# Tiers

| SSL plans | Standard | UCC / SAN | Wildcard |
|---|---|---|---|
| Websites | 1 | Starts at 5 (upgradeable to 100) *1 | 1 Website and all its sub-domains *1 |
| Strongest encryption on the market (SHA-2 & 2048-bit encryption) | ✔ | ✔ | ✔ |
| Available in... | DV, OV, and EV | DV, OV, and EV | DV and OV |
| Boosts Google ranking | ✔ | ✔ | ✔ |

First choose a plan (above), then choose a type (below)...

| SSL types | Standard Domain Validation (DV) | Deluxe Organization Validation (OV) | Premium Extended Validation (EV) |
|---|---|---|---|
| Proves domain ownership | ✔ | ✔ | ✔ |
| Validates organization | | ✔ | ✔ |
| Shows business is legitimate | | | ✔ |
| Display business name in green address bar | | | ✔ |
| Padlock in address bar | ✔ | ✔ | ✔ |
| Protects multiple websites | ✔ (UCC / SAN SSL only) | ✔ (UCC / SAN SSL only) | ✔ (UCC / SAN SSL only) |
| Protects 1 website and all its sub-domains | ✔ (Wildcard SSL only) | ✔ (Wildcard SSL only) | |
| Security trust seal | ✔ | ✔ | ✔ |
| Warranty | USD $10,000 | USD $25,000 | USD $50,000 |
| Great for... | Blogs, social, and personal sites | Business – information, non-profits, education, government | Business eCommcerce |

**Notes:**

- *1 UCC/SAN and Wilcard SSLs require all websites must be on the same hosting account

# Qualifying

## Country/language restrictions

Please reference this Help Article to confirm your customer's country/language qualifies for a specific SSL type and plan.

## Who needs an SSL?

Anyone with a website needs an SSL.

- Blogs, personal or informational sites – SSL boosts Google ranking and prevents hackers from intercepting sensitive information when visiting the website.
- Business and non-profit sites – SSL established site legitimacy and protects visitor's information like login credentials and personal data.
- ecommerce sites – SSL secures customers' payment information.

## When is an SSL not the answer?

- Site is compromised – A SSL will not protect against weak FTP passwords or vulnerable scripts. For hacked site, offer **Website Security**.
- Site is static (information only), has no areas for visitor input.

---

### Why would a site need to be protected with an SSL?

An SSL protects your customers by encrypting sensitive data like usernames, passwords and credit card numbers as they pass through your site.

- Customers are looking for it – visitors want to know the sites they visit are secure
- Higher Google search ranking. Google uses SSL as a ranking signal. SSL-encrypted sites will be ranked higher than non-encrypted sites.
- "HTTPS everywhere" is a movement led by Google, Mozilla, and Apple, just to name a few, to make the Internet a safe place by default. HTTPS is not a nice-to-have anymore, it's a must-have. Browsers are or will be calling out non-secure sites with warnings and alert messages.
- Big security breaches grab the headlines, but the reality is small business are at higher risk. There's a rise in cyber attacks on small business simply because they're easy targets. Small business owners are less aware and less equipped to handle attacks. 80% of cyber attacks could be stopped by adopting simple basics such as an SSL.

---

### What SSL should my customer purchase?

We speak to tons of customers every single day that could benefit from a Secure Certificate. But which one should they get? The first step to answering this question is to understand the domain name or names that your customer wants to secure.

- **Protect One Website**: Protects a website like coolexample.com
- **Protect Multiple Websites**: (UCC Certificate), Protects multiple websites like coolexample.com and amazingexample.net
- **Protect One Website and All its Subdomains**: (Wildcard Certificate), *.siteprotection.com will protect www.coolexample.com, cart.coolexample, and site.coolexample.com

Once we've determined how many domain/s need to be covered, our next step is to determine the appropriate level of validation for your customer.

The important thing to stress to your customer is that no matter what option they select, in order to issue their certificate as quickly as possible, we need them to actively

participate in the validation process.

### They have the following options:

- **Standard SSL**: We validate whether or not the customer owns the domain name/s attached to the certificate request. Some of our methods include: emailing the contacts we find in a WhoIs database, having the customer change the domain's DNS, or having the customer create a temporary web page.
    - This type of validation is intended for individuals, blogs, social websites – essentially, any website that isn't a business.
    - These certificates are typically issued within minutes.
- **Deluxe SSL**: We validate domain ownership and some aspects of the customer's organization. Typically, we are looking to verify that their organization is currently registered with a government authority (think Secretary of State). But we can also validate Small Businesses and Sole Proprietors.
    - This type of validation is intended for businesses and organizations.
    - For more information on how we validate Deluxe Certificates, please see this Help article.
    - These certificates are typically issued within two to five business days
- **Premium**: (Extended Validation) Certificates; these are currently not available for Wildcard certificates, and come with a free standard SSL that can be used while we are validating the customer's organization: in addition to validating domain ownership, for EV certificates we provide the highest level of organization authentication. EV certificates display as a green bar in certain browsers, which is a large selling point to many business. We validate these certificates by using a combination of online tools, legal documents, and outbound calls to various sources.
    - This type of validation is intended for businesses and organizations, and is the best option for any eCommerce customer.
    - For more information on how we validate EV Certificates, please see this Help article.
    - These certificates are typically issued within 30 days.

---

SSL hosting compatibility with other products

### Managed WordPress

- Wildcard SSL certificates will not work on Managed WordPress.
- When working with Ultimate and Developer Managed WordPress accounts, its possible to secure each individual site with single certificates, however there is another option which will save the customer time and money.

### Shared Hosting

- You may only install a certificate on the primary domain on the 4GH Hosting – addon domains can be covered by a UCC SSL certificate.
- UCC and Wildcard SSL certificates cannot be shared between Shared Hosting plans.
- When setting up an SSL certificate to Shared Hosting, the drop–down will only display paid plans that are not pending any changes.

### Template-based Hosting

**GoCentral**

- All tiers come with an SSL certificate.

**Website Builder v6 and v7**

- Only single SSL certificates will work with WSB v6 and v7.
- The top tier comes with an SSL certificate.  For the tiers that do not come with an SSL certificate, if the customer wishes to have an SSL certificate, an SSL may be purchased.

**Online Store (legacy standalone product)**

- Online Store already comes with an SSL certificate.

# Consulting

- **What are you doing to secure your customer's information right now?**
- **How do you prevent browser warnings when customers enter your site?**
- **What have you done so far to insure customers are finding your site when they search for (your business type)?**
- **I noticed you had a contact form on your website, have you thought about how to protect your clients' information?**

## Facts

- 60% of cyber attacks are aimed at small businesses (The State of Cyber Security 2017)
- Those cyber attacks cost small businesses $84k–$148k (UPS Capital)
- 30% of websites do not have a trusted SSL Certificate (Google)
- 43% of consumers abandon sites when they see security alert messages (Netcraft survey 2018)

## Talking tips

### One-sentence message

Keep data safe and hackers locked out while aligning your website with the "HTTPS Everywhere" initiative using the world's toughest SSL encryption.

### Two-sentence message

Keep payment info and sensitive details safe, secure and locked down tight. You'll boost online sales and build trust.

### 15-second audio offer

Hackers are out there, waiting. Give them an opening and they'll steal credit card numbers, passwords and more from your website. But an SSL Certificate tells them to

move on, they don't stand a chance. Your customers can rest assured that their information stays private.

30–second audio offer

Hackers are out there, waiting. Give them an opening and they'll steal credit card numbers, passwords and more from your website. But an SSL Certificate tells them to move on, they don't stand a chance. Your customers can rest assured that their information stays private. They can browse, shop and share with confidence, knowing that the information they enter on any secured page is protected. And it's all backed by our dedicated security team.

100–word message

Secure transactions and sensitive data with an SSL Certificate.  You and your customers need a simple, cost–effective way to protect the passwords and credit card numbers submitted to your website.  With an SSL Certificate, shoppers will buy with confidence, knowing the information they enter is protected with the industry's highest levels of security, all backed by our dedicated security team.  You'll also enjoy the added benefit of higher Google rankings.  Our award–winning SSL Certificates work with all major browsers, and they protect an unlimited number of servers.

Value Proposition

- Keep sensitive/private data (e.g customer info, payment info etc.) safe and secure.
- Build visitor confidence and trust.
- Increases search rankings.

# Personalization

SSLs are for everyone who has a website but they are especially easy to sell to anyone where security is important

- Doctors
- Laywers
- Anyone that deals with any personal information beyond names on their website.

It's a liability to have your customer's information traveling through your website without being secured.  I'm sure you've heard of companies who've lost their customer's information, its never good for publicity. (don't mention specific companies, the customer will know of one)

eCommerce sites

I see that you take orders online / you have an eCommerce site.  Are you not concerned about having your customers' information be encrypted during the ordering process?  Many customers prefer to make payments through secured websites that have padlocks.

### Blogger/social site

Web security is vital to all of us.  I see you have a blog/social website where you collect your customers' sensitive information (such as passwords, credit card information, contact information, etc).  How do you make sure this information is secure?  Having an SSL Certificate will provide a secure tunnel that encrypts and protects users' information.

# Benefits

## Increasing online sales

### Get higher search rankings on Google

Google is a heavy investor in Internet security and safety. They now use HTTPS as a search signal in their ranking algorithm. An SSL secured website (HTTPS vs. non-secured HTTP) will help boost your search ranking on Google.

- References:
  - Official Google Webmaster Central Blog: HTTPS as a ranking signal
  - Should I Switch From HTTP to HTTPS for SEO Reasons? – Forbes

**Why us?** Our Standard SSL certificate is an easy, cost-effective way to secure sensitive data and help increase your Google rank.

### Avoid browser warnings that could turn away customers

Instantly let customers know they can shop safely. The green address bar is like a billboard that screams "Safe. Secure. Hacker-free."

**Why us?** Our prominent security indicators such as https prefix, padlock and green bar let customers know their information is safe.

### Convert visitors to buyers

Security cues like our Trust Seal on your order page and the browser bar padlock icon tell visitors their private details are safe. That means more purchases – win! – and fewer abandoned carts – win-win!

**Why us?** SSL Certificates are a cost-effective way to increase sales by reducing cart abandonment.

### Protect multiple domains and sub-domains so your entire website is secure

Customers will buy with confidence, knowing that the information they enter on any secured page is protected. And that means they'll come back again... and again.

**Why us?** We have the tools you need to make sure your website is secure – your whole website.

### Unlimited, free 24/7 help from security experts

Need help setting up your SSL Certificate or troubleshooting a security issue? Call us any time, day or night.

**Why us?** We're here for you 24/7/365.

## Securing sensitive data and joining the HTTPS movement

### Keep sensitive data safe by transmitting information via a secure channel.

SSL Certificates are a simple, cost–effective way to protect the private information – passwords, credit card numbers – submitted to your website. They're like a dedicated superhero for your site, minus the cape.

**Why us?** Our award–winning SSL Certificates work with all major browsers and they protect an unlimited number of servers.

### Industry–leading SHA–2 and 2048–bit encryption

We use 2048–bit encryption strength to stop hackers in their tracks. That's the strongest in the market today. Virtually uncrackable.

**Why us?** You'll benefit from the highest levels of security the industry offers.

### Show your site is secure

When a visitor enters an SSL–protected page, their browser bar displays a padlock icon and the https:// prefix in the URL address. They see that and they know your site's locked down tight. Some visitors want even more proof. They can click on the Site Seal and see your site provides secure data transactions. And that you've invested in the safety and security of your visitors' information. We've got your back and we're at your side, too.

**Why us?** Websites protected by our Premium EV SSL display a green address bar – a prominent security indicator that gives visitors the green light to purchase.

### Be the role model. Show visitors you care

Web security is vital to all of us – from shopping online to social sharing to reading the news. Now, tech giants like Google are calling for increased security on the web – including using HTTPS – and advocates are calling news outlets and online organizations to be responsible for visitor security by providing encrypted connections. HTTPS is a must–have.

**Why us?** Our award-winning SSL Certificates work with all major browsers and devices, and protect an unlimited number of servers.

### Get higher search rankings on Google

Google is a heavy investor in Internet security and safety. They now use HTTPS as a search signal in their ranking algorithm. An SSL secured website (HTTPS vs. non-secured HTTP) will help boost your search ranking on Google.

- Official Google Webmaster Central Blog: HTTPS as a ranking signal
- Should I Switch From HTTP to HTTPS for SEO Reasons? – Forbes

**Why us?** Our Standard SSL certificate is an easy, cost-effective way to secure sensitive data and help increase your Google rank.

### Less Likely To Be Hacked

An SSL is trusted by customers, meaning they will feel safer using your website. When browsers are forced to use HTTPS connections it raises the security policy, meaning less opportunities for hackers

# Free SSL versus Paid SSL

## The Competition

### Let's Encrypt

Let's Encrypt is a non-profit organization that issues free Domain Validated (DV) SSL certificate to anyone who owns a website.

✔ Pros
- It's free
- It provides the same encryption and displays the HTTPS and lock icon

✖ Cons
- It requires user to install a client application and admin root access (not everyone knows how to do this)
- It doesn't provide customer support, only knowledge base and forum.
- It's prone to issue certificates to fake sites (due to lack of strict authentication used by established CAs)

### StartCom

StartCom offers free Domain Validated (DV) SSL via StartSSL with additional fees for revocation and reissue. StartCom was acquired by WoSign in 2016.
**More info**:

- All Startcom certificates were removed from Google Chrome in March 2017, including certificates previously issued, with similar removals from other browsers expected to follow.[3]
- In August 2016 it was reported that StartCom was sold to WoSign, a Chinese CA.[13][25][26] The original disclosure was taken down for legal reasons.[27] However, repostings of the original articles are still available.[25] The relationship is unclear, but it seems as if the StartCom technical infrastructure was being used by WoSign when they were caught issuing about a hundred[28] improperly validated SSL certificates, including a certificate for github.com.[13][29]

✔ Pros
- It's free, to start at least.
- It provides the same encryption and displays the HTTPS and lock icon.

✖ Cons
- It will charge for revocation and reissues.
- It will try to upgrade customers to paid.
- It is currently dis-trusted by major browsers like Google right now due to improperly validating certs.

### Comodo

Comodo is a paid CA that partnered with CloudFlare and cPanel to provide free shared SSL at the server level. Comodo also offers a free 90-day trial, but customers will pay after the trial period ends.

## FAQ

### Are free and paid SSL the same, and what are the differences?

Free SSLs are often domain validation (DV) SSL certificates issued by a known Certificate Authority (CA). The encryption technology used is virtually the same. The difference comes in added services such as setup process, revocation, reissuance, customer support, warranty, and of course, the cost to the customer. Also very important is CA trust by major browsers such as Google Chrome, Mozilla Firefox, etc.

### Are there any flaws with free SSLs?

It's great that there are organizations offering free SSL for the good of the Internet. SSL should be the default security for all websites, and we fully support that.

Because free SSLs are easy to obtain, they have become a primary target for bad actors. For example: **Let's Encrypt** issued 15,000 certificates to domains with “PayPal” in subject name. Interestingly enough, PayPal itself does not use **Let's Encrypt**, so presumably these 15,000 sites are illegitimate and possibly have nefarious intentions.

The fundamental principle of SSL is the trust associated with the CA that issues the certificate. If a CA issues tens of thousands of certs to illegitimate sites then that CA's certificate should not be trusted.

- Here's a good read: [Free public certificate authorities: Nice idea, big flaw | InfoWorld]

### The DMV Analogy

Think of CAs as DMV. In order to get an ID from the DMV, you need to provide proof of identity (birth certificate, marriage license or other government–issued ID) and DMV will verify those documents and issue your ID card. Then you can present that ID as official identification to the public. If there's a flaw in the DMV process, then the ID cards they issue can't be trusted anymore. Similar w/ SSL certificates, if the CA is not trusted or have flaws in their validation process, then the certificates they issue should not be trusted, and ultimately undermines the system.

## Overcome Objections

### Why should I pay when I can get it free?

Nothing is completely free. Free SSLs from Let's Encrypt require you to install and run a client app and enter command line on your server. There is no customer care to get support from if you run into issues. It's probably ok if you know what you're doing, but not ideal if you need a simple solution.

### Don't I get the same features/benefit from free SSL?

Yes and No. You get the same encryption technology that will protect the data transmitted from website to server. Beyond that, free SSLs don't offer customer support/care, some CAs such as StartCom charge fees for revocation and reissues, so you'll be nickeled and dimed for every routine service that comes up.

### Free SSL certificates are just as good or trustworthy as paid

Free SSLs don't have the same trust level as paid SSLs. Paid CAs invest a lot in strict validation and vetting process to abide by industry rules and regulations. They have good track records of proper validation and issuance and low risk of

## Free vs. Paid Summary

| | Free | Paid |
|---|---|---|
| Encryption | ✔ | ✔ |
| Customer support | | ✔ |
| Comprehensive SSL options | | ✔ |
| Warranty | | ✔ |
| Potentially more fees | Yes | No |
| CA trust | Low | High |

fraudulent certs. Their certs are trusted by browsers and browsers pass on that trust to end-users.

# Overcoming Objections

## SSL Certificate Competitors

Below are SSL's main competitors...but you can also find the competitors who offer free SSLs here: Free SSL versus Paid SSL

| Features | Our SSL | Global Sign | Thawte | Comodo | GeoTrust |
|---|---|---|---|---|---|
| Name of the cert | Standard SSL | DomainSSL | SSL 123 | Comodo SSL | Quick SSL Premium |
| No of certs included | 1 | 1 | 1 | 1 | 1 |
| Multiple year options | up to 3 years | up to 3 years | up to 3 years | up to 3 years | |
| Domains secured | Single domain name (FQDN) + www SAN | Single domain name (FQDN) + www SAN | Single domain name (FQDN) + www SAN | Single domain name (FQDN) + www SAN | 1 |
| Issuance speed | within a few minutes | within a few minutes | within a few minutes | within a few minutes | issued within 1-3 days |
| Validation required | Domain validation | Domain validation | Domain validation | Domain validation | Domain validation |
| Encryption strength | up to 256-bit | up to 256-bit | up to 256-bit | up to 256-bit | up to 256-bit |
| Browser compatibility | 99.9% | 99% | | 99.9% | 99+% |
| SSL Trust seal | Included | Included | Included | Included | Included (dynamic seal) |
| 2048 bit Root | Yes | Yes | Yes | Yes | Yes |
| Support options | Free Phone, Chat 24x7 | Free Phone and Email, Mon-Fri 8am-10pm EST + limited evening and weekend support | Free Phone, Email, Chat 24x5 | Free Email, Chat 24x7 | Free Phone, Email, Chat 24x5 |

| Features | Our SSL | Global Sign | Thawte | Comodo | GeoTrust |
|---|---|---|---|---|---|
| Free trial | No | Yes, Valid for 45 days | No | Yes, Valid for 90 days | Yes for 30 days but only for testing, not for production |
| Refund Policy | Full refund within 30 days of issuance | Full refund within 7 days of issuance | Full refund within 30 days of issuance | Full refund within 30 days of issuance | Full refund within 30 days of issuance |
| Reliability | Highly reliable | Reliable | Reliable | Reliability questionable | Highly reliable |
| Warranty | $10,000 | $10,000 | $500,000 | $250,000 | $500,000 |

I don't think security is important

I talk to customers every day that have had problems with their site, its better to be preventative with these sorts of things.

Why should I pay for an SSL when I can get one for free other places?

Nothing is completely free. Free SSLs from Let's Encrypt require you to install and run a client app and enter command line on your server. There is no customer care to get support from if you run into issues. It's probably ok if you know what you're doing, but not ideal if you need a simple solution.
Free SSL versus Paid SSL

Don't I get the same features and benefits from a free SSL that I can get somewhere else?

Yes and No. You get the same encryption technology that will protect the data transmitted from website to server. Beyond that, free SSLs don't offer customer support/care, some CAs such as StartCom charge fees for revocation and reissues, so you'll be nickeled and dimed for every routine service that comes up.
Free SSL versus Paid SSL

I don't really need an SSL Certificate.

For your business to succeed, customers must trust you. If your website asks visitors for any sensitive information – credit card numbers, usernames, passwords, contact information or other personal data – your company's reputation depends on protecting each and every detail. An SSL Certificate provides this critical layer of security for your site.

An SSL Certificate won't make a difference.

Customers who trust your website are more likely to do business with you. If a website is secured by an SSL Certificate, it displays a URL that starts with “https” and a padlock icon

in the address bar. Visitors look for the padlock icon and other signs your site is a safe place to shop and share information.

### It's too complicated.

If you have a hosting account with us and purchase our SSL, we'll automatically set up and install your SSL Certificate. If your website is not hosted with us, just log in to your account and request your certificate. We'll ask you for information about the type of certificate you ordered. Verifying everything you submit takes just a few minutes for Standard SSL Certificates (or up to a week for Extended Validation).

### It's going to take too long.

The issue time varies depending on the type of certificate you ordered, but typically a Domain SSL Certificate takes only minutes, while an Extended SSL Certificate takes a few days or up to a week.

### I already have Website Security.

Website Security scans a website for malware and vulnerabilities, automatically removing the malware it has detected. An SSL Certificate provides a secure tunnel that encrypts and protects the user's information (i.e. username, password, credit card number) in online transactions.

### I don't sell products on my website. I don't need SSL protection.

An SSL Certificate protects more than just payment transactions. By providing a secure communication tunnel it encrypts and protects all data passing through your website. If your site handles private info such as username, password, email address (not to mention birth dates and social security numbers), protecting data is even more crucial. Without an SSL Certificate, an attacker can see this info in clear text. This would allow someone else to impersonate your visitor, and lead to numerous possibilities of serious security compromises. While Premium (EV) SSL is best practice for eCommerce sites, a Standard (DV) SSL certificate is ideal for blog and social websites.

## General questions

### What is an SSL?

**SSL (Secure Sockets Layer)** is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

**In customer terms:** It encrypts data transmitted between your browser and website, such as an admin login or a contact form submission instead of transferring the data in plain text.

### Why can't I purchase an SSL for more than 2 years to match my other products?

Internet security moves fast, we make sure you have the most up to date security by forcing re-keys every 2 years.

### Can I install 1 SSL to multiple servers?

Yes, you need to export the private key that the CSR was generated on, and import that private key to any other server you want to install the SSL on. If the servers have different operating systems, you install the private key and then download the appropriate certificate and intermediate bundle for each server type. Installing that private key on the other servers creates that “handshake” to allow it to encrypt properly.

### How many sites does it cover?

- Standard – covers the MAIN domain (no add-on domains) for a hosting account.
- UCC – Covers the main domain plus 4 extra domains installed to the same hosting. You can add blocks of 5 to the initial 4 up to 20 total. Above that you can add in quantities of 10 until you hit 50 total. After that, it jumps to quantities of 100. NOTE: you cannot upgrade later, so you need to know the maximum number of SANs you may need for the purchasing period before you buy to avoid needing to buy a larger one later on.
- Wildcard – Covers 1 domain and all its subdomains that are hosting on the server/hosting account.

### How do I cover a domain that isn't the main domain on my hosting?

You can either buy a UCC SSL for the main domain and add it as one of the extra domains, or swap the domain you wish to cover into the main domain for that hosting account.

### My hosting is elsewhere, can I still use your SSLs?

Maybe, you'll need to confirm with your host if they allow for 3rd party SSL installs. Some shared hosting providers do and all VPS and Dedicated Servers do.