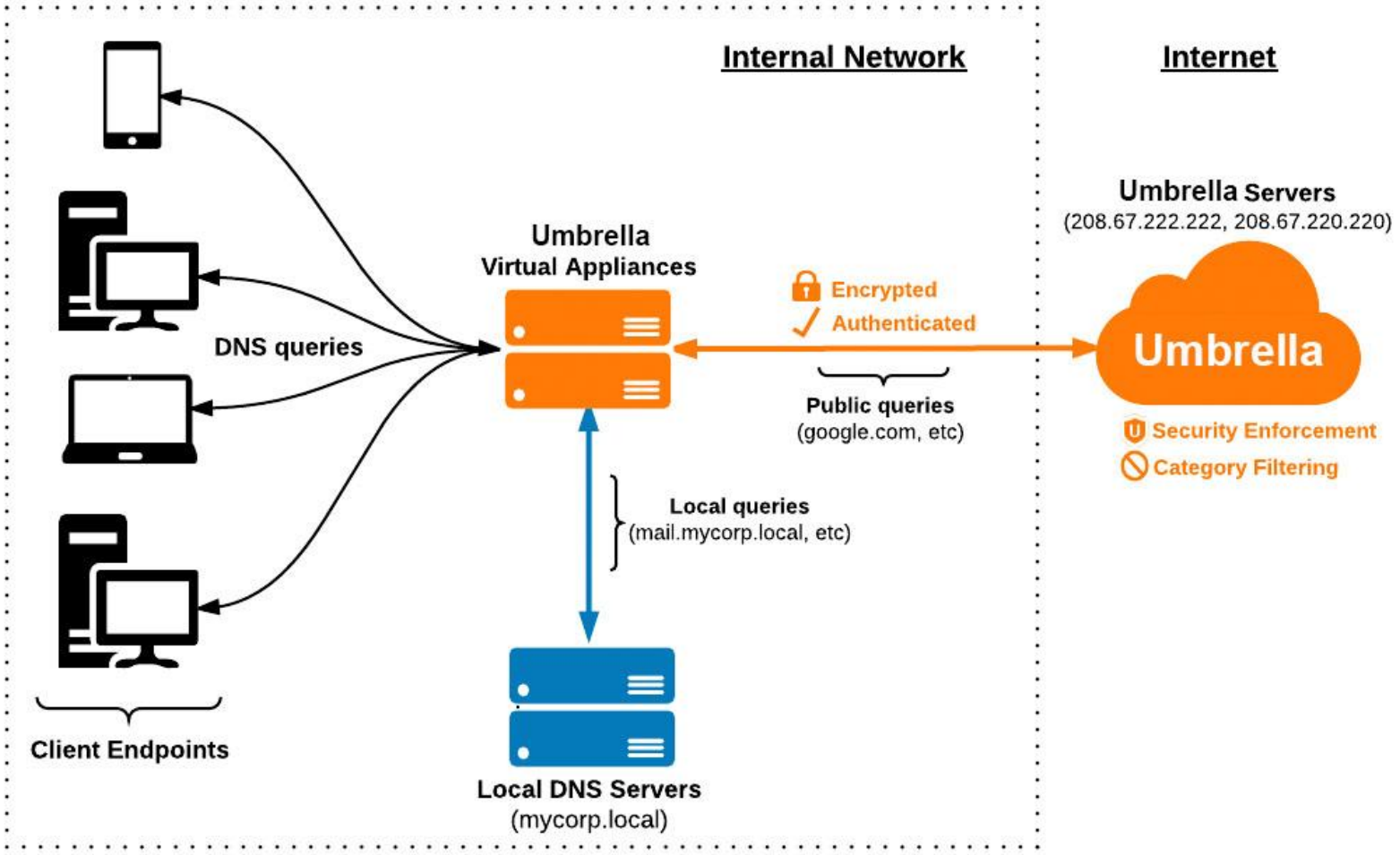
Division of information Systems

Cisco Umbrella



Prepared by
DIS APSCN/LAN Support

Contents

Changelog

7/1/2024 – Added missing Cisco Security for Chromebook Migration Google Identity Authorization step (pages 64-67). Removed outdated “Deploy the G Suite Identity Service” instructions (removed from pages 86-89).

6/5/2024 – New Cisco Secure Client (Roaming Client Replacement) deployment steps added (starting on page 92) and old Roaming Client deployment steps removed.

5/6/2024 – New Cisco Security for Chromebook Migration steps added (starting on page 62) and old Chromebook Extension steps removed. Also added the Changelog section at beginning of document and updated Table of Contents.

5/5/2026 – Added API Key setup steps to complete before VAs and AD Connector installations. Instructions starting on page 11.

https://docs.umbrella.com/deployment-umbrella/docs/welcome-to-cisco-umbrella

Basic Level Filtering

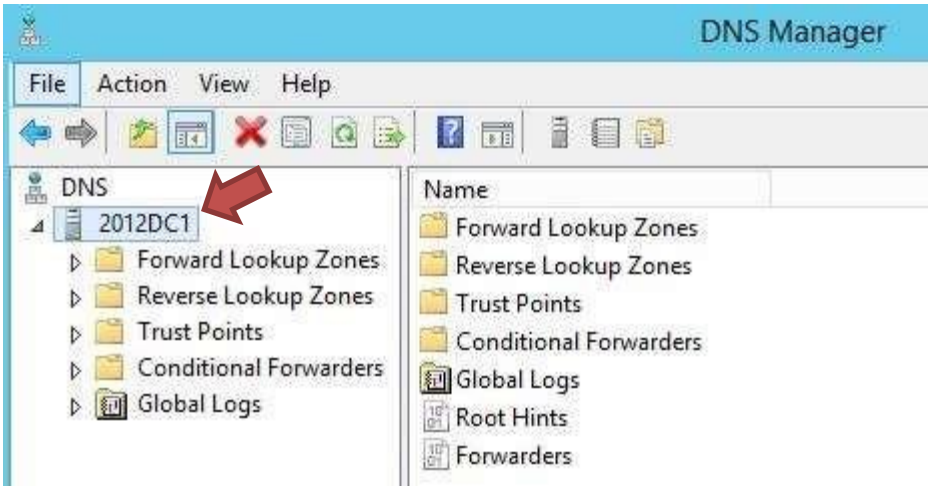
The most basic implementation of the Cisco Umbrella filter will afford you the state's default filtering level for all your users. Simple and quick to implement, this level of filtering makes no distinction between your users and is not Active Directory aware. All it requires is a change to the DNS forwarders on your local DNS server(s).

OpenDNS Forwarders

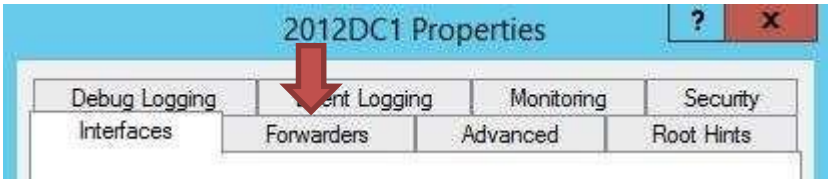
Add the OpenDNS Forwarders to ALL of your DNS servers. The OpenDNS Forwarders are **208.67.222.222**, **208.67.220.220, 208.67.220.222, and 208.67.222.220**

1. Open **DNS Manger** or type **DNSMGMT** from run or CMD prompt

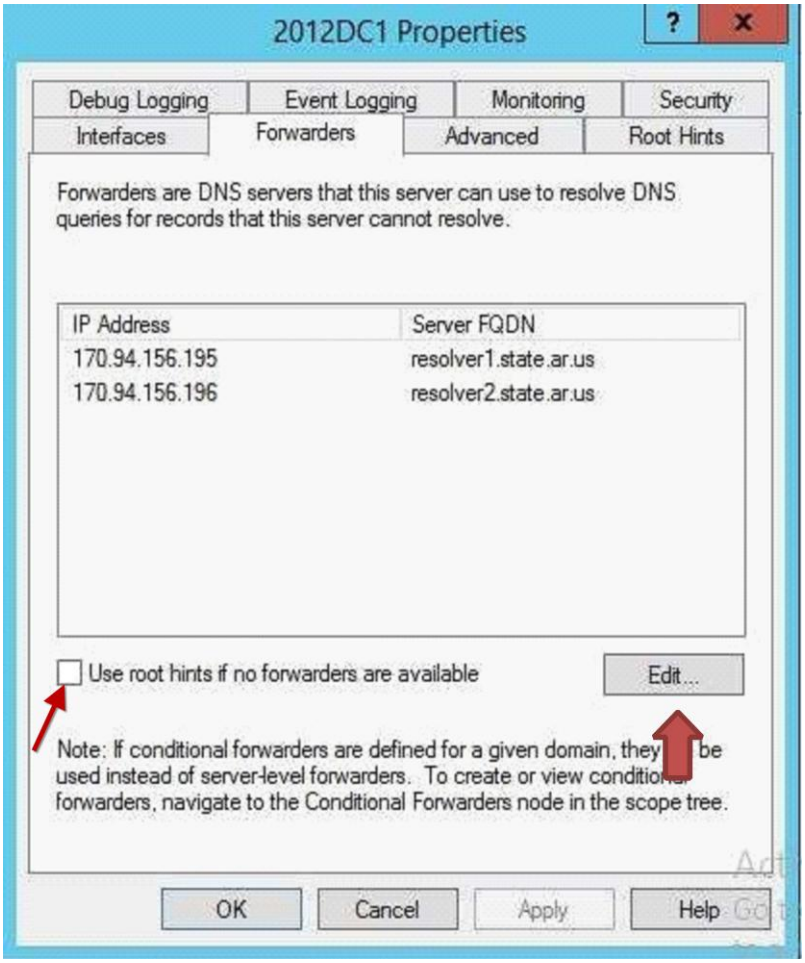
2. **Select** your **server name**, right click the **server name** and click **Properties**



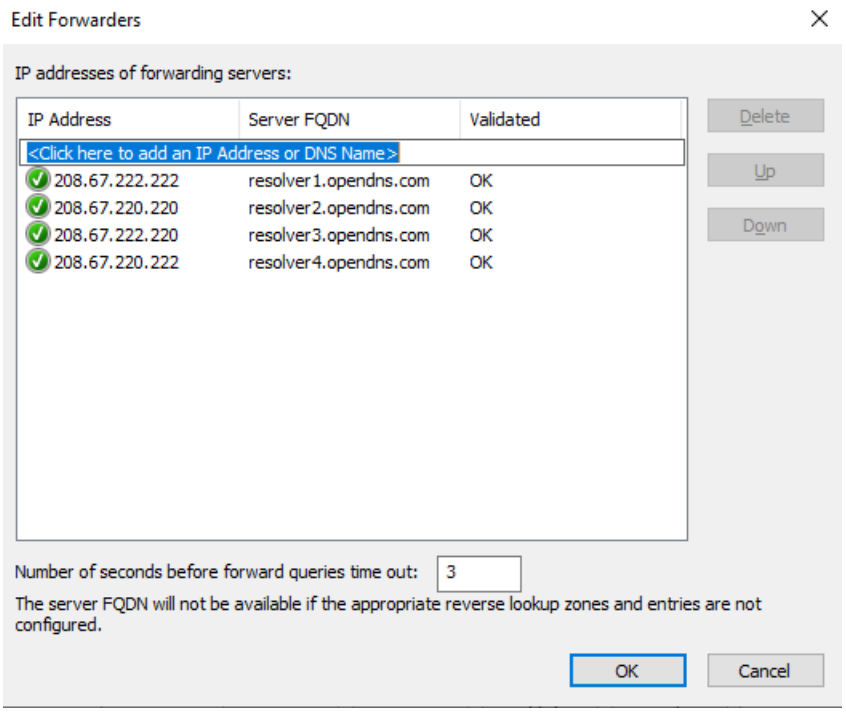
3. In your DNS Server **Properties**, select the **Forwarders** tab



4. **Uncheck** the use root hints box and then click **Edit**



5. **Delete ALL** existing DNS Forwarders, add **208.67.222.222, 208.67.220.220, 208.67.220.222, and 208.67.222.220** as your new forwarders



6. Click **OK > OK > Close your DNS Manager**

7. Do this on **every server that has DNS installed**

Local IP Level Filtering

A second level of OpenDNS implementation requires installation of multiple virtual appliances on virtual hosts within your network. Best Practices call for installing at least two appliances on two separate

physical hosts for redundancy and fault protection. These appliances allow for more detailed reporting, and custom filtering.

Virtual Appliance Requirements

Virtual Appliances (VAs) are needed for detailed reporting and identity information, Active Directory Integration, and granular Policy Management. Listed below are the requirements needed for the VAs to work.

1. **2 VAs per Site** – In order for automatic updates to occur without downtime and for redundancies sake at the DNS level, you must have two VAs per site, each on separate Hypervisor servers.
2. **VA Specs** – Each VA requires the following resources:
    a. **1 Virtual CPU**
    b. **2048 MB of RAM Recommended** (minimum 512MB)
    c. **7GB of disk space**
    NOTE: The above resources allow each VA to process millions of DNS requests per day. It is estimated that 1 VA with the above mentioned amount of resources can serve over 100,000 endpoints.
3. **Correct Date/Time –** The incorrect date or time can cause update or sync issues with the VAs. Ensure your Hypervisor host has the correct date and time. The VA syncs time independently and is always set to UTC.
4. **VMWare or Hyper-V –** The VAs can run either on VMware or Hyper-V
    a. **VMware** requires ESX or ESXi 4.1 update 2 (or newer)
    b. **Hyper-V** requires one of the following Windows Server Operating Systems:
        i. **Windows Server 2012, SP1, or R2 (Standard or Datacenter), 2016, or 2019 with Hyper-V role**
        ii. **Hyper-V Server 2012, 2012 R2, 2016, or 2019**

VA Networking Requirements

Once VAs are deployed and ready to be utilized, endpoint clients must exclusively resolve DNS through the VAs and not your local DNS forwarders. This is usually accomplished through the network's DHCP configuration. The following firewall/ACL requirements ensure VAs can communicate with the Umbrella cloud services and local DNS forwarders/servers.

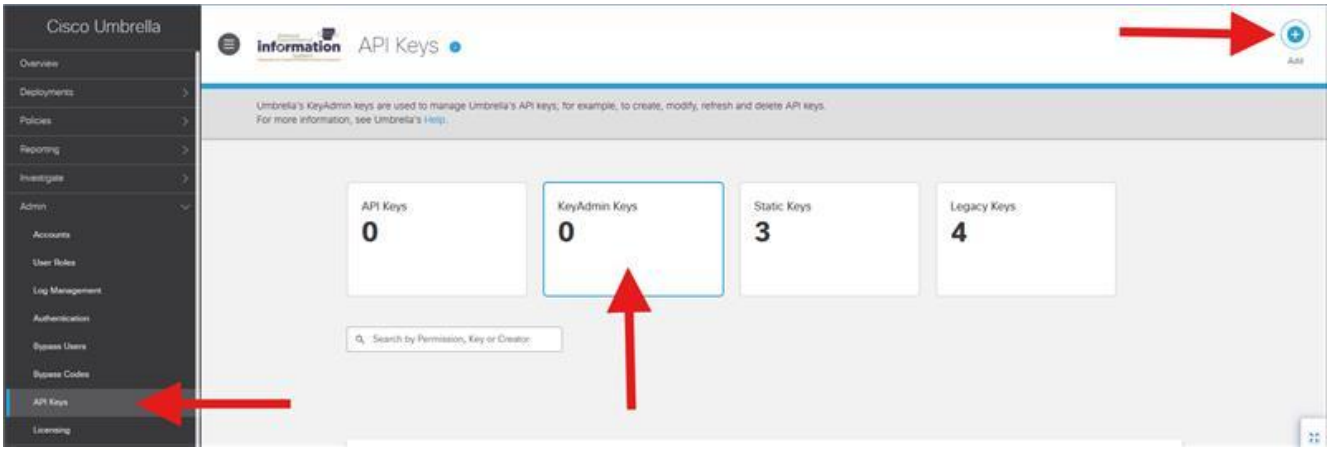
Port and Protocol	Source	Destination	Note
53 TCP + UDP	Virtual Appliance	Local DNS servers	Standard DNS traffic for internal domains.

53 TCP + UDP 443 TCP + UDP 5353 TCP + UDP	Virtual Appliance	Umbrella resolvers **Default**: • 208.67.220.220/32 • 208.67.222.222/32 If you have configured the VA to use other Umbrella resolvers: **Alternate**: • 208.67.220.222/32 • 208.67.222.220/32 **IPv6**: • 2620:119:35::35 • 2620:119:53::53 **US-only**: • 208.67.221.76/32 • 208.67.223.76/32 **US-only IPv6**: • 2620:119:17::76 • 2620:119:76::76	Standard and encrypted DNS queries to Umbrella resolvers. Port 443 is used as failover if your firewall does not allow DNSCrypt on port 53. Port 5353 is used as failover if DNSCrypt is not allowed on port 53 and port 443.
443 TCP	Virtual Appliance	• api.opendns.com • (67.215.92.210 • 146.112.255.152/29) • ocsp.digicert.com • crl4.digicert.com • cisco.com	HTTPS—Used for registration, health checks, and updates from Umbrella. ocsp.digicert.com and crl4.digicert.com use a CDN and are not assigned static IP addresses, thus are subject to change. Currently, these domains resolve to the following IPs: • 72.21.91.29 • 117.18.237.29 • 93.184.220.29 • 205.234.175.175
80 TCP	Virtual Appliance	• ocsp.digicert.com • crl4.digicert.com	HTTP—Used for fetching the SSL revocation list to initiate the HTTPS connection.
443 TCP	Virtual Appliance	disthost.umbrella.com	Updates to the VA
Port and Protocol	**Source**	**Destination**	**Note**
22 25 53 80 443 or 4766 TCP	Virtual Appliance	s.tunnels.ironport.com	Required for the customer-initiated SSH support tunnel. For more information, see On-Demand Tech Support SSH Tunnel for Virtual Appliances.
123 UDP	Virtual Appliance	NTP servers **Default**: • ntp.ubuntu.com • (91.189.94.4/32 • 91.189.89.199/32 • 91.189.91.157/32	NTP—Protocol to synchronize time.

		• 91.189.89.198/32) If you have configured custom NTP servers on the VA, use those IPs instead.	
443 TCP	Chromebook client	Virtual Appliance(s)	Required for Chromebook client trusted network feature.
443 TCP	Umbrella AD Connector	Virtual Appliance(s)	Used to send user/IP mapping (one-way) from the Active Directory (AD) connector to the VA.

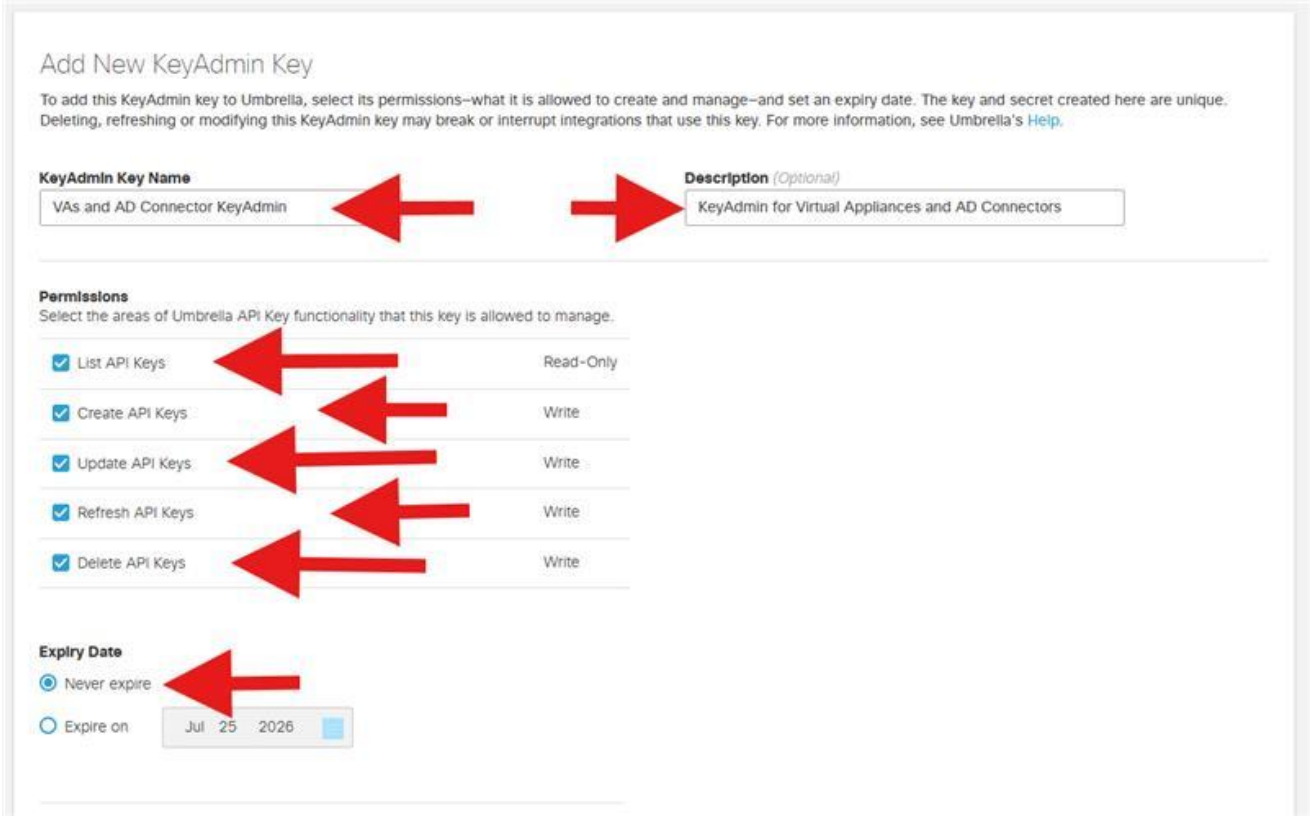
Creating API Keys for VAs and AD Connectors

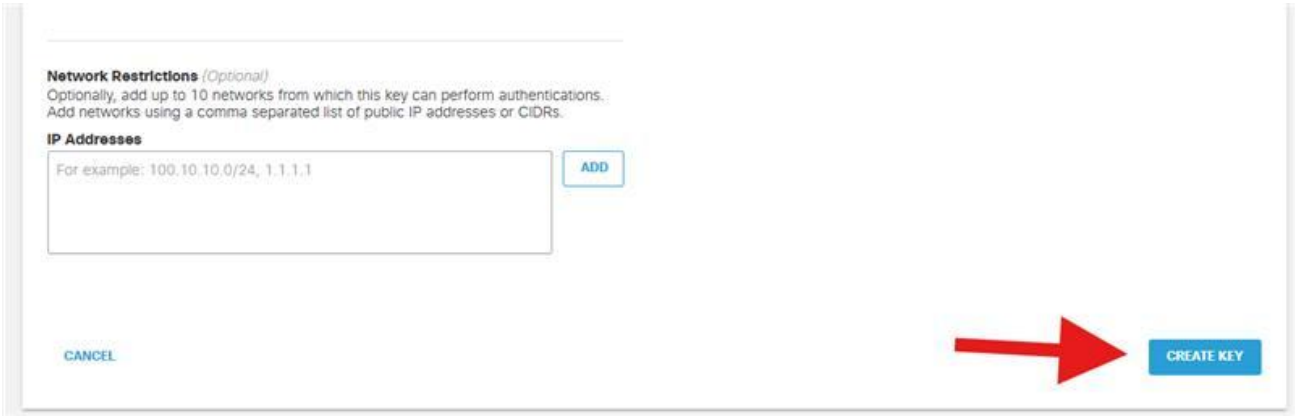
Step 1: Navigate to Admin > API Keys. Then click KeyAdmin Keys, then click Add.



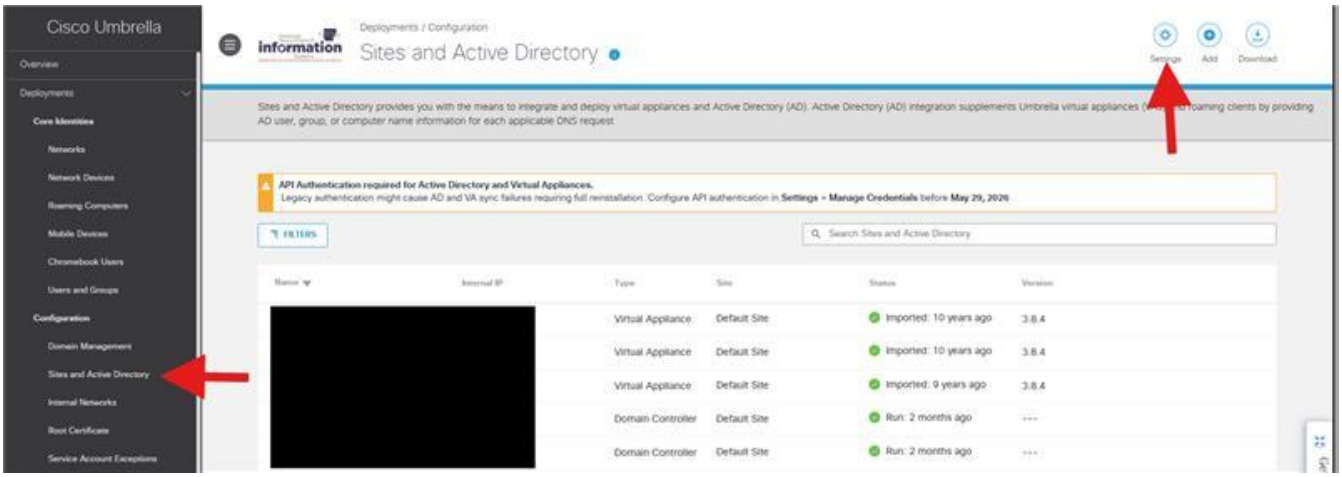
Step 2: Give the KeyAdmin a name and description, then check all 5 options under Permissions, then click Never expire under Expiry Date, then click Create Key.

COPY the API Key and Key Secret to notepad, you will need this later and once you click off of this page you will no longer be able to view the secret unless you create a new key!!!!

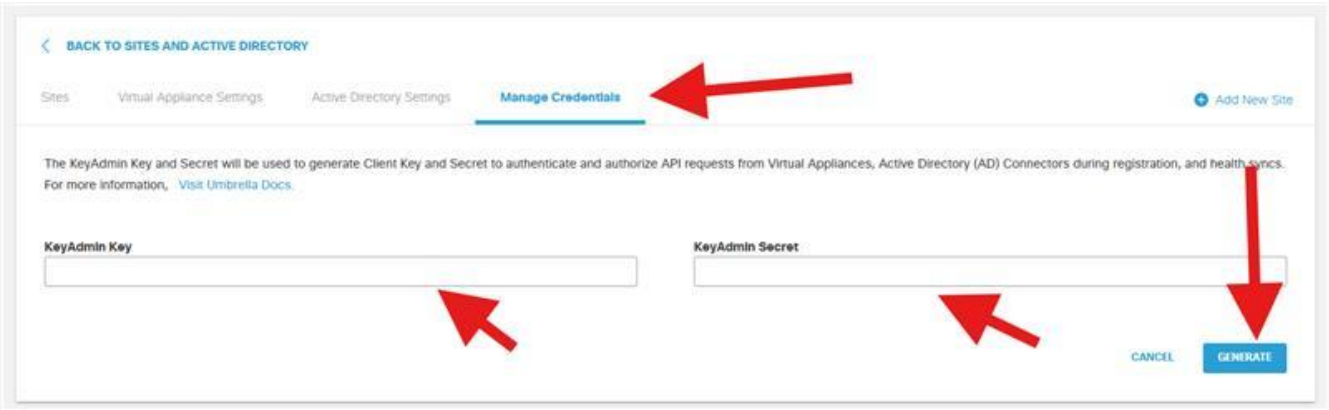




Step 3: Navigate to Deployments > Sites and Active Directory, then click Settings.

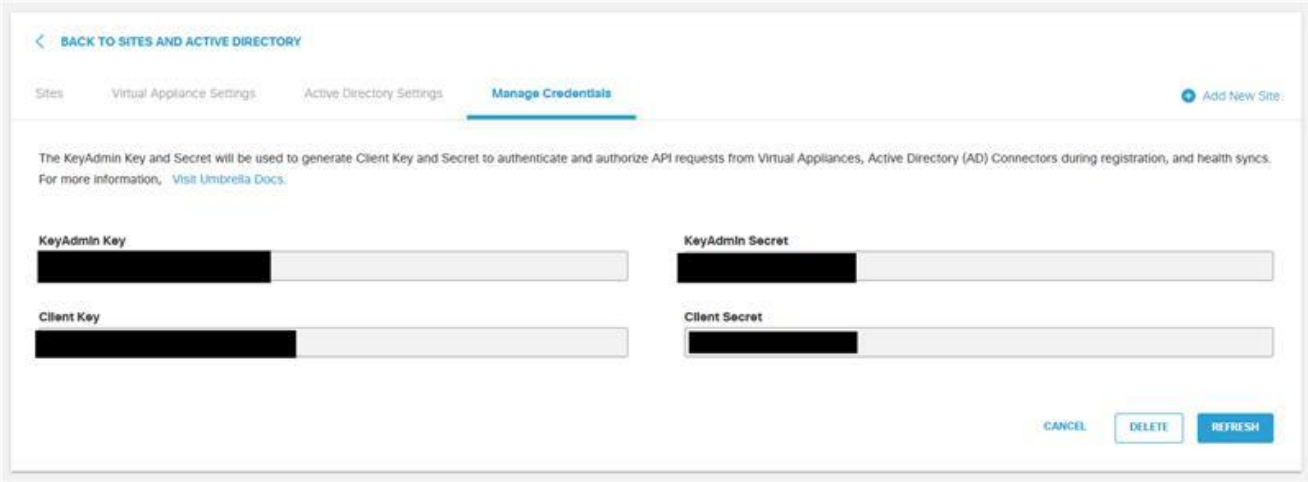


Step 4: Click the Manage Credentials tab and paste the KeyAdmin key and secret from the previous step, then click Generate.



Step 5: Make sure api.umbrella.com is allowed in your filters.

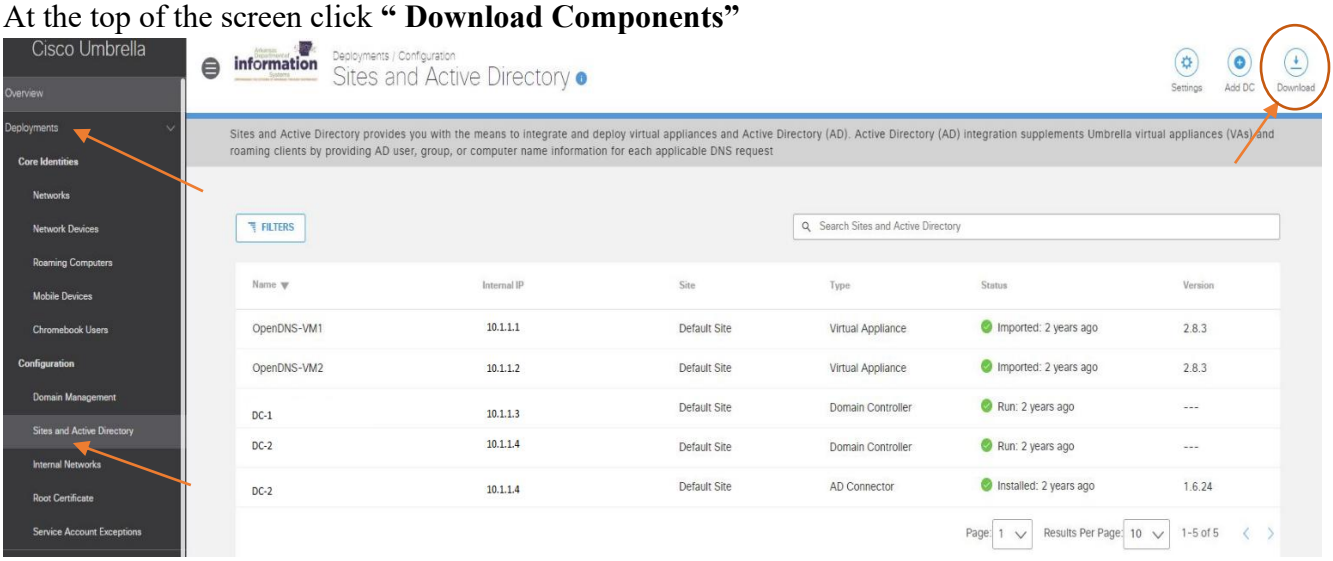
API Authentication has now been setup, continue to the next steps.



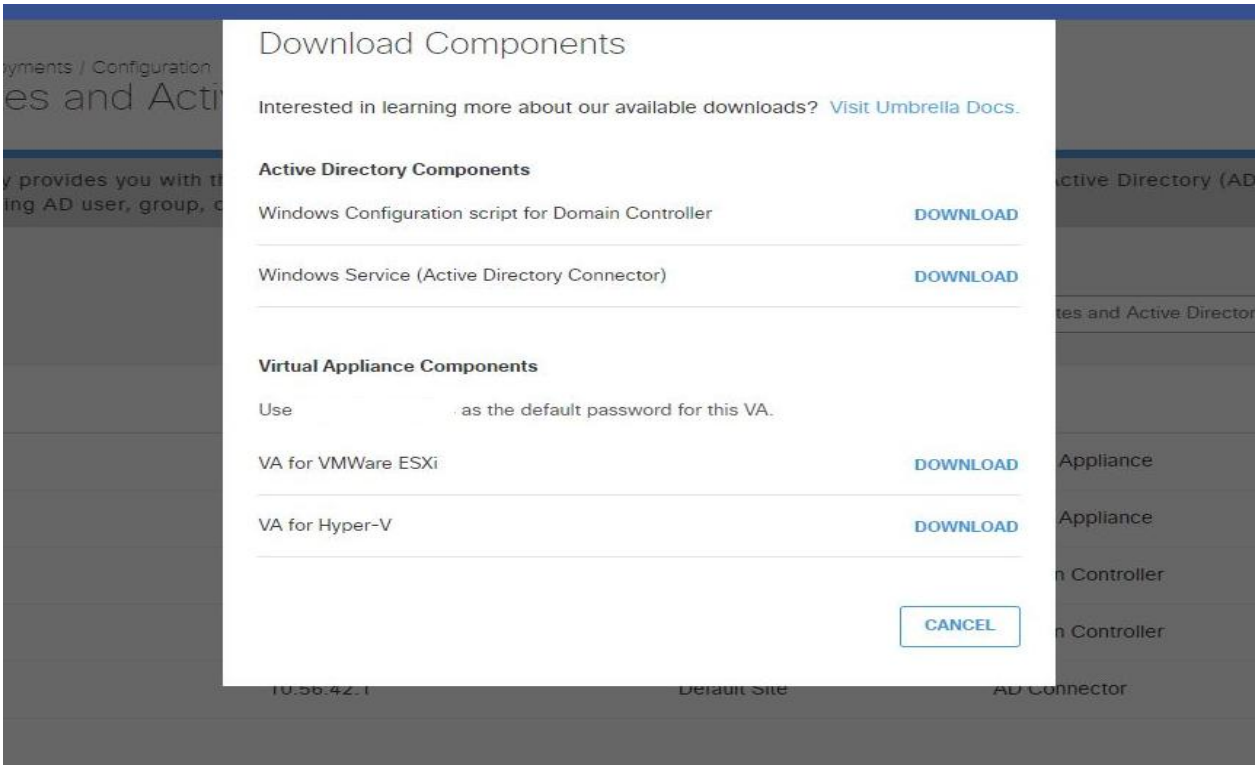
Download Virtual Appliance:

1. Create a folder called **openDns** to download the necessary files to.
2. Navigate to **Unmbrella.com** and login. Then navigate to **Deployments > Sites and Active Directory** (under Configuration).

3. At the top of the screen click **" Download Components"**



4. Depending on whether you're using VMWare or Hyper-V, download the appropriate "**VA for"**



5. If you plan to integrate Active Directory to your system, Download the **Windows Configuration** script and **Windows Service** (see Configure Active Directory)

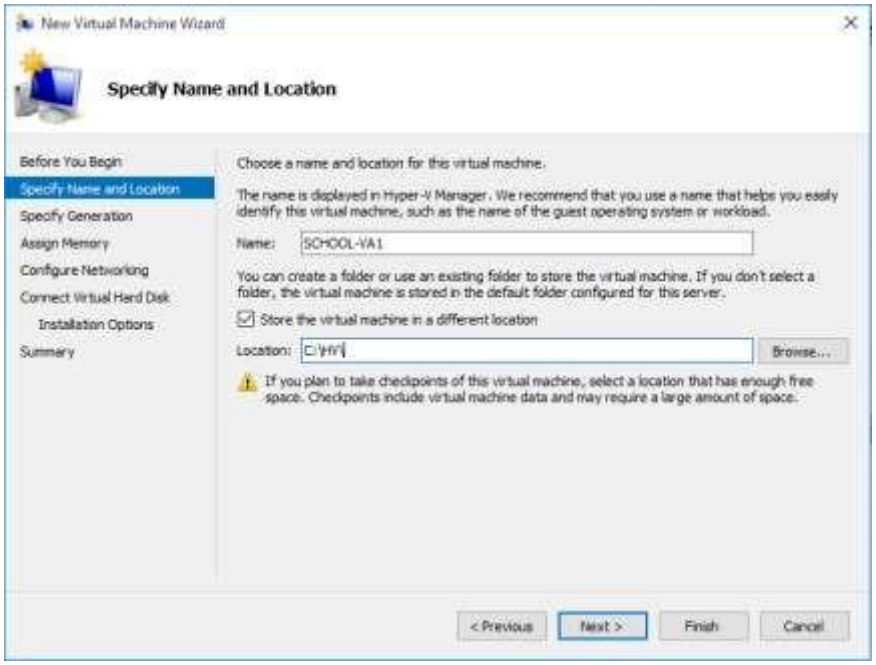
   Each new school must download their own files from their Umbrella Portal as the files are tagged to that school when downloaded.

Hyper-V Virtual Appliance Deployment

To deploy the VA in Hyper-V for Windows Server it is best to create a new VM and attach the Hard Disk after the fact. For Server 2012 R2 it is mandatory.

1. Select your Hyper-V Server Name on the left and then select **New > Virtual Machine** in the **Actions** menu along the right side of **Hyper-V Manager**
2. Click **Next** on the **Before You Begin** page if you get that
3. Name the VA with the format **SCHOOL-VA** followed by the number for the VA.
   a. If this is your first VA then the name should be **YOURSCHOOL-VA1.**
   b. Check the **Store the virtual machine in a different location**

c. Navigate to the location where VM's are stored on this network

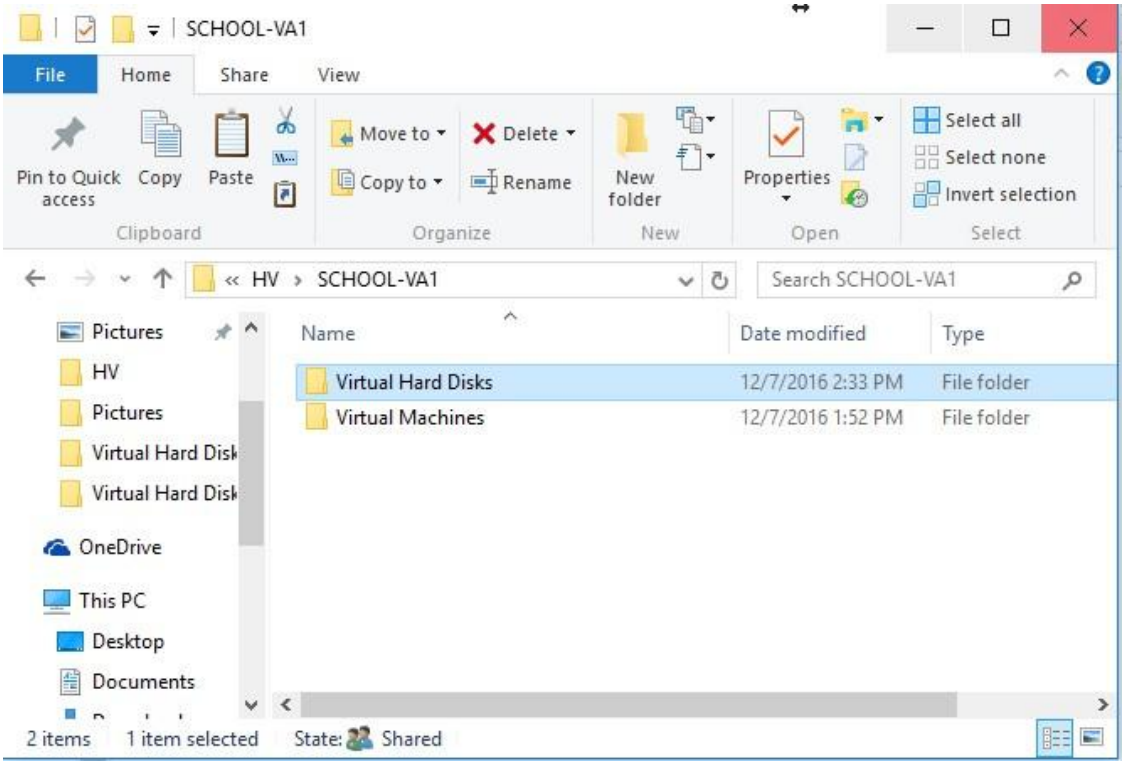


4. Click **Next**
5. Make sure **Generation 1** is selected. The VA's are built using this format. Click **Next**
6. Assign **1024MB** of RAM to the VM. As mentioned in the VA Requirements section, 512 MB is estimated to serve 100,000 endpoints a day. Click **Next**
7. Select your Network Adapter and click **Next**
8. Select the option at the bottom: **Attach a virtual hard disk later** and click **Next**
9. Click **Finish**

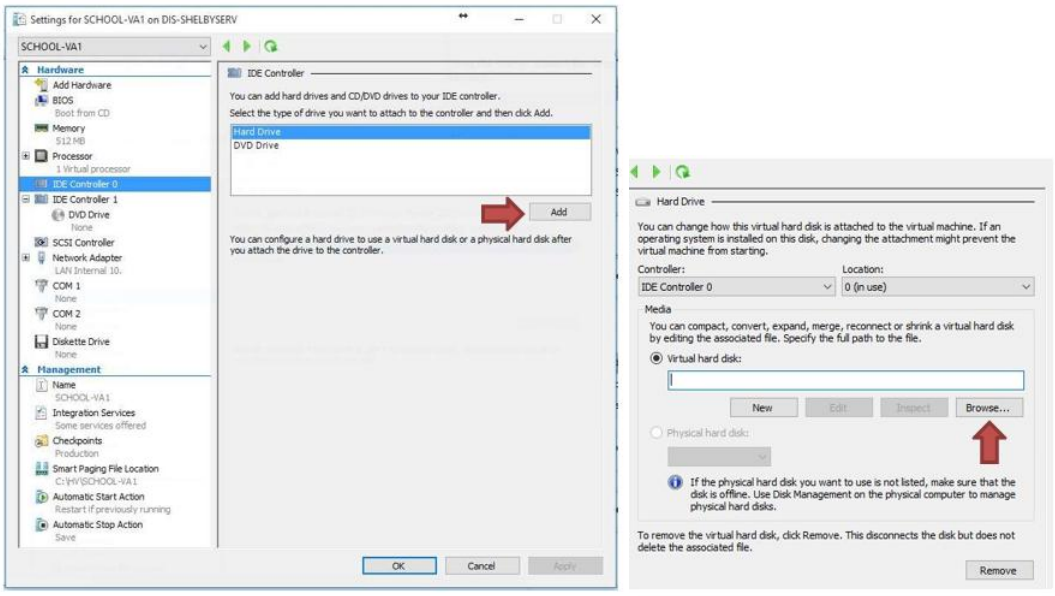
Now we need to copy the .VHD files you downloaded in the Prerequisite section to the newly created VM location and configure the VM Settings.

1. Find the file you downloaded all of your Prerequisite files to. Find a .zip file named **OpenDNSVirtualMachine-20151203** and extract it.
2. Open the newly extracted file and **Copy** the **Virtual Hard Disks** folder.
3. Navigate to the folder containing the VM on the Hyper-V Server (The location assigned in step 3 of the previous section.)
4. **Paste** the **Virtual Hard Disks** folder into the folder named after the VM you created.

5. Go into the **Virtual Hard Disks** folder and rename the two .VHD files to **dynamic-va-1** and **forwarderva-1** (change the 1 to a 2 if this is your second VA)

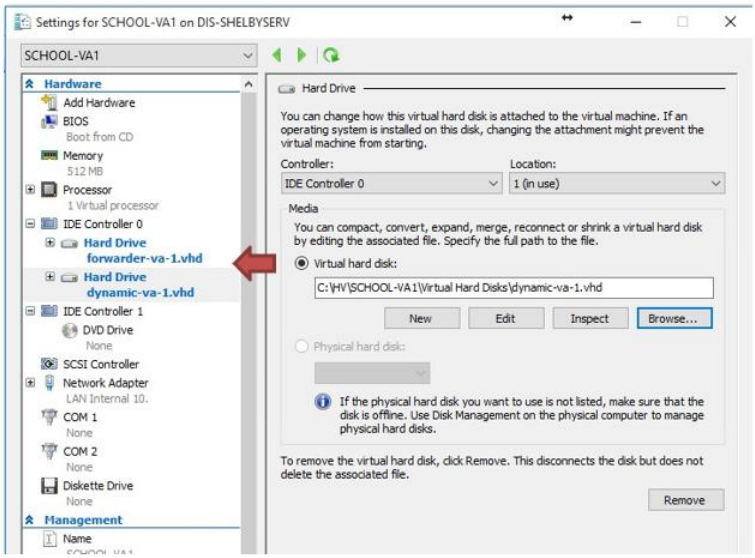


6. Go back to your **Hyper-V Manager**
7. **Right Click** the VM that you created and go to **Settings**
8. Select **IDE Controller 0**
9. Make sure **Hard Drive** is selected on the right hand side and click **Add**



10. Click **Browse** and navigate to the location of the hard drives you just copied above.
11. Select **forwarder-va-1** (or **-2**) and click **Open**

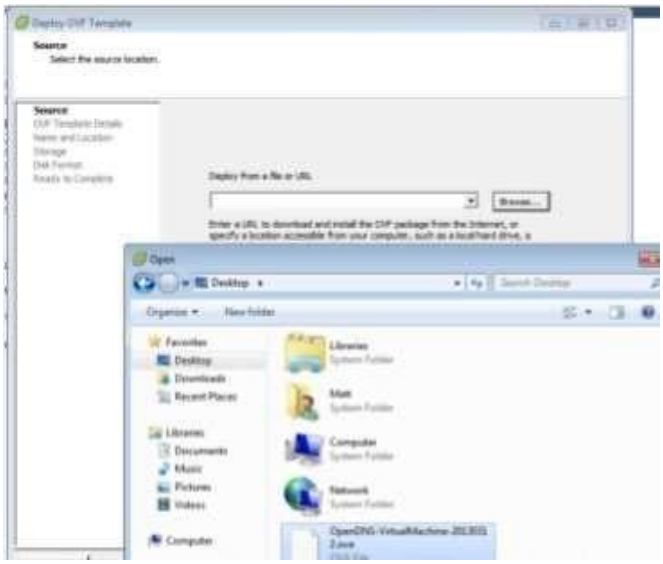
12. Repeat steps 8-10 for the **dynamic-va-1**



13. Click **Apply** and **OK**

NOTE: forwarder-va-1 must be the first drive (location 0)!!

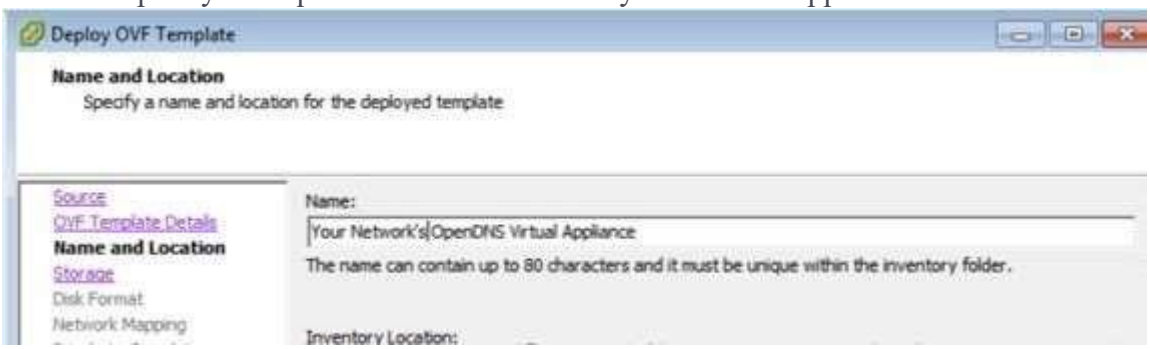
VMWare Virtual Appliance Deployment



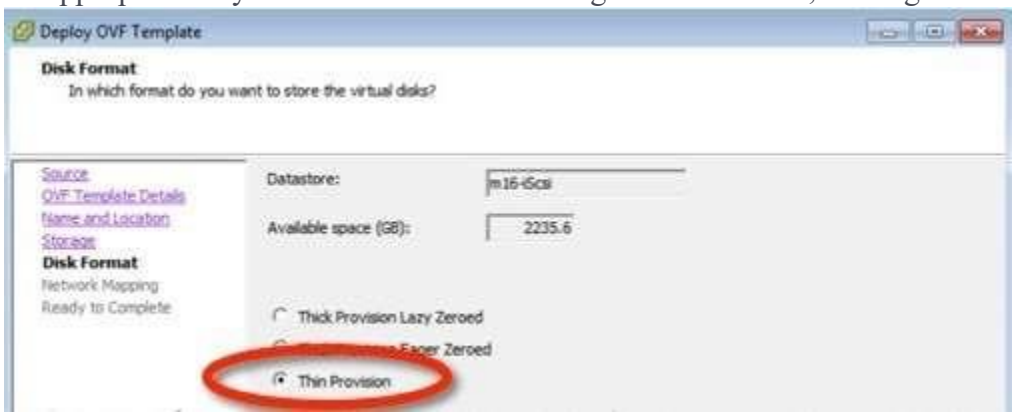
1. Log into your VMware vSphere client and select the 'File' tab.
2. Click Deploy OVF Template, choosing the .OVA template downloaded from the Umbrella dashboard.

3. Follow the deployment wizard prompts, but be sure to follow these key steps:

-For the **source**, browse to the **.ova** file you downloaded during the Prerequisite section. -Specify a unique name and location of your Virtual Appliance



4. Next, select the disks appropriate to your environment and during the disk format, making sure to select **Thin Provision**.



5. Next, select or map a network:

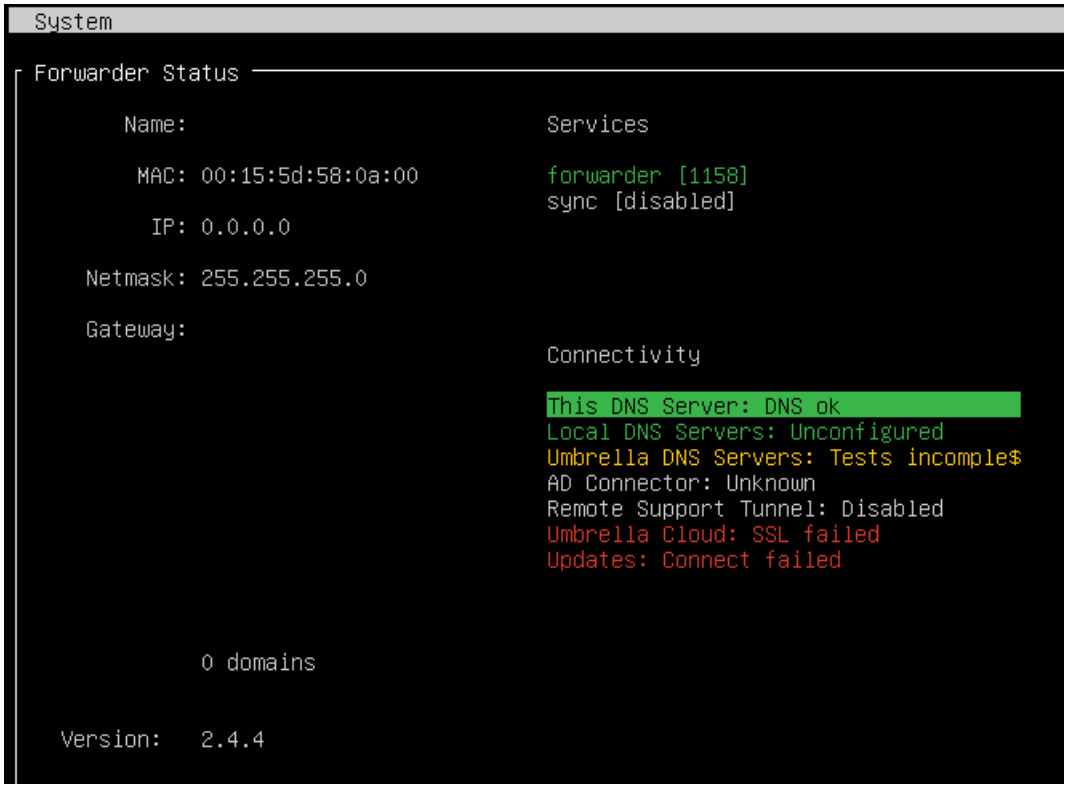
6. Click **Finish**.

The systems will begin deploying the Virtual Appliance and subsequent prompts will update you regarding the status.

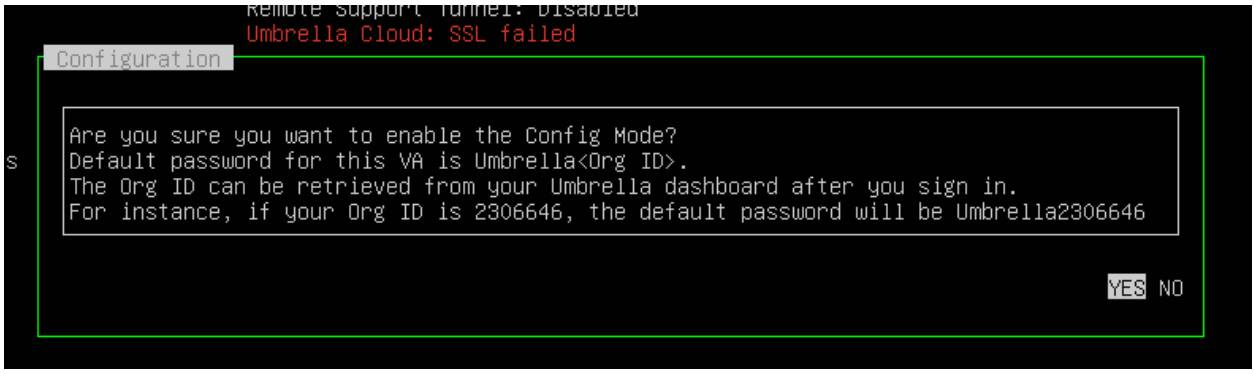
Configure the Virtual Appliances

It's time to configure the VAs. You will need the following information.

1. **Right Click** the VM and click **Connect**
2. At the top of the new window select the **Green Power Button**
3. Let the VM load until you see the following image (If you have DHCP it will automatically obtain an IP, my example does not)



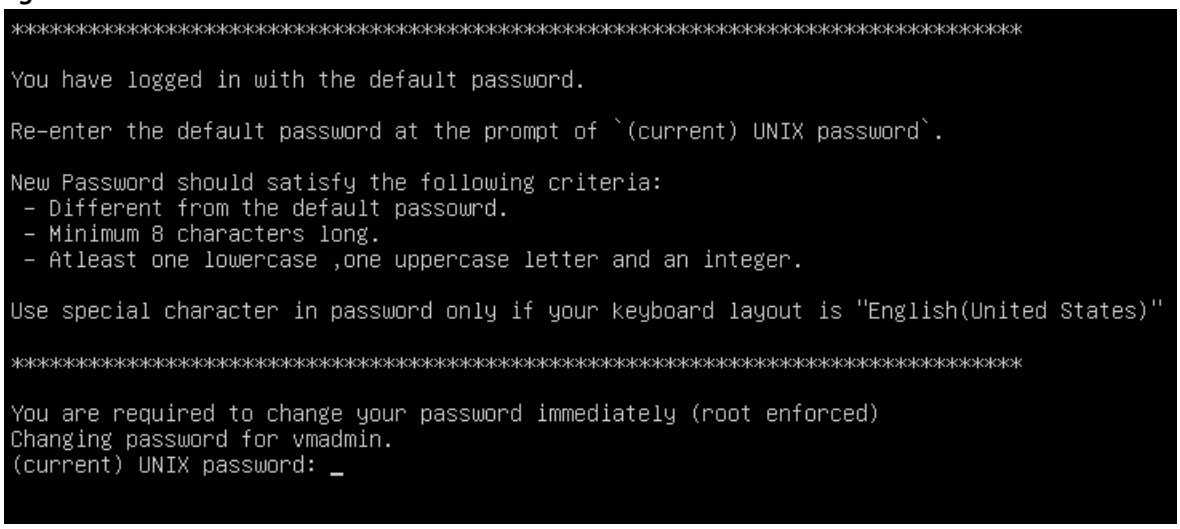
4. Press **Ctrl+B** to enter Config Mode



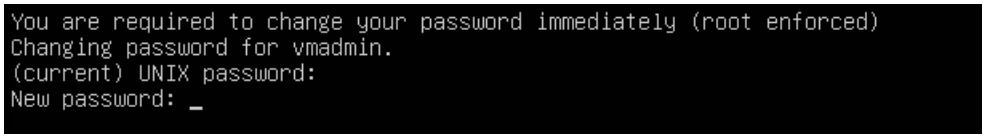
5. You will find your Org ID in the URL of your Umbrella Dashboard. In the example below the Org ID is 2385312

6. Enter the default password, in this example I will use ***Umbrella2385312*** (you won't see any text when typing the passwords)

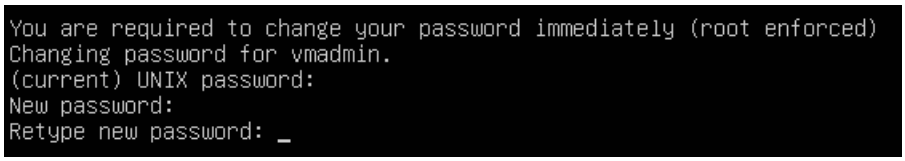
7. Once logged in, you will be prompted to change the password. ***First you will enter the default password again. Umbrella2385312***



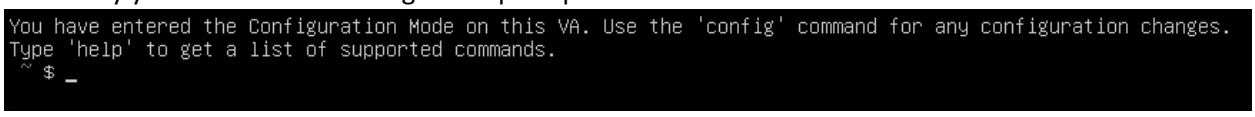
8. Then you will enter your new password. Must be complex password.



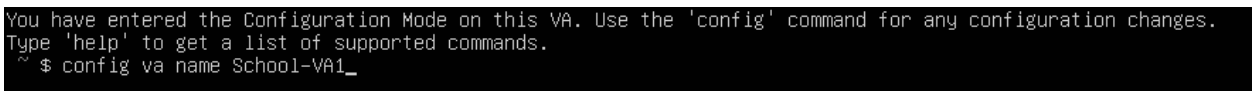
9. Retype the new password



10. Finally you will be at the config mode prompt.



11. To set the Virtual Appliance name type: ***config va name School-VA1*** (Use your school name) then press enter



12. After you press enter you will see it sets the name.

```
 ~ $ config va name School-VA1
name:  -> School-VA1
 ~ $ _
```

13. To set the IP address type: ***config va interface <IP address> <Subnet> <Gateway>*** then press enter

```
~ $ config va interface 192.168.88.11 255.255.255.0 192.168.88.2_
```

14. After you press enter you will see it sets the IP info.

```
 ~ $ config va interface 192.168.88.11 255.255.255.0 192.168.88.2
ip:  -> 192.168.88.11
netmask:  -> 255.255.255.0
gateway:  -> 192.168.88.2
 ~ $ _
```

15. To set the local DNS servers (most commonly your DC's) type ***config localdns add <dns1>*** then press enter, type ***config localdns add <dns2>*** then press enter. Each DNS server has to be added with the command individually.

```
config localdns add 192.168.88.10
```

```
config localdns add 192.168.88.11
```

16. After you press enter you will see it sets the local DNS

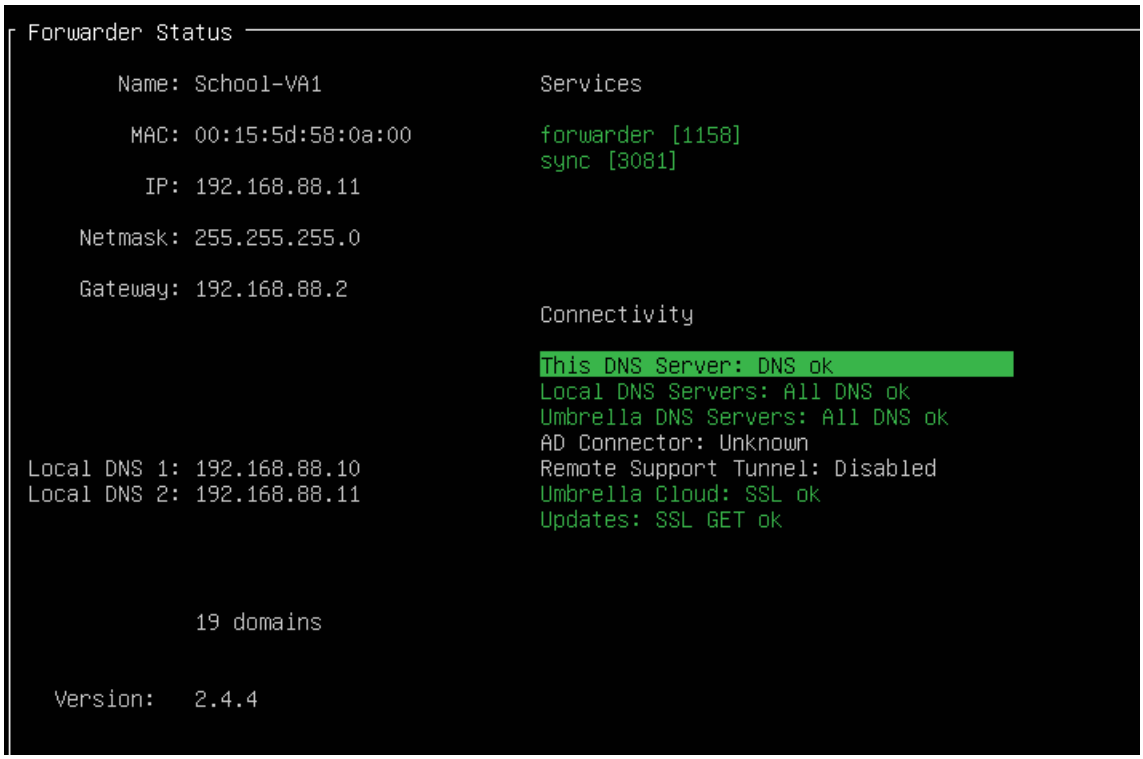
```
Localdns Server 192.168.88.10 is added successfully
```

```
Localdns Server 192.168.88.11 is added successfully
```

17. That completes the config process, type ***exit*** to exit the config mode

```
~ $ exit_
```

18. You will now see that your VA is fully configured.



NOTE: If **Support Tunnel: SSH** is red and says failed, it may take a little longer for it to make a connection. It won't hurt anything
if it doesn't at all. This tunnel is for OpenDNS techs to be able to remote into your VA to assist you if you request it.

It is also normal to see the "AD Connector: Unknown" message, as the *optional* Active Directory integration has not been configured as of yet.

Repeat Steps for the second VA

Repeat the above steps to configure a second VA. A second VA is required for continuous operation, high availability, and automatic upgrades. Do not clone the first VA. Umbrella will not recognize a cloned VA.

Warning

Umbrella VAs cannot be cloned. Ensure that your second VA is set up manually. Umbrella will not recognize a cloned VA.

Local IP and Active Directory Filtering

Finally, OpenDNS can be fully linked to your Active Directory structure. This option provides you with the most detail in reporting and identity.

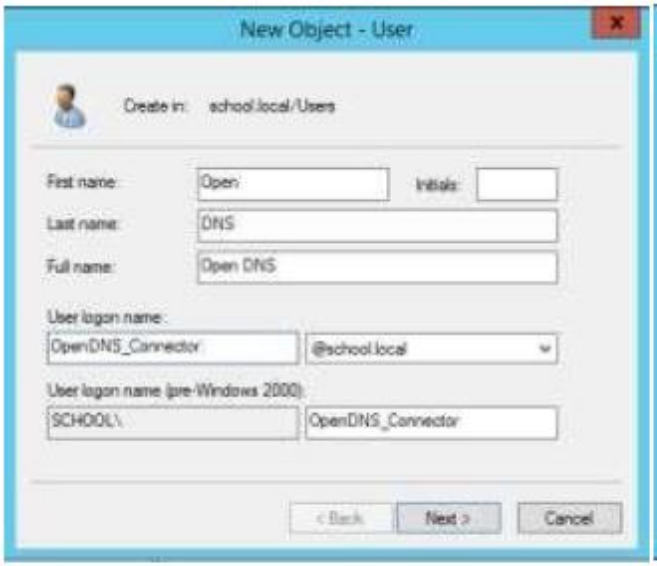
Prerequisites

- Windows Server 2012, 2012 R2, 2016 or 2019 with the latest service packs and 100MB free hard disk drive space. Service packs prior to SP2 are not supported.
- .NET Framework 4.5, or 4.7.
  .NET Framework 3.5 should not be running on the same system. If .NET Framework 3.5 is required, confirm that all Windows patches on this server are applied.
- If a local anti-virus application is running, allow list the OpenDNSAuditClient.exe and OpenDNSAuditService.exe processes.

Create AD User:

If you are going to use the AD connector then a user needs to be created and assigned to specific groups for the connector to access AD.

1. Open **Active Directory Users and Computers** and Navigate to **YourDomain.local > Users**
2. **Right Click > New > User**
3. Make the *User logon name*: **OpenDNS_Connector**
4. When creating the password, do not use a backslash or quotation marks.

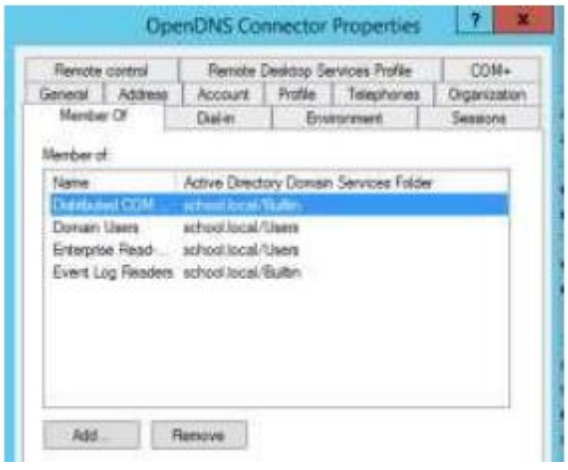


Once the user is created, add the user to the following groups by **right clicking the user** > **Properties** > **Member Of** tab > **Add**

a. **Event Log Readers**
b. **Distributed COM Users**
c. **Enterprise Read-only Domain Controllers**

Click **Apply** and **OK**

NOTE: Make the user **exactly** like the picture.

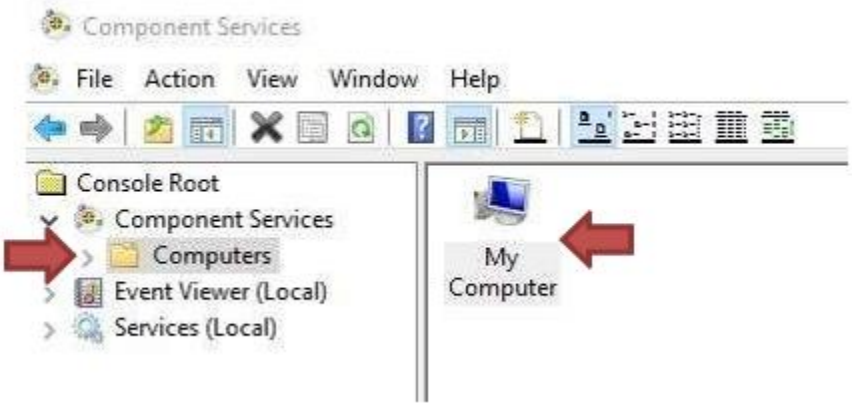


DCOM Permissions

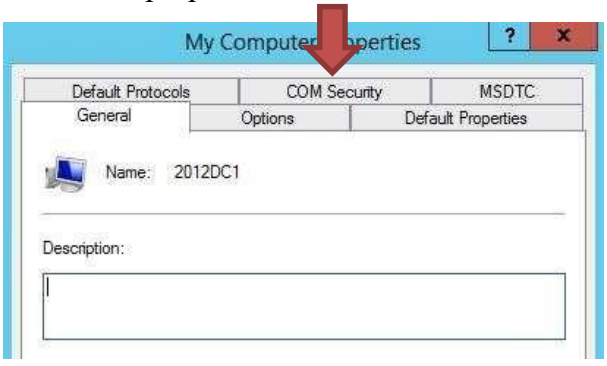
Even though we have added the new user to the correct member groups in AD, we need to manually add the OpenDNS_Connector user permissions. This may seem redundant but sometimes, even though the user is part of the groups, they don't always get the permissions needed. Let's start with the DCOM permissions.

1. Open a **CMD Prompt** and type **DCOMCNFG**

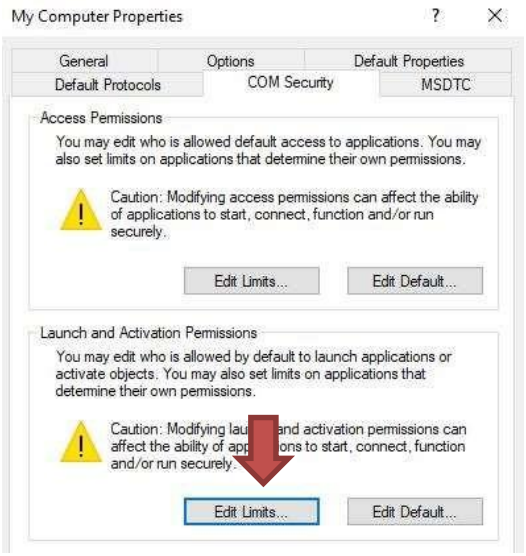
1. When the new window opens, expand **Component Services** and click on **Computers.** **Right Click** on **My Computer** and select **Properties**



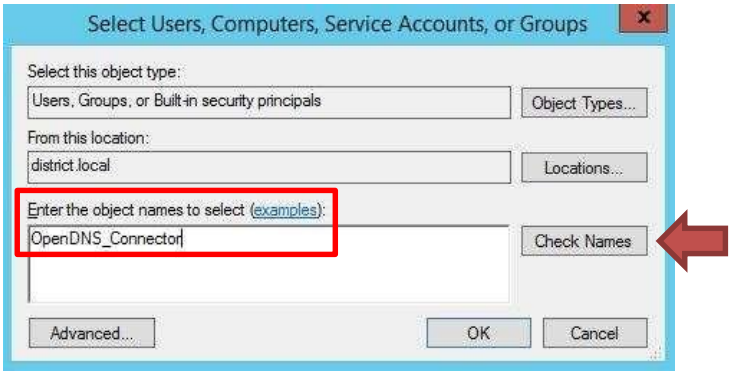
2. In the new properties windows, click the **COM Security** tab



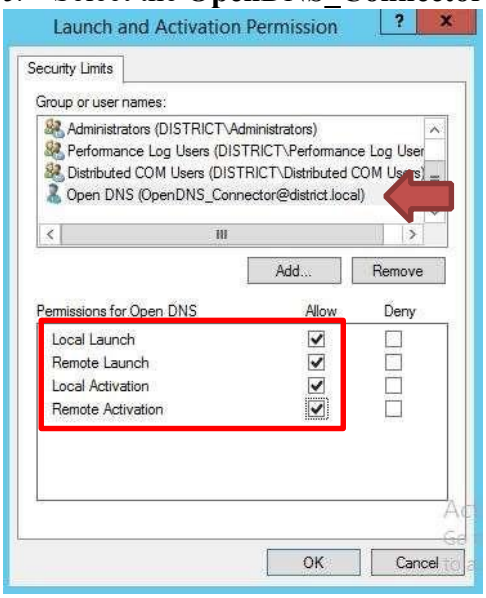
3. Under the **Launch and Activation Permissions** section, click on **Edit Limits…**



4. Select **Add..** then type in **OpenDNS_Connector** in the box and click **Check Names** and **OK**



5. Select the **OpenDNS_Connector** user and **put a check mark in <u>all four</u> boxes below**.



6. Click **OK > OK > Close** the **Component Services** window.

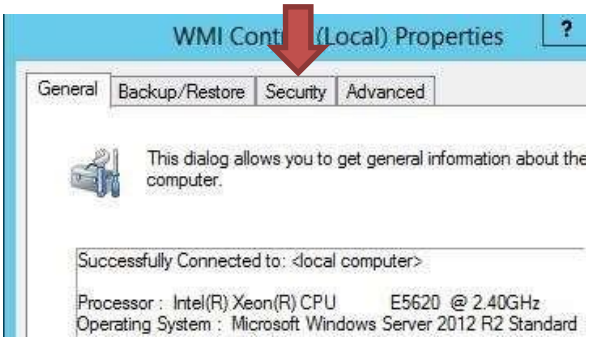
7. **Restart** the machine.

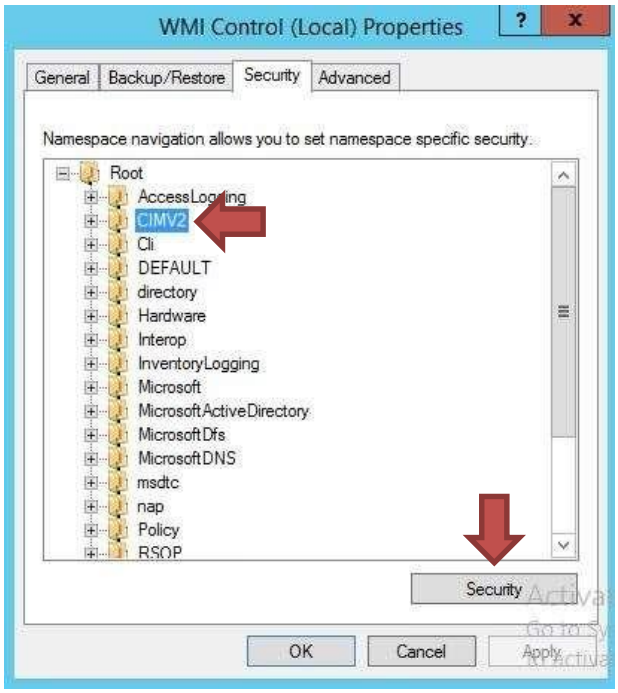
WMI Permissions

1. Open a **CMD Prompt** and type **WMIMGMT** and press **Enter**

2. When the **WmiMgmt** window opens, right click on **WMI Control (Local)** and select **Properties**

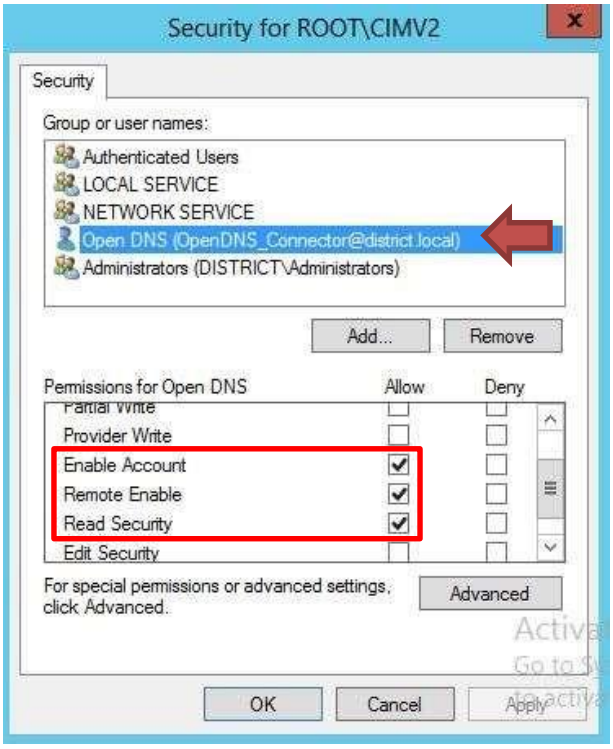
3. Select the **Security** tab, **expand Root**, **highlight CIMV2,** then click the **Security** button at the bottom on the window





4. Verify that the **OpenDNS_Connector** user is listed with the following permissions.
   Enable Account: Allow
   Remote Enable: Allow
   Read Security: Allow

   If it is not, then **add** it with these permissions.



5. Click **OK > OK > Close the WmiMgmt** window.

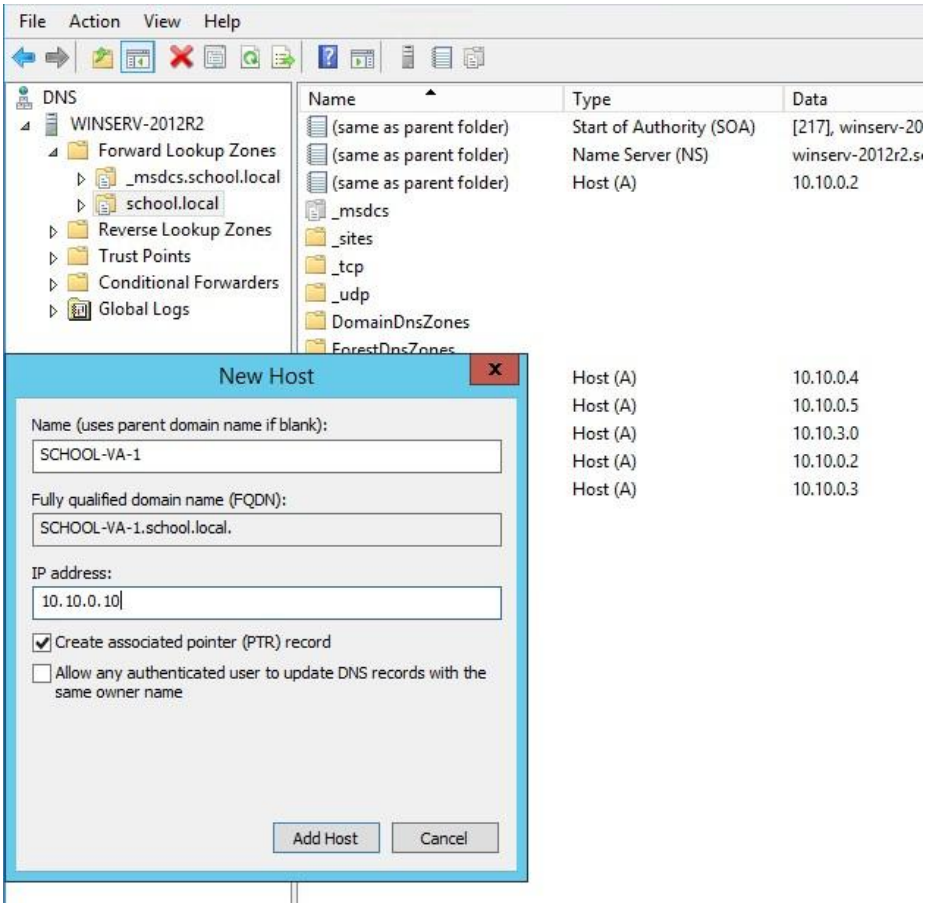
Active Directory Integration

Configure DNS

It's time to prepare your network for Active Directory Integration. You will want to create PTR and A records for your VAs on your DNS servers.

1. Open your **Server Manager** on your Primary DNS server
2. Click **Tools > DNS**
3. Expand your **server name** > **Forward Lookup Zones**
4. **Right Click** your domain and select **New Host (A or AAAA)**
5. In the first box put the **name** of the VA that you used when you configured it.
6. In the IP Address: box put the **IP** used during the configuration.
7. Make sure **Create associated pointer (PTR) record** is checked
8. Click **OK**.

9. Repeat steps 4-8 to add your second VA.

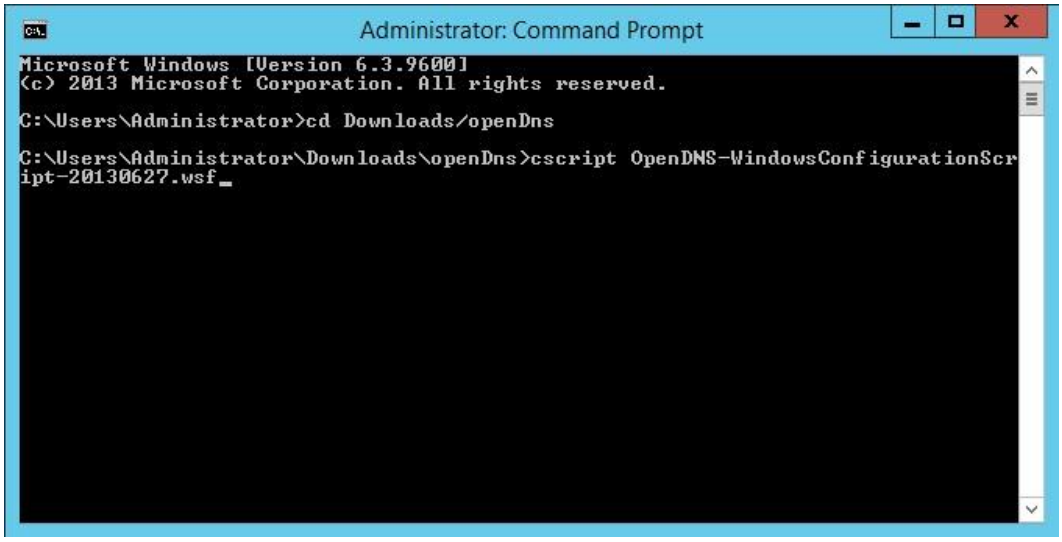


Do an **nslookup** in Command Prompt using the **IP** of the VA followed by another using the **NAME** of the VA to test that the records are created correctly and functioning.

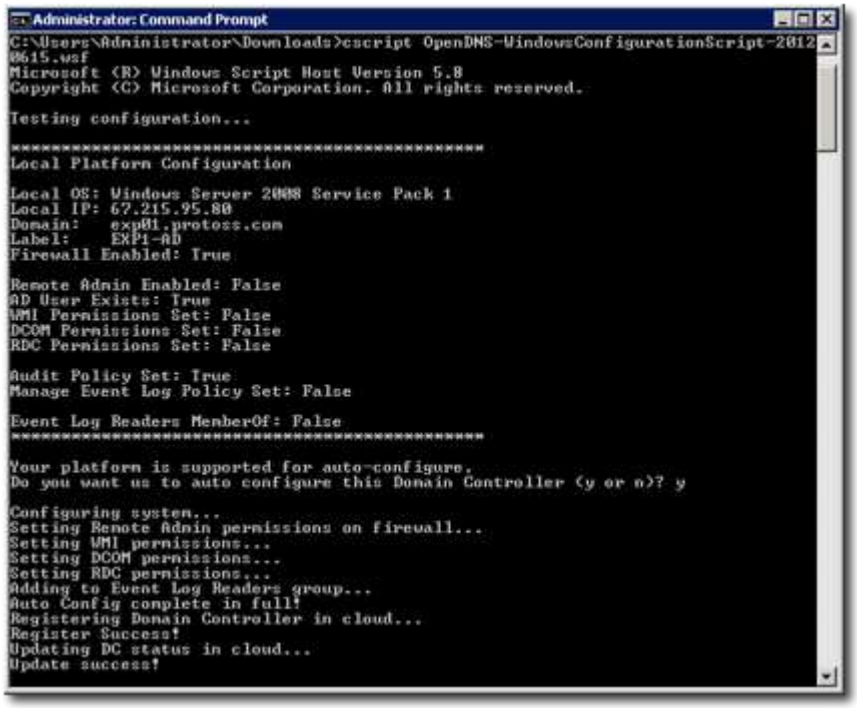
Configure Active Directory

Now we need to configure Active Directory to prepare it for the Connector. In order to do so we need to run a script that you downloaded during the Prerequisite portion of this guide. Make sure your openDns folder that you downloaded all of your prerequisite files to, is in the Downloads folder or a folder easy to navigate to. For this guide we will use the Downloads folder.

1. Open an **ADMIN CMD Prompt** on your server and navigate to your **openDns folder** inside your **Downloads** folder. (CMD: **cd Downloads/openDns**)
2. Type: **cscript OpenDNS-WindowsCon** and press the **Tab** button to auto fill the rest of the name or manually complete the name and press **Enter**.



3. The script will display your current configuration, then offer to auto-configure the Domain Controller.
   Press **Y** and **Enter**.



4. Copy the script to each one of your **DCs** and repeat steps 1-3 to fully prepare your AD environment for the connector.
5. Verify your AD Server shows up in the OpenDns Dashboard.

Connect Active Directory

The next step is to install the Active Directory Connector now that the VAs have been installed and the Script has been ran on ALL of your DCs. You will need the password to the OpenDNS_Connector user that you configured at the beginning of this guide. You only need one connector per site.

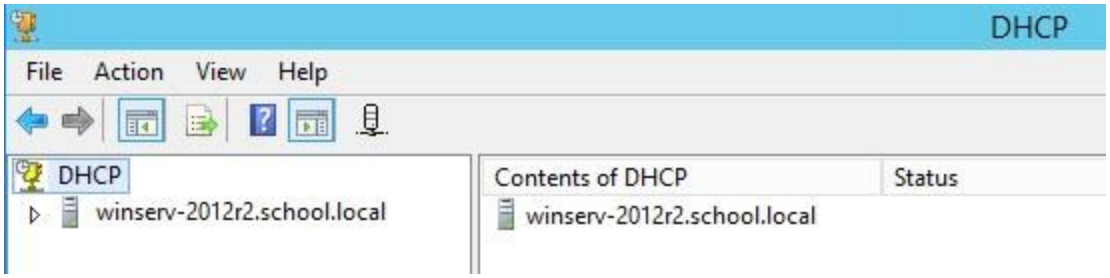
1. Open the openDns folder that houses all of your Prerequisite files. Find the .zip file **OpenDNS-WindowsService-20160128.zip** and extract it.
2. Once extracted, open the folder and run the **setup.msi**
3. When prompted, enter the password you used to configure the user **OpenDNS_Connector** in the Prerequisite section of this book.
4. Follow the setup wizard prompts and click **Close** when finished.
5. Verify that the server name you installed the connector on shows up in the OpenDns Dashboard (Settings > Sites and Active Directory) and that in the **Type Column** it shows **AD Connector** next to it.

NOTE: You can verify that the integration is complete by verifying that the jellies in the status column of **Sites and Active Directory** in the **Dashboard** are showing green in all boxes, especially the AD Connector box and the AD Server Box. It may take a few minutes for them to turn green and the import to show results. Once they are green you can verify further by going to **Policies** > **Policy List** and creating a **new Policy** and confirming that your groups are present.

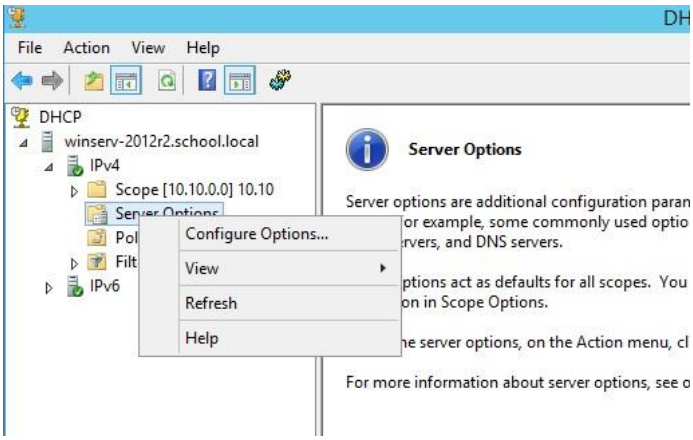
Setup DHCP

Now that you have your VAs installed and configured, your AD is integrated into the Umbrella Dashboard, and your Policies List is setup the last thing you need to do is configure your DHCP to handout your new VAs as the DNS servers for your network.

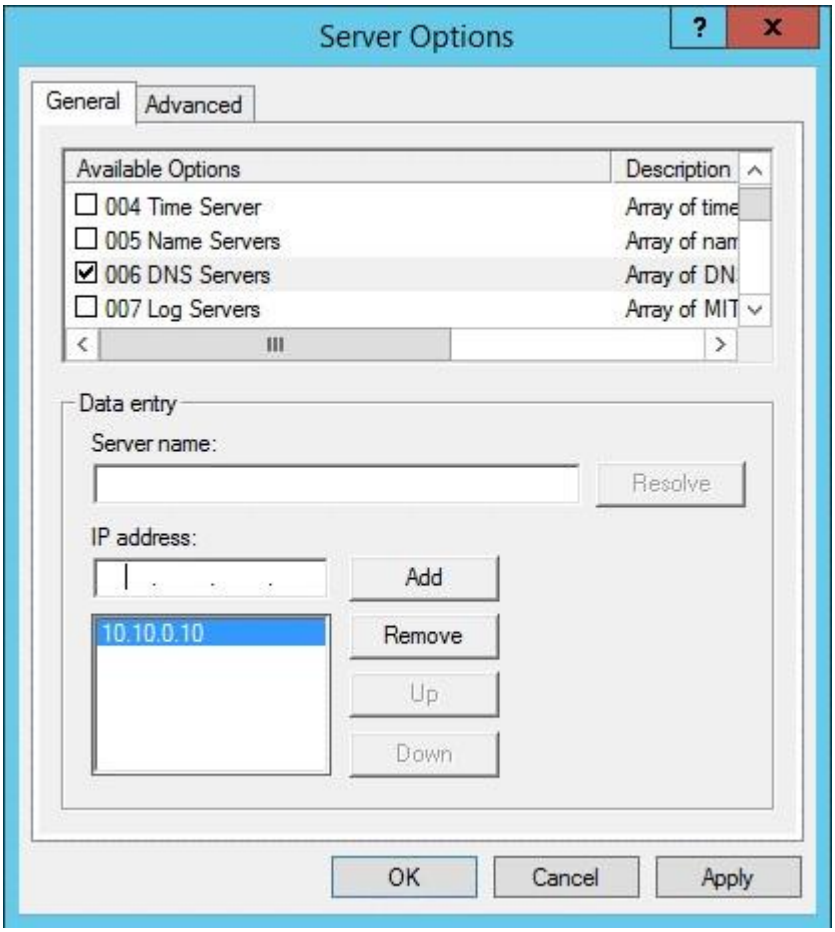
1. On your **DHCP Server** open **Server Manager > Tools > DHCP**
2. Expand your **Server Name > IPv4**



3. Left Click on **Server Options** in order to get the right click menu to be available. 4. Right Click **Server Options** and select **Configure Options**



5. Put a check in the box next to **006 DNS Servers**
   NOTE: If there is already a Check Box here just delete and servers already listed.
6. Either put the name of the VA in the Server Name: box and click resolve or enter the IP Address in the box below it and click Add.
7. Repeat Step 6 for your second VA.



8. Click **Apply** and **Ok**

NOTE: Depending on your lease time, after updating the DNS Servers in the DHCP options, wait for DHCP leases on the endpoints to expire and see the new changes. In most cases, DHCP lease durations are 7 days or less, but sometimes may be set to higher values.

Final Configuration

Configure Internal Network

Internal Networks allows to you manage your Umbrella policy for subnets of computers based on the internal IP addresses of your network.

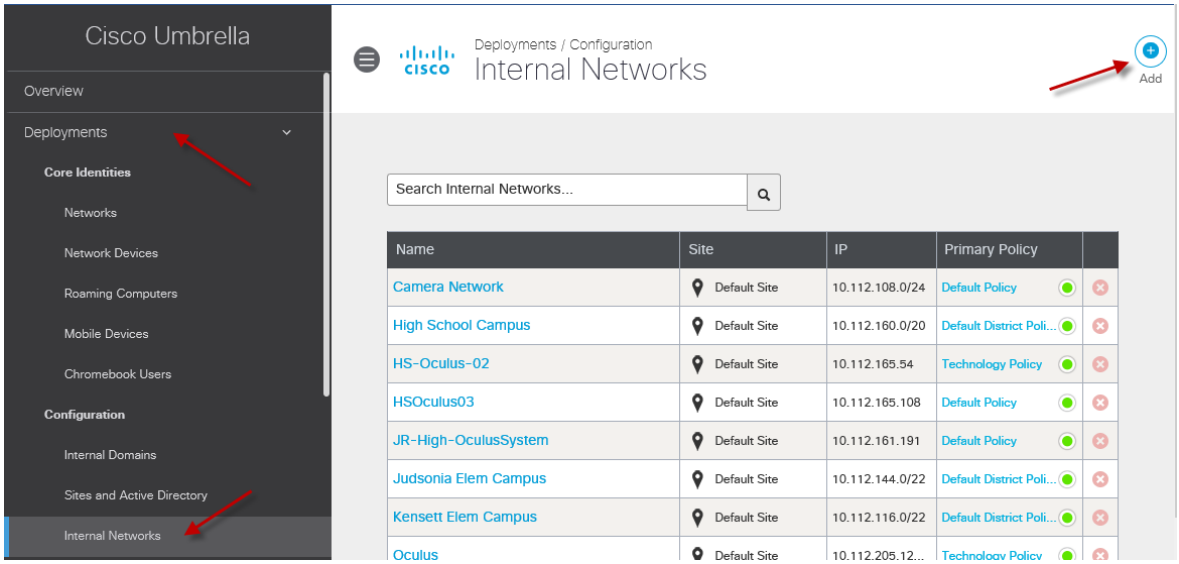
After an Umbrella Virtual Appliance (VA) has been deployed, an Internal Networks identity can be configured. To set this up, drop one of our lightweight VAs into your network, direct your DNS traffic through it, and start mapping your network based on specific internal IP addresses and/or subnets.

The purpose of the Internal Networks identity is to define a subnet that's non-routable (or RFC1918 compliant) as an identity you can apply policy to. To create an Internal Networks identity, define a subnet that's non-routable (or RFC 1918 compliant) as an identity you can apply policy to. For example, if your Internal Network is defined as 192.168.0/24, any computer, tablet or device with an IP on that subnet would receive the filtering policy defined for it whenever it made a request to access the Internet.

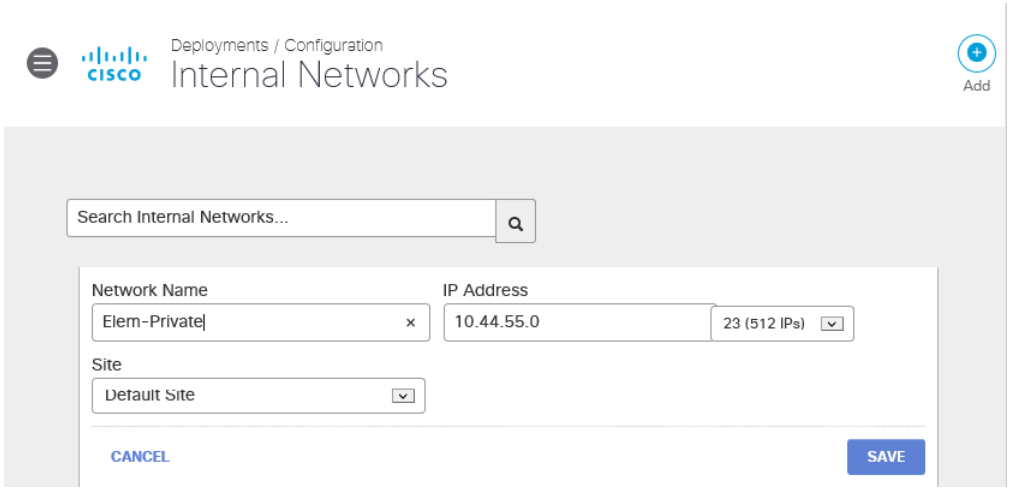
From there you can begin to build multiples sites if you have more than one physical location or if you have more than one Internal Network to configure.

The Umbrella VA will have your DNS traffic pointed to it for this configuration and anything identified as coming from the networks you've defined will have the policies applied.

1. Navigate to **Deployments** > **Configuration** > **Internal Networks** and click **Add**.



2. You'll be asked to name your network and provide a valid subnet. In this case, we've picked a /24 subnet, so the final octet of the IP will be .0



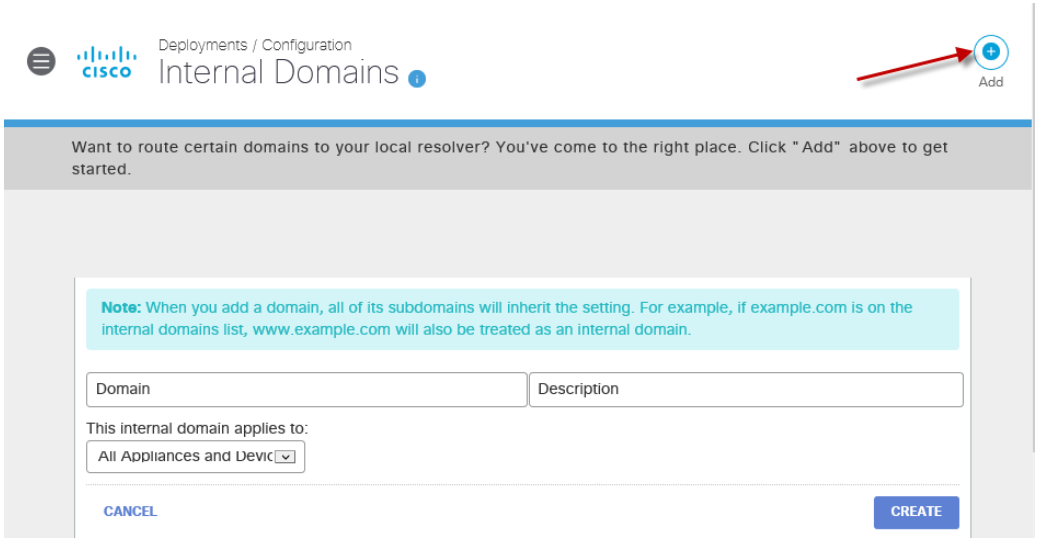
3. Click **Save**.

Note: If you are unable to save your changes, it may be because the Cisco Umbrella Internal Networks setup does not allow an invalid range to be configured. The basic principle is that the final octet of your IP range should match the mask for that range. More information about subnet masks, as well as tools, are easily available from many third-party websites.

You can assign an individual Internal Network policy to a single IP address or to an entire DHCP scope that's already been configured for your network.

Domain Management

1. In the Umbrella dashboard, navigate to **Deployments** > **Configuration** > **Domain Management**.



Any DNS queries received by the VAs which match a domain on the Domain Management list, or subdomain thereof, will be forwarded to the local DNS server as described in Configuring your VAs.

The following domains/zones are pre-populated and do not need to be added:

- RFC1918—Non-publicly routable address spaces used only for reverse DNS on internal networks. All local IP address space for reverse lookups (PTR records) is covered with this entry. Adding in-addr.arpa reverse lookup zones is not needed.
- .local—Any domain name with a TLD of .local.

You have a choice of what type of identities are set to respect these internal domains:

- All Appliances and Devices
- Roaming Devices Only
- Virtual Appliances Only

If you do not plan on using Umbrella roaming clients**, you may leave this option at the default setting (All Appliances and Devices). If you plan on using Umbrella roaming clients, we recommend reading the following document and document subsection for more information:
•Appx B. Virtual Appliances
•Appx D. Internal Domains

Which domains should be added?

Any domain name which has a forward lookup zone on your local DNS servers must be added. If you already know which domains to add, click here to skip this section.

On Windows Server, this information is located in the DNS Manager tool.

1. Open the DNS Manager (Start > Run > and type "dnsmgmt.msc").
2. Expand the Server name and Forward Lookup Zones sections. Any domains listed here are treated as local by your local DNS forwarders and must be added to the Internal Domains section of the Umbrella dashboard. This is a critical part of the setup process.

Configure Policies

Before we convert your network to OpenDNS you might want to setup your filtering Policies. OpenDNS Policies are a top down process, meaning your endpoints will start from the top of the list and work their way through to the bottom. If they do not get blocked by any policy that is linked to them, then they will be allowed access.

The bottom Policy will always be Default Policy and this is the state level policy that blocks Pornography only. It uses the "**Centralized Default Settings**" Category Setting which is managed by the state and can only be edited by the state.

This guide will walk you through setting up your own **District Default Policy** to site above the **State Default Policy** so that you can manage your bottom level filter. It is recommended that you make this a very restrictive policy to be your safety net at the bottom of your policy list.

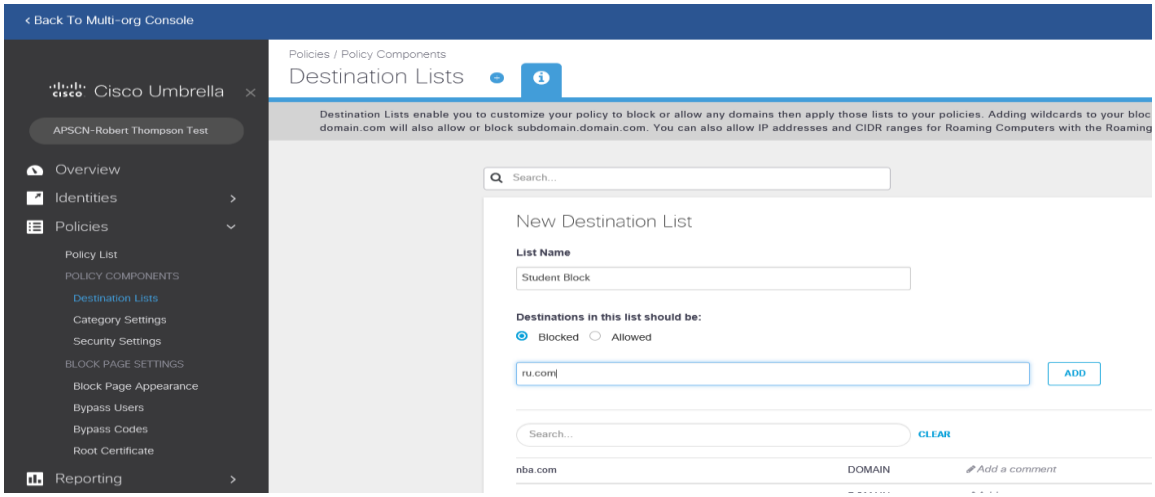
Before we can create the Policy itself, we need to create the **Destination Lists, Category Settings, Application Settings,** and **Security Settings.**

Destination Lists

For each policy you will need **2** Destination Lists, one will be an **Allow** list and the other will be a **Block** list. These two will be your **granular control** on each policy allowing you to Block or Allow websites on a URL basis. If your End Users find a website that is being blocked by a Category in your Policy and you do not want to unblock the whole Category to allow access to this particular website, you would put the website in the Allow Destination list.

1. Navigate to **Policies > Destination Lists**
2. You will see two Destination Lists already exist. **Global Allow List** and **Global Block List**
    a. The **Global Allow** and **Global Block** will always be attached to every Filter Policy and **cannot be removed**. For this reason, you should be very careful what you add to these two destination lists.
    b. If you already have a Whitelist or a Blacklist from another filter, you can upload using a **.CSV** file with each domain on a new line, and select **Bulk Upload Domains.**
3. To **create a new Destination List**, click the **small blue plus sign** at the top of the page.

4. Type a **name** and **choose** whether this is an **Allow** or a **Block** list and click **Save**.
5. Create both a **Default Allow** and a **Default Block** Destination List.

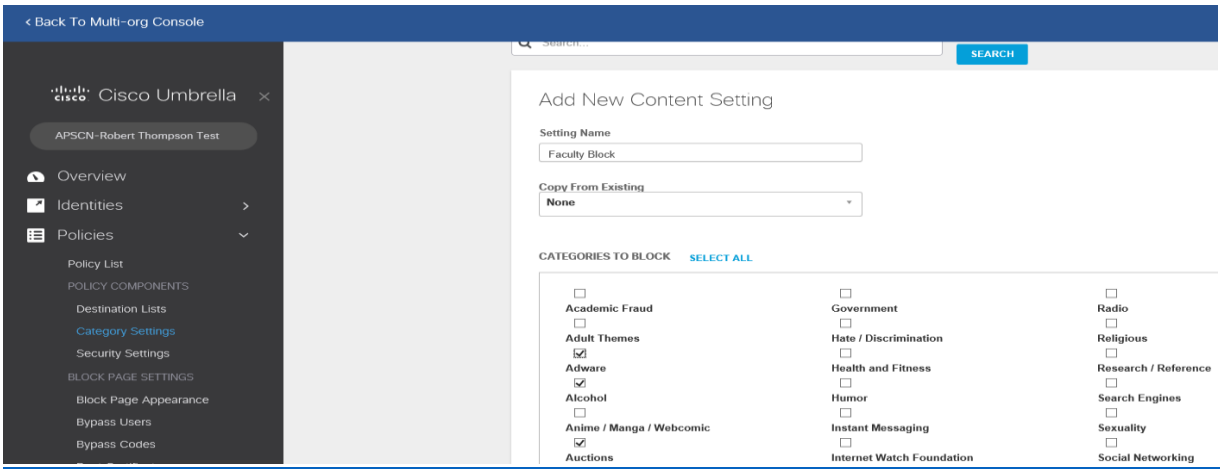


Category Settings

1. In the OpenDns Dashboard, Navigate to **Policies > Category Settings**
2. Here you will be able to VIEW the "**Centralized Default Settings**" Category List **but not edit it**. Another Category List should already exist called **Default Settings**. This one you can edit but not delete so let's click on it.

    a. To add your own Category Lists in the future, click the **blue plus sign** at the top of the page.

3. Navigate through the list putting checks in everything that you want blocked in your overall filter.

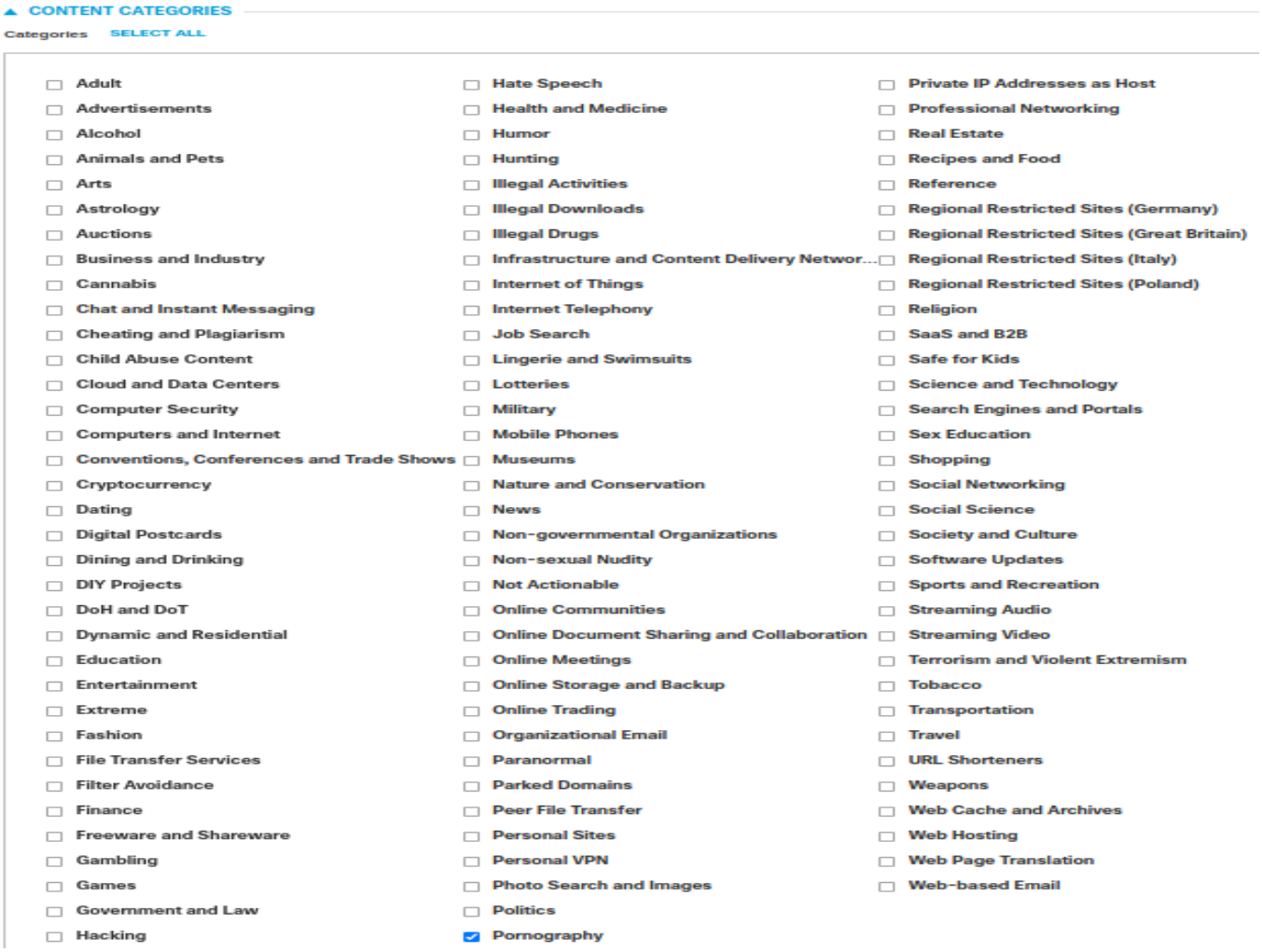


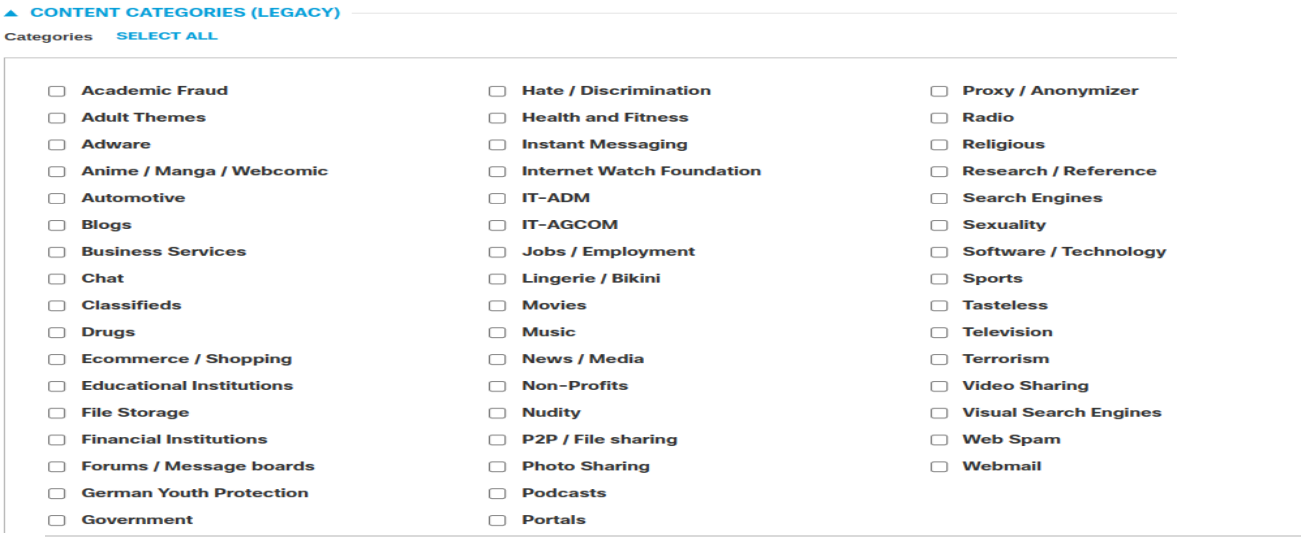
    a. **Always** check **Pornography** when creating **EVERY Category Setting**. This is because once a user authenticates to a Policy in OpenDNS, they are then governed by that policy only. I.E. If Pornography is blocked in every Category Setting for every policy OTHER than your Students, then when students authenticate and pull

the Student Policy, they would be allowed to access porn no matter what policy is above or below them.

b. This filter will be the Default Filter that devices on your network will get if they do not fit into any Identity Groups in any other filter.

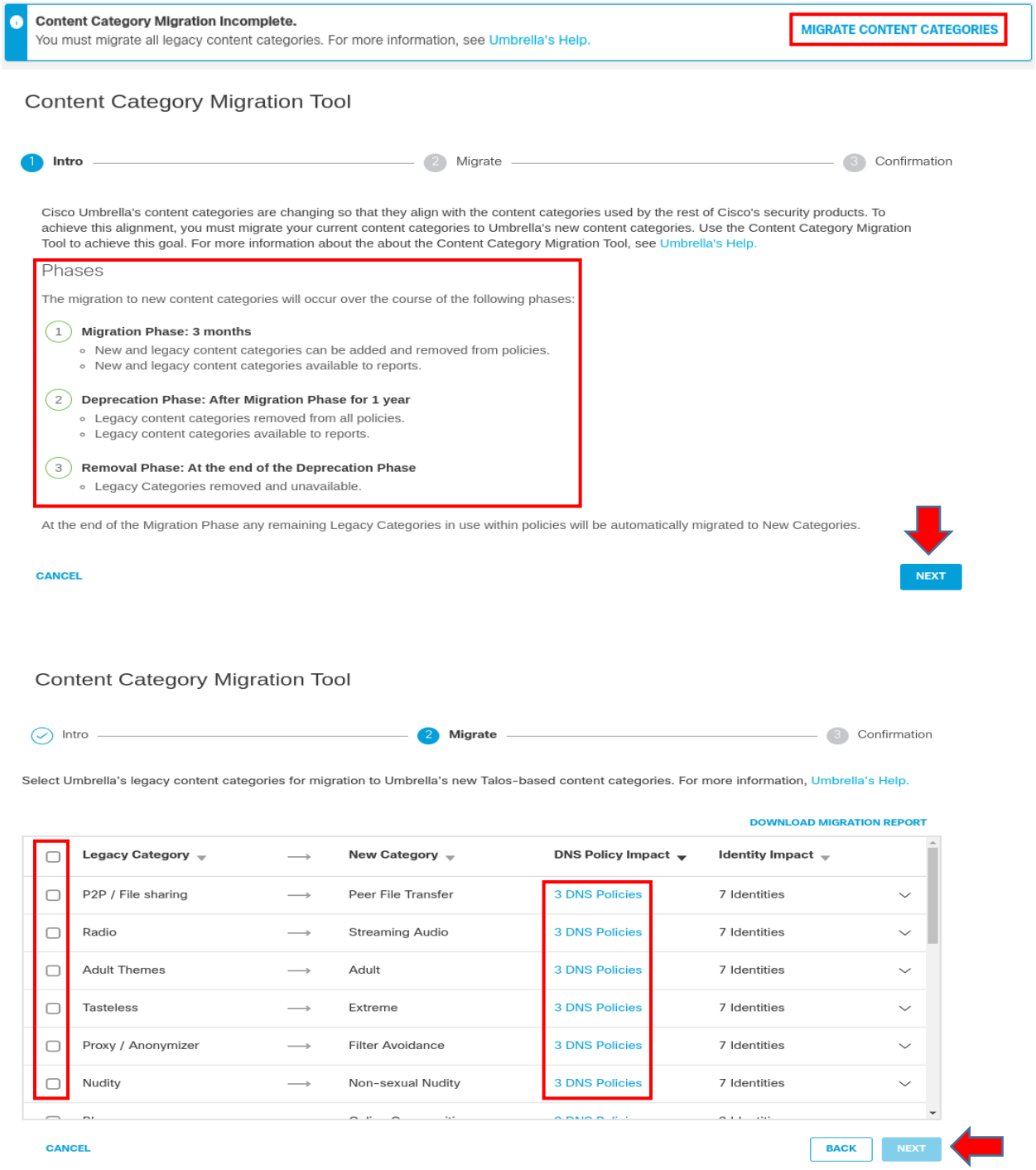
When you have selected all of the Categories that you want blocked by default on your network, click **Save.** Below is the list of all Content Categories.



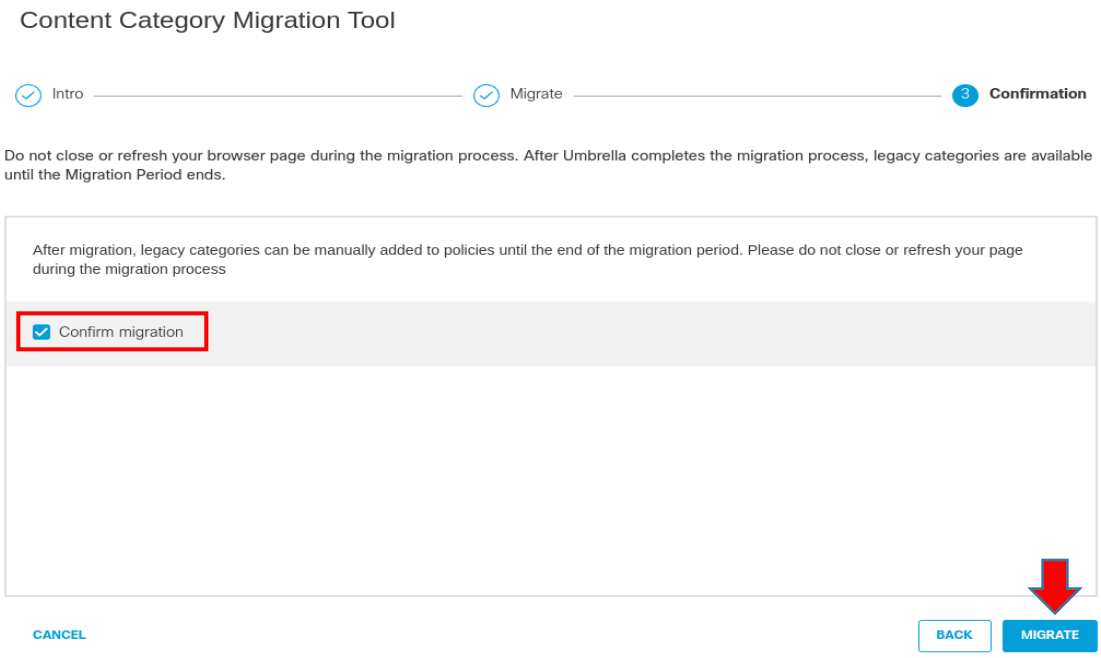


Migrating Legacy Content Categories

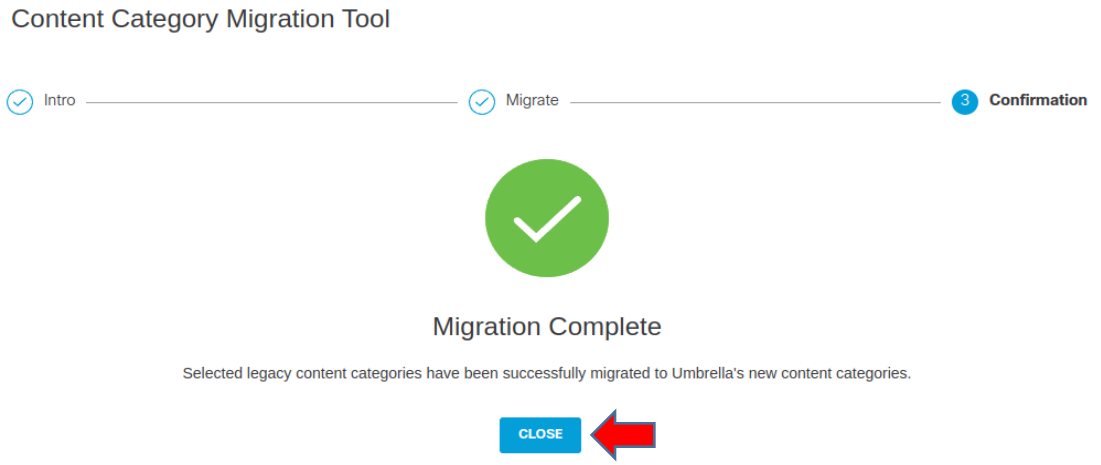
Umbrella has reorganized the content categories and when you go to the All Policies page you will see an option at the top to begin migrating Legacy Categories to Talos Categories. The Migration Tool will walk you through the whole process. To begin click on Migrate Content Categories. This will open the Content Category Migration Tool and explain the Deprecation Phases. Click Next.



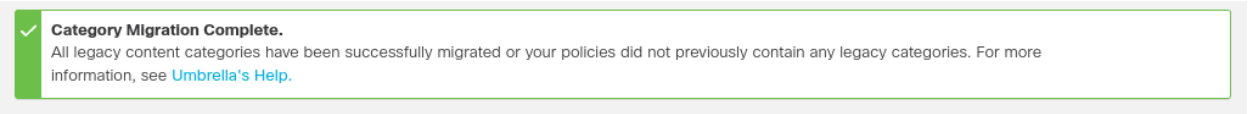
You can click on the DNS Policies that will be impacted and it gives more info. On the Migrate screen check the box next to the Legacy Category to be migrated and click Next.



On the Confirmation screen, Check the box next to Confirm migration and Click Migrate.



When the Migration is Complete, Click Close. Back under the All Policies screen you will now have a confirmation that the Category Migration has completed.



Below is a list of the Legacy Category and the new Talos Category.

Legacy Category	Talos Category
Academic Fraud	Cheating and Plagiarism
Adult Themes/ Adult	Adult
Anime/Manga/Webcomic	Entertainment
Automative	Transportation
Blogs	Online Communities

Business Services	Business and Industry
Chat	Chat and Instant Messaging
Classifieds	Auctions
Drugs	Illegal Drugs
Ecommerce/Shopping	Shopping
Educational Institutions	Education
File Storage	Online Storage and Backup
Financial Institutions	Finance
Forums/Message Boards	Online Communities
German Youth Protection	Regional Restricted Sites (Germany)
Government	Government and Law
Hate/Discrimination	Hate speech
Health and Fitness	Health and Medicine
Instant Messaging	Chat and Instant Messaging
IT-ADM/ IT-AGCOM	Regional Restricted Sites (Italy)
Jobs/Employment	Job Search
Lingerie/Bikini	Lingerie and Swimsuits
Movies	Streaming Video
Music	Streaming Audio
News/Media	News
Non-profits	Non-governmental Organizations
Nudity	Non-sexual Nudity
P2P/File Sharing	Peer File Transfer
Photo Sharing	Photo Search and Images
Podcasts	Streaming Audio
Portals	Search Engines and Portals
Proxy/Anonymizer	Filter Avoidance
Radio	Streaming Audio
Religious	Religion
Research/Reference	Reference
Search Engines	Search Engines and Portals
Sexuality	Adult
Software/Technology	Computers and Internet
Sports	Sports and Recreation
Tasteless	Extreme
Television	Streaming Video
Terrorism	Terrorism and Violent Extremism
Video Sharing	Streaming Video
Visual Search Engines	Photo Search and Images
Webmail	Web-based Email

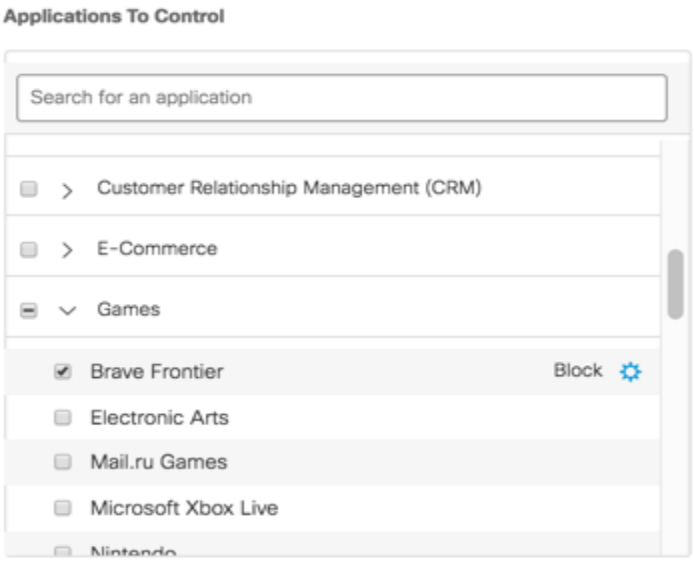
Application Settings

You can also block application categories or specific apps by configuring application settings in your policies.

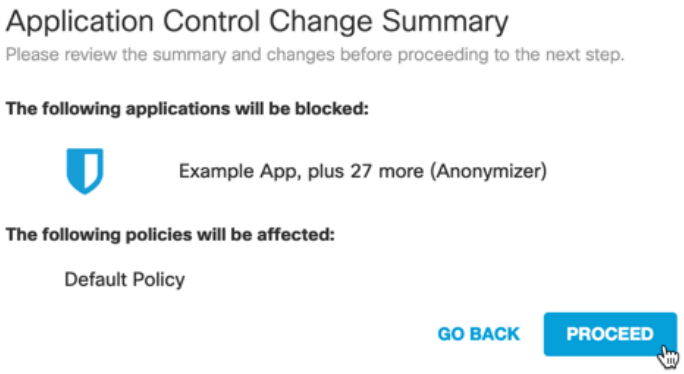
1. Navigate to **Policies > Policy Components > Application Settings.**

2. Expand an existing policy or click **Add** to create a new policy.

3. Select application categories to be blocked, or expand a category to select specific apps.



When some, but not all apps in a category are blocked, the checkbox next to the category shows a dash. When all apps in a category are blocked, the checkbox shows a checkmark. When no apps are blocked, the checkbox is empty. When settings are changed and saved in an existing policy, the Application Control Change Summary appears. Click **Proceed** after reviewing the summary.



Block Page Bypass

Block Page Bypass will not be available for any apps blocked at the domain level in Application Settings. The block page will be a static block page without the ability to enter Block Page Bypass codes.

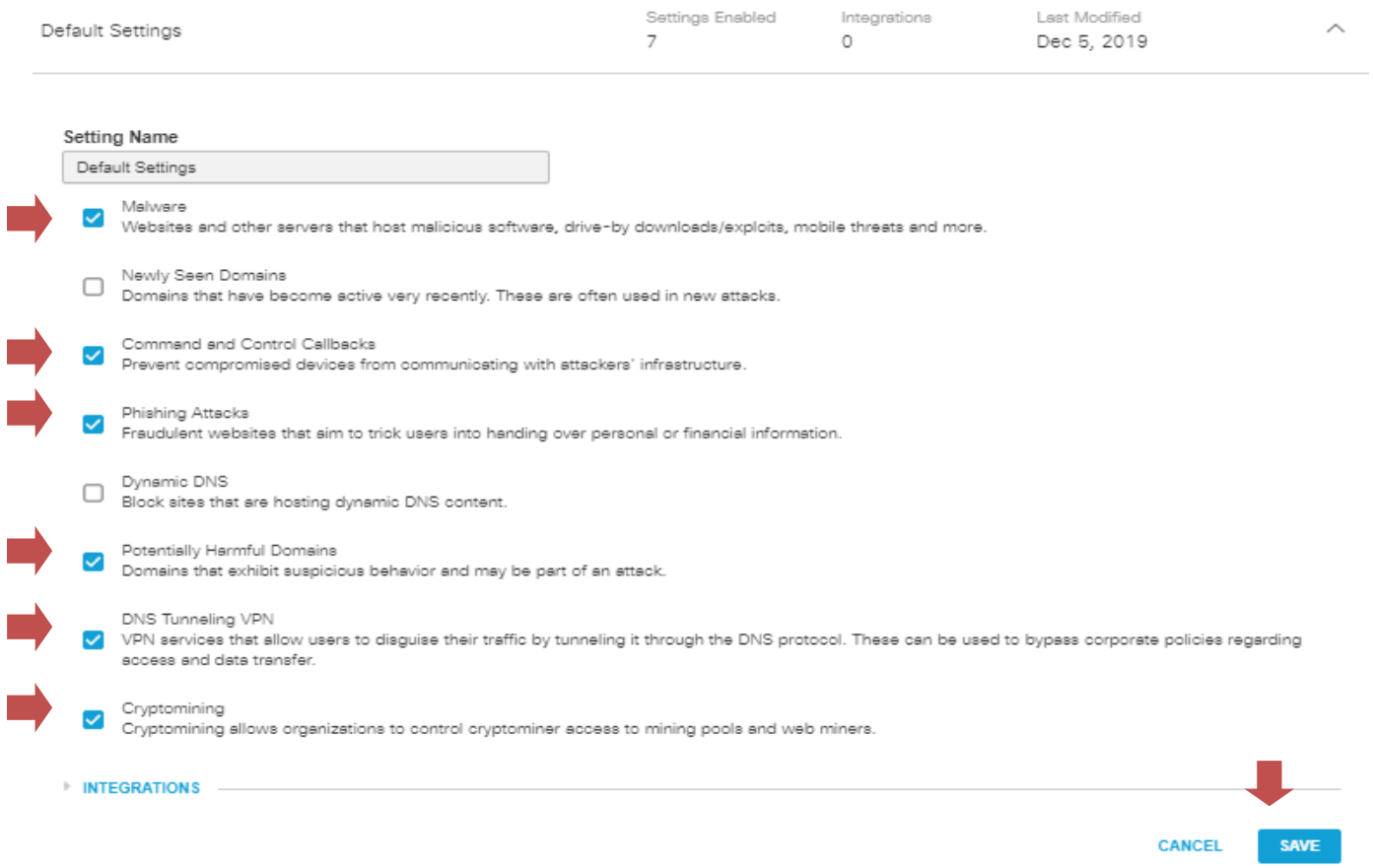
Note: For more application blocking options, use application settings.

5. (Optional) Check **Label application as** and select a label if you want to set a label in addition to blocking the app.
6. Click **Save**.

Security Settings

Now we will adjust the **Default Security** settings for your network. With **Category Settings** and **Destination Lists**, you **create a new one** every time you need to create a **new policy**. With **Security settings**, you have this option as well but it is **more common practice** to see the **Default Security Settings** used in **90% of the Filter Policies**. If you need **to create a new Security Setting**, click the **Small Blue Plus Sign** at the top of the page.

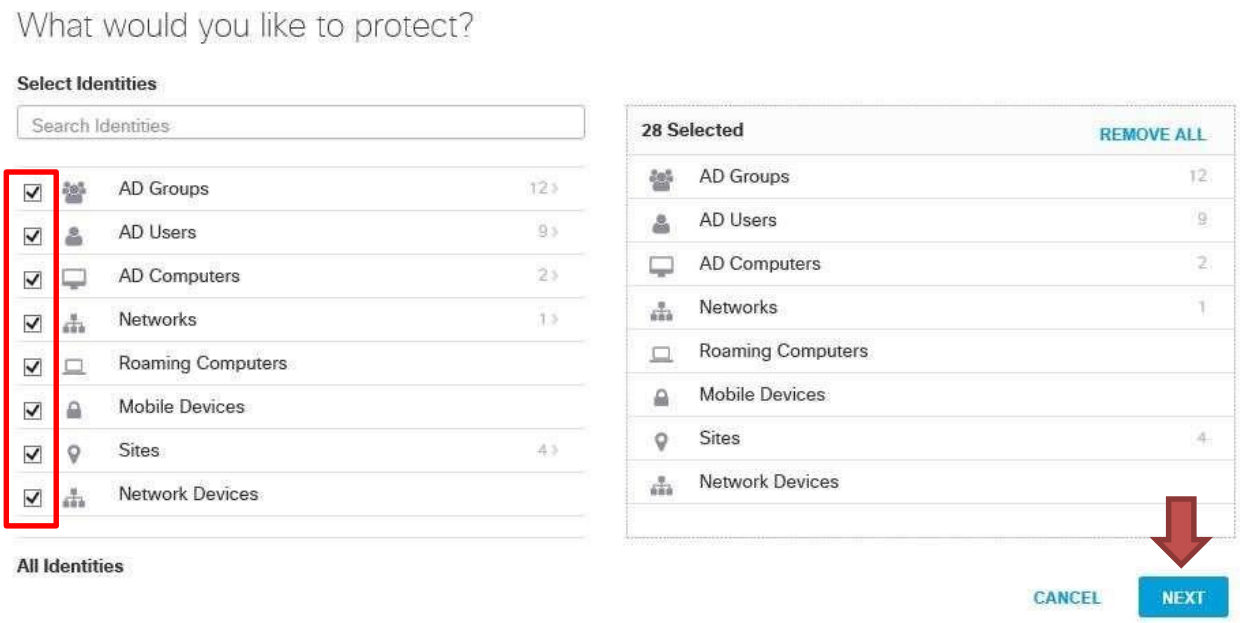
1. Navigate to **Policies > Security Settings**
2. Select the **Default Settings**
3. At the bottom, put a check mark in the box next to any box you want to have blocked on your network. Most common options that are chosen are:
    a. Malware
    b. Command and Control Callbacks
    c. Phishing Attacks
    d. Potentially Harmful Domains
    e. DNS Tunneling VPN
    f. Cryptomining
4. Click **Save.**



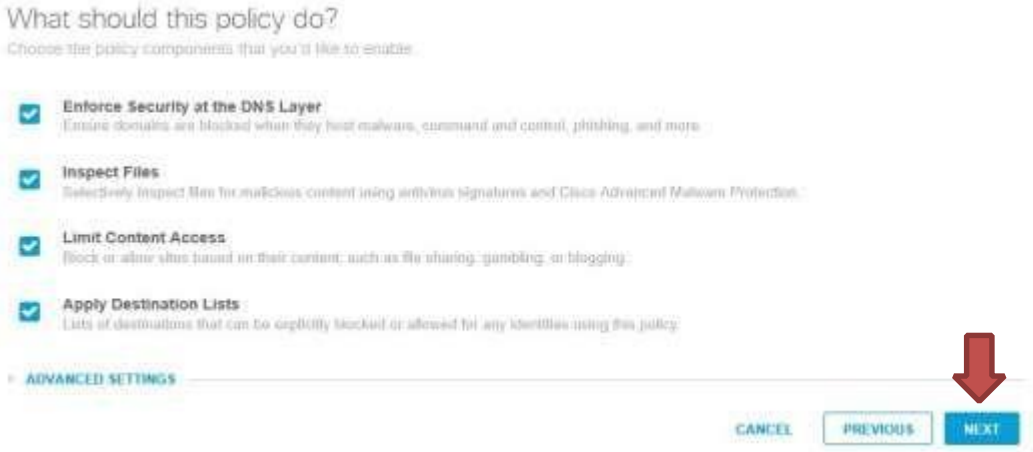
Policies

You can now create your new **District Default Policy**. In your Policy List you will see a **Default Policy**. This policy will always be at the bottom of your list and it contains the **Central Settings** that are managed by the state. You **cannot** edit or remove this policy.

1. Navigate to **Policies > Policy List**
2. Click the **Blue Plus Sign** at the top of the page
3. Since this is a **District Wide Default Policy** we will be selecting **ALL Identities**
    a. For **Student, Faculty, etc** policies, click on the **AD Groups** identity and search for the **corresponding Active Directory Group**.



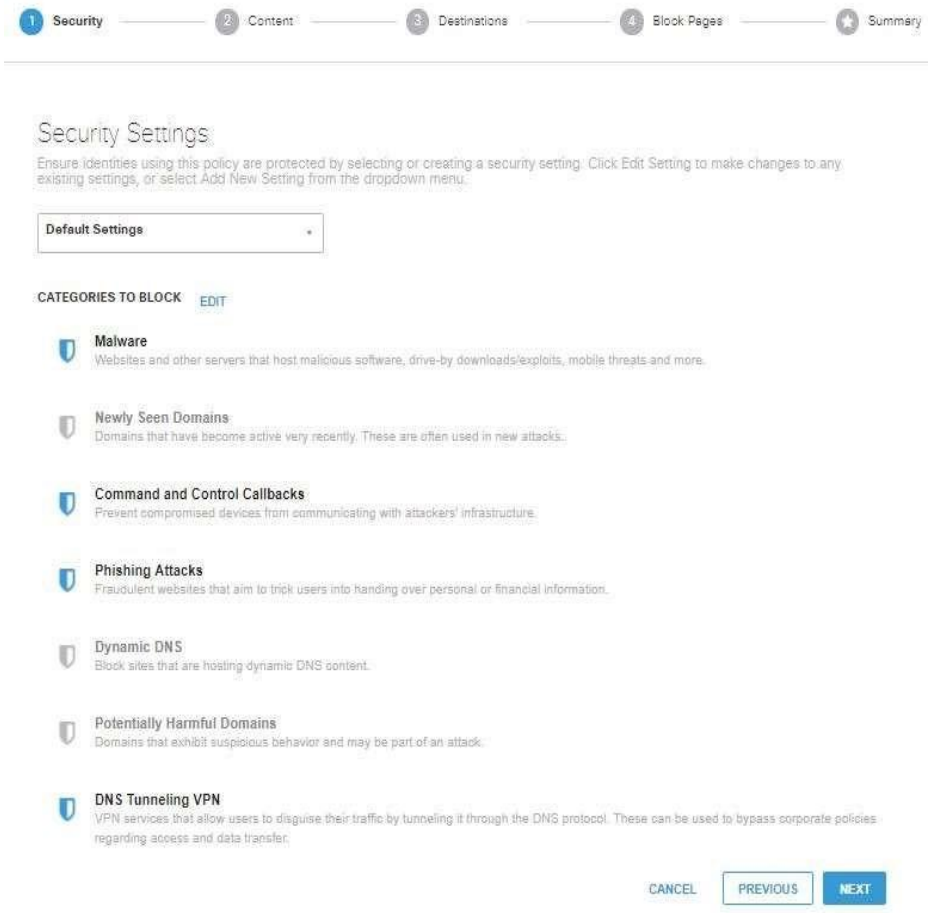
4. Click **Next**
5. On the "What should this policy do?" page, click **Next**



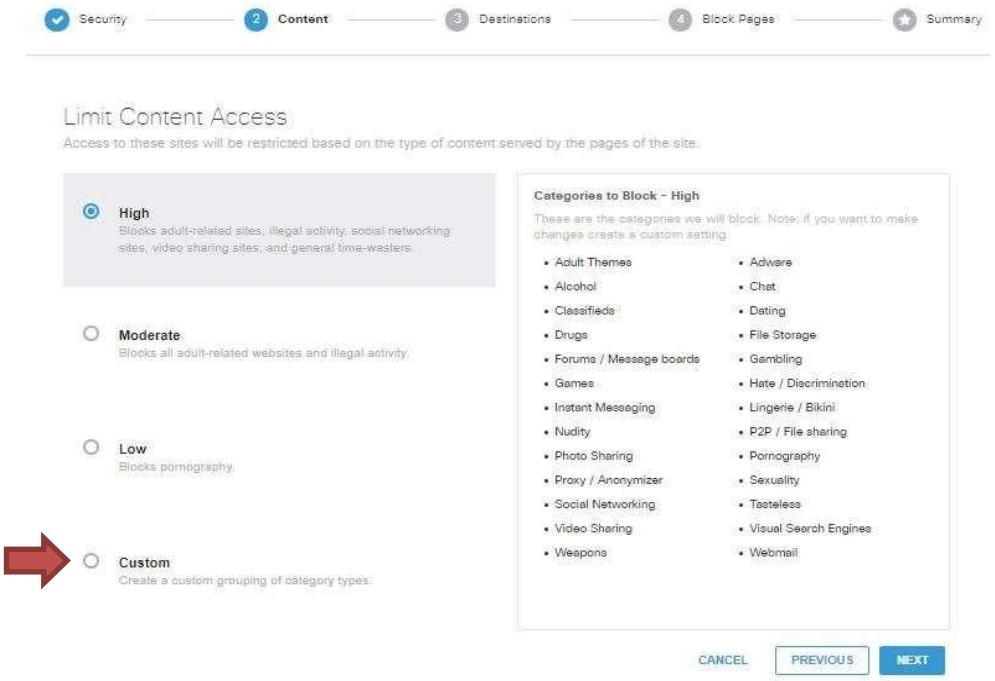
6. On the **Security Settings** page, click the **drop down** and select **Default Settings** then click **Next**

    a. The Security Settings can be edited from this page by clicking **Edit** but changes made here will also be made to **<u>every policy</u>** that uses the **Security Settings component**

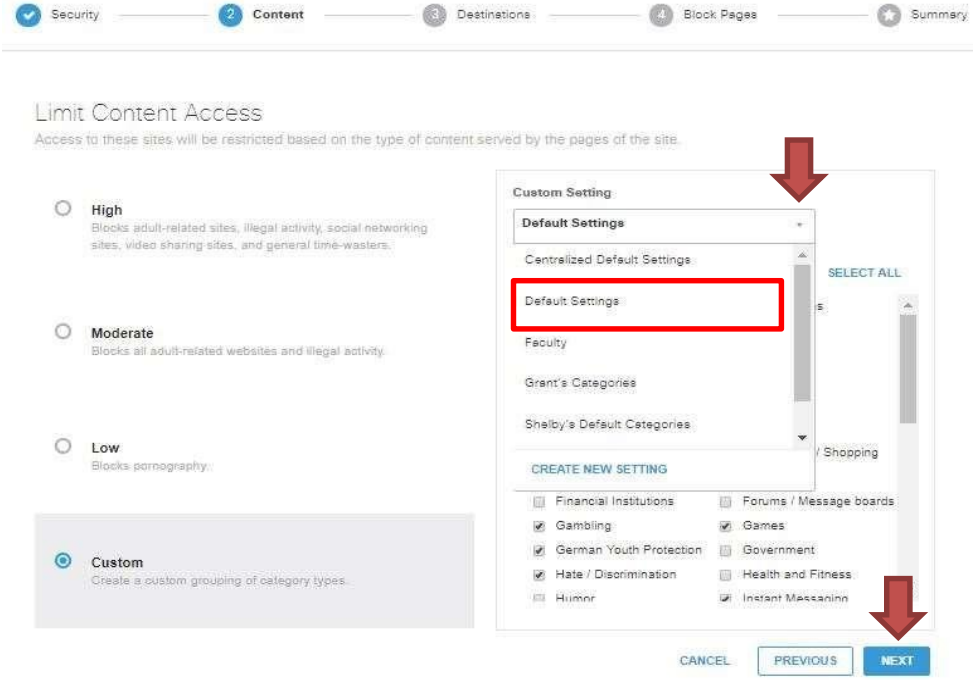
that has been chose here.



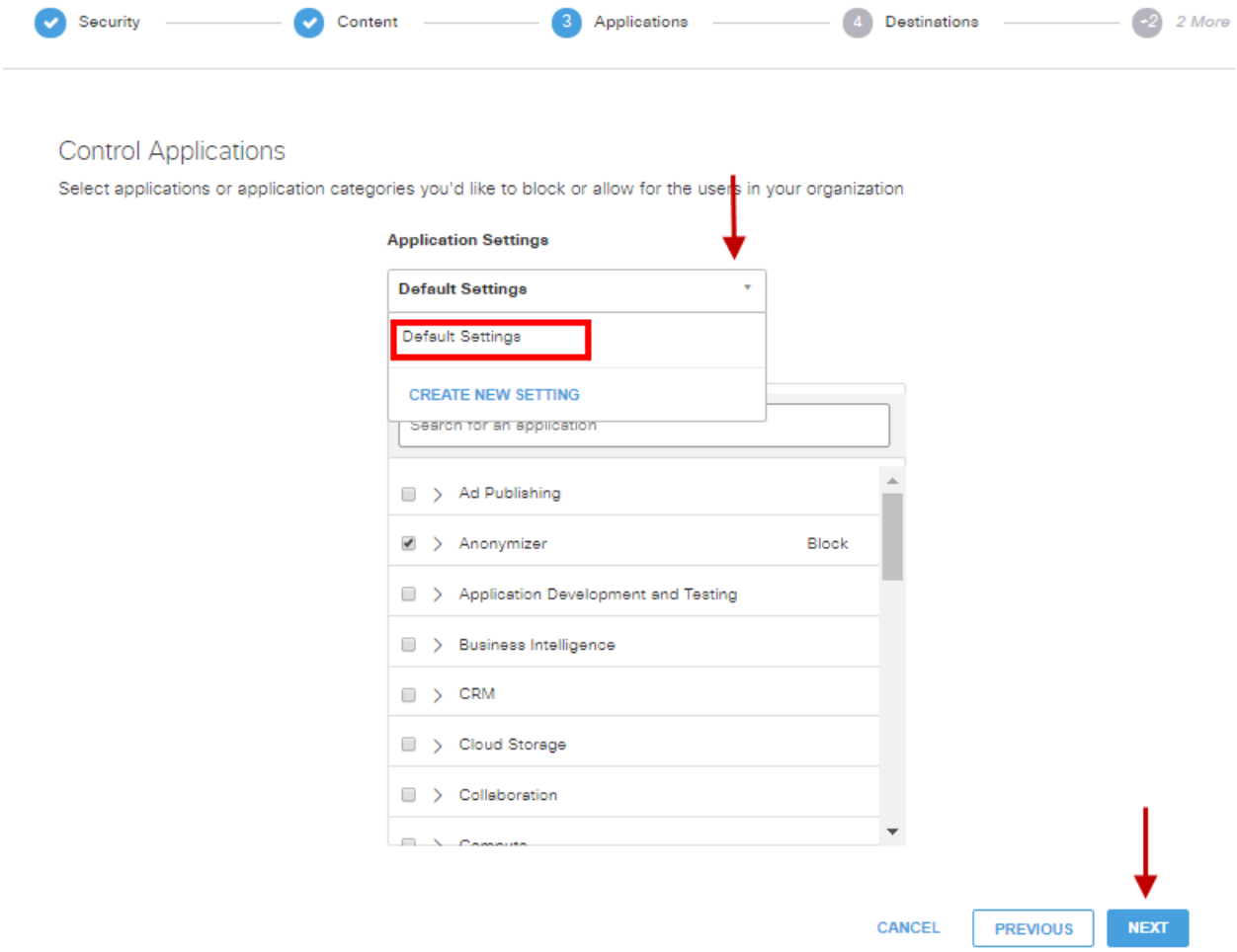
7. On the **Content Page** select **Custom,** then from the drop down on the top right, select **Default Settings** and click **Next**



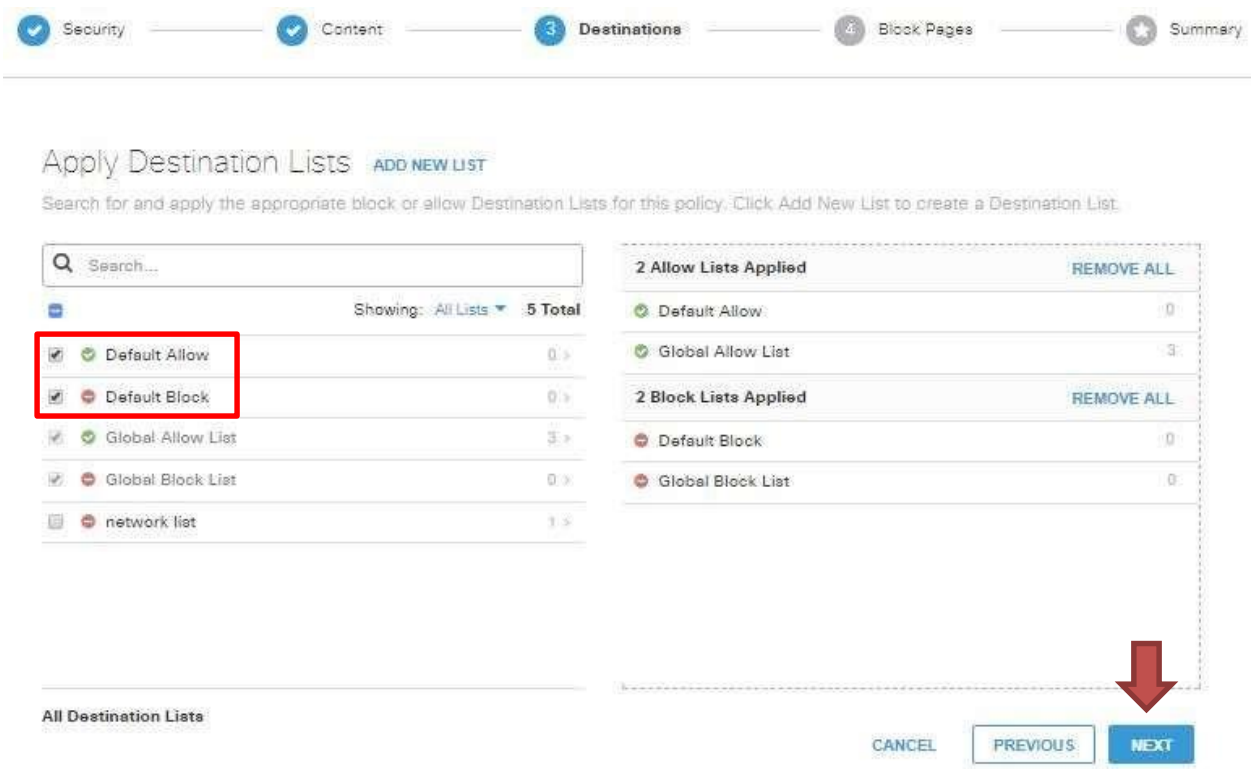
.



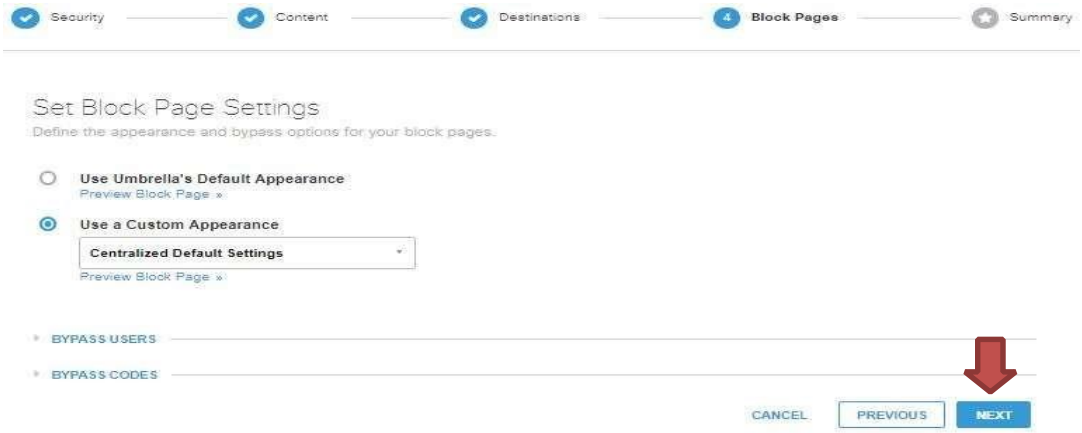
8. On the **Applications Page** choose to use the **Default Settings** or if you have created a custom Applications Settings for this specific policy select it from the drop down list and click **Next**
   a The Applications Settings can be created or edited from this page but changes made here will also be made to **every policy** that uses the **Application Settings component** that has been chosen here.


Security
Content
3
Applications
4
Destinations
+2
2 More
Control Applications
Select applications or application categories you'd like to block or allow for the users in your organization
Application Settings
Default Settings
Default Settings
CREATE NEW SETTING
Search for an application
Ad Publishing
Anonymizer
Block
Application Development and Testing
Business Intelligence
CRM
Cloud Storage
Collaboration
CANCEL
PREVIOUS
NEXT

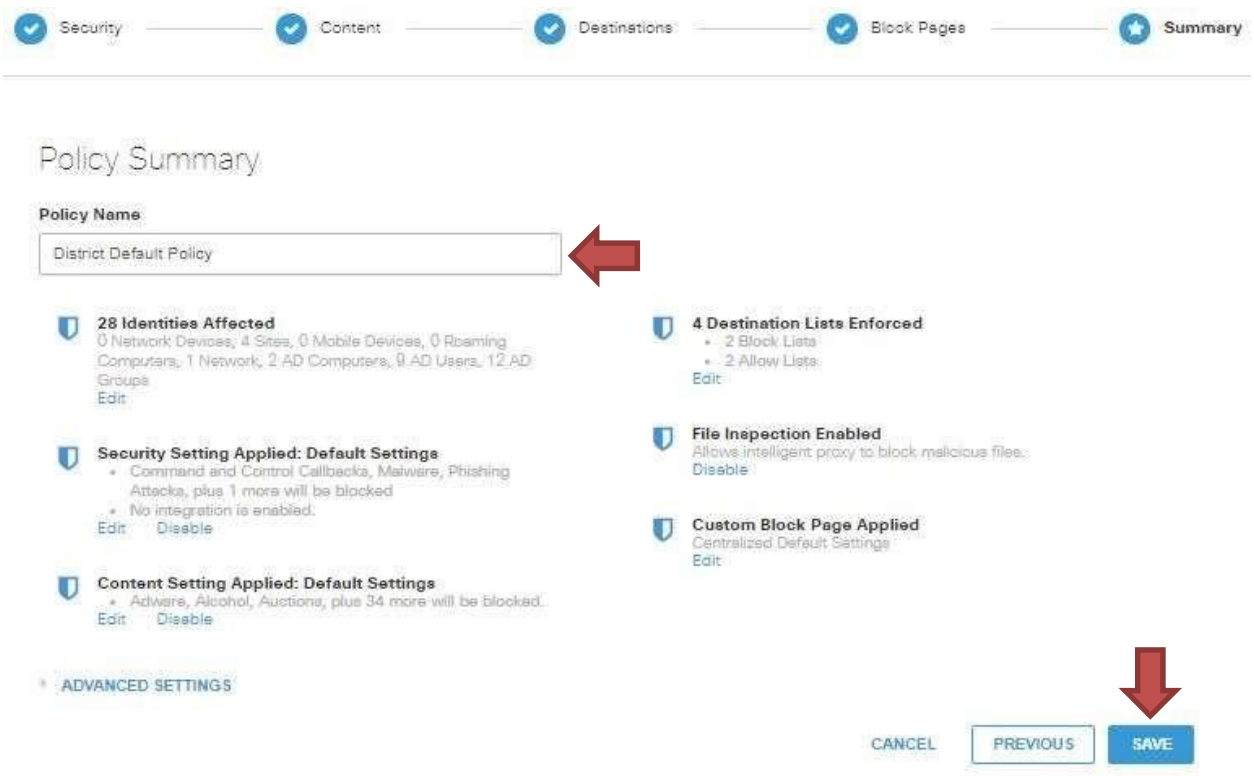
9. On the **Destinations Page, y**our **Global Block** and **Global Allow** Destination Lists will already be populated here. Put a checkmark in the box next to your Default Allow and Default Block list on the left hand side. You will see them populate in the area on the right hand side along with the Global Allow and Global Block lists.
    a. Your Global Destination Lists will be in every policy and cannot be removed so be careful with your Destination Lists.
9. Click **Next**



10. Choose weather you want to use the Umbrella Default Appearance or Custom Appearance then click **Next**.



11. Name your policy **District Default Policy** and verify that all of your settings are correct. Once you are done, click **Save.**



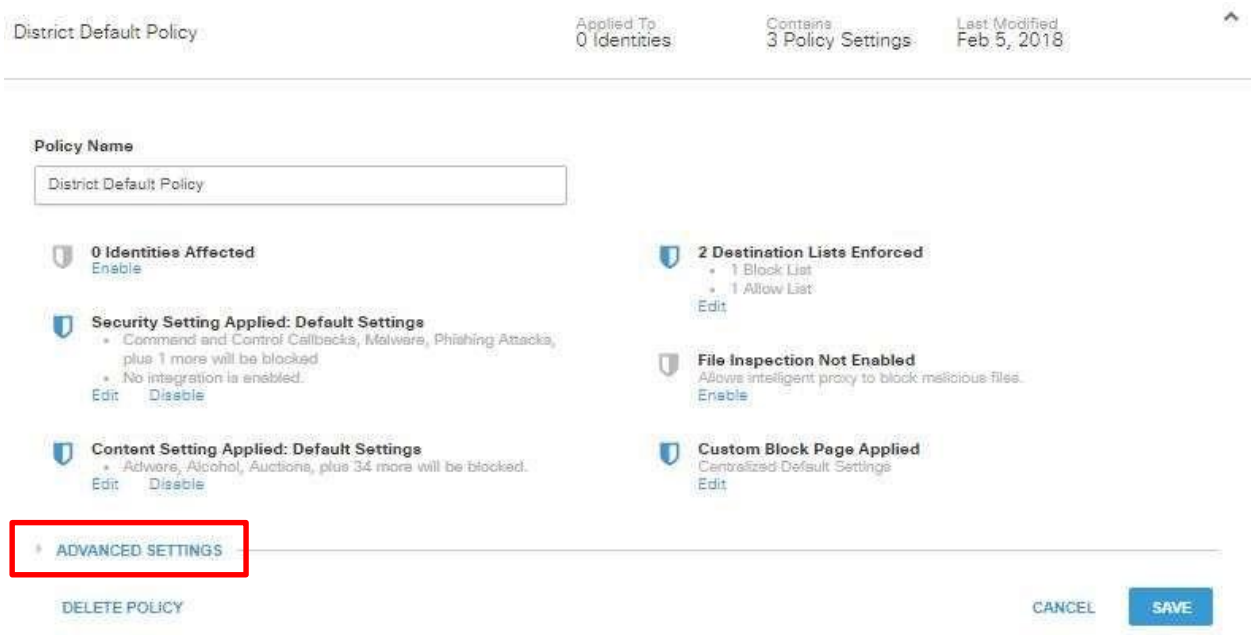
The policy that was just created will be the Default Policy for the District. If a user does not authenticate against Active Directory, that user will be filtered according to this policy. That is why it is recommended to make this policy so strict and also why every Identity is selected at the beginning of creating this policy.

Follow these steps again to create a Student, Faculty, and Administration policy but do **NOT** select every Identity. Instead navigate into **AD Groups** and search for the corresponding **Active Directory Group**. You will need to create new individual components for each new policy.

OpenDNS Policies are a top down process. This means that when a user tries to authenticate to a policy, it will start at the top of the list and work its way down. That is why your most **LEAST** restrictive policies, **I.E. IT or Administration**, should be at the **top** and your **MOST** restrictive policies, **I.E. Students and the District Default Policy,** should be at the **bottom**.

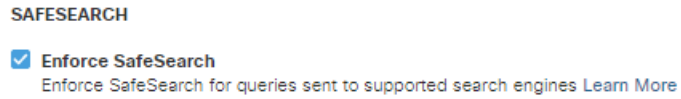
Policy Advanced Settings

After the policy has been created, clicking on the policy again will display page that is very similar to the summary page seen during the last step of the policy creation. The policy can be edited here as required. At the bottom is a drop down called **Advanced Settings**.



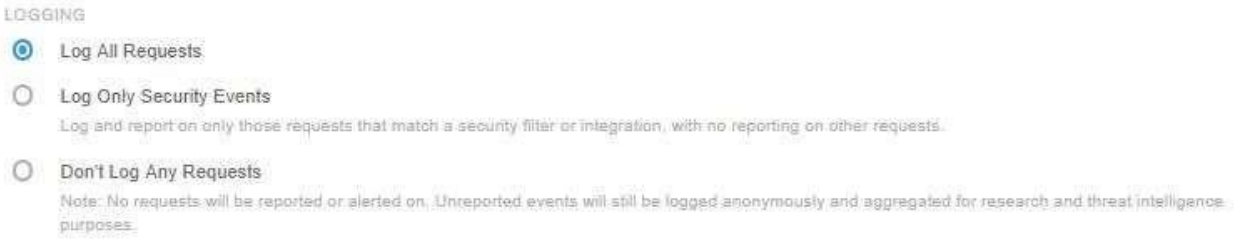
Clicking the **Advanced Settings** drop down will display a few advanced features.

1. The first option is to Enforce SafeSearch. SafeSearch is an automated filter of pornography and other offensive content that's built into search engines. If anyone enters an inappropriate or suggestive phrase, no results will be returned that could be considered unsafe or problematic. This method of enforcing SafeSearch is supported for Google, YouTube, and Bing.



2. The second option listed is **Allow-Only Mode.** This option disables any block settings in the policy because it will block every single web connection by default. With this option enabled, users who authenticate to this policy will **ONLY** be able to access the websites that are listed in the **Allow Destination Lists**. This is useful for students who have broken the rules to many times. An Active
Directory group can be created called No Internet. A Policy would then be created using only that AD Group as an identity. This policy will then be moved to the very top of the list. If a student needs internet access for specific sites for class work but are no longer allowed to access anything else, then they can be moved to the No Internet Group in Active Directory which will cause them to authenticate to this policy and only be allowed access to the websites listed in the Allow Destination Lists.

3. The final option is **Logging.** This is set to **Log All Requests** by default and should remain that way on every policy. Without this option enabled, Activity Search will no display any results resulting in no longer having the ability to pull reports.



Deploying Umbrella Certificate

Advanced Umbrella features, such as IP Layer Enforcement and the ability to block your own custom URLs require that the Cisco Root CA be installed locally.

In addition, by installing the certificate, you avoid a common problem with block pages that your users may encounter. When HTTPS enabled domains are blocked by your policy, Cisco Umbrella presents a block page to you which is also served over HTTPS. This block page is encrypted with a certificate signed by the Cisco Root CA. In order to avoid certificate errors when accessing the block page, you must install the Cisco Root CA in your browser, or if you have a network of computers, in your users' browsers.

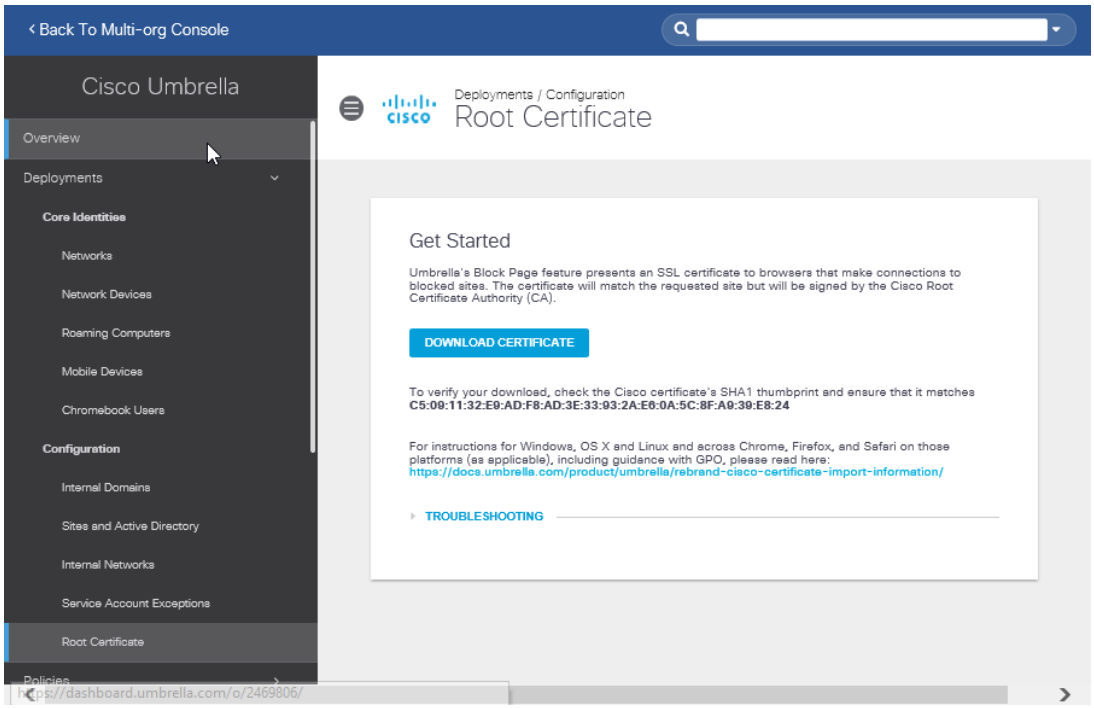
Why Deploy Certificate?

Umbrella's Block Page and Block Page Bypass feature present an SSL certificate to browsers that make connections to HTTPS sites. The certificate will match the requested site but will be signed by the Cisco Root Certificate Authority (CA). If the Cisco Root CA is not trusted by your browser, an error may be displayed. Typical errors include "The security certificate presented by this website was not issued by a trusted certificate authority" (Internet Explorer), "The site's security certificate is not trusted!" (Google Chrome) or "This Connection is Untrusted" (Mozilla Firefox). Although the error is expected, the messages displayed can be confusing and annoying and you may wish to stop them from appearing.

To avoid these errors entirely, install the Cisco Root CA in your browser, or the browsers of your users (if you're a network admin). This can be done on a per-browser, per-machine basis for personal use or small deployments. For larger deployments, an automatic installation through Group Policy (GPO) can be done. Note that the automatic installation through GPO will only work for users with Internet Explorer, Edge, or Chrome on Windows systems. As such, if your network includes some users who use Firefox or Safari browsers, and for users on non-Windows operating systems, the manual installation procedures must be followed.

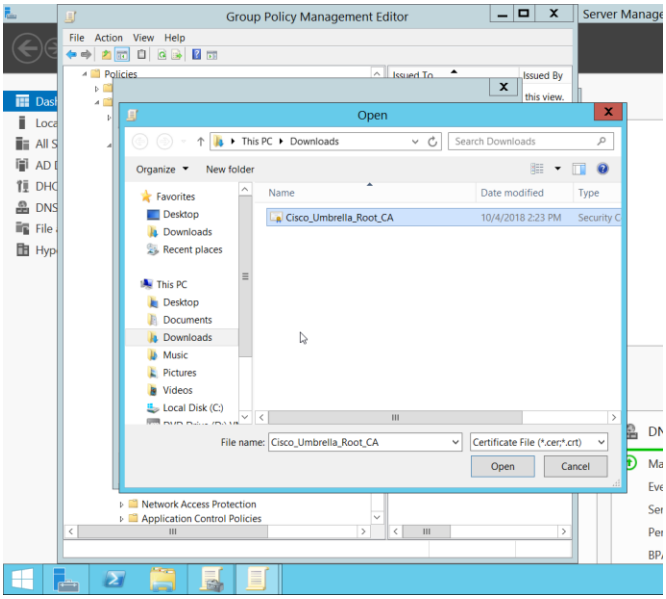
Download Certificate

In the Umbrella console under Deployment there is a link to download the root certificate which is necessary for proper processing of the Umbrella block page for destinations which are https:// encrypted sites. This certificate is also necessary for the option of decrypting DNS requests related to https encrypted sites.



This certificate can be pushed to all windows workstations with group policy, and to Chromebooks with Google admin. You can use the Apple MDM to push it to iOS devices.

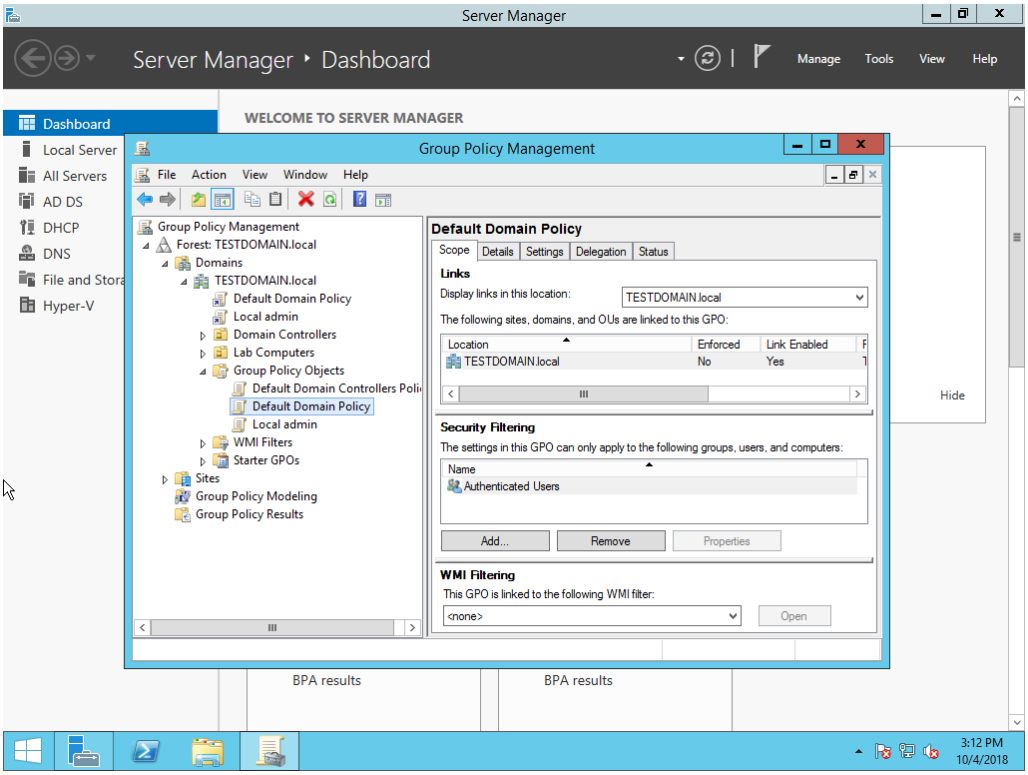
Download the certificate to a network location that is accessible to the device from which you will be implementing the distribution.



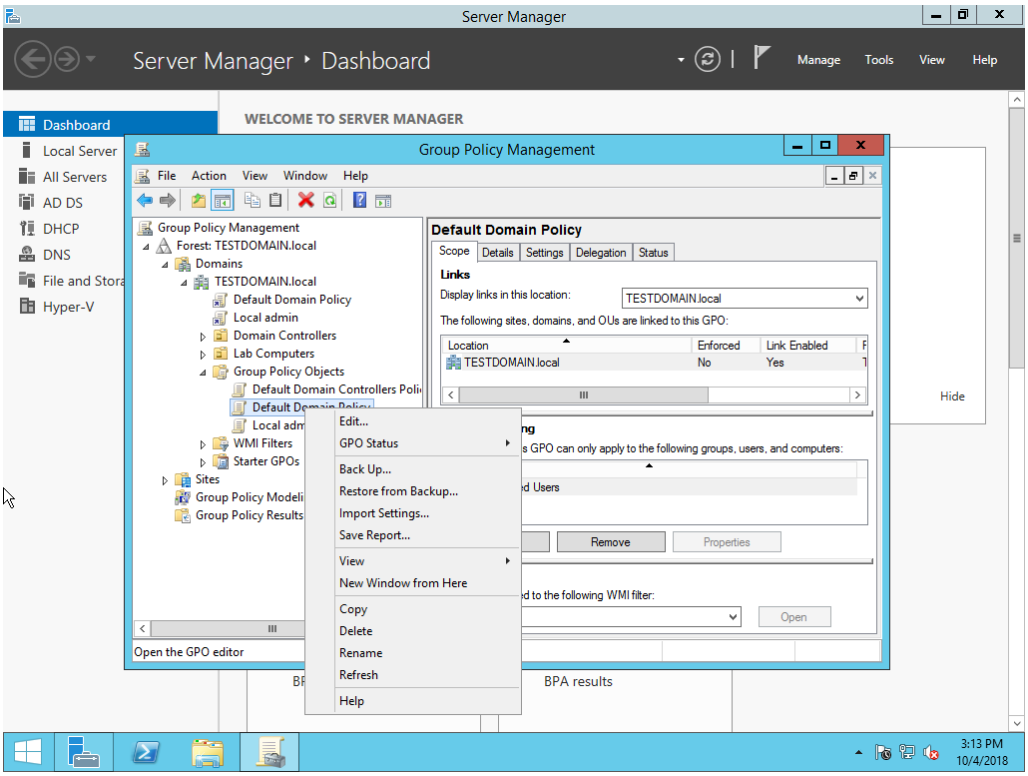
Deploy Certificate with GPO

To deploy the certificate to Windows devices using group policy, follow the instructions below:

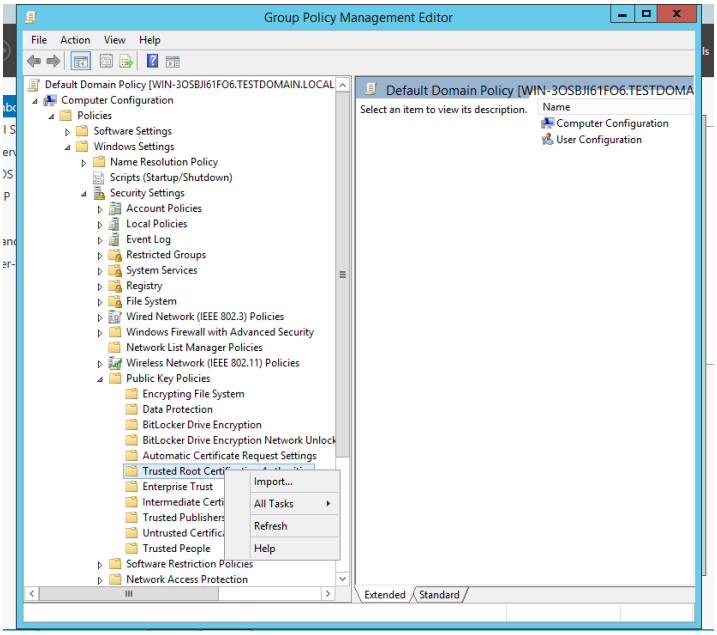
1. On a domain controller in the forest of the account partner organization, start the **Group Policy Management** snap-in.



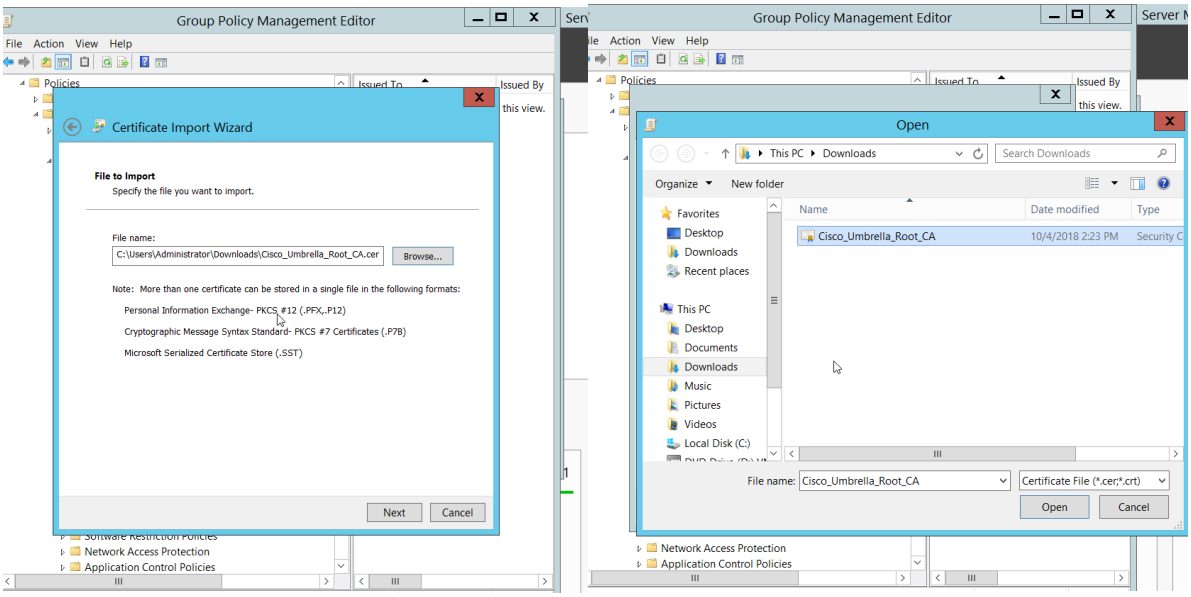
2. Find the Default Domain Polity Group Policy Object (GPO). Right-click the GPO, and then click **Edit**.



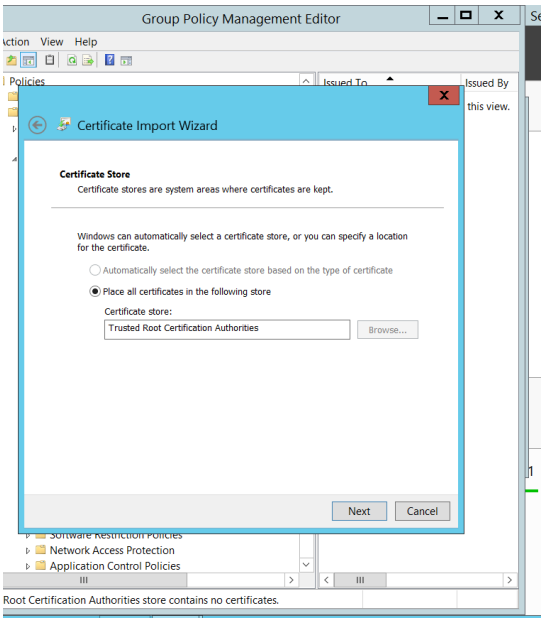
3. In the console tree, open **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies**, right-click **Trusted Root Certification Authorities**, and then click **Import**.



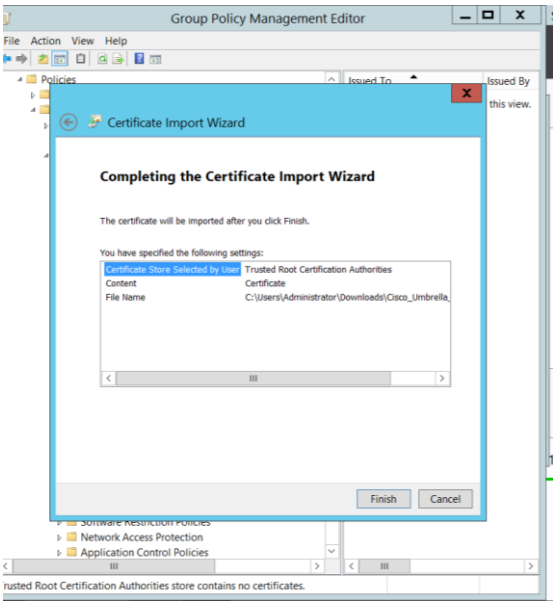
4. On the **Welcome to the Certificate Import Wizard** page, click **Next**.
5. On the **File to Import** page, type the path or browse to the appropriate certificate files and click **Next**.



6. On the **Certificate Store** page, click **Place all certificates in the following store**, and then click **Next**.



7. On the **Completing the Certificate Import Wizard** page, verify that the information you provided is accurate, and then click **Finish**.



Deploy Certificate to Chrome Devices with Google Admin

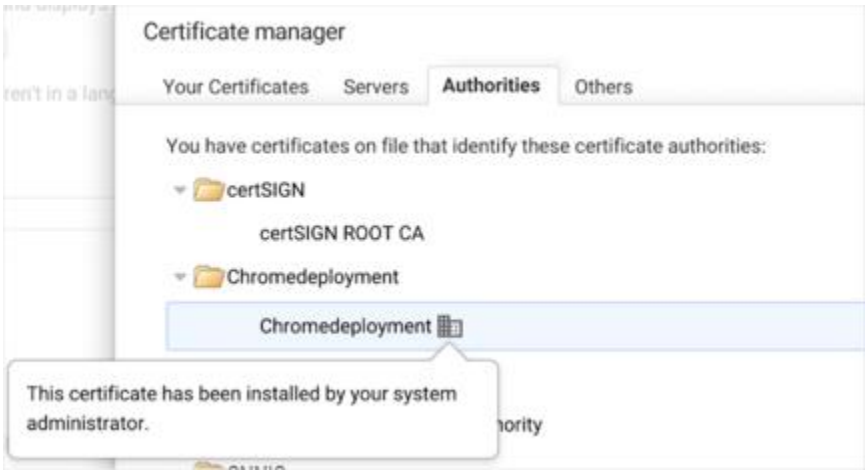
To distribute the certificate using Google Admin, do the following:

1. Sign in to the Google Admin console.
2. Click **Device management**.
3. On the left, click **Network**.
4. Click **Certificates**.
5. (Optional) On the left, choose the organizational unit where you want to add the certificate.
   Note: The top-level organization is selected by default to give all users (including those in suborganizations) access to any added certificates.
6. Click **Add Certificate**.
7. Choose the certificate file to upload and click **Open**.
   Note: DER-encoded certificates are not supported. Chrome devices only accept PEM format.
8. (Optional) If the certificate will be used as a root CA for an SSL-inspecting web filter or to allow the browser to validate the full digital certificate chain of servers, check the **Use this certificate as an HTTPS certificate authority** box.
9. Click **Save** and then **Done** to confirm.

Verify the CA on managed Chrome devices

1. Go to **chrome://settings/certificates**.
2. Click **Authorities**.
3. Scroll down to see the newly-added CAs.

CAs set up in your Admin console are highlighted as follows:



With respect to your iOS devices, contact your management provider or install each device with the certificate individually.

ByPass User

Setting up your Block Page Bypass

An important step when configuring policies is to ensure that you're giving the right information to your users if they are blocked under Security or Content categories. As the Umbrella administrator, you may wish to exempt users from being blocked during certain times and you can set up the rights to do that as well.

Some helpful terms to know:

- **Block Page—**The page that's displayed in the browser when a user of your Umbrella service tries to go to a website that's been blocked under the category defined by the policy for the Identity that user falls under.
- **Block Page Bypass**—The method by which certain users who have been given special authority can bypass a normal block page. There are two ways you can bypass a block page: having a user account (a bypass user) or having a special code (a bypass code).
- **Block Page Bypass User—**A special user account that gives the rights to certain individuals or a group of individuals to go to blocked sites while still being part of the enforcement given to the larger policy group to which they they belong.
- **Block Page Bypass Code—**A code that can be given to individuals or groups of individuals to allow them to go to some or all blocked websites until such time as the code expires.

Not all categories can be bypassed. If a user is blocked for a Security or Malware category, the site is considered malicious and should not be accessed under any circumstances. If you think a domain shouldn't be blocked, please email us at security-block@opendns.com.

If you'd like to know more about a block or have us review it in more detail, open a case by emailing umbrella-support@cisco.com with information about the domain and our support and security teams will review.

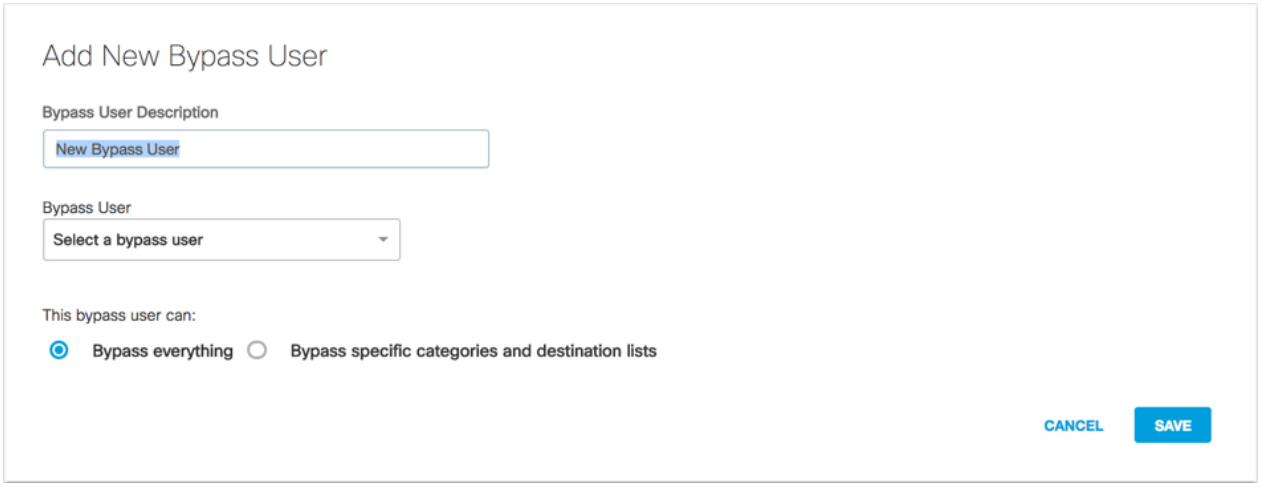
The following policy settings can be bypassed:

- Content category blocks
- Destination list blocks—these are destination lists you've created
- The phishing security block

Setting up a Block Page Bypass User

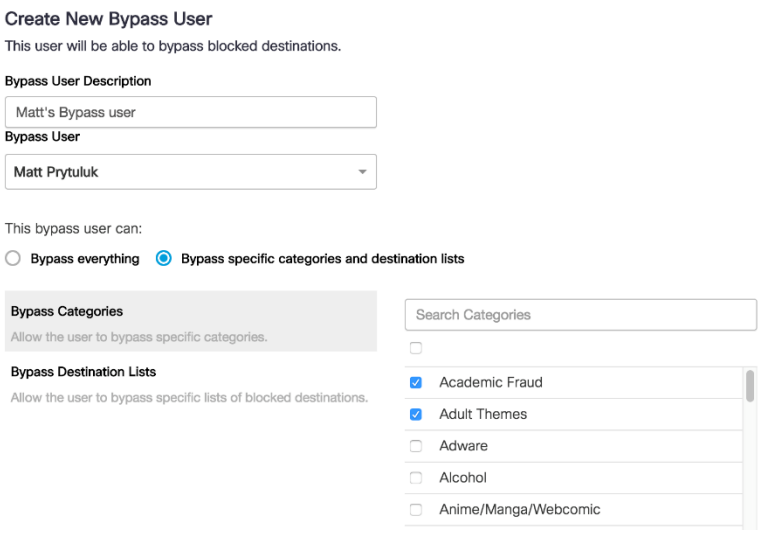
A "Block Page Bypass" user is special username and password that can be given to one or more users in order to provide them with rights to bypass pages that are typically blocked through policy settings. This user can be thought of as being a special set of rights that are given to individuals as required. The Block Page Bypass user has no ability to log into the dashboard or do any administrative functions other than bypass blocked sites.

1. Navigate to **Admin > Bypass Users**. Alternately, the block page bypass user can be created by editing the Block Page Appearance in the summary of a policy. The edit for this setting is in the lower right corner of the policy summary.



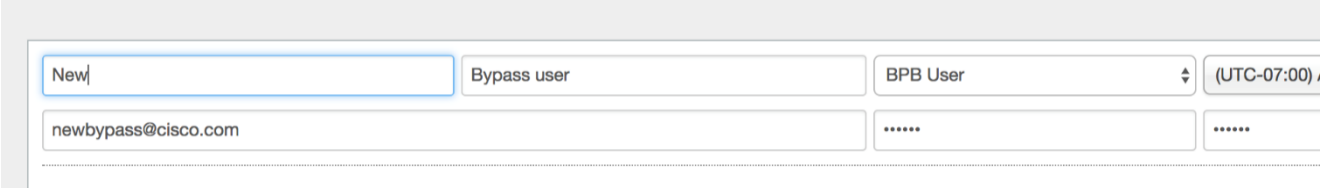
2. From the **Bypass User** drop-down list, choose a ***<user>***.
   When a block page shows up, the user then enters their credentials and bypasses it.
3. Select how the user can bypass a block page.
4. Click **Save**.

   The "Block Page Bypass" user gives the rights to certain individual people, or a group of people to go to blocked sites while still being part of the enforcement given to the larger policy group they belong to.

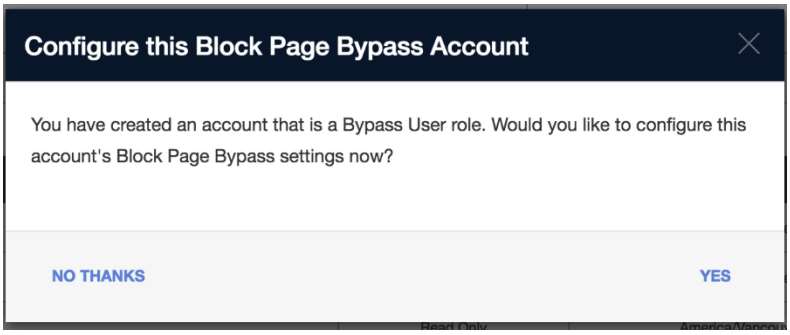


To setup a brand new bypass user, that is, an account with rights to authenticate against the block page and continue browsing, first, create the user with the Block Page Bypass role.

1. Navigate to **Admin > Accounts** and click the + (**Add)** icon.
2. Choose Block Page Bypass from the drop-down list.

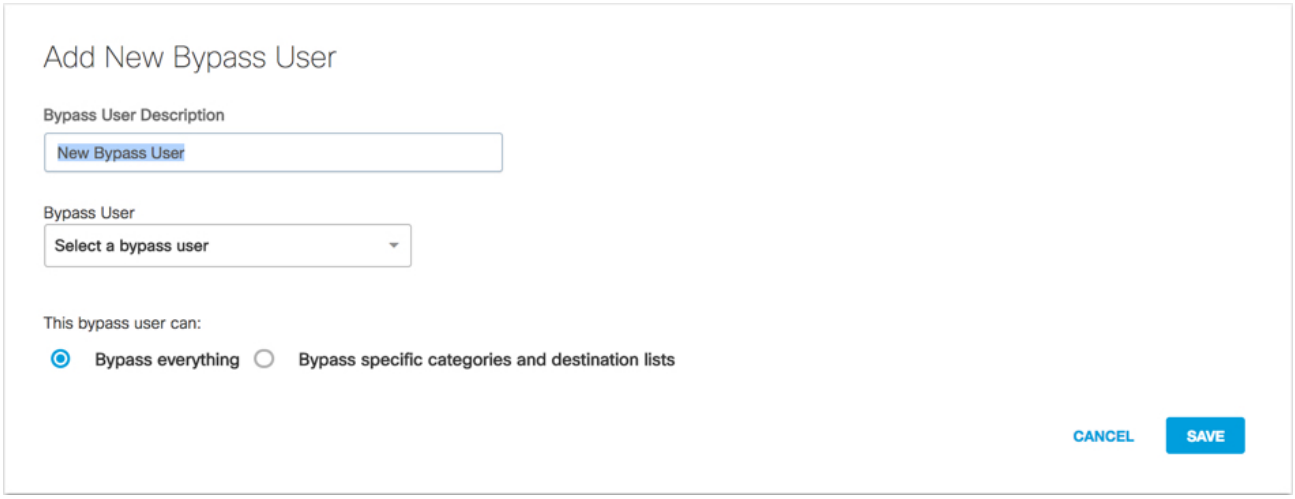


3. Click **Create** and in the pop-up modal click **Yes** to configure Block Page Bypass settings for the user. The Add New Bypass User page opens (Policies > Bypass Users).



4. If you click **No Thanks**, you can change the settings for the user you've created under **Admin > Bypass Users** or add the settings as part of the policy summary as described earlier.

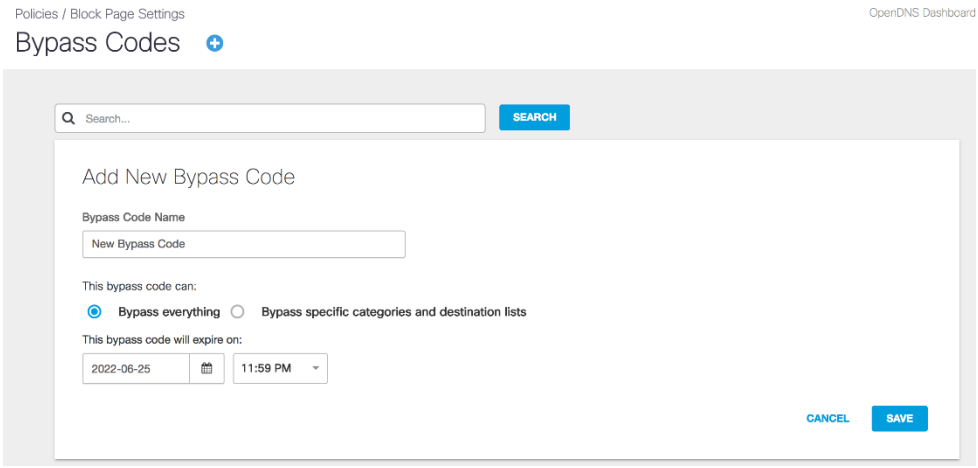
5. Add a new bypass user and click **Save**.



Creating a Block Page Bypass Code

A Block Page Bypass Code is a code that can be given to users through email, instant messenger or the phone to allow an instant bypass of a particular blocked page.

1. Navigate to **Admin > Bypass Codes** and click the + (**Add)** icon.
   You can also access this page from the Summary page of a policy. Click **Edit** for the Block page applied.

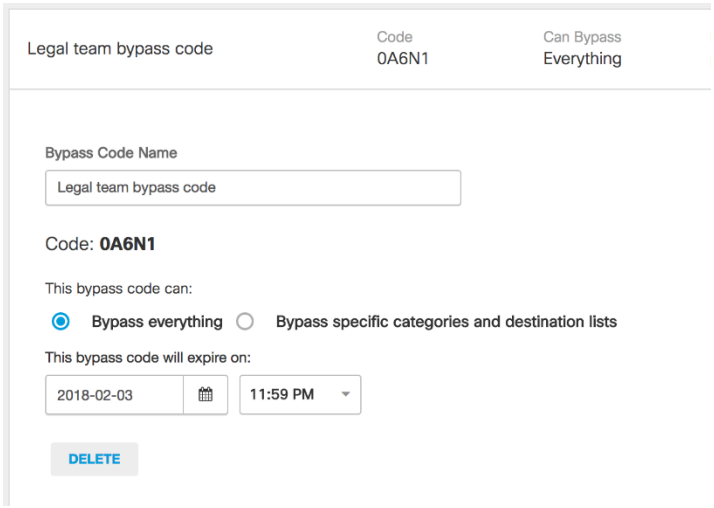


2. Set the code to either allow access to all sites or a subset of the content category or destination lists you've defined.
3. The code can be set to expire at a day in the future and at an hour of that date.
4. Click **Save**.

Removing a Bypass Code

1. Navigate to **Policies > Block Page Settings > Bypass Codes**.

2. Expand the code you want to delete and click **Delete**.



Applying Bypass Codes/Users to a policy

Before you will be able to use your new bypass user or bypass code, you must first link it to a policy!

1. Navigate to **Policies > All Policies**

2. Click on the policy you want to apply the bypass user or code to.

3. Click Edit under the Block Page that is Applied.

4. Expand either Bypass Code or Bypass User and select the user or code you want to apply.

5. Click Set & Return, then SAVE!

Interacting with a Block Page As a User

As an administrator, you can preview the block page; however, not all elements of the page will be accurately reflected in Preview Mode. This is a problem that's being worked on and will change in the future.

As a standard (non-bypass) user, if you were to go to a website blocked under your Umbrella policy, you would see a standard block page like this. This example has a custom block page message that includes a link to an acceptable use policy from this organization, as well as a custom logo for this organization.

Note:

Keep in mind that the block page bypass will not work with domains blocked due to malicious activity (such as malware or phishing). You can only access the bypass block page if the domain was blocked due to content category settings or domain block lists. The "Admin" link will not appear if the domain was blocked as malicious activity.

At the bottom of the block page, there are two hyperlinks that may appear:

- **Contact your network administrator**—Allows a user to email the administrator if the user thinks the block is in error.
- **Administrative Bypass**—This allows a user with a bypass user or a code to access the part of the page that asks for that information. Below is the same block page for a policy that has both a user and a code configured for it.

After clicking on the Administrative Bypass link you will be able to authenticate with either your Bypass User or Bypass Code

After you enter your email/password or bypass code and click bypass you will see the following box

You can now click on Continue browsing at <URL> and continue to the site. A popup box will come up and needs to stay open until you are finished with the bypass. When finished click Log Out to end your bypass session.

Cisco Security for Chromebook Migration

Reference: https://support.umbrella.com/hc/en-us/articles/13818088861588-Updated-Prepare-for-Upcoming-Changes-Umbrella-Chromebook-Client-and-SWG-Umbrella-Chromebook-Client

NOTE: The old Umbrella Chromebook Client will still be supported until June 2025. Make sure you are fully migrated over to the new Cisco Security for Chromebook App before June 2025.

NOTE: Once migrated to the new app you will no longer be able to view the internal IP address of Chromebooks in Activity Reports.

Prerequisites:

To enable DoH and SWG protection on Cisco Secure Chromebook client, the following prerequisites must be met:

- You must have Umbrella login credentials.
- You must have a Google Workspace admin account to push Cisco Security for Chromebook client to all the Chromebook devices.
- We recommend that you synchronize Google Workspace identities with Umbrella to apply the Google Workspace user and organizational unit-based policies. For information about integrating the Google Workspace identities, see Integrate Google Workspace Identities.
- Chrome OS 110 or later is required to enable DoH-based DNS layer protection on Chromebooks.
- Chromebooks must *not* be in Kiosk mode.
- For DNS layer protection, ports 53 UDP and 443 TCP must be allowed. For SWG layer protection, port 8888 (TCP) must be accessible to 146.112.0.0/16 and 155.190.0.0/16.
- You must have access to https://registration.polaris.qq.opendns.com, https://sync.hydra.opendns.com, and https://doh.umbrella.com.
- Chromebooks must be connected and logged in.
- Install Cisco Umbrella root certificate on your Chromebooks to avoid certificate errors when accessing an Umbrella block page. For more information on this installation, see Install the Cisco Umbrella Root Certificate.
  For more information about how to push the Umbrella root certificate from the Google admin console to all your Chromebook devices, see Set up TLS (or SSL) inspection on Chrome devices.
- In the Google Workspace Admin console, you must disallow the incognito window. From the Incognito mode menu, choose **Disallow incognito** mode. For more information, see Incognito Mode in Chrome Enterprise and Education Help.
  For SWG, you can optionally configure the DNS servers on your network to forward DNS traffic to

Cisco Umbrella. This configuration provides the most accurate selection of SWG Data Center locations. For more information, see Point your DNS to Cisco Umbrella.

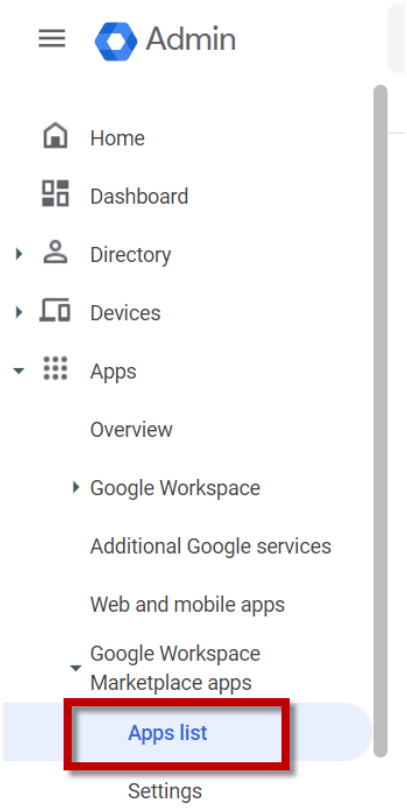
- Third-party web filtering or web proxy solutions may interfere with the SWG proxy setup of Umbrella Chromebook client. We recommend that you remove these solutions before deploying Cisco Security for Chromebook client.
- The following devices and operating systems are not supported:
    - Chrome browser on OS X, Windows, and Linux.
    - Devices running variations or third-party distributions of ChromeOS, such as Neverware CloudReady.
- Network requirements

Protection	Port and Protocol	Source / Destination	Notes
DNS and SWG Layer	53 (UDP)	-	Configured DNS resolvers should be reachable.
DNS and SWG Layer	443 (TCP)	Registration. polaris.qq.opendns.com	HTTPS. Used for registration of client.
DNS and SWG Layer	443 (TCP)	sync.hydra.opendns.com	HTTPS. Used to synchronize device details and to fetch configuration.
DNS and SWG Layer	443 (TCP)	doh.umbrella.com	HTTPS. Used to resolve DNS requests.

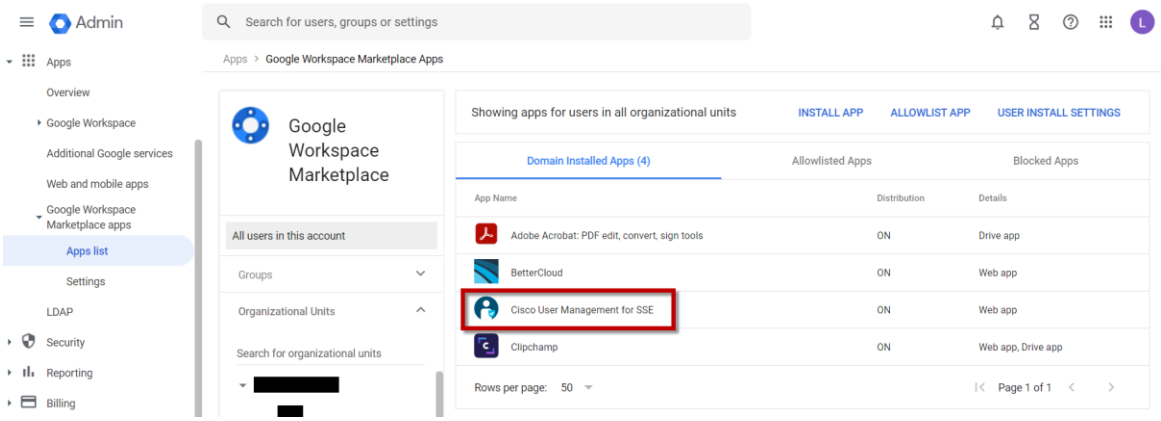
Cisco User Management for SSE Setup (Google Workspace Integration)

1. Log into your Gsuite Admin Console at https://admin.google.com

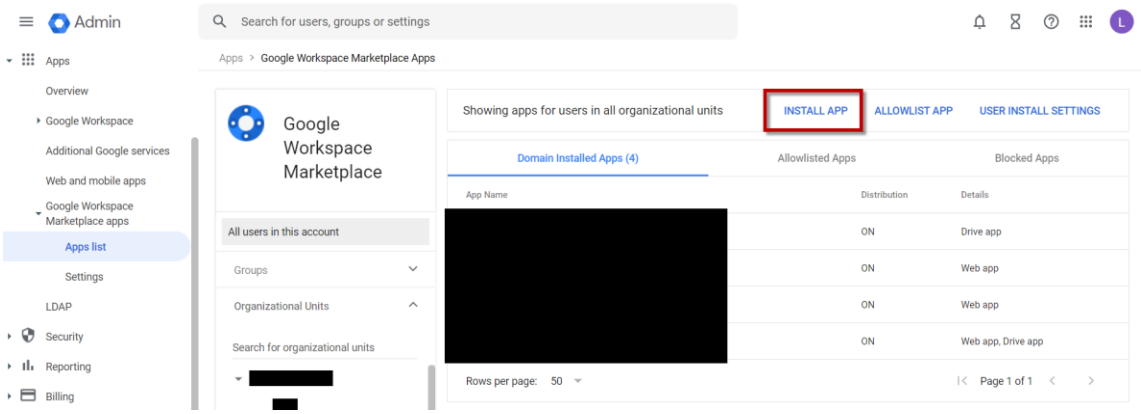
2. Navigate to Apps/Google Workspace Marketplace apps/Apps list.



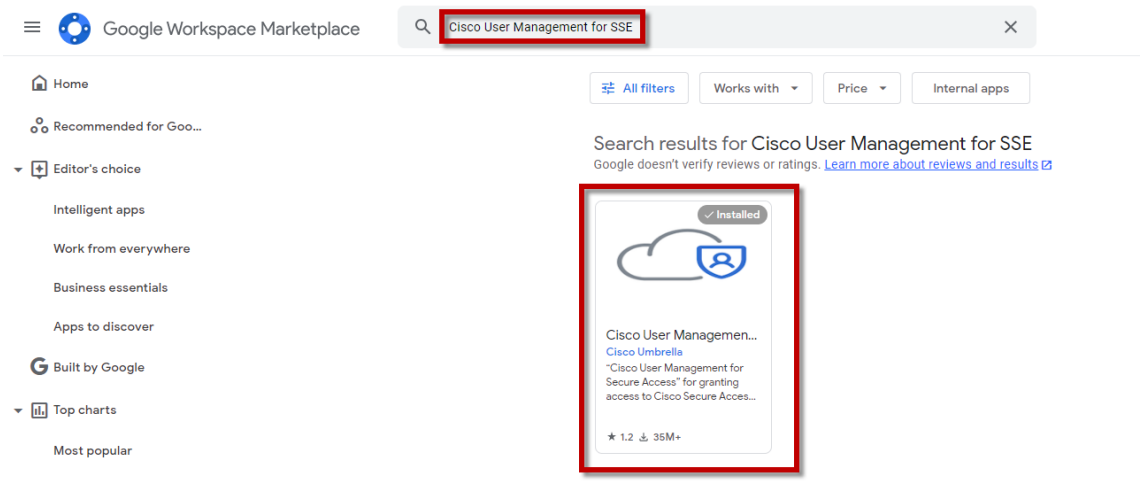
3. Search for "Cisco User Management for SSE" in your Domain Installed Apps.
   If not already installed then proceed to step 4.
   If already installed then proceed to step 7.



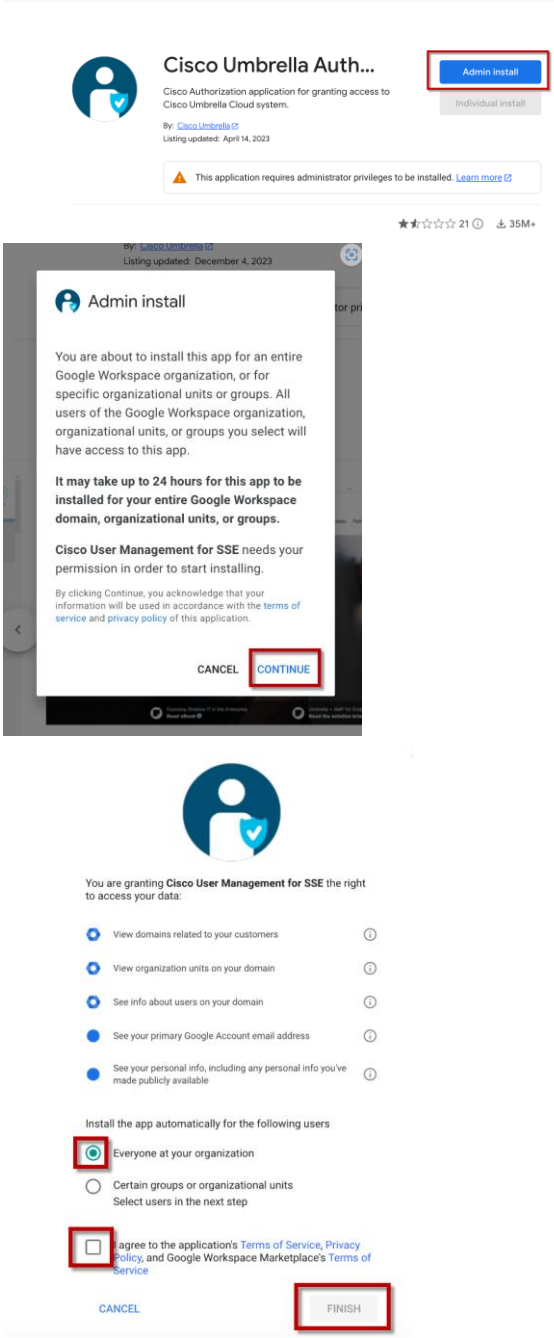
4. Click on "INSTALL APP."



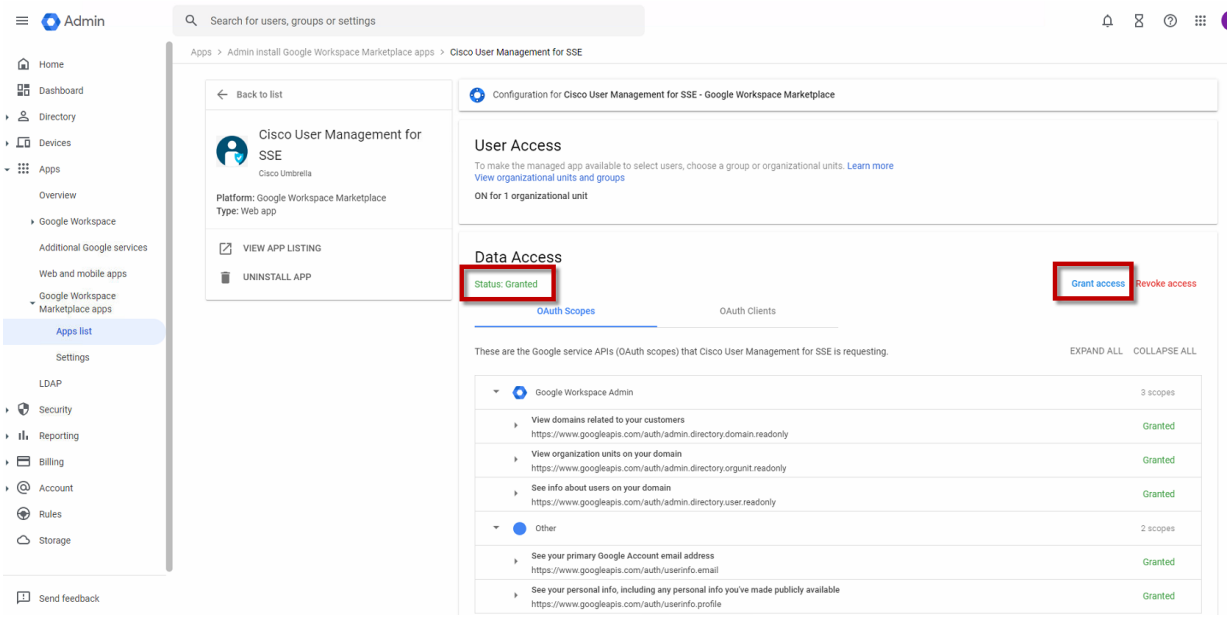
5. In the search bar search for “Cisco User Management for SSE” and click on the App.



6. Click Admin Install, then CONTINUE, then check “I agree…” and finally FINISH.

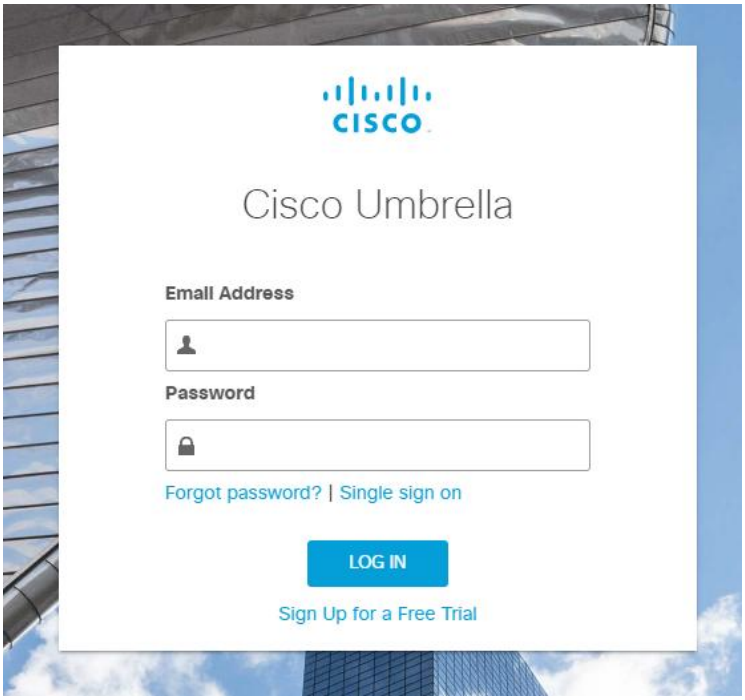


7. Once installed you should see the following screen with Status: Granted in green. If you do not then click on “Grant access” to finish the setup. Then proceed to the Umbrella Setup section of this guide.

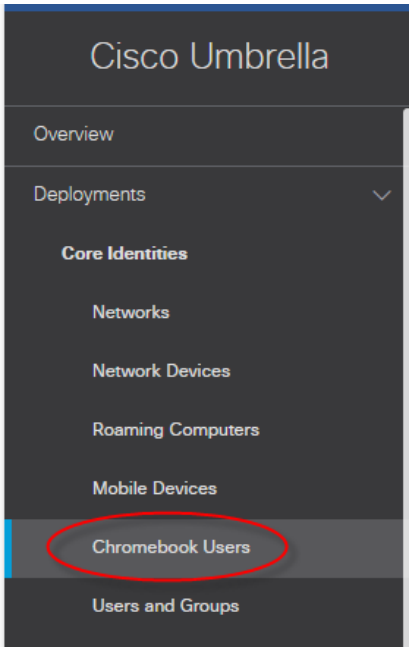


Umbrella Setup

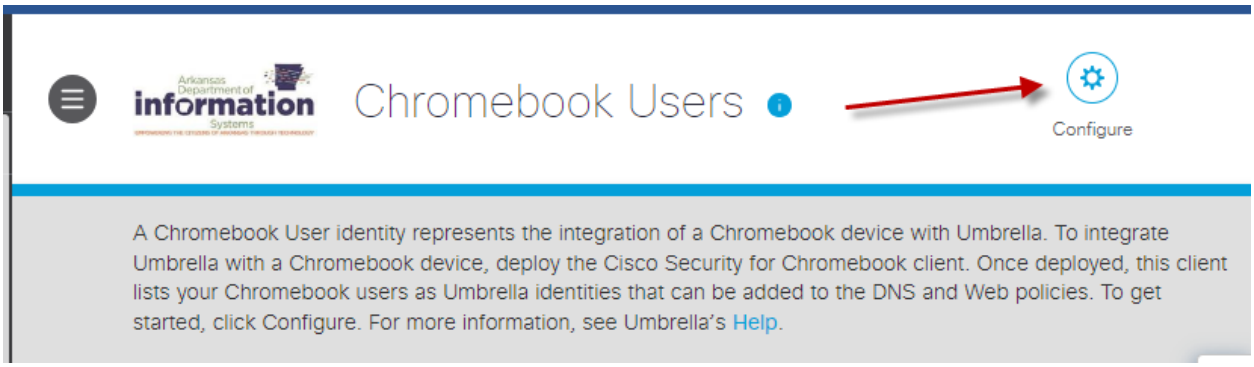
1. Login to the Umbrella Dashboard at https://login.umbrella.com/



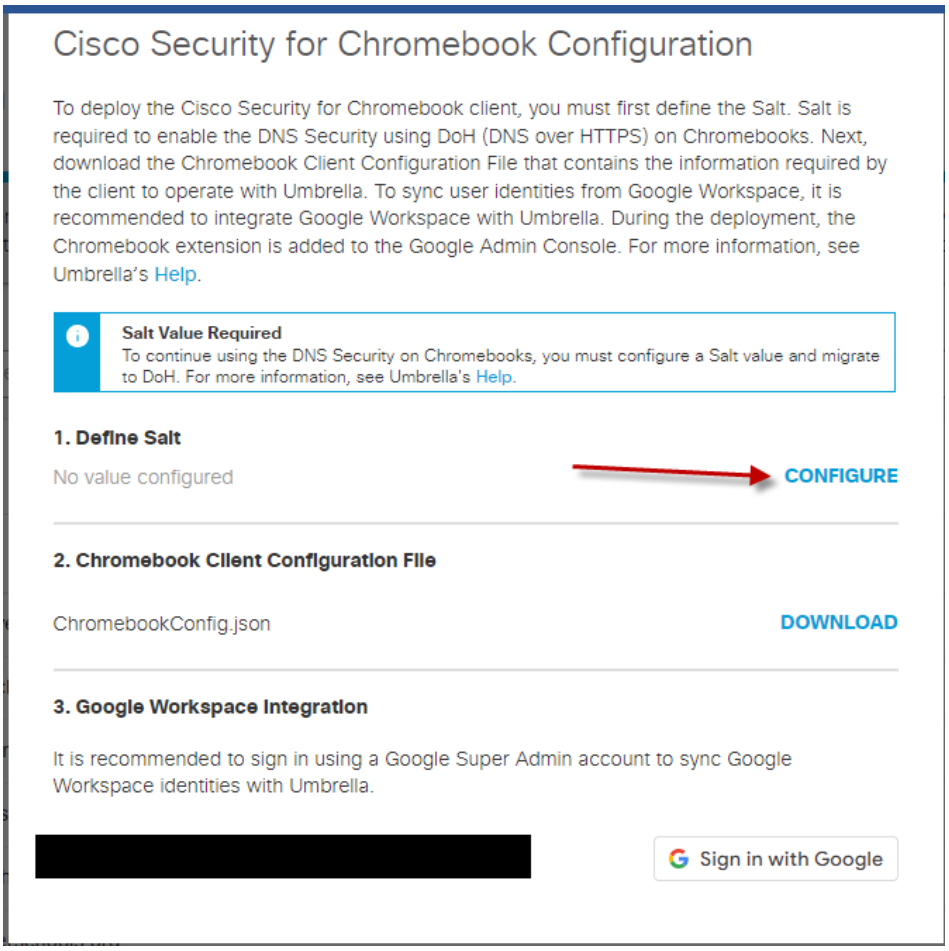
2. Navigate to Deployments/Core Identities/Chromebook Users



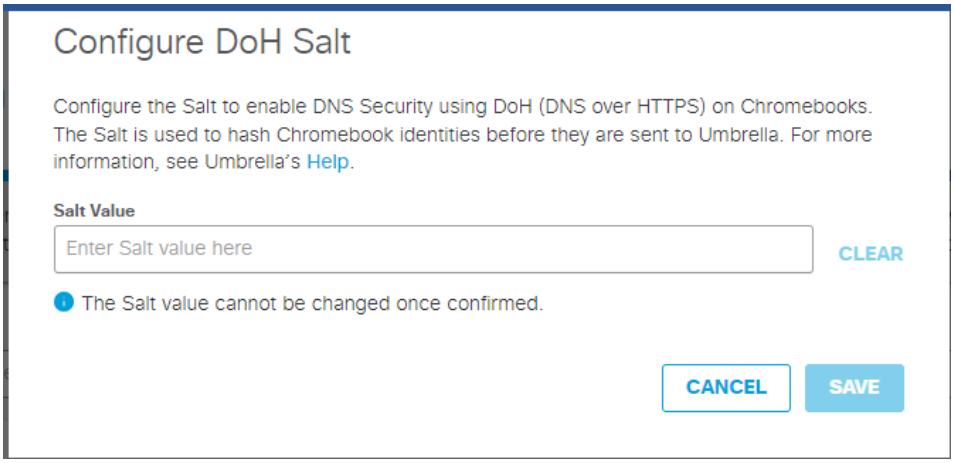
3. Click configure in the top right corner of the webpage.



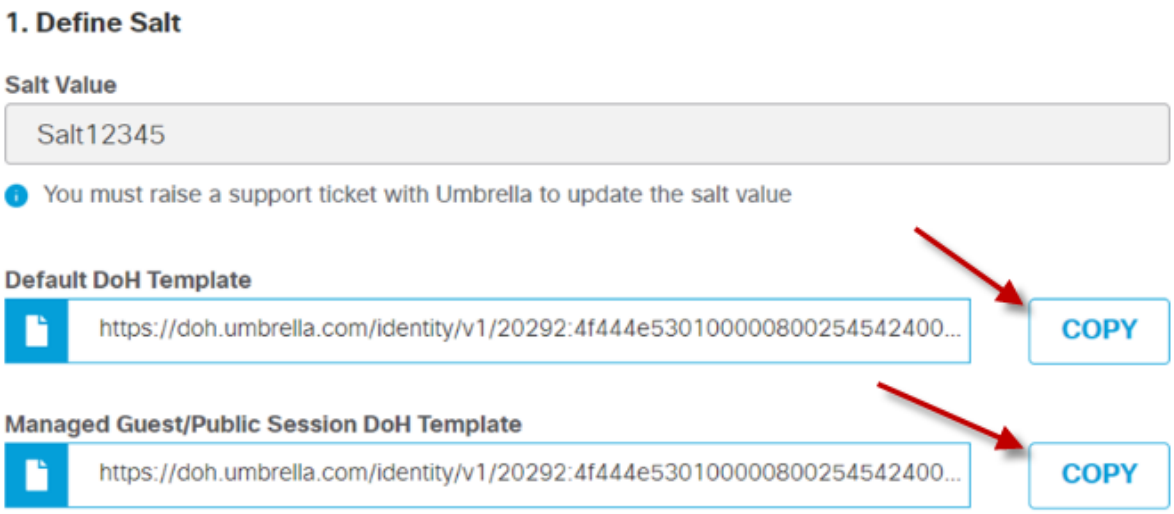
4. Define a salt value by clicking "Configure" on the right side. NOTE: Once the value is set it cannot be changed!!!



5. Enter a value for the Salt then click “save.”
   The Salt value must be between 8 and 32 characters and can contain letters and numbers but NO special characters.

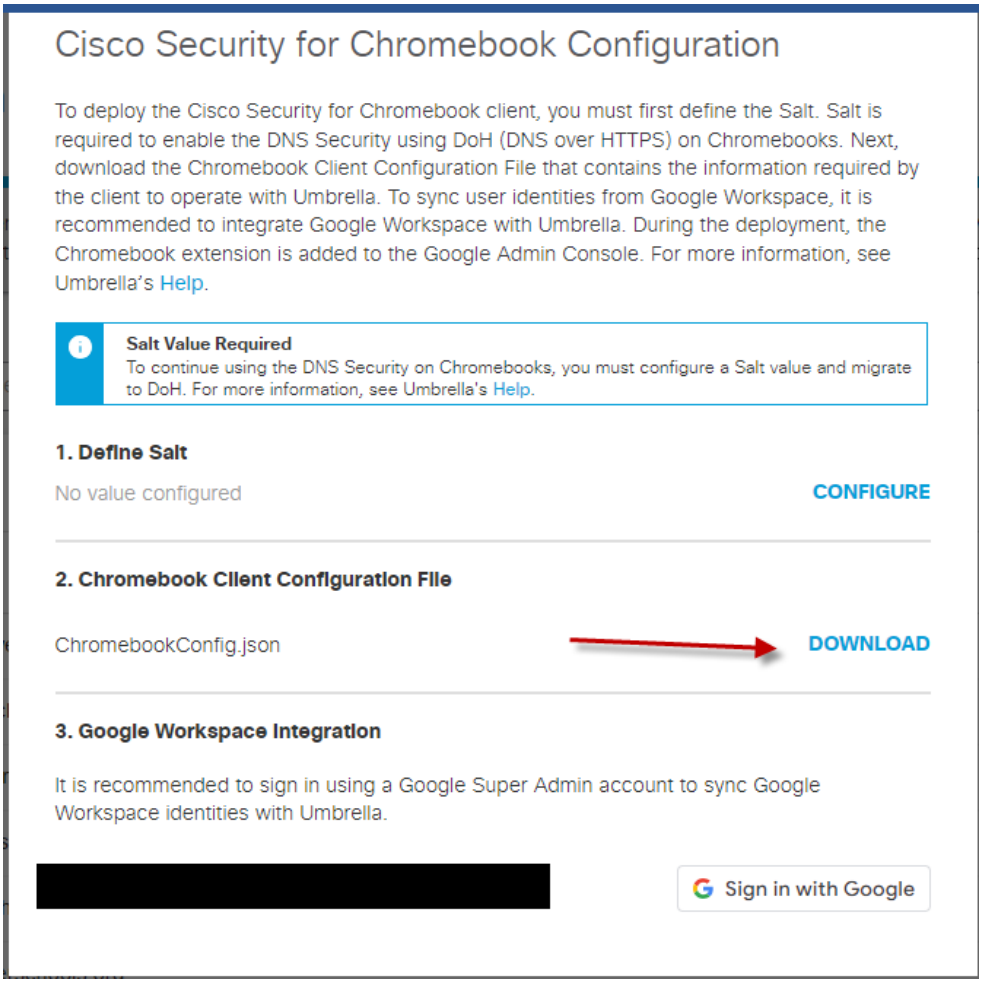


6. Once the Salt is configured there will be two Template URLs created, copy these to a text file and make sure to notate which one is the Default DOH Template and which one is the Managed Guest/Public Session DoH Template. You will use the Default DoH Template later for your managed Chromebooks. The Managed Guest/Public Session DoH Template is only used for Managed Guest sessions.

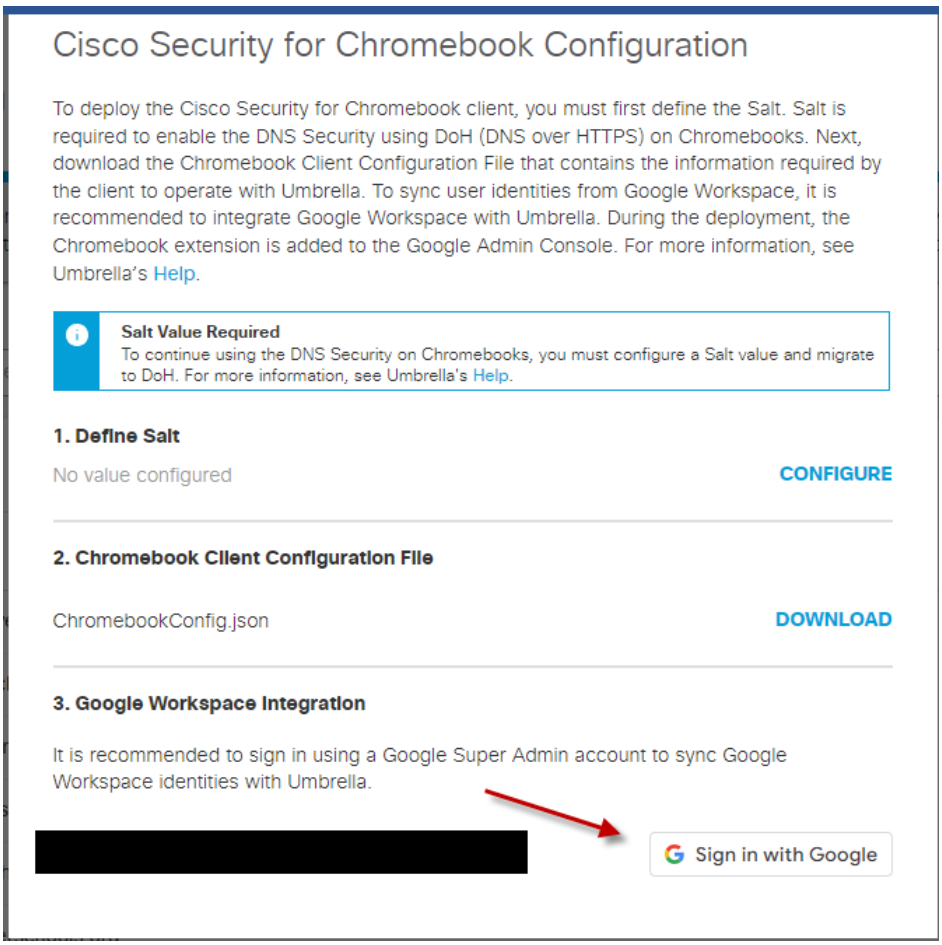



```
Default
https://doh.umbrella.com/identity/v1/20292:4f444e5301.....................................


Managed Guest
https://doh.umbrella.com/identity/v1/20292:4f444e53010000080.....................................
```

7. Download the Chromebook Client Configuration File and note the location you downloaded it to. This Json file will be used later when installing the new Cisco Security for Chromebook app. If you lose the file or need to redownload it, you can always return to this webpage later.

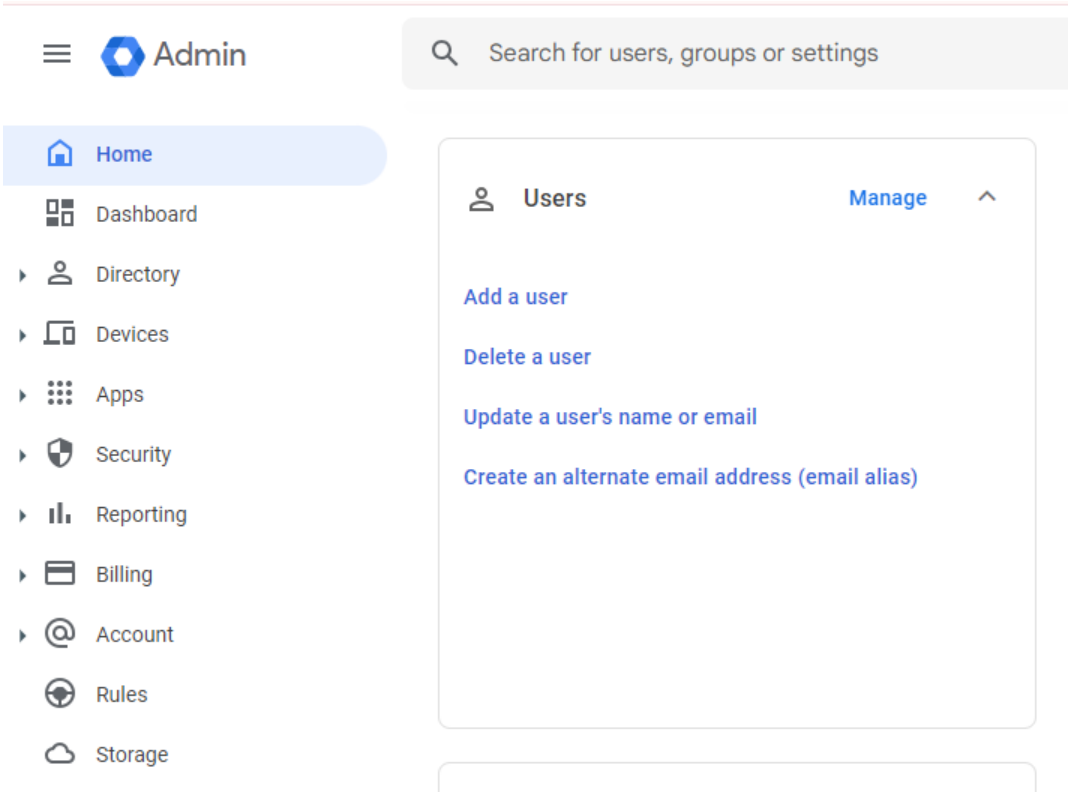


8. For Google Workspace Integration click “Sign in with Google” and sign in using a Gsuite Super Admin account tied to your domain. Once completed you should see your Super Admin email address listed.

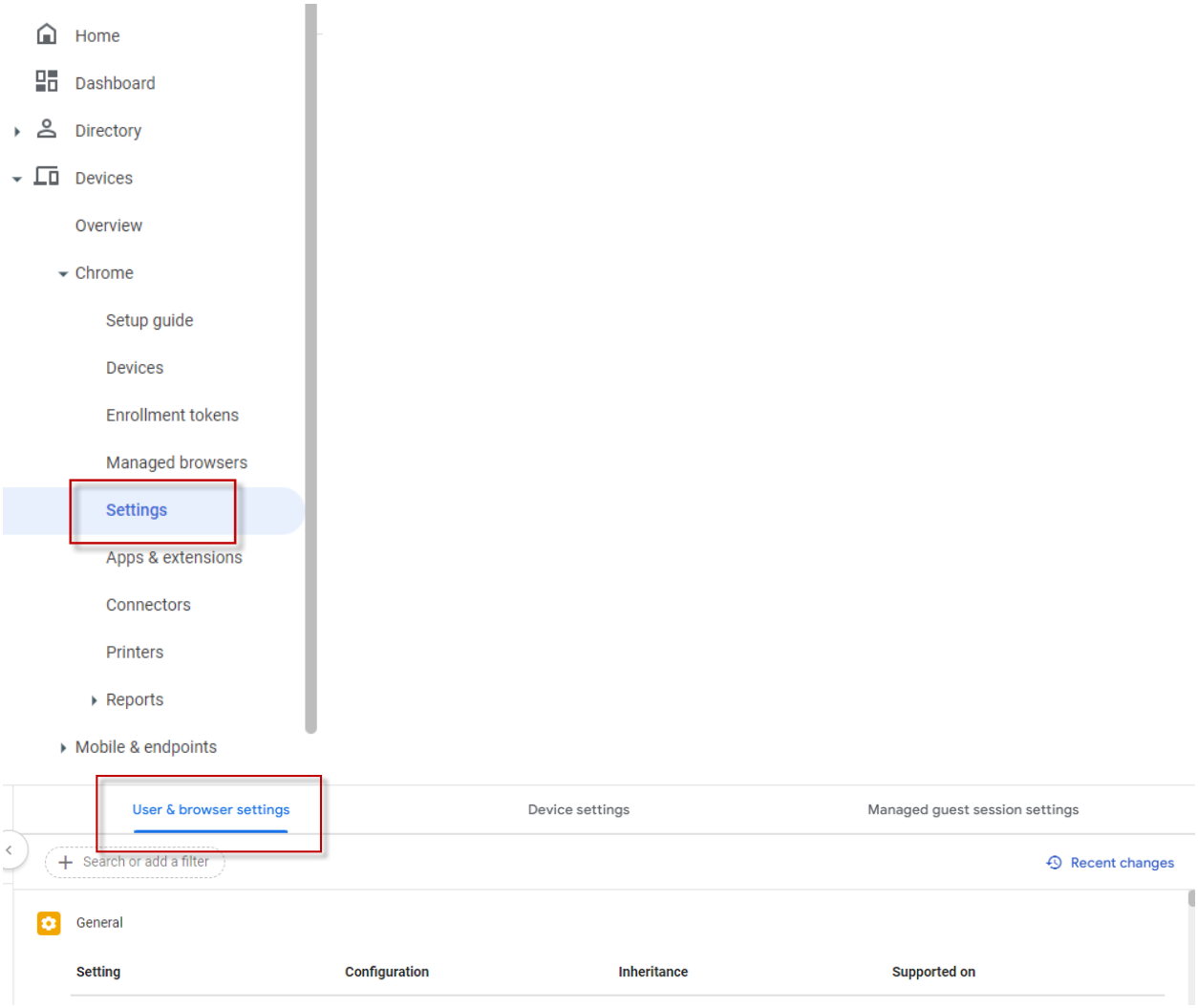


Google Setup

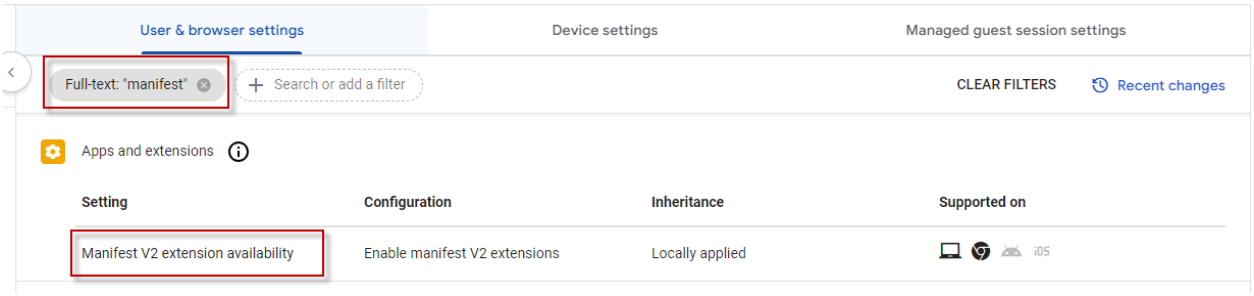
9. For the next step you will log into your Gsuite Admin Console at https://admin.google.com

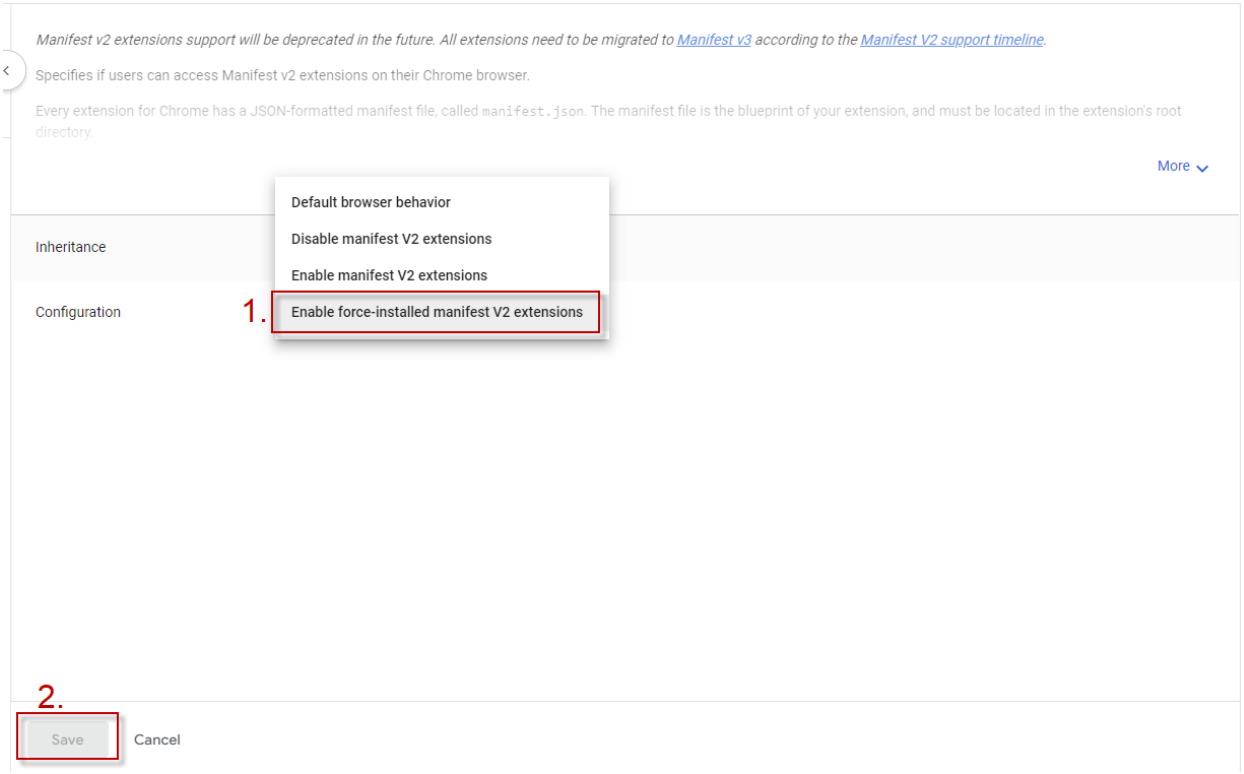


10. Navigate to Devices/Chrome/Settings/User & browser settings and select the OU you will be deploying the new extension to (preferably the top level of the Domain).

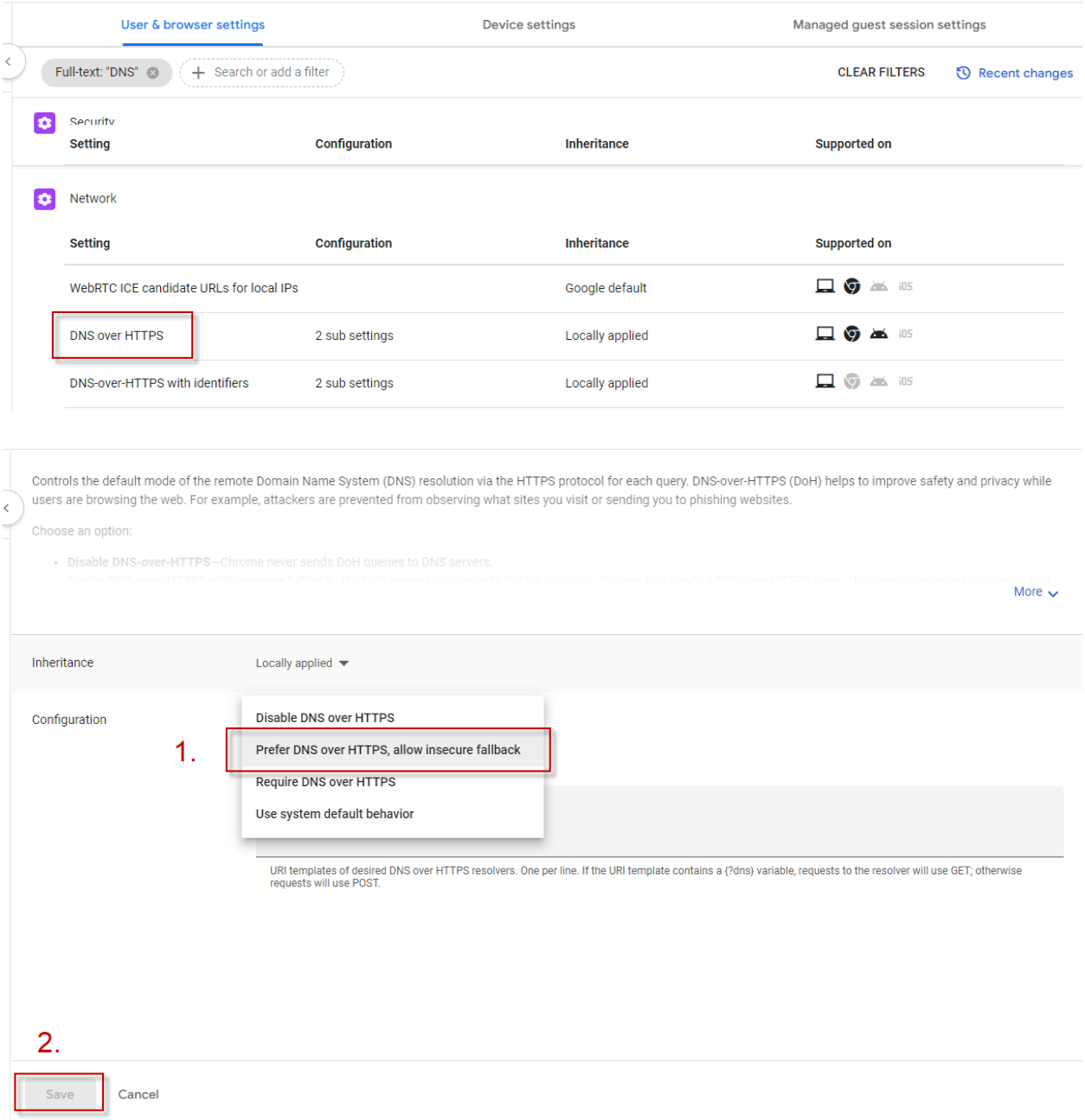


11. In the “Search or add a filter” field enter “Manifest” then click the “Manifest V2 Extension Availability” setting. Then select “Enable force-installed manifest V2 extensions” then click “Save.”

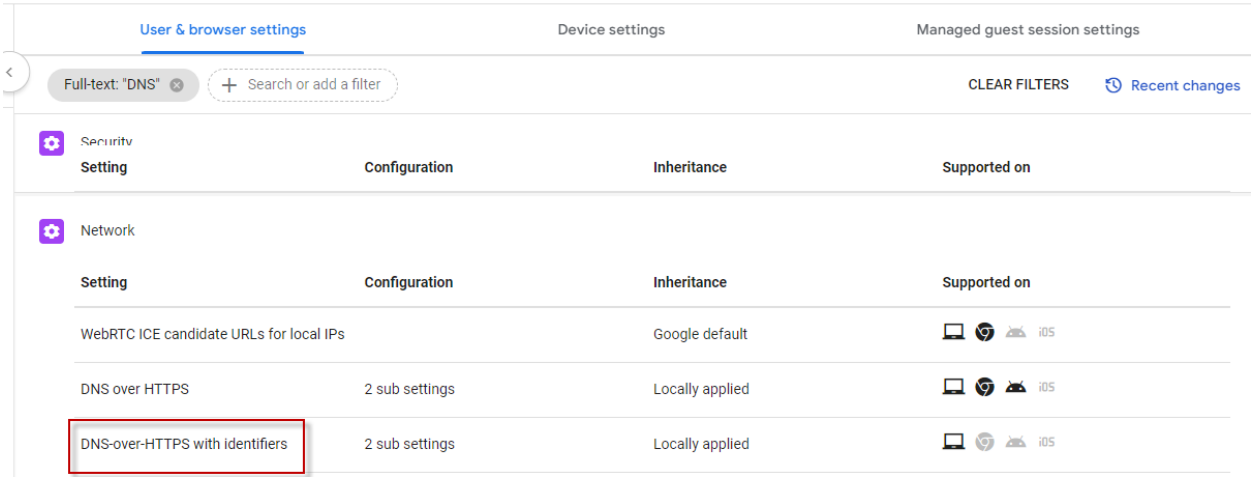


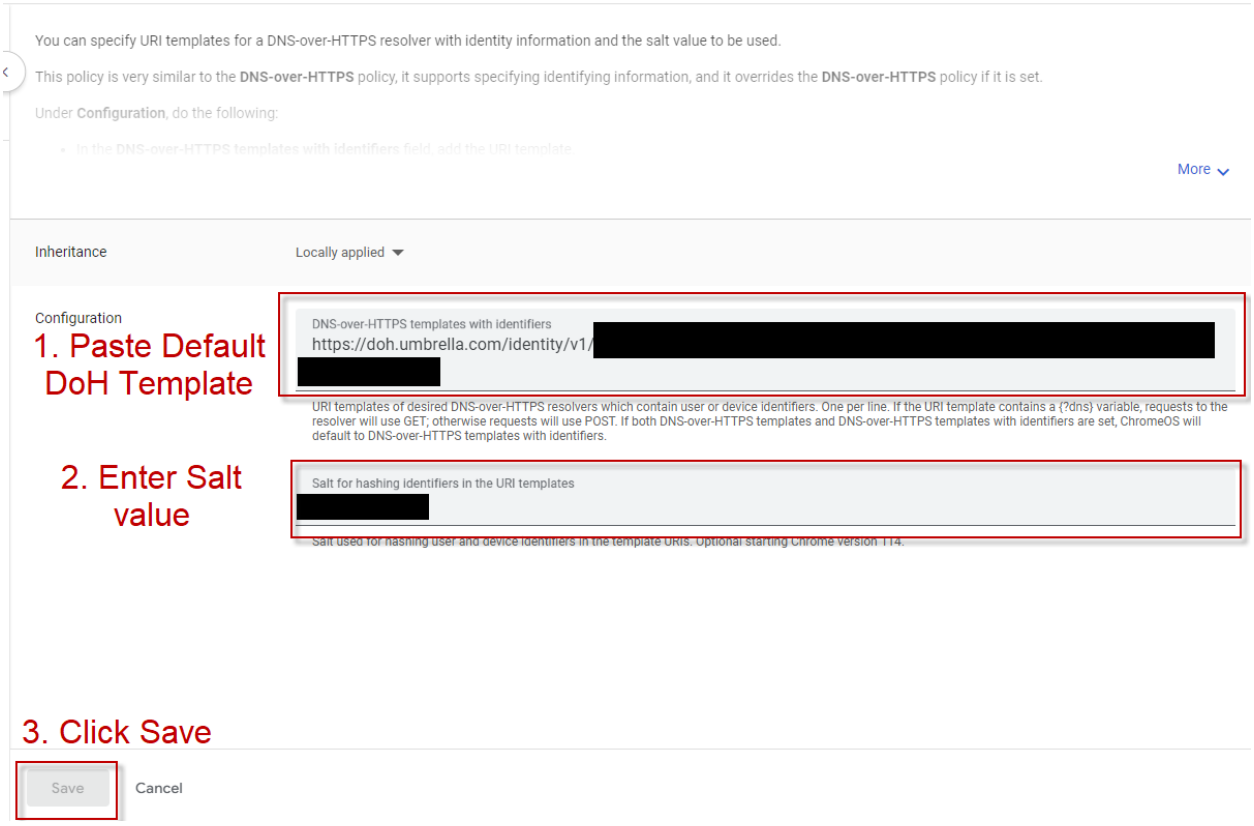


12. In the “Search or add a filter” field enter “DNS” then in the Network section click the “DNS-over-HTTPS” setting. Select “Prefer DNS over HTTPS, allow insecure fallback” then click “Save.”

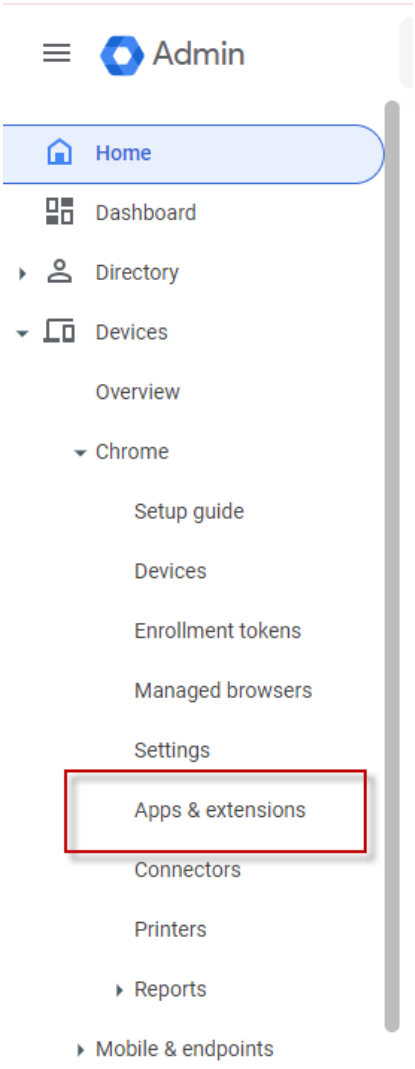


13. In the “Search or add a filter” field enter “DNS” then click the “DNS-over-HTTPS with Identifiers” setting. Copy and paste the Default DoH Template URL Link you saved in a Txt file earlier, then type the Salt Value you set earlier, then click “Save.”

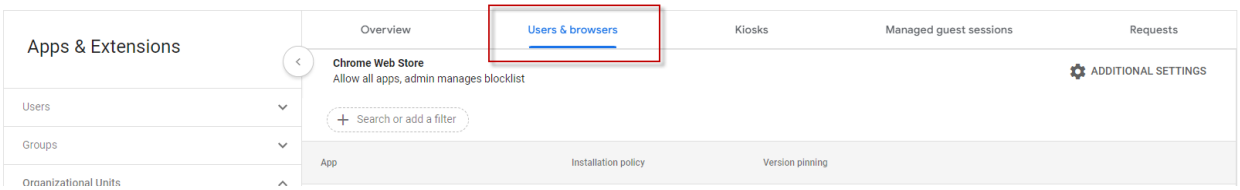




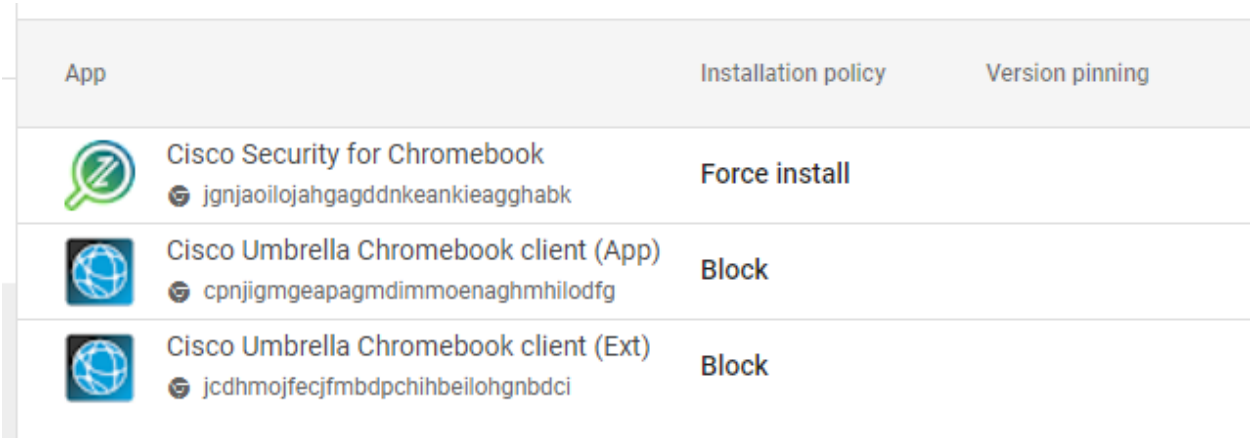
14. Navigate to Devices/Chrome/Apps & extensions.



15. Select Users & browsers.



16. NOTE: For the next steps keep in mind that you will want to block/remove the old Cisco Umbrella Chromebook clients while deploying the new Cisco Security for Chromebook app. So, ensure that the old Cisco clients are removed from every OU that may have had them deployed. Each OU should look similar to this image when you are finished with the deployment.

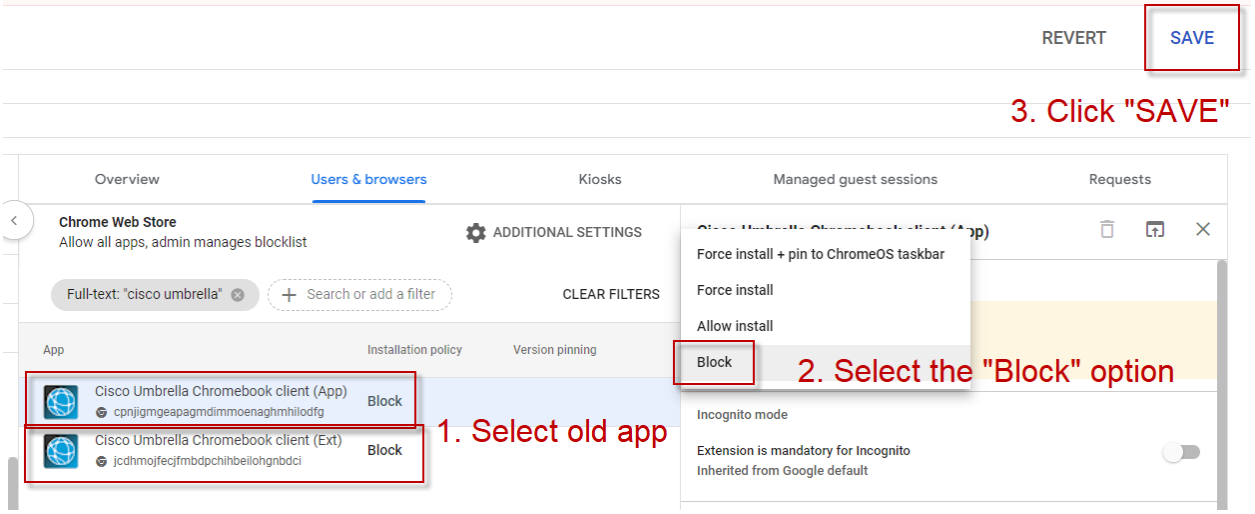


An additional note the new Cisco Security for Chromebook will need to be deployed to Gsuite Users NOT Chromebooks. If you deploy to an OU that only contains Chromebooks, they will not receive the app. If the OU contains both Users and Chromebooks, only the Users will receive the app.

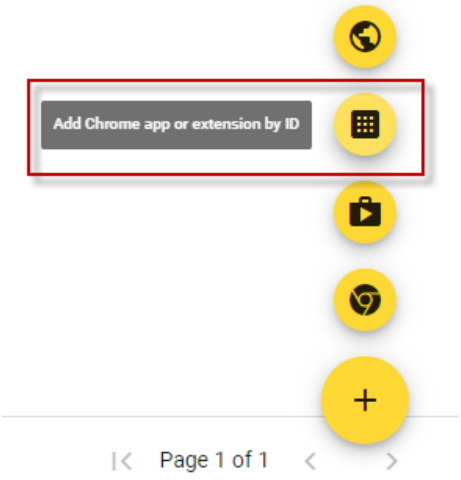
17. Block the old Cisco Umbrella Chromebook Clients in every OU they are deployed from:
    In each OU the existing App and Ext are deployed in search for the following IDs set their installation policy to Block.

    Chrome App IDs to Block:

        Cisco Umbrella Chromebook client (App) - cpnjigmgeapagmdimmoenaghmhilodfg
        Cisco Umbrella Chromebook client (Ext) - jcdhmojfecjfmbdpchihbeilohgnbdci

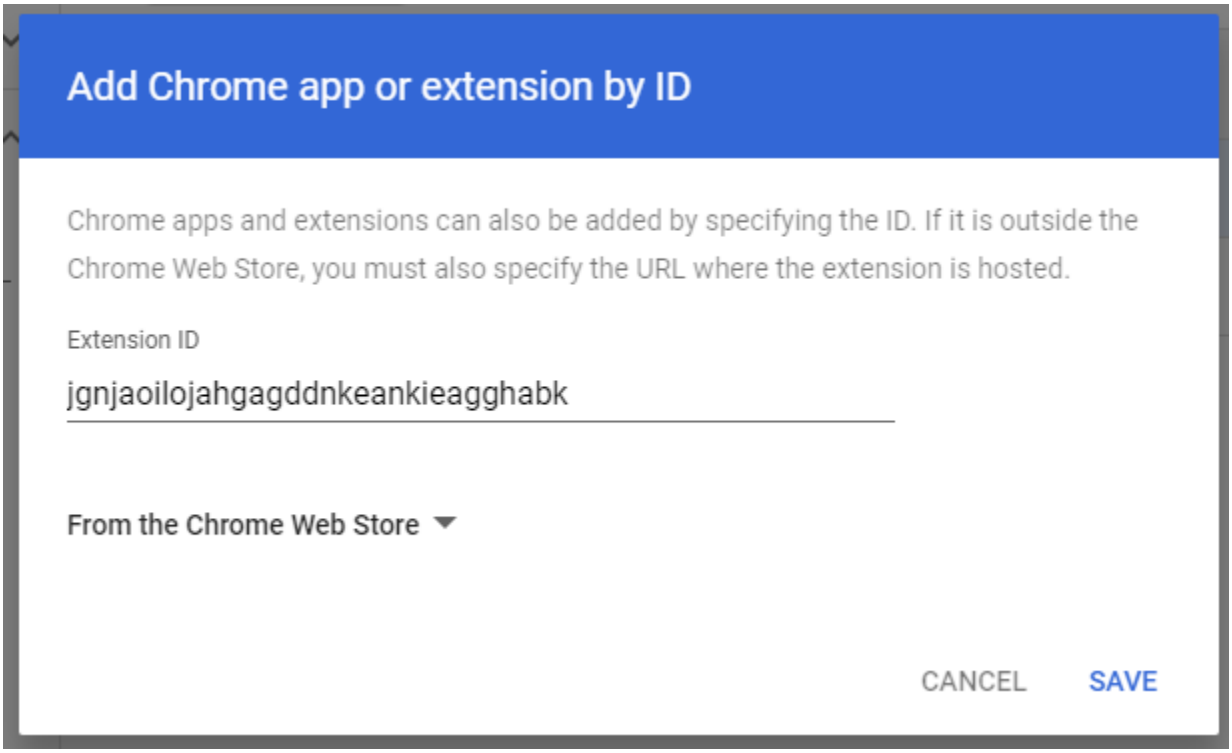


18. Deploy the new Cisco Security for Chromebook app:
    Select the OU you would like to deploy the new Cisco Security for Chromebook application to then hover over the yellow plus icon in the lower right corner of the webpage and click the “Add Chrome app or extension by ID” option.

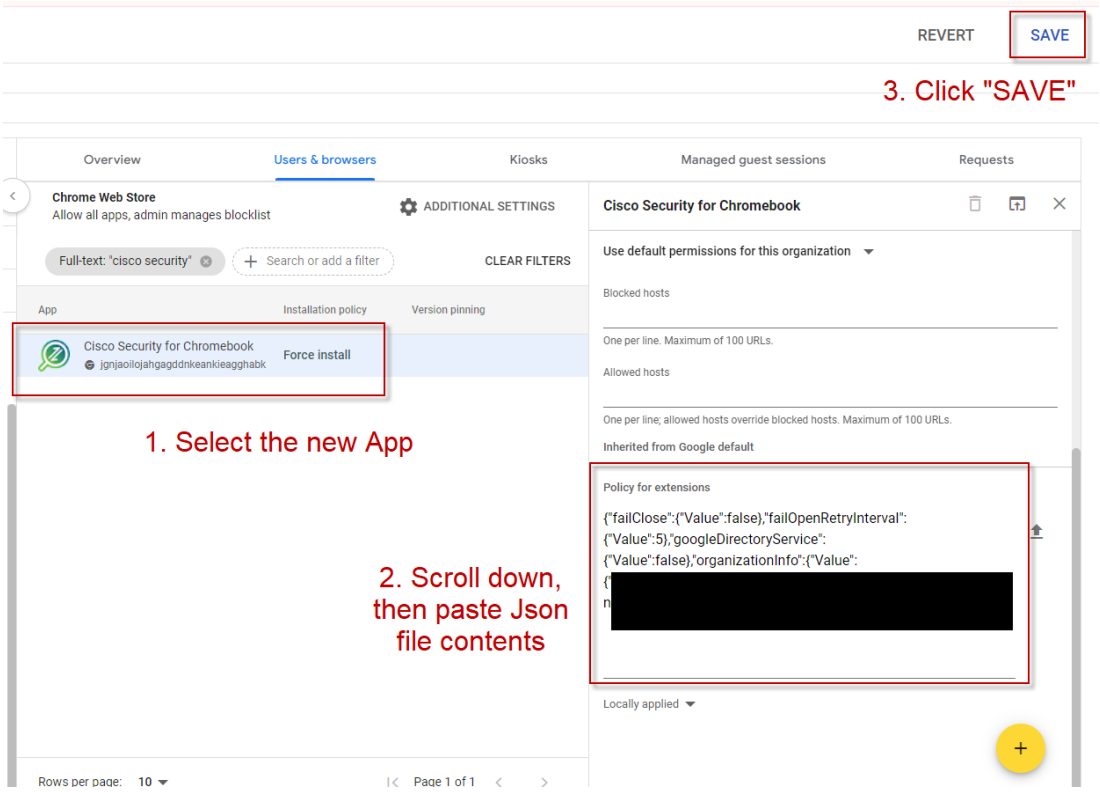


19. Search by Chrome App ID and make sure that “From the Chrome Web Store” option is selected, then press “SAVE.”

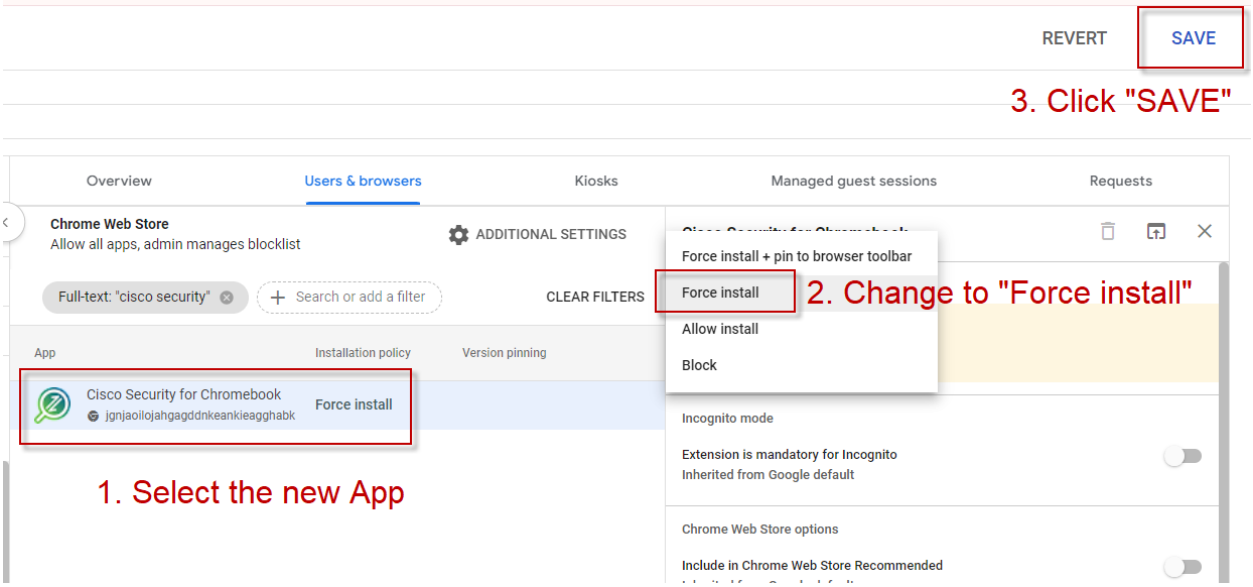
    Chrome App ID: jgnjaoilojahgagddnkeankieagghabk



20. Select the newly added Cisco Security for Chromebook App, scroll down in the settings then copy/paste the contents of the Json file you downloaded earlier. Then click “SAVE” in the top right of the webpage.

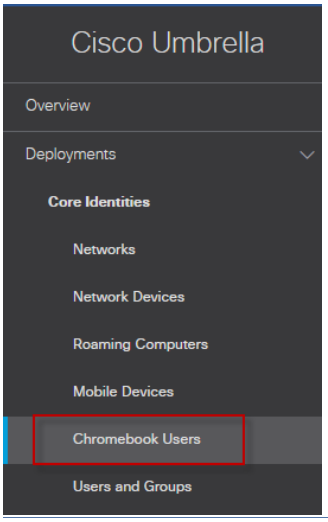


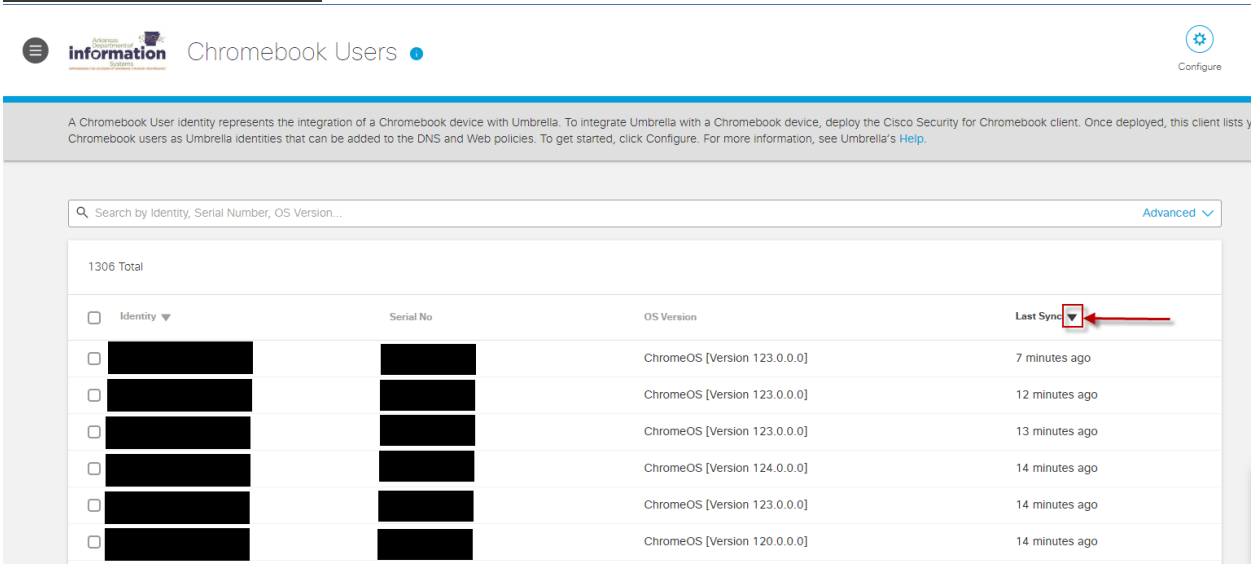
21. Select the Cisco Security for Chromebook App again and change the Installation policy from Allow install to Force install.



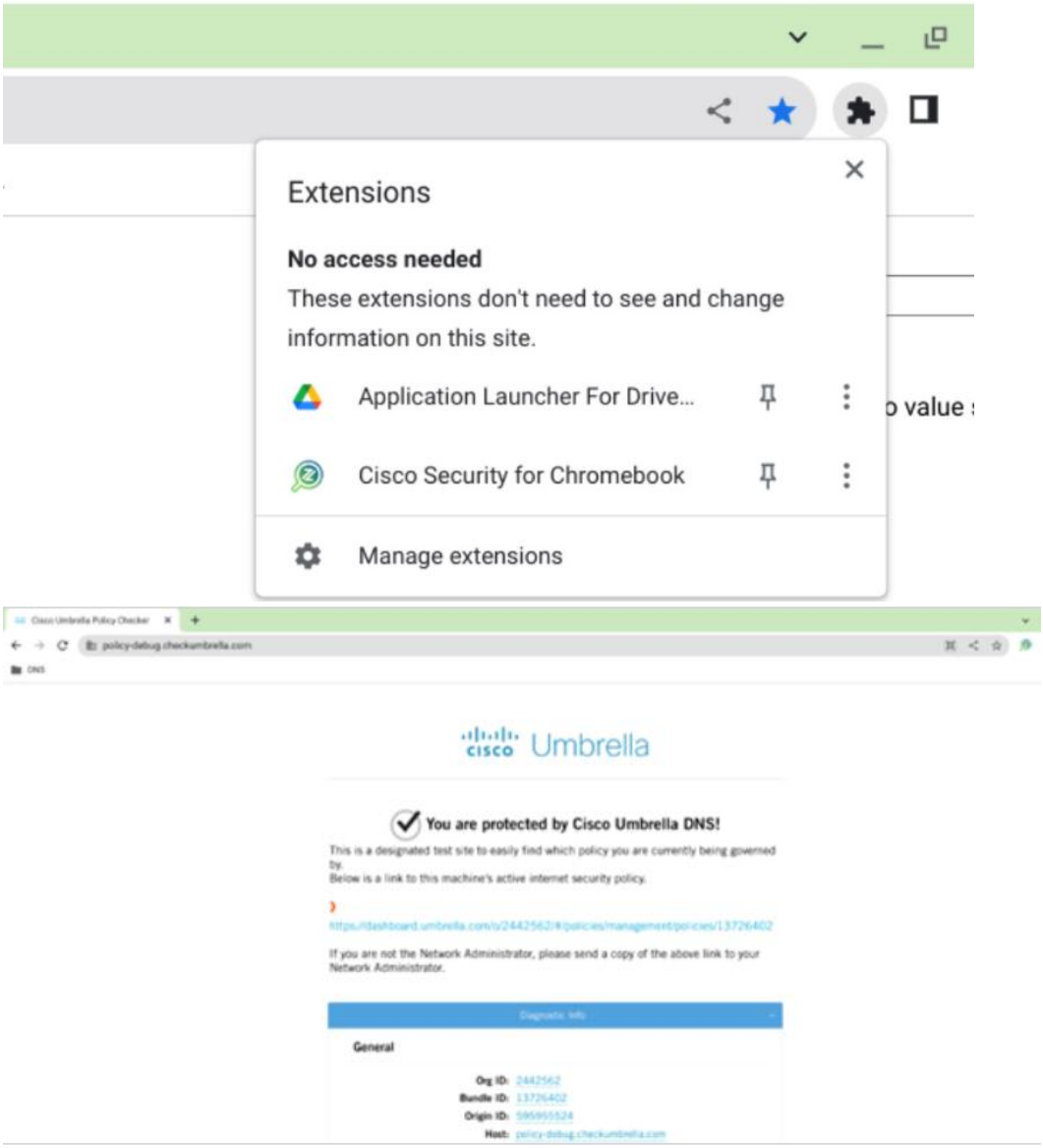
Testing and Troubleshooting

22. Once deployed you can check on the sync status by going back to the Chromebook Users page in Umbrella Dashboard and search for the user's identity or the device's serial number. Or you can sort by the "Last Sync" column.
    Note it may take a few minutes before users start showing up as synced.





23. You can also check if the App has successfully deployed to a Chromebook by checking the logged in users Extensions as well as visiting https://policy-debug.checkumbrella.com while logged in as the user.



Apply Policies

To apply your policies to your organization's Chromebooks, see the Cisco Umbrella Chromebook Client Policy Configuration Guide.

Make sure you have *deployed* the Cisco Umbrella Chromebook client before you configure policies. For more information, see the Cisco Umbrella Chromebook Client Deployment Guide.

For general information about configuring policies in Cisco Umbrella, see Create and Apply Policies.

Overview

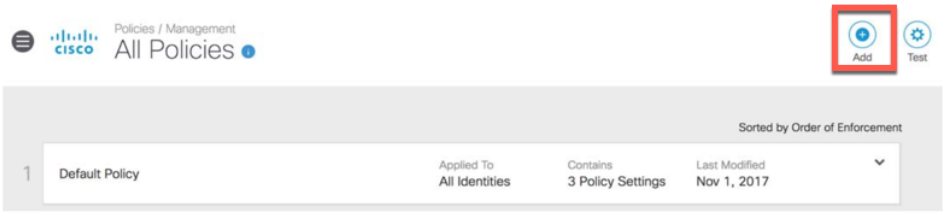
The overall process is to create a Chromebook-specific policy that will work together with your "network usage" policy that applies to all devices connected to your networks. You place the Chromebook policy at the top of your policies list, so it will be invoked first. This ensures that the *Chromebook policy* is applied to your Chromebooks. Then your *network policy* comes into effect for all other devices connected to your network.

To maintain end-user privacy when Chromebooks are connected at remote locations, you can also disable *Content Logging* and include only security-related events in your reporting.

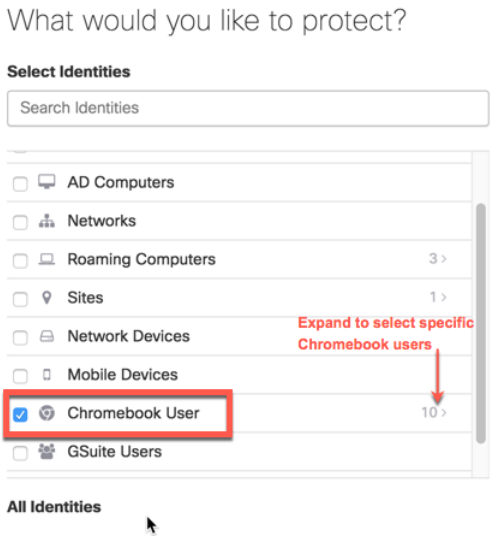
Create a Chromebook-specific policy

Follow these steps to create a policy to apply to all Chromebook users when connected to your network as well as *outside* of your networks.

1. Navigate to **Policies > Management > All Policies** and click **Add**.
   The Policy Wizard opens.

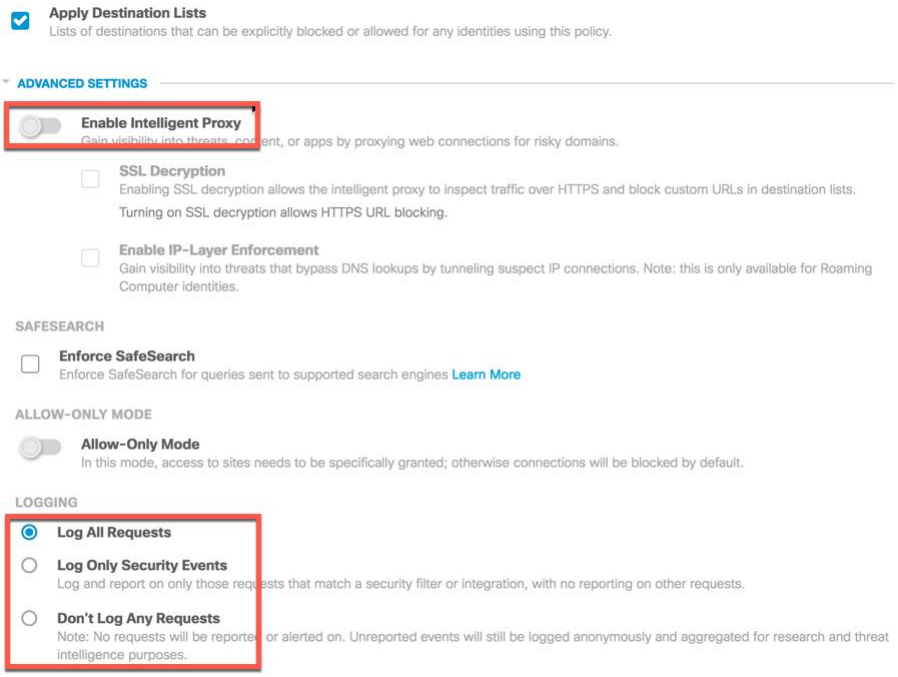


2. Select Chromebooks (some or all). Do not select any networks.

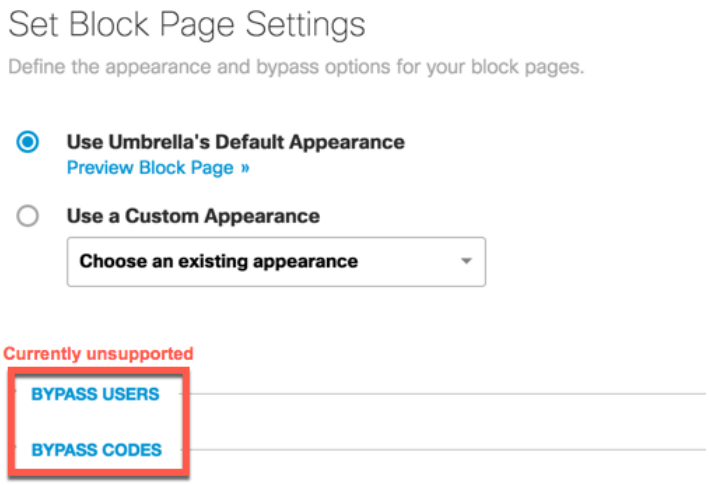


3. Click **Next**.
   Choose the content settings and security settings to apply to Chromebooks. A common practice is to **enable the default security settings** and **disable content filtering to maintain user privacy.**

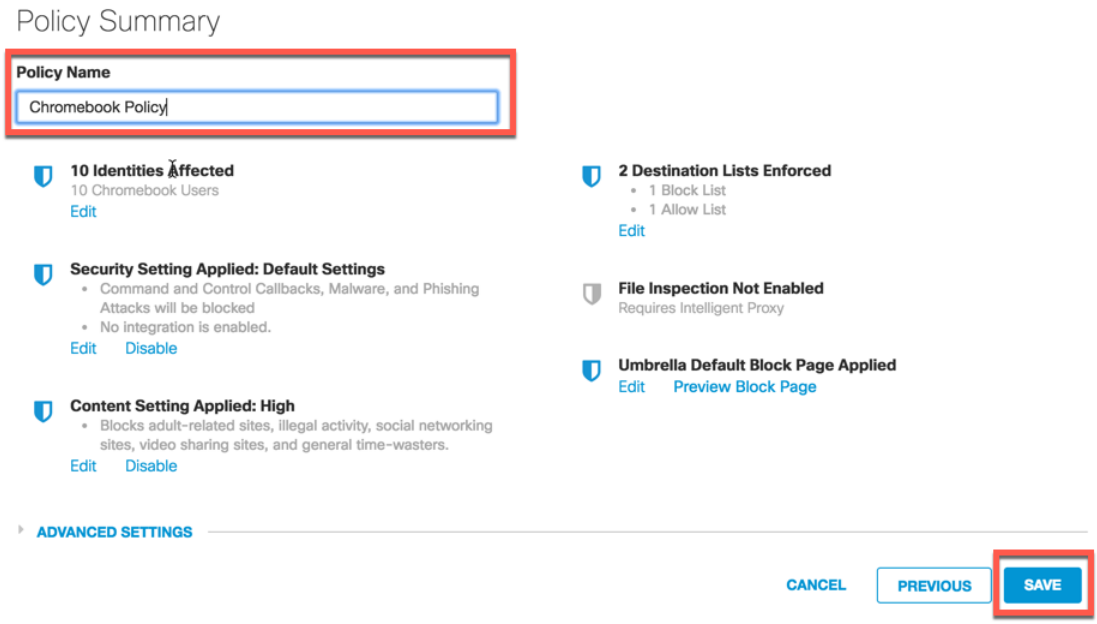
4. Expand **Advanced Settings** and turn off **Enable Intelligent Proxy**.
   The Intelligent Proxy is not supported at this time.
   Optionally, you can choose to log only Security Events to protect users' privacy.



5. Click **Next**. Generally no changes are needed to the Security Settings.
6. Click **Next**. Similarly, Content Access settings often remain the same.
7. Click **Next**. Make any needed changes to the Application Settings.
8. Click **Next**. Make any needed changes to Destination Lists.
9. Click **Next**.
   The Custom block page, Bypass Users, and Bypass Codes features on this page are not yet supported by the Chromebook client.



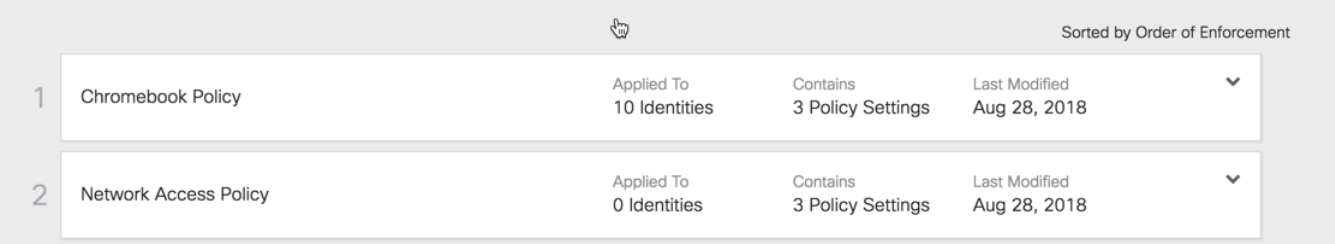
9. Click **Next**. Give your policy a name (the name is arbitrary), then click *Save*.



Your policy is automatically applied to Chromebooks. The process takes up to about 90 seconds.

Arrange policies in order

Policies in Cisco Umbrella are applied in sequence from the top of the Policy List down. **Make sure that your Chromebook policy appears *above* your network usage policy.** This ensures that your Chromebooks are protected by your Chromebook-specific policy and all devices on your network (that are not Chromebooks) are protected by your Network Access policy.



Trusted Network Detection

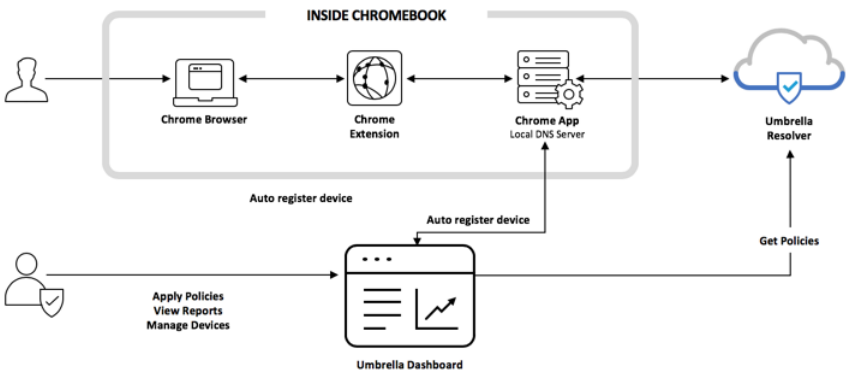
The version of the Cisco Umbrella Chromebook client (UCC) released November 28, 2018 introduced **trusted network detection**. Trusted network detection enables UCC to work with Umbrella virtual appliances (VAs) so that in a situation in which a network can be trusted by the UCC because it is protected by Umbrella VAs (for example, in an on-premise network), a Chromebook-specific policy can take precedence over the existing network policy.

How trusted network detection works

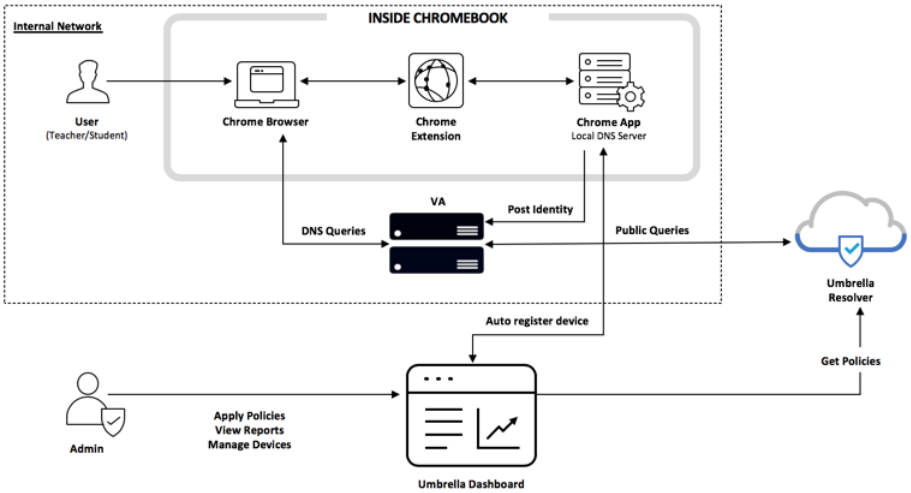
When the UCC detects a VA in a network, it sends the Chromebook user's identity to the VA and then deactivates. The VA continues to handle DNS requests from Chromebooks by appending the users' identities to all requests to Umbrella resolvers.

When the UCC fails to detect a VA, the UCC directly sends DNS requests to Umbrella resolvers.

This update is reflected in the following architecture diagrams. First is the **original** UCC architecture.



The November 28 release means the UCC system is better represented this way.



Important

In order to enable trusted network protection, both the Umbrella Chromebook client software **and** the Umbrella virtual appliance software must be updated.

Software requirements

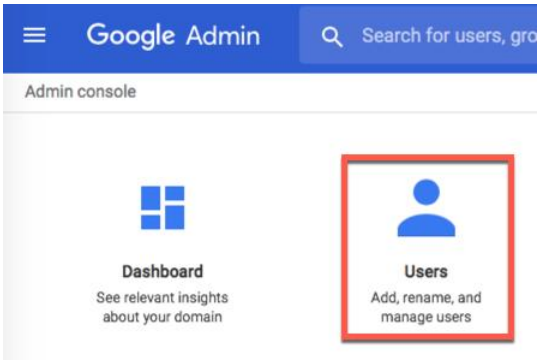
In order to enable trusted network detection, the following minimum software versions are required:

- Umbrella Chromebook client extension 1.2.0
- Umbrella Chromebook client app 1.2.5
- Umbrella virtual appliance 2.3.2

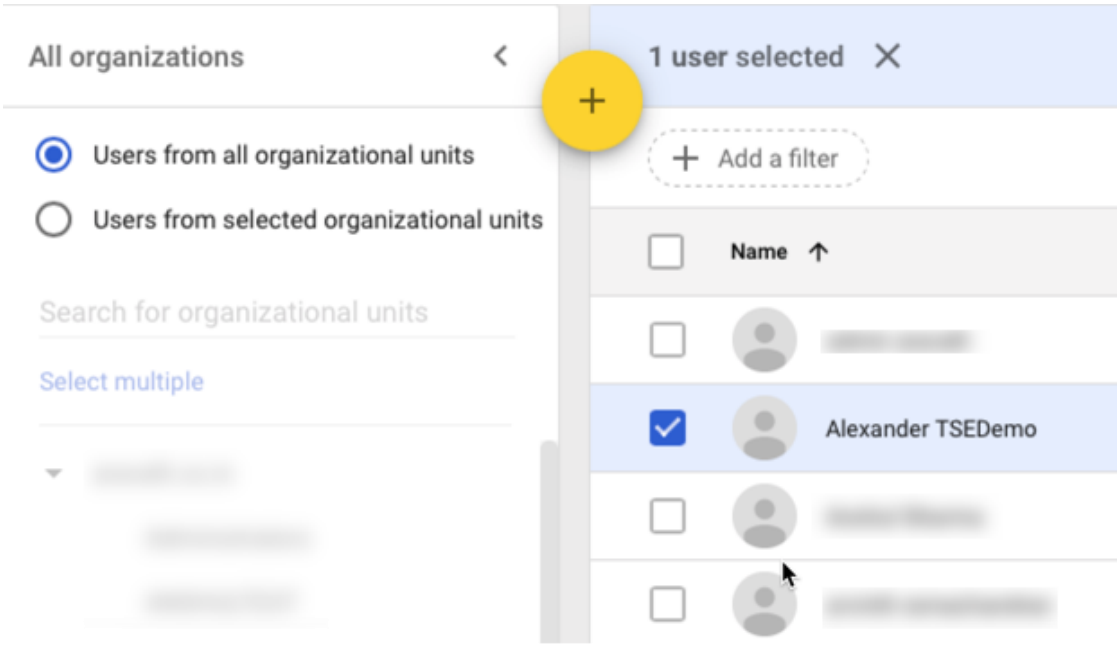
Removing Cisco Chromebook client software

To remove the software for a specific user:

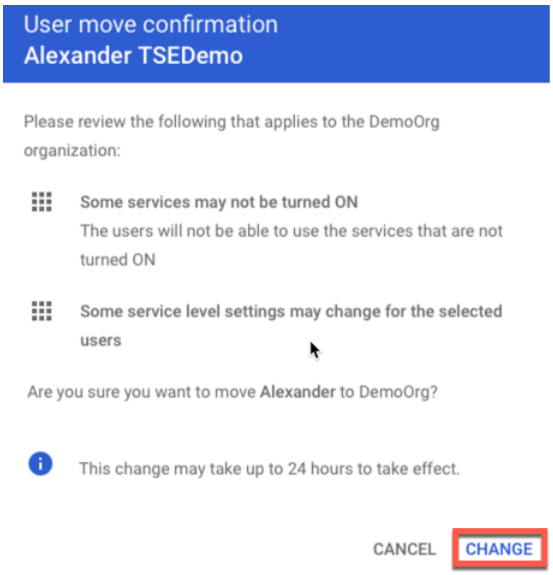
1. Log into your G Suite admin console, then click **Users**.



2. Choose a user, then choose **More > Change Organizational Unit**.



3. Click *Change** to confirm your choice.

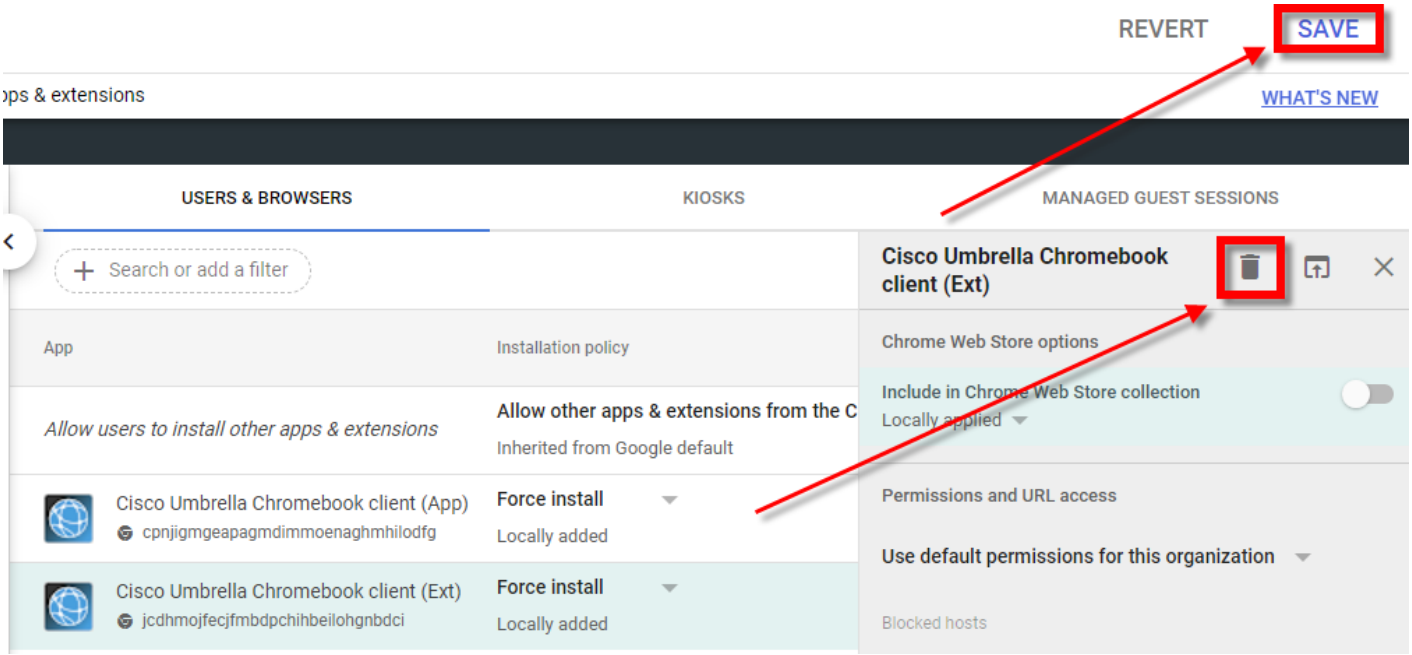


You have finished removing the Chromebook client for that user.

To remove the software for all members of an Organizational Unit (OU):

1. Follow the instructions for Installing the Cisco Umbrella Chromebook client **extension**.

2. Select the OU you wish to remove the extention from, then select Cisco Umbrella Chromebook client (Ext)
3. Click the **trash** icon to remove the extension, then click **SAVE**



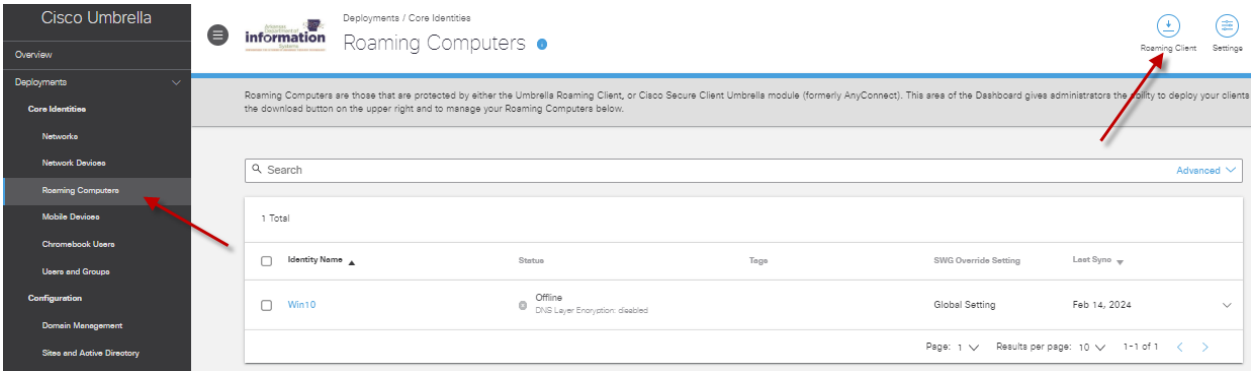
Cisco Secure Client (Roaming Client Replacement) Migration

Reference: https://support.umbrella.com/hc/en-us/articles/17890678933012-How-do-I-install-Cisco-Secure-Client-with-the-Umbrella-Module

NOTE: The old Cisco Umbrella Roaming Client will no longer be supported after April 2, 2025, please ensure you are fully migrated over to the new Cisco Secure Client before Aprile 2, 2025.

Also note that if you are running an existing version of the Roaming Client then the Cisco Secure Client installer will uninstall the Roaming Client and import it's settings.

Download the Cisco Secure Client from the following location in your Cisco Umbrella Dashboard

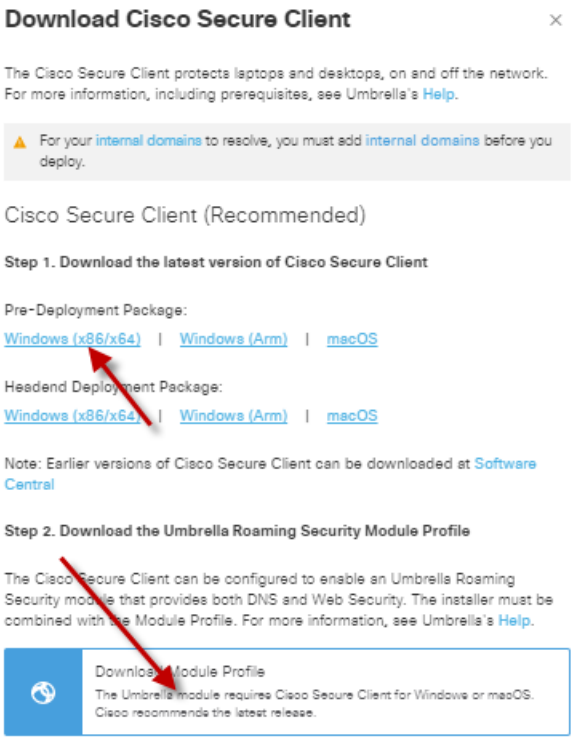


Step 1. Download the latest version of Cisco Secure Client

Select the Pre-Deployment Package: Windows (x86/x64)

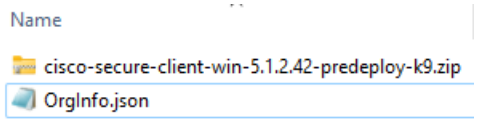
Step 2. Download the Umbrella Roaming Security Module Profile

Important! Make sure to keep the default name OrgInfo.json



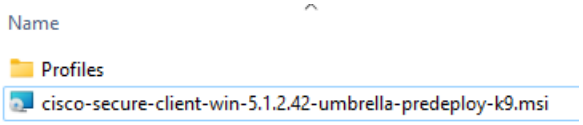
After the files have downloaded, make sure they are both saved in a known location.

Extract the .zip file



After the files are extracted, only keep the **umbrella**-predeploy-k9.msi file AND the Profiles/umbrella Folder

Copy the OrgInfo.json file you downloaded into the Profiles/umbrella Folder



Determine which installation options you will need:

Basic Setup - No Restart

msiexec.exe /package cisco-secure-client-win-5.1.2.42-umbrella-predeploy-k9.msi /norestart /passive

Setup - Hide From Programs

msiexec.exe /package cisco-secure-client-win-5.1.2.42-umbrella-predeploy-k9.msi /passive ARPSYSTEMCOMPONENT=1 /norestart

Setup - Lockdown Service

msiexec.exe /package cisco-secure-client-win-5.1.2.42-umbrella-predeploy-k9.msi /passive LOCKDOWN=1 /norestart

Setup - Hide From Programs and Lockdown Service

msiexec.exe /package cisco-secure-client-win-5.1.2.42-umbrella-predeploy-k9.msi /passive ARPSYSTEMCOMPONENT=1 LOCKDOWN=1 /norestart

iOS Mobile Security- iPads in Umbrella

The *Cisco Security Connector—Umbrella Setup Guide* only explains how to configure the Umbrella portion of the Cisco Security Connector (CSC). For information about how to configure your Mobile Device Manager (MDM) system, see your MDM system's documentation.

The Cisco Security Connector provides visibility and control for organization-owned and MDM managed mobile Apple iOS devices, such as iPhones and iPads. The CSC's Umbrella component directs DNS traffic, including functionality for the intelligent proxy, to the Cisco Umbrella cloud where filtering against malicious sites, such as phishing sites or sites that exfiltrate information, takes place.

The CSC's Umbrella portion does not require an on-demand or always-on VPN or a full proxy to gain complete visibility and control through cloud security (not locally on the device). This makes for both easier management and simpler, more effective security.

Note: Your iOS mobile device must be supervised and managed by an MDM system.

For more information about the Cisco Security Connector, see Cisco Security Connector (CSC).

Requirements

For the Cisco Security Connector:

- iOS device running iOS version 13.2 or higher.
- Your iOS device must be running in supervised mode.
- Your iOS device must be managed using a Mobile Device Manager (MDM) system and Apple School Manager or Apple Business Manager.

- Five MB free space.

One of the following supported MDM systems:

- Meraki System Manager (SM) with API access enabled.
  Note: Only System Manager and Combined network types are supported.
- Apple Configurator 2.5 or higher.
- IBM MaaS360.
- Intune.
- **Jamf.**
- MobiConnect
- MobileIron Enterprise Mobility Management (EMM) On-Prem and Cloud versions 9.4 or higher.
- Workspace ONE.
- Generic— ***MOSYLE*** - Other MDMs may be used to manage your organization-owned iOS mobile device; however, success results may vary. For more information, see Register an iOS Device through a Generic MDM System.

For information about configuring your specific MDM system, see your MDM system's documentation or contact your MDM's support team.

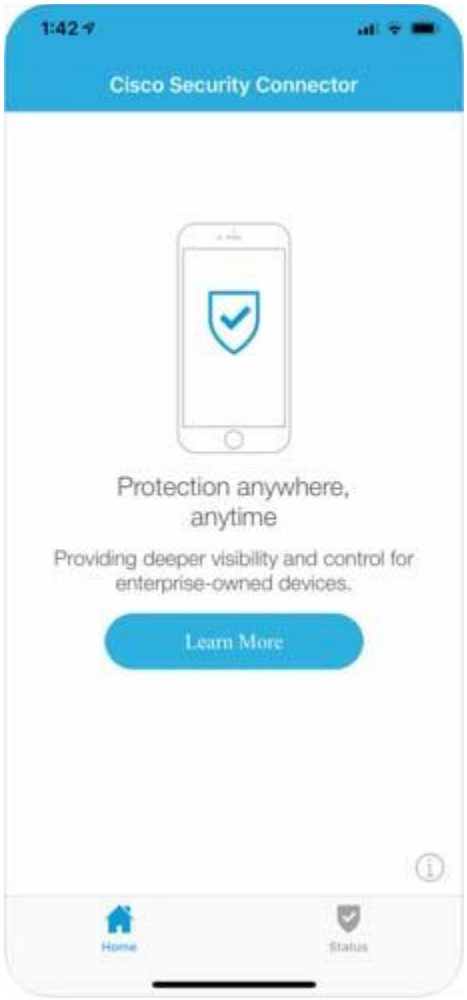
You will also need:

- Cisco Umbrella account.
- Direct access to the IPv4 IP addresses 208.67.222.222 or 208.67.220.220 is required for IPv4 DNS protection on ports 53 and 443.
- Direct access to the IPv6 IP addresses 2620:119:35::35 or 2620:119:53::53, or access to IPv4 addresses on ports 53 and 443 through NAT64/DNS64 translation is required for IPv6 DNS protection.
  Note: If DNS protection fails to engage, DNS traffic is not encrypted.
- The device must be able to communicate with `registration.polaris.qq.opendns.com` for registration and validation purposes at least once a day—when actively used—otherwise, the device cannot be protected.
- Depending on the MDM, you may also require each device's serial number.

1. Install the Cisco Security Connector App

1. On your iOS device, download and install the Cisco Security Connector app.

   Get the Cisco Security Connector app from the App store. Depending on your MDM, you may be able to deploy the Cisco Security Connector to supervised iOS mobile devices through your MDM.

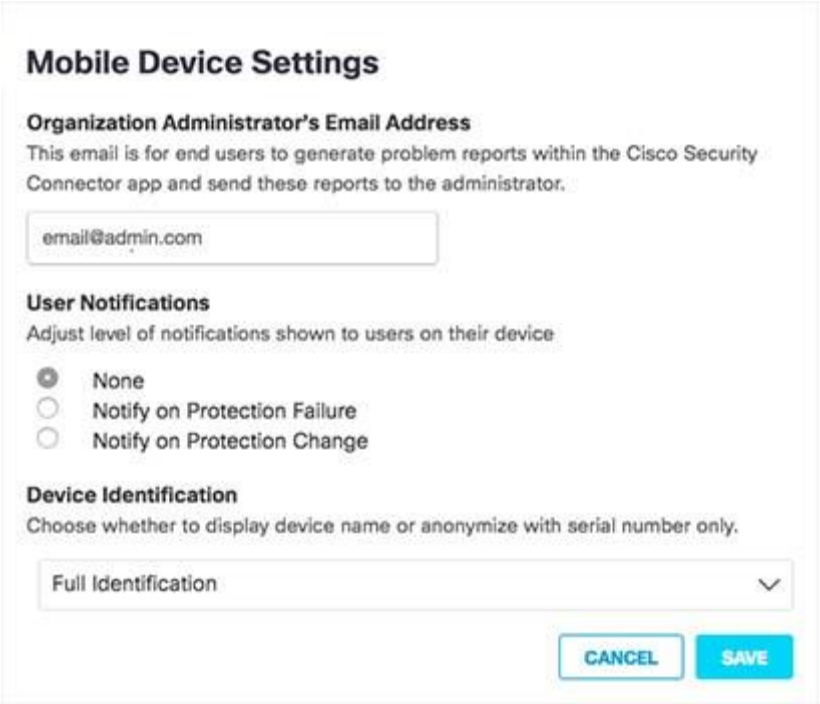


2. Add an Organization Administrator's Email Address

This is the email address that your end-user can use to send diagnostic reports from the app by clicking the **I** icon from within the iOS device. These reports can then be passed onto Cisco support. Once set, this email address is automatically added when managing an MDM.

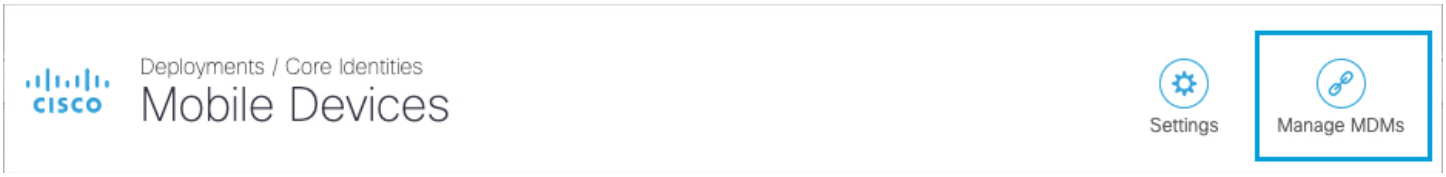
1. Navigate to **Deployments > Core Identities > Mobile Devices** and click **Settings**.

2. In **Mobile Device Settings**, add an email address, select a notifications level, choose a device identification method, and click **Save**.

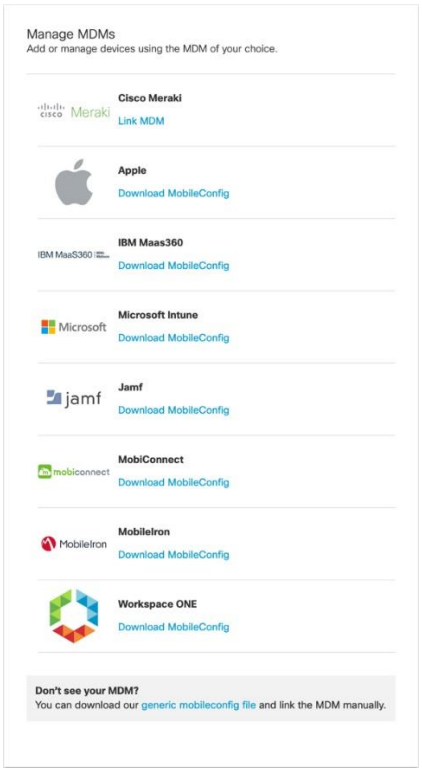


3. Register Your iOS Device Through Your MDM to Umbrella

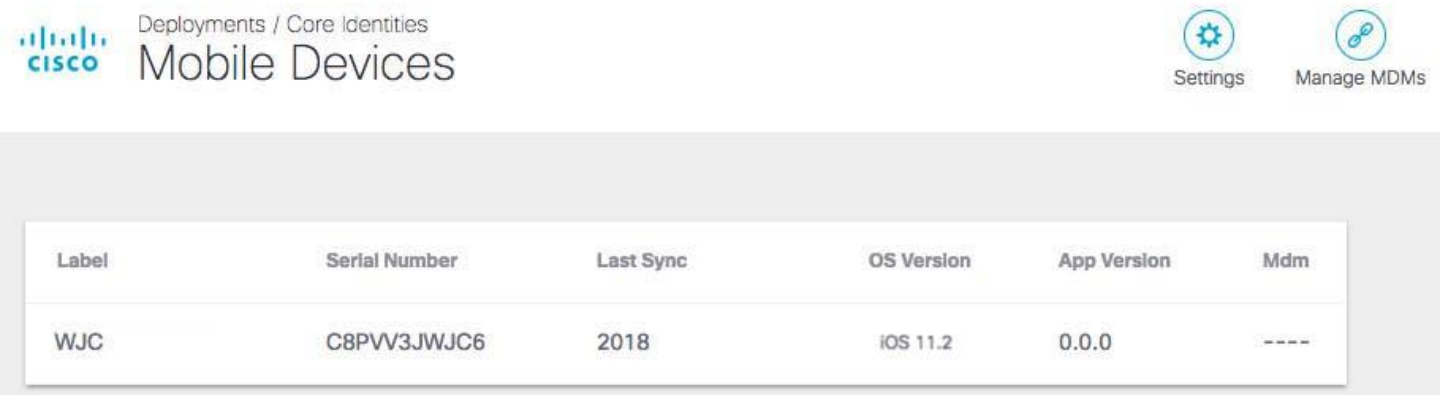
1. In Umbrella, navigate to **Deployments > Core Identities > Mobile Devices** and click **Manage MDMs**.



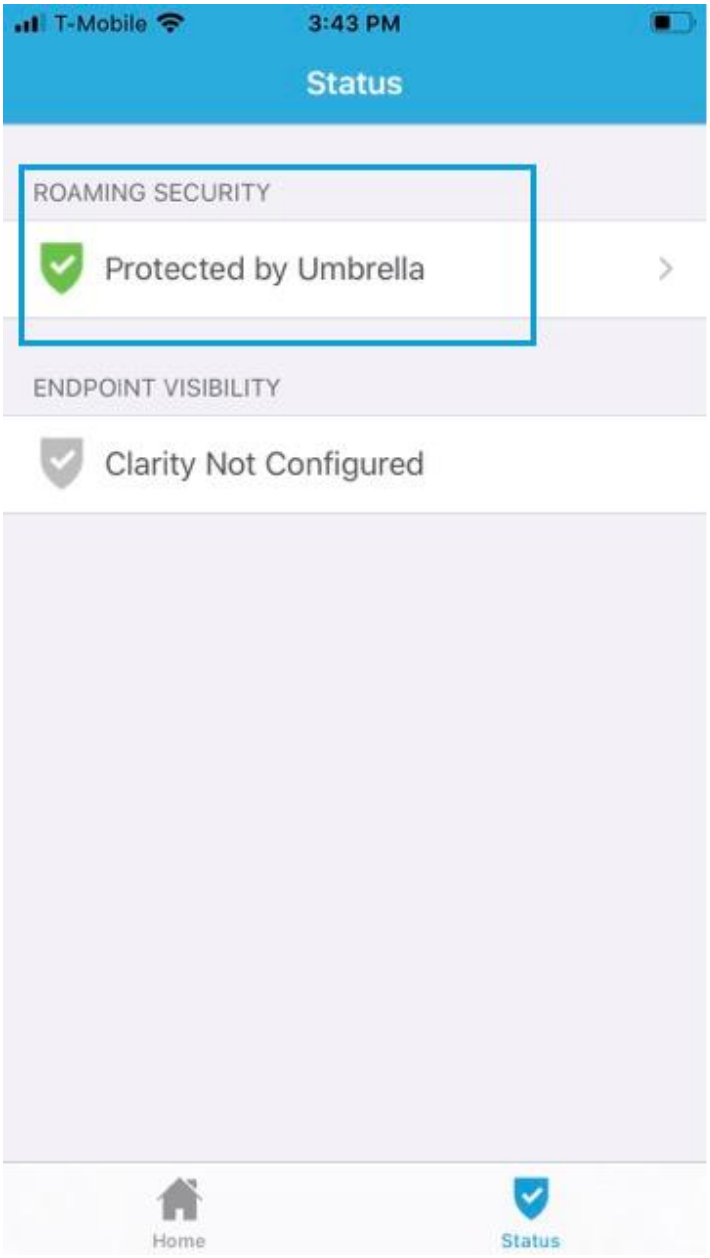
2. Click the appropriate MDM.



4. When you have successfully registered your iOS device, Umbrella lists it at **Deployments > Core Identities > Manage MDMs**.



5. On your mobile device, in the Cisco Security Connector app, tap the **Status** icon and confirm that it shows **Protected by Umbrella**. For protection details, tap **Protected by Umbrella**.



Jamf

By downloading an XML file from Umbrella, optionally updating it, and then pasting part of its contents into your Jamf system, Jamf is able to push configuration information to both the Cisco Security Connector (CSC) and Umbrella so that your iOS device is registered with Umbrella. The result is that your iOS device is protected by Umbrella.

For information about configuring Jamf, see Jamf's documentation.

Anonymization

Umbrella provides you with the option of anonymizing mobile devices for reporting and administration purposes. When you anonymize a mobile device, its label is hidden and replaced by your device's serial number. The label name is anonymized in both the Umbrella dashboard and in the CSC app UI. For information about how to anonymize your device, see Anonymize Devices.

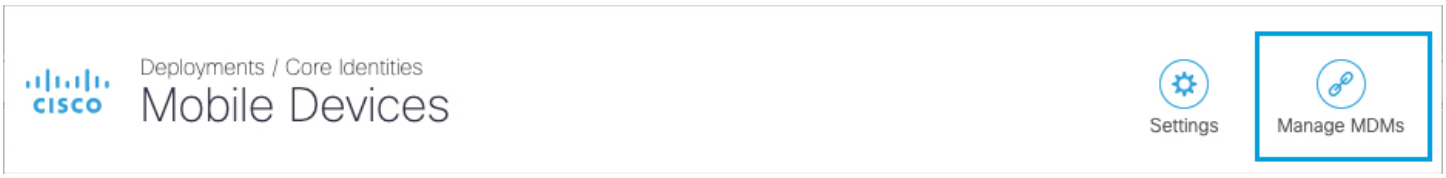
Prerequisites

- Jamf Pro 10.2.0 or higher.
- You must first configure your Jamf MDM system. Configure Jamf as required so that it is able to push configuration information to both CSC and Umbrella. For information about configuring Jamf, see Jamf documentation. For support, contact Jamf support.
- The Cisco Security Connector app is installed on your iOS device.
- iOS device running iOS version 13.2 or higher.
- Your iOS device must be running in supervised mode.
- Your iOS device must be managed by Jamf and Apple School Manager or Apple Business Manager.
- You have added an administrator email address.
  This address is used by CSC to send you diagnostic reports that you can pass on to Cisco support as needed.
- You'll need the serial number for each iOS device to be registered with Umbrella.
- Cisco Umbrella account.
- Direct access to the IPv4 IP addresses 208.67.222.222 or 208.67.220.220 is required for IPv4 DNS protection on ports 53 and 443.
- Direct access to the IPv6 IP addresses 2620:119:35::35 or 2620:119:53::53, or access to IPv4 addresses on ports 53 and 443 through NAT64/DNS64 translation is required for IPv6 DNS protection.
  Note: If DNS protection fails to engage, DNS traffic is not encrypted.
- If anonymizing devices, **Mobile Device Settings** are updated to **By Serial Number Only**. For more information see, Anonymize Devices.
- Your iOS device must be able to communicate with .opendns.com for registration and validation purposes at least once a day.

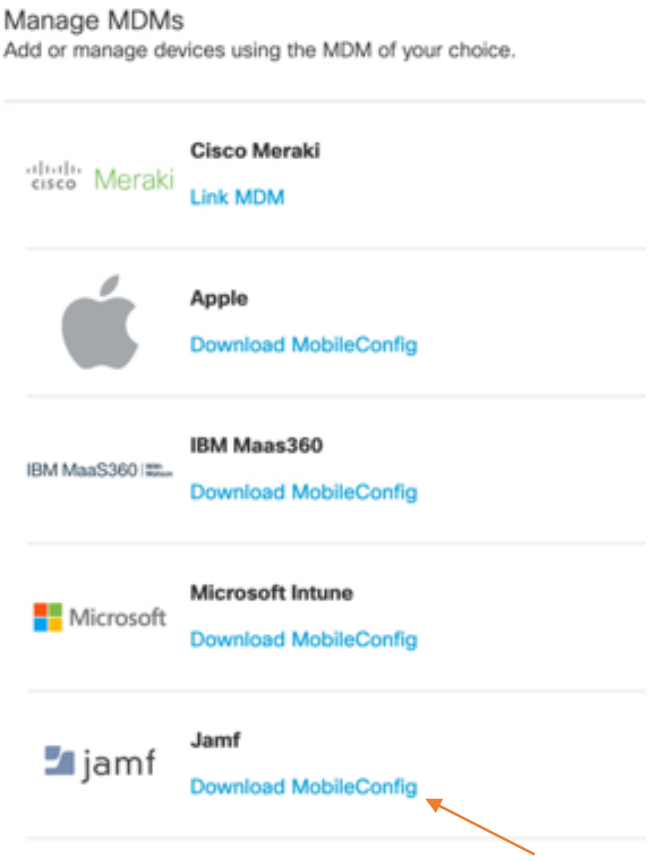
Register Your iOS Device

Note: You must log into your Umbrella dashboard as an administrator.

1. In Umbrella, navigate to **Deployments > Core Identities > Mobile Devices** and click **Manage MDMs**.

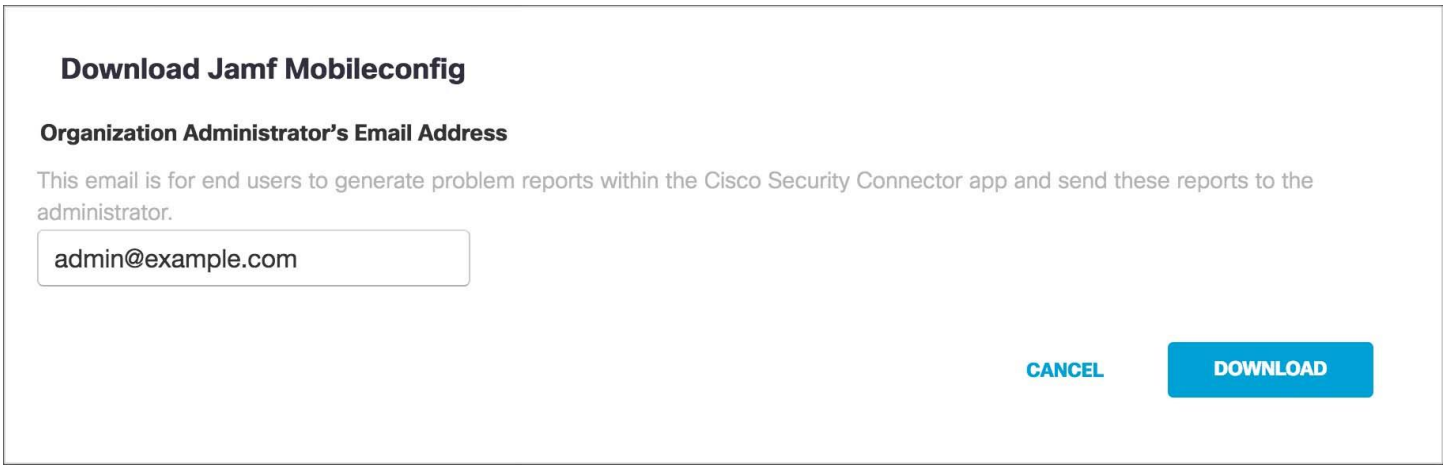


2. Under **Jamf**, click **Download MobileConfig**.



3. Add an email address to generate problem reports and click **Download**.

   This email address is where diagnostic reports are sent when a user clicks the **I** icon from within the iOS device. Once set, this email address is automatically added when managing an MDM.



4. Copy and paste the XML code between the **<!-- Jamf... -->** comments into your MDM profile.

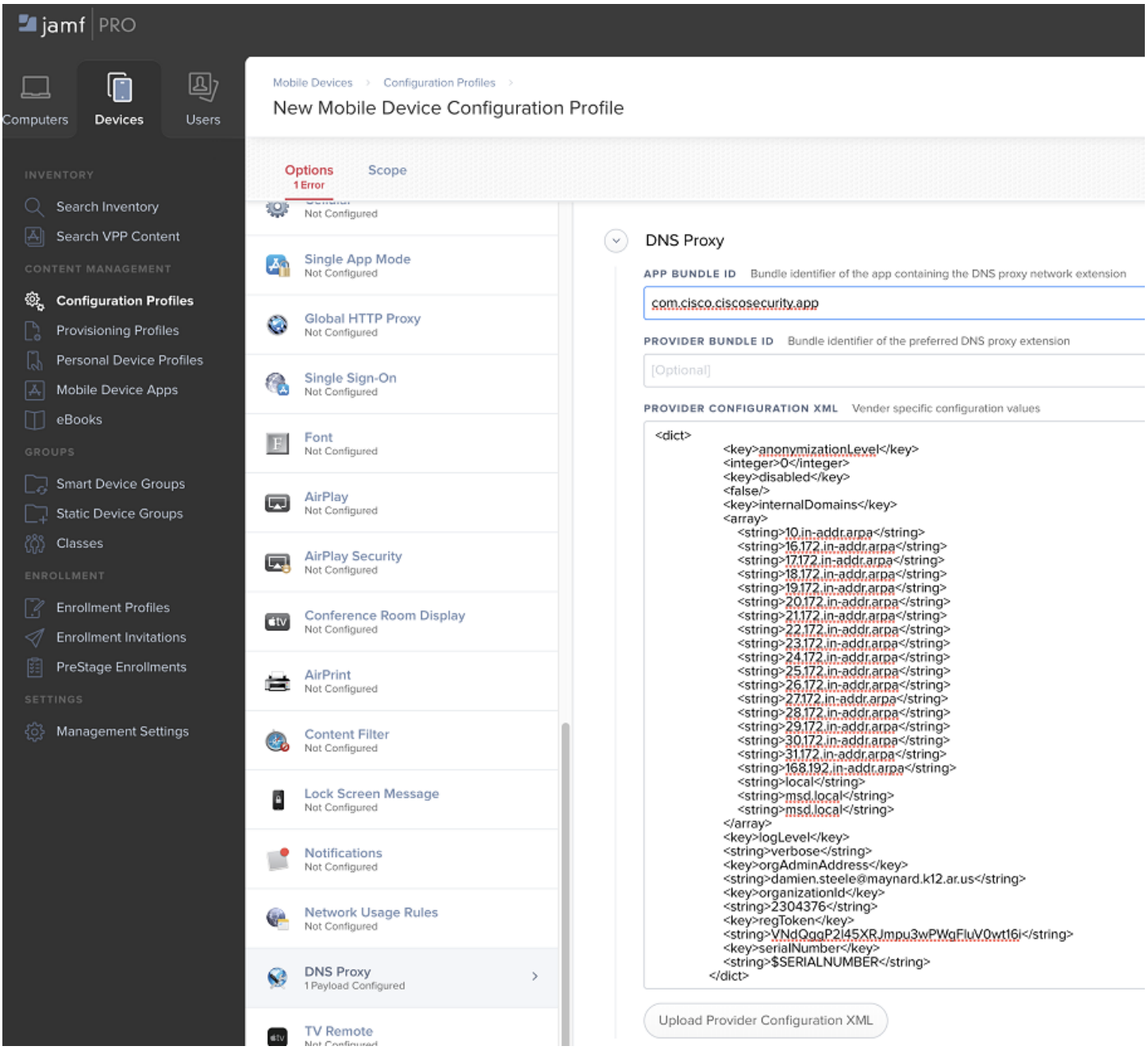
- **XML**

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
    <dict>
        <key>PayloadContent</key>
        <array>
<!-- Jamf - copy from here to paste into the Jamf UI to provision a DNS proxy -->
    <dict>

 .....

    </dict>
<!-- Jamf - end copy -->
```

5. In your new profile, applied for the CSC group, choose **Custom Settings** and then **Configure**. Paste the edited XML here.
   If successful, your mobile device registers with Umbrella and is listed at **Deployments > Core Identities > Sylvia Massy**. CSC on your mobile device updates to connect to Umbrella so that your iOS device is protected by Umbrella.

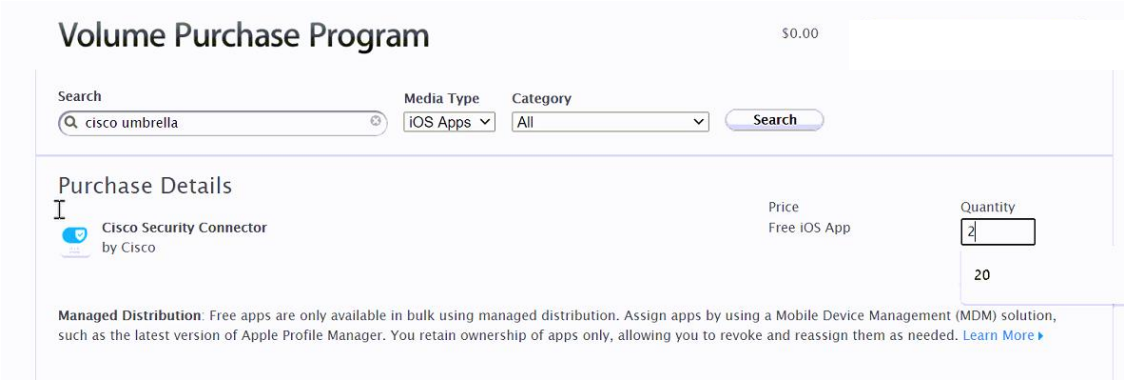
6. Example of what is put into the Config Profile in Jamf from the downloaded jamf.xml file obtained from Umbrella: (your organization id string and regToken will be different)

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-1.0.dtd">
<plist version="1.0">
    <dict>
        <key>PayloadContent</key>
        <array>
            <dict>
                <key>AppBundleIdentifier</key>
                <string>com.cisco.ciscosecurity.app</string>
                <key>PayloadDescription</key>
                <string>Cisco Umbrella</string>
                <key>PayloadDisplayName</key>
                <string>Cisco Umbrella</string>
                <key>PayloadIdentifier</key>
                <string>com.apple.dnsProxy.managed.DBE2A157-E134-3E8C-B4FB-23EDF48A0CD1</
string>
                <key>PayloadType</key>
                <string>com.apple.dnsProxy.managed</string>
                <key>PayloadUUID</key>
                <string>E5D191FD-6E01-4733-9720-E27BFBCB8DC5</string>
                <key>PayloadVersion</key>
                <integer>1</integer>
                <key>ProviderBundleIdentifier</key>
                <string>com.cisco.ciscosecurity.app.CiscoUmbrella</string>
                <key>ProviderConfiguration</key>
<!-- Jamf - copy from here to paste into the Jamf UI to provision a DNS proxy -->
                <dict>
                    <key>anonymizationLevel</key>
                    <integer>0</integer>
```


jamf PRO
Computers
Devices
Users
INVENTORY
Search Inventory
Search VPP Content
CONTENT MANAGEMENT
Configuration Profiles
Provisioning Profiles
Personal Device Profiles
Mobile Device Apps
eBooks
GROUPS
Smart Device Groups
Static Device Groups
Classes
ENROLLMENT
Enrollment Profiles
Enrollment Invitations
PreStage Enrollments
SETTINGS
Management Settings
Mobile Devices
Configuration Profiles
New Mobile Device Configuration Profile
Options
1 Error
Scope
Not Configured
Single App Mode
Not Configured
Global HTTP Proxy
Not Configured
Single Sign-On
Not Configured
Font
Not Configured
AirPlay
Not Configured
AirPlay Security
Not Configured
Conference Room Display
Not Configured
AirPrint
Not Configured
Content Filter
Not Configured
Lock Screen Message
Not Configured
Notifications
Not Configured
Network Usage Rules
Not Configured
DNS Proxy
1 Payload Configured
TV Remote
DNS Proxy
APP BUNDLE ID
Bundle identifier of the app containing the DNS proxy network extension
com.cisco.ciscosecurity.app
PROVIDER BUNDLE ID
Bundle identifier of the preferred DNS proxy extension
[Optional]
PROVIDER CONFIGURATION XML
Vender specific configuration values
<dict>
<key>anonymizationLevel</key>
<integer>0</integer>
<key>disabled</key>
<false/>
<key>internalDomains</key>
<array>
<string>10.in-addr.arpa</string>
<string>16.172.in-addr.arpa</string>
<string>17.172.in-addr.arpa</string>
<string>18.172.in-addr.arpa</string>
<string>19.172.in-addr.arpa</string>
<string>20.172.in-addr.arpa</string>
<string>21.172.in-addr.arpa</string>
<string>22.172.in-addr.arpa</string>
<string>23.172.in-addr.arpa</string>
<string>24.172.in-addr.arpa</string>
<string>25.172.in-addr.arpa</string>
<string>26.172.in-addr.arpa</string>
<string>27.172.in-addr.arpa</string>
<string>28.172.in-addr.arpa</string>
<string>29.172.in-addr.arpa</string>
<string>30.172.in-addr.arpa</string>
<string>31.172.in-addr.arpa</string>
<string>168.192.in-addr.arpa</string>
<string>local</string>
<string>msd.local</string>
<string>msd.local</string>
</array>
<key>logLevel</key>
<string>verbose</string>
<key>orgAdminAddress</key>
<string>damien.steele@maynard.k12.ar.us</string>
<key>organizationId</key>
<string>2304376</string>
<key>regToken</key>
<string>VNdQqqP2l45XRJmpu3wPWqFluV0wt16i</string>
<key>serialNumber</key>
<string>$SERIALNUMBER</string>
</dict>
Upload Provider Configuration XML

Mosyle

1. Download the Cisco Security Connector from the Apple Volume Purchase Program



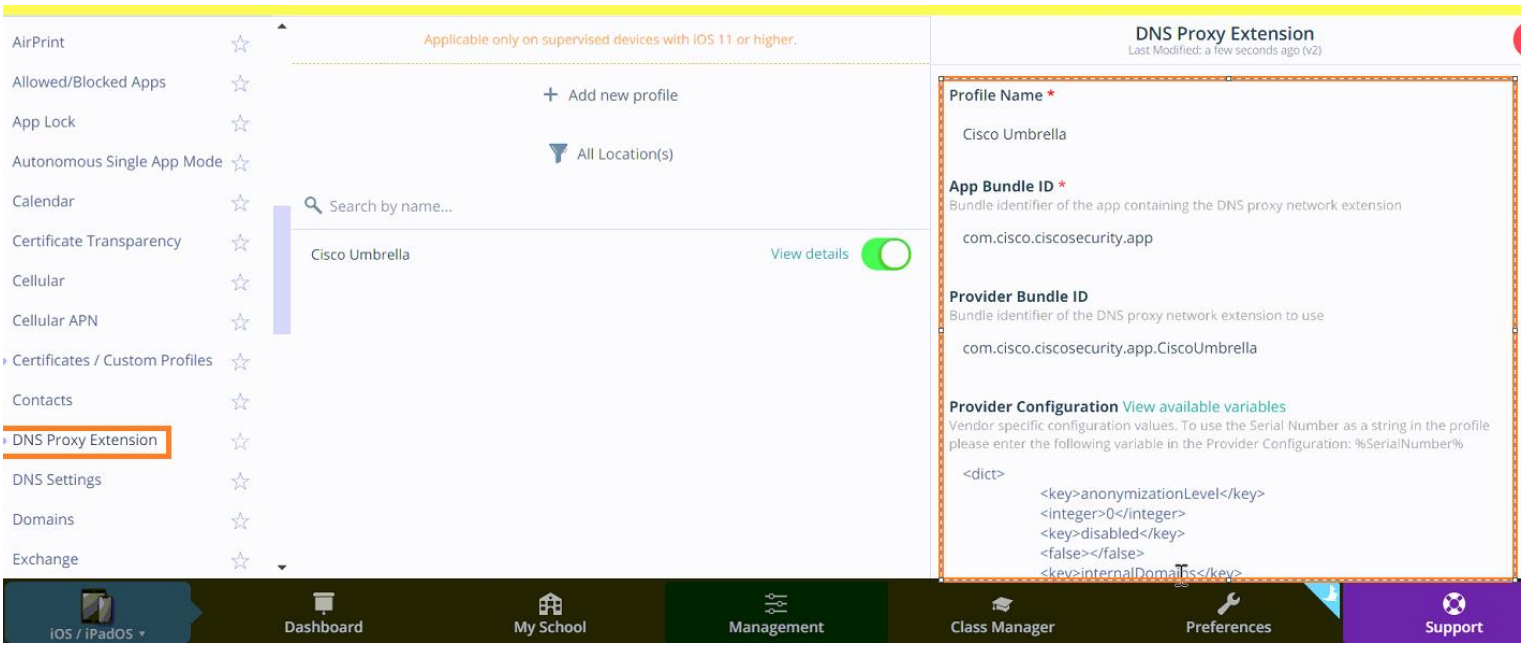
2. Push out the Cisco Security Connector App with Mosyle.
3. Download the Generic Mobileconfig file.

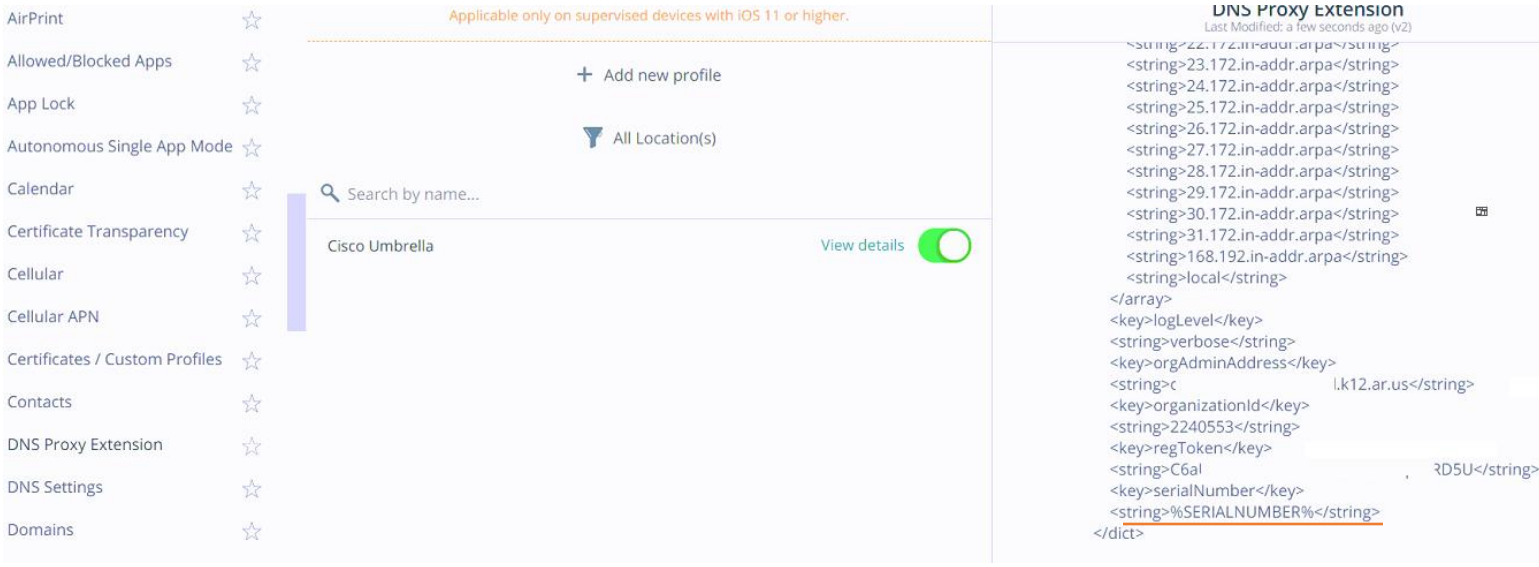
   Example:

4. In Mosyle, navigate to DNS Proxy Extension and enter the following:
   - Name – Cisco Umbrella
   - App Bundle Id – com.cisco.ciscosecurity.app
   - Provider Bundle ID - com.cisco.ciscosecurity.app.CiscoUmbrella
   - Provider Configuration – everything in the generic mobile config file.xml from

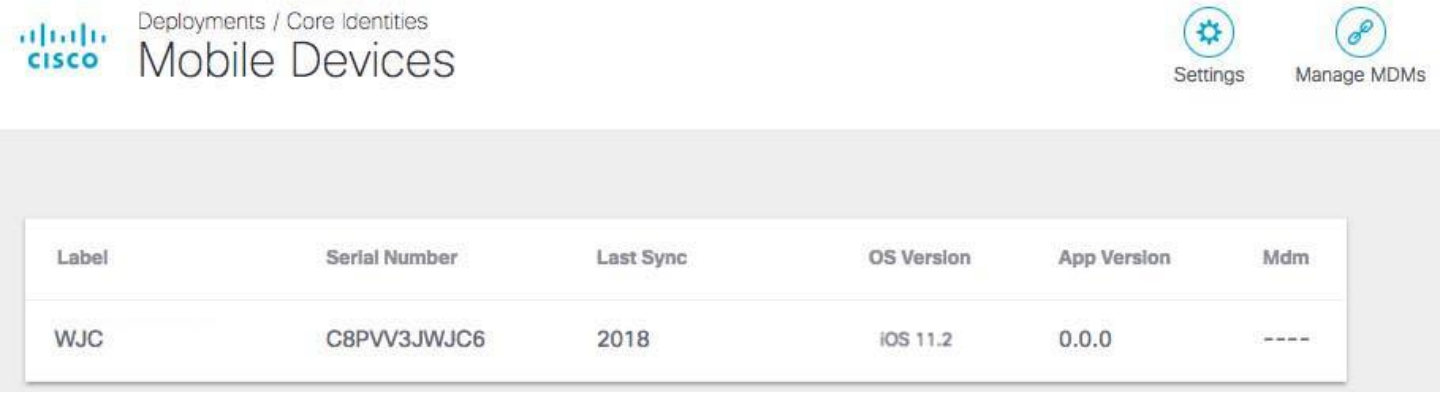
```
<dict>
  <key>anonymizationLevel</key>
  <integer>0</integer>
  <key>disabled</key>
  <false/>
        ....
        ....
        ....
        <key>serialNumber</key>
  <string>{SERIAL_NUMBER}</string>
</dict>
```

   - Replace SERIAL_NUMBER with %SERIALNUMBER%

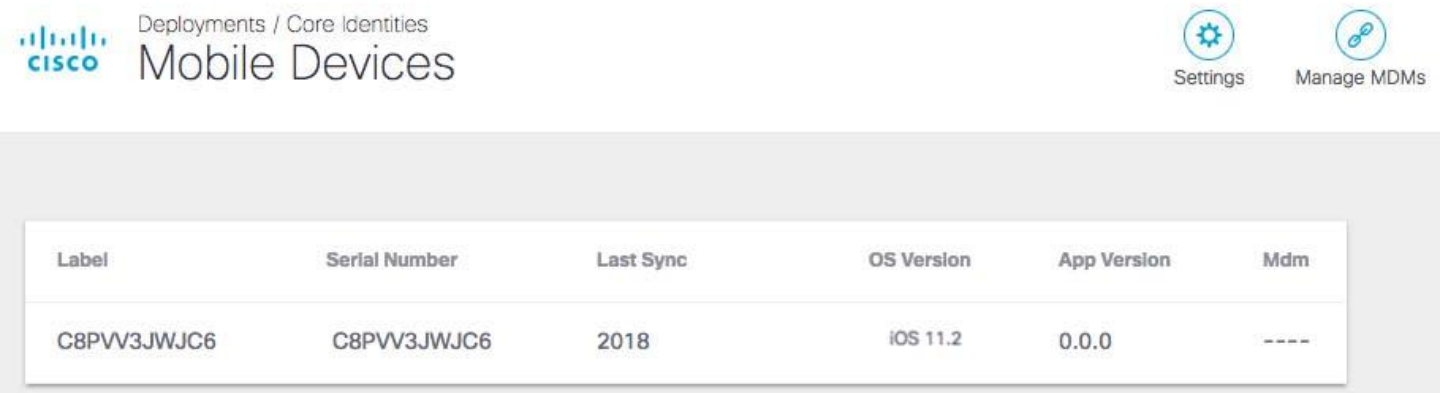




5. Assign it to the students/staff/devices you want and push out those settings in Mosyle.



If you have anonymized your device (see Anonymize Devices), Umbrella hides the device's true label name by replacing it with the device's serial number. Existing active devices anonymize with 24 hours. New devices anonymize immediately.



As no changes can be made in Umbrella to the actual provisioned device, these mobile devices are simply listed in Umbrella as identities; however, you can now use Umbrella to apply policies to these mobile device identities. For more information, see Apply Umbrella Policies.

Android Mobile Security

Umbrella has just recently released feature. If you would like to try it, please see the latest documentation here.

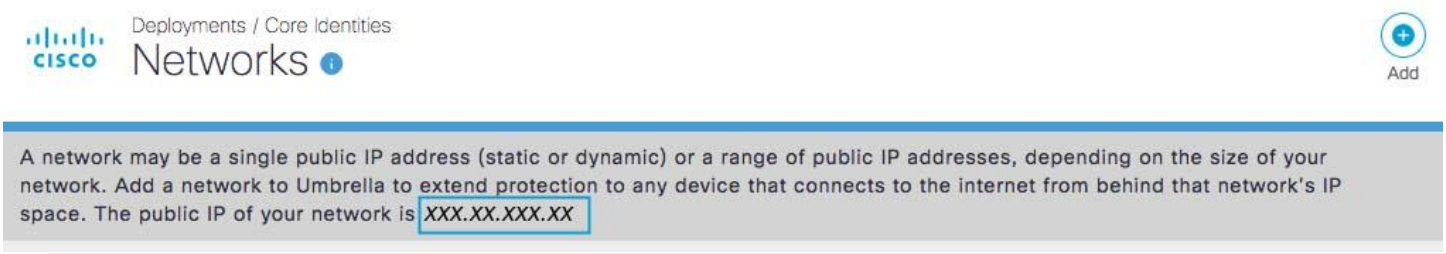
Adding an additional Fixed/Static Network (MiFi/Jetpack)

Step 1 – Obtain a static IP/range from your ISP

First, determine the IP address of your network.

2. In Umbrella, navigate to **Deployments > Core Identities > Networks**.

   You'll find your IP address listed at the top of the page. If you don't see your IP address, click the **i** (**Information**) icon.

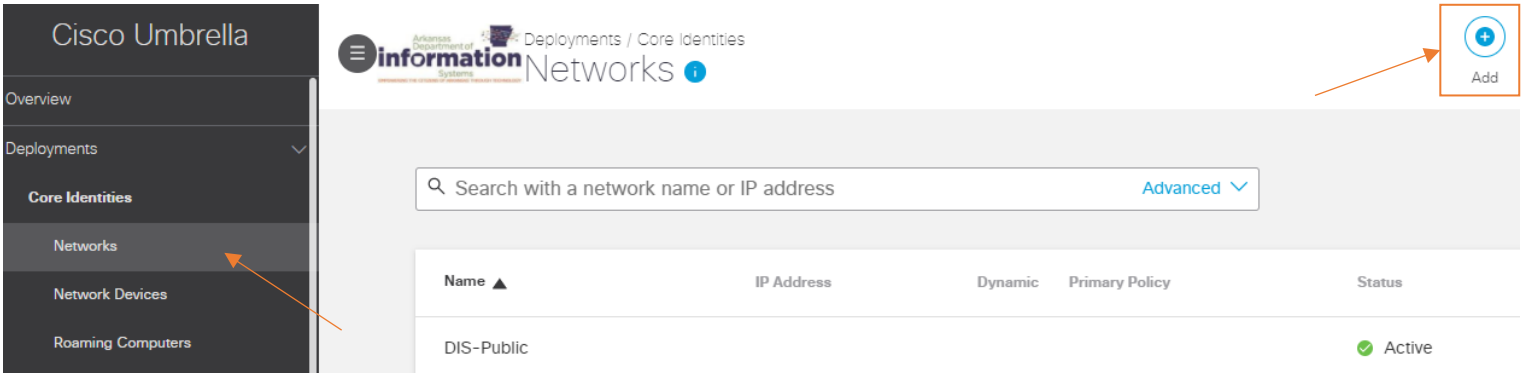


Pre-registering Your Networks

If you plan to have multiple network identities, it's a good idea to immediately register all of your networks with Umbrella. Chances are that if you have more than one public egress IP in your organization, you'll have more than one network identity. Having the networks pre-registered ensures that they're available right away when you do point traffic. It also ensures that all the IP space that belongs to your company is correctly assigned in our systems. Until traffic is pointed to Umbrella's DNS service, no protection is available and there is no reporting so there's no harm in adding all networks beforehand.

Step 2 – Set up the Network Identity

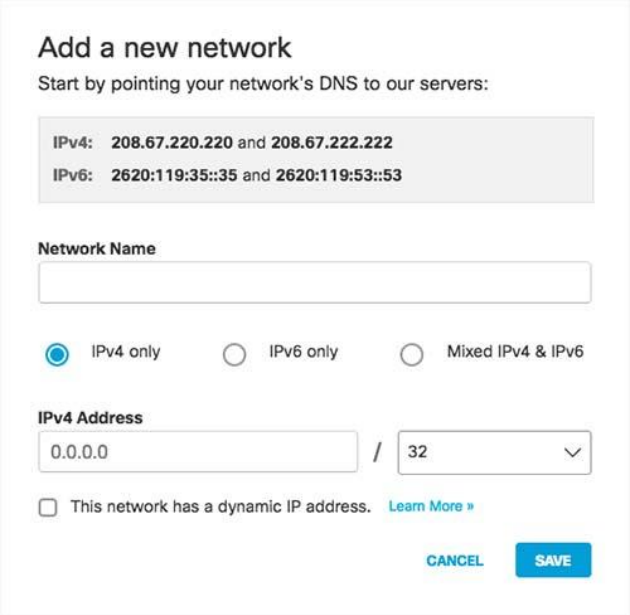
.Navigate to **Deployments > Core Identities > Networks** and click **Add**.



Note: If possible, add the network from the IP being registered; otherwise, an email is generated, which requires that a link is visited from the IP address of the network being registered.

2. In the **Add a New Network** modal, give your network identity a meaningful **Network Name**.

   Giving your identity a good network name will help you find it easily when you later add a policy against it through the Policy wizard.



3. Select an internet protocol—IPv4, IPv6, or both.

   Select a protocol based on the Umbrella IP address to which you have configured your router.

4. Add the network's IP address along with the subnet mask, usually a /32 subnet for IPv4 and /64 subnet for IPv6.

5. Click **Save**.

   Once the service validates your IP address, the network is listed at **Deployments > Core Identities > Networks**. Initially, Umbrella lists your new network identity's status as **Inactive**. Network status only changes to **Active** when DNS traffic is sent to Umbrella from the network.

   The policy applied to your new identity depends on your policy configurations. If you have a policy configured that includes network identities, Umbrella applies that policy; otherwise; Umbrella applies the Default policy.

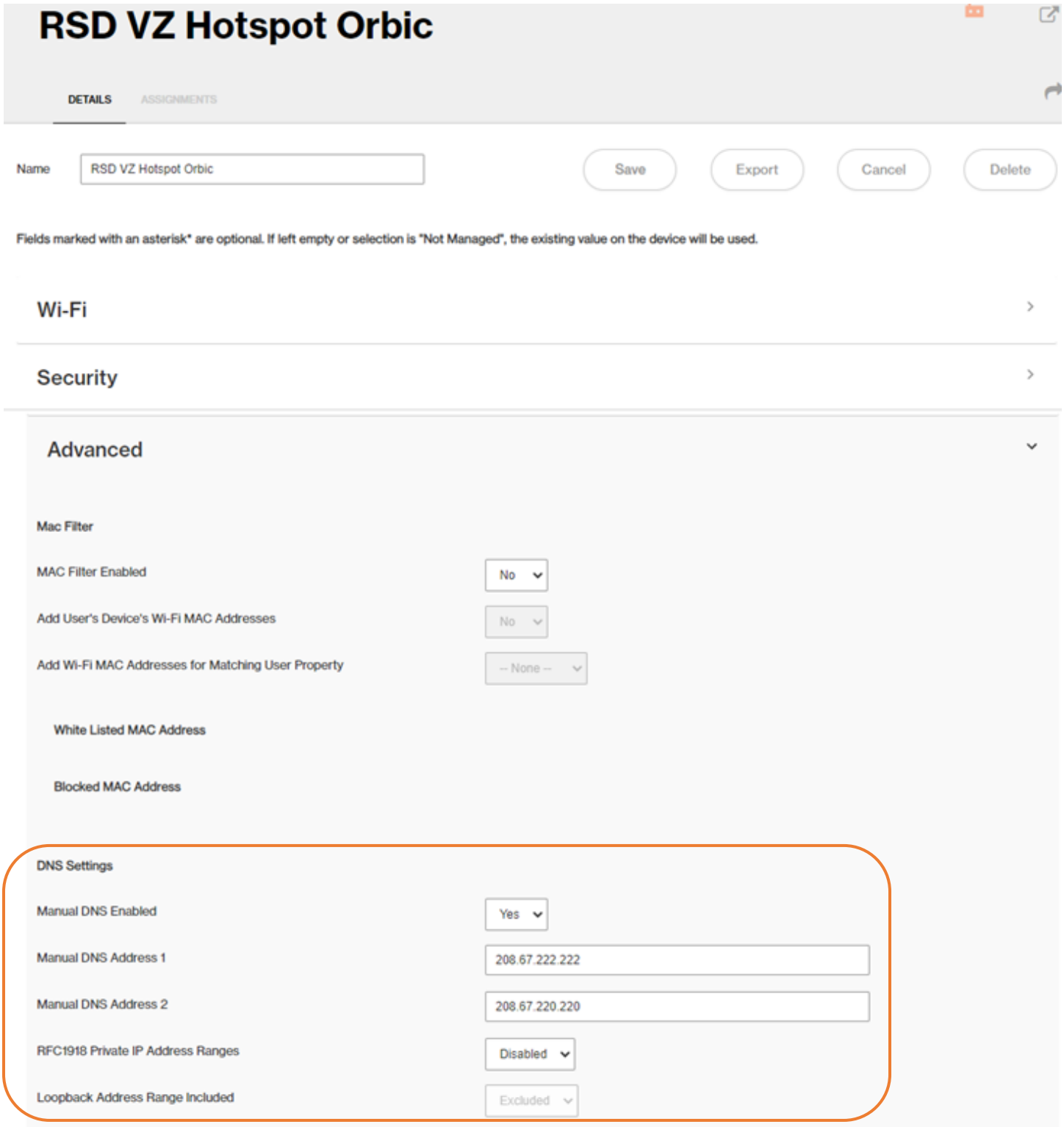
Name	IP Address	Dynamic	Primary Policy	Status
Network Identity One	12.12.12.2		Default Policy	Inactive

Name	IP Address	Dynamic	Primary Policy	Status
Network Identity One	12.12.12.2		Default Policy	Active

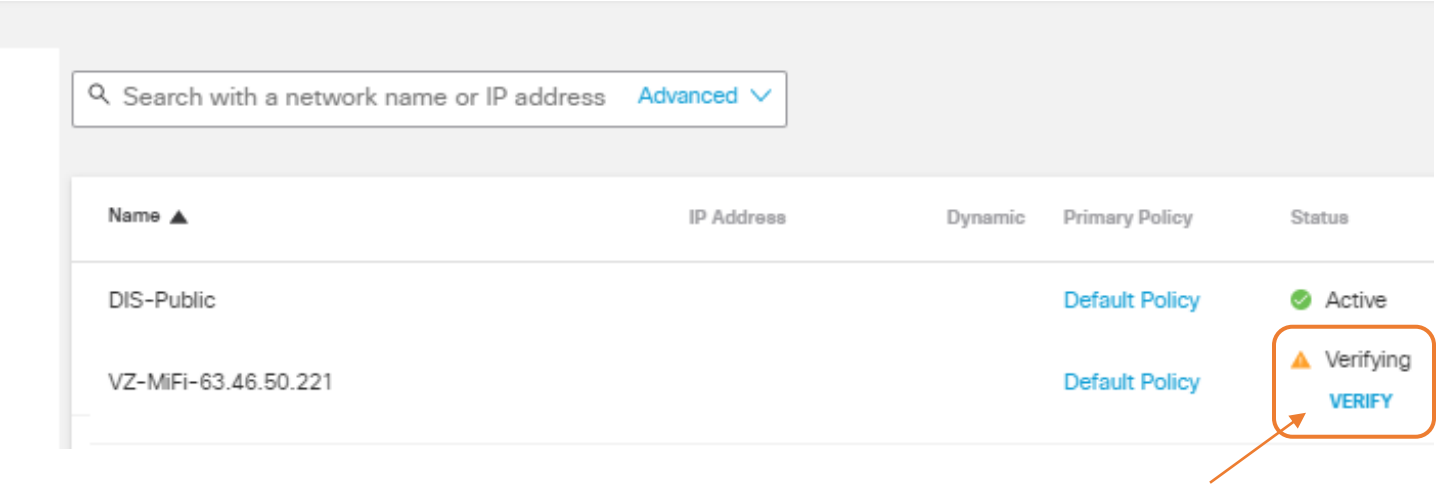
Step 3 – Change the DNS Settings on Your Relevant Network Device

You need only do this on your edge DNS equipment, typically a DNS or DHCP server, or a router—this could be your DSL router or cable modem if that's the only router in your network. **Change DNS to 208.67.222.222 and 208.67.220.220**

Example for Verizon Orbic Hotspot:



Login to Umbrella with the laptop or device that is connected to the MiFi you are setting up and click on Verify from that device:

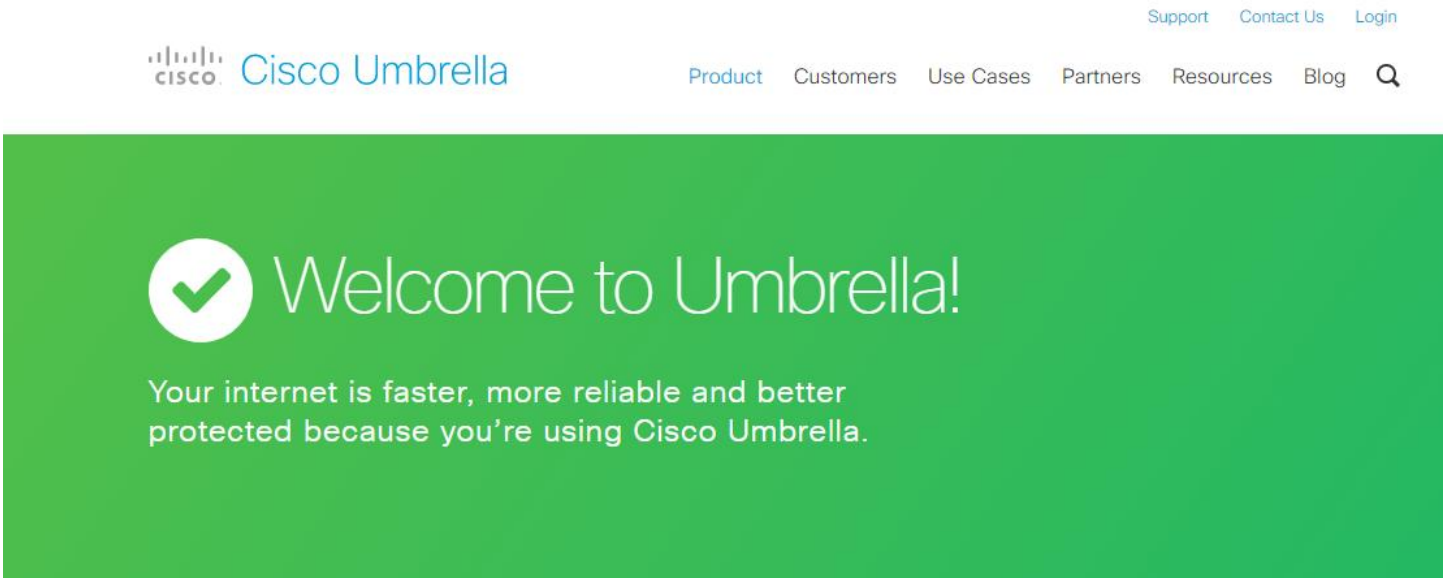


Step 4 – Test Your Network after it's verified and active

Verify that your DNS connections are routed through Cisco Umbrella's global network by navigating to the following page in your client's browser: https://welcome.umbrella.com/. You should see the Welcome to Umbrella page.

Note: You may need to restart your client's network interface or your computer.

To test your security settings, navigate to http://examplemalwaredomain.com/.



Appendix:

Application Category Descriptions

- **Ad Publishing**—Applications that enable publishers and ad networks to manage ad serving and trafficking.
- **Anonymizer**—Services that provide an anonymous proxy tool that attempts to make activity on the Internet untraceable.
- **Application Development and Testing**—Applications suited for application development and testing cycles, or for building integration applications in the cloud and within the enterprise.
- **Backup and Recovery**—Applications for backup and recovery of file systems and raw data stores on servers and desktop systems.
- **Business Intelligence**—Applications for analytics such as dashboards, reporting systems, scenario modeling, and data analysis.
- **Cloud Broker**—Applications that manage the use, performance, and delivery of cloud services and negotiate relationships between cloud providers and cloud consumers.
- **Cloud Carrier**—Intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers through a network, telecommunication, and other access devices.
- **Cloud Service Provider**—Based on NIST definition of a cloud service, which we believe is being (slowly) adopted as the industry standard. The NIST definition includes the following criteria: "on-demand self-service, rapid elasticity, and measured service. CASI additionally adds vendor intent to provide computing-related services (Compute, Network, Storage and/or Software Application). If in doubt whether web or cloud, we will be conservative and assume cloud until we can prove otherwise.
- **Cloud Storage**—Applications that offer massively scalable storage capacity that can be used for applications, and file storage.
- **Collaboration**—Applications that enhance communication and collaboration in workgroups, within enterprises, and across enterprises.
- **Compute**—Fundamental computing resources for running cloud-based systems that can be dynamically provisioned and configured as needed.
- **Content Delivery Network (CDN)**—Applications that store content and files to improve the performance and cost of delivering content for web-based systems by offering a large distributed system of servers deployed in multiple data centers across the Internet.

- **Content Management**—Applications for managing the production of and access to content, enforcing document production workflows, and providing workspaces for groups or enterprises to find and access documents.
- **Customer Relationship Management (CRM)**—Applications that manage interactions with current and future customers, including organization and automation across sales, marketing, and customer service functions.
- **Database Management**—Applications offering scalable data management solutions for structured or unstructured data, relational database solutions or scalable non-SQL datastores.
- **E-Commerce**—Applications that facilitate the buying and selling of products or services.
- **Education**—Applications that provide educational or training courses, general learning opportunities or specific employee training independent of their location.
- **Enterprise Resource Planning (ERP)**—Applications that manage operations or management of a business; which can include internal and external resources, including tangible assets, financial resources, materials, and human resources.
- **Financial Services**—Applications for managing financial processes and information.
- **Games**—Online and mobile games.
- **Healthcare**—Healthcare related apps and services.
- **Hosting Services**—Applications that enable corporate or individual websites or other content to be accessible over the internet.
- **Human Resources**—Applications for managing human resources and HR functions.
- **IT Service Management**—Applications that support specific IT functions to plan, deliver, operate and control IT services.
- **Legal**—Applications that provide access to legal documents and public records and support legal content.
- **Marketing & Sales**—Applications that are specifically designed for marketing and sales functions.
- **Media**—Applications that host or stream media as a service.
- **Office Productivity**—Applications for producing information and other standard office-oriented tasks such as documentation, presentations, project management, etc.
- **Others**—Used for those services where no existing categorization would fit.
- **P2P**—Peer to Peer torrents like apps and protocols.
- **Search**—Web or app-based search.

- **Security**—Applications that support security activities to ensure adherence to regulatory compliance rules and protect information, data applications, and infrastructure.
- **Service Management**—Applications that support general operational activities outside of the IT function.
- **Shopping**—Web or app-based basic online shopping.
- **Social Networking**—Applications that establish and maintain a connection among users that are tied in one or more specific types of interdependency.
- **Software Repository**—Software repositories.
- **Travel**—Travel-related apps and services.
- **Web Content**—Mostly app-based services that provide content. It can be via login and/or paid portal.

Content Category Descriptions

- **Academic Fraud**—Sites that promote educational fraud, including but not limited to plagiarism and cheating.
- **Adult**:
  - **Adult Themes**—Sites that are adult in nature and are not defined in other rating categories.
    Note: Select this category only if you want to be very restrictive on your network.
  - **Sexuality**—Sites that provide information, images or implications of bondage, sadism, masochism, fetish, beating, body piercing or self-mutilation. This category is not intended for LGBT-related sites that do not fall under the aforementioned criteria.
- **Alcohol**—Sites about alcohol use, commercial and otherwise.
- **Arts**—Galleries and exhibitions; artists and art; photography; literature and books; performing arts and theater; musicals; ballet; museums; design; architecture. Does not include movies or television.
- **Astrology**—Astrology; horoscope; fortune-telling; numerology; psychic advice; tarot.
- **Auctions**:
  - **Auctions**—Sites for buying and selling through an auction.
  - **Classifieds**—Sites for buying and selling (or bartering) goods and services. Includes sites with real estate and housing listings.

- **Automotive**—Sites about automobiles, including manufacturers, news, reviews, and hobbyist information.
- **Business Services**—Sites for corporations and businesses of all sizes, especially company websites.
- **Chat**:
  - **Chat**—Sites where you can chat in real-time with groups of people. Includes IRC and video chat sites.
  - **Instant Messaging**—Sites that offer access or software to communicate in real-time with other individuals.
    - **Child Abuse Content (CAC)**—Sites that contain child sexual abuse content. For more information, see the Internet Watch Foundation.
- **Computer Security**—Offering security products and services for corporate and home users.
- **Dating**—Sites for meeting other people.
- **Digital Postcards**—Dating, online personals, matrimonial agencies.
- **Dining and Drinking**—Eating and drinking establishments; restaurants, bars, taverns, and pubs; restaurant guides and reviews.
- **DIY Projects**—Guidance and information to create, improve, modify, decorate and repair something without the aid of experts or professionals.
- **Drugs**—Sites about illegal or recreational drug use.
- **Dynamic and Residential**—IP addresses of broadband links that usually indicate users attempting to access their home network, for example for a remote session to a home computer.
- **Ecommerce/Shopping**—Sites that are online stores for products and services.
- **Educational Institutions**—Sites for schools, covering all age levels and types.
- **Entertainment**:
  - **Anime/Manga/Webcomic**—Sites that host online comics, cartoons, and graphic novels.
- **Fashion**—Clothing and fashion; hair salons; cosmetics; accessories; jewelry; perfume; pictures and text relating to body modification; tattoos and piercing; modeling agencies. Dermatological products are classified as Health and Nutrition.
- **File Storage**—Sites that offer space for hosting, sharing and backup of digital files.
- **File Transfer Services**—File transfer services with the primary purpose of providing download services and hosted file sharing.
- **Financial Institutions**—Sites for banks, brokerages, trusts, and other financial organizations.

- **Freeware and Shareware**—Providing downloads of free and shareware software.
- **Gambling**—Sites that offer gambling or information about gambling.
- **Games**—Sites that offer gameplay and information about games (news, tips, cheat codes).
- **German Youth Protection**—Content deemed harmful to minors. This category helps prevent viewing of youth-endangering content in Germany. Block pages for this category will include German text. This list is not controlled by Umbrella and is created to be controlled by the BPjM (Federal Review Board for Media Harmful to Minors) to be compliant with German Law. For more information, see General Information.
  Note: We do not guarantee compliance with German law.
- **Government**—Sites operated by government agencies, including city, state, regional, county and federal levels. Also includes .mil domains.
- **Hacking**—Discussing ways to bypass the security of websites, software, and computers.
- **Hate/Discrimination**—Sites that promote intolerance based on gender, age, race, nationality, religion, sexual orientation or other group identities.
- **Health and Fitness**—Sites that offer information about health care and health services. Includes fitness related sites and information about health and fitness.
- **Humor**—Sites that are intended to be funny or humorous.
- **Hunting**—Professional or sports hunting, gun clubs, and other hunting-related sites.
- **Illegal Activities**:
  - **Illegal Activities**—Promoting crime, such as stealing, fraud, illegally accessing telephone networks; computer viruses; terrorism, bombs, and anarchy; websites depicting murder and suicide as well as explaining ways to commit them.
  - **Terrorism**—Sites that promote terrorism or are linked with terrorist organizations.
- **Illegal Downloads**—Providing the ability to download software or other materials, serial numbers, key generators, and tools for bypassing software protection in violation of copyright agreements. Torrents are classified as Peer File Transfer.
- **Infrastructure**:
  - **URL Shortener**—An online application or service that converts a regular URL into a condensed format.
  - **Infrastructure**—Content delivery infrastructure and dynamically generated content; websites that cannot be classified more specifically because they are secured or otherwise difficult to classify.

- **Internet Telephony**—Telephonic services using the internet.
- **IT-ADM**—Sites that offer gambling or information about gambling and tobacco. For more information, see the Italian Nacional Agency.
- **IT-AGCOM**—Sites that are deemed to infringe on intellectual property. For more information, see the Italian National Agency.
- **Jobs/Employment**—Sites that offer job listings, resume services, interview coaching, and similar employment-related services.
- **Lingerie/Bikini**—Sites displaying or dedicated to lingerie/bikini that could be considered adult-only.
- **Lotteries**—Sweepstakes, contests, and state-sponsored lotteries.
- **Military**—Military, such as the armed forces, military bases, military organizations, anti-terrorism.
- **Mobile Phones**—Short Message Services (SMS); ringtones and mobile phone downloads. Cellular carrier websites are included in the Business and Industry category.
- **Nature**—Natural resources; ecology and conservation; forests; wilderness; plants; flowers; forest conservation; forest, wilderness, and forestry practices; forest management (reforestation, forest protection, conservation, harvesting, forest health, thinning, and prescribed burning); agricultural practices (agriculture, gardening, horticulture, landscaping, planting, weed control, irrigation, pruning, and harvesting); pollution issues (air quality, hazardous waste, pollution prevention, recycling, waste management, water quality, and the environmental cleanup industry); animals, pets, livestock, and zoology; biology; botany.
- **News/Media**—Sites that offer news and information, including newspapers, broadcasters, and other publishers.
- **Non-Profits**—Sites for non-profit or charity organizations and services.
- **Nudity**—Sites that provide images or representations of nudity.
- **Online Communities**:
  - **Blogs**—Personal Sites or group journals, diaries or publications.
  - **Forums/Message Boards**—Sites with discussions, including bulletin boards, message boards, and forums.
- **Online Meetings**—Online meetings, desktop sharing, remote access, and other tools that facilitate multi-location collaboration.
- **Online Trading**—Online brokerages; websites that enable the user to trade stocks online; information relating to the stock market, stocks, bonds, mutual funds, brokers, stock analysis and commentary, stock screens, stock charts, IPOs, stock

splits. Services for spread betting on stocks and shares are classified as Gambling. Other financial services are classified as Finance.

- **Organizational Email**—Websites used to access business email (often through Outlook Web Access).
- **P2P/File Sharing**—Sites that facilitate the sharing of digital files between individuals, especially through peer-to-peer software, including torrent sites.
- **Paranormal**—UFOs, ghosts, cryptid, telekinesis, urban legends, and myths.
- **Parked Domains**—Sites that are placeholders "parked" for future use. Current uses may include single-page advertising sites.
- **Personal Sites**—Websites about and from private individuals; personal homepage servers; websites with personal contents; personal blogs with no particular theme.
- **Personal VPN**—Virtual private network (VPN) sites or tools that are typically for personal use and may or may not be approved for corporate usage.
- **Photo Search and Images**:
  - **Visual Search Engines**—Sites for searching for images based on keywords.
  - **Photo Sharing**—Sites for sharing photographs, as individual images, galleries, and albums.
- **Politics**—Sites about politics, politicians, political parties and organizations. Government sites are separate.
- **Pornography**—Anything relating to pornography, including mild depiction, soft pornography or hard-core pornography.
- **Professional Networking**—Social networking for career or professional development. See also Social Networking.
- **Proxy/Anonymizer**—Sites providing proxy bypass information or services. Also, sites that allow the user to surf the net anonymously, including sites that allow the user to send anonymous emails.
- **Real Estate**—Information that would support the search for real estate; office and commercial space; real estate listings, such as rentals, apartments, and homes; house building.
- **Religious**—Sites about religion, religious teachings and groups, and spirituality.
- **Research/Reference**—Sites such as encyclopedias, dictionaries as well as other research-related resources.
- **SaaS and B2B**—Web portals for online business services; online meetings.
- **Safe for Kids**—Directed at, and specifically for, young children.

- **Science and Technology**—Science and technology, such as aerospace, electronics, engineering, mathematics, and other similar subjects; space exploration; meteorology; geography; environment; energy (fossil, nuclear, renewable); communications (telephones, telecommunications).
- **Search Engines and Portals**:
  - **Search Engines**—Sites that offer result listings based on keywords.
  - **Portals**—Sites that offer gateways to the Internet as a whole, often including bundled services on their site.
- **Sex Education**—Factual websites dealing with sex; sexual health; contraception; pregnancy.
- **Social Networking**—Sites that promote interaction and networking between people.
- **Social Science**—Sciences and history related to society; archaeology; anthropology; cultural studies; history; linguistics; geography; philosophy; psychology; women's studies.
- **Society and Culture**—Family and relationships; ethnicity; social organizations; genealogy; seniors; child-care.
- **Software/Technology**—Sites about computing, hardware, and technology, including news, information, code and vendor information.
- **Software Updates**—Websites that host updates for software packages.
- **Sports**—Sites about sports of all kinds, from professional to amateur, from news to league information and schedules. Includes martial arts and MMA related sites.
- **Streaming Audio**:
  - **Music**—Sites about music, including news, band and fan information.
  - **Radio**—Sites that offer online radio listening or promote radio stations.
  - **Podcasts**—Sites that offer podcasts, digital media files distributed over the Internet, often using syndication feeds, for playback on portable media players and personal computers. Both audio and video podcasts are included.
- **Streaming Video**:
  - **Movies**—Sites that promote movies or offer movie watching online.
  - **Video Sharing**—Sites for sharing video content.

- **Tasteless**—Sites that contain information on such subjects as mutilation, torture, horror, or the grotesque. Includes pro-anorexia and pro-suicide related sites.

- **Television**—Sites that promote television shows or offer television watching online.
- **Tobacco**—Sites about tobacco use and related products, commercial and otherwise.
- **Travel**—Sites with travel information and services, including reservations for airlines, cars, hotels, vacations, and trips.
- **Weapons**—Sites about weapons, commercial and otherwise.
- **Web Hosting**—Website hosting; bandwidth services.
- **Web Page Translation**—Translation of web pages between languages.
- **Webmail**—Sites that offer the ability to send or receive email.

Troubleshooting

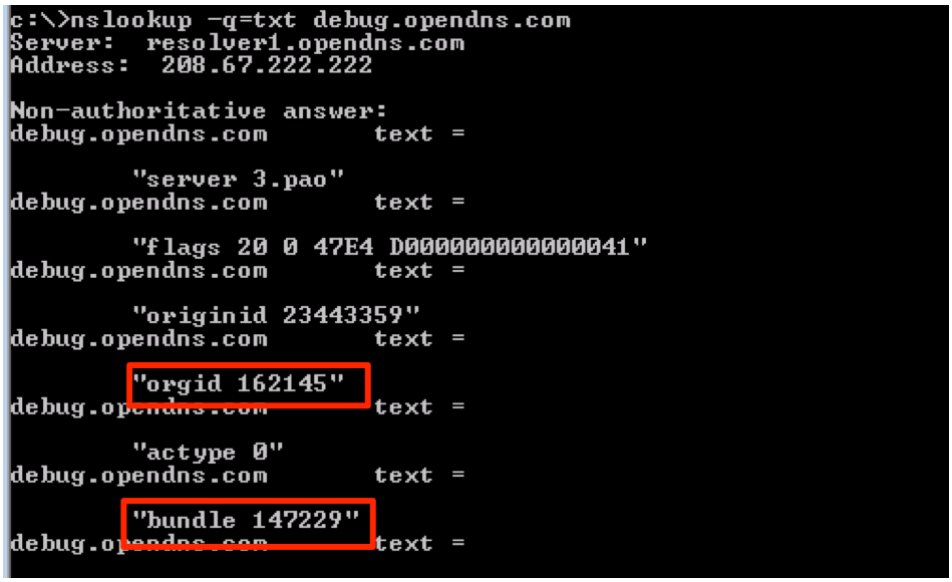
What Policy is being applied?

Windows or Mac

The first step is to collect the debug output from the client machine that you wish to determine the applied policy for. Debug output can be gathered by running the following commands from a command prompt on Windows, or a Terminal window on OS X:

nslookup -q=txt debug.opendns.com

The output should look similar to this:



For our purpose, the important information here is the OrgID and the Bundle. The OrgID is the identifier of your organization's dashboard, and the Bundle is the identifier of the applied policy within that organization.

Next, log in to your Umbrella dashboard and open a new tab or window in the browser. Then, plug the two variables pulled from the debug output into the URL below:

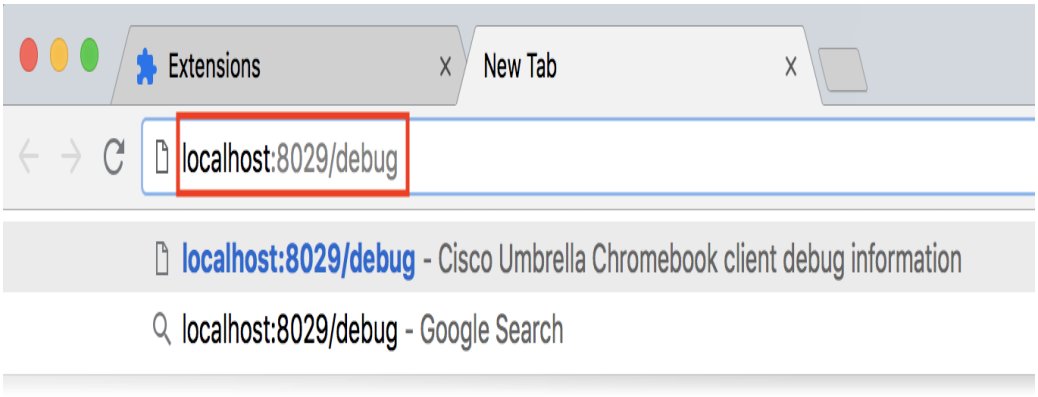
https://dashboard.umbrella.com/o/<OrgID>/#/configuration/policy/<Bundle-ID>

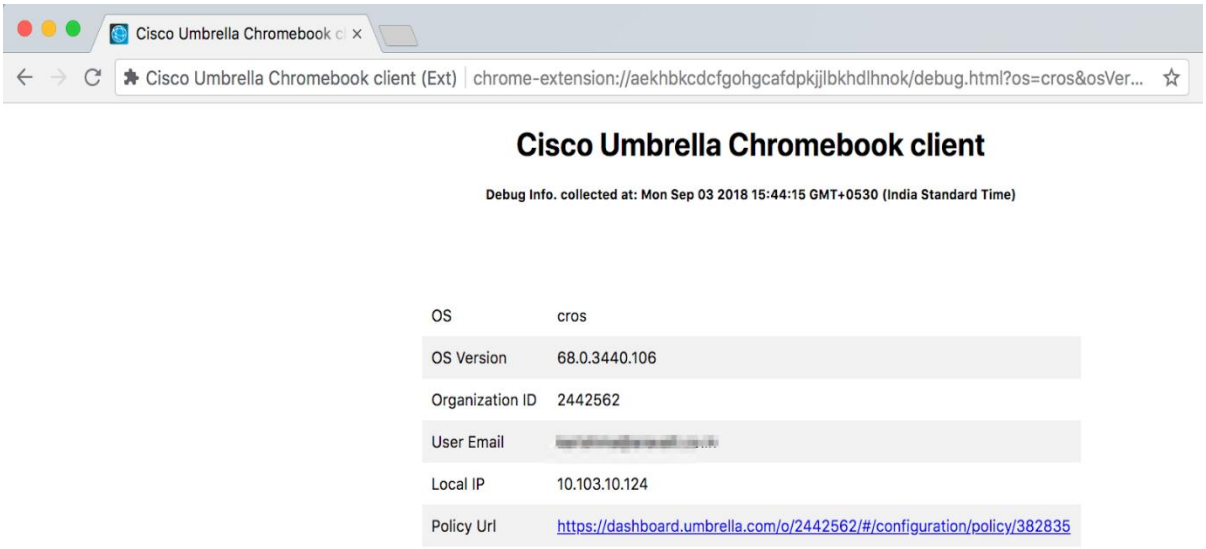
This will take you directly to the policy that was applied to the computer (or user) the debug output was run on, at the time it was run.

Chromebook

Access the diagnostic page by browsing to **http://localhost:8029/debug** in a new tab.

The output should look similar to this:



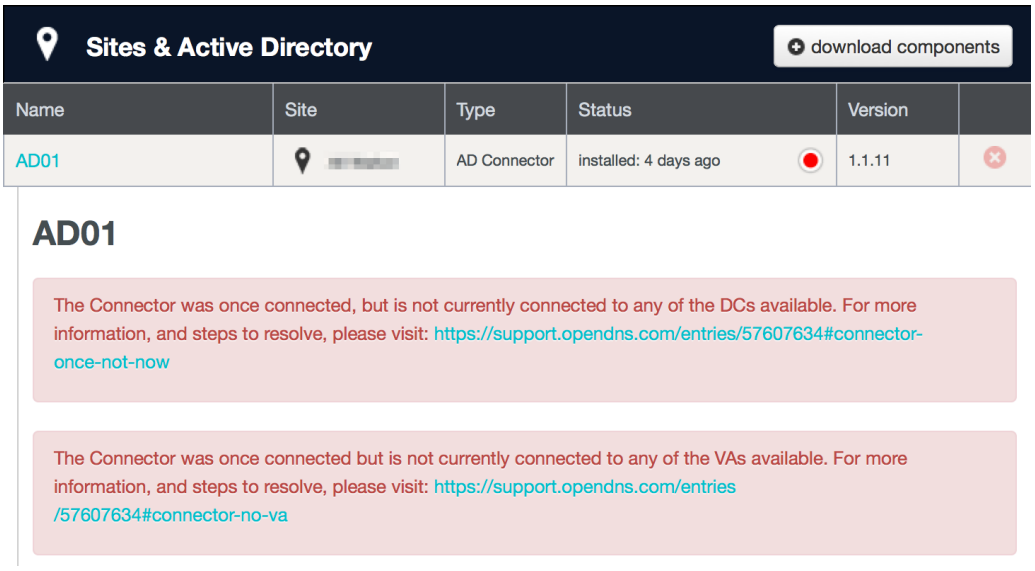


For our purpose, the important information here is the "OrganizationID" and the "Policy Url". The "OrganizationID" is the identifier of your organization's dashboard, and the "Policy Url" is the identifier of the applied policy within that organization.

Next, log in to your Umbrella dashboard and open a new tab or window in the browser. Then, navigate to the "Policy Url" which will take you directly to the policy that was applied to the computer (or user) the debug output was run on, at the time it was run.

Gathering or clearing AD Connector Logs

A functional AD Connector is green. Grey, yellow, and red statuses usually reflect a problem.



For each AD Connector which cannot connect to a Domain Controller, or has an error/warning in the Dashboard, you should provide the AD Connector Log so Umbrella support can examine the findings.

Logs

To obtain the logs manually, follow the steps below:

- Attach the file C:\Program Files (x86)\OpenDNS\OpenDNS Connector\v1.x.x\OpenDNSAuditClient.log
- Attach the latest couple .zip log files from C:\Program Files (x86)\OpenDNS\OpenDNS Connector\v1.x.x\ to the support ticket (do not send more than 3 .zip files)
  - If the files are over 20MB, split them into two responses or contact us for upload details.

If working with a fresh configuration which has never worked, or if asked to send **new logs**:

- Stop the OpenDNS AD Connector service,
- Delete the file "C:\Program Files (x86)\OpenDNS\OpenDNS Connector\v1.x.x\OpenDNSAuditClient.log".
- Start the service up again.
- Wait 5 minutes and reply with this file.

This allows the file to be fresh and only with the most recent startup attempt.

CIDR Table

CIDR	SUBNET
0	0.0.0.0
1	128.0.0.0
2	192.0.0.0
3	224.0.0.0
4	240.0.0.0
5	248.0.0.0
6	252.0.0.0
7	254.0.0.0
8	255.0.0.0
9	255.128.0.0
10	255.192.0.0
11	255.224.0.0
12	255.240.0.0
13	255.248.0.0
14	255.252.0.0
15	255.254.0.0
16	255.255.0.0
17	255.255.128.0
18	255.255.192.0
19	255.255.224.0
20	255.255.240.0
21	255.255.248.0
22	255.255.252.0
23	255.255.254.0
24	255.255.255.0
25	255.255.255.128
26	255.255.255.192
27	255.255.255.224
28	255.255.255.240
29	255.255.255.248
30	255.255.255.252
31	255.255.255.254
32	255.255.255.255