

# **EXTENDED VALIDATION (EV) CERTIFICATE CUSTOMER EDUCATION CONTENT KIT**

## Congrats on your EV SSL certificate

You're a leader that refuses to compromise on your brand, personal identity or customer experience online and that's why you've chosen Extended Validation SSL. EV SSL provides the highest level of identity and brand protection.

However, one challenge for customers is understanding how—and why—EV SSL is the best choice for businesses to safeguard their personal data and finances. This content was created to help you promote and build trust with your customers and website visitors by showing your commitment to their online protection. We hope that it assists your customers and visitors with understanding how to look beyond the lock, and the importance of recognizing authentic websites and the business identity behind them. Feel free to edit and share any of the content included in this kit.

We've included a variety of text and image options that your web team can leverage to edit and post on a web page, blog post, email campaign or social media. You can download any of the files provided in this kit [here](#). Because you already talk to your customers about security and privacy, this kit also shows you how to inform both your customers and website visitors about the importance of an authentic website identity.

Sincerely,

The DigiCert Team

# Table of Contents

- I. Main Content
  - A. What's the difference?
  - B. Look beyond the lock
  - C. Not all security or website encryption is the same
  - D. Providing a clearer picture of the brand behind our website
  - E. Putting your trust—and our brand identity—first
  - F. Our commitment
- II. Additional Supporting Materials
  - A. We've leveled up our online security
  - B. Social Media content
  - C. Visual support to help customers identify validated sites
  - D. Choosing the right web browser

## What's the difference?

### How to tell the website you're viewing is authentic

Dear customer,

Did you know the average person spends almost seven hours online every day—with half of that time on a mobile phone? That equates to an incredible 106 days in a year.<sup>1</sup> Despite all of this time online, it's still difficult to identify that certain websites are legitimate or authentic even though they may say "Secure" in the browser.

The following steps teach you how to look beyond the lock to analyze a website's [SSL certificate](#) from your desktop computer to ensure their brand name hasn't been compromised.

1

### EV SSL SECURITY

Click on the padlock icon in the address bar to view our SSL certificate. Our website is secured by an EV SSL certificate from DigiCert, which provides advanced brand protection by verifying that we are both the correct website domain owner and publicly advertised business affiliated with the website. See visuals [here](#).

2

### WHAT ARE THEIR ROOTS?

Look for an EV root in the details of the certificate. This means a brand has passed an 18-step approval and vetting process to secure its SSL certificate.

3

### LOOK FOR THE SITE SEAL

Proceed with caution if a site isn't using an EV certificate. Check for other trust indicators like the DigiCert site seal, or the Norton powered by DigiCert site seal.

## Look beyond the lock

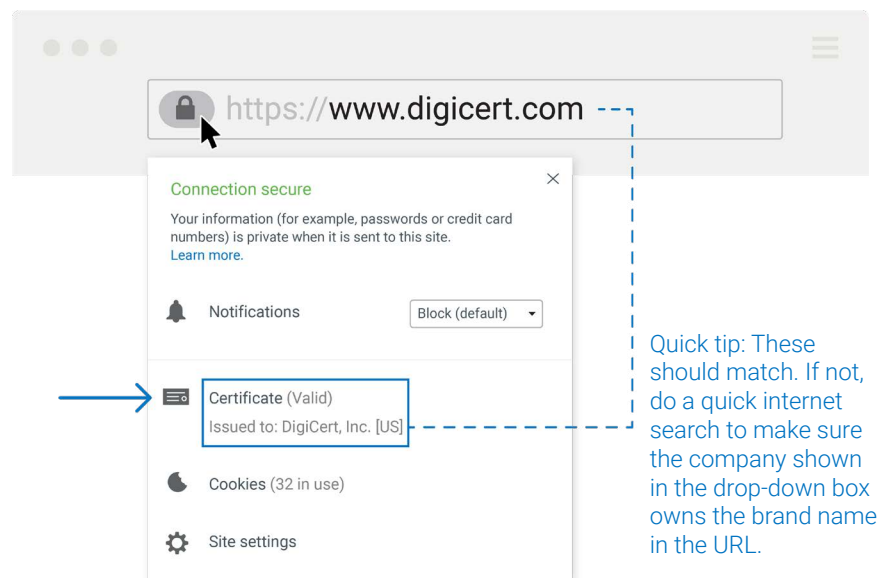
### The padlock icon in a web address bar reveals more information about a website than you think

With just one click of the padlock icon, you can identify a website's true owner and determine if the website you're visiting is safe to share your personal information with. The caveat? Only websites protected by the highest form of TLS/SSL certificate coverage—Extended Validation (EV)—will readily include that information. Both Organization Validated (OV) and Domain Validated (DV) certificates do not display the domain owner's name when you click on the padlock. That's why looking beyond the lock matters. If you see an organization's name in the drop-down message, you can be confident that the company owns the domain and their website is legitimate.

Here's how to look beyond the lock:

### STEP 1

Click on the padlock icon in your browser address bar to the left of the URL.



The example above shows how certificates appear from Google Chrome. To see other browser examples click [here](#).

### STEP 2

When a website is protected by an Extended Validation (EV) TLS/SSL certificate, visitors will easily be able to identify the organization that owns the website, like in the example above, to determine exactly who controls and manages the site.

If a website has not been fully vetted with EV, the pop-up message will simply indicate that the connection is "secure," or the TLS/SSL certificate is valid. That means your information is encrypted, but the website owner has not been fully identified. While lacking this information doesn't necessarily indicate that a website is fraudulent, it should cause a website visitor to be more critical about the website's authenticity and to be extra careful about sharing their personal information.

Other ways to check for a website owner's identity:

- Look for a site seal that is a visual trust mark indicating the site has been vetted by a third party like DigiCert.



Remember, if you're unsure about your security on a website, then you should look beyond the lock to protect yourself from online abuse.

## Not all security or website encryption is the same

We refuse to compromise on our customers' data privacy and security. That's why our website is secured by an Extended Validation SSL certificate from DigiCert.

## Did you know not every website that has a "secured" padlock in the address bar should be considered safe?

The "secure" website message in the browser only indicates that the website is using encryption. What if the website you're sending your information to is inauthentic and unverified? With an Extended Validation SSL certificate, our business passed an 18-step validation process to prove that we are the authentic and legitimate owners of our URL. That's why we encourage you to look beyond the lock.

Here's what the three types of SSL certificates will reveal about a website's authenticity:

### 1 DV SSL

Cheap and fast. Encryption and domain verification only. Website may not belong to the company it's suggesting it does. Proceed with caution.

### 2 OV SSL

Ensures a website is managed by an authentic, publicly listed business. It verifies the business locality and name.

### 3 EV SSL

Provides advanced measures to ensure a business is authentic and legitimate.

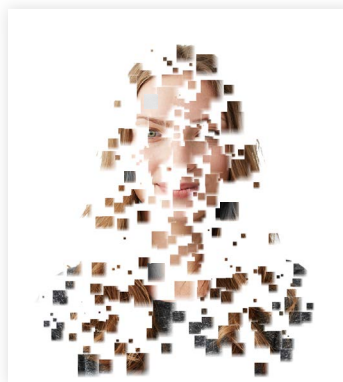
Take your online security more seriously by ensuring you're browsing legitimate websites with the highest level of SSL brand protection. Learn more about identifying secure websites [here](#).

## PROVIDING A CLEARER PICTURE OF THE BRAND BEHIND OUR WEBSITE

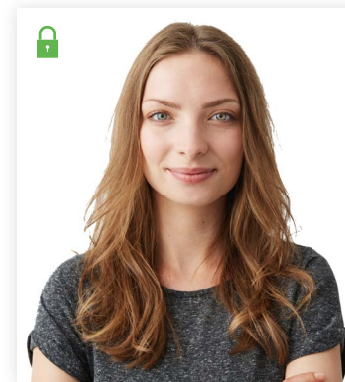
Your online security is not something we're willing to risk. That's why we use an EV SSL certificate on our website to ensure that you know (company name) is, in fact, (company name). Learn more about the different types of SSL certificates and why EV SSL provides the best safeguards for companies who aren't willing to compromise their brand identity online.



**Domain Validated SSL (DV)**  
certificates provide the lowest level of authentication, meaning anonymous entities can get a certificate. It's anonymous and unclear who's behind the site.



**Organization Validated SSL (OV)**  
certificates provide additional checks to ensure brand protections. While not 100%, it's a better picture of who's really behind the site.

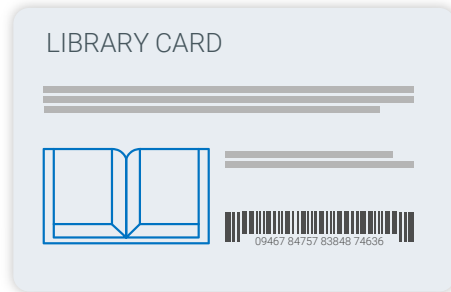


**Extended Validation SSL (EV)**  
certificates guarantee the highest standard of brand protections. With EV, brands signal a commitment to customers that transactions are secure. Full picture of who you're sharing your sensitive information with.

## PUTTING YOUR TRUST—AND OUR BRAND IDENTITY—FIRST

### The level of authenticity customers expect

We are who we say we are online—and we can prove it. Our website is protected by an EV SSL certificate from DigiCert, which provides the greatest safeguards against customer fraud and identity theft for brands. It also ensures your data is securely encrypted on our website.



#### Domain Validated SSL (DV) Certificates

Similar to a generic library card, the DV SSL certificate displays the lowest level of identity authenticity on the web—nearly anonymous.



#### Organization Validated SSL (OV) Certificates

Your driver's license is a standard form of ID that requires a more complex process to acquire—like the vetting process for an OV SSL certificate.



#### Extended Validation SSL (EV) Certificates

Your passport is the most valuable ID you can own, requiring a sophisticated and rigorous process to obtain it—similar to an EV SSL certificate—and allowing other governments to recognize and trust you.

## Our commitment

### Keeping your online information secure while you're online

We've taken extra precautions to keep your data secure on our website and we wanted to give you some tips to protect your information online.

#### Look for the padlock

Make sure the website you're browsing is encrypted by an SSL (Secure Sockets Layer) certificate. If a website shows a "Not Secure" message it means your data may be at risk.

#### Look beyond the lock

Click on the padlock in your browser and view "details." See if the company location and legal entity is identified. It's very important that you know who you're sharing your information with.

#### Is the company verified?

Companies with high-assurance EV SSL certificates provide details about the business name, category, location and prove that they represent a legitimate business.

#### Don't just 'trust your gut'

Websites that have a padlock and say "Secured" in the browser could still be trying to phish you. DV SSL certificates are easy to obtain and frequently used by scam artists.

We're proud to be partnering with DigiCert, the industry leader in TLS/SSL certificates, to secure and encrypt all transactions on our website with an Extended Validation SSL certificate. The most innovative companies, including 89% of the Fortune 500 and 97 of the 100 top global banks, choose DigiCert for its expertise in identity and encryption.<sup>1</sup> To learn more about SSL certificates, and why they're important to internet security as a whole, click [here](#).

1

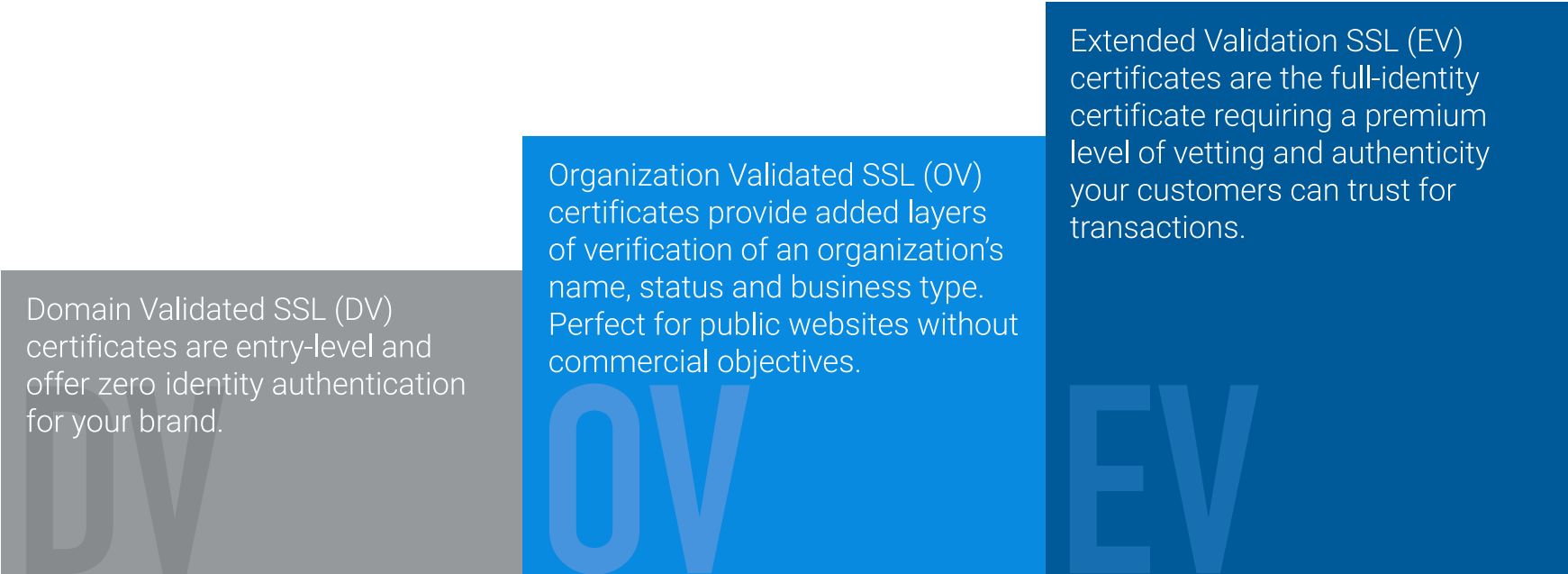
DigiCert Internal Customer Analysis, October 2017. Forbes Fortune 500 & Global 2000 2017 Publication.

# **ADDITIONAL SUPPORTING MATERIALS**

## WE'VE LEVELED UP OUR ONLINE SECURITY

In order to ensure our customers are having the safest experience online, we've chosen to secure our website with an EV certificate.

Domain Validated SSL (DV) certificates are entry-level and offer zero identity authentication for your brand.



Organization Validated SSL (OV) certificates provide added layers of verification of an organization's name, status and business type. Perfect for public websites without commercial objectives.

Extended Validation SSL (EV) certificates are the full-identity certificate requiring a premium level of vetting and authenticity your customers can trust for transactions.

## Social media content support

Help your customers understand the risks of phishing attacks by sharing these social media posts to your channels.

**\$17,700**  
is lost every  
minute due to  
phishing attacks

[Top cybersecurity facts, figures and statistics for 2020, March 2020](#)

Almost all of these businesses now use a padlock and a form of encryption. That's why companies like us—who aren't willing to risk their brand name or customers' security—use EV SSL certificates.

**Phishing attacks**  
account for more than  
**80%** of reported  
security incidents

[Top cybersecurity facts, figures and statistics for 2020, March 2020](#)

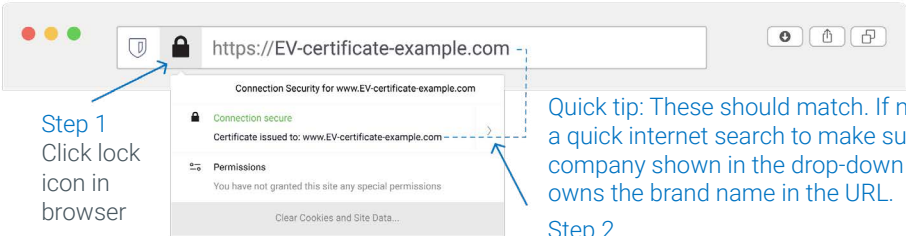
EV SSL certificates are the best way to guard against phishing attacks. That's why companies like us—who aren't willing to risk their brand name or customers' security—use EV.

# Visual support to help customers identify validated sites

You can view TLS/SSL certificates in your web browser of choice by following the steps below. Please see the step-by-step examples provided for Firefox, Safari and Chrome browsers.

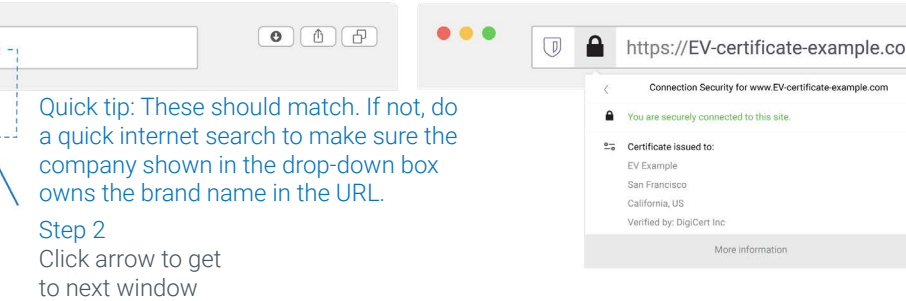
## Firefox

Step 1  
Click lock icon in browser

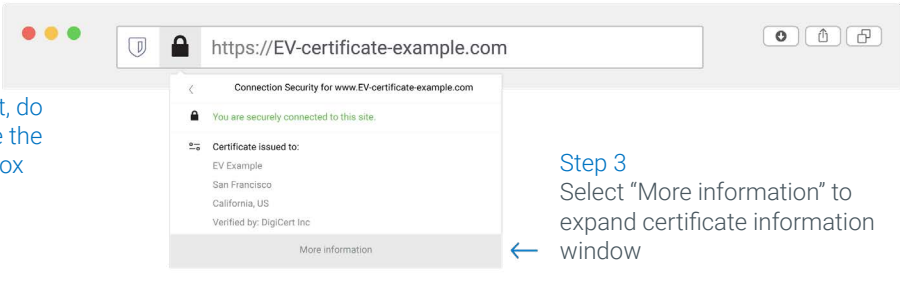


Quick tip: These should match. If not, do a quick internet search to make sure the company shown in the drop-down box owns the brand name in the URL.

Step 2  
Click arrow to get to next window



Step 3  
Select "More information" to expand certificate information window



### Domain Validated SSL (DV) Certificate

Certificate

www.DV-certificate-example.com	Organization Validated Server	Organization Validated Root
<b>Subject Name</b> Common Name www.DV-certificate-example.com		
<b>Issuer Name</b> Country US Organization DigiCert Inc Common Name DigiCert Global CA G2		
<b>Validity</b> Not Before 3/3/2020, 5:00:00 AM (Mountain Daylight Time) Not After 8/1/2020, 6:00:00 AM (Mountain Daylight Time)		

### Organization Validated SSL (OV) Certificate

Certificate

www.OV-certificate-example.com	Organization Validated Server	Organization Validated Root
<b>Subject Name</b> Country or Region US State/Province California Locality San Francisco Organization OV Certificate Example Common Name www.OV-certificate-example.com		
<b>Issuer Name</b> Country US Organization DigiCert Inc Common Name DigiCert Global CA G2		
<b>Validity</b> Not Before 3/3/2020, 5:00:00 AM (Mountain Daylight Time) Not After 8/1/2020, 6:00:00 AM (Mountain Daylight Time)		

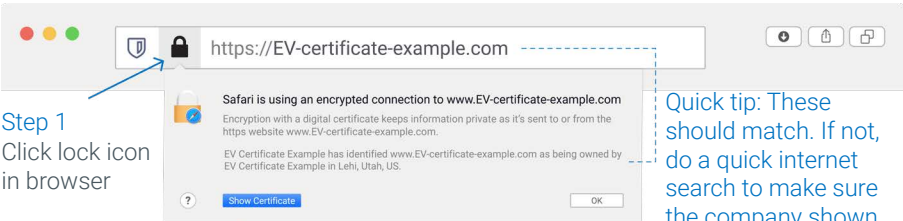
### Extended Validation SSL (EV) Certificate

Certificate

www.EV-certificate-example.com	Extended Validated Server	Extended Validated Root
<b>Subject Name</b> Business Category Private Organization Inc. Country/Region US Inc. State/Province California Serial Number 251212 Country or Region US State/Province California Locality San Francisco Organization EV Certificate Example Organizational Unit DCG-PSG Common Name www.EV-certificate-example.com		
<b>Issuer Name</b> Country US Organization DigiCert Inc Organizational Unit www.EV-certificate-example.com Common Name DigiCert Global CA G2		
<b>Validity</b> Not Before 3/3/2020, 5:00:00 AM (Mountain Daylight Time) Not After 8/1/2020, 6:00:00 AM (Mountain Daylight Time)		

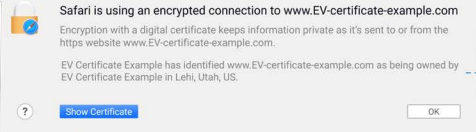
# Safari

Step 1  
Click lock icon in browser

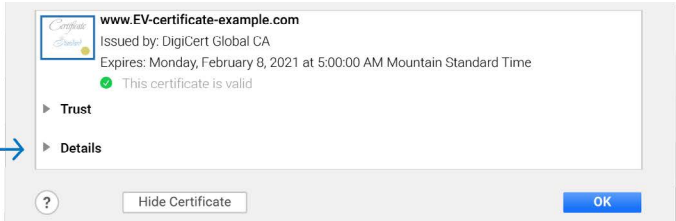


Quick tip: These should match. If not, do a quick internet search to make sure the company shown in the drop-down box owns the brand name in the URL.

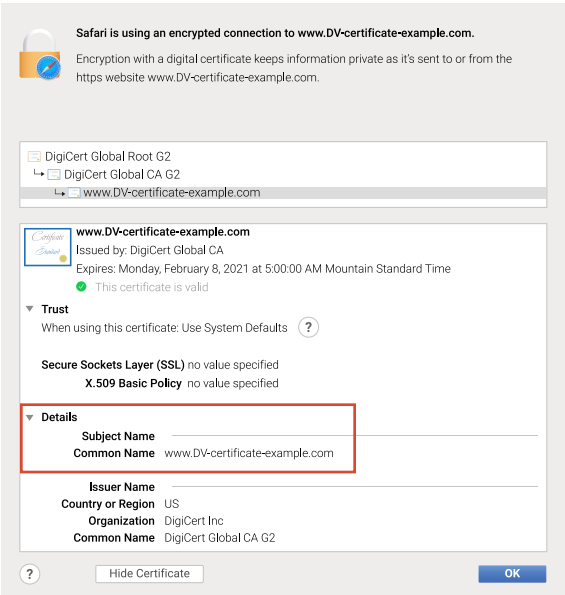
Step 2  
Select "Show Certificate" to expand window



Step 3  
Click gray triangle to expand to see details



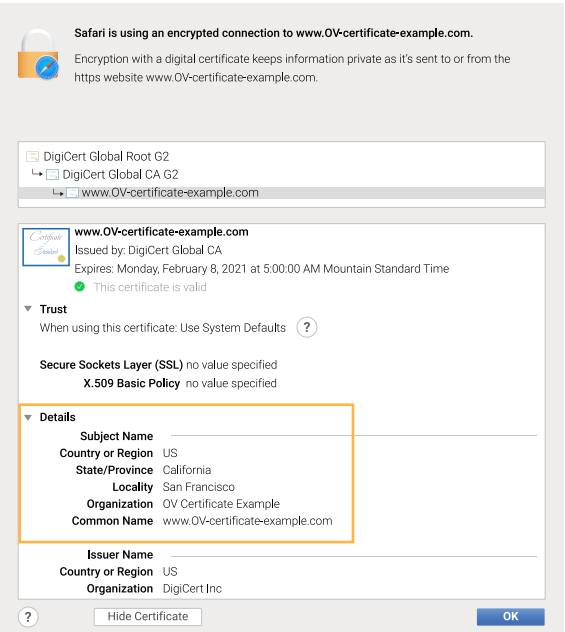
## Domain Validated SSL (DV) Certificate



**Details**

Subject Name	www.DV-certificate-example.com
Common Name	www.DV-certificate-example.com

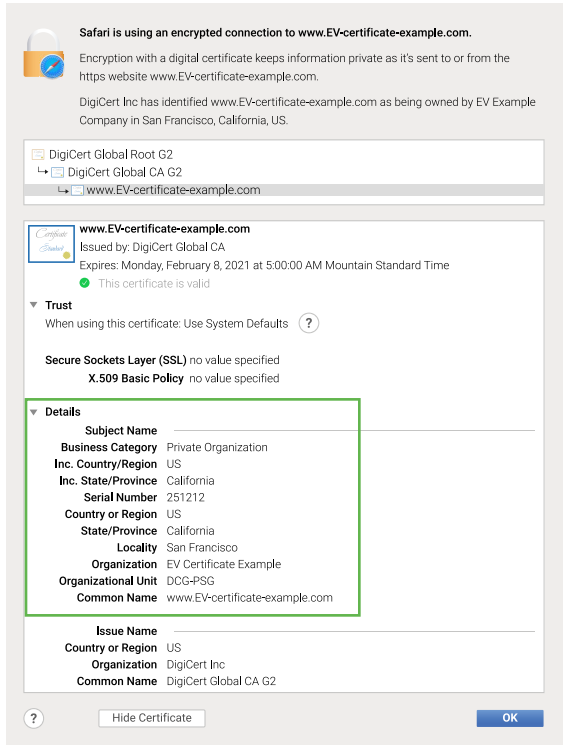
## Organization Validated SSL (OV) Certificate



**Details**

Subject Name	
Country or Region	US
State/Province	California
Locality	San Francisco
Organization	OV Certificate Example
Common Name	www.OV-certificate-example.com

## Extended Validation (EV) SSL Certificate

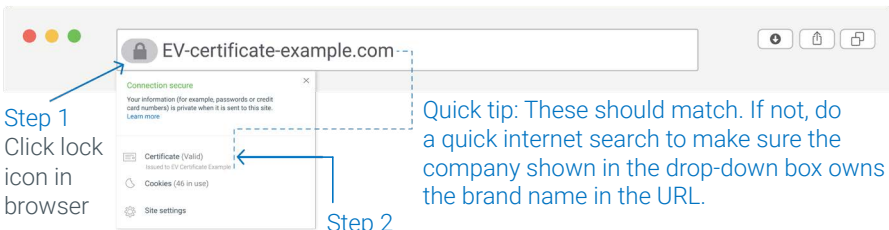


**Details**

Subject Name	
Business Category	Private Organization
Inc. Country/Region	US
Inc. State/Province	California
Serial Number	251212
Country or Region	US
State/Province	California
Locality	San Francisco
Organization	EV Certificate Example
Organizational Unit	DCG-PSG
Common Name	www.EV-certificate-example.com

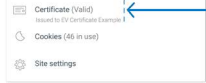
# Chrome

Step 1  
Click lock icon in browser

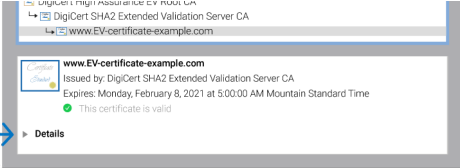


Quick tip: These should match. If not, do a quick internet search to make sure the company shown in the drop-down box owns the brand name in the URL.

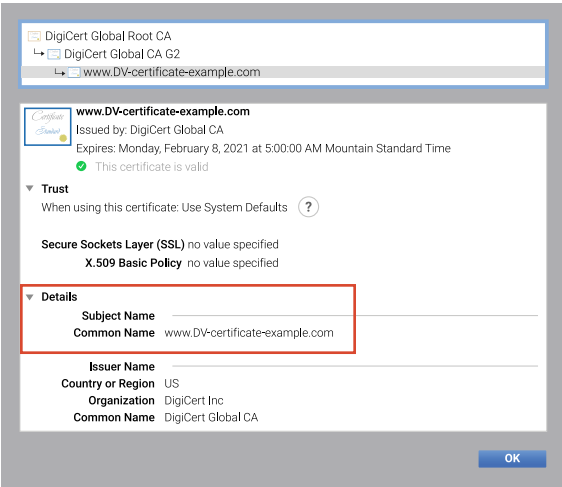
Step 2  
Select "Certificate" to expand certificate details window



Step 3  
Click gray triangle to expand to see details



## Domain Validated SSL (DV) Certificate



**Trust**  
When using this certificate: Use System Defaults

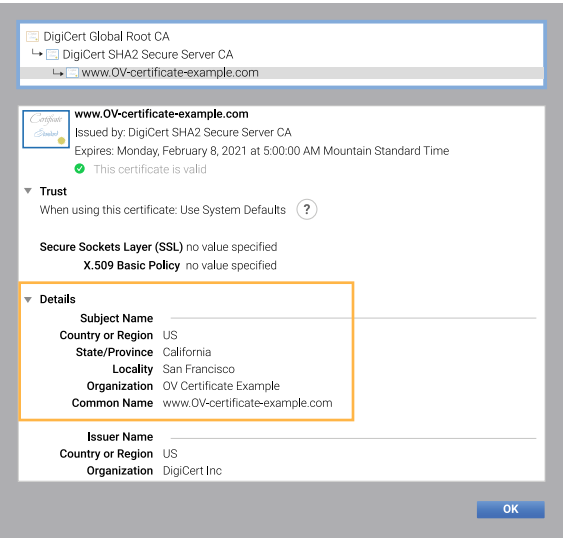
**Secure Sockets Layer (SSL)** no value specified  
**X.509 Basic Policy** no value specified

**Details**

Subject Name	
Common Name	www.DV-certificate-example.com
Issuer Name	
Country or Region	US
Organization	DigiCert Inc
Common Name	DigiCert Global CA

OK

## Organization Validated SSL (OV) Certificate



**Trust**  
When using this certificate: Use System Defaults

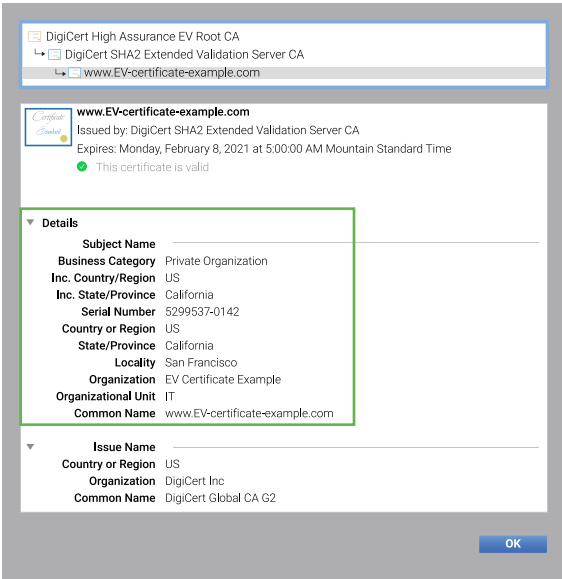
**Secure Sockets Layer (SSL)** no value specified  
**X.509 Basic Policy** no value specified

**Details**

Subject Name	
Country or Region	US
State/Province	California
Locality	San Francisco
Organization	OV Certificate Example
Common Name	www.OV-certificate-example.com
Issuer Name	
Country or Region	US
Organization	DigiCert Inc

OK

## Extended Validation SSL (EV) Certificate



**Trust**  
When using this certificate: Use System Defaults

**Secure Sockets Layer (SSL)** no value specified  
**X.509 Basic Policy** no value specified

**Details**

Subject Name	
Business Category	Private Organization
Inc. Country/Region	US
Inc. State/Province	California
Serial Number	5299537-0142
Country or Region	US
State/Province	California
Locality	San Francisco
Organization	EV Certificate Example
Organizational Unit	IT
Common Name	www.EV-certificate-example.com
Issue Name	
Country or Region	US
Organization	DigiCert Inc
Common Name	DigiCert Global CA G2

OK

## Securely browse the web

Not all web browsers are created equal. When it comes to your online privacy and security, some web browsers are secure but collect more data to track and market your activity around the internet. For the highest level of privacy and security, Fast Company recommends using these three browsers:

1. [Firefox](#) – Can be configured to block cookies & data collection
2. [Brave](#) – Forces HTTPS secure encryption on all websites
3. [Tor](#) – Can disguise your location

## More tips for safely browsing the web:

### Use more than one browser

For example, only use Safari for your personal accounts, and Firefox for internet browsing or vice versa.

### Review SSL certificates

View more details within the address bar by clicking on the padlock icon. Make sure the website you're viewing is verified.

### Avoid "Not Secure" websites

Websites with the "Not Secure" message do not use SSL certificates and your data could be intercepted by hackers.

We are committed to your online security and that is why we've implemented a high-assurance EV SSL certificate from DigiCert on our website. To learn more about why SSL certificates matter, click [here](#).

