



Qualys Context XDR v1.x

Release Notes

Version 1.0.2

March 23, 2022

Here's what's new in Qualys Context XDR 1.0.2!

[Newly Added Sources Tab](#)

[Quick Filters Added on the Threat Intel Tab](#)

[Updated Threat Intel Source Registration Page](#)

[Support for New Threat Intel Source Provider - Abuse.ch](#)

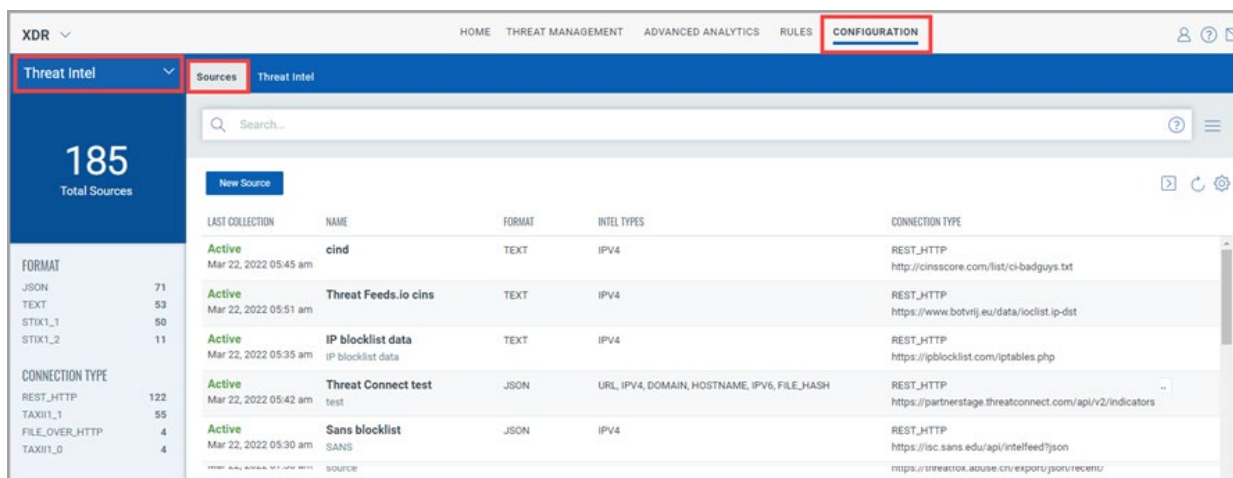
[Enhancements to the Appliances Tab](#)

[Enhancements to the Signals Tab](#)

Context XDR 1.0.2 brings you more improvements and updates! [Know more](#)

Newly Added Sources Tab

We have introduced a new **Sources** tab under **Threat Intel** configuration. You can configure a **New Source** to collect threat intel feeds from the list of available 3rd party threat intel data providers and enrich your data with additional context.

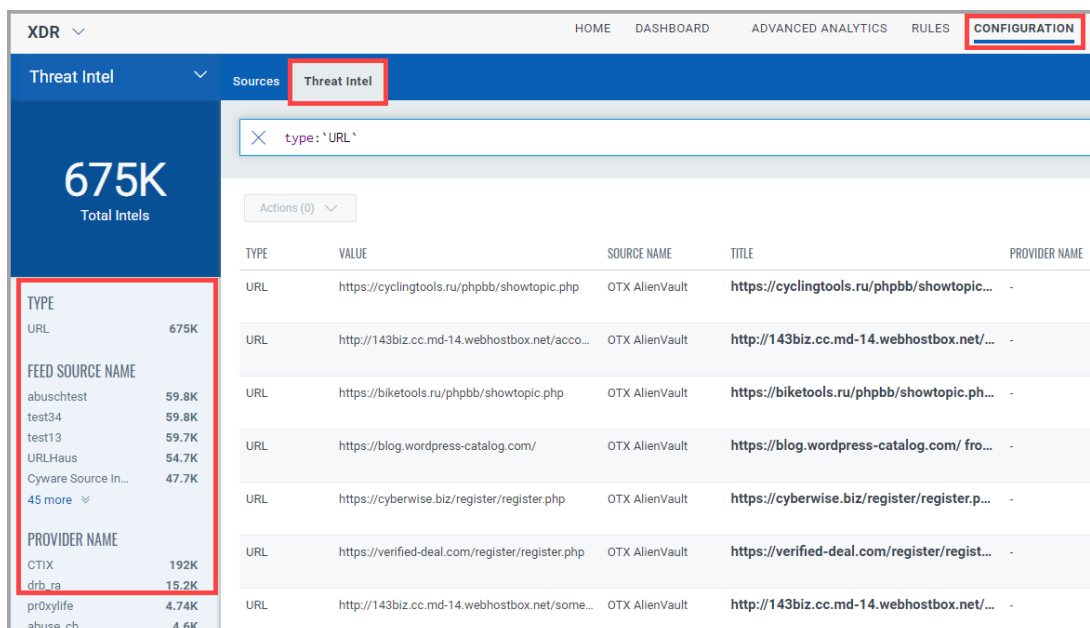


LAST COLLECTION	NAME	FORMAT	INTEL TYPES	CONNECTION TYPE
Active Mar 22, 2022 05:45 am	cind	TEXT	IPV4	REST_HTTP http://cinsscore.com/list/ci-badguys.txt
Active Mar 22, 2022 05:51 am	Threat Feeds.io cins	TEXT	IPV4	REST_HTTP https://www.botvrij.eu/data/oclist.ip-dst
Active Mar 22, 2022 05:35 am	IP blocklist data IP blocklist data	TEXT	IPV4	REST_HTTP https://ipblocklist.com/iptables.php
Active Mar 22, 2022 05:42 am	Threat Connect test test	JSON	URL, IPV4, DOMAIN, HOSTNAME, IPV6, FILE_HASH	REST_HTTP https://partnerstage.threatconnect.com/api/v2/indicators
Active Mar 22, 2022 05:30 am	Sans blocklist SANS	JSON	IPV4	REST_HTTP https://isc.sans.edu/api/intelfeed?json https://threatfox.abuse.ch/export/json/recent/

Quick Filters Added on the Threat Intel Tab

With this release, we have introduced quick filters on the **Threat Intel** tab under **Configuration**. You can view the newly added quick filters such as **Type**, **Feed Source Name**, and **Provider Name** on the left pane.

Use these filters to quickly look for data you are interested in. For example, if you need to view all logs sources from URL, just click **URL** under **Type**.



TYPE	VALUE	SOURCE NAME	TITLE	PROVIDER NAME
URL	https://cyclingtools.ru/phpbb/showtopic.php	OTX AlienVault	https://cyclingtools.ru/phpbb/showtopic...	-
URL	http://143biz.cc.md-14.webhostbox.net/acco...	OTX AlienVault	http://143biz.cc.md-14.webhostbox.net/...	-
URL	https://biketools.ru/phpbb/showtopic.php	OTX AlienVault	https://biketools.ru/phpbb/showtopic.ph...	-
URL	https://blog.wordpress-catalog.com/	OTX AlienVault	https://blog.wordpress-catalog.com/ fro...	-
URL	https://cyberwise.biz/register/register.php	OTX AlienVault	https://cyberwise.biz/register/register.p...	-
URL	https://verified-deal.com/register/register.php	OTX AlienVault	https://verified-deal.com/register/regist...	-
URL	http://143biz.cc.md-14.webhostbox.net/some...	OTX AlienVault	http://143biz.cc.md-14.webhostbox.net/...	-

Updated Threat Intel Source Registration Page

We have now simplified the registration of Threat Intelligence feeds with required details getting auto-populated based on the providers you select.

Simply, click **Configuration > Threat Intel > Sources > New Source** to configure the Threat Feed. On the **Create Feed** page, select any **Provider** (Free or Paid) from the list of options. The required details such as **Source**, **Feed Connection Type**, **Feed Format**, **URL**, etc., are pre-populated based on the selected Provider.

You need to provide the AccessId and Secretkey details of Authentication for the paid threat feed providers. You may need to provide details for fields that are not auto populated.

The screenshot displays the 'Create Feed' interface. On the left, a sidebar shows the progress: 'STEPS 1/4' with steps 1 (Basic Details), 2 (Schedule), 3 (Feed Selection), and 4 (Review & confirm). Step 1 is active. The main form is titled 'Threat Intel Source Basic Information' and contains the following sections:

- Threat Source Name ***: A text input field with the placeholder 'Give a unique name'.
- Description**: A text area with the placeholder 'Add a brief description for this rule'.
- Providers And Sources**: Two dropdown menus. The 'Provider *' dropdown is set to 'Abuse.ch'. The 'Source *' dropdown is set to 'Select'.
- Connections**: Two dropdown menus. The 'Feed Connection Type *' dropdown is set to 'Select'. The 'Feed Format *' dropdown is set to 'Select'.
- URL ***: A text input field with the placeholder 'Provide threat URL'.
- Authentication**: A dropdown menu for 'Mode of Authentication' set to 'Select'.

At the bottom of the form are two buttons: 'Cancel' and 'Test Connection and Next'.

Support for New Threat Intel Source Provider - Abuse.ch

Context XDR now supports open source threat intel data provider **Abuse.ch** for sources **URLhaus** and **ThreatFox**.

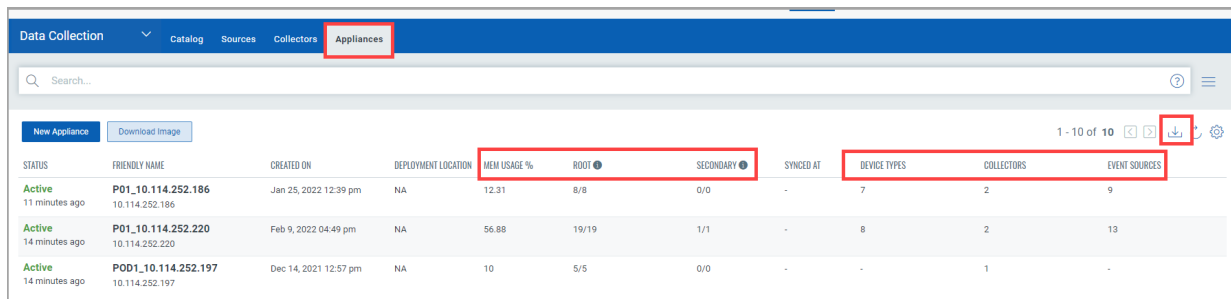
Simply, click **Configuration > Threat Intel > Sources > New Source** and select **Abuse.ch** as provider and choose the source from the available options. After successful configuration, your data is enriched with additional contextual data from **Abuse.ch** threat intel feeds.

The screenshot shows the 'Create Feed' interface for configuring a Threat Intel Source. The form is titled 'Threat Intel Source Basic Information' and is divided into several sections. On the left, a sidebar shows the progress: 'STEPS 1/4' with '1 Basic Details' selected, followed by '2 Schedule', '3 Feed Selection', and '4 Review & confirm'. The main form area includes: 'Threat Source Name *' with a text input field containing 'Give a unique name'; 'Description' with a text area containing 'Add a brief description for this rule'; 'Providers And Sources' section with two dropdown menus: 'Provider *' (set to 'Abuse.ch') and 'Source *' (showing a list with 'URLhaus' and 'ThreatFox' options, with a hand cursor pointing at the 'URLhaus' option); and 'Connections' section with two dropdown menus: 'Feed Connection Type *' (set to 'Select') and 'Feed Format *' (set to 'Select').

Enhancements to the Appliances Tab

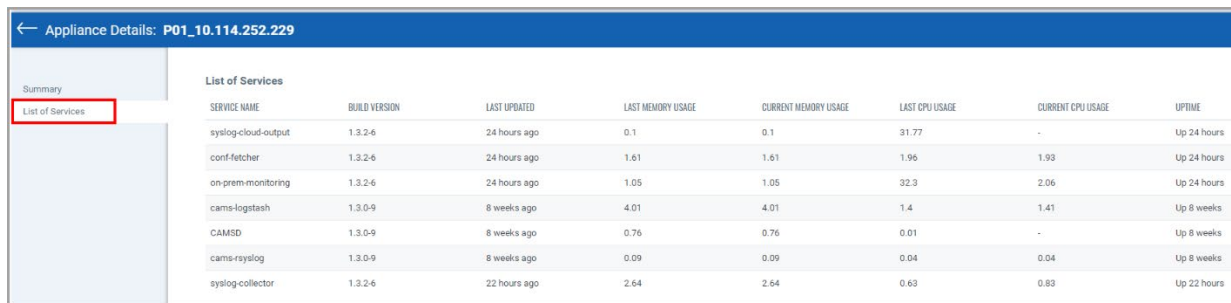
The **Appliances** tab under **Configuration** now displays additional details such as **Mem Usage**, **Root**, **Secondary**, **Device Types**, **Collectors**, and **Event Sources** on the **Appliances** tab of Configuration.

You can also download/export data on the page by simply clicking the download icon . Choose the available formats and click **Download**.



STATUS	FRIENDLY NAME	CREATED ON	DEPLOYMENT LOCATION	MEM USAGE %	ROOT	SECONDARY	SYNCED AT	DEVICE TYPES	COLLECTORS	EVENT SOURCES
Active 11 minutes ago	P01_10.114.252.186 10.114.252.186	Jan 25, 2022 12:39 pm	NA	12.31	8/8	0/0	-	7	2	9
Active 14 minutes ago	P01_10.114.252.220 10.114.252.220	Feb 9, 2022 04:49 pm	NA	56.88	19/19	1/1	-	8	2	13
Active 14 minutes ago	P001_10.114.252.197 10.114.252.197	Dec 14, 2021 12:57 pm	NA	10	5/5	0/0	-	-	1	-

You can now view the list of services running on the selected appliance. Simply click **Configuration > Data Collection > Appliances** and click **View Details** option from the quick actions menu to view the **List of Services** running on the selected appliance.



SERVICE NAME	BUILD VERSION	LAST UPDATED	LAST MEMORY USAGE	CURRENT MEMORY USAGE	LAST CPU USAGE	CURRENT CPU USAGE	UPTIME
syslog-cloud-output	1.3.2-6	24 hours ago	0.1	0.1	31.77	-	Up 24 hours
conf-fetcher	1.3.2-6	24 hours ago	1.61	1.61	1.96	1.93	Up 24 hours
on-prem-monitoring	1.3.2-6	24 hours ago	1.05	1.05	32.3	2.06	Up 24 hours
cams-logstash	1.3.0-9	8 weeks ago	4.01	4.01	1.4	1.41	Up 8 weeks
CAMSD	1.3.0-9	8 weeks ago	0.76	0.76	0.01	-	Up 8 weeks
cams-rsyslog	1.3.0-9	8 weeks ago	0.09	0.09	0.04	0.04	Up 8 weeks
syslog-collector	1.3.2-6	22 hours ago	2.64	2.64	0.63	0.83	Up 22 hours

Enhancements to the Signals Tab

We have newly introduced the following details on the Signals tab under Threat Management.

- **Product:** You can now filter Events from various products such as EDR, CXDR, etc.
- **Additional Details:** You can view additional details for specific signals.
- **Asset:** You can view the summary details of the selected asset.

XDR

HOME DASHBOARD THREAT MANAGEMENT ADVANCED ANALYTICS RULES CONFIGURATION

Threat Management

Threat Hunting Signals Events DLQ

6.04K
Total Signals

TYPE

CORRELATION 5.76K

EDR 285

TACTIC

Privilege Escalation... 694

Initial Access 465

Credential Access 299

Execution 282

Impact 235

2 more

Q Search...

Last 7 Days

1 - 50 of 6040

AGE	RISK SCORE	RULE NAME	TYPE	PRODUCT	SOURCE	CRITICALITY	SOURCE IP	USER	ASSET	ADDITIONAL DETAILS	RESPONSE
3 hours ago Mar 23, 2022 04:58 pm	7	SignalSuppression_06_03	3s	CXDR	Medium	1.2.3.4	-	64	sourceips: 1.2.3.4 destinationips: 1.2.3.4	0	
3 hours ago Mar 23, 2022 04:58 pm	7	SignalSuppression_06_03	3s	CXDR	Medium	1.2.3.4	-	64	sourceips: 1.2.3.4 destinationips: 1.2.3.4	0	
3 hours ago Mar 23, 2022 04:58 pm	7	SignalSuppression_06_03	3s	CXDR	Medium	1.2.3.4	-	64	sourceips: 1.2.3.4 destinationips: 1.2.3.4	0	
4 hours ago Mar 23, 2022 04:20 pm	7	SignalSuppression_06_03	3s	CXDR	Medium	1.2.3.4	-	64	sourceips: 1.2.3.4 destinationips: 1.2.3.4	0	
4 hours ago Mar 23, 2022 04:20 pm	7	SignalSuppression_06_03	3s	CXDR	Medium	1.2.3.4	-	64	sourceips: 1.2.3.4 destinationips: 1.2.3.4	0	

We have also enhanced the following changes on the UI:

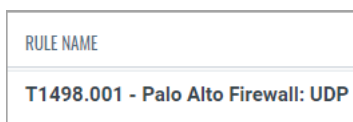
- **Age** details is moved to first column.
- Shortened **Rule Name** if the Mitre information is not available



The table shows a 'RULE NAME' column with the value 'Suspicious Mutex'.

RULE NAME
Suspicious Mutex

- If Mitre information is available, then the **Rule Name** shows as `tactic_id - technique_name` format.



The table shows a 'RULE NAME' column with the value 'T1498.001 - Palo Alto Firewall: UDP'.

RULE NAME
T1498.001 - Palo Alto Firewall: UDP

Issues Addressed

- We fixed an issue where if the TTL is not selected for Signal/Alert Suppression, then the maximum default value is set to 7 days as default.