailed at fastlytlsupdates@fastly.com for general questions.

Shared TLS Certificate Service

Fastly's Shared TLS Certificate Service allows you to serve HTTPS traffic using the Fastly Subject Alternative Name (SAN) certificate. You get to add up to five of your second-level domains and addresses to it, but Fastly does the certificate administration.

To purchase and use this option, follow the instructions in our guide to managing domains on TLS certificates. You'll be billed automatically as a result of the changes you make in the Fastly web interface. Each time you add a second-level domain to a shared TLS certificate, your bill will increase. We charge you for additions one month at a time, at the end of the month, for whole calendar months only. We don't charge you for any partial months of use.

Shared TLS Wildcard Certificate Service

Fastly's Shared TLS Wildcard Certificate Service allows you to serve HTTPS traffic using the Fastly SAN certificate. You get to add up to five of your wildcard domains and addresses to it, but Fastly does the certificate administration.

To purchase and use this option, follow the instructions in our guide to managing domains on TLS certificates. You'll be billed automatically as a result of the changes you make in the Fastly web interface. Each time you add a wildcard domain to a shared TLS certificate, your bill will increase. We charge you for additions one month at a time, at the end of the month, for whole calendar months only. We don't charge you for any partial months of use.

Third-party information

These articles provide information about third-party technology and services incorporated into the Fastly CDN service.

https://docs.fastly.com/products/third-party-information

Cloud-hosted products

https://docs.fastly.com/products/cloud-hosted-products

The following Fastly products may use third-party cloud infrastructure to process or store content or requests for content according to our cloud infrastructure security program:

- Fastly Image Optimizer
- Fastly WAF Support and SLA
- Live Event Monitoring

The following Fastly products may use third-party cloud infrastructure to process or store content or requests for content according to this cloud infrastructure data center and physical security program:

- Signal Sciences Cloud WAF

Open source software in downloadable components

https://docs.fastly.com/products/open-source-software-in-downloadable-components

The following table provides information about open source technology incorporated into the downloaded components for Next-Gen WAF.

NOTE: This page will be updated to identify changes to open source third-party technology included in the current version of the downloadable software components.

Technology	Version	License
Datadog Go	v2.2.0+incompatible	MIT
glob	0.2.3	MIT
Go App Engine packages	1.4.0	Apache 2.0
go-codec	1.1.7	MIT
go-diff	1.0.1-0.20180205163309-da645544ed44	MIT
gogoprotobuf	1.3.1	NewBSD
gohistogram	1.0.0	MIT
go-license	0.0.0-20180405065157-c69f41c2c8d6	MIT
Go Networking	0.0.0-20200226121028-0de0cce0169b	NewBSD
Google APIs generated by gogoprotobuf	1.3.0	Apache 2.0
gopsutil	0.0.0-20190627142359-4c8b404ee5c5	NewBSD
go-reuseport	0.0.1	ISC
gorilla/mux	1.7.3	NewBSD
Gorilla Websocket	1.4.2	FreeBSD
GoVersionInfo	0.0.0-20190209210621-63e6d1acd3dd	MIT
gRPC-Go	1.21.0	Apache 2.0
gRPC Go Middleware	1.2.0	Apache 2.0
gRPC Go Proxy	0.0.0-20181017164139-0f1106ef9c76	Apache 2.0
jaeger-client-go	2.22.1+incompatible	Apache 2.0

Technology	Version	License
jose	1.1.2	Apache 2.0
Logrus	1.4.2	MIT
mapstructure	1.1.2	MIT
mgo	0.0.0-20181015135952-eeefdecb41b8	FreeBSD
msgp	1.1.2	MIT
OpenTracing API for Go	1.1.0	Apache 2.0
Oxy	1.1.0	Apache 2.0
pflag	1.0.4-0.20181223182923-24fa6976df40	NewBSD
pkg/errors	0.9.1	FreeBSD
pkg/profile	1.4.0	FreeBSD
protobuf	1.3.2	NewBSD
protoc-gen-validate	0.1.0	Apache 2.0
reopen	1.0.0	MIT
snappy	0.0.1	NewBSD
sys	0.0.0-20200908134130-d2e65c121b96	NewBSD
viper	1.4.0	MIT

Sub-processors

https://docs.fastly.com/products/sub-processors

Fastly engages certain sub-processors in connection with the provision of the Fastly Services. A sub-processor is a Fastly affiliate engaged in the processing of personal data (each a “Fastly Affiliate”) or a third-party service provider engaged by Fastly, Inc. or a Fastly Affiliate to process personal data on behalf of Fastly’s Subscribers.

Fastly maintains a list of the names, entity type and locations of all sub-processors of personal data contained in Subscriber Data and caused to be submitted to Fastly via the Services according to Subscriber’s configuration of the Services, which is set forth below. For more information on Fastly’s data processing obligations, please see our data processing terms.

Name of Sub-Processor	Entity Type	Entity Location
Fastly Australia Pty Ltd	Fastly Affiliate	Australia
Fastly Cloud Iberica, S.L.	Fastly Affiliate	Spain
Fastly GmbH	Fastly Affiliate	Germany
Fastly India Private Limited	Fastly Affiliate	India
Fastly International (Holdings) Limited	Fastly Affiliate	United Kingdom
Fastly Kabushiki Kaisha	Fastly Affiliate	Japan
Fastly Limited	Fastly Affiliate	United Kingdom
Signal Sciences, LLC	Fastly Affiliate	United States
Google LLC	Third-party sub-processor	United States
Amazon Web Services, Inc.	Third-party sub-processor	United States
Microsoft Corporation	Third-party sub-processor	United States

Name of Sub-Processor	Entity Type	Entity Location
MongoDB Atlas	Third-party sub-processor	United States

Subscribers may subscribe to receive email notifications of sub-processor changes at https://docs.fastly.com/changes. Notices of updates to this page will be posted on our changelog.

Third-party technology

https://docs.fastly.com/products/third-party-technology

These articles provide information about third-party technology and services incorporated into the Fastly CDN service:

- Geolocation VCL features
- Device detection variables
- Nearline Cache
- TLS service options

In addition, these articles describe third-party services that interoperate with Fastly CDN services:

- Integrations with Non-Fastly Services
- Streaming logs

The Signal Sciences Cloud WAF and Next-Gen WAF use the MaxMind GeoLite2 databases.