Troubleshoot Umbrella Wireless Controller (9800) Integration

Contents

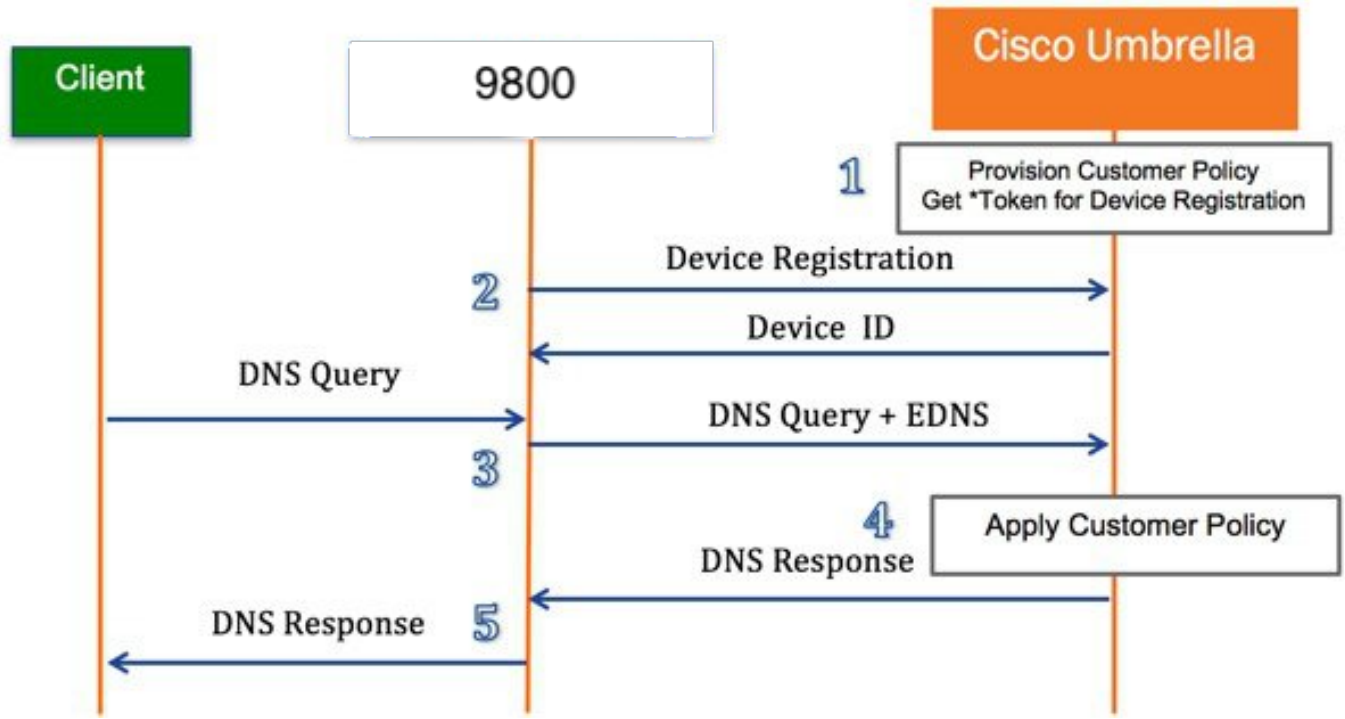
Introduction

This document describes how to troubleshoot 9800 series wireless controller integration with Umbrella.

Overview

This article is a continuation of[Cisco Catalyst 9200 and Catalyst 9300 Switches](#) and serves as a guide to troubleshooting registration issues as well as the workflow between 9800 and Cisco Umbrella.

Cisco Umbrella general workflow



4415377983508

1. Wireless controller registration with Cisco Umbrella server is a one-time process and happens over a secure HTTPS tunnel.
2. Obtain API Token for device (9800) registration from the Cisco Umbrella Dashboard.
3. Apply the Token on 9800. This registers the device to the Cisco Umbrella account. Next, create Cisco Umbrella Profile/s on 9800. Profiles are automatically pushed to the Cisco Umbrella as Identities and policy are enforced on a per-identity basis.
4. Wireless client traffic flows to the Cisco Umbrella server.
5. A wireless client sends a DNS request to 9800.
6. 9800 snoops the DNS packet and tags it with a Cisco Umbrella Profile. The profile is the identity of the packet which also resides on Cisco Umbrella.
7. This EDNS packet is redirected to the Cisco Umbrella cloud server for name resolution.
8. Cisco Umbrella then enforces a policy on it depending on the identity and applies category-based filtering rules to ensure organizational compliance.
9. Depending on the rules, it either returns a blocked page or resolved IP address to the client for the DNS request queried.

Detailed steps to configure 9800 are in the Security Configuration Guide.

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 9800 via CLI using either of these methods:
   Import from URL
   Issue the command and allow 9800 to 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:

   ```
   crypto pki trustpool import terminal
   ```

3. Enter the API token to 9800 CLI using the command:

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

Verifying the Cisco Umbrella configuration

To view the Cisco Umbrella configuration details, use this command:

```
Device# show umbrella config


Umbrella Configuration
=======================
Token: 5XXXXXXABXXXXXFXXXXXXXXXDXXXXXXXXXXXABXX
API-KEY: NONE
OrganizationID: xxxxxxx
Local Domain Regex parameter-map name: dns_bypass
DNSCrypt:Enabled
Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
UDP Timeout: 5 seconds
Resolver address:
1. 208.67.220.220
2. 208.67.222.222
3. 2620:119:53::53
4. 2620:119:35::35



ewc1#show umbrella deviceid detailed

Device registration details
1.global
     Tag : global
     Device-id : 010a2ed75e520fda
     Description : Device Id recieved successfully
     WAN interface : None



ewc1#show umbrella dnscrypt
   DNSCrypt: Enabled
   Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
   Certificate Update Status:
        Last Successfull Attempt: 10:40:58 UTC Apr 8 2020
   Certificate Details:
       Certificate Magic     : DNSC
       Major Version         : 0x0001
       Minor Version         : 0x0000
       Query Magic           : 0x7163373861576F6F
       Serial Number         : 1574811744
       Start  Time           : 1574811744 (23:42:24 UTC Nov 26 2019)
       End Time              : 1606347744 (23:42:24 UTC Nov 25 2020)
       Server Public Key     : 88B4:E44B:35E9:64B4:90BD:DABA:E825:A24B:0415:A08B:E19D:7DDB:87A3:3CD7:7E

       Client Secret Key Hash: E323:7E82:C0C2:1F0C:55AE:1473:862D:6D26:9607:B41D:3F51:F587:9482:8709:40
       Client Public key     : 8D52:4D73:CF69:4890:F130:2845:4CBE:A9CA:87AF:4CDA:FE17:C626:2F8A:1780:CD

       NM key Hash           : FAAD:4C16:6DA3:D6F3:655D:FF98:36B7:73E7:9D1C:21F5:A0E3:A083:17D7:C308:52
```

Debugging & logging

To disable DNSCrypt, use this command:

```
parameter-map type umbrella global > no dnscrypt
```

You might see this error: "Unable to import certificate using URL":

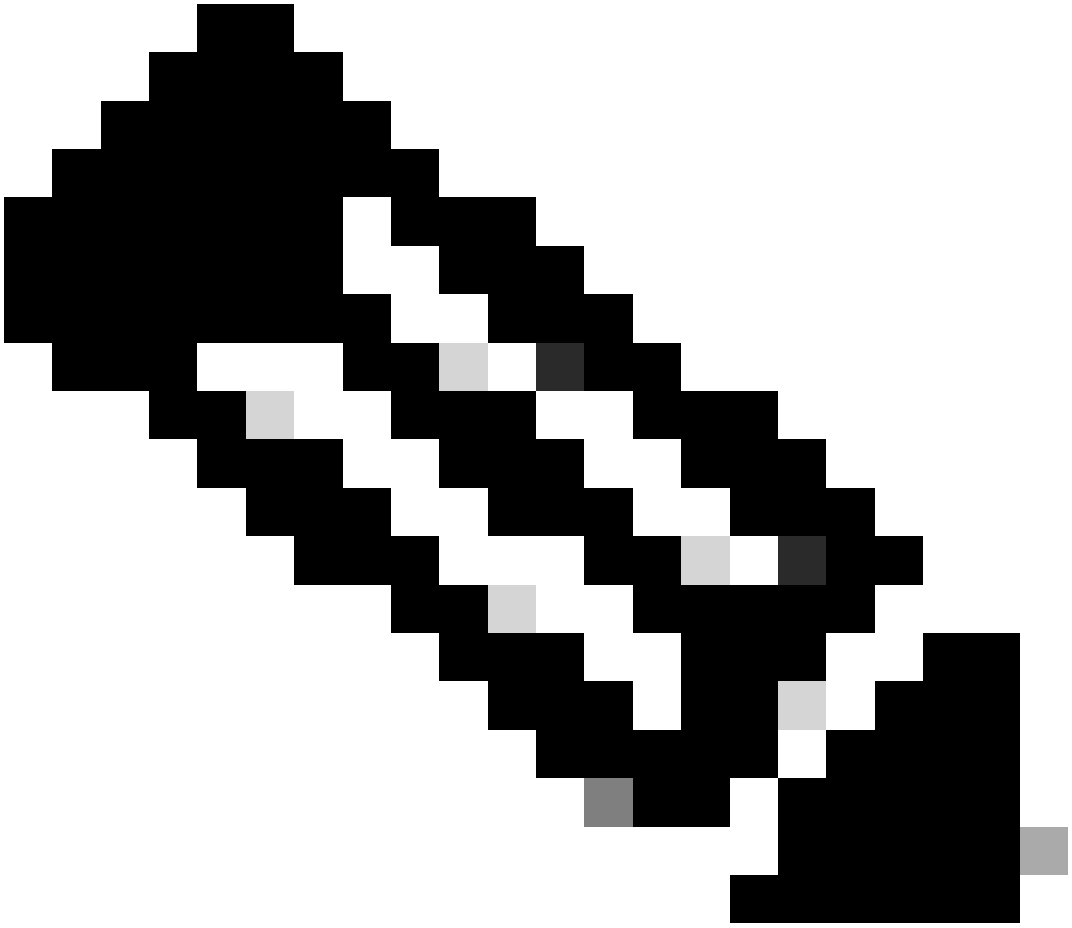
```
crypto pki trustpool import urlhttp://www.cisco.com/security/pki/trs/ios.p7b

% Error: failed to open file.

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

Workaround:

Manually copy and paste the PEM-formatted CA certificate from this location.

Next, enable device registration debug logs:

```
debug umbrella dnscrypt
debug umbrella device-registration
debug umbrella config
term monitor
```



Note: There can be instances where multiple 9800's could be assigned the same deviceId. This happens in the case of virtual 9800 (Embedded Wireless Controller (WC)).

All the virtual WC's have the same hardcoded MAC address: **"CC46D6CCCCCC".**

Debug sample from eWC A:

<#root>

```
Nov 2 19:21:18.903 Central: UMBRELLA-DEV-REG:Device registration process start: umbrella parameter-map
Nov 2 19:21:18.915 Central: UMBRELLA-DEV-REG:Socket 0 event handler: event type = WRITE EVENT
Nov 2 19:21:18.915 Central: UMBRELLA-DEV-REG:Send POST request invoked
Nov 2 19:21:18.915 Central: UMBRELLA-DEV-REG:Get registration request info invoked
Nov 2 19:21:18.915 Central: UMBRELLA-DEV-REG:Get registration request info: Found new queued request fo
Nov 2 19:21:18.915 Central: UMBRELLA-DEV-REG:Send POST request for umbrella parameter-map global (tag:
Nov 2 19:21:18.915 Central: UMBRELLA-DEV-REG:Send POST request for umbrella parameter-map global (tag:
Nov 2 19:21:18.915 Central: UMBRELLA-DEV-REG:Send POST request for umbrella parameter-map global (tag:
Nov 2 19:21:18.915 Central: UMBRELLA-DEV-REG:
Nov 2 19:21:18.915 Central: Dev reg json buffer :{"model":"B77A8731C7F4D6E92C07D7DCB68961470000A553","m
Nov 2 19:21:18.915 Central: UMBRELLA-DEV-REG:
Nov 2 19:21:18.915 Central: umbrella parameter-map name :global macAddr :cc46.d6cc.cccc
```

```
Nov 2 19:21:18.915 Central: UMBRELLA-DEV-REG:Build POST request invoked: post size = 238, size = 141
Nov 2 19:21:18.915 Central: UMBRELLA-DEV-REG:Build POST request: hostname = api.opendns.com
Nov 2 19:21:18.915 Central: UMBRELLA-DEV-REG:Build POST request: URI = /v3/networkdevices
Nov 2 19:21:18.916 Central: UMBRELLA-DEV-REG:Build POST request done
Nov 2 19:21:18.916 Central: UMBRELLA-DEV-REG:Send POST request for umbrella parameter-map global (tag:
Nov 2 19:21:18.916 Central: UMBRELLA-DEV-REG:Send POST request for umbrella parameter-map global (tag:
Host: api.opendns.com
Authorization:OpenDNS,api_key="B0E16D19C32D42EC996B635X4X9005B9",token="B77A8731C7F4D6E92C07D7DCB689614
Content-Type: application/json
Content-Length: 141

{"model":"B77A7561C7F4ABC92C07D7DCB68961470000A553","macAddress":"CC46D6CCCCCC","label":"global","tag":
---------------------------------------<OUTPUT OMITTED>---------------------------------------
Nov 2 19:21:23.553 Central: UMBRELLA-DEV-REG:Registration response: msg_part = 3, bytes = 256, resp: co
x-envoy-upstream-service-time: 1462
x-xss-protection: 1; mode=block
x-ingress-point: mil1

{"

deviceId":"010a7859d0d39393"

,"deviceKey":"B77A8731C7F4D6E92C07D7DCB68961470000A553-CC46D6CCCCCC-global","label":"global","seria
Nov 2 19:21:23.553 Central: UMBRELLA-DEV-REG:Registration response: msg_part = 4, bytes = 1
78, resp: lNumber":"9KZNYR9FPPQ","phishing":1,"createdAt":1635877282,"originId":xxxxxxxx,"
apiKey":"b0e16d19c32d42ec996b635x4x9005b9","deviceTypeId":1,"vendorId":51,"organizationId":xxxxx}
```

Debug Sample from eWC B:

<#root>

```
Nov 2 19:21:41.909 Central: UMBRELLA-DEV-REG:Device registration process start: umbrella parameter-map
Nov 2 19:21:41.919 Central: UMBRELLA-DEV-REG:Socket 0 event handler: event type = WRITE EVENT
Nov 2 19:21:41.919 Central: UMBRELLA-DEV-REG:Send POST request invoked
Nov 2 19:21:41.919 Central: UMBRELLA-DEV-REG:Get registration request info invoked
Nov 2 19:21:41.919 Central: UMBRELLA-DEV-REG:Get registration request info: Found new queued request fo
Nov 2 19:21:41.919 Central: UMBRELLA-DEV-REG:Send POST request for umbrella parameter-map global (tag:
Nov 2 19:21:41.919 Central: UMBRELLA-DEV-REG:Send POST request for umbrella parameter-map global (tag:
Nov 2 19:21:41.919 Central: UMBRELLA-DEV-REG:Send POST request for umbrella parameter-map global (tag:
Nov 2 19:21:41.919 Central: UMBRELLA-DEV-REG:
Nov 2 19:21:41.919 Central: Dev reg json buffer :{"model":"B77A7561C7F4ABC92C07D7DCB68961470000A553","ma
Nov 2 19:21:41.919 Central: UMBRELLA-DEV-REG:
Nov 2 19:21:41.919 Central: umbrella parameter-map name :global macAddr :cc46.d6cc.cccc
Nov 2 19:21:41.919 Central: UMBRELLA-DEV-REG:Build POST request invoked: post size = 238, size = 141
Nov 2 19:21:41.919 Central: UMBRELLA-DEV-REG:Build POST request: hostname = api.opendns.com
Nov 2 19:21:41.919 Central: UMBRELLA-DEV-REG:Build POST request: URI = /v3/networkdevices
Nov 2 19:21:41.919 Central: UMBRELLA-DEV-REG:Build POST request done
Nov 2 19:21:41.919 Central: UMBRELLA-DEV-REG:Send POST request for umbrella parameter-map global (tag:
Nov 2 19:21:41.919 Central: UMBRELLA-DEV-REG:Send POST request for umbrella parameter-map global (tag:
Host: api.opendns.com
Authorization:OpenDNS,api_key="B0E16D19C32D42EC996B635X4X9005B9",token="B77A8731C7F4D6E92C07D7DCB689614
Content-Type: application/json
Content-Length: 141

{"model":"B77A8731C7F4D6E92C07D7DCB68961470000A553","macAddress":"CC46D6CCCCCC","label":"global","tag":
---------------------------------------<OUTPUT OMITTED>---------------------------------------
Nov 2 19:21:41.919 Central: UMBRELLA-DEV-REG:Registration response: msg_part = 3, bytes = 256, resp: co
x-envoy-upstream-service-time: 1462
x-xss-protection: 1; mode=block
```

```
x-ingress-point: mil1

{"

deviceId":"010a7859d0d39393"

,"deviceKey":"B77A8731C7F4D6E92C07D7DCB68961470000A553-CC46D6CCCCCC-global","label":"global","serialNum
Nov 2 19:21:41.919 Central: UMBRELLA-DEV-REG:Registration response: msg_part = 4, bytes = 1
78, resp: lNumber":"9KZNYR9FPPQ","phishing":1,"createdAt":1635877282,"originId":573529511,"
apiKey":"b0e16d19c32d42ec996b635x4x9005b9","deviceTypeId":1,"vendorId":51,"organizationId":xxxxx}
```

Here, the POST request contains API token (legacy device API token from the Cisco Umbrella Dashboard), API key, model number (same as API token), MAC address of the wireless LAN controller (WLC), name of the parameter map (tag), and the device serial number.

The Device ID is generated using the API token, API key, tag, and MAC address. Since both of these 9800's have the same values for the above, the same Device ID is assigned to both of them.

This is an expected behavior. To fix this issue, you must create a custom `parameter-map` on one or both of the 9800's;

```
parameter-map type umbrella <custom name>
```

By creating a custom `parameter-map "cpm"`, we are creating a new tag which results in a different Device ID (`deviceId`).

```
<#root>

{

"deviceId":"010a30f6275c92ce"

,"deviceKey":"0DCDA24CDD6A92D714FE357539FDCAE80051BA0A-DD46D6BBCCCC-global","label":"global","serialNum

{

"deviceId":"010a341b037ea6b9"

,"deviceKey":"0DCDA24CDD6A92D714FE357539FDCAE80051BA0A-DD46D6BBCCCC-cpm","label":"global","serialNumber
```