



# Qualys Context XDR v1.x

## Release Notes

Version 1.0.5

May 31, 2022

Here's what's new in Qualys Context XDR 1.0.5!

[New Definition Column Added for Special Objects](#)

[Enhancements to the Appliance Details](#)

[Additional Fields Added for Windows Events ID 4688](#)

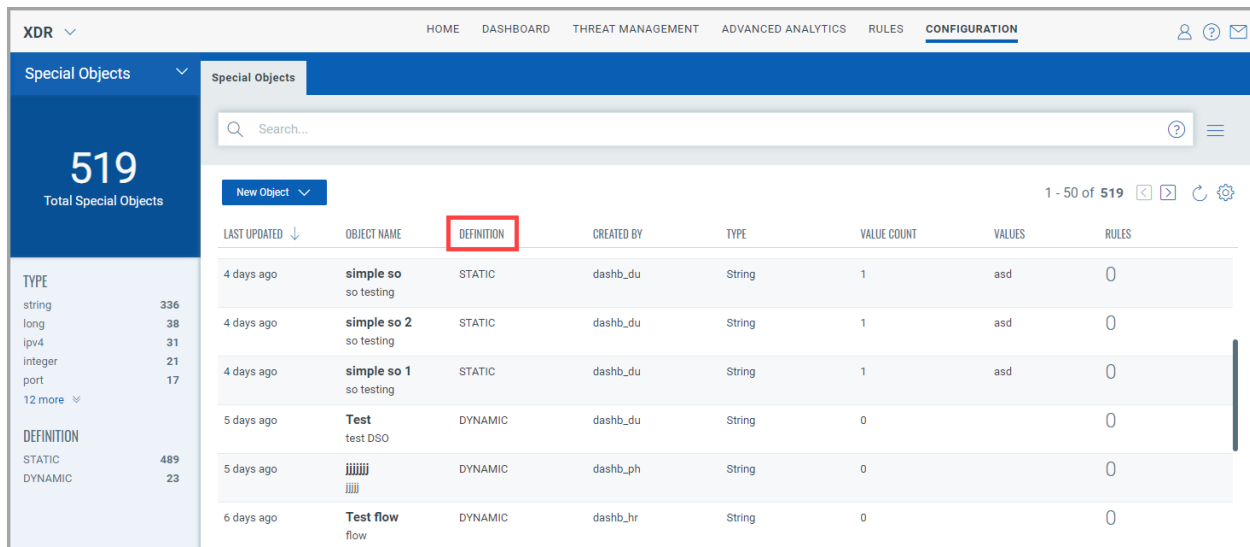
Context XDR 1.0.5 brings you more improvements and updates!

## New Definition Column Added for Special Objects

With this release, we have now added a **Definition** column for Special Objects page, where you can view the type of object: **Static** or **Dynamic**.

- **Static** - Allows you to configure the values/attributes that are controlled from the UI.
- **Dynamic** - Allows you to configure multiple rules that can add or remove fields/values from the special object.

Navigate to **Configuration > Special Objects** and you view the **Definition** column added. You can click **New Object** and select Static or Dynamic type of special object you want to create. Then, enter the required details for the special object to be created. For more information, you can refer to the online help.



LAST UPDATED ↓	OBJECT NAME	DEFINITION	CREATED BY	TYPE	VALUE COUNT	VALUES	RULES
4 days ago	simple so so testing	STATIC	dashb_du	String	1	asd	0
4 days ago	simple so 2 so testing	STATIC	dashb_du	String	1	asd	0
4 days ago	simple so 1 so testing	STATIC	dashb_du	String	1	asd	0
5 days ago	Test test DSO	DYNAMIC	dashb_du	String	0		0
5 days ago	iiiiiii	DYNAMIC	dashb_ph	String	0		0
6 days ago	Test flow flow	DYNAMIC	dashb_hr	String	0		0

### Notes:

- Under **Special Objects**, sorting of data for the **Definition** column needs enhancement.
- The Special Object search results may include events with Null/Blank values for Dynamic Special Objects.
- For Dynamic Special Objects, Search functionality for **Associated Rules** tab may not display accurate results.

## Enhancements to the Appliance Details

We have newly added MTU and NIC details under Summary page of an Appliance.

- **MTU** - Maximum Transmission Unit (MTU) is the maximum size of the packet that can be transmitted from a network interface.
- **NIC** - Network Interface Controller (NIC) is a hardware component which a device or machine can be connected over a network.

You can navigate to **Configuration > Data Collection > Appliances** tab. Select any appliance and click **View Details** from the quick actions menu. Then, you can view the **Summary** page for the **MTU** and **NIC** details.

← Appliance Details: **DataMonitoring\_Test\_Appliance**

Summary  
List of Services

4 Collectors      20 Event Sources

**Lookup code**  
ff201188-a4da-4b14-9ada-303b0797217a ⓘ

**General Details**

Description:	
Activation Key:	8681194508
Status:	<b>Active</b>
Appliance ID:	3c6770d2-f2cb-4cd5-8952-869ca03ee6cf
Memory Usage (%):	43.18
Current Root Disk Usage (%):	40
Last Root Disk Usage (%):	40
Current Secondary Disk Usage (%):	1
Last Secondary Disk Usage (%):	1
Last updated on:	a few seconds ago
Created on:	6 months ago
Deployment Location:	Pune
Ipv4 Address:	10.44.150.51
Host Name:	CAMSD
Name Servers:	10.44.148.41,10.44.148.55
<b>MTU:</b>	<b>1500</b>
<b>NIC:</b>	<b>6</b>

We have also added new columns for **Status**, **Network IO**, and **Block IO** details on List of Services page of an Appliance.

- **Status** - Displays the current status of a service.
- **Network IO** - Displays the total bytes received and transmitted over the network by the corresponding container.
- **Block IO** - Displays the number of bytes written/read from your container to the disk.

Simply, navigate to **Configuration > Data Collection > Appliances** tab. Select any appliance and click **View Details** from the quick actions menu. Then, click **List of Services** to view the details of newly added columns.

← Appliance Details: P01\_10.114.252.235

Summary	List of Services								
List of Services	STATUS	SERVICE NAME	BUILD VERSION	LAST UPDATED	MEMORY	CPU	UPTIME	NETWORK IO	BLOCK IO
	Running	cams-rsyslog	1.4.0-7	6 days ago	0.06 / 0.06	0.03 / 0.04	Up 6 days	487MB / 9.38MB	19.3MB / 2.43MB
	Running	syslog-collector	1.3.4-6	3 hours ago	1.57 / 1.57	0.57 / 0.4	Up 3 hours	0B / 0B	0B / 10.2MB
	Running	syslog-cloud-output	1.3.4-6	3 hours ago	0.06 / 0.05	0.01 / -	Up 3 hours	0B / 0B	0B / 0B
	Running	cams-logstash	1.4.0-7	6 days ago	1.58 / 1.57	0.89 / 1.02	Up 6 days	206MB / 251MB	89.8MB / 552MB
	Running	CAMSD	1.4.0-7	6 days ago	0.54 / 0.62	0.26 / 75.56	Up 6 days	0B / 0B	20.2GB / 622MB
	Running	ad-collector	1.3.4-6	2 hours ago	2.79 / 2.24	5.33 / 2.46	Up 2 hours	323kB / 232kB	0B / 336kB
	Running	on-prem-monitoring	1.3.4-6	3 hours ago	2.73 / 2.7	0.81 / 5.32	Up 3 hours	447kB / 539kB	0B / 635kB
	Running	conf-fetcher	1.3.4-6	3 hours ago	2.3 / 2.26	0.88 / 1.03	Up 3 hours	634kB / 330kB	0B / 483kB

## Additional Fields Added for Windows Events ID 4688

With this release, you can view the new event values added such as command, destinationProcess, ProcessId, WinLogMandatoryLabel, winLogTargetLogonId, and winLogTokenElevationType fields for Windows Events ID 4688.

You can navigate to **Threat Management > Events** tab. Then, use search tokens filter with 'deviceType:`Operating System` and externalId:'4688' and destinationProcess:\*' to view the Windows OS events. Click **Events Values** to view the newly added fields.

Threat Management | Threat Hunting | Signals | **Events** | DLQ

5 Total Events

DEVICE TYPE: Operating System 5

Search: deviceType:`Operating System` and externalId:'4688' and destinationProcess:\*

Apr 28, 2022 03:50 PM 19 days ago

action: Process Creation collectorId: 3fa85f64-5717-4562-b3fc-2c963f66afa6 collectorReceivedTime: Apr 1, 2022 01:01 AM command: C:\\Windows\\System32\\WScript.exe deviceEventId: Microsoft-Windows-Security-Auditing:4688 deviceHost: DESKTOP-HRS9VRH deviceModel: Windows deviceName: DESKTOP-HRS9VRH deviceSeverity: eventId: 17fa5cde-a966-44f5-a261-1b68744aa42c eventName: A new process has been created eventTime: Apr 28, 2022 03:50 PM eventType: Audit Success externalId: 4688

EVENT VALUES (31)	JSON VIEW	RAW MESSAGE
action		Process Creation
collectorId		3fa85f64-5717-4562-b3fc-2c963f66afa6
collectorReceivedTime		Apr 1, 2022 01:01 AM
command		C:\\Windows\\System32\\WScript.exe
destinationProcess		Registry
destinationUserId		S-1-0-0
deviceEventId		Microsoft-Windows-Security-Auditing:4688
deviceHost		DESKTOP-HRS9VRH
deviceModel		Windows

Search: deviceType:`Operating System` and externalId:'4688' and destinationProcess:\*

Options

guid	54849625-5478-4994-a5ba-3e3b0328c30d
osDetails	19044.1586
outcome	success
processId	0x4
tags	Windows
timezone	UTC
version	10.0
winlogComputerName	DESKTOP-HRS9VRH
winLogMandatoryLabel	S-1-16-16384
winlogSubjectLogonId	0x3e7
winlogSubjectSid	S-1-5-18
winLogTargetLogonId	0x0
winLogTokenElevationType	%1936