Cisco Start™
SIMPLE SMART SECURE

Cisco Umbrella Branch

Easy Setup Guide

Free Trial: You have 13 days left.

Overview

Message Center

IMPORTANT CHANGES TO FIREWALL RULES FOR ROAMING CLIENT USERS

As part of an upgrade to capabilities for roaming clients, a new domain for the Umbrella roaming client syncing to Umbrella has been created. Action is required to ensure this domain (sync.hydra.opendns.com) is permitted in your firewall. Read more:

Malware: 1 request in the last 24 hours (View Details)

Botnet: 0 requests in the last 24 hours (View Details)

You can easily set up the Cisco Umbrella Branch on your Cisco ISR 4000 Series in this step-by-step guide.

1 Prerequisites

Before you configure the Cisco Umbrella Branch feature on the Cisco ISR 4000 Series, ensure that you have the following:

- **Cisco Umbrella Branch License**
- **Security K9 License**
- **ROM Monitor (ROMMON) Version 16.2(1r) or Later**: You can upgrade from any ROMMON version to release 16.2(1r). For more information, see "3 Appendix".
- **Cisco IOS XE Denali 16.3 or Later**
- **Default DNS Server Gateway Configured on Cisco ISR 4000 Series**: Ensure that the DNS traffic goes through Cisco ISR 4000 Series.
- **Name Server (*ip name-server x.x.x.x*) and Domain Lookup (*ip domain-lookup*) Configured on Cisco ISR 4000 Series**: To successfully resolve the FQDN and register the tag to the Cisco Umbrella Branch portal.
- **Certificate Authority (CA) for Cisco Umbrella Branch Registration**: Certificate must be manually imported to Cisco ISR 4000 Series. You can send an email to the administrator to request the certificate for your device. Provide the following details in the email:
  - Customer Name
  - Cisco ISR 4000 Series Model Name
  - Geographical Location of Cisco ISR 4000 Series
  - Cisco Service Delivery Manager Contact (if known)

Umbrella Branch Licenses SKU	Description
UMB-BRAN-4321	Umbrella Branch License for Cisco ISR 4321
UMB-BRAN-4331	Umbrella Branch License for Cisco ISR 4331
UMB-BRAN-4351	Umbrella Branch License for Cisco ISR 4351
UMB-BRAN-4431	Umbrella Branch License for Cisco ISR 4431
UMB-BRAN-4451	Umbrella Branch License for Cisco ISR 4451

2 Configuring Umbrella Branch

This guide outlines how to configure the Cisco ISR 4000 Series to register with the Cisco Umbrella Dashboard as a **Network Device** and enforce policy based on **Device ID** as well as **Tags**.

The process of registration is fairly straightforward. In order to authenticate the ISR to the Umbrella dashboard, the **API Token** must be obtained from your Umbrella dashboard and installed on the ISR.

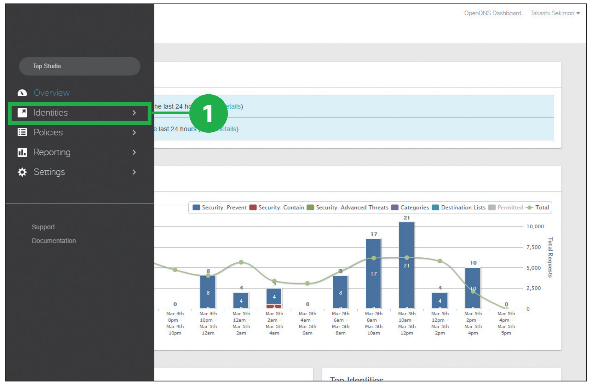
Then you simply log into the device's command interface and follow the steps below to configure your ISR. Once completed, the ISR will register as a device in your Umbrella dashboard and a policy can then be defined for the ISR or any additional tags.

To configure Umbrella Branch on your ISR, perform these steps.

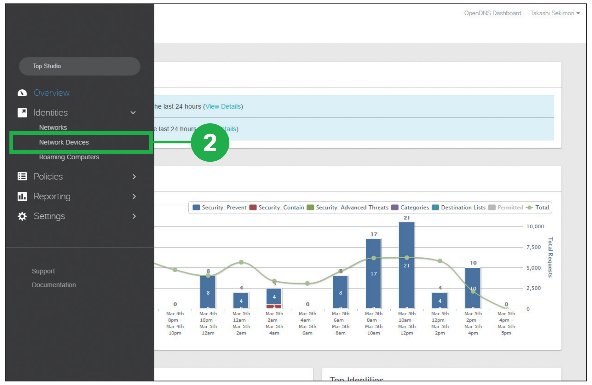
- Obtaining API Token
- Importing CA and adding API token
- Registering Umbrella Branch Tag

2-1 Obtaining API Token

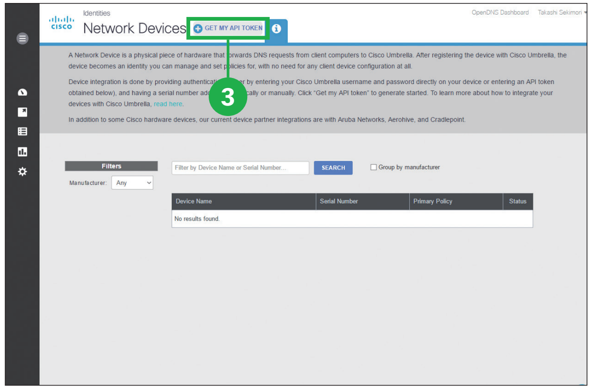
You need to get your Network Device API Token from your Umbrella dashboard.



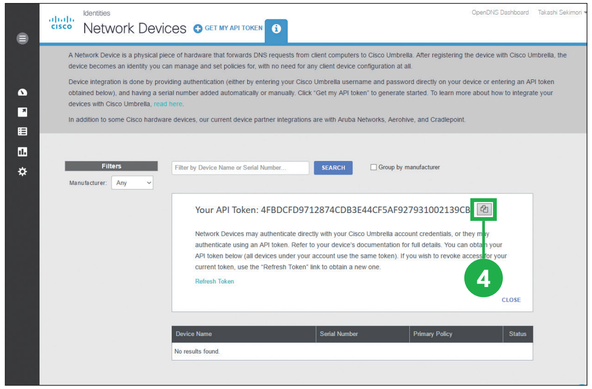
1 Click [Identities].



2 Click [Network Devices].



3 Click [GET MY API TOKEN].



A Network Device is a physical piece of hardware that forwards DNS requests from client computers to Cisco Umbrella. After registering the device with Cisco Umbrella, the device becomes an identity you can manage and set policies for, with no need for any client device configuration at all.

Device integration is done by providing authentication (either by entering your Cisco Umbrella username and password directly on your device or entering an API token obtained below), and having a serial number added automatically or manually. Click “Get my API token” to generate started. To learn more about how to integrate your devices with Cisco Umbrella, read here.

In addition to some Cisco hardware devices, our current device partner integrations are with Aruba Networks, Aerohive, and Cradlepoint.

Filter by Device Name or Serial Number...

□ Group by manufacturer

Your API Token: 4FBDCFD9712874CDB3E44CF5AF927931002139CB

Network Devices may authenticate directly with your Cisco Umbrella account credentials, or they may authenticate using an API token. Refer to your device’s documentation for full details. You can obtain your API token below (all devices under your account use the same token). If you wish to revoke access for your current token, use the “Refresh Token” link to obtain a new one.

Refresh Token

Device Name	Serial Number	Primary Policy	Status
No results found.			

4 Click the file icon [⧉].

Copy the API token to your clipboard or to a text file so that you can complete the next steps.

2-2 Importing CA and adding API token

Communication for device registration to the Umbrella server is via HTTPS. This requires a root certificate to be installed on the ISR.
Run the following commands on your ISR:

```
enable
configure terminal
```

1 Enter the *configure terminal (conf t)* command.

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

2 Enter the *crypto pki trustpool import* command.

Simply import the cert directly from Cisco.

```
% PEM files import succeeded.
```

3 Verify that the PEM import is successful.

You should receive a message after importing the certificate.

Next, while still in Configure Terminal mode, add the API token to the ISR by running the following commands:

```
parameter-map type opendns global
token <API TOKEN>
```

4 Substitute the *<API TOKEN>* variable with your token (copied at the step 2-1 4).

This is the sample configuration:

```
enable
configure terminal
parameter-map type opendns global
 token AABBA59A0BDE1485C912AFE472952641001EEECC
 local-domain dns_bypass
 udp-timeout 25 (The range is from 1 to 30 seconds).
 dnscrypt
 public-key key (Key should contain only hexadecimal digit).
 resolver ipv4 10.1.1.2
exit
```

2-3 Registering Umbrella Branch Tag

A tag is essentially another network that is behind the ISR that can be registered alone and given its own Device ID in the Umbrella dashboard. This can be a VLAN or a physical interface. Each tag will use the same API Token, so minimal extra configuration is needed to register a newly tagged interface. Tags are not unique, but the combination of Model + MAC Address + Tag is unique within an organization.
To register the Umbrella Branch tag, perform these steps:

1 **Configure the OpenDNS Out on the WAN interface.**

```
interface gigabitEthernet 0/0/0
 opendns out
```

Caution

Configure the OpenDNS Out command **before** you configure OpenDNS In command. Registration will be successful only when port 443 is in an open state and allows the traffic to pass through the existing firewall.

2 **Configure the OpenDNS In on the LAN interface.**

```
interface gigabitEthernet 0/0/1
 opendns in mydevice_tag
```

After configuring the OpenDNS In with a tag using the ***opendns in mydevice_tag*** command, the ISR will register the tag to the Umbrella Branch portal and initiate the registration process by resolving api.opendns.com.

MEMO

For Cisco ISR 4000 Series, the length of the hostname and OpenDNS tag should not exceed 49 characters.

Caution

You need to have a name server (***ip name-server x.x.x.x***) and domain lookup (***ip domain-lookup***) configured on your ISR to successfully resolve the FQDN.

2-4 Configuring ISR as a Pass-Through Server

Optionally, you can identify the traffic to be bypassed using domain names. In the ISR, you can define these domains in the form of a regular expression. If the DNS query that is intercepted by the ISR matches one of the configured regular expressions, then the query is bypassed to the specified DNS server without redirecting to the Umbrella Branch cloud.
This sample configuration shows how to define a regex parameter-map with a desired domain name and regular expressions:

```
Device# configure terminal
Device(config)# parameter-map type regex dns_bypass
Device(config)# pattern www.fisco.com
Device(config)# pattern .*engineering.fisco.*

_Attach the regex param-map with the OpenDNs global configuration as shown below:_

Device(config)# parameter-map type openness global
Device(config-profile)# token AADDD5FF6E510B28921A20C9B98EEEFF
Device(config-profile)# local-domain dns_bypass
```

2-5 Verifying Umbrella Branch Configuration

You can verify the Umbrella Branch configuration using the following commands:

Router# ***show opendns config***

Output example:

```
Open DNS Configuration
=========================
  Token: AAAAAD288BA440D10E207350339F497A001CCBBB
  Local Domain Regex parameter-map name: NONE
  DNSCrypt: Not enabled
  Public-key: NONE
  Timeout: NONE
  Resolver address: NONE
Open DNS Interface Config:
     Number of interfaces with “opendns out” config: 1
       1. GigabitEthernet0/0/1
          Mode     :  OUT
     Number of interfaces with “opendns in” config: 1
       1. GigabitEthernet0/0/0
          Mode     : IN
          Tag      : test1
          Device-id: ...Pending...
```

Device# ***show opendns deviceid***

Output example:

```
Device registration details

Interface Name          Tag             Status          Device Id
GigabitEthernet0/0/0    test1           REQ QUEUED      -
GigabitEthernet0/0/0.1  test498         200 SUCCES      010af8cde579a997
GigabitEthernet0/0/0.2  utah-win-intf   200 SUCCES      010a0a25d20088b8
GigabitEthernet0/0/0.3  utah-win-intf   200 SUCCES      010a0a25d20088b8
GigabitEthernet0/0/0.4  mydevice_tag    REQ QUEUED      -
```

Device# ***show opendns dnscrypt***

Output example:

```
DNSCrypt: Enabled
Public-key:   B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:-
CA43:FB79
Certificate Update Status:
   Last Successful Attempt: 10:55:40 UTC Apr 14 2016
   Last Failed Attempt: 10:55:10 UTC Apr 14 2016
Certificate Details:
   Certificate Magic: DNSC
   Major Version: 0x0001
   Minor Version: 0x0000
               Server    Public-key:    ED19:BFBA:FAFC:9257:DFDC:68C7:69BF:AC24:94CD:743F:3C-
1D:4966:134D:FE2C:4BDC:F315
   Query Magic: 0x717744506545635A
   Serial Number: 1435874751
   Start  Time: 1435874751 (22:05:51 UTC Jul 2 2015)
   End Time: 1467410751 (22:05:51 UTC Jul 1 2016)
   Client Public key: 106AE7C2373E5EA68FF90FDA116912D67AF16751F3EEABCB5D8CAAD565D-
8A44E
```

3 Appendix

The Cisco Umbrella Branch feature is available on the Cisco IOS XE Denali 16.3 or later. You may need to upgrade your IOS XE image to those versions.
Before you upgrade your IOS XE image to Denali 16.3 or later, you may need:

- Upgarde your IOS XE image to release 3.16.
- Upgrade your ROM Monitor (ROMMON) image to release 16.2(1r) or later.

You can download each software image from Cisco.com and upload it to flash using tftp, scp, or a usb key.

This example shows how to upgrade IOS XE image.

```
Device# copy tftp: flash:
Address or name of remote host [10.10.20.2]?
Source filename [isr4300OpenDNS.bin]?
Destination filename [isr4300OpenDNS.bin]?
Accessing t ftp://10.10.20.2/isr4300OpenDNS.bin ...
Security Configuration Guide: Cisco Umbrella Branch
6
Cisco Umbrella Branch
Restrictions for Cisco Umbrella Branch
Loading isr4300OpenDNS.bin from 10.10.20.2 (via GigabitEthernet0/0/1):
!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!C
[OK 509907627 bytes]
509907627 bytes copied in 414.230 secs (1230977 bytes/sec)
```

This example shows how to upgrade ROMMON image.

```
Device# upgrade rommonitor filename bootflash:rommon_isr_usd_rel_ios_package_SSA.bin16_2_1r
R0 Chassis model ISR4321/K9 has a single rommonitor.
Upgrade rommonitor
Target copying rommonitor image file
selected : 0
Booted : 0
Reset Reason: 0
Info: Upgrading entire flash from the rommon package
4259840+0 records in
4259840+0 records out
262144+0 records in
262144+0 records out
655360+0 records in
655360+0 records out
4194304+0 records in
4194304+0 records out
File is a FIPS ROMMON image
FIPS1403 Load Test on has PASSED.
Authenticity of the image has been verified.
Switching to ROM 1
8192+0 records in
8192+0 records out
Upgrade image MD5 signature is b702a0a59a46a20a4924f9b17b8f0887
4259840+0 records in
4259840+0 records out
4194304+0 records in
4194304+0 records out
4194304+0 records in
4194304+0 records out
262144+0 records in
262144+0 records out
Upgrade image MD5 signature verification is b702a0a59a46a20a4924f9b17b8f0887
Switching back to ROM 0
ROMMON upgrade complete.
```

Caution

After the upgrade is complete, reload the device. Ensure that you issue the show platform command to verify that the ROMMON upgrade is successful.