Install Root Certificate on SDWAN vEdges

Contents

Introduction

This document describes how to install a root certificate in SD-WAN vEdges with different tools.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Catalyst Software-Defined Wide Area Network (SD-WAN)
- Certificates
- Basic Linux

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

- Cisco Catalyst SD-WAN Validator 20.6.3
- Cisco vEdge 20.6.3

Problem

A digital certificate is an electronic file that certifies the authenticity of a device, server, or user through the use of cryptography and public key infrastructure (PKI). Digital certificate authentication helps organizations ensure that only trusted devices and users can connect to their networks.

The identity for vEdge hardware routers is provided by a device certificate signed by Avnet, generated during the manufacturing process and burned into the Trusted Platform Module (TPM) chip. The Symantec/DigiCert and Cisco root certificates are pre-loaded in software for trust for the control components' certificates. Additional root certificates must either be loaded manually, distributed automatically by the SD-WAN Manager, or installed during the automated provisioning process.

One of the most common issues in SD-WAN is the Control Connections failure due to invalid certificate. This happens either because the certificate was never installed or due to corruption on it.

In order to validate the Control Connection error legend, use the EXEC command **show control connections-history**.

<#root>

```
vEdge #

show control connections-history


Legend for Errors
ACSRREJ    - Challenge rejected by peer.           NOVMCFG   - No cfg in vmanage for device.
BDSGVERFL  - Board ID Signature Verify Failure.    NOZTPEN   - No/Bad chassis-number entry in ZTP.
BIDNTPR    - Board ID not Initialized.             OPERDOWN  - Interface went oper down.
BIDNTVRFD  - Peer Board ID Cert not verified.      ORPTMO    - Server's peer timed out.
BIDSIG    - Board ID signing failure.              RMGSPR    - Remove Global saved peer.
CERTEXPRD  - Certificate Expired                   RXTRDWN   - Received Teardown.
CRTREJSER  - Challenge response rejected by peer.  RDSIGFBD  - Read Signature from Board ID failed.


CRTVERFL   - Fail to verify Peer Certificate.

          SERNTPRES - Serial Number not present.
CTORGNMMIS - Certificate Org name mismatch.        SSLNFAIL  - Failure to create new SSL context.
DCONFAIL   - DTLS connection failure.              STNMODETD - Teardown extra vBond in STUN server
DEVALC     - Device memory Alloc failures.         SYSIPCHNG - System-IP changed
DHSTMO     - DTLS HandShake Timeout.               SYSPRCH   - System property changed
DISCVBD    - Disconnect vBond after register reply.  TMRALC    - Timer Object Memory Failure.
DISTLOC    - TLOC Disabled.                        TUNALC    - Tunnel Object Memory Failure.
DUPCLHELO  - Recd a Dup Client Hello, Reset Gl Peer.  TXCHTOBD  - Failed to send challenge to BoardID.
DUPSER     - Duplicate Serial Number.              UNMSGBDRG - Unknown Message type or Bad Register
DUPSYSIPDEL- Duplicate System IP.                  UNAUTHEL  - Recd Hello from Unauthenticated peer
HAFAIL     - SSL Handshake failure.                VBDEST    - vDaemon process terminated.
IP_TOS     - Socket Options failure.               VECRTREV  - vEdge Certification revoked.
LISFD      - Listener Socket FD Error.             VSCRTREV  - vSmart Certificate revoked.
MGRTBLCKD  - Migration blocked. Wait for local TMO.  VB_TMO    - Peer vBond Timed out.
MEMALCFL   - Memory Allocation Failure.            VM_TMO    - Peer vManage Timed out.
NOACTVB    - No Active vBond found to connect.     VP_TMO    - Peer vEdge Timed out.
NOERR      - No Error.                             VS_TMO    - Peer vSmart Timed out.
NOSLPRCRT  - Unable to get peer's certificate.     XTVMTRDN  - Teardown extra vManage.
NTPRVMINT  - Not preferred interface to vManage.   XTVSTRDN  - Teardown extra vSmart.
STENTRY    - Delete same tloc stale entry.

PEER     PEER     PEER              SITE        DOMAIN PEER             PRIVATE  PEER             PUBLIC
TYPE     PROTOCOL SYSTEM IP         ID          ID     PRIVATE IP       PORT     PUBLIC IP        PORT
----------------------------------------------------------------------------------------------------------
vbond    dtls     -                 0           0      10.10.10.1     12346    10.10.10.1     12346   pu
vbond    dtls     -                 0           0      10.10.10.2     12346    10.10.10.2     12346   pu
```

Some common causes for the error label CRTVERFL are:

- The expiration time of the certificate.
- Root-ca is different.

    - Whether an update of root-ca happens in controllers.
    - Certificate Authority (CA) different by Cisco is used and devices need the manual installation of the root-ca.
- Change of Certificate Authority in the Overlay.

Note: For more information on Control Connections errors visit [Troubleshoot SD-WAN Control Connections.]()

The root-ca file needs to be exactly the same across all components in the Overlay. There are two ways to validate the root-ca file in used is not the correct one

1. Review the size of the file, this is helpfull in situations in which the root-ca had an update.

<#root>

```
vBond:/usr/share/viptela$ ls -l
total 5
-rw-r--r-- 1 root root   294 Jul 23 2022 ISR900_pubkey.der
-rw-r--r-- 1 root root  7651 Jul 23 2022 TPMRootChain.pem
-rw-r--r-- 1 root root 16476 Jul 23 2022 ViptelaChain.pem
-rwxr-xr-x 1 root root 32959 Jul 23 2022 ios_core.pem

-rw-r--r-- 1 root root 24445 Dec 28 13:59 root-ca.crt
```

<#root>

```
vEdge:/usr/share/viptela$ ls -l
total 6
drwxr-xr-x 2 root root   4096 Aug 28  2022 backup_certs
-rw-r--r-- 1 root root   1220 Dec 28 13:46 clientkey.crt
-rw------- 1 root root   1704 Dec 28 13:46 clientkey.pem
-rw------- 1 root root   1704 Dec 28 13:46 proxy.key
-rw-r--r-- 1 root root      0 Aug 28  2022 reverse_proxy_mapping


-rw-r--r-- 1 root root  23228 Aug 28  2022 root-ca.crt
```

2. Second and most reliable way to validate that the file is exactly the same as the source file is with the **md5sum root-ca.crt** vshell command. Once the md5 is provided, compare the result of both components Controller and Edge device.

<#root>

```
vBond:/usr/share/viptela$

md5sum root-ca.crt



a4f945b9a1f50f1fa68d539dcf2e54f2 root-ca.crt
```

<#root>

```
vEdge:/usr/share/viptela$

md5sum root-ca.crt



b36358d01b36254a54db2f8db2266ced root-ca.crt
```

Note: As the **md5sum root-ca.crt** vshell command is used to verify the integrity of files, as virtually any change to a file causes the MD5 hash to be different.

Solution

The root certificate chain of a device can be installed with multiple tools. There are two ways to install it with the use of Linux commands.

Create root-ca with Linux CAT Command in vShell

Note: This procedure applies for root-ca files that do not have blank lines inside the content, for situations with blank lines used Linux vi editor procedure.

Step 1. Obtain and copy root-ca.crt file from the validator.

The root-ca is the same across all controllers and can be copied from any of them in the path **/usr/share/viptela/**.

<#root>

```
vBond#

 vshell


vBondvBond:~$

cat /usr/share/viptela/root-ca.crt


-----BEGIN CERTIFICATE-----
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/ArrOPO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R7Orfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz1O/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zA0BgNVHQ8BAf8E
```

```
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
```

Step 2. Create the root-ca.crt file in the vedge.

From vshell, navigate to /**home/admin** or **/home/<username>** and create root-ca.crt file.

<#root>

```
vEdge#
```

```
vshell
```

```
vEdge:~$
```

```
 cat <<"" >> root-ca.crt
```

```
> -----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
>
vEdge:~$
```

Step 3. Validate it is complete.

<#root>

```
vEdge:~$
```

```
cat root-ca.crt
```

```
-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
```

```
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
vEdge:~$
```

Note: It is important to validate the file is complete, if not complete, delete the file with **rm root-ca.crt** vshell command and create it again from Step 2.

Exit vshell and continue with the Section.

<#root>

```
vEdge:~$

exit
```

Create root-ca with VI Text Editor in vShell

Step 1. Obtain and copy root-ca.crt file from the validator.

The root-ca is the same across all controllers and can be copied from any of them in the path **/usr/share/viptela/**.

<#root>

```
vBond#

 vshell


vBond:~$

cat /usr/share/viptela/root-ca.crt


-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
```

Step 2. Create the root-ca.crt file into the vedge.

From vshell, navigate to **/home/admin** or /**home/<username>** and create root-ca.crt file.

<#root>

```
vEdge#
```

```
vshell
```

```
vEdge:~$
```

```
 cd /usr/share/viptela/
```

```
vEdge:~$
```

```
pwd
```

```
/home/admin
vEdge:~$ vi root-ca.crt
```

Once click enter, editor prompt appears.

Step 3. Enter into insert mode

- Type: **i** and paste the content of the certificate from Step 1. Scroll down and validate certificate is complete.

Step 4. Escape insert mode and save certificate.

- Press **ESC** key.
- Type **:wq!** followed by enter in order to save changes and exit the editor.

<#root>

```
vEdge:/usr/share/viptela$
```

```
cat root-ca.crt
```

```
-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
```

Step 5. Validate it is complete.

<#root>

```
vEdge:~$
```

```
cat root-ca.crt
```

```
-----BEGIN CERTIFICATE-----
MIIEOzCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjM1OTU5WjCByjEL
U2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9y
SdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQG
BO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+
rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/
NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8E
BAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAH
BgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVy
aXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEFH/TZafC3ey78DAJ80M5+gKv
hnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
vEdge:~$
```

Note: It is important to validate the file is complete, if not complete, delete the file with **rm root-ca.crt** vshell command and create it again from Step 2.

Exit vshell and continue with the Section.

<#root>

```
vEdge:~$
```

```
exit
```

Install Certificate

Step 1. Install the root-ca certificate with the command **request root-cert-chain install <path>.**

<#root>

```
vEdge#
```

```
request root-cert-chain install /home/admin/root-ca.crt
```

```
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/PKI.pem via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
```

Step 2. Validate it is installed with the **show control local properties** command.

<#root>

```
vEdge#

show control local-properties


personality vedge
organization-name organization-name
root-ca-chain-status Installed

certificate-status Installed
certificate-validity Valid
certificate-not-valid-before Apr 11 17:57:17 2023 GMT
certificate-not-valid-after Apr 10 17:57:17 2024 GMT
```