Deploy Umbrella DNS for Aruba WLAN Administrators

Contents

Introduction

This document describes how to deploy the Umbrella DNS service for Aruba WLAN administrators.

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

Aruba Networks has these three wireless LAN (WLAN) product lines and operating systems for different market segments and deployment scenarios:

- ArubaOS: for large organizations and high density deployments
- Aruba Instant / InstantOS: for small-to-medium sized businesses and distributed enterprises

- Aruba Instant On: for home and small office users

This article provides guidelines for Aruba WLAN administrators to adopt and deploy Umbrella DNS service.

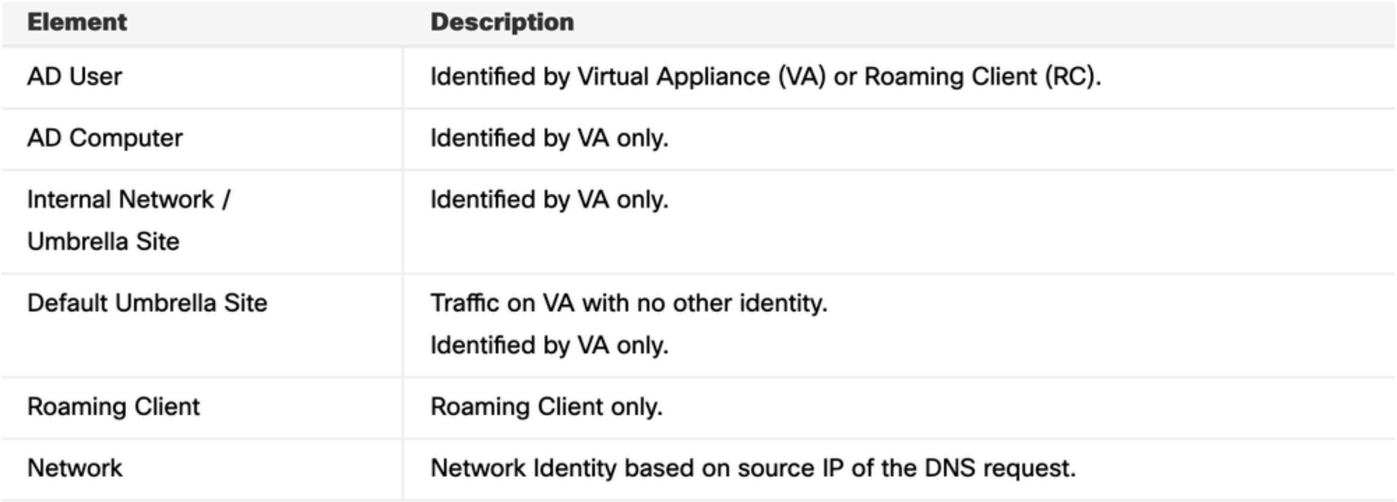
Deployment Methods

Methods of deployment depend on your Aruba operating system and how you plan to use Umbrella.

If you run any of the three previously-mentioned Aruba operating systems, you can start deploying Umbrella DNS by consulting the Umbrella user guide. Video tutorials are available as well.

If you run Aruba Instant, you have an additional option of using the Umbrella network device integration available in InstantOS. Please note, however, that if you choose this option, you **cannot** see wireless clients' internal/private IP addresses on the WLAN in Umbrella reporting, such as the Activity Search report. DNS queries from clients map to Instant AP clusters' network device identities in Umbrella, and information regarding the individual clients is not available. From the perspective of Umbrella cloud, DNS queries can appear to come from the Instant AP clusters rather than the Wi-Fi clients.

As such, if you have a requirement to trace individual clients' DNS queries or to tailor DNS policies for individual clients on a WLAN, you can deploy Umbrella through standard methods described in the Umbrella DNS user guide (without using the network device integration through Aruba Instant), and consider including Umbrella virtual appliances in their deployment plans.



Element	Description
AD User	Identified by Virtual Appliance (VA) or Roaming Client (RC).
AD Computer	Identified by VA only.
Internal Network / Umbrella Site	Identified by VA only.
Default Umbrella Site	Traffic on VA with no other identity. Identified by VA only.
Roaming Client	Roaming Client only.
Network	Network Identity based on source IP of the DNS request.

4403300507924

Aruba Instant Integration

Aruba Instant's Umbrella (OpenDNS) network device integration can be beneficial in environments where all Wi-Fi clients connected to an Instant AP cluster is subject to a singular Umbrella DNS policy, and where there is no need to review individual clients' DNS queries in Umbrella reports. This section explains how to setup the integration.

Note: The integration uses a legacy version of Umbrella's network devices API. The legacy version does not require customers to generate API tokens from their Umbrella dashboards, but the newer versions do.

Umbrella legacy APIs reached end-of-life on 2023-09-01, after which date support is no longer provided for the integration. If you encounter any issue with the integration after 2023-09-01, please complete the "Get Started" section in the deployment guide to deploy Umbrella without using the integration.

These requirements need to be met in order to use the integration:

- APs need to run InstantOS version 8.10.0.1 or newer (as of May 2022).
- The Umbrella dashboard account used for the integration needs to have Full Admin role.
- The account's email address cannot be associated with more than one Umbrella dashboard. If you are not sure whether the email address is only associated with a single dashboard, you can contact Cisco Umbrella Support to verify.
- Single sign-on (SSO) and two-factor authentication (2FA) cannot be enabled for the account.
- If there is a network security appliance (like a firewall) between APs and Internet, the appliance needs to allow unfiltered and non-inspected connections to 208.67.220.220, 208.67.222.222, 67.215.92.210, and 146.112.255.152/29 (.152 ~ .159).

Configuration

At a high level, there are four configuration steps in enabling the integration:

1. Set a name for AP cluster

2. Enter account credentials

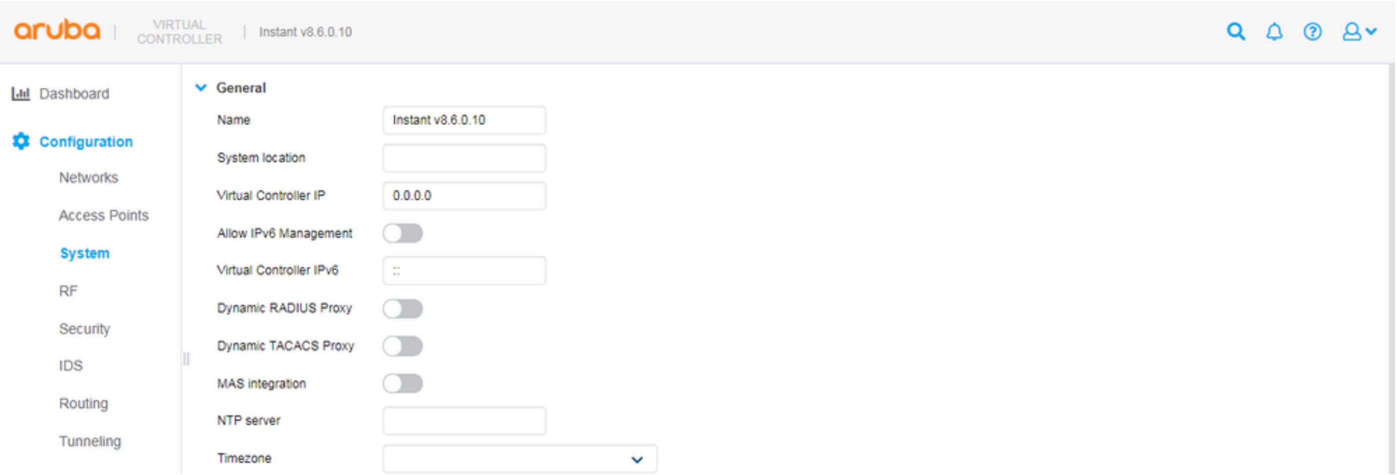
3. Intercept DNS queries

4. Apply DNS policy

Set a Name for AP Cluster

When an Instant cluster successfully registers itself to an Umbrella dashboard for the first time, a network device entry is added to Umbrella dashboard under **Deployments** > **Network Devices**. Device name of a new entry comes from the system name configured on a cluster's virtual controller.

To set the system name on an Instant virtual controller, navigate to **Configuration** > **System**.



General

Name	Instant v8.6.0.10
System location	
Virtual Controller IP	0.0.0.0
Allow IPv6 Management	○
Virtual Controller IPv6	::
Dynamic RADIUS Proxy	○
Dynamic TACACS Proxy	○
MAS integration	○
NTP server	
Timezone	

4404011628308

Note that the name value is copied only once during initial registration. If a system/device name is changed on either the Instant or Umbrella side afterwards, you must manually update the name on the other side.

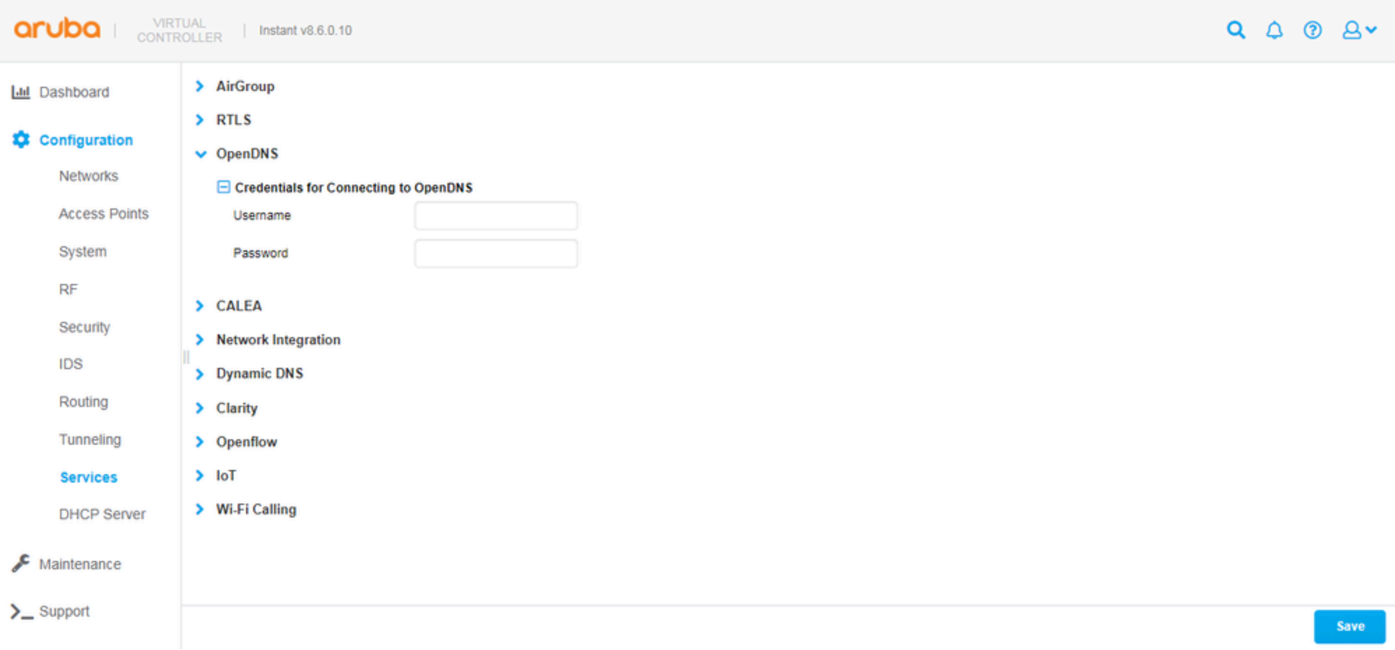
Enter Account Credentials

If the requirements listed in the **Prerequisites** section are met, you can add an Instant cluster to your Umbrella dashboard as a network device. To do so from a cluster's virtual controller:

1. Navigate to **Configuration** > **Services** > **OpenDNS.**

2. Enter the login credentials of an Umbrella account.

3. Select **Save**.



Credentials for Connecting to OpenDNS

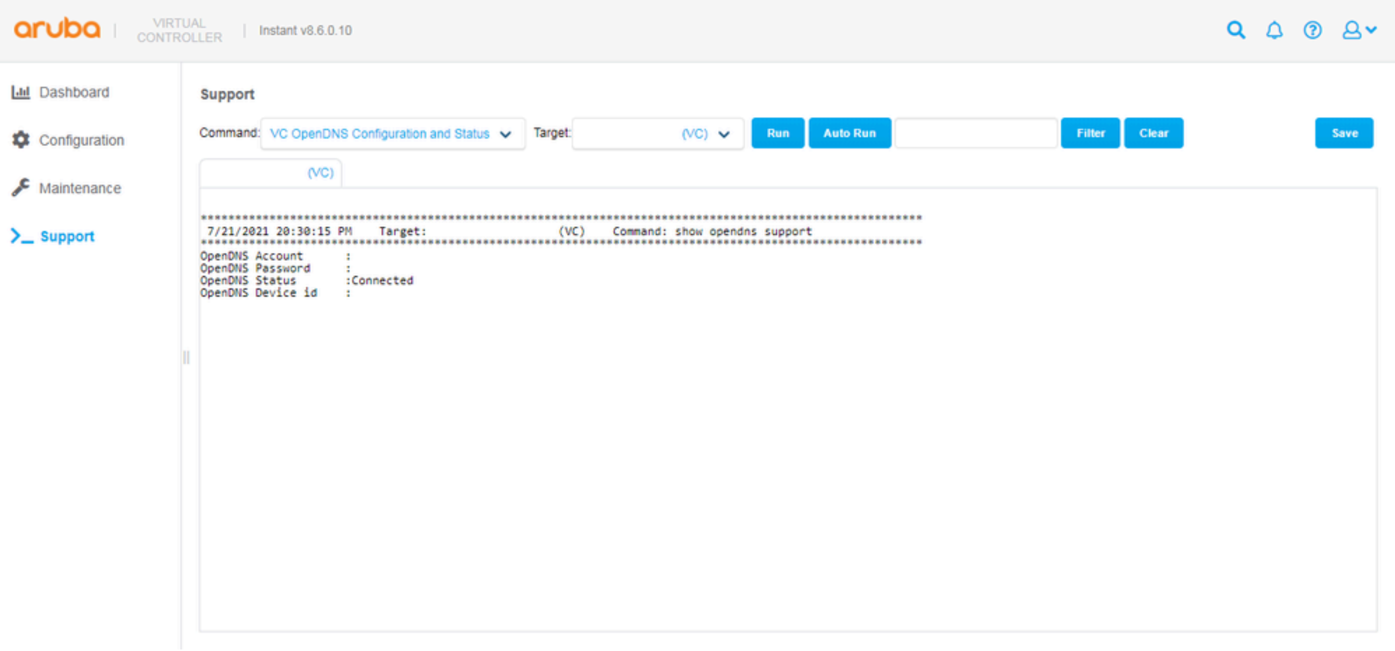
Username

Password

4404019266196

If the virtual controller (VC) successfully connects to Umbrella, you can see a **Connected** status when you navigate to Support and run the "VC OpenDNS Configuration and Status" (`show opendns support`) command.

You can also see a device ID, which is generated by Umbrella when a new network device is created and saved into the Instant VC configuration. The latter part is important. Since each Instant cluster needs to have a unique Umbrella network device ID, the device ID must not be copied from one cluster's configuration to another. A valid device ID typically has 16 digits.



Support

Command: VC OpenDNS Configuration and Status   Target: (VC)

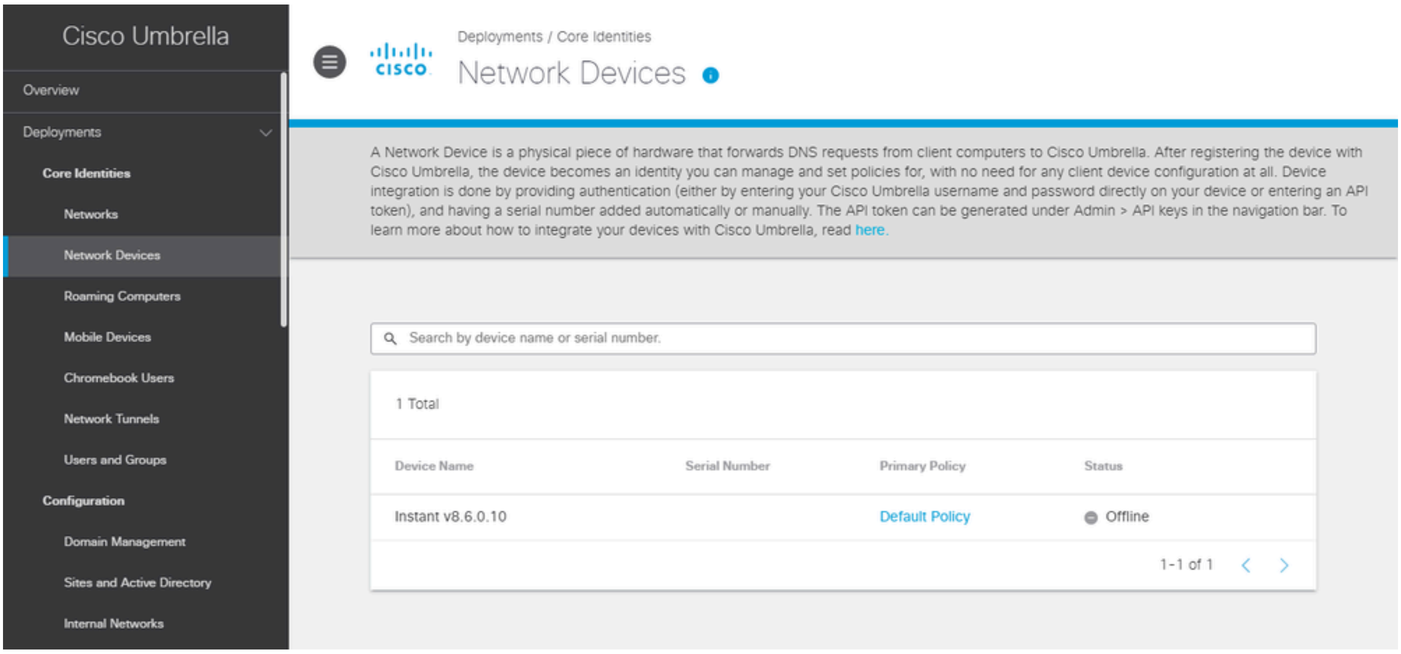
(VC)

```
*****************************************************************************************
 7/21/2021 20:30:15 PM    Target:                        (VC)    Command: show opendns support
*****************************************************************************************
OpenDNS Account      :
OpenDNS Password     :
OpenDNS Status       :Connected
OpenDNS Device id    :
```

4404019268116

If the command output shows a **Not connected** status, you can try to find out why by running "AP Tech Support Dump" (`show tech-support`) and "AP Tech Support Dump Supplemental" (`show tech-support supplemental`) commands, and then searching for "opendns" in the logs. The command outputs can also be shared with Aruba TAC for troubleshooting purposes.

If everything is working correctly, you can see a new entry in Umbrella dashboard under **Deployments > Network Devices**, where you can search for an Instant AP cluster by its name or delete an existing entry if you wish to generate a new device ID.



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), and having a serial number added automatically or manually. The API token can be generated under Admin > API keys in the navigation bar. To learn more about how to integrate your devices with Cisco Umbrella, read here.

Device Name	Serial Number	Primary Policy	Status
Instant v8.6.0.10		Default Policy	● Offline

4404011658516

Intercept DNS Queries

Upon confirming that a cluster has been successfully added to your Umbrella dashboard as a network device, you can set the cluster to begin intercepting DNS queries sent from wireless clients (that are connected to APs in the cluster). Once it is set, regardless of what DNS server IP addresses are configured on the NICs of wireless clients, the clients' DNS queries can be intercepted by the cluster and forwarded to Umbrella's anycast resolvers at 208.67.220.220 and 208.67.222.222.

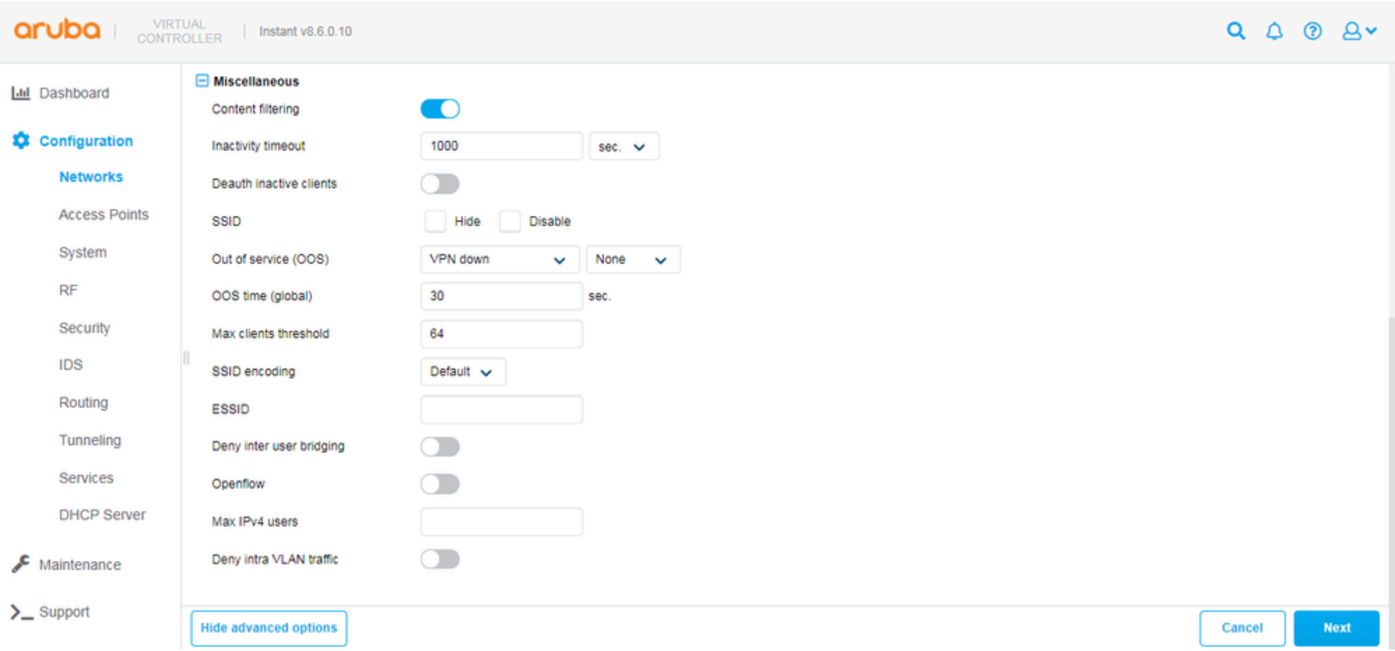
To intercept DNS queries:

1. Navigate to a cluster's virtual controller under **Configuration** > **Networks**.

2. Select a wireless network.

3. Edit the network, select **Show advanced options**, and scroll to the **Miscellaneous** section.

4. Enable the **Content filtering** option, and keep selecting **Next** until you can select the **Finish** button to save the change.

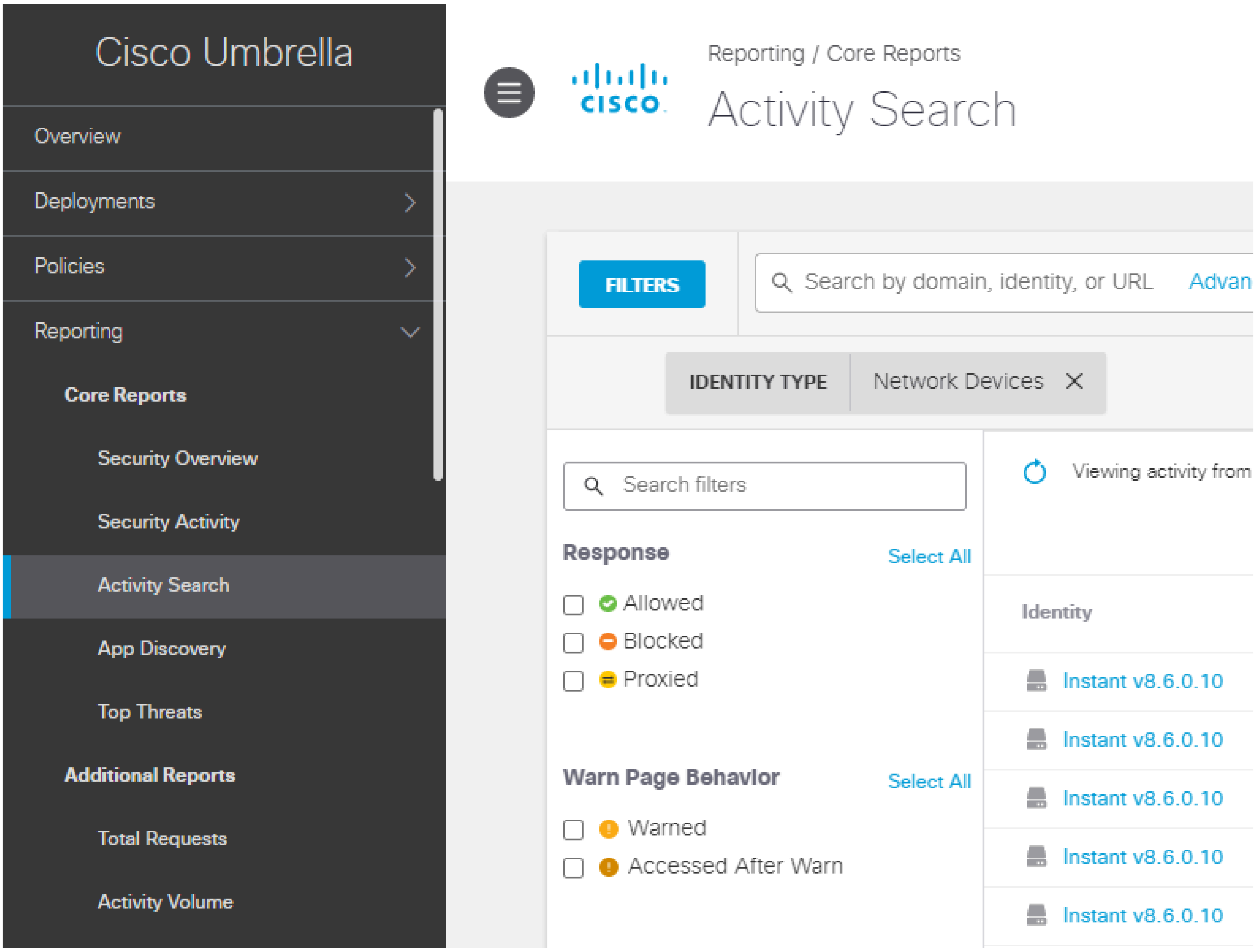


Miscellaneous

Content filtering	On
Inactivity timeout	1000 sec.
Deauth inactive clients	Off
SSID	□ Hide □ Disable
Out of service (OOS)	VPN down; None
OOS time (global)	30 sec.
Max clients threshold	64
SSID encoding	Default
ESSID	
Deny inter user bridging	Off
Openflow	Off
Max IPv4 users	
Deny intra VLAN traffic	Off

4404011668500

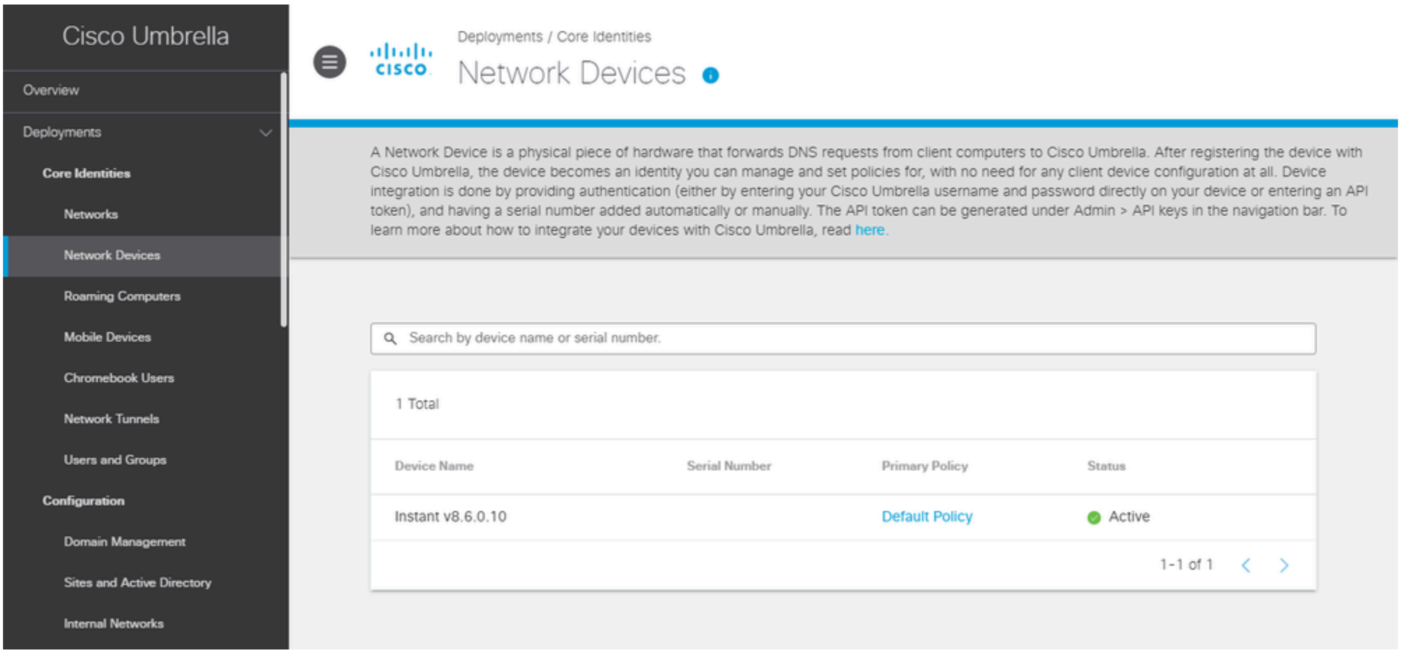
After the option is turned on, you can start seeing DNS queries in the Umbrella dashboard under **Reporting** > **[Activity Search](#)**.The identity of the queries can map to a network device name, which is typically the system name configured on an AP cluster's virtual controller. Note that it can take some time (around 15 minutes) for queries to be processed and displayed in the dashboard GUI.



Identity
Instant v8.6.0.10
Instant v8.6.0.10
Instant v8.6.0.10
Instant v8.6.0.10
Instant v8.6.0.10

4404011721620

In the Umbrella dashboard under **Deployments > Network Devices**, it can take up to 24 hours for a device to change to an active/online status. Status of a network device merely indicates whether DNS queries were intercepted by the device and forwarded to Umbrella in the 24 hours prior, and does **not** influence how a device communicates with Umbrella. An offline/inactive status can simply mean that no wireless client was connected to an AP cluster in the past 24 hours and cannot prevent the cluster from utilizing Umbrella service.



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), and having a serial number added automatically or manually. The API token can be generated under Admin > API keys in the navigation bar. To learn more about how to integrate your devices with Cisco Umbrella, read here.

1 Total

Device Name	Serial Number	Primary Policy	Status
Instant v8.6.0.10		Default Policy	● Active

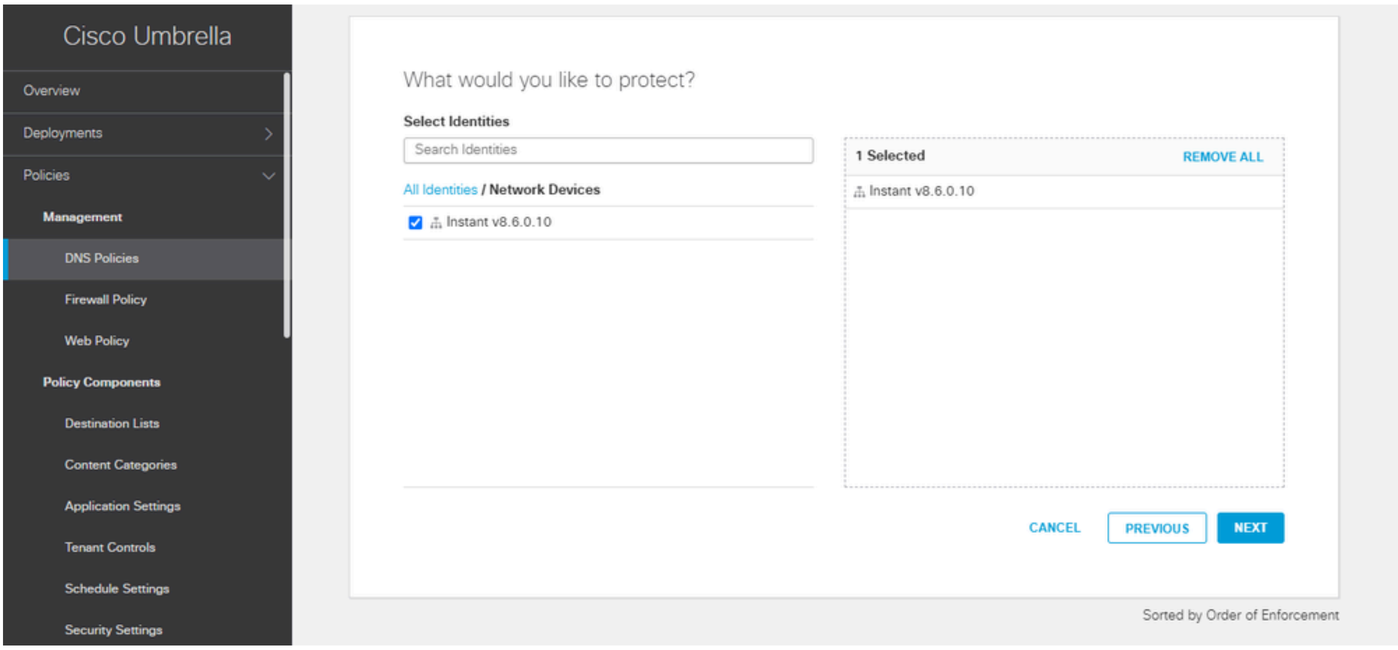
1-1 of 1

4404011756308

Apply DNS Policy

In Umbrella, the "Default Policy" automatically includes all identities (like network devices) added to a dashboard. It is not necessary to create additional DNS policies if all AP clusters in your deployment can be subject to the same policy. If this is the case for you, skip to the next section.

Alternatively, if you wish to apply a custom policy to a specific network device, you need to add a new policy in the Umbrella dashboard under **Policies > All Policies (DNS Policies),** and select the network device in the policy.



What would you like to protect?

Select Identities

Search Identities

All Identities / Network Devices

☑ Instant v8.6.0.10

1 Selected

Instant v8.6.0.10

4404011773588

When there is more than one policy on the DNS Policies (All Policies) page, the policies are evaluated from top-to-bottom on a first-match basis. For more information, please see the policy precedence documentation and the best practices for defining policies documentation.

Internal DNS

In an environment where internal DNS servers exist, and you want to forward DNS queries for certain (internal) domains to the internal DNS servers, you can use the Enterprise Domains feature in Instant.

DNS queries can continue to be intercepted by AP cluster after the feature is enabled, except that queries for the specified domains can no longer be forwarded to Umbrella. Instead, they can be forwarded to the DNS server IP addresses originally configured on the wireless clients' NICs (like via DHCP). The feature is similar to the Internal Domains functionality available in standard Umbrella deployment methods (with virtual appliances), where the Aruba Instant integration is not used.

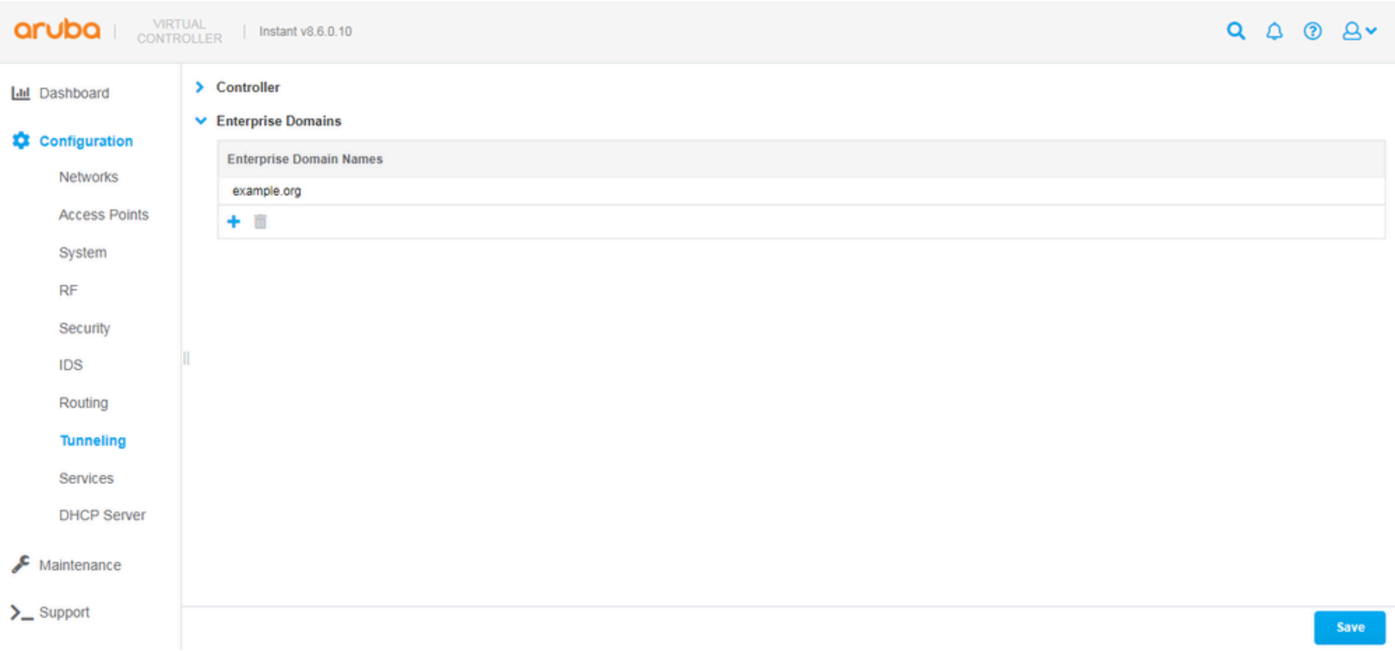
To configure the feature on an Instant virtual controller:

1. Navigate to **Configuration** > **Tunnelling** > **Enterprise Domains**.

2. Add domains to, or remove domains from, the **Enterprise Domain Names** list.

3. Select **Save**.

There is an implicit wildcard for any domain added to the list, so example.org implies *.example.org.

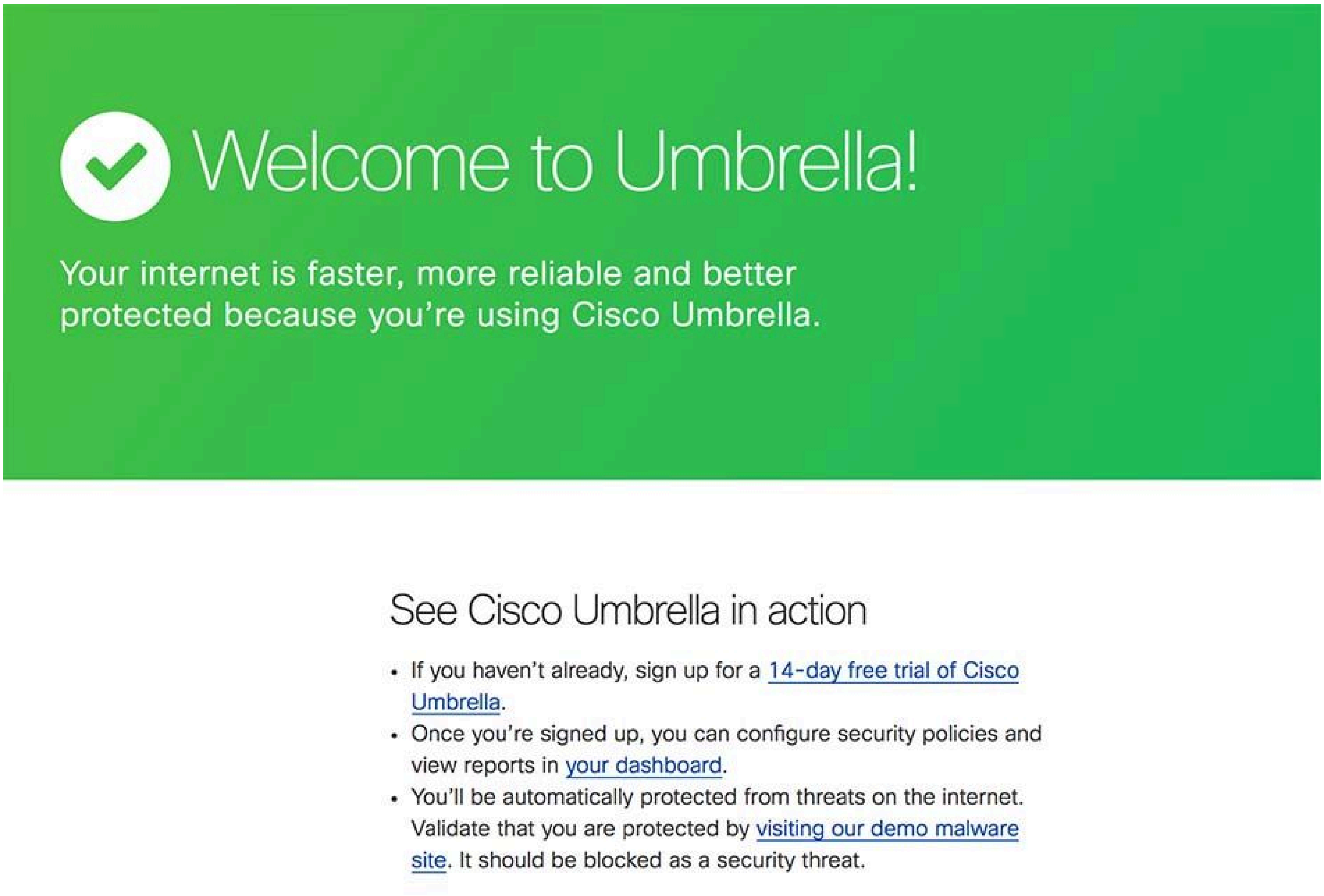


Enterprise Domain Names
example.org

4404238114452

Verification

Whether you have deployed Umbrella on your WLAN using the standard methods referenced in the "Deployment Overview" section of this guide, or the integration described in the "Aruba Instant Integration" section, you can verify that wireless clients are using Umbrella DNS by browsing to https://welcome.umbrella.com/ from one of the clients. You then see a green check similar to the screenshot displayed in the [Umbrella documentation](#).



Welcome to Umbrella!

Your internet is faster, more reliable and better protected because you're using Cisco Umbrella.

See Cisco Umbrella in action

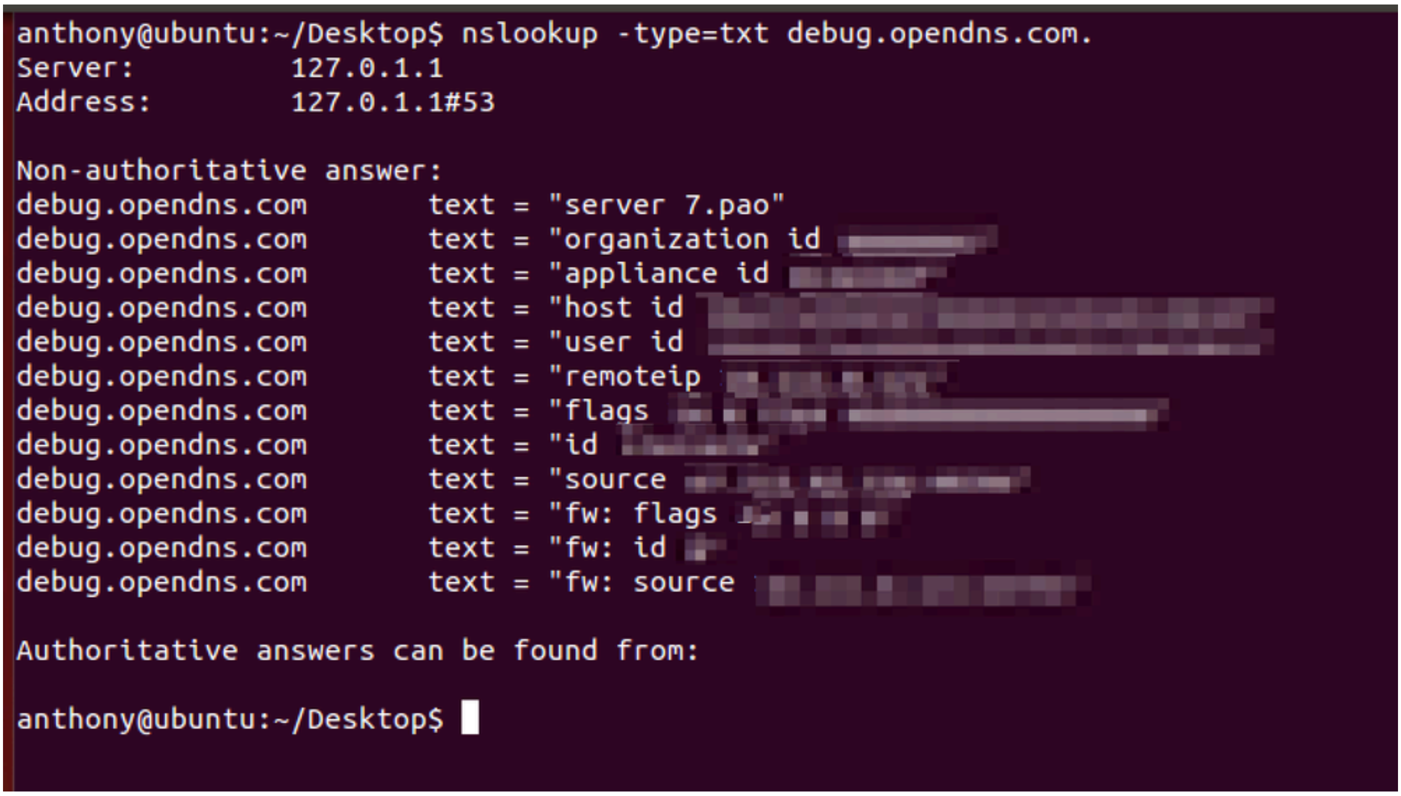
- If you haven't already, sign up for a 14-day free trial of Cisco Umbrella.
- Once you're signed up, you can configure security policies and view reports in your dashboard.
- You'll be automatically protected from threats on the internet. Validate that you are protected by visiting our demo malware site. It should be blocked as a security threat.

4404011960212

Alternatively, you can verify this by running this command in a wireless client's command prompt.

```
nslookup -type=txt debug.opendns.com.
```

You can see an output with a number of text lines, similar to this screenshot:

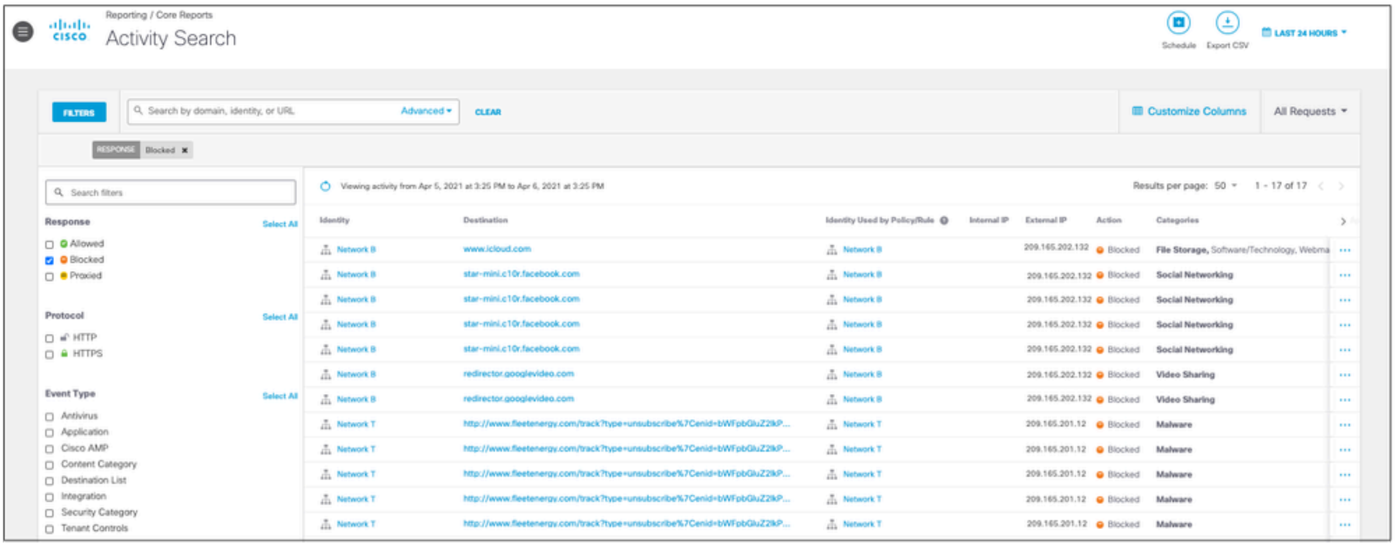


```
anthony@ubuntu:~/Desktop$ nslookup -type=txt debug.opendns.com.
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
debug.opendns.com       text = "server 7.pao"
debug.opendns.com       text = "organization id [redacted]
debug.opendns.com       text = "appliance id [redacted]
debug.opendns.com       text = "host id [redacted]
debug.opendns.com       text = "user id [redacted]
debug.opendns.com       text = "remoteip [redacted]
debug.opendns.com       text = "flags [redacted]
debug.opendns.com       text = "id [redacted]
debug.opendns.com       text = "source [redacted]
debug.opendns.com       text = "fw: flags [redacted]
debug.opendns.com       text = "fw: id [redacted]
debug.opendns.com       text = "fw: source [redacted]

Authoritative answers can be found from:

anthony@ubuntu:~/Desktop$ █
```

4404011980436

From the command output, you can see your Umbrella dashboard's org ID in the "orgid" or "organization id" line, and if you use the Instant integration, you can see the extra "device" line that contains a device ID.

To review DNS queries in your Umbrella dashboard, navigate to **Reporting** > **Activity Search**. Note that it can take some time (about 15 minutes) for queries to display in the dashboard GUI. Instructions on how to use Activity Search are available at in the Umbrella documentation.



Reporting / Core Reports

Activity Search

Search by domain, identity, or URL

RESPONSE Blocked ✖

Search filters

Response Select All

- □ Allowed
- ☑ Blocked
- □ Proxied

Protocol Select All

- □ HTTP
- □ HTTPS

Event Type Select All

- □ Antivirus
- □ Application
- □ Cisco AMP
- □ Content Category
- □ Destination List
- □ Integration
- □ Security Category
- □ Tenant Controls

Viewing activity from Apr 5, 2021 at 3:25 PM to Apr 6, 2021 at 3:25 PM

Results per page: 50 1 - 17 of 17

Identity	Destination	Identity Used by Policy/Rule	Internal IP	External IP	Action	Categories
Network B	www.icloud.com	Network B		209.165.202.132	Blocked	**File Storage,** Software/Technology, Webma
Network B	star-mini.c10r.facebook.com	Network B		209.165.202.132	Blocked	**Social Networking**
Network B	star-mini.c10r.facebook.com	Network B		209.165.202.132	Blocked	**Social Networking**
Network B	star-mini.c10r.facebook.com	Network B		209.165.202.132	Blocked	**Social Networking**
Network B	star-mini.c10r.facebook.com	Network B		209.165.202.132	Blocked	**Social Networking**
Network B	redirector.googlevideo.com	Network B		209.165.202.132	Blocked	**Video Sharing**
Network B	redirector.googlevideo.com	Network B		209.165.202.132	Blocked	**Video Sharing**
Network T	http://www.fleetenergy.com/track?type=unsubscribe%7Cenid=bWFpbGluZ2lkP...	Network T		209.165.201.12	Blocked	**Malware**
Network T	http://www.fleetenergy.com/track?type=unsubscribe%7Cenid=bWFpbGluZ2lkP...	Network T		209.165.201.12	Blocked	**Malware**
Network T	http://www.fleetenergy.com/track?type=unsubscribe%7Cenid=bWFpbGluZ2lkP...	Network T		209.165.201.12	Blocked	**Malware**
Network T	http://www.fleetenergy.com/track?type=unsubscribe%7Cenid=bWFpbGluZ2lkP...	Network T		209.165.201.12	Blocked	**Malware**
Network T	http://www.fleetenergy.com/track?type=unsubscribe%7Cenid=bWFpbGluZ2lkP...	Network T		209.165.201.12	Blocked	**Malware**

4404019393044