

CPPM 6.8 - CLUSTER CONFIGURATION USING CERTIFICATES

VERSION 1.0

A decorative graphic consisting of a large, dark gray, irregular polygonal shape that occupies the bottom half of the page. A thin, light gray diagonal line crosses the shape from the upper left towards the lower right.

Table of Contents

<i>Certificate role in cluster configuration in 6.8</i>	3
<i>HTTPS Server certificate</i>	3
Step -1 CSR Generation	3
Step -2 Import signed certificate	4
Step -3 Import certificate in subscriber trust list	4
Step -4 Configure cluster	4
<i>Database Server certificate</i>	6
Import DB server certificate	6
Step -1 CSR Generation	6
Step -2 Import certificate	6
Step -3 Import certificate in subscriber trust list	7

Certificate role in cluster configuration in 6.8

In 6.8, for enhance cluster security introduce https and database server certificate which role play vital role between cluster nodes.

Https server Certificate validation – It is mandatory that nodes (subscriber's) should trust https certificate of publisher node. It should be present in CPPM nodes trust list before configure cluster.

In order to adhere best practice https server certificate is signed by public Certificate Authority, which includes all nodes FQDN name in subject alternate name (SAN) field.

Database server Certificate – This is new certificate type in 6.8 to enhance security in the cluster replication between the cluster's nodes. It should be present in CPPM nodes (subscriber's) trust list before configuration cluster.

In order to adhere best practice, do not use self-sign CPPM database server certificate instead of that signed database server certificate by internal/external Certificate Authority.

HTTPS Server certificate

Step -1 CSR Generation

Generate CSR from Publisher CPPM node & Subscriber nodes and sign with Root CA server

Administration » Certificates » Certificate Store

The screenshot displays the 'Certificate Store' interface within the 'Administration » Certificates » Certificate Store' path. The main heading is 'Certificate Store', and a sub-note states: 'Allows you to create multiple service certificates, each of which can be associated with a specific ClearPass service.' On the right, there are three links: 'Create Self-Signed Certificate', 'Create Certificate Signing Request' (highlighted with an orange box), and 'Import Certificate'. Below these links, there are tabs for 'Server Certificates' and 'Service & Client Certificates'. The 'Create Certificate Signing Request' dialog box is open, showing fields for: Common Name (CN): CPPM1.lab.com; Organization (O): XYZ; Organizational Unit (OU): IT; Location (L): Bangalore; State (ST): Karnataka; Country (C): IN; Subject Alternate Name (SAN): DNS:CPPM2.lab.com, DNS:testguest.lab.com (with callouts for 'Subscriber Node fqdn' and 'Guest URL'); Private Key Password: (masked); Verify Private Key Password: (masked); Private Key Type: 2048-bit RSA; Digest Algorithm: SHA-512. The dialog has 'Submit' and 'Cancel' buttons at the bottom. In the background, the 'HTTPS Server Certificate' section is visible with an 'Export' button.

Note: -

1. Adhere best practice use public signed https certificate.

2. We could also use internal root CA server for sign https certificate (only useful for Lab environment)

Step -2 Import signed certificate

Login on Publisher and import the public signed certificate - Administration » Certificates » Certificate Store

The screenshot shows the 'Certificate Store' page in the Administration menu. The 'Import Certificate' dialog box is open, displaying the following fields:

- Certificate Type: Server Certificate
- Server: CPPM3
- Usage: HTTPS Server Certificate
- Upload Method: Upload Certificate and Use Saved Private Key
- Certificate File: Choose file certnew (2).cer

Below the fields, there are two notes:

- Note:** Certificates with a wildcard as the common name (ex: *.arubanetworks.com) and Extended Validation certificates (EV, "Green Bar") are not recommended for use as the RADIUS/EAP server certificate. Some clients may be unable to authenticate when these types of certificates are used.
- Note:** Import of a Database Server Certificate requires a server reboot after waiting a few minutes for changes to take effect.

The dialog box has 'Import' and 'Cancel' buttons at the bottom right.

Step -3 Import certificate in subscriber trust list

Login on subscriber's node and import publisher https server certificate in the trust list - Administration » Certificates » Trust List >> Add

The screenshot shows the 'Add Certificate' dialog box with the following fields:

- Certificate File: Choose file certnew (1).cer
- Usage: ☐ EAP ☐ RadSec ☐ Database ☒ Others

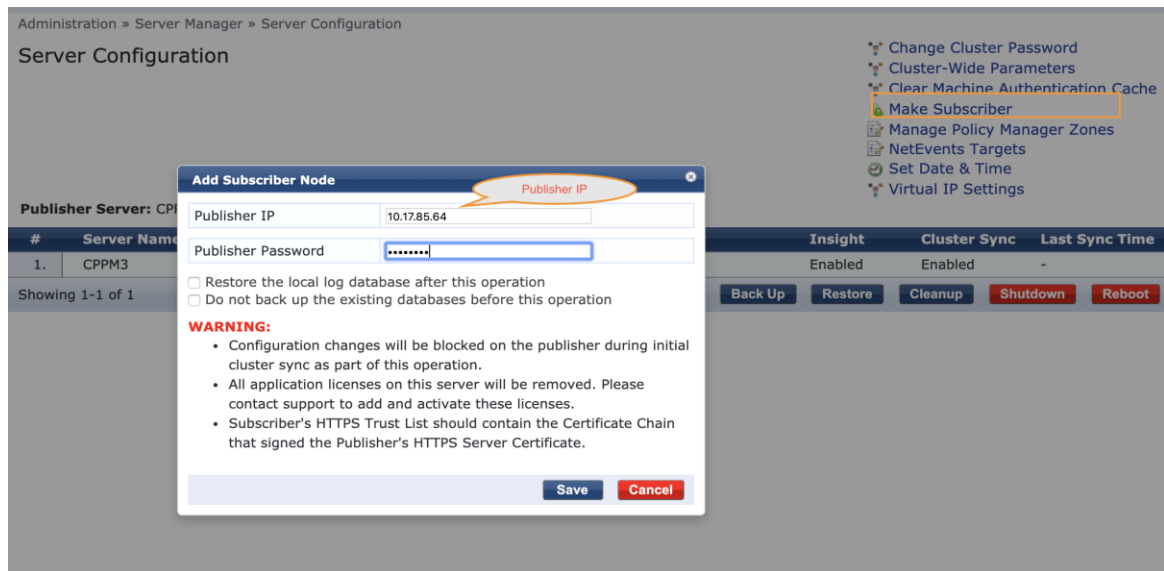
The dialog box has 'Add Certificate' and 'Cancel' buttons at the bottom right.

Note: -

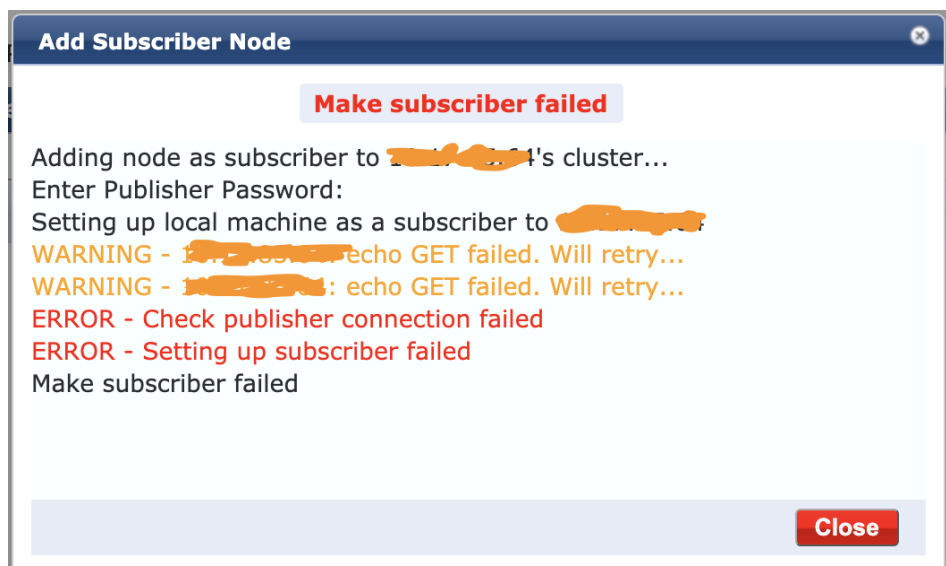
1. Root CA chain should be in trust list before import cert.
2. When generate CSR private key does save in CPPM database. which does expire after 15 days, after expired private key we can't recover private key

Step -4 Configure cluster

Login on CPPM node (subscriber) and joining the node in the cluster



If publisher CPPM node https certificate is not trust list of subscriber node failed with below error.



Database Server certificate

This is new feature introduced in 6.8, This provides customers an ability to import a certificate signed by the Certificate Authority of their choice hence enhancing security between the cluster members.

Note: - In 6.8, database server certificate support only 1 year. This was fixed in 6.8.1 where the default Database certificate validity was increased back to 5 years.

Import DB server certificate

Step -1 CSR Generation

Generate CSR from CPPM UI - Administration » Certificates » Certificate Store (select usage – Database server certificate)

The screenshot displays the 'Certificate Store' interface in the CPPM UI. The breadcrumb navigation is 'Administration » Certificates » Certificate Store'. The page title is 'Certificate Store'. A description states: 'Allows you to create multiple service certificates, each of which can be associated with a specific ClearPass service.' There are two tabs: 'Server Certificates' (selected) and 'Service & Client Certificates'. In the top right corner, there are three links: 'Create Self-Signed Certificate', 'Create Certificate Signing Request' (highlighted with an orange box), and 'Import Certificate'. Below the tabs, there is a 'Select Server:' dropdown set to 'CPPM3' and a 'Select Usage:' dropdown set to 'Database Server Certificate' (highlighted with an orange box). The main area shows a table with columns for 'Subject', 'Issued by', 'Issue Date', 'Expiry Date', 'Validity Status', and 'Details'. A modal dialog titled 'Create Certificate Signing Request' is open in the center. It contains the following fields: 'Common Name (CN):' with value 'CPPM1.lab.com', 'Organization (O):' with value 'xyz', 'Organizational Unit (OU):' with value 'IT', 'Location (L):' with value 'Bangalore', 'State (ST):' with value 'Karnataka', 'Country (C):' with value 'IN', 'Subject Alternate Name (SAN):' with value 'DNS:CPPM2.lab.com,DNS:CPPM3.lab.com', 'Private Key Password:' (masked with dots), 'Verify Private Key Password:' (masked with dots), 'Private Key Type:' set to '2048-bit RSA', and 'Digest Algorithm:' set to 'SHA-256'. At the bottom of the dialog are 'Submit' and 'Cancel' buttons. An 'Export' button is visible on the right side of the main interface.

Step -2 Import certificate

Login on Publisher, after signed the certificate by Certificate Authority, need to import database server certificate on CPPM node.

Administration » Certificates » Certificate Store

Administration » Certificates » Certificate Store

Certificate Store

Allows you to create multiple service certificates, each of which can be associated with a specific ClearPass service.

[Create Self-Signed Certificate](#)
[Create Certificate Signing Request](#)
[Import Certificate](#)

Server Certificates Service & Client Certificates

Select Server: CPPM3 Select Usage: Database Server Certificate

Subject: Issued by: Issue Date: Expiry Date: Validity Status: Details:

Import Certificate

Certificate Type: Server Certificate
 Server: CPPM3
 Usage: Database Server Certificate
 Upload Method: Upload Certificate and Use Saved Private Key
 Certificate File: Choose file dbcert.cer

Note: Certificates with a wildcard as the common name (ex: *.arubanetworks.com) and Extended Validation certificates (EV, "Green Bar") are not recommended for use as the RADIUS/EAP server certificate. Some clients may be unable to authenticate when these types of certificates are used.
Note: Import of a Database Server Certificate requires a server reboot after waiting a few minutes for changes to take effect

[Import](#) [Cancel](#)

[Export](#)

Step -3 Import certificate in subscriber trust list

Login on subscriber's node and import publisher database server certificate in the trust list -
Administration » Certificates » Trust List >> Add

Add Certificate

Certificate File: Choose file dbcert.cer
 Usage: ☐ EAP ☐ RadSec ☒ Database ☐ Others

[Add Certificate](#) [Cancel](#)