Recommendations and Limitations

This section outlines best practices, provides recommendations and also lists the limitations for certificate usage and trustpoint configuration.

General Guidelines

- For the C9800-CL in a public cloud, it is mandatory to use a Layer 3 port for wireless management. This interface is used to communicate with APs and other peer controllers to create Mobility Tunnels.
- Enable the HTTP server. This is required for secure web access and for Simple Certificate Enrollment Protocol (SCEP).
- Synchronize device clocks to a single NTP server for certificate validity.
- Assign trustpoints to the application. Use the WebUI to assign trustpoints as it is much simpler than using the CLI. Refer to Assign a Trustpoint for a Specific Service using the WebUI .
- Configure a hostname and a domain-name on the Cisco 9800. When you enroll for a certificate, the default subject-name is derived from the hostname.
- Catalyst 9800 supports using wildcard domain names in the CN field of the certificate.
- For clients to trust the web authentication certificate, define a hostname that matches the Common Name (CN) in the certificate. You can configure it through the global parameter setting for webauth, where you can define the hostname for the Virtual IP address being used for web authentication.

```
9800-L # configure terminal
9800-L (config)#parameter-map type webauth global
9800-L (config-params-parameter-map)#type webauth
9800-L (config-params-parameter-map)#timeout init-state sec 1234
9800-L (config-params-parameter-map)#virtual-ip ipv4 192.0.2.1 virtual-host
webauth.mywlc.mydomain.com
```

To ensure that the certificate is trusted by the web browser make a note of the following:

- The Common Name (or a SAN field) must match the URL visited by the browser. Since SAN configuration is not supported in the certificate signing request (CSR), in 17.3. x versions either from the CLI or GUI, you can use OpenSSL to generate a certificate signing request (CSR) containing the SAN fields.
- The certificate should be within its validity period. Note that some browsers now do not trust certificates with a validity period of more than one year, particularly for certificates that pertain to client web browser, i.e. web admin and webauth.

- The certificate must be issued by a CA or chain of CA whose root is trusted by the browser. For this, the certificate provided by the web server must contain all the certificates of the chain until (not necessarily included) a certificate trusted by the client browser (typically the Root CA).