



Cisco Umbrella WLAN Integration Guide

Introduction	2
Pre-requisite	2
Components Used	2
Conventions	2
Feature Introduction	2
Cisco Umbrella General Work Flow	3
Configuring the Cisco Umbrella Wireless LAN Controller Integration	4
OpenDNS WLAN configuration modes	25
Cisco Umbrella Activity Reporting	27
OpenDNS Support	28
OpenDNS Limitations	29

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 document was created from 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, make sure that you understand the potential impact of any command.

Conventions

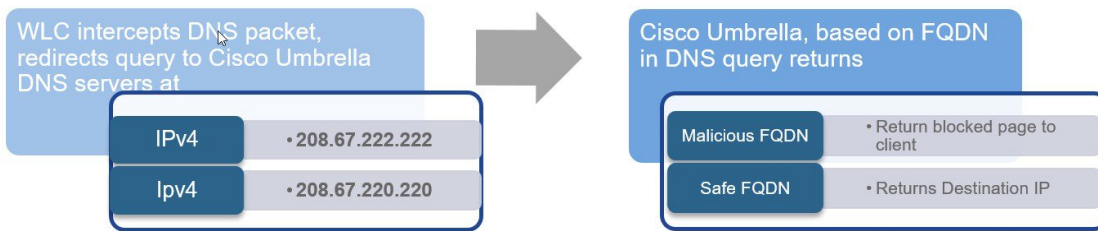
Refer to Cisco Technical Tips Conventions for more information on document conventions.

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.

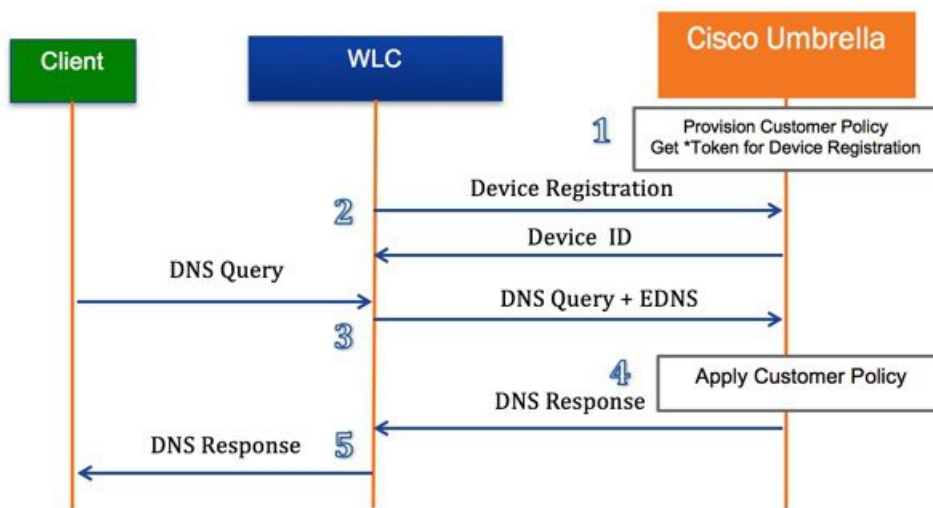
Terminology involved in the working of the feature:

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

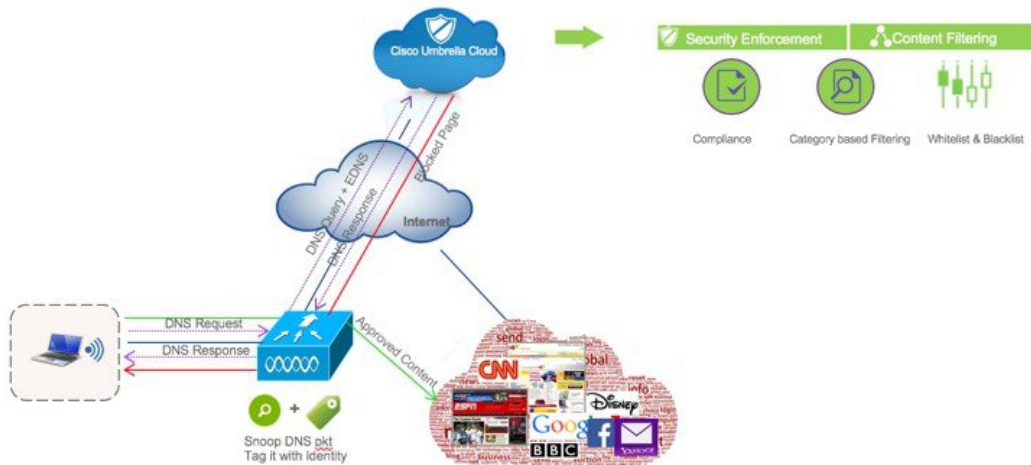


DNS request always precedes web request. Wireless Lan Controller intercepts DNS request from the client and redirects the query to Cisco Umbrella in the cloud (208.67.222.222, 208.67.220.220). Cisco Umbrella servers resolve the DNS query and enforces preconfigured security filtering rules on a per identity 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 offers 14 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/>

14 Day Free Trial of Cisco Umbrella

Get started in 30 seconds

No credit card or phone call required

WHAT IS INCLUDED?

- ✔ Threat protection like no other – block malware, C2 callbacks, and phishing.
- ✔ Predictive Intelligence – automates threat protection to detect attacks before they are launched.
- ✔ Worldwide Coverage, Fast – no hardware to install or software to maintain.
- ✔ Weekly security report – get a personalized summary of malware requests & more, directly to your inbox.

All fields are required

First name

Last name

Company Email

Company Phone

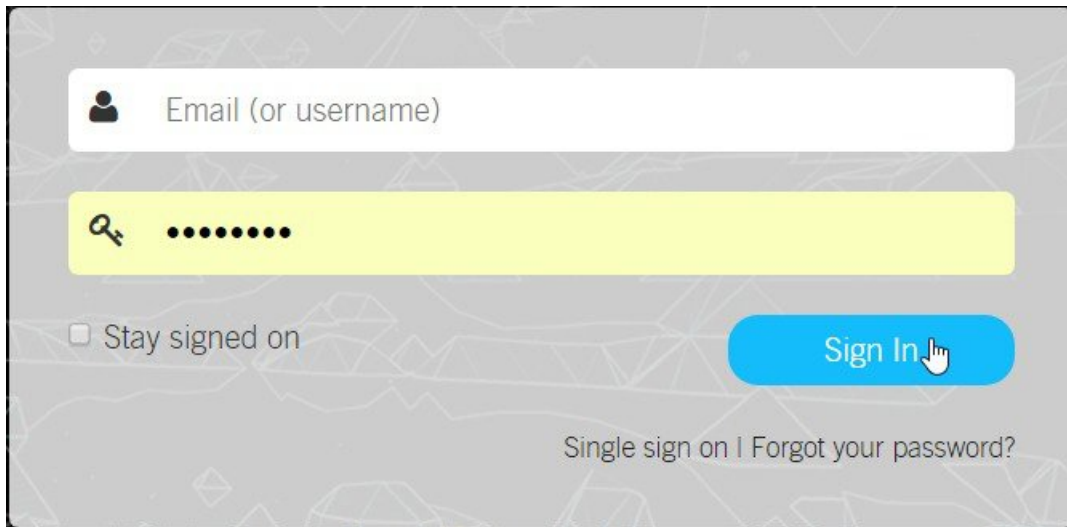
Company Name

Select your country

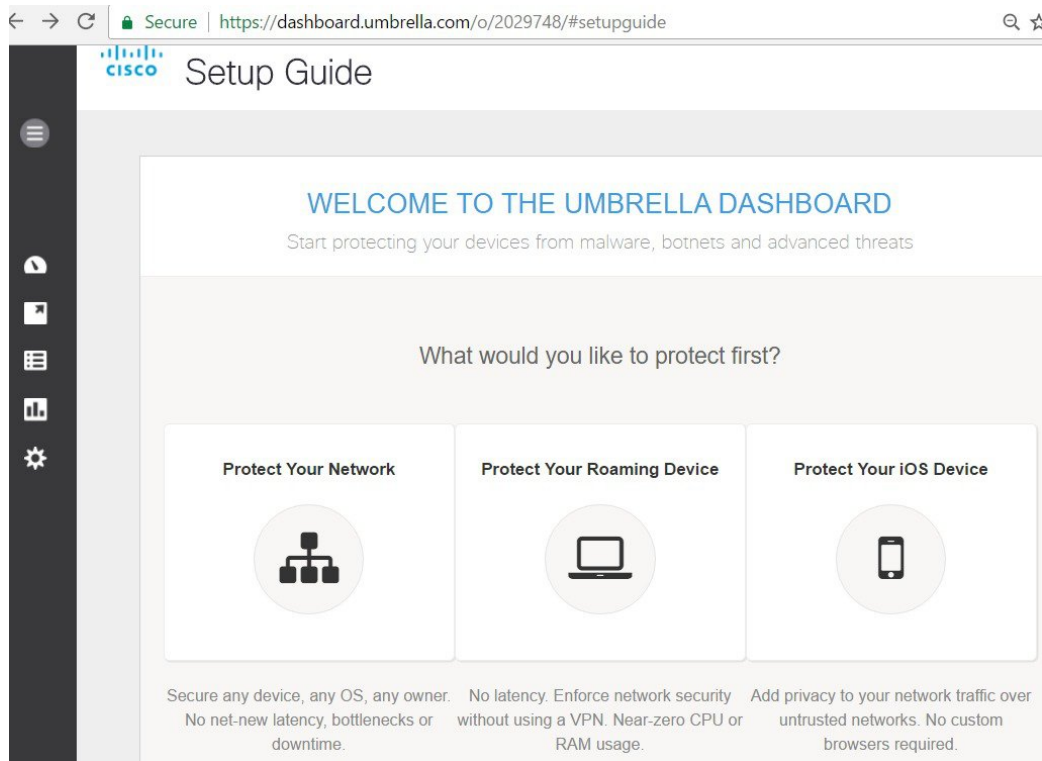
Are you an MSP, IT services provider or reseller? No

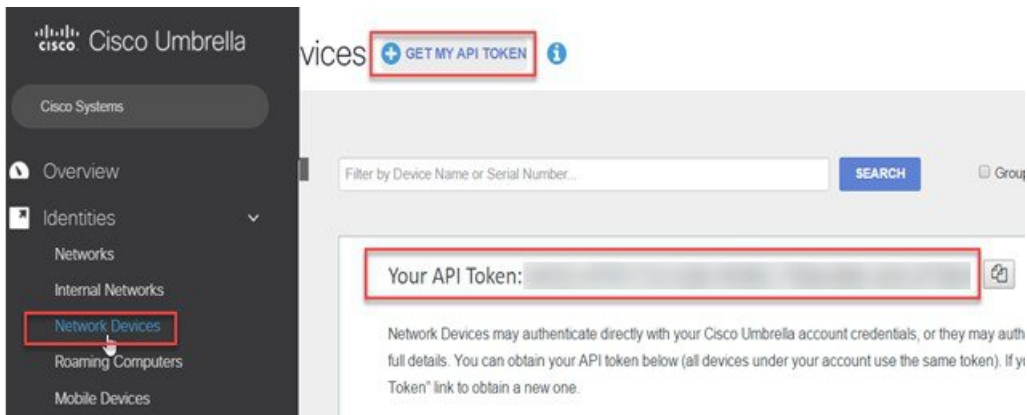
CREATE MY TRIAL

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**.

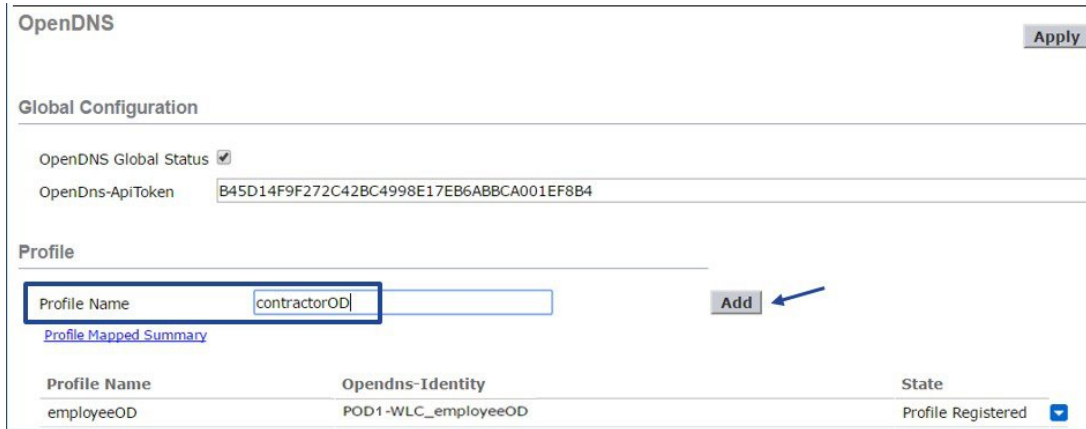


CLI command: `config Cisco Umbrella enable`

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

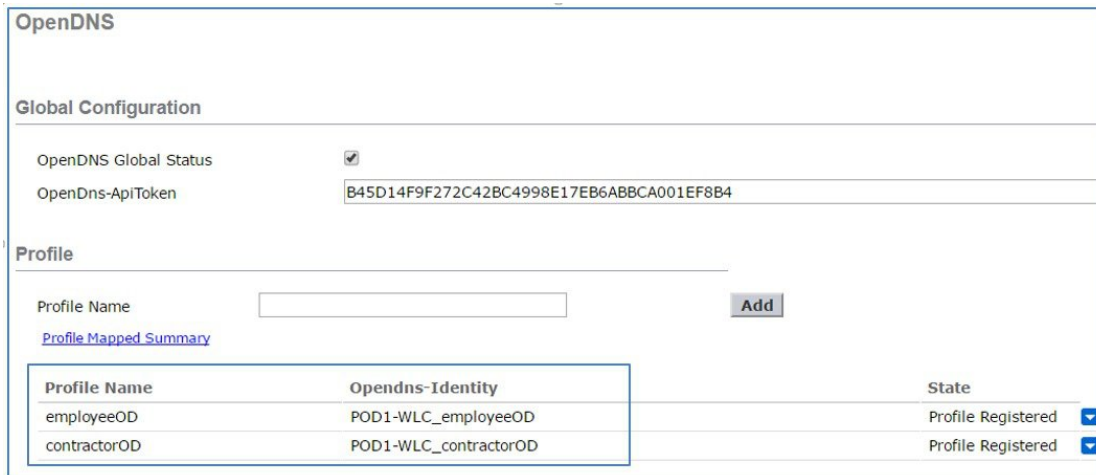


Step 7 From the same page, create OpenDNSProfiles **Security > OpenDNS >General**.



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

Step 8 On WLC, create two OpenDNS profiles, one for employee(**employeeOD**) and another for contractor (**contractorOD**) via CLI or GUI. These profiles should automatically be pushed to your OpenDNS account as **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

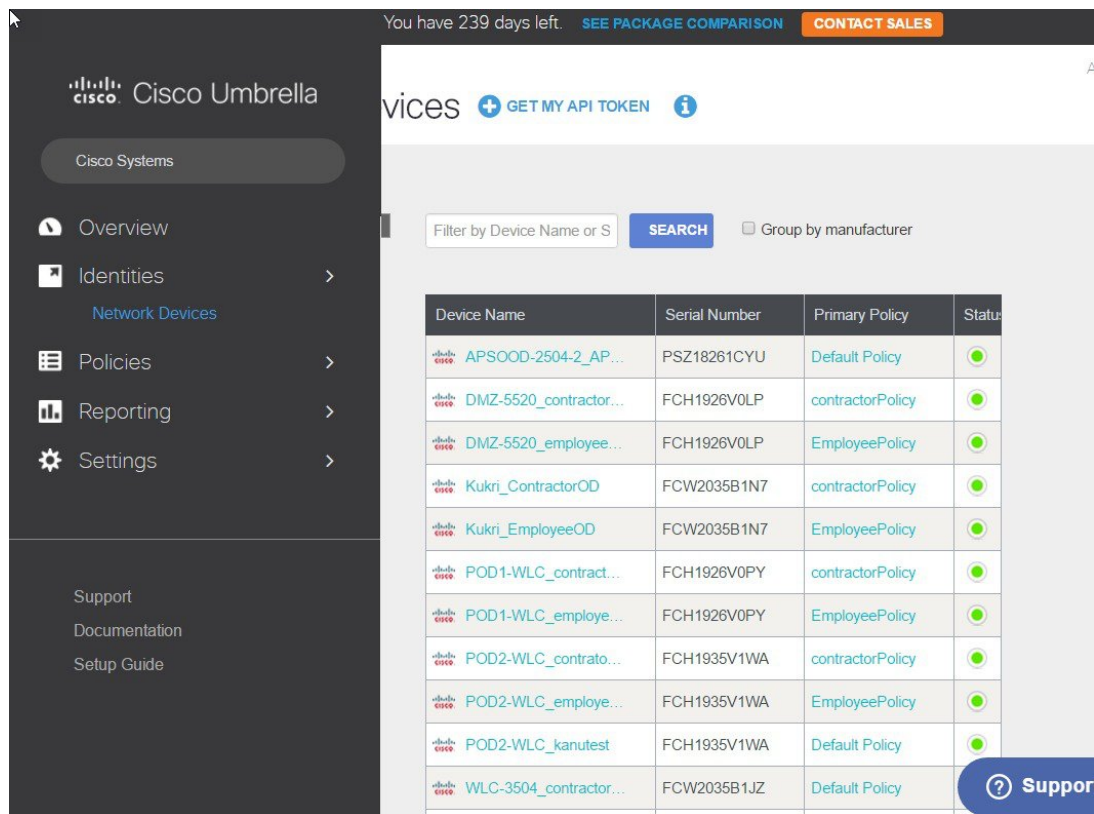
Profiles Mapped to APGroup WLAN-IDs
=====
Profile Name                Site Name / WLAN IDs <Mapped>
-----
employeeOD                  NONE
contractorOD                NONE

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**.



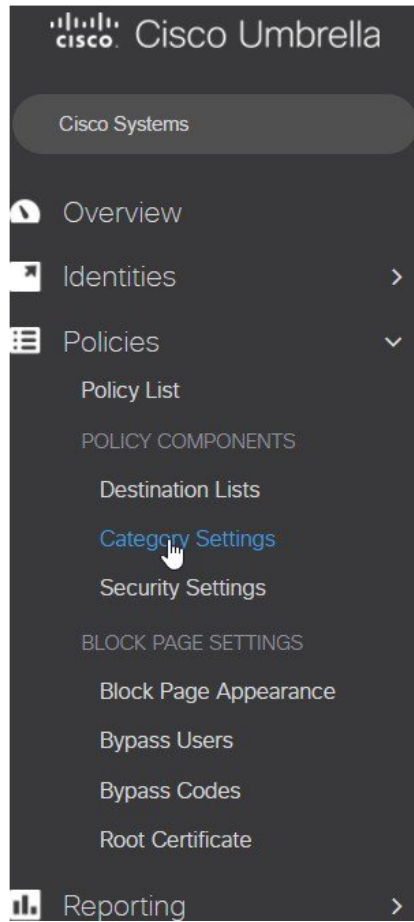
Verify that your WLC with both Identities **employeeOD** and **contractorOD** show up under Device Name.

Identities
 Network Devices [GET MY API TOKEN](#) [i](#)

Filters
 Filter by Device Name or Serial Number... [SEARCH](#) Group by manufacturer
 Manufacturer: Any

Device Name	Serial Number	Primary Policy	Status
POD1-WLC_contractorOD	FCH1926V0PY	contractorPolicy	●
POD1-WLC_employeeOD	FCH1926V0PY	EmployeePolicy	●
POD2-WLC_contractorOD	FCH1935V1WA	contractorPolicy	●
POD2-WLC_employeeOD	FCH1935V1WA	EmployeePolicy	●

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.

Policies / Policy Components A

Content Categories +

SEARCH

contractorCategory	Categories Blocked 39	Type Custom	Last Modified Oct 2, 2016	▼
Default Settings	Categories Blocked 0	Type Custom	Last Modified Sep 6, 2016	▼
employeeCategory	Categories Blocked 15	Type Custom	Last Modified Apr 10, 2017	▼

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.

employeeCategory

Categories Blocked
15

Type
Custom

Last Modified
Apr 11, 2017

Setting Name

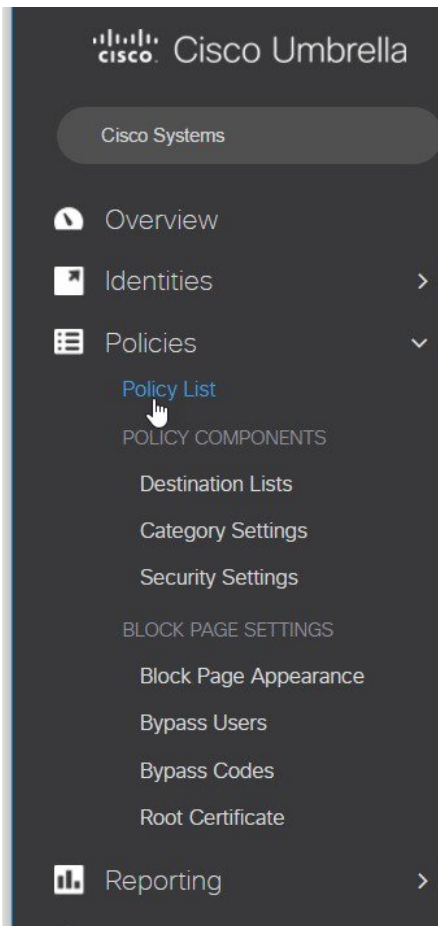
employeeCategory

CATEGORIES TO BLOCK [SELECT ALL](#)

- | | | |
|---|---|--|
| <input type="checkbox"/> Academic Fraud | <input type="checkbox"/> German Youth Protection | <input type="checkbox"/> Portals |
| <input checked="" type="checkbox"/> Adult Themes | <input checked="" type="checkbox"/> Government | <input checked="" type="checkbox"/> Proxy / Anonymizer |
| <input checked="" type="checkbox"/> Adware | <input type="checkbox"/> Hate / Discrimination | <input type="checkbox"/> Radio |
| <input checked="" type="checkbox"/> Alcohol | <input type="checkbox"/> Health and Fitness | <input type="checkbox"/> Religious |
| <input type="checkbox"/> Anime / Manga / Webcomic | <input type="checkbox"/> Humor | <input type="checkbox"/> Research / Reference |
| <input type="checkbox"/> Auctions | <input type="checkbox"/> Instant Messaging | <input type="checkbox"/> Search Engines |
| <input type="checkbox"/> Automotive | <input type="checkbox"/> Internet Watch Foundation | <input checked="" type="checkbox"/> Sexuality |
| <input type="checkbox"/> Blogs | <input type="checkbox"/> Jobs / Employment | <input type="checkbox"/> Social Networking |
| <input type="checkbox"/> Business Services | <input checked="" type="checkbox"/> Lingerie / Bikini | <input type="checkbox"/> Software / Technology |
| <input type="checkbox"/> Chat | <input checked="" type="checkbox"/> Movies | <input type="checkbox"/> Sports |
| <input type="checkbox"/> Classifieds | <input type="checkbox"/> Music | <input checked="" type="checkbox"/> Tasteless |
| <input checked="" type="checkbox"/> Dating | <input checked="" type="checkbox"/> News / Media | <input type="checkbox"/> Television |
| <input checked="" type="checkbox"/> Drugs | <input type="checkbox"/> Non-Profits | <input type="checkbox"/> Tobacco |
| <input type="checkbox"/> Ecommerce / Shopping | <input checked="" type="checkbox"/> Nudity | <input type="checkbox"/> Travel |
| <input type="checkbox"/> Educational Institutions | <input type="checkbox"/> P2P / File sharing | <input type="checkbox"/> URL Shortener |

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

Policies

Policy List

Policies dictate the security protection, category settings, and individual destination lists you can apply to some or all of your identities. Policies also control log levels and how block pages are displayed. Policies are enforced in a descending order, so your top policy will be applied before the second if they share the same identity. To change the priority of your policies, simply drag and drop the policy in the order you'd like. More policy info can be found in [this article](#).

POLICY TESTER Sorted by Order of Enforcement

1	EmployeePolicy	Applied To 12 Identities	Contains 3 Policy Settings	Last Modified May 11, 2017	▼
2	contractorPolicy	Applied To 12 Identities	Contains 3 Policy Settings	Last Modified May 11, 2017	▼
3	Default Policy	Applied To All Identities	Contains 3 Policy Settings	Last Modified Jan 13, 2017	▼

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.

EmployeePolicy Applied To: 12 Identities Contains: 3 Policy Settings Last Modified: May 11, 2017

Policy Name
EmployeePolicy

- 12 Identities Affected**
12 Network Devices
Edit
- 2 Destination Lists Enforced**
• 1 Block List
• 1 Allow List
Edit
- Security Setting Applied: Default Settings**
• Command and Control Callbacks, Malware, and Phishing
Attacks will be blocked
Edit Disable
- Content Setting Applied: employeeCategory**
Adware, Alcohol, Dating, plus 12 more will be blocked.
Edit Disable
- Custom Block Page Applied**
Employee Blocked page
Edit

▶ **ADVANCED SETTINGS**

DELETE POLICY **CANCEL** **SAVE**

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

What would you like to protect?

Select Identities

Search Identities

- AD Groups
- AD Users
- AD Computers
- Networks
- Roaming Computers
- Mobile Devices
- Sites 1 >
- Network Devices 26 >**

12 Selected REMOVE ALL

- DMZ-5520_employeeOD
- POD4-WLC_employeeOD
- POD5-WLC_employeeOD
- POD6-WLC_employeeOD
- POD3-WLC_employeeOD
- POD2-WLC_employeeOD**
- POD1-WLC_employeeOD**
- POD8-WLC_employeeOD
- POD7-WLC_employeeOD

All Identities **CANCEL** **SET & RETURN**

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

High
 Blocks adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters.

Moderate
 Blocks all adult-related websites and illegal activity.

Low
 Blocks pornography.

Custom
 Create a custom grouping of category types.

Custom Setting

employeeCategory

CATEGORIES TO BLOCK SELECT ALL

<input type="checkbox"/> Academic Fraud	<input checked="" type="checkbox"/> Adult Themes
<input checked="" type="checkbox"/> Adware	<input checked="" type="checkbox"/> Alcohol
<input type="checkbox"/> Anime / Manga / Webco...	<input type="checkbox"/> Auctions
<input type="checkbox"/> Automotive	<input type="checkbox"/> Blogs
<input type="checkbox"/> Business Services	<input type="checkbox"/> Chat
<input type="checkbox"/> Classifieds	<input checked="" type="checkbox"/> Dating
<input checked="" type="checkbox"/> Drugs	<input type="checkbox"/> Ecommerce / Shopping
<input type="checkbox"/> Educational Institutions	<input type="checkbox"/> File Storage
<input type="checkbox"/> Financial Institutions	<input type="checkbox"/> Forums / Message boar...
<input type="checkbox"/> Gambling	<input type="checkbox"/> Games
<input type="checkbox"/> German Youth Protection	<input checked="" type="checkbox"/> Government
<input type="checkbox"/> Hate / Discrimination	<input type="checkbox"/> Health and Fitness

CANCEL
SET & RETURN

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**.

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups
<input type="checkbox"/> Enabled	contractor					contractor
<input type="checkbox"/> Enabled	employee					Employee

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

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, PassiveID, and Threat Centric. The left sidebar shows 'Identity Groups' with a tree view under 'User Identity Groups' containing: ALL_ACCOUNTS (default), contractor, Employee, GROUP_ACCOUNTS (default), GuestType_Contractor (default), GuestType_Daily (default), GuestType_Weekly (default), kevin_g, MyGroup, OWN_ACCOUNTS (default), and TRUSTSEC_ADMIN. The main content area is titled 'User Identity Groups' and contains a table of groups:

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Weekly (default)	Identity group mirroring the guest type
<input type="checkbox"/> MyGroup	MyGroup
<input type="checkbox"/> OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group
<input type="checkbox"/> TRUSTSEC_ADMIN	TRUSTSEC_ADMIN
<input type="checkbox"/> contractor	contractor
<input type="checkbox"/> kevin_g	

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**.

The screenshot shows the Cisco Identity Services Engine (ISE) Policy configuration page. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes Authentication, Authorization, Profiling, Posture, Client Provisioning, and Policy Elements. The left sidebar shows 'Results' with a tree view under 'Authorization Profiles' containing: Authentication, Authorization, Profiling, Posture, and Client Provisioning. The main content area is titled 'Authorization Profiles > employee' and shows the configuration for an 'Authorization Profile' named 'employee'. The configuration includes:

- * Name: employee
- Description: (empty)
- * Access Type: ACCESS_ACCEPT
- Network Device Profile: Cisco
- Service Template:
- Track Movement:
- Passive Identity Tracking:

Below the configuration are sections for 'Common Tasks' and 'Advanced Attributes Settings'. The 'Common Tasks' section includes checkboxes for: DACL Name, ACL (Filter-ID), VLAN, and Voice Domain Permission. The 'Advanced Attributes Settings' section shows a rule: Cisco:cisco-av-pair = role=employee.

▼ **Advanced Attributes Settings**

Cisco:cisco-av-pair	=	role=employee	+
---------------------	---	---------------	---

▼ **Attributes Details**

Access Type = ACCESS_ACCEPT
cisco-av-pair = role=employee

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Authorization Profiles > contractor

Authorization Profile

* Name: contractor

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement: ⓘ

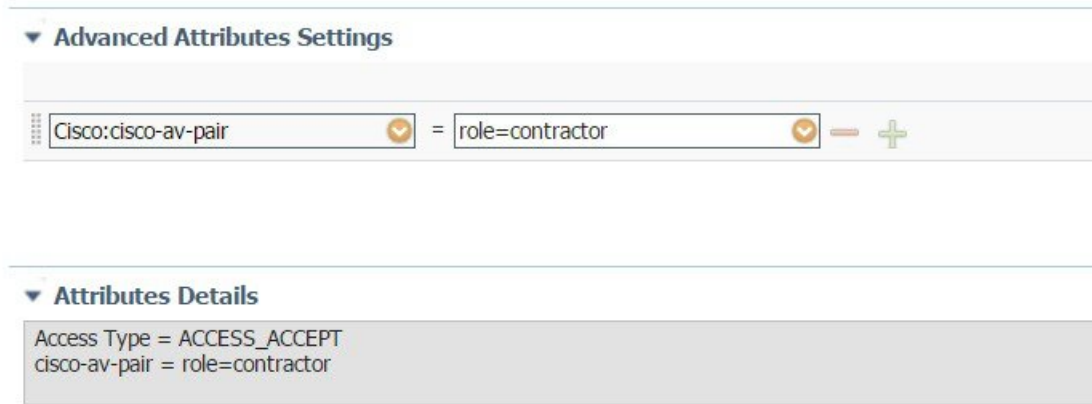
Passive Identity Tracking: ⓘ

▼ **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**)

Policy List

Number of Policies 2

Policy Name	Policy ID
employee	1
contractor	2

- 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**.

Policy > Edit

[< Back](#) [Apply](#)

Policy Name employee
Policy Id 1

Match Criteria

Match Role String employee
Match EAP Type none

Device List

Device Type [Add](#)

Action

IPv4 ACL none
URL ACL none
VLAN ID 0
Qos Policy none
Average Data Rate 0
Average Real time Data Rate 0
Burst Data Rate 0
Burst Real time Data Rate 0
Session Timeout (seconds) 1800
Sleeping Client Timeout (min) 720
Flexconnect ACL none
AVC Profile none
mDNS Profile none
OpenDNS Profile employeeOD

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

Policy List

Number of Policies 2

Policy Name	Policy ID
employee	1
contractor	2

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**.

Policy > Edit

< Back
Apply

3

Policy Name contractor
Policy Id 2

Match Criteria

1

Match Role String contractor
Match EAP Type none

Device List

Device Type Add

Action

IPv4 ACL none
URL ACL none
VLAN ID 0
Qos Policy none
Average Data Rate 0
Average Real time Data Rate 0
Burst Data Rate 0
Burst Real time Data Rate 0
Session Timeout (seconds) 1800
Sleeping Client Timeout (min) 720
Flexconnect ACL none
AVC Profile none
mDNS Profile none
2
OpenDNS Profile contractorOD

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**.

WLANs > Edit 'POD1'

< Back Apply

General Security QoS **Policy-Mapping** Advanced

Priority Index (1-16) 1

Local Policy employee

Add

Priority Index Local Policy Name

Similarly, apply the contractor policy to the WLAN.

General Security QoS **Policy-Mapping** Advanced

Priority Index (1-16)

Local Policy employee

Add

Priority Index	Local Policy Name
1	employee
2	contractor

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

CISCO MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs

WLANs

Advanced

mDNS

mDNS Snooping Enabled

TrustSec

Security Group Tag 0

OpenDNS

OpenDNS Mode Forced

OpenDNS Profile contractorOD

- 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 .

Profile Name	Opendns-Identity	State
employeeOD	POD1-WLC_employeeOD	Profile Registered <input checked="" type="checkbox"/>

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

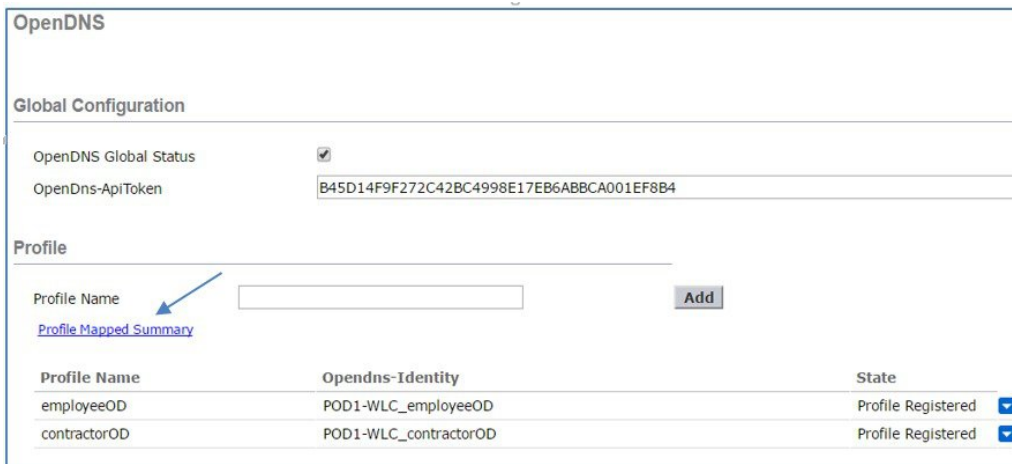
- b) To map the Profile to AP Group, go to **WLANs> Advanced> AP Groups**. Select the AP group you want and go to **WLANs** tab. Hover the mouse over the blue button on the right and select **OpenDNS Profile**.

WLAN ID	WLAN SSID(2/6)	Interface/Interface Group(G)	SNMP NAC State
1	pod2	management	Disabled

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.

OpenDNS Profile Map Summary

WLAN	AP Group	Local Policy
Profile Name	WLAN IDs Mapped	
employeeOD	NONE	
contractorOD	1	

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

OpenDNS Profile Map Summary

WLAN	AP Group	Local Policy						
<table><thead><tr><th>Profile Name</th><th>AP Groups Mapped</th></tr></thead><tbody><tr><td>employeeOD</td><td>NONE</td></tr><tr><td>contractorOD</td><td>APgrp1, 1</td></tr></tbody></table>			Profile Name	AP Groups Mapped	employeeOD	NONE	contractorOD	APgrp1, 1
Profile Name	AP Groups Mapped							
employeeOD	NONE							
contractorOD	APgrp1, 1							

From CLI

```
<POD2-WLC> >show.opendns.summary
OpenDnsGlobalStatus..... Enabled
OpenDns-ApiToken..... B45D14F9F272C42BC4998E17EB6ABBCA001EF8B4

  Profile-Name                Opends-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.

The screenshot shows the configuration page for a Cisco Wireless LAN Controller (WLC) in the 'Advanced' tab. The 'Advanced' tab is highlighted with a red box. The configuration includes:

- Optimized Roaming Disassociation Timer (0 to 40 TBTT): 40
- BSS Max Idle Service:
- Directed Multicast Service:
- Tunneling: Tunnel Profile: None
- mDNS: mDNS Snooping: Enabled
- TrustSec: Security Group Tag: 0
- OpenDNS: OpenDNS Mode: Forced (highlighted with a red box), OpenDNS Profile: None

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 opensns 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 opensns ip only. Client who do not have opensns ip as one of configured DNS IP can reject this causing connectivity issues.

Adding opensns 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 opensns ip only

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

3. OpenDNS Ignore mode

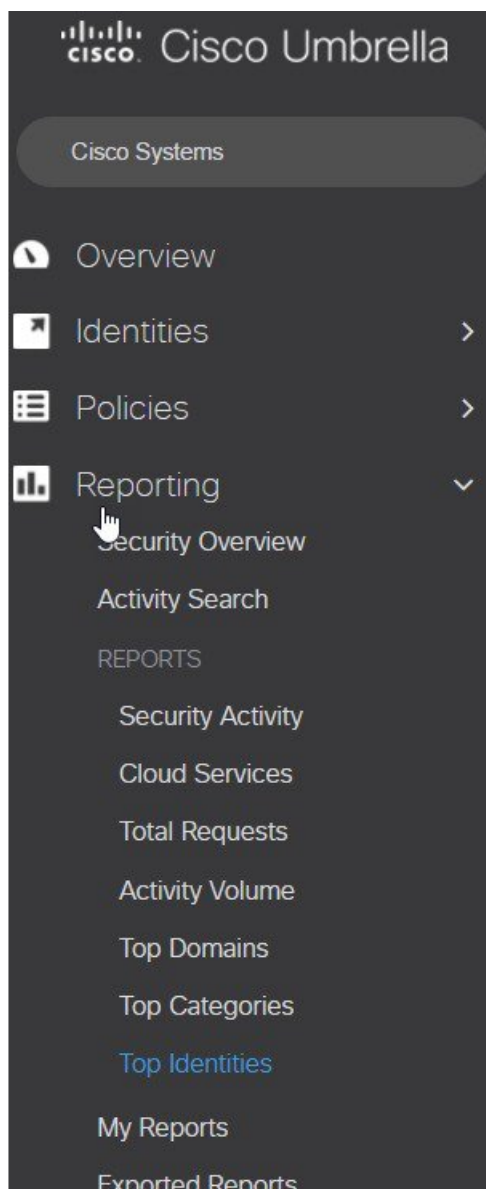
WLC honors the DNS server used by the client; it could be Cisco Umbrella cloud servers or enterprise/ external DNS

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.



Top Identities - All Identities - All Destinations - Last 24 hours (UTC-08:00 [Change time zone](#)) - All Categories - All Security Categories

Filters Hide

Filter by Identity:

Filter by Destination:

NOTE: Only malicious domains are supported.

Filter by date:

Filter by Categories: CHOOSE >

Filter by Security Categories: CHOOSE >

RUN REPORT

Rank	Identity	Requests
1	WLC-5520_employeeOD	106
2	WLC-5520_contractorOD	61

Top Domains - All Identities - Last 24 hours (UTC-08:00 [Change time zone](#)) - All Responses - All Destinations - All Categories - All Security Categories

Filters Hide

Filter by Identity:

Include all traffic

Filter by date:

Filter by Response:

Filter by Destination:

Filter by Categories: CHOOSE >

Filter by Security Categories: CHOOSE >

RUN REPORT

Rank	Domain	Categories	Requests
1	guzzoni.apple.com	Software/Technology	19
2	time-ios.apple.com	Software/Technology	15
3	www.apple.com	Software/Technology	14
4	www.icloud.com	File Storage, Software/Technology, Webmail	14
5	apple.com	Software/Technology	13
6	time-ios.g.aaplimg.com		8
7	mesu.apple.com	Software/Technology	8
8	x02wapi.webexconnect.com		4
9	cisco.webex.com	Business Services, Software/Technology	4
10	isj3cmx.webexconnect.com		3
11	www.cisco.com	Business Services, Software/Technology	3
12	init-r01st.rush.apple.com	Software/Technology	2

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.