

Cisco Umbrella



Have you completed your Weatec application?
If not, contact your deacon for an application before continuing
to setup this Weatec approved filter!

Who is it for?

Cisco Umbrella is a DNS level filter that is great as security defense as well as a web filter.

Pros:

- One point of management for the whole network.
- Has the option to integrate with a domain
- Can enforce Google Safe Search
- Work well with software that require security such as auto diagnostic software.
- Very easy to install
- Blocks Ransomware, Malware, Phishing and C2 Callbacks

Cons:

- Price

Note: After testing, Cisco Umbrella has been approved as an acceptable content filter according to the requirements set forth in the *Weaverland Conference Electronic Technology Usage Guidelines*. Please remember that no filter can be guaranteed to filter out all objectionable content; therefore the Weatec Accountability Software must be installed on all devices in order to be in compliance with Weaverland Conference guidelines. The accountability software logs all web traffic, thus fostering brotherhood accountability. So even if objectionable content is missed by Cisco Umbrella, the content will still trigger a flag on the accountability server. Use the Weaverland Conference template as a minimum; there is nothing preventing you from choosing stricter settings.

How to Acquire

Find more details at <https://umbrella.cisco.com/products/packages/>

To ask questions, learn current pricing, or get started with Cisco,

Contact page: <https://umbrella.cisco.com/contact-us>

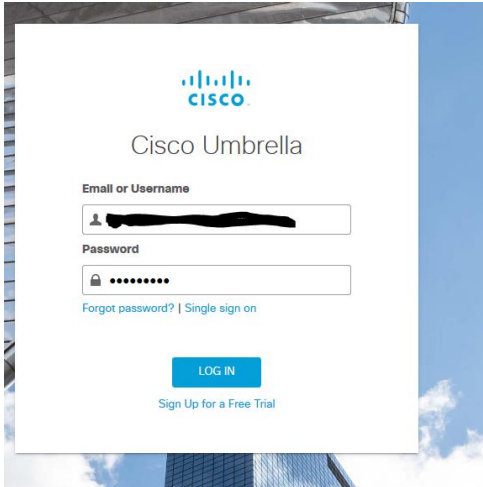
How to Install

Work with Cisco or your local IT provider to install.

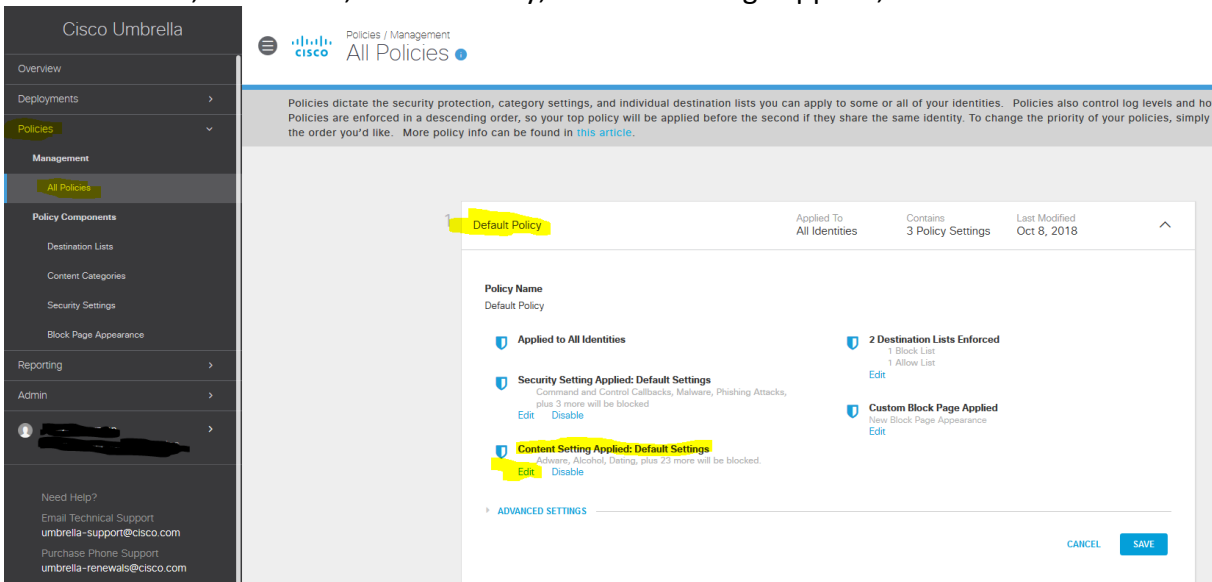
Documents <https://docs.umbrella.com/deployment-umbrella/docs>

How to Configure

Login:



Got to Policies, All Policies, Default Policy, Content Settings Applied, and click edit



Select Custom and check off the categories to be blocked. Using the Weatec guidelines

Default Policy Applied To All Identities Contains 3 Policy Settings Last Modified Oct 8, 2018

Limit Content Access

Access to these sites will be restricted based on the type of content served by the pages of the site. For more information about categories, [click here](#)

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

Moderate
Blocks all adult-related websites and illegal activity.

Low
Blocks pornography.

Custom
Create a custom grouping of category types.

Custom Setting

Default Settings

CATEGORIES TO BLOCK [SELECT ALL](#)

<input checked="" type="checkbox"/> Academic Fraud	<input checked="" type="checkbox"/> Adult Themes
<input checked="" type="checkbox"/> Adware	<input checked="" type="checkbox"/> Alcohol
<input checked="" type="checkbox"/> Anime / Manga / Webcomic	<input checked="" type="checkbox"/> Arts
<input checked="" type="checkbox"/> Astrology	<input type="checkbox"/> Auctions
<input type="checkbox"/> Automotive	<input checked="" type="checkbox"/> Blogs
<input type="checkbox"/> Business Services	<input checked="" type="checkbox"/> Chat
<input type="checkbox"/> Classifieds	<input type="checkbox"/> Computer Security
<input checked="" type="checkbox"/> Dating	<input checked="" type="checkbox"/> Digital Postcards
<input type="checkbox"/> Dining and Drinking	<input type="checkbox"/> DIY Projects
<input checked="" type="checkbox"/> Drugs	<input checked="" type="checkbox"/> Dynamic and Residential
<input type="checkbox"/> Ecommerce / Shopping	<input type="checkbox"/> Educational Institutions
<input checked="" type="checkbox"/> Fashion	<input type="checkbox"/> File Storage

[CANCEL](#) [SET & RETURN](#)

When complete click **Set& Return**

You are also able to check a custom Block or allow list

Under the policy click edit on the destination list and you are then able to create allow or block list that can be applied to the all policies are just certain users.

You should also turn on all the security settings

1 Default Policy Applied To All Identities Contains 3 Policy Settings Last Modified Oct 8, 2018

Policy Name
Default Policy

Applied to All Identities

Security Setting Applied: Default Settings
Command and Control Callbacks, Malware, Phishing Attacks, plus 4 more will be blocked
[Edit](#) [Disable](#)

Content Setting Applied: Default Settings
Adware, Alcohol, Dating, plus 23 more will be blocked.
[Edit](#) [Disable](#)

2 Destination Lists Enforced
1 Block List
1 Allow List
[Edit](#)

Custom Block Page Applied
New Block Page Appearance
[Edit](#)

[ADVANCED SETTINGS](#)

[CANCEL](#) [SAVE](#)

Security Settings

Ensure identities using this policy are protected by selecting or creating a security setting. Click Edit Setting to make changes to any existing settings, or select Add New Setting from the dropdown menu.

Default Settings ▾

CATEGORIES TO BLOCK [EDIT](#)



Malware

Websites and other servers that host malicious software, drive-by downloads/exploits, mobile threats and more.



Newly Seen Domains

Domains that have become active very recently. These are often used in new attacks.



Command and Control Callbacks

Prevent compromised devices from communicating with attackers' 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

CANCEL

SET & RETURN

How to Get Help

Contact Cisco

Online: <https://umbrella.cisco.com/contact-us>

Email umbrella-support@cisco.com

Or

Contact the Weatec Helpdesk:

Phone: (717) 723-8978

Email: helpdesk@weatec.com