

Cisco Umbrella



Prepared by DIS APSCN/LAN Support

Contents

Umbrella Documentation	5
Basic Level Filtering	5
OpenDNS Forwarders	5
Local IP Level Filtering	
Virtual Appliance Requirements	9
VA Networking Requirements	9
Download Virtual Appliance:	
Hyper-V Virtual Appliance Deployment	12
VMWare Virtual Appliance Deployment	15
Configure the Virtual Appliances	17
Repeat Steps for the second VA	20
Warning	20
Local IP and Active Directory Filtering	
Prerequisites	21
Create AD User:	21
DCOM Permissions	22
WMI Permissions	24
Active Directory Integration	25
Configure DNS	25
Configure Active Directory	27
Connect Active Directory	
Setup DHCP	28
Final Configuration	
Configure Internal Network	
Domain Management	32
Configure Policies	33
Destination Lists	
Category Settings	34
Migrating Legacy Content Categories	
Application Settings	
Block Page Bypass	40
Security Settings	40
Policies	41

Policy Advanced Settings	47
Deploying Umbrella Certificate	
Why Deploy Certificate?	49
Download Certificate	50
Deploy Certificate with GPO	51
Deploy Certificate to Chrome Devices with Google Admin	54
Verify the CA on managed Chrome devices	54
ByPass User	55
Setting up your Block Page Bypass	55
Setting up a Block Page Bypass User	56
Creating a Block Page Bypass Code	58
Removing a Bypass Code	58
Interacting with a Block Page As a User	59
Chromebook Client	
Installation Guide	63
Prerequisites	63
Networking Requirements	63
Recommendations	64
Implementing Trusted Network Detection	64
Part 1: Obtain the configuration file from Umbrella	64
JSON File Example (Without VA):	65
JSON File Example (With VA):	65
Part 2: Install the Cisco Umbrella Chromebook client extension	67
Part 3: Install the Cisco Umbrella Chromebook client Application	70
Installation Caveats	75
Apply Policies	75
Overview	75
Create a Chromebook-specific policy	76
Arrange policies in order	79
Trusted Network Detection	79
How trusted network detection works	79
Software requirements	
Deploy the G Suite Identity Service	
Enabling the G Suite Identity Service	

Install the Cisco Umbrella Authorizer App	81
Enter your G Suite super administrator ID in the Umbrella Dashboard	82
Removing Cisco Chromebook client software	85
Roaming Client Setup	
iOS Mobile Security- iPads in Umbrella	
Requirements	
1. Install the Cisco Security Connector App	
2. Add an Organization Administrator's Email Address	90
3. Register Your iOS Device Through Your MDM to Umbrella	90
Jamf	
Prerequisites	93
Register Your iOS Device	94
Mosyle	
Android Mobile Security	100
Adding an additional Fixed/Static Network	100
(MiFi/Jetpack)	100
Step 1 – Obtain a static IP/range from your ISP	
Pre-registering Your Networks	
Step 2 – Set up the Network Identity	
Step 3 – Change the DNS Settings on Your Relevant Network Device	
Step 4 – Test Your Network after it's verified and active	
Appendex:	106
Application Category Descriptions	
Content Category Descriptions	
What Policy is being applied?	
Windows or Mac	
Chromebook	
Gathering or clearing AD Connector Logs	
Logs	
CIDR Table	

Umbrella Documentation

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

	2012DC1	Prop	erties	?
Debug Logging	ent Loggi	ng	Monitoring	Security
Interfaces	Forwarders	A	dvanced	Root Hints

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

	Event Logging	Monitoring	Security
Interfaces	Forwarders	Advanced	Root Hints
orwarders are DN ueries for records	S servers that this ser that this server canno	ver can use to reso t resolve.	lve DNS
IP Address	S	erver FQDN	
170.94.156.195	re	solver1.state.ar.us	
170.94.156.195 resolver1.state.ar			
170.94.156.196	re	solver2.state.ar.us	
1 / U.94. 156. 196	re no forwarders are ava	solver2.state.ar.us	Edit
] Use root hints if	re no forwarders are ava	solver2.state.ar.us illable	Edit

 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

Edit Forwarders

IP addresses of forwarding servers:

	·		
IP Address	Server FQDN	Validated	Delete
<click a<="" add="" an="" here="" ip="" th="" to=""><th>Address or DNS Name></th><th></th><th></th></click>	Address or DNS Name>		
208.67.222.222	resolver1.opendns.com	OK	Up
0 208.67.220.220	resolver2.opendns.com	OK	
0 208.67.222.220	resolver3.opendns.com	OK	D <u>o</u> wn
208.67.220.222	resolver4.opendns.com	OK	
Number of seconds before	forward queries time out:	3	
The server FQDN will not be configured.	e available if the appropriate r	everse lookup zones and entr	ies are not
		ОК	Cancel

- 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. 1024 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 +	Virtual Appliance	Local DNS servers	Standard DNS traffic for internal domains.
UDP			

53 TCP +	Virtual Appliance	Umbrella resolvers	Standard and encrypted DNS queries to Umbrella resolvers.
UDP	II	Default:	Port 443 is used as failover if your firewall does not allow
443 TCP +		• 208.67.220.220/32	DNSCrypt on port 53
		• 208.67.222.222/32	Part E2E2 is used as failover if DNSCrupt is not allowed on part E2
		If you have configured the VA to	and part 442
5353 ICP +		use other Umbrella resolvers:	and port 443.
UDP		Alternate:	
		 208.67.220.222/32 208.67.222.220/32 	
		IPv6:	
		2620:119:35::352620:119:53::53	
		US-only:	
		208.67.221.76/32208.67.223.76/32	
		US-only IPv6:	
		• 2620:119:17::76	
		• 2620:119:76::76	
142 TOD	X 7. 1 A 1.	• api.opendns.com	
443 ICP	Virtual Appliance	• (67.215.92.210	HTTPS—Used for registration, health checks, and updates from
		• 146.112.255.152/29)	Umbrella.
		crl4.digicert.com	ocsp.digicert.com and crl4.digicert.com use a CDN and are not
		• cisco.com	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
		the second second	
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	Source	Destination	Note
Protocol			
22	Virtual Appliance	s.tunnels.ironport.com	Required for the customer-initiated SSH support tunnel. For
25 53 80 443			more information, see <u>On-Demand Tech Support SSH Tunnel for</u>
or 4766 TCP			<u>Virtual Appliances</u> .
123 UDP	Virtual Appliance	NTP servers	NTP—Protocol to synchronize time.
		Default:	
		 ntp.ubuntu.com (91 189 94 4/32) 	
		• 91.189.89.199/32	
		• 91.189.91.157/32	

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

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**"

Cisco Umbrella	e information Site	yments / Configuration es and Active Directory o				Settings Add DC Download
Deployments V Core Identities	Sites and Active Directory roaming clients by providi	/ provides you with the means to integrate and d ing AD user, group, or computer name informatio	eploy virtual appliances and Active D on for each applicable DNS request	irectory (AD). Active Directory (/	AD) integration supplements Umbrella vi	irtual appliances (VAs) and
Networks Network Devices	FILTERS			Q Search Sites and Active Direc	tory	
Roaming Computers Mobile Devices	Name 💌	Internal IP	Site	Туре	Status	Version
Chromebook Users Configuration	OpenDNS-VM1 OpenDNS-VM2	10.1.1.1	Default Site	Virtual Appliance	 Imported: 2 years ago Imported: 2 years ago 	2.8.3
Sites and Active Directory	DC-1 DC-2	10.1.1.3 10.1.1.4	Default Site Default Site	Domain Controller	 Run: 2 years ago Run: 2 years ago 	
Root Certificate	DC-2	10.1.1.4	Default Site	AD Connector	Installed: 2 years ago	1.6.24
internal Networks Root Certificate Service Account Exceptions	DC-2	10.1.1.4	Default Site	AD Connector	Installed: 2 years ago Page: 1 Results Per Page: 10	1.6.24 ✓ 1-5 of 5 🔇

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

vments / Configuration	Download Components		
es and Acti	Interested in learning more about our availab	ble downloads? Visit Umbrella Do	cs.
y provides you with th	Active Directory Components		ctive Directory (AD
ing AD user, group, c	Windows Configuration script for Domain Contr	oller DOWNLO	AD
	Windows Service (Active Directory Connector)	DOWNLO	AD
	Virtual Appliance Components Use as the default password VA for VAMAre ESVi	for this VA.	Appliance
	VA for VIVIVVare ESA	DOWNLO	AD Applance
	VA for Hyper-V	DOWNLO	Appliance
			n Controller
		CANCEL	n Controller
	10.56.42.1	Delaun Site	AD Connector

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.

- 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

New Virtual Machine Wiz Specify Nan	ard ne and Location	×
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Writual Herd Disk Installation Options Summery	Choose a name and location for this virtual machine. The name is displayed in Hyper-V Manager. We recommend that you use a name that h identify this virtual machine, such as the name of the guest operating system in worklo Name: SCHOOL-VA1 You can create a folder or use an existing folder to store the virtual machine. If you do folder, the virtual machine is stored in the default folder configured for this server. Store the virtual machine in a different location Location: CVMV	ebs you easily ad. Init select a Browse
	If you plan to take checkpoints of this votual machine, select a location that has espace. Checkpoints include votual machine data and may require a large amount o	Sough free Fapace

- 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)

📙 🛃 📒 = SCHOOL-VA1	C	2	₩ Í	- 🗆 🗙
File Home Share	View			~ 🕜
Pin to Quick Copy Paste	Move to • X Delete • Copy to • • Rename Organize	New folder	Properties	Select all Select none Invert selection
← → ~ ↑ □ « HV >	SCHOOL-VA1	v Ö	Search SCHOO	L-VA1 Q
Pictures X A	lame		Date modified	Туре
 Pictures Virtual Hard Disk Virtual Hard Disk OneDrive This PC Desktop Documents 	Virtual Machines		12/7/2016 1:52 PM	File folder
2 items 1 item selected St	ate: 🎎 Shared			

- 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

SCHOOL-VA1	~ 4 Þ Q						
Add Hardware Add Hardware Bool From CD Bool From CD Memory S12 MB Processor 1 Virtual processor Ull IDE Consume 0	The Controller You can add hard drives and CD/DVD Select the type of drive you want to Hard Drive DVD Drive) drives to your IDE controller. attach to the controller and the	n dick Add.	4 Þ IG			
Bill DE Controler 1 Bonn Bonn Bonn Soss Controler Methods Adapter LAV Internal 10. CON 1 Bonn CON 2 Sonn Dokette Drive Bonn Bo	You can configure a hard drive to us you attach the drive to the controlle	e a virtual hard disk or a physicz	Add I hard disk after	Hard Drive You can change how this v operating system is installe virtual machine from startin Controller: IDE Controller 0 Media You can compact, conve by editing the associate Virtual hard disk:	irtual hard disk is d on this disk, ch ig. vrt, expand, mer d file. Specify the	attached to the virtual anging the attachment Location: 0 (in use) ge, reconnect or shrink full path to the file.	machine. If an might prevent the a virtual hard disk
Anne Scholoz.vA1 Scholoz.vA1 Scholoz.vA1 Son exclos offered Ordspoints Production Maret Raging File Location CLYVPORDO-VA1 Production Restrict (ForeNaday numming Automatic Star Action Restrict (ForeNaday numming Automatic Stap Action				Physical hard disk: If the physical disk is offine. I physical hard disk is office. I	lew hard disk you wa Jse Disk Manager isks. disk, dick Remov	Inspect of to use is not listed, r ment on the physical co	Browse make sure that the mputer to manage disk but does not

- 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



 select the 'File' tab.
 Click Deploy OVF Template, choosing the .OVA template downloaded from the Umbrella

1. Log into your VMware vSphere client and

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

dashboard.

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

Deploy OVF Template	
Name and Location Specify a name and loca	ation for the deployed template
Source OVF Template Details	Name: Your Network'd OpenDNS Virtual Appliance
Name and Location Storage Disk Format	The name can contain up to 80 characters and it must be unique within the inventory folder.
Advantation of the second second	

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

Deploy OVF Template			
Disk Format In which format do you	want to store the virtual disks?		
Source OVF Template Details Name and Locator Storal Disk Format	Datastore: Available space (G8):	m16-6cs 2235.6	
Network Mapping Ready to Complete	C Thick Provision Lazy 2	leroed	
	Thin Provision	Zeroed	

Thin Provision.

5. Next, select or map a network:

OVF Template Details Name and Location	Map the networks used in this OVF ten	plate to networks in your inventory	
Host / Cluster	Source Networks	DestinationNetworks	
Resource Pool	Network	VM Network	
Storage Disk Format		VM Network vlan-static4-10, 122,4	<u>^</u>
Network Mapping		matt-ylan-190	

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)

	System		
	r Forwarder Sta	atus ———	
	Norra		0-rules-
	Name:		Services
	MAC:	00:15:5d:58:0a:00	forwarder [1158] sync [disabled]
I	IP:	0.0.0.0	
I	Netmask:	255.255.255.0	
I	Gateway:		Connectivitu
I			
I			This DNS Server: DNS ok Local DNS Servers: Unconfigured
I			Umbrella DNS Servers: Tests incomple\$
I			Remote Support Tunnel: Disabled
I			Updates: Connect failed
		0 domains	
	Version:	2.4.4	

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

	Configuration
s	Are you sure you want to enable the Config Mode? Default password for this VA is Umbrella‹Org ID>. The Org ID can be retrieved from your Umbrella dashboard after you sign in. For instance, if your Org ID is 2306646, the default password will be Umbrella2306646
	YES NO

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

Org ID is 2385312 ← → C Attps://dashboard.umbrella.com/o/2385312/#/deployments/configuration/adconfiguration 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.

You are required to change your password immediately (root enforced) Changing password for vmadmin. (current) UNIX password: New password: _

9. Retype the new password

You are required to change your password immediately (root enforced) Changing password for vmadmin. (current) UNIX password: New password: Retype new password: _

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

```
You have entered the Configuration Mode on this VA. Use the 'config' command for any configuration changes.
Type 'help' to get a list of supported commands.
```

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

You have entered the Configuration Mode on this VA. Use the 'config' command for any configuration changes. Type 'help' to get a list of supported commands. ~ \$ config va name School–VA1_ 12. After you press enter you will see it sets the name.



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.



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.

```
Forwarder Status
       Name: School-VA1
                                           Services
        MAC: 00:15:5d:58:0a:00
                                            forwarder [1158]
         IP: 192.168.88.11
    Netmask: 255.255.255.0
    Gateway: 192.168.88.2
                                           Connectivity
                                           This DNS Server: DNS ok
                                           Local DNS Servers: All DNS ok
Umbrella DNS Servers: All DNS ok
                                           AD Connector: Unknown
Local DNS 1: 192.168.88.10
                                           Remote Support Tunnel: Disabled
Local DNS 2: 192.168.88.11
                                           Umbrella Cloud: SSL ok
                                           Updates: SSL GET ok
              19 domains
              2.4.4
  Version:
```

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 <u>should not</u> 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.

	Ne	w Object - User	×		New Object - User	
8 Dea	te in: echodilo	cel/Users		🔏 Constein sc	hool local/Users	
First name	Open	Initializ:		Password		
Last name:	DNS			Confirm password:		
Full name:	Open DN	\$		User must change pass	word at next logon	
User lagon name				User cannot change p	browerd	
OpenDNS_Can	vedor	eschool local		Password never expres		
User lagon name	e (pre-Windows 2	(000)		Account is deabled		
SCHOOL\		OpenDNS_Connector				
	8.1-	cfinik Net 2	Cancel		< Back Next >	Cancel
ce the use	er is creat	ed, add the user to the	e following	Escute costs	Banda Dadon Satura Bolla	004-
ups by ri	ght click	ing the user > Prope	erties >	General Add	ress Account Profile Telephones	Organizatio
mber Of	f tab > Ad	ld		Member Of	Dial-en Environment	Seasone
a Ev	ent Log H	Readers		Member of	Active Directory Donate Services Fold	Ser 1
h Die	tributed	COMUSars		End interview (CDV)	H in Franzikovski Tituðar	
c En	torprice	Com Users	Controllors	Enterprise Rea	dachoollocal/Usen	
C. LI	ter prise i	Ceau-only Domain C	Jointi oners	Event Log Rec	sders school tocal /Builtin	

Renove

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**

Jsers, Groups, or Built-in security principals	Object Types
om this location	
istrict local	Locations
nter the object names to select (<u>examples)</u> :	- 1997
OpenDNS_Connector	Check Names

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.

 Click OK > OK > Close the WmiMgmt window.

Authenticated Use	rs		
LOCAL SERVICE			
Server K SERV	/ICE		
Open DNS (Open)	DNS_Connecto	pr@district.loca	
Administrators (DIS	STRICT\Admin	istrators)	
		Add	Remove
	NC	A11-	D
Partial Write	NS	Allow	Deny
Provider Write			ĒĔ
Enable Account		✓	
Remote Enable			
Read Security		~	
Edit Security			
or special permissions	or advanced s	ettings,	Advanced
			100,000,0000

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.

DNS	Name 📩	Туре	Data
 WINSERV-2012R2 ✓ Forward Lookup Zones ▷school.local ▷school.local ▷Reverse Lookup Zones ▷Trust Points ▷Conditional Forwarders ▷Global Logs 	 (same as parent folder) (same as parent folder) (same as parent folder) (same as parent folder) _msdcs _sites _tcp _udp DomainDnsZones _srestDnzZones 	Start of Authority (SOA) Name Server (NS) Host (A)	[217], winserv-20 winserv-2012r2.s 10.10.0.2
New Ho	st	Host (A)	10.10.0.4
(1778-1771) 		Host (A)	10.10.0.5
Name (uses parent domain name if bla	ank):	Host (A)	10.10.3.0
SCHOOL-VA-1		Host (A)	10.10.0.2
Fully gualified domain name (FODN):		Host (A)	10.10.0.3
SCHOOL-VA-1.school.local.			
TD address			
10 10 0 10			
Create associated pointer (PTR) re Allow any authenticated user to up same owner name	accord podate DNS records with the Add Host Cancel		

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 <u>ADMIN</u> 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.
- 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**



- 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.

Available Options		Description /
004 Time Server		Array of time
005 Name Server	rs	Array of nam
☑ 006 DNS Servers	3	Array of DN
007 Log Servers	2019	Array of MIT \
Data entry Server name:		Resolve
Data entry Server name: P address:	. Add	Resolve
Data entry Server name: IP address:	. Add Remove	Resolve
Data entry Server name: IP address: 10.10.0.10	- Add Remove	Resolve

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**.

Cisco Umbrella	Deployments / Configura	ation			(
Overview		WUINS			
Deployments 🔨 🗸					
Core Identities	Search Internal Networks				
Networks		q			
Network Devices	Name	Site	IP	Primary Policy	
Roaming Computers	Camera Network	Oefault Site	10.112.108.0/24	Default Policy	8
Mobile Devices	High School Campus	Default Site	10.112.160.0/20	Default District Poli	8
Chromebook Users	HS-Oculus-02	O Default Site	10.112.165.54	Technology Policy	8
Configuration	HSOculus03	Default Site	10.112.165.108	Default Policy	8
Internal Domains	JR-High-OculusSystem	Oefault Site	10.112.161.191	Default Policy	8
Sites and Active Directory	Judsonia Elem Campus	Default Site	10.112.144.0/22	Default District Poli	8
lateral Maturalia	Kensett Elem Campus	Default Site	10.112.116.0/22	Default District Poli	0
Internal Networks	Orantur				

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

0	ahaha cisco	Deployments / Con Internal N	_{figuration} Jetworks	6			(Add
	Search Int	ernal Networks		٩			
	Network	Name		IP Address			
	Elem-F	Private	×	10.44.55.0	23 (512 IPs) 🔽		
	Site	t Site			L		
	CANC	EL				SAVE	

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.

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

0	ahaha cisco	Deployments / Configuration Internal Domains 🕤		Add
	Want to r started.	oute certain domains to your local resolver? You	've come to the right place. Click "Add"	above to get
	Note: interna	When you add a domain, all of its subdomains will inh al domains list, www.example.com will also be treated	nerit the setting. For example, if example.cor d as an internal domain.	n is on the
	Domain	1	Description	
	This inte	rnal domain applies to: pliances and Devic		
	CANC	a		CREATE

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 inaddr.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.

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

< Ba	ack To Multi-org Console						
	'liste Cisco Umbrell	a ×	Policies / Policy Components Destination Lists	0	6		
			Destination Lists enable you to domain.com will also allow or l	cust block	tomize your policy to block or allow any domains then apply those lis s subdomain.domain.com. You can also allow IP addresses and CIDR	ts to yo ranges	our policies. Adding wildcards to your bloc for Roaming Computers with the Roaming
•	Overview			Q	Search		
~		>					
E		~			New Destination List		
					List Name		
					Student Block		
	Destination Lists				Destinations in this list should be:		
	Security Settings				Blocked Allowed		
	Block Page Appearance				ru.com		ADD
	Bypass Users						
	Bypass Codes				Search		CLEAR
ıl.		>			nba.com DOMAI	N	₽ Add a comment

Category Settings

- 1. In the OpenDns Dashboard, Navigate to **Policies > Category Settings**
- Here you will be able to VIEW the "Centralized Default Settings" Category List <u>but not</u> <u>edit it</u>. 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.

< Back To Multi-org Console			
	Search	SEARCH	
esco Umbrella ×	Add New Content Setting		
APSCN-Robert Thompson Test	Setting Name Faculty Block		
 Overview 	Conv From Existing		
Identities >	None	*	
😑 Policies 🗸 🗸			
Policy List	CATEGORIES TO BLOCK SELECT ALL		
POLICY COMPONENTS			
Destination Lists	Academic Fraud	Government	Radio
Ontennas Cattings			
Category Settings	Adult Themes	Hate / Discrimination	Religious
Security Settings			
BLOCK PAGE SETTINGS	Adware	Health and Fitness	Research / Reference
Block Page Appearance	Alcohol	Humor	Search Engines
Bypass Users	Animo / Manga / Webcomic	Lastant Moscoging	Sovuality
Bunger Codes	Anime / wanga / webcomic	metanic meesaging	Jexuanty
	Auctions	Internet Watch Foundation	Social Networking

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.

CONTENT CATEGORIES

Adult		Hate Speech		Private IP Addresses as Host
Advertisements		Health and Medicine		Professional Networking
Alcohol		Humor		Real Estate
Animals and Pets		Hunting		Recipes and Food
Arts		Illegal Activities		Reference
Astrology		Illegal Downloads		Regional Restricted Sites (Germany)
Auctions		Illegal Drugs		Regional Restricted Sites (Great Britain
Business and Industry		Infrastructure and Content Delivery Networ	•	Regional Restricted Sites (Italy)
Cannabis		Internet of Things		Regional Restricted Sites (Poland)
Chat and Instant Messaging		Internet Telephony		Religion
Cheating and Plagiarism		Job Search		SaaS and B2B
Child Abuse Content		Lingerie and Swimsuits		Safe for Kids
Cloud and Data Centers		Lotteries		Science and Technology
Computer Security		Military		Search Engines and Portals
Computers and Internet		Mobile Phones		Sex Education
Conventions, Conferences and Trade Shows		Museums		Shopping
Cryptocurrency		Nature and Conservation		Social Networking
Dating		News		Social Science
Digital Postcards		Non-governmental Organizations		Society and Culture
Dining and Drinking		Non-sexual Nudity		Software Updates
DIY Projects		Not Actionable		Sports and Recreation
DoH and DoT		Online Communities		Streaming Audio
Dynamic and Residential		Online Document Sharing and Collaboration		Streaming Video
Education		Online Meetings		Terrorism and Violent Extremism
Entertainment		Online Storage and Backup		Tobacco
Extreme		Online Trading		Transportation
Fashion		Organizational Email		Travel
File Transfer Services		Paranormal		URL Shorteners
Filter Avoidance		Parked Domains		Weapons
Finance		Peer File Transfer		Web Cache and Archives
Freeware and Shareware		Personal Sites		Web Hosting
Gambling		Personal VPN		Web Page Translation
Games		Photo Search and Images		Web-based Email
Government and Law		Politics		
Hacking	~	Pornography		

▲ CONTENT CATEGORIES (LEGACY)

Categories SELECT ALL

Academic Fraud	Hate / Discrimination	Proxy / Anonymizer
Adult Themes	Health and Fitness	Radio
Adware	Instant Messaging	Religious
Anime / Manga / Webcomic	Internet Watch Foundation	Research / Reference
	□ IT-ADM	Search Engines
Blogs		Sexuality
Business Services	Jobs / Employment	Software / Technology
Chat	Lingerie / Bikini	Sports
Classifieds		Tasteless
Drugs		Television
Ecommerce / Shopping	News / Media	Terrorism
Educational Institutions	Non-Profits	Video Sharing
File Storage	Nudity	Visual Search Engines
Financial Institutions	P2P / File sharing	Web Spam
Forums / Message boards	Photo Sharing	Webmail
German Youth Protection	Podcasts	
Government	Portals	

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 II	nust migrate all legacy content categories.	For more information, see Umbrella	a's Help.	N	IIGRATE CONTENT CATEGORIES
Con	tent Category Migration To	ol			
lnt	tro	2 Migrate			Confirmation
Cisc achie Tool	o Umbrella's content categories are changing eve this alignment, you must migrate your cu to achieve this goal. For more information ab	g so that they align with the content rrent content categories to Umbrella yout the about the Content Category	categories used by the I's new content categor Migration Tool, see U	rest of Cisco's security ries. Use the Content C nbrella's Help.	r products. To ategory Migration
Pha	ases				
The	migration to new content categories will occu	Ir over the course of the following ph	nases:		
1	 Migration Phase: 3 months New and legacy content categories can New and legacy content categories avai 	be added and removed from policie lable to reports.	s.		
2	 Deprecation Phase: After Migration Phase Legacy content categories removed from Legacy content categories available to remove the second s	u se for 1 year n all policies. eports.			
3	 Removal Phase: At the end of the Depression Legacy Categories removed and unavai 	e cation Phase lable.			
At th	e end of the Migration Phase any remaining	Legacy Categories in use within poli	icies will be automatics	ally migrated to New Ca	Iterrories
CANC	EL				A 1073 CTT
Cor	ntent Category Migration To	ool			NEXT
Cor	ntent Category Migration To	00			— 3 Confirmation
Cor	ntent Category Migration To	POI Migrate ration to Umbrella's new Talos-bas	ed content categories	. For more information,	— (3) Confirmation Umbrella's Help.
Cor	ntent Category Migration To	POI 2 Migrate ration to Umbrella's new Talos-bas	ed content categories	For more information,	— ③ Confirmation Umbrella's Help. D MIGRATION REPORT
Cor	ntent Category Migration To ntro Jmbrella's legacy content categories for mig Legacy Category	nol ration to Umbrella's new Talos-bas New Category 👻	ed content categories	For more information, DOWNLOA	 Confirmation Umbrella's Help. D MIGRATION REPORT t +
Cor	ntent Category Migration To ntro	DOI A Migrate ration to Umbrella's new Talos-bas New Category Peer File Transfer	ed content categories DNS Policy Impact	For more information, DOWNLOA Identity Impac 7 Identities	— ③ Confirmation Umbrella's Help. D MIGRATION REPORT t ✓
Cor	ntent Category Migration To ntro	OOI Image: Constraint of the second	ed content categories DNS Policy Impact 3 DNS Policies 3 DNS Policies	For more information, DOWNLOA Identity Impac 7 Identities 7 Identities	The second secon
Cor	ntent Category Migration To htro	Migrate aration to Umbrella's new Talos-bas New Category Peer File Transfer Streaming Audio Adult	ed content categories DNS Policy Impact 3 DNS Policies 3 DNS Policies 3 DNS Policies	For more information, DOWNLOA Identity Impac 7 Identities 7 Identities 7 Identities	The NEXT
	ntent Category Migration To ntro Jmbrella's legacy content categories for mig Legacy Category → → P2P / File sharing → Radio → Adult Themes →	New Category Peer File Transfer Streaming Audio Adult Extreme	ed content categories DNS Policy Impact 3 DNS Policies 3 DNS Policies 3 DNS Policies 3 DNS Policies	For more information, DOWNLOA Identity Impac 7 Identities 7 Identities 7 Identities 7 Identities	The NEXT
Cor	Legacy Category — P2P / File sharing — Radio — Adult Themes — Tasteless — Proxy / Anonymizer —	New Category Peer File Transfer Streaming Audio Adult Extreme Filter Avoidance	DNS Policies 3 DNS Policies 3 DNS Policies 3 DNS Policies 3 DNS Policies 3 DNS Policies	For more information, DOWNLOA V Identity Impac 7 Identities 7 Identities 7 Identities 7 Identities 7 Identities	The NEXT
	Legacy Category → Legacy Category → P2P / File sharing → Radio → Adult Themes → Tasteless → Proxy / Anonymizer → Nudity →	Migrate aration to Umbrella's new Talos-bas New Category Peer File Transfer Streaming Audio Adult Extreme Filter Avoidance Non-sexual Nudity	ed content categories DNS Policy Impact 3 DNS Policies 3 DNS Policies 3 DNS Policies 3 DNS Policies 3 DNS Policies	For more information, DOWNLOA Identity Impact 7 Identities 7 Identities 7 Identities 7 Identities 7 Identities 7 Identities 7 Identities	The NEXT
Cor	Legacy Category → Legacy Category → P2P / File sharing → Radio → Adult Themes → Tasteless → Proxy / Anonymizer → Nudity →	New Category Peer File Transfer Streaming Audio Adult Extreme Filter Avoidance Non-sexual Nudity	ed content categories DNS Policy Impert 3 DNS Policies 3 DNS Policies 3 DNS Policies 3 DNS Policies 3 DNS Policies 3 DNS Policies 4 Content categories 5 Content catego	For more information, DOWNLOA V Identity Impac 7 Identities 7 Identities 7 Identities 7 Identities 7 Identities 7 Identities 0 1 Identities	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.
Content Category Migration Tool

6	Intro Migrate	_ 3	Confirmation
Do unt	not close or refresh your browser page during the migration process. After Umbrella completes the migration process, legacy il the Migration Period ends.	y categori	es are available
	After migration, legacy categories can be manually added to policies until the end of the migration period. Please do not close or re during the migration process	fresh your	page
C	Confirm migration		
			↓
	CANCEL	ВАСК	MIGRATE

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.

l.	/	Category Migration Complete.
		All legacy content categories have been successfully migrated or your policies did not previously contain any legacy categories. For more
		information, see Umbrella's Help.

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.

Applications To Control

Searc	h for an application		
	Customer Relationship Management (CRM)		
$\square \rightarrow$	E-Commerce		
• ~	Games		
ø	Brave Frontier	Block	٥
	Electronic Arts		
	Mail.ru Games		
	Microsoft Xbox Live		
	Nintendo		

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.

Application Control Change Summary

Please review the summary and changes before proceeding to the next step.

The following applications will be blocked:





Example App, plus 27 more (Anonymizer)

The following policies will be affected:

Default Policy



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.

D	efault	Settings	Settings Enabled 7	Integrations 0	Last Modified Dec 5, 2019	^
	Settir Defa	ng Name ault Settings Melware	drive deve deventes de la vertaite poe	bile threate cod more	-	
-	_	Newly Seen Domains	anve-by downloads/exploits, mo	one threats and more	7.	

 Command and Control Callbacks Prevent compromised devices from communicating with stackers' infrastructure. Phishing Attacks Fraudulent websites that aim to trick users into handing over personal or financial information. Dynamic DNS Block sites that are hosting dynamic DNS content. Potentially Harmful Domains Domains that exhibit suspicious behavior and may be part of an attack. DNS Tunneling VPN VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer. Cryptomining Cryptomining allows organizations to control cryptominer access to mining pools and web miners. 		U	Domains that have become active very recently. These are often used in new attacks.
 Phishing Attacks Fraudulent websites that aim to trick users into handing over personal or financial information. Dynamic DNS Block sites that are hosting dynamic DNS content. Potentially Harmful Domains Domains that exhibit suspicious behavior and may be part of an attack. DNS Tunneling VPN VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer. Cryptomining Cryptomining allows organizations to control cryptominer access to mining pools and web miners. 		~	Command and Control Callbacks Prevent compromised devices from communicating with attackers' infrastructure.
 Dynamic DNS Block sites that are hosting dynamic DNS content. Potentially Harmful Domains Domains that exhibit suspicious behavior and may be part of an attack. DNS Tunneling VPN VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer. Cryptomining Cryptomining allows organizations to control cryptominer access to mining pools and web miners. 		~	Phishing Attacks Fraudulent websites that aim to trick users into handing over personal or financial information.
 Potentially Harmful Domains Domains that exhibit suspicious behavior and may be part of an attack. DNS Tunneling VPN VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer. Cryptomining Cryptomining allows organizations to control cryptominer access to mining pools and web miners. INTEGRATIONS 			Dynamic DNS Block sites that are hosting dynamic DNS content.
 DNS Tunneling VPN VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer. Cryptomining Cryptomining allows organizations to control cryptominer access to mining pools and web miners. INTEGRATIONS 		~	Potentially Harmful Domains Domains that exhibit suspicious behavior and may be part of an attack.
Cryptomining Cryptomining allows organizations to control cryptominer access to mining pools and web miners. INTEGRATIONS	•	~	DNS Tunneling VPN VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer.
▶ INTEGRATIONS		~	Cryptomining Cryptomining allows organizations to control cryptominer access to mining pools and web miners.
	Þ	INT	EGRATIONS

CANCEL

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 <u>cannot</u> 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**.

What would you like to protect?

Select Identities

AD Groups	12
🛔 AD Users	9
AD Computers	2
Networks	Ť
Roaming Computers	
Mobile Devices	
Sites	4
Network Devices	
	 AD Groups AD Users AD Computers Networks Roaming Computers Mobile Devices Sites Network Devices

4. Click Next

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

	the start in the second s		
	Enforce Security at the DNS Layer Emission domains are blocked when they heat malware, command and control, philbling, and more		
	Inspect Files Take Servy Inspect Nen Technologies, content using within an signatures and Clace Advanced Malaxies Protection		
	Limit Content Access Risci: or allow show based on their certaint, such as the sharing, gambling, or blogging.		
	Apply Destination Lists Luis of destinations that can be orgitally blocked or alreaded for any identifies using the justry		_
ADV	VANCED SETTINGS		
	CANCER	 REVIENTS	MUX

- 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.

	identities using this policy are protected by selecting or creating a security setting. Click Edit Setting to make changes to any
isting	settings, or select Add New Setting from the dropdown menu.
Defau	t Settings .
ATEGO	DRIES TO BLOCK EDIT
D	Malware Websites and other servers that host malicious software, drive-by downloads/exploits, mobile threats and more.
U	Newly Seen Domains Domains that have become active very repently. These are often used in new attacks.
D	Command and Control Calibacks Prevent compromised devices from communicating with attackers' infrastructure.
U	Phishing Attacks Fraudulent websites that aim to trick users into handing over personal or financial information.
U	Dynamic DNS Block sites that are hosting dynamic DNS content.
U	Potentially Harmful Domains Domains that exhibit suspicious behavior and may be part of an attack.
	Potentially Harmful Domains Domains that exhibit suspicious behavior and may be part of an attack. DNS Tunneling VPN UNN more than the same that include their testing to the post of the post the ONS material. These are the used to have a post testing to the one of the have a post testing testing to the one of the have a post testing

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

_im	it Content Access	201 201 201 20	
Aoces	s to these sites will be restricted based on the type of conten	it served by the pages of the site.	
		Categories to Block - High	
0	High Blocks addi-related sites, illegal activity sporal networking	These are the categories we w	ill block. Note: if you want to make
	sites, video sharing sites, and general time-wasters.	Adult Themas	• Arivera
		Alcohol	Chat
		Classifieds	Dating
0	Moderate	Drugs	File Storage
	Blocks all adult-related websites and illegal activity.	 Forums / Message boards 	Gambling
		• Games	Hate / Discrimination
		 Instant Messaging 	Lingerie / Bikini
0	1 min	Nuclity	P2P / File sharing
0	Blocks pomography.	 Photo Sharing 	 Pornography
		 Proxy / Anonymizer 	Sexuality
		 Social Networking 	 Tasteless
		Video Sharing	Visual Search Engines
0	Custom	 Weapons 	 Webmail
Secur	ity 📀 Content 🚳 De	CA setinations (4) Bi	NCEL PREVIOUS NE
Secur	ity (2) Content (3) De	CA estinations (2) Bi	NCEL PREVIOUS NO
Secur	ity 2 Content 8 De Content Access to these sites will be restricted based on the type of content	ca estinations	NCEL PREVIOUS NO
Secur	ity 2 Content 8 De Content Access to these sites will be restricted based on the type of content High	ca estinations	NCEL PREVIOUS NO
Secur imit O	ity (2) Content (8) De Content Access to these sites will be restricted based on the type of content High Blocks adult-related sites, likegal activity, social networking sites, wide sharing sites, and general time-wasters.	CA estinations (2) Bi t served by the pages of the site Custom Setting Default Settings	NCEL PREVIOUS NO
Secur Imit O	ity 2 Content 3 De Content Access to these sites will be restricted based on the type of content High Blocks adult-related sites, likegal activity, social networking sites, video sharing sites, and general time-weaters.	Ca estinations & Bi t served by the pages of the sits. Custom Setting Default Settings Centrelized Default Settings	NCEL PREVIOUS NO
Secur imit O	try 2 Content 3 De Content Access to these sites will be restricted based on the type of content High Blocks adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters.	CA estinations	NCEL PREVIOUS NO
Secur Imit O	try 2 Content 3 De CONTENT ACCESS to these sites will be restricted based on the type of content High Blocks adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters. Moderate	CA estinations	NCEL PREVIOUS NE
Secur imit O	ity 2 Content 3 De CONTENT ACCESS to these sites will be restricted based on the type of content High Blocks adult-related sites, liegal activity, social networking sites, video sharing sites, and general time-wasters. Moderate Blocks all adult-related websites and liegal activity.	Cateronal Catero	NCEL PREVIOUS NO
Secur Imit O	ity 2 Content S De Content Access to these sites will be restricted based on the type of content High Blocks adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters. Moderate Blocks all adult-related websites and lilegal activity.	CA estinations (2) Bi t served by the pages of the site Custom Setting Default Settings Default Settings Default Settings Faculty Grant's Categories	NCEL PREVIOUS NE
Secur Imit CO	try 2 Content 2 Content 2 Content 2 Content 2 Content Access to these sites will be restricted based on the type of content 2 High 2 Blocks adult-related sites, lilegal activity, social networking sites, video sharing sites, and general time-wasters.	CA estinations CA is served by the pages of the site Custom Setting Default Settings Default Settings Default Settings Faculty Grant's Categories Shalby's Default Categories	NCEL PREVIOUS NE
imit ocess O	try 2 Content 2 Content 2 Content 2 Content 2 Content Access to these sites will be restricted based on the type of content High Blocks adult-related sites, lilegal activity, social networking sites, video sharing sites, and general time-wasters.	Categories Shelby's Default Categories	NCEL PREVIOUS NE
imit coss 0	try 2 Content © De CONTENT ACCESS to these sites will be restricted based on the type of content High Blocks adult-related sites, lilegal activity, social networking sites, video sharing sites, and general time-wasters. Moderate Blocks all adult-related websites and lilegal activity. Low Blocks pornography:	ca estinations () Ei t served by the pages of the site Custom Setting Default Settings Centralized Default Settings Default Settings Faculty Grant's Categories Shaitoy's Default Cetegories Shaitoy's Default Cetegories	NCEL PREVIOUS NE
	try 2 Content © De CONTENT ACCESS to these sites will be restricted based on the type of content High Blocks adult-related sites, lilegal activity, social networking sites, video sharing sites, and general time-wasters. Moderate Blocks all adult-related websites and lilegal activity. Low Blocks pernography:	estinations CA estinations CA t served by the pages of the site. Custom Setting Default Settings Centralized Default Settings Default Settings Default Settings Faculty Grant's Categories Shelby's Default Categories CREATE NEW SETTING CREATE NEW SETTING	NCEL PREVIOUS NE
	try 2 Content © De CONTENT ACCESS to these sites will be restricted based on the type of content High Blocks adult-related sites, lilegal activity, social networking sites, video sharing sites, and general time-wasters. Moderate Blocks adult-related websites and ilegal activity. Low Blocks pornography:	Castinations Ca estinations Casting Bi Custom Setting Default Settings Centralized Default Settings Default Settings Faculty Grant's Categories Shelby's Default Categories Shelby's Default Categories CREATE NEW SETTING Financial Institutions Cambing	NCEL PREVIOUS NE
	try 2 Content © Definition of the second of	Castinations Casting Bill Custom Setting Custom Settings Custom Settings Centralized Default Settings Default Settings Default Settings Faculty Grant's Categories Shelby's Default Categories CREATE NEW SETTING Financial Institutions Casting Cambling Casting Categories	NCEL PREVIOUS NE

- 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	Conten	t 3 Applications	4	Destinations	-2	2 More
----------	--------	------------------	---	--------------	----	--------

Control Applications

Default Settings	τ		
Default Settings			
CREATE NEW SETTING			
Search for an application			
Ad Publishing		•	
🗷 > Anonymizer	Block		
Application Development	and Testing		
Business Intelligence			
> CRM			
Cloud Storage			
Collaboration			
		•	

Select applications or applicatio

- 9. On the **Destinations Page**, your **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

Q	Search		2 Allow Lists Applied	REMOVE ALL
2		Showing: All Lists 🔻 5 Total	O Default Allow	0
Ø	Default Allow	0.5	Slobal Allow List	S 33
Ø	Default Block	Q >	2 Block Lists Applied	REMOVE ALL
ē.	🥏 Global Allow List		Default Block	0
8	Global Block List	0.>	Global Block List). 0 5
9	network list	1.5		

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

Security	Content	Oestinations	Block Pages	🔘 Summary
Set Block P	age Settings			
Define the appears	ance and bypass options for you	ar block pages.		
O Use Umbrel Preview Block	la's Default Appearance			
Use a Custo	om Appearance			
Centralized	I Default Settings	46 ⁻		
Preview Block	k Page »			
DVDASS HEEDS				
DITASSOSEICS				
BYPASS CODES				
			CANCEL PREV	/IOUS NEXT

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

Poli	cy Summary		
Policy Distr	Name		
U	28 Identities Affected © Network: Devices, 4 Sites, 0 Mobile Devices, 0 Rosming Computers, 1 Network, 2 AD Computers, 9 AD Usera, 12 AD Groups Edit	U	4 Destination Lists Enforced • 2 Block Lists • 2 Allow Lists Edit
U	Security Setting Applied: Default Settinge • Command and Control Callbacka, Malware, Phishing Attacka, plus 1 more will be blocked • No intermettion is concluded	U	File Inspection Enabled Allows intelligent proxy to block melicious files. Disable
	Edit Dissble	U	Custom Block Page Applied Centralized Default Settings Edit
U	Content Setting Applied: Default Settings * Adware, Alcohol, Austiona, plus 34 more will be blocked. Edit Disable		_
AD	VANCED SETTINGS		

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 <u>NOT</u> 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 <u>LEAST</u> restrictive policies, **I.E. IT or Administration**, should be at the **top** and your <u>MOST</u> 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**.

trict [Default Policy	Applied To 0 Identities	Contains Last Modified 3 Policy Settings Feb 5, 2018	
Policy Distri	Name ct Default Policy]		
0	0 Identities Affected Enable	U	2 Destination Lists Enforced • 1 Block List • 1 Altow List Edit	
U	Security Setting Applied: Default Settings Command and Control Cellbecks, Malware, Phishing Attacks, plus 1 more will be blocked No integration is enabled. Edit Disable	U	File Inspection Not Enabled Adows intelligent proxy to block melloious files. Enable	
D	Content Setting Applied: Default Settinge Advore, Alcohol, Auctione, plue 34 more will be blocked. Edit Diseble	U	Custom Block Page Applied Centralized Default Settings Edit	

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

 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.
 SAFESEARCH

```
Enforce SafeSearch
Enforce SafeSearch for queries sent to supported search engines Learn More
```

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 <u>ONLY</u> 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.

ALLOW-DINLY MODE

Allow-Only Mode

In this mode, access to sites needs to be specifically granted; otherwise connections will be blocked by default.

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.

LOG	BING
٥	Log All Requests
0	Log Only Security Events Log and report on only those requests that match a security filter or integration, with no reporting on other requests.
0	Don't Log Any Requests Note: No requests will be reported or alerted on. Unreported events will still be logged anonymously and aggregated for research and threat intelligence purposes.

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.

< Back To Multi-org Console	۹. ۲
Cisco Umbrella	Configuration Configuration Root Certificate
Overview	
Deployments ~	
Core Identities	
Networks	Get Started
Network Devices	blocked sites. The certificate will match the requested site but will be signed by the Cisco Root Certificate Authority (CA).
Roaming Computers	DOWNLOAD CERTIFICATE
Mobile Devices	To varify your download, oback the Cisco certificate's SHA1 thumborint and ensure that it matches
Chromebook Users	C5:09:11:32:E9:AD:F8:AD:3E:33:93:2A:E8:0A:5C:8F:A9:30:E8:24
Configuration	For instructions for Windows, OS X and Linux and across Chrome, Firefox, and Safari on those platforms (as applicable), including guidance with GPC, please read here:
Internal Domains	https://docs.unitrens.com/product/unitrens/resiand-cisco-certificate-import-information/
Sites and Active Directory	TROUBLESHOOTING
Internal Networks	
Service Account Exceptions	
Root Certificate	
Policies https://dashboard.umbrella.com/o/2469806/	>

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.

Raine -	<u>.</u>	G	Group	Policy Manage	ment Editor	r	-	D X	Server N	lanag
	File Actio	on View Help								
	(* 🔿 🖄	Group Policy Management Editor								
	4 📫 Po	licies			lss	ed To	• •	Issued By		
Dasi							^	this view.	1	
Loca	Þ	<u>.</u>			Open				X	
All S		🍥 🛞 – 🛧 🚺	 This 	PC Downloads		~ C	Search Downl	oads	Q	
🖬 AD I		Organize 👻 New f	older					•	. 0	
TI DHO		☆ Favorites	^	Name	•		Date mo	odified	Туре	
		Desktop		Cisco_Umbrel	la_Root_CA		10/4/20	18 2:23 PM	Security C	
File .	1	Downloads								
ш нур		Recent places	_							
		ika This PC	_							
		Le Desktop								
		Documents								
		Downloads		L2						
		Music Dicturer								
		Videos								
		Local Disk (C:)								
		PUD Datas (DA)	<u> </u>	<	111				>	9 04
		File	e nam	e: Cisco_Umbrella_F	Root_CA		 Certificate 	File (*.cer;*	.crt) v	当 UI
							Open		ancel	D Ma
									al.	Eve
		Network Access Prote	ection							- LV
		Application Control P	Policie	s	~					se
	<	III			> <	111		>	-	Pe
	L		_							BP
	. 2	3 📜 📓		J						

Deploy Certificate with GPO

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

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

a	Server Manager	_ 0 ×
€∋∙	Server Manager • Dashboard • 🕲 🚩 Manage Tools	View Help
Dashboard	WELCOME TO SERVER MANAGER	
All Server	Image: Stroup Policy Management Image: File Action View Window Help Image: File Action View Window Help Image: File Action View Window Help	
1 DHCP	Group Policy Management ▲ Forest: TESTDOMAIN.local ▲ Default Domain S ▲ Default Domain Policy ● Default Domain Policy ● Default Domain Policy ● Default Domain Controllers ● Default Domain Controllers ● Default Domain Policy ● Default Domain Controllers ● Default Domain Policy ● Default	Hide
	BPA results BPA results	~
	2 🔒 📓 🔹	3:12 PM 10/4/2018

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

P		Server Manager	_ 0 X
€⊛∙	Server Manager • Dashboa	rd 🛛 🗸 🕄 🖡 Manage Tools	View Help
🔛 Dashboard	WELCOME TO SERVER M	ANAGER	^
Local Server	<u>s</u>	Group Policy Management	
All Servers	📓 File Action View Window Help	_ <i>B</i> ×	
AD DS	🗢 🔿 🙍 🖬 🖬 🗶 🍳 👘		
前 DHCP	Group Policy Management	Default Domain Policy	=
🔒 DNS	A Forest: TESTDOMAIN.local A Domains	Scope Details Settings Delegation Status	
File and Stora	A 👔 TESTDOMAIN.local	Links	
🛅 Hyper-V	Default Domain Policy	Display links in this location:	
	 Domain Controllers 	The following sites, domains, and OUs are linked to this GPO:	
	▷ I Lab Computers	TESTDOMAIN.local No Yes 1	
	Group Policy Objects I Default Domain Controllers Policy		
	Default Demain Dolige		Hide
	Local adm Edit MMI Eithern GPO Statur	ng	
	Starter GPOs	s GPO can only apply to the following groups, users, and computers:	
N	▷ Sites Back Op Back Op	Backup d Users	
43	Group Policy Modeli Import Settin	зс	
	Save Report	Remove Properties	
	View	· · · · · · · · · · · · · · · · · · ·	
	New Window	from Here	
	Сору	Open	
	< III Delete		
	Open the GPO editor Rename		
	BF	BPA results	
	Help		
			3:13 PM
		▲ 10 ¥	10/4/2018

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.

File Action View Help Image: Section of the se	TESTDOMA
	TESTDOMA figuration tion
	TESTDOMA figuration tion
	TESTDOMA
A Policies Select an item to view its description. Marce mouter Configuration S > ⊡ Software Settings Select an item to view its description. Marce mouter Configuration A □ Windows Settings Select an item to view its description. Select an item to view its description.	iguration tion
S b Computer Conf an a Windows Settings & User Configurat	figuration tion
n 🔺 🗎 Windows Settings 🐒 User Configurat	tion
Image: Second	
S 📄 Scripts (Startup/Shutdown)	
a 🚡 security Settings	
Account Policies	
Local Policies	
10 b a Event Log	
Sector Gradienter Gradienter	
D A system Services ■	
P a registry	
b Wired Network (IEEE 802.3) Policies	
Windows Firewall with Advanced Security	
Network List Manager Policies	
Wireless Network (IEEE 802.11) Policies	
🔺 🚞 Public Key Policies	
Encrypting File System	
🖆 Data Protection	
BRLocker Drive Encryption	
BitLocker Drive Encryption Network Unlock	
Trusted Root Certification and a state	
Enterprise Truct Import	
Intermediate Certi All Tasks	
Trusted Publishers	
Untrusted Certifica	
Trusted People Help	
Software Restriction Policies	
Network Access Protection	
Kitended (Standard /	

- 4. On the Welcome to the Certificate Import Wizard page, click Next.
- 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.

on View Help	
📰 🟥 🙆 🍺 🛛 🗊	
licies	Issued By
Certificate Import Wizard	this view.
Certificate Store Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location for the certificate.	
Automatically select the certificate store based on the type of certificate	
Cartificate store:	
Trusted Root Certification Authorities Browse	
Next Cancel	
Software Restriction Policies Software Restriction	
Application Control Policies	
	>

7. On the Completing the Certificate Import Wizard page, verify that the information you provided is

accurate, and then click **Finish**.

	Group	Policy Management Editor	
Action Vi	ew Help		
🕈 🗹 🔝 E	1 Q 🗃 🖬 🖻		
Policies		A Issued To	Issued By
			this view.
	Sertificate Import V	Wizard	
4			
	Completing the C	Certificate Import Wizard	
	The certificate will be impor	ted after you click Finish.	
	You have specified the follow	wing settings:	
	Certificate Store Selected	by User Trusted Root Certification Authorities	
	Content	Certificate	
	File Name	C:\Users\Administrator\Downloads\Cisco_Umbrei	a.
	4		
	× .		
		Finish Ca	ncel
	Notware Resolution Policies		
P 🔤	Application Control Deligion	-	
	Application Control Policies		

Deploy Certificate to Chrome Devices with Google Admin

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

- 1. <u>Sign in</u> to the <u>Google Admin console</u>.
- 2. Click Device management.
- 3. On the left, click **Network**.
- 4. Click Certificates.
- (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.
- 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. <u>Verify the CA on managed Chrome devices</u>
- 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:

Certificate manager Your Certificates Servers	Authorities	Others
You have certificates on file CertSIGN CertSIGN ROOT C Chromedeployment	that identify thes	e certificate authorities:
Chromedeployme	nt 🏢	
ate has been installed by your sy or.	stem	
	Certificate manager Your Certificates Servers You have certificates on file CertSIGN CertSIGN ROOT C. Chromedeployment Chromedployment Chromedeployment Chromedploymen	Certificate manager Your Certificates Servers Authorities You have certificates on file that identify thes CertSIGN CertSIGN ROOT CA Chromedeployment Chromedployment Chromedeployment C

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

<u>ByPass User</u> 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 umbrellasupport@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.

Add New Bypass User	
Bypass User Description	
New Bypass User	
Bypass User	
Select a bypass user *	
This bypass user can:	
 Bypass everything O Bypass specific categories and destination lists 	
	CANCEL SAVE

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.

Create New Bypass User

Matt's Bypass user	
Bypass User	
Matt Prytuluk ~	
This bypass user can: Bypass everything	stination lists
Bypass Categories Allow the user to bypass specific categories.	Search Categories
Bypass Categories Allow the user to bypass specific categories. Bypass Destination Lists	Search Categories
Bypass Categories Allow the user to bypass specific categories. Bypass Destination Lists Allow the user to bypass specific lists of blocked destinations.	Search Categories Academic Fraud Adult Themes
Bypass Categories Allow the user to bypass specific categories. Bypass Destination Lists Allow the user to bypass specific lists of blocked destinations.	Search Categories Academic Fraud Adult Themes Adware
Bypass Categories Allow the user to bypass specific categories. Bypass Destination Lists Allow the user to bypass specific lists of blocked destinations.	Search Categories Academic Fraud Adult Themes Adware Alcohol

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.

New	Bypass user	BPB User	\$ (UTC-07:00)
newbypass@cisco.com		•••••	•••••

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**.

New Bypass User		
ypass User		
Select a bypass user *		
his bypass user can:		
Bypass everything O Bypass specific categories and destination lists		
Bypass everything O Bypass specific categories and destination lists		

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.

Policies / Block Page Settings Bypass Codes Output Output		OpenDNS Dashboard
Q Search	SEARCH	
Add New Bypass Code Bypass Code Name New Bypass Code This bypass code can: Bypass everything O Bypass specific categorie This bypass code will expire on:	es and destination lists	
2022-06-25		CANCEL SAVE

- 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**.

Legal team bypass code	Code 0A6N1	Can Bypass Everything
Bypass Code Name		
Legal team bypass code		
Code: 0A6N1 This bypass code can:		
Bypass everything Bypa Bypass everything Bypa	ss specific categories a	nd destination lists
2018-02-03 🛍 11:59 PM	-	
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.

	Cisco Umbrella
4	This site is blocked.
far	nilydoctor.org
> Ad	ninistrative Bypass
	Sorry, familydoctor.org has been blocked by your network administrator.
	> Diagnostic Info
	Terms Privacy Policy Contact

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

familydoctor.org	
Administrative Bypass	
lock Page Bypass is a feature that allows aut	horized users to bypass this block page. If you're
uthorized, you can log in with your Cisco Umb ode provided by your network administrator.	prella credentials. Otherwise, you can use a temporar
mail Address (or Username)	Bypass Code
	•••••
Password	01/01/02
000110	BYPASS
mail Address (or Username)	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: Cisco Umbrella	
Block P	age Bypass	
You are curr	ently using bypass code TT***.	
This code ex	pires in 11 hours.	
LOG OUT		

Chromebook Client

The Cisco Umbrella Chromebook client provides DNS layer protection for Chromebook users whether they are connected to your networks or remotely, no matter which Chromebook device they use.

You can use the Chromebook client to accomplish three main goals:

- Protection from phishing: Protect against phishing threats automatically with Umbrella's global network data
 and predictive intelligence to discover internet infrastructure used to host phishing sites—before employees or
 students ever receive the phishing email.
- Content category filtering: Gain visibility and control of content on and off network. Organizations can help ensure compliance with the Children's Internet Protection Act (CIPA) utilizing over 80 content categories, as well as their own allow and block lists of domains.
- Per-user visibility and policy: Enforce policy-based protection whether users are on or off the network. If user becomes infected, pinpoint activity to a specific user to expedite remediation.

How the Umbrella Chromebook client works

Chromebook users are protected by the Cisco Umbrella Chromebook client in the following sequence:

- A user enters a URL in the Chromebook browser.
- The Chromebook client extension copies the domain name from the URL and sends it to the Chromebook client app.
- The app creates an EDNS query, then sends the DNS request, including the EDNS information, to the Umbrella resolver.
- Depending on the applicable policies applied in the Umbrella dashboard, the resolver responds by either blocking the IP address of disallowed domains or resolving the IP address in the case of acceptable domains.



The Umbrella Chromebook client is deployed using a Chrome extension and application available on the Chrome Web Store.

Installation Guide

There are three parts to this installation:

- Downloading the configuration file from the Umbrella Dashboard
- Installing the Cisco Umbrella Chromebook client extension on your Chromebooks
- Installing the Cisco Umbrella Chromebook client application on your Chromebooks

In addition, you can find instructions for removing Cisco Umbrella Chromebook software in the last section of this guide.

Prerequisites

In order to install the Cisco Umbrella Chromebook client, you must:

- be a G Suite admin account in order to log into admin.google.com.
- have a valid Umbrella dashboard login.
- Chromebooks must have Chrome OS v55 or later.
- Chromebooks are not in Kiosk mode
- Port 53 UDP accessible to 208.67.220.220 and 208.67.222.222
- <u>https://registration.polaris.qq.opendns.com</u> is accessible
- Unsupported :
 - Chrome browser on OS X, Windows, and Linux
 - Devices running variations or third-party distributions of Chrome OS, such as Neverware CloudReady.

Networking Requirements

The Cisco Umbrella Chromebook client uses the following ports:

Port and Protocol	Source / Destination	Notes
53 (TCP + UDP)	208.67.222.222/32,	Used for EDNS Queries
	208.67.220.220/32	
443 (TCP)	registration.polaris.qq.opendns.com	HTTPS - Used for registration
443 (TCP)	Virtual Appliances	Used for the Trusted Network Detection feature.

Recommendations

Disallow the *incognito window* for Chromebook users in the G Suite Admin Console.

GANIZATIONS	Search settings		
		Idle time in minutes (leave empty for system defa	ult)
		Action on idle	
		Sleep (default)	\$
		Action on lid close	
		Sleep (default)	\$
		Lock screen on sleep	
		Allow user to configure	\$
	Locally applied	Incognito Mode Disallow incognito mode	ė.
Students			9
Teachers	Browser History	Always save browser history	
	Inherited	Aimaya save biomaer matory	•
10	Clear Browser History	Clear Browser History 🖓	

Implementing Trusted Network Detection

If you are implementing <u>Trusted Network Detection</u>, Cisco Umbrella recommends that you check your DHCP server to make sure that it is providing Chromebook devices with the same VA IP address as other devices on your network.

Part 1: Obtain the configuration file from Umbrella

The configuration file contains the information required for the Cisco Umbrella Chromebook client to work with Umbrella.

- 1. Log into dashboard.umbrella.com
- 2. Open Deployments, then select Chromebook Users.
- 3. Select *Configure*, then download the configuration file:

Configure Umbrella Chromebook Clients

Protecting Chromebook Computers

Enable Umbrella security for your Chromebooks by installing the Chromebook client Extension and App. You configure the Umbrella App by using the Google Admin Console to upload this data file

1. Download your organization's configuration file from the link below:

CHROMEBOOKCONFIG.JSON (Size ~0.1 kB)

2. Install the Chromebook client software (Extension and App) by following the Chrome Setup Guide

 Sign in with super admin email id of your Google Admin Console to sync GSuite identities into Umbrella.

SUPER ADMIN SIGN IN

JSON File Example (Without VA):

Note: cannot contain line breaks or spaces

{"googleDirectoryService":{"Value":True},"organizationInfo":{"Value":{"organizationId":7896540,"regToke n":" kBCTNrrRerVQep49ErsR1AbLURODxKXn "}},"publicSession":{"Value":false},"vaIPs":{"Value":[]}}

VA customers only

To use the Cisco Umbrella Chromebook client in a network with Cisco Umbrella Virtual Appliances, you must add the IP addresses of your VAs to the configuration file before uploading it. Each VA IP addresses must be enclosed in double quotes, comma-separated. This example illustrates a network with two VAs:

"valPs":{"Value":["192.168.100.10","192.168.100.11"]}

JSON File Example (With VA):

Note : Cannot contain line breaks or spaces

{"googleDirectoryService":{"Value":True},"organizationInfo":{"Value":{"organizationId":7896540,"regToke n":"kBCTNrrRerVQep49ErsR1AbLURODxKXn"}},"publicSession":{"Value":false},"vaIPs":{"Value":["192.168. 100.10","192.168.100.11"]}}

Or

```
{
 "organizationInfo":{
  "Value":{
    "organizationId":1234567,
    "regToken":"GtTYPQfgSzQtGzYUrINmbjgTu5XriDtn"
  }
 },
 "valPs":{
  "Value":[
    "192.168.100.10",
    "192.168.100.11"
  ]
 },
 "googleDirectoryService": {
       "Value": true
}
}
```

Make sure you save the file in a known location. You will upload this file during the installation of the Cisco Umbrella Chromebook client **application**.

Part 2: Install the Cisco Umbrella Chromebook client extension

1. Log into <u>https://admin.google.com</u>.

≡	Google Admin	Q Search for users, gro	ups, and settings (e.g. setup M	IX records)	
Admi	n console				
	-				?
	Users	Company profile	Billing	Apps	Support
	Add, rename, and manage users	Update information about your company	View charges and manage licenses	Manage apps and their settings	Talk with our support team
		@	~		<u></u>
	Admin roles	Domains	Reports	Security	Groups
	Add new admins	Add domains or domain aliases	Track usage of services	Manage security features	Create groups and mailing lists

2. Select Devices.



Devices Secure corporate data on devices

3. In the Device Management window, select **Chrome Management**.

DEVICE SETTINGS

Networks

Chrome management

4. In the Chrome Management window, select **Apps & extensions**.

Chrome Management
Devices View and manage Chrome devices
Managed browsers View and manage Chrome browsers
User & browser settings Manage user-based settings on Chrome browsers and Chrome devices
Apps & extensions Manage Android apps and Chrome apps and extensions

5. On the left side, select the OU of the **Users** you want to deploy the extension to, or the top level domain if you want to push it to everyone.



6. At the bottom right, click the **Yellow +** then click the icon that resembles a calculator.



7. Search for the ID of the Cisco Umbrella Chromebook client extension **jcdhmojfecjfmbdpchihbeilohgnbdci** then click **save**. (Searching by name will not work.)

Add Chrome app or extension by ID
Chrome apps and extensions can also be added by specifying the ID. If it is outside the Chrome Web Store, you must also specify the URL where the extension is hosted.
Extension ID
jcdhmojfecjfmbdpchihbeilohgnbdci
From the Chrome Web Store 🐨
CANCEL SAVE
8. Click on the drop down that currently says Allow Install
Cisco Umbrella Chromebook client (Ext)

9. Select Force Install.

jcdhmojfecjfmbdpchihbeilohgnbdci

This ensures that Chromebook users in the selected Organization Unit cannot remove or disable the extension.

Locally added



10. Select Save.

You have finished installing the Cisco Umbrella Chromebook client **extension**. Next proceed with the next section to install the Cisco Umbrella Chromebook client **application**.

			REVERT	SAVE	
> Apps & extens	sions		WHA	<u>T'S NEW</u>	
	USERS & BROWSERS	KIOSKS	MANAGED GUEST SESSIONS		
ID:	"jcdhmojfecjfmbdpchihbeilohgnbdci" 🔇		Cisco Umbrella Chromebook	ti ×	
CLE	AR FILTERS		Chrome Web Store options Include in Chrome Web Store collection Inherited from Google default		
Арр		Installation policy			
Allow L	isers to install other apps & extensions	Allow other apps & extensions from the Ch Inherited from Google default	Permissions and URL access		
	Cisco Umbrella Chromebook client (Ext) S jcdhmojfecjfmbdpchihbeilohgnbdci	Force install - Locally added	Use default permissions for this organization 🤝	r	
			Blocked hosts		

Part 3: Install the Cisco Umbrella Chromebook client Application

1. Log into <u>https://admin.google.com</u>.

	Google Admin	Q Search for users, gro	ups, and settings (e.g. setup N	1X records)	
Admi	n console				
					?
	Users	Company profile	Billing	Apps	Support
	Add, rename, and manage users	Update information about your company	View charges and manage licenses	Manage apps and their settings	Talk with our support team
		@	~		<u></u>
	Admin roles	Domains	Reports	Security	Groups
	Add new admins	Add domains or domain aliases	Track usage of services	Manage security features	Create groups and mailing lists

2. Select Devices.



Devices Secure corporate data on devices

3. In the Device Management window, select **Chrome Management**.

DEVICE SETTINGS

Networks

Chrome management

4. In the Chrome Management window, select **Apps & extensions**.

Chrome Management
Devices View and manage Chrome devices
Managed browsers View and manage Chrome browsers
User & browser settings Manage user-based settings on Chrome browsers and Chrome devices
Apps & extensions Manage Android apps and Chrome apps and extensions

5. On the left side, select the OU of the **Users** you want to deploy the application to, or the top level domain if you want to push it to everyone.


6. At the bottom right, click the Yellow + then click the icon that resembles a calculator.



7. Search for the ID of the Cisco Umbrella Chromebook client application **cpnjigmgeapagmdimmoenaghmhilodfg** then click **Save.**

(Searching by name will not work.)

Add Chrome app or extension by ID

Chrome apps and extensions can also be added by specifying the ID. If it is outside the Chrome Web Store, you must also specify the URL where the extension is hosted.

Extension ID

cpnjigmgeapagmdimmoenaghmhilodfg

From the Chrome Web Store 📼

CANCEL SAVE

8. Click on the drop down that currently says Allow Install



9. Select Force Install.

This ensures that Chromebook users in the selected Organization Unit cannot remove or disable the extension.



10. Paste the contents of the perviously saved json file in the Policy for extensions box

Cisco Umbrella Chromebook client (App) Scpnjigmgeapagmdimmoenaghmhilodfg	Force install Locally added	Ŧ	Use default permissions for this organization 🔍
			Blocked hosts
			One per line
			One per line; allowed hosts override blocked hosts Inherited from Google default
			Policy for extensions
			{"googleDirectoryService": {"Value":True},"organizationInfo":{"Value": {"organizationId":2290882,"regToken":"kBCTNrrRer Qep8ia49EgAbLURODxKXn"}},"publicSession": {"Value":false},"valPs":{"Value":["192.168.100.10", "192.168.100.11"]}}

11. Select Save. You have finished installing the Cisco Umbrella Chromebook client Application

		REVERT	SAVE
			WHAT'S NEW
ERS & BROWSERS	KIOSKS	MANAGED GUEST SES	SIONS
apagmdimmoenaghmhilodfg" (8	Elsco Umbrella Chromebook client (App)	
		Chrome Web Store options	
	Installation policy	Include in Chrome Web Store collection Inherited from Google default	
all other anns & extensions	Allow other apps & extensions from the C		
	Inherited from Google default	Permissions and URL access	
valle Obromohook client (App)	Force install		

Installation Caveats

It can take Google four to eight hours to push the Cisco Umbrella Chromebook client to all of your Chromebooks. The Chromebooks must be connected and logged in for the installation to take place.

After the client is installed in a Chromebook, allow a few hours for Chromebook traffic to begin to appear in your Umbrella dashboard.

Apply Policies

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

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

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.

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

⊜	cisco	Policies / Management All Policies o				Add Test
					Sorted by	Order of Enforcement
1	Default	Policy	Applied To All Identities	Contains 3 Policy Settings	Last Modified Nov 1, 2017	~

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

What would you like to protect?

Select	Identities						
Searc	Search Identities						
	AD Computers						
□ ♣	Networks						
	Roaming Computers	3 >					
0 9	Sites	1>					
08	Network Devices	Expand to select specific Chromebook users					
	Mobile Devices						
0	Chromebook User	10>					
	GSuite Users						

All Identities

3. Click Next.

k

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.**

 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.

Apply Destination Lists

Lists of destinations that can be explicitly blocked or allowed for any identities using this policy.

V	Enat Gain	Ie Intelligent Proxy usibility into threats, cor ent, or apps by proxying web connections for risky domains.
		SL Decryption Enabling SSL decryption allows the intelligent proxy to inspect traffic over HTTPS and block custom URLs in destination lists.
		Turning on SSL decryption allows HTTPS URL blocking.
		Enable IP-Layer Enforcement Gain visibility into threats that bypass DNS lookups by tunneling suspect IP connections. Note: this is only available for Roaming Computer identities.
AF	SEARCH	
	Enforce :	SafeSearch SafeSearch for queries sent to supported search engines Learn More
LL	W-ONLY	MODE
0	Allow In this	v-Only Mode s mode, access to sites needs to be specifically granted; otherwise connections will be blocked by default.
06	SING	
0	Log All I	lequests
0	Log Only Log and i	/ Security Events eport on only those requests that match a security filter or integration, with no reporting on other requests.
0		

- 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.
- Click Next. The Custom block page, Bypass Users, and Bypass Codes features on this page are not yet supported by the Chromebook client.

Set Block Page Settings

Define the appearance and bypass options for your block pages.

۲	Use Umbrella's Default Appearance Preview Block Page »	e			
0	Use a Custom Appearance				
	Choose an existing appearance	~			
Curre	ently unsupported				
В	YPASS USERS				
в	YPASS CODES				

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

Policy Summary

ſ	Policy Name		
I	Chromebook Policy		
	10 Identities & ffected 10 Chromebook Users Edit	2 Destination Lists Enforced 1 Block List 1 Allow List Edit	
	 Security Setting Applied: Default Settings Command and Control Calibacks, Malware, and Phishing Attacks will be blocked No integration is enabled. Edit Disable 	File Inspection Not Enabled Requires Intelligent Proxy	
	 Content Setting Applied: High Blocks adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters. Edit Disable 	Umbrella Default Block Page Applied Edit Preview Block Page	
	ADVANCED SETTINGS		
		CANCEL PREVIOUS	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 Chromebookspecific policy and all devices on your network (that are not Chromebooks) are protected by your Network Access policy.

		CED .		Sorted by Order of Enforceme		
1	Chromebook Policy	Applied To 10 Identities	Contains 3 Policy Settings	Last Modified Aug 28, 2018	~	
2	Network Access Policy	Applied To 0 Identities	Contains 3 Policy Settings	Last Modified Aug 28, 2018	~	

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

Deploy the G Suite Identity Service

The G Suite identity service feature is an enhancement to the Cisco Umbrella Chromebook client and adds the Organizational Unit (OU)-based Umbrella policy enforcement capabilities. For overview information, refer to <u>Umbrella for G Suite Identity Service</u>.

Enabling the G Suite Identity Service

Enabling the G Suite identity service for the Cisco Umbrella Chromebook client requires two steps:

- Install the Cisco Umbrella Authorizer marketplace app.
- Enter the G Suite account super administrator ID in the Cisco Umbrella dashboard.

Install the Cisco Umbrella Authorizer App

The *Cisco Umbrella Authorizer* marketplace application authorizes the scopes needed by Umbrella to retrieve information from your G Suite account. Follow these steps to install the app in your Google administration console:

- 1. Open your G Suite administration console, using the super administrator ID.
- 2. <u>Navigate to the app</u> in the Google marketplace.

≡ G Suite Marketplace	Q Search apps	
Business Tools Accounting & Finance Administration & Management ERP & Logistics	Cisco Umbrella Authorizer Cisco Authorization application for granting access to Cisco Umbrella Cloud system. Cisco Umbrella ******* (9) 48 users UNAVAILABLE FOR INDIVIDUAL INSTALL	
HR & Legal Marketing & Analytics Sales & CRM	Cisco Uniformita Instance Hangement Image: Hangement Image: Hangement Krists Anderson Policy (List) Image: Hangement	
Productivity Creative Tools Web Development Office Applications Task Management Education Academic Resources	Margine	
Teacher & Admin Tools Communication Utilities	Model Image: Second S	
Recommended for G Suite Works with Google Drive	'Cisco Umbrella Authorization' application for GSuite admins provides authorization for fetching identity information into Cisco Umbrella Cloud system. Once authorized the customer can login into Cisco Umbrella Cloud system to create user and orgunit level security policies Reviews English + Recent +	

3. Click Domain Install, then in the dialog that appears, click Accept

Google		0
	Cisco Umbrella Authorizer You are granting Cisco Umbrella Authorizer the right to access your domain data:	
	View domains related to your customers	
	View organization units on your domain	
	View users on your domain	
	Turn ON for :	
	-	
	I agree to the application's Terms of Service, Privacy Policy and G Suite Marketplace Terms of Service	
	Cancel Accept	

Enter your G Suite super administrator ID in the Umbrella Dashboard

- 1. In Cisco Umbrella, navigate to **Deployments > Chromebook Users**.
- 2. Click **Configure**. The Configure Chromebook Umbrella Clients window appears.

Configure Umbrella Chromebook Clients

Protecting Chromebook Computers

Enable Umbrella security for your Chromebooks by installing the Chromebook client Extension and App. You configure the Umbrella App by using the Google Admin Console to upload this data file

1. Download your organization's configuration file from the link below:

chromebookconfig.json (Size ~0.1 kB)

2. Install the Chromebook client software (Extension and App) by following the Chrome Setup Guide.

3. Sign in with super admin email id of your Google Admin Console to sync GSuite identities into Umbrella.

SUPER ADMIN SIGN IN

3. Click Super Admin Sign In. In the window that appears, choose the super administrator account:



(i) ▲ https://accounts.google.com/signin/oauth/oauthchooseaccount?c ··· ♥

G Sign in with Google



Choose an account

to continue to Cisco Umbrella Authorizer

The beam of the second secon

To continue, Google will share your name, email address, language preference, and profile picture with Cisco Umbrella Authorizer. Before using this app, you can review Cisco Umbrella Authorizer's **privacy policy** and **terms of service**.

English (United States) 🔻

Help Privacy Terms

公

4. Sign in to sync your G Suite identities with Cisco Umbrella. This can take up to 15 minutes.

The Umbrella Policies page displays two new containers: G Suite OUs and G Suite Users

REMEMBER! To add your G Suite OU's and Users to the correct policy or they will get the bottom default policy!

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**.

All organizations <		+	1 use	r selected X	
O Users from all organizational units	-		+ Add a filter		
 Users from selected organizational 	units			Name 🛧	
Search for organizational units				•	
•			✓	Alexander TSEDemo	
				•	
				•	

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

		REVERT
ops & extensions		WHAT'S NEW
USERS & BROWSERS	KIOSKS	MANAGED GUEST SESSIONS
+ Search or add a filter		Cisco Umbrella Chromebook client (Ext)
Арр	Installation policy	Chrome Web Store options
Allow users to install other apps & extensions	Allow other apps & extensions from the C Inherited from Google default	Include in Chrome Web Store collection
Cisco Umbrella Chromebook client (App) e cpnjigmgeapagmdimmoenaghmhilodfg	Force install Locally added	Permissions and URL access
Cisco Umbrella Chromebook client (Ext) c jcdhmojfecjfmbdpchihbeilohgnbdci	Force install Locally added	Blocked hosts

Roaming Client Setup

Windows/Mac OS

If you have Windows or MacOS devices that you would like to protect when they go offsite then you can download the roaming client for them. Navigate to Deployments->Roaming Computers and click on the Roaming Client download icon in the top right-hand corner. Then, download and install the client that pertains to that OS.



For more documentation and prerequisites please click here.

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

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**.

Orga	inization Administrator's Email Address	in the Cisco Security
Conn	ector app and send these reports to the administrator.	in the clace decunty
em	ail@admin.com	
User	Notifications	
Adjus	st level of notifications shown to users on their device	
0	None	
0	Notify on Protection Failure	
0	Notify on Protection Change	
Devi	ce Identification	
Choo	se whether to display device name or anonymize with	serial number only.
Fu	III Identification	~

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.

	Cisco Meraki
cisco Meraki	Link MDM
4	Apple
	Download MobileConfig
	IBM Maas360
BM MaaS360 Ittee	Download MobileConfig
	Microsoft Intune
IVIICTOSOT	Download MobileConfig
	Jamf
Jann	Download MobileConfig
	MobiConnect
mobiconnect	Download MobileConfig
Mahilakan	MobileIron
Inoplication	Download MobileConfig
	Workspace ONE
-	Download MobileConfig

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

alialia cisco	Deployments / Core Identities Mobile Devices			Settings	Manage MDMs
Label	Serial Number	Last Sync	OS Version	App Version	Mdm
WJC	C8PVV3JWJC6	2018	iOS 11.2	0.0.0	

 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.



<u>Jamf</u>

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 <u>Anonymize</u> <u>Devices</u>.

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 <u>supervised mode</u>.
- Your iOS device must be managed by Jamf and Apple School Manager or Apple Business Manager.
- You have <u>added an administrator email address</u>.
 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, <u>Anonymize Devices</u>.
- 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.

Manage MDMs Add or manage devices using the MDM of your choice.					
diala cisco Meraki	Cisco Meraki Link MDM				
Ú	Apple Download MobileConfig				
IBM MaaS360 III	IBM Maas360 Download MobileConfig				
Microsoft	Microsoft Intune Download MobileConfig				
🋂 jamf	Jamf 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.

ganization Administrator's Email Address		
s email is for end users to generate problem reports within the Cisco Security Connector a ministrator.	app and send the	se reports to the
dmin@example.com		
	CANCEL	DOWNLOAD

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

• <u>XML</u>

xml version="1.0" encoding="UTF-8"?
plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-</td
1.0.dtd">
<pre><plist version="1.0"></plist></pre>
<pre><dict></dict></pre>
<pre><key>PayloadContent</key></pre>
<pre>lamf - conv from here to paste into the lamf UI to provision a DNS provy></pre>
copy from here to paste fitto the same of to provision a bits proxy / cdicts
•••••
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</th <th>n="1.0" encoding="UTF-8"?></th>	n="1.0" encoding="UTF-8"?>
pl:</td <td>ist PUBLIC "-//Ápple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/</td>	ist PUBLIC "-//Ápple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
PropertyList-	-1.0.dtd">
<plist td="" version<=""><td>on="1.0"></td></plist>	on="1.0">
<dict></dict>	
<kev:< td=""><td>PavloadContent</td></kev:<>	PavloadContent
<arr< td=""><td>3V></td></arr<>	3V>
	dict>
	<kev>AppBundleIdentifier</kev>
	<string>com.cisco.ciscosecurity.app</string>
	<key>PayloadDescription</key>
	<string>Cisco Umbrella</string>
	<key>PayloadDisplayName</key>
	<string>Cisco Umbrella</string>
	<key>PayloadIdentifier</key>
	<pre><string>com.apple.dnsProxy.managed.DBE2A157_E134_3E8C_B4FB-23EDF48A0CD1<!--/pre--></string></pre>
string>	
	<key>PayloadType</key>
	<string>com.apple.dnsProxy.managed</string>
	<key>PayloadUUID</key>
	<pre><string>E5D191FD-6E01-4733-9720-E27BFBCB8DC5</string></pre>
	<key>PayloadVersion</key>
	<integer>1</integer>
	<key>ProviderBundleIdentifier</key>
	<string>com.cisco.ciscosecurity.app.CiscoUmbrella</string>
	<key>ProviderConfiguration</key>
Jamf - (</td <td>copy from here to paste into the Jamf UI to provision a DNS proxy> <pre><dict></dict></pre></td>	copy from here to paste into the Jamf UI to provision a DNS proxy> <pre><dict></dict></pre>
	<key>anonymizationLevel</key> <integer>0</integer>



Mosyle

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

earch	Media Type Category		
Q cisco umbrella	IOS Apps V All	✓ Search	
urchase Details		Price	Quantity
Cisco Security Connector by Cisco		Free iOS App	2
			20

- 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 <u>Anonymize Devices</u>), 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.

cisco Deployments MODILE	Core Identities			Setting	S Manage MDMs
Label	Serial Number	Last Sync	OS Version	App Version	Mdm
C8PVV3JWJC6	C8PVV3JWJC6	2018	IOS 11.2	0.0.0	

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 <u>Apply Umbrella Policies</u>.

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.

Deployments / Core Identities



A network may be a single public IP address (static or dynamic) or a range of public IP addresses, depending on the size of your network. Add a network to Umbrella to extend protection to any device that connects to the internet from behind that network's IP space. The public IP of your network is XXX.XXX.XX

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.

Cisco Umbrella	e inf		ants / Core Identities			
Overview						Add
Deployments 🗸 🗸						
Core Identities		۹ Search with a n	etwork name or IP address		Advanced 🗸	
Networks						
Network Devices		Name 🔺	IP Address	Dynamic	Primary Policy	Status
Roaming Computers		DIS-Public				Active

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.

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.

IPv4:	208.67.22	0.220 an	d 208.67.23	22.222			
IPv6:	2620:119	35::35 ar	nd 2620:119	9:53::5	3		
Netwo	rk Name						
\bigcirc	IPv4 only	0	IPv6 only		0	Mixed I	Pv4 & IPv6
Pv4 Ad	ddress						
000	0			1	32		V

- 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. <u>Change DNS to 208.67.222.222 and 208.67.220.220</u> Example for Verizon Orbic Hotspot:

RSD VZ Hotspot Orbic				
	DETAILS ASSIGNMENTS			2
N	Name RSD VZ Hotspot Orbic	Save Export Cancel	Delete	
F	Fields marked with an asterisk* are optional. If left empty or selection	on is "Not Managed", the existing value on the device will be used.		
	Wi-Fi		>	
	Security		>	
	Advanced		v	
	Mac Filter			
	MAC Filter Enabled	No 🗸		
	Add User's Device's Wi-Fi MAC Addresses	No 🗸		
	Add Wi-Fi MAC Addresses for Matching User Property	None 🗸		
	White Listed MAC Address			
	Blocked MAC Address			
	240 Quittan			
	Divs Settings			
	Manual DNS Enabled	Yes V		
	Manual DNS Address 1	208.67.222.222		
	Manual DNS Address 2	208.67.220.220		
	RFC1918 Private IP Address Ranges	Disabled 🗸		
	Loopback Address Range Included	Excluded V		

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:

Search with a network name or I	Paddress Advanced V			
Name 🔺	IP Address	Dynamic	Primary Policy	Status
DIS-Public			Default Policy	Activ
VZ-MiFi-63.46.50.221			Default Policy	Verify

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/.



Appendex:

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 youthendangering 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 proanorexia 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:

Extensions	× New Tab	×
$\leftrightarrow \rightarrow \mathbf{C}$ \square localhost:8029/debug		
🗅 localhost:8029/debug	- Cisco Umbrella Chrome	ebook client debug information
Q localhost:8029/debug -	Google Search	

→ C \$C	isco Umbrella Chromebook client	(Ext) chrome-e	extension://aekhbkcdcfgohgcafdpkjjlbkhdlhnok/debug.html?os=cros&osVer	7	
Cisco Umbrella Chromebook client					
	Debug Info. collected at: Mon Sep 03 2018 15:44:15 GMT+0530 (India Standard Time)				
		OS	cros		
		OS Version	68.0.3440.106		
		Organization ID	2442562		
		User Email	Next Advanced Los A		
		Local IP	10.103.10.124		
		Policy Url	https://dashboard.umbrella.com/o/2442562/#/configuration/policy/382835		

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.

<u>Logs</u>

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
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