API Compatibility Matrix

APIs Compatibility Matrix

Application	Service Version	Data Type	API	API Version
Duo	-	Account Log	Method/Endpoint: GET /admin/v1/info/summary	v1
		Activity Log	Method/Endpoint: GET /admin/v2/logs/activity	v2
		Administrator Log	Method/Endpoint: GET /admin/v1/logs/administrator	v1
		Authentication Log	Method/Endpoint: GET /admin/v2/logs/authentication	v2
		Authentication Log (Legacy v1)]	Method/Endpoint: GET /admin/v1/logs/authentication	v1
		Endpoint Log	Method/Endpoint: GET /admin/v1/endpoints	v1
		Telephony Log	Method/Endpoint: GET /admin/v2/logs/telephony	v2
		Telephony Log (Legacy v1)	Method/Endpoint: GET /admin/v1/logs/telephony	v1
		Trust Monitor	Method/Endpoint: GET /admin/v1/trust_monitor/events	v1
		Users list	Method/Endpoint: GET /admin/v1/users	v1
Secure Firewall (eStreamer)	7.4.1	-	eStreamer SDK	7.4.0
Secure Firewall (Syslog)	7.4.1	-	TCP/UDP inputs used	No API
Secure Firewall (ASA)	-	-	TCP/UDP inputs used	No API

Application	Service Version	Data Type	API	API Version
Secure Firewall (API)	7.4.1	-	Management Center REST API	7.4.1
SMA	Versions: 3.5.160 - 171	Submissions	Method/Endpoint: GET /api/v2/search/submissions	v2
XDR Incidents	1.0.107	Incidents Summary	Method/Endpoint: GET /iroh/private-intel/incident-summary/search	No API version
		Incidents	Method/Endpoint: GET /iroh/private-intel/incident/search	No API version
		User details (whoami)	Method/Endpoint: GET /iroh/profile/whoami	No API version
Cisco Multi-Cloud Defense	24.06	-	HTTP Event Collector is used	No API version
Secure Email Threat Defense	Works with any version of Email Threat Defense	Email Metadata	Method/Endpoint: POST /messages/search	v1|v2
	-	Download links	Method/Endpoint: POST /v1/logs/downloadLinks	

Application	Service Version	Data Type	API	API Version
Secure Network Analytics	7.5.1	Authentication	Method/Endpoint: POST /token/v2/authenticate	v2
		Traffic queries	Method/Endpoint: POST	v1
		Traffic queries search results	Method/Endpoint: GET	v1
		Traffic results	Method/Endpoint: GET	v1
		Filtered traffic	Method/Endpoint: GET	v1
		Alarm Report	Method/Endpoint: POST	v1
		Network Performance Report	Method/Endpoint: POST	v1
		Flow Collection Trend by FC	Method/Endpoint: POST	v1
		SAL Collection Trend	Method/Endpoint: POST	v1
		NVM Collection Trend	Method/Endpoint: POST	v1
		Todays Summary	Method/Endpoint: POST	v2
		Top Ports queries	Method/Endpoint: POST	v1
		Top Ports search results	Method/Endpoint: GET	v1

Application	Service Version	Data Type	API	API Version
		Top Ports results	Method/Endpoint: GET	v1
		Top Hosts queries	Method/Endpoint: POST	v1
		Top Hosts search results	Method/Endpoint: GET	v1
		Top Hosts results	Method/Endpoint: GET	v1
		Top Conversations queries	Method/Endpoint: POST	v1
		Top Conversations search results	Method/Endpoint: GET	
		Top Conversations results	Method/Endpoint: GET	

Application	Service Version	Data Type	API	API Version
Secure Endpoint	5.4.20241024	Fetch list of events	Method/Endpoint: GET /v1/events	v1
		Fetch list of event types	Method/Endpoint: GET /v1/event_types	v1
		Fetch list of groups filtered by name	Method/Endpoint: GET /v1/groups	v1
		Fetch list of compromises	Method/Endpoint: GET /v1/compromises	v1
		Fetch list of vulnerabilities filtered by group guid	Method/Endpoint: GET /v1/vulnerabilities	v1
		Fetch list of computers filtered by group guid	Method/Endpoint: GET /v1/computers	v1
		Fetch malware threats metric dashboard details	Method/Endpoint: GET /v1/metrics/top_malware_threats	v1
CII	-	Exchange the client credentials for an access token	OORT Public API Method/Endpoint: POST / …/api	No API version
		Register webhook	OORT Public API Method/Endpoint: mutation / registerWebhookWithApiKey	No API version
		Delete webhook	OORT Public API Method/Endpoint: mutation / unregisterWebhook	No API version
CVI	-	GZIP File with list of vulnerabilities	Method/Endpoint: GET /vulnerability_definitions/vi_data_snapshot	v1
AI Defense	-	-	HTTP Event Collector is used	No API version