Secure login with Paxton10

Overview

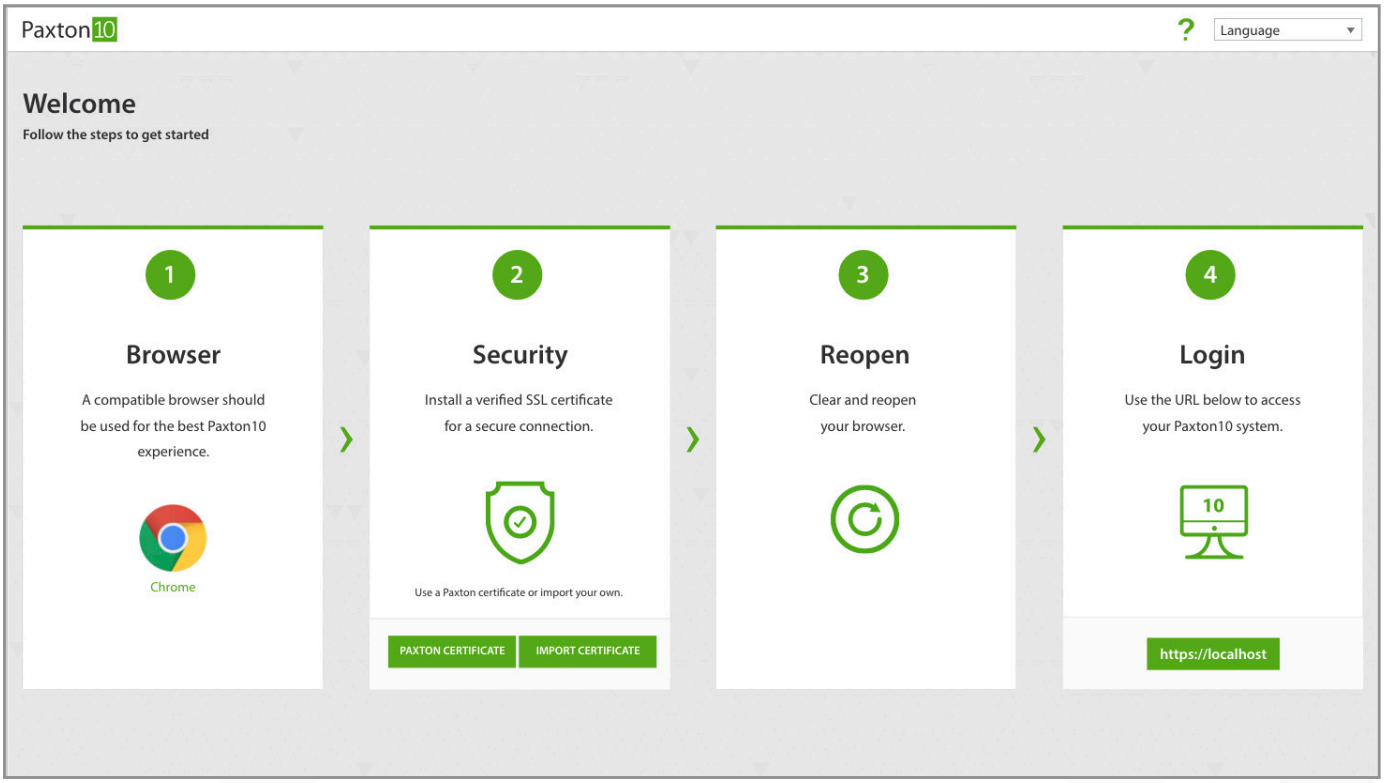
Paxton10 uses HTTPS to secure the communication between the client (your computer) and the Paxton10 server. Before logging in to Paxton10, it is advised to install an SSL/TLS certificate onto your computers and devices, for them to recognise the Paxton10 server and the encryption used.

There are two options: for a simple and fast solution we offer a Paxton certificate. You can also use your own certificate on your Paxton10 system.

Paxton10 setup page (Initial setup)

On the bottom of the Paxton10 server, there is an address in the form: http://Paxton10-xxxxxx/setup.

When first setting up your Paxton10 system, you can configure your certificate settings within this setup page. This can only be accessed on systems that have not yet been set up and have no user accounts, for security purposes. If you have already set up your system and want to manage your certificate settings, please scroll down to '**Updating certificate settings**'.

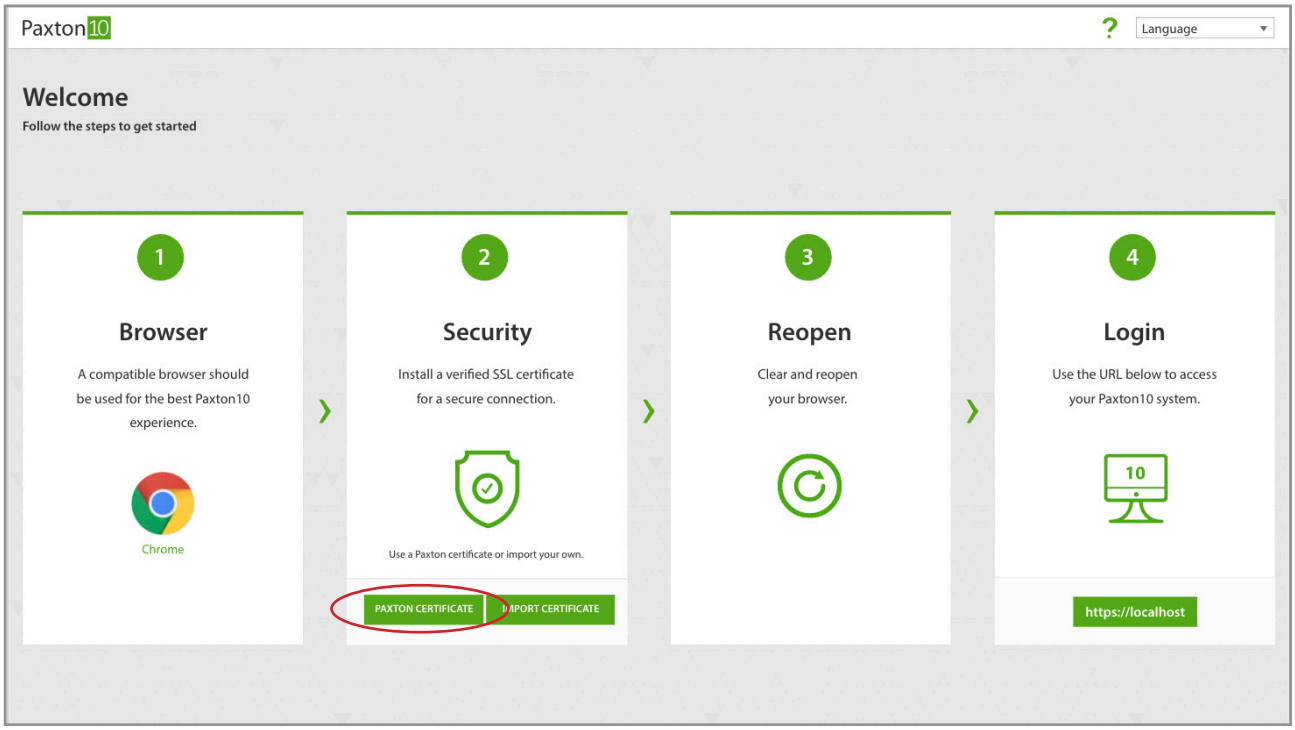


Using the Paxton certificate

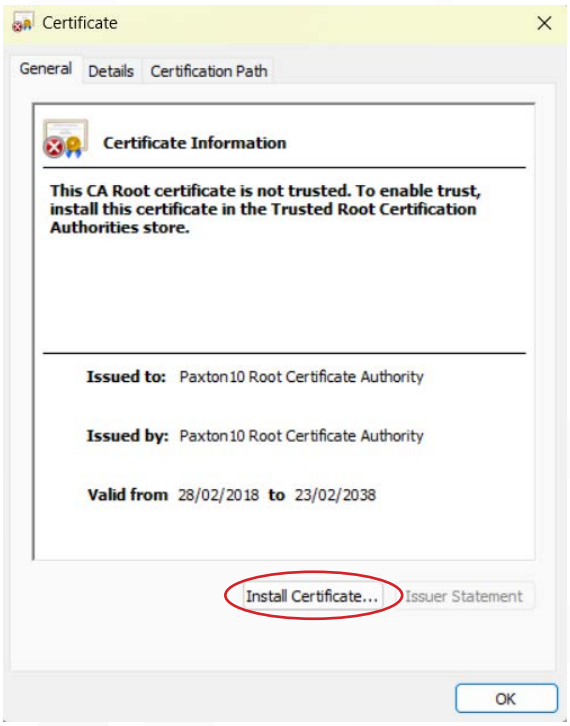
Please note; the Paxton10 system provides a default, self-signed SSL certificate from a common Root CA.

If you wish to use the certificate provided by Paxton, please follow these steps:

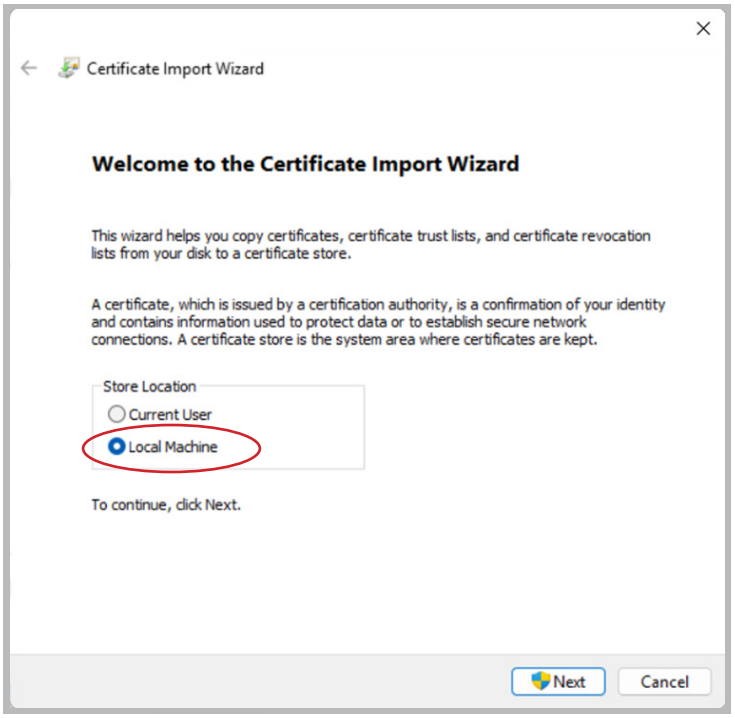
1. Navigate to the setup page
2. Click '**Paxton Certificate**'



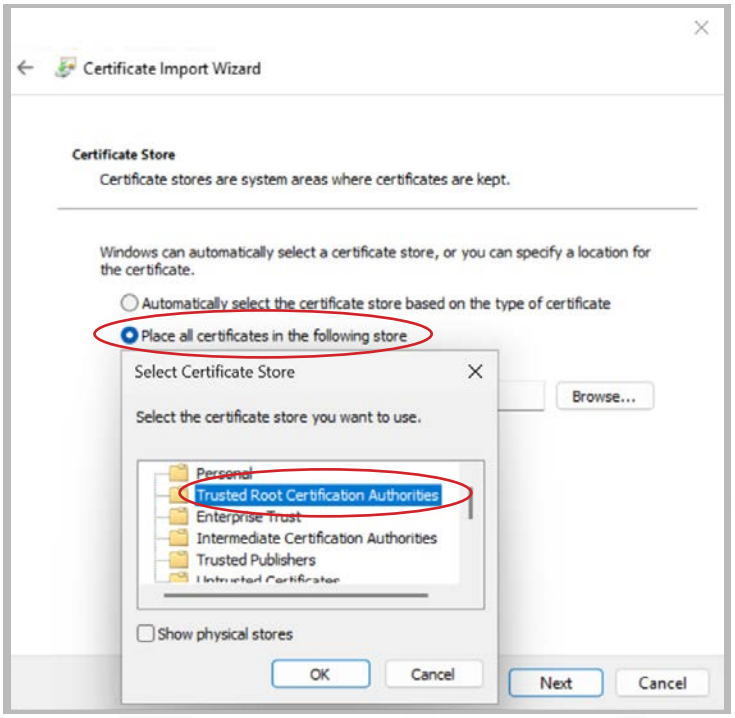
3. Locate and run the downloaded file.
4. Click '**Install Certificate**'.



5. Select '**Local Machine**' and click '**Next**'. You may need administrator permissions to do this.



6. Select '**Place all certificates in the following store**' and click '**Browse**'.



7. Select '**Trusted Root Certification Authorities**', click '**OK**' and then '**Next**'.

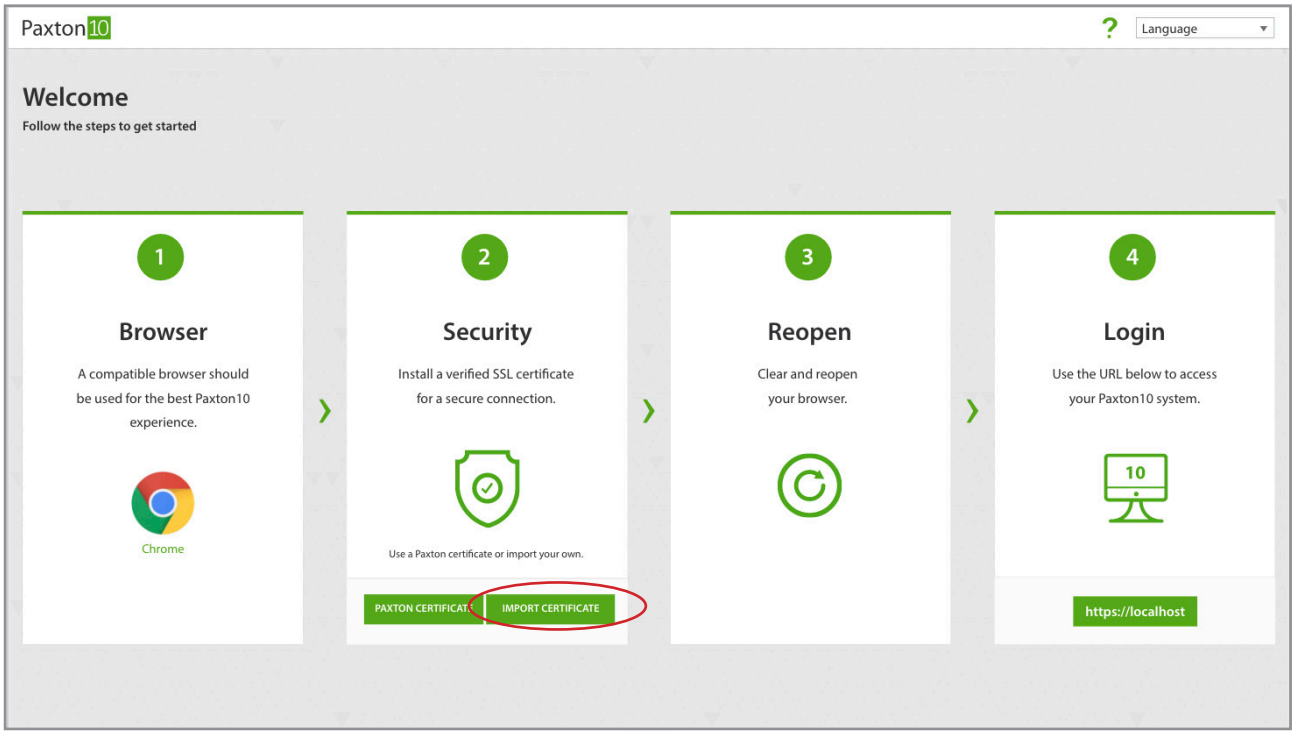
8. Click '**Finish**' then close all instances of your browser and open it again.

9. Navigate to the https://paxton10-XXXXXX address which will now show as '**Connection is secure**'.

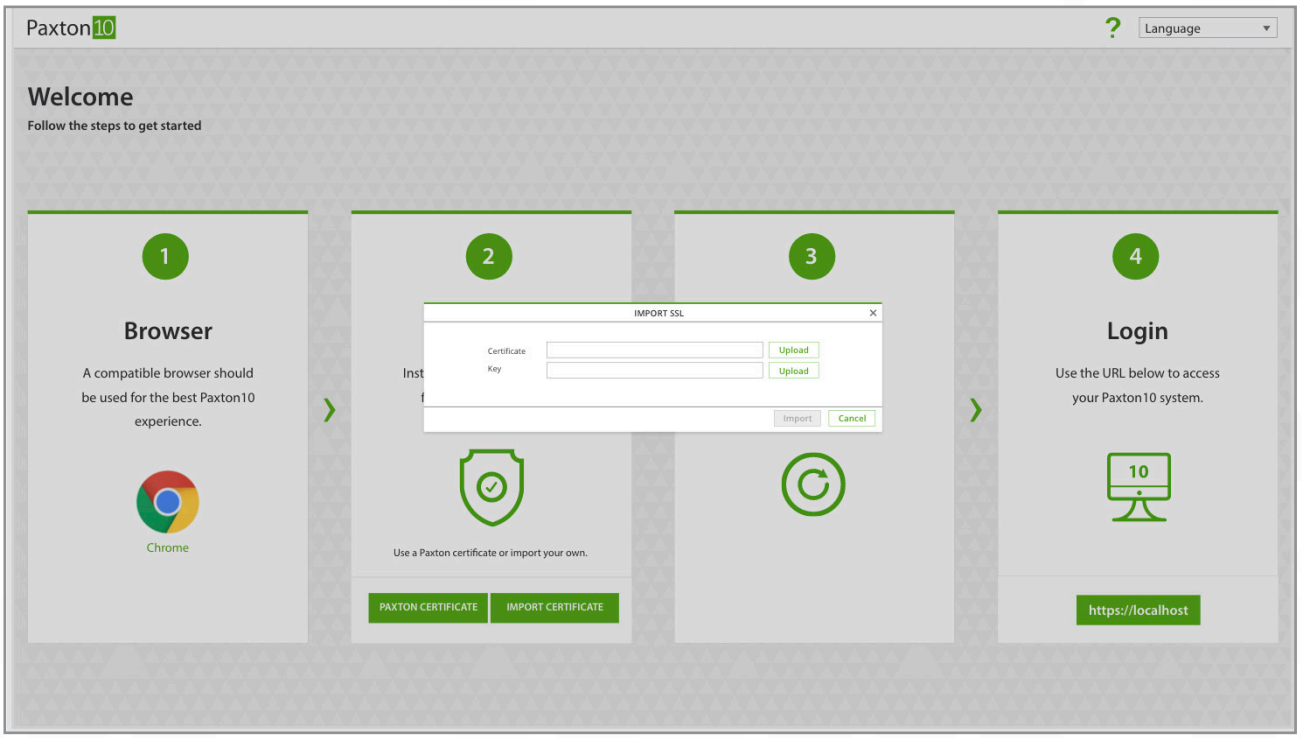
Using your own custom certificate

If you wish to use your own custom certificate with Paxton10, please follow these steps:

1. Navigate to the setup page
2. Click '**Import certificate**'



3. Browse t your certificate and corresponding RSA key and click '**Upload**'



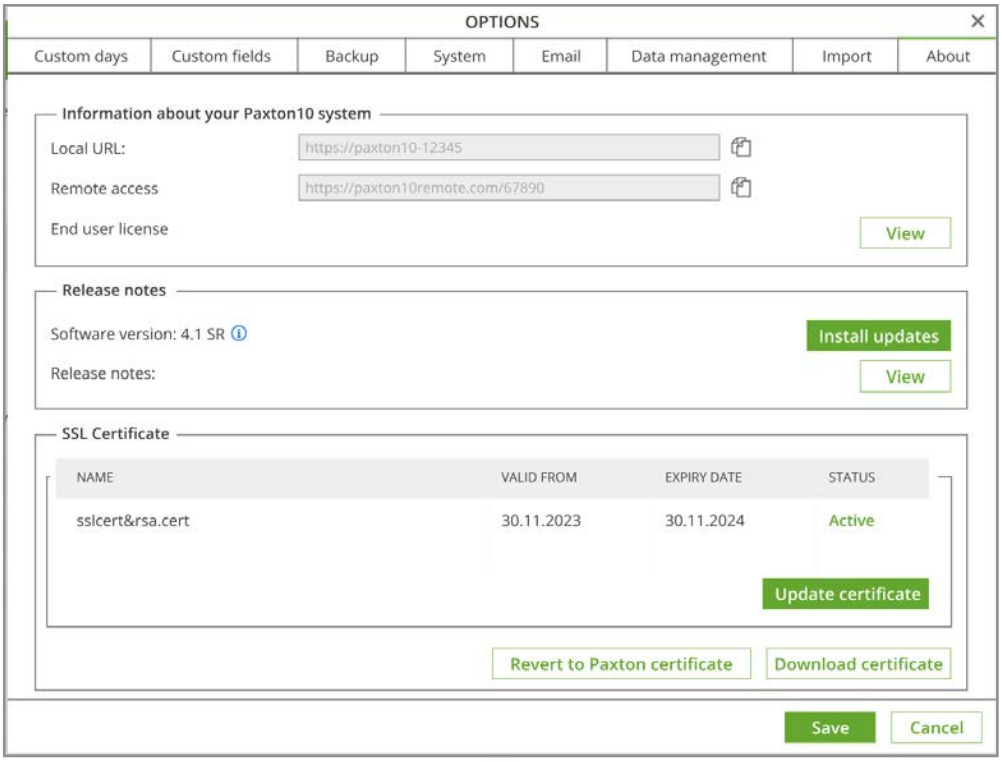
4. Browse and login to Paxton10

Note: This is an advanced setting that should only be completed by someone who has knowledge of SSL certificates.

Managing certificate settings

After your system has been set up, any further changes you wish to make to your certificate must be made from within the Paxton10 system, when logged in as a system engineer.

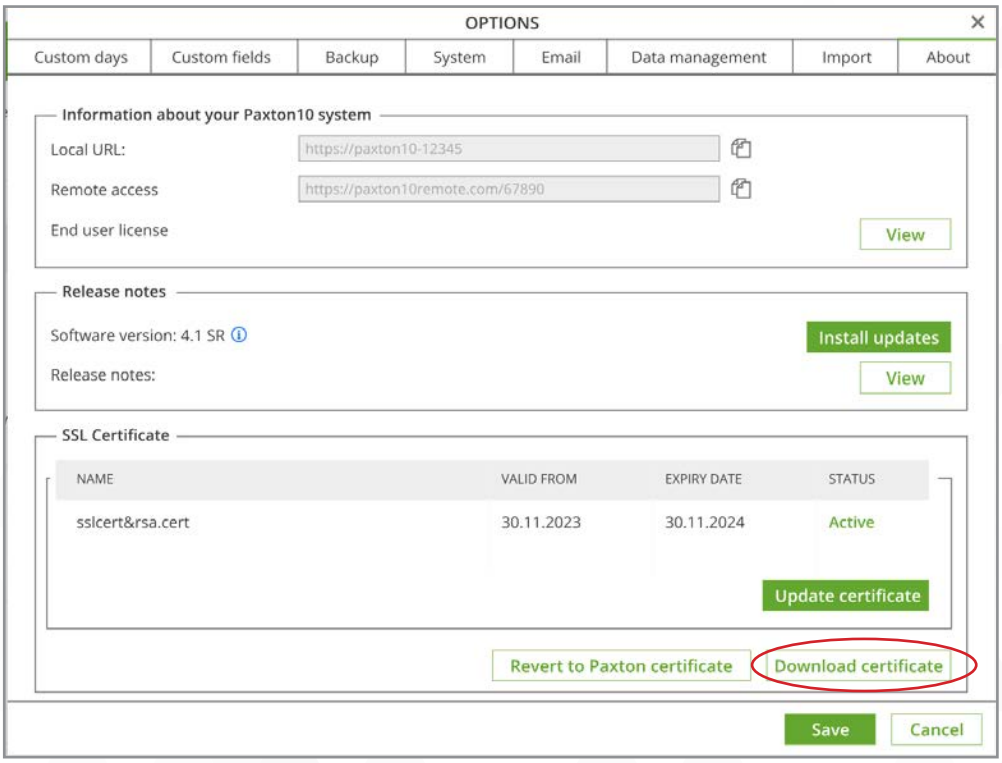
This screen will also give you information about the currently used certificate. If you are using a custom certificate, it will tell you the current status and when it will expire.



Downloading certificate

Each computer you are accessing Paxton10 from will need the certificate installed. To download the certificate from within Paxton10 follow these steps:

1. Navigate to the system options
2. Click '**Download certificate**'



3. Locate and run the downloaded file

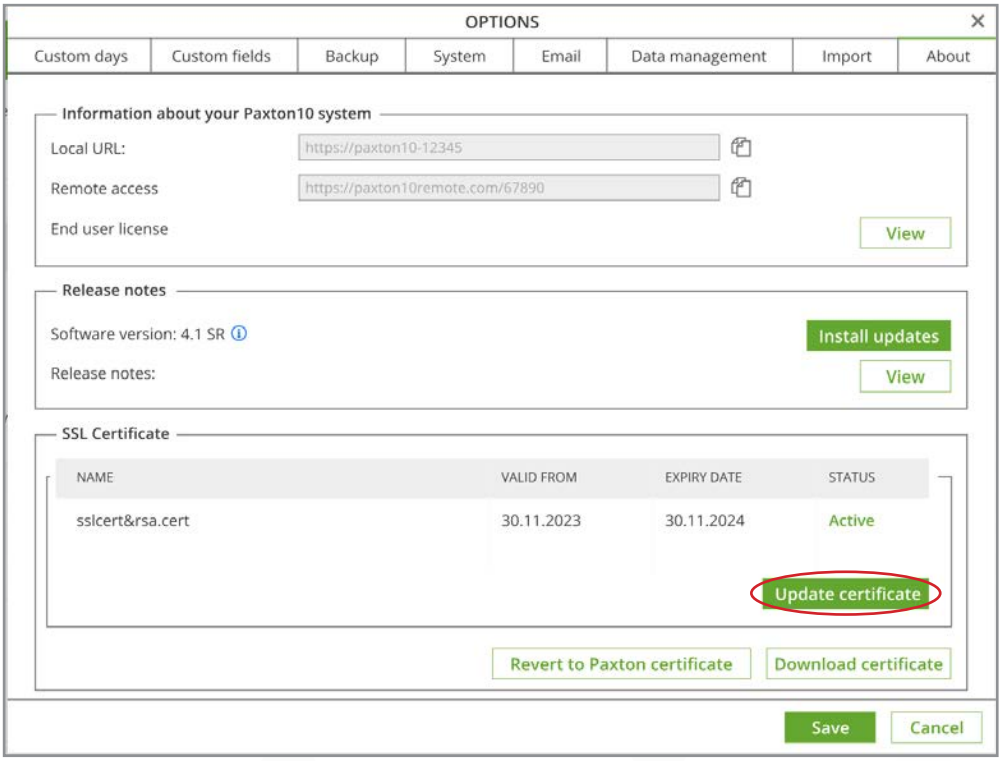
4. Follow the on-screen prompts to install the certificate

Update certificate

To update your certificate, please follow the below:

1. Navigate to the system options

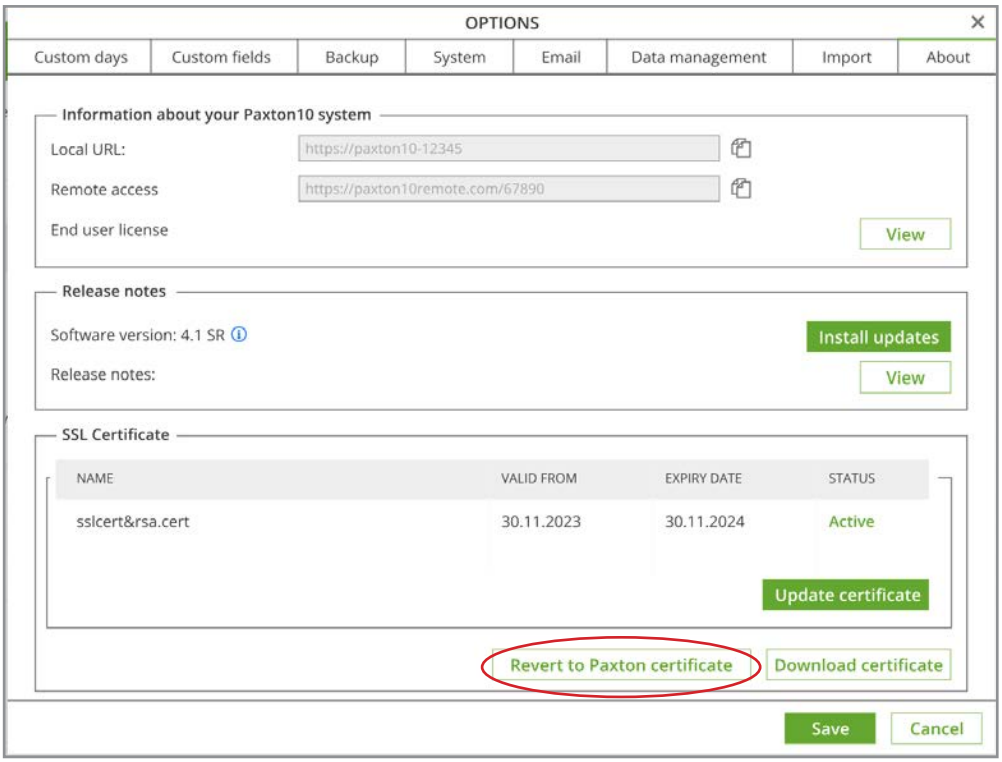
2. Click '**Update certificate**'



3. Browse to your certificate and corresponding RSA key and click '**Upload**'

Reverting to Paxton certificate

You may be using a custom SSL certificate, but want to revert to using the Paxon supplied certificate. To do that you will need to navigate to the system options and click '**Revert to Paxon certificate'**.



What is TLS/SSL?

TLS (Transport Layer Security) and SSL (Secured Sockets Layer) are methods used to ensure data is safe and secure when communicating across a network.

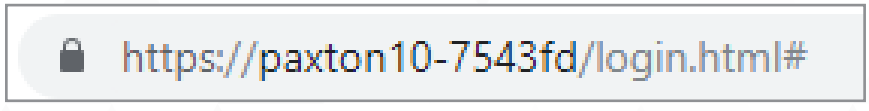
When you are using a TLS/SSL enabled connection, the data being sent and received will be unreadable to any eavesdroppers that may be trying to steal information.

To use TLS/SSL, a digital certificate should be installed on both PCs that are communicating with each other.

How do I tell if a website is using TLS/SSL?

When browsing to a website, if TLS/SSL isn't enabled then you will see a "Not secure" message in the address bar. These websites will also start with http://.

If the website you are browsing to does have TLS/SSL enabled then you will see a padlock in the address bar. These websites will start with https://.



Frequently Asked Questions

Can I log in to Paxton10 from anywhere?

The setup page and local URL found on the setup page can only be used when you're located on the same network as the server.

The system administrator may choose to enable remote access, which will create a new remote URL. The remote URL can be used to log in to your Paxton10 system from anywhere with an internet connection. Speak to your system administrator for more information.

Which internet browsers can I use to access Paxton10 software?

It is advised to use the latest versions of Google Chrome to access and administer your Paxton10 system.
Your Paxton10 system can also be accessed using Google Chrome on a smartphone or tablet, or via the Paxton Connect Admin app, available on the Apple App Store and Google Play Store.

Why does my browser say that Paxton10 is insecure or unsafe?

Each Paxton10 server contains its own unique security certificate, encrypting and securing communication to and from it. Follow the steps above to download the certificate to your computer or device so that your browser can recognise the Paxton10 server and see it as secure.

Do I have to install the Paxton10 certificate?

No, Paxton10 is secured through TLS/SSL and not installing the certificate will not cause a threat to security or your data. However, many internet browsers will prevent, or advise against, using Paxton10 without the correct certificate installed.

© Paxton Ltd Rev E