Troubleshoot the Umbrella ISR4k Integration

Contents

Introduction

This document describes how to troubleshoot the Umbrella ISR4k integration

Prerequisites

Requirements

There are no specific requirements for this document.

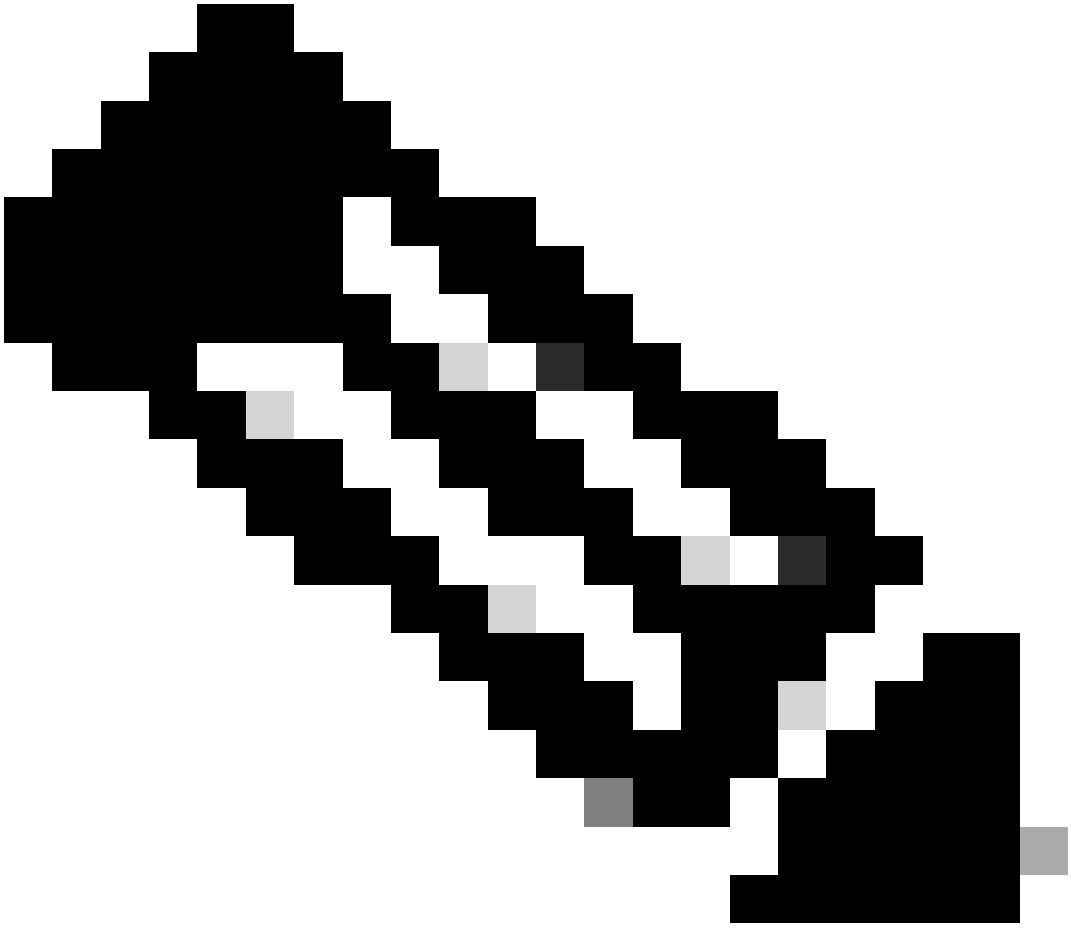
Components Used

The information in this document is based on Cisco Umbrella.

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.

Overview

This article is a continuation of Cisco Umbrella Integration for ISR4k deployment guide and is provided as a guide to aid troubleshooting registration issues, as well as problems with internal and external DNS resolution.



Note: The renewed cert for api.opendns.com from 29-May-2024 is now signed by a new chain/intermediate/root. The new root is DigiCert Global Root G2 (serial: 033af1e6a711a9a0bb2864b11d09fae5).

Registration and Certificate Import

1. Obtain your API Token from Umbrella Dashboard: **Admin > API Keys > (create) Legacy Network Devices.**

2. Import the CA certificate to the ISR4k via CLI using either of these methods:

Import from URL:
Issue the command and allow ISR4k fetch the cert:

```
crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b
```

Import directly in terminal:
Copy and paste the CA certificate (see attachment) using the command:

(This certificate is for *DigiCert Global Root G2*.)

```
crypto pki trustpool import terminal
-----BEGIN CERTIFICATE-----
MIIDjjCCAnagAwIBAgIQAzrx5qcRqaC7KGSxHQn65TANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0xMzA4MDExMjAwMDBaFw0zODAxMTUxMjAwMDBaMGExCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IEcyMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuzfNNNx7a8myaJCtSnX/RrohCgiN9RlUyfuI
2/Ou8jqJkTx65qsGGmvPrC3oXgkkRLpimn7Wo6h+4FR1IAWsULecYxpsMNzaHxmx
1x7e/dfgy5SDN67sH0NO3Xss0r0upS/kqbitOtSZpLYl6ZtrAGCSYP9PIUkY92eQ
q2EGnI/yuum06ZIya7XzV+hdG82MHauVBJVJ8zUtluNJbd134/tJS7SsVQepj5Wz
tCO7TG1F8PapspUwtP1MVYwnSlcUfIKdzXOS0xZKBgyMUNGPHgm+F6HmIcr9g+UQ
vIOlCsRnKPZzFBQ9RnbDhxSJITRNrw9FDKZJobq7nMWxM4MphQIDAQABo0IwQDAP
BgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUTiJUIBiV
5uNu5g/6+rkS7QYXjzkwDQYJKoZIhvcNAQELBQADggEBAGBnKJRvDkhj6zHd6mcY
1Yl9PMWLSn/pvtsrF9+wX3N3KjITOYFnQoQj8kVnNeyIv/iPsGEMNKSuIEyExtv4
NeF22d+mQrvHRAiGfzZ0JFrabA0UWTW98kndth/Jsw1HKj2ZL7tcu7XUIOGZX1NG
Fdtom/DzMNU+MeKNhJ7jitralj41E6Vf8PlwUHBHQRFXGU7Aj64GxJUTFy8bJZ91
8rGOmaFvE7FBcf6IKshPECBV1/MUReXgRPTqh5Uykw7+U0b6LJ3/iyK5S9kJRaTe
pLiaWN0bfVKfjllDiIGknibVb63dDcY3fe0Dkhvld1927jyNxF1WW6LZZm6zNTfl
MrY=
-----END CERTIFICATE-----
```

Copy and paste the Intermediate certificate using the command:

(This certificate is for *DigiCert Global G2 TLS RSA SHA256 2020 CA1*.)

```
crypto pki trustpool import terminal
-----BEGIN CERTIFICATE-----
MIIEyDCCA7CgAwIBAgIQDPW9BitWAvR6uFAsI8zwZjANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0yMTAzMzAwMDAwMDBaFw0zMTAzMjkyMzU5NTlaMFkxCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxMzAxBgNVBAMTKkRpZ2lDZXJ0IEdsb2Jh
bCBHMiBUTFMgUlNBIFNIQTI1NiAyMDIwIENBMTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAMz3EGJPprtjb+2QUlbFbSd7ehJWivH0+dbn4Y+9lavyYEEV
cNsSAPonCrVXOFt9slGTcZUOakGUWzUb+nv6u8W+JDD+Vu/E832X4xT1FE3LpxDy
FuqrIvAxIhFhaZAmunjZlx/jfWardUSVc8is/+9dCopZQ+GssjoP8Oj812s3wWPc
3kbW2OX+fSP9kOhRBx5Ro1/tSUZUfyyIxfQTnJcVPAPooTncaQwywa8WV0yUR0J8
osicfebUTVSvQpmowQTCd5zWSOTOEeAqgJnwQ3DPP3ZrOUxJqyRewg2C/Uaoq2yT
zGJSQnWS+Jr6Xl6ysGHlHx+5fwmY6D36g39HaaECAwEAAaOCAYIwggF+MBIGA1Ud
EwEB/wQIMAYBAf8CAQAwHQYDVR0OBBYEFHSFgMBmx9833s+9KTeqAx2+7c0XMB8G
A1UdIwQYMBaAFE4iVCAYlebjbuYP+vq5EuOGF485MA4GA1UdDwEB/wQEAwIBhjAd
BgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwdgYIKwYBBQUHAQEEajBoMCQG
CCsGAQUFBzABhhhodHRwOi8vb2NzcC5kaWdpY2VydC5jb20wQAYIKwYBBQUHMAKG
NGh0dHA6Ly9jYWNlcnRzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RH
Mi5jcnQwQgYDVR0fBDswOTA3oDWgM4YxaHR0cDovL2NybDMuZGlnaWNlcnQuY29t
L0RpZ2lDZXJ0R2xvYmFsUm9vdEcyLmNybDA9BgNVHSAENjA0MAsGCWCGSAGG/WwC
```

```
ATAHBgVngQwBATAIBgZngQwBAgEwCAYGZ4EMAQICMAgGBmeBDAECAzANBgkqhkiG
9w0BAQsFAAOCAQEAkPFwyyiXaZd8dP3A+iZ7U6utzWX9upwGnIrXWkOH7U1MVl+t
wcW1BSAuWdH/SvWgKtiwla3JLko716f2b4gp/DA/JIS7w7d7kwcsr4drdjPtAFVS
slme5LnQ89/nD/7d+MS5EHKBCQRfz5eeLjJ1js+aWNJXMX43AYGyZmOpGrFmCW3R
bpD0ufovARTFXFZkAdl9h6g4U5+LXUZtXMYnhIHUfoyMo5tS58aI7Dd8KvvwVVo4
chDYABPPTHPbqjc1qCmBaZx2vN4Ye5DUys/vZwP9BFohFrH/6j/f3IL16/RZkiMN
JCqVJUzKoZHm1Lesh3Sz8W2jmdv51b2EQJ8HmA==
-----END CERTIFICATE-----
```

3. Enter the API token to ISR4k CLI using the command:

```
parameter-map type umbrella global
token XXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

4. This is the bare minimum sample configuration on ISR4k:

```
interface GigabitEthernet0/0/0
ip address 192.168.50.249 255.255.255.252
ip nat outside
umbrella out

interface GigabitEthernet0/0/1.10
encapsulation dot1Q 10
ip address 192.168.8.254 255.255.255.0
ip nat inside
umbrella in odns_v10_5
```

Additional information:

- Ensure you configure the "umbrella out" before "umbrella in" command.
- Registration can be successful only when port 443 is in an open state and allows the traffic to pass through any existing firewall.
- In older Cisco IOS XE Denali version, the OpenDNS command is used instead of Umbrella.

Verifying the Certificate Import and Device Registration

1. Verify if the CA certificate has been stored successfully on the ISR4k device:

- If the certificate import was done using the URL, issue the command `dir nvram:` to verify that the **ios.p7b** certificate is successfully stored in the device NVRAM.

```
ISR4k02-CWSSDMLAB#dir nvram:
Directory of nvram:/

32769  -rw-        3086                    <no date>  startup-config
32770  ----        3582                    <no date>  private-config
32771  -rw-        3086                    <no date>  underlying-config
    1  ----         426                    <no date>  persistent-data
    2  -rw-        1182                    <no date>  ISR4451-X-4x1GE_0_0_0
    4  -rw-          17                    <no date>  ecfm_ieee_mib
    5  -rw-           0                    <no date>  ifIndex-table
    6  -rw-        1736                    <no date>  QuoVadisRoot#D3ACCA.cer
    8  -rw-         793                    <no date>  CiscoECCRoot#2CA.cer
    9  -rw-         791                    <no date>  CiscoRootCAM#1CA.cer
   10  -rw-        1697                    <no date>  QuoVadisRoot#5C6CA.cer
   12  -rw-        1088                    <no date>  CiscoRootCA2#CCA.cer
   14  -rw-        1467                    <no date>  QuoVadisRoot#509CA.cer
   16  -rw-         825                    <no date>  CiscoRXC-R2#1CA.cer
   17  -rw-         464                    <no date>  CiscoECCRoot#1CA.cer
   18  -rw-         846                    <no date>  DSTRootCAX3#406BCA.cer
   19  -rw-        1492                    <no date>  QuoVadisRoot#508BCA.cer
   21  -rw-         805                    <no date>  CiscoLicensi#1CA.cer
   22  -rw-        1176                    <no date>  DigiCertGlob#BC91CA.cer
   24  -rw-        2945                    <no date>  cwmp_inventory
   27  -rw-      146259                    <no date>  ios.p7b
```

115016968663

- If the certificate import was done using the copy/paste method, run the command `show cry pki trustpool` and verify the **serial number** and **cn** of the certificate:

```
#sh umbrella deviceid
Device registration details
Interface Name          Tag                 Status          Device-id
GigabitEthernet0/0/1    [redacted]          200 SUCCESS     010a9e60fe3b4689

#sh crypto pki trustpool | inc Digi
    cn=DigiCert Global Root G2
    o=DigiCert Inc
    cn=DigiCert Global Root G2
    o=DigiCert Inc
    cn=DigiCert Global Root CA
    o=DigiCert Inc
    cn=DigiCert Global Root CA
    o=DigiCert Inc
    cn=DigiCert Global Root CA
    o=DigiCert Inc
    cn=DigiCert TLS RSA SHA256 2020 CA1
    o=DigiCert Inc
    http://crl3.digicert.com/DigiCertGlobalRootCA.crl
    http://crl4.digicert.com/DigiCertGlobalRootCA.crl
[redacted]#
```

28552066223252

2. To verify the successful registration of the ISR4k, run the command `show umbrella deviceid`.

Sample output:

```
Device registration details

Interface Name                          Tag            Status       Device Id

interface GigabitEthernet0/0/1.10     odns_v10_5     200 SUCCES   010a04efd4e4bc14

interface GigabitEthernet0/0/1.11     odns_v11       200 SUCCES   010a04efd4e4xy15
```

Dashboard output:

115016791766

Debugging & Logging

- Verify ISR4k version: `show version` or `show platform` (required Cisco IOS XE Denali 16.3 or newer)
- Enable device registration debug logs: "`debug umbrella device-registration`" then "`show logging`" (to disable - `no debug umbrella device-registration`)

These are sample logs:

Certificate missing:

```
Jun 13 04:05:32.639: %OPENDNS-3-SSL_HANDSHAKE_FAILURE: SSL handshake failed
```

Certificate installed and device is successfully registered:

```
*%PKI-6-TRUSTPOOL_DOWNLOAD_SUCCESS: Trustpool Download is successful
*%OPENDNS-6-DEV_REG_SUCCESS: Device id for interface/tag GigabitEthernet0/0/1/odns_v10_5 is 010a0e4bc14
```

Api.opendns.com is not resolvable:

<#root>

%UMBRELLA-3-DNS_RES_FAILURE:

Failed to resolve name api.opendns.com

Retry attempts:0

- Verify DNS resolution: There is no 'dig' or 'nslookup' command available on ISR4k. It is best use "`ping hostname source interface #`" from the ISR4k CLI
- ISR with VRF configured: On the interface, make sure you have "`ip name-server vrf <vrf_name> <dns_server_ip>`" configured and verify with "`ping vrf <vrf_name> api.opendns.com`"
- Ensure "ip dns server" is configured: This allows the ISR to be queried directly.
- To disable DNSCrypt, enter this command: `parameter-map type umbrella global > no dnscrypt`
- Internal domain verification: Run the command `show umbrella config` and look for the Local Domain Regex, for example:
  - `show umbrella config` > Local Domain Regex parameter-map: dns bypass
  - `show run | be dns_bypass`
  - `show platform hardware qfp active feature dns-snoop-agent client hw-pattern-list`
- Unable to import certificate using URL or certificate imported using terminal is getting deleted after reboot:

```
crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b

% Error: failed to open file.

% No certificates imported from http://www.cisco.com/security/pki/trs/ios.p7b.
```

Workaround: manually download "ios.p7b" cert bundle via curl and copy to the Router's flash > Clear existing certificate from pool > Import "ios.p7b" cert bundle from flash:

```
<#root>

Show run | sec crypto pki

crypto pki certificate pool

 cabundle nvram:Trustpool15.cer


crypto pki trustpool clean
```

```
crypto pki trustpool import url flash:ios.p7b

Reading file from bootflash:ios.p7b

% PEM files import succeeded.
```