Cisco Umbrella Integration

Prerequisites for Cisco Umbrella Integration

- Cisco Umbrella subscription license must be available. Go to https://umbrella.cisco.com/products/umbrella-enterprise-security-packages and click **Request a quote** to get the license.
- The device must be set as the default Domain Name System (DNS) server gateway and the domain name server traffic should go through the Cisco device.
- Communication for device registration to the Umbrella server is through HTTPS. This requires a root certificate to be installed on the device. You can download the certificate using this link: https://www.digicert.com/CACerts/DigiCertSHA2SecureServerCA.crt.
- The Cisco Industrial Ethernet switch runs the Cisco IOS XE release 17.2.1 software image or later.
- The Cisco Industrial Ethernet switch must have a DNA Advantage or higher license to enable Umbrella.

The following network requirements must be met:

- The device must be set as the default DNS server gateway and ensure that the Domain Name Server (DNS)traffic goes through the Cisco Industrial Ethernet switch.
- Communication for device registration to the Cisco Umbrella server is via HTTPS. This requires a root certificate to be installed on the router. To download this certificate directly from a link instead of pasting it in, you can find the certificate here:

  https://www.digicert.com/CACerts/DigiCertSHA2SecureServerCA.crt
- For initial registration, the interface configured as “umbrella out” must be able to access api.opendns.com over port 443 in order to complete initial registration.

Restrictions for Cisco Umbrella Integration

- Cisco Umbrella Integration does not work in the following scenarios:
  - If an application or host uses IP address instead of DNS to query domain names.
  - If a client is connected to a web proxy and does not send DNS query to resolve the server address.
  - If DNS queries are generated by a Cisco switching device.
  - If DNS queries are sent over TCP.
  - If DNS queries have record types other than address mapping and text.
- DNSv6 queries are not supported.
- DNS64 and DNS46 extensions are not supported.
- Extended DNS conveys only the IPv4 address of the host, and not the IPv6 address.
- Umbrella configurations on port-channel is not supported
- Umbrella may be configured to use 10G uplink ports as OUT only.
- No dscp markings are entertained for DNS traffic going via Umbrella interfaces. This is applicable to all punted traffic on Umbrella interfaces.
- For umbrella Interfaces, all egress ACL/s rules wouldn’t take affect for DNS traffic. This applies to CPU injected traffic for DNS.
- DNS packet fragmentation is not supported.
- QinQ and Security Group Tag (SGT) packets are not supported.
- When the Cisco Umbrella Integration policy blocks a DNS query, the client is redirected to a Cisco Umbrella block page. HTTPS servers provide these block pages and the IP address range of these block pages is defined by the Cisco Umbrella portal.
- User authentication and identity is not currently supported.
- Umbrella Connector maintains a list of IP address that is known for malicious traffic. When the Cisco Umbrella roaming client detects the destination of packets to those addresses, it forwards those addresses to Cisco Umbrella cloud for further inspection.
- Currently, there is no direct cloud access support.
- Updated resolver IPs do not take effect, DNS traffic is redirected to Cisco Umbrella cloud irrespective of user-configured resolver IPs.
- Network Address Translation (NAT) is not supported on interfaces that has Cisco Umbrella enabled on it.

Information About Cisco Umbrella Integration

The following sections provide details about the Cisco Umbrella Integration feature.

Benefits of Cisco Umbrella Integration

Cisco Umbrella Integration provides security and policy enforcement at the DNS level. It enables the administrator to split the DNS traffic and directly send some of the DNS traffic to a specific DNS server that is located within the enterprise network. This helps the administrator to bypass the Cisco Umbrella Integration.

Cloud-Based Security Service Using Cisco Umbrella Integration

The Cisco Umbrella Integration feature provides cloud-based security service by inspecting the DNS query that is sent to the DNS server through a Cisco device. When a host initiates the traffic and sends a DNS query, the Cisco Umbrella Connector in the device intercepts and inspects the DNS query. The Umbrella Connector is a component in the Cisco device that intercepts DNS traffic and redirects it to the Cisco Umbrella cloud for security inspection and policy application. The Umbrella cloud is a cloud-based security service that inspects the queries received from Umbrella Connectors, and based on the Fully Qualified Domain Name (FQDN), determines if the content provider IP addresses should be provided or not in the response.

If the DNS query is for a local domain, the query is forwarded without changing the DNS packet to the DNS server in the enterprise network. The Cisco Umbrella Resolver inspects the DNS queries that are sent from an external domain. An extended DNS record that includes the device identifier information, organization ID, and client IP address is added to the query and sent to the Umbrella Resolver. Based on all this information, the Umbrella Cloud applies different policies to the DNS query.

The Umbrella Integration cloud might take one of the following actions based on the policies configured on the portal and the reputation of the DNS FQDN:

- Blacklist action: If the FQDN is found to be malicious or blocked by the customized enterprise security policy, the IP address of the Umbrella Cloud's blocked landing page is returned in the DNS response.
- Whitelist action: If the FQDN is found to be nonmalicious, the IP address of the content provider is returned in the DNS response.
- Greylist action: If the FQDN is found to be suspicious, the intelligent proxy unicast IP addresses are returned in the DNS response.

When the DNS response is received, the device forwards the response back to the host. The host extracts the IP address from the response, and sends the HTTP or HTTPS requests to this IP address.

Handling of Traffic by Cisco Umbrella Cloud

With the aid of the Cisco Umbrella Integration feature, HTTP and HTTPs client requests are handled in the following ways:

- If the FQDN in the DNS query is malicious (falls under blacklisted domains), the Umbrella Cloud returns the IP address of the blocked landing page in the DNS response. When the HTTP client sends a request to this IP address, the Umbrella Cloud displays a page that informs the user that the requested page was blocked and the reason for the blocking.
- If the FQDN in the DNS query is nonmalicious (falls under whitelisted domains), the Umbrella Cloud returns the IP address of the content provider. The HTTP client sends the request to this IP address and gets the requested content.
- If the FQDN in the DNS query falls under greylisted domains, the Umbrella DNS resolver returns the unicast IP addresses of the intelligent proxy in the DNS response. All the HTTP traffic from the host to

the grey domain gets proxied through the intelligent proxy and undergoes Uniform Resource Locator (URL) filtering.

Note One potential limitation in using an intelligent proxy unicast IP addresses is the probability of the datacenter going down when a client tries to send the traffic to the intelligent proxy unicast IP address. In this scenario, the client has completed DNS resolution for a domain that falls under the grey-listed domain, and the client's HTTP or HTTPS traffic is sent to one of the obtained intelligent proxy unicast IP addresses. If that datacenter is down, the client has no way of knowing about it.

The Umbrella Connector does not act on the HTTP and HTTPS traffic. The Connector does not redirect any web traffic or alter any HTTP or HTTPS packets.

DNS Packet Encyrption

DNS packets sent from a Cisco device to the Cisco Umbrella Integration server must be encrypted if the extended DNS information in the packet contains information such as user IDs, internal network IP addresses, and so on. When the DNS response is sent back from the DNS server, the device decrypts the packet and forwards it to the host.

Note

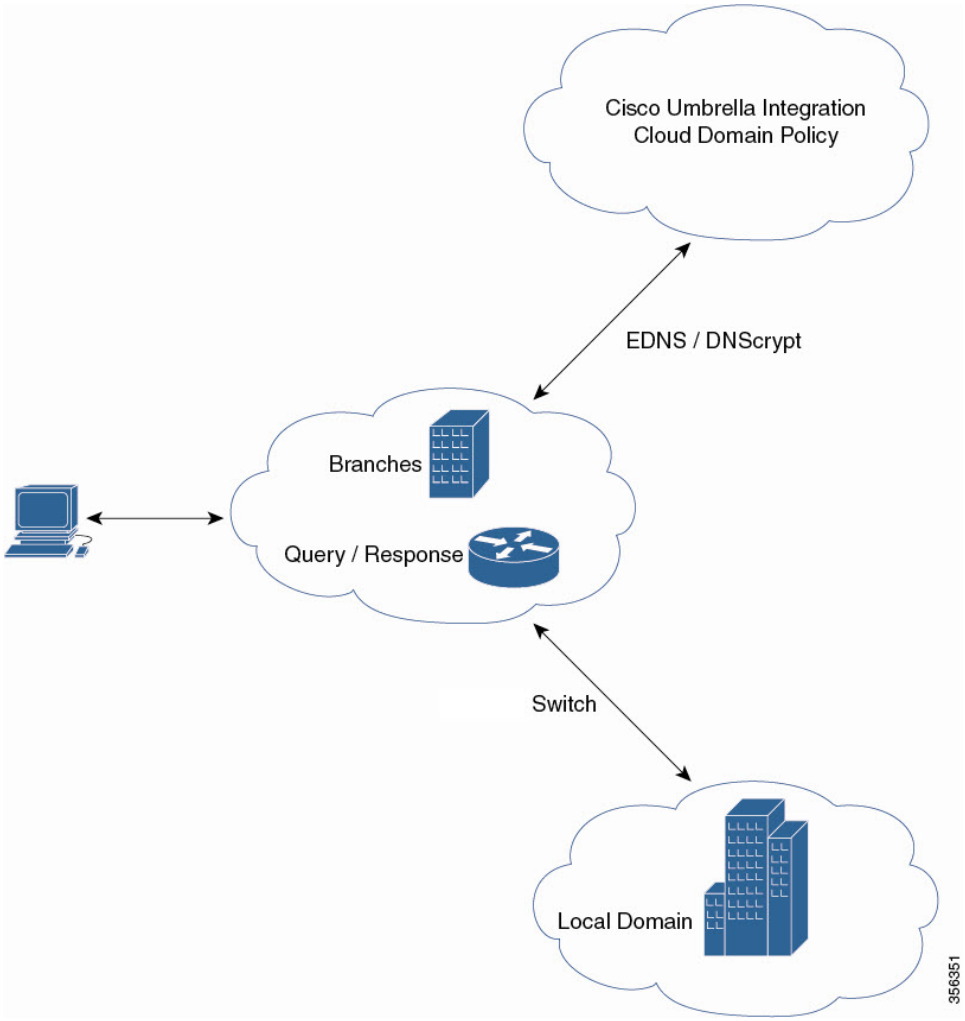
- You can encrypt DNS packets only when the DNScrypt feature is enabled on the Cisco device.
- The IP address of the client is exported to Umbrella Cloud for tracking statistics. We recommend that you do not disable DNScrypt, as the IP would then be sent out unencrypted.

Cisco devices use the following Anycast recursive Cisco Umbrella Integration servers:

- 208.67.222.222
- 208.67.220.220
- 2620:119:53::53
- 2620:119:35::35

The following figure displays the Cisco Umbrella Integration topology.

Figure 1: Cisco Umbrella Integration Topology



DNSCrypt and Public Key

The following subsections provide detailed information about DNScrypt and Public Key.

DNSCrypt

DNSCrypt is an encryption protocol to authenticate communications between a Cisco device and the Cisco Umbrella Integration feature. When the **parameter-map type umbrella** command is configured and the **umbrella out** command is enabled on a WAN interface, DNSCrypt gets triggered, and a certificate is downloaded, validated, and parsed. A shared secret key, which is used to encrypt DNS queries, is then negotiated. For every hour that this certificate is automatically downloaded and verified for an upgrade, a new shared secret key is negotiated to encrypt DNS queries.

When DNSCrypt is used, a DNS request packet's size is more than 512 bytes. Ensure that these packets are allowed through the intermediary devices. Otherwise, the response might not reach the intended recipients.

Public Key

Public key is used to download the DNSCrypt certificate from Umbrella Cloud. This value is preconfigured to B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79, which is the public key of the Cisco Umbrella Integration Anycast servers. If there is a change in the public key, and if you modify the **public-key** command, you have to remove the modified command to restore the default value.

⚠

Caution If you modify the value, the DNSCrypt certificate download might fail.

The **parameter-map type umbrella global** command configures a parameter-map type in umbrella mode. When you configure a device using this command, the DNSCrypt and public key values are autopopulated.

We recommend that you change the **parameter-map type umbrella global** parameters only when you perform certain tests in the lab. If you modify these parameters, it can affect the normal functioning of the device.

How to Configure Cisco Umbrella Integration

The following sections provide information about the various tasks that comprise Cisco Umbrella integration.

Configuring the Umbrella Connector

Before you begin

Get the application programming interface (API) token from the Cisco Umbrella registration server.

Have the root certificate establish the HTTPS connection with the Cisco Umbrella registration server. Import the root certificate of DigiCert into the device using the **crypto pki trustpool import terminal** command in global configuration mode.

There are two methods of importing the certificate.

1. Importing from a URL
2. Importing directly in a Terminal

To Import from a URL, Issue the command and allow Industrial Ethernet switch to fetch the cert:

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

To import from a terminal, perform the following:

The following is the root certificate of DigiCert:

```
-----BEGIN CERTIFICATE-----
MIIElDCCA3ygAwIBAgIQAf2j627KdciIQ4tyS8+8kTANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0xMzAzMDgxMjAwMDBaFw0yMzAzMDgxMjAwMDBaME0xCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxJzAlBgNVBAMTHkRpZ2lDZXJ0IFNIQTIg
U2VjdXJlIFNlcnZlciBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ANyuWJBNwcQwFZA1W248ghX1LFy949v/cUP6ZCWA1O4Yok3wZtAKc24RmDYXZK83
nf36QYSvx6+M/hpzTc8zl5CilodTgyu5pnVILR1WN3vaMTIa16yrBvSqXUu3R0bd
KpPDkC55gIDvEwRqFDu1m5K+wgdlTvza/P96rtxcflUxDOg5B6TXvi/TC2rSsd9f
```

```
/ld0Uzs1gN2ujkSYs58O09rg1/RrKatEp0tYhG2SS4HD2nOLEpdIkARFdRrdNzGX
kujNVA075ME/OV4uuPNcfhCOhkEAjUVmR7ChZc6gqikJTvOX6+guqw9ypzAO+sf0
/RR3w6RbKFfCs/mC/bdFWJsCAwEAAaOCAVowggFWMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDgYDVR0PAQH/BAQDAgGGMDQGCCsGAQUFBwEBBCgwJjAkBggrBgEFBQcwAYYY
aHR0cDovL29jc3AuZGlnaWNlcnQuY29tMHsGA1UdHwR0MHIwN6A1oDOGMWh0dHA6
Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwwN6A1
oDOGMWh0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RD
QS5jcmwwPQYDVR0gBDYwNDAyBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8v
d3d3LmRpZ2ljZXJ0LmNvbS9DUFMwHQYDVR0OBBYEFA+AYRyCMWHVLyjnjUY4tCzh
xtniMB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA0GCSqGSIb3DQEB
CwUAA4IBAQAjPt9L0jFCpbZ+QlwaRMxp0Wi0XUvgBCFsS+JtzLHgl4+mUwnNqipl
5TlPHoOlblyYoiQm5vuh7ZPHLgLGTUq/sELfeNqzqPlt/yGFUzZgTHbO7Djc1lGA
8MXW5dRNJ2Srm8c+cftIl7gzbckTB+6WohsYFfZcTEDts8Ls/3HB40f/1LkAtDdC
2iDJ6m6K7hQGrn2iWZiIqBtvLfTyyRRfJs8sjX7tN8Cp1Tm5gr8ZDOo0rwAhaPit
c+LJMto4JQtV05od8GiG7S5BNO98pVAdvzr508EIDObtHopYJeS4d60tbvVS3bR0
j6tJLp07kzQoH3jOlOrHvdPJbRzeXDLz
-----END CERTIFICATE-----
```

Verify that the privacy-enhanced mail (PEM) import is successful. A confirmation message is displayed after importing the certificate.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type umbrella global**
4. **dnscrypt**
5. **token** *value*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**parameter-map type umbrella global** **Example:** `Device(config)# parameter-map type umbrella global`	Configures the parameter map type as umbrella mode, and enters parameter-map type inspect configuration mode.
Step 4	**dnscrypt** **Example:**	Enables DNS packet encryption on the device.

	Command or Action	Purpose
	`Device(config-profile)# dnscrypt`	
Step 5	**token** *value* **Example:** `Device(config-profile)# token AABBA59A0BDE1485C912AFE472952641001EEECC`	Specifies the API token issued by the Cisco Umbrella registration server.
Step 6	**end** **Example:** `Device(config-profile)# end`	Exits parameter-map type inspect configuration mode and returns to privileged EXEC mode.

Registering the Cisco Umbrella Tag

Before you begin

- Configure the Umbrella Connector.
- Configure the **umbrella out** command before configuring the **umbrella in** command. Registration is successful only when port 443 is in Open state and allows the traffic to pass through the existing firewall.
- After you configure the **umbrella in** command with a tag, the device initiates the registration process by resolving api.opendns.com. Configure a name server by using the **ip name-server** command, and a domain lookup by using the **ip domain-lookup** command configured on the device to successfully resolve the FQDN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **umbrella out**
5. **exit**
6. **interface** *interface-type interface-number*
7. **umbrella in** *tag-name*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-type interface-number* **Example:** `Device(config)# interface gigabitEthernet 1/1`	Specifies the WAN interface, and enters interface configuration mode.
Step 4	**umbrella out** **Example:** `Device(config-if)# umbrella out`	Configures Umbrella Connector on the interface to connect to the Umbrella Cloud servers.
Step 5	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode, and enters global configuration mode.
Step 6	**interface** *interface-type interface-number* **Example:** `Device(config)# interface gigabitEthernet 1/2`	Specifies the LAN interface, and enters interface configuration mode.
Step 7	**umbrella in** *tag-name* **Example:** `Device(config-if)# umbrella in mydevice_tag`	Configures the Umbrella Connector on the interface that is connected to the client. • The length of the Umbrella tag should not exceed 49 characters. • After you configure the **umbrella in** command with a tag, the device registers the tag to the Cisco Umbrella Integration server.
Step 8	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring a Cisco Device as a Pass-through Server

You can identify the traffic that is to be bypassed by using domain names. You can define these domains in the form of regular expressions on a Cisco device. If the DNS query that is intercepted by the device matches one of the configured regular expressions, the query is bypassed to the specified DNS server without being redirected to the Umbrella Cloud.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type regex** *parameter-map-name*
4. **pattern** *expression*
5. **exit**
6. **parameter-map type umbrella global**
7. **token** *value*
8. **local-domain** *regex_param_map_name*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**parameter-map type regex** *parameter-map-name* **Example:** `Device(config)# parameter-map type regex dns_bypass`	Configures a parameter-map type to match the specified traffic pattern, and enters parameter-map type inspect configuration mode.

Step 4	**pattern** *expression*
	Example:
	`Device(config-profile)# pattern www.cisco.com`
	`Device(config-profile)# pattern .*example.cisco.*`
		Configures a local domain or URL that is used to bypass the Umbrella Cloud.

Step 5	**exit** **Example:**	Exits parameter-map type inspect configuration mode and enters global configuration mode.

	Command or Action	Purpose
	`Device(config-profile)# exit`	
Step 6	**parameter-map type umbrella global** **Example:** `Device(config)# parameter-map type umbrella global`	Configures the parameter map type as umbrella mode, and enters parameter-map type inspect configuration mode.
Step 7	**token** *value* **Example:** `Device(config-profile)# token AADDD5FF6E510B28921A20C9B98EEEFF`	Specifies the API token issued by the Cisco Umbrella registration server.
Step 8	**local-domain** *regex_param_map_name* **Example:** `Device(config-profile)# local-domain dns_bypass`	Attaches the regular expression parameter map with the Umbrella global configuration.
Step 9	**end** **Example:** `Device(config-profile)# end`	Exits parameter-map type inspect configuration mode and returns to privileged EXEC mode.

Verifying the Cisco Umbrella Integration Configuration

Use the following commands in any order to view the Cisco Umbrella Integration configuration.

The following example shows a sample output of the **show umbrella config** command:

```
Device# show umbrella config
Umbrella Configuration
=======================
Token: EB74330C50767B6A63770EA6C3408DCF00282D8E
API-KEY: NONE
OrganizationID: 2633102
Local Domain Regex parameter-map name: NONE
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
Umbrella Interface Config:
Number of interfaces with "umbrella out" config: 1
1. GigabitEthernet1/4
Mode : OUT
```

```
VRF : global(Id: 0)
Number of interfaces with "umbrella in" config: 2
1. GigabitEthernet1/9
Mode : IN
DCA : Disabled
Tag : IE_uniquetag
Device-id : 010a424c1597fe09
VRF : global(Id: 0)
2. GigabitEthernet2/3
Mode : IN
DCA : Disabled
Tag : IE_tag_2
Device-id : 010adaf012a36ad6
VRF : global(Id: 0)
Configured Umbrella Parameter-maps:
1. global
```

The following example shows a sample output of the **show umbrella deviceid** command:

```
Device# show umbrella deviceid

Device registration details
Interface Name Tag Status Device-id
GigabitEthernet1/9 IE_uniquetag 200 SUCCESS 010a424c1597fe09
GigabitEthernet2/3 IE_tag_2 200 SUCCESS 010adaf012a36ad6
```

The following example shows a sample output of the **show umbrella dnscrypt** command:

```
Device#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: 20:01:18 IST Dec 17 2019
Certificate Details:
Certificate Magic : DNSC
Major Version : 0x0001
Minor Version : 0x0000
Query Magic : 0x7163373861576F6F
Serial Number : 1574811744
Start Time : 1574811744 (05:12:24 IST Nov 27 2019)
End Time : 1606347744 (05:12:24 IST Nov 26 2020)
Server Public Key :
88B4:E44B:35E9:64B4:90BD:DABA:E825:A24B:0415:A08B:E19D:7DDB:87A3:3CD7:7EDF:8E2F
Client Secret Key Hash:
0FB9:520E:5228:FB2C:D521:1E9E:2ACB:AC3D:B520:A795:F54C:C608:604B:A410:17F1:1284
Client Public key :
E42F:507E:F052:72DD:1BC8:4857:2AE0:2F9F:ED87:1687:AAE4:095D:D933:48F0:5D60:3662
NM key Hash : EDC3:25DD:4D21:103E:7E49:1EFA:75ED:4D6F:A450:107D:C6E8:1C41:9CF7:4039:FA89:2CED
```

The following example shows a sample output of the **show umbrella deviceid detailed** command:

```
Device# show umbrella deviceid detailed

Device registration details
1.GigabitEthernet1/9
Tag : IE_uniquetag
Device-id : 010a424c1597fe09
Description : Device Id recieved successfully
WAN interface : GigabitEthernet1/4
WAN VRF used : global(Id: 0)
2.GigabitEthernet2/3
Tag : IE_tag_2
```

```
Device-id : 010adaf012a36ad6
Description : Device Id recieved successfully
WAN interface : GigabitEthernet1/4
WAN VRF used : global(Id: 0)
```

The following is a sample output of the **show platform software dns-umbrella statistics** command. The command output displays traffic-related information such as the number of queries sent, number of responses received, and so on.

```
Device# show platform software dns-umbrella statistics

=======================================
Umbrella Statistics
=======================================
Total Packets : 7848
DNSCrypt queries : 3940
DNSCrypt responses : 0
DNS queries : 0
DNS bypassed queries(Regex) : 0
DNS responses(Umbrella) : 0
DNS responses(Other) : 3906
Aged queries : 34
Dropped pkts : 0
```

Troubleshooting Cisco Umbrella Integration

You can troubleshoot issues related to the Cisco Umbrella Integration feature configuration by using the following commands.

Table 1: debug Commands for Cisco Umbrella Integration Feature

Command	Purpose
debug umbrella config	Enables Umbrella configuration debugging.
debug umbrella device-registration	Enables Umbrella device registration debugging.
debug umbrella dnscrypt	Enables Umbrella DNSCrypt encryption debugging.

From the command prompt of a Windows machine, or the terminal window or shell of a Linux machine, run the **nslookup -type=txt debug.opendns.com** command. The IP address that you specify with the **nslookup -type=txt debug.opendns.com** command must be the IP address of the DNS server.

```
nslookup -type=txt debug.opendns.com 10.0.0.1
Server: 10.0.0.1
Address: 10.0.0.1#53
Non-authoritative answer:
debug.opendns.com text = "server r6.xx"
debug.opendns.com text = "device 010A826AAABB6C3D"
debug.opendns.com text = "organization id 1892929"
debug.opendns.com text = "remoteip 10.0.1.1"
debug.opendns.com text = "flags 436 0 6040 39FF000000000000000"
debug.opendns.com text = "originid 119211936"
debug.opendns.com text = "orgid 1892929"
debug.opendns.com text = "orgflags 3"
debug.opendns.com text = "actype 0"
debug.opendns.com text = "bundle 365396"
```

```
debug.opendns.com text = "source 10.1.1.1:36914"
debug.opendns.com text = "dnscrypt enabled (713156774457306E)"
```

Feature Information for Cisco Umbrella Integration

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 2: Feature Information for Cisco Umbrella Integration

Feature Name	Releases	Feature Information
Cisco Umbrella Integration	Cisco IOS XE Amsterdam 17.2.1	The Cisco Umbrella Integration feature enables cloud-based security service by inspecting the DNS query that is sent to any DNS server through Cisco devices. The security administrator configures policies on the Cisco Umbrella Cloud to either allow or deny traffic towards the FQDN.