

Renew Umbrella Root Certificate for Token Based Configuration

Contents

[Introduction](#)

[Prerequisite](#)

[Requirements](#)

[Components Used](#)

[Background](#)

[Steps to Perform](#)

[Troubleshooting](#)

[Verification](#)

[Related Information](#)

Introduction

This document describes the process to renew the Umbrella root certificate when token based registration is used for Cisco IOS® XE SD-WAN devices.

Prerequisite

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of Public Key Infrastructure (PKI).
- Knowledge of Cisco SD-WAN technology

This workflow is only to be used if you are using token based Umbrella registration. In case you are using API based registration, steps mentioned in Field Notice [FN74166](#) to be followed to get the root certificate installed.

Components Used

The information in this document is based on these software and hardware versions:

- C8000V version 17.6.6
- vManage version 20.6.6

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.

Background

Umbrella renewed the certificate for FQDN api.opendns.com starting 29-May-2024 and the certificate was signed by a new root-ca **DigiCert Global Root G2**. If the Edge device does not have this root-ca present in PKI certificate list and if it uses token based Umbrella Registration, the Umbrella registration is going to fail. The workflow in this document covers how to install the root-ca on the Edge router.

Steps to Perform

Please check if the Edge device has token based Umbrella registration. This is how the configuration would look like.

```
parameter-map type umbrella global
  token 83F1YHF457592596A3D8CF52YHDFSDRD
```

Other configuration that is required for the Edge device registration process to initiate and for it to take the root certificate and have it installed.

```
parameter-map type umbrella global
  vrf 10
  dns-resolver umbrella >>>>required

ip nat inside source list nat-acl interface GigabitEthernet0/0/0 overload

interface GigabitEthernet0/0/0
  ip dhcp client client-id ascii FGL233913F6
  ip address 10.122.164.132 255.255.255.128
  ip nat outside >>>>>
  negotiation auto
end
```

On the Edge device check if the root certificate **trustidrootx3_ca_092024.ca** exists at location **/bootflash**.

```
cedge-ISR1100-4G#dir bootflash: | in .ca
30 -rw- 237 Aug 13 2024 08:47:55 +00:00 pki_certificates
25 -rw- 1294 Aug 13 2024 08:46:54 +00:00 trustidrootx3_ca_092024.ca
```

Download this root certificate "DigiCert Global Root G2" on the Edge device at location **/bootflash/sdwan** with name **trustidrootx3_ca_092024.ca**.

```
-----BEGIN CERTIFICATE-----
MIIDjjCCAnagAwIBAgIQAzrx5qcRqaC7KGSxHQn65TANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRG1naUNlbnQgSW5jMRkwFwYDVQQLEwB3
d3cuZG1naWNlbnQyY29tMSAwHgYDVQQDExEaWdpQ2VydCBHbG9iYU9wY2VydCBH
MjAeFw0xMzA4MDExMjA4MDEzODAxMTUxMjA4MDEzODAxMTUxMjA4MDEzODAxMTUx
MRUwEwYDVQQKEwxEaWdpQ2VydCBHbG9iYU9wY2VydCBHbG9iYU9wY2VydCBHbG9i
b20xIDAeBgNVBAMTFORpZ21DZXJ0IEEdsb2JhbCBSb290IEcyMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEaUzfnNNx7a8myaJCtSnX/RrohCgin9R1UyfuI
```

```
2/Ou8jqJkTx65qsGGmvPrC3oXgkkRLpimn7Wo6h+4FR1IAWsULecYxpsMNzaHmx
1x7e/dfgy5SDN67sH0N03Xss0r0upS/kqbit0tSZpLYl6ZtrAGCSYP9PIUkY92eQ
q2EGnI/yuum06ZIya7XzV+hdG82MHauVBJVJ8zUt1uNjbd134/tJS7SsVQepj5Wz
tC07TG1F8PapsUwtP1MVYwnS1cUfIKdzXOS0xZKBgyMUNGPHgm+F6HmIcr9g+UQ
vI01CsRnKPZzFBQ9RnbDhxSJITRNrw9FDKZJJobq7nMwxM4MphQIDAQABo0IwQDAP
BgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAWIBhjAdBgNVHQ4EFgQUTiJUIBiV
5uNu5g/6+rks7QYXjzkWQYJKoZIhvcNAQELBQADggEBAGBnKJRvDkhj6zHd6mcY
1Yl9PMWLSn/pvtsrF9+wX3N3KjIT0YFnQoQj8kVnNeyIv/iPsGEMNKSuIEyExtv4
NeF22d+mQrvHRAiGfzZ0JFrabA0UWTW98kndth/Jsw1HKj2ZL7tCu7XUIOGZX1NG
Fdtom/DzMNU+MeKNhJ7jitra1j41E6Vf8P1wUHBHQRFxGU7Aj64GxJUTFy8bJZ91
8rG0maFvE7FBcf6IKshPECBV1/MURexGRPTqh5Uykw7+U0b6LJ3/iyK5S9kJRaTe
pLiaWN0bfVKfj11DiIGknibVb63dDcY3fe0Dkhv1d1927jyNxF1WW6LZZm6zNTf1
MrY=
-----END CERTIFICATE-----
```

Move the old root-certificate under **/bootflash:trustidrootx3_ca_092024.ca** to **/bootflash/sdwan** by renaming it to **trustidrootx3_ca_092024.ca.bkp**.

```
copy bootflash:trustidrootx3_ca_092024.ca bootflash:sdwan/trustidrootx3_ca_092024.ca.bkp
```


Delete the root certificate **trustidrootx3_ca_092024.ca** from **/bootflash**.

```
cedge-ISR1100-4G#delete bootflash:trustidrootx3_ca_092024.ca
```

Move the new root certificate **trustidrootx3_ca_092024.ca** under **/bootflash/sdwan** to **/bootflash**.

```
copy bootflash:sdwan/trustidrootx3_ca_092024.ca bootflash:
```

Reload the Edge device.

 **Note:** This process needs to be followed if you have token based Umbrella registration. In case API based registration is used, the process in the Field notice referenced in this document is to be followed.

Troubleshooting

These debug can be enabled on the Edge device to see if the new root certificate is getting installed.

```
cedge-ISR1100-4G#debug umbrella device-registration
```

To see the logs you can either do **show logging** or check the file **IOSRP_R0** under **/tmp/rp/trace**. You

would see these logs.

Success

```
2024/08/13 08:36:18.289855465 {IOSRP_R0-0}{1}: [iosrp] [24596]: UUID: 0, ra: 0, (info): *Aug 13 08:36:
```

Failure

```
2024/08/13 08:36:20.838420795 {IOSRP_R0-0}{1}: [iosrp] [24596]: UUID: 0, ra: 0, (warn): *Aug 13 08:36:
```

Verification

To verify if the certificate is installed successfully on the Edge device, you could use these commands.

```
cedge-ISR1100-4G#show crypto pki certificates
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 033AF1E6A711A9A0BB2864B11D09FAE5
  Certificate Usage: Signature
  Issuer:
    cn=DigiCert Global Root G2
    ou=www.digicert.com
    o=DigiCert Inc
    c=US
  Subject:
    cn=DigiCert Global Root G2
    ou=www.digicert.com
    o=DigiCert Inc
    c=US
  Validity Date:
    start date: 12:00:00 UTC Aug 1 2013
    end date: 12:00:00 UTC Jan 15 2038
  Associated Trustpoints: trustidrootx3_ca_092024
  Storage: nvram:DigiCertGlob#FAE5CA.cer
```

```
cedge-ISR1100-4G#show crypto pki trustpoints
Trustpoint SLA-TrustPoint:
  Subject Name:
    cn=Cisco Licensing Root CA
    o=Cisco
    Serial Number (hex): 01
  Certificate configured.
```

```
Trustpoint trustidrootx3_ca_092024:
  Subject Name:
    cn=DigiCert Global Root G2
    ou=www.digicert.com
```

o=DigiCert Inc

c=US

Serial Number (hex): 033AF1E6A711A9A0BB2864B11D09FAE5
Certificate configured.

Related Information

- [Cisco Umbrella Integration](#)
- [Technical Support & Documentation - Cisco Systems](#)