

# Error Messages, IT and System Issues

## What should I do if my system is down?

If you receive a 404 Error, or cannot log into the system and receive an error page instead, please see the SuperControl status page below for the latest updates on System Performance:

<https://www.supercontrolstatus.co.uk/> On this page you can subscribe to receive system alerts which is handy so you know the real time situation and receive updates the moment they are posted.

From time to time you may receive a denial of access from Incapsula:

<https://help.supercontrol.co.uk/m/73864/l/934113-why-am-i-receiving-an-access-denied-message-from-incapsula>

# Why am I receiving an "Access denied" message from Incapsula?

Our WAF system blocks your application due to suspicious behaviour.

This can be related with two things:

**First thing:** Your application doesn't have proper security (WAF etc.) and someone can scan your webpage to find a weak point.

Now is time to take action and protect your web page with the WAF. On the market is a lot of the solutions. One of them are standalone but this will be no needed to you. In your case we propose a cloud WAF one of the proposal below:

<https://www.cloudflare.com/plans/> but you can pick one that you think is best for your business.

**Second thing:** If you have WAF but still get the block screen ask your developer about any code changes as there can be a wrong request which can be treated like a potential attack.

If you want to get confirmation or you are unsure, please deliver the incident ID. Below we mark where to find this:

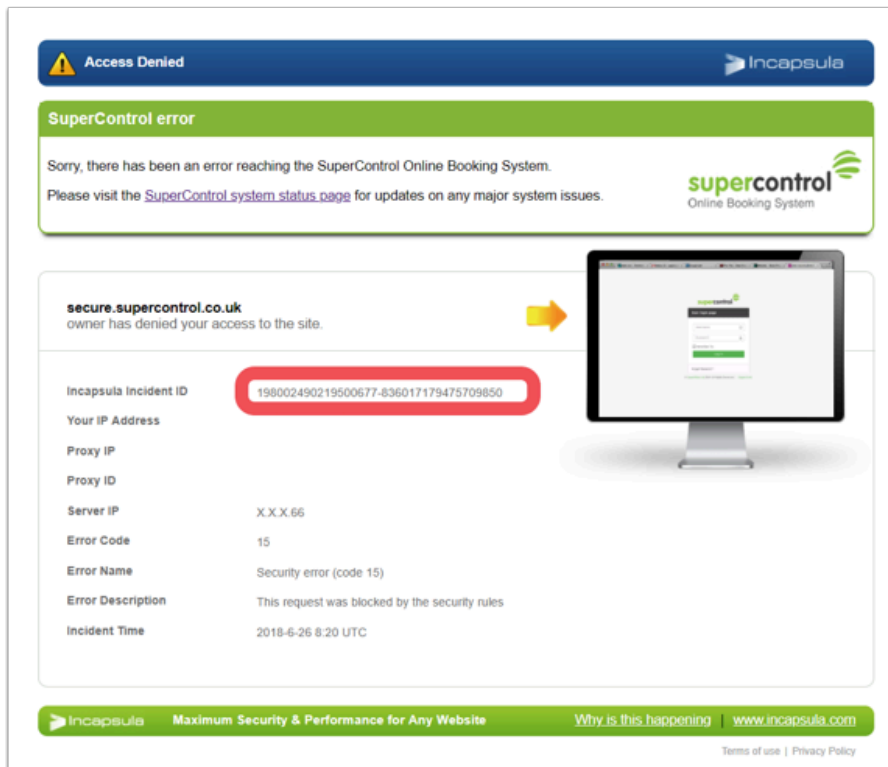
## Technical terms used in the instructions:

**WAF** - Web application firewall. Security system protects the application from attacks and suspicious actions.

**Whitelist** - Function on WAF that allows use of SuperControl without any security restrictions.

**Standalone** - Physical or virtual machine/environment where the customer/owner is fully responsible for working and configuration.

**Cloud** - Hosted on the "share" physical infrastructure but only the owner has access to this account for configuration.



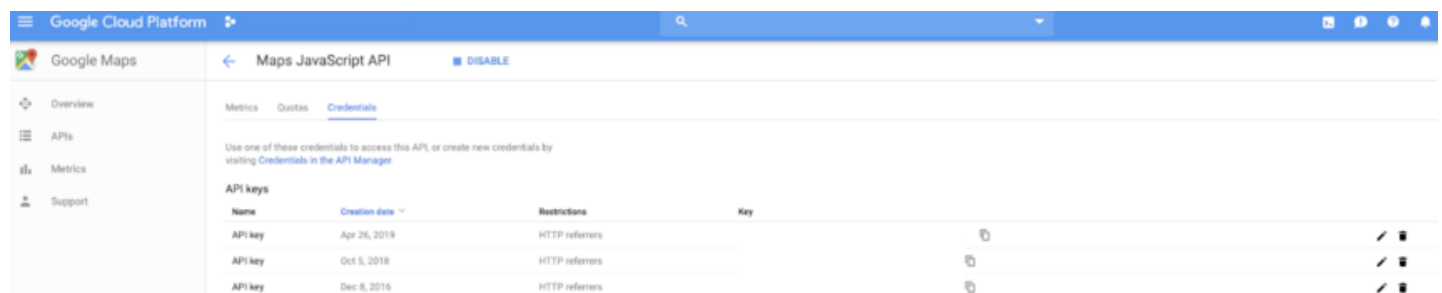
Once we receive this the support team will help solve this issue. We know this can highly impact your business and in 99% we can resolve this type of the problems in 2 hours.

## Why am I seeing on Google Maps "Referrer Not Allowed error and maps are not loading on my website"?

### Step 1:

You need to whitelist our domain.

Within Google Maps API Console - you need to find your key and click edit.



Under Website Restrictions, click Add an item:

Google Cloud Platform

APIs & Services

Restrict and rename API key

REGENERATE KEY DELETE

Name \*

API key

**Key restrictions**

Restrictions help prevent unauthorized use and quota theft. [Learn more](#)

**Application restrictions**

An application restriction controls which websites, IP addresses, or applications can use your API key. You can set one application restriction per key.

☐ None

☒ HTTP referrers (web sites)

☐ IP addresses (web servers, cron jobs, etc.)

☐ Android apps

☐ iOS apps

**Website restrictions**

Restrict key usage requests to the specified websites.

⚠ If left blank, your API key will accept requests from any website.

ADD AN ITEM

You should then enter the following and click Done.

**\*.supercontrol.co.uk/\***

**\*.supercontrol.co.uk/\***

New item

Referer \*

\*.supercontrol.co.uk/\*

CANCEL DONE



Please also ensure Application Restrictions is set to HTTP Referrers.

### Application restrictions

An application restriction controls which websites, IP addresses, or applications can use your API key. You can set one application restriction per key.

- ☐ None
- ☒ HTTP referrers (web sites)
- ☐ IP addresses (web servers, cron jobs, etc.)
- ☐ Android apps
- ☐ iOS apps

For more information, you can follow this guide.

[https://developers.google.com/maps/documentation/javascript/get-api-key#restrict\\_key](https://developers.google.com/maps/documentation/javascript/get-api-key#restrict_key)

## Step 2:

Once the above has been completed, ensure that within your SuperControl account you have entered your Google API key. This can be added via Admin menu > Website integration > Additional content.

This will then resolve the Referer Not Allowed error.

## macOS / Mac OS X Invalid SSL

Occasionally older MacOS / Mac OS X systems may not have the required SSL certificate chains needed to access SuperControl and will result in an SSL error indicating that your connection to this site is not secure.

The easiest solution is to [upgrade your OS X installation](#) - this usually resolves the issue and ensures your Mac has all the latest security updates. If this is not possible then the following instructions should enable you to use SuperControl in a secure way without having to forceably accept the certificate.

Applies to:

- OS X El Capitan 10.11
- macOS Sierra 10.12
- macOS High Sierra 10.13
- macOS Mojave 10.14
- macOS Catalina 10.15

Components affected:

- Safari
- Google Chrome
- Mozilla FireFox
- Apple Keychain Access

Prerequisites:

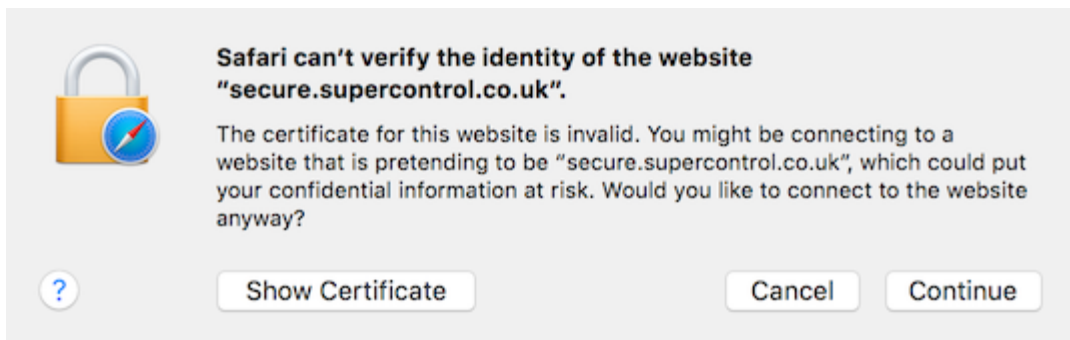
- Basic Mac knowledge, downloading and opening files
- Basic Keychain Access knowledge

To resolve this issue please follow the steps below.

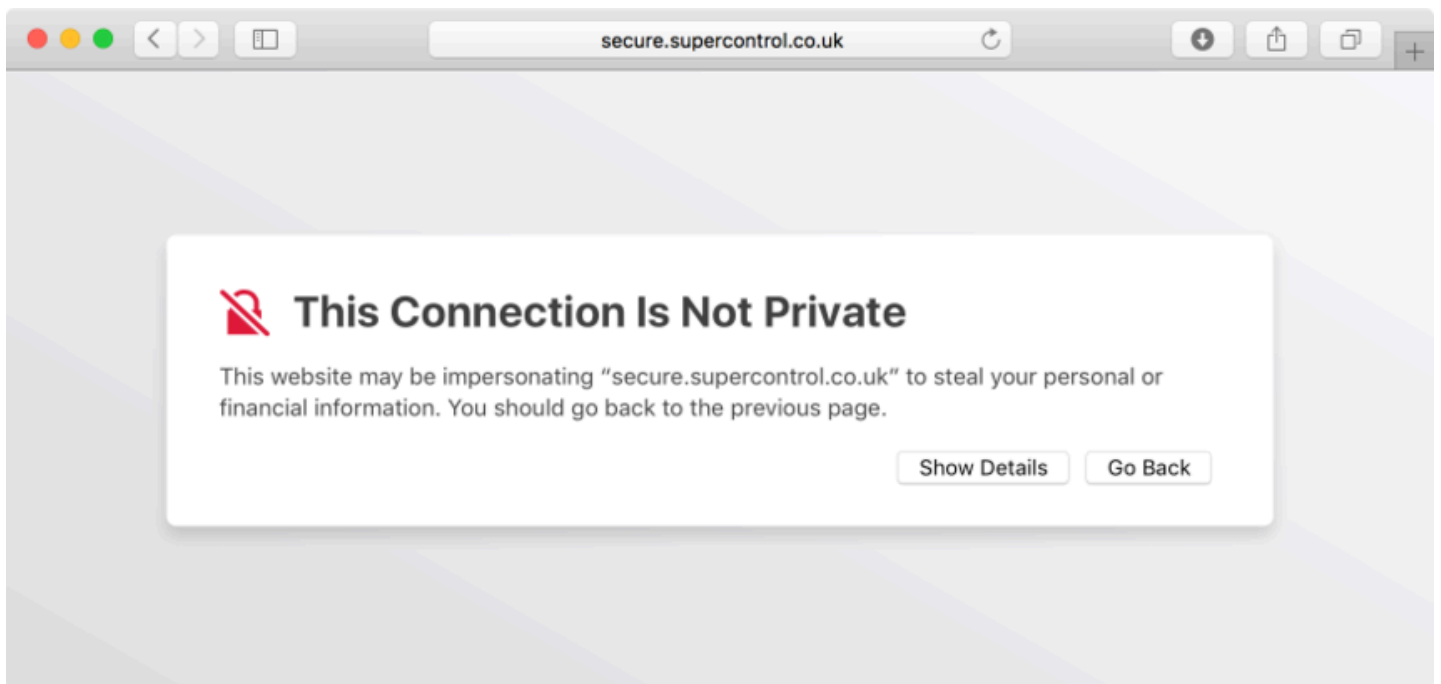


Care should be taken when following these steps. Should you have any questions please raise a support ticket.

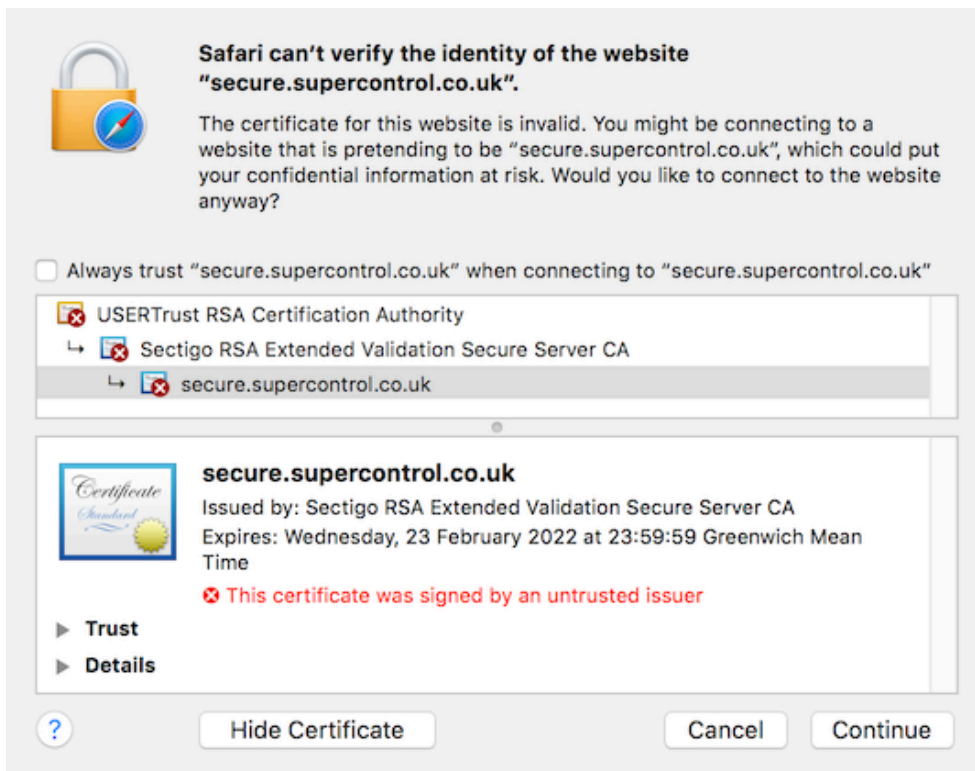
In Safari the following error will be shown:




Or on later versions of Safari:

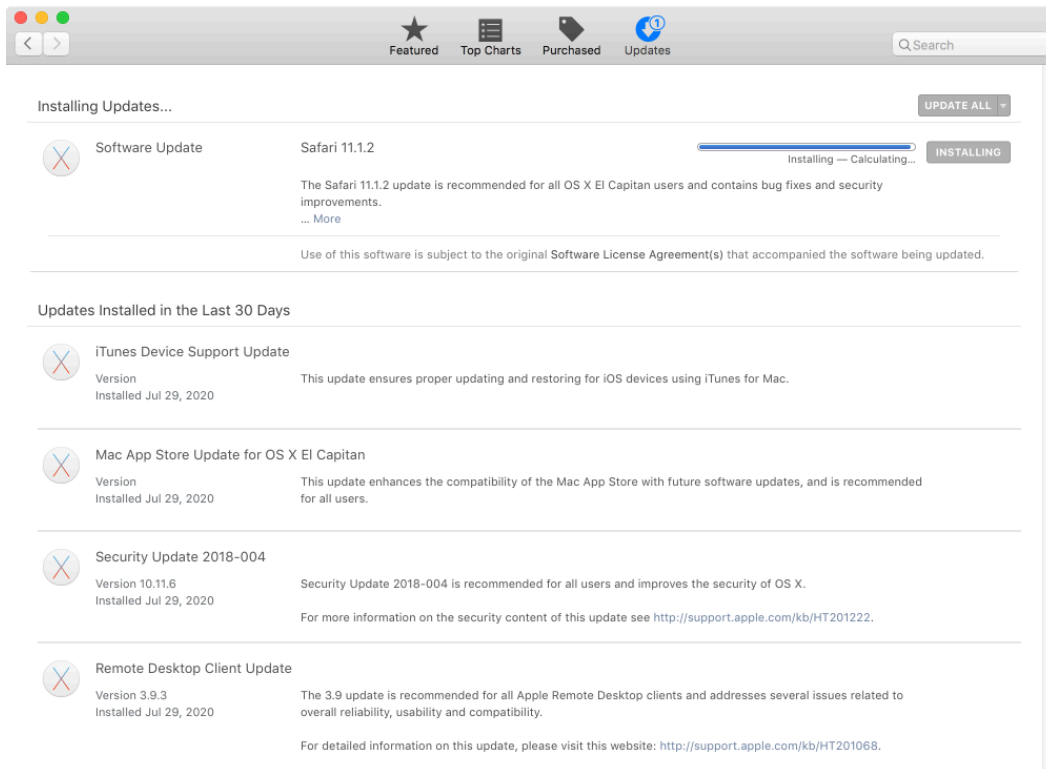


Selecting Show Certificate / Show Details will indicate that the SSL Certificate is invalid:



## Software update

-  Ensure all [software updates](#) are installed for your version of macOS / OS X via Software Update.

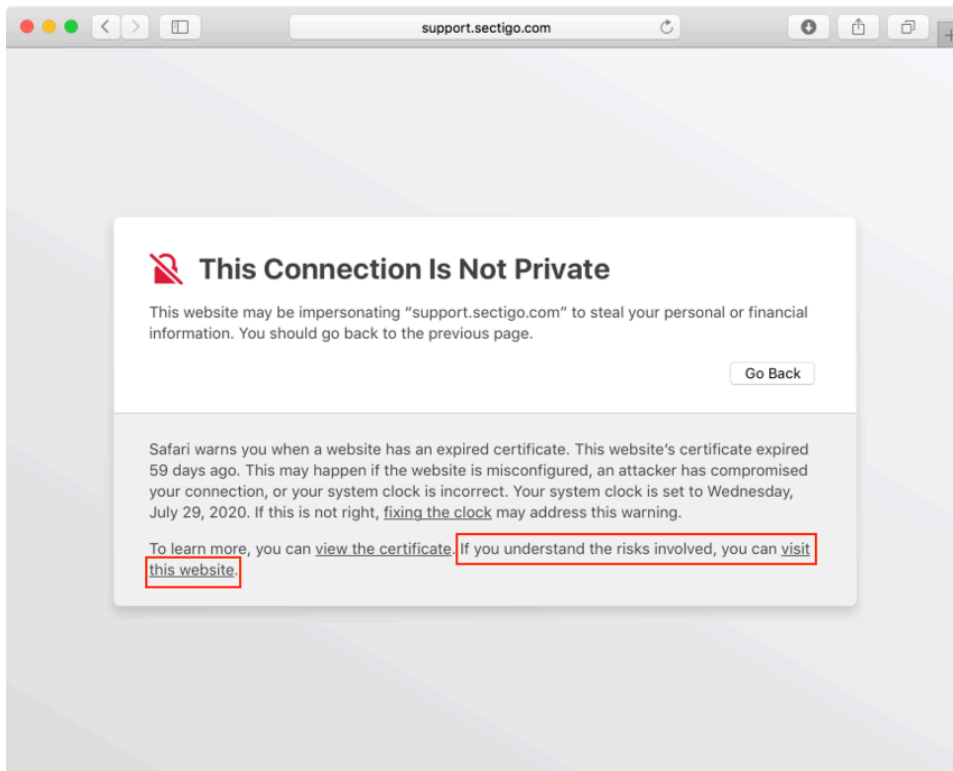


## Download and install certificate chain

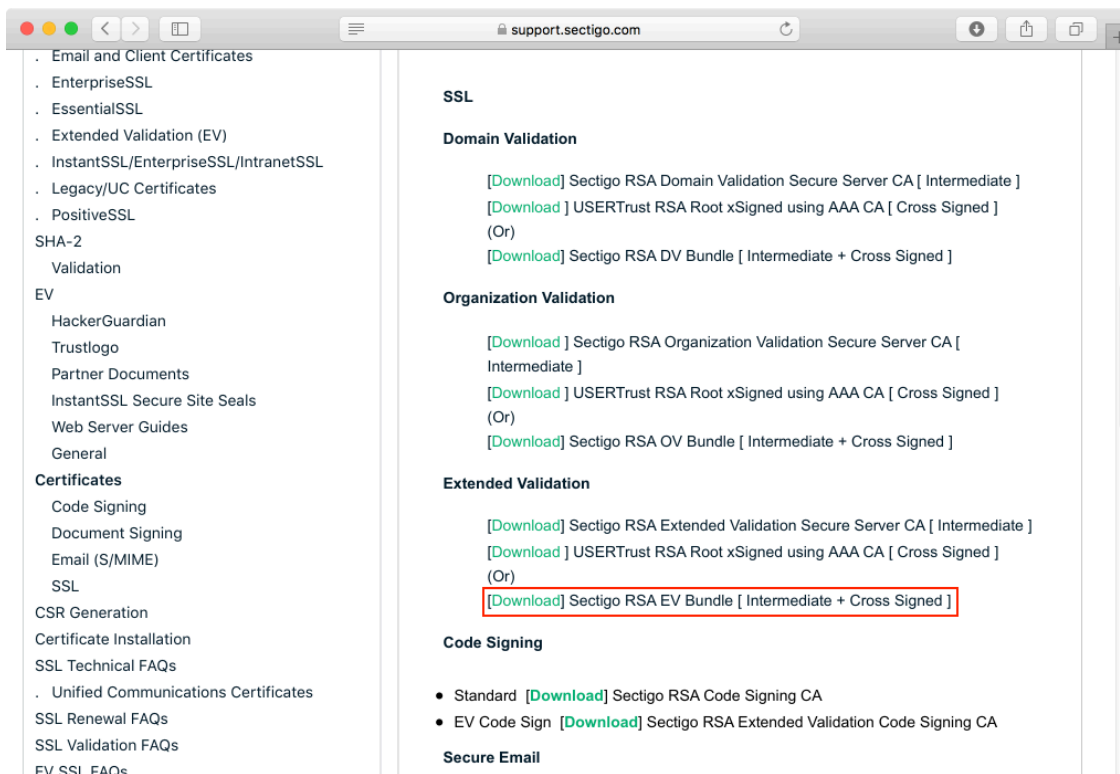
Visit [https://support.sectigo.com/Com\\_KnowledgeDetailPage?Id=kA01N000000rfBO](https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA01N000000rfBO)

If you receive a SSL error click Show Details and visit this website and confirm that you wish to visit this website. You may be prompted to enter your password to allow this.

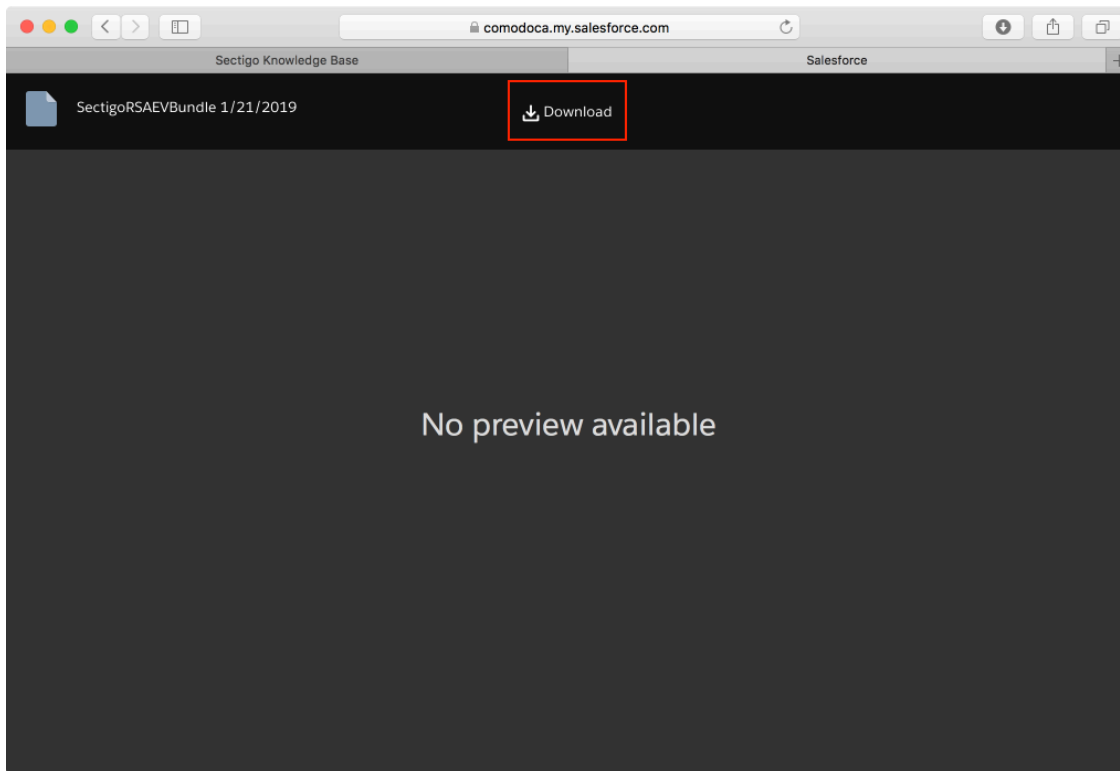




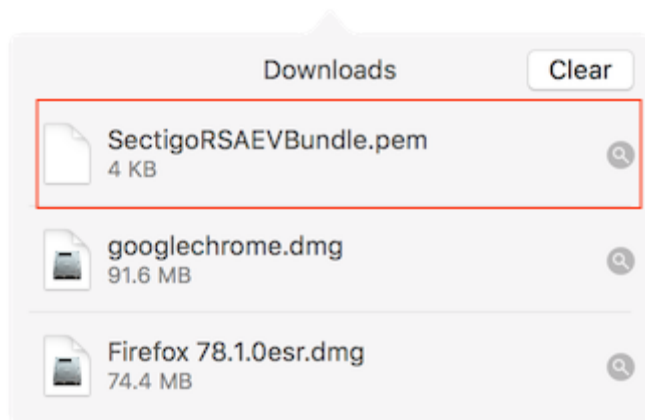
Scroll down to Extended Validation and select [\[Download\] Sectigo RSA EV Bundle \[Intermediate + Cross Signed\]](#) .



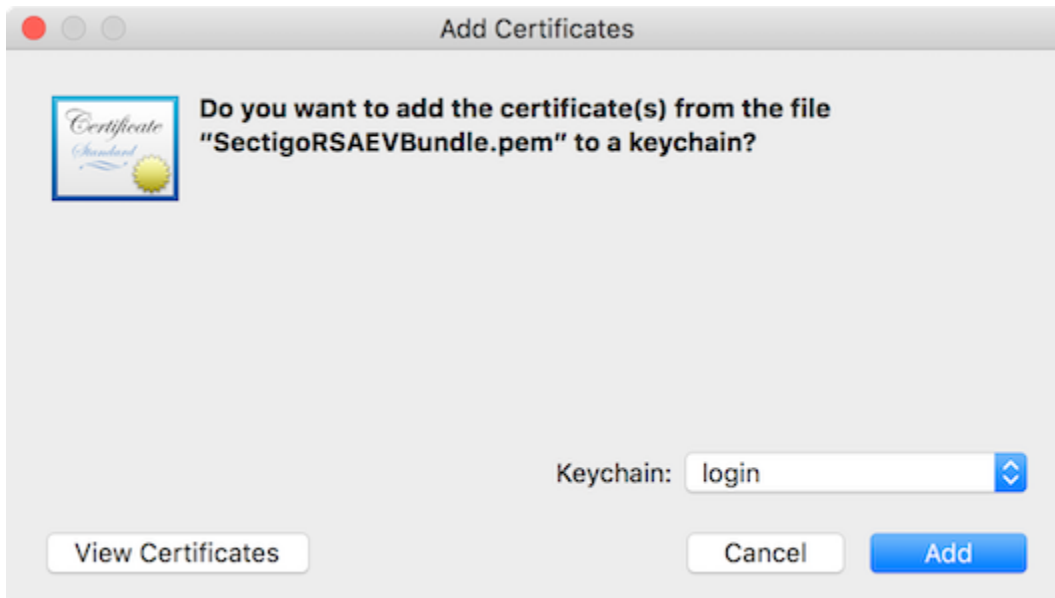
When redirected, click on the Download link at the top of this page:



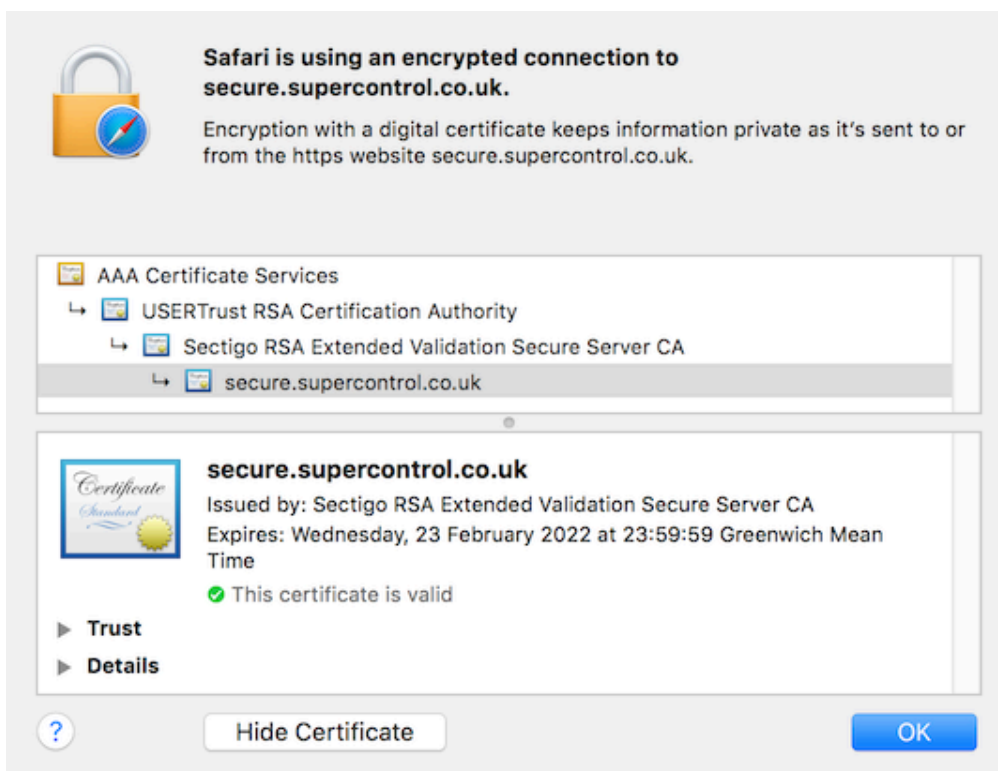
Once downloaded - click on the newly downloaded file to open it:



This should open up Keychain Access where you can add the new certificate bundle - accept the defaults and click add.



Reloading SuperControl in your browser should now accept the SSL certificate and no errors will be shown.



All browsers will now recognise the SSL certificate used by SuperControl - no further action is required for Google Chrome or Mozilla FireFox.

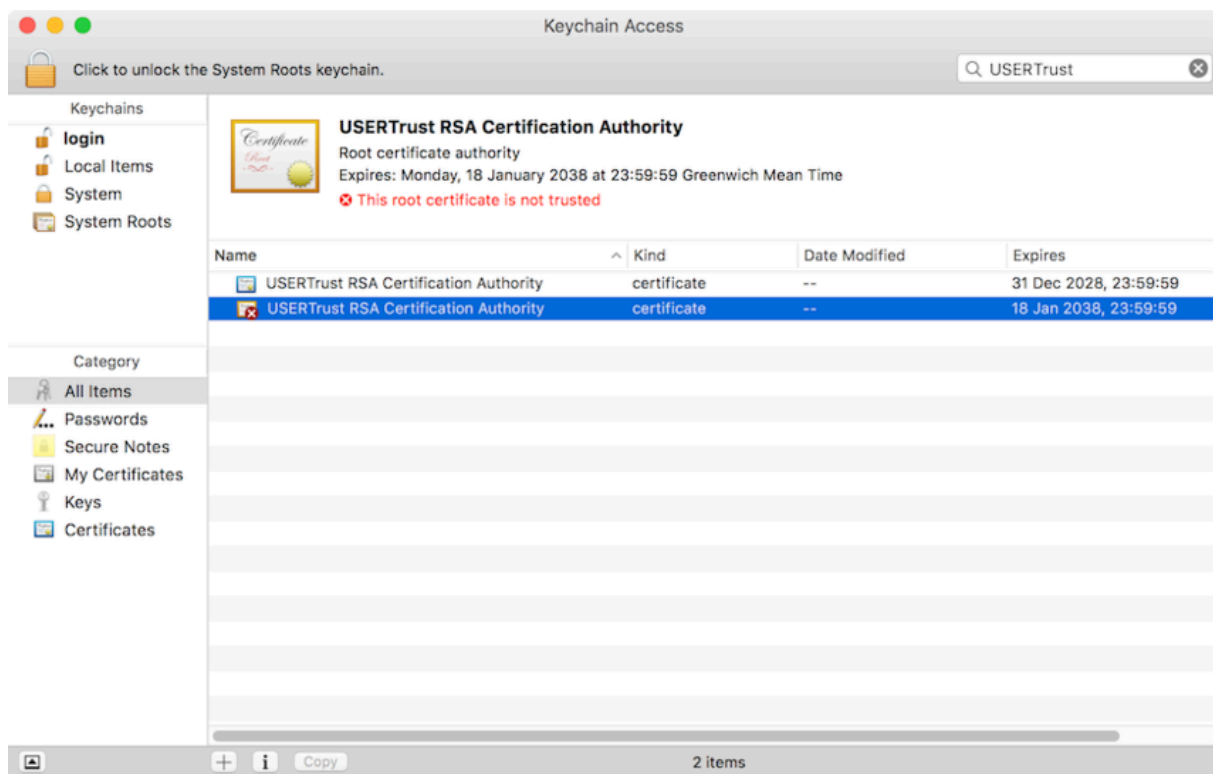
## Optional steps

💡 For additional compatiability you can also download the following certificate bundles following the steps above to add these to your system:

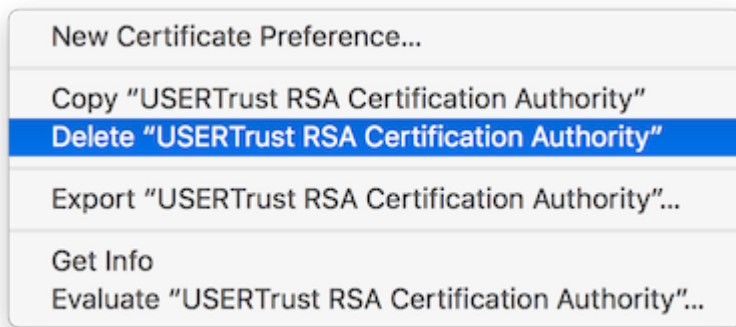
- [Download] Sectigo RSA DV Bundle [ Intermediate + Cross Signed ]
- [Download] Sectigo RSA OV Bundle [ Intermediate + Cross Signed ]
- [Download] SHA-2 Root : USERTrust RSA Certification Authority

## Optional - delete untrusted USERTrust RSA Certification Authority from Keychain Access

In the Keychain Access app search all items for USERTrust:



Right click and select delete.



## Archive



SectigoRSA.zip