Cisco Start

Cisco Umbrella Branch

かんたんセットアップ ガイド

本ガイドの手順で Cisco Umbrella Branch を
Cisco ISR 4000 シリーズにかんたんにセットアップできます

1 前提条件
2 Umbrella Branch の設定
3 付録

CISCO

1 前提条件

Cisco Umbrella Branch を Cisco ISR 4000 シリーズに設定するためには、次のライセンスや環境などが必要です。

- **Cisco Umbrella Branch ライセンス**
- **Security K9 ライセンス**
- **ROM Monitor (ROMMON) バージョン 16.2(1r) 以降**：どの ROMMON バージョンからでもリリース 16.2(1r) にアップグレードできます。詳細は、「3 付録」をご覧ください。
- **Cisco IOS XE Denali 16.3 以降**
- **デフォルト DNS サーバ ゲートウェイを Cisco ISR 4000 シリーズで構成**：DNS トラフィックが Cisco ISR 4000 シリーズを通過する必要があります。
- **ネーム サーバ（*ip name-server x.x.x.x*）およびドメイン ルックアップ（*ip domain-lookup*）を Cisco ISR 4000 シリーズで構成**：FQDN を解決して、タグを Cisco Umbrella Branch ポータルに登録するために必要です。
- **Cisco Umbrella Branch 登録用 Certificate Authority (CA)**: CA を手動で Cisco ISR 4000 シリーズにインポートする必要があります。ネットワーク管理者に CA の発行を依頼する場合には、次のような情報が必要です。
  - 顧客名
  - Cisco ISR 4000 シリーズのモデル名
  - Cisco ISR 4000 シリーズの地理情報
  - シスコ サービス デリバリ マネージャの問い合わせ先（わかる場合）

Umbrella Branch 製品型番	製品説明
UMB-BRAN-4321	Cisco ISR 4321 用 Umbrella Branch ライセンス
UMB-BRAN-4331	Cisco ISR 4331 用 Umbrella Branch ライセンス
UMB-BRAN-4351	Cisco ISR 4351 用 Umbrella Branch ライセンス
UMB-BRAN-4431	Cisco ISR 4431 用 Umbrella Branch ライセンス
UMB-BRAN-4451	Cisco ISR 4451 用 Umbrella Branch ライセンス

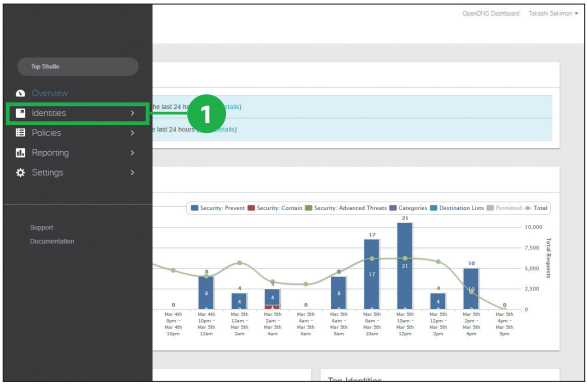
2 Umbrella Branch の設定

本ガイドでは、Cisco ISR 4000 シリーズ（ISR）を Umbrella ダッシュボードに**ネットワーク デバイス**として登録して、**デバイス ID** や**タグ**に基づいてポリシーを適用する方法を説明します。登録する方法は簡単です。まず、ISR を Umbrella ダッシュボードで認証するために、Umbrella ダッシュボードから **API トークン**を取得して ISR にインストールします。次に、ISR の CLI（コマンドライン インターフェイス）にログインして、本ガイドの手順に従って ISR を設定します。設定が完了すると、ISR は Umbrella ダッシュボードにネットワーク デバイスとして登録されて、ISR または任意のタグに対してポリシーを定義できるようになります。
Umbrella Branch を ISR に設定する手順は次のとおりです。

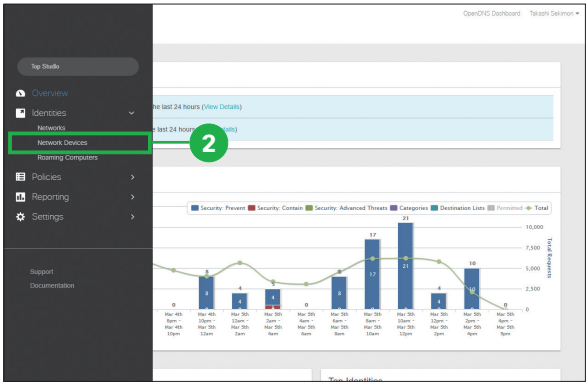
- API トークンの取得
- CA のインポートおよび API トークンの追加
- Umbrella Branch タグの登録

2-1 API トークンの取得

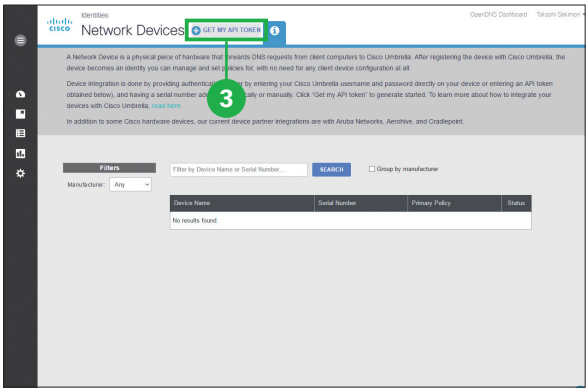
Umbrella ダッシュボードから API トークンを取得します。



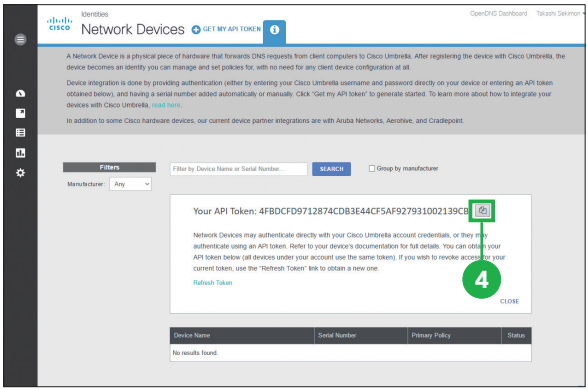
1 ［Identities］をクリック



2 ［Network Devices］をクリック



3 ［GET MY API TOKEN］をクリック



4 ［ ］をクリック

クリップボードに API トークンがコピーされます。テキスト ファイルなどに保存して、以降の手順で使用できるようにしましょう。

2-2 CA のインポートおよび API トークンの追加

Umbrella サーバへのデバイス登録は HTTPS 経由の通信となるため、ISR にルート証明書をインストールする必要があります。
まず、ISR で次のコマンドを実行します。

```
enable
configure terminal
```

1 *configure terminal（conf t）* **コマンドを入力**

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

2 *crypto pki trustpool import* **コマンドを入力**

Cisco.com から証明書を直接インポートします。

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

3 **PEM ファイルのインポートが成功したことを確認**

証明書をインポートするとメッセージが表示されます。

次に、グローバル コンフィギュレーション モードのまま、API トークンを追加するために次のコマンドを実行します。

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

4 **左の *<API TOKEN>* は「2-1」のステップ❹でコピーしたトークンに置き換え**

サンプル設定です。

```
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 Umbrella Branch タグの登録

タグは ISR の背後にある本質的に別のネットワークとして扱われ、Umbrella ダッシュボードに単独で登録すれば独自のデバイス ID が与えられます。タグ付けは、VLAN や物理インターフェイスに対して可能です。それぞれのタグは同じ API トークンを使用するため、新しくタグ付けしたインターフェイスを登録するために必要となる追加設定は最小限です。タグそのものは一意ではなく、モデル名 + MAC アドレス + タグの組み合わせが組織内で一意となります。
Umbrella Branch タグを登録するためには、次の手順を実行します。

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

1 WAN インターフェイスに OpenDNS Out を設定

注意

OpenDNS In コマンドを設定する**前に**、OpenDNS Out コマンドを設定します。登録は、ポート 443 がオープンで、トラフィックが既存のファイアウォールを通過できる場合にのみ成功します。

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

2 LAN インターフェイスに OpenDNS In を設定

opendns in mydevice_tag コマンドを使用して OpenDNS In にタグを設定すると、ISR はタグを Umbrella Branch ポータルに登録し、api.opendns.com を解決して登録プロセスを開始します。

MEMO

Cisco ISR 4000 シリーズでは、ホスト名および OpenDNS タグの長さが 49 文字を超えないようにしてください。

注意

FQDN を解決してタグを Cisco Umbrella Branch ポータルに登録するためには、Cisco ISR 4000 シリーズでネーム サーバ（***ip name-server x.x.x.x***）およびドメイン ルックアップ（***ip domain-lookup***）を構成する必要があります

2-4 ISR をパス スルー サーバとして設定

必要に応じて、ドメイン名を使用してバイパスさせるトラフィックを特定できます。 ISR では、これらのドメインを正規表現の形式で定義できます。ISR で傍受される DNS クエリが設定された正規表現のいずれかと一致する場合、そのクエリは Umbrella Branch クラウドにはリダイレクトされず、指定された DNS サーバにバイパスされます。
次のサンプル設定は、任意のドメイン名と正規表現を使用して、正規表現のパラメータ マップを定義する方法の一例です。

```
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 設定の確認

Umbrella Branch の設定は、次のコマンドで確認できます。

Router# ***show opendns config***

出力例：

```
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***

出力例：

```
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*

出力例：

```
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 付録

Umbrella Branch 機能は、Cisco IOS XE Denali 16.3 以降で使用できます。以前のバージョンから IOS XE Denali 16.3 以降にアップグレードするためには、次のような環境が必要になる場合があります。

- IOS XE イメージをリリース 3.16 にアップグレード
- ROM モニタ(ROMMON)イメージをリリース 16.2(1r) 以降にアップグレード

ソフトウェア イメージは Cisco.com でダウンロードできます。ISR のフラッシュ メモリへのアップロードには、TFTP、SCP、USB メモリなどを使用します。

次のサンプル設定は、IOS XE イメージをアップグレードする方法の一例です。

```
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)
```

次のサンプル設定は、ROMMON イメージをアップグレードする方法の一例です。

```
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.
```

注意

アップグレードが完了したら、ISR を再起動します。*show platform* コマンドを実行して、ROMMON のアップグレードが成功したことを確認してください。

付録 サポート情報について

Cisco Umbrella のサポート情報は、次の Web サイトをご覧ください。

- **Cisco Umbrella Support（FAQ など）**
  https://support.umbrella.com/hc/en-us

- **Cisco Umbrella Documentation（セットアップ ガイドなど）**
  https://docs.umbrella.com/product/umbrella

©2017 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。
「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R)
この資料の記載内容は 2017 年 6 月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

お問い合わせ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

1292-1706-02A-TO