Configure URL Filtering

For supported software information, click here.

With URL filtering, you create filters that prevent access to specific URLs, thus allowing you to control web-browsing activity within an organization. Uncontrolled access to internet websites can expose an organization to security risks, such as threat propagation, loss of data, and lack of compliance.

You use URL filtering in conjunction with application objects and next-generation firewall (NGFW) to identify and control access to HTTP and HTTPS websites. You can associate URL-filtering profiles with security policies, and you can use URL categories as match criteria in access policies to gain visibility and control of the traffic that traverses the NGFW.

Versa Operating System^{TM} (VOS^{TM}) devices categorize and continuously update URL information, including URL categories and a reputations. VOS devices create a local database that can store up to 20 million URLs. In addition, Versa supports a cloud-based URL database that contains more than 31 billion URLs. You can configure real-time cloud lookup to determine URL categories and reputations in the cloud-based URL database.

VOS devices classify URLs into 82 predefined categories, and you can create custom URL categories and associate them with reputations. You use both predefined and custom URL categories to create policies that restrict access to websites based on the URL's category and reputation.

You can also define URL deny lists and allow lists, and you can create policies that restrict access to websites based on those lists.

As part of URL-filtering policy enforcement, you can redirect users to captive portal pages.

View and Configure URL Categories

VOS devices support a wide-range of predefined URL categories that you can apply in different types of security policies. You can look up URL categories in the database of predefined URLs to determine the category and reputation associated with the URL. The predefined URL database is updated (either daily or in real time) by means of security package (SPack) updates. For more information, see Use Security Packages.

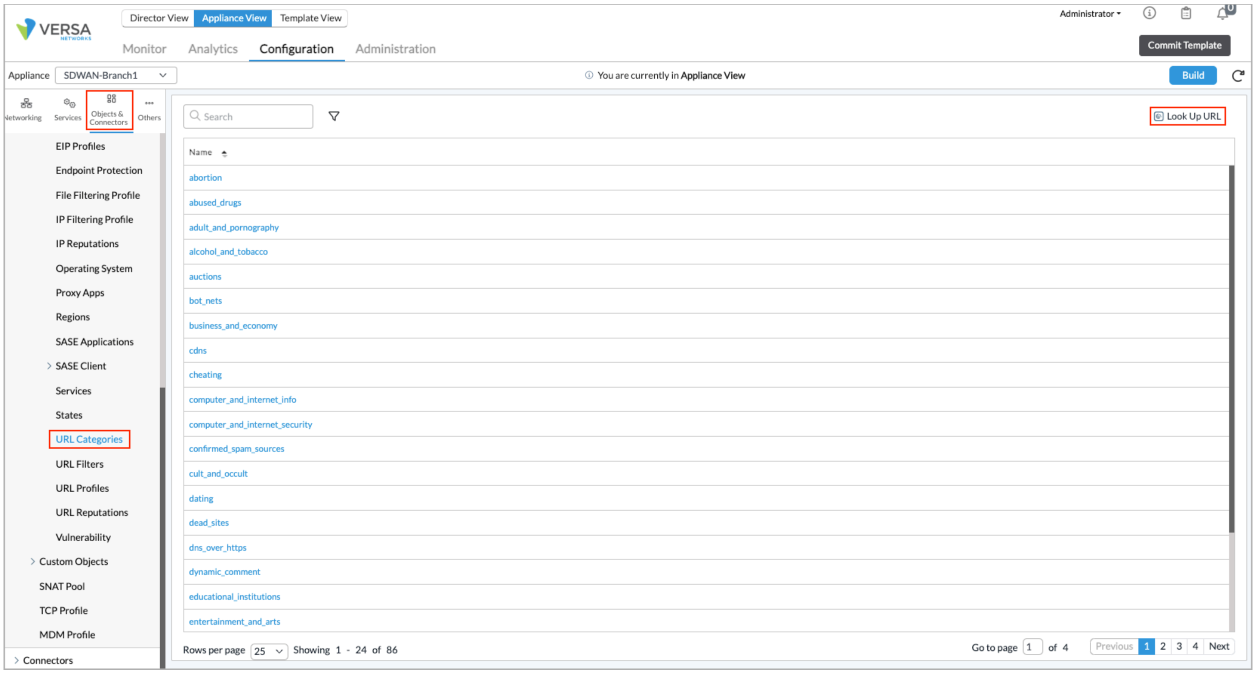
You can configure NGFW policy rules based on predefined and custom URL categories. You can create URL policy rules for both match and action criteria.

View Predefined URL Categories

You can view the predefined URL categories and reputation in the VOS device's URL database. The table at the end of this section lists the predefined URL categories that are currently supported.

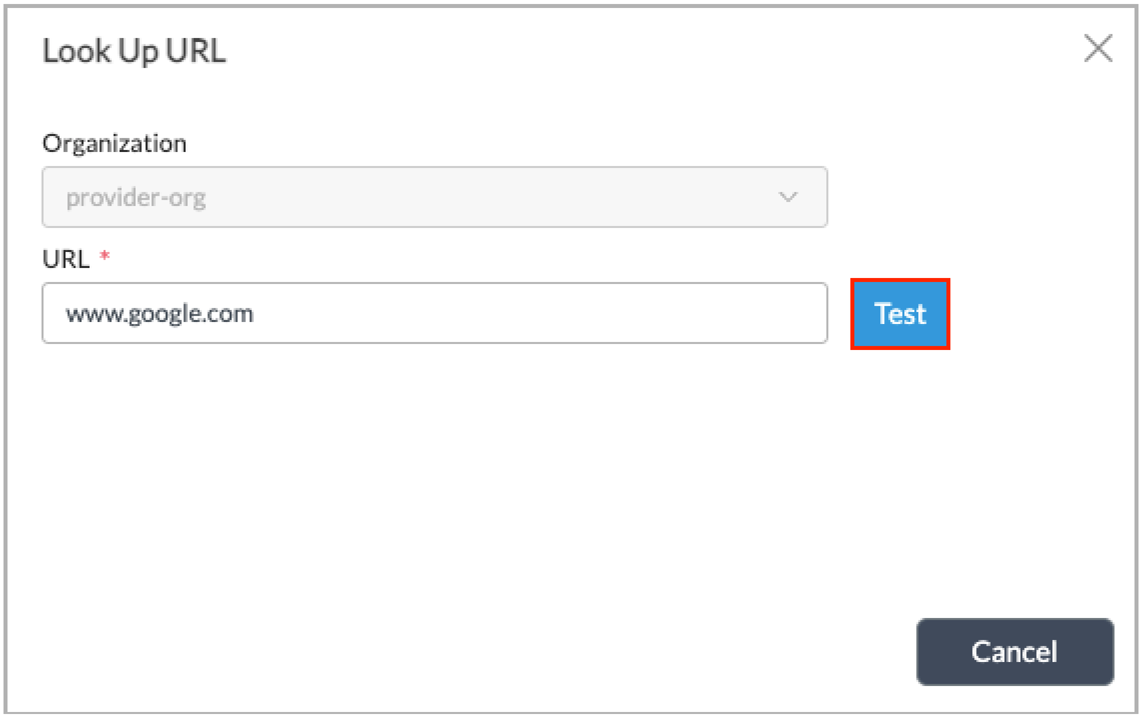
To view the predefined URL categories:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Predefined > URL Categories in the left menu bar. The main pane displays a list of URL categories.



Name
abortion
abused_drugs
adult_and_pornography
alcohol_and_tobacco
auctions
bot_nets
business_and_economy
cdns
cheating
computer_and_internet_info
computer_and_internet_security
confirmed_spam_sources
cult_and_occult
dating
dead_sites
dns_over_https
dynamic_comment
educational_institutions
entertainment_and_arts

4. Click the Look Up URL icon to display more information about a specific URL. In the Look Up URL popup window, enter information for the following fields.



Look Up URL

Organization

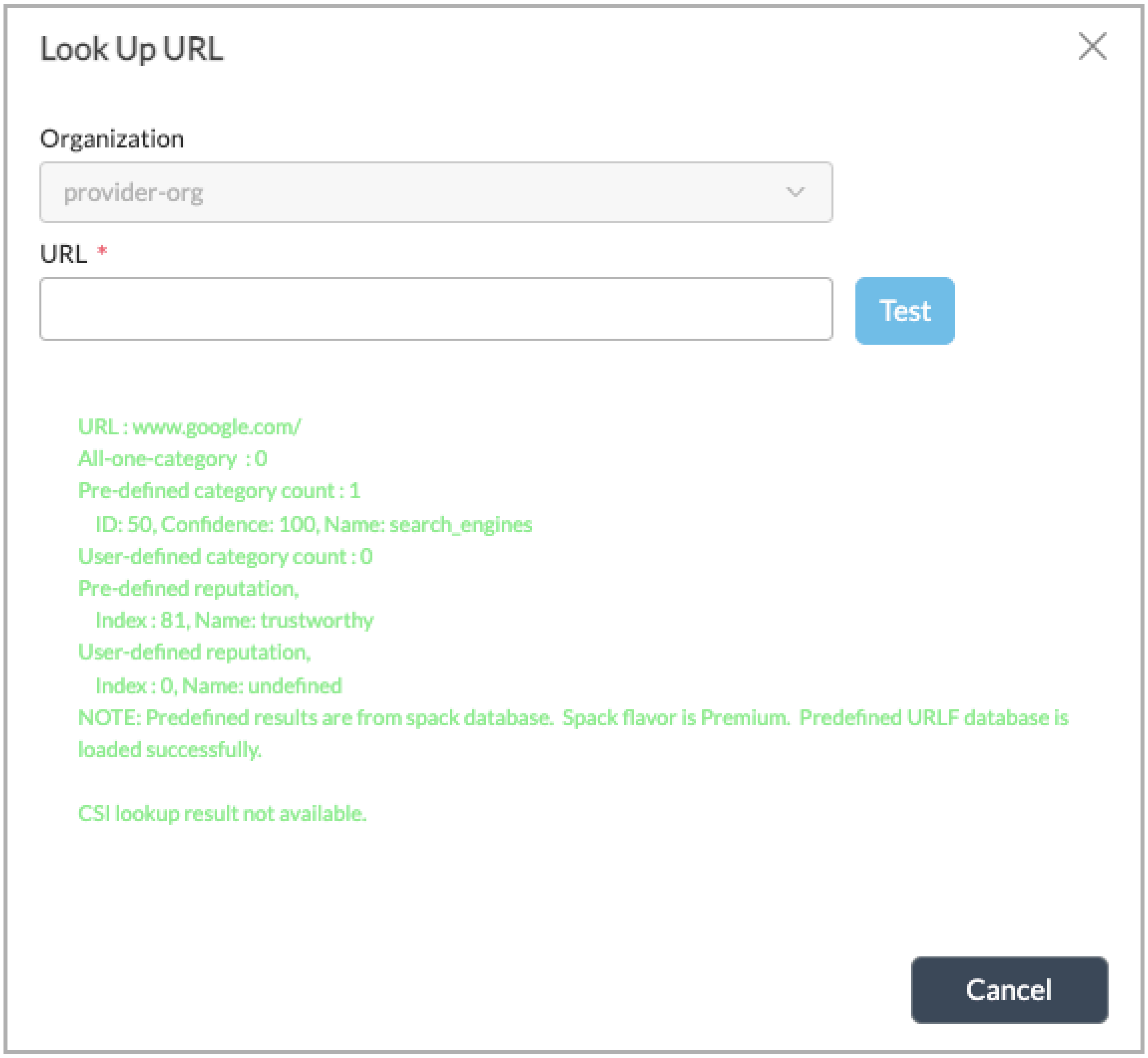
provider-org

URL *

www.google.com

Field	Description
Organization	Select the organization for which you want to look up the URL category.
URL	Enter a URL that you want to look up its URL category. For example, www.google.com.

5. Click Test. The Look Up URL popup window displays information about the URL, including its predefined category and reputation. For example:



```
URL : www.google.com/
All-one-category  : 0
Pre-defined category count : 1
   ID: 50, Confidence: 100, Name: search_engines
User-defined category count : 0
Pre-defined reputation,
   Index : 81, Name: trustworthy
User-defined reputation,
   Index : 0, Name: undefined
NOTE: Predefined results are from spack database.  Spack flavor is Premium.  Predefined URLF database is
loaded successfully.

CSI lookup result not available.
```

6. Click Cancel.

The following table lists the predefined URL categories that the VOS software currently supports.

Category Name	Description
Abortion	Abortion topics, either prolife or prochoice. Examples of websites that fall into this category: http://abortion.procon.org, http://www.nafcanada.org.
Abused Drugs	Discussion or remedies for illegal, illicit, or other commonly abused drugs such as heroin, cocaine, and other street drugs. Information about legal highs, including glue sniffing, misuse of prescription drugs, and abuse of other legal substances. Examples of websites that fall into this category: http://shroomery.org, http://passyourdrugtest.com.
Adult and Pornography	Sexually explicit material for the purpose of arousing a sexual or prurient interest. Adult products including sex toys, CD-ROMs, and videos. Online groups, including newsgroups and forums, that are sexually explicit in nature. Erotic stories and textual descriptions of sexual acts. Adult services including videoconferencing, escort services, and strip clubs. Sexually explicit art. Examples of websites that fall into this category: http://playboy.com, http://union.fr.
Alcohol and Tobacco	Sites that provide information about, promote, or support the sale of alcoholic beverages or tobacco products and associated paraphernalia. Examples of websites that fall into this category: http://thompsoncigar.com, http://wineinsiders.com.
Auctions	Sites that support the offering and purchasing of goods between individuals as their main purpose. Does not include classified advertisements. Examples of websites that fall into this category: http://ebay.com, http://quibids.com.
Bot Nets	URLs, typically IP addresses, that are determined to be part of a bot network, from which network attacks are

	launched. Attacks may include spam messages, denial of service (DoS), SQL injections, proxy jacking, and other unsolicited contacts.
Business and Economy	Business firms, corporate websites, business information, economics, marketing, management, and entrepreneurship. Examples of websites that fall into this category: http://samsung.com, http://ups.com.
Cheating	Sites that support cheating and plagiarism and that contain related materials, including free essays, and exam copies. Examples of websites that fall into this category: http://essaymania.com, http://echeat.com.
Computer and Internet Info	General computer and internet sites, and technical information. SaaS sites and other URLs that deliver internet services. Examples of websites that fall into this category: http://ranking.com, http://system.netsuite.com.
Computer and Internet Security	Computer security and internet security, and security discussion groups. Examples of websites that fall into this category: http://siteadvisor.com, http://webroot.com.
Content Delivery Networks	Delivery of content and data for third parties, including ads, media, files, images, and video. Examples of websites that fall into this category: http://metacdn.com, http://edgestream.com.
Cult and Occult	Methods, means of instruction, or other resources to interpret, affect, or influence real events through the use of astrology, spells, curses, magic powers, satanic or supernatural beings. Includes horoscope sites. Examples of websites that fall into this category: http://horoscopes.com, http://astronet.hu.
Dating	Dating websites focused on establishing personal relationships. Examples of websites that fall into this

	category: http://eharmony.com, http://christianmingle.com.
Dead Sites	Sites that do not respond to http queries. Policy engines should usually treat these as uncategorized sites. Examples of websites that fall into this category: http://g00gle.com, http://whitehouse.info.
DNS over HTTPS	Known DNS Over HTTPs (DoH) providers and domains. Examples of websites that fall into this category: https://cloudflare-dns.com and https://doh.opendns.com.
Dynamically Generated Content	Domains that generate content dynamically based on arguments to their URLs or other information (such as geolocation) on incoming web requests.
Educational Institutions	Preschool, elementary, secondary, high school, college, university, and vocational schools and other educational content and information, including enrollment, tuition, and syllabi. Examples of websites that fall into this category: http://mit.edu, http://ucsd.edu, http://www.carlsbadusd.k12.ca.us/.
Entertainment and Arts	Motion pictures, videos, television, music and programming guides, books, comics, movie theaters, galleries, artists, or reviews about entertainment. Performing arts, such as theater, vaudeville, opera, and symphonies. Museums, galleries, and art or artist sites, such as sculpture and photography. Examples of websites that fall into this category: http://eonline.com, http://highlightgallery.com.
Fashion and Beauty	Fashion or glamour magazines, beauty, clothes, cosmetics, style. Examples of websites that fall into this category: http://visionmodels.co.uk/, http://genejuarez.com.
Financial Services	Banking services and other types of financial information,

	such as loans, accountancy, actuaries, banks, mortgages, and general insurance companies. Does not include sites that offer market information, or brokerage or trading services. Examples of websites that fall into this category: http://firstpremierbankcards.com, http://paypal.com.
Gambling	Gambling or lottery web sites that invite the use of real or virtual money. Information or advice for placing wagers, participating in lotteries, gambling, or running numbers. Virtual casinos and offshore gambling ventures. Sports picks and betting pools. Virtual sports and fantasy leagues that offer large rewards or request significant wagers. Note that hotel and resort sites that do not enable gambling on the site are categorized in Travel or Local Information. Examples of websites that fall into this category: http://www.powerball.com/pb_home.asp, http://www.zjlottery.com.
Games	Game playing or downloading, video games, computer games, electronic games, tips, and advice about games or how to obtain cheat codes. Sites dedicated to selling board games, andjournals and magazines dedicated to game playing. sites that support or host online sweepstakes and giveaways. Fantasy sports sites that also host games or game playing. Examples of websites that fall into this category: http://duowan.com, http://ubi.com.
Generative AI	Artificial intelligence tools and systems that are used to generate new text, images, video, audio, code, or other types of synthetic data. Examples of websites that fall into this category: https://bard.google.com and https://chat.openai.com/chat.
Government	Information about government, government agencies, and government services such as taxation, public services, and emergency services. Sites that discuss or explain laws of various governmental entities. Local, county, state, and national government sites. Examples

	of websites that fall into this category: http://www.nasa.gov, http://premier-ministre.gouv.fr.
Gross	Vomit and other bodily functions, bloody clothing, and so forth. Examples of websites that fall into this category: http://ratemyvomit.com, http://bloody-disgusting.com.
Hacking	Illegal or questionable access to or use of communications equipment or software. Development and distribution of programs that may allow compromising of networks and systems. Avoidance of licensing and fees for computer programs and other systems. Examples of websites that fall into this category: http://hackplayers.com, http://hackforums.net.
Hate and Racism	Sites that contain content and language in support of hate crimes and racism such as Nazi, neo-Nazi, and Ku Klux Klan. Examples of websites that fall into this category: http://nazi-lauck-nsdapao.com/, http://americannaziparty.com/, http://kkk.com/.
Health and Medicine	General health, fitness, and well-being, including traditional and non-traditional methods and topics. Medical information about ailments and various conditions, dentistry, psychiatry, optometry, and other specialties. Hospitals and medical offices. Medical insurance. Cosmetic surgery. Examples of websites that fall into this category: http://webmd.com, http://missionvalleymedical.com.
Home and Garden	Home issues and products, including maintenance, home safety, decor, cooking, gardening, home electronics, and design. Examples of websites that fall into this category: http://homedepot.com, http://waysidegardens.com.
Hunting and Fishing	Sport hunting, gun clubs, and fishing. Examples of

	websites that fall into this category: http://fishingworks.com, http://wildlifelicense.com.
Illegal	Criminal activity, how not to get caught, copyright and intellectual property violations. Examples of websites that fall into this category: http://newid.com, http://kidneykidney.com.
Image and Video Search	Photo and image searches, online photo albums and digital photo exchange, image hosting. Examples of websites that fall into this category: http://images.google.fr, http://gettyimages.com.
Individual Stock Advice and Tools	Promotion and facilitation of securities trading and management of investment assets. Information about financial investment strategies, quotes, and news. Examples of websites that fall into this category: http://stockstar.com, http://morningstar.com.
Internet Communications	Internet telephony, messaging, VoIP services and related businesses. Examples of websites that fall into this category: http://skype.com, http://www.chatib.com/.
Internet Portals	Web sites that aggregate a broader set of internet content and topics and that typically serve as the starting point for an end user. Examples of websites that fall into this category: http://yahoo.com, http://qq.com.
Job Search	Assistance in finding employment, tools for locating prospective employers, or employers looking for employees. Examples of websites that fall into this category: http://monster.com, http://51job.com.
Keyloggers and Monitoring	Downloads and discussion about software agents that track a user's keystrokes or monitor their web surfing habits. Examples of websites that fall into this category: http://keylogger.org, http://spy-tools-directory.com.

Kids	Sites designed specifically for children and teenagers. Examples of websites that fall into this category: http://www.mundogaturro.com, http://www.ri-ra.ie/.
Legal	Legal websites, law firms, discussions and analysis of legal issues. Examples of websites that fall into this category: http://www.pepperlaw.com, http://earlcaterlaw.com.
Local Information	City guides and tourist information, including restaurants, area and regional information, and local points of interest. Examples of websites that fall into this category: http://downtownlittlerock.com, http://sandiegorestaurants.com.
Low-THC Cannabis Products	Sites with content about low-THC, non-psychoactive products, including CBD oils, resin, extracts, herbs, capsules, supplements, foods, drinks, and toiletries/skin care products. Examples of websites that fall into this category: https://alwayspureorganics.com and https://directhemp.com.
Malware Sites	Malicious content, including executables, drive-by infection sites, malicious scripts, viruses, trojans, and code. For more information, see http://en.wikipedia.org/wiki/Malware.
Marijuana	Marijuana use, cultivation, history, culture, legal issues. Examples of websites that fall into this category: http://howtogrowmarijuana.com, http://cannaweed.com.
Military	Information about military branches, armed services, and military history. Examples of websites that fall into this category: http://defense.gov, http://goarmy.com.
Motor Vehicles	Car reviews, vehicle purchasing or sales tips, parts catalogs. Auto trading, photos, discussion about vehicles including motorcycles, boats, cars, trucks and RVs. Journals and magazines about vehicle modifications.

	Examples of websites that fall into this category: http://www.carmax.com, http://trade-a-plane.com.
Music	Music sales, distribution, streaming, information about musical groups and performances, lyrics, and the music business. Examples of websites that fall into this category: http://itunes.com, http://bandcamp.com.
News and Media	Current events or contemporary issues of the day. Radio stations and magazines, newspapers online, headline news sites, news wire services, personalized news services, and weather sites. Examples of websites that fall into this category: http://abcnews.go.com, http://newsoftheworld.co.uk.
Nudity	Nude or seminude depictions of the human body. These depictions are not necessarily sexual in intent or effect, but may include sites containing nude paintings or photo galleries of artistic nature. Nudist or naturist sites that contain pictures of nude individuals. Examples of websites that fall into this category: http://gorod.tomsk.ru/index-1221486260.php, http://www.pornomedia.com/extra/strange/wwbeauty.
Online Greeting Cards	Online greeting card sites. Examples of websites that fall into this category: http://123greetings.com, http://greeting-cards.com.
Parked Domains	URLs that host limited content or click-through ads that may generate revenue for the hosting entities but generally do not contain content useful to the end user. Under construction sites, folders, and web server default home pages. Examples of websites that fall into this category: http://000.com, http://buythisdomain.com.
Pay to Surf	Sites that pay users in the form of cash or prizes, for clicking on or reading specific links, email, or web pages.

	Examples of websites that fall into this category: http://cashcrate.com, http://inboxdollars.com.
Peer to Peer	Peer-to-peer clients and access. Torrents, music download programs. Examples of websites that fall into this category: http://mininova.org, http://bitcomet.com/.
Personal Sites and Blogs	Personal websites and blogs posted by individuals or groups. Examples of websites that fall into this category: http://blogger.com, http://wordpress.org.
Personal Storage	Online storage and posting of files, music, pictures, and other data. Examples of websites that fall into this category: http://box.net, http://freefilehosting.net.
Philosophy and Political Advocacy	Politics, philosophy, discussions, promotion of a particular viewpoint or stance to further a cause. Examples of websites that fall into this category: http://deomcrats.org, http://political.com.
Phishing and Other Frauds	Phishing, pharming, and other sites that pose as a reputable site, usually to harvest personal information from a user. These sites are typically quite short-lived, so examples do not last long. For more information, see http://en.wikipedia.org/wiki/Phishing.
Proxy Avoidance and Anonymizers	Proxy servers and other methods to gain access to URLs in any way that bypasses URL filtering or monitoring. Web-based translation sites that circumvent filtering. Examples of websites that fall into this category: http://anonymouse.org, http://surfen-op-school.com.
Questionable	Tasteless humor, get-rich-quick sites, and sites that manipulate the browser user experience or client in some unusual, unexpected, or suspicious manner. Examples of websites that fall into this category: http://9gag.com, http://collegehumor.com.

Real Estate	Information about renting, buying, or selling real estate or properties. Tips about buying or selling a home. Real estate agents, rental or relocation services, and property improvement. Examples of websites that fall into this category: http://prudentialproperties.com, http://realtor.com.
Recreation and Hobbies	Information, associations, forums and publications about recreational pastimes such as collecting, kit airplanes, outdoor activities such as hiking, camping, rock climbing, specific arts, craft, or techniques. Animal- and pet-related information, including breed specifics, training, shows, and humane societies. Examples of websites that fall into this category: http://petloverspublications.com, http://craftster.org.
Reference and Research	Personal, professional, or educational reference material, including online dictionaries, maps, census, almanacs, library catalogs, genealogy, and scientific information. Examples of websites that fall into this category: http://reference.com, http://wikipedia.org.
Religion	Conventional or unconventional religious or quasi-religious subjects. Churches, synagogues, or other houses of worship. Examples of websites that fall into this category: http://therocksandiego.org, http://biblesociety.ca.
Search Engines	Search interfaces using key words or phrases. Returned results may include text, websites, images, videos, and files. Examples of websites that fall into this category: http://google.com, http://sogou.com.
Self-Harm	URLs promoting anorexia, bulimia, and other types of self-harm. Examples of websites that fall into this category: https://lostallhope.com and https://poemsofselfharm.tumblr.com.
Sex Education	Information about reproduction, sexual development,

	safe sex practices, sexually transmitted diseases, sexuality, birth control, sexual development, tips for better sex. Products used for sexual enhancement, and contraceptives. Examples of websites that fall into this category: http://sexetc.org, http://healthywomen.org/healthcenter/sexual-health.
Shareware and Freeware	Software, screensavers, icons, wallpapers, utilities, ringtones. Downloads that request a donation, open source projects. Examples of websites that fall into this category: http://download.com, http://sourceforge.net.
Shopping	Department stores, retail stores, company catalogs, and other sites that allow online consumer or business shopping and the purchase of goods and services. Examples of websites that fall into this category: http://amazon.com, http://groupon.com.
Social Networking	Social networking sites that have user communities in which users interact, post messages, pictures, and otherwise communicate. These sites were formerly part of Personal Sites and Blogs, but have been moved to this new category to allow for differentiation and more granular policy. Examples of websites that fall into this category: http://facebook.com, http://twitter.com.
Society	A variety of topics, groups, and associations relevant to the general populace, broad issues that impact a variety of people, including safety, children, societies, and philanthropic groups. Examples of websites that fall into this category: http://dar.org, http://unicefusa.org.
Spam URLs	URLs contained in spam. For more information, see http://en.wikipedia.org/wiki/Spam_(electronic).
Sports	Team or conference web sites, international, national, college, professional scores and schedules; sports-

	related online magazines or newsletters, fantasy sports, and virtual sports leagues. Examples of websites that fall into this category: http://nba.com, http://schoenen-dunk.de.
Spyware and Adware	Spyware or adware sites that provide or promote information gathering or tracking that is unknown to, or without the explicit consent of, the end user or the organization. Unsolicited advertising popups and programs that may be installed on a user's computer. For more information, see http://en.wikipedia.org/wiki/Spyware.
Streaming Media	Sales, delivery, or streaming of audio or video content, including sites that provide downloads for viewers. Examples of websites that fall into this category: http://youtube.com, http://ustream.tv, http://warpradio.com.
Swimsuits & Intimate Apparel	Swimsuits, intimate apparel, or other types of suggestive clothing. Examples of websites that fall into this category: http://victoriassecret.com, http://www.jockey.com.
Training and Tools	Distance education and trade schools, online courses, vocational training, software training, skills training. Examples of websites that fall into this category: http://trainingtools.com, http://prezi.com.
Translation	URL and language translation sites that allow users to see URL pages in other languages. These sites can also allow users to circumvent filtering as the target page's content is presented within the context of the translator's URL. These sites were formerly part of Proxy Avoidance and Anonymizers, but have been moved to this category to allow for differentiation and more granular policy. Examples of websites that fall into this category: http://translate.google.com, http://microsofttranslator.com.

Travel	Airlines and flight booking agencies. Travel planning, reservations, vehicle rentals, descriptions of travel destinations, or promotions for hotels or casinos. Car rentals. Examples of websites that fall into this category: http://cheapflights.com, http://expedia.com.
Violence	Sites that advocate violence, depictions, and methods, including game/comic violence and suicide. Examples of websites that fall into this category: http://happytreefriends.com, http://torturegame.org.
Weapons	Sales, reviews, or descriptions of weapons such as guns, knives or martial arts devices, or provide information about their use, accessories, or other modifications. Examples of websites that fall into this category: http://browning.com, http://e-gunparts.com.
Web Advertisements	Advertisements, media, content, and banners. Examples of websites that fall into this category: http://casalemedia.com, http://justwebads.com.
Web-Based Email	Sites offering web-based email and email clients. Examples of websites that fall into this category: http://google.com/mail, http://foxmail.com.
Web Hosting	Free or paid hosting services for web pages and information concerning their development, publication, and promotion. Examples of websites that fall into this category: http://siteground.com, http://bluehost.com.

Create Custom URL Categories

You can create custom URL categories based on string and regular expression (regex) pattern matches. You can also create custom URL category objects, and you can override predefined URL category values.

For each custom URL category, you configure a confidence value. The confidence value is used to break a tie when multiple URL categories match a URL.

You can upload files that contain either string and regex patterns for matching URLs and URL reputations.

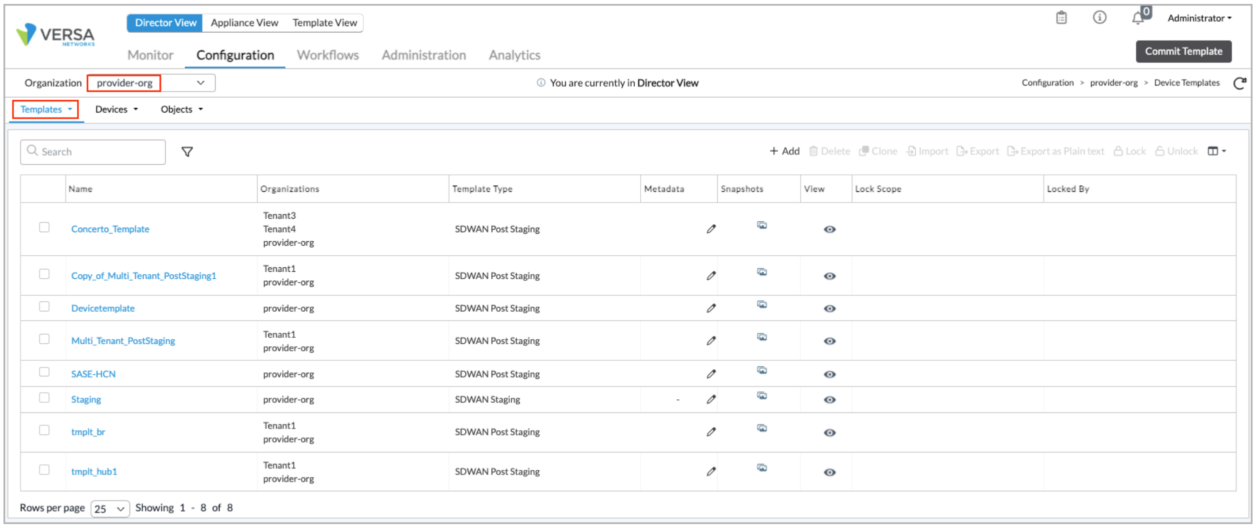
For more information, see Configure Custom URL Categories in Configure Layer 7 Objects.

Configure Global URL-Filtering Settings

You can configure global URL-filtering settings to categorize URLs. VOS devices then use these settings as the explicit defaults for all URL-filtering operations. You can override the global settings by creating individual URL-filtering profiles, as discussed in Configure a URL-Filtering Profile, below

To configure global URL-filtering settings:

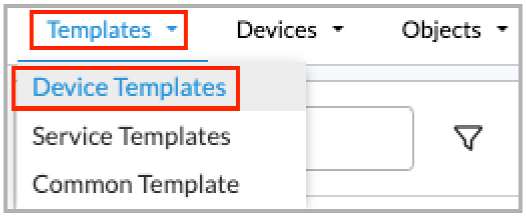
1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select an organization in the horizontal menu bar.



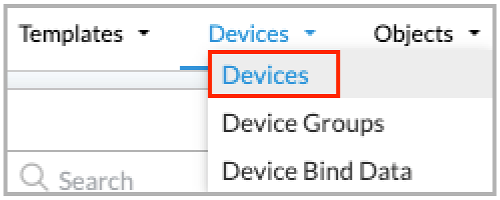
	Name	Organizations	Template Type	Metadata	Snapshots	View	Lock Scope	Locked By
□	Concerto_Template	Tenant3 Tenant4 provider-org	SDWAN Post Staging	✎	🖼	👁		
□	Copy_of_Multi_Tenant_PostStaging1	Tenant1 provider-org	SDWAN Post Staging	✎	🖼	👁		
□	Devicetemplate	provider-org	SDWAN Post Staging	✎	🖼	👁		
□	Multi_Tenant_PostStaging	Tenant1 provider-org	SDWAN Post Staging	✎	🖼	👁		
□	SASE-HCN	provider-org	SDWAN Post Staging	✎	🖼	👁		
□	Staging	provider-org	SDWAN Staging	- ✎	🖼	👁		
□	tmplt_br	Tenant1 provider-org	SDWAN Post Staging	✎	🖼	👁		
□	tmplt_hub1	Tenant1 provider-org	SDWAN Post Staging	✎	🖼	👁		

Rows per page 25 Showing 1 - 8 of 8

    c. To make the global URL-filtering settings permanent, select Templates > Device Templates in the horizontal menu bar. Then, in the main pane, select the template that you want to modify. The view changes to Appliance view.

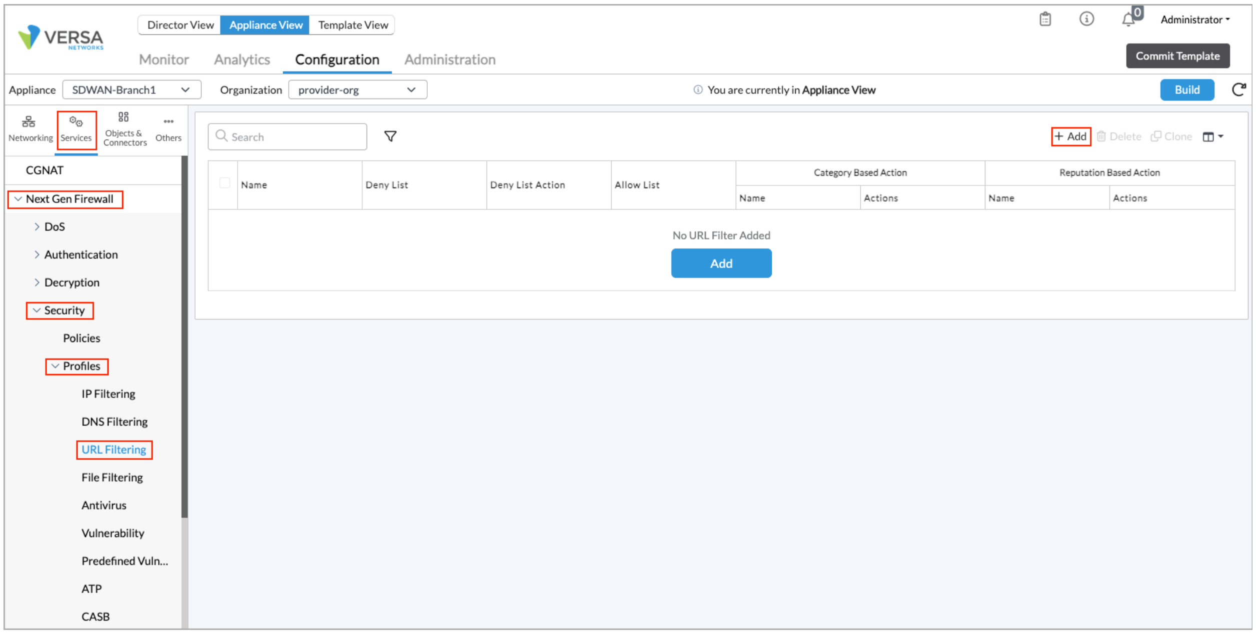


    d. To have the global URL-filtering settings apply to an individual device, select Devices > Device in the horizontal menu bar. Then, in the main pane, select the device name. The view changes to Appliance view. Note that this configuration is not permanent and is overwritten the next time you apply a template to the device.

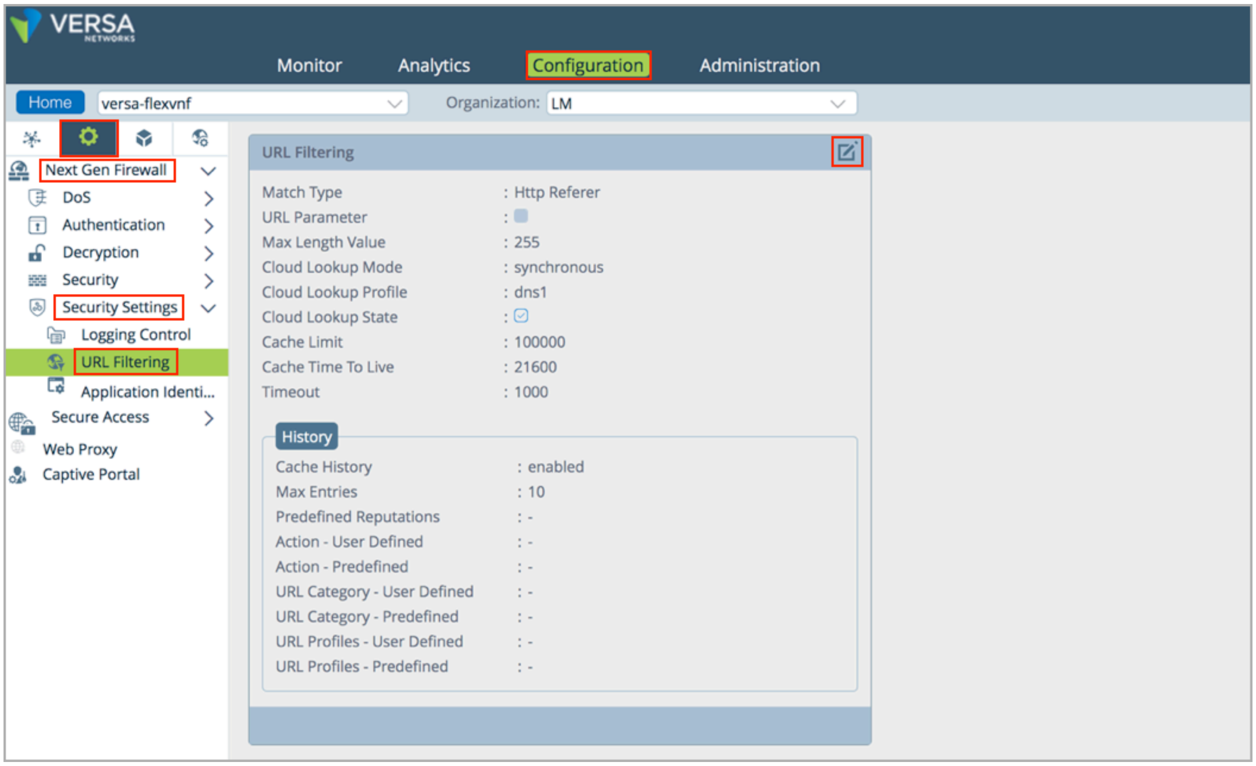


2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Security Settings > URL Filtering in the left menu bar. The main pane displays the URL Filtering pane.

   For Releases 22.1.3 and later:



For Releases 21.2 and earlier:



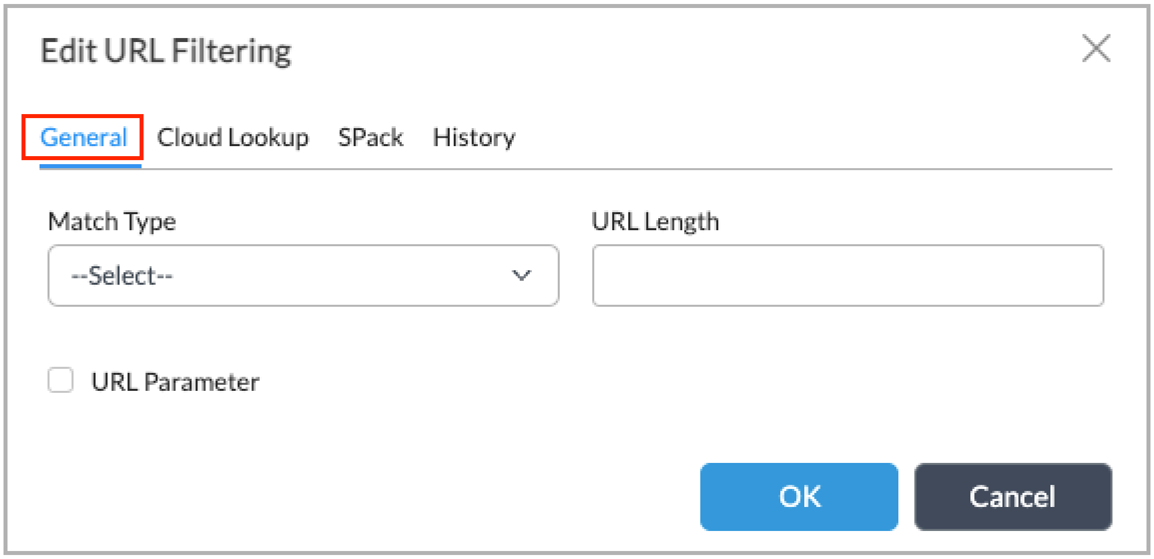
URL Filtering

Match Type	: Http Referer
URL Parameter	: ☐
Max Length Value	: 255
Cloud Lookup Mode	: synchronous
Cloud Lookup Profile	: dns1
Cloud Lookup State	: ☑
Cache Limit	: 100000
Cache Time To Live	: 21600
Timeout	: 1000

History

Cache History	: enabled
Max Entries	: 10
Predefined Reputations	: -
Action - User Defined	: -
Action - Predefined	: -
URL Category - User Defined	: -
URL Category - Predefined	: -
URL Profiles - User Defined	: -
URL Profiles - Predefined	: -

4. Click the Edit icon. The Edit URL Filtering popup window displays.
5. Select the General Tab, and then enter information for the following fields. Note that URL filtering can work with or without SSL decryption enabled. When you enable SSL decryption, URL filtering can create more granular filters.



Edit URL Filtering

Match Type: --Select--

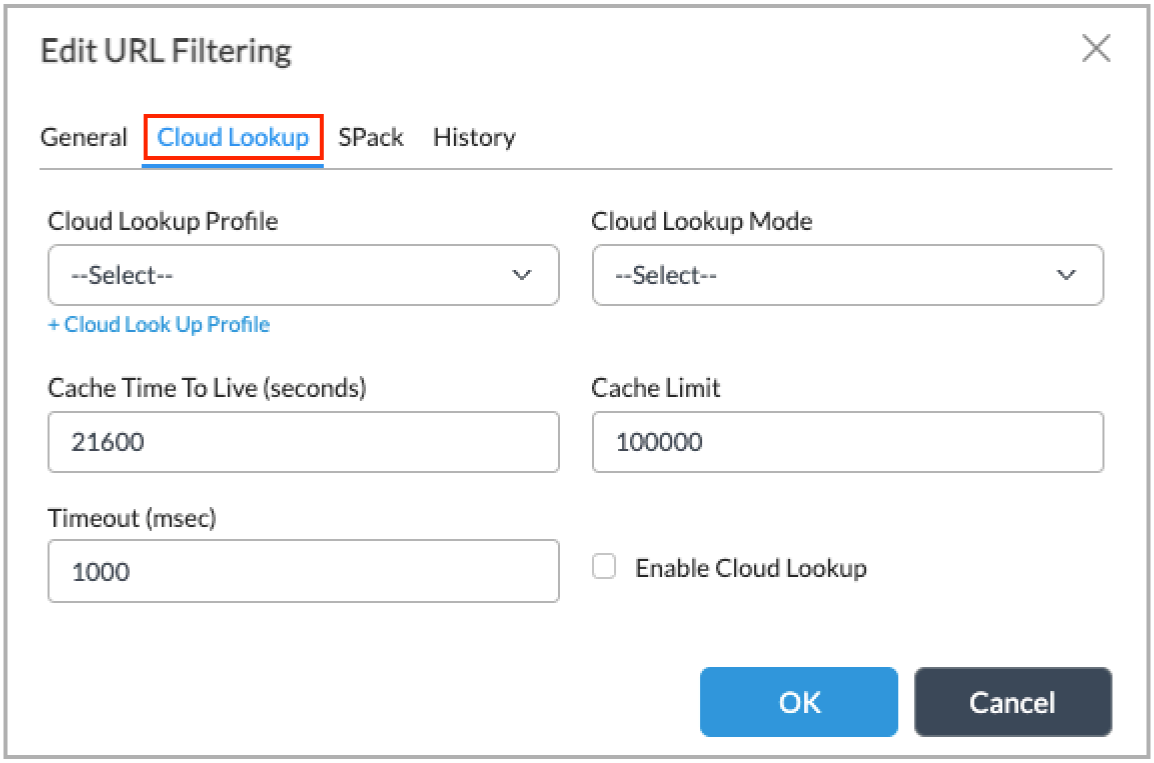
URL Length:

☐ URL Parameter

Field	Description
Match Type	Select the field type to match the URL category: ◦ HTTP Host URI—The system performs URL filtering based on the hostname requested in the HTTP request header or, if HTTPS is used, based on the SNI field in the TLS hello message. This is the default. ◦ HTTP Referer—The VOS device performs URL filtering based on the HTTP Referer field, if this field is present in the HTTP request. Web browsers use the HTTP referrer match type to tell web servers which site redirected a user to the website. For example, suppose you go to the website supernews.com that contains a link to another website called supertoys.com. If you click the link to supertoys.com, your web browser inserts supernews.com into the HTTP Referer field, which tells the supertoys.com web server that you were referred there by the supernews.com site. As an example to illustrate how the VOS device uses the Match Type field, suppose you configure URL filtering to allow all news websites and to block all toys websites. If you select the HTTP Referer option, the VOS devices classifies both supernews.com and supertoys.com as part of the News category, and both are allowed. If you select the HTTP Host URI option, supernews.com is classified as part of the News and supertoys.com is classified as part of the Toys category. As a result, the VOS devices blocks supertoys.com. *Default:* HTTP Host URI
URL Length	Enter the maximum length of the URL to log to Versa Analytics. For this option to work, you must also enable the URL Parameter option. If the length of the URL exceeds the configured value, the VOS device truncates the leading characters until the URL reaches the configured length. For example, if the URL length is 10 characters, and if the request is for the URL abc.def.ghi.com, the VOS device logs the

	URL as ef.ghi.com. *Range*: 0 through 255 *Default*: 255
URL Parameter	Click to send the full URL to Versa Analytics. By default, the VOS device logs only the hostname of the requested URL. For this option to work, you must also configure a value in the URL Length field.

6. Select the Cloud Lookup tab and enter information for the following fields.



Cloud Lookup Profile: --Select--

Cloud Lookup Mode: --Select--

Cache Time To Live (seconds): 21600

Cache Limit: 100000

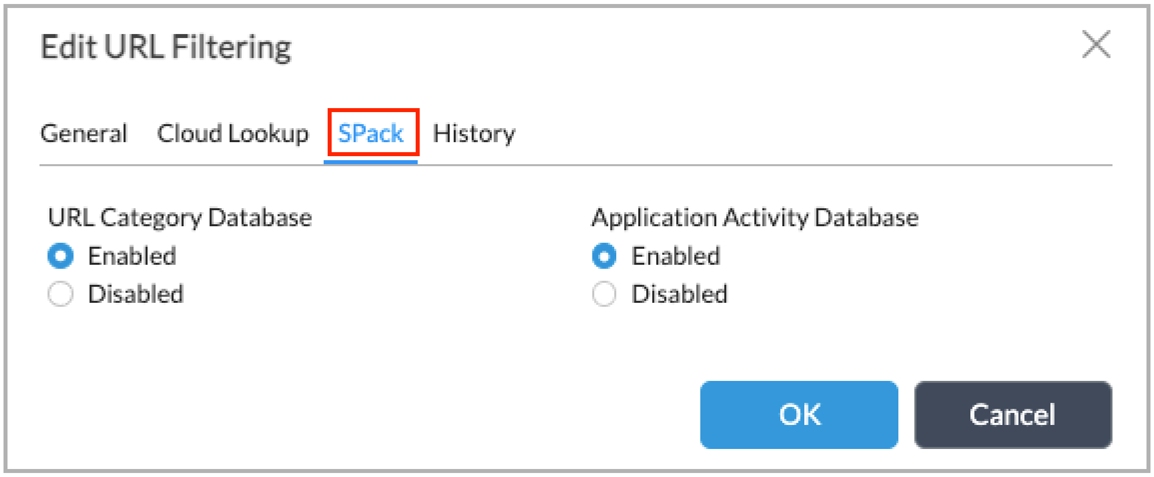
Timeout (msec): 1000

□ Enable Cloud Lookup

Field	Description
Cloud Lookup Profile	Select the cloud lookup profile. For information about creating a cloud profile, see Configure a Cloud Profile.
Cloud Lookup Mode	Select the cloud lookup mode to use for searching the URL filter classification: ◦ Asynchronous—The VOS device sends a cloud lookup request and loads the page before it receives the category information from the lookup response. In this mode, the VOS device does not hold up the session. The first time a URL is requested, it remains uncategorized. The default action taken on an uncategorized URL depends on the URL-filtering profile, and the LEF log category is marked as uncategorized. ◦ Synchronous—The VOS device sends a cloud lookup request and holds up the current session until it receives a response. The decision to display the webpage depends on the URL-filtering profile associated with the URL category or reputation. The LEF log carries the name of the category received in the response. If the VOS device does not receive a response within the timeout period, it releases the sessions and considers it to be an uncategorized session. The result of the cloud URL lookup is cached locally. Subsequent requests to the same URL use the URL categorization results from the local cache.
Cache Time To Live	Enter how long to retain entries in the cloud lookup cache. *Range*: 0 through 86400 seconds *Default*: 21600 seconds (6 hours)
Cache Limit	Enter the maximum number of entries to retain in the cloud lookup cache. *Range*: 1 through 1,000,000 *Default*: 100000
Timeout	Enter how long to wait for a response from a cloud lookup request before timing out. *Range*: 100 through 10000 milliseconds

	Default: 1000 milliseconds
Enable Cloud Lookup	Click to enable cloud lookup. When you enable cloud lookup, the VOS device, integrated with the SPack URL Reputation and Category Database, can connect to the Versa Networks cloud database, which includes approximately 2 billion categorized URLs. Cloud lookup is disabled by default. If cloud lookup is not enabled, and the requested URL is not found in the SPack database, the URL is assigned a default reputation of Suspicious and categorized as Uncategorized. For more information, see Configure Cloud URL Lookup, below.

7. (For Releases 22.1.3 and later.) Select the SPack tab, and then click the appropriate Enabled or Disabled settings for URL Category Database and Application Activity Database.

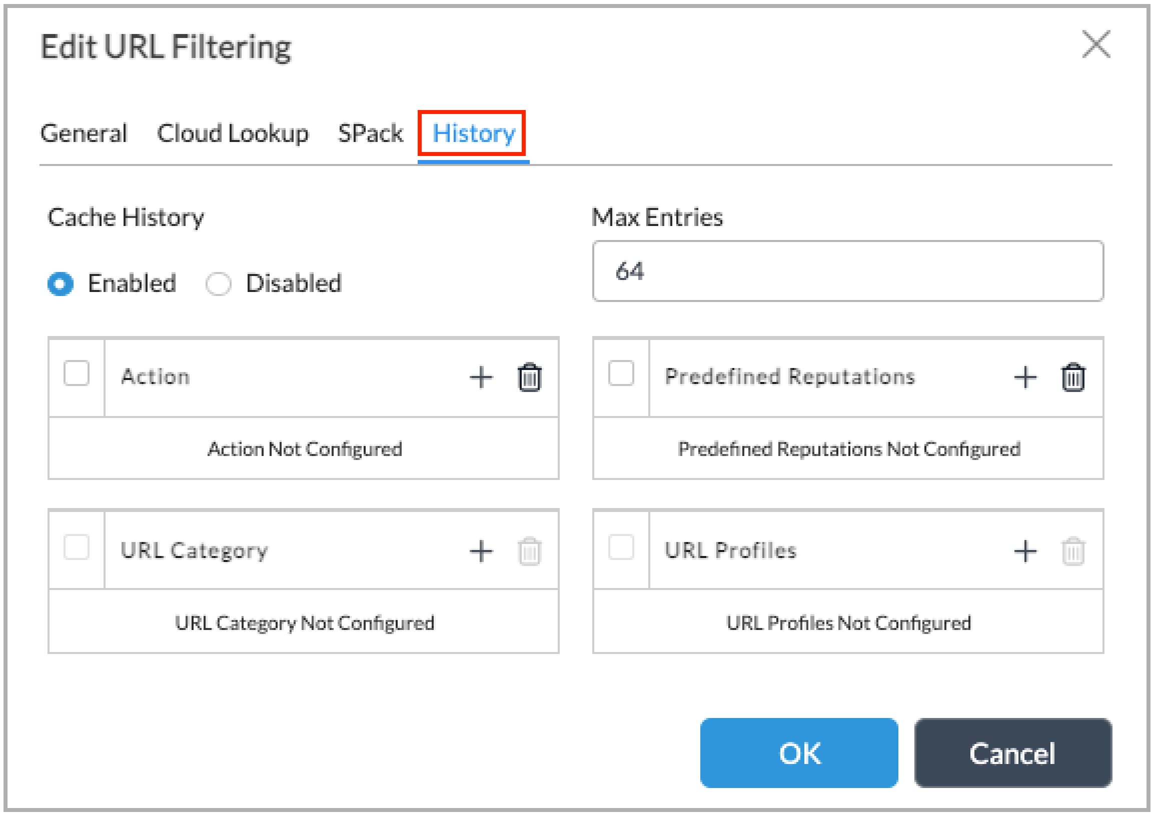


Edit URL Filtering

URL Category Database
● Enabled
○ Disabled

Application Activity Database
● Enabled
○ Disabled

8. Select the History tab to configure which URLs are stored in the URL-filtering history, which is a local cache on the VOS device. Having a cache of stored URLs is useful to help troubleshoot the VOS device. The history stores more detailed information than is available in the Versa Analytics logs. Note that the Action, Predefined Reputations, URL Category, and URL Profiles fields operate as AND statements. For example, if you select the Allow action and the Gambling URL category, only URLs that match both the Allow and Gambling criteria are saved; other URLs are not saved.
Enter information for the following fields.



Edit URL Filtering

Cache History

● Enabled ○ Disabled

Max Entries: 64

□	Action
	Action Not Configured

□	Predefined Reputations
	Predefined Reputations Not Configured

□	URL Category
	URL Category Not Configured

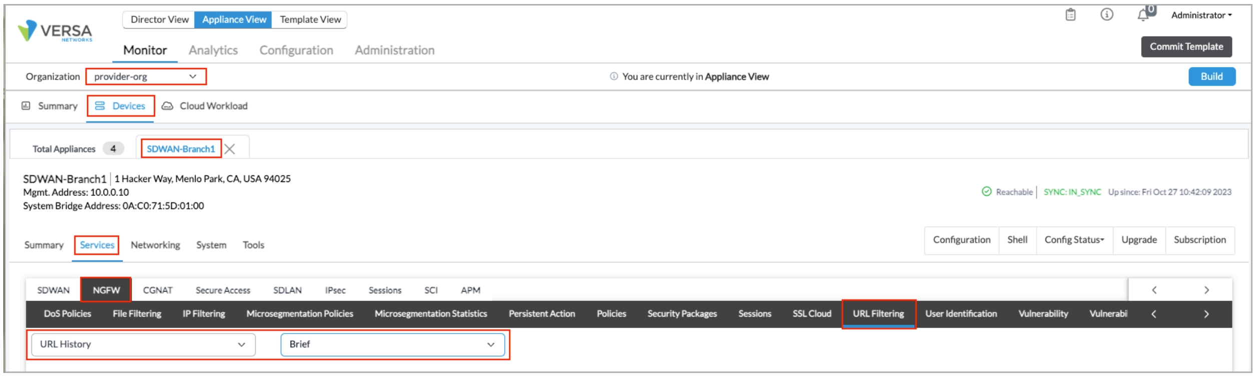
□	URL Profiles
	URL Profiles Not Configured

Field	Description
Cache History (Group of Fields)	
◦ Enabled	Click to enable the caching of the URL-filtering history.
◦ Disabled	Click to disable the caching of the URL-filtering history. This is the default
◦ Maximum Entries	Enter the maximum number of URL-filtering history entries to store. *Range*: 1 through 128 *Default*: 64
Action	Click the + Add icon and select the actions. URLs matching these actions are saved in the cache history.
Predefined Reputations	Click the + Add icon and select the reputations. URLs matching these reputations are saved in the cache history.
URL Category	Click the + Add icon and select the URL categories. URLs matching these categories are saved in the cache history.
URL Profiles	Click the + Add icon and select the URL profiles. URLs matching these profiles are saved in the cache history.

8. Click OK.

To monitor the URL-filtering history:

1. In Director view:
   a. Select the Monitor tab in the top menu bar.
   b. Select an organization in the left menu bar, and then select Devices in the horizontal menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Services tab, and then select the NGFW tab.
3. Select the URL Filtering tab in the horizontal menu bar.
4. Select URL History in the first drop-down list.
5. Select Brief or Detail in the second drop-down list.

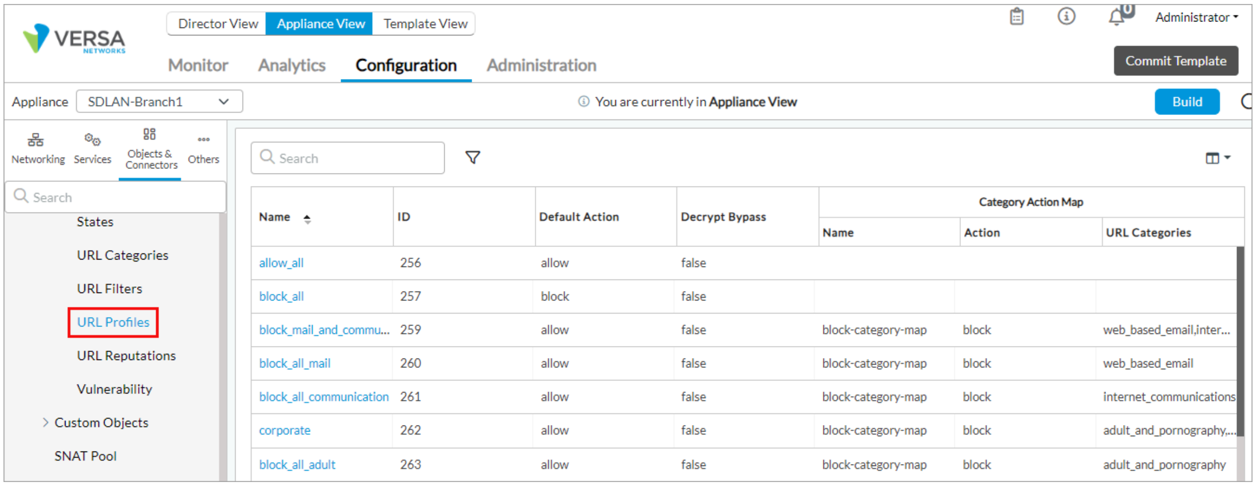


View Predefined URL-Filtering Profiles

Versa provides a number of predefined URL-filtering profiles, including the Versa-recommended URL-filtering profile, which is called Corporate, that you can use in access policies.

To view the predefined URL-filtering profiles:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects and Connectors > Objects > Predefined > URL Profiles in the left menu bar.



Name	ID	Default Action	Decrypt Bypass	Category Action Map		
				Name	Action	URL Categories
allow_all	256	allow	false			
block_all	257	block	false			
block_mail_and_commu...	259	allow	false	block-category-map	block	web_based_email,inter...
block_all_mail	260	allow	false	block-category-map	block	web_based_email
block_all_communication	261	allow	false	block-category-map	block	internet_communications
corporate	262	allow	false	block-category-map	block	adult_and_pornography,...
block_all_adult	263	allow	false	block-category-map	block	adult_and_pornography

4. Click on a profile to view details. The following table describes the predefined URL filtering profiles:

Field	Description
Allow All	Allows all traffic.
Block All	Blocks all traffic.
Block All Adult	Blocks all adult traffic.
Block All Adult and Ads	Block all adult and advertisement traffic.
Block All Adult Games and Ads	Block all adult games and advertisement traffic.
Block All Communication	Blocks all communication traffic.
Block All Mail	Blocks all email traffic.
Block Mail and Communication	Blocks all email and communication traffic.
Corporate (Versa Recommended Profile)	Allows all traffic, except for the following categories: ◦ Abused drugs—Discussion or remedies for illegal, illicit, or other commonly abused drugs such as heroin, cocaine, and other street drugs. Information about legal highs, including glue sniffing, misuse of prescription drugs, and abuse of other legal substances. ◦ Adult and pornography—Sexually explicit material for the purpose of arousing a sexual or prurient interest. Adult products including sex toys, CD-ROMs, and videos. Online groups, including newsgroups and forums, that are sexually explicit in nature. Erotic stories and textual descriptions of sexual acts. Adult services including videoconferencing, escort services, and strip clubs. Sexually explicit art. ◦ Gambling—Gambling or lottery web sites that invite the use of real or virtual money. Information or advice for placing wagers, participating in lotteries, gambling, or running numbers. Virtual casinos and offshore gambling ventures. Sports picks and betting pools. Virtual sports and fantasy leagues that offer large rewards or request significant wagers. Note that hotel and resort sites that do not enable gambling on the site are categorized in Travel or Local Information./li> ◦ Illegal—Criminal activity, how not to get caught, copyright and intellectual property violations. ◦ Marijuana—Marijuana use, cultivation, history, culture, legal issues.

	◦ Military—Information about military branches, armed services, and military history. ◦ Nudity—Nude or seminude depictions of the human body. These depictions are not necessarily sexual in intent or effect, but may include sites containing nude paintings or photo galleries of artistic nature. Nudist or naturist sites that contain pictures of nude individuals. ◦ Phishing and other frauds—Phishing, pharming, and other sites that pose as a reputable site, usually to harvest personal information from a user. These sites are typically quite short-lived. ◦ Proxy avoidance and anonymizers—Proxy servers and other methods to gain access to URLs in any way that bypasses URL filtering or monitoring. Web-based translation sites that circumvent filtering. ◦ Translation—URL and language translation sites that allow users to see URL pages in other languages. These sites can also allow users to circumvent filtering as the content on the target page is presented within the context of the translator's URL. These sites were formerly part of the proxy avoidance and anonymizers category, but have been moved to this category to allow for differentiation and more granular policy. ◦ Violence—Sites that advocate violence, depictions, and methods, including game or comic violence and suicide. ◦ Weapons—Sales, reviews, or descriptions of weapons such as guns, knives or martial arts devices, or information about their use, accessories, or other modifications.

Configure URL-Filtering Profiles

URL-filtering profiles enforce actions on HTTP flows based on URL category and URL reputation. You can use predefined URL-filtering profiles, and you can create custom profiles. You can use a single URL-filtering profile with one or more security policy rules. URL filtering processes any traffic that matches a security policy rule in a URL-filtering profile. Any logs that are generated are sent to the logging profile associated with the URL-filtering profile.

In URL-filtering profiles, you can create allow lists and deny lists of URLs.

When a user on a tenant VOS device attempts to open an HTTP or HTTPS session, the device performs the following actions:

- Evaluate the security policy and selects the one that matches the HTTP or HTTPS session.
- Check whether a URL-filtering profile is associated with the security policy. If so, the VOS device uses the profile to process the session.
- Check whether cloud lookup is configured for the URL-filtering profile:
  - If cloud lookup is configured and enabled for the profile, enable cloud lookup for the session.
  - If cloud look up is configured but not enabled, disable cloud lookup for the session.
- If cloud lookup is not configured for the URL-filtering profile, the device uses the following URL-filtering settings for the tenant:
  - If cloud lookup is configured and enabled for the tenant, enables cloud lookup for the session.
  - If cloud lookup is configured and but not enabled, disables cloud lookup for the session.

If you configure URL-filtering settings, they override any tenant URL-filtering settings.

The URL-filtering profile processes enforceable actions for a session in the following order:

- Deny listed URLs—Specify either fixed strings or regular expression (regex) patterns to match deny listed URLs. Specify the deny list action to take for all matching HTTP flows. If the deny list action is not configured, the default drop session action is taken.
- Allow listed URLs—Specify either fixed strings or perl-compatible regular expression (PCRE) patterns to match allow listed URLs. URLs that match the allow list configuration are allowed, and no security actions are taken. Optionally, you can enable logging to create a log of allow listed URLs.
- Category action map—A set of rules that specify the URL-filtering action to take for each URL category that is associated with a URL. In each rule, you can specify one or more predefined or custom URL categories. The action can be a packet or session action, or a predefined or custom captive portal action. VOS devices evaluate URL category and URL reputation action rules simultaneously, and they enforce the more severe action. For example, if the category rule action is to block and the reputation rule is to allow, the block action is taken.
- Reputation action map—A set of rules that specify the URL-filtering action to take for each URL reputation that is associated with the URL. In each rule, you can specify one or more URL reputation values. The action can be a packet or session action, or a predefined or custom captive portal action.

If this evaluation does not determine an action, the default action configured for the URL-filtering profile is taken.

URL-Filtering Actions

There is a set of predefined URL-filtering actions that you can apply in URL-filtering profiles. A URL-filtering profile consists of a collection of URL-filtering controls that is applied to the security policy rule to enforce the security access policy. You can also create custom URL-filtering actions.

The following are the URL-filtering action types:

- Session and packet actions
- Predefined captive portal actions
- User-defined captive portal actions

Session and Packet Actions

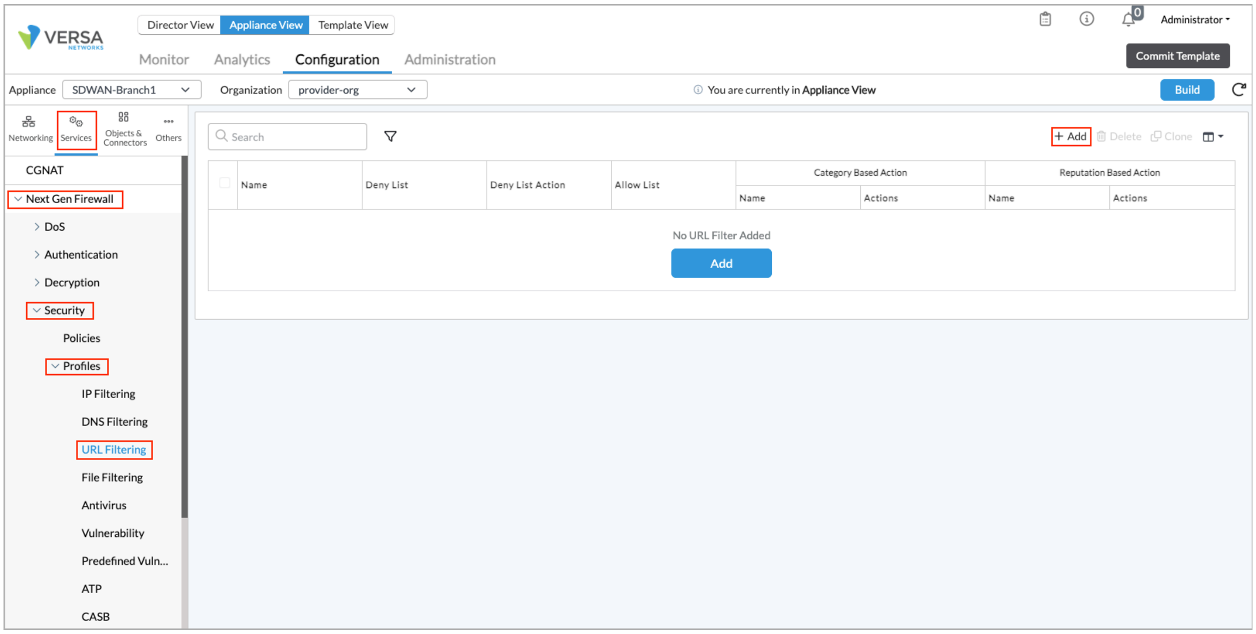
When a user visits a webpage using a URL, you can enforce a policy action based on the URL category or URL reputation associated with the URL. The following session and packet actions are available:

- Alert—Allow the URL and generate an entry in the URL-filtering log.
- Allow—Allow the URL without generating an entry in the URL-filtering log.
- Drop packet—The browser waits for a response from the server and then drops the packet. It is not possible to determine whether the packet was dropped because of no response from the server or because a firewall blocked access to the website.
- Drop session—The browser waits for a response from the server and drops the session. It is not possible to determine whether the session was dropped because of no response from the server or because a firewall blocked access to the website.
- Reject—The browser displays an alert and resets the connection to the server. It is not possible to determine whether this occurred because of a delayed response from the server or because a firewall blocked access to the website.

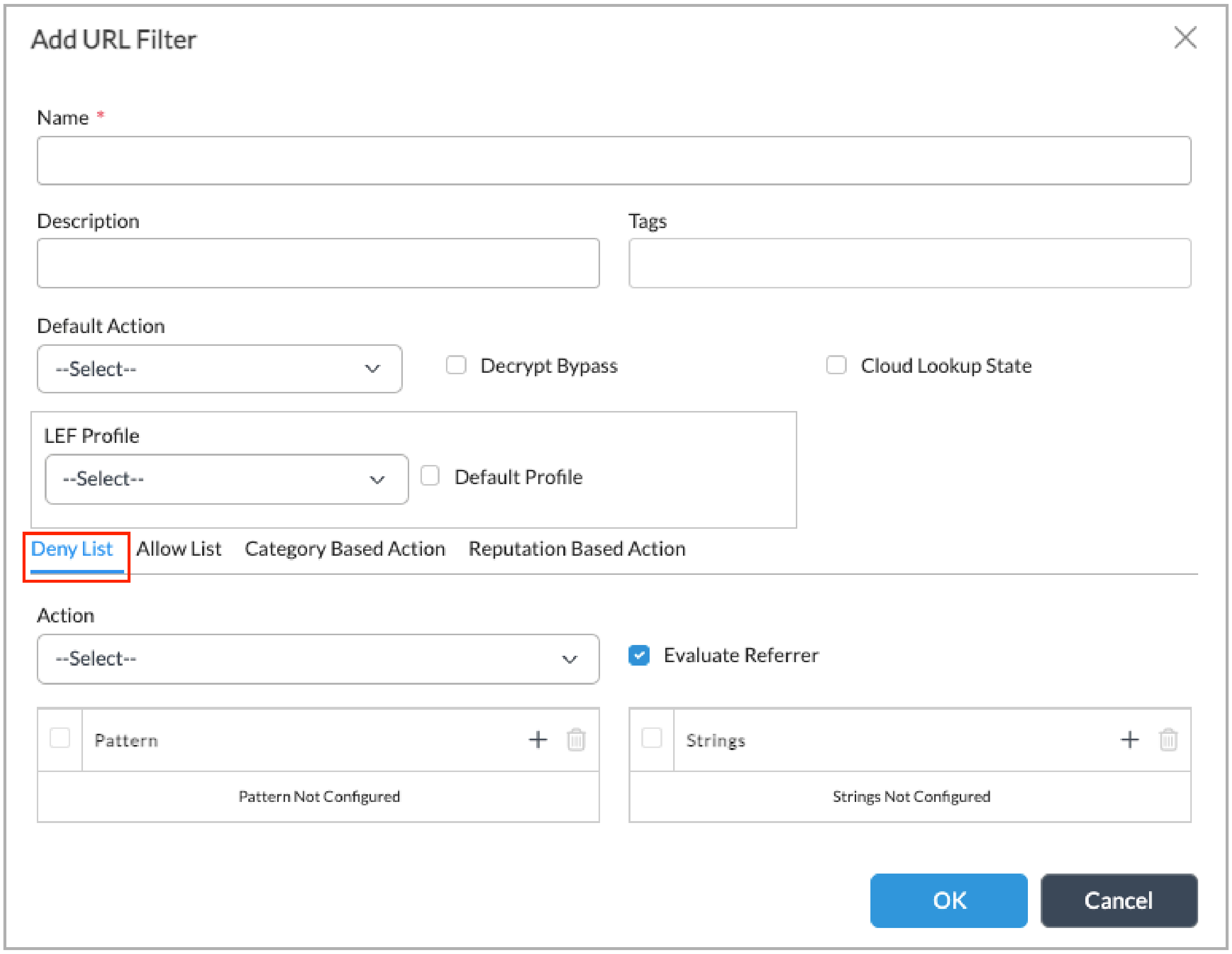
Configure a URL-Filtering Profile

To configure a URL-filtering profile:

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next Gen Firewall > Security > Profiles > URL Filtering in the left menu bar.



4. Click the + Add icon. In the Add URL Filter popup window, enter information for the following fields.



Add URL Filter

Name *

Description

Tags

Default Action

--Select--

□ Decrypt Bypass

□ Cloud Lookup State

LEF Profile

--Select--

□ Default Profile

Deny List | Allow List | Category Based Action | Reputation Based Action

Action

--Select--

☑ Evaluate Referrer

□	Pattern
	Pattern Not Configured

□	Strings
	Strings Not Configured

Field	Description
Name	Enter a name for the URL filter.
Description	Enter a text description for the URL filter.
Tags	Enter a keyword or phrase that allows you to filter the URL filter. This is useful when you have many policies and want to view those that are tagged with a particular keyword.
Default Action	Select the default action to apply to the URL filter: ◦ Alert—Allow the URL and generate an entry in the URL-filtering log. ◦ Allow—Allow the URL without generating an entry in the URL-filtering log.

Field	Description
	◦ Ask—The browser presents an information page that allows the user to either cancel the operation by clicking Cancel or continue with the operation by clicking OK (for HTTP and HTTPS). ◦ Block—Block the URL and generate an entry in the URL-filtering log. No response page is display, and the user cannot continue with the website. ◦ Drop packet—The browser waits for a response from the server and then drops the packets. It is not possible to determine whether the packet was dropped because of no response from the server or because a firewall blocked access to the website. ◦ Drop session—The browser waits for a response from the server and drops the session. It is not possible to determine whether the session was dropped because of no response from the server or because a firewall blocked access to the website. ◦ Justify—The browser presents an information page that allows the user to either cancel the operation by clicking Cancel or continue with the operation after entering a justification message and clicking OK (for HTTP and HTTPS). ◦ Reject—The browser displays an alert and resets the connection to the server. It is not possible to determine whether this occurred because of no response from the server or because a firewall blocked access to the website.
Decrypt Bypass	Click to enable decrypt bypass, which disables decryption of SSL traffic that matches the predefined captive portal actions for this URL-filtering profile after captive portal redirection. The decryption policy decrypts SSL sessions to display only the captive portal response. After the captive portal action is performed, SSL decryption is bypassed, and users can directly access the URL. To disable decryption for traffic matching a custom action, select a custom action (Default action) and select Decrypt-Bypass. If you do not select the Decrypt Bypass option, SSL

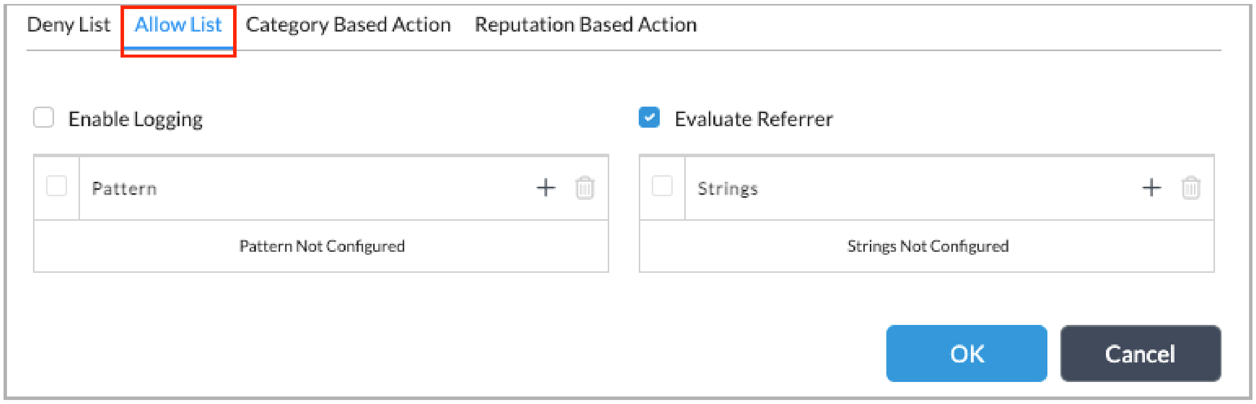
Field	Description
	decryption is enabled and URL filtering uses the host and URI of the actual URL for categorization. This action further decrypts captive portal redirection from actions such as Ask and Justify. Note that this setting is relevant only when you use the SSL decryption and captive portal. You do not need to enable SSL decryption for a regular URL filtering to work.
Cloud Lookup State	Click to enable cloud lookup.
LEF Profile	Select a LEF profile to register logs of the URL filter. Logs are sent to the active collector of the LEF profile. For information about configuring a LEF profile, see Configure Log Export Functionality. For information about associating a LEF profile with features and services, see Apply Log Export Functionality.
Default Profile	Click to use the default LEF profile instead of the profile selected in the previous field. For information about configuring a default LEF profile, see Configure Log Export Functionality.

8. Select the Deny List tab, and then enter information for the following fields. For Releases 21.1.1 and earlier, this tab is called Blacklist.

Field	Description
Action	Select an action to take on a deny listed URL: ◦ Alert ◦ Allow ◦ Ask ◦ Block ◦ Drop Packet ◦ Drop Session ◦ Justify ◦ Reject For more information, see Session and Packet

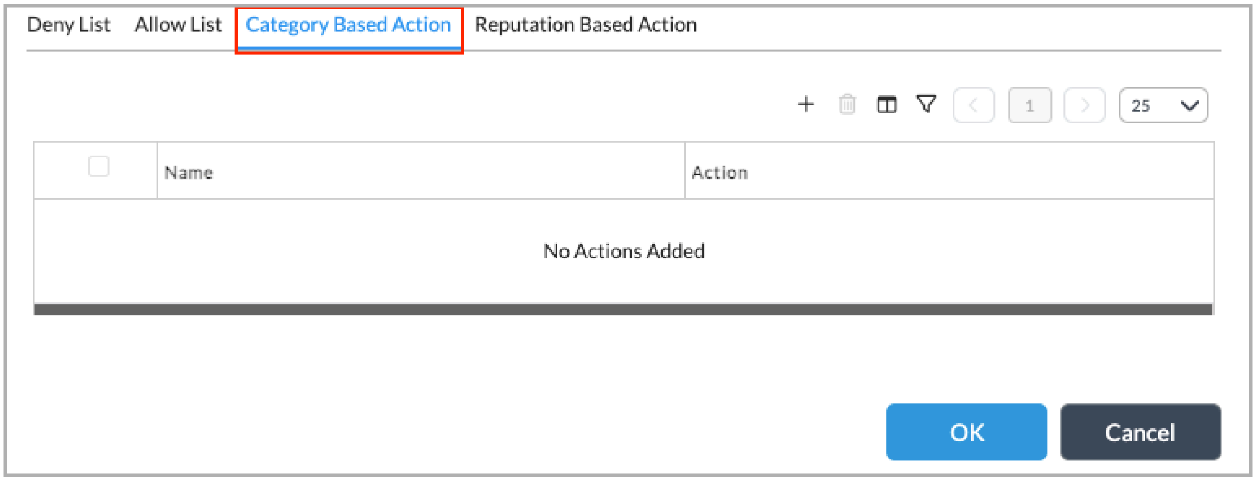
Field	Description
	Actions, above.
Evaluate Referrer	Click to enable deny list evaluation based on the referrer value.
Pattern	Click the + Add icon to add specific URLs to block. You can specify a fixed string or a regex pattern.
Strings	Click the + Add icon to specify the complete URL string of a URL to block.

9. Click OK to save the configuration.
10. Select the Allow List tab and enter information for the following fields. For Releases 21.1.1 and earlier, this tab is called Whitelist.



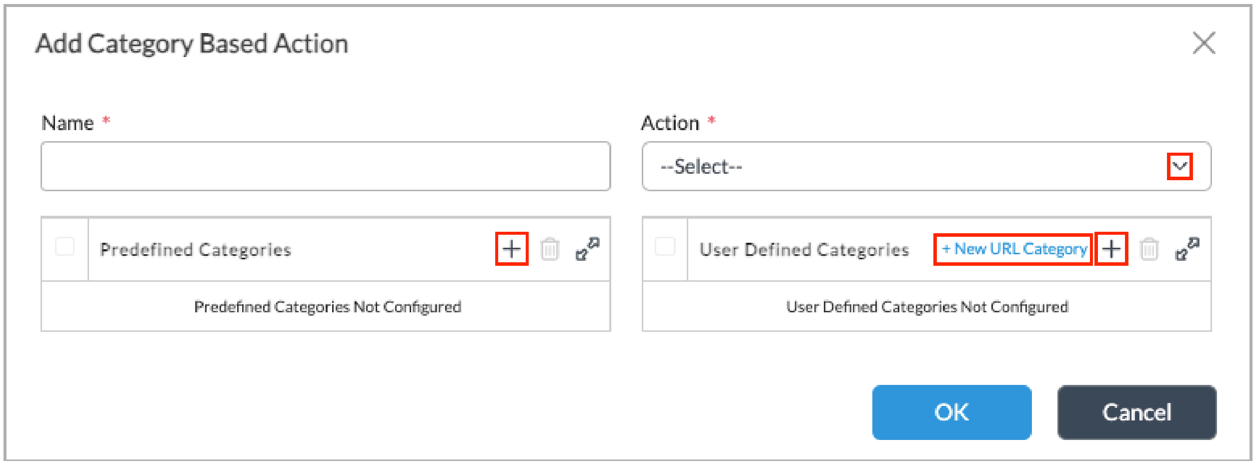
Field	Description
Enable Logging	Select to log allow listed URLs.
Pattern	Click the + Add icon to add specific URLs to allow. You can specify a fixed string or a regex pattern.
Strings	Click the + Add icon to specify the complete URL string of a URL to allow.

11. Click OK to save the configuration.
12. Select the Category-Based Action tab, and click the + Add icon to add actions for categories.

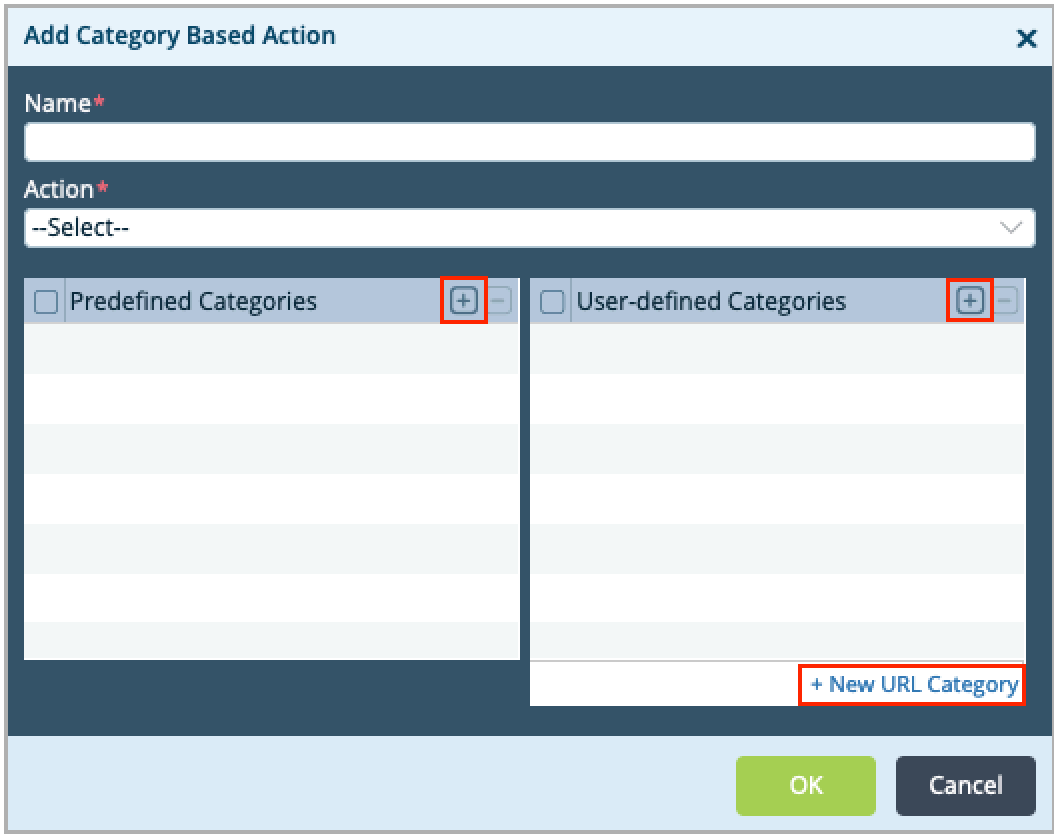


13. In the Add Category-Based Action popup window, enter information for the following fields.

    For Releases 22.1.3 and later:


Add Category Based Action
Name *
Action *
--Select--
Predefined Categories
Predefined Categories Not Configured
User Defined Categories
+ New URL Category
User Defined Categories Not Configured
OK
Cancel

    For Releases 21.2 and earlier:

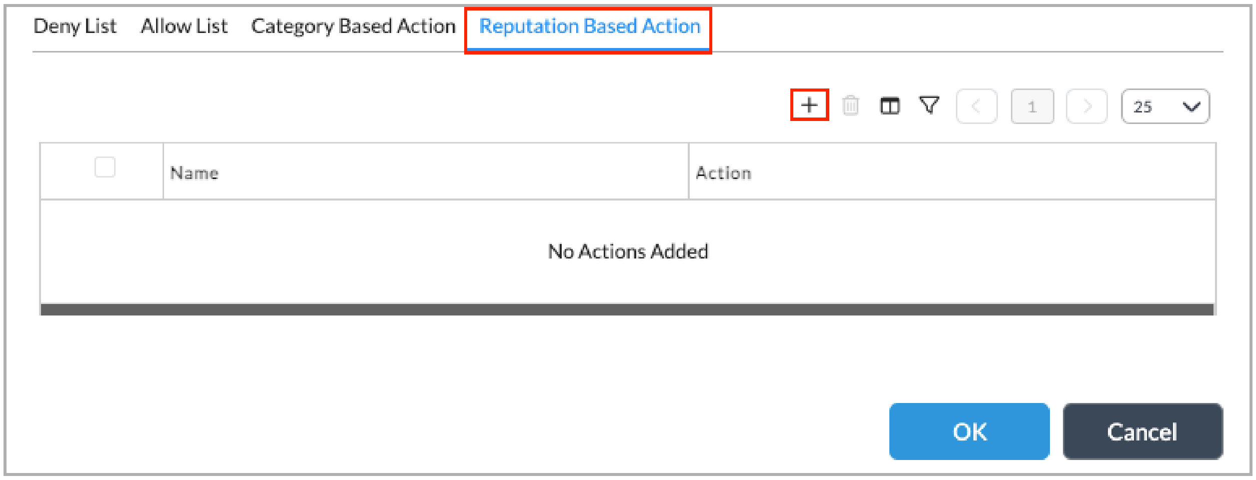


Field	Description
Name	Enter a name for the category action.
Action	Select an action to take for deny listed URLs: ◦ Alert ◦ Allow ◦ Ask ◦ Block ◦ Drop Packet ◦ Drop Session ◦ Justify ◦ Reject For more information, see Session and Packet Actions, above.
Predefined Categories	Click the + Add icon to select a predefined category.

Field	Description
User-defined Categories	Click the + Add icon to select a custom category.
+ New URL Category	Click to define a new URL category. For more information, see Configure Layer 7 Objects.

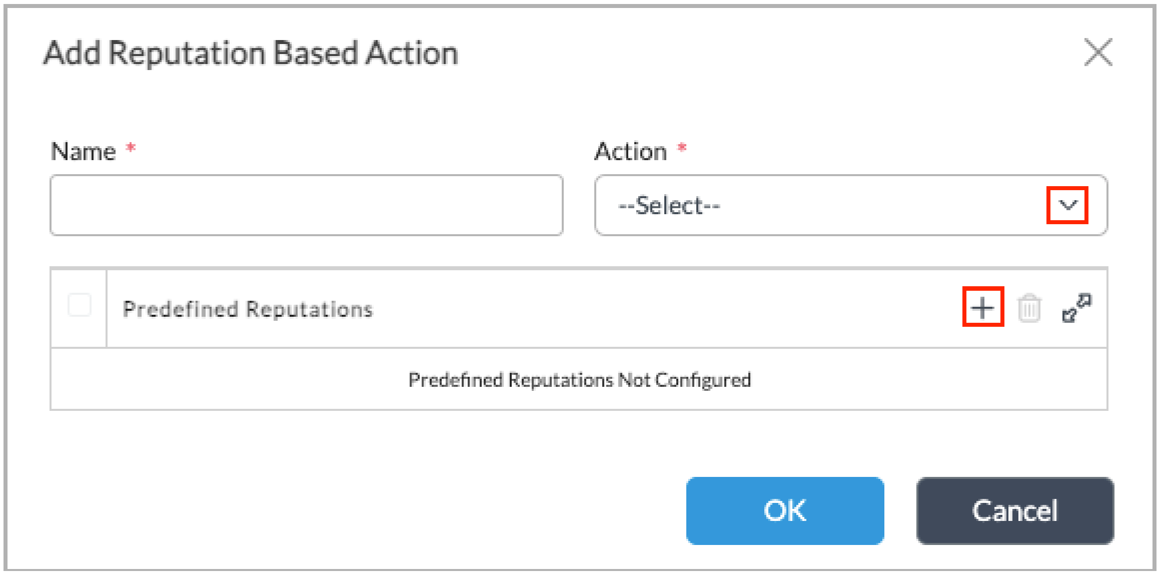
13. Click OK to save the configuration.

14. Select the Reputation-Based Action tab, and click the + Add icon to add actions for categories.

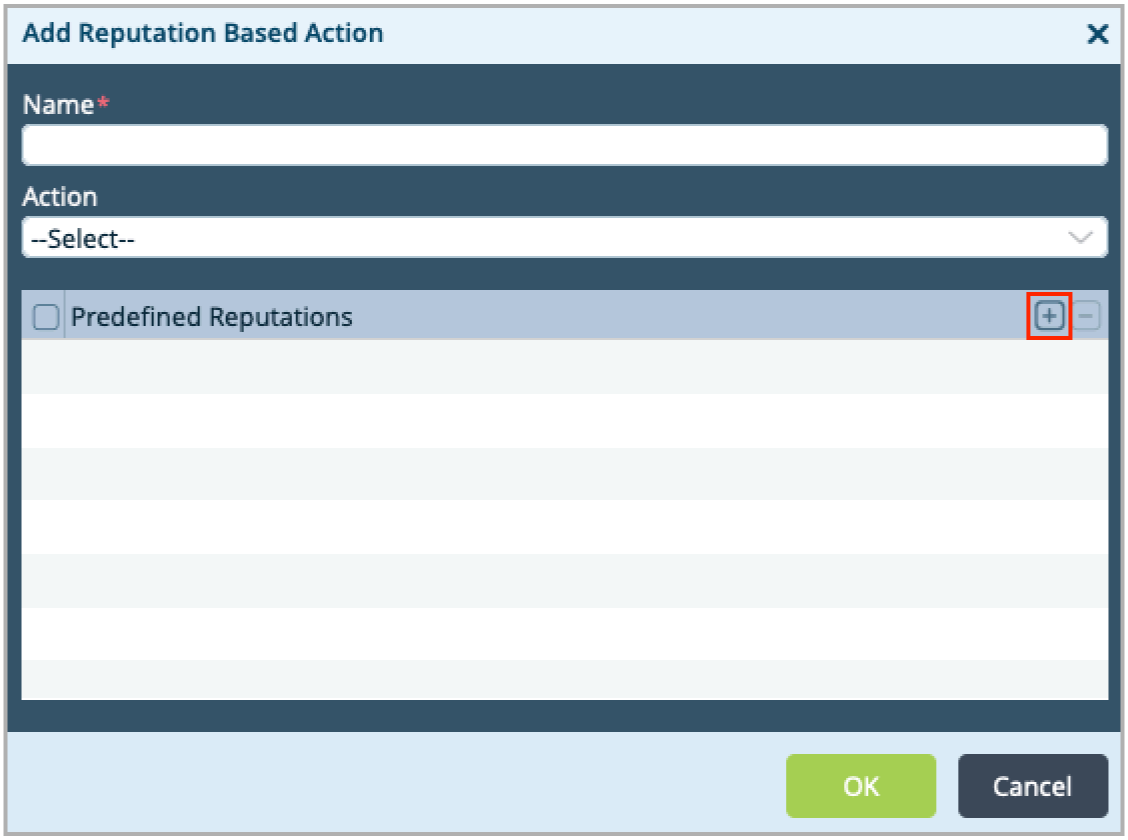


15. In the Add Reputation-Based Action popup window, enter information for the following fields.

For Releases 22.1.3 and later:


Add Reputation Based Action
Name *
Action *
--Select--
Predefined Reputations
Predefined Reputations Not Configured
OK
Cancel

For Releases 21.2 and earlier:



Field	Description
Name	Enter name for the reputation-based action.
Action	Select an action to take for deny listed URLs: ◦ Alert ◦ Allow ◦ Ask ◦ Block ◦ Drop Packet ◦ Drop Session ◦ Justify ◦ Reject For more information, see Session and Packet Actions, above.

Field	Description
Predefined Reputations	Click the ⊞ Add icon to select a predefined reputation.

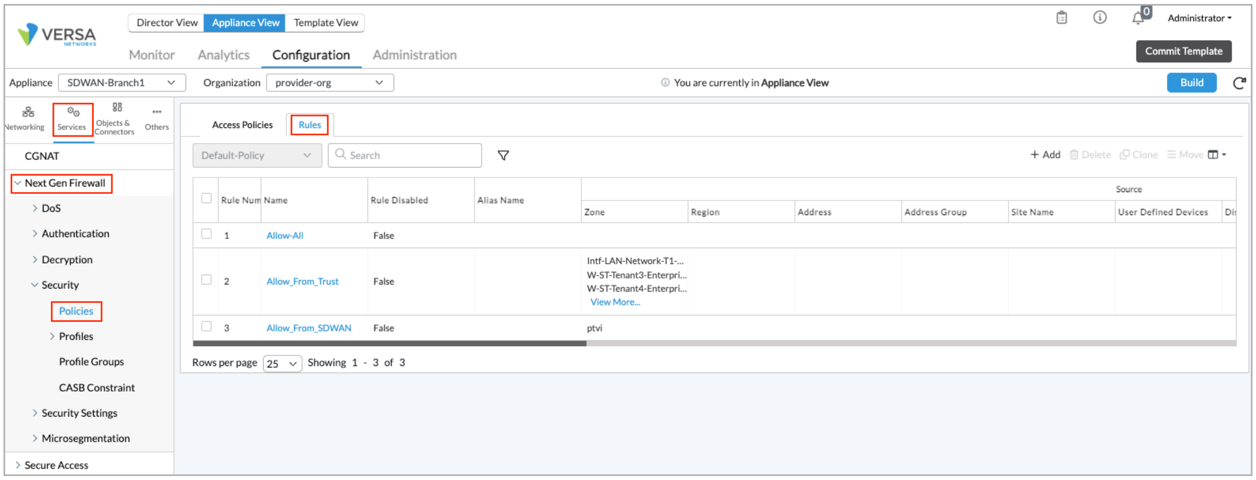
12. Click OK.

Apply a URL-Filtering Profile to an Access Policy

You can apply a URL-filtering profile to a security access policy. To define and configure a security access policy, see Configure Security Access Policy Rules.

To apply a URL-filtering profile to an access policy:

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Security > Policies in the left menu bar, and then select the Rules tab.



Appliance: SDWAN-Branch1 Organization: provider-org

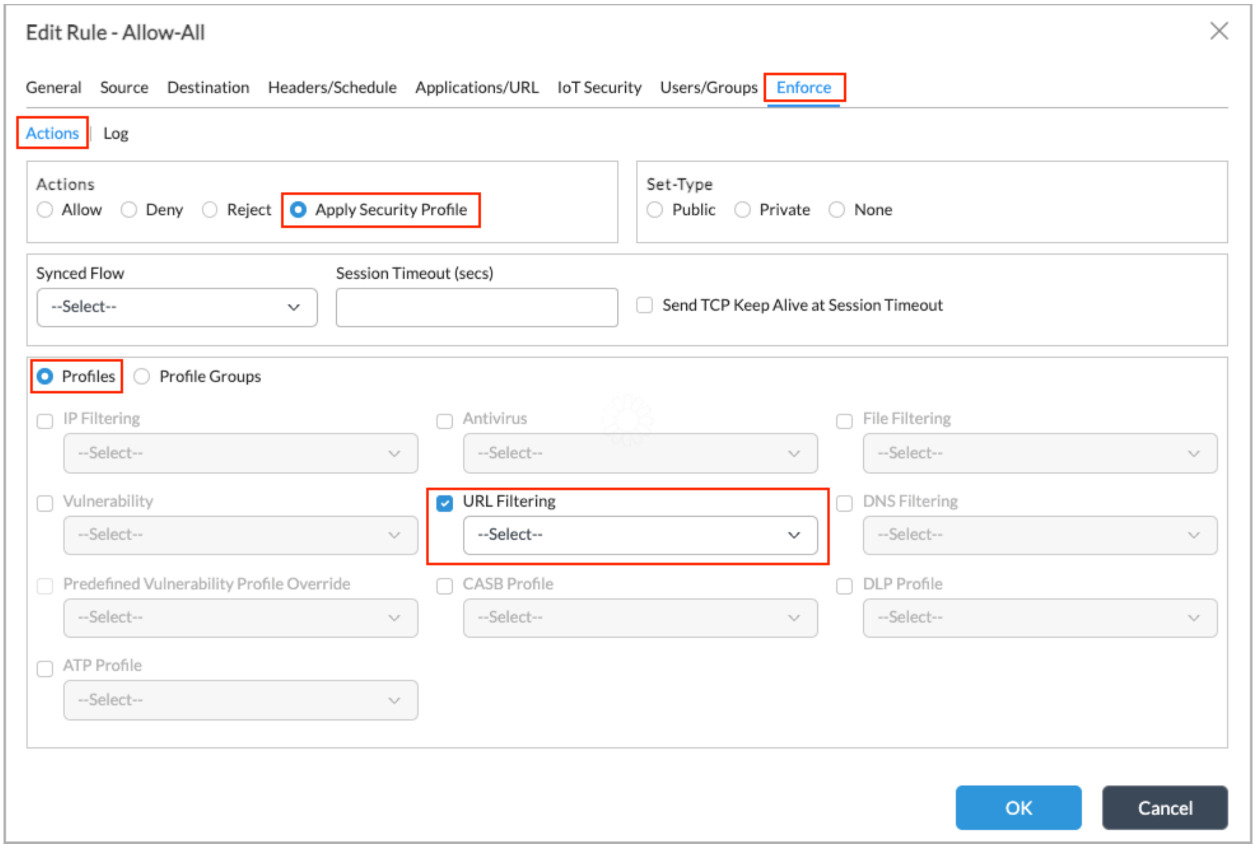
You are currently in **Appliance View**

Default-Policy

				Source						
Rule Num	Name	Rule Disabled	Alias Name	Zone	Region	Address	Address Group	Site Name	User Defined Devices	Di
1	Allow-All	False								
2	Allow_From_Trust	False		Intf-LAN-Network-T1-... W-ST-Tenant3-Enterpri... W-ST-Tenant4-Enterpri... View More...						
3	Allow_From_SDWAN	False		ptvi						

Rows per page 25 Showing 1 - 3 of 3

4. Select a security access policy rule. The Edit Rule popup window displays.


Edit Rule - Allow-All

Actions: ○ Allow ○ Deny ○ Reject ● Apply Security Profile

Set-Type: ○ Public ○ Private ○ None

Synced Flow: --Select--

Session Timeout (secs):

□ Send TCP Keep Alive at Session Timeout

● Profiles ○ Profile Groups

□ IP Filtering: --Select--

□ Antivirus: --Select--

□ File Filtering: --Select--

□ Vulnerability: --Select--

☑ URL Filtering: --Select--

□ DNS Filtering: --Select--

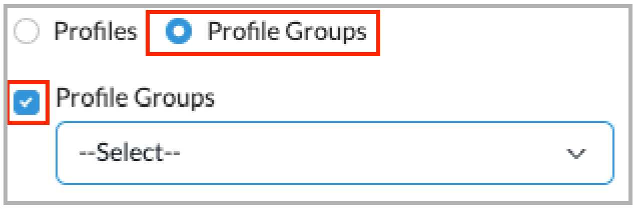
□ Predefined Vulnerability Profile Override: --Select--

□ CASB Profile: --Select--

□ DLP Profile: --Select--

□ ATP Profile: --Select--

5. Select the Enforce tab.
6. In the Actions group of fields, click Apply Security Profile. Doing this enables the Profiles section on the popup window.
7. Click Profiles, and then click URL Filtering and select the URL-filtering profile to use for the rule. The field displays the predefined and custom URL-filtering profiles. For more information about predefined URL-filtering profiles, see View Predefined URL-Filtering Profiles above.
8. If you have created profile groups, click Profile Groups, and then select the profile group to use for the rule from the list of predefined and custom URL-filtering profile groups. For more information, see Configure Security Profile Groups.


○ Profiles ● Profile Groups

☑ Profile Groups: --Select--

9. Click OK.

View and Configure URL Reputation

VOS devices support predefined and user-defined URL reputations. URLs are assigned a reputation indicator to identify and group applications based on the associated reputation. The lower the value, the higher the reputation of the URL.

View a Predefined URL Reputation

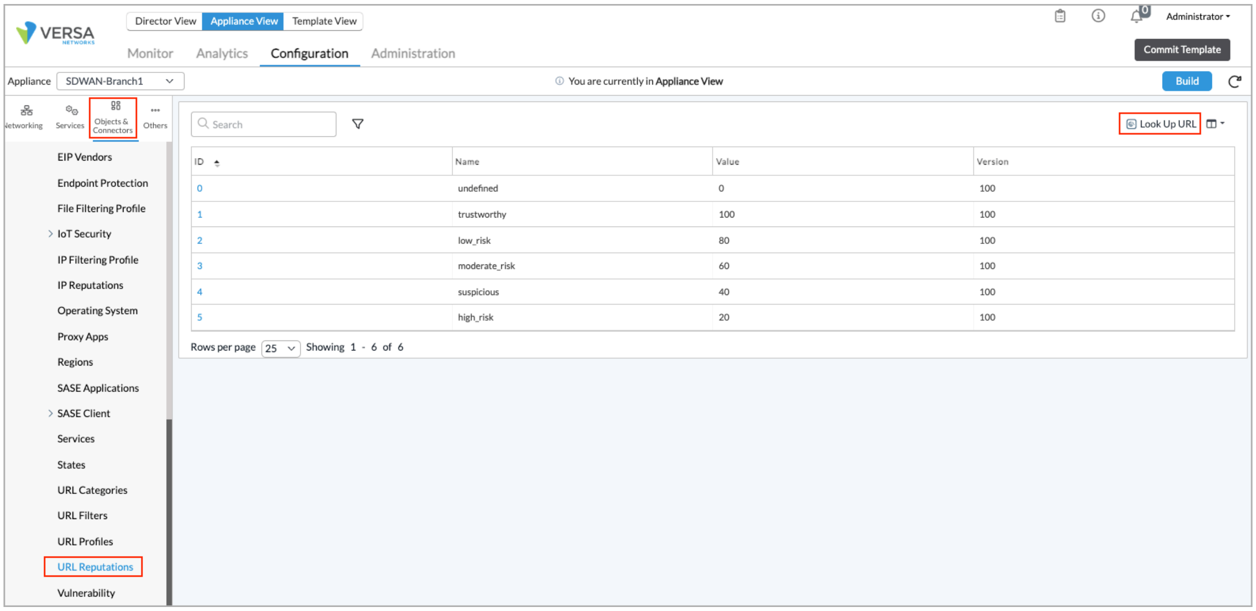
On a VOS device, you can view the predefined URL reputations in the URL database on a VOS device. You can use the URL reputation values as a basis for enforcing policy actions. The predefined URL database lookup results in both the URL category and the URL reputation getting associated with the URL. The predefined URL database is updated (either on a daily or real-time basis) via security-package updates.

The following are the predefined URL reputation types:

- Trustworthy
- Low Risk
- Moderate Risk
- Suspicious
- High Risk
- Undefined

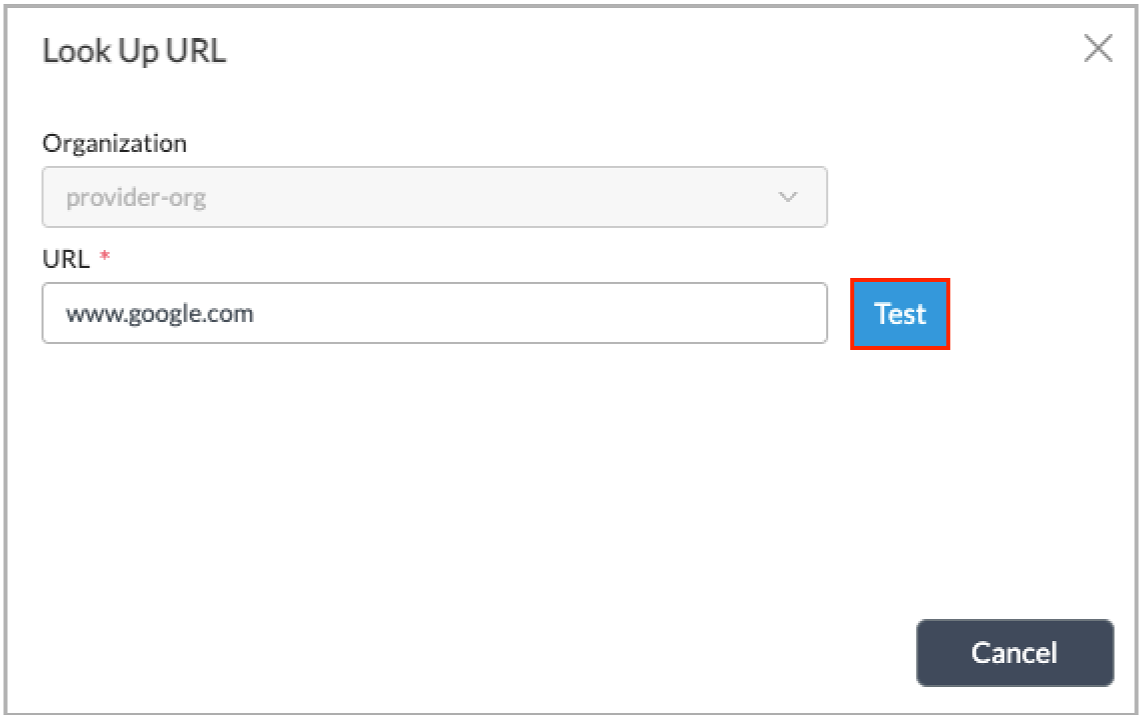
To view predefined URL reputations:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Predefined > URL Reputations. The main pane displays the URL reputations.



ID	Name	Value	Version
0	undefined	0	100
1	trustworthy	100	100
2	low_risk	80	100
3	moderate_risk	60	100
4	suspicious	40	100
5	high_risk	20	100

4. Click the Look Up URL icon to display more information about a URL. In the Look Up URL popup window, enter information for the following fields.



Look Up URL

Organization

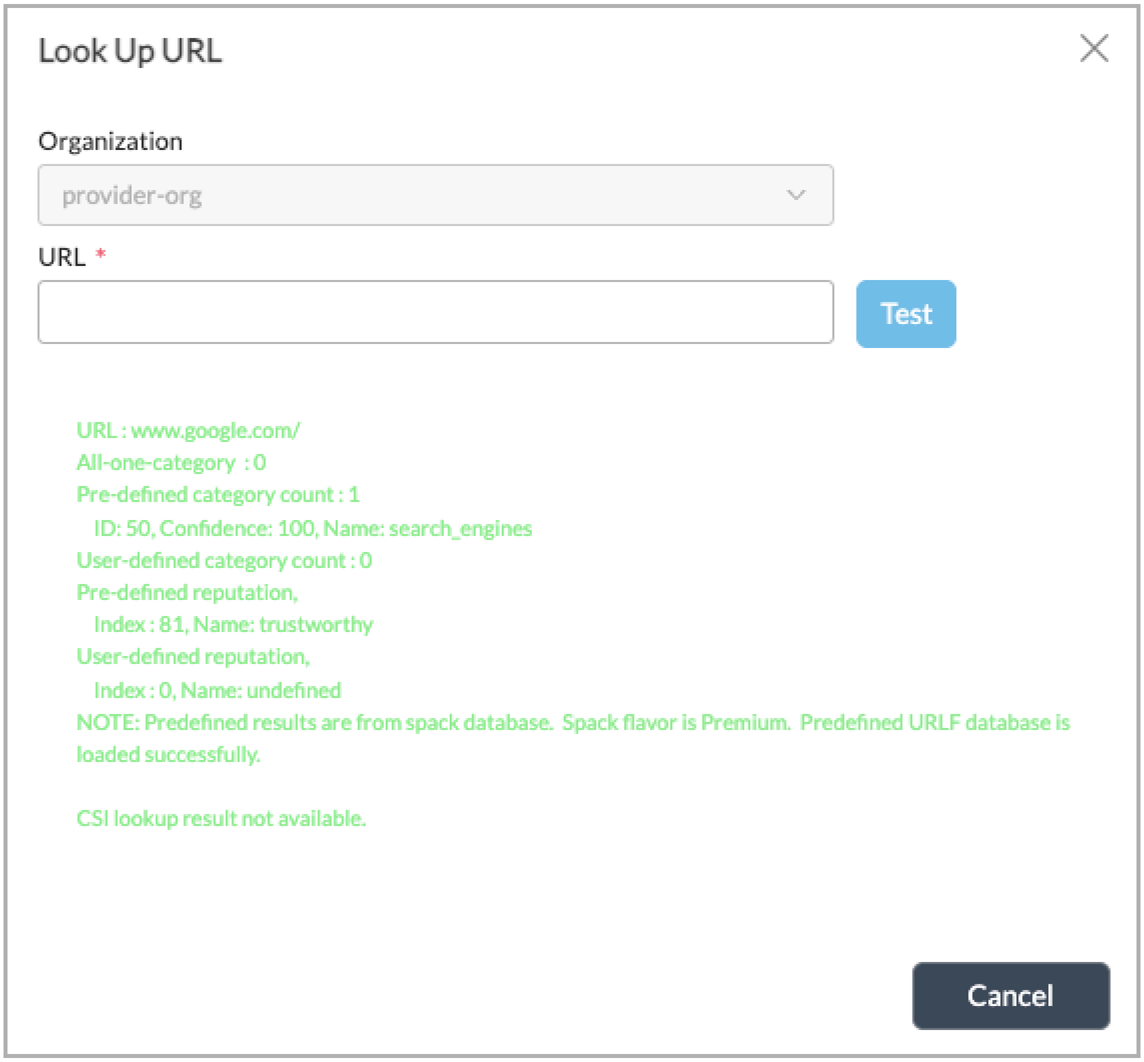
provider-org

URL *

www.google.com

Field	Description
Organization	Select the organization for which to define the URL category.
URL	Enter a URL whose URL category to look up. For example, enter www.google.com.

5. Click Test. The Look Up URL popup window displays information about the URL, including its category and reputation. For example:



Organization: provider-org

URL *

```
URL : www.google.com/
All-one-category  : 0
Pre-defined category count : 1
   ID: 50, Confidence: 100, Name: search_engines
User-defined category count : 0
Pre-defined reputation,
   Index : 81, Name: trustworthy
User-defined reputation,
   Index : 0, Name: undefined
NOTE: Predefined results are from spack database.  Spack flavor is Premium.  Predefined URLF database is
loaded successfully.

CSI lookup result not available.
```

6. Click Cancel.

Configure a Custom URL Reputation

You can create custom URL reputations based on string and regular expression (regex) pattern matches. You can create custom URL reputation objects, and you can override predefined URL reputation values.

You can upload files that contain either string and regex patterns for matching URLs and URL reputations.

For information, see Configure Custom URL Categories.

Configure Cloud URL Lookup

A VOS device that is running the premium SPack has an embedded URL database of more than 2 million categorized domain names. If a URL category or reputation information is not available in the VOS device's database, you can configure real-time cloud lookup to request this information from a cloud server, which has a database of more than 2 billion categorized URLs. You enable cloud lookup when you configure global URL-filtering, as described in Configure Global URL-Filtering Settings, above.

To configure cloud URL lookup:

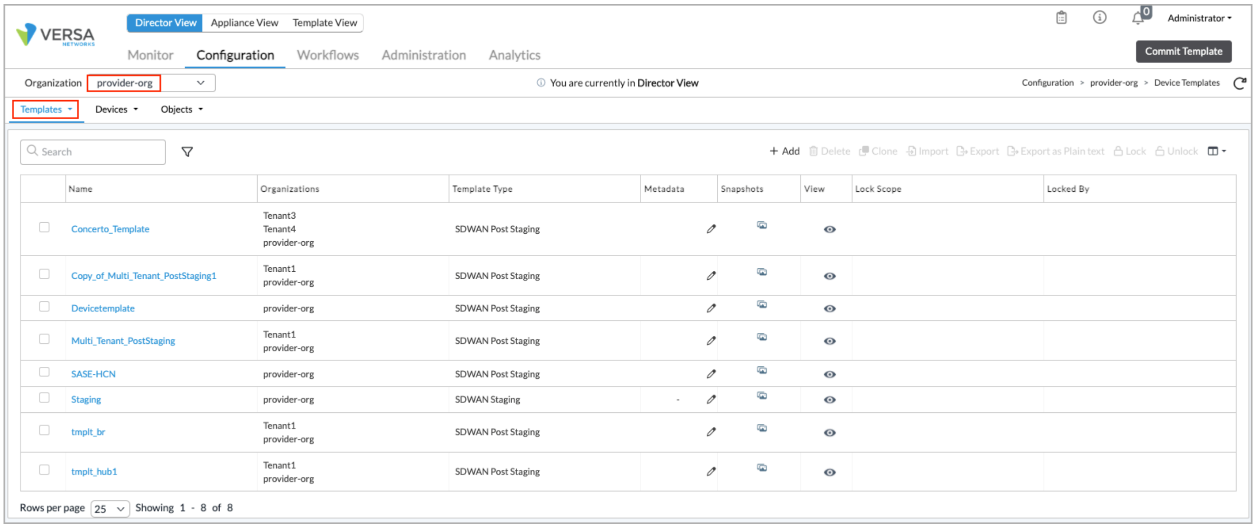
1. Configure SNAT pools for the cloud URL lookup.
2. Configure a cloud profile for cloud URL lookup.
3. Configure DNS servers on the VOS device. For more information, see Configure DNS Servers.
4. Configure DNS proxy on the VOS device for the transport selected in the SNAT pool.

Configure SNAT Pools for the Cloud URL Lookup

To request URL information from the cloud, the VOS devices must know which networks or interfaces to use. Source NAT (SNAT) is one method to use to configure these resources on the VOS device.

To configure an SNAT pool:

1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select an organization in the horizontal menu bar.



Organization provider-org

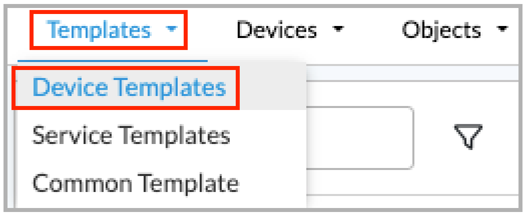
You are currently in Director View

Configuration > provider-org > Device Templates

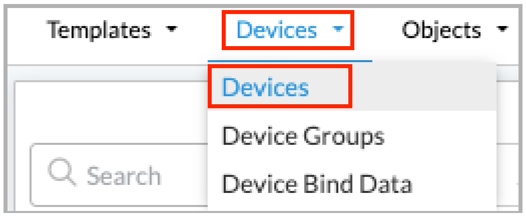
	Name	Organizations	Template Type	Metadata	Snapshots	View	Lock Scope	Locked By
☐	Concerto_Template	Tenant3 Tenant4 provider-org	SDWAN Post Staging	✎	🖼	👁		
☐	Copy_of_Multi_Tenant_PostStaging1	Tenant1 provider-org	SDWAN Post Staging	✎	🖼	👁		
☐	Devicetemplate	provider-org	SDWAN Post Staging	✎	🖼	👁		
☐	Multi_Tenant_PostStaging	Tenant1 provider-org	SDWAN Post Staging	✎	🖼	👁		
☐	SASE-HCN	provider-org	SDWAN Post Staging	✎	🖼	👁		
☐	Staging	provider-org	SDWAN Staging	- ✎	🖼	👁		
☐	tmplt_br	Tenant1 provider-org	SDWAN Post Staging	✎	🖼	👁		
☐	tmplt_hub1	Tenant1 provider-org	SDWAN Post Staging	✎	🖼	👁		

Rows per page 25 Showing 1 - 8 of 8

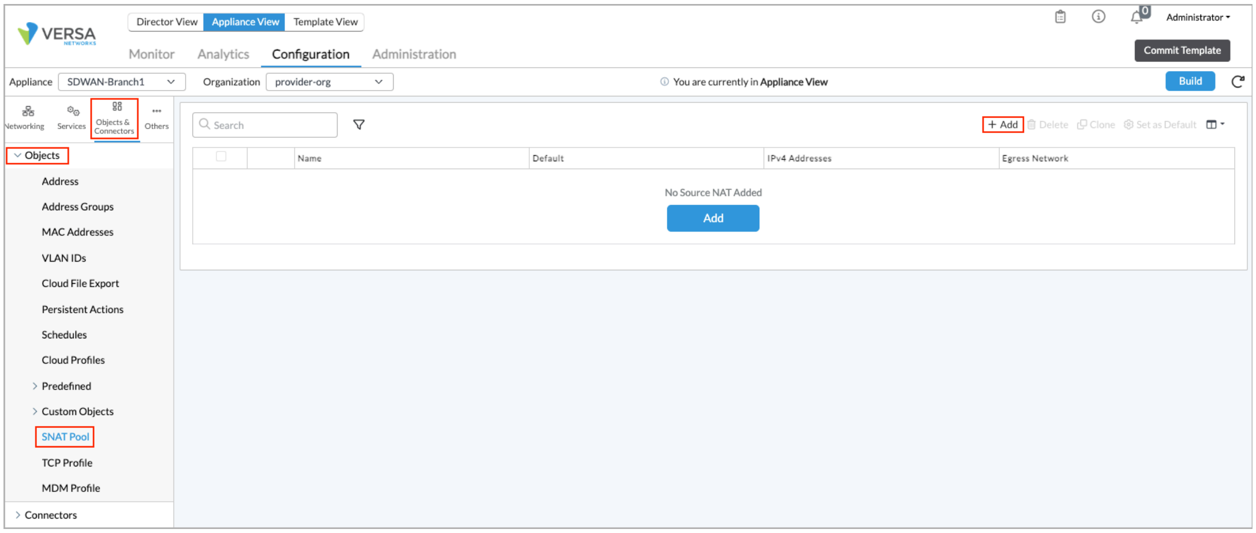
    c. To make the SNAT settings permanent, select Templates > Device Templates in the horizontal menu bar, and then select the template name in the main pane. The view changes to Appliance view.



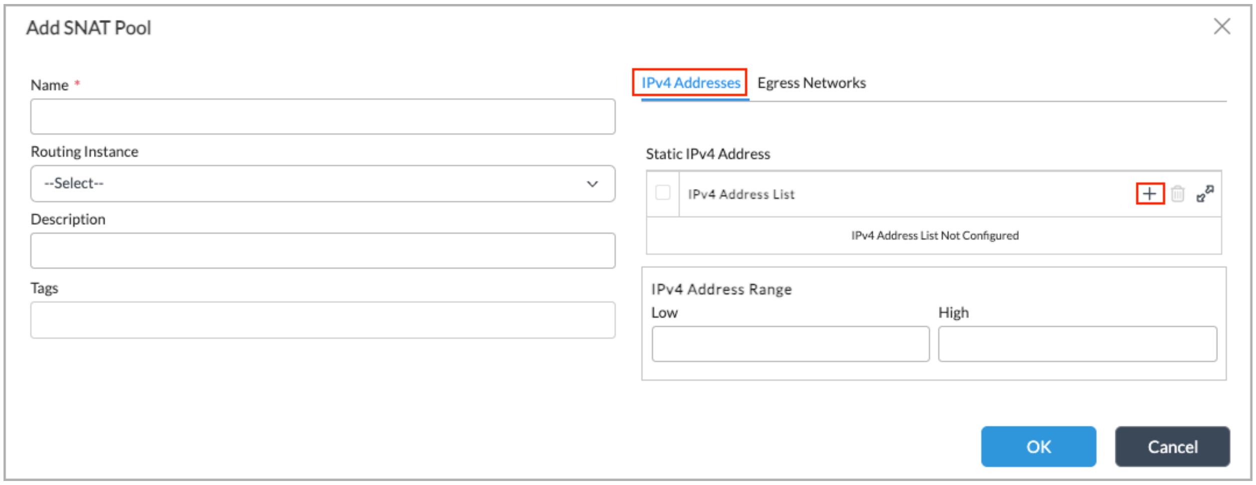
d. To change the configuration temporarily for a device, select Devices > Device in the horizontal menu bar, and then select the device name in the main pane. The view changes to Appliance view.

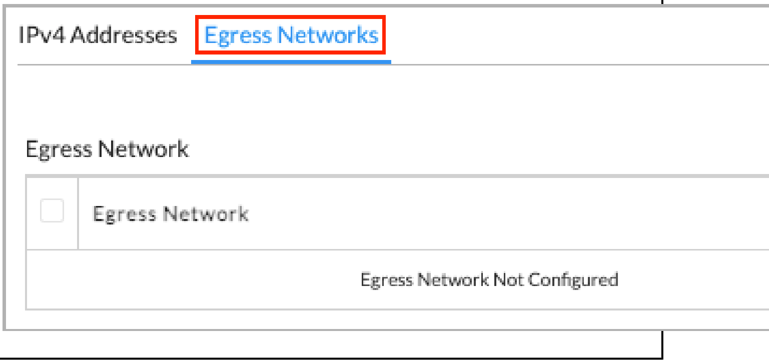


2. If you selected Templates > Device Templates in Step 1c, select a template in the main pane.
3. If you selected Devices > Devices in the Step 1d, select a device in the main pane.
4. Select Objects & Connectors > Objects > SNAT Pool in the left menu bar.



5. Click the + Add icon. In the Add SNAT Pool popup window, enter information for the following fields.


Add SNAT Pool
Name *
Routing Instance
--Select--
Description
Tags
IPv4 Addresses
Egress Networks
Static IPv4 Address
IPv4 Address List
IPv4 Address List Not Configured
IPv4 Address Range
Low
High
OK
Cancel

Field	Description
Name	Enter a name for the SNAT pool.
Description	Enter a text description for the SNAT pool.
Tags	Enter a keyword or phrase that allows you to filter the SNAT pool name. Tags are useful when you have multiple pool names and you want to view those that are tagged with a particular keyword.
Routing Instance	Select the routing instance to associate with the SNAT pool. Typically, you select one of the WAN VRFs, such as Internet-Transport-VR.
IPv4 Addresses (Tab)	Configure an IPv4 SNAT pool to use for cloud lookup requests. You can use either individual static IPv4 addresses or a range of IPv4 addresses, but you cannot use both. Note that for an SNAT pool you can configure either IPv4 addresses or egress networks, but not both.
◦ Static IPv4 Address	Click the + Add icon, and enter an IPv4 static address to add to the SNAT pool.
◦ IPv4 Address Range	Enter the address range of the SNAT pool: ◦ Low—Enter the lowest IPv4 address in the SNAT pool address range. ◦ High—Enter the highest IPv4 address in the SNAT pool address range.
Egress Networks (Tab)	 IPv4 Addresses Egress Networks Egress Network □ Egress Network Egress Network Not Configured

	In the Egress Network table, click the + Add icon and select an egress network to use for cloud lookup requests. Note that for an SNAT pool you can configure either IPv4 addresses or egress networks, but not both.

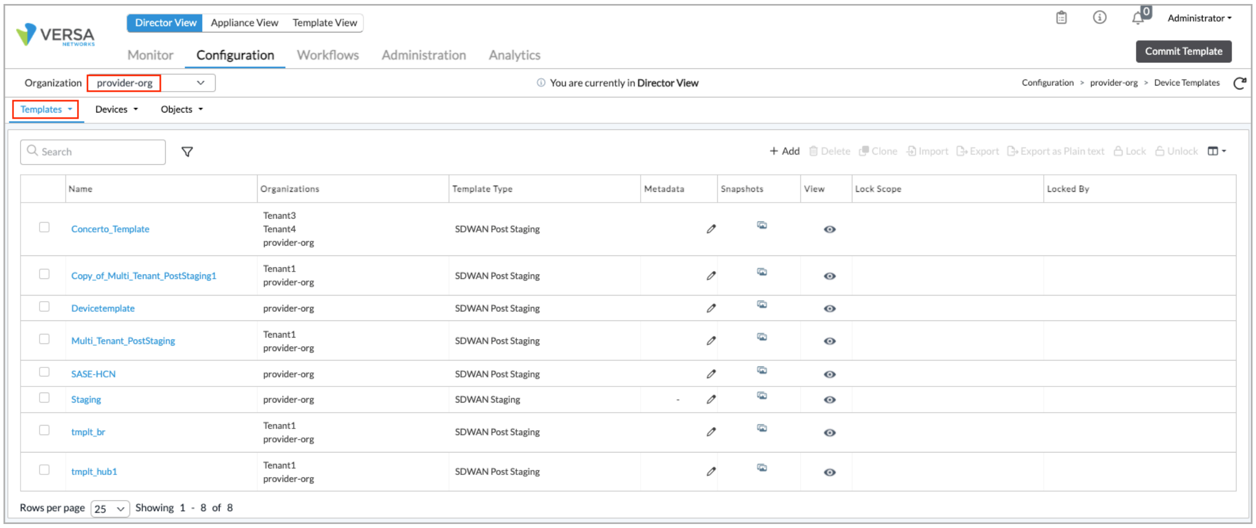
6. Click OK.

Configure a Cloud Profile for Cloud URL Lookup

To enable cloud URL lookup on a VOS device, you must configure a cloud profile to look up information about the URL on a cloud server. For more information, see Configure a Cloud Profile.

To configure a cloud profile for cloud URL lookup:

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select an organization in the Organization field.

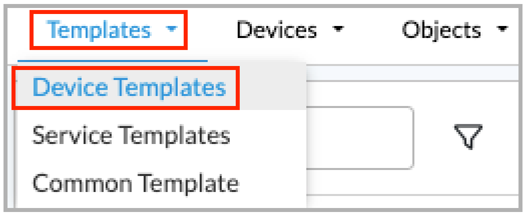


Organization: provider-org

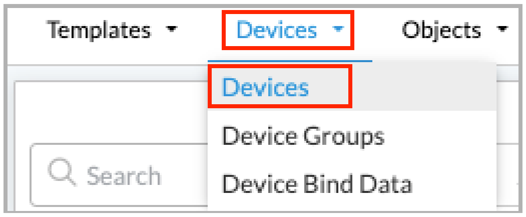
	Name	Organizations	Template Type	Metadata	Snapshots	View	Lock Scope	Locked By
☐	Concerto_Template	Tenant3 Tenant4 provider-org	SDWAN Post Staging	✎	⧉	👁		
☐	Copy_of_Multi_Tenant_PostStaging1	Tenant1 provider-org	SDWAN Post Staging	✎	⧉	👁		
☐	Devicetemplate	provider-org	SDWAN Post Staging	✎	⧉	👁		
☐	Multi_Tenant_PostStaging	Tenant1 provider-org	SDWAN Post Staging	✎	⧉	👁		
☐	SASE-HCN	provider-org	SDWAN Post Staging	✎	⧉	👁		
☐	Staging	provider-org	SDWAN Staging	- ✎	⧉	👁		
☐	tmplt_br	Tenant1 provider-org	SDWAN Post Staging	✎	⧉	👁		
☐	tmplt_hub1	Tenant1 provider-org	SDWAN Post Staging	✎	⧉	👁		

Rows per page 25 Showing 1 - 8 of 8

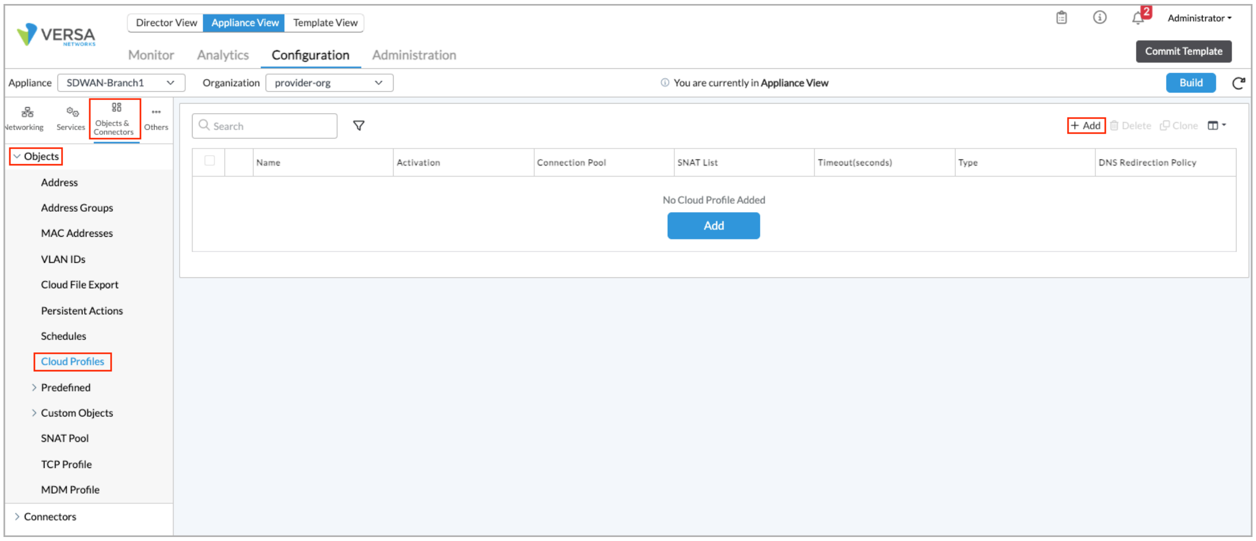
   c. To have the global URL-filtering settings be permanent, select Templates > Device Templates in the horizontal menu bar. Then select the device name or post-staging template name in the main pane. The view changes to Appliance view.



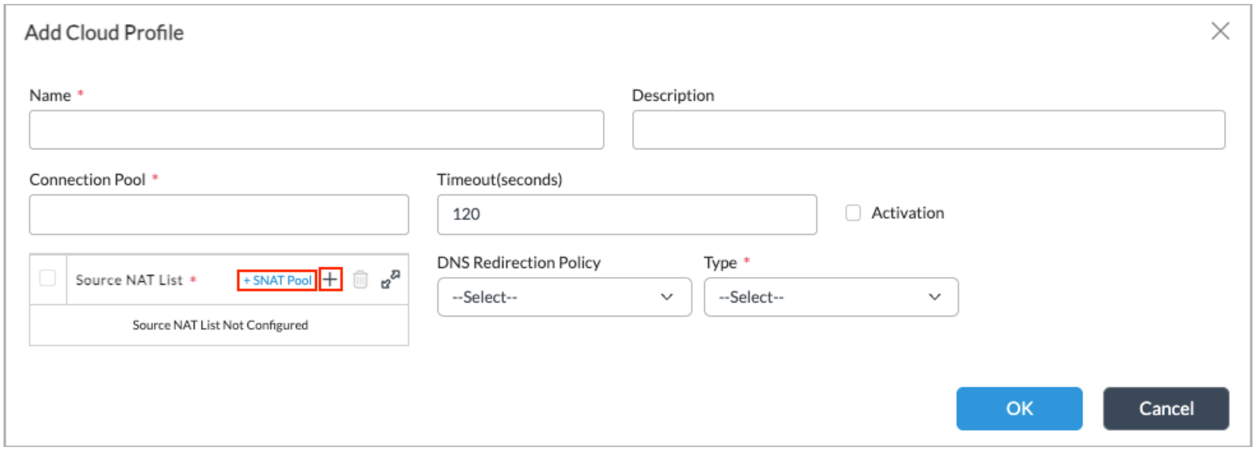
d. To have the global URL-filtering settings apply to an individual device, select Devices > Device in the horizontal menu bar. Then select the device name in the main pane. The view changes to Appliance view.



2. Select Objects & Connectors > Objects > Cloud Profiles in the left menu bar.



3. Click the + Add icon. In the Add Cloud Profile popup window, enter information for the following fields.



Add Cloud Profile

Name *

Description

Connection Pool *

Timeout(seconds): 120

□ Activation

□ Source NAT List * + SNAT Pool

Source NAT List Not Configured

DNS Redirection Policy: --Select--

Type *: --Select--

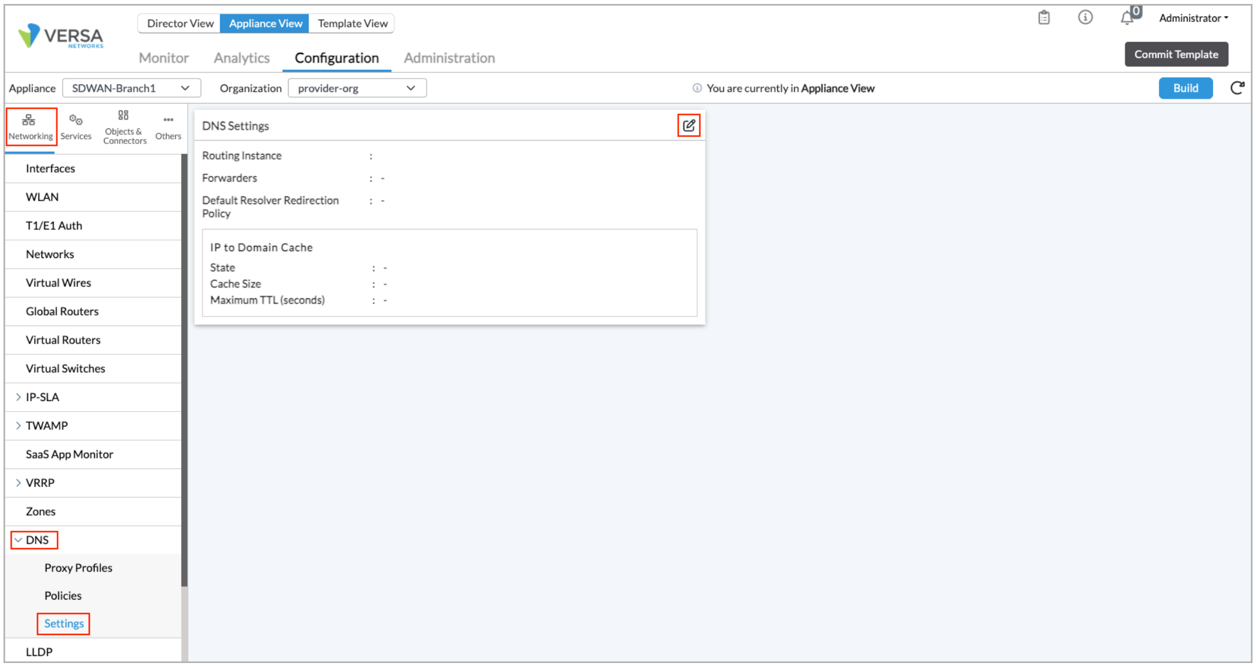
Field	Description
Name	Enter a name for the cloud profile.
Description	Enter a text description for the cloud profile.
Connection Pool	Enter the maximum number of simultaneous connections to the SSL cloud server. enough for cloud URL lookup. *Range*: 1 to 100000 *Default*: None
Timeout	Enter the maximum timeout period to wait for a response from the SSL cloud serve *Range*: 1 through 4294967295 seconds *Default*: 120 seconds
Activation	Click to activate the cloud-lookup profile. If you do not activate the cloud-lookup pro
Source NAT Pool	Select the SNAT pool you configured in the previous section to configure the cloud
DNS Redirection Policy	You do not need to select a DNS redirection policy for cloud URL lookup.
Type	Select URLF Cloud Profile.

4. Click OK.

Configure DNS Proxy

To look up the URL of a cloud server, you must configure a DNS proxy for the transport selected for the SNAT pool:

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > DNS > Settings in the left menu bar. The main pane displays the DNS Settings pane.

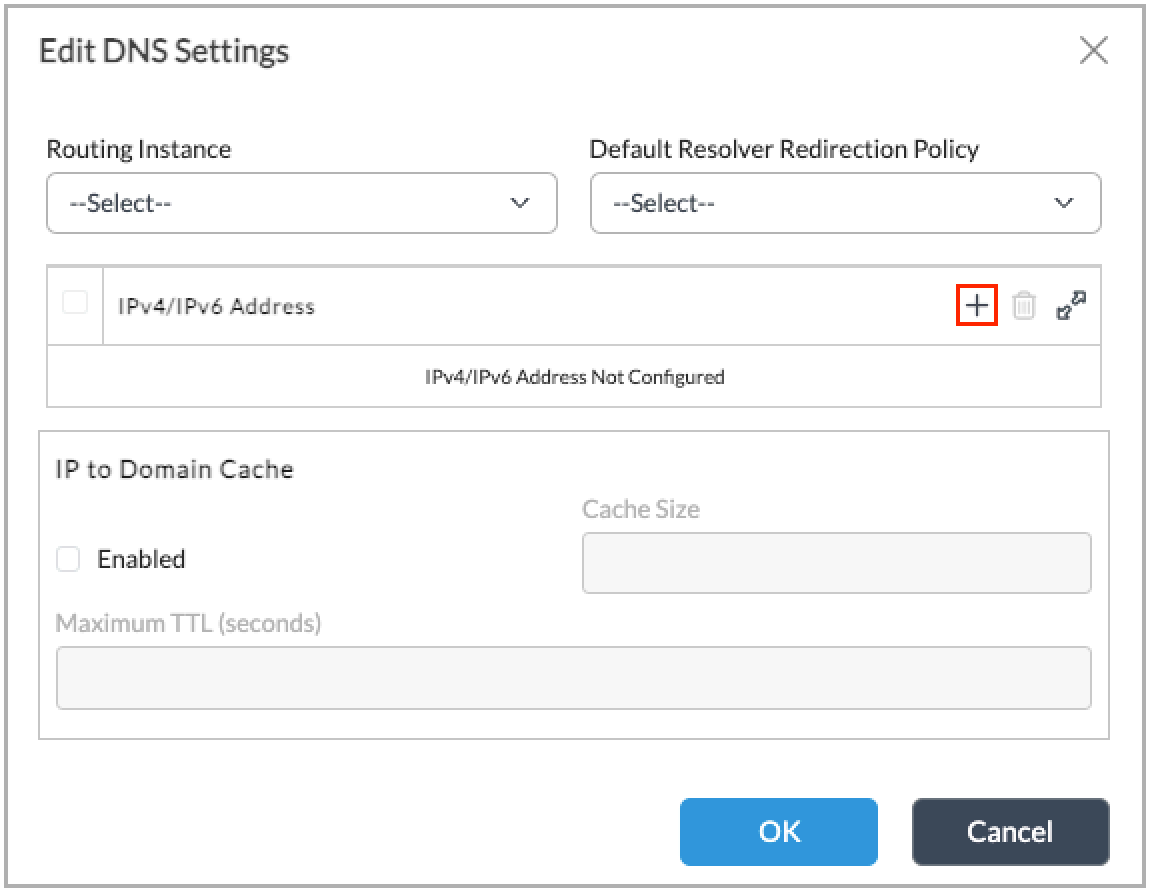


DNS Settings

Routing Instance :
Forwarders : -
Default Resolver Redirection Policy : -

IP to Domain Cache
State : -
Cache Size : -
Maximum TTL (seconds) : -

4. Click the Edit icon. In the Edit DNS Settings popup window, enter the following information.



Edit DNS Settings

Routing Instance: --Select--

Default Resolver Redirection Policy: --Select--

□ IPv4/IPv6 Address

IPv4/IPv6 Address Not Configured

IP to Domain Cache

□ Enabled

Cache Size

Maximum TTL (seconds)

Field	Description
Routing Instance	Select the routing instance to use to reach the DNS server.
Default Resolver Redirection Policy	Select the default resolver redirection policy to resolve domains.
IPv4/IPv6 Address	Click the + Add icon, then enter the IPv4 or IPv6 address of the DNS server. You can enter mulitple IP addresses.
IP to Domain Cache (Group of Fields)	
◦ Enabled	Click to enable caching of IP address to domain lookup information.
◦ Cache Size	Enter the maximum number for cache entries.
◦ Maximum TTL (seconds)	Enter the maximum time-to-live value, in seconds.

5. Click OK.

Configure Captive Portal

To control the URLs that users can view when they are accessing internet webpages, you can configure captive portal. For the URLs whose access you want to control, you redirect users to a captive portal webpage on which you can display standard or customized messages that provide information about the webpage. For these webpages, you can control access or block access completely. You associate the captive portal pages with specific URLs or URL categories when you define the action, or enforcement, clause in a URL-filtering policy.

For Releases 21.2.1 and later, you can configure service endpoints with captive portal, which allow you to install service filters for each routing instance. Service endpoints provide a service for a particular IP address or a list of IP addresses instead of using wildcard host addresses for each routing instance. You can define clear-text (HTTP) and secure traffic ports (HTTPS) for captive portal, and you can define URLs and certificates for each routing instance.

To configure captive portal, you create a URL-filtering profile that includes a captive portal action, and then you enable URL filtering in the security access policy rule, as described in Configure Security Access Policy Rules. You can include predefined and customizable captive portal actions in the URL-filtering profile.

For the captive portal page itself, you can display one of the standard VOS pages, or you can upload and use a custom page.

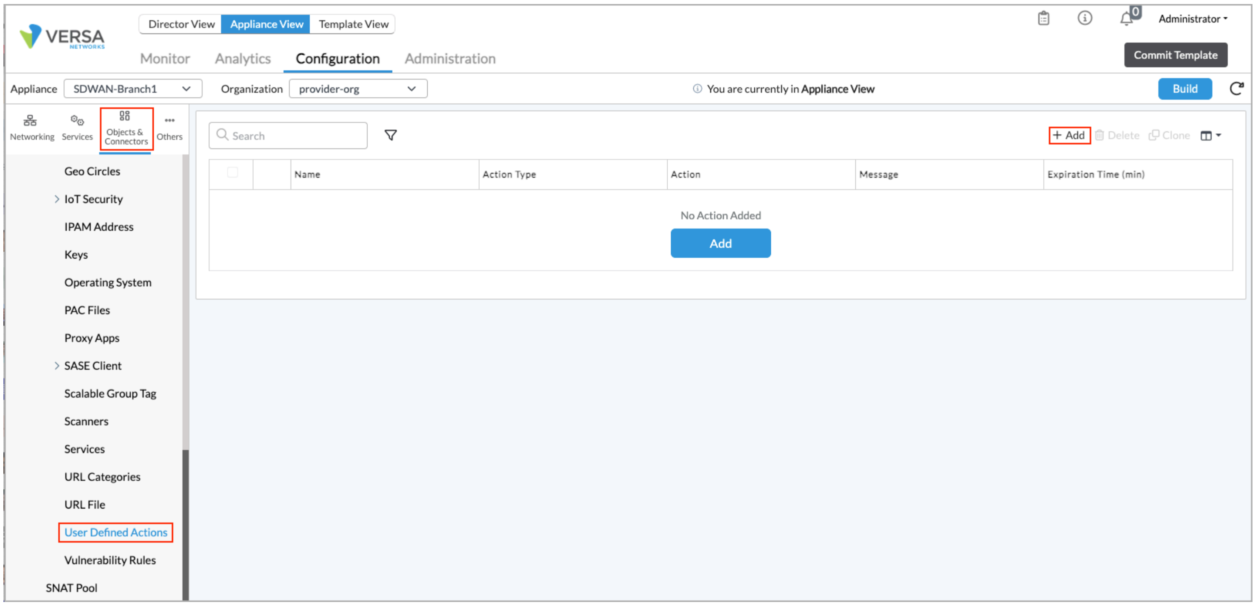
For captive portal to work, you must enable SSL decryption in order to redirect URL requests to captive portal pages. If you do not enable SSL decryption, the SSL connection is allowed if the captive portal action is set to Inform, and the connection is reset if the action is set to Block, Ask, Justify, or Override.

Configure Captive Portal

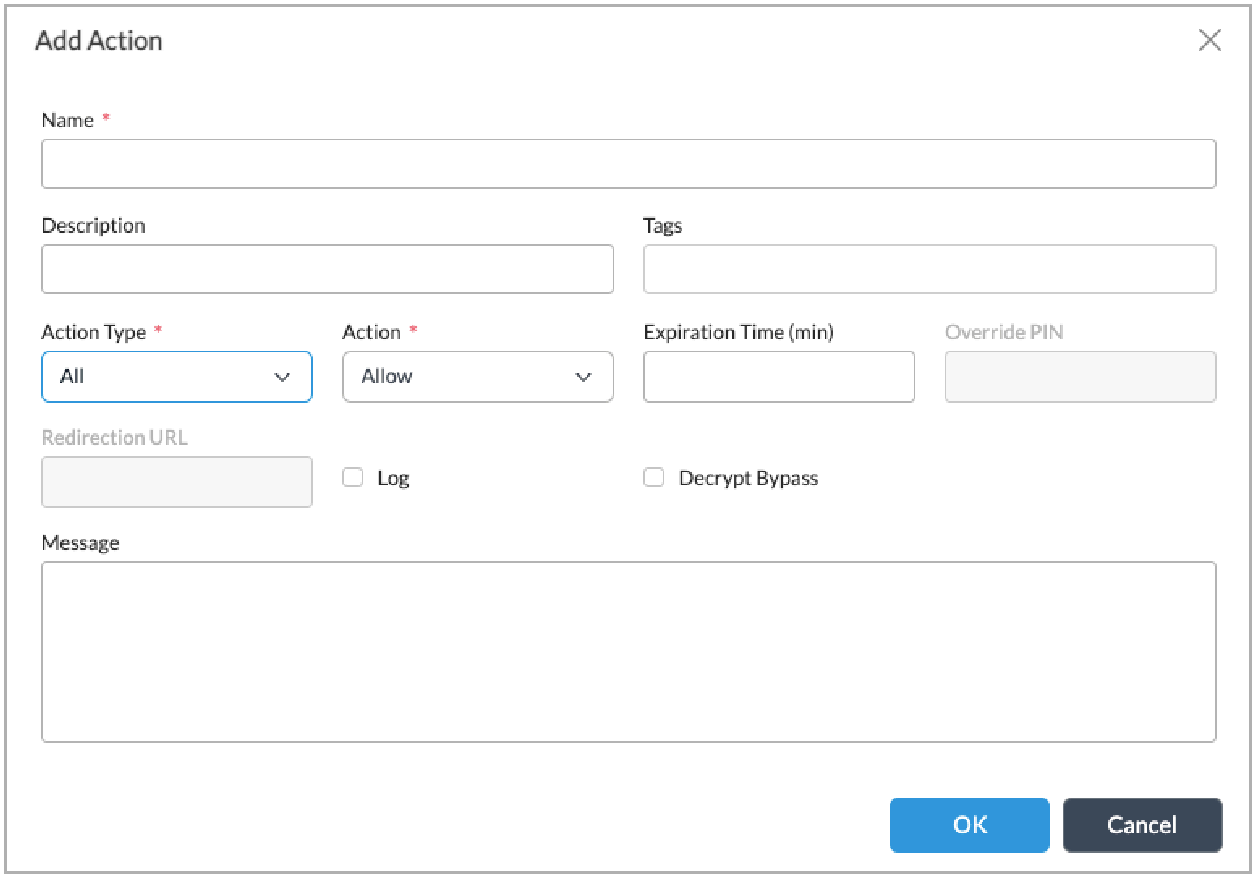
To display the default VOS captive portal pages with the default messages, you must configure predefined captive portal actions. To customize messages on the default captive portal pages or on captive portal pages that you have uploaded, or to set an override PIN, you must to create user-defined actions.

To configure captive portal, you create a captive portal action that you then associate with a URL-filtering profile:

1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Configuration > Objects & Connectors > Objects > Custom Objects > User-Defined Actions in the left menu bar.



4. Click the + Add icon. In the Add Action popup window, enter information for the following fields.



Add Action

Name *

Description

Tags

Action Type * All

Action * Allow

Expiration Time (min)

Override PIN

Redirection URL

□ Log

□ Decrypt Bypass

Message

Field	Description
Name	Enter a name for the captive portal action. The name cannot contain spaces or special characters except for underscores (_) and hyphens (-).
Description	Enter a text description for the captive portal action.
Tags	Enter a keyword or phrase that allows you to filter the captive portal action. This is useful when you have many actions and want to view those that are tagged with a particular keyword.
Action Type	Select the type of predefined action to take when the page is redirected: ◦ All ◦ CASB (for Releases 22.1.3 and later) ◦ Decrypt ◦ DNS (for Releases 22.1.3 and later) ◦ IPS ◦ IPREP ◦ URLF The action type options represent the module for which the user-defined action was configured. For example, if the value is URLF, the action can be used only in URL-filtering profiles.
Action	Select the action to take when a user is redirected to a captive portal: ◦ Allow—Allow the URL without generating an entry in the URL-filtering log. You can apply the the Allow action to all action types. ◦ Ask—The browser presents an information page that prompts the user to either cancel the operation by clicking Cancel or continue with the operation by clicking OK (for HTTP and HTTPS). You can apply the the Ask action to the following Action types: ▪ IPREP ▪ URLF

	◦ Block—Block the URL and generate an entry in the URL-filtering log. No response page is displayed, and the user cannot continue to the website. You can apply the the Block action to the following Action types: ▪ CASB (for Releases 22.1.3 and later) ▪ DNS (for Releases 22.1.3 and later) ▪ IPREP ▪ URLF ◦ Custom Redirection—The browser redirects the user to the specified URL. Session information such as the URL requested by the user, the IP address of the HTTP/HTTPS request, and the URL-filtering profile to process are included in the redirected URL to the web server that hosts the redirected URL page. After the redirection occurs, the external web server, not the VOS device, handles the captive portal functionality. You can customize the session information parameters that are passed to the web server. For more information, see Modify Captive Portal Settings. You can apply the Override action to the following Action types: ▪ IPREP ▪ URLF ◦ Drop Packet—The browser waits for a response from the server and then drops the packets. It is not possible to determine whether the packet was dropped because of a delayed response from the server or because a firewall blocked access to the website. You can apply the the Drop Packet action to the following Action types: ▪ Decrypt ▪ DNS (for Releases 22.1.3 and later) ▪ IPS ▪ URLF ◦ Drop Session—The browser waits for a response from the server and drops the session. It is not possible to determine whether the session was dropped because of a delayed response from the server or because a firewall blocked access to the website. You can apply the the Drop Session action to all Action types. ◦ Inform—The browser presents an information page that prompts the user to continue after clicking OK (for HTTP and HTTPS). You can

	apply the the Inform action to the following Action types: ▪ IPREP ▪ URLF ◦ Justify—The browser presents an information page that prompts the user to either cancel the operation by clicking Cancel or continue with the operation after entering a justification message and clicking OK (for HTTP and HTTPS). You can apply the Justify action to the following Action types: ▪ IPREP ▪ URLF ◦ Override—The browser prompts the user to enter a PIN (4 to 6 digits). This action generates an entry in the URL-filtering log. You can apply the Override action to the following Action types: ▪ IPREP ▪ URLF ◦ Reset Client—The host responds by sending a TCP Reset packet to the client, and the browser displays an error message indicating that the connection has been reset. It is not possible to determine whether the web server reset the connection or the firewall reset the session. You can apply the the Reset Client action to the following Action types: ▪ DNS (for Releases 22.1.3 and later) ▪ IPS ◦ Reset Client and Server—The host responds by sending a TCP Reset packet back to the client and server. The browser displays an error message indicating that the connection was reset. It is not possible to determine whether the web server reset the connection or the firewall reset the session. You can apply the the Reset Client and Server action to all Action types. ◦ Reset Server—The host responds by sending a TCP Reset packet to the server. The browser waits for a response from the server and then drops the session. It is not possible to determine whether the session was dropped because of a delayed response from the server or because a firewall blocked access to the website. You can apply the the Reset Server action to the following Action types:

	▪ DNS (for Releases 22.1.3 and later) ▪ IPS ◦ Sink Hole—(For Releases 22.1.3 and later.) Resolve disallowed domains to a sinkhole server. You can apply the Override action to the following Action types: ▪ DNS ▪ IPREP ▪ URLF
Expiration Time	Enter how often to redirect a user to the captive portal, in minutes. When a user first enters a URL and is redirected to a captive portal page, the VOS device creates a cache entry, which expires after a global expiration time. While the cache entry is active, the device does not enforce the captive portal action, and users can view the webpage at the initial URL and at all URLs that belong to the same URL category, without seeing the captive portal page, with one exception. If the captive portal action is Block, all URLs are redirected to the Block page, regardless of the expiration time. For information about global expiration time setting, see Modify Captive Portal Settings. *Range*: 1 through 65535 minutes *Default*: 30 minutes
Override PIN	For the Override action, enter the PIN value, which is a 4-, 5-, or 6-digit number.
Redirection URL	For the Custom Redirection action, enter the URL to which to redirect the user.
Log	Click to log captive portal actions. If you do not enable logging, the custom message that you enter in the Message field is not displayed in the log displayed in Versa Analytics.
Decrypt Bypass	Click to disable SSL encryption for matching traffic, to allow you to define websites that are not subject to decryption.

Message	Enter a message to display on the captive portal page.

5. Click OK.
6. Configure a URL-filtering profile, as described in Configure a URL-Filtering Profile.
7. Configure security access policy rules, as described in Configure Security Access Policy Rules.

Upload a Custom Captive Portal Page

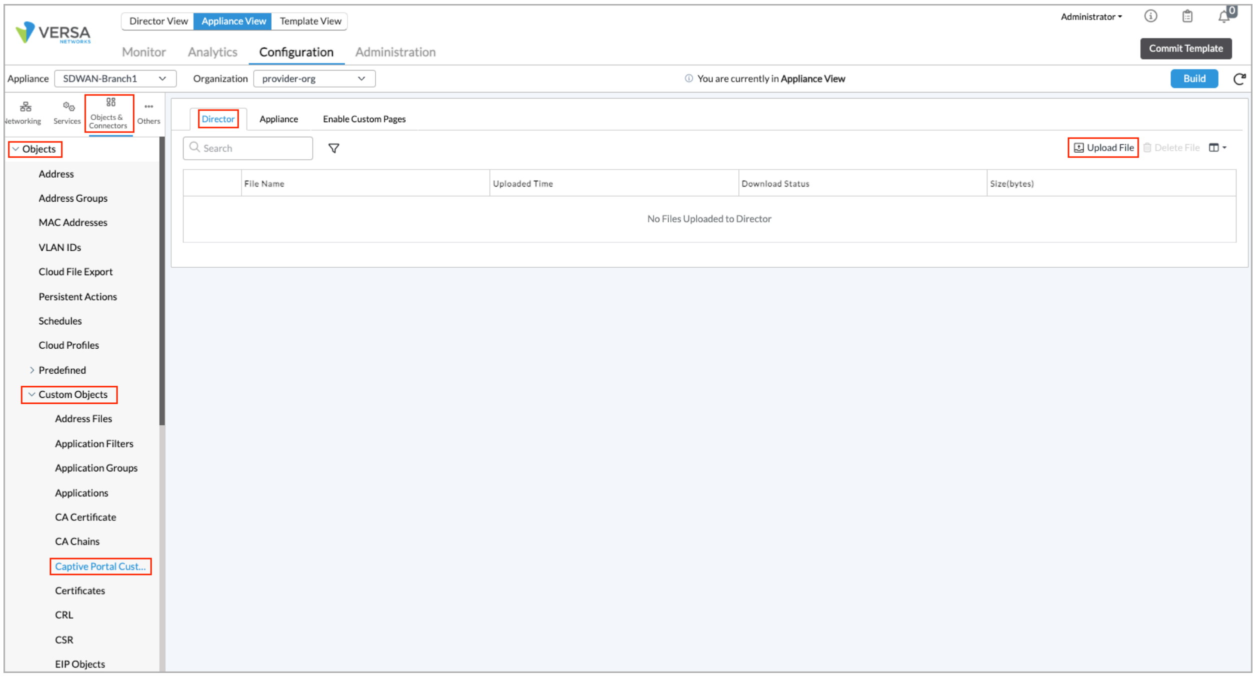
If you do not want to use one of the default VOS captive portal pages, you can upload a custom captive portal page. You must compress the files for the captive portal webpage into a .zip file. The main index file in the .zip file must be named index.htm, and it must contain the custom captive portal page HTML files, CSS files, and image files. You can use the following variables in the index.htm file:

- $category—Display the URL category to which the URL belongs.
- $host—Display the IP address of the client machine.
- $message—Display a message to the user.
- $reputation—Display the reputation of the URL.
- $url—Display the URL that the user is attempting to access.
- $user—Display the name of the user.

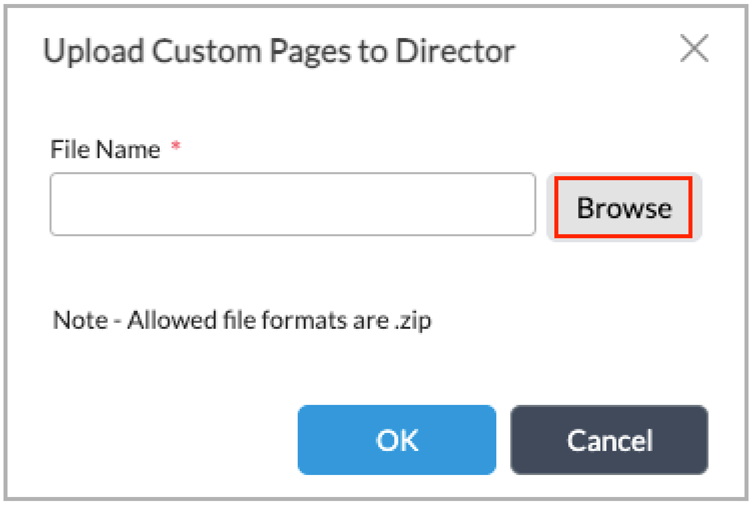
To upload a custom captive portal page:

Note: In addition to using the following procedure, you can also upload custom captive portal pages using the files and folders feature. For more information, see Manage Files and Folders.

1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select an organization in the left menu bar.
    c. Select Devices > Devices in the horizontal menu bar.
    d. Or, select the Administration tab in the top menu bar, and select Appliances in the left menu bar.
    e. Select a device name in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Custom Objects > Captive Portal Custom Pages in the left menu bar. The main pane displays a list of the custom captive portal pages that have already been uploaded to the Director node.



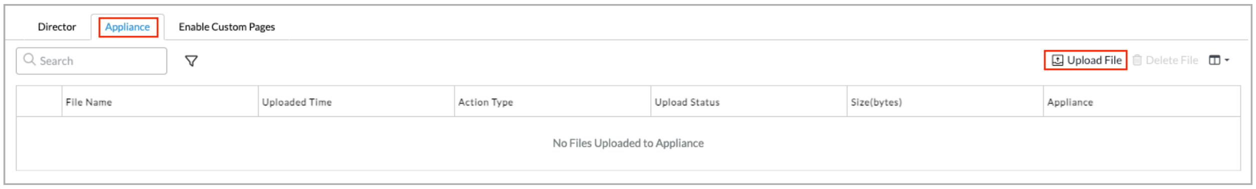
4. Select the Director tab in the horizontal menu bar.
5. Click the 📤 Upload icon.
6. In the Upload Custom Pages Director popup window, click Browse to select the .zip file that contains custom captive portal page.


Upload Custom Pages to Director

File Name *

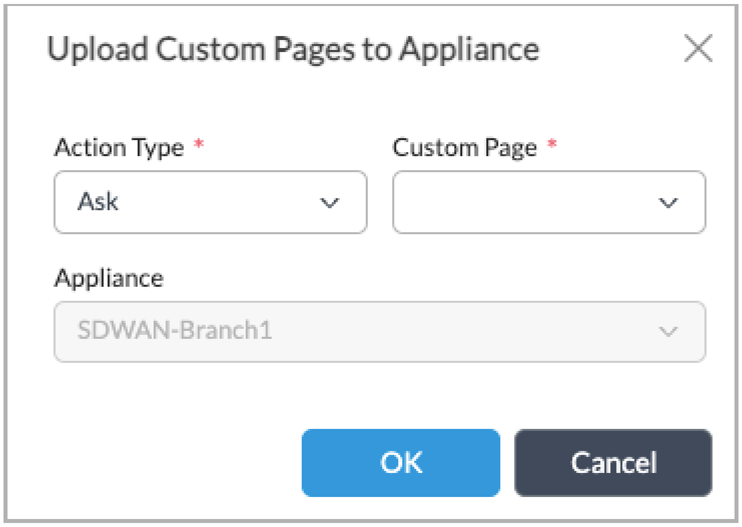
Note - Allowed file formats are .zip

7. Click OK.
8. Select the Appliance tab in the horizontal menu bar.



	File Name	Uploaded Time	Action Type	Upload Status	Size(bytes)	Appliance
	No Files Uploaded to Appliance					

9. Click the Upload icon. In the Upload Custom Pages to Appliance popup window, enter information for the following fields.



Upload Custom Pages to Appliance

Action Type * : Ask

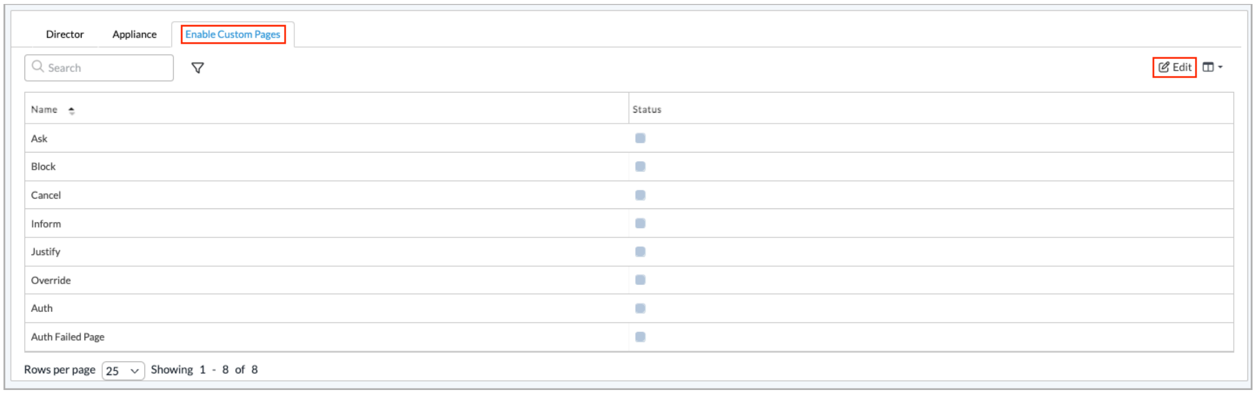
Custom Page * :

Appliance: SDWAN-Branch1

Field	Description
Action Type	Select the action to take when a user attempts to access a URL: ◦ Ask—Prompt the user to confirm that they want to visit the webpage that they are browsing. If a user confirms, they are redirected to the webpage. Otherwise, the operation is canceled. ◦ Auth—(For Releases 22.1.3 and later.) Display the Authentication page when the user is redirected for local or LDAP authentication. ◦ Auth Fail—(For Releases 22.1.3 and later.) Display the Authentication Fail page when local or LDAP user authentication fails. ◦ Block—Deny access to the webpage. ◦ Cancel—Display the Cancel page when a user clicks Cancel on the Ask, Justify, or Override captive portal page. ◦ Inform—Redirect the user to a webpage containing an information message. After the user reads the message, they are redirected to the requested webpage. ◦ Justify—Prompt the user to enter a justification message and click continue before they are allowed to go to the requested webpage. The justification message entered by the user is logged to Versa Analytics. ◦ Override—Prompt the user to enter the override PIN value. A user can access the requested webpage only if they enter a valid PIN. Logs are sent to Versa Analytics when users attempt to enter the PIN and then continue to the webpage.
Custom Page	Select the custom page from the list of uploaded custom page .zip files.
Appliance	Displays the device that you selected in Step 1.

10. Select the Enable Custom Pages tab to enable the action types for the captive portal.

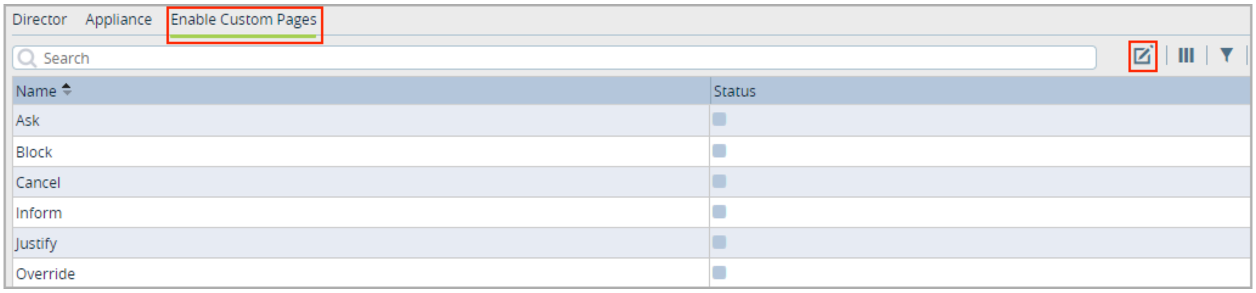
    For Releases 22.1.3 and later:



Name	Status
Ask	■
Block	■
Cancel	■
Inform	■
Justify	■
Override	■
Auth	■
Auth Failed Page	■

Rows per page 25 Showing 1 - 8 of 8

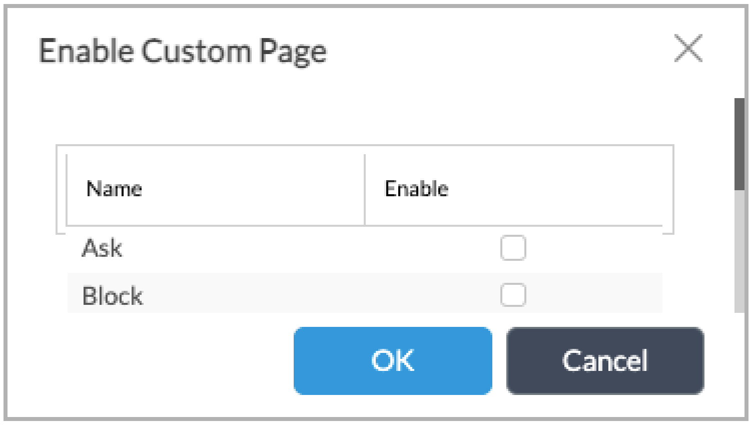
For Releases 21.2 and earlier:



Name	Status
Ask	■
Block	■
Cancel	■
Inform	■
Justify	■
Override	■

11. Click the Edit icon. The Enable Custom Page popup window displays.

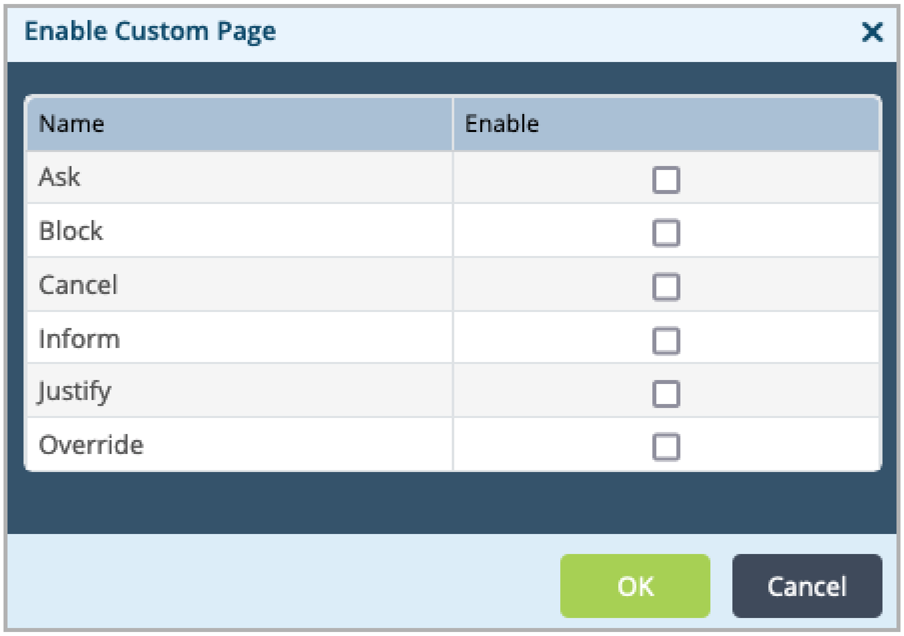
For Releases 22.1.3 and later:



Enable Custom Page

Name	Enable
Ask	☐
Block	☐

For Releases 21.2 and earlier:



Enable Custom Page

Name	Enable
Ask	□
Block	□
Cancel	□
Inform	□
Justify	□
Override	□

12. Click one or more action types to associate with the custom captive portal page. In the Releases 22.1.3 and later, use the scroll bar to view all the action types.
    - Ask
    - Block
    - Justify
13. Click OK.

Modify Captive Portal Settings

Some captive portal actions are supported by default, and you do not need to customize their configuration. However, you must customize other actions, such as override or inform. For example, configuring an override action with a default PIN might cause security issues, because the default PIN is compromised easily. Therefore, only the following captive portal actions are supported as predefined captive portal actions:

- Ask
- Block
- Justify

The default expiration time for the predefined captive portal actions is 30 minutes. When the user is redirected to a captive portal page that corresponds to a predefined captive portal action, the default message is displayed. To display a different message, you must create a user-defined captive portal action of the appropriate type with the custom message.

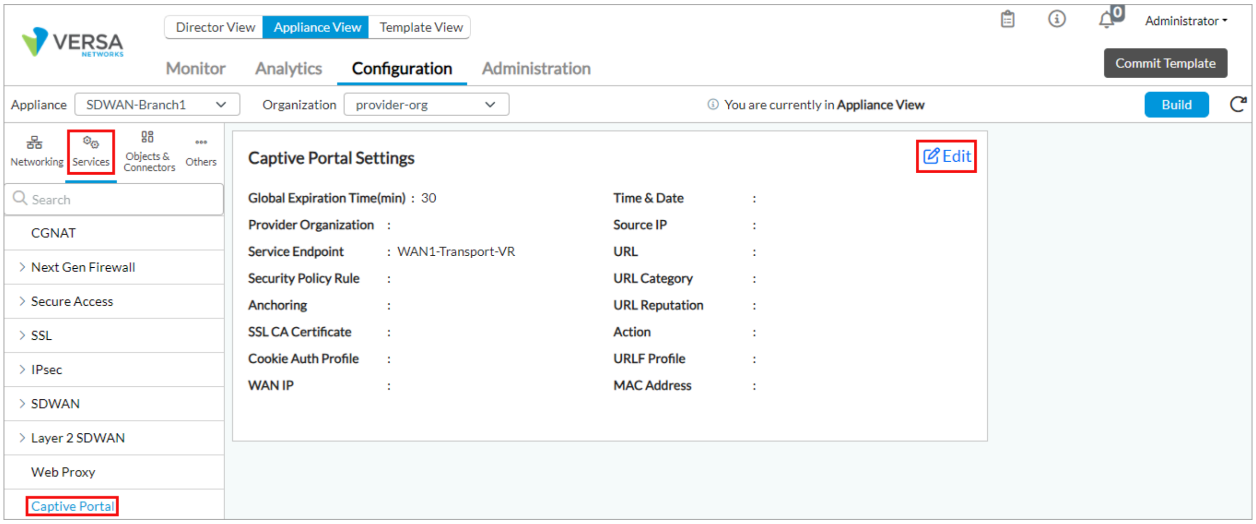
To view the predefined captive portal settings for a VOS device:

1. In Director view:

   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Captive Portal in the left menu bar. The Captive Portal Settings pane displays the captive portal settings.

To modify the predefined captive portal settings:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Captive Portal in the left menu bar. The dashboard displays the Captive Portal Settings pane.

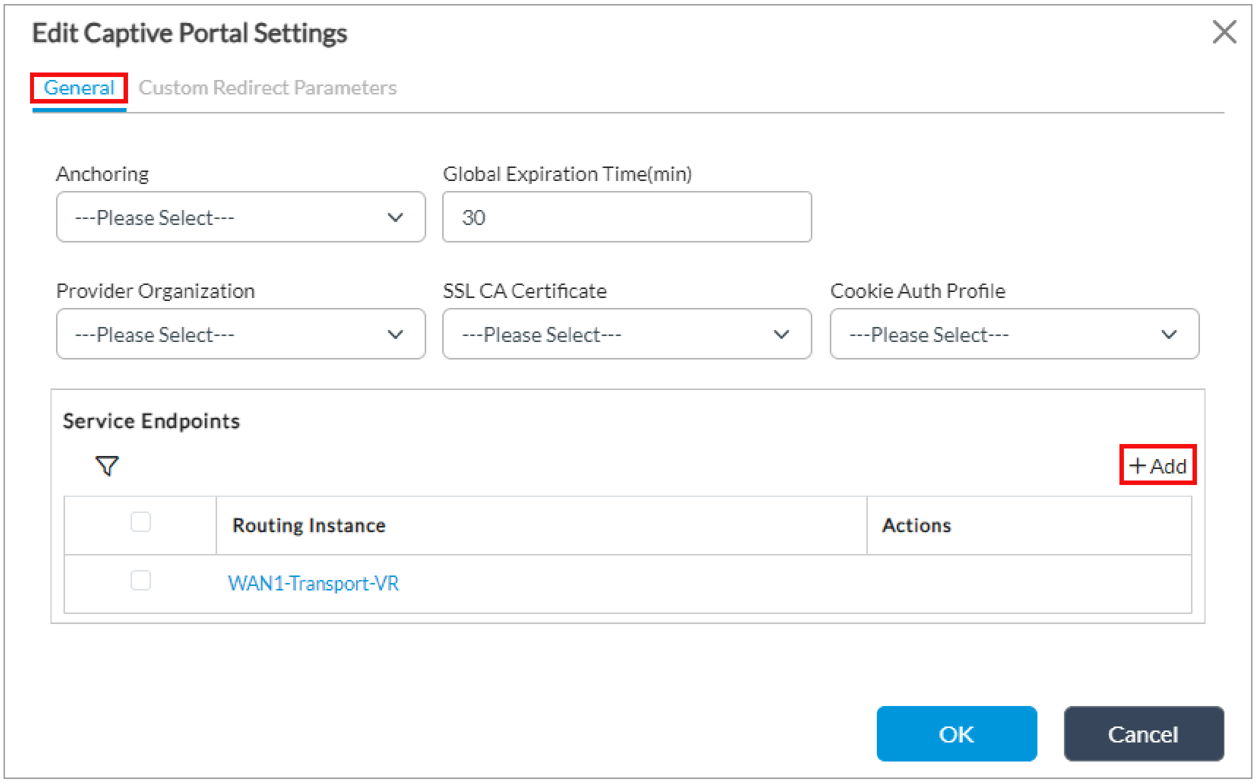


Appliance: SDWAN-Branch1
Organization: provider-org
You are currently in Appliance View

Captive Portal Settings

Global Expiration Time(min)	30	Time & Date	
Provider Organization		Source IP	
Service Endpoint	WAN1-Transport-VR	URL	
Security Policy Rule		URL Category	
Anchoring		URL Reputation	
SSL CA Certificate		Action	
Cookie Auth Profile		URLF Profile	
WAN IP		MAC Address	

4. Click the Edit icon. The Edit Captive Portal Settings popup window displays.
5. Select the General tab, and then enter information for the following fields.



Edit Captive Portal Settings

Anchoring: ---Please Select---

Global Expiration Time(min): 30

Provider Organization: ---Please Select---

SSL CA Certificate: ---Please Select---

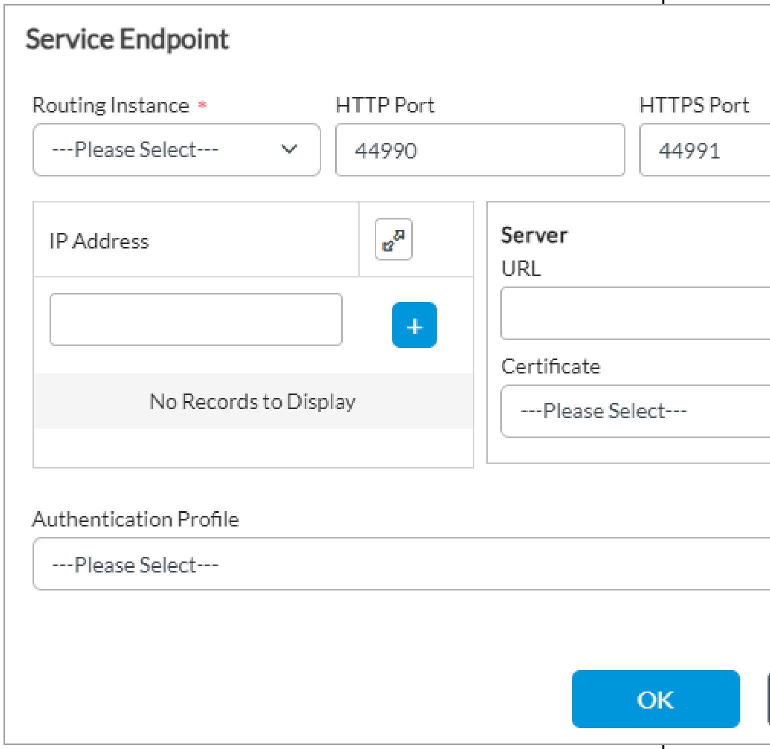
Cookie Auth Profile: ---Please Select---

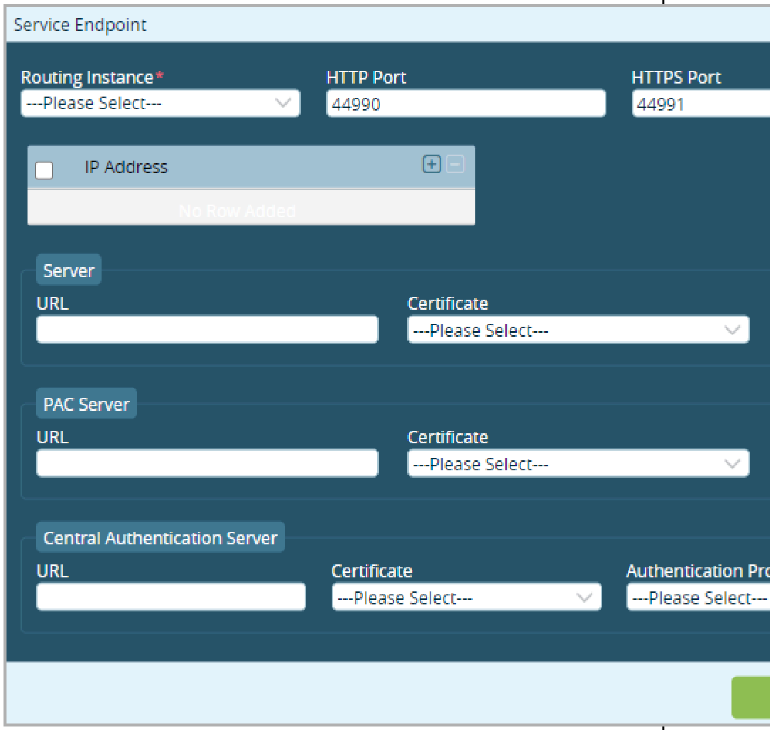
Service Endpoints

□	Routing Instance	Actions
□	WAN1-Transport-VR	

Field	Description
Anchoring	Select the mechanism to use to cache the captive portal action. After the captive portal page is displayed to the user, the VOS device caches the action and the cache entry is keyed to an anchor type: ◦ Both IP and MAC addresses—Set the cache key to a combination of the source IP address and the source MAC address of the URL request. ◦ IP address—Set the cache key to the source IP address of the. requested URL. ◦ MAC address—Set the cache key to the source MAC address of the requested URL. After creating the cache entry, the VOS device does not enforce the captive portal action on subsequent requests to any URL that belongs to the same URL category as the cache entry, based on the anchor type.
Global Expiration Time	Enter how often users are redirected to the captive

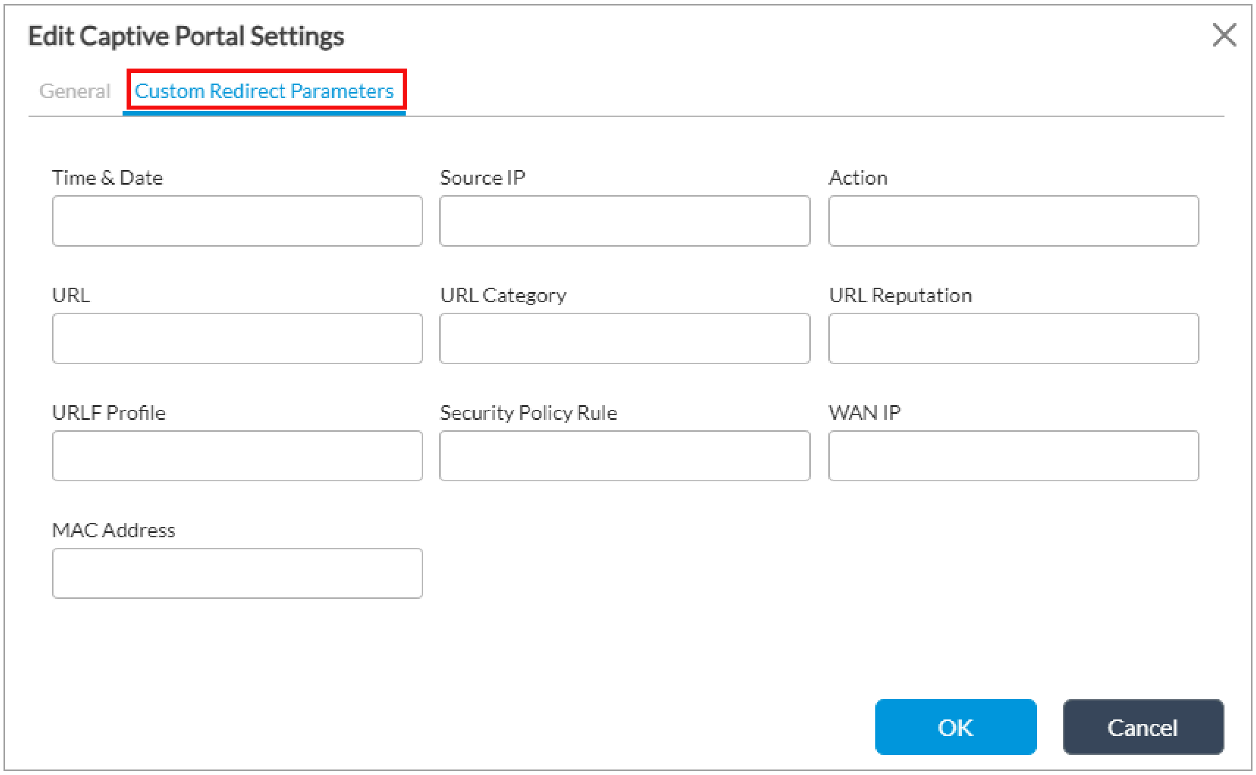
Field	Description
	portal, in minutes. The first time a user enters a URL and is redirected to a captive portal page, the VOS device creates a cache entry. This cache entry expires after the global expiration time. Between the first time the user is redirected to the captive portal page and the expiration time, the captive portal action is not enforced and the user can go to the URL directly, without first seeing the captive portal page. *Range:* 1 through 65535 minutes *Default:* 30 minutes
Provider Organization	Select the provider organization associated with the captive portal, to allow captive portal to display provider-branded webpages.
SSL CA Certificate	Select the CA certificate to use for the captive server portal over SSL.
Cookie Auth Profile	(For Releases 22.1 and later.) Select an authentication profile to authenticate cookies. For more information, see Configure an Authentication Profile.
Service Endpoints	(For Releases 21.2.1 and later.) Displays the routing instance selected as the service endpoint for the captive portal. Click the + Add icon to add a service endpoint. The Service Endpoint popup window displays. Enter information for the following fields. For Releases 22.1.3 and later:

Field	Description
	 Service Endpoint Routing Instance *: ---Please Select--- HTTP Port: 44990 HTTPS Port: 44991 IP Address No Records to Display Server URL Certificate: ---Please Select--- Authentication Profile: ---Please Select--- For Releases 21.2 and earlier:

Field	Description
	 Service Endpoint Routing Instance* ---Please Select--- HTTP Port 44990 HTTPS Port 44991 IP Address No Row Added Server URL Certificate ---Please Select--- PAC Server URL Certificate ---Please Select--- Central Authentication Server URL Certificate ---Please Select--- Authentication Pro ---Please Select--- ◦ Routing Instance—Select the routing instance (VRF) to use to access the captive portal pages. If you do not select a routing instance, captive portal pages are enabled only in the global routing instance. ◦ HTTP Port—Enter the number of the HTTP port to use to redirect captive portal pages over HTTP. *Default*: 44990 ◦ HTTPS Port—Enter the number of the HTTPS port to use to redirect captive portal pages over HTTPS. *Default*: 44991 ◦ IP Address—Click the + Add icon to add a service endpoint IP address. Any traffic destined to these IP addresses are serviced by the captive portal. Captive portal redirection that is based on the server URL is routed to one of these IP addresses. ◦ Authentication Profile—Select the authentication profile to use. ◦ Server (Group of Fields) ▪ URL—Enter the captive portal server URL

Field	Description
	that is used to redirect traffic when any captive portal action is applied. This URL resolves to one of the IP address in the IP address list. ▪ Certificate—Select the certificate to use for captive portal over SSL. ◦ PAC Server (Group of Fields) (For Release 21.2 and earlier.) ▪ URL—Enter the URL of the proxy autoconfiguration (PAC) file to configure a URL proxy. A PAC file defines how web browsers can automatically choose the appropriate proxy server to fetch a given URL. You can upload PAC files to a VOS device. For more information, see Upload PAC Files. ▪ Certificate—Select the certificate to use for the PAC URL. ◦ Central Authentication Server (Group of Fields) (For Release 21.2 and earlier.) ▪ URL—Enter the URL of the central authentication server. ▪ Certificate—Select the CA certificate to use for the captive server portal over SSL. ▪ Authentication Profile—Select the authentication profile to use to authenticate the central authentication server.

6. Select the Custom Redirect Parameters tab to configure URL query parameters. These parameters are text strings that provide additional information to the web server that is making the request, and they are attached to the end of the redirect URL Note that you can redirect requests to different locations based on the URL category, URL reputation, or URL allow list and deny list match criteria.



Edit Captive Portal Settings

Field	Description
Time & Date	Enter the text string to use as the timestamp when a user session is redirected to the URL hosted on the external web server.
Source IP	Enter the text string to use as the source IP address of the session for which to redirect to the external web server.
Action	Enter the text string to use as the user-defined action that redirects users to the external web server.
URL	Enter the text string to use as the URL to redirect to the external web server.
URL Category	Enter the text string to use as URL category to redirect to the external web server.
URL Reputation	Enter the text string to use as the URL reputation to redirect to the external web server.
URLF Profile	Enter the text string to use as the URL-filtering profile to redirect to the external web server.
Security Policy Rule	Enter the text string to use as the security profile to redirect to the external web server.
WAN IP	(For Releases 22.1.4 and later.) Enter the text string to use as the IP address of the WAN interface to redirect to the external web server.
MAC Address	(For Releases 22.1.4 and later.) Enter the text string to use as MAC address to redirect to the external web server.

7. Click OK.

Configure URL Files

When you configure URL category objects, you can enter the URLs and URL reputations individually or you can enter them in a file and then upload the file while you are adding the URL category. To use a file when you are configuring URL categories objects, you create a CSV file and then upload it.

Each line in the CSV file specifies a single URL and its associated reputation. Each line has three values and can be in one of the following formats:

string,*url*,*url-reputation*

patterns,*regex-pattern*,*url-reputation*

The first value of each line must be the keyword *string* or *patterns*. The value *string* indicates that the second value is a fully qualified domain name. The value *patterns* indicates that the second value is a regular expression (regex) that matches one or more URLs. In the regex pattern, you must escape the backslash (\) and open curly brace ({) characters by preceding them with a backslash. For example, to specify the regex pattern

```
([^\/.]+.)?[0-5-7|1]{0,5}microsoftonline.com/.*%$
```

You enter it as follows:

```
([^\\/.]+.)?[0-5-7|1]\{0,5}microsoftonline.com/.*%$
```

The third value in each line is the URL's reputation. The reputation can be one of the following values, which are listed in order from safest (or most trustworthy) to riskiest:

- trustworthy
- low_risk
- moderate_risk
- suspicious
- high_risk
- undefined

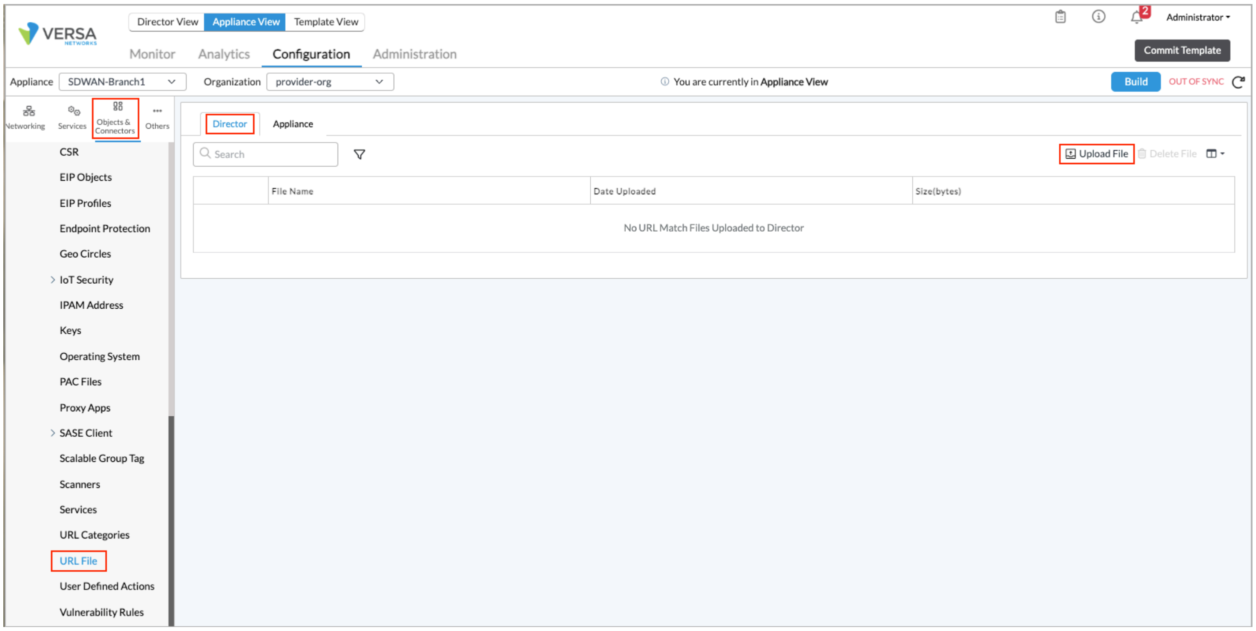
The following are examples of lines you can include in the CSV file:

- patterns,.*google.*,low_risk
- patterns,.*bing.*,low_risk
- string,www.facebook.com,undefined
- patterns,.*versa-networks.*,trustworthy
- patterns,.*twitter.*,moderate_risk

Each file can contain a maximum 65,535 lines.

Upload URL Files

1. In Director view:
    a. Select the Configuration tab in the top menu bar.
    b. Select Devices > Devices in the horizontal menu bar.
    c. Select an organization in the left menu bar.
    d. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Custom Objects > URL File in the left menu bar. The main pane displays the list of uploaded URL files.



Appliance SDWAN-Branch1

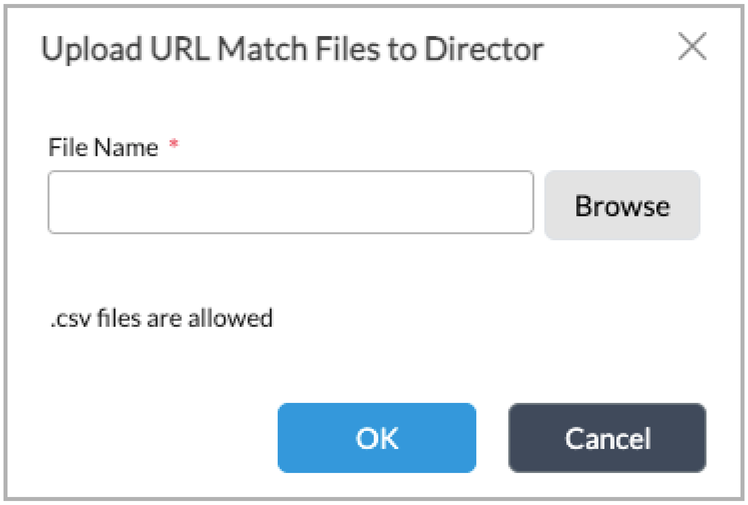
Organization provider-org

You are currently in Appliance View

File Name	Date Uploaded	Size(bytes)

No URL Match Files Uploaded to Director

4. Click the Upload icon to upload the URL file. In the Upload URL Match Files to Director popup window, enter information for the following fields.



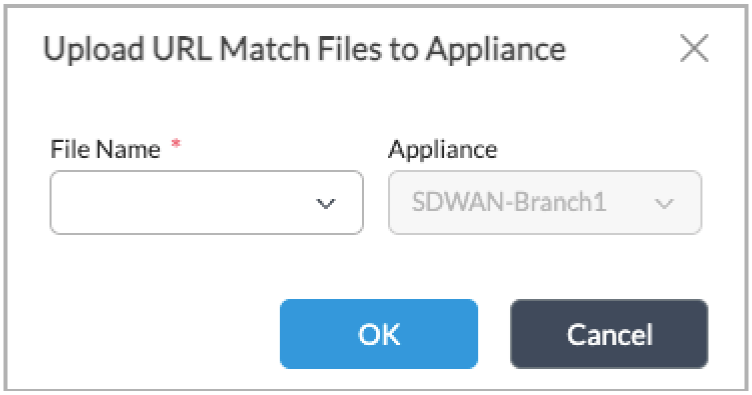
Upload URL Match Files to Director

File Name *

.csv files are allowed

Field	Description
Filename	Enter the name of a URL file to upload, or click the Browse button to select a file. The file must be in CSV format, and each line of the file must be in one of the following formats: ◦ patterns,*URLstring/pattern*,*reputation* ◦ string,*URLstring/pattern*,*reputation* For example: ◦ patterns,.*google.*,undefined ◦ patterns,.*bing.*,undefined ◦ string,www.facebook.com,undefined ◦ patterns,.*versa-networks.*,undefined ◦ patterns,.*twitter.*,undefined

5. Click OK. The main pane displays the uploaded file.
6. Select the Appliance tab.
7. Click the Upload icon to upload the file to the selected appliance. The Upload URL Match Files to Appliance popup window displays.


Upload URL Match Files to Appliance

File Name *

Appliance: SDWAN-Branch1

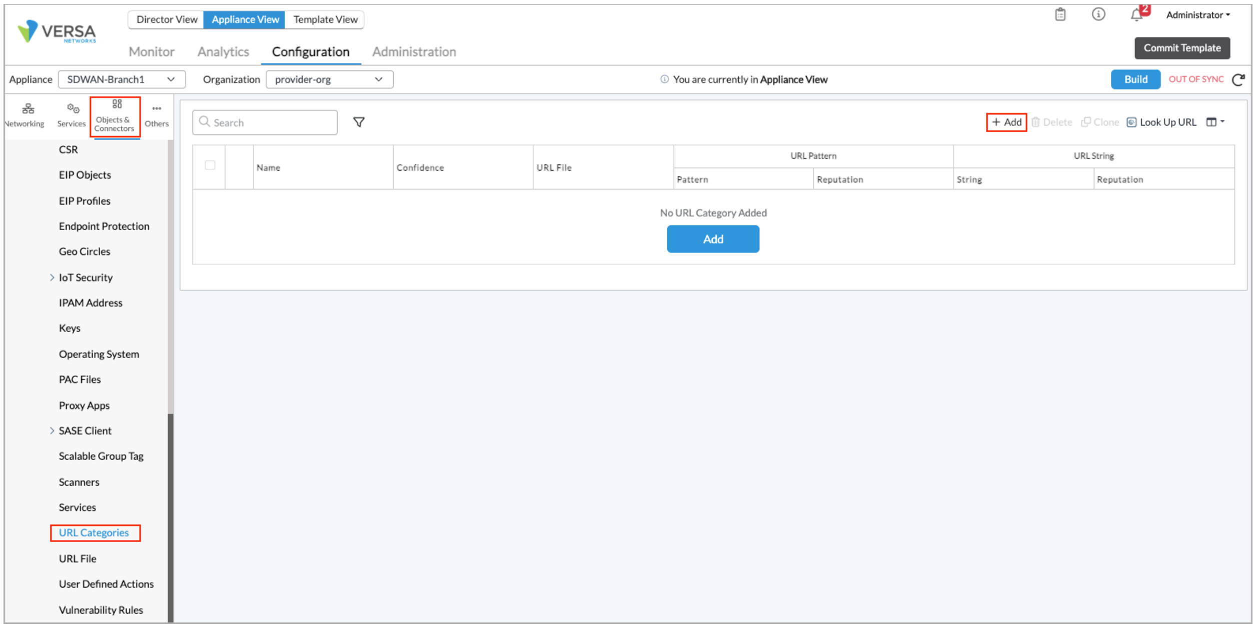
8. In the Filename field, select a URL file. The list displays the files that you uploaded in Step 4.
9. Click OK to upload the file. The main pane displays the uploaded file.

Use URL Files To Configure URL Category Objects

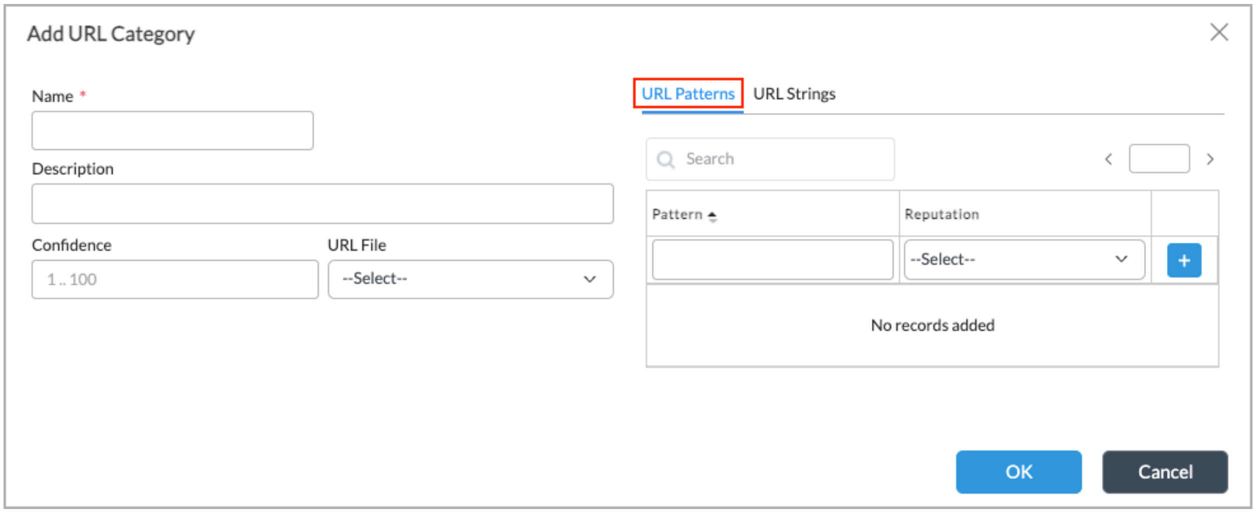
You can use URL files that you have uploaded to configure URL category objects:

1. In Director view:

   a. Select the Configuration tab in the top menu bar.
   b. Select Templates in the horizontal menu bar.
   c. Select an organization in the left navigation bar.
   d. Select a template from the dashboard. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Custom Objects > URL Categories in the left menu bar. The main pane displays the URL categories.



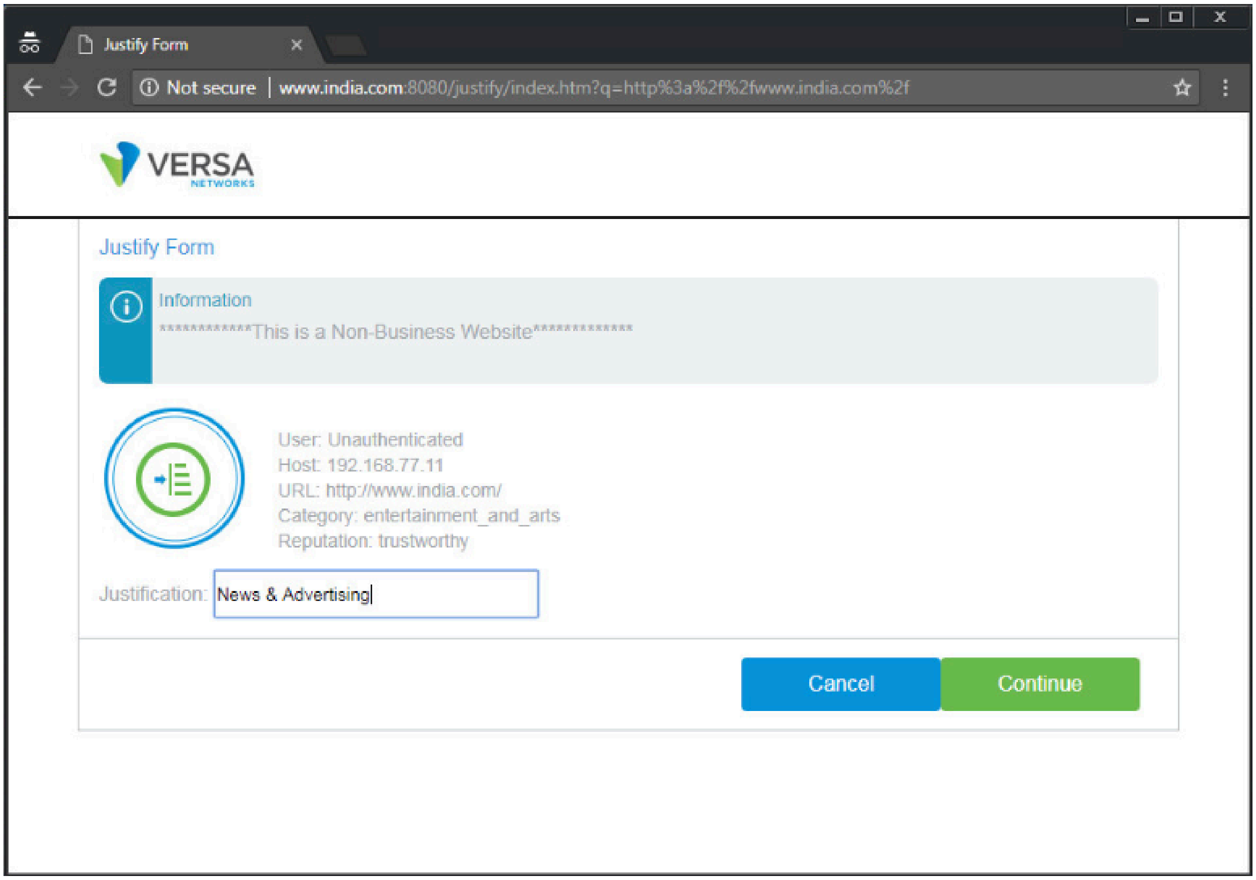
4. Click the + Add icon to add a new category. The Add URL Category popup window displays. For information about adding a URL category, see Configure Layer 7 Objects.
5. In the URL File field, select a URL file. The list displays the files that you uploaded in the procedure in the previous section.



6. Click OK.

Example of URL Filtering and Captive Portal

The following example shows a customized message that uses URL filtering and a captive portal to ask the user to justify browsing a particular webpage that is not allowed as the standard enterprise policy.


Justify Form
Not secure
www.india.com:8080/justify/index.htm?q=http%3a%2f%2fwww.india.com%2f
VERSA
NETWORKS
Cancel
Continue

Justify Form

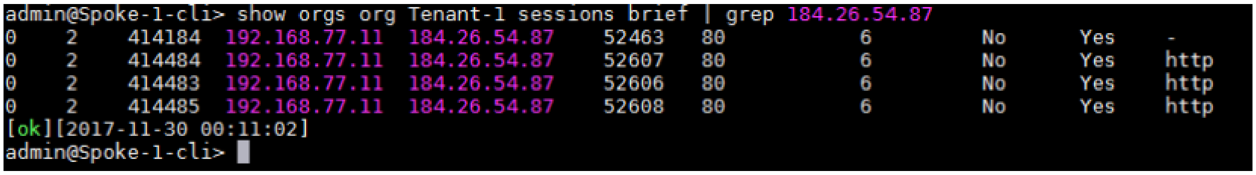
Information

************This is a Non-Business Website*************

User: Unauthenticated
Host: 192.168.77.11
URL: http://www.india.com/
Category: entertainment_and_arts
Reputation: trustworthy

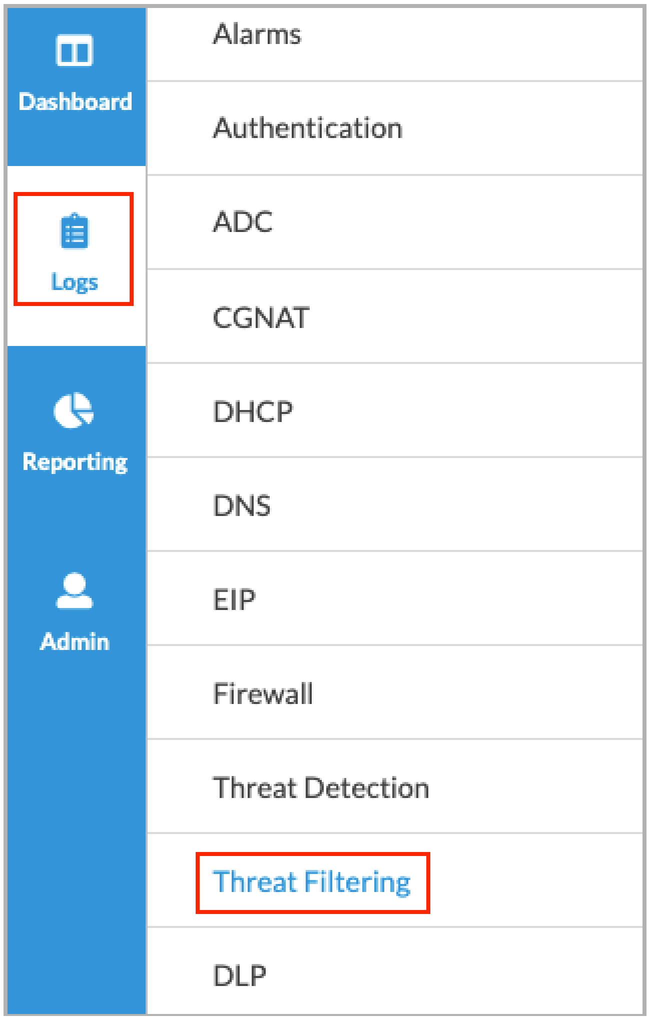
Justification: News & Advertising

To verify the action from the branch CLI, enter the **show orgs org Tenant-1 sessions brief | grep** *website-ip-address* command:

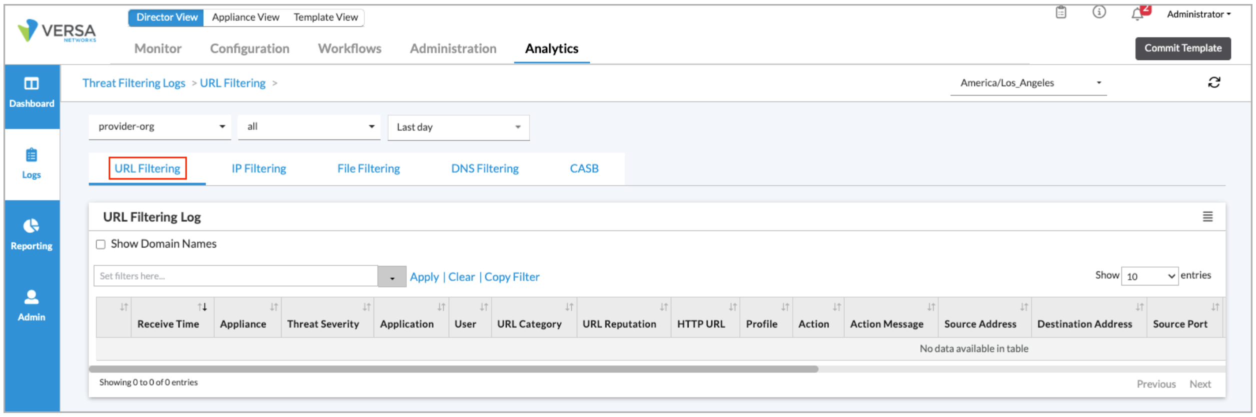


```
admin@Spoke-1-cli> show orgs org Tenant-1 sessions brief | grep 184.26.54.87
0    2    414184  192.168.77.11  184.26.54.87     52463   80           6         No      Yes    -
0    2    414484  192.168.77.11  184.26.54.87     52607   80           6         No      Yes    http
0    2    414483  192.168.77.11  184.26.54.87     52606   80           6         No      Yes    http
0    2    414485  192.168.77.11  184.26.54.87     52608   80           6         No      Yes    http
[ok][2017-11-30 00:11:02]
admin@Spoke-1-cli>
```

To verify the action from an Analytics node, for Releases 22.1 and later, in Director view, select the Analytics tab in the top menu bar. The Analytics application screen displays. Select Logs > Threat Filtering in the left menu bar.



Select URL Filtering in the horizontal menu bar.



URL Filtering Log

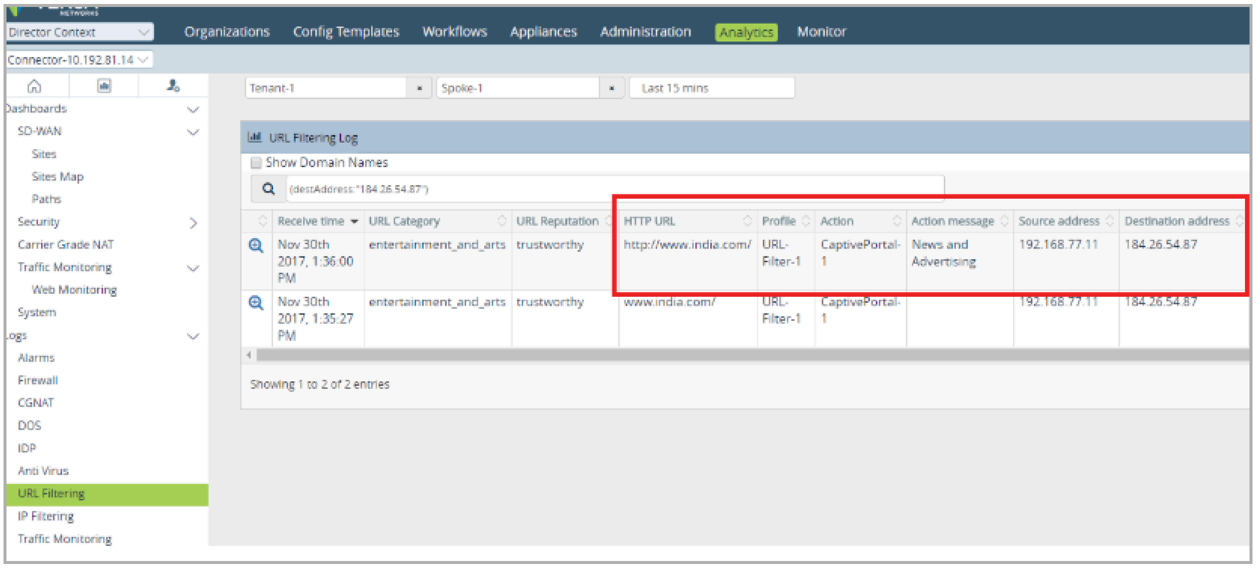
☐ Show Domain Names

Show 10 entries

	Receive Time	Appliance	Threat Severity	Application	User	URL Category	URL Reputation	HTTP URL	Profile	Action	Action Message	Source Address	Destination Address	Source Port
											No data available in table			

Showing 0 to 0 of 0 entries

To verify the action from an Analytics node, for Releases 21.2 and earlier, in Director view, select the Analytics tab in the top menu bar. The Analytics application screen displays. Select Logs > URL Filtering in the left menu bar.



(destAddress:"184.26.54.87")

	Receive time	URL Category	URL Reputation	HTTP URL	Profile	Action	Action message	Source address	Destination address
	Nov 30th 2017, 1:36:00 PM	entertainment_and_arts	trustworthy	http://www.india.com/	URL-Filter-1	CaptivePortal-1	News and Advertising	192.168.77.11	184.26.54.87
	Nov 30th 2017, 1:35:27 PM	entertainment_and_arts	trustworthy	www.india.com/	URL-Filter-1	CaptivePortal-1		192.168.77.11	184.26.54.87

Showing 1 to 2 of 2 entries

Troubleshoot URL Filtering

To troubleshoot security issues related to URL filtering, issue the following CLI commands:

- **show orgs org-services** *tenant-name* **url-filtering**
- **show orgs org-services** *tenant-name* **url-filtering user-defined-url-categories list**
- **show orgs org-services** *tenant-name* **security url-filtering statistics url-category global**
- **show orgs org-services** *tenant-name* **security url-filtering statistics url-category predefined**
- **show orgs org-services** *tenant-name* **security url-filtering statistics url-category user-defined**
- **show orgs org-services** *tenant-name* **security url-filtering statistics url-reputation predefined**
- **show orgs org-services** *tenant-name* **security url-filtering statistics url-reputation user-defined**
- **show orgs org-services** *tenant-name* **security url-filtering statistics cloud-lookup**
- **show orgs org-services** *tenant-name* **security profiles url-filtering predefined statistics**
- **show orgs org-services** *tenant-name* **security profiles url-filtering user-defined statistics**

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Release 21.1.1 supports the caching of the URL-filtering history.
- Release 21.2.1 supports service endpoints.
- Release 22.1.3 supports resolving of disallowed domains to a sinkhole server; the Action types CASB and DNS; uploading and managing custom captive portal pages using the files and folders; the Auth and Auth Fail actions types when uploading a custom captive portal page to an appliance.
- Release 22.1.4 supports text strings for WAN IP and MAC Address in the Custom Redirect Parameters tab of the

Edit Captive Portal Settings window.

Additional Information

Apply Log Export Functionality
Configure a Cloud Profile
Configure Layer 7 Objects
Configure Log Export Functionality
Configure NGFW
Configure Security Profile Groups
Configure SNAT Pools
Configure Stateful Firewall
Manage Files and Folders
Upload PAC Files
Use Security Packages
Versa Analytics Scaling Recommendations