AsyncOS 16.0 API - Addendum to the Getting Started Guide for Cisco Secure Web Appliance with Hybrid SWG

March 24, 2026

Contents

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 bandwidth_limit	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	

	200 Ok	Object bandwidth_limit	Represents configured overall bandwidth limit.

Definitions

bandwidth_limit

Table 3 – Attributes for bandwidth_limit

Name	Type	Description	Required (In PUT)
bandwidth_limit	Integer	Unit of bandwidth limit is Kbps. It can have value from 0-524288 Kbps. Value '0' represents 'No limit'.	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
	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 Identification_profile_collection_schema	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 Identification_profile_schema	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 multi_status_response	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 Identification_profile_schema	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 multi_status_response	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 multi_status_response	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 Identification_profile_schema	Every element in this list represents a single identification profile.	Yes	Yes

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 Identification_method_schema	A dictionary which represents authentication and identification methods.	No	No
members	Objects members_schema	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: • Sso_none (for Authentication User), • sso_ise (for Transparently identify users with ISE), • sso_asa (for Transparently identify users with ASA), • sso_tui (for Transparently identify users with authentication Realm)	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.
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 'authenticate', 'guest', 'block' (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_Ise with auth and sso_none.	Only if sso_tui, sso_Ise with auth and sso_none.

Identification Profiles

Name	Type	Description	Required	
			POST	PUT
auth_surrogate_by_proto	Auth surrogate by protocols	Protocol wise authentication surrogates.	No. Default value will be selected as 'ip', for all selected protocols in member.	No. Default value will be selected as 'ip', 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 user_agents	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

Name	Type	Description	Required	
			POST (At least one member should be	PUT (Whatever user wants to modify, is a required
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 Secure Web Appliance.	No	No
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 Secure Web 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 response_status	Success list, with profile name and messages.
failure_list	Array of objects response_status	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
	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	Array of objects Attributes for	List of access policies and their configuration payload.	Mandatory

Access Policies

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	**o**bjects multi_status_response	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	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.	
	207 Multi status	objects multi_status_response	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	**o**bjects multi_status_response	Dictionary of success and Failure list. Failure list contains proper error message, specifying reason of failure.	

Definitions

access_policies_schema

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

Access Policies

Name	Type	Format	Description	Remarks	Required	
					POST	PUT
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
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 membership_schema		Defined in membership_schema	Not applicable for global_policy	mandatory	optional
protocols_user_agents	Objects protocols_user_agents schema		Defined in protocols_user_agents schema		optional	optional
url_filtering	Objects url_filtering schema		Defined in url_filtering schema		optional	optional

Name	Type	Format	Description	Remarks	Required	
					POST	PUT
avc	Objects avc_schema		Defined in avc_schema		optional	optional
adc	Objects adc_schema		Defined in adc_schema		optional	optional
objects	Objects Objects schema		Defined in Objects schema		optional	optional
amw_reputation	Objects amw_reputation_schema		Defined in amw_reputation_schema		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 Id_profile_schema	mandatory	optional

Access Policies

Name	Type	Format	Description	Required	
				POST	PUT
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
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 membership_schema		Defined in members_schema . None of the associated ID profile has defined url_categories.	optional	optional
user_agents	Objects user_agents		Defined in user_agents schema. None of the associated ID profile has defined user agents.	optional	optional
time_range	Objects Id_profile_schema		Defined in Id_profile_schema	optional	optional

Name	Type	Format	Description	Required	
				POST	PUT
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 “global identification profile”, “_all_” represents “All identification profiles. In GET’s response the global identification profile is not shown as empty string, it is shown as “global_identification_profile” 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"]	“All Authenticated Users”: represents all the authenticated users. The selected ID profile must have auth enabled “Selected groups and users”: selected ID profile must have support. In addition, you must provide groups_and_users_schema “Guests”: If ID profile supports guest then this option can be chosen. In case of “all identification profiles” at least one of the ID profiles must support guest. “No Authentication”: If no authentication is required. In case if selected ID profile is “global profile” and doesn’t have auth associated, then no authentication is implicit but still for the sake of schema validation the value “No Authentication” is mandatory.	No	No
groups_and_users	Objects groups_and_users_schema		Defined in groups_and_users_schema . This is mandatory if “auth” is chosen as “Selected groups and users”.	Conditional	Conditional

Name	Type	Format	Description	Required	
				POST	PUT
auth_realm	String	Name of the specific realm or 'all realm' as applicable.	If the ID profile has auth realm as 'All Realms', then it is mandatory to provide either 'All Realms' or the specific realm 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
auth_group	List of Objects auth_group_schema		Defined in auth_group_schema	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 adv_malware_protection_schema		Advanced malware protection settings. Defined in adv_malware_protection_schema	No	No
cisco_dvs_amw	Objects cisco_dvs_amw_schema		Cisco DVS antimalware settings. Defined in cisco_dvs_amw_schema .	No	No
web_reputation	Objects web_reputation_schema		Web reputation setting. Defined in web_reputation_schema 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 "enable", "disable"	Status of the file reputation filtering.	Yes	Yes
file_reputation	Objects file_reputation_schema		List of block file reputation categories. Default status is always "monitor" 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 amw_scanning_schema		Defined in amw_scanning_schema	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 “enable”, “disable”	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 amw_scanners_schema		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 “enable”, “disable”	Enable/Disable Sophos (only if adaptive scanning is disabled). Only one among Sophos or McAfee can be enabled.	Yes	Yes
sophos	String	One among “enable”, “disable”	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 “enable”, “disable”	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 web_reputation_score_schema	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 Secure Web Appliance.	No	No
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 protocols_user_agents schema payload is provided and state is not provided, state of protocols_user_agents schema is set to custom by default.	optional	optional
block_protocols	Array of strings		Protocols to be blocked.	optional	optional

Name	Type	Format	Description	Required	
				POST	PUT
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
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 protocols_user_agents 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 custom_cats schema .	optional	optional
predefined_cats	object		Defined in predefined_cats schema.	optional	optional
yt_cats	object		Defined in yt_cats schema .	optional	optional
overall_quota_profile	string		Set a quota that applies to all web surfing activities.	optional	optional

Access Policies

Name	Type	Format	Description	Required	
				POST	PUT
exception_referred_embedded_content	object		Exceptions to Blocking for Embedded/Referred Content. Defined in exception_referred_embedded_content_schema	optional	optional
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 safe_search schema		Defined in safe_search schema .	optional	optional
content_rating	Objects content_rating schema		Defined in content_rating schema .	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

Name	Type	Description	Required	
			POST	PUT
monitor	Array of strings	List of custom categories to monitor.	optional	optional
warn	Array of strings	List of custom categories to warn.	optional	optional
quota_based	Objects quota_based	Custom categories to configure for time and volume quotas. Defined in quota_based.	optional	optional
time_based	Objects time_based_schema	Custom categories to configure for time range. Defined in time_based_schema	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 quota_profile.	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

Time Range

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/conditional	Optional/conditional	Available only for custom categories
action_redirect	string	Redirect to if in time range.	Optional/conditional	Optional/conditional	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
warn	Array of strings	List of predefined categories to warn.	optional	optional

Name	Type	Description	Required	
			POST	PUT
quota_based	object	predefined categories to configure for time and volume quotas. Defined in quota_based schema.	optional	optional
time_based	Objects time_based_schema	Predefined categories to configure for time range. Defined in time_based_schema .	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 time_based_schema	youtube categories to configure for time range. Defined in time_based_schema .	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 content_referred_by_cats_schema	Sets Exception for Content Referred by The Categories. Defined in content_referred_by_cats_schema.	optional	optional
referred_content	Objects referred_content schema	Set Exception for referred_content 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. Bu 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

Access Policies

Name	Type	Format	Description	Required	
				POST	PUT
max_object_size_mb	Objects max_object_size_mb_schema		Object blocking settings by size in mb. Defined in max_object_size_mb_schema	optional	optional
object_type	Objects object_type_schema		Action for object and mime types. Defined in object_type_schema .	optional	optional
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	

Access Policies

Name	Type	Format	Description	Required		
				POST	PUT	condition
applications	object		Defined in adc_schemaTable 55 - Attributes for ADC schema Table 55 - Attributes for ADC schema Name state applications Applications schema	optional	optional	
range_request	Objects range_request_schema		Defined in range_request_schema	Conditional /optional	Conditional/optional	Available only if Range Request Forwarding is enabled.

adc_schemaTable 55 - Attributes for ADC schema

Table 55 - Attributes for ADC schema

Name	Type	Format	Description	Required		
				POST	PUT	condition

state	string	Custom/use_global	state of adc	optional	optional	
applications	object		defined in applications schema	optional	optional	

Applications schema

Table 56 – Attributes for Applications schema

Name	Type	Description	Required	
			POST	PUT
<application type>	object	Type of the application. See applications info. Defined in Application type schema .	optional	optional

Application type schema

Table 57 – 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 monitor_schema		Defined in monitor_schema for applications.	optional	optional

Table 58 – 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 59 – 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 60 – 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

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/conditional	Optional/conditional	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 pac_basic_setting		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			
Parameters	None			
Request body	Name	Type	Description	Required

	pac_basic_setting	Object pac_basic_setting	Defined in pac_basic_setting 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
	204 No Content	Empty body	The request has been processed successfully and all the given PAC file settings are applied.

	207 Multi status	**o**bjects multi_status_response	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	**o**bjects multi_status_response	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
	204 No Content	Empty body	All the files are deleted successfully
	207 Multi status	**o**bjects multi_status_response	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

PAC File Host Settings

Method	GET		
Parameters	None		
Request body	**None**		
Response	Code	Type	Description
	200 Ok	Object pac_basic_setting	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
	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 multi_status_response	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 multi_status_response	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 multi_status_response	Dictionary of success and Failure list. Failure list contains proper error message, specifying reason of failure.

Definitions – Payload Configurations

pac_basic_setting

Table 61 - 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	
pac_server_ports	Array of integer	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 62 - 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 63 - 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, “example.cisco.com”.	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 64- 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

	domain_name	String	Valid domain name string.	Domain name. For example, “example.cisco.com”	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 65- 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 “delete_all” if all the domain maps must be deleted.	Yes
Request body	None			
Response	Code	Type	Description	
	200 Ok			

Upstream Proxy

Retrieving the Upstream Proxy Details

Table 66 – Attributes for Retrieving the Upstream Proxy Details

API	/wsa/api/v2.0/configure/ network/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 67 - 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
	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 68 – 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 69 – 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. “delete_all” to delete all the proxy groups.	Yes
Request body	None			
Response	Code	Type	Description	

	200 Ok		

Modifying the Upstream Proxy Servers

Table 70 - 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, “test1”.	Yes
	proxy_servers	Array of dict.	{ “host”: <hostname>, “retries”: <no of retries>, “port”:<port num>}	Adds the proxy server to the existing server list for the specified proxy group.	Yes

Adding an Upstream Proxy Server

Table 71 - 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 72 - 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
	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 73 - 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 74 – 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
	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 75 - 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 76 – 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 77 – Attributes for PUT HTTP Proxy–OCSP Settings

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

	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 78 – 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, “accesslogs”	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 79 – Attribute of PUT Log Subscriptions

API	/wsa/api/v2.0/configure/system/log_subscriptions
Method	PUT
Parameters	None

Log Subscriptions

Request body	Name	Type	Format	Description	Required
	new_log_name	String	Valid log name	For example, “log_name_1”	No
	log_name	String	Previous log name to be modified.	For example, “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	{
			"max_num_files": <num>,
			"method": <method>}
				Expected a dictionary with all the retrieval method parameters and their values. Below are the settings for each retrieval method
				"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",
				"scp_host": "ciscoscp.com",
				"scp_key_method": "auto"
				}
				"retrieval_method": {
					No

				<pre>"method": "syslog_push", "syslog_facility": "user", "syslog_protocol": "UDP", "syslog_msg_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	
	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.
	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 80 – 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

	retrieval_method	Object	{
			“max_num_files”: <num>,
			“method”: <method>}
				Expected a dictionary with all the retrieval method parameters and their values. Below are the settings for each retrieval method
				"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",
				"scp_host": "ciscoscp.com",
				"scp_key_method": "auto"
				}
				"retrieval_method": {
					No

				<pre>"method": "syslog_push", "syslog_facility": "user", "syslog_protocol": "UDP", "syslog_msg_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	
	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.
	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.

	rollover_by_time	Object	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_custom_tim
				For example, {
				"rollover_interval": "daily"
				"rollover_daily_time": 1303
				}
					No

			e": 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"

	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"

	rollover_by_time	Object	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":
				For example, {
				"rollover_interval": "daily"
				"rollover_daily_time": 1303
				}
					No

			"custom", "rollover_custom_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	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"

	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 81 – Attributes for DELETE Log Subscriptions

API	wsa/api/v2.0/configure/system/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 82 - 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 83 - 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 84 – 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 85 – 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".
	download_as_file	Boolean	True/False	Specify whether the response must be a downloadable file or a General response. The value is “True” for Downloadable format.	Yes

Header Based Authentication

Retrieving Header Based Authentication

Table 86 - 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 xauth_header_setting	It contains a dictionary with all the configuration parameters of header-based authentication.

Enabling or Disabling Header Based Authentication

Table 87 – Attributes for Enabling or Disabling Header Based Authentication

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 is used to enable/disable header-based authentication. Values are: • Enable • 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 88 – 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
	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 89 - 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 90 - 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 '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_std_group

Table 91 - 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 '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_user

Table 92 - 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 93 - 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
text_format	String	Represents the character encoding type for the header value. Possible values are 'UTF-8' or 'ASCII'.	No	Yes

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

response_status

Table 94 - Attributes for response_status

Name	Type	Description
status	Integer	Response Code

error_response

Table 95 - Attributes for error_response

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

End-User Notification

Retrieving End-User Notification

Table 96 - Attributes for retrieving the End-User Notification

API	/wsa/api/v3.0/security_services/eun_config
Method	GET

End-User Notification

Parameters	None		
Request body	None		
Response	Code	Type	Description
	200 Ok	Objects eun_config_schema	Displays the configuration of the End-User Notification page.

Modifying the End-User Notification

Table 97 – Attributes for modifying the End-User Notification

API	/wsa/api/v3.0/security_services/eun_config			
Method	PUT			
Parameters	None			
Request body	Name	Type	Description	Required
	eun_config_schema	Objects for eun_config_schema	Payload for End-User Notification configuration.	Mandatory
Response	Code	Type	Description	
	204 No Content	Empty body	The request has been processed successfully and the end-user notification configuration has been updated with the given payload.	

Definitions

eun_config_schema

Table 98 – Attributes for eun_config_schema

Name	Type	Format	Description	Remarks	Required	
					POST	PUT
http_https	Object http_https_schema				N/A	Mandatory

http_https_schema

Table 99 – Attributes for http_https_schema

Name	Type	Format	Description	Remarks	Required	
					POST	PUT
general_settings	Object general_settings_schema		Defined in http_https_schema		N/A	Optional
end_user_notification_pages	Object end_user_notification_pages_schema		Defined in http_https_schema		N/A	Optional
end_user_url_filtering_warning_page	Object end_user_url_filtering_warning_page_schema		Defined in http_https_schema		N/A	Optional

general_settings_schema

Table 100 – Attributes for general_settings_schema

Name	Type	Format	Description	Remarks	Required	
					POST	PUT
logo_image	String		The logo image can be any of the following: None, Cisco, or Custom. Every notification and acknowledgement page may optionally display an image.		N/A	Optional
logo_url	String	HTTP/HTTPS URLs must contain a well-formed hostname or IP address. Optionally, a port may be included, but a query string (?) is not permitted.	The URL for Custom logo image.	If the logo image is selected as Custom, the logo_url is a mandatory field.		Optional (When the logo image is None or Cisco) Mandatory (When logo_image is Custom)

end_user_notification_pages_schema

Table 101 – Attributes for end_user_notification_pages_schema

Name	Type	Format	Description	Remarks	Required	
					POST	PUT
notification_type	String		The notification type can either be "Use In-Box End User Notification" or "Redirect to Custom URL".		N/A	Optional
notification_page_url	String	HTTP/HTTPS URLs must contain a well-formed hostname or IP address. Optionally, a port may be included, but a query string (?) is not permitted.	All blocked requests will be redirected to this URL.	If notification_type is "Redirect to Custom URL", this URL is mandatory.	N/A	Optional (When the notification_type is set to "Use On-Box End User Notification") Mandatory (When the notification_type is set to "Redirect to Custom URL")
custom_message	String	Valid HTML using only HTML tags and HTML symbols. The allowed HTML tags are <a>, , <b>, <big>, <code>, , <i>, <small>, , and . Minimum Length:0 Maximum Length:65536	Every notification page includes additional text, such as a link to your company's policies			

End-User Notification

Name	Type	Format	Description	Remarks	Required	
					POST	PUT
contact	String	The contact information must be a string and cannot be blank.	Retrieves the Contact information.		N/A	Mandatory
email_address	String	If the address is not an email address, it should be left blank.			N/A	Optional
end_user_feedback	Bool		False		N/A	Optional

end_user_url_filtering_warning_page_schema

Table 102 – Attributes for end_user_url_filtering_warning_page_schema

Name	Type	Format	Description	Remarks	Required	
					POST	PUT
time_between_warning	Integer		The value is displayed in seconds.	Currently the time is set to one hour.	N/A	Optional
custom_message	String	Valid HTML using only HTML tags and HTML symbols. The allowed HTML tags are <a>, , <b>, <big>, <code>, , <i>, <small>, , and . Minimum Length:0 Maximum Length:65536			N/A	Optional

HTTP ReWrite Profiles

Retrieving the HTTP ReWrite Profiles

Table 103 - 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 http_rewrite_profile_collection_schema	It contains a list of http rewrite profiles, their configurations, and global settings.

Modifying the HTTP ReWrite Profiles

Table 104 - 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	Array of objects http_rewrite_profile_collection_schema	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 global_settings_schema	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 multi_status_response	Dictionary of success and failure list. Failure list contains the appropriate error message, specifying reason for failure.	

Adding the HTTP ReWrite Profiles

Table 105 - 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	Array of objects http_rewrite_profile_collection_schema	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 global_settings_schema	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 multi_status_response	Dictionary of success and failure list. Failure list contains the appropriate error message, specifying reason for failure.	

Deleting the HTTP ReWrite Profiles

Table 106 - 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 multi_status_response	Dictionary of success and failure list. Failure list contains the appropriate error message, specifying reason for failure.
	406 Not Acceptable	Objects error_response	Error message saying that profile_name and alternate_profile_name cannot be same.

Definitions

http_rewrite_profile_collection_schema

Table 107 - Attributes for http_rewrite_profile_collection_schema

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

http_rewrite_profile_schema

Table 108 - 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 header_schema	List of headers to be added, modified, or deleted in outbound traffic.	Yes	No

header_schema

Table 109 - 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

HTTP ReWrite Profiles

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'.	Yes	Yes
binary_encoding	String	Represents the binary encoding type for the header value. Possible values are 'Base64' or 'No Encoding'.	Yes	Yes

global_settings_schema

Table 110 - 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_groups	String	Represents the rewrite format for X-Authenticated-Groups. It should be a combination of $authMechanism, $domainName and $groupName in the same	Yes	Yes

Name	Type	Description	Required	
			POST	PUT
		sequence. Possible separators are '\\' or '/ '.		
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 111 - Attributes for multi_status_response

Name	Type	Description
success_list	Array of objects response_status	Success list, with profile name and messages.
failure_list	Array of objects response_status	Failure list, with profile name and messages.
success_count	Integer	Success Count
failure_count	Integer	Failure Count

response_status

Table 112 - Attributes for response_status

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

Smart Software Licenses

Name	Type	Description
profile_name	String	Profile name

error_response

Table 113- Attributes for error_response

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

Smart Software Licenses

Retrieving the Smart Software Licenses

Table 114 - Attributes for Retrieving the Smart Software Licenses

API	wsa/api/v3.0/system_admin/sl_licenses		
Method	GET		
Parameters	None		
Request body		None	
Response	Code	Type	Description
	200 Ok	array	List of license details with license_name and auth_status. grace_period is returned if the auth_status of any of the licenses is 'Out Of Compliance'.

Modifying the Smart Software Licenses

Table 115 - Attributes for Modifying the Smart Software Licenses

API	wsa/api/v3.0/system_admin/sl_licenses			
Method	PUT			
Parameters	None			
Request body	Name	Type	Format	Required
		object	request_release_schema	Mandatory
Response	Code	Type	Description	
	202 Accepted	object	The request or release for the licenses is in progress.	
	400 Bad request syntax or unsupported method	object	The request or release for the licenses failed.	

Retrieving the Smart License Agent Status

Table 116- Attributes for Retrieving the Smart License Agent

API	wsa/api/v3.0/system_admin/smart_agent_status			
Method	GET			
Response	Code	Type		Description
	200 Ok	object		Details of Cisco Smart Software License configuration such as enable or disable status, registration status and so on.

Modifying the Smart License Agent Status

Table 117 - Attributes for Modifying the Smart License Agent

API	wsa/api/v3.0/system_admin/smart_agent_status			
Method	PUT			
Parameters	None			
Request body	Name	Type	Description	Format
	Not Required			

Smart Software Licenses

Response	Code	Type	Description
	202 Accepted	Empty body	The request has been processed successfully and the smart license agent update is in progress.

Retrieving the Software Licenses

Table 118- Attributes for Retrieving the Software Licenses

API	wsa/api/v3.0/system_admin/smart_software_licensing_status		
Method	GET		
Parameters	None		
Request body	None		
Response	Code	Type	Description
	200 Ok	array	Details of Cisco Smart Software License configuration such as enable or disable status, registration status and so on.

Modifying the Software Licenses

Table 119 - Attributes for Modifying the Software Licenses

API	wsa/api/v3.0/system_admin/smart_software_licensing_status			
Method	PUT			
Parameters	None			
Request body	Name	Type	Description	Format
	smart_license_status	String	Enables smart license	Only “enable”

	registration_token	String	Registers the instance on CSSM with valid token.	
	action	String	Selected action allows different configurations.	one form “register”, “re-register”, “de-register”, “renew-auth” and “renew-cert”
	test_interface	String	Selected test_interface updates the test interface to register with smart license	“Data” or “Management”
	transport_mode	String		“direct” or “transport_gateway”
	transport_url	String		
Response	Code	Type	Description	
	204 Ok	Empty body	The request has been processed successfully and the smart license configuration has been updated.	

Required Fields:

Name	PUT
smart_license_status	Mandatory for enabling license only
registration_token	Mandatory for registration/reregistration only
action	Mandatory for various updates
test_interface	Mandatory to update test_interface, can be send only with action:”register”
transport_mode	Mandatory to update transport mode
transport_url	Required only with transport_mode: “transport_gateway”

Definitions – Payload Configurations

request_release_schema

Name	Type	Format	Description	Remarks	Required	
					POST	PUT
request	Array	Items: string. must be non-repetitive and be one of valid_license_names			nil	optional
release	Array	Items: string. must be non-repetitive and be one of valid_license_names			nil	optional

```
valid_license_names = ['Secure Web Appliance Web Reputation Filters', 'Secure Web Appliance Malware Analytics Reputation', 'Secure Web Appliance Anti-Virus McAfee', 'Secure Web Appliance Web Proxy and DVS Engine', 'Secure Web Appliance Cisco Web Usage Controls', 'Secure Web Appliance Anti-Virus Webroot', 'Secure Web Appliance L4 Traffic Monitor', 'Secure Web Appliance Cisco AnyConnect SM for AnyConnect', 'Secure Web Appliance Anti-Virus Sophos', 'Secure Web Appliance Malware Analytics', 'Secure Web Appliance HTTPs Decryption']
```

System Setup Wizard Settings

Retrieving the End User License Agreement Details

Table 120 - Attributes for Retrieving the End User License Agreement Details

API	wsa/api/v3.0/system_admin/cisco_end_user_license_agreement			
Method	GET			
Response	Code	Type		Description
	200 Ok	object		Details of End User License Agreement. (The get response can be downloaded as a file on local system).

Modifying the System Setup Wizard Settings

Note: You must go through the EULA agreement before performing the PUT request to setup the system setup wizard.

Table 121 – Attributes for System Setup Wizard Settings

API	wsa/api/v3.0/system_admin/system_setup_wizard				
Method	PUT				
Parameters	None				
Request body	Name	Type	Format	Description	Required
		object	ssw_settings_schema	Object with SSW settings.	Mandatory
Response	Code	Type		Description	
	204 No-content	Empty body		The request has been processed successfully.	
	400 Bad Request	object		Description of the error.	

Definitions – Payload Configurations

ssw_settings_schema

Table 122 – Attributes for ssw_settings_schema

Name	Type	Format	Remarks	Required
				PUT
cisco_license_agreement	String	Enum - Must be one of “accept” or “decline”	Mandatory when using smart license.	Conditional
appliance_mode	String	Enum - Must be one of “standard”, “scansafe” or “hybrid”.	Only “standard” mode is supported by REST API. Default: “standard”	optional
system_settings	object	system_settings_schema		optional
network_context	object	network_context_schema		optional
network_interface	object	network_interface_schema		optional

System Setup Wizard Settings

Name	Type	Format	Remarks	Required
				PUT
network_l4tm	object	network_l4tm_schema		optional
network_routes	object	network_routes_schema	Required if interfaces other than m1 (with IPv4) have been configured.	Conditional
transparent_connection	object	transparent_connection_schema		optional
network_admin	object	network_admin_schema		Required
network_security	object	See ftp_settings_schema		optional

system_settings_schema

Table 123- Attributes for system_settings_schema

Name	Type	Format	Remarks	Required
				PUT
hostname	String	Valid hostname	Default: hostname of the secure web appliance.	optional
dns_servers	object	dns_servers_schema		optional
ntp_server	object	ntp_server_schema		optional
timezone	object	timezone_schema		optional

dns_servers_schema

Table 124 - Attributes for dns_servers_schema

Name	Type	Format	Remarks	Required
				PUT
dns_choice	String	Enum. Must be one of “self” or “root”.	Default: current dns_choice of appliance	optional
user_dns	Array	List of valid IP addresses.	Maximum number of items in list is 3.	optional

ntp_server_schema

Table 125 - Attributes for ntp_server_schema

Name	Type	Format	Remarks	Required
				PUT
query_interval_time	integer	Duration in seconds. The value should be between 8 and 129600.	Default: current interval time if configured else 86400.	optional
sync_up_delay_ms	integer	Duration in milliseconds. The value should be between 1 and 3600000.	Default: current sync up delay time if configured else 500.	optional
server_name	String	Valid hostname, IPv4 or IPv6 address.	Default: current server name if configured else 'time.sco.cisco.com'.	optional
server_auth	object	server_auth_schema		optional

server_auth_schema

Table 126 - Attributes for server_auth_schema

Name	Type	Format	Remarks	Required
				PUT
status	String	Enum. The value mst be one of “enable” or “disable”.	Default: current server auth status else ‘disable’.	optional
key_id	String	Integer between 1 and 65535.	Required if server_auth is set to “enable” (by default or by user).	Conditional

System Setup Wizard Settings

Name	Type	Format	Remarks	Required
				PUT
key_val	Base64 encoded string	Key_val must be encoded using base-64 encoding before passing. If key_type is “sha1”, key_val must be 39 characters or less and contain no spaces. If key_type is “md5”, key_val must be 31 characters or less and contain no spaces.	Required if server_auth is set to “enable” (by default or by user)	Conditional
key_type	String	Enum. The value must be one of “md5” or “sha1”.	Default: “md5”	Optional

timezone_schema

Table 127 - Attributes for timezone_schema

Name	Type	Format	Remarks	Required
				PUT
region	String	Must be a valid region from timezone_dict.	Default: “GMT Offset”	Optional
country	String	Must be a valid country from timezone_dict.	Default: Alphabetically first country under the specified region in the timezone_dict.	Optional
timezone_or_gmt_offset	String	Must be a valid timezone from timezone_dict.	Default: Alphabetically first time zone under the specified country in the timezone_dict.	Optional

network_context_schema

Table 128 - Attributes for network_context_schema

Name	Type	Format	Remarks	Required
				PUT
other_proxy	String	Enum. The value must be one of “yes” or “no”.	Default: “no”	optional
group_name	String	Max length is 32 characters.	Required if other_proxy is set to “yes”.	Conditional
host	String	Valid hostname, IPv4 or IPv6. This IP address should not already be in use.	Required if other_proxy is set to “yes”.	Conditional
port	String	Integer between 1 and 65535. Valid portname which is not already in use.	Default: 3128	Optional

network_interface_schema

Table 129 - Attributes for network_interface_schema

Name	Type	Format	Remarks	Required
				PUT
m1	object	m1_schema		optional
p1	object	p1_schema		optional

m1_schema

Table 130 - Attributes for m1_schema

Name	Type	Format	Remarks	Required
				PUT
management_only	String	Enum – must be one of “yes” or “no”	Default: “no”	optional
ipv4_address_netmask	String	Valid IPv4 CIDR	Default: Current IPv4 CIDR for management.	optional
hostname	String	Valid hostname	Default: Current hostname	optional

System Setup Wizard Settings

Name	Type	Format	Remarks	Required
				PUT
ipv6_address_netmask	String	Valid IPv6 CIDR. If empty string is passed, it clears any default ipv6 configuration.	Default: Current IPv6 CIDR for management if configured else empty string	Optional

p1_schema

Table 131 - Attributes for p1_schema

Name	Type	Format	Remarks	Required
				PUT
ipv4_address_netmask	String	Valid IPv4 CIDR. If empty string is passed, it clears any default ipv4 configuration.	Default: Current IPv4 CIDR for data.	optional
hostname	String	Valid hostname. If empty string is passed, it clears any default hostname.	Default: Current hostname.	optional
ipv6_address_netmask	String	Valid IPv6 CIDR. If empty string is passed, it clears any default ipv6 configuration.	Default: Current IPv6 CIDR for data if configured else empty string.	Optional

network_l4tm_schema

Table 132 - Attributes for network_l4tm_schema

Name	Type	Format	Remarks	Required
				PUT
wiring_type	String	Enum – must be one of “simplex” or “duplex”	Default: “simplex”	Optional

network_routes_schema

Table 133 - Attributes for network_routes_schema

Name	Type	Format	Remarks	Required
				PUT
management	object	routes_schema	Required if ipv4_address_netmask under m1 is specified and default_gateway is not present by default.	Conditional
data	object	routes_schema	Required if ipv4_address_netmask under p1 is specified and default_gateway is not present by default.	Conditional
management_v6	object	routes_schema	Required if ipv6_address_netmask under m1 is specified and default_gateway is not present by default.	Conditional
data_v6	object	routes_schema	Required if ipv6_address_netmask under p1 is specified and default_gateway is not present by default.	Conditional

routes_schema

Table 134 - Attributes for routes_schema

Name	Type	Format	Remarks	Required
				PUT
default_gateway	String	Valid IP address with appropriate version. The IP address cannot be empty and cannot be a loopback, link-local or multicast address and must be directly reachable in the network set being configured.	Default: Current default_gateway if configured. If not configured, this field is required.	Conditional
static_routes_table	Array	Items: static_route_schema	Default: empty	optional

static_route_schema

Table 135 - Attributes for static_route_schema

Name	Type	Format	Remarks	Required
				PUT
internal_network	String	Valid IP address or a CIDR network. The destination cannot already be defined by another route.		Required
name	String	Non-blank string		Required
internal_gateway	String	Valid IP address	IP of the gateway must be reachable in the interface set specified.	Required

transparent_connection_schema

Table 136 - Attributes for transparent_connection_schema

Name	Type	Format	Remarks	Required
				PUT
redirection_device	String	Enum: must be one of "l4switch", "no_device" and "wccp_v2_router".	Default: "l4switch"	Optional
wccp_v2_router	object	wccp_v2_router_schema		Optional

wccp_v2_router_schema

Table 137 - Attributes for wccp_v2_router_schema

Name	Type	Format	Remarks	Required
				PUT
standard_service_id	object	standard_service_id_schema		Required

standard_service_id_schema

Table 138 - Attributes for standard_service_id_schema

Name	Type	Format	Remarks	Required
				PUT
status	String	Enum: must be either “enable” or ”disable”	Default: Current status if configured else “disable”	Optional
router_addresses	Array	Items must be valid IP addresses.	Required when above “status” is set to “enable”	Conditional
router_security_status	String	Enum: must be either “enable” or ”disable”.	Default: “disable”	Optional
passphrase	Base64 encoded string	The passphrase must be encoded using base-64 encoding before passing. The passphrase must be 7 or fewer characters	Required when router_security_status is “enable”	Conditional

network_admin_schema

Table 139 - Attributes for network_admin_schema

Name	Type	Format	Remarks	Required
				PUT
passphrase	Base64 encoded string	The passphrase **must be encoded using base-64 encoding** before passing. It may not start or end with a space or be a blank string. It must contain at least 8 characters, one upper (A-Z) and one lower (a-z) case letter, at least one number (0-9), at least one special character and not a commonly used.		Required

System Setup Wizard Settings

Name	Type	Format	Remarks	Required **PUT**
mail_to_addrs	Array	Each item in the array must be a valid email address. An email address is a localname followed by the '@' symbol followed by a domain name. A regular localname can contain the following characters: any number or letter and any of the following characters: !#$%&'*+/=?^_`{|}~-. A quoted localname is enclosed in double quotes. Inside the double quotes you may have almost any printable character. You can escape the following special characters with a backslash: tab, space, double quote, backslash. The maximum total length of a user name or other local-part is 64 characters. The maximum total length of a domain name or number is 255 characters.		Required
smtp_relay_host	String	Must be 255 characters or less and must be a valid hostname or an IP address		Optional
smtp_relay_port	Integer	Must be a number from 1 to 65535	Default: 25	Optional
autosupport	String	Enum: must be either “enable” or ”disable”	Default: “enable”	Optional
network_participation	object	network_participation_schema		Optional

network_participation_schema

Table 140 - Attributes for network_participation_schema

Name	Type	Format	Remarks	Required
				PUT
status	String	Enum: must be one of “enable” and “disable”	Default: “enable”	Optional
participation_level	String	Enum: must be one of “standard” and “limited”	Default: “standard”	Optional

network_security_schema

Table 141 - Attributes for network_security_schema

Name	Type	Format	Remarks	Required
				PUT
global_policy_default_action	String	Enum: must be either “monitor” or ”block”	Default: “monitor”	optional
monitor_action	String	Enum: must be either “monitor” or ”block”	Default: “monitor”	optional
acceptable_use_controls	String	Enum: must be either “enable” or ”disable”	Default: “enable” if there are available URL engines else “disable”	optional
url_engine	String	Must be one of available URL engines	Default: “firestone” or “webcat” whichever is available	optional
reputation_filtering	String	Enum: must be either “enable” or ”disable”	Default: “enable”	optional
malware_analytics	String	Enum: must be either “enable” or ”disable”	Default: “enable”	Optional
malware_spyware_scanning	object	malware_spyware_scanning_schema		optional

System Setup Wizard Settings

Name	Type	Format	Remarks	Required
				PUT
cisco_data_security_filtering	String	Enum: must be either “enable” or ”disable”	Default: “enable”	optional

malware_spyware_scanning_schema

Table 142 – Attributes for malware_spyware_scanning_schema

Name	Type	Format	Remarks	Required
				PUT
sophos	String	Enum: must be either “enable”/”disable”	Default value is “enable”	Optional
webroot	String	Enum: must be either “enable”/”disable”	Default value is “enable”	Optional
mcafee	String	Enum: must be either “enable”/”disable”	Default value is “enable”	Optional
detected_malware_action	String	Enum: must be either “monitor” or ”block”	Default: “monitor”	Optional

Sample Code

```
timezone_dict:

{
    "Europe": {
        "Turkey": [
            "Istanbul"
        ],
        "Moldova (Republic of)": [
            "Chisinau"
        ],
        "Italy": [
            "Rome"
        ],
        "Czech Republic": [
            "Prague"
        ],
        "San Marino": [
            "San_Marino"
        ],
        "Luxembourg": [
            "Luxembourg"
```

```
        ],
        "France": [
            "Paris"
        ],
        "Andorra": [
            "Andorra"
        ],
        "Slovakia": [
            "Bratislava"
        ],
        "Gibraltar": [
            "Gibraltar"
        ],
        "Ireland": [
            "Dublin"
        ],
        "United Kingdom of Great Britain and Northern Ireland": [
            "London"
        ],
        "Norway": [
            "Oslo"
        ],
        "Lithuania": [
            "Vilnius"
        ],
        "Holy See": [
            "Vatican"
        ],
        "Belarus": [
            "Minsk"
        ],
        "Montenegro": [
            "Podgorica"
        ],
        "Slovenia": [
            "Ljubljana"
        ],
        "Germany": [
            "Berlin",
            "Busingen"
        ],
        "Bosnia and Herzegovina": [
            "Sarajevo"
        ],
        "Belgium": [
            "Brussels"
        ],
        "Spain": [
            "Madrid"
        ],
        "Ukraine": [
            "Uzhgorod",
            "Kiev",
            "Simferopol",
            "Zaporozhye"
        ],
        "Netherlands": [
            "Amsterdam"
        ],
        "Estonia": [
            "Tallinn"
        ],
        "Macedonia (the former Yugoslav Republic of)": [
            "Skopje"
        ],
```

```
        "Denmark": [
            "Copenhagen"
        ],
        "Poland": [
            "Warsaw"
        ],
        "Finland": [
            "Helsinki"
        ],
        "Russian Federation": [
            "Kirov",
            "Ulyanovsk",
            "Moscow",
            "Samara",
            "Volgograd",
            "Kaliningrad",
            "Saratov",
            "Astrakhan"
        ],
        "Sweden": [
            "Stockholm"
        ],
        "Latvia": [
            "Riga"
        ],
        "Croatia": [
            "Zagreb"
        ],
        "\xc3\x85land Islands": [
            "Mariehamn"
        ],
        "Guernsey": [
            "Guernsey"
        ],
        "Monaco": [
            "Monaco"
        ],
        "Switzerland": [
            "Zurich"
        ],
        "Jersey": [
            "Jersey"
        ],
        "Bulgaria": [
            "Sofia"
        ],
        "Romania": [
            "Bucharest"
        ],
        "Albania": [
            "Tirane"
        ],
        "Portugal": [
            "Lisbon"
        ],
        "Malta": [
            "Malta"
        ],
        "Serbia": [
```

```
            "Belgrade"
        ],
        "Liechtenstein": [
            "Vaduz"
        ],
        "Austria": [
            "Vienna"
        ],
        "Greece": [
            "Athens"
        ],
        "Hungary": [
            "Budapest"
        ],
        "Isle of Man": [
            "Isle_of_Man"
        ]
    },
    "Australia": {
        "Australia": [
            "Melbourne",
            "Eucla",
            "Brisbane",
            "Lindeman",
            "Broken_Hill",
            "Hobart",
            "Lord_Howe",
            "Perth",
            "Sydney",
            "Currie",
            "Darwin",
            "Adelaide"
        ]
    },
    "Arctic": {
        "Svalbard and Jan Mayen": [
            "Longyearbyen"
        ]
    },
    "Africa": {
        "Sao Tome and Principe": [
            "Sao_Tome"
        ],
        "Kenya": [
            "Nairobi"
        ],
        "Sudan": [
            "Khartoum"
        ],
        "Guinea": [
            "Conakry"
        ],
        "Tanzania United Republic of": [
            "Dar_es_Salaam"
        ],
        "Congo, Democratic Republic of the": [
            "Kinshasa",
            "Lubumbashi"
        ],
        "Ethiopia": [
            "Addis_Ababa"
        ],
        "Rwanda": [
            "Kigali"
        ],
```

```
        "Somalia": [
            "Mogadishu"
        ],
        "Swaziland": [
            "Mbabane"
        ],
        "Nigeria": [
            "Lagos"
        ],
        "Cameroon": [
            "Douala"
        ],
        "Burkina Faso": [
            "Ouagadougou"
        ],
        "Benin": [
            "Porto-Novo"
        ],
        "Ghana": [
            "Accra"
        ],
        "Western Sahara": [
            "El_Aaiun"
        ],
        "Algeria": [
            "Algiers"
        ],
        "Zambia": [
            "Lusaka"
        ],
        "Djibouti": [
            "Djibouti"
        ],
        "Malawi": [
            "Blantyre"
        ],
        "Togo": [
            "Lome"
        ],
        "Eritrea": [
            "Asmara"
        ],
        "Zimbabwe": [
            "Harare"
        ],
        "Liberia": [
            "Monrovia"
        ],
        "Sierra Leone": [
            "Freetown"
        ],
        "Spain": [
            "Ceuta"
        ],
        "Mauritania": [
            "Nouakchott"
        ],
        "Libya": [
            "Tripoli"
```

```
        ],
        "Gambia": [
            "Banjul"
        ],
        "Central African Republic": [
            "Bangui"
        ],
        "Morocco": [
            "Casablanca"
        ],
        "Namibia": [
            "Windhoek"
        ],
        "South Sudan": [
            "Juba"
        ],
        "Guinea-Bissau": [
            "Bissau"
        ],
        "Mali": [
            "Bamako"
        ],
        "Egypt": [
            "Cairo"
        ],
        "Angola": [
            "Luanda"
        ],
        "Chad": [
            "Ndjamena"
        ],
        "South Africa": [
            "Johannesburg"
        ],
        "Tunisia": [
            "Tunis"
        ],
        "C\xc3\xb4te d'Ivoire": [
            "Abidjan"
        ],
        "Equatorial Guinea": [
            "Malabo"
        ],
        "Lesotho": [
            "Maseru"
        ],
        "Senegal": [
            "Dakar"
        ],
        "Congo": [
            "Brazzaville"
        ],
        "Mozambique": [
            "Maputo"
        ],
        "Uganda": [
            "Kampala"
        ],
        "Burundi": [
            "Bujumbura"
        ],
        "Gabon": [
            "Libreville"
        ],
        "Niger": [
```

```
            "Niamey"
        ],
        "Botswana": [
            "Gaborone"
        ]
    },
    "Pacific": {
        "Palau": [
            "Palau"
        ],
        "Northern Mariana Islands": [
            "Saipan"
        ],
        "Pitcairn": [
            "Pitcairn"
        ],
        "French Polynesia": [
            "Marquesas",
            "Gambier",
            "Tahiti"
        ],
        "Vanuatu": [
            "Efate"
        ],
        "Nauru": [
            "Nauru"
        ],
        "Micronesia (Federated States of)": [
            "Pohnpei",
            "Chuuk",
            "Kosrae"
        ],
        "Tuvalu": [
            "Funafuti"
        ],
        "United States of America": [
            "Honolulu"
        ],
        "American Samoa": [
            "Pago_Pago"
        ],
        "Papua New Guinea": [
            "Bougainville",
            "Port_Moresby"
        ],
        "United States Minor Outlying Islands": [
            "Wake",
            "Midway"
        ],
        "Solomon Islands": [
            "Guadalcanal"
        ],
        "Marshall Islands": [
            "Kwajalein",
            "Majuro"
        ],
        "Cook Islands": [
            "Rarotonga"
        ],
```

```
        "Chile": [
            "Easter"
        ],
        "Kiribati": [
            "Tarawa",
            "Enderbury",
            "Kiritimati"
        ],
        "Tonga": [
            "Tongatapu"
        ],
        "New Caledonia": [
            "Noumea"
        ],
        "Ecuador": [
            "Galapagos"
        ],
        "Niue": [
            "Niue"
        ],
        "Wallis and Futuna": [
            "Wallis"
        ],
        "New Zealand": [
            "Chatham",
            "Auckland"
        ],
        "Samoa": [
            "Apia"
        ],
        "Tokelau": [
            "Fakaofo"
        ],
        "Guam": [
            "Guam"
        ],
        "Norfolk Island": [
            "Norfolk"
        ],
        "Fiji": [
            "Fiji"
        ]
    },
    "Etc": {
        "GMT": [
            "GMT-10",
            "GMT-11",
            "GMT-12",
            "GMT-1",
            "GMT+8",
            "GMT+9",
            "GMT+1",
            "GMT+2",
            "GMT+3",
            "GMT+4",
            "GMT+5",
            "GMT+6",
            "GMT+7",
            "GMT+12",
            "GMT+10",
            "GMT+11",
            "GMT-8",
            "GMT-9",
            "GMT-6",
            "GMT-7",
```

```
            "GMT-4",
            "GMT-5",
            "GMT-2",
            "GMT-3",
            "GMT"
        ]
    },
    "Antarctica": {
        "Antarctica": [
            "Troll",
            "DumontDUrville",
            "Vostok",
            "Syowa",
            "Palmer",
            "Casey",
            "Rothera",
            "McMurdo",
            "Davis",
            "Mawson"
        ],
        "Australia": [
            "Macquarie"
        ]
    },
    "Indian": {
        "Mauritius": [
            "Mauritius"
        ],
        "Madagascar": [
            "Antananarivo"
        ],
        "Maldives": [
            "Maldives"
        ],
        "Rxa9union": [
            "Reunion"
        ],
        "Mayotte": [
            "Mayotte"
        ],
        "Christmas Island": [
            "Christmas"
        ],
        "Cocos (Keeling) Islands": [
            "Cocos"
        ],
        "British Indian Ocean Territory": [
            "Chagos"
        ],
        "Seychelles": [
            "Mahe"
        ],
        "Comoros": [
            "Comoro"
        ],
        "French Southern Territories": [
            "Kerguelen"
        ]
    },
```

```
    "Atlantic": {
        "Portugal": [
            "Azores",
            "Madeira"
        ],
        "Faroe Islands": [
            "Faroe"
        ],
        "Iceland": [
            "Reykjavik"
        ],
        "South Georgia and the South Sandwich Islands": [
            "South_Georgia"
        ],
        "Saint Helena Ascension and Tristan da Cunha": [
            "St_Helena"
        ],
        "Cabo Verde": [
            "Cape_Verde"
        ],
        "Falkland Islands (Malvinas)": [
            "Stanley"
        ],
        "Bermuda": [
            "Bermuda"
        ],
        "Spain": [
            "Canary"
        ]
    },
    "Asia": {
        "Afghanistan": [
            "Kabul"
        ],
        "Qatar": [
            "Qatar"
        ],
        "Bangladesh": [
            "Dhaka"
        ],
        "Bhutan": [
            "Thimphu"
        ],
        "Iran (Islamic Republic of)": [
            "Tehran"
        ],
        "Kuwait": [
            "Kuwait"
        ],
        "Nepal": [
            "Kathmandu"
        ],
        "Mongolia": [
            "Hovd",
            "Choibalsan",
            "Ulaanbaatar"
        ],
        "Azerbaijan": [
            "Baku"
        ],
        "Macao": [
            "Macau"
        ],
        "Syrian Arab Republic": [
            "Damascus"
```

```
        ],
        "Turkmenistan": [
            "Ashgabat"
        ],
        "Bahrain": [
            "Bahrain"
        ],
        "Viet Nam": [
            "Ho_Chi_Minh"
        ],
        "Saudi Arabia": [
            "Riyadh"
        ],
        "Singapore": [
            "Singapore"
        ],
        "China": [
            "Shanghai",
            "Urumqi"
        ],
        "Armenia": [
            "Yerevan"
        ],
        "Russian Federation": [
            "Ust-Nera",
            "Vladivostok",
            "Barnaul",
            "Anadyr",
            "Novokuznetsk",
            "Irkutsk",
            "Yakutsk",
            "Yekaterinburg",
            "Novosibirsk",
            "Krasnoyarsk",
            "Sakhalin",
            "Omsk",
            "Magadan",
            "Khandyga",
            "Srednekolymsk",
            "Tomsk",
            "Chita",
            "Kamchatka"
        ],
        "Jordan": [
            "Amman"
        ],
        "Iraq": [
            "Baghdad"
        ],
        "Hong Kong": [
            "Hong_Kong"
        ],
        "Korea (Republic of)": [
            "Seoul"
        ],
        "India": [
            "Kolkata"
        ],
        "Kyrgyzstan": [
```

```
            "Bishkek"
        ],
        "Georgia": [
            "Tbilisi"
        ],
        "Lao People's Democratic Republic": ["Vientiane"], "Korea (Democratic People's Republic
of)": [
            "Pyongyang"
        ],
        "Oman": [
            "Muscat"
        ],
        "Philippines": [
            "Manila"
        ],
        "Indonesia": [
            "Jakarta",
            "Makassar",
            "Pontianak",
            "Jayapura"
        ],
        "Israel": [
            "Jerusalem"
        ],
        "Tajikistan": [
            "Dushanbe"
        ],
        "Cambodia": [
            "Phnom_Penh"
        ],
        "Thailand": [
            "Bangkok"
        ],
        "Yemen": [
            "Aden"
        ],
        "Palestine, State of": [
            "Hebron",
            "Gaza"
        ],
        "Pakistan": [
            "Karachi"
        ],
        "Myanmar": [
            "Yangon"
        ],
        "Kazakhstan": [
            "Aqtau",
            "Aqtobe",
            "Atyrau",
            "Qyzylorda",
            "Qostanay",
            "Oral",
            "Almaty"
        ],
        "Lebanon": [
            "Beirut"
        ],
        "Brunei Darussalam": [
            "Brunei"
        ],
        "Uzbekistan": [
            "Tashkent",
            "Samarkand"
        ],
```

```
        "Malaysia": [
            "Kuala_Lumpur",
            "Kuching"
        ],
        "Timor-Leste": [
            "Dili"
        ],
        "United Arab Emirates": [
            "Dubai"
        ],
        "Sri Lanka": [
            "Colombo"
        ],
        "Japan": [
            "Tokyo"
        ],
        "Taiwan": [
            "Taipei"
        ],
        "Cyprus": [
            "Famagusta",
            "Nicosia"
        ]
    },
    "America": {
        "Canada": [
            "Regina",
            "Goose_Bay",
            "Whitehorse",
            "Winnipeg",
            "Vancouver",
            "St_Johns",
            "Rankin_Inlet",
            "Cambridge_Bay",
            "Moncton",
            "Rainy_River",
            "Inuvik",
            "Toronto",
            "Fort_Nelson",
            "Creston",
            "Blanc-Sablon",
            "Yellowknife",
            "Dawson_Creek",
            "Nipigon",
            "Thunder_Bay",
            "Atikokan",
            "Halifax",
            "Swift_Current",
            "Iqaluit",
            "Resolute",
            "Edmonton",
            "Glace_Bay",
            "Dawson",
            "Pangnirtung"
        ],
        "Brazil": [
            "Sao_Paulo",
            "Cuiaba",
            "Maceio",
```

```
            "Santarem",
            "Manaus",
            "Boa_Vista",
            "Noronha",
            "Araguaina",
            "Fortaleza",
            "Belem",
            "Porto_Velho",
            "Campo_Grande",
            "Eirunepe",
            "Rio_Branco",
            "Recife",
            "Bahia"
        ],
        "Saint Martin (French part)": [
            "Marigot"
        ],
        "Virgin Islands (British)": [
            "Tortola"
        ],
        "Peru": [
            "Lima"
        ],
        "Virgin Islands (U.S.)": [
            "St_Thomas"
        ],
        "Bolivia, Plurinational State of": [
            "La_Paz"
        ],
        "Panama": [
            "Panama"
        ],
        "Costa Rica": [
            "Costa_Rica"
        ],
        "Saint Pierre and Miquelon": [
            "Miquelon"
        ],
        "Bahamas": [
            "Nassau"
        ],
        "Aruba": [
            "Aruba"
        ],
        "Suriname": [
            "Paramaribo"
        ],
        "Argentina": [
            "Argentina/Salta",
            "Argentina/Jujuy",
            "Argentina/Tucuman",
            "Argentina/San_Juan",
            "Argentina/San_Luis",
            "Argentina/La_Rioja",
            "Argentina/Catamarca",
            "Argentina/Ushuaia",
            "Argentina/Cordoba",
            "Argentina/Mendoza",
            "Argentina/Buenos_Aires",
            "Argentina/Rio_Gallegos"
        ],
        "Anguilla": [
            "Anguilla"
        ],
        "Ecuador": [
```

```
            "Guayaquil"
        ],
        "Martinique": [
            "Martinique"
        ],
        "Cuba": [
            "Havana"
        ],
        "El Salvador": [
            "El_Salvador"
        ],
        "United States of America": [
            "Kentucky/Louisville",
            "Nome",
            "Denver",
            "Kentucky/Monticello",
            "Sitka",
            "New_York",
            "Phoenix",
            "Los_Angeles",
            "Yakutat",
            "Boise",
            "Indiana/Tell_City",
            "Indiana/Knox",
            "Anchorage",
            "Detroit",
            "Adak",
            "Indiana/Petersburg",
            "Indiana/Indianapolis",
            "North_Dakota/Center",
            "Indiana/Marengo",
            "Indiana/Winamac",
            "Metlakatla",
            "North_Dakota/New_Salem",
            "North_Dakota/Beulah",
            "Chicago",
            "Juneau",
            "Menominee",
            "Indiana/Vevay",
            "Indiana/Vincennes"
        ],
        "Saint Kitts and Nevis": [
            "St_Kitts"
        ],
        "Guatemala": [
            "Guatemala"
        ],
        "Chile": [
            "Santiago",
            "Punta_Arenas"
        ],
        "Puerto Rico": [
            "Puerto_Rico"
        ],
        "Antigua and Barbuda": [
            "Antigua"
        ],
        "Haiti": [
            "Port-au-Prince"
```

```
        ],
        "Belize": [
            "Belize"
        ],
        "Saint Lucia": [
            "St_Lucia"
        ],
        "Dominica": [
            "Dominica"
        ],
        "Montserrat": [
            "Montserrat"
        ],
        "Cayman Islands": [
            "Cayman"
        ],
        "Trinidad and Tobago": [
            "Port_of_Spain"
        ],
        "French Guiana": [
            "Cayenne"
        ],
        "Guyana": [
            "Guyana"
        ],
        "Grenada": [
            "Grenada"
        ],
        "Guadeloupe": [
            "Guadeloupe"
        ],
        "Dominican Republic": [
            "Santo_Domingo"
        ],
        "Jamaica": [
            "Jamaica"
        ],
        "Greenland": [
            "Scoresbysund": "Scoresbysund/Ittoqqortoormiit",
            "Danmarkshavn",
            "Thule": "Thule/Pituffik",
            "Nuuk"
        ],
        "Honduras": [
            "Tegucigalpa"
        ],
        "Bonaire, Sint Eustatius and Saba": [
            "Kralendijk"
        ],
        "Mexico": [
            "Monterrey",
            "Matamoros",
            "Mexico_City",
            "Chihuahua",
            "Hermosillo",
            "Cancun",
            "Bahia_Banderas",
            "Mazatlan",
            "Merida",
            "Ojinaga",
            "Tijuana"
        ],
        "Nicaragua": [
            "Managua"
        ],
```

```
        "Cura\xc3\xa7ao": [
            "Curacao"
        ],
        "Saint Barth\xc3\xa9lemy": [
            "St_Barthelemy"
        ],
        "Uruguay": [
            "Montevideo"
        ],
        "Venezuela, Bolivarian Republic of": [
            "Caracas"
        ],
        "Saint Vincent and the Grenadines": [
            "St_Vincent"
        ],
        "Sint Maarten (Dutch part)": [
            "Lower_Princes"
        ],
        "Colombia": [
            "Bogota"
        ],
        "Paraguay": [
            "Asuncion"
        ],
        "Turks and Caicos Islands": [
            "Grand_Turk"
        ],
        "Barbados": [
            "Barbados"
        ]
    }
}
```

Decryption Profiles

Retrieving the Decryption Profiles

Table 143 - Attributes for Retrieving the Decryption Profiles

API	wsa/api/v3.0/web_security/decryption_policies		
Method	GET		
Parameters	None		
Request body	None		
Response	Code	Type	Description

	200 Ok	array	List of all decryption policies available and their configuration. If policy names are provided, returns all the decryption policies with matching policy_names.

Modifying the Decryption Profiles

Table 144 - Attributes for Modifying the Decryption Profiles

API	wsa/api/v3.0/web_security/decryption_policies			
Method	PUT			
Parameters	None			
Request body	Name	Type	Description	Required
	decryption_policies	Array of objects decryption_policies schema	List of decryption policies and their configuration payload.	Yes
Response	Code	Type	Description	
	204 No Content	Empty body	The request has been processed successfully and all the given decryption policies are updated with the given payload.	
	207 Multi Status	Multi status response	Dictionary of success and Failure list. Failure list will contain proper error message, specifying reason of failure.	

Adding the Decryption Profiles

Table 145 - Attributes for Adding the Decryption Profiles

API	wsa/api/v3.0/web_security/decryption_policies
Method	POST

Decryption Profiles

Parameters	None			
Request body	Name	Type	Description	Required
	decryption_policies	Array of objects	List of decryption policies and their configuration payload.	Yes
Response	Code	Type	Description	
	204 No Content	Empty body	The request has been processed successfully and all the provided decryption policies are created with the given payload.	
	207 Multi Status	Multi status response	Dictionary of success and Failure list. Failure list will contain proper error message, specifying reason of failure.	

Deleting the Decryption Profiles

Table 146 - Attributes for Deleting the Decryption Profiles

API	wsa/api/v3.0/web_security/decryption_policies			
Method	DELETE			
Parameters	Name	Type	Description	Required
	offset	Integer		optional
	limit	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 decryption policies have been deleted. If policy_names parameter is not provided, all the policies except the global_policy gets deleted.
	207 Multi status	object	Dictionary of success and Failure list. Failure list will contain proper error message, specifying reason of failure.

Definitions

decryption_policies schema

Table 147 - Attributes for decryption_policies schema

Name	Type	Description	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
new_policy_name	String	Same as policy_name	updates the policy_name	Not applicable for global_policy
policy_status	String	Enable/disable	Status of the policy	Not applicable for global_policy
policy_description	String		Description of the policy	Not applicable for global_policy
policy_order	Integer		Order of policy in collection of policies.	Not applicable for global_policy
policy_expiry_status	string	disable	Disables the policy expiry	

Decryption Profiles

Name	Type	Description	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
membership	Object membership_schema		Defined in membership_schema	Not applicable for global_policy
url_filtering	Object		Defined in url_filtering schema	
web_reputation	Object web_reputation_schema		Defined in web_reputation_schema	
default_action	String	use_global, decrypt, drop, pass_through	Default action for HTTPS	use_global cannot be used for global policy

membership_schema

Table 148 - Attributes for membership_schema

Name	Type	Description	Required	
			POST	PUT
Identification_profiles	Array	Array of ID profile objects	Defined in Id_profile_schema	mandatory

Name	Type	Description	Required	
			POST	PUT
subnets	Array of strings	Valid IPv4/ipv6 addresses/ranges/subnets	Subnets for decryption policy if none of the associated ID profile has defined it.	optional
ports	Array of strings	Valid port numbers	Port numbers for decryption policy of none of the associated ID profile has defined it.	optional
url_categories	object		Defined in url_categories_membership schema. None of the associated ID profile has defined url_categories.url_category	optional
user_agents	object		Defined in User_agents schema. None of the associated ID profile has defined user agents.	optional
time_range	object		Defined in time_range schema	optional

Decryption Profiles

Name	Type	Description	Required	
			POST	PUT
user_location	String	One of the value “local” or “remote”	User location details, applicable only if AnyConnect secure mobility is enabled.	

Id_profile_schema

Table 149 - Attributes for Id_profile_schema

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

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

Decryption Profiles

Name	Type	Description	Required	
			POST	PUT
groups_and_users	Object		Defined in groups_and_users_schema . This is mandatory if “auth” is chosen as “Selected groups and users”.	Conditional
auth_realm	String	Name of specific realm or ‘all realm’ as applicable.	If ID profile has auth realm as ‘All Realms’ then it is mandatory to provide either ‘All Realms’ or the specific realm otherwise if ID profile has only one realm associated then this is not mandatory.	Conditional

groups_and_users_schema

Table 150 - 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

Name	Type	Format	Description	Required	
				POST	PUT
auth_group	Object auth_group_schema		Defined in auth_group_schema	No	No

auth_group_schema

Table 151 - Attributes for auth_group_schema

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

url_categories_membership

Table 152 - Attributes for url_categories_membership

Name	Type	Format	Description	Required	
				POST	PUT
predefined	List of Strings		URL categories defined by Secure Web Appliance.	No	No
custom	List of Strings		URL categories defined by user.	No	No

time_range

Table 153 - Attributes for time_range

Name	Type	Description	Required	
			POST	PUT
time_range_name	String	Name of a valid time range profile.	Yes	Yes

Decryption Profiles

Name	Type	Description	Required	
			POST	PUT
is_inverse	Integer	Whether use the time defined in time_range_name profile or use the time profile other than defined in time_range_name based upon values 0,1	Yes	Yes

url_filtering schema

Table 154 - Attributes for url_filtering schema

Name	Type	Format	Description	Required	
				POST	PUT
state	string	use_global/custom	url filtering settings. If url_filtering 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 custom_cats schema.	optional	optional
predefined_cats	object		Defined in predefined_cats schema	optional	optional
overall_quota_profile	string		set a quota that applies to all web surfing activities.	optional	optional
uncategorized_url	string	Use_global/pass_through/monitor/decrypt/drop	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

custom_cats schema

Table 155 - Attributes for custom_cats schema

Name	Type	Description	Required	
			POST	PUT
pass_through	Array of strings	List of custom categories to allow	optional	optional
monitor	Array of strings	List of custom categories to monitor	optional	optional
decrypt	object	List of custom categories to decrypt	optional	optional
drop	Array of strings	List of custom categories to drop	optional	optional
exclude	Array of strings	List of custom categories to exclude	optional	optional
Use_global	Array of strings	List of custom categories to set use_global settings. Not applicable for global policy	optional	optional
quota_based	object	Custom categories to configure for time and volume quotas. Defined in quota_based schema	optional	optional
time_based	object	Custom categories to configure for time range. Defined in time_based schema.	optional	optional

quota_based schema

Table 156 - Attributes for quota_based schema

Name	Type	Description	Required	
			POST	PUT
<url category name>	object	Categories to be configured for quota-based profiles. Defined in quota_based schema .	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 157 - 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 in time_based	optional	optional

time_range_schema

Table 158 - Attributes for time_range_schema

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/conditional	Optional/conditional	Available only for custom categories
action_redirect	string	Redirect to if in time range	Optional/conditional	Optional/conditional	Available only for custom categories

predefined_cats schema

Table 159 - Attributes for predefined_cats schema

Name	Type	Description	Required	
			POST	PUT
pass_through	Array of strings	List of predefined categories to pass_through	optional	optional
monitor	Array of strings	List of predefined categories to monitor	optional	optional
decrypt	Array of strings	List of predefined categories to decrypt	optional	optional
drop	Array of strings	List of predefined categories to drop	optional	optional

Name	Type	Description	Required	
			POST	PUT
use_global	Array of strings	List of predefined categories to set use_global settings. Not applicable for global policy.	optional	optional
quota_based	object	predefined categories to configure for time and volume quotas. Defined in quota_based schema .	optional	optional
time_based	object	predefined categories to configure for time range. Defined in time_based schema.	optional	optional

web_reputation_schema

Table 160 - Attributes for web_reputation_schema

Name	Type	Format	Description	Required	
				POST	PUT
state	String	use_global/custom/disable	Describes whether to use custom settings or disable or inherit all the settings from Global policy.	Optional	Optional
score	Object		Sets action for sites with matching wbrs score. Defined in score_schema	optional	optional
no_score_action	string	Use_global/monitor/pass_through/decrypt/drop	Used to set action for sites that do not have a Web Reputation Score. Sets to action Monitor by default, use_global action is not applicable for global policy.	optional	optional

score_schema

Table 161 - Attributes for score_schema

Name	Type	Format	Description	Required	
				POST	PUT
drop	Array of strings	Float Value between -10.0 to 10.0	Drops HTTPS connection for this score range. Default is -10.0 to 6.0. Empty list sets the action to NA.	optional	optional

pass_through	Array of strings	Float Value between -10.0 to 10.0	HTTPS request is passed through without decryption for this score range. Default is 6.0 to 10.0. Empty list sets the action to NA.	optional	optional

Note: There is no decrypt array required in score schema. Decrypt values will be set based on drop and pass_through values. Hence, values of decrypt array if provided in score schema will not be considered or validated.

Routing Profiles

Retrieving the Routing Profiles

Table 162 - Attributes for Retrieving the Routing Profiles

API	wsa/api/v3.0/web_security/routing_policies				
Method	GET				
Parameters	Name	Type	Description	Remarks	Required
	offset	Integer			Optional
	limit	Integer			Optional
	policy_names	String	List of routing 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 routing_policies available and their configurations. If policy_names is provided, returns all the routing policies with matching policy_names.	

Modifying the Routing Profiles

Table 163 - Attributes for Modifying the Routing Profiles

API	wsa/api/v3.0/web_security/routing_policies			
Method	PUT			
Parameters	None			
Request body	Name	Type	Description	Required
	routing_policies	array	List of routing policies and their configuration payload.	Mandatory
Response	Code	Type	Description	
	204 Ok	Empty body	The request has been processed successfully and all the given routing policies are updated with the given payload.	
	207 Multi status	Multi status response	Dictionary of success and Failure list. Failure list will contain proper error message, specifying reason of failure.	

Adding the Routing Profiles

Table 164 - Attributes for Adding the Routing Profiles

API	wsa/api/v3.0/web_security/routing_policies			
Method	POST			
Parameters	None			
Request body	Name	Type	Description	Required
	routing_policies	array	List of routing policies and their configuration payload	Mandatory
Response	Code	Type	Description	
	204 Ok	Empty body	The request has been processed successfully and all the given routing policies are created with the given payload.	
	207 Multi status	Multi status response	Dictionary of success and Failure list. Failure list will contain proper error message, specifying reason of failure.	

Deleting the Routing Profiles

Table 165 - Attributes for Deleting the Routing Profiles

API	wsa/api/v3.0/web_security/routing_policies			
Method	DELETE			
Parameters	Name	Type	Description	Required
	offset	Integer		optional
	limit	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 routing policies have been deleted. If policy_names parameter is not provided, all the policies except the global_policy gets deleted.	
	207 Multi status	object	Dictionary of success and Failure list. Failure list will contain proper error message, specifying reason of failure.	

Definitions – Payload Configurations

routing_policies schema

Table 166 - Attributes for routing_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	nil	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
membership	object		Defined in membership_schema	Not applicable for global_policy	mandatory	optional
ip_spoofing	String		Defined in ip_spoofing		optional	optional
Routing_destination	object		Defined in routing_destination		optional	optional

membership schema

Table 167 - Attributes for membership schema

Name	Type	Format	Description	Required	
				POST	PUT
Identification_profiles	Array	Array of ID profile objects	Defined in Id_profile_schema	mandatory	optional
subnets	Array of strings	Valid IPv4/ipv6 addresses/ranges/subnets	Subnets for routing policy if none of the associated ID profile has defined it.	optional	optional
ports	Array of strings	Valid port numbers	Port numbers for routing policy of none of the associated ID profile has defined it.	optional	optional
url_categories	object		Defined in url_categories_membership schema. None of the associated ID profile has defined url_categories.	optional	optional
user_agents	object		Defined in user_agents schema. None of the associated ID profile has defined user agents.	optional	optional
time_range	object		Defined in time_range Schema.	optional	optional
user_location	String	One of the value “local” or “remote”	User location details, applicable only if AnyConnect secure mobility is enabled.		

Id_profile_schema

Table 168 - 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 “global identification profile”, “_all_” represents “All identification profiles. In GET’s response the global identification profile is not shown as empty string, it is shown as “global_identification_profile” instead.	Yes	Yes
auth	String	one among: ["All Authenticated Users", "Selected Groups and Users”, "Guests", "No Authentication"]	“All Authenticated Users”: represents all the authenticated users. The selected ID profile must have auth enabled “Selected groups and users”: selected ID profile must have support for this. In addition to this, user needs to provide “groups_and_users” “Guests”: If ID profile supports guest, then this option can be chosen. In case of “all identification profiles” at least one of the ID profiles must support guest. “No Authentication”: If no authentication is required. In case if selected ID profile is “global profile” and doesn’t have auth associated, then no authentication is implicit but still for the sake of schema validation the value “No Authentication” is mandatory.	No	No

Routing Profiles

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

groups_and_users_schema

Table 169 - 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
auth_group	Object		Defined in auth_group_schema	No	No

auth_group_schema

Table 170 - 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 associated with the given realm	Yes	Yes

url_categories_membership

Table 171 - Attributes for url_categories_membership

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

time_range

Table 172 - 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 defined in time_range_name profile or use the time profile other than defined in time_range_name based upon values 0,1.	Yes	Yes

ip_spoofing

Table 173 - Attributes for ip_spoofing

Name	Type	Description	Required	
			POST	PUT
ip_spoofing	String	Name of a valid ip spoofing profile	No	No

routing_destination

Table 174 - Attributes for routing_destination

Name	Type	Description	Required	
			POST	PUT
routing_destination	Object	Defined in proxy_group_schema	No	No

proxy_group_schema

Table 175 - Attributes for Adding the Routing Profiles

Name	Type	Description	Required	
			POST	PUT
upstream_proxy_group	String	Name of a valid upstream proxy group.	No	No

IP Spoofing Profiles

Retrieving the IP Spoofing Profiles

Table 176 - Attributes for Retrieving the IP Spoofing Profiles

API	wsa/api/v3.0/web_security/ip_spoofing_profiles				
Method	GET				
Parameters	Name	Type	Description	Remarks	Required
	offset	Integer			Optional

	limit	Integer			Optional
	profile_names	String	List of ip_spoofing_profiles with the matching profile_names to be returned.		Optional
Request body		None			
Response	Code	Type	Description		
	200 Ok	array	List of all ip_spoofing_profiles available and their configurations. If profile_names are provided, returns all the IP Spoofing profiles with matching profile_names.		

Modifying the IP Spoofing Profiles

Table 177 - Attributes for Modifying the IP Spoofing Profiles

API	wsa/api/v3.0/web_security/ip_spoofing_profiles			
Method	PUT			
Parameters	None			
Request body	Name	Type	Description	Required
	ip_spoofing_profiles	array	List of IP spoofing profiles and their configuration payload.	Mandatory
Response	Code	Type	Description	
	204 Ok	Empty body	The request has been processed successfully and all the given IP spoofing profiles are updated with the given payload.	
	207 Multi status	Multi status response	Dictionary of success and Failure list. Failure list will contain proper error message, specifying reason of failure.	

Adding the IP Spoofing Profiles

Table 178 - Attributes for Adding the IP Spoofing Profiles

API	wsa/api/v3.0/web_security/ip_spoofing_profiles			
Method	POST			
Parameters	None			
Request body	Name	Type	Description	Required
	ip_spoofing_profiles	array	List of IP spoofing profiles and their configuration payload.	Mandatory
Response	Code	Type	Description	
	204 Ok	Empty body	The request has been processed successfully and all the given IP spoofing profiles are created with the given payload.	
	207 Multi status	Multi status response	Dictionary of success and Failure list. Failure list will contain proper error message, specifying reason of failure.	

Deleting the IP Spoofing Profiles

Table 179 - Attributes for Deleting the IP Spoofing Profiles

API	wsa/api/v3.0/web_security/ip_spoofing_profiles				
Method	DELETE				
Parameters	Name	Type	Description	Remarks	Required
	profile_names	String	Profiles with matching profile_names to be deleted.	If not provided, all IP spoofing profiles will be deleted.	optional

	alternate_profile_name	String	Alternate profile name to be provided for the associated routing policies to fallback to. Allowed values: Profile names of existing profiles, 'Do not use IP Spoofing', 'Use Client IP' or 'use_global'	Only single profile name to be provided. If not provided, default will be 'use_global'	optional
Request body		None			
Response	Code	Type	Description		
	204 No Content	Empty	The IP spoofing profiles have been deleted. If profile_names parameter is not provided, all the profiles get deleted.		
	207 Multi status	object	Dictionary of success and Failure list. Failure list will contain proper error message, specifying reason of failure.		

Definitions – Payload Configurations

ip_spoofing_profiles schema

Name	Type	Format	Description	Remarks	Required	
					POST	PUT
profile_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 profile. Unique identifier of the profile.		Mandatory	Mandatory
new_profile_name	String	Same as profile_name.	updates the profile_name		nil	optional
ip_address	String	Valid IPv4 or IPv6 IP address.			Mandatory	optional

Configuration Files

Retrieving the Configuration Files

Table 180 - Attributes for Retrieving the Configuration Files

API	wsa/api/v3.0/system_admin/configuration_file

Configuration Files

Method	GET			
Parameters	Name	Type	Description	Required
	filename	string	Represents the config filename you require for downloaded or e-mailed file. If not provided, api_server will generate a random one.	No
	mail_to	List of strings	This parameter will be used as a destination email-ids for config files. It can be a single email-id or multiple commas separated email ids.	No
Request body	None			
Response	Code	Type	Description	
	200 Ok	Response content will be a file with content-type application/octet-stream.	It contains xml format of config file.	

Modifying the Configuration Files

Table 181 - Attributes for Modifying the Configuration Files

API	sa/api/v3.0/system_admin/configuration_file		
Method	PUT		
Parameters	None		
Request body	Type	Description	Required
	key value pairs as form-data defined configuration_file form data	It contains key value pairs and should be passed as form-data.	Yes
Response	Code	Type	Description

	200 Ok	A dictionary response which contains a success message. It will have following format: `{ "message": msg_string }`	It represents success response.

Retrieving the Appliance Configuration Files

Table 182 - Attributes for Retrieving the Appliance Configuration Files

API	wsa/api/v3.0/system_admin/appliance_config_files		
Method	GET		
Parameters	None		
Request body	None		
Response	Code	Type	Description
	200 Ok	Object appliance_config_files Table 189 - Attributes for appliance_config_files	It represents saved config files on Secure Web Appliance.

Retrieving the Configuration Files – Backup Settings

Table 183 - Attributes of Retrieving the Configuration Files - Backup Settings

API	wsa/api/v3.0/system_admin/config_backup_server		
Method	GET		
Parameters		None	
Request body		None	
Response	Code	Type	Description
	200 Ok	object	Current settings of the configuration backup server.

Modifying the Configuration Files – Backup Settings

Table 184 – Attributes of Modifying the Configuration Files – Backup Settings

API	wsa/api/v3.0/system_admin/config_backup_server			
Method	PUT			
Parameters	None			
Request body	Name	Type	Description	Required
	config_backup_server	config_backup_put_schema	Object with config backup settings	Mandatory
Response	Code	Type	Description	
	204 No-content	Empty body	The request has been processed successfully.	
	200 OK	object	SSH key to be placed in the authorized_keys file on the remote host so that the log files can be uploaded.	
	400 Bad Request	object	Description of error	

Modifying the Configuration Files – Reset

Table 185 – Attributes for Configuration Files – Reset

API	wsa/api/v3.0/system_admin/configuration_file			
Method	PUT			
Parameters	None			
Request body	Key	Value	Description	Required
Form-data	action	reset	Action to reset the system configuration to factory settings.	Mandatory

Form-data	reset_network_settings	True/False	Basic network settings (interface configuration, routing tables, and DNS settings) will be retained if reset_network_settings is set to False and will be reset on True. By default, the value is False.	Optional.
Response	Code	Type	Description	
	200 Ok	object	Success message stating that all settings have been restored to the factory defaults	
	4xx	object	Error message, specifying reason of failure.	

Definitions – Payload Configurations

config_backup_server schema

Name	Type	Format	Remarks	Required
				PUT
config_backup_status	String	Enum - Must be one of "enable" or "disable"		Optional
save_passphrase	boolean	True/false	Default: false	optional
retrieval_method	String	Enum – must be one of "scp_push" or "ftp_push"	Mandatory when enabling config backup.	Conditional
ftp_settings	object	See ftp_settings_schema	Either of the two is mandatory when enabling config backup. Cannot configure both ftp_settings_schema and scp_settings_schema at the same time	Conditional
scp_settings	object	See scp_settings_schema		Conditional

ftp_settings_schema

Table 186- Attributes of ftp_settings_schema

Name	Type	Format	Remarks	Required
				PUT
ftp_host	String	Must be a valid hostname or an IP.	Mandatory when enabling config backup or when changing the retrieval method from scp_push to ftp_push.	Conditional
directory	String	Valid directory path. Characters allowed are letters, numbers, dash, underscore, slash, backslash and period.	Mandatory when enabling config backup or when changing the retrieval method from scp_push to ftp_push.	Conditional
username	String	Valid username. Must contain only English alphabet, number and special characters '.', '@', '-' and '_' only. Non-ASCII symbols and spaces are not allowed.	If field is not provided, previous username will be retained, if any. To reset username to default (blank string), pass blank string for key “username”.	Optional
passphrase	String	Passphrase must be encoded using base-64 encoding before passing.	If field is not provided, previous passphrase will be retained, if any. To remove or reset passphrase to default (blank string), pass blank string for key “passphrase”.	Optional

scp_settings_schema

Table 187 - Attributes for scp_settings_schema

Name	Type	Format	Remarks	Required
				PUT
scp_host	String	Must be a valid hostname or an IP.	Mandatory when enabling config backup or when changing the retrieval method from ftp_push to scp_push.	Conditional

Name	Type	Format	Remarks	Required
				PUT
directory	String	Valid directory path – characters allowed are letters, numbers, dash, underscore, slash, backslash, and period.	Mandatory when enabling config backup or when changing the retrieval method from ftp_push to scp_push.	Conditional
username	String	Valid username – must contain only English alphabet, number and special characters '.', '@', '-' and '_' only. Non-ASCII symbols and spaces are not allowed.	If field is not provided, previous username will be retained, if any. To reset username to default (blank string), pass blank string for key “username”.	Optional
scp_port	String	Must be a number from 1 to 65535	Default scp_port is 22	Optional
host_key_checking	object	See host_key_checking_schema		Optional

host_key_checking_schema

Table 188 - Attributes for host_key_checking_schema

Name	Type	Format	Remarks	Required
				PUT
status	String	Enum. Must be either enable or disable.	Default value is “disable”.	Optional
key_method	String	Enum. Must be either auto or manual.	Default value is “auto”.	Optional
ssh_key	String	Valid ssh key	Default value is empty string.	Optional

appliance_config_files

Table 189 - Attributes for appliance_config_files

Name	Type	Description

appliance_config_files	List of strings	Each element this list represents config file name which has been saved on WSA appliance.

configuration_file form data

Table 190 - Attributes for configuration_file form data

Name	Type	Description	Required condition
action	String	Represents the action you want to perform on the configuration file. Possible values are 'save', 'load'. For saving config file on appliance use 'save'. The value 'load' will be used for setting a new config.	Mandatory
source	String	It represents the source, from which file will be used for loading the config. Possible values are 'local', 'appliance' and 'text'.	Only if action is 'load'.
filename	String	It represents user defined name for config file you want to save on appliance.	Not mandatory but exists only if action is 'save'. If not provided, system will generate a unique string as filename.
passphrase_action	String	It represents the action that should be performed on all passphrases present in config, while saving a file on appliance. Possible values are 'mask' and 'encrypt'	Not mandatory but exists only if action is 'save'. If not provided, 'mask' will be chosen as default value.
uploaded_file	File	It represents the config file that you upload to install on Secure Web Appliance.	Only If action is 'load' and source is 'local'.
appliance_file	String	Represents filename of config present on appliance.	Only If action is 'load' and source is 'appliance'.
config_text	String	It represents content of config file, if you are uploading a xml config as text (not contained in a file).	Only If action is 'load' and source is 'text'.

Authentication Realms

Retrieving the Authentication Realms

Table 191 - Attributes for Retrieving the Authentication Realms

API	wsa/api/v3.0/network/auth_realms			
Method	GET			
Parameters	Name	Type	Description	Required
	realm_names	List of Strings	Response will contain only those realms that has been provided as the query parameter. If provided names do not exist, an empty list will be returned. This parameter will have more priority than offset and limit if all given.	No
	offset	Integer	Represents start index of realm in configured realm list, from which user wants to start filtering.	No
	limit	Integer	Represents, number of realm user from which the user wants to filter starting from the given offset.	No
Request body	None			
Response	Code	Type	Description	
	200 Ok	A JSON object authentication_realms	A json response, containing list of authentication realm objects.	

Adding the Authentication Realm Settings

Table 192 - Attributes for Adding the Authentication Realm Settings

API	wsa/api/v3.0/network/auth_realms		
Method	POST		
Parameters	None		
Request body	Type	Description	Required
	A JSON object authentication_realms	It contains a list of auth realm objects. A single request can create multiple auth realms.	Yes
Response	Code	Type	Description

	204 No Content	Empty Response.	If all of auth realms given in request body has been processed successfully then api_server sends this response.
	207 Multi-Status	Object (multi-status)	If at least one of auth realm object passed in request body couldn't processed successfully then server generates a multi-status response

Retrieving the Authentication Realm Sequence Settings

Table 193 – Attributes for Retrieving the Authentication Realm Sequence Settings

API	wsa/api/v3.0/network/auth_sequences			
Method	GET			
Parameters	Name	Type	Description	Required
	sequence_names	List of Strings	Response will contain only those sequences that has been provided as the query parameter. If provided names do not exist, an empty list will be returned. This parameter will have more priority than offset and limit if all given.	No
	offset	Integer	Represent start index of sequence in configured sequence list, from which user wants to start filtering.	No
	limit	Integer	Represents number of sequence user wants to filter starting from given offset.	No
Request body	None			
Response	Code	Type	Description	
	200 Ok	A JSON object authentication_realms	A json response, containing list of authentication sequence objects.	

Modifying the Authentication Realm Sequence Settings

Table 194 – Attributes for Modifying the Authentication Realm Sequence Settings

API	wsa/api/v3.0/network/auth_sequences		
Method	POST		
Parameters	None		
Request body	Type	Description	Required
	A JSON object (authentication_sequences)	It contains a list of auth sequence objects. A single request can update multiple auth sequences.	Yes
Response	Code	Type	Description
	204 No Content	Empty Response.	If all auth sequences given in request body has been processed successfully, then api_server sends this response.
	207 Multi-Status	Object (multi-status)	If at least one of auth sequence object passed in request body cannot be processed successfully, then server generates a multi-status response.

Adding the Authentication Realm Sequence Settings

Table 195 – Attributes for Adding the Authentication Realm Sequence Settings

API	wsa/api/v3.0/network/auth_sequences		
Method	POST		
Parameters	None		
Request body	Type	Description	Required
	A JSON object authentication_sequences	It contains a list of auth sequence objects. A single request can create multiple auth sequences.	Yes
Response	Code	Type	Description
	204 No Content	Empty Response.	If all auth sequences given in request body has been processed successfully, then api_server sends this response.

	207 Multi-Status	Object (multi-status)	If at least one of auth sequence object passed in request body cannot be processed successfully, then the server generates a multi-status response.

Retrieving the Global Authentication Settings

Table 196 – Attributes for Retrieving the Global Authentication Settings

API	/wsa/api/v3.0/network/global_auth_setting			
Method	GET			
Response	Code	Type		Description
	200 Ok	object		Details of Global Authentication Settings available and the configurations such as Authentication Token TTL, Credential Encryption, Header Based Authentication, and so on.

Modifying the Global Authentication Settings

Table 197 – Attributes for Modifying the Global Authentication Settings

API	/wsa/api/v3.0/network/global_auth_setting		
Method	PUT		
Parameters	None		
Response	Code	Type	Description
	204 Ok	Empty body	The request has been processed successfully and the Global Authentication Settings has been updated.

Definitions

authentication_sequences

Table 198 - Attributes for authentication_sequences

Name	Type	Description	Required condition	
			POST	PUT
auth_sequences	List of objects auth_sequence	Every object in list will represent one authentication sequence.	Yes	Yes

auth_sequence

Table 199 - Attributes for auth_sequence

Name	Type	Description	Required condition	
			POST	PUT
name	string	Name of authentication sequence	Yes	Yes
schemes	Object schemes	This object contains different types of auth schemes and associated auth realms list. At least one scheme is required with non-empty list.	Yes	No
New_name	string	Updated name of existing authentication sequence. It is meaningless in POST request	No	No

schemes

Table 200 – Attributes for schemes

Name	Type	Description	Required condition	
			POST	PUT
Kerberos	List of strings	List of already existing auth realms which support 'Kerberos' auth scheme.	No	No
NTLMSSP	List of strings	List of already existing auth realms which support 'NTLMSSP' auth scheme.	No	No
Basic	List of strings	List of already existing auth realms which support 'Basic' auth scheme.	No	No

authentication_realms

Table 201 – Attributes for authentication_realms

Name	Type	Description	Required condition	
			POST	PUT
authentication_realms	List of objects auth_realm_ldap or auth_realm_ad	Every object in the list will represent one authentication realm.	Yes	Yes

auth_realm_ldap

Table 202 – Attributes for auth_realm_ldap

Name	Type	Description	Required condition	
			POST	PUT
name	String	Name of auth realm which also work as an unique identifier.	Yes	Yes
type	String	Type of realm. It will be always "LDAP".	Yes	No
version	Integer	Represents version of LDAP. It can have values: 2 or 3.	Yes	No
ldap_server	Object ldap_server	Represents LDAP server settings.	Yes	No

Name	Type	Description	Required condition	
			POST	PUT
query_credential	Object query_credential	Represents query credential settings.	No	No
base_dn	String	Represents base DN. example: dc=mycompany, dc=com	Yes	No
use_secure_ldap	Boolean	Represents whether to use secure LDAP or not. It will only exist if LDAP version is 3.	No	No
tui_enabled	Boolean	Represents whether Transparent User Identification has been enabled or not. It will only exist if LDAP version is 3.	No	No
advance_settings	Object advance_settings	It represents connection settings with LDAP server.	No	No

ldap_server

Table 203- Attributes for ldap_server

Name	Type	Description	Required condition	
			POST	PUT
interface	String	It represents source interface of WSA device.	Yes	No
servers	List of Objects servers	These are the list of LDAP server-port combinations. You can specify up to three servers.	Yes	No

servers

Table 204 - Atttributes for servers

Name	Type	Description	Required condition	
			POST	PUT
host	String	Represents host name or IP of LDAP server.	Yes	No
port	Integer	Represents port of LDAP server. If not provided, default port 389 for standard LDAP or 686 for secure LDAP will be selected.	No	No

query_credential

Table 205 - Attributes for query_credential

Name	Type	Description	Required condition	
			POST	PUT
bind_dn	String	It represents the user on the external LDAP server permitted to search the LDAP directory. The following text lists some example users for this field: cn=administrator,cn=Users,dc=domain,dc=com sAMAccountName=jdoe,cn=Users,dc=domain,dc=com.	Yes	No
passphrase	String	The passphrase associated with the user, in the bind_dn field. Its value will be base64 encoded.	Yes	No

advance_settings

Table 206 - attributes for advance_settings

Name	Type	Description	Required condition	
			POST	PUT
request_per_second	Integer	Request limit per second to LDAP server. Value 0 represents unlimited.	No (Allowed only if presistent_connection_enabled is True)	Yes (Allowed only if presistent_connection_enabled is True)
presistent_connection_enabled	Boolean	Whether to use persistent connection or not, with LDAP server.	Yes	No

external_auth_settings

Table 207 - Attributes for external_auth_settings

Name	Type	Description	Required condition	
			POST	PUT
name	String	It represents name of external authentication query settings. If not provided in POST method, default value will be, “name_of _realm. .externalauth” For example, If auth realm name is ‘myRealm’ then its default value will be ‘myRealm .externalauth’	No	No
user_authentication	Object user_authentication – External Authentication	It contains info related to user authentication.	Yes	No
group_membership	Object group_membership	It contains info related to group membership.	Yes	No

user_authentication – External Authentication

Table 208 - Attributes for user_authentication – External Authentication

Name	Type	Description	Required condition	
			POST	PUT
base_dn	String	Base DN to navigate to the correct location in the LDAP directory tree to begin a search.	Yes	No

query_string	String	The query to return the set of authentication groups,
		
		for example:
		
		`(&(objectClass=posixAccount)(uid={u}))`
		
		`or`
		
		`(&(objectClass=user)(sAMAccountName={u}))`
			Yes	No

full_name_attribute	String	Attribute containing user's full name. For example, displayName, gecos and so on .	Yes	No
deny_expired_account_login	Boolean	It represents, whether to deny login to expired accounts or not, based on RFC 2307 account expiration LDAP attributes.	No	No

group_membership

Table 209 - Attributes for group_membership

Name	Type	Description	Required condition	
			POST	PUT
membership_query	String	Query String to determine if a user is a member of a group. For example: `(&(objectClass=posixAccount)(uid={u}))`	Yes	Yes
member_attribute	String	Attribute in these records that holds each member's username (or a DN for the user's record). For example, gecos and so on.	Yes	No
group_name_attribute	String	Attribute in these records that contains the group name.	Yes	No
base_dn	String	It represents, the Base DN to navigate to the correct location in the LDAP directory tree to begin a search.	Yes	No

user_group_queries

Table 210- Attributes for user_group_queries

Name	Type	Description	Required condition	
			POST	PUT
user_authentication	Object user_authentication – User/Group Queries	It contains user authentication info.	Yes	No
group_authorization	Object group_authorization Table 212 - Attributes for group_authorization	It contains group authorization info.	Yes	No

user_authentication – User/Group Queries

Table 211 – Attributes for user_authentication – User/Group Queries

Name	Type	Description	Required condition	
			POST	PUT
username_attribute	String	It represents user name attribute. These are unique identifiers in the LDAP directory that specify a username. Possible values: 1. Predefined values: uid, cn, and sAMAccountName 2. Custom values: User can provide a custom identifier eg. 'UserAccount'	Yes	No
user_filter_query	String	The User Filter Query is an LDAP search filter that locates the users Base DN. This is required if the user directory is in a hierarchy below the Base DN, or if the login name is not included in the user-specific component of that users Base DN. Possible values: 1. 'none': Filters any user 2. (objectcalss=person) 3. Any custom value is also acceptable, but the value should be a valid logical expression in prefix notation. Valid examples are '(object=value)', and '(&(object1=value1)(object2=value2))' .	Yes	No

group_authorization

Table 212 – Attributes for group_authorization

Name	Type	Description	Required condition	
			POST	PUT
auth_type	String	Type of group authorization. Possible values are: 1. 'No Authorization': No group authorization query 2. 'group_object': Define group authorization using LDAP group object 3. 'user_object': Define group authorization using LDAP user object	Yes	No

Authentication Realms

Name	Type	Description	Required condition	
			POST	PUT
group_membership_attribute (current key is membership_in_user_object, it will be changed in upcoming commit)	String	Group membership attribute within user/group object. Possible values: 1. 'memberOf' 2. 'member' 3. 'uniquemember' 4. A custom string can also be used here.	Yes	No
group_name_attribute	String	Attribute that contains the group name. It can be any alphanumeric value. Example: cn	Yes	No
group_filter_query	String	Query string to determine if object is a group. The value should be a valid logical expression in prefix notation. Valid examples are '(object=value)', and '(&(object1=value1)(object2=value2))' . Examples: (objectclass=groupofnames), (objectclass=groupofuniquenames), (objectclass=group) and so on.	Yes	No
is_membership_attribute_dn	Boolean	Whether group membership attribute is a DN or not.	Yes (only if auth_type is user_object).	No

Key	Value
action_auth_service_unavailable	Permit, Block
failed_auth_handling	IP, UserSubmitted

Key	Value
re_authentication	disabled, embedlinkinblockpage
basic_auth_token_ttl	Integer value for seconds
credential_encryption	0 to disable, 1 to enable
https_redirect_port	Port number(integer) Range: [1, 65535]
redirect_hostname	Host name
surrogate_timeout	Integer value for seconds
client_ip_idle_timeout	Integer value for seconds
restriction_timeout	Integer value for seconds, 0 to disable session restriction
xauth_header_based_auth	enable, disable
xauth_retain_auth_egress	enable, disable
xauth_header_mode	standard, custom
xauth_use_group_header	enable, disable
xauth_std_user_text_format	ASCII, UTF8
xauth_std_user_Binary_encoding	No Encoding, Base64
xauth_std_group_text_format	ASCII, UTF8
xauth_std_group_Binary_encoding	No Encoding, Base64
xauth_custom_user_text_format	ASCII, UTF8
xauth_custom_user_Binary_encoding	No Encoding, Base64
xauth_custom_group_text_format	ASCII, UTF8
xauth_custom_group_Binary_encoding	No Encoding, Base64
ssl_certificate	File type
ssl_certificate_key	File type
passphrase	Base 64 encoded password

Umbrella Seamless ID

Retrieving the Umbrella Seamless ID

Table 213 - Attributes for Retrieving the Umbrella Seamless ID

API	wsa/api/v3.0/web_security/umbrella_seamless_id		
Method	GET		
Parameters	None		
Request body	None		
Response	Code	Type	Description
	200 Ok	array	Details of Cisco Umbrella Seamless ID that is available and configurations such as host, ports, and organization ID.

Modifying the Umbrella Seamless ID

Table 214 - Attributes for Modifying the Umbrella Seamless ID

API	wsa/api/v3.0/web_security/umbrella_seamless_id			
Method	PUT			
Parameters	None			
Request body	Name	Type	Description	Required
	cisco_umbrella_seamless_id	Object	Details of Cisco Umbrella Seamless ID.	Mandatory
Response	Code	Type	Description	

	204 Ok	Empty body	The request has been processed successfully and the provided Seamless ID has been updated.

Performing Start Test for Umbrella Seamless ID

Table 215 - Attributes for Performing Start Test for Umbrella Seamless ID

API	/wsa/api/v3.0/web_security/swg_connectivity_test		
Method	GET		
Parameters	Name	Type	Description
	host	String	Host IP/DNS
	ports	Array of strings	List of ports (, separated) or range of ports.
Response	Code	Type	Description
	204 Ok	Empty body	The request has been processed successfully and the provided Seamless ID has been updated.

Definitions

cisco_umbrella_seamless_id schema

Table 216 - Attributes for cisco_umbrella_seamless_id schema

Name	Type	Format	Description	Remarks	PUT	
					Create	Update
swg_proxy	Object	swg_proxy_schema	Name of the policy. Unique identifier of the policy.	Not applicable for global_policy.	mandatory	optional
Org_id	String	Same as policy_name	updates the policy_name	Not applicable for global_policy.	mandatory	optional

swg_proxy_schema

Table 217 - Attributes for swg_proxy_schema

Name	Type	Description	Required	
			POST	PUT
host	String	Host IP or DNS	optional	optional

Identity Service Engine

Name	Type	Description	Required	
			POST	PUT
ports	Array of strings	List of ports (, separated) or range of ports.	optional	optional

Identity Service Engine

Retrieving the Identity Service Engine Settings

Table 218 - Attributes for Retrieving the Identity Service Engine Settings

API	wsa/api/v3.0/network/ise		
Method	GET		
Parameters	None		
Request body	None		
Response	Code	Type	Description
	200 Ok	object	Current settings of ISE.

Modifying the Identity Service Engine Settings

Table 219 - Attributes for Modifying the Identity Service Engine Settings

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

	ise_service_status	String	To enable or disable ISE feature. Accepted values: • Enable • Disable	optional
Response	primary_ise_pxgrid	Object	Primary ISE pxGrid Server configuration.	
	secondary_ise_pxgrid	Object	Secondary ISE pxGrid Server configuration.	
	wa_client_cert	Object	Web Appliance Client Certificate Settings.	
	ers_settings	Object	External Restful Service Settings.	
	sxp_status	String	To enable or disable ISE SXP feature. Accepted values: • Enable • Disable	
Response	Code	Type	Description	
	204 No Content	Empty body	The request has been processed successfully and the provided ISE parameters are updated.	

Uploading the Identity Service Engine Certificate Details

Table 220 – Attributes for Uploading the Identity Service Engine Certificate Details

API	wsa/api/v3.0/network/ise_cert			
Method	POST			
Parameters	Name	Type	Value	Required
	cert_type	String	primary_pxgrid	Mandatory
Form data	Name	Type	Remarks	Required
	file	File	file location	Mandatory
Response	Code	Type	Description	
	204 No Content	Empty body	The certificate was uploaded successfully.	

Downloading the Identity Service Engine Certificate Details

Table 221 – Attributes for Uploading the Identity Service Engine Certificate Details

API	wsa/api/v3.0/network/ise_download_cert				
Method	GET				
Parameters	Name	Type	Description	Remarks	Required
	cert_type	String	Name of cert to be downloaded	Must be one of: • primary_pxgrid • secondary_pxgrid • wa_client_uploaded • wa_client_generated • csr	Mandatory
Request body		None			
Response	Code	Type	Description		
	200 Ok	File	Certificate file with .pem extension.		

Performing Start Test for the Identity Service Engine

Table 222 – Attributes for Performing Start Test for the Identity Service Engine

API	wsa/api/v3.0/network/ise/start_test		
Method	GET		
Parameters		None	
Request body		None	
Response	Code	Type	Description
	200 Ok	object	Current settings of ISE

Definitions

primary_ise_pxgrid schema

Table 223 - Attributes for primary_ise_pxgrid schema

Name	Type	Description	Required
host	String	Host IP or hostname	optional

secondary_ise_pxgrid schema

Table 224 - Attributes for secondary_ise_pxgrid schema

Name	Type	Description	Required
host	String	Host IP or hostname	optional

Wa_client_cert schema

Table 225 - Attributes for Wa_client_cert schema

Name	Type	Description	Required
generated	Object	Object to generate wa client certificate. The current_cert will be set to "generated."	optional
current_cert	String	generated or uploaded	optional

generated schema

Table 226 - Attributes for generated schema

Name	Type	Format	Description	Remarks	Required
common_name	String	Valid name	Max 64 chars		mandatory
organization	String	Valid name	Max 64 chars	Should not have empty value if the status is enabled in the configuration.	mandatory

Identity Service Engine

Name	Type	Format	Description	Remarks	Required
org_unit	String	Valid name	Max 64 chars	Should not have empty value if the status is enabled in the configuration.	mandatory
country	String	Alphabets	Only 2 Chars	If false, the primary_server parameters should have a valid value.	mandatory
expiry_duration	Integer	Values can be 24 to 60	Number of months before expiration	This value will be converted to date and stored in the Secure Web Appliance.	mandatory
basic_constraints	String	“critical” or “non critical”			mandatory

ers_settings schema

Table 227 - Attributes for ers_settings schema

Name	Type	Format	Description	Remarks	Required
status	String	“enable” or “disable”	To enable or disable ERS.		optional
username	String	Valid ERS username format (1 to 255 chars).	ERS admin credentials.	Should not have empty value if the status is enabled in the configuration.	optional
password	String	Any string (1 to 255 chars)	ERS admin credentials: Base64 encoded password	Should not have empty value if the status is enabled in the configuration.	optional

Name	Type	Format	Description	Remarks	Required
ers_same_as_ise	boolean	true / false	If true, pxgrid server is considered.	If false, the primary_server parameter should have a valid value.	optional
primary_server	String	Hostname or IP Address	ERS primary server		optional
secondary_server	String	Hostname or IP Address	ERS secondary server		optional
port	Integer	1 - 65535			optional

Anti-Malware Reputation

Retrieving the Anti-Malware Reputation Details

Table 228 - Attributes for Retrieving Anti-Malware Reputation Details

API	wsa/api/v3.0/security_services/anti_malware_and_reputation		
Method	GET		
Parameters	None		
Request body	None		
Response	Code	Type	Description
	200 Ok	object	Object that consists details of the following: • anti_malware_scanning_services • web_reputation_services • malware_analytics_services settings

Modifying the Anti-Malware Reputation Details

Table 229 - Attributes for Modifying the Anti-Malware Reputation Details

API	wsa/api/v3.0/security_services/anti_malware_and_reputation				
Method	PUT				
Request Type	Form-data				
Request body	Key		Content Type	Description	Required
	Name	Type			
	request	text	application/json	The request body containing the settings.	Mandatory
	reputation_server_cert	file	auto	Public key for file reputation server.	Mandatory if the file reputation server is private cloud.
	reputation_server_ca_cert	file	auto	Uploaded CA certificate file for file reputation server certificate.	Mandatory if the file reputation server is private cloud and the CA is the uploaded CA.
	analysis_server_ca_cert	file	auto	Uploaded CA certificate file for file analysis server certificate.	Mandatory if the file analysis server is private cloud and the CA is the uploaded CA.
Response	Code		Type	Description	
	204 Ok		Empty body	The request has been processed successfully and the settings in the request has been updated.	

Definitions

request

Table 230 - Attributes for request of Anti-Malware Reputation Details

Name	Type	Description	Required
web_reputation_services	object	Settings for Reputation Services. Defined in web_reputation_services schema	optional
malware_analytics_services	object	Settings for Malware Analytics Services. Defined in malware_analytics_services schema .	optional
anti_malware_scanning_services	object	Settings for anti_malware_scanning_services. Defined in anti_malware_scanning_services schema .	optional

web_reputation_services schema

Table 231 - Attributes for web_reputation_services schema

Name	Type	Format	Description	Required
web_reputaion_filtering	string	Enable/disable	Enables or disables web reputation filtering. The end user license for file reputation needs to be accepted to update the setting.	optional
adaptive_scanning	string	Enable/disable	Enables or disables adaptive scanning. The end user license for file reputation needs to be accepted to update the setting. These settings cannot be updated if web_reputation_filtering is disabled.	optional

anti_malware_scanning_services schema

Table 232 - Attributes for anti_malware_scanning_services schema

Name	Type	Format	Description	Required
dvs_max_object_size_mb	integr		DVS Engine Object Scanning Limits. For multiple scanning engines, object scanning settings are applied separately to each.	optional
sophos		enable/disable	Enables or disables the Sophos engine.	optional
webroot	string	enable/disable	Enables or disables the webroot engine.	optional
webroot_threat_risk_threshold	integer		Webroot threat risk threshold. The valid range is from 51 through 100. The recommended minimum value is 90.	optional
mcafee	string	enable/disable	Enables or disables the mcafee engine.	optional
mcafee_heuristic_scanning	string	enable/disable	Enables or disables the mcafee heuristic scanning.	optional

malware_analytics_services schema

Note: Malware Analytics services requires network communication to the cloud servers on ports 32137 (for File Reputation) and 443 (for File Analysis).

Table 233 - Attributes for malware_analytics_services schema

Name	Type	Format	Description	Required
file_reputation_filtering	string	Enable/disable	Enables or disables file reputation filtering. The end user license for file reputation needs to be accepted to update the setting.	optional
file_analysis	string	Enable/disable	Enables or disables file analysis. The end user license for file analysis needs to be accepted to update the setting. This field cannot be updated if file reputation filtering is disabled.	optional
analysis_file_types	object		Defined in analysis_file_types schema.	optional
advanced_settings	object		Defined in advanced_settings schema.	optional

analysis_file_types schema

Table 234 - Attributes for analysis_file_types schema

Name	Type	Format	Description	Required
<file_group>	object		File group name. Defined in File_group schema.	optional

File_group schema

Table 235 - Attributes for File_group schema

Name	Type	Fomat	Description	Required
selected	array	<file_type_name>(.file_type)	List of file types to be selected	optional
not_selected	array	<file_type_name>(.file_type)	List of file types to be not selected	

advanced_settings schema

Table 236 - Attributes for advanced_settings schema

Name	Type	Format	Description	Required
routing_table	string	Data/Management	Routing table value can only be updated if management proxy is in use.	optional

Anti-Malware Reputation

Name	Type	Format	Description	Required
file_reputation	object		Defined in file_reputation schema.	optional
file_analysis	object		Defined in file_analysis schema.	optional
cache_expiry_period	object		Defined in Cache_expiry_period schema .	
file_analysis_threshold	object		Defined in file_analysis_threshold schema .	optional

Cache_expiry_period schema

Cache Expiry Period based on File Reputation disposition.

Table 237 - Attributes for Anti-Malware Reputation Details

Name	Type	Forrmat	Description	Required
unknown	strings	seconds	Value in between 900 to 604800	optional
malicious	string	seconds	Value in between 900 to 604800	optional
clean	string	seconds	Value in between 900 to 604800	optional

file_analysis_threshold schema

Table 238 - Attributes for file_analysis_threshold schema

Name	Type	Format	Description	Required
cloud_service	strings	Enable/disable	Enables or disables cloud service. When enabled, uses default value from cloud service.	optional
score	string		Updates file analysis threshold score. The valid range is from 1 through 100. **Note**: The range can be set if the cloud service is in disabled status only.	optional

file_reputation schema

Table 239 - Attributes for Anti-Malware Reputation Details

Name	Type	Format	Description	Required
server	object		Defined in file_reputation_server schema.	optional
proxy_settings	object		Defined in file_reputation_proxy_settings schema.	optional
heart_beat_interval	integer	seconds	Hear beat interval for file reputation server.	
query_timeout	integer	seconds	Query timeout for file reputation server.	

file_reputation_server schema

Table 240 - Attributes for Anti-Malware Reputation Details

Name	**Type**	**Format**	**Description**	**Required**
cloud_server	strings	Domain name	One among available servers. Can be public server domain name or private.	optional
server	string	Hostname or IP	Private server name. Applicable only if cloud_server is private.	optional
cert_authority	string		Applicable only if cloud_server is private. The values are: • Trusted—Use Cisco Default Certificate Authority • uploaded—Use Uploaded Certificate Authority	optional

file_reputation_proxy_settings schema

Table 241 - Attributes for file_reputation_proxy_settings schema

Name	Type	Format	Description	Required
username	strings	Valid username	Tunnel proxy username.	optional
passphrase		b64 ebcoded	Tunnel proxy passphrase.	optional
port	integer		Tunnel proxy port number.	optional
server	string	Hostname/ip	Tunnel proxy server details.	optional
relax_cert_validation	string	Enable/disable	Enables or disables certificate validation relaxation.	optional

file_analysis schema

Table 242 - Attributes for file_analysis schema

Name	Type	Format	Description	Required
server	object		Defined in file_analysis_server schema	optional
proxy_settings	object		Defined in file_analysis_proxy_settings schema	optional

file_analysis_server schema

Table 243 - Attributes for file_analysis_server schema

Name	Type	Format	Description	Required
cloud_server	strings	Domain name	One among available servers. Can be public server domain name or private.	optional
tg_servers	array	Hostname or IP	List of threat grid servers. Applicable only if cloud_server is private.	optional
cert_authority	string		Applicable only if cloud_server is private. The values are: • Trusted—Use Cisco Default Certificate Authority • uploaded—Use Uploaded Certificate Authority	optional

file_analysis_proxy_settings schema

Table 244 - Attributes for file_analysis_proxy_settings schema

Name	Type	Format	Description	Required
username	strings	Valid username	username	optional
passphrase		b64 ebcoded	passphrase	optional
port	integer		proxy port number	optional

Name	Type	Format	Description	Required
server	string	Hostname/ip	proxy server details	optional
use_file_reputation_proxy	string	Enable/disable	Reuses configuration from the file reputation proxy.	optional

General Purpose APIs

SecureX

Retrieving the Registered User Information

Table 245 - 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 246 - Attributes for Securex Ribbon Registration

API	/wsa/api/v2.0/ctr/user_info			
Method	POST			
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.	

Modifying the Registered User Information

Table 247 - 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 248 - Attributes for response_status

Name	Type	Description
Status	Integer	Response Code

error_response

Table 249 - 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 250 - 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 auth_settings	It represents a subset of auth settings. It contains enough information for associating an auth realm with identification_profile.

Definitions

auth_settings

Table 251 – 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 realm_settings	Every object in this list represents an authentication realm.
sequences	List of objects sequence_settings	Every object in this list represents a realm sequence.

realm_settings

Table 252 – 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 253 – 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 254 – 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 User_agents	It contains allowed **user agent's** string representations.

Definitions

User_agents

Table 255 – Attributes for User_agent

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

URL Categories

Retrieving URL Categories

Table 256 – 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 url_category	It represents predefined and custom url categories.

Definitions

url_category

Table 257 – Attributes for url_category

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

Time Ranges

Retrieving Time Ranges

Table 258 – 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 time_ranges	Represents a collection of time ranges that are defined in the system.

Definitions

time_ranges

Table 259 – Attributes for time_ranges

Name	Type	Description
time_ranges	List of objects time_ranges	Every element in this list represents a time_range.

time_range

Table 260 – Attributes for time_range

Name	Type	Description
time_values	List of objects time_values	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”. For more examples see, Secure Web Appliance GUI time_ranges page.

time_values

Table 261 - Attributes for time_values

Name	Type	Description
time_of_day	String (all_day) or object ({ "from": <from_value> "to": <to_value>, })	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 262 - 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 quotas	It represents predefined and custom url categories.

Definitions

quotas

Table 263 – Attributes for Quotas

Name	Type	Description
quotas	List of objects quota	It represents a list of AVC defined url categories.

quota

Table 264 – Attributes for Quota

Name	Type	Description
name	String	Name of quota
time_zone	String	Represents time zone. For example, “America/Los_Angeles”. For more examples see, Secure Web Appliance GUI quotas page.
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 Secure Web Appliance system. It is available in response only if no reset time has been selected for this quota.

Proxy Settings

Retrieving Proxy Settings

Table 265 – Attributes of Retrieving Proxy Settings

API	/wsa/api/v3.0/generic_resources/proxy_settings

General Purpose APIs

Method	GET		
Parameters	None		
Request body	None		
Response	Code	Type	Description
	200 Ok	Object proxy_setting	Minimal details about all the proxies. Whether different types of proxies are enabled or not.

Definitions

Proxy_settings

Table 266 – Attributes for Proxy_settings

Name	Type	Description
proxy_settings	Object proxy_setting	It has multiple key-value pairs which represent state of different types of proxy.

proxy_setting

Table 267 – Attributes for Proxy_setting

Name	Type	Description
web	Object ({ “status”: <enable/disable>, “mode”: <transparent/forward> })	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.

Name	Type	Description
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 268 – 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 eun_config_schema	You are provided with a dictionary representing allowed and not allowed identification methods.

Retrieving ADC Details

Table 269 – Attributes for retrieving ADC Details

API	/wsa/api/v3.0/web_security/adc		
Method	GET		
Parameters	None		
Request body	None		
Response	Code	Type	Description

	200 Ok	Objects	You are provided with ADC details such as version, applications, categories, activity regexes, and application domains.

Definitions

identification_methods

Table 270 - Attributes for identification_methods

Name	Type	Description
identification_methods	Object eun_config_schema	It is a dictionary representing allowed as well as not allowed identification methods.

identification_methods

Table 271 - Attributes for identification_method

Name	Type	Description
tui	String (Enum enable/disable)	Whether Secure Web Appliance can Transparently identify users with Auth realms or not.
authentication	String (Enum enable/disable)	Whether Secure Web Appliance can identify users with Authentication or not.
asa	String (Enum enable/disable)	Whether Secure Web Appliance can Transparently identify users with ASA or not.
ise	String (Enum enable/disable)	Whether Secure Web 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"
                ]
            },
            "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": {
```

Static Data


```
                "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"
                ]
            },
            "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": {},
            "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": {},
```

Static Data


```
            "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"
                ]
            },
            "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": {},
            "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": [
```

Static Data


```
                "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"
            ]
        },
        "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": [
```

Static Data


```
                    "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"
                ]
            }
        }
    },
    "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"
                ]
            },
            "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"
                ]
            },
```

Static Data


```
            "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": {},
            "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": {},
        "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",
```

Static Data


```
                    "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"
                ]
            },
            "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 272 provides the static list.

Table 272 – 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 Secure Web Appliance. Table 273 provides the supported MIME types:

Table 273 – 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

Static Data

Group/Category Type	Object Type
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)
Archives	StuffIt BinHex LHARC ARC ARJ
Installers	UNIX/LINUX Packages

Group/Category Type	Object Type
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 Secure Web Appliance. Table 274 provides the objects and their MIME types which can be used as the custom MIME types.

Table 274 - Custom MIME Types

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

Static Data

Category Type	Object	MIME Type
	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	
	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

Category Type	Object	MIME Type
	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
	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 Grahics Document	application/vnd.sun.xml.draw
	OpenOffice Impress Presentation	application/vnd.sun.xml.impress

Static Data

Category Type	Object	MIME Type
	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
	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

Category Type	Object	MIME Type
	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
	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

Static Data

Category Type	Object	MIME Type
	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
	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

Category Type	Object	MIME Type
	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
	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 275 lists the allowed values for malware_categories, other_categories, and file_reputation. These values are used either in **block** or **monitor** list.

Static Data

Table 275 – Allowed Values

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

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