Troubleshoot Common Issues for Certificate Configuration

The following lists the common problems and resolution related to certificates. If your solution is not listed here, use the commands listed below to debug further.

Configuring the CA server "Failure Reason: Time has not been set. Cannot start the Certificate Server "

Possible Cause

Clock is not set on the controller.

Recommended Solution

Set the clock on 9800 using the command.

```
Device(config)#clock calendar-valid
```

Configuring the CA server ""Error in receiving Certificate Authority certificate"

Possible Cause

Lost connectivity to the managemet interface.

Recommended Solution:

Check if the management interface IP of the virtual controller is reachable.

Error message “This certificate is not trusted”

Possible Cause

Missing entries in certificate chain.

Recommended Solution:

Build a chain of certificates beginning with the certificate of the CA that issued the controller certificate on the controller. Include all the CA certificates and place the trusted CA certificate on top. You must place the entire chain in the same file. This means your file contains content such as this example:

```
--- BEGIN CERTIFICATE ---
*device certificate*
--- END CERTIFICATE ---
```

```
--- BEGIN CERTIFICATE ---
*intermediate CA certificate*
--- END CERTIFICATE ---
--- BEGIN CERTIFICATE ---
*Root CA certificate*
--- END CERTIFICATE ---
```

Trying to import a PKCS12 certificate which is missing the CA

Possible Cause

The pfx file might not contain the entire chain.

Recommended Solution:

Use the command to troubleshoot certificate issues.

```
Device#debug crypto pki transactions
```

1. Export the private key out.

   ```
   openssl pkcs12 -in <pkcs12 file> -out cert.key -nocerts -nodes
   ```

2. Combine the certificate as PEM.

   ```
   openssl pkcs12 -in <pkcs12 file> -out certificate.pem -nokeys -clcerts
   ```

3. Download the intermediate CA certificate as PEM. In case of a public CA, you can download the PEM file from the internet. In case of several levels of the intermediate CA, you can combine all of them into a single PEM file and name it CA.pem.

4. Rebuild the PKCS 12 file from the key, device certificates and CA certificate.

   ```
   openssl pkcs12 -export -out fixedcertchain.pfx -inkey cert.key -in certificate.pem -
   certfile CA.pem
   ```

5. Import the “fixedcertchain” to the Catalyst 9800. You must place the entire chain in the same file. This means your file will contain content as below.

   ```
   --- BEGIN CERTIFICATE ---
    *device certificate*
   --- END CERTIFICATE ---
   --- BEGIN CERTIFICATE---
    *intermediate CA certificate*
   --- END CERTIFICATE ---
   --- BEGIN CERTIFICATE ---
    *Root CA certificate*
   --- END CERTIFICATE ---
   ```

Certificate cannot be uploaded to the controller.

Possible Cause

Not connected to the TFTP server .

Certificate validity date or isssuer details is incorrect.

Recommended Solution:

Check details using

```
Device#show crypto pki certificates <cert-name>
Certificate
Status: Available
Certificate Serial Number (hex): 00A2020356CF31C818 Certificate Usage: General Purpose
Issuer:
cn=CA-KCG-lab
ou=lab-mex-wireless
o=mex-wireless
l=Guadalupe
st=Nuevo Leon
c=MX
Subject:
Name: *.lab-kcg.com
cn=*.lab-kcg.com
ou=lab-mex-wireless
o=mex-wireless
l=Benito Juarez
st=CDMX
c=MX
Validity Date:
start date: 17:14:54 UTC Feb 15 2018
end date: 17:14:54 UTC Mar 11 2023
Associated Trustpoints: cert-name
Storage: nvram:CA-KCG-lab#C818.cer
```

AP with MIC/SUDI fails to join the controller

Possible cause

Issue with management interface trustpoint settings

Recommended Solution

In case the AP cannot join the controller, you can verify the if the trustpoint is corrrect

Physical controllers

```
show wireless management trustpoint
Trustpoint Name : CISCO_IDEVID_SUDI
Certificate Info : Available
Certificate Type : MIC
Private key Info : Available
FIPS suitability : Not Applicable
```

Virtual controllers

```
show wireless management trustpoint
Trustpoint Name : ewlc-tp1
Certificate Info : Available
Certificate Type : SSC
Certificate Hash :
4a5d777c5b2071c17faef376febc08398702184e
Private key Info : Available
FIPS suitability : Not Applicable
```

If required, remove the wireless management trustpoint for the controller to fall back on the SUDI trustpoint using the following command in the global configuration mode.

```
Device(config)#no wireless management trustpoint
```

Syslog Error message

```
Dec 31 18:32:04.072: %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain
validation has failed. The certificate (SN: 0159BC17) has expired. Validity
period ended on 2027-02-23T22:32:59ZDec 31 18:32:04.073:
%CERT_MGR_ERRMSG-3-CERT_VALIDATION_ERR: Chassis 1 R0/0: wncd: Certificate
Validation Error, Cert validation
status:pki_ssl_status@pki_ssl_status:PKI_SSL_ERRORDec 31 18:32:04.073:
%DTLS_TRACE_MSG-3-WLC_DTLS_ERR: Chassis 1 R0/0: wncd: DTLS Error,
session:9.10.30.117[5256] MAC: 70db.9888.cc20, Certificate validation
failed
```

Possible Cause

AP is trying to join the controller using an expired certificate.

Recommended Solution:

Allow APs to join with expired certificates by configuring policy maps

1. Create a certificate map and add the rules.

   ```
   Device#configure terminal
   Device(config)#crypto pki certificate map map1 1
   Device(config)issuer-name co (issuer-name of AP/mobility peer's cert)
   ```

   Example:

   ```
   Device#configure terminal
   Device(config)#crypto pki certificate map map1 1
   Device(config)#issuer-name co Cisco Manufacturing CA
   ```

2. Allow this policy-map to validate expired certs, under the trustpool policy.

   ```
   Device#configure terminal
   Device(config)#crypto pki certificate map map1 2
   Device(config)issuer-name co act2 sudi ca
   ```

   ```
   Device#configure terminal
   Device(config)#crypto pki trustpool policy
   Device(config)#match certificate map1 allow expired-certificate
   ```

Table 1: Additional Debug Commands

Command	Description
debug crypto pki validation	Displays debugging messages related to public key infrastructure (PKI) path validation.
debug crypto pki transactions	Displays debugging messages related to public key infrastructure (PKI) certificates.
debug crypto ssl dtls events	Displays debugging messages related to encrypted ssl packets for DTLS events.
debug crypto ssl dtls errors	Displays debugging messages related to encrypted ssl packets for DTLS errors.
debug crypto ssl dtls packets	Displays debugging messages related to encrypted ssl packets for DTLS packet dump.

Command	Description
debug crypto ikev2	Displays debugging messages related to encrypted ikev2 traffic.
debug crypto est-client	Displays debugging messages related to clients who have been Enrolled Over Secure Transport(EST).
debug crypto pki scep	Displays debugging messages related to clients who have been enrolled over Simple Certificate Enrollment Protocol (SCEP).
debug crypto tls-tunnel error	Displays debugging messages related to errors in the tls-tunnel channel.
debug crypto tls-tunnel event	Displays debugging messages related to events in the tls-tunnel channel.