WiNG 5.X Feature Guide

EAP-TLS with Onboard RADIUS on AP

Part No. TME-03-2016-01 Rev. B

Table of Contents

1. Overview

This guide will explain how to configure an onboard RADIUS server on an Access Point as main or failover method to authenticate wireless clients using 802.1X with EAP-TLS method using client-side certificates. It will also cover Access Point certificate provisioning in order to be able to authenticate clients using EAP-TLS as well as automatic Certificate Revocation List download to keep updated list of revoked certificates.

Running EAP-TLS authentication method with onboard RADIUS server can be used either as a main authentication server or as a failover AAA server, should the primary become unreachable to provide full service survivability.

1.1 Trust Model in EAP-TLS

Trust model in EAP-TLS deployments is based on the trust model of Public Key Infrastructure. The Secured Socket Layer (SSL) Handshake is happening over EAP transport protocol at Layer 2.

EAP terminology is important to note here, as examples below will be using the same terminology. In the RFC3748 that covers Extended Authentication Protocol (EAP) there are 3 main components:

1) **Supplicant** – this is a client device or end user machine, which initiates the EAP
2) **Authenticator** – the Access Point to which the client is trying to associate and that establishes a communication to the Authentication Server.
3) **Authentication Server** – the RADIUS server that responds to EAP messages to the authenticator.

In regards to PKI trust model there are several trust relationships that needs to be maintained:

1.1.1 Client Trusting Server

The Supplicant (or the client device, for example, an Android or Windows 7) must trust one root certification authority. This is given by the Supplicant's certificate signature. Using this root certification authority the client can validate the Authentication server that it is communicating with.

1.1.2 Server Trusting Client

To support EAP-TLS, the Authentication Server (most commonly a RADIUS server) must have a certificate signed by the Certification Authority that the Supplicant (client device) trusts as well. The Authentication Server in order will trust a client certificate that was signed by the same root certification authority that issued client's certificate.

1.1.3 Certification Authority

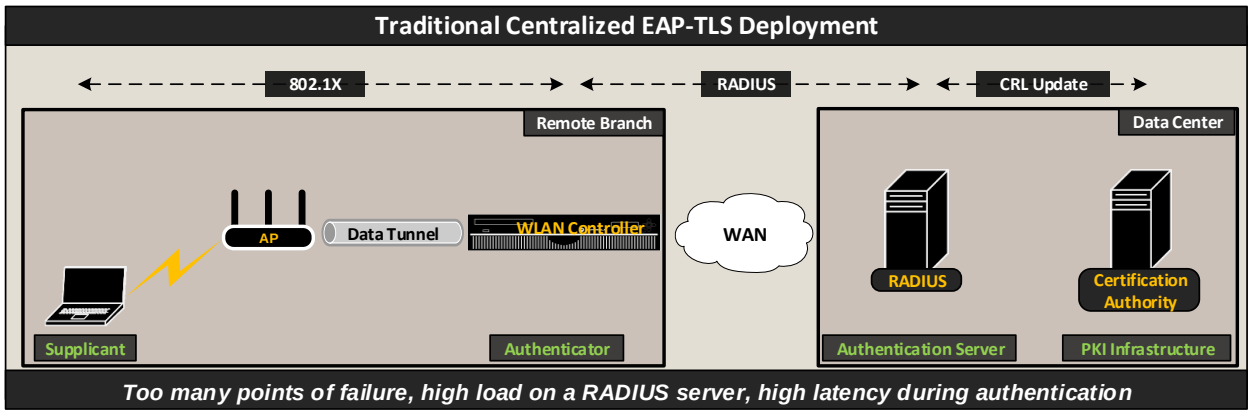
The Certification Authority acts as a third party that can validate the identity of the certificate holder. For this we have the digital signature of the authority (the certification-authority entity) that issued the certificate to the certificate holder.

Any device will have a list of trusted root certification authorities. This list is known as a certificate trust list (CTL). Any certificate in this list is automatically trusted by the client. Also note that a certificate of a trusted root certification authority is self-signed.

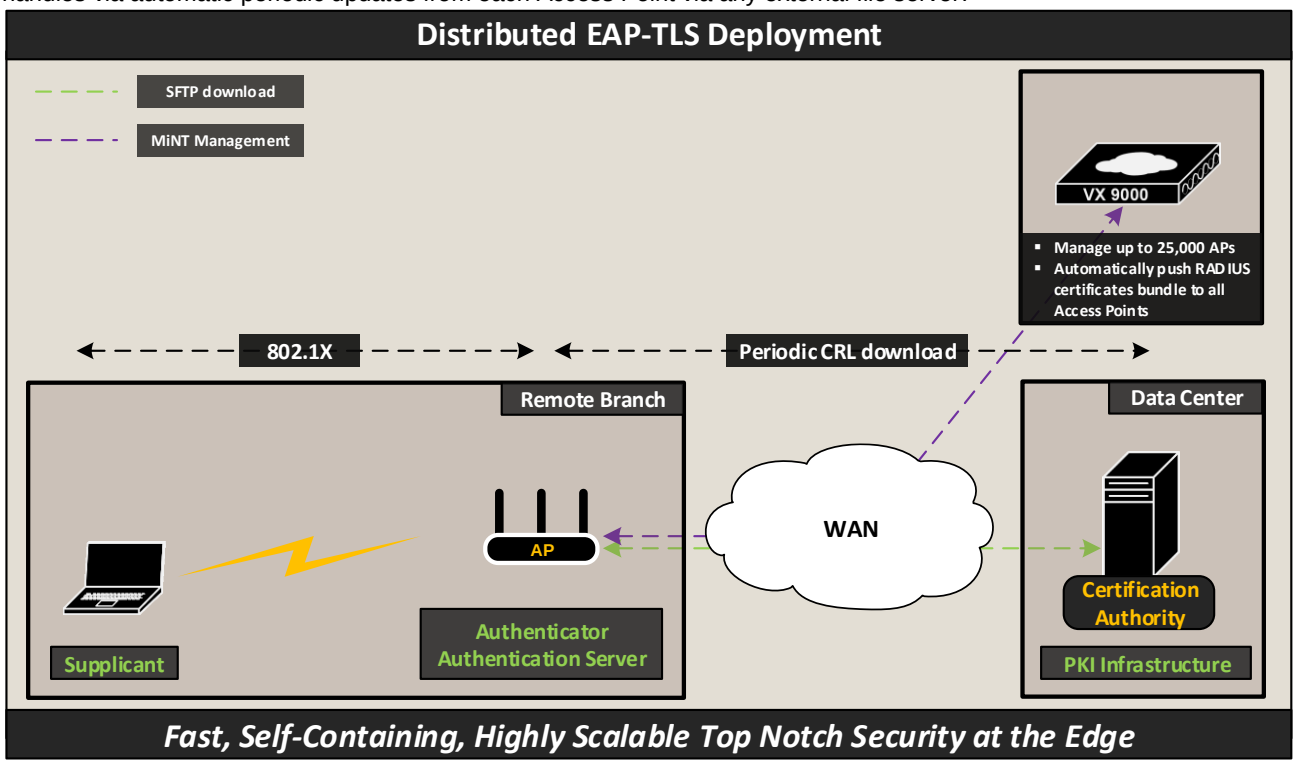
The certificate is validated using the public-private key pairs of the certification authority. If you trust the certification authority, then you trust this certification authority's certificate. The certification authority's certificate includes the certification authority's public key.

1.2 EAP-TLS Deployment Architectures

In traditional EAP-TLS centralized deployments proposed by many vendors today AAA server is located somewhere in customer's Data Center authenticating thousands of clients concurrently, along with PKI infrastructure (usually tiered Certification Authorities). While PKI infrastructure is generally able to manage large number of certificate due to the non-real-time nature of the process, the centralized AAA servers are often prone to overload in large deployments when handling thousands of RADIUS Requests per second from hundreds of different remote locations. This at least slows down the whole EAP authentication process for the wireless client, resulting in poor experience.



Zebra WiNG 5 leveraging distributed architecture advantages introduces distributed EAP TLS deployment model. In this model WiNG5 has combined the functions of the Authenticator and Authentication Server into each Access Point, creating a unified self-containing and highly scalable solution for EAP-TLS Deployment. In this scenario each Access Point is automatically provisioned with the RADIUS Server certificate bundle upon adoption, while CRL updates are handles via automatic periodic updates from each Access Point via any external file server:



2. Issuing certificates for the Access point.

It is important to remember that EAP-TLS authentication method requires both client-side and server-side certificates in order to perform mutual EAP-TLS authentication. This section will cover creation and import RADIUS server certificate to the Access Point that will be trusted by a Corporate Root Certification Authority.

Components used:

- Windows 2012 R2 server with Certification Authority and Domain Controller roles installed and configured.
- VX9000 controller running 5.8.1.0-012R WiNG release.
- AP7502 Access point running 5.8.1.0-012R WiNG release.
- iPad Mini 3 running iOS 9.1
- Sony Xperia Z1 running Android 5.1.1

2.1 Creating a RADIUS server trustpoint for the Access Points.

Trustpoint is a bundle of certificates and RSA private key needed to identify an end entity (client or server), as well as all the CAs (Root and Intermediate CAs) and end entity private key. Trustpoints can be used for different purposes, in this case it is required to create a trustpoint that will have a signed RADIUS server certificate and all Certification Authorities in the Root CA chain.

1	**From the Controller issue a command to generate an RSA private key and Certificate Signing Request (CSR). The purpose here is to generate generic radius server certificate that can be used with a wildcard domain name, so this trustpoint can be automatically uploaded later on to any Access Point at any given RF Domain from the VX 9000 Controller:**

```
VX#crypto pki export request generate-rsa-key onboardradius subject-name onboardradius.lab.local CZ JM
BRNO ZEBRA TMELABS fqdn *.zebranoc.com sftp://user:pass@tme-dc-1.zebranoc.com/onboardradius.csr
Successfully generated and exported certificate request
```

2	**Export generated private key from the VX, so it can be used later on to create a trustpoint bundle that can be imported to all Access Points:**

```
VX#crypto key export rsa onboardradius sftp://user:pass@tme-dc-1.zebranoc.com/onboardradius.prv
passphrase 1234
RSA Key successfully exported
```

3	**Resulted private key *must be decrypted* to allow its seamless export later on. Use *openssl* tools (link to download windows binaries):** **Open Windows Command Line or Powershell inside the C:\OpenSSL-Win32\bin folder (or any folder where openssl binaries are installed):**

```
C:\OpenSSL-Win32\bin>openssl.exe rsa -in C:\onboardradius.prv -out C:\onboardradius-nokey.prv
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Enter pass phrase for C:\Users\Viacheslav\Desktop\onboardradius.prv:
writing RSA key
```

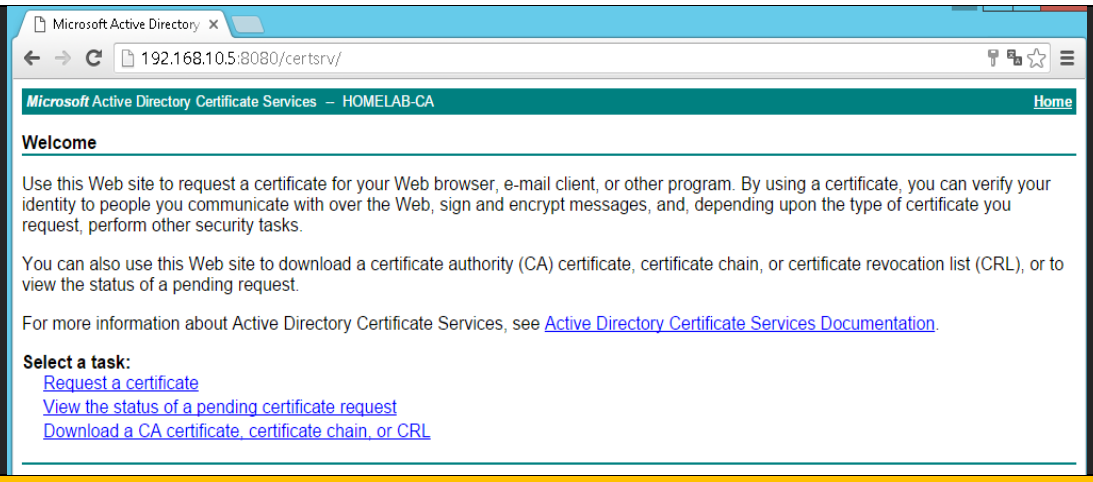
4	**Decrypted Private RSA key file:**


```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAn4kncx8VHDGM5gtVU6vEqA6NeWf37Ok1TWwQqcbPAsERAQB/
sO9Eo/+am1Sgv7dJeWCHgtZJ8x0rJuUHgwoFfEqr3cc6dmCuccaLSSN5bbohDmZ8
/Ol+AFC81F2syoqnZBdry8XktjqFWsDgloUjhWinqcfY6QMG8z0LED5zpB5ky712
yg0UgeR8obATrjKaR+ncI4P6qdKhJiBf4fHffNSZTRbyzJ2AyQm5Xr86FsxNSwou
MdBnaKKCzOqFoJmnO3SBeBeZ9qTju32itU0Z4Fon4/cpWTLkuDipVeLfVbzN8kq4
cZ43RHJJCfEudofN1nP8Z/c39RHzIehM/E/SEQIDAQABAoIBAQCEjJ0FTjbo5NZv
L81mJlnPU8ABtftMkHqj5/x0QuUuIaDyFysAo9uA8tbO5eJlR3C5cxVEBK0OXBbF
SxcRrdre6N+g9W3CexOVHmQNkXbLTxE1+LsyGwGAW5RDJQ1yfv8S70610Kb1LOwt
egFfriDUMB7VtmCnQMeegwJVLb5BBVuyF77gbTdOcVHQeC51vuierJcTd/JFSUpr
1B4UZseDdMwdreSLA6d2iosTSzdROpcrARoNrgThQwdlnXdAZEfo/GzyUFZ51gV2
CN/CLPVSPn3ENlAaukTyHWxg6Sgv2f+7Ag0arWJHdEFJ58mqm0Arp/49Du4VfTD6
/EV0T+fBAoGBAND4U1kkrKPiCw19+B86bvW6gXJ4Sjigup+5X8VRoK5JkqYDALU9
IaIc7tS865UnYA9cjIM4rUO8rkEGq+FmfIv3UEaXsag2682u1Wo7OSOSUtq4LbLP
PHT9sfKXOJ9Gd8oO0vrekRtSpurXM8zgDNf3VKl30heE8JvgvyMjdIr5AoGBAMNw
tHl3Cd5E5EUTkHfDxcG456jLlyie4Bs9wP7fOQDlayWM9eqyirXKw2ogZzYXV+3/
wOE/f8san2DL4LFMOw2xF4gYROrerguxG8Fwo4TyU79UNbokJ7gFebPaEA41ug5A
JOxr0xMJNb6nJKpLVRO2V0unvdR3BEAnxYq2qm3ZAoGAUyeuCxgT9vb5TPompU6c
Xv5DiqihaF1VRj//A0cTOKegSp2BR52254q54z/2QxkzGYnLhGAmWoEXmlqsRPqC
bzQP5rdwg66vMN70n9xHRYdxnwWRcckTlr5pdE6GwqLJAkfZ3uh4N7YxI9xVCZ7S
nZIXR4SdvqwxDuZlSPdP5gkCgYBuSQ0udcPlzz5Y1H9zdeAEP01KcQhtfanM9X4Q
1PofzVY3LGIg/HtVtoOrQXm8hlOyE95NvT1p6S4Cu0miAvhX85Tp0XgiaWIhauHU
uLEtdmlX0Dc5QOnA6CYTHXxt6FeDbyLm3rmPRmUznrIL/tKVexGruY5fdIHLiiXo
7schkQKBgA4NI7C94dOJm2cAvaKm6BSuoAinmnZ/5dpbmKl0zXTK9EH8EKKR1mGK
CR/RDEePUo+kOafVev6cRb23s5I90W5KcxyITe4ftoLCDpj1q7lmgcQ0qKD+dPv6
SwJ6L7QuvbmUah0yzjhAQcRw3tW+i2/ELMJ9T8cH2MYUpSedtoyN
-----END RSA PRIVATE KEY-----
```

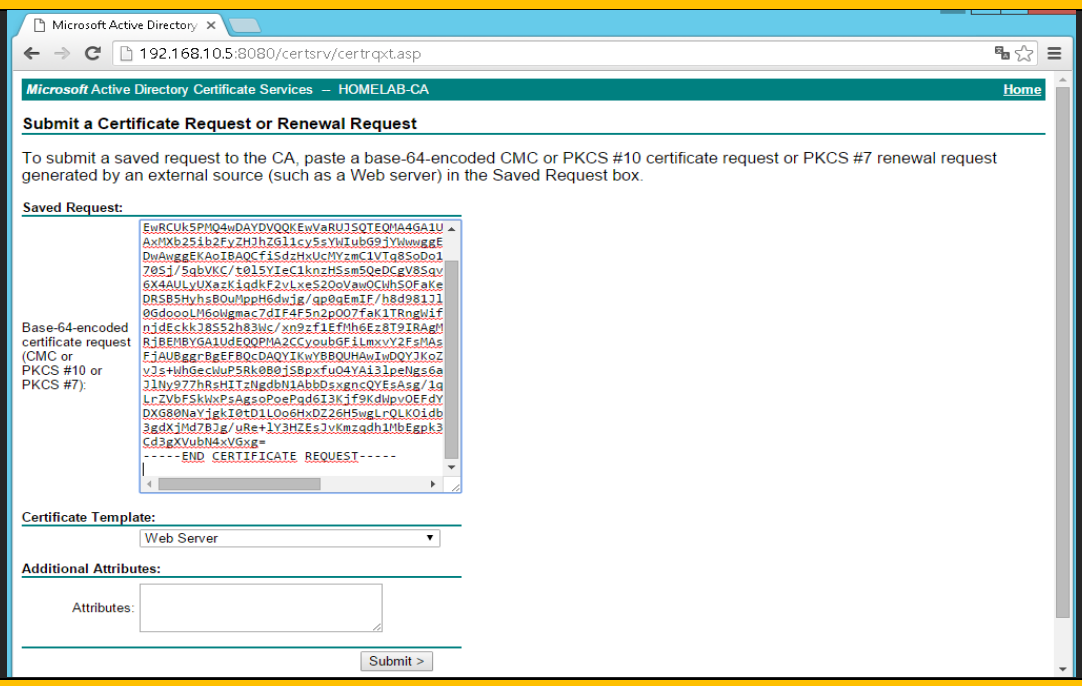

5	**Copy resulted file into your SFTP/FTP root folder replacing existing `onboardradius.prv` file. The goal of this operation is to have private key unencrypted available for export.**
6	**Open the imported CSR in any text editor and copy all the contents to the clipboard:**


```
-----BEGIN CERTIFICATE REQUEST-----
MIIDBzCCAe8CAQAwbTELMAkGA1UEBhMCQ1oxCzAJBgNVBAgTAkpNMQ0wCwYDVQQH
EwRCUk5PMQ4wDAYDVQQKEwVaRUJSQTEQMA4GA1UECxMHVE1FTEFCUzEgMB4GA1UE
AxMXb25ib2FyZHJhZGl1cy5sYWIubG9jYWwwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCfiSdzHxUcMYzmC1VTq8SoDo15Z/fs6TVNbBCpxs8CwREBAH+w
70Sj/5qbVKC/t0l5YIeC1knzHSsm5QeDCgV8Sqvdxzp2YK5xxotJI3ltuiEOZnz8
6X4AULyUXazKiqdkF2vLxeS2OoVawOCWhSOFaKepx9jpAwbzPQsQPnOkHmTLvXbK
DRSB5HyhsBOuMppH6dwjg/qp0qEmIF/h8d981J1NFvLMnYDJCblevzoWzE1LCi4x
0GdoooLM6oWgmac7dIF4F5n2pOO7faK1TRngWifj9ylZMuS4OKlV4t9VvM3ySrhx
njdEckkJ8S52h83Wc/xn9zf1EfMh6Ez8T9IRAgMBAAGgVTBTBgkqhkiG9w0BCQ4x
RjBEMBYGA1UdEQQPMA2CCyoubGFiLmxvY2FsMAsGA1UdDwQEAwIEsDAdBgNVHSUE
FjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwDQYJKoZIhvcNAQEFBQADggEBAF0v90BY
vJs+WhGecWuP5Rk0B0jSBpxfuO4YAi31peNgs6aD/UcLaknH4ZgE6G+9aQ5tpY0T
JlNy977hRsHITzNgdbN1AbbDsxgncQYEsAsg/1qYCd2zjxyyz8NCzwkwGoo3gCQO
LrZVbFSkWxPsAgsoPoePqd6I3Kjf9KdWpvOEFdY43bVsP/RvY5Wws5FCwH4Gj1jP
DXG80NaYjgkI0tD1LOo6HxDZ26H5wgLrQLKOidbTmt5HRKcRnAFKWGj1PZo6G/wA
3gdXjMd7BJg/uRe+lY3HZEsJvKmzqdh1MbEgpk3HVl+P7klIDeLJMmT5Am6qwx3V
Cd3gXVubN4xVGxg=
-----END CERTIFICATE REQUEST-----
```

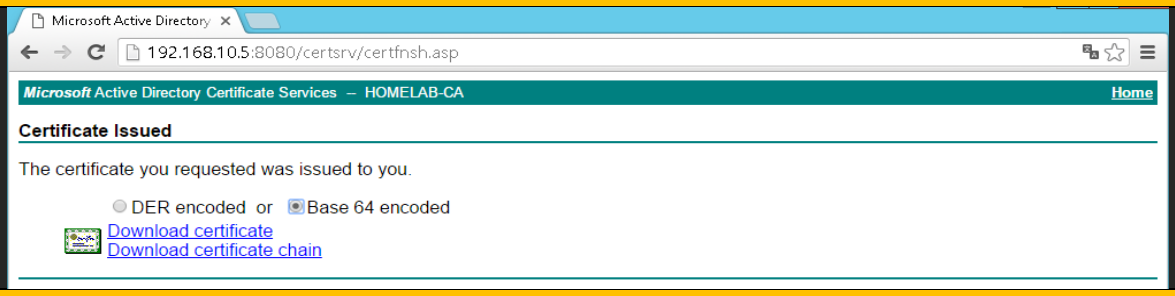

7	**Login to the Microsoft CA certification authority web enrolment service @ *<windows-server-address>/certsrv*. Login using Administrator or Enrollment Agent account:**



8	Press on ***Request a certificate -> advanced certificate request ->*** select ***Certificate Template*** as ***"Web Server",*** paste CSR contents into Saved Request Field and press ***Submit***:

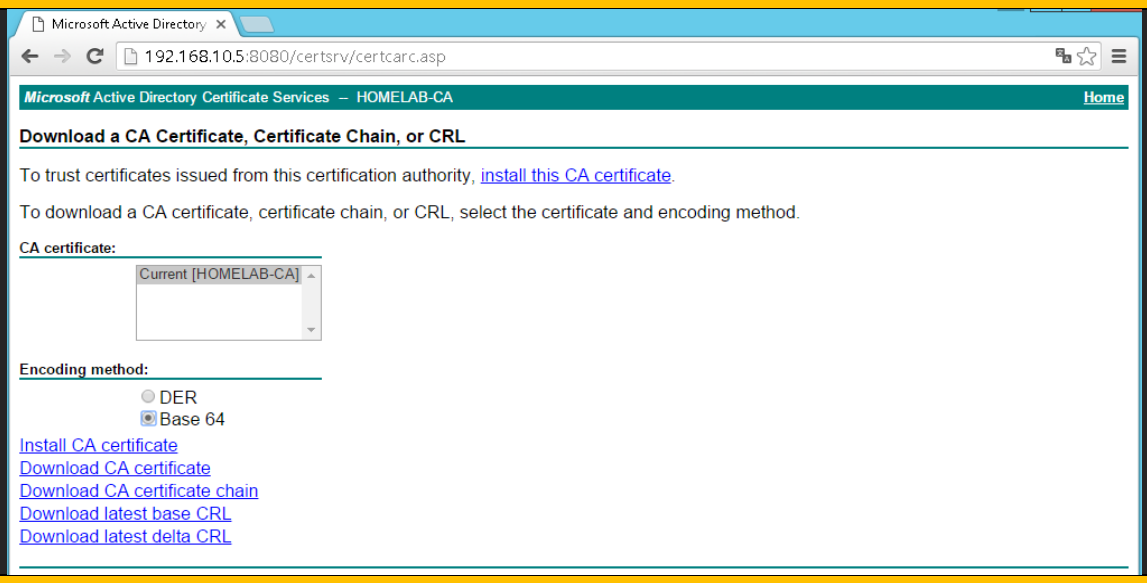


9	**Choose Base64 encoded certificate and click on Download Certificate:**



10	**Rename downloaded filename to `onboardradius.crt` (file extension must be *.crt*) and place the file into the root of your FTP/SFTP server.**

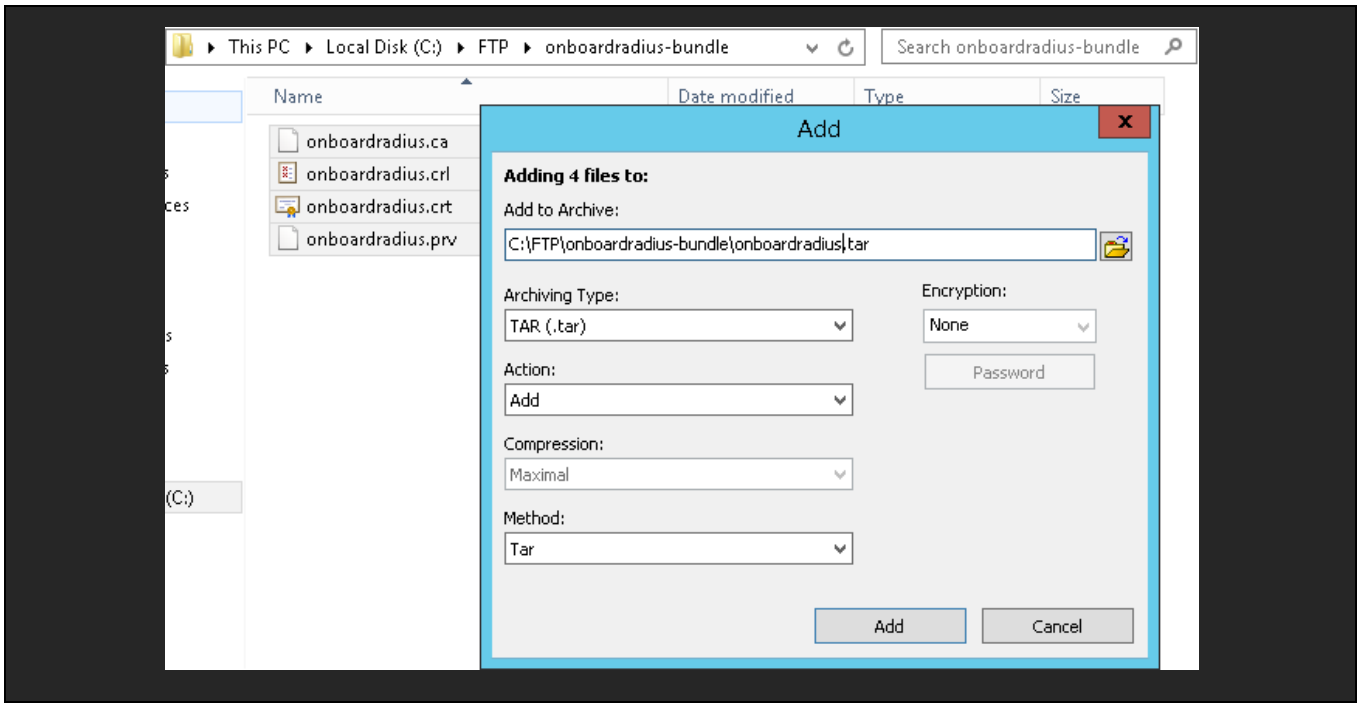
11	**On the Home screen of Certificate Services web page go to *"Download a CA certificate, certificate chain, or CRL"*. Then select your root CA, select encoding method as *Base64* and click on *Download certificate*:**



12	**Rename downloaded CA certificate file to `onboardradius.ca` and place it to the root of your SFTP/FTP server.**
13	**As a result in the root of your fileserver (SFTP/FTP) you should have these 3 files prepared:**

`onboardradius.prv`	RSA private key for the RADIUS server certificate
`onboardradius.crt`	public signed X509 certificate signed by private CA
`onboardradius.ca`	root CA certificate (or CA chain with all intermediary CAs)

14	**Create a trustpoint bundle using these 3 files using *IZarc* utility if you are using Windows, other utilities will not work with WiNG. Create a .tar package:** **onboardradius.tar**



2.2 Automatically Distributing a Trustpoint Bundle to the Access Points

In order to provide RADIUS server services to authenticate wireless clients using EAP-TLS, each Access Point must have a trustpoint bundle to present RADIUS server certificate to the client that is trying to authenticate. This section covers automatic upload of the trustpoint bundle to adopted Access Points.

1	**Upload trustpoint .tar bundle to the Controller first:**

```
VX#file-sync load-file trustpoint onboardradius sftp://usr:pwd@tme-dc-1.zebranoc.com/onboardradius.tar
--------------------------------------------------------------------------------
     CONTROLLER          STATUS                          MESSAGE
--------------------------------------------------------------------------------
  VX                 Success          Successfully initiated load file
--------------------------------------------------------------------------------
```

2	**Verify that the trustpoint has been successfully loaded to the Controller:**

```
VX#show file-sync load-file-status
Download of onboardradius trustpoint is complete
```

3	**Add configuration to the Access Point profile to use new trustpoint.** ***Important*** **– this step must be performed before uploading trustpoint bundle from the Controller to the Access Points.**

```
VX#conf
Enter configuration commands, one per line.  End with CNTL/Z.
VX-1(config)#profile anyap GENERIC-AP
VX-1(config-profile-GENERIC-AP)#trustpoint radius-ca onboardradius
VX-1(config-profile-GENERIC-AP)#trustpoint radius-server onboardradius
VX-1(config-profile-GENERIC-AP)#commit write
VX-1(config-profile-GENERIC-AP)#end
```

4	**Distribute the trustpoint down to the Access Points (All or per RF Domain):**

```
VX-1#file-sync trustpoint onboardradius ?
  DEVICE-NAME  Name/MAC address of AP
  all          All access points
  rf-domain    Upload all access points belonging to an RF Domain

VX-1#file-sync trustpoint onboardradius all
-------------------------------------------------------------------------------
        CONTROLLER            STATUS                    MESSAGE
-------------------------------------------------------------------------------
  00-0C-29-DA-47-C7        Fail           Could not find any matching APs
  00-0C-29-50-EE-80        Success        Added 12 APs to upload queue
-------------------------------------------------------------------------------

VX-1#show file-sync status
Number of APs currently being synced : 2
Number of APs waiting in queue to be synced : 0
-----------------------------------------------------------------------------------------------------
        AP           STATE     UPLOAD TIME PROGRESS RETRIES LAST SYNC ERROR        SYNCED BY
-----------------------------------------------------------------------------------------------------
  ap7502-6A2270   downloading   immediate   100      0       -               00-0C-29-50-EE-80
  6522-1-office   downloading   immediate   100      0       -               00-0C-29-50-EE-80
-----------------------------------------------------------------------------------------------------
```

5	**Verify that the trustpoint is now loaded on the Access Point:**

```
VX-1#show crypto pki trustpoints all on ap7502-6A2270

Trustpoint Name: onboardradius
-------------------------------------------------------------------------------
  CRL present: no
  Server Certificate details:
    Key used: onboardradius-srvr-priv-key
    Serial Number: 14000000749d68b08e499eecb3000000000074
    Subject Name:
      /C=CZ/ST=JM/L=Brno/O=Zebra/OU=TMELABS/CN=radius
    Issuer Name:
      /DC=local/DC=lab/CN=HOMELAB-CA
    Valid From : Thu Dec 10 11:21:26 2015 UTC
    Valid Until: Sat Dec  9 11:21:26 2017 UTC

  CA Certificate details:
    Serial Number: 71248696d64ddfa6482392195c668bd1
    Subject Name:
      /DC=local/DC=lab/CN=HOMELAB-CA
    Issuer Name:
      /DC=local/DC=lab/CN=HOMELAB-CA
    Valid From : Sat Apr  5 17:11:56 2014 UTC
    Valid Until: Fri Apr  5 17:21:52 2019 UTC


Trustpoint Name: default-trustpoint        (self signed)
-------------------------------------------------------------------------------
  CRL present: no
  Server Certificate details:
```

```
    Key used: default_rsa_key
    Serial Number: 05fa
    Subject Name:
      /CN=AP7502-84-24-8D-6A-22-70
    Issuer Name:
      /CN=AP7502-84-24-8D-6A-22-70
    Valid From : Wed Jan  1 00:01:37 2014 UTC
    Valid Until: Sat Dec 30 00:01:37 2023 UTC
```

6	**Optionally configure automatic file-sync at the controller to allow for automatic trustpoint uploads for new Access Points upon adoption:**

```
VX-1#conf
Enter configuration commands, one per line.  End with CNTL/Z.
VX-1(config)#profile vx9000 NOC
VX-1(config-profile-NOC)#file-sync auto
VX-1(config-profile-NOC)#commit write
VX-1(config-profile-NOC)#end
```

2.3 Configure Automatic CRL Updates

Certificate Revocation Lists can be automatically downloaded by the APs at specified time intervals (from 1 to 168 hours) from external file server via file-sync operation.

1	**Optionally configure automatic CRL file download from an external file server.** **In this example CRL file is stored on an external HTTPS server and Access Points will update it every 24 hours:**

```
VX-1#conf
Enter configuration commands, one per line.  End with CNTL/Z.
VX-1(config)#profile anyap REMOTE-AP
VX-1(config-profile-REMOTE-AP)#crypto pki import crl TMELABS-PKI https://tme-dc-
1.zebranoc.com/CRLD/TME-CA-ROOT.crl 24
VX-1(config-profile-REMOTE-AP)#commit write
VX-1(config-profile-REMOTE-AP)#end
```

2.4 Wireless LAN and AP profile configuration

2.4.1 Creating RADIUS Server Policy for the Access Points

```
!
radius-server-policy ONBOARD-TLS
 authentication eap-auth-type tls ignore-username-validation
!
```

2.4.2 Assign RADIUS Policy to an AP profile:

```
!
profile anyap REMOTE-AP
 no mint mlcp vlan
 no autoinstall configuration
 no autoinstall firmware
 use radius-server-policy ONBOARD-TLS
 interface radio1
 interface radio2
 interface ge1
 interface fe1
 interface fe2
 interface fe3
 interface vlan1
  ip address dhcp
  ip dhcp client request options all
 interface pppoe1
 use firewall-policy default
 logging on
 logging buffered debugging
 service pm sys-restart
!
```

2.4.3 Create AAA policy and add onboard RADIUS as a failover method if primary authentication server fails:

```
!
aaa-policy REDUNDANT-AAA
 authentication server 1 host radius-primary.zebranoc.com secret 0 radiussecret
 authentication server 1 timeout 1 attempts 2
 authentication server 1 retry-timeout-factor 50
 authentication server 2 onboard self
!
```

2.4.4 Create an 802.1X WLAN and assign it to the AP Profile:

```
!
wlan 8021X-CORP
 ssid 8021X-CORP
 vlan 1
 bridging-mode local
 encryption-type ccmp
 authentication-type eap
 no answer-broadcast-probes
 use aaa-policy REDUNDANT-AAA
!
profile anyap REMOTE-AP
 no mint mlcp vlan
 no autoinstall configuration
```

```
 no autoinstall firmware
 use radius-server-policy ONBOARD-TLS
 interface radio1
  wlan 8021X-CORP bss 1 primary
 interface radio2
 interface ge1
 interface fe1
 interface fe2
 interface fe3
 interface vlan1
  ip address dhcp
  ip dhcp client request options all
 interface pppoe1
 use firewall-policy default
 logging on
 logging buffered debugging
 service pm sys-restart
!
```

3. Connect a wireless client and verify functionality using remote-debug wireless

```
VX#remote-debug wireless rf-domain twinpeaks-domain clients all max-events 999 d
uration 999 events eap radius wpa-wpa2 management
Printing upto 999 messages from each remote system for upto 999 seconds. Use Ctrl-C to abort
[ap7502-6A2270] 16:37:22.928: mgmt:rx auth-req from 9C-F3-87-6B-9C-40 on radio 0 (mgmt.c:3801)
[ap7502-6A2270] 16:37:22.929: mgmt:tx auth-rsp to 9C-F3-87-6B-9C-40 on radio 0. status: success (mgmt.c:1302)
[ap7502-6A2270] 16:37:22.934: mgmt:rx association-req from 9C-F3-87-6B-9C-40 on radio ap7502-6A2270:R1 signal-strength is -
54dBm (mgmt.c:3782)
[ap7502-6A2270] 16:37:22.934: mgmt:Client 9C-F3-87-6B-9C-40 negotiated WPA2-EAP on wlan (aptlstest) (mgmt.c:3352)
[ap7502-6A2270] 16:37:22.934: mgmt:tx association-rsp success to 9C-F3-87-6B-9C-40 on wlan (aptlstest) (ssid:aptlstest) with
ftie 0 (mgmt.c:33
[ap7502-6A2270] 16:37:22.935: eap:sending eap-code-request code 1, type 1 to 9C-F3-87-6B-9C-40 (eap.c:944)
[ap7502-6A2270] 16:37:22.935: eap:sending eap-id-req to 9C-F3-87-6B-9C-40 (eap.c:971)
[ap7502-6A2270] 16:37:22.974: eap:rx eap id-response from 9C-F3-87-6B-9C-40 (eap.c:677)
[ap7502-6A2270] 16:37:22.974: radius:aaa-policy REDUNDANT-AAA user: Slava mac: 9C-F3-87-6B-9C-40 server_is_candidate: 1 1 0
0 0 0 (radius.c:47
[ap7502-6A2270] %%%%>16:37:22.979: radius:radius server hostname [radius-primary.zebranoc.com] not resolved. request for 9C-
F3-87-6B-9C-40 dro
[ap7502-6A2270] %%%%>16:37:23.480: radius:radius server hostname [radius-primary.zebranoc.com] not resolved. request for 9C-
F3-87-6B-9C-40 dro
[ap7502-6A2270] 16:37:23.981: eap:sending eap-failure to 9C-F3-87-6B-9C-40 (eap.c:987)
[ap7502-6A2270] %%%%>16:37:23.981: radius:no response from radius server REDUNDANT-AAA:1 for wireless client 9C-F3-87-6B-9C-
40 (eap.c:366)
[ap7502-6A2270] 16:37:23.982: mgmt:tx deauthentication [reason: radius server timeout (code:23)] to 9C-F3-87-6B-9C-40
(mgmt.c:1849)
[ap7502-6A2270] 16:37:24.328: mgmt:rx auth-req from 9C-F3-87-6B-9C-40 on radio 0 (mgmt.c:3801)
[ap7502-6A2270] 16:37:24.328: mgmt:tx auth-rsp to 9C-F3-87-6B-9C-40 on radio 0. status: success (mgmt.c:1302)
[ap7502-6A2270] 16:37:24.331: mgmt:rx association-req from 9C-F3-87-6B-9C-40 on radio ap7502-6A2270:R1 signal-strength is -
54dBm (mgmt.c:3782)
[ap7502-6A2270] 16:37:24.331: mgmt:Client 9C-F3-87-6B-9C-40 negotiated WPA2-EAP on wlan (aptlstest) (mgmt.c:3352)
[ap7502-6A2270] 16:37:24.332: mgmt:tx association-rsp success to 9C-F3-87-6B-9C-40 on wlan (aptlstest) (ssid:aptlstest) with
ftie 0 (mgmt.c:33
[ap7502-6A2270] 16:37:24.332: eap:sending eap-code-request code 1, type 1 to 9C-F3-87-6B-9C-40 (eap.c:944)
[ap7502-6A2270] 16:37:24.332: eap:sending eap-id-req to 9C-F3-87-6B-9C-40 (eap.c:971)
[ap7502-6A2270] 16:37:24.358: eap:rx eap id-response from 9C-F3-87-6B-9C-40 (eap.c:677)
[ap7502-6A2270] 16:37:24.358: radius:aaa-policy REDUNDANT-AAA user: Slava mac: 9C-F3-87-6B-9C-40 server_is_candidate: 1 1 0
0 0 0 (radius.c:47
[ap7502-6A2270] 16:37:24.360: radius:access-req sent to 127.0.0.1:1812 (attempt 1) for 9C-F3-87-6B-9C-40 (user:Slava)
(radius.c:2996)
[ap7502-6A2270] 16:37:24.364: radius:RAD MSG AUTHENTICATOR (radius.c:1180)
[ap7502-6A2270] 16:37:24.364: radius:rx access-challenge from radius server for 9C-F3-87-6B-9C-40 (radius.c:3793)
[ap7502-6A2270] 16:37:24.364: eap:sending eap-code-request code 1, type 13 to 9C-F3-87-6B-9C-40 (eap.c:944)
```

```
[ap7502-6A2270] 16:37:24.364: eap:sending eap-req [eap_type:13(eap-tls)] to 9C-F3-87-6B-9C-40 (eap.c:979)
[ap7502-6A2270] 16:37:24.450: eap:rx eap pkt from 9C-F3-87-6B-9C-40 (eap.c:700)
[ap7502-6A2270] 16:37:27.42: radius:access-req sent to 127.0.0.1:1812 (attempt 1) for 9C-F3-87-6B-9C-40 (user:Slava)
(radius.c:2996)
[ap7502-6A2270] 16:37:27.330: radius:RAD_MSG_AUTHENTICATOR (radius.c:1180)
[ap7502-6A2270] 16:37:27.330: radius:rx access-challenge from radius server for 9C-F3-87-6B-9C-40 (radius.c:3793)
[ap7502-6A2270] 16:37:27.330: eap:sending eap-code-request code 1, type 13 to 9C-F3-87-6B-9C-40 (eap.c:944)
[ap7502-6A2270] 16:37:27.330: eap:sending eap-req [eap_type:13(eap-tls)] to 9C-F3-87-6B-9C-40 (eap.c:979)
[ap7502-6A2270] 16:37:27.370: eap:rx eap pkt from 9C-F3-87-6B-9C-40 (eap.c:700)
[ap7502-6A2270] 16:37:27.372: radius:access-req sent to 127.0.0.1:1812 (attempt 1) for 9C-F3-87-6B-9C-40 (user:Slava)
(radius.c:2996)
[ap7502-6A2270] 16:37:27.381: radius:RAD_MSG_AUTHENTICATOR (radius.c:1180)
[ap7502-6A2270] 16:37:27.381: radius:rx UserName Slava for 9C-F3-87-6B-9C-40 (radius.c:1315)
[ap7502-6A2270] 16:37:27.381: radius:rx access-accept for 9C-F3-87-6B-9C-40 (radius.c:3558)
[ap7502-6A2270] 16:37:27.381: radius:radius: updating interim acct timeout of 9C-F3-87-6B-9C-40 to 1800 seconds
(radius.c:2136)
[ap7502-6A2270] 16:37:27.382: eap:sending eap-success to 9C-F3-87-6B-9C-40 (eap.c:987)
[ap7502-6A2270] 16:37:27.384: wpa-wpa2:tx msg #1 to 9C-F3-87-6B-9C-40 attempt: 1 (80211i.c:527)
[ap7502-6A2270] 16:37:27.390: wpa-wpa2:rx msg #2 from mu 9C-F3-87-6B-9C-40 (80211i.c:1074)
[ap7502-6A2270] 16:37:27.390: wpa-wpa2:tx msg #3 to 9C-F3-87-6B-9C-40 attempt: 1 (80211i.c:801)
[ap7502-6A2270] 16:37:27.394: wpa-wpa2:rx msg #4. WPA2-AES handshake done. 9C-F3-87-6B-9C-40 DATA-READY (80211i.c:1058)
```