



# AsyncOS 14.0 API - Addendum to the Getting Started Guide for Cisco Web Security Appliances

May 05, 2021

## Overall Bandwidth

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version must be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2021 Cisco Systems, Inc. All rights reserved.

## Contents

<b>Overall Bandwidth</b> .....	<b>6</b>
Retrieving the Overall Bandwidth Details.....	6
Modifying the Overall Bandwidth Details .....	6
Definitions .....	7
<b>Identification Profiles</b> .....	<b>7</b>
Retrieving the Identification Details.....	7
Modifying the Identification Profiles .....	8
Adding the Identification Profiles .....	9
Deleting the Identification Profile .....	9
Definitions .....	10
<b>Access Policies</b> .....	<b>16</b>
Retrieving an Access Policy .....	16
Modifying an Access Policy .....	17
Adding an Access Policy .....	18
Deleting an Access Policy .....	19
Definitions .....	20
<b>PAC File Host Settings</b> .....	<b>45</b>
Retrieving the PAC File Basic Settings.....	45
Modifying the PAC File Basic Settings.....	45
Retrieving the PAC Files .....	46
Adding a New PAC File.....	46
Modifying the Existing PAC Files .....	47
Deleting a PAC File.....	47
Retrieving a PAC File and the Hostname Association.....	48
Adding a PAC File and the Hostname Association.....	48
Modifying the Existing PAC File and the Hostname Association .....	49
Deleting a PAC File and the Hostname Association .....	49
Definitions – Payload Configurations .....	50
<b>Domain Map</b> .....	<b>51</b>
Retrieving the Domain Map Details .....	51
Modifying the Domain Map Details.....	51
Adding a Domain Map .....	52
Deleting the Domain Map .....	52
<b>Upstream Proxy</b> .....	<b>53</b>
Retrieving the Upstream Proxy Details .....	53
Modifying the Upstream Proxy Settings .....	54
Adding an Upstream Proxy .....	54
Deleting the Upstream Proxy.....	55
Modifying the Upstream Proxy Servers .....	56
Adding an Upstream Proxy Server .....	56

Deleting the Upstream Proxy Servers.....	57
<b>HTTPS Proxy .....</b>	<b>57</b>
Retrieving the HTTPS Proxy Details .....	57
Modifying the HTTP Proxy Settings.....	58
Retrieving the HTTP Proxy—Download Certificate File .....	61
Retrieving the HTTP Proxy OCSP Settings .....	61
Modifying the HTTP Proxy—OCSP Settings.....	62
<b>Log Subscriptions.....</b>	<b>64</b>
Retrieving the Log Subscriptions .....	64
Modifying the Log Subscriptions .....	65
Adding the Log Subscriptions .....	70
Deleting the Log Subscriptions .....	80
Modifying the Log Subscriptions—Rollover .....	81
Retrieving the Log Subscriptions for the Fetch Field Lists.....	82
Retrieving the Log Subscriptions to Fetch Default Values for a Log Type .....	82
Adding the Log Subscriptions—Deanonimization.....	83
<b>Header Based Authentication .....</b>	<b>84</b>
Retrieving Header Based Authentication .....	84
Enabling or Disabling Header Based Authentication.....	84
Modifying Header Based Authentication Configuration.....	85
Definitions .....	87
<b>HTTP ReWrite Profiles .....</b>	<b>91</b>
Retrieving the HTTP ReWrite Profiles.....	91
Modifying the HTTP ReWrite Profiles .....	91
Adding the HTTP ReWrite Profiles .....	92
Deleting the HTTP ReWrite Profiles.....	93
Definitions .....	94
<b>General Purpose APIs .....</b>	<b>98</b>
SecureX.....	98
Retrieving the Registered User Information.....	98
Adding the Registered User Information .....	99
Modifying the Registered User Information .....	99
Auth Settings .....	100
Retrieving the Auth Settings .....	100
User Agents .....	102
Retrieving the User Agents .....	102
URL Categories .....	103
Retrieving URL Categories .....	103
Time Ranges .....	104
Retrieving Time Ranges .....	104
Quotas .....	106

Overall Bandwidth

Retrieving Quotas .....	106
Proxy Settings .....	107
Retrieving Proxy Settings.....	107
Identification Methods .....	109
Retrieving Identification Methods.....	109
<b>Static Data.....</b>	<b>110</b>
Applications .....	110
Youtube Categories .....	122
Objects .....	122
Custom MIME Types .....	124
Anti-Malware Categories.....	131

## APIs for Web

### Overall Bandwidth

#### Retrieving the Overall Bandwidth Details

Table 1 - Attributes for Retrieving the Overall Bandwidth Details

API	/wsa/api/v3.0/web_security/overall_bandwidth_limit		
Method	GET		
Parameters	None		
Request body	None		
Response	Code	Type	Description
	200 Ok	Object <a href="#">bandwidth_limit</a>	Represents configured overall bandwidth limit.

#### Modifying the Overall Bandwidth Details

Table 2 - Attributes for Retrieving the Overall Bandwidth Details

API	/wsa/api/v3.0/web_security/overall_bandwidth_limit			
Method	PUT			
Parameters	None			
Request body	Name	Type	Description	Required
	bandwidth_limit	Integer	Unit of bandwidth limit is Kbps. It can have value from 0-524288 Kbps. Value '0' represents 'No limit'.	Yes
Response	Code	Type	Description	

Identification Profiles

	200 Ok	Object <a href="#">bandwidth_limit</a>	Represents configured overall bandwidth limit.
--	--------	--	--

Definitions

[bandwidth\\_limit](#)

Table 3 - Attributes for [bandwidth\\_limit](#)

Name	Type	Description	Required (In PUT)
<a href="#">bandwidth_limit</a>	Integer	Unit of bandwidth limit is Kbps. It can have value from 0-524288 Kbps. <b>Value '0' represents 'No limit'.</b>	Yes

Identification Profiles

Retrieving the Identification Details

Table 4 - Attributes for Retrieving the Identification Details

API	/wsa/api/v3.0/web_security/identification_profiles			
Method	GET			
Parameters	Name	Type	Description	Required
	offset	Integer	It represents the beginning index in the collection of identification profiles that starts from 1.	No
	limit	Integer	It represents the length of the subcollection if you want after a specific offset. If only 'limit' is provided as a request parameter (missing offset), then the offset will be considered as 1.	No

Identification Profiles

	profile_names	String	These are comma-separated names of identification profiles. It will have more priority over offset and limit, if all of them are available in a single request.	No
Request body	None			
Response	Code	Type	Description	
	200 Ok	objects <a href="#">Identification_profile_collection_schema</a>	It contains a list of identification profiles. If no profile is found with the given filter parameters, you must return an empty list.	

## Modifying the Identification Profiles

Table 5 - Attributes for Modifying the Identification Profiles

API	/wsa/api/v3.0/web_security/identification_profiles			
Method	PUT			
Parameters	None			
Request body	Name	Type	Description	Required
	Identification_profiles	Array of objects <a href="#">Identification_profile_schema</a>	It contains a collection of identification profiles. If you must post or PUT for only single profile, it contains details for only that profile.	Yes
Response	Code	Type	Description	



Identification Profiles

	204 No Content	Empty body	If everything in request body is correct.
	207 Multi status	objects <a href="#">multi_status_response</a>	Dictionary of success and Failure list. Failure list contains the appropriate error message, specifying reason of failure.

## Adding the Identification Profiles

Table 6 - Attributes for Adding the Identification Profiles

API	/wsa/api/v3.0/web_security/identification_profiles			
Method	POST			
Parameters	None			
Request body	Name	Type	Description	Required
	Identification_profiles	Array of objects <a href="#">Identification_profile_schema</a>	It contains a collection of identification profiles. If you must post or PUT for only single profile, it contains details for only that profile.	Yes
Response	Code	Type	Description	
	204 No Content	Empty body	If everything in request body is correct.	
	207 Multi status	objects <a href="#">multi_status_response</a>	Dictionary of success and Failure list. Failure list contains an appropriate error message, that specifies the reason for the failure.	

## Deleting the Identification Profile

Table 7 - Attributes for Deleting the Identification Profile

API	/wsa/api/v3.0/web_security/identification_profiles			
Method	DELETE			
Parameters	Name	Type	Description	Required
	profile_names	String	These are comma-separated names of identification profiles.	No
Request body	None			
Response	Code	Type	Description	
	204 No Content	Empty	If all requested profile got deleted.	
	207 Multi Status	objects <a href="#">multi_status_response</a>	Dictionary of success and Failure list. Failure list contains proper error message, specifying reason of failure.	

## Definitions

### Identification\_profile\_collection\_schema

Table 8 - Attributes for Identification\_profile\_collection\_schema

Name	Type	Description	Required	
			POST	PUT
Identification_profiles	Array of objects <a href="#">Identification_profile_schema</a>	Every element in this list represents a single identification profile.	Yes	Yes

Identification Profiles

Identification\_profile\_schema

Table 9 - Attributes for Identification\_profile\_schema

Name	Type	Description	Required	
			POST	PUT
profile_name	String	Unique identifier of profile	Yes	Yes
new_profile_name	String	It represents new profile name. (Valid only in case of PUT)	Not used in POST	Only when name change is required.
status	String	Whether profile is enabled or disabled. Possible values: enable, disable	No	No
description	String	Description of a profile.	No	No
order	Integer	Index of this specific profile in the collection. Its starts from 1. Global profile does not have this field.	Yes	No
identification_method	Objects <a href="#">Identification_method_schema</a>	A dictionary which represents authentication and identification methods.	No	No

Identification Profiles

Name	Type	Description	Required	
			POST	PUT
members	Objects <a href="#">members_schema</a>	A combination of transaction members, like protocol, proxy ports, user agents and so on.	Yes (At least one-member field is required)	No

Identification\_method\_schema

Table 10 - Attributes for Identification\_method\_schema

Name	Type	Description	Required	
			POST	PUT
sso_scheme	String	Represents type of identification and authentication method. Possible values are: <ul style="list-style-type: none"> <li><input type="checkbox"/> Sso_none (for Authentication User),</li> <li><input type="checkbox"/> sso_ise (for Transparently identify users with ISE),</li> <li><input type="checkbox"/> sso_asa (for Transparently identify users with ASA),</li> <li><input type="checkbox"/> sso_tui (for Transparently identify users with authentication Realm)</li> </ul>	Yes, if Auth is not exempted in the identification method.	Yes, if Auth is not exempted in the identification method.
auth_sequence	String	Auth sequence or realm	Yes, if authentication is required.	Yes, if authentication is required.

Identification Profiles

Name	Type	Description	Required	
			POST	PUT
auth_scheme	Array of Strings	Auth schemes in selected realm or sequences	A list of supported schemes in selected auth_sequence.	A list of supported schemes in selected auth_sequence.
prompt_on_sso_failure	Integer	If transparent identification fails, what should be the action. Possible values are <b>'authenticate', 'guest', 'block'</b> (only if ISE)	No	No
use_guest_on_auth_failure	Integer	Action. If you fail to authenticate. Possible values are: 1 (Allow as guest) and 0 (not allow)	Only if sso_tui, sso_lse with auth and sso_none.	Only if sso_tui, sso_lse with auth and sso_none.
auth_surrogate_by_proto	Auth surrogate by protocols	Protocol wise authentication surrogates.	No. Default value will be <b>selected as 'ip'</b> , for all selected protocols in member.	No. Default value will be selected as <b>'ip'</b> , for all selected protocols in the member.
use_forward_surrogates	Integer	Whether apply or not same surrogate settings to explicit forward requests. Possible values are: 1 and 0.	No	No

members\_schema

Table 11 – Attributes for members\_schema

Name	Type	Description	Required	
			POST (At least one member should be)	PUT (Whatever user wants to modify, is a required)
proxy_ports	Array of strings	Connecting proxy ports. It can be a list of ports or range of ports.	No	No
protocols	Array of strings	Protocols list. Possible values are 'http', 'https', 'ftp', 'nativeftp', 'others.	No	No
ip	String	List of client's IPs or IP ranges.	No	No
url_categories	url categories	A dictionary which contains predefined, custom as well uncategorized set of URLs.	No	No
user_agents	Objects <a href="#">user_agents</a>	List of user agents, which can be classified as this profile. It represents the client type (like browsers) with which you can interact.	No	No
location	member	Location of User. Possible values are, 'local', 'remote' and 'both'.	Yes. If Any connect is enabled, then only this option will be allowed.	Yes. If Any connect is enabled, then only this option will be allowed.

url\_categories

Table 12 - url\_categories

Name	Type	Description	Required	
			POST	PUT
predefined	Array of Strings	URL categories defined by Web Security Appliance.	No	No

Identification Profiles

Name	Type	Description	Required	
			POST	PUT
custom	Array of Strings	URL categories defined by user.	No	No
uncategorized	String	Uncategorized URL categories. Possible values are: 'enable', 'disable'.	No	No

user\_agents

Table 13 - Attributes for user\_agents

Name	Type	Description	Required	
			POST	PUT
predefined	Array of Strings	User agents defined by Web Security Appliance. For example, different types of browsers with their versions.	No	No
custom	Array of Strings	User agents defined by user.	No	No
is_inverse	Integer	Whether selected user agents can work as exception or not. Possible values are: 0, 1.	No	No

multi\_status\_response

Table 14 - Attributes for multi\_status\_response

Name	Type	Description
success_list	Array of objects <a href="#">response_status</a>	Success list, with profile name and messages.

Access Policies

Name	Type	Description
failure_list	Array of objects <a href="#">response_status</a>	Failure list, with profile name and messages.
success_count	Integer	Success count
failure_count	Integer	Failure count

[response\\_status](#)

Table 15 – Attributes for [response\\_status](#)

Name	Type	Description
status	Integer	Response code
message	string	Error/Success message
profile_name	string	Profile name

## Access Policies

### Retrieving an Access Policy

Table 16 – Attributes for Access Policies

API	/wsa/api/v3.0/web_security/access_policies				
Method	GET				
Parameters	Name	Type	Description	Remarks	Required
	offset	Integer	It represents the beginning index in the collection of access policies that starts from 1.		Optional



Access Policies

	limit	Integer	It represents the length of the subcollection if you want after a specific offset. If only 'limit' is provided as a request parameter (missing offset), then the offset will be considered as 1.		Optional
	policy_names	String	List of access_policies with the matching policy_names to be returned.	For global policy, policy_names are global_policy	Optional
Request body		None			
Response	Code	Type		Description	
	200 Ok	array		List of all access_policies present and their configurations. If policy_names is provided, returns all the access policies with matching policy_names.	

## Modifying an Access Policy

Table 17 - Attributes for PUT API

API	/wsa/api/v3.0/web_security/access_policies				
Method	PUT				
Parameters	None				
Request body	Name	Type	Description	Required	

Access Policies

	access_policies	Array of objects Attributes for <a href="#">access_policies_schema</a>	List of access policies and their configuration payload.	Mandatory
Response	Code	Type	Description	
	204 No Content	Empty body	The request has been processed successfully and all the given access policies are updated with the given payload.	
	207 Multi status	objects <a href="#">multi_status_response</a>	Dictionary of success and Failure list. Failure list contains proper error message, specifying reason of failure.	

## Adding an Access Policy

Table 18 – Attributes for POST API

API	/wsa/api/v3.0/web_security/access_policies			
Method	POST			
Parameters	None			
Request body	Name	Type	Description	Required
	access_policies	Array of objects Attributes for <a href="#">access_policies_schema</a>	List of access policies and their configuration payload.	Mandatory
Response	Code	Type	Description	
	204 No Content	Empty body	The request has been processed successfully and all the given access policies are created with the given payload.	

Access Policies

	207 Multi status	objects <a href="#">multi_status_response</a>	Dictionary of success and Failure list. Failure list contains proper error message, specifying reason of failure.
--	------------------	--	--

## Deleting an Access Policy

Table 19 - Attributes for DELETE API

API	/wsa/api/v3.0/web_security/access_policies			
Method	DELETE			
Parameters	Name	Type	Description	Required
		Integer		optional
		Integer		optional
	policy_names	String	Policies with matching policy_names to be deleted.	optional
Request body	None			
Response	Code	Type	Description	
	204 No Content	Empty	The access policies have been deleted. If policy_names parameter is not provided, all the policies except the global_policy get deleted.	
	207 Multi status	objects <a href="#">multi_status_response</a>	Dictionary of success and Failure list. Failure list contains proper error message, specifying reason of failure.	

## Definitions

Table 20- Attributes for access\_policies\_schema

Name	Type	Format	Description	Remarks	Required	
					POST	PUT
policy_name	String	starts with a letter or number. Valid characters are letters, numbers, period, and space. Maximum length of the string is 40.	Name of the policy. Unique identifier of the policy	Not applicable for global_policy	Mandatory	Mandatory
new_policy_name	String	Same as policy_name	updates the policy_name	Not applicable for global_policy	N/A	optional
policy_status	String	Enable/disable	Status of the policy	Not applicable for global_policy	mandatory	optional
policy_description	String		Description of the policy	Not applicable for global_policy	optional	optional
policy_order	Integer		Order of policy in collection of policies.	Not applicable for global_policy	mandatory	optional
policy_expiry_status	string	disable	Disables the policy expiry		N/A	optional

Access Policies

Name	Type	Format	Description	Remarks	Required	
					POST	PUT
policy_expiry	String	MM/DD/YYYY HH:MM	Enables the policy expiry and sets the expiry date and time of the policy	Not applicable for global_policy	optional	optional
membership	Objects <a href="#">membership_schema</a>		Defined in <a href="#">membership_schema</a>	Not applicable for global_policy	mandatory	optional
protocols_user_agents	Objects <a href="#">protocols_user_agents_schema</a>		Defined in <a href="#">protocols_user_agents_schema</a>		optional	optional
url_filtering	Objects <a href="#">url_filtering_schema</a>		Defined in <a href="#">url_filtering_schema</a>		optional	optional
avc	Objects <a href="#">avc_schema</a>		Defined in <a href="#">avc_schema</a>		optional	optional

Name	Type	Format	Description	Remarks	Required	
					POST	PUT
objects	Objects <a href="#">Objects schema</a>		Defined in <a href="#">Objects schema</a>		optional	optional
amw_reputation	Objects <a href="#">amw_reputation_schema</a>		Defined in <a href="#">amw_reputation_schema</a>		optional	optional
http_rewrite_profile	String		Name of the http rewrite profile.		optional	optional

membership\_schema

Table 21 - Attributes for membership schema

Name	Type	Format	Description	Required	
				POST	PUT
Identification_profiles	Array of objects	Array of ID profile objects	Defined in <a href="#">Id_profile_schema</a>	mandatory	optional
subnets	Array of strings	Valid IPv4/ipv6 addresses/ranges/subnets	Subnets for access policy if none of the associated ID profile has defined it.	optional	optional

Access Policies

Name	Type	Format	Description	Required	
				POST	PUT
protocols	string	Valid protocol name: “http”, “https”, “ftp”, “nativeftp”, “others”	protocols for access policy if none of the associated ID profile has defined it.	optional	optional
ports	Array of strings	Valid port numbers and port ranges	Port numbers for access policy of none of the associated ID profile has defined it.	optional	optional
url_categories	Objects <a href="#">membership_schema</a>		Defined in <a href="#">url_categories_membership</a> schema. None of the associated ID profile has defined url_categories.	optional	optional
user_agents	Objects <a href="#">user_agents</a>		Defined in <a href="#">user_agents</a> schema. None of the associated ID profile has defined user agents.	optional	optional
time_range	Objects <a href="#">time_range</a>		Defined in <a href="#">time_range</a> schema	optional	optional
user_location	Array of Strings	One of the values “local” or “remote”	User location details, applicable only if AnyConnect secure mobility is enabled.	optional	optional

Id\_profile\_schema

Table 22 - Attributes for Id\_profile\_schema

Name	Type	Format	Description	Required	
				POST	PUT
profile_name	String	Name of profile (string)	String of profile name. empty string represents <b>“global identification profile”</b> , <b>“_all_”</b> represents <b>“All identification profiles.”</b> In GET’s response the global identification profile is not shown as empty string, it is shown as <b>“global_identification_profile”</b> instead.	Yes	Yes



Access Policies

Name	Type	Format	Description	Required	
				POST	PUT
auth	String	one among: [" All Authenticated Users" , " Selected Groups and Users", " Guests" , " No Authentication "]	<p><b>"All Authenticated Users"</b>: represents all the authenticated users. The selected ID profile must have auth enabled</p> <p><b>"Selected groups and users"</b>: selected ID profile must have support. In addition, you must provide <a href="#">groups_and_users_schema</a></p> <p><b>"Guests"</b>: If ID profile supports guest then this option can be chosen. In case of <b>"all identification profiles"</b> at least one of the ID profiles must support guest.</p> <p><b>"No Authentication"</b>: If no authentication is required. In case if selected ID profile is <b>"global profile"</b> and doesn't have auth associated, then no authentication is implicit but still for the sake of schema validation the value <b>"No Authentication"</b> is mandatory.</p>	No	No

Name	Type	Format	Description	Required	
				POST	PUT
groups_and_users	Objects <a href="#">groups_and_users_schema</a>		Defined in <a href="#">groups_and_users_schema</a> . This is mandatory if <b>“auth” is chosen as “Selected groups and users”</b> .	Conditional	Conditional
auth_realm	String	Name of the specific realm or <b>‘all realm’</b> as applicable.	If the ID profile has auth <b>realm as ‘All Realms’</b> , then it is mandatory to provide <b>either ‘All Realms’ or the specific realm</b> otherwise if ID profile has only one realm that is associated then this is not mandatory.	Conditional	Conditional

groups\_and\_users\_schema

Table 23 - Attributes for groups\_and\_users\_schema

Name	Type	Format	Description	Required	
				POST	PUT
username	Array	Array of username string	List of username strings.	No	No
sgt	Array	Array of sgt strings	Valid sgt strings.	No	No
ise_group	Array	Array of ISE group strings	Valid ISE group string.	No	No
fallback_username	Array	Array of username strings	List of username strings.	No	No

Access Policies

Name	Type	Format	Description	Required	
				POST	PUT
auth_group	List of Objects <a href="#">auth_group_schema</a>		Defined in <a href="#">auth_group_schema</a>	No	No

auth\_group\_schema

Table 24 - Attributes for auth\_group\_schema

Name	Type	Format	Description	Required	
				POST	PUT
realm	String		Valid realm (string)	Yes	Yes
groups	Array	Array of strings	List of valid group names that are associated with the given realm.	Yes	Yes

amw\_reputation\_schema

Table 25 - Attributes for amw\_reputation\_schema

Name	Type	Format	Description	Required	
				POST	PUT
state	String	One among "use_global", "custom"	Describes whether to use custom settings or inherit all the settings from Global policy.	Yes	No
adv_malware_protection	Objects <a href="#">adv_malware_protection_schema</a>		Advanced malware protection settings. Defined in <a href="#">adv_malware_protection_schema</a>	No	No

Name	Type	Format	Description	Required	
				POST	PUT
cisco_dvs_amw	Objects <a href="#">cisco_dvs_amw_schema</a>		Cisco DVS antimalware settings. Defined in <a href="#">cisco_dvs_amw_schema</a>	No	No
web_reputation	Objects <a href="#">web_reputation_schema</a>		Web reputation setting. Defined in <a href="#">web_reputation_schema</a>  Applicable only when the adaptive scanning is disabled.	No	No

adv\_malware\_protection\_schema

Table 26 - Attributes for adv\_malware\_protection\_schema

Name	Type	Format	Description	Required	
				POST	PUT
file_reputation_filtering	String	One among <b>“enable”</b> , <b>“disable”</b>	Status of the file reputation filtering.	Yes	Yes
file_reputation	Objects <a href="#">file_reputation_schema</a>		List of block file reputation categories. Default status is always <b>“monitor”</b> if not specified here.	No	No

file\_reputation\_schema

Table 27 - Attributes for file\_reputation\_schema

Name	Type	Format	Description	Required	
				POST	PUT
block	String Array	Array of valid file reputation categories	Categories of the file reputation to be blocked.	No	No

cisco\_dvs\_amw\_schema

Table 28 - Attributes for cisco\_dvs\_amw\_schema

Name	Type	Format	Description	Required	
				POST	PUT
suspect_user_agent_scanning	String	One among "block", "scan", "none"	"none" is to disable the suspect_user_agent scanning. "block", "scan" enables suspect_user_agent and perform the corresponding action "monitor" or "block"	No	No
amw_scanning	Objects <a href="#">amw_scanning_schema</a>		Defined in <a href="#">amw_scanning_schema</a>	No	No
block_malware_categories	String array	Array of valid malware categories	Valid malware categories to be blocked. Default action is monitor.	Yes	Yes
block_other_categories	String array	Array of valid other categories	Valid other categories to be blocked. Default action is monitor.	Yes	Yes

amw\_scanning\_schema

Table 29 - Attributes for amw\_scanning\_schema

Name	Type	Format	Description	Required	
				POST	PUT
amw_scan_status	String	One among <b>“enable”</b> , <b>“disable”</b>	Enable/disable amw scanning status. (if the adaptive scanning is enabled no explicit status for Sophos/mcafee/Webroot to be provided).	Yes	No
amw_scanners	Objects <a href="#">amw_scanners_schema</a>		Status of anti-malware scanners (Sophos/McAfee/Webroot). Applicable only if adaptive scanning is disabled	Yes	Yes

amw\_scanners\_schema

Table 30 - Attributes for amw\_scanners\_schema

Name	Type	Format	Description	Required	
				POST	PUT
mcafee	String	One among <b>“enable”</b> , <b>“disable”</b>	Enable/Disable Sophos (only if adaptive scanning is disabled). Only one among Sophos or McAfee can be enabled.	Yes	Yes
sophos	String	One among <b>“enable”</b> , <b>“disable”</b>	Enable/Disable Sophos (only if the adaptive scanning is disabled). Only one among Sophos or McAfee can be enabled.	Yes	Yes
webroot	String	One among <b>“enable”</b> , <b>“disable”</b>	Enable/disable Webroot (only applicable if adaptive scanning is disabled)	Yes	Yes

web\_reputation\_schema

Table 31- Attributes for web\_reputation\_schema

Name	Type	Format	Description	Required	
				POST	PUT
filtering	String	One among “enable”, “disable”	Enable or disable web reputation setting.	Yes	No
score	Object		Web reputation score. Defined in <a href="#">web_reputation_score_schema</a> .	No	No

web\_reputation\_score\_schema

Table 32- Attributes for web\_reputation\_score\_schema

Name	Type	Format	Description	Required	
				POST	PUT
block_below	Number	Number between -10, 10	Web reputation to be blocked below the given number.	No	No
allow_above	Number	Number between -10, 10	Web reputation score to be allowed.	No	No

url\_categories\_membership

Table 33- Attributes for url\_categories\_membership

Name	Type	Format	Description	Required	
				POST	PUT
predefined	Array of Strings		URL categories defined by Web Security Appliance.	No	No

Access Policies

Name	Type	Format	Description	Required	
				POST	PUT
custom	Array of Strings		URL categories defined by user.	No	No
uncategorized	String	One among “enable”, “disable”	uncategorized url category	No	No

time\_range

Table 34- Attributes for time\_range

Name	Type	Description	Required	
			POST	PUT
time_range_name	String	Name of a valid time range profile.	Yes	Yes
is_inverse	Integer	Whether use the time that is defined in the time_range_name profile or use the time profile other than defined in time_range_name based on values 0,1.	Yes	Yes



protocols\_user\_agents schema

Table 35- Attributes for protocols\_user\_agents schema

Name	Type	Format	Description	Required	
				POST	PUT
state	string	use_global/custom/disable	Protocols and user agent settings. If <a href="#">protocols_user_agents schema</a> payload is provided and state is not provided, state of <a href="#">protocols_user_agents schema</a> is set to custom by default.	optional	optional
block_protocols	Array of strings		Protocols to be blocked.	optional	optional
allow_connect_ports	Array of strings	Port range or numbers. To allow all ports via HTTP CONNECT enter 1-65535. Leave field blank to block all ports.	Enables applications to tunnel outbound traffic over HTTP unless the protocol is blocked above. Traffic that is tunneled through HTTP CONNECT will not be scanned, except for SSL ports (specified on Security Services > HTTPS Proxy)	optional	optional

Name	Type	Format	Description	Required	
				POST	PUT
block_custom_user_agents	Array of strings	any regular expression, one regular expression per line, to block user agents	Custom user agents to be blocked. See the example of user agent pattern.	optional	optional

url\_filtering schema

Table 36- Attributes for url\_filtering schema

Name	Type	Format	Description	Required	
				POST	PUT
state	string	use_global/custom	url filtering settings. If <a href="#">protocols_user_agents</a> schema payload is provided and state is not provided, state of url_filtering is set to custom by default.	optional	optional
custom_cats	object		Set action for custom categories. Defined in <a href="#">custom_cats</a> schema	optional	optional
predefined_cats	object		Defined in <a href="#">predefined_cats</a> schema.	optional	optional
yt_cats	object		Defined in <a href="#">yt_cats</a> schema	optional	optional
overall_quota_profile	string		Set a quota that applies to all web surfing activities.	optional	optional
exception_referred_embedded_content	object		Exceptions to Blocking for Embedded/Referred Content. Defined in <a href="#">exception_referred_embedded_content_schema</a>	optional	optional

Access Policies

Name	Type	Format	Description	Required	
				POST	PUT
uncategorized_url	string	Use_global/block/monitor/warn	Set action for urls that do not match any category.	optional	optional
update_cats_action	string	Use_global/ most restrictive/ least restrictive	Set action for new categories.	optional	optional
safe_search	Objects <a href="#">safe_search schema</a>		Defined in <a href="#">safe_search schema</a>	optional	optional
content_rating	Objects <a href="#">content_rating schema</a>		Defined in <a href="#">content_rating schema</a>	optional	optional

custom\_cats schema

Table 37- Attributes for custom\_cats schema

Name	Type	Description	Required	
			POST	PUT
block	Array of strings	List of custom categories to block.	optional	optional
exclude	Array of strings	List of custom categories to exclude.	optional	optional
redirect	object	Custom categories to redirect. Defined in redirect schema.	optional	optional
allow	Array of strings	List of custom categories to allow.	optional	optional
monitor	Array of strings	List of custom categories to monitor.	optional	optional

Access Policies

Name	Type	Description	Required	
			POST	PUT
warn	Array of strings	List of custom categories to warn.	optional	optional
quota_based	Objects <a href="#">quota_based</a>	Custom categories to configure for time and volume quotas. Defined in <a href="#">quota_based</a> .	optional	optional
time_based	Objects <a href="#">time_based_schema</a>	Custom categories to configure for time range. Defined in <a href="#">time_based_schema</a>	optional	optional

redirect schema

Table 38- Attributes for redirect schema

Name	Type	Format	Description	Required	
				POST	PUT
<url category name>	string	Valid http/s url	The url to redirect to.	optional	optional

quota\_based schema

Table 39- quota\_based schema

Name	Type	Description	Required	
			POST	PUT
<url category name>	object	Categories to be configured for quota-based profiles. Defined in <a href="#">quota_profile</a> .	optional	optional

Name	Type	Description	Required	
			POST	PUT
quota_profile	string	Time and volume quotas to be configured for the category.	optional	optional

time\_based\_schema

Table 40- Attributes for time\_based schema

Name	Type	Description	Required	
			POST	PUT
<url category name>	object	Categories to be configured for time-based profiles. Defined in time based_profile.	optional	optional

Table 41 - Attributes for Time Range

Name	Type	Description	Required		
			POST	PUT	condition
time_range	string	Time range profile.	optional	optional	
action	string	Action to be taken if in time range.	optional	optional	
otherwise	string	Action to be taken if not in time range.	optional	optional	
otherwise_redirect	string	Redirect to if in time range.	Optional/ condition al	Optional/ condition al	Available only for custom categories
action_redirect	string	Redirect to if in time range.	Optional/ condition al	Optional/ condition al	Available only for custom categories

predefined\_cats schema

Table 42 - Attributes for predefined\_cats schema

Name	Type	Description	Required	
			POST	PUT
block	Array of strings	List of predefined categories to block.	optional	optional
monitor	Array of strings	List of predefined categories to monitor.	optional	optional

Name	Type	Description	Required	
			POST	PUT
warn	Array of strings	List of predefined categories to warn.	optional	optional
quota_based	object	predefined categories to configure for time and volume quotas. Defined in quota_based schema.	optional	optional
time_based	Objects <a href="#">time_based_schema</a>	Predefined categories to configure for time range. Defined in <a href="#">time_based_schema</a> .	optional	optional

yt\_cats schema

Table 43 - Attributes for yt\_cats schema

Name	Type	Description	Required	
			POST	PUT
block	Array of strings	List of youtube categories to block.	optional	optional
monitor	Array of strings	List of youtube categories to monitor.	optional	optional
warn	Array of strings	List of youtube categories to warn.	optional	optional
time_based	Objects <a href="#">time_based_schema</a>	youtube categories to configure for time range. Defined in <a href="#">time_based_schema</a> .	optional	optional

exception\_referred\_embedded\_content\_schema

Table 44 - Attributes for exception\_referred\_embedded\_content schema

Name	Type	Format	Description	Required	
				POST	PUT
state	string	Enable/disable	State of the referrer exceptions.	optional	optional
exceptions	Array of object		Defined in exceptions schema.	optional	optional

Exceptions schema

Table 45 - Attributes for Exceptions schema

Name	Type	Description	Required	
			POST	PUT
content_referred_by_cats	Objects <a href="#">content_referred_by_cats</a>	Sets Exception for Content Referred by The Categories. Defined in <a href="#">content_referred_by_cats</a> .	optional	optional
referred_content	Objects <a href="#">referred_content</a> schema	Set Exception for <a href="#">referred_content</a> schema	optional	optional

content\_referred\_by\_cats\_schema

Table 46- Attributes for content\_referred\_by\_cats\_schema

Name	Type	Description	Required	
			POST	PUT
custom_cats	Array of strings	List of custom categories.	optional	optional
predefined_cats	Array of strings	List of custom categories.	optional	optional

referred\_content schema

Table 47 – Attributes for referred\_content schema

Name	Type	Format	Description	Required	
				POST	PUT
custom_cats	Array of strings		List of custom categories.	optional	optional
predefined_cats	Array of strings		List of predefined categories.	optional	optional
type	string	Selected/all/except	Exception type.	optional	optional
applications	Array of strings		List of applications.	optional	optional

safe\_search schema

Table 48 – Attributes for safe\_search schema

Name	Type	Format	Description	Required	
				POST	PUT
status	string	Enable/disable/use_global	Status of the safe search. By default, it is disabled for global policy and use_global for custom policies.	optional	optional
unsupported_safe_search_engine	string	monitor/block	Search engines that do not support safe search. By default, action is block if safe search status is enabled.	optional	optional



content\_rating schema

Table 49 - Attributes for content\_rating schema

Name	Type	Format	Description	Required	
				POST	PUT
status	string	enable/disable/use_global	Status of the content rating. By default, it is disabled for global policy and use_global for custom policies.	optional	optional
action	string	block/warn	Action if site setting allows adult or explicit content. By default, action is block if content rating status is enabled.	optional	optional

Objects schema

Table 50 - Attributes for Objects schema

Name	Type	Format	Description	Required	
				POST	PUT
state	string	custom/disable/use_global	State of the object. By default, the state is use_global for custom policies and custom if the object payload is provided.	optional	optional
max_object_size_mb	Objects <a href="#">max_object_size_mb_schema</a>		Object blocking settings by size in mb. Defined in <a href="#">max_object_size_mb_schema</a>	optional	optional
object_type	Objects <a href="#">object_type_schema</a>		Action for object and mime types. Defined in <a href="#">object_type_schema</a>	optional	optional

Name	Type	Format	Description	Required	
				POST	PUT
block_custom_mime_types	Array of strings	Valid mime type. See object and mime type references.	Action for custom mime types.	optional	optional

max\_object\_size\_mb\_schema

Table 51 - Attributes for max\_object\_size\_mb\_schema

Name	Type	Format	Description	Required	
				POST	PUT
ftp	integer	Range 0-1024	Maximum download size for ftp. By default, size is 0 (No Maximum).	optional	optional
http_or_https	integer	Range 0-1024	Maximum download size for http/https. By default, size is 0 (No Maximum).	optional	optional

object\_type\_schema

Table 52 - Attributes for object\_type\_schema

Name	Type	Description	Required	
			POST	PUT
<mime type category name>	object	Category name of the mime type. Defines action for each mime type for that category. Defined in the action schema.	optional	optional

Action schema

Table 53 - Attributes for Action schema

Name	Type	Description	Required	
			POST	PUT
monitor	Array of strings	List of mime types to be monitored for a mime type category.	optional	optional
block	Array of strings	List of mime types to be blocked for a mime type category.	optional	optional
inspect	Array of strings	List of mime types to be inspect for a mime type category. Applicable only for Inspectable Archive mime types.	optional	optional
allow	Array of strings	List of mime types to be allowed for a mime type category. Applicable only for Inspectable Archive mime types.	optional	optional

avc\_schema

Table 54 - Attributes for avc\_schema

Name	Type	Format	Description	Required		
				POST	PUT	condition
state	string	custom/use_global	State of avc	optional	optional	
applications	object		Defined in <a href="#">Applications schema</a>	optional	optional	
range_request	Objects <a href="#">range_request_schema</a>		Defined in <a href="#">range_request_schema</a>	Conditional/optional	Conditional/optional	Available only if Range Request Forwarding is enabled.

Applications schema

Table 55 – Attributes for Applications schema

Name	Type	Description	Required	
			POST	PUT
<application type>	object	Type of the application. See applications info. Defined in <a href="#">Application type schema</a>	optional	optional

Application type schema

Table 56 – Application type schema

Name	Type	Format	Description	Required	
				POST	PUT
default_action	string	monitor/block	Sets the action for all the applications under the application type.	optional	optional
default_bandwidth_limit	string	Range - 1 and 102400 kbps. 0 for no bandwidth limit.	By default, bandwidth limit is 0 (no bandwidth limit for the application type). default_bandwidth_limit is only applicable for Media and Facebook application type.	optional	optional
block	Array of strings		List of applications to block for an application type.	optional	optional
monitor	Objects <a href="#">monitor_schema</a>		Defined in <a href="#">monitor_schema</a> for applications.	optional	optional

Table 57 - Attributes for monitor\_schema application

Name	Type	Description	Required	
			POST	PUT
<application name>	object	Name of the application to monitor for the application type.	optional	optional

monitor\_schema

Table 58 - Attributes for monitor\_schema

Name	Type	Format	Description	Required	
				POST	PUT
bandwidth_limit	string	Enable/disable	If enabled assigns the default bandwidth value for the application. If the disabled bandwidth limit is set to 0. By default, bandwidth_limit is disabled and applicable only for applications under Facebook and Media application type.	optional	optional
restrict	Array of strings		To enable list of restricted behavior for the application.	optional	optional

range\_request\_schema

Table 59 - Attributes for range\_request schema

Name	Type	Format	Description	Required		
				POST	PUT	condition
exception_list	array	The exception list may include domain names, IP addresses, host names, URLs, and regular expressions.	List of exceptions for range request	Optional/conditional	Optional/conditional	Available only if at least one application is blocked or restricted

PAC File Host Settings

Name	Type	Format	Description	Required		
				POST	PUT	condition
bypass	string	Do not forward range requests or Forward range requests.	Bypass for range request. Default is do not forward range requests.	Optional/condition	Optional/condition	Available only if at least one application is blocked or restricted

## PAC File Host Settings

### Retrieving the PAC File Basic Settings

API	/wsa/api/v3.0/security_services/pac_basic_setting					
Method	GET					
Parameters	None					
Request body	None					
Response	Code	Type		Description		
	200 Ok	Objects in <a href="#">pac_basic_setting</a>		PAC file basic setting:  status  pac_file_expiry  pac_server_ports  pac_expiration_interval		

### Modifying the PAC File Basic Settings

API	/wsa/api/v3.0/security_services/pac_basic_setting					
Method	PUT					

PAC File Host Settings

Parameters	None			
Request body	Name	Type	Description	Required
	<a href="#">pac_basic_setting</a>	Object <a href="#">pac_basic_setting</a>	Defined in <a href="#">pac_basic_setting</a> schema	Mandatory
Response	Code	Type	Description	
	204 No Content	Empty body	The request has been processed successfully and all the given PAC file settings are applied.	

### Retrieving the PAC Files

API	/wsa/api/v3.0/security_services/pac_file			
Method	GET			
Parameters	file_name (optional): file name (to be downloaded)			
Request body	None			
Response	Code	Type	Description	
	204 No Content	Empty body	List of PAC files is returned. If query parameter 'file_name' is provided, the content of PAC file with given name (if present) will be returned.	

### Adding a New PAC File

API	/wsa/api/v3.0/security_services/pac_file			
Method	POST			
Parameters	None			
Request body	Multipart/form-data (file to be uploaded)			
Response	Code	Type	Description	

PAC File Host Settings

	204 No Content	Empty body	The request has been processed successfully and all the given PAC file settings are applied.
	207 Multi status	objects <a href="#">multi_status_response</a>	Dictionary of success and Failure list. Failure list contains proper error message, specifying reason of failure.

### Modifying the Existing PAC Files

API	/wsa/api/v3.0/security_services/pac_file		
Method	PUT		
Parameters	None		
Request body	Multipart/form-data (file to be updated)		
Response	Code	Type	Description
	204 No Content	Empty body	The request has been processed successfully and the given PAC file has been modified.
	207 Multi status	objects <a href="#">multi_status_response</a>	Dictionary of success and Failure list. Failure list contains proper error message, specifying reason of failure.

### Deleting a PAC File

API	/wsa/api/v3.0/security_services/pac_file		
Method	DELETE		
Parameters	file_name (mandatory): name of files to be deleted		
Request body	None		
Response	Code	Type	Description



PAC File Host Settings

	204 No Content	Empty body	All the files are deleted successfully
	207 Multi status	objects <a href="#">multi_status_response</a>	Dictionary of success and Failure list. Failure list contains proper error message, specifying reason of failure.

### Retrieving a PAC File and the Hostname Association

API	/wsa/api/v3.0/security_services/pacfile_host		
Method	GET		
Parameters	None		
Request body	None		
Response	Code	Type	Description
	200 Ok	Object <a href="#">pac_basic_setting</a>	List of PAC file and corresponding hostname mapping.

### Adding a PAC File and the Hostname Association

API	/wsa/api/v3.0/security_services/pacfile_host			
Method	POST			
Parameters	None			
Request body	Name	Type	Description	Required
	hostname_pac_mapping	Array of PAC file hostname mapping	List of dictionaries containing hostname and associated PAC file name.	Yes
Response	Code	Type	Description	

PAC File Host Settings

	204 No Content	Empty body	The request has been processed successfully and all the given PAC file and hostname mappings have been created.
	207 Multi status	objects <a href="#">multi_status_response</a>	Dictionary of success and Failure list. Failure list contains proper error message, specifying reason of failure.

### Modifying the Existing PAC File and the Hostname Association

API	/wsa/api/v3.0/security_services/pacfile_host			
Method	POST			
Parameters	None			
Request body	Name	Type	Description	Required
	hostname_pac_mapping	Array of PAC file hostname mapping	List of dictionaries containing hostname and an associated PAC file name. Defined in hostname_pac_mapping schema.	Yes
Response	Code	Type	Description	
	204 No Content	Empty body	The request has been processed successfully and all the given PAC file and hostname mappings have been updated.	
	207 Multi status	objects <a href="#">multi_status_response</a>	Dictionary of success and Failure list. Failure list contains proper error message, specifying reason of failure.	

## Deleting a PAC File and the Hostname Association

API	/wsa/api/v3.0/security_services/pacfile_host		
Method	DELETE		
Parameters	host_name (mandatory): hostnames for which the mapping to be deleted.		
Request body	None		
Response	Code	Type	Description
	204 No Content	Empty body	The pac file mapping for the given hostnames are successfully removed.
	207 Multi status	objects <a href="#">multi_status_response</a>	Dictionary of success and Failure list. Failure list contains proper error message, specifying reason of failure.

## Definitions – Payload Configurations

### pac\_basic\_setting

Table 60 - pac\_basic\_setting

Name	Type	Format	Description	Required		
				POST	PUT	condition
status	String	Value one among “enable”, “disable”	Status of PAC setting	NA	Mandatory	
Pac_file_expiry	String	Value one among “enable”, “disable”	status of PAC file expiry setting	NA	Optional	
pac_expiration_interval	Integer	Integer value >= 1	PAC file expiration interval in minutes	NA	Optional	

Domain Map

Name	Type	Format	Description	Required		
				POST	PUT	condition
pac_server_ports	Array of integers	Array of valid port numbers ranging between 1 and 65535	Ports to enable PAC file hosting service. If not provided, default port will be set.	NA	Optional	

## Domain Map

### Retrieving the Domain Map Details

Table 61 - Attributes for Retrieving the Domain Map Details

API	/wsa/api/v2.0/configure/web_security/domain_map			
Method	GET			
Parameters	Name	Type	Description	Required
	offset	Integer	Offset among the list of domain map	If limit is present
	limit	Integer	Number of records to be displayed starting from offset.	If offset is present
	domain_name	String	Domain name string. Multiple names must be separated by comma.	No
Request body	None			
Response	Code	Type	Description	
	200 Ok		Domain map settings	

## Modifying the Domain Map Details

Table 62 - Attributes for Modifying the Domain Map Details

API	/wsa/api/v2.0/configure/web_security/domain_map				
Method	PUT				
Parameters	None				
Request body	Name	Type	Format	Description	Required
	new_domain_name	String	Valid domain name string	New domain names to be replaced.	No
	domain_name	String	Valid domain name string	Domain name. For example, <b>"example.cisco.com"</b> .	Yes
	order	Number		Desired order of the domain entry.	No
	IP_addresses	Array of strings	Example: "002:45:32::00:12/24", "2.2.2.1-10"	List of IP address (ipv4/ipv6) strings.	No

## Adding a Domain Map

Table 63- Attributes for Adding a Domain Map

API	/wsa/api/v2.0/configure/web_security/domain_map				
Method	POST				
Parameters	None				
Request body	Name	Type	Format	Description	Required

Upstream Proxy

	domain_name	String	Valid domain name string.	Domain name. For example, <b>“example.cisco.com”</b>	Yes
	order	Number		Desired order of the domain entry	Yes
	IP_addresses	Array of strings	Example: "002:45:32::00:12/24", "2.2.2.1-10"	List of IP address (ipv4/ipv6) strings	Yes

## Deleting the Domain Map

Table 64- Attributes for Deleting the Domain Map

API	/wsa/api/v2.0/configure/web_security/domain_map			
Method	DELETE			
Parameters	Name	Type	Description	Required
	domain_name	Array of String	Domain name(s) to be deleted. Select <b>“delete_all”</b> if all the domain maps must be deleted.	Yes
Request body	None			
<b>Response</b>	Code	Type	Description	
	200 Ok			

## Upstream Proxy

### Retrieving the Upstream Proxy Details

Table 65 - Attributes for Retrieving the Upstream Proxy Details

API	/wsa/api/v2.0/configure/network/upstream_proxy
-----	--

Upstream Proxy

Method	GET			
Parameters	Name	Type	Description	Required
	offset	Integer	Offset among the list of domain map	If limit is present.
	limit	Integer	Number of records to be displayed starting from offset.	If offset is present.
	group_name	String	Group name string. Multiple names must be separated by comma.	No
Request body	None			
Response	Code	Type	Description	
	200 Ok		Domain map settings	

## Modifying the Upstream Proxy Settings

Table 66 - Modifying the Upstream Proxy Settings

API	/wsa/api/v2.0/configure/network/upstream_proxy				
Method	POST				
Parameters	None				
Request body	Name	Type	Format	Description	Required
	group_name	String	Valid group name string	group name for example, "test1"	Yes
	proxy_servers	Array of dict.	{ "host": <hostname>, "retries": <no of retries>, "port":<port num>	Proxy server details (each having information: host, port, and retries).	Yes

Upstream Proxy

	failure_handling	strings	Values among "connect", "drop"	Failure handling decision.	Yes
	load_balancing	String	Values among: ["none", "fewest-connections", "least-recently-used", "hash-based", "round-robin"]	Valid load-balancing mechanism.	Yes

## Adding an Upstream Proxy

Table 67 - Attributes for Adding an Upstream Proxy

API	/wsa/api/v2.0/configure/network/upstream_proxy				
Method	PUT				
Parameters	None				
Request body	Name	Type	Format	Description	Required
	new_group_name	String	Valid group name string	New group name.	No
	group_name	String	Valid group name string	group name For example, "test1".	Yes
	failure_handling	strings	Values among "connect", "drop"	Failure handling decision.	Yes
	load_balancing	String	Values among: ["none", "fewest-connections", "least-recently-used", "hash-based", "round-robin"]	Valid load-balancing mechanism.	Yes



## Deleting the Upstream Proxy

Table 68 – Attributes for Deleting the Upstream Proxy

API	/wsa/api/v2.0/configure/network/upstream_proxy			
Method	DELETE			
Parameters	Name	Type	Description	Required
	proxy_group	Array of String	Proxy group names to be deleted. <b>“delete_all”</b> to delete all the proxy groups.	Yes
Request body	None			
Response	Code	Type	Description	
	200 Ok			

## Modifying the Upstream Proxy Servers

Table 69 – Attributes for Modifying the Upstream Proxy Servers

API	/wsa/api/v2.0/configure/network/upstream_proxy/servers				
Method	POST				
Parameters	None				
Request body	Name	Type	Format	Description	Required
	group_name	String	Valid group name string	group name. For example, <b>“test1”</b> .	Yes
	proxy_servers	Array of dict.	{ <b>“host”</b> : <hostname>, <b>“retries”</b> : <no of retries>, <b>“port”</b> :<port num>}	Adds the proxy server to the existing server list for the specified proxy group.	Yes

## Adding an Upstream Proxy Server

Table 70 - Attributes for Adding an Upstream Proxy Server

API	/wsa/api/v2.0/configure/network/upstream_proxy/servers				
Method	PUT				
Parameters	None				
Request body	Name	Type	Format	Description	Required
	group_name	String	Valid group name string	group name. For example, "test1".	Yes
	proxy_servers	Array of objects	List of dict(s), each dict having keys - ['host', 'retries', 'port'] and at least one of ["new_host", "new_port", "new_retries"].	Modifies the proxy server to the existing server list for the specified proxy group.	Yes

## Deleting the Upstream Proxy Servers

Table 71 - Attributes for Deleting the Upstream Proxy Servers

API	/wsa/api/v2.0/configure/network/upstream_proxy/servers				
Method	DELETE				
Parameters	None				
Request body	Name	Type	Format	Description	Required
	group_name	String	Valid group name string	group name. For example, "test1"	Yes

HTTPS Proxy

	proxy_servers	Array of objects	List of dict(s), each dict having keys - ['host', 'retries', 'port']	Deletes the proxy server to the existing server list for the specified proxy group.	Yes
--	---------------	------------------	--	---	-----

## HTTPS Proxy

### Retrieving the HTTPS Proxy Details

Table 72 - Retrieving the HTTPS Proxy Details

API	/wsa/api/v2.0/configure/security_services/proxy/https				
Method	GET				
Parameters	None				
Request body	None				
Response	Code	Type	Description		
	200 Ok	Object	HTTPS Proxy configuration.		

### Modifying the HTTP Proxy Settings

Table 73 - Attributes for Modifying the HTTP Proxy Settings

API	/wsa/api/v2.0/configure/security_services/proxy/https				
Method		PUT			
Parameters		None			
Request body	Name	Type	Format	Description	Required

HTTPS Proxy

	accept_license	Boolean		True/False	Conditional. When the feature key is submitted, and license is to be accepted.
	https_enabled	Boolean	True/False	Status of https.	No
	https_ports	List of port string	" 121" or " 8080,8443" or " 55-66"	List of the https ports comma (,) separated or range.	No
	Authentication	Boolean	True/False	Status of authentication.	No
	user_acknowledgement	Boolean	True/False	Status of user acknowledgment.	No
	application_visibility2	Boolean	True/False	Application visibility status.	No
	expired_cert	String	String - Valid values - ['drop', 'decrypt', 'scan']	Action for expired cert.	No
	invalid_leaf_cert	String	String - Valid values - ['drop', 'decrypt', 'scan']	Action for invalid leaf cert.	No

	unrecognized_root	String	String - Valid values - ['drop', 'decrypt', 'scan']	Action for an unrecognized root.	No
	invalid_signing_cert	String	String - Valid values - ['drop', 'decrypt', 'scan']	Action for an invalid signing cert.	No
	mismatched_hostname	String	String - Valid values - ['drop', 'decrypt', 'scan']	Action for mismatch hostname.	No
	other_error	String	String - Valid values - ['drop', 'decrypt', 'scan']	Action in case of other errors.	No
	current_cert_type	String	String - Valid values - ['generated', 'uploaded']	Status of the current certificate whether it is part of request (for example, that is uploaded) or to be generated.	No
	common_name	String	A valid common name	Common name of the certificate.	Yes, if cert type is generated

	org	String	A valid org name	Organization	Yes, if cert type is generated
	org_unit	String	A valid Org unit name	Org unit of certificate	Yes, if cert type is generated
	country	String	A valid country name ISO 2 letter code	Country of certificate.	Yes, if cert type is generated
	expires	Number		Number in months for expiry	Yes, if cert type is generated
	is_x509v3_critical	Boolean	True/False	Enable x509v_critical or not	Yes, if cert type is generated
	certificate	File input (multipart/form-data)		A certificate file.	Yes, if cert type is uploaded.
	key	File input (multipart/form-data)		A key file.	Yes, if cert type is uploaded.
	password	String		Password associated with certificate.	Yes, if cert type is uploaded.
	signed_cert	File input (multipart/form-data)		Signed certificate	Yes, if cert type is generated.
Response	Code		Type	Description	
	200 Ok		Dictionary		

## Retrieving the HTTP Proxy–Download Certificate File

Table 74 - Attributes for HTTP Proxy–Download Certificate File

API	/wsa/api/v2.0/configure/security_services/proxy/https/download			
Method	GET			
Parameters	Name	Type	Description	Required
	cert_type	String	Valid values: ['generated', 'csr', 'uploaded']	Yes
Request body	None			
Response	Code	Type	Description	
	200 Ok		Cert file	

## Retrieving the HTTP Proxy OCSP Settings

Table 75 - Attributes for HTTP Proxy - OCSP settings

API	/wsa/api/v2.0/configure/security_services/proxy/ocsp			
Method	GET			
Parameters	None			
Request body	None			
Response	Code	Type	Description	
	200 Ok		OCSP setting	

## Modifying the HTTP Proxy–OCSP Settings

Table 76 - Attributes for PUT HTTP Proxy–OCSP Settings

API	/wsa/api/v2.0/configure/security_services/proxy/ocsp			
Method	PUT			

HTTPS Proxy

Parameters	None				
Request body	Name	Type	Format	Description	Required
	ocsp_enabled	Boolean	True/False	Status of OCSP	No
	ocsp_valid_response_cache_timeout	Number	Number in seconds	Valid OCSP Cache timeout in seconds.	No
	ocsp_invalid_response_cache_timeout	Number	Number in seconds	Invalid OCSP Cache timeout in seconds.	No
	ocsp_network_error_cache_timeout	Number	Number in seconds	OCSP network error Cache timeout in seconds.	No
	ocsp_clock_skew	Number	Number in seconds	OCSP clock skew in seconds.	No



HTTPS Proxy

	ocsp_network_error_timeout	Number	Number in seconds	OCSP network error timeout in seconds.	No
	ocsp_result_handling	Dictionary	{ "unknown":<"drop"/"decrypt"/"scan"> "revoked": "<"drop"/"decrypt"/"scan"> "error": "<"drop"/"decrypt"/"scan">}	Dictionary with following keys - unknown, revoked, and error each having valid values from - ("drop", "decrypt", "scan")	No
	ocsp_use_nonce	Boolean	True/False		No
	ocsp_use_upstream_proxy	Boolean	True/False	Use upstream proxy for OCSP.	No
	ocsp_proxy_group	String		OCSP group name string.	No

Log Subscriptions

	ocsp_proxy_group_exempt_list	List of strings		For example: [" 1.1.1.1", " 2.2.2.2"]	
--	------------------------------	-----------------	--	---	--

## Log Subscriptions

### Retrieving the Log Subscriptions

Table 77 - Attributes for GET Log Subscriptions

API	/wsa/api/v2.0/configure/system/log_subscriptions			
Method	GET			
Parameters	Name	Type	Description	Required
	offset	Integer	Offset among the list of domain map	If limit is present.
	limit	Integer	Number of records to be displayed starting from offset.	If offset is present.
	log_name	String	Log name. For example, <b>“accesslogs”</b>	No
	summary	Boolean	Whether to show summary	No
Request body	None			
Response	Code	Type	Description	
	200 Ok		Log subscription settings	

## Modifying the Log Subscriptions

Table 78 - Attribute of PUT Log Subscriptions

API	/wsa/api/v2.0/configure/system/log_subscriptions				
Method	PUT				
Parameters	None				
Request body	Name	Type	Format	Description	Required
	new_log_name	String	Valid log name	e.g., "log_name_1"	No
	log_name	String	Previous log name to be modified.	e.g., "prev_log_name"	Yes
	log_level	String	Level of logs one among: 'debug', 'information', 'critical', 'warning', 'trace').	Log level	No
	log_type	String	Type of log.	For example, "CLI Audit Logs". You can obtain the list from Field List API of all the Log Types.	Yes
	log_file_name	String	File name	Log file name.	No
	rollover_file_size	Integer	Size in KB	Rollover size of log file. For example, "10240".	No

	retrieval_method	Object	<pre>{   "max_num_files":   &lt;num&gt;,   "method":   &lt;method&gt;} </pre>	<p>Expected a dictionary with all the retrieval method parameters and their values. Below are the settings for each retrieval method</p> <pre>"retrieval_method": {   "max_num_files" : 10,   "method": "local" } "retrieval_method": {   "method": "ftp_push",   "ftp_directory": "/upload/new",   "ftp_username": "rtestuser",   "ftp_host": "ciscoftp.com",   "ftp_password": "pass1234" } "retrieval_method": {   "method": "scp_push",   "scp_username": "acssacac",   "scp_directory": "/update/",   "scp_key":</pre>	No
--	------------------	--------	---	---	----

Log Subscriptions

				<pre> "strict",   "scp_host": " ciscoscp.com",   "scp_key_metho d": " auto"   }   "retrieval_method": {   "method": "syslog_push",   "syslog_facility": "user",   "syslog_protocol ": " UDP",   "syslog_msg_siz e": 1222,   "syslog_hostnam e": " ciscosyslog.com",   "syslog_port": 514   } </pre>	
	method	String	Retrieval Method - Possible Values (" local" -> FTP on None, " ftp_push" -> FTP on Remote Server, " scp_push" -> SCP on Remote Server, " syslog_push" -> Syslog Push)	Retrieval method	

Log Subscriptions

	ftp_directory	String	FTP Directory	For example, /upload/new"	No. Accepted only if the method is local.
	ftp_username	String	FTP Username	For example, "rtestuser".	No. Accepted only if the method is ftp_push.
	ftp_host	String	FTP Host	For example, "ciscoftp.com".	No. Accepted only if the method is ftp_push.
	ftp_password	String	FTP Password (plain string)	For example, "pass1234".	No. Accepted only if ftp_push is selected.
	scp_username	String	SCP Username	For example, "user1".	No. Accepted only if the method is scp_push.
	scp_directory	String	SCP Directory	For example, "/update"	No. Accepted only if the method is scp_push.
	scp_key	String	SCP Key	For example, "strict".	No. Accepted only if the method is scp_push.
	scp_host	String	SCP Host	For example, "ciscoscp.com".m	No. Accepted only if the method is scp_push.

Log Subscriptions

	scp_key_method	String	SCP Key method: "auto"/"manual"	For example, "auto".	No. Accepted only if the method is scp_push.
	scp_value	String	SCP string: "ssh-rsa ADDQWE#@RE... root@host.cisco"	SCP enter manually, required when ACP KEY METHOD is selected as manual.	No. Accepted only if method is scp_push.
	syslog_facility	String	SYSLOG Facility - Possible Values (Obtain list from Fields List API)	For example, "user"	No. Accepted only if the method is syslog_push.
	syslog_protocol	String	SYSLOG Protocol - Possible values :("TCP", "UDP").	For example, "UDP"	No. Accepted only if the method is syslog_push.
	syslog_msg_size	Integer	SYSLOG Maximum message size	For example, 1222	No. Accepted only if the method is syslog_push.
	syslog_hostname	String	SYSLOG Hostname	For example, "ciscosyslog.com"	No. Accepted only if the method is syslog_push.
	syslog_port	Integer	Valid port number	For example, 4433	No. Accepted only if the method is syslog_push.

## Adding the Log Subscriptions

Table 79 – Attributes for POST Log Subscriptions

API	/wsa/api/v2.0/configure/system/log_subscriptions				
Method	POST				
Parameters	None				
Request body	Name	Type	Format	Description	Required
	new_log_name	String	Valid log name	For example, "log_name_1"	Yes
	log_level	String	Level of logs one among: 'debug', 'information', 'critical', 'warning', 'trace')	Log level	No
	log_type	String	Type of log	For example, "CLI Audit Logs". You can get the list from Field List API of all the Log Types.	Yes
	log_file_name	String	File name	Log file name.	No
	rollover_file_size	Integer	Size in KB	Rollover size of log file. For example, "10240".	No



Log Subscriptions

	retrieval_method	Object	<pre>{   "max_num_files":   &lt;num&gt;,   "method":   &lt;method&gt;} </pre>	<p>Expected a dictionary with all the retrieval method parameters and their values. Below are the settings for each retrieval method</p> <pre>"retrieval_method": {   "max_num_files" : 10,   "method" : "local"   }   "retrieval_method": {   "method" : "ftp_push",   "ftp_directory": "/upload/new",   "ftp_username": "rtestuser",   "ftp_host": "ciscoftp.com",   "ftp_password": "pass1234"   }   "retrieval_method": {   "method" : "scp_push",   "scp_username": "acssacac",   "scp_directory": "/update/",   "scp_key": "strict",</pre>	No
--	------------------	--------	---	--	----

				<pre> "scp_host": "ciscoscp.com", "scp_key_method": "auto" } "retrieval_method": { "method": "syslog_push", "syslog_facility": "user", "syslog_protocol": "UDP", "syslog_message_size": 1222, "syslog_hostname": "ciscosyslog.com", "syslog_port": 514 } </pre>	
	method	String	Retrieval Method - Possible Values ("local" -> FTP on None, "ftp_push" -> FTP on Remote Server, "scp_push" -> SCP on Remote Server, "syslog_push" -> Syslog Push)	Retrieval method	

Log Subscriptions

	ftp_directory	String	FTP Directory	For example, "/upload/new" .	No. Accepted only if the method is local.
	ftp_username	String	FTP Username	For example, "rtestuser".	No. Accepted only if the method is ftp_push.
	ftp_host	String	FTP Host	For example, "ciscoftp.com".	No. Accepted only if the method is ftp_push.
	ftp_password	String	FTP Password (plain string)	For example, "pass1234".	No. accepted only if ftp_push is selected
	scp_username	String	SCP Username	For example, "user1".	No. Accepted only if the method is scp_push.
	scp_directory	String	SCP Directory	For example, "/update".	No. Accepted only if the method is scp_push.
	scp_key	String	SCP Key	For example, "strict".	No. Accepted only if the method is scp_push.
	scp_host	String	SCP Host	For example, "ciscoscp.com".	No. Accepted only if the method is scp_push.

Log Subscriptions

	scp_key_method	String	SCP Key method: "auto"/" manual"	For example, "auto"	No. Accepted only if the method is scp_push.
	scp_value	String	SCP string: "ssh-rsa ADDQWE#@RE... root@host.cisco"	SCP Enter Manually, required when ACP KEY METHOD is selected as manual	No. Accepted only if method the is scp_push.
	syslog_facility	String	SYSLOG Facility - Possible Values (Can get from Fields List API)	For example, "user"	No. Accepted only if the method is syslog_push.
	syslog_protocol	String	SYSLOG Protocol - Possible values ("TCP", "UDP")	For example, "UDP"	No, accepted only if method is syslog_push
	syslog_msg_size	Integer	SYSLOG Maximum message size	For example, 1222	No. Accepted only if the method is syslog_push
	syslog_hostname	String	SYSLOG Hostname	For example, "ciscosyslog.com"	No. Accepted only if the method is syslog_push.
	syslog_port	Integer	Valid port number	For example, 4433	No. ccepted only if the method is syslog_push.

Log Subscriptions

	<p>rollover_by_time</p>	<p>Object</p>	<p>ROLLOVER BY TIME. All the possible settings: "rollover_by_time": {     "rollover_interval": "none"     }     "rollover_by_time": {         "rollover_interval": "daily"         "rollover_daily_time": 1303     }     "rollover_by_time": {         "rollover_interval": "weekly",         "rollover_days": [             "mon",             "tue",             "wed"         ],         "rollover_weekly_time": 223     }     "rollover_by_time": {         "rollover_interval": "custom",         "rollover_cus</p>	<p>For example, {     "rollover_interval": "daily"     "rollover_daily_time": 1303 }</p>	<p>No</p>
--	-------------------------	---------------	--	--	-----------

Log Subscriptions

			tom_time" : 2880 }		
	rollover_interval	String	ROLLOVER Interval - Possible Values (" none", " daily", " weekly", " custom")	For example, "none"	No
	rollover_custom_time	Integer	ROLLOVER CUSTOM TIME in minutes. For example, 00:23 -> 23, 1:23 -> 83, 1d -> 24*60 mins	For example, 2880	No, accepted only if "recover_interval" is "custom"
	rollover_daily_time	Integer	ROLLOVER_DAILY Time Eg. 00:23 -> 23, 1:23 -> 83	For example, 1303	No, accepted only if "rollover_interval" is "daily"
	rollover_days	List of strings	ROLLOVER Days - Possible Values ("mon", " tue", " wed", " thu", " fri", " sat", " sun")	For example, ["mon", "tue", "wed"]	No, accepted only if "rollover"interval" is "weekly"
	rollover_weekly_time	Integer	ROLLOVER_WEEKLY Time in minutes. For example, 00:23 -> 23, 1:23 -> 83	For example, 223	No, accepted only if "rollover_interval" is "weekly"
	selected_field	List of strings	SELECTED Field - W3C Selected Fields, List we can get from Fields List API	For example, [ " timestamp", " DCF", " bytes", " c-a-ip" ]	No, accepted only when "log_type" is "W3C Logs"

Log Subscriptions

	anonymization_passphrase	String	ANONYMIZATION Passphrase	For example, "Agt!1111"	No. Accepted only when "log_type" is "W3C Logs", and some anonymized fields such as "c-a-ip" are entered in selected_fields.
	w3c_log_type	String	W3C_LOG Type - Possible Values ("w3c_type_std", "w3c_type_cta", "w3c_type_cloudlock")	For example, "w3c_type_std"	No, accepted only when "log_type" is "W3C Logs"
	custom_fields	String	Custom fields	For example, "% ("	No, accepted only when "log_type" is "W3C Logs"
	log_compression	Boolean	True/False	Log compression status	No
	log_exclusion	List of integers	Log Exclusion in W3C logs	For example, [404, 400]	No, accepted only when "log_type" is "W3C Logs"

	<p>rollover_by_time</p>	<p>Object</p>	<p>ROLLOVER BY TIME. All the possible settings: "rollover_by_time": {     "rollover_interval": "none"     "rollover_by_time": {         "rollover_interval": "daily"         "rollover_daily_time": 1303     }     "rollover_by_time": {         "rollover_interval": "weekly",         "rollover_days": [             "mon",             "tue",             "wed"         ],         "rollover_weekly_time": 223     }     "rollover_by_time": {         "rollover_interval": "custom",         "rollover_cus</p>	<p>For example, {     "rollover_interval": "daily"     "rollover_daily_time": 1303 }</p>	<p>No</p>
--	-------------------------	---------------	--	--	-----------



Log Subscriptions

			tom_time" : 2880 }		
	rollover_interval	String	ROLLOVER Interval - Possible Values (" none", " daily", " weekly", " custom")	For example, <b>"none"</b>	No
	rollover_custom_time	Integer	ROLLOVER CUSTOM TIME in minutes. For example, 00:23 -> 23, 1:23 -> 83, 1d - > 24*60 mins	For example, 2880	No, accepted only if <b>"recover_interval"</b> is <b>"custom"</b>
	rollover_daily_time	Integer	ROLLOVER_DAILY Time Eg. 00:23 -> 23, 1:23 -> 83	For example, 1303	No, accepted only if <b>"rollover_interval"</b> is <b>"daily"</b>
	rollover_days	List of strings	ROLLOVER Days - Possible Values ("mon", " tue", " wed", " thu", " fri", " sat", " sun").	For example, ["mon", "tue", "wed"]	No, accepted only if <b>"rollover"interval</b> is <b>"weekly"</b>
	rollover_weekly_time	Integer	ROLLOVER_WEEKLY Time in minutes. For example, 00:23 -> 23, 1:23 -> 83	For example, 223	No, accepted only if <b>"rollover_interval"</b> is <b>"weekly"</b>
	selected_field	Array of strings	SELECTED Field - W3C Selected Fields, List we can get from Fields List API	For example, [ " timestamp", " DCF", " bytes", " c-a-ip" ]	No, accepted only when " log_type" is " W3C Logs"

Log Subscriptions

	anonymization_passphrase	String	ANONYMIZATION Passphrase	For example, "Agt!1111"	No, accepted only when "log_type" is "W3C Logs", and some anonymized fields such as "c-a-ip" are passed in "selected_fields"
	w3c_log_type	String	W3C_LOG Type - Possible Values ("w3c_type_std", "w3c_type_cta", "w3c_type_cloudlock")	For example, "w3c_type_std"	No, accepted only when "log_type" is "W3C Logs"
	custom_fields	String	Custom fields	For example, "% ("	No, accepted only when "log_type" is "W3C Logs"
	log_compression	Boolean	True/False	Log compression status	No
	log_exclusion	Array of integers	Log Exclusion in W3C logs	For example, [404, 400]	No, accepted only when "log_type" is "W3C Logs"

## Deleting the Log Subscriptions

Table 80 - Attributes for DELETE Log Subscriptions

API	wsa/api/v2.0/configure/system/log_subscriptions
-----	---

Log Subscriptions

Method	DELETE				
Parameters	None				
Request body	Name	Type	Format	Description	Required
	delete_all	Boolean	True/False	True if we want to delete all the log subscriptions	No
	log_name	Array of Strings	String or list of strings	For example, ["accesslogs", "cli_logs"] or "accesslogs"	Yes

## Modifying the Log Subscriptions—Rollover

Table 81 - Attributes for PUT Log Subscriptions for Rollover

API	/wsa/api/v2.0/configure/system/log_subscriptions/rollover				
Method	PUT				
Parameters	None				
Request body	Name	Type	Format	Description	Required
	rollover_all	Boolean	True/False	True if you require to rollover all the Log Subscriptions.	No
	log_name	String or Array of strings	String or list of strings	For example, "accesslogs", "cli_logs"] or "accesslogs" .	Yes

## Retrieving the Log Subscriptions for the Fetch Field Lists

Table 82 – Attributes for GET Log Subscriptions for Fetch Field List

API	/wsa/api/v2.0/configure/system/log_subscriptions/fields			
Method	GET			
Parameters	Name	Type	Description	Required
	fetch	String. Possible Values (" facility_list", " type_list", " w3c_available_log_fields_list")		Yes
Request body	None			
Response	Code	Type	Description	
	200 Ok		Log subscription settings	

## Retrieving the Log Subscriptions to Fetch Default Values for a Log Type

Table 83 – Attributes for Log Subscriptions to Fetch Default Values for Log Type

API	/wsa/api/v2.0/configure/system/log_subscriptions/defaults			
Method	GET			
Parameters	Name	Type	Description	Required
	log_type	String	For example, "audit_logs"	Yes
Request body	None			
Response	Code	Type	Description	
	200 Ok		Log subscription default values for the given log type	

## Adding the Log Subscriptions–Deanonymization

Table 84 - Attributes for POST Log Subscriptions–Deanonymization

API	/wsa/api/v2.0/configure/system/log_subscriptions/deanonymization				
Method	POST				
Parameters	None				
Request body	Name	Type	Format	Description	Required
	uploaded_file	Multipart-formdata	File	For example, file.csv	No. Mandatory if "encrypted_content" is set as "encrypted_file"
	log_name	String	An existing W3C log name on the machine	For example, w3c_std	Yes
	passphrase	String	passphrase	Passphrase to deanonymize the encrypted content. For example, Abcd@1234	No. Mandatory when the passphrase is not set for the log_name provided already.
	encrypted_content	String	Encrypted content (string)	String of anonymized content separated by comma	No. Mandatory when "encrypted_content" is set as "encrypted_text"

Header Based Authentication

	download_as_file	Boolean	True/False	Specify whether the response must be a downloadable file or a General response. The <b>value is "True"</b> for Downloadable format.	Yes
--	------------------	---------	------------	---	-----

## Header Based Authentication

### Retrieving Header Based Authentication

Table 85 - Attributes for Retrieving Header Based Authentication

API	/wsa/api/v3.0/network/xauth_header_setting		
Method	GET		
Parameters	None		
Request body	None		
Response	Code	Type	Description
	200 Ok	Object <a href="#">xauth_header_setting</a>	It contains a dictionary with all the configuration parameters of header-based authentication

### Enabling or Disabling Header Based Authentication

Table 86 - Attributes for Enabling or Disabling Header Based Authentication

API	/wsa/api/v3.0/network/xauth_header_setting
Method	PUT

Header Based Authentication

Parameters	None			
Request body	Name	Type	Description	Required
	xauth_header_based_auth	String	It is used to enable/disable header-based authentication. Values are:  <input type="checkbox"/> Enable  <input type="checkbox"/> Disable	Yes
Response	Code	Type	Description	
	204 No Content	Empty body	If everything in the request body is correct.	

## Modifying Header Based Authentication Configuration

Table 87 - Attributes for Modifying Header Based Authentication Configuration

API	/wsa/api/v3.0/network/xauth_header_setting			
Method	PUT			
Parameters	None			
Request body	Name	Type	Description	Required
	xauth_header_based_auth	String	It contains either enable or disable, other values are not allowed. It represents if the header-based authentication is enabled or disabled.	Yes
	xauth_use_group_header	String	It represents if consider group headers is enabled or disabled.	Yes

Header Based Authentication

	xauth_retain_auth_egress	String	It represents if retain authentication details on egress is enabled or disabled.	Yes
	xauth_header_mode	String	It represents which header is used, whether its standard or custom.	Yes
	xauth_std_user	Object	It represents the “text_format” and “Binary_encoding” of standard X-Authenticated-User.	Yes
	xauth_std_group	Object	It represents the “text_format” and “Binary_encoding” of standard X-Authenticated-Groups	Yes
	xauth_custom_user	Object	It represents the “name”, “text_format” and “Binary_encoding” of the custom X-Authenticated-User.	Yes
	xauth_custom_group	Object	It represents the “name”, “text_format” and “Binary_encoding” of the custom X-Authenticated-Groups	Yes
Response	Code	Type	Description	
	204 No Content	Empty body	If everything in the request body is correct.	



## Definitions

### xauth\_header\_setting

Name	Type	Description	Required	
			GET	PUT
xauth_header_setting	Objects	Every element in this Object represents the configuration parameters that are related to header-based authentication	Yes	Yes

Table 88 - Attributes for xauth\_header\_setting

Name	Type	Description	Required	
			GET	PUT
xauth_header_based_auth	String	To enable or disable header based authentication.	No	Yes
xauth_use_group_header	String	To enable or disable consider group headers.	No	Yes
xauth_retain_auth_egress	String	To enable or disable retain authentication header details on the egress.	No	Yes
xauth_header_mode	String	To configure standard or custom header	No	Yes

xauth\_std\_user

Table 89 - Attributes for xauth\_std\_user

Name	Type	Description	Required	
			POST	PUT
text_format	String	Represents the character encoding type for the header value. Possible values are <b>'UTF-8' or 'ASCII'</b>	No	Yes
Binary_encoding	String	Represents the binary encoding type for the header value. Possible values are <b>'Base64' or 'No Encoding'</b>	No	Yes

xauth\_std\_group

Table 90 - Attributes for xauth\_std\_group

Name	Type	Description	Required	
			POST	PUT
text_format	String	Represents the character encoding type for the header value. Possible values are <b>'UTF-8' or 'ASCII'</b>	No	Yes
Binary_encoding	String	Represents the binary encoding type for the header value. Possible values are <b>'Base64' or 'No Encoding'</b>	No	Yes

xauth\_custom\_user

Table 91 - Attributes for xauth\_custom\_user

Name	Type	Description	Required	
			POST	PUT
Name	String	Represents the customized name that is provided for X-Authenticated-user.	No	Yes
text_format	String	Represents the character encoding type for the header value. Possible values are 'UTF-8' or 'ASCII'.	No	Yes
Binary_encoding	String	Represents the binary encoding type for the header value. Possible values are 'Base64' or 'No Encoding'	No	Yes

xauth\_custom\_group

Table 92 - Attributes for xauth\_custom\_group

Name	Type	Description	Required	
			POST	PUT
Name	String	Represents the customized name that is given for X-Authenticated-user.	No	Yes

Header Based Authentication

Name	Type	Description	Required	
			POST	PUT
text_format	String	Represents the character encoding type for the header value. Possible values are 'UTF-8' or 'ASCII'.	No	Yes
Binary_encoding	String	Represents the binary encoding type for the header value. Possible values are 'Base64' or 'No Encoding'.	No	Yes

response\_status

Table 93 - Attributes for response\_status

Name	Type	Description
status	Integer	Response Code

error\_response

Table 94 - Attributes for error\_response

Name	Type	Description
code	Integer	Response Code
message	String	Error Message
explanation	String	Explanation

## HTTP ReWrite Profiles

### Retrieving the HTTP ReWrite Profiles

Table 95 - Attributes for Retrieving the HTTP ReWrite Profiles

API	/wsa/api/v3.0/web_security/http_rewrite_profiles		
Method	GET		
Parameters	None		
Request body	None		
Response	Code	Type	Description
	200 Ok	Objects <a href="#">http_rewrite_profile_collection_schema</a>	It contains a list of http rewrite profiles, their configurations, and global settings.

### Modifying the HTTP ReWrite Profiles

Table 96 - Attributes for Modifying the HTTP ReWrite Profiles

API	/wsa/api/v3.0/web_security/http_rewrite_profiles			
Method	PUT			
Parameters	None			
Request body	Name	Type	Description	Required

HTTP ReWrite Profiles

	http_rewrite_profiles	Array of objects <a href="#">http_rewrite_profile_collection_schema</a>	It contains a list of http rewrite profiles. If you must POST or PUT for only single profile, it contains details only for that profile.	Yes
	global_settings	Objects <a href="#">global_settings_schema</a>	It represents the X-Authenticated header global settings.	No
Response	Code	Type	Description	
	204 No Content	Empty body	If everything in request body is correct.	
	207 Multi Status	Objects <a href="#">multi_status_response</a>	Dictionary of success and failure list. Failure list contains the appropriate error message, specifying reason for failure.	

## Adding the HTTP ReWrite Profiles

Table 97 - Attributes for Adding the HTTP ReWrite Profiles

API	/wsa/api/v3.0/web_security/http_rewrite_profiles			
Method	POST			
Parameters	None			
Request body	Name	Type	Description	Required

HTTP ReWrite Profiles

	http_rewrite_profiles	Array of objects <a href="#">http_rewrite_profile_collection_schema</a>	It contains a list of http rewrite profiles. If you must POST or PUT for only single profile, it contains details only for that profile.	Yes
	global_settings	Objects <a href="#">global_settings_schema</a>	It represents the X-Authenticated header global settings.	No
Response	Code	Type	Description	
	204 No Content	Empty body	If everything in the request body is correct.	
	207 Multi Status	Objects <a href="#">multi_status_response</a>	Dictionary of success and failure list. Failure list contains the appropriate error message, specifying reason for failure.	

## Deleting the HTTP ReWrite Profiles

Table 98 - Attributes for Deleting the HTTP ReWrite Profile

API	/wsa/api/v3.0/web_security/http_rewrite_profiles			
Method	DELETE			
Parameters	Name	Type	Description	Required
	profile_name	String	Represents the profile name to be deleted.	Yes

	alternate_profile_name	String	Represents the http rewrite profile to be replaced in access policies in place of deleted profile.	Yes
Request body	None			
Response	Code	Type	Description	
	204 No Content	Empty body	If the requested profile got deleted	
	207 Multi Status	Objects <a href="#">multi_status_response</a>	Dictionary of success and failure list. Failure list contains the appropriate error message, specifying reason for failure.	
	406 Not Acceptable	Objects <a href="#">error_response</a>	Error message saying that profile_name and alternate_profile_name cannot be same.	



## Definitions

### http\_rewrite\_profile\_collection\_schema

Table 99 - Attributes for http\_rewrite\_profile\_collection\_schema

Name	Type	Description	Required	
			POST	PUT
http_rewrite_profiles	Array of objects <a href="#">http_rewrite_profile_schema</a>	Every element in this list represents a single http rewrite profile.	Yes	Yes
global_settings	Objects <a href="#">global_settings_schema</a>	It represents the X-Authenticated header global settings.		

### http\_rewrite\_profile\_schema

Table 100 - Attributes for http\_rewrite\_profile\_schema

Name	Type	Description	Required	
			POST	PUT
profile_name	String	Unique identifier of profile	Yes	Yes
new_profile_name	String	It represents a new profile name. (Valid only if it is PUT)	Not used in POST	Only when name change is required
headers	Array of objects <a href="#">header_schema</a>	List of headers to be added, modified, or deleted in outbound traffic.	Yes	No

Name	Type	Description	Required	
			POST	PUT

header\_schema

Table 101 - Attributes for header\_schema

Name	Type	Description	Required	
			POST	PUT
header_name	String	Unique identifier of header in the selected profile. This is the name of the header that is added, modified, or deleted in the outgoing traffic.	Yes	Yes
header_value	String	Represents the value of the header which will be added, modified, or deleted in the outgoing traffic for the corresponding header name.	Yes	Yes
text_format	String	Represents the character encoding type for the header value. Possible values are <b>'UTF-8'</b> or <b>'ASCII'</b> .	Yes	Yes
binary_encoding	String	Represents the binary encoding type for the header value. Possible values are <b>'Base64'</b> or <b>'No Encoding'</b> .	Yes	Yes

global\_settings\_schema

Table 102 - Attributes for global\_settings\_schema

Name	Type	Description	Required	
			POST	PUT
rewrite_format_for_user	String	Represents the rewrite format for X-Authenticated-User.  It should be a combination of \$authMechanism, \$domainName and \$userName in the same sequence. Possible separators are '\ ' or '/ '.	Yes	Yes
rewrite_format_for_group s	String	Represents the rewrite format for X-Authenticated-Groups.  It should be a combination of \$authMechanism, \$domainName and \$groupName in the same sequence. Possible separators are '\ ' or '/ '.	Yes	Yes
delimiter_for_groups	String	Represents the delimiter between the groups in X-Authenticated-Groups.  Possible values are Comma (,), Colon (:), Semicolon(;), Backslash(\), Vertical bar( ).	Yes	Yes

multi\_status\_response

Table 103 - Attributes for multi\_status\_response

Name	Type	Description
success_list	Array of objects <a href="#">response_status</a>	Success list, with profile name and messages.
failure_list	Array of objects <a href="#">response_status</a>	Failure list, with profile name and messages.
success_count	Integer	Success Count
failure_count	Integer	Failure Count

response\_status

Table 104 - Attributes for response\_status

Name	Type	Description
status	Integer	Response Code
message	String	Error/Success Message
profile_name	String	Profile name

error\_response

Table 105- Attributes for error\_response

Name	Type	Description
code	Integer	Response Code

General Purpose APIs

Name	Type	Description
message	String	Error Message
explanation	String	Explanation

## General Purpose APIs

### SecureX

#### Retrieving the Registered User Information

Table 106 - Attributes for Registered User Information

API	/wsa/api/v2.0/ctr/user_info		
Method	GET		
Parameters	None		
Request body	None		
Response	Code	Type	Description
	200 Ok	Object	It contains a dictionary with all the parameter of registered user.

#### Adding the Registered User Information

Table 107 - Attributes for Securex Ribbon Registration

API	/wsa/api/v2.0/ctr/user_info		
Method	POST		
Parameters	None		

General Purpose APIs

Request body	Name	Type	Description	Required
	User_info	object	Dictionary of the client name, secret, and server	Yes
Response	Code	Type	Description	
	200	Empty body	If everything in the request body is correct.	

### Modifying the Registered User Information

Table 108 - Attributes for Modifying SecureX Registered User Information

API	/wsa/api/v2.0/ctr/user_info			
Method	PUT			
Parameters	None			
Request body	Name	Type	Description	Required
	User_info	Object	Dictionary of the client name, secret, and server.	Yes
Response	Code	Type	Description	
	200	Empty body	If everything in the request body is correct.	

Definitions

response\_status

Table 109 - Attributes for response\_status

Name	Type	Description
Status	Integer	Response Code

error\_response

Table 110 - Attributes for error\_response

Name	Type	Description
Code	Integer	Response Code
Message	String	Error Message
Explanation	String	Explanation

## Auth Settings

### Retrieving the Auth Settings

Table 111 - Attributes for Retrieving the Auth Settings

API	/wsa/api/v3.0/generic_resources/auth_settings		
Method	GET		
Parameters	None		
Request body	None		
Response	Code	Type	Description
	200 Ok	Object <a href="#">auth_settings</a>	It represents a subset of auth settings. It contains enough information for associating an auth realm with identification_profile.

Definitions

auth\_settings

Table 112 - Attributes for auth\_settings

Name	Type	Description
header_based_auth	String	Represents, whether header-based authentication is enabled or not (in Global Authentication Settings).
realms	List of objects <a href="#">realm_settings</a>	Every object in this list represents an authentication realm.
sequences	List of objects <a href="#">sequence_settings</a>	Every object in this list represents a realm sequence.

realm\_settings

Table 113 - Attributes for realm\_settings

Name	Type	Description
name	String	Realm name
schemes	List of strings	Every element in this list represents a type of authentication scheme. For example, Kerberos, NTLMSSP, Basic, Header, and so on.
type	String	Enum (AD, LDAP)
supports_tui	Boolean	It represents whether Transparent User Identification has been enabled or not for this realm.



sequence\_settings

Table 114 - Attributes for sequence\_settings

Name	Type	Description
name	String	Name of realm sequence.
schemes	List of strings	Every element in this list represents type of authentication scheme. For example, Kerberos, NTLMSSP, Basic, Header, and so on.

## User Agents

### Retrieving the User Agents

Table 115 - Attributes for User Agents

API	/wsa/api/v3.0/generic_resources/user_agents		
Method	GET		
Parameters	None		
Request body	None		
Response	Code	Type	Description
	200 Ok	Object <a href="#">User_agents</a>	It contains allowed <b>user agent's</b> string representations.

Definitions

User\_agents

Table 116 - Attributes for User\_agent

Name	Type	Description
user_agents	List of strings	Elements in this list represent allowed user agents in Web Security Appliance. For example, Chrome/48, windows_updater, Firefox/40 and so on.

URL Categories

Retrieving URL Categories

Table 117 - Attributes for URL categories

API	/wsa/api/v3.0/generic_resources/url_categories		
Method	GET		
Parameters	None		
Request body	None		
Response	Code	Type	Description
	200 Ok	Object <a href="#">url_category</a>	It represents predefined and custom url categories.

Definitions

url\_category

Table 118 - Attributes for url\_category

Name	Type	Description
predefined	List of strings	It represents a list of AVC defined url categories.

General Purpose APIs

Name	Type	Description
custom	List of strings	It represents list of admin defined user categories.

## Time Ranges

### Retrieving Time Ranges

Table 119 - Attributes for Time Ranges

API	/wsa/api/v3.0/web_security/time_ranges		
Method	GET		
Parameters	None		
Request body	None		
Response	Code	Type	Description
	200 Ok	Object <a href="#">time_ranges</a>	Represents a collection of time ranges that are defined in the system.

### Definitions

#### time\_ranges

Table 120 - Attributes for time\_ranges

Name	Type	Description
time_ranges	List of objects <a href="#">time_range</a>	Every element in this list represents a time_range.

time\_range

Table 121 - Attributes for time\_range

Name	Type	Description
time_values	List of objects <a href="#">time_values</a>	Every element in this list represents part of a single day along with applicable weekday names.
name	String	Name of time range.
time_zone	String	Represents time zone. For example, "America/Los_Angeles". <b>For more examples</b> see, Web Security Appliance GUI time_ranges page.

time\_values

Table 122 - Attributes for time\_values

Name	Type	Description
time_of_day	String (all_day) or object ( <pre>{   "from": &lt;from_value&gt;   "to": &lt;to_value&gt;, }</pre>	Represents part of the day. If it is a full day, the value is "all_day". Otherwise, sometime range with, from and to in 24 hr format (For example: 18:10).
valid_days	List of strings	Enum of days of week. For example, Sunday, Monday and so on.

## Quotas

### Retrieving Quotas

Table 123 – Attributes for Retrieving Quotas

API	/wsa/api/v3.0/web_security/quotas		
Method	GET		
Parameters	None		
Request body	None		
Response	Code	Type	Description
	200 Ok	Object <a href="#">quotas</a>	It represents predefined and custom url categories.

### Definitions

#### quotas

Table 124 – Attributes for Quotas

Name	Type	Description
quotas	List of objects <a href="#">quota</a>	It represents a list of AVC defined url categories.

#### quota

Table 125 – Attributes for Quota

Name	Type	Description
name	String	Name of quota
time_zone	String	Represents time zone. For example, “America/Los_Angeles”. <b>For more examples</b> see, Web Security Appliance GUI quotas page.

General Purpose APIs

Name	Type	Description
time_quota_secs	integer	Allowed time limit in seconds.
volume_quota	integer	Allowed data limit in bytes.
reset_time	String	It represents time at which applied will be renewed. It is available in response only if no specific time_range has been selected for this quota.
time_range	String	It represents one of time_range identifier in the Web Security Appliance system. It is available in response only if no reset time has been selected for this quota.

## Proxy Settings

### Retrieving Proxy Settings

Table 126 - Attributes of Retrieving Proxy Settings

API	/wsa/api/v3.0/generic_resources/proxy_settings		
Method	GET		
Parameters	None		
Request body	None		
Response	Code	Type	Description
	200 Ok	Object <a href="#">proxy_setting</a>	Minimal details about all the proxies. Whether different types of proxies are enabled or not.

Definitions

Proxy\_settings

Table 127 – Attributes for Proxy\_settings

Name	Type	Description
proxy_settings	Object <a href="#">proxy_setting</a>	It has multiple key-value pairs which represent state of different types of proxy.

proxy\_setting

Table 128 – Attributes for Proxy\_setting

Name	Type	Description
web	Object ( <pre>{   "status": &lt;enable/disable&gt;,   "mode": &lt;transparent/forward&gt; }</pre> )	It represents whether web proxy is enabled or not. And if it is enabled, what is the mode of the proxy (transparent/forward).
socks	String	Whether socks proxy is enabled or not. Values can be enable/disable.
https	String	Whether https proxy is enabled or not. Values can be enable/disable.
ftp	String	Whether ftp proxy is enabled or not. Values can be enable/disable.

## Identification Methods

### Retrieving Identification Methods

Table 129 - Attributes for Retrieving Identification Methods

API	/wsa/api/v3.0/generic_resources/ identification_methods		
Method	GET		
Parameters	None		
Request body	None		
Response	Code	Type	Description
	200 Ok	Object <a href="#">identification_methods</a>	You are provided with a dictionary representing allowed and not allowed identification methods.

#### Definitions

##### identification\_methods

Table 130 - Attributes for identification\_methods

Name	Type	Description
identification_methods	Object <a href="#">identification_methods</a>	It is a dictionary representing allowed as well as not allowed identification methods.

##### identification\_methods

Table 131 - Attributes for identification\_method

Name	Type	Description
tui	String (Enum enable/disable)	Whether Web Security Appliance can Transparently identify users with Auth realms or not.



Static Data

Name	Type	Description
authentication	String (Enum enable/disable)	Whether Web Security Appliance can identify users with Authentication or not.
asa	String (Enum enable/disable)	Whether Web Security Appliance can Transparently identify users with ASA or not.
ise	String (Enum enable/disable)	Whether Web Security Appliance can Transparently identify users with ISE or not.

## Static Data

### Applications

While configuring the Application column and adding custom Applications Visibility and Control in access policy, you must be aware of the supported restrict actions for different types of applications. Currently, there are no REST APIs for obtaining this information. A static dictionary is created for this purpose. This dictionary can be used as any PUT or POST request for an access policy.

Some of the applications might not have any restrict action. In such cases, keep the dictionary value empty.

In the GUI, a group of different types of applications, for example, Gmail, Yahoo mail, and so on, that belong to a group, **“Webmail”** is available. This dictionary also has information about which application belongs to which group.

```
"applications": {
  "Webmail": {
    "monitor": {
      "Eyejot": {},
      "Outlook.com": {
        "restrict": [
          "Block File Attachment Upload",
          "Block File Attachment Download",
          "Block Sending Email"
        ]
      },
    },
    "GMX E-Mail": {
      "restrict": [
        "Block File Attachment Upload",
        "Block File Attachment Download",
        "Block Sending Email"
      ]
    },
  },
}
```

Static Data

```

    "AOL Mail": {
      "restrict": [
        "Block File Attachment Upload",
        "Block File Attachment Download",
        "Block Sending Email"
      ]
    },
    "Comcast Webmail": {
      "restrict": [
        "Block File Attachment Upload",
        "Block File Attachment Download",
        "Block Sending Email"
      ]
    },
    "MobileMe": {
      "restrict": [
        "Block File Attachment Upload",
        "Block File Attachment Download",
        "Block Sending Email"
      ]
    },
    "Hushmail": {
      "restrict": [
        "Block File Attachment Upload",
        "Block File Attachment Download",
        "Block Sending Email"
      ]
    },
    "Yahoo Mail": {
      "restrict": [
        "Block File Attachment Upload",
        "Block File Attachment Download",
        "Block Sending Email"
      ]
    },
    "Gmail": {
      "restrict": [
        "Block File Attachment Upload",
        "Block File Attachment Download",
        "Block Sending Email"
      ]
    }
  },
  "File Sharing": {
    "monitor": {
      "Gigaup": {},
      "ADrive": {},
      "YouSendIt": {},
      "Issuu": {},
      "SkyDrive": {
        "restrict": [
          "Block File Upload",
          "Block Download Documents",
          "Block Editing"
        ]
      }
    },
    "Weiyun": {
      "restrict": [
        "Block File Upload",
        "Block Sharing",
        "Block Download Documents"
      ]
    }
  }

```

## Static Data

```
    ]
  },
  "ifile.it": {},
  "RapidShare": {},
  "FileServe": {
    "restrict": [
      "Block File Upload"
    ]
  },
  "DepositFiles": {},
  "Okurin": {
    "restrict": [
      "Block File Upload",
      "Block Download Documents"
    ]
  },
  "Amazon Cloud Drive": {
    "restrict": [
      "Block File Upload",
      "Block Download Documents",
      "Block Sharing"
    ]
  },
  "Zbigz": {},
  "Yahoo Box": {},
  "LeapFile": {},
  "DocStoc": {
    "restrict": [
      "Block File Upload",
      "Block Download Documents"
    ]
  },
  "BitTorrent": {},
  "dl free": {
    "restrict": [
      "Block File Upload",
      "Block Download Documents"
    ]
  },
  "Filemail": {},
  "MediaFire": {},
  "Dropbox": {
    "restrict": [
      "Block File Upload",
      "Block Dropbox Folder Sharing",
      "Block Download Documents"
    ]
  },
  "eSnips": {
    "restrict": [
      "Block File Upload",
      "Block Download Documents"
    ]
  },
  "DivShare": {
    "restrict": [
      "Block File Upload",
      "Block Download Documents",
      "Block Sharing"
    ]
  },
  "sendspace": {},
  "FileDropper": {},
```

## Static Data

```
"TransferBigFiles": {},
"Google Drive": {
  "restrict": [
    "Block File Upload",
    "Block Download Documents",
    "Block Sharing",
    "Block Editing"
  ]
},
"AxiFile": {
  "restrict": [
    "Block File Upload",
    "Block Download Documents"
  ]
},
"netload": {
  "restrict": [
    "Block File Upload",
    "Block Download Documents"
  ]
},
"bonpoo": {},
"RayFile": {
  "restrict": [
    "Block Download Documents"
  ]
},
"Megashares": {},
"Datei.to": {
  "restrict": [
    "Block File Upload",
    "Block Download Documents"
  ]
},
"Filer.cx": {},
"4shared": {},
"PutLocker": {},
"WeTransfer": {},
"Fluxiom": {},
"Box.net": {},
"Megaupload": {},
"iCloud": {
  "restrict": [
    "Block iCloud Mail",
    "Block iCloud Calendar",
    "Block iCloud Bookmarks",
    "Block iCloud Contacts",
    "Block iCloud Photos"
  ]
},
"FileHost.ro": {}
},
"Google+": {
  "monitor": {
    "Google+ Hangouts/Chat": {},
    "Google+ Photos": {
      "restrict": [
        "Block File Upload",
        "Block +1/Tag"
      ]
    }
  }
},
```

Static Data

```

    "Google+ Location Tagging": {},
    "Google+ Games": {},
    "Google+ Videos": {
      "restrict": [
        "Block File Upload"
      ]
    },
    "Google+ General": {
      "restrict": [
        "Block Posting Text"
      ]
    }
  }
},
"Presentation / Conferencing": {
  "monitor": {
    "Crossloop": {},
    "Techinline": {},
    "Glide": {},
    "eRoom.net": {},
    "Twiddla": {},
    "WebEx": {},
    "TeamViewer": {}
  }
},
"Instant Messaging": {
  "monitor": {
    "MessengerFX": {},
    "Fetion": {
      "restrict": [
        "Block File Transfer"
      ]
    },
    "MSN Messenger": {
      "restrict": [
        "Block File Transfer"
      ]
    },
    "Mibbit": {},
    "Yahoo Messenger": {
      "restrict": [
        "Block File Transfer"
      ]
    },
    "KoolIM": {},
    "ILoveIM": {},
    "Google Talk": {},
    "AOL Instant Messenger": {}
  }
},
"Internet Utilities": {
  "monitor": {
    "Google Calendar": {
      "restrict": [
        "Block File Upload",
        "Block Posting Text",
        "Block Sending Email",
        "Block Download Documents"
      ]
    },
    "Google Translate": {},
    "Google Analytics": {},
    "Google App Engine": {},

```

Static Data

```

        "eBay": {},
        "Yahoo Toolbar": {}
    }
},
"Media": {
    "monitor": {
        "Photobucket": {
            "restrict": [
                "Block File Upload",
                "Block Download Documents",
                "Block Sharing"
            ]
        },
        "Fotki": {},
        "QuickTime": {},
        "Windows Media": {},
        "Nico Nico Douga": {},
        "Flickr": {
            "restrict": [
                "Block File Upload",
                "Block Posting Text"
            ]
        },
        "Live365": {},
        "Hulu": {},
        "Dailymotion": {
            "restrict": [
                "Block File Upload",
                "Block Posting Text"
            ]
        },
        "Pandora TV": {},
        "500px": {
            "restrict": [
                "Block File Upload",
                "Block Posting Text",
                "Block Like/Tag"
            ]
        },
        "YouTube": {
            "restrict": [
                "Block File Upload",
                "Block Posting Text",
                "Block High Definition"
            ]
        },
        "Jango": {},
        "Livestream": {},
        "ASF": {},
        "Vimeo": {},
        "Megavideo": {},
        "Silverlight": {},
        "PPS.tv": {
            "restrict": [
                "Block File Upload",
                "Block Posting Text"
            ]
        },
        "Gyao": {
            "restrict": [
                "Block Posting Text"
            ]
        }
    }
}

```

## Static Data

```
    },
    "Tudou": {
      "restrict": [
        "Block File Upload",
        "Block Posting Text",
        "Block Like/Tag"
      ]
    },
    "Netflix": {},
    "RealMedia": {},
    "PPTV": {
      "restrict": [
        "Block File Upload",
        "Block Posting Text"
      ]
    },
    "Picasa": {},
    "Youku": {
      "restrict": [
        "Block File Upload",
        "Block Posting Text",
        "Block Like/Tag"
      ]
    },
    "Pandora": {},
    "Joost": {},
    "56.com": {
      "restrict": [
        "Block File Upload",
        "Block Posting Text"
      ]
    },
    "Winamp Remote": {},
    "FreeeTV": {},
    "MPEG": {},
    "Flash Video": {},
    "Last.fm": {},
    "Viddler": {},
    "SmugMug": {
      "restrict": [
        "Block File Upload",
        "Block Posting Text",
        "Block Like",
        "Block Sharing"
      ]
    },
    "Deezer": {},
    "Shutterfly": {}
  },
  "default_bandwidth_limit": ""
},
"Collaboration": {
  "monitor": {
    "Pastebin": {
      "restrict": [
        "Block Posting Text",
        "Block Download Documents"
      ]
    }
  },
  "Wikipedia": {
    "restrict": [
      "Block File Upload",
      "Block Posting Text"
    ]
  }
}
```

```
    ],
    },
    "Answers.com": {
        "restrict": [
            "Block Posting Text"
        ]
    }
},
"Myspace": {
    "monitor": {
        "Myspace Music": {},
        "Myspace Videos": {
            "restrict": [
                "Block File Upload",
                "Block Like/Tag"
            ]
        },
    },
    "Myspace General": {
        "restrict": [
            "Block Posting Text",
            "Block Like/Tag"
        ]
    },
    "Myspace Photos": {
        "restrict": [
            "Block File Upload",
            "Block Like/Tag"
        ]
    }
},
"LinkedIn": {
    "monitor": {
        "LinkedIn Inbox": {
            "restrict": [
                "Block Posting Text"
            ]
        },
    },
    "LinkedIn General": {
        "restrict": [
            "Block Installation of Third-Party Applications",
            "Block Recommendations",
            "Block Groups",
            "Block Events",
            "Block Status Updates"
        ]
    },
    "LinkedIn Contacts": {
        "restrict": [
            "Block Posting Text"
        ]
    },
    "LinkedIn Profile": {
        "restrict": [
            "Block Posting Text"
        ]
    },
    "LinkedIn Jobs": {
        "restrict": [
            "Block Job Search",
            "Block Job Posting"
        ]
    }
}
```



Static Data

```

    ]
  }
}
},
"Software Updates": {
  "monitor": {
    "Windows Update": {},
    "Sophos Update": {},
    "Trendmicro Antivirus Update": {},
    "Symantec Liveupdate": {},
    "McAfee AutoUpdate": {}
  }
},
"iTunes": {
  "monitor": {
    "iTunes iPhone": {
      "restrict": [
        "Block iTunes App Install",
        "Block iTunes Music",
        "Block iTunes Video",
        "Block iTunes Podcast",
        "Block iTunes iBook"
      ]
    },
    "iTunes Desktop": {
      "restrict": [
        "Block iTunes App Install",
        "Block iTunes Music",
        "Block iTunes Video",
        "Block iTunes iBook"
      ]
    },
    "iTunes iPad": {
      "restrict": [
        "Block iTunes App Install",
        "Block iTunes Music",
        "Block iTunes Video",
        "Block iTunes Podcast",
        "Block iTunes iBook"
      ]
    },
    "iTunes iPod": {
      "restrict": [
        "Block iTunes App Install",
        "Block iTunes Music",
        "Block iTunes Video",
        "Block iTunes Podcast",
        "Block iTunes iBook"
      ]
    }
  }
},
"Enterprise Applications": {
  "monitor": {
    "SugarCRM": {},
    "SharePoint": {
      "restrict": [
        "Block File Upload",
        "Block Blog Posting",
        "Block Download Documents",
        "Block Editing Calendar",
        "Block Admin Operations"
      ]
    }
  }
}

```

## Static Data

```

    },
    "Concur": {},
    "Amazon S3": {
      "restrict": [
        "Block File Upload"
      ]
    }
  },
  "Games": {
    "monitor": {
      "Evony": {},
      "Hangame.co.jp": {},
      "Wii": {},
      "Pogo": {}
    }
  },
  "Facebook": {
    "monitor": {
      "Facebook Applications: Utilities": {},
      "Facebook Photos and Videos": {
        "restrict": [
          "Block File Upload"
        ]
      },
      "Facebook Applications: Other": {},
      "Facebook Events": {},
      "Facebook Applications: Entertainment": {},
      "Facebook Applications: Sports": {},
      "Facebook Applications: Games": {},
      "Facebook Messages and Chat": {
        "restrict": [
          "Block File Attachment Upload",
          "Block File Attachment Download",
          "Block Video Chat"
        ]
      },
      "Facebook General": {
        "restrict": [
          "Block Posting Text",
          "Block Like/Tag",
          "Block Installation of Third-Party Applications"
        ]
      },
      "Facebook Notes": {}
    },
    "default_bandwidth_limit": "2000"
  },
  "Proxies": {
    "monitor": {
      "PHPProxy": {},
      "Zelune": {},
      "Suresome": {},
      "ASProxy": {},
      "CamoProxy": {},
      "KProxy": {},
      "CoralCDN": {},
      "CGIProxy": {},
      "Guardster": {},
      "FlyProxy": {},
      "Glype": {},
      "Vtunnel": {}
    }
  }
}

```

Static Data

```

        "Surrogafier": {},
        "Socks2HTTP": {},
        "Avoidr": {},
        "Other Web Proxy": {},
        "Proxono": {},
        "Megaproxy": {}
    }
},
"Social Networking": {
    "monitor": {
        "Weibo": {
            "restrict": [
                "Block File Upload",
                "Block Posting Text"
            ]
        },
        "Kaixin001": {
            "restrict": [
                "Block File Upload",
                "Block Posting Text",
                "Block Like/Tag",
                "Block Sending Email",
                "Block Download Documents"
            ]
        },
        "Pinterest": {
            "restrict": [
                "Block File Upload",
                "Block Posting Text",
                "Block Like"
            ]
        },
        "RenRen": {
            "restrict": [
                "Block File Upload",
                "Block Posting Text",
                "Block Like/Tag"
            ]
        },
        "Slashdot": {},
        "Google Groups": {
            "restrict": [
                "Block Posting Text"
            ]
        },
        "Zhihu": {
            "restrict": [
                "Block File Upload",
                "Block Posting Text",
                "Block Like/Tag",
                "Block Sharing"
            ]
        },
        "Yahoo Mobage": {},
        "Reddit": {},
        "Tencent Weibo": {
            "restrict": [
                "Block File Upload",
                "Block Posting Text",
                "Block Like/Tag"
            ]
        },
        "Ameba": {},
    }
}

```

Static Data

```

    "Quora": {
      "restrict": [
        "Block File Upload",
        "Block Posting Text",
        "Block Like/Tag",
        "Block Sharing"
      ]
    },
    "FriendFeed": {},
    "Digg": {},
    "Two Channel": {},
    "Gree": {},
    "Mixi": {},
    "StumbleUpon": {
      "restrict": [
        "Block File Upload",
        "Block Posting Text",
        "Block Like/Tag"
      ]
    },
    "XING": {},
    "Sohu Weibo": {
      "restrict": [
        "Block File Upload",
        "Block Posting Text"
      ]
    },
    "Twitter": {
      "restrict": [
        "Block Posting to Twitter",
        "Block Posts Using Third-Party Clients",
        "Block Unsupported Third-Party Applications"
      ]
    },
    "Delicious": {},
    "Scribd": {
      "restrict": [
        "Block File Upload",
        "Block Download Documents",
        "Block Posting Text"
      ]
    },
    "Google Wave": {}
  }
},
" Blogging": {
  "monitor": {
    "Blogger": {
      "restrict": [
        "Block Posting Text"
      ]
    },
    "LiveJournal": {
      "restrict": [
        "Block Posting Text"
      ]
    },
    "Tumblr": {
      "restrict": [
        "Block Posting Text"
      ]
    }
  }
},

```

Static Data

```

    "Wordpress": {
      "restrict": [
        "Block Posting Text"
      ]
    },
    "FC2 Blog": {
      "restrict": [
        "Block File Upload",
        "Block Posting Text"
      ]
    },
    "Disqus": {
      "restrict": [
        "Block Like",
        "Block Posting Text"
      ]
    }
  }
}

```

## Youtube Categories

There are no REST APIs for allowed YTC categories. [Table 132](#) provides the static list.

Table 132 - YTC Categories Statics Data

Autos & Vehicles
Comedy
Education
Entertainment
Film & Animation
Gaming
Howto & Style
Music
News & Politics
Nonprofits & Activism

## Objects

While editing Objects column of access\_policy, you must be aware of the supported MIME types in Web Security Appliance. [Table 133](#) provides the supported MIME types:

Table 133 - MIME Types

Group/Category Type	Object Type
Executable Code	UNIX Executable Windows Executable Java Applet
Web Page Content	Images Flash
Media	Photographic Images Video Audio
P2P Metafiles	BitTorrent Links (.torrent)
Document Types	PostScript Document (PS) OpenOffice Document OASIS Open Document Format Microsoft Office XML Document Portable Document Format (PDF) FrameMaker Document (FM) Rich Text Format (RTF)

Static Data

Group/Category Type	Object Type
Archives	Stuftit BinHex LHARC ARC ARJ
Installers	UNIX/LINUX Packages
Inspectable Archives	7zip GZIP BZIP2 CPIO RAR LHA Compress Archive (Z) ZIP Archive TAR Microsoft CAB
Miscellaneous	Calendar Data

## Custom MIME Types

For blocking the custom MIME types, you must be aware of the string that is supported by Web Security Appliance. [Table 134](#) provides the objects and their MIME types which can be used as the custom MIME types.

Table 134 - Custom MIME Types

Category Type	Object	MIME Type
Archives	ARC	application/x-arc

Static Data

Category Type	Object	MIME Type
	ARJ	application/x-arj
	BinHex	application/mac-binhex40
	LHARC	application/x-lharc
	Stuffit	application/x-stuffit
	Inspectable Archives	
	7zip	application/x-7z-compressed
	BZIP2	application/x-bzip2
	Compress Archive (Z)	application/x-compress
	CPIO	application/x-cpio
	GZIP	application/x-gzip
	LHA	application/x-lha
	Microsoft CAB	application/vnd.ms-cab-compressed
	RAR	application/x-rar
	TAR	application/x-tar
	ZIP Archive	application/zip
Document Types	FrameMaker Document (FM)	application/x-mif
	Portable Document Format (PDF)	application/pdf
	PostScript Document (PS)	application/postscript
	Rich Text Format (RTF)	text/rtf
	Microsoft Office	



Static Data

Category Type	Object	MIME Type
	Microsoft Access Database (MDB)	application/x-msaccess
	Microsoft Help Document, (HLP)	application/vnd.ms-htmlhelp
	Microsoft Excel Document (XLS)	application/vnd.ms-excel
	Microsoft PowerPoint Document (PPT)	application/vnd.ms-powerpoint
	Microsoft Word Document (DOC)	application/msword
	Microsoft CDF Document (CDF)	application/ms-cdf
	Microsoft VISIO Document (VSD)	application/vnd.visio
	OASIS Open Document Format	
	OpenDocument Text (ODT)	application/vnd.oasis.opendocument.text
	OpenDocument Graphics (ODG)	application/vnd.oasis.opendocument.graphics
	OpenDocument Presentation (ODP)	application/vnd.oasis.opendocument.presentation
	OpenDocument Spreadsheet (ODS)	application/vnd.oasis.opendocument.spreadsheet
	OpenDocument Chart (ODC)	application/vnd.oasis.opendocument.chart

Static Data

Category Type	Object	MIME Type
	OpenDocument Formula (ODF)	application/vnd.oasis.opendocument.formula
	OpenDocument Database (ODD)	application/vnd.oasis.opendocument.database
	OpenDocument Image (ODI)	application/vnd.oasis.opendocument.image
	OpenOffice Document	
	OpenOffice Writer Document	application/vnd.sun.xml.writer
	OpenOffice Calc Spreadsheet	application/vnd.sun.xml.calc
	OpenOffice Draw Graphics Document	application/vnd.sun.xml.draw
	OpenOffice Impress Presentation	application/vnd.sun.xml.impress
	OpenOffice Math Formulae	application/vnd.sun.xml.math
	OpenOffice Base Database	application/vnd.sun.xml.base
	XML Document (XML)	
	XML Document	application/xml
	XML Document	image/svg+xml
Executable Code	Java Applet	application/x-java-applet
	UNIX Executable	
	UNIX Core Dump	application/x-coredump

Static Data

Category Type	Object	MIME Type
	UNIX Object	application/x-object
	UNIX Shell Script	text/x-awk
	UNIX Shell Script	text/x-gawk
	UNIX Shell Script	text/x-nawk
	UNIX Shell Script	text/x-shellscript
	UNIX Executable	application/x-executable
	UNIX Shared Library	application/x-sharedlib
	PERL Script	text/x-perl
	Windows Executable	
	DOS Executable	application/x-dosexec
	Microsoft BAT File	text/x-msdos-batch
Installers	UNIX/LINUX Packages	
	UNIX/Linux Packages	application/x-svr4-package
	UNIX/Linux Packages	application/x-debian-package
	UNIX/Linux Packages	application/x-rpm
Media	Audio	
	AAC Audio	audio/x-hx-aac-adts
	AAC Audio	audio/x-hx-aac-adif
	AAC Audio	audio/x-mp4a-latm
	AIFF Audio	audio/x-aiff
	FLAC Audio	audio/x-flac
	MIDI Audio	audio/midi
	MOD Audio	audio/x-mod

Static Data

Category Type	Object	MIME Type
	MP4 Audio	audio/mp4
	MPEG Audio	audio/mpeg
	RealMedia Audio	audio/x-pn-realaudio
	Sun/NeXT Audio	audio/x-adpcm
	Sun/NeXT Audio	audio/basic
	Sun/NeXT Audio	audio/x-dec-basic
	WAV Audio	audio/x-wav
	G.721 ADPCM	audio/x-adpcm
	OGG Audio	application/ogg
	Unknown Audio	audio/x-unknown
	Video	
	3GPP Video	video/3gpp
	3GPP2 Video	video/3gpp2
	SGI and Apple Media Video	image/jp2
	FLC Video	video/flc
	FLI Video	video/fli
	FLV Video	video/x-flv
	MPEG Video	video/h264
	MPEG Video	video/mp2p
	MPEG Video	video/mp2t
	MPEG Video	video/mp4v-es

Static Data

Category Type	Object	MIME Type
	MNG Video	video/x-mng
	MNG Video	video/x-jng
	MPEG Video	video/mpeg
	MPEG-4 Video	video/mp4
	MPEG-4 Video	video/mpeg4-generic
	QuickTime Video	video/quicktime
	QuickTime Video	image/x-quicktime
	Real Media Video	application/vnd.rn-realmedia
	SGI Video	video/x-sgi-movie
	WebM Video	video/webm
	Windows Media Video	video/x-ms-asf
	Windows Media Video	video/x-msvideo
	Unknown Video	video/x-unknown
	Photographic Image Processing Formats (TIFF/PSD)	
	Coreldraw Image	image/x-coreldraw
	TIFF Image	image/tiff
	PhotoShop Image	image/vnd.adobe.photoshop
P2P Metafiles	BitTorrent Links (.torrent)	application/x-bittorrent
Web Page Content	Flash	application/x-shockwave-flash
	Images	
	Images	image/x-ms-bmp

Static Data

Category Type	Object	MIME Type
	Images	image/gif
	Images	image/jpeg
	Images	image/png
Miscellaneous	Calendar Data	text/calendar

## Anti-Malware Categories

In access policy, while editing Anti-Malware and Reputation Settings, you must be aware of the allowed values of malware categories in the following PUT/POST format:

```
{
  "amw_reputation": {
    "cisco_dvs_amw": {
      "malware_categories": {...},
      "other_categories": {...}
    },
    "adv_malware_protection": {
      "file_reputation": {...},
      ...
    }
  },
  ...
}
```

Table 135 lists the allowed values for malware\_categories, other\_categories, and file\_reputation. These values are used either in block or monitor list.

Table 135 - Allowed Values

Objects	Categories	Condition	Allowed Values
cisco_dvs_amw	malware_categories	Sophos is enabled	Other Malware PUA Virus

Static Data

Objects	Categories	Condition	Allowed Values
		Webroot is enabled	Adware Browser Helper Object Commercial System Monitor Dialer Generic Spyware Hijacker Other Malware Phishing URL System Monitor Trojan Downloader Trojan Horse Trojan Phisher Worm
		Mcafee is enabled	Adware Generic Spyware Other Malware Trojan Horse Virus
	other_categories	Sophos is enabled	Encrypted File Unscannable
		Webroot is enabled	Unscannable

Static Data

Objects	Categories	Condition	Allowed Values
		Mcafee is enabled	Encrypted File Unscannable
adv_malware_protection	file_reputation		Known Malicious High-Risk Files