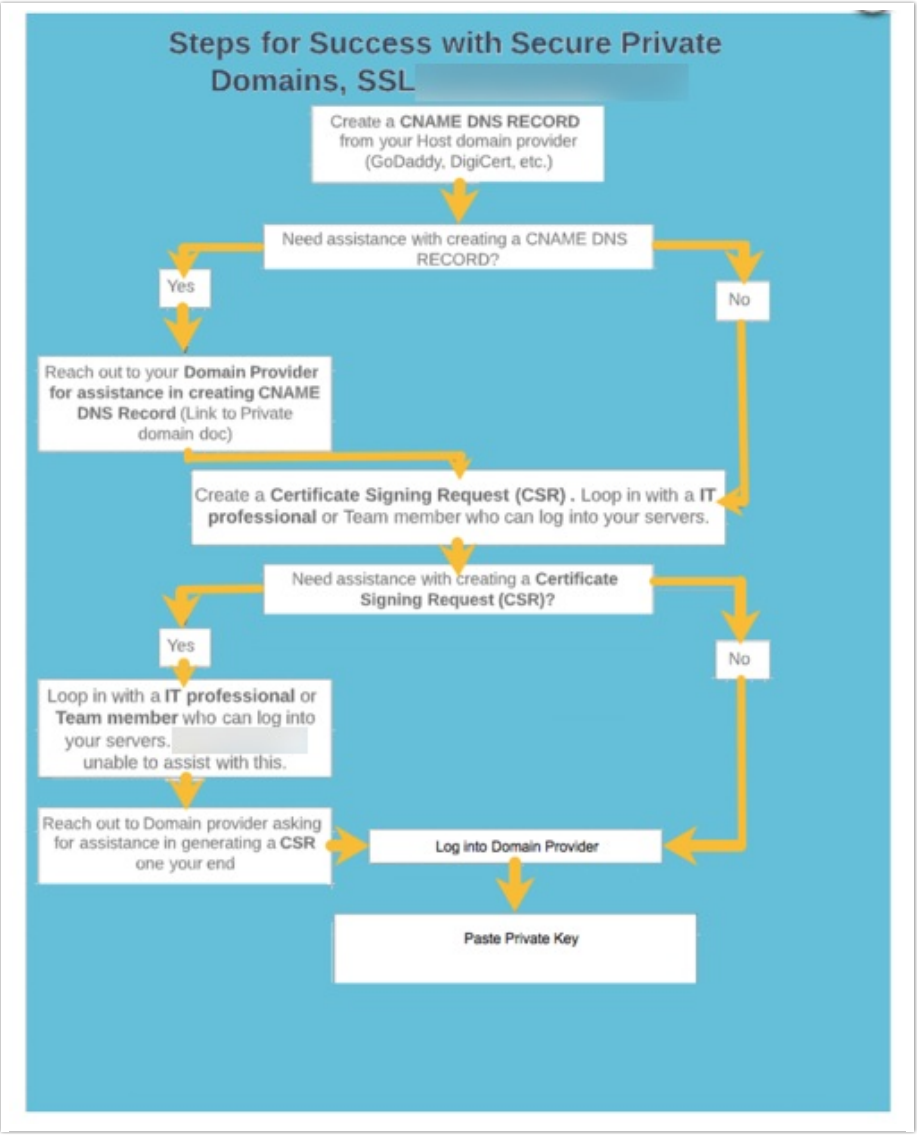
Set Up a Secure Private Domain

> Alchemer Accounts have access to create one private domain. Additional domains are available for purchase.

In order to create a secure link that uses your private domain, you'll need to set up your SSL certificate within Alchemer. *We are no longer able to set up/renew your SSL certificate for you.*

The process to create a secure private domain is as follows. Each step is marked with who owns that portion of the process, representing who to reach out to for additional questions and support:



What is an SSL certificate?

> Alchemer requires an SSL provided by a domain provider and will not validate on a self-signed certificate.

Secure Socket Layer (SSL) is an extra layer of security used to transport data safely between client (respondent) and survey by using an encryption algorithm. SSL is used when links are set up to use the secure https protocol. An SSL certificate is necessary to create an SSL connection for a given domain. When an internet user attempts to send confidential information to a web server, the user's browser accesses the server's SSL certificate and establishes a secure connection.

SSL Setup

Creating an SSL Certificate is a process that is owned by the **Domain provider** (GoDaddy, DigiCert, etc.). For assistance in setting up and creating SSL Certificates, reach out to your specific domain provider. To create an SSL, one must have completed the steps found in the Set up a Private Domain documentation. Follow the aforementioned link to begin setting up a private domain in Alchemer. Alchemer does **NOT** support SSL creation as what is needed for success is owned by the domain provider.

If you indicated that you wish to set up a Custom SSL Certificate when setting up your Private Domain, your final step in the setup process is to provide the following pieces of information which will be supplied by your domain provider, aka certificate authority, (ex. GoDaddy):

- Private Key
- Certificate
- Root & Intermediate Bundle

If your domain is managed by an IT professional at your organization, you will **need** to loop them in. If you do not have IT assistance, your domain provider (ex. GoDaddy) will be able to assist you in this process.

Paste your Private Key, Certificate, and Root & intermediate Bundle into the corresponding fields and click **Save Settings**. *These should be in Privacy Enhanced Mail (PEM) format for Apache servers.*

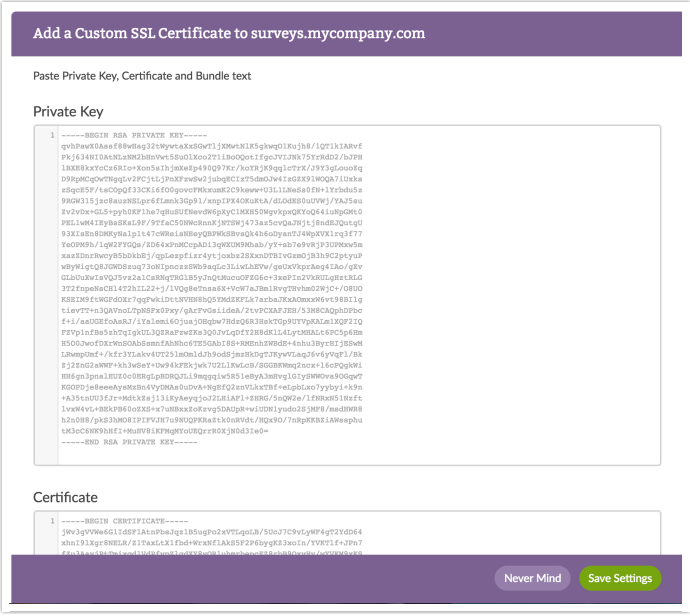
Private Keys Cannot Be Encrypted

The key must in in an unencrypted RSA format to have a successful setup. To un-encrypt the key you can do the following:

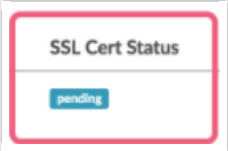
1. Put the password-protected key in a folder.
2. Open a command prompt
3. Go to the OpenSSL\bin directory
4. Run the command C:\OpenSSL-Win64\bin>set OPENSSL_CONF=c:\OpenSSL-Win64\bin\openssl.cfg

5. Run the command openssl.exe rsa -in d:\cert\server.key -out D:\cert\serverd.key to decrypt the private key
6. Enter the private key password when prompted
7. Open the file to verify that the text "ENCRYPTED" is no longer there

If you navigated away from your domain you can return to **Integrations** > **Custom Domains**, edit your domain and click the **Setup** button under **Custom SSL Certificate**.



On saving, Alchemer will do some initial validation checks to ensure that the format is correct. After saving, your SSL Cert Status will show as pending while the system validates with your certificate authority. It can take up to 30 minutes to validate your certificate.



SSL Certificate Statuses and Error States

There are five possible SSL Cert Statuses.

- **Pending** - This displays for recently added SSL certs. Certs will display as pending until they are verified with the certificate authority and subsequently installed.
- **Valid** - Active, valid certificate.
- **Revoked** - Revoked by the certificate authority or certificate authority is no longer valid.
- **Expired** - Certificate is expired/no longer valid. The cert will stay installed until you replace it.

Depending on the survey taker's browser they may still be able to bypass security warning to proceed to your survey.

- **Expiring Soon** - Certificate has 60 or fewer days until expiration. Learn how to update your certificate in the Certificate Expiration section of this tutorial.

Updating an Expired Certificate

In your list of domains under **Integrations > Custom Domains**, the certificate expiration date is available for review. As this date nears we will send emails to all users set up as account administrators. An initial email will be sent when there are 60 days left before your certificate expires. Two additional reminder emails will be sent at 30 days and 0 days until expiration. *Please ensure that admin users' email addresses are valid to ensure that critical notifications like these are received. Need to change your email address?*

To update your certificate you'll first need to renew your certificate with your domain provider. You'll again need the following information from your domain provider:

- Private Key
- Certificate
- Root & Intermediate Certificate Bundle

When you have your renewed certificate info, go to Integrations > Custom Domains and select your domain to edit. Click **Replace** and confirm that you wish to replace your current certificate by clicking **Update Certificate**.

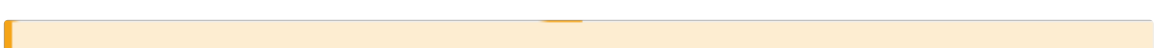
Paste the Private Key, Certificate, and Root & Intermediate Certificate Bundle into the corresponding fields and click **Save Settings**. Your SSL Cert Status will show as pending while it is validated by the system. It can take up to 20 minutes to validate your certificate.

Overview of Steps to Obtain a Certificate

Generating a CSR is the first step towards setting up an SSL and it ***must*** be done on the user's end. This document is from GoDaddy and notes how to set up a CSR and this document is for DigiCert outlining the same process for their domains. One will need to reach out to their specific domain provider for obtaining a certificate

As much as we LOVE to help our customers, it is important that you obtain your own certificate. This way, the certificate will be in *your organization's name and will be controlled by you*. Below we cover the steps to obtain a certificate at a high level as this looks different depending on your operating system and the certificate authority you choose to work with.

1. Generate a Certificate Signing Request (CSR). These steps vary depending on your operating system but here are a few helpful docs on doing so. There is a more robust list of domain providers in the FAQ section:Gener
    - https://www.thesslstore.com/blog/what-is-a-csr/
    - https://www.godaddy.com/help/apache-generate-csr-certificate-signing-request-5269
    - https://www.digicert.com/csr-ssl-installation/apache-openssl.htm



- Generating a CSR requires a different process based on the operating system in use.

2. Once you have created your CSR, you will paste or upload it into the order form on your certificate authority's website. The CA will use the information in your CSR to create a certificate for you. They will then provide you with the **Certificate and Root & Intermediate bundle** required to set up your SSL in Alchemer.

3. The **Private Key**, the final piece you need to complete your SSL set up in Alchemer, is created when you generate your CSR. This is found in the file that is created with your domain providers assistance

If you need help with these steps, your best resource will be your IT team or the Certificate Authority company.

Alchemer will not generate a Certificate Signing Request on behalf of your organization. It is important that one obtains their own certificate. The certificate will be in your or your organization's name and will be controlled by you.

Glossary of Terms

SSL - Secure Socket Layer (SSL) is an extra layer of security used to transport data safely between client (respondent) and survey by using an encryption algorithm. SSL is used when links are set up to use the secure https protocol.

SSL Certificate - SSL Certificates are small data files that digitally bind a cryptographic key to an organization’s details. A certificate serves as an electronic passport that establishes an online entity's credentials when doing business on the Web. When an Internet user attempts to send confidential information to a Web server, the user's browser accesses the server's digital certificate and establishes a secure connection.

Certificate Authority - Certificate Authorities, aka CAs, are companies that issue digital certificates that contain identity credentials to help websites, people, and devices represent their authentic online identity. A CA acts as a trusted third party. Some common CAs include GoDaddy, VeriSign, GeoTrust, Comodo, Symantec, Digicert, etc.

Certificate Signing Request (CSR) - A Certificate Signing Request is a file that contains information a Certificate Authority (or CA, the companies who issue SSL certificates) need to create your SSL certificate. A CSR is a request to have a certificate created and digitally signed by a Certificate Authority.

Private Key - The SSL protocol uses a pair of keys – one private, one public – to authenticate, secure, and manage secure connections. These keys are created together as a pair and work together during the SSL handshake process to set up a secure session. The **private key** is a text file used to secure and verify connections. *The private key should be closely guarded since anyone with access to it can use it in nefarious ways.*

Root & Intermediate Certificate Bundle - Many certificate authorities use an intermediate certificate as a stand-in for their root certificate in order to ensure that it remains secure. If your CA uses intermediate certificates the cert that they provide you with will have all certs as a "bundle" or "chain".

Revocation - From time to time certificates will be revoked for security reasons. If this happens for any reason you will need to obtain a new cert from your CA and replace your existing cert in Alchemer.

FAQ

Can Alchemer set up/renew my SSL certificate for me?
Alchemer previously offered to provision and renew SSL certificates as a service. This service is no longer offered and as such you will need set up your SSL certificate within Alchemer using the above instructions.

How can I find out who my domain administrator is?
Just visit the Whols database and type in your domain.

Are wildcard certificates supported?
Using wildcard certs is not recommended for security reasons but they are supported. Follow the above same setup process for wildcard certs.

Can Alchemer generate the Certificate Signing Request (CSR) for my domain?
As much as we LOVE to help our customers, it is important that you obtain your own certificate. This way, the certificate will be in your or your organization's name and will be controlled by you. If you need help with these, your best resource will be your IT team or the Certificate Authority company. Here are a couple of resources for generating CSRs:

- https://www.thesslstore.com/blog/what-is-a-csr/
- https://www.godaddy.com/help/apache-generate-csr-certificate-signing-request-5269
- https://www.digicert.com/csr-ssl-installation/apache-openssl.htm
- Comodo CSR Generation Instructions
- DigiCert CSR Generation Instructions
- Entrust CSR Generation Instructions
- GeoTrust CSR Generation Instructions
- Thawte CSR Generation Instructions

What is the expected format for the Private Key, Certificate, and Root & Intermediate Bundle fields?
These data placed in these fields should be in Privacy Enhanced Mail (PEM) format for Apache servers.

How long will it take to verify my certificate?
It can take up to 30 minutes to verify your SSL Certificate. Alchemer uses industry-standard Open SSL libraries to perform the verification.

Comodo CSR Generation Instructions

DigiCert CSR Generation Instructions

Entrust CSR Generation Instructions

GeoTrust CSR Generation Instructions

Thawte CSR Generation Instructions

SSL Resources

How to Create an SSL Certificate on a Windows Server

Digicert SSL Certificate Installation

How to Generate a CSR for Microsoft IIS 8

How to Install an SSL/TLS Certificate in Mac OS X El Capitan

Related Articles