Issue

While configuring interlock with wildcard certificates you may face the following error if the configuration is invalid:

```
error during connect: Get https://test.ucp.example.com:443/v1.39/info: x509: certificate is valid for
*.example.com, not test.ucp.example.com
```

Prerequisites

Before performing these steps, you must meet the following requirements:

- Interlock enabled
- Using wildcard certificates for Interlock configuration

Resolution

The error seen above when using wildcard certificates for interlock configuration is due to invalid configuration. Wildcard certs generally are used for first-level subdomains of the domain in question. In the example above, the wildcard certificate is valid for `*.example.com`. This means that the cert would be valid for `ucp.example.com`, `docker.example.com`, `anything.example.com`, etc. The certificate valid for `*.example.com` would NOT work however when adding a subdomain level such as `test.ucp.example.com` or `anything.ucp.example.com`.

The resolution is to:

A) Use valid wildcard certificate configuration per the expected domain levels. Example above being `*.example.com`

B) Use subject alternative names within the wildcard certs for the exact domain level matches

What's Next

https://docs.docker.com/ee/ucp/interlock/usage/tls/