Use your own TLS certificates

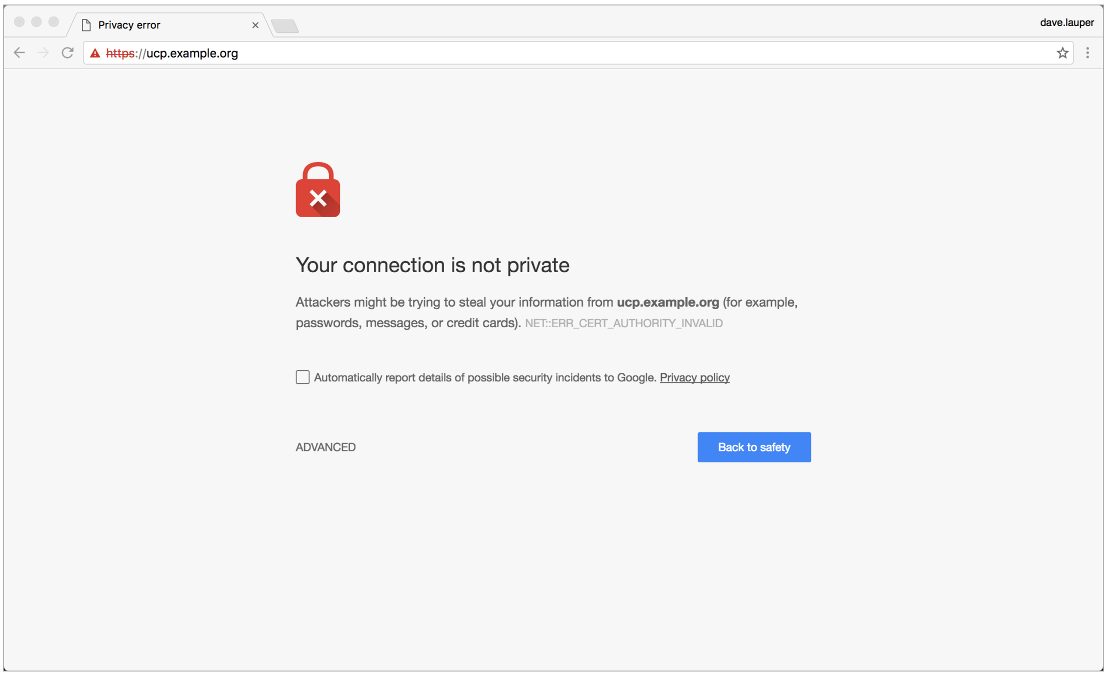
Estimated reading time: 1 minute

✓ These are the docs for UCP version 2.2.18

To select a different version, use the selector below.

2.2.18 ▾

All UCP services are exposed using HTTPS, to ensure all communications between clients and UCP are encrypted. By default, this is done using self-signed TLS certificates that are not trusted by client tools like web browsers. So when you try to access UCP, your browser warns that it doesn't trust UCP or that UCP has an invalid certificate.



Your connection is not private

Attackers might be trying to steal your information from **ucp.example.org** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically report details of possible security incidents to Google. Privacy policy

The same happens with other client tools.

```
$ curl https://ucp.example.org

SSL certificate problem: Invalid certificate chain
```

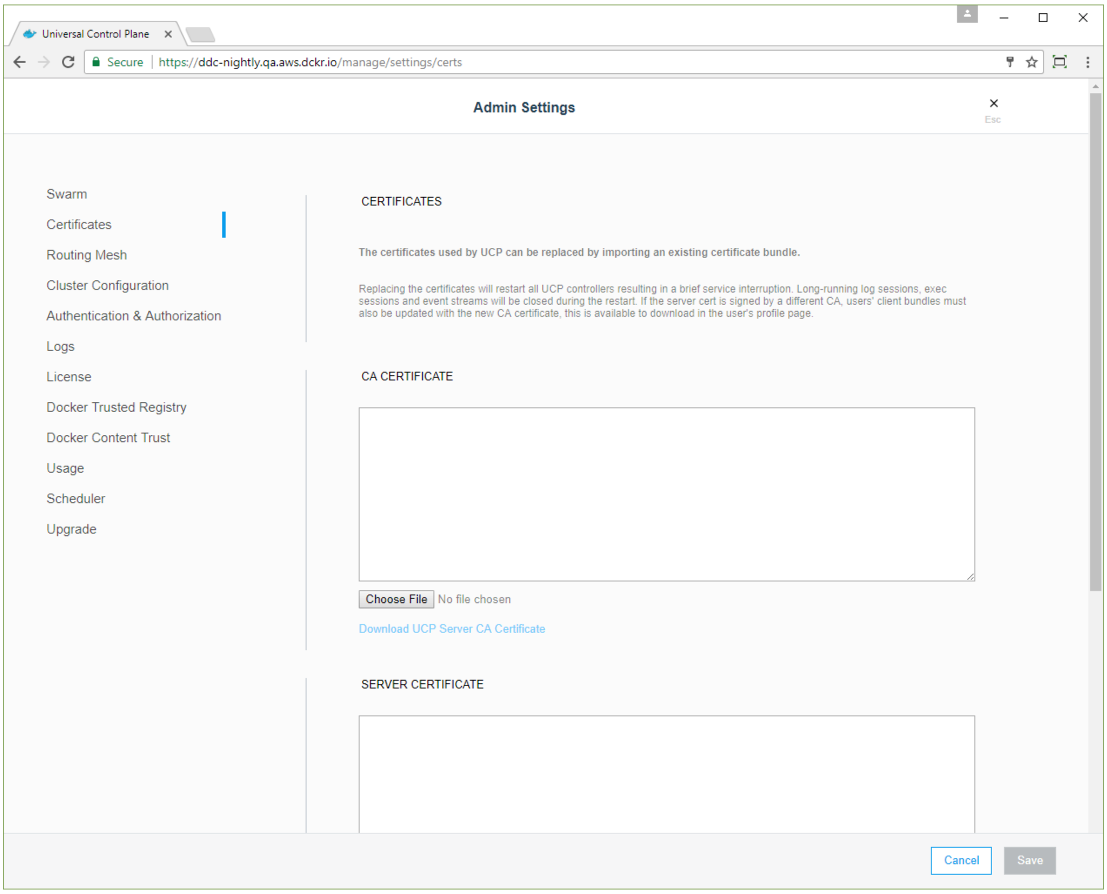
You can configure UCP to use your own TLS certificates, so that it is automatically trusted by your browser and client tools.

To ensure minimal impact to your business, you should plan for this change to happen outside business peak hours. Your applications will continue running normally, but existing UCP client certificates will become invalid, so users need to download new ones to access UCP from the CLI (https://docs.docker.com/datacenter/ucp/2.2/guides/user/access-ucp/cli-based-access/).

Configure UCP to use your own TLS certificates and keys

In the UCP web UI, log in with administrator credentials and navigate to the **Admin Settings** page.

In the left pane, click **Certificates**.



CERTIFICATES

The certificates used by UCP can be replaced by importing an existing certificate bundle.

Replacing the certificates will restart all UCP controllers resulting in a brief service interruption. Long-running log sessions, exec sessions and event streams will be closed during the restart. If the server cert is signed by a different CA, users' client bundles must also be updated with the new CA certificate, this is available to download in the user's profile page.

CA CERTIFICATE

SERVER CERTIFICATE

Upload your certificates and keys:

- A `ca.pem` file with the root CA public certificate.
- A `cert.pem` file with the TLS certificate for your domain and any intermediate public certificates, in this order.
- A `key.pem` file with TLS private key. Make sure it is not encrypted with a password. Encrypted keys should have `ENCRYPTED` in the first line.

Finally, click **Save** for the changes to take effect.

After replacing the TLS certificates, your users can’t authenticate with their old client certificate bundles. Ask your users to go to the UCP web UI and get new client certificate bundles (https://docs.docker.com/datacenter/ucp/2.2/guides/user/access-ucp/cli-based-access/).

If you deployed Docker Trusted Registry, you also need to reconfigure it to trust the new UCP TLS certificates. Learn how to configure DTR (https://docs.docker.com/datacenter/dtr/2.3/reference/cli/reconfigure/).

Where to go next