Cisco Umbrella WLAN Integration Guide

Revised: May 11, 2018

Introduction

This document introduces Cisco Umbrella (formerly OpenDNS) and provides general guidelines for its deployment. The purpose of this document is to:

- Provide an overview of Cisco Umbrella WLAN feature
- Highlight supported key features
- Provide details on deploying and managing Cisco Umbrella on WLC

Pre–requisite

AireOS 8.4 or newer is required on the Cisco Wireless LAN Controller to support Cisco.

Note In order to upgrade to AireOS 8.4, customers must have AireOS 8.0 or higher release

Components Used

The information in this documentwas created from devices in a specificlab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

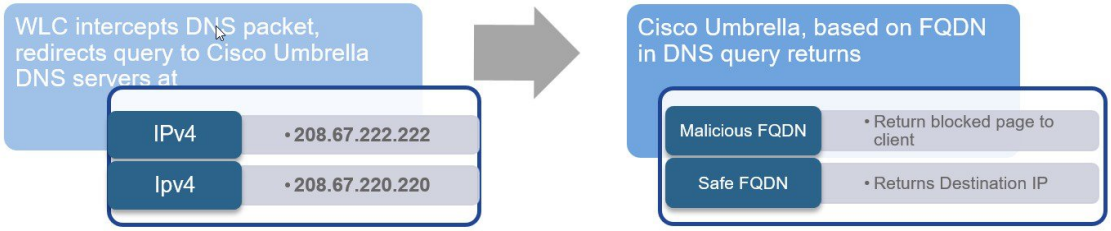
Refer to Cisco Technical Tips Conventions for more information on document conventions.

Feature Introduction

Cisco Umbrella is a Cloud delivered network security service, which gives insights to protect devices from malware and breach protection in real time. It uses evolving big data and data mining methods to proactively predict attacks also do category based filtering.

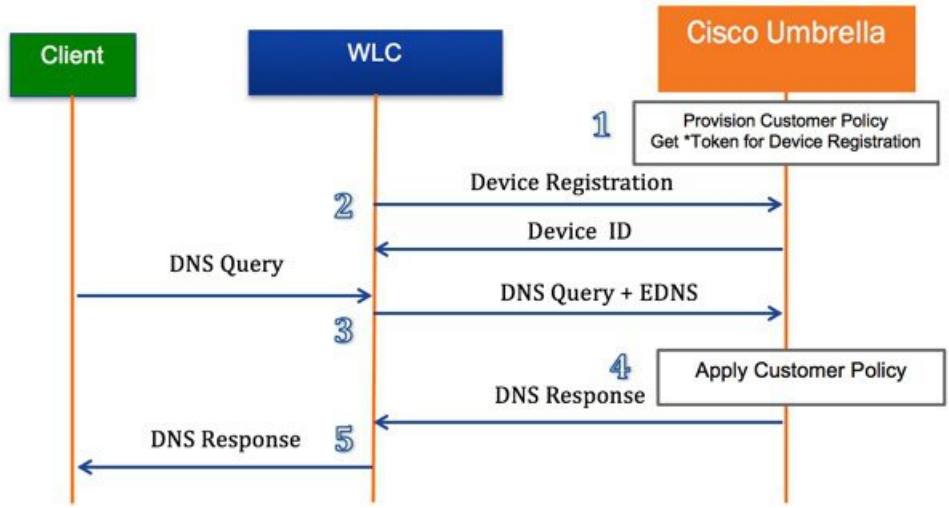
Terminology involved in the working of the feature:

1. **API Token** is issued from Cisco Umbrella Portal and is only used for device registration
2. **Device Identity** is a unique device identifier. Policy is enforced per identifier
3. **EDNS** is an Extension mechanism for DNS which carries tagged DNS packet
4. **FQDN** is Fully Qualified Domain Name

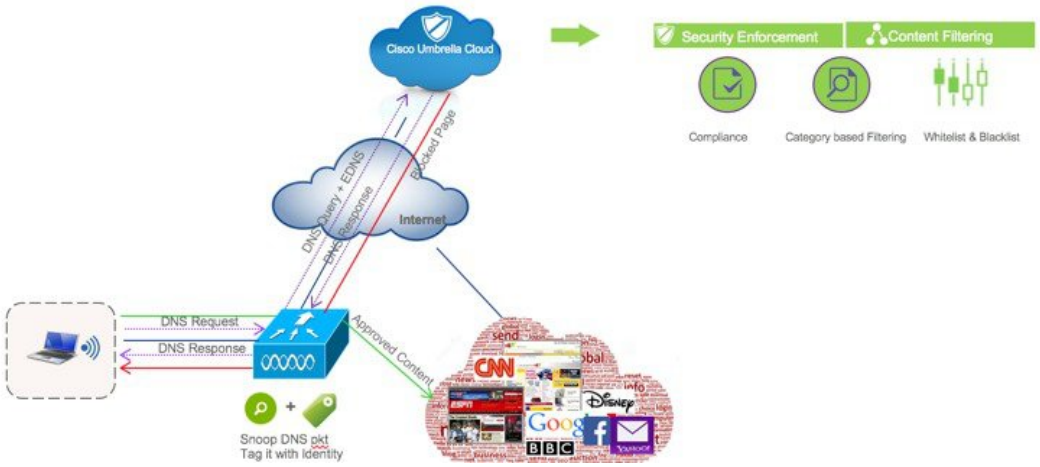


DNS request always precedes web request. Wireless Lan Controller intercepts DNS request from the client and redirects the query to Cisco Umbrella in the cloud (208.67.222.222, 208.67.220.220). Cisco Umbrella servers resolve the DNS query and enforces preconfigured security filtering rules on a per identity basis to mark the domain as either malicious which will return a blocked page to client or safe returning resolved IP address to client.

Cisco Umbrella General Work Flow



1. WLC registration with Cisco Umbrella server is a one-time process and happens over a secure HTTPS tunnel
2. Obtain API Token for device (WLC) registration from Cisco Umbrella dashboard
3. Apply the Token on Wireless Lan Controller. This should register the device to Cisco Umbrella account. Next, create Cisco Umbrella Profile/s on WLC. Profiles will automatically be pushed to the Cisco Umbrella as Identities and policy will be enforced on a per identity basis
4. Wireless client traffic flow from to Cisco Umbrella server
5. A wireless client sends a DNS request to WLC
6. WLC snoops the DNS packet and tags it with a Cisco Umbrella Profile. 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 organization compliance
9. Depending on the rules, it either returns a blocked page or resolved ip address to the client for the DNS request queried



Configuring the Cisco Umbrella Wireless LAN Controller Integration

Procedure

Step 1 Cisco Umbrella provisioning involves creating a user account on Cisco Umbrella cloud.

Subscription is per account and Cisco Umbrella offers14 day obligation free trial license.

Permanent License is covered under CiscoOne Advanced Subscription.

Step 2 Next, enable Wireless Controller (GUI or CLI) for Cisco Umbrella .

Step 3 WLC registers to the cloud account over a secure HTTPS tunnel.

Step 4 Configure profiles (identities) on WLC. Profile can be mapped to either WLAN, AP group or incorporated into local policy.

Step 5 WLC redirects DNS packets to Cisco Umbrella cloud.

Step 6 Security policies on Cisco Umbrella are applied per Identity.

Cisco Umbrella configuration steps on Wireless Controller involve enabling Cisco Umbrella function, configuring API Token, creating Profile/s and mapping the profile to either a WLAN, an AP group or a Local Policy.

The policy priority order (starting from highest) is:

1. Local Policy
2. AP Group
3. WLAN

Cisco Umbrella profile when mapped to local policy allows for a granular differentiated user browsing experience based on dynamic evaluation of attributes (user role, device type etc). In rest of the document, we will discuss following two scenarios:

- **Scenario 1**–Configure WLC for Cisco Umbrella and incorporate Cisco Umbrella profile in a user role based local policy. We will also touch upon basic configuration on Cisco Umbrella Server.
- **Scenario 2**–Configure WLC for Cisco Umbrella and apply Cisco Umbrella profile on a WLAN and AP Group.

Scenario 1: Configuring Local Policies for Cisco Umbrella

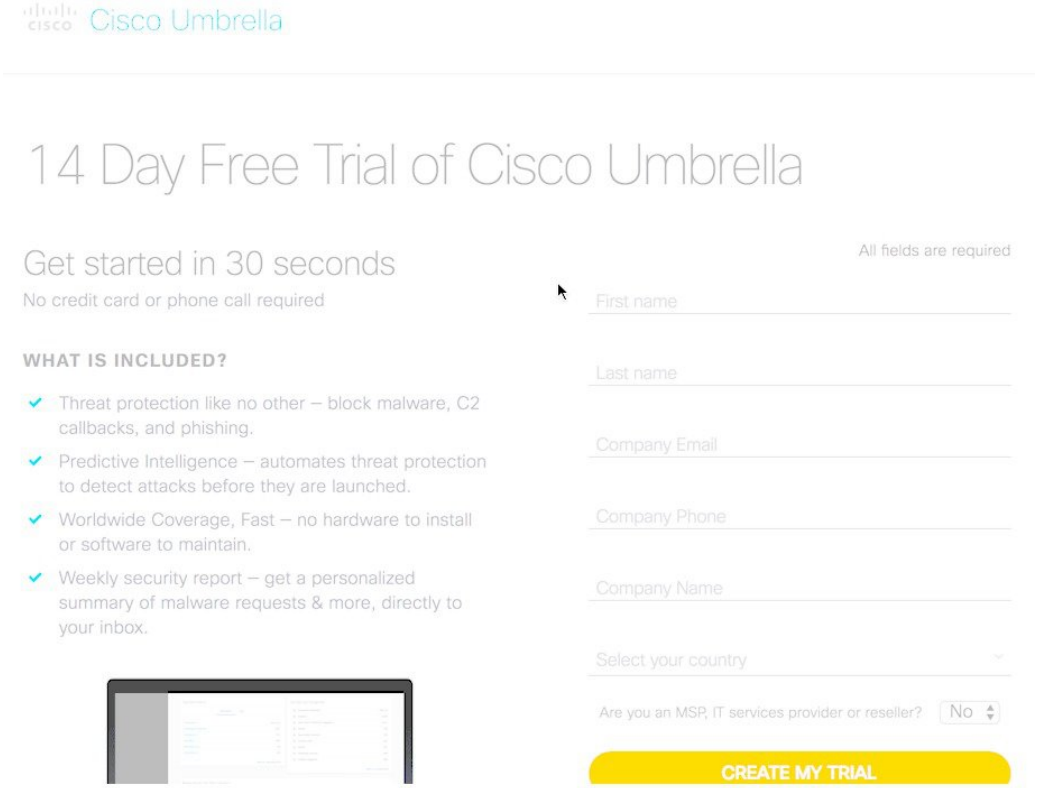
In an organization, our goal is to restrict internet access (for particular websites) to users based on their role types. For example, employees should be permitted full internet access barring sites such as adult, gambling, nudity and contractor access should be more rigid barring them access to social websites, sports, adult, gaming, nudity, etc.

We will be using an external AAA server to authenticate a user and based on the identity, pass the role as either contractor or employee to WLC. On the WLC, user will configure two policies – one for employee and the other for contractor and apply a different Cisco Umbrella profile to each to restrict their browsing activity when connected to the same dot1x enabled WLAN. To achieve this, we will be configuring the following order:

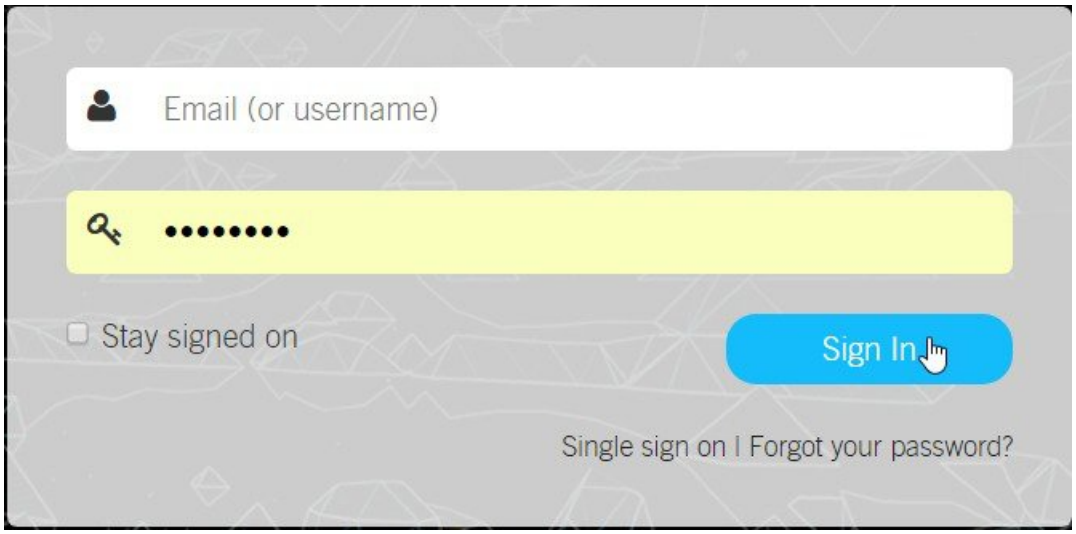
1. On Cisco Umbrella Server: Create an account, generate API token for device (WLC) registration
2. On WLC: Enable Cisco Umbrella globally, apply API token and create Cisco Umbrella profiles for employee and contractor.
3. On Cisco Umbrella Server: Create Category definitions/rules and Policies for employee and contractor.
4. On WLC: Create Local policy each for employee and contractor tying the AAA returned role and Cisco Umbrella profile under each.
5. On WLC: Tie the two local policies to the dot1x WLAN

Procedure

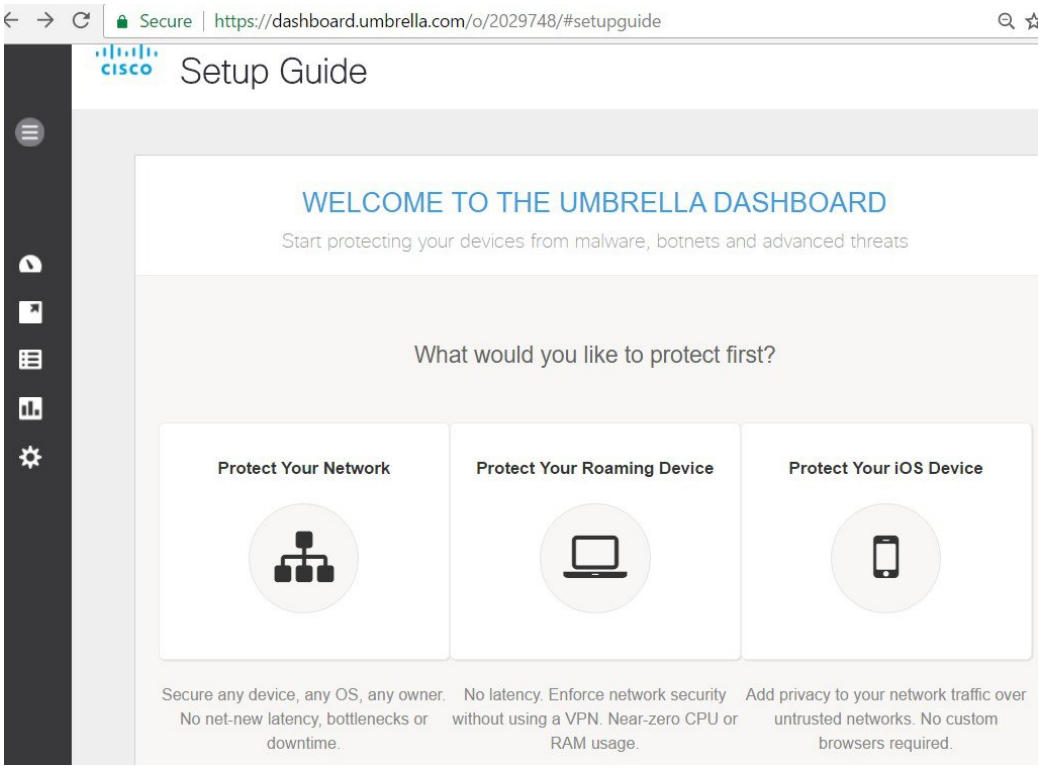
Step 1 Create your own 14 day trial account here https://signup.umbrella.com/

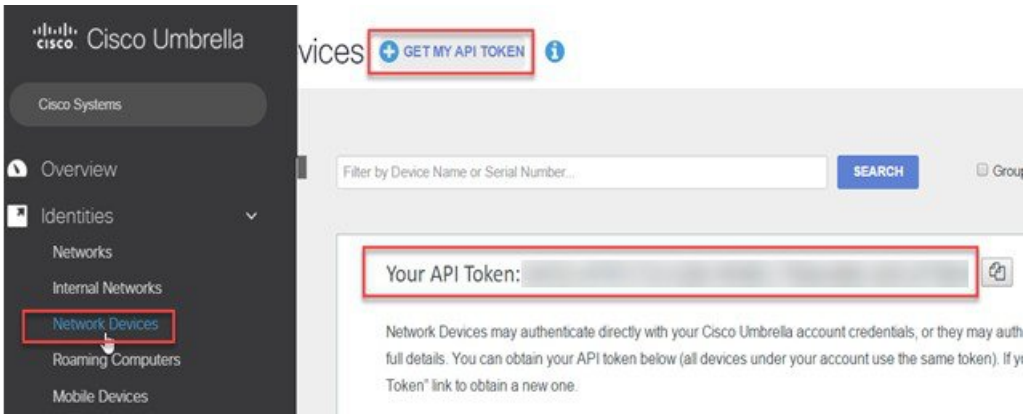


Step 2 Login to your account at https://login.umbrella.com/

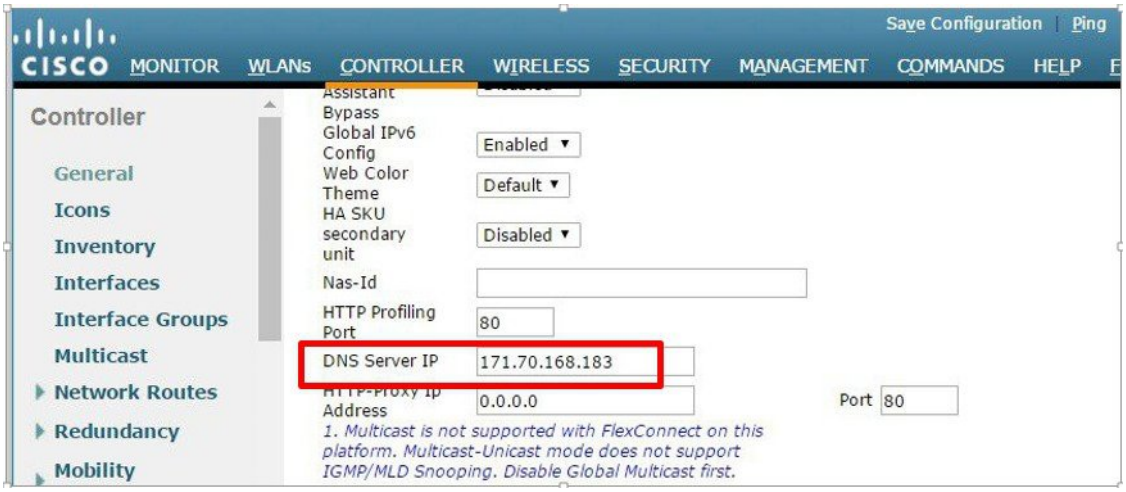


Step 3 From Cisco Umbrella main dashboard landing page, click **Identities** from the side menu, then choose **Network Devices**. At the top of the page, click the + icon and click on **GET MY API TOKEN** as shown below.





Step 4 From WLC main menu, go to **Controller** > **General** and enter a **DNS Server IP** address that can resolve domains. This is needed for the first time before enabling Cisco Umbrella feature on the WLC.

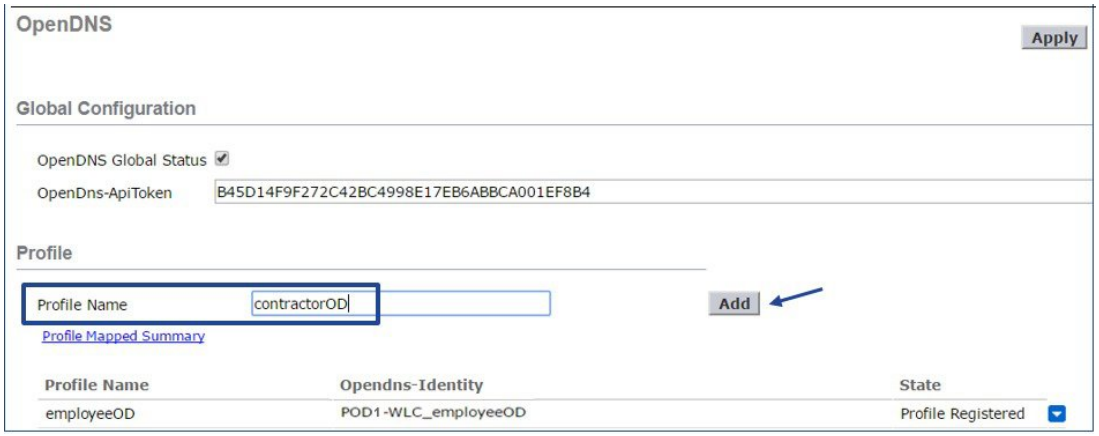


Step 5 From WLC main menu, go to **Security** >**OpenDNS** > **General**> **enable OpenDNS Global Status**.


```
CLI command:config Cisco Umbrella  enable
```

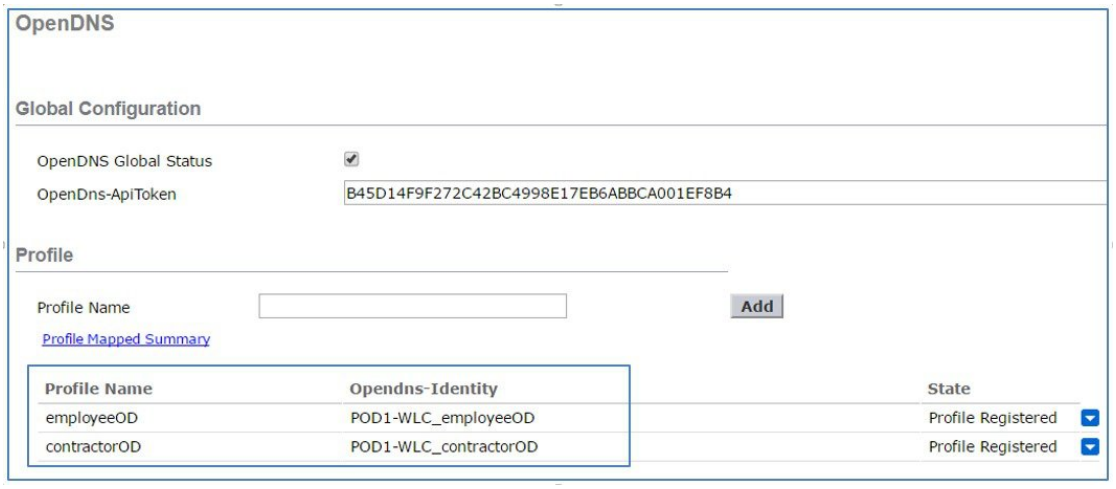
Step 6 On the same WLC screen, configure API Token obtained from Umbrella dashboard earlier(**Step 3**)

Step 7 From the same page, create OpenDNSProfiles **Security** > **OpenDNS** >**General**.




```
CLI command: config Cisco Umbrella  profile create <profile-name>
```

Step 8 On WLC, create two OpenDNS profiles, one for employee(**employeeOD**) and anotherfor contractor (**contractorOD**) via CLI or GUI. These profiles shouldautomatically be pushed to your OpenDNS accountas **Identities**and you should see the **State** of the Profiles populated as **Profile Registered.** This is subject to a successful connection between the WLC and Umbrella server.

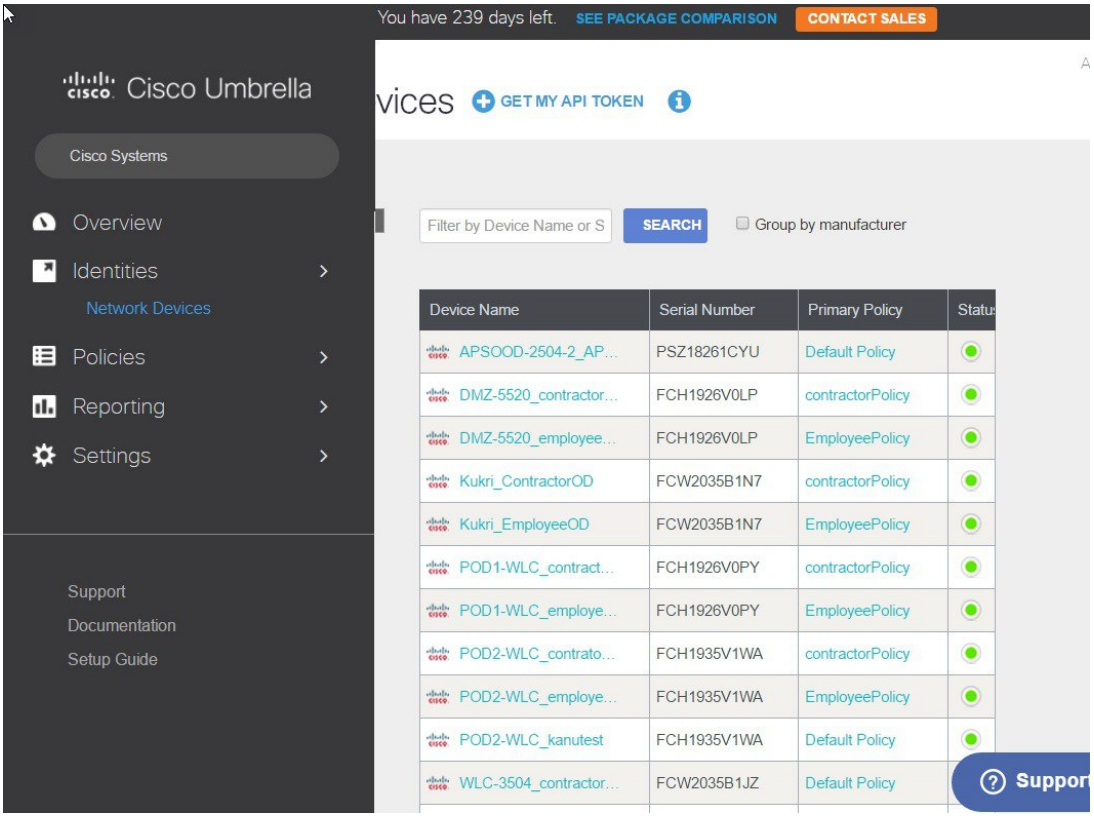


On CLI, you can verify the two profiles as shown:

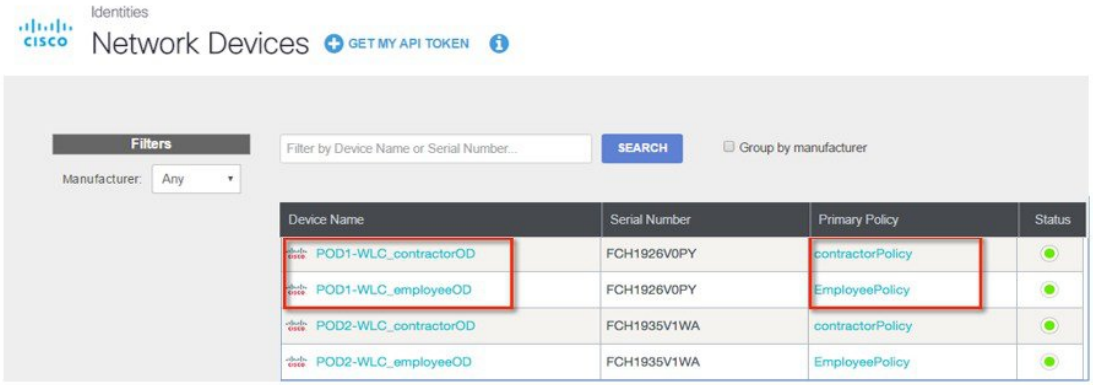
```
(POD1-WLC) >show opendns summary

OpenDnsGlobalStatus.............................. Enabled
OpenDns-ApiToken................................. B45D14F9F272C42BC4998E17EB6ABBCA001EF8B4

  Profile-Name                    Opendns-Identity                              State
  ============                    ================                              ========
  employeeOD                      POD1-WLC_employeeOD                  Profile Registered
  contractorOD                    POD1-WLC_contractorOD                Profile Registered

Profiles Mapped to WLANIDs
==========================

Profile Name                    WLAN IDs (Mapped)
----------------                -----------------
employeeOD                      NONE
contractorOD                    1

Profiles Mapped to APGroup WLAN-IDs
===================================

Profile Name                   Site Name / WLAN IDs (Mapped)
----------------               -----------------------------
employeeOD                     NONE
contractorOD                   NONE

Profiles Mapped to Local Policies
=========================

Profile Name                    Local Policies (Mapped)
----------------                -----------------------
employeeOD                      NONE
contractorOD                    NONE
```

Note Each OpenDNS Profile has a unique **Opendns-Identity** generated on controller (in the format <WLC name>_<profile name>) which will be pushed to the associated OpenDNS account on cloud.

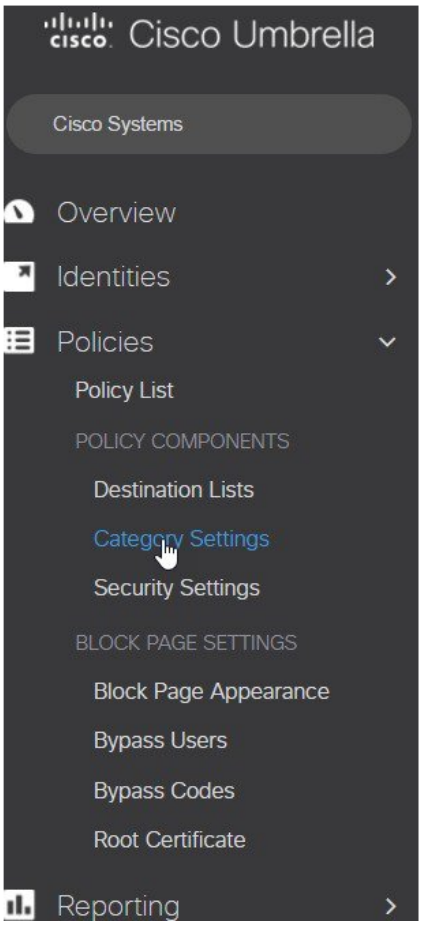
a) From Cisco Umbrella Dashboard, on the left menu, click on **Identities** > **Network Devices**.



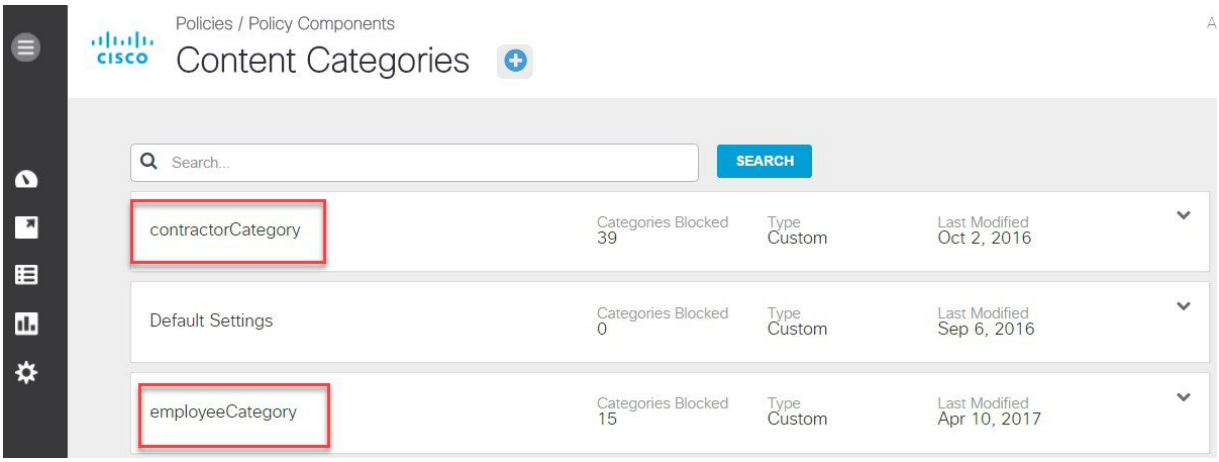
Verify that your WLC with both Identities **employeeOD** and **contractorOD** show up under Device Name.



b) Next, create classification rules for employee and contractor user roles checking which domains should be blocked for both. From the left menu bar, **Policies** > **Category Settings**.

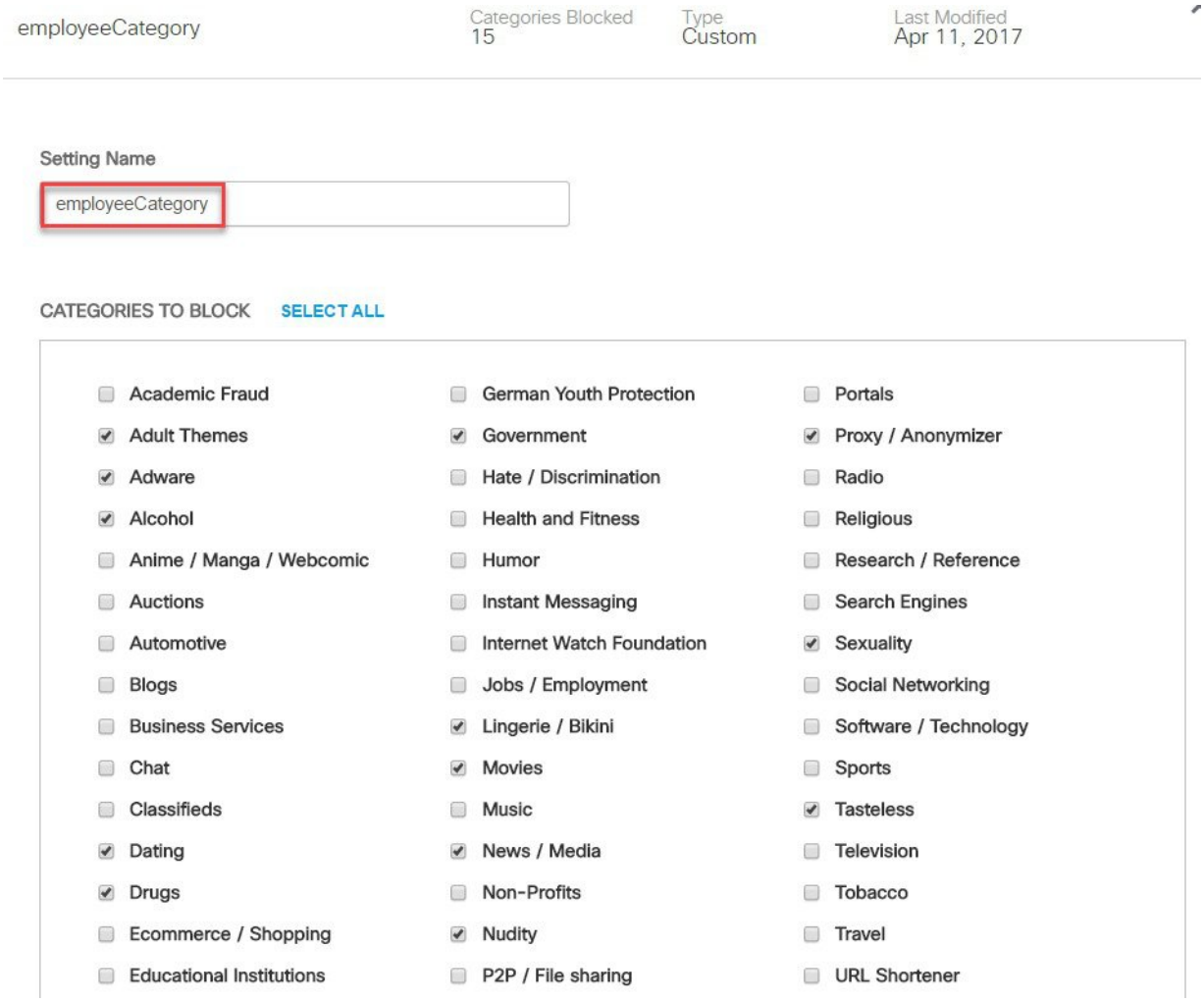


We have created **employeeCategory** and **contractorCategory** for this exercise.

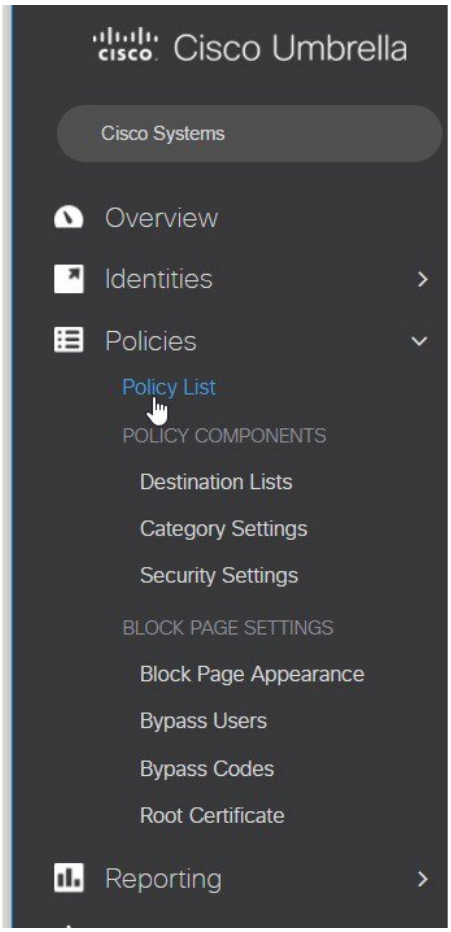


The **employeeCategory** is restricting certain sites categories, example: Adult theme, Adware, Gambling. Similarly, **contractorCategory** is restricting more content, example: Adult theme, Adware, Gambling, Games, News, Social Networking.

Click on **employeeCategory** to view the blocked categories. You can edit the list to add/remove categories.

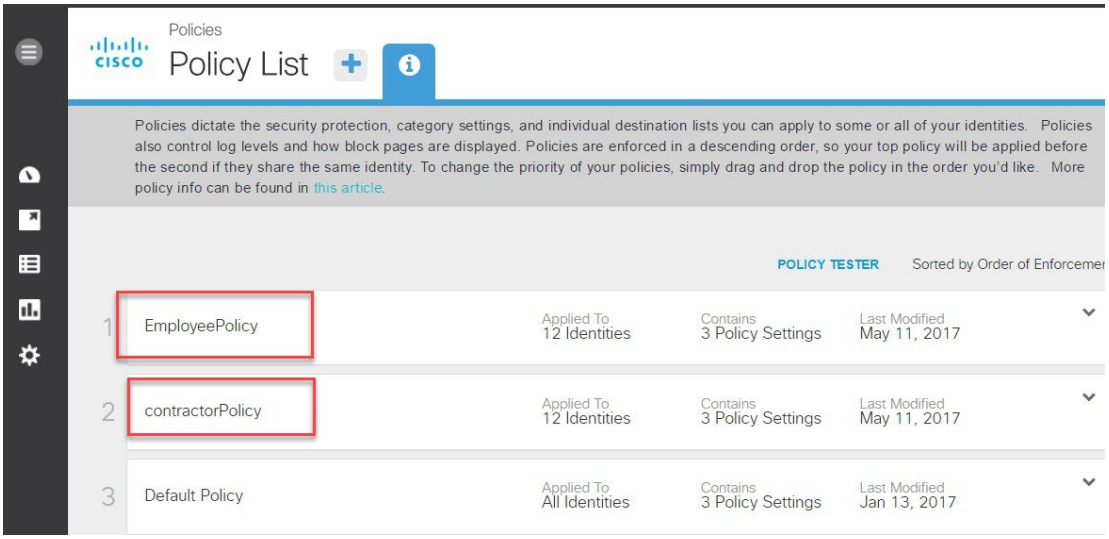


Step 9 Finally, create and configure two Policies on the Cisco Umbrella server. From the left menu bar, browse to **Policies** > **Policy List**.

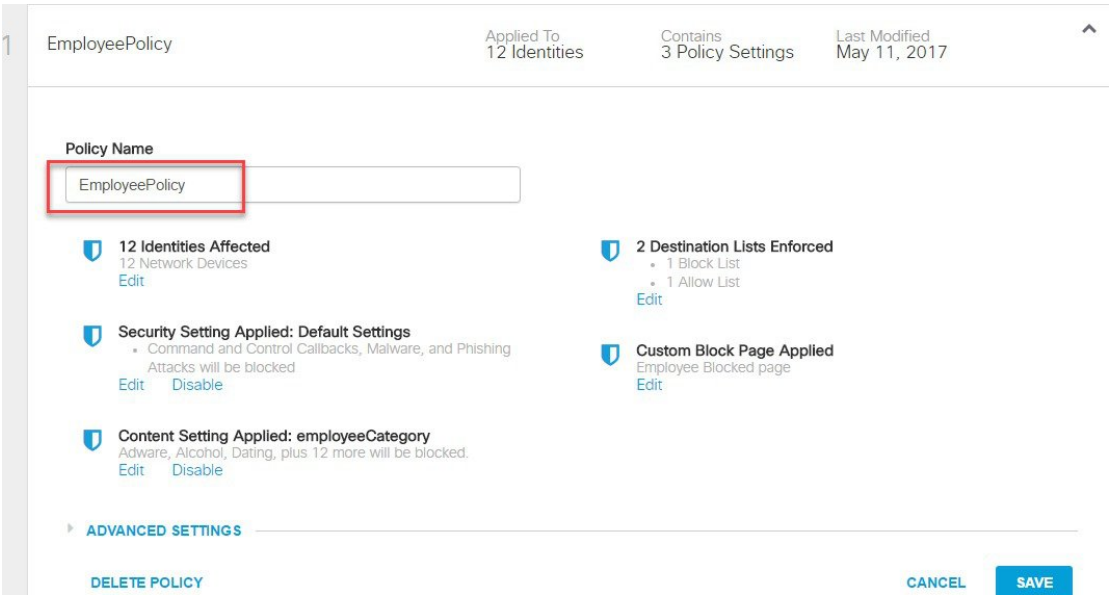


We have created these two policies:

1. EmployeePolicy
2. Contractor Policy

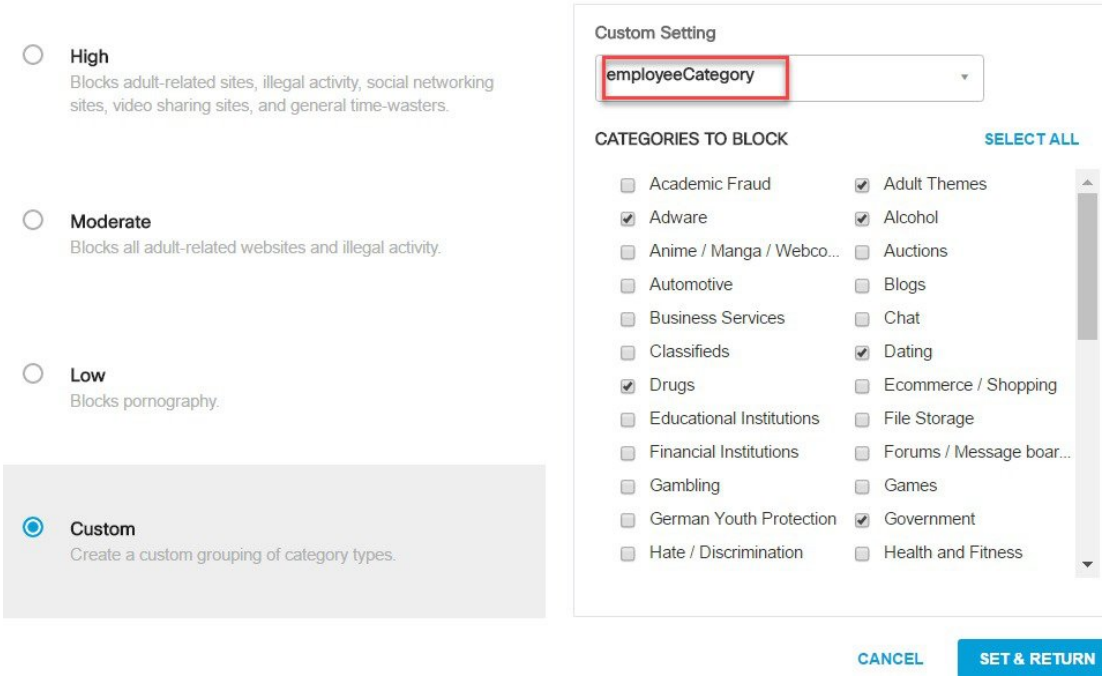


A Policy Wizard exists under each Policy screen showing Identities affected and the mapped category setting. Here, **EmployeePolicy** is assigned to **employeeOD** Identity and tied to a category**employeeCategory** (created in the last step). Similarly, **contractorPolicy** is assigned to **contractorOD** Identity and tied to a custom category **contractorCategory** created earlier.



Click on **Edit** under **Identities Affected** to see all the identities/network devices (PodX-WLC_employeeOD) mapped to this Policy.

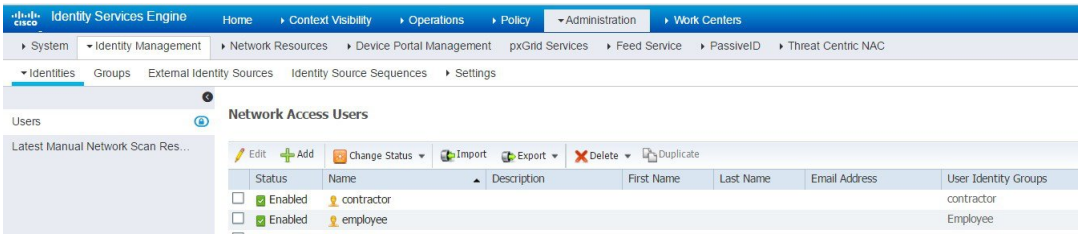
Click **SET & RETURN** and go to **Content Setting Applied** to verify category setting applied to this Policy as shown below.



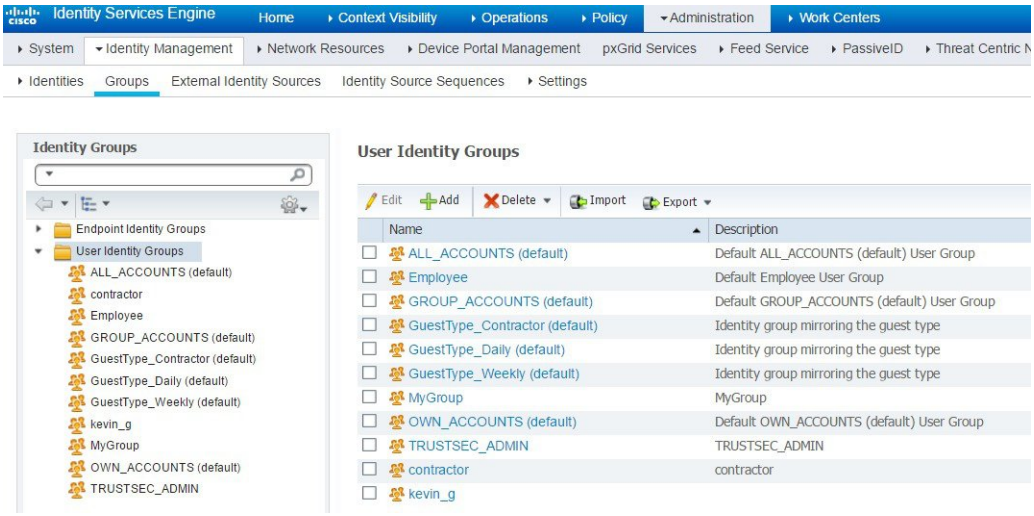
Step 10 Configuring User Roles on ISE.

a) Configure the AAA server or ISE to allow users to be 802.1x authenticated and have the AAA server send the ROLE string back to the wireless controller for local policy enforcement.

As illustrated below, on ISE, configure users, that is, employee and contractor and groups, that is, group **employee** and **contractor**.

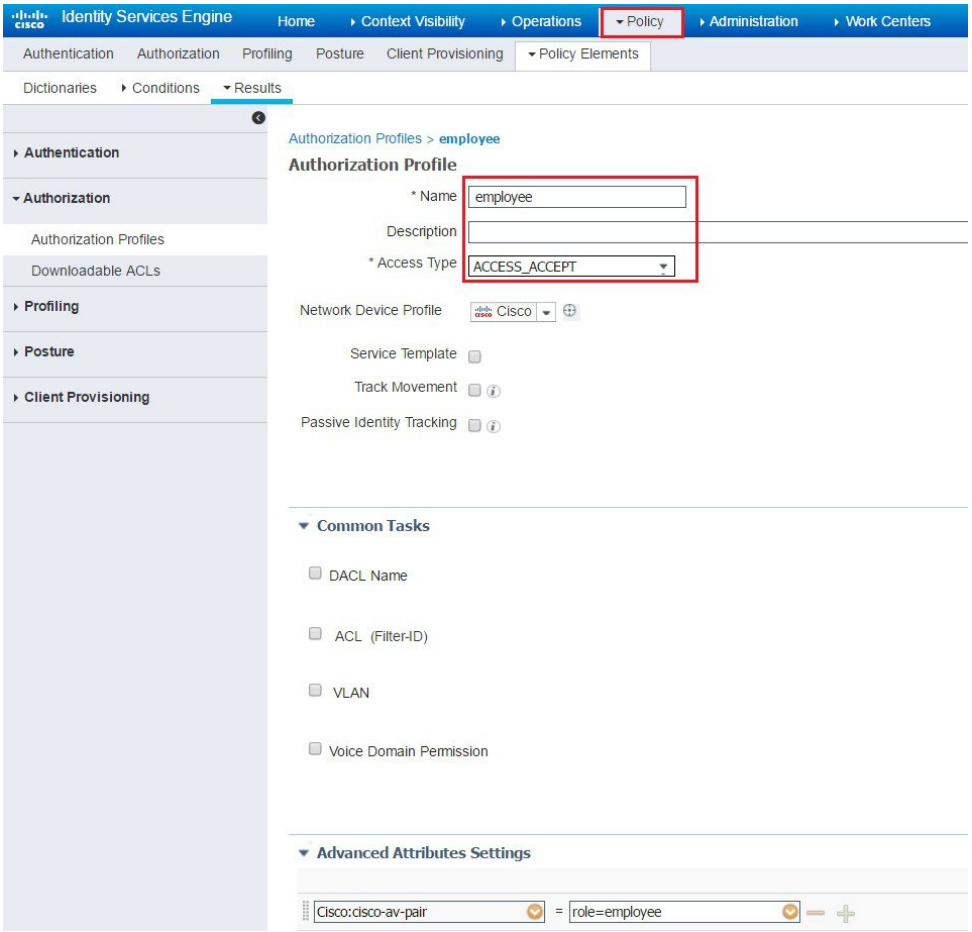


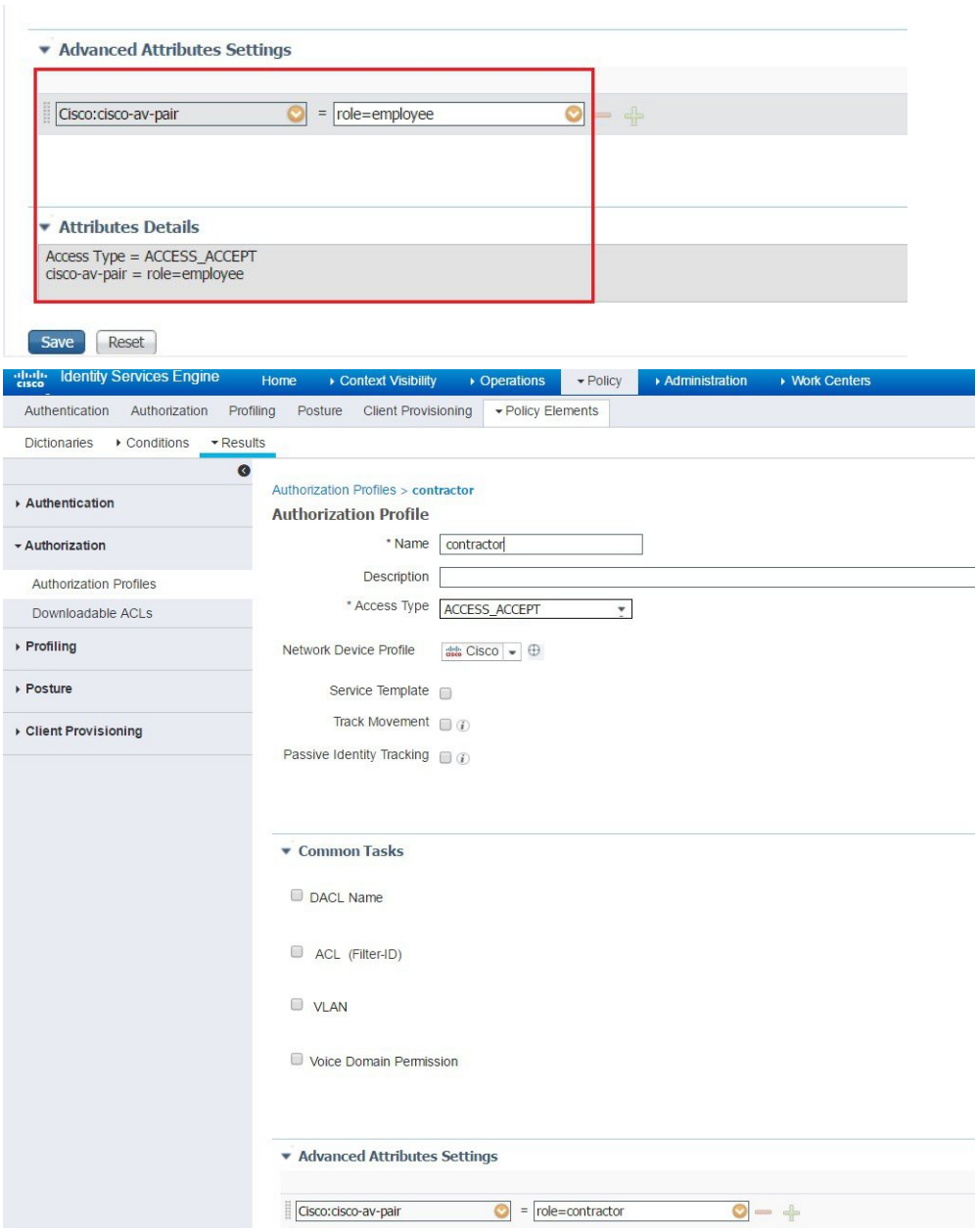
b) Next, configure groups, that is, group Employee and contractor.



Note In this section on ISE, we are testing with ISE internal users. If ISE is pointing to an external user database like Active Directory, the rule would change pointing to the respective user AD group.

c) Create an ISE policy for a specific group of users with a desired role, that is, **employee** or **contractor**.




Advanced Attributes Settings
Cisco:cisco-av-pair
=
role=employee
Attributes Details
Access Type = ACCESS_ACCEPT
cisco-av-pair = role=employee
Save
Reset
Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Authentication
Authorization
Profiling
Posture
Client Provisioning
Policy Elements
Dictionaries
Conditions
Results
Authentication
Authorization
Authorization Profiles
Downloadable ACLs
Profiling
Posture
Client Provisioning
Authorization Profiles > contractor
Authorization Profile
* Name
contractor
Description
* Access Type
ACCESS_ACCEPT
Network Device Profile
Cisco
Service Template
Track Movement
Passive Identity Tracking
Common Tasks
DACL Name
ACL (Filter-ID)
VLAN
Voice Domain Permission
Advanced Attributes Settings
Cisco:cisco-av-pair
=
role=contractor

At this point, it is assumed that administrator has configured the necessary authentication rules on ISE/AAA server for wireless users to return **Authorization Profiles** including access type (accept/reject) and user role (employee/contractor) as shown above.

Step 11 Configuring Local Policies for OpenDNS.

User can now configure user role based Local Policy and tie the Cisco Umbrella profile to it. Finally, map the local policy to a particular WLAN.

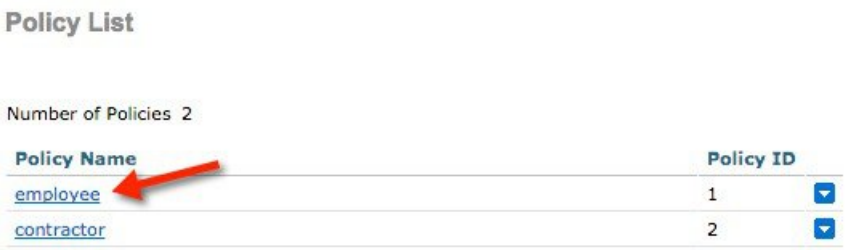
a) Now create two local polices for employee and contractors on the WLC.

From WLC main menu go to **Security** > **Local Policies** then click **New**.

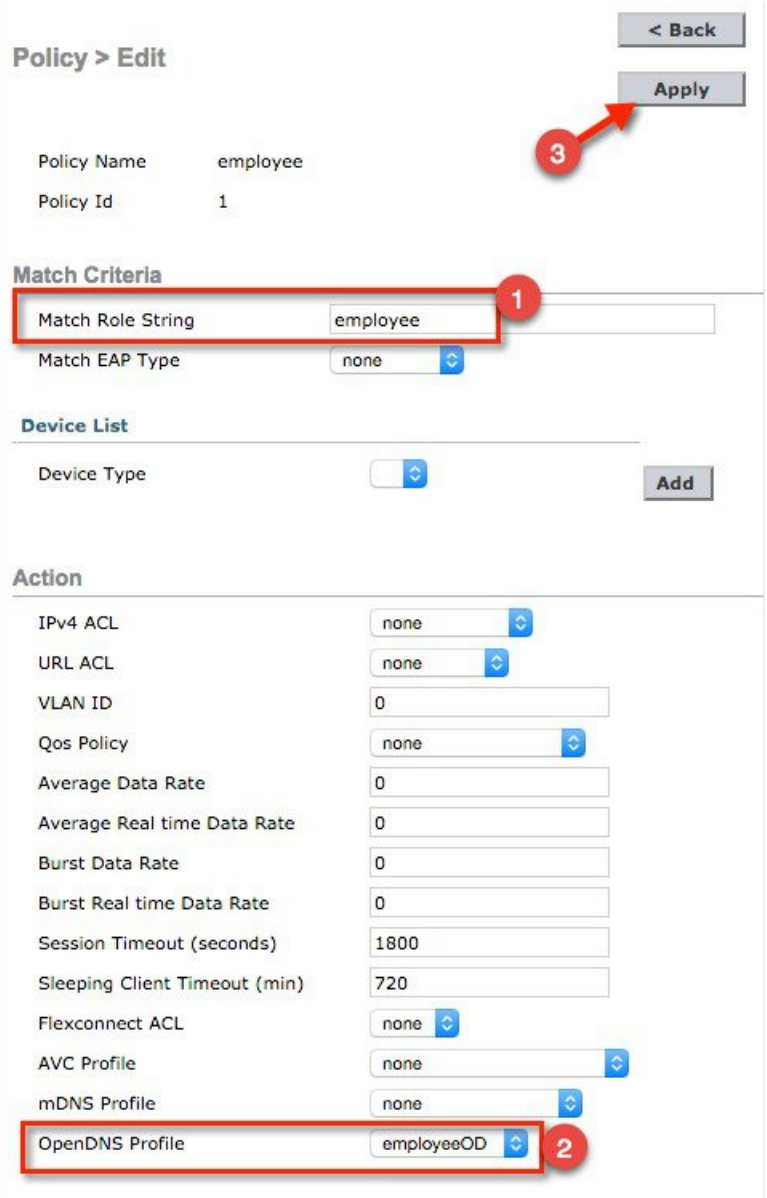
Create Local Policy name as "**employee**" and "**contractor**" and click **Apply**.

Similarly, create another one for contractor.

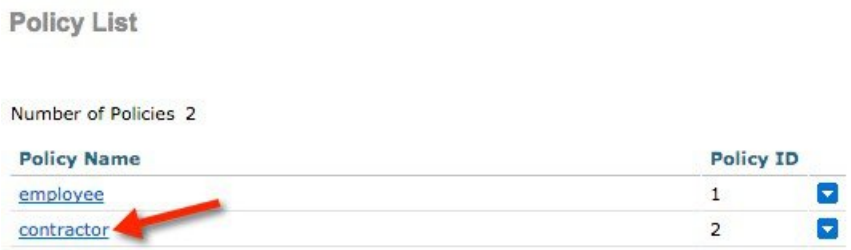
b) Click on the **employee** Local Policy and configure it with employee OpenDNS profile (**employeeOD**)



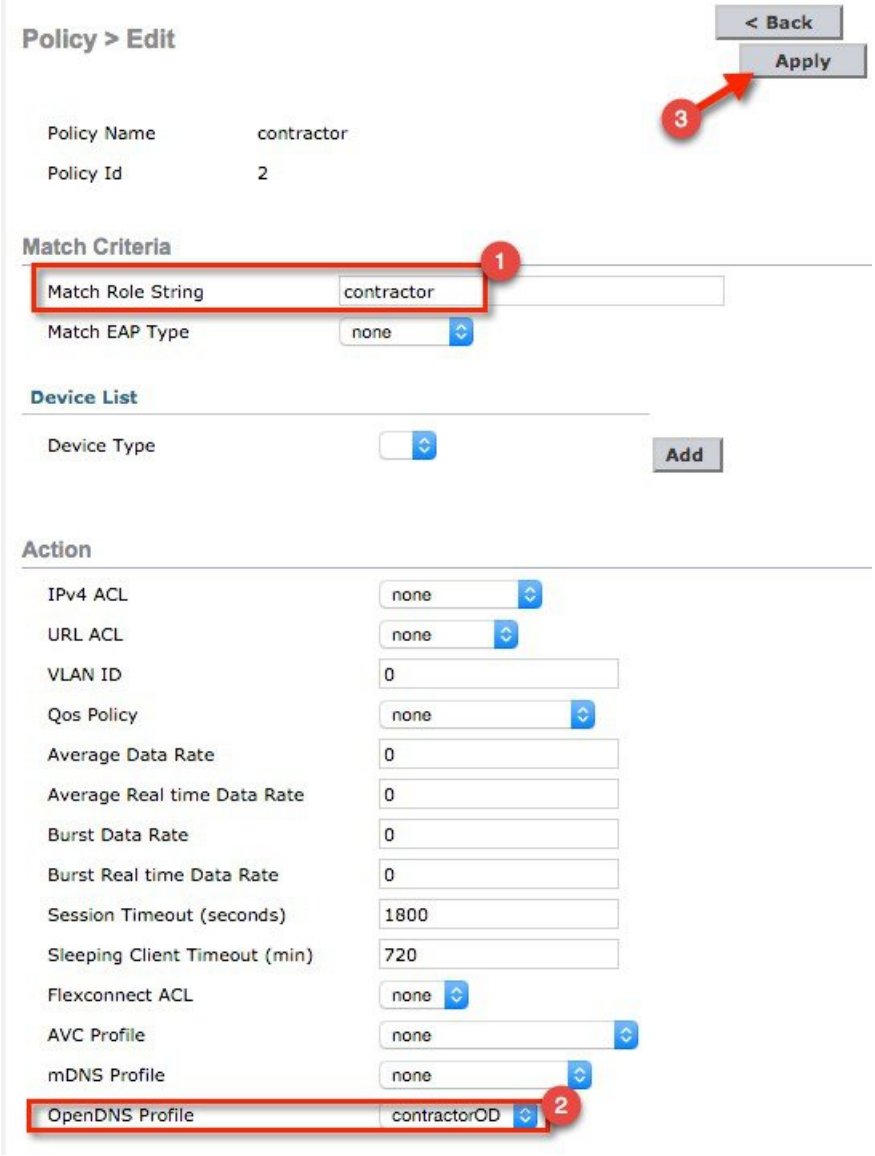
c) Under **Match** Criteria configure **Match Role String** as "**employee**" and under the **Action** list go to **Cisco Umbrella Profile**. From the dropdown list select "**employeeOD** then click **Apply**.



d) Now click **Back** to go to the Local Policy page then click on **contractor** policy.



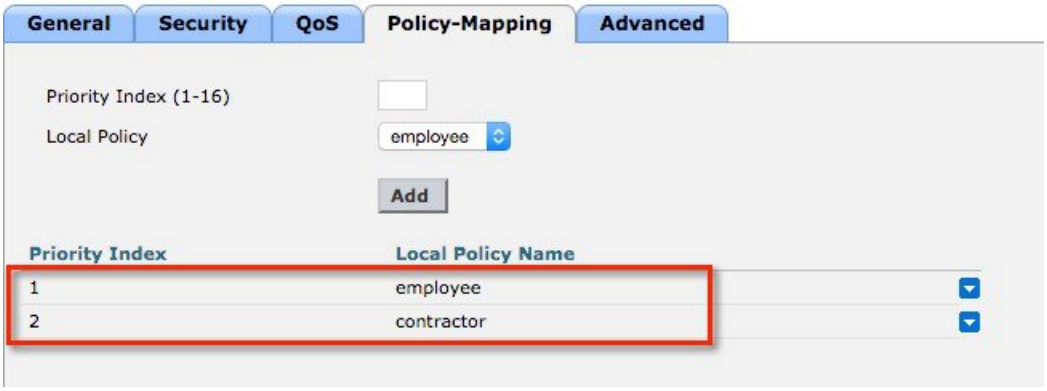
Under **Match** Criteria configure **Match Role String** as "**contractor**" and under the **Action** list select **OpenDNS profile** for contractor from the dropdown select "**contractorOD**" then click **Apply**.



Step 12 Configuring OpenDNS on WLAN.

a) From WLC main menu navigate to **WLAN** > **WLAN ID** >**Policy-Mapping**. Assign **Priority Index 1** and Select **employee** from the Local Policy dropdown menu Click **Add**.

Similarly, apply the contractor policy to the WLAN.



As a result,a user logging in with employee credentials will be associated with "**role = employee**"and will be inherit employee OpenDNSprofile (**employeeOD**) on the WLC. Similarly,a user logging in contractor credentials will be associated with "**role = contractor**" and will be inherit contractor OpenDNS profile(**contractorOD**) on the WLC.

b) For the WLC to redirect all DNS for a WLAN to the Cisco Umbrella DNS server, the **openDNS Mode** must be set to **Forced** as shown below. This is done by going to **WLAN** > **Advanced**.

c) Verify

1. Connect a client to your WLAN with employee user credentials
2. Try accessing sites that are blocked under the category filtering rules you created for employee. For blocked sites, client will get a display page stating the site/domain is restricted

3. Try to associate to the same WLAN using contractor user credentials and repeat the test. You will notice the difference in browsing access granted to an employee versus a contractor

Scenario: 2 Configuring WLAN/AP Group for Cisco Umbrella

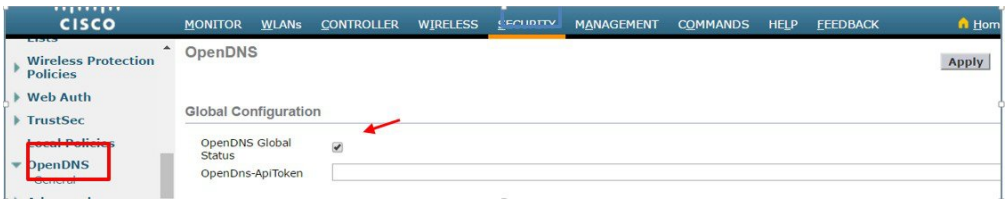
Similar to Local Policy, OpenDNS profile can be attached to a WLAN or to an AP group. Section below shows screenshots from GUI and CLI commands on how to tie OpenDNS profile to a WLAN and AP group. It is assumed that the Cisco Umbrella account is already created and API token is copied from the Umbrella dashboard.

Procedure

Step 1 From WLC main menu, go to **Controller** >**General** and enter a **DNS Server IP** address that can resolve domains. This is needed for the first time before enabling Cisco Umbrella feature on the WLC.


```
CLI command: config OpenDNS  server-ipv4 primary <primary-server> secondary <secondary-server>
```

Step 2 Enable openDNS globally on WLC by going to **Security**> **OpenDNS** >**General**.

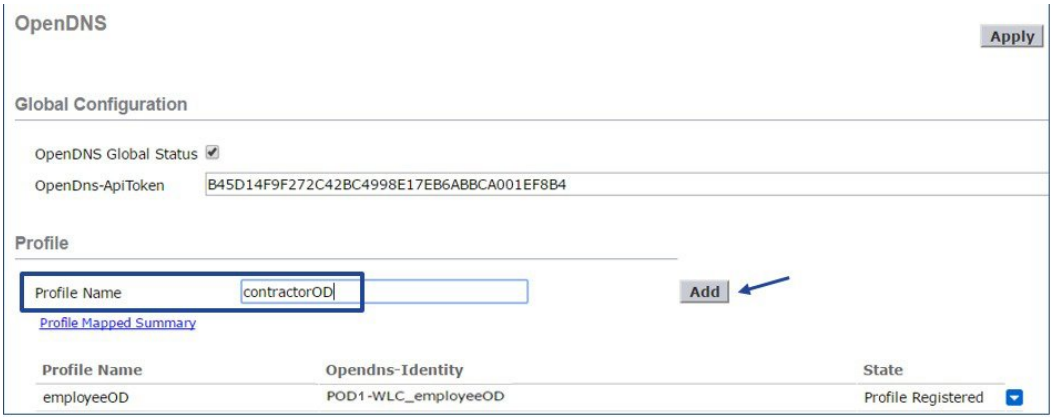



```
CLI command: config Cisco Umbrella  enable
```

Step 3 Configure API Token obtained from Cisco Umbrella account.


```
CLI command: config Cisco Umbrella  api-token <token>
```

Step 4 Create OpenDNS Profiles .




```
CLI command:config Cisco Umbrella  profile create <profile-name>
```

Step 5 Map the Profile to WLAN or AP group.

a) To tie the OpenDNS profile to a WLAN, go to **WLANs**> **WLAN Id**>**Advanced** and under **OpenDNS profile** select **contractorOD** profile we created above.

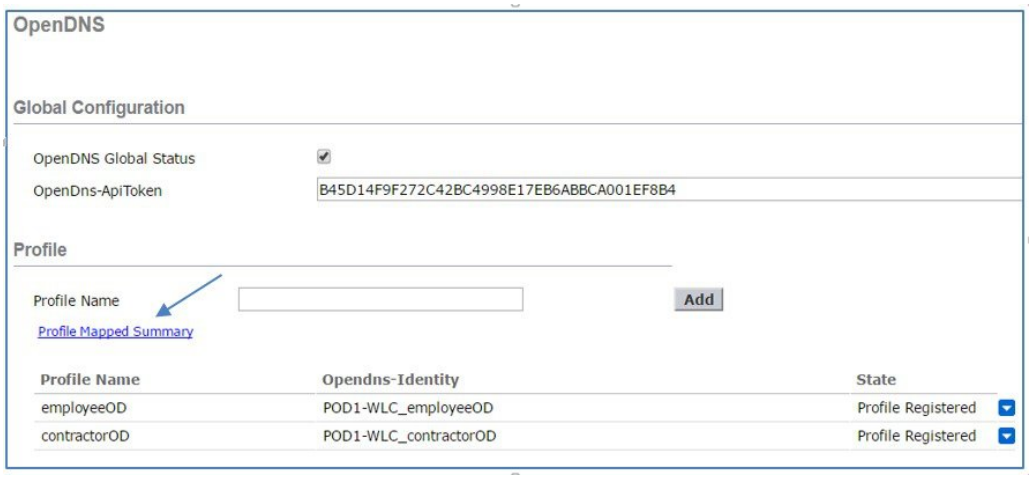

```
CLI command: config wlan opeDNS-profile <wlan-id> <profile name> enable
```

b) To map the Profile to AP Group, go to **WLANs**> **Advanced**> **AP Groups**. Select the AP group you want and go to **WLANs** tab. Hover the mouse over the blue button on the right and select **OpenDNS Profile**.

In the screenshot below, we selected AP Group **APgrp1** and mapped **contractorOD** Cisco Umbrella profile to **WLAN 1**.

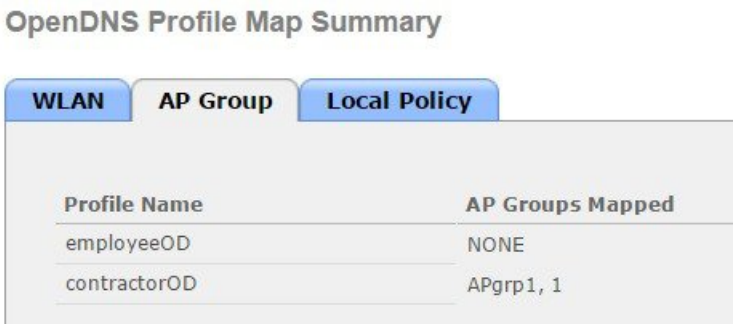

```
CLI command:config wlan apgroup Cisco Umbrella -profile <wlan-id> <site-name> <profile-name> enable
```

To view OpenDNS mapping, go to **Security** > **OpenDNS** > **General** and click on Profile Mapped Summary as shown:



Here, the OpenDNS Profile contractorOD is mapped WLAN ID 1.

On the same**OpenDNS Profile Map Summary** page, under AP Group, profile **contractorOD** is also mapped to AP Group **APgrp1** as shown

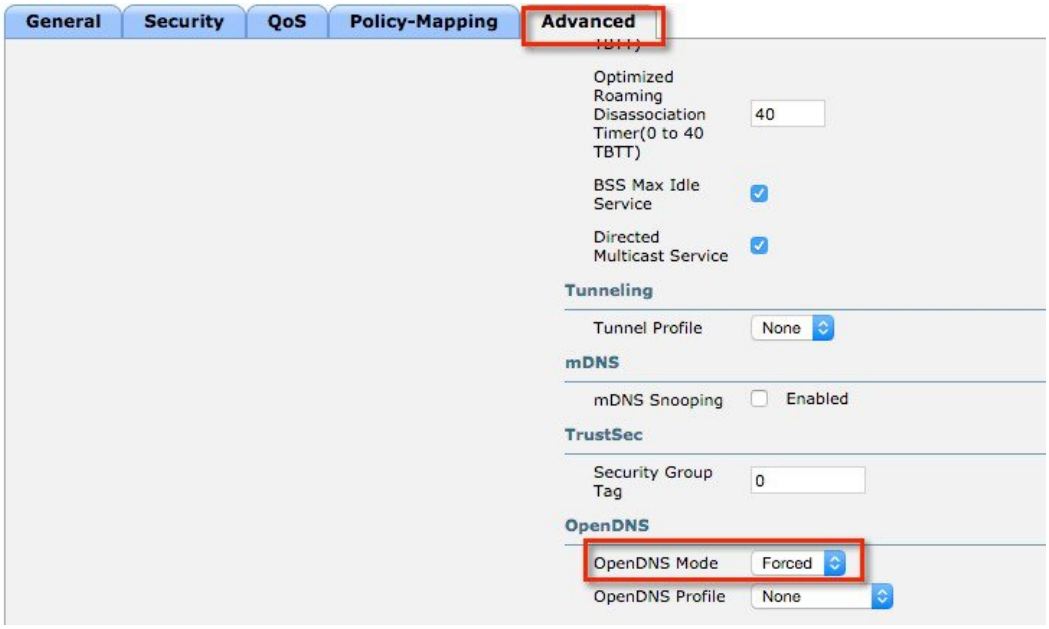


From CLI

```
(POD2-WLC) >show opendns summary

OpenDnsGlobalStatus.............................. Enabled
OpenDns-ApiToken................................. B45D14F9F272C42BC4998E17EB6ABBCA001EF8B4

  Profile-Name                    Opendns-Identity                              State
  ============                    ================                              ========
  employeeOD                      POD2-WLC_employeeOD                  Profile Registered
  contractorOD                    POD2-WLC_contractorOD                Profile Registered

Profiles Mapped to WLANIDs
==========================

Profile Name                    WLAN IDs (Mapped)
----------------                -----------------
employeeOD                      NONE
contractorOD                    1

Profiles Mapped to APGroup WLAN-IDs
===================================

Profile Name                   Site Name / WLAN IDs (Mapped)
----------------                -----------------
employeeOD                      NONE
contractorOD                    APgrp1, 1

Profiles Mapped to Local Policies
=========================

Profile Name                    Local Policies (Mapped)
----------------                -----------------
employeeOD                      NONE
contractorOD                    NONE
```

OpenDNS WLAN configuration modes

Administrator can configure OpenDNS on a WLAN in three modes under WLAN advanced tab.



1. **DHCP Proxy for DNS override**

   Interface level config. Part of DHCP process to propagate OpenDNS ip address to all WLANs associated to Interface. Happens in the client join phase.

2. **OpenDNS Force mode: (Enabled by default)**

   Enforced per WLAN, blocks intentional client activity after client has associated to WLAN.

Note

1. If the client device has DNS for any IP address other than opendns ip's this option will cause the client traffic to be blackholed.
2. WLC does not do a proxy in force mode but will simply re-direct all the DNS packets to OpenDNS only , so the reply to the client is received from opendns ip only. Client who do not have opendns ip as one of configured DNS IP can reject this causing connectivity issues.

   Adding opendns as one of the DNS IP will help in some of these cases.

WLC does not do a proxy in force mode but will simply re-direct all the DNS packets to OpenDNS only , so the reply to the client is received from opendns ip only

If DNS ip change by user is to be allowed , we should use OpenDNS Ignore mode .

3. **OpenDNS Ignore mode**

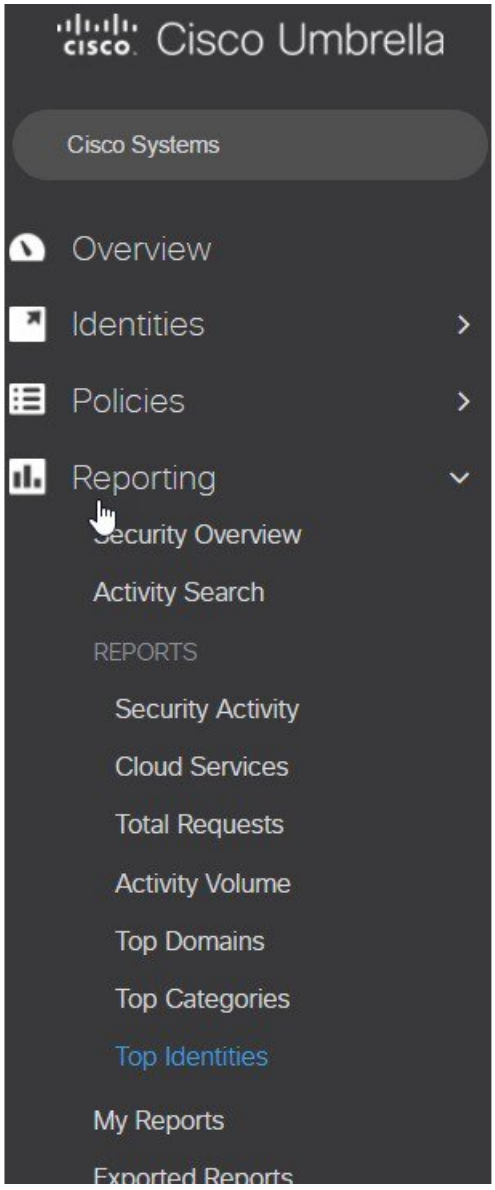
   WLC honors the DNS server used by the client; it could be Cisco Umbrella cloud servers or enterprise/ external DNS

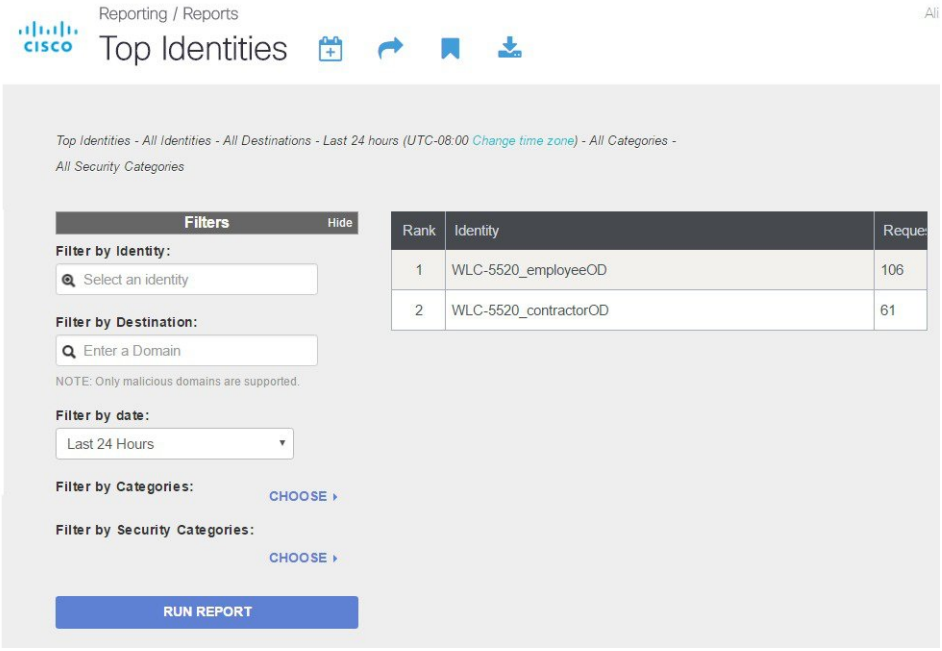
4. **OpenDNS Copy mode (not included in 8.4 release)**

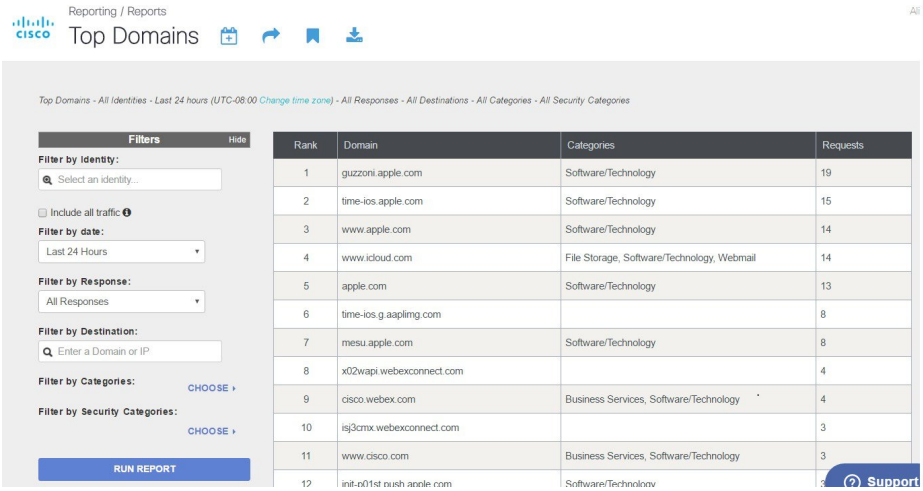
   A copy of OpenDNS packets where all internet bound DNS traffic is forwarded to Cisco Umbrella cloud servers without any policy options (no block/redirect)

Cisco Umbrella Activity Reporting

Administrator can login to Cisco Umbrella server to view and generate reports regarding the clients activity, find the infected devices, targeted users trying to access forbidden sites. These reports can be filtered by client identity, destination and source IP. Reporting may take up to 2 hours to appear after a new identity is registered.







OpenDNS Support

- WLC supported platform- 5508,5520,7500,8510,8540. ME, vWLC is not supported
- AP mode supported–Local mode, Flex central switching.
- 10 different OpenDNS Profiles configurable on WLC
- Guest (Foreign–Anchor) scenario, profile applies at Anchor WLC

OpenDNS Limitations

- Client is connected to a web proxy and does not send DNS query to resolve the server address
- Application or host uses IP address directly instead of DNS to query domains

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.