Qualys Context Extended Detection and Response (XDR)
Getting Started Guide

June 6, 2023
# Table of Contents

**About this Guide** ................................................................................................................. 4  
About Qualys .......................................................................................................................... 4  
Qualys Support ..................................................................................................................... 4  

**About XDR** ............................................................................................................................ 5  

**Get Started with XDR** ........................................................................................................ 6  
Set Up Qualys Cloud Agents ................................................................................................... 7  
Set Up Third-party Data Collection ......................................................................................... 7  

**Threat Management** ............................................................................................................ 8  
Threat Hunting Tab .................................................................................................................. 9  
Signals Tab .................................................................................................................................. 10  
Events Tab ................................................................................................................................ 11  

**Rules** ..................................................................................................................................... 13  
Create a New Rule ................................................................................................................... 13  
Activate Rules .......................................................................................................................... 13  
Export/Import Rules ................................................................................................................. 15  
View Configured Rules ............................................................................................................ 16  

**Advanced Analytics** .......................................................................................................... 19  
Overview Tab .......................................................................................................................... 19  
Users Tab ................................................................................................................................. 20  

**Configuration** ..................................................................................................................... 24  
Configure Data Collection ...................................................................................................... 24  
Configure Response Templates ............................................................................................... 28  
Configure Special Objects ...................................................................................................... 28  
Configure Threat Intel ........................................................................................................... 29  
Configure a Cloud Agent Profile ............................................................................................ 29  
Configure User Lists ............................................................................................................... 29
About this Guide

Thank you for your interest in Qualys Context Extended Detection and Response (XDR).
Qualys Context Extended Detection and Response (XDR) is a next-gen Security Analytics and Incident Response solution that natively integrates and correlates security telemetry across the security stack for an end-to-end platform.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/
About XDR

Qualys Context Extended Detection and Response (XDR) enables you to collect event data from various assets by leveraging the qualys cloud agents. You can also configure XDR to ingest 3rd party logs to extend detection. Qualys uses several algorithms in the background to correlate the data coming from these varying sources to offer you a single-pane view of your security posture.

A typical organization deploys several products and applications like firewall, Intrusion Prevention Systems (IPS), vulnerability management systems, EDRs, and a plethora of other systems to secure their organization against cyber threats. Qualys Context XDR leverages the infrastructure existing for other Qualys products like the cloud agents and other sensors to ingest real-time telemetry from all of these systems and collate it all on the qualys cloud platform. Qualys Context XDR then integrates this with the data already existing on the Qualys cloud platform from different qualys products to offer interesting insights out-of-the-box on the XDR dashboards.

Qualys splits the enabling process over several phases as listed below:

To know more information on above phases, refer to the Enablement Guides in the Online Help.
Get Started with XDR

With Qualys Context XDR, you can collect event data from various assets by leveraging the qualys cloud agents. You can also configure XDR to ingest 3rd party logs to extend detection. Qualys uses several algorithms in the background to correlate the data coming from these varying sources to offer you a single-pane view of your security posture.

Follow the instructions in these sections to configure Qualys Context XDR to collect data:

Set Up Qualys Cloud Agents
Set Up Third-party Data Collection

After successfully setting up Qualys Context XDR, you will be able to:

View events and signals from the configured data sources. See the Threat Management section for more information.

Configure Qualys Context XDR to use real-time threat intelligence and machine learning to automatically prioritize vulnerabilities. See the Rules section for more information.

Qualys Context XDR Dashboards

Qualys Context XDR integrates with Unified Dashboard (UD) to bring information from all Qualys applications into a single place for visualization. UD provides a powerful, new dashboard framework along with platform service that will be consumed and used by all other products to enhance the existing dashboard capabilities.

Qualys Context XDR offers several dashboards out-of-the-box. Each dashboard displays a short description of the information it offers. You can also easily configure widgets to pull information from other modules/applications and add them to your dashboard. You can also add as many dashboards as you like to customize your view.
Set Up Qualys Cloud Agents

Qualys Context XDR allows you to leverage existing qualys cloud agents to collect event logs from assets on which agents are deployed. You can also deploy fresh agents and configure them to collect logs for XDR.

**Note:** If you do not have qualys cloud agents deployed already, follow the instructions in the qualys cloud agent getting started guide or refer the online help to install and deploy cloud agents on your assets.

Follow these steps to configure existing qualys cloud agents to collect event logs:

1. Enable XDR via configuration profile
2. Activate Cloud Agents for XDR
3. Configure a Cloud Agent Profile

To know more information on above steps, refer the Online Help.

Set Up Third-party Data Collection

Qualys Context XDR allows you to collect logs from third-party firewalls, enabling detection across multi-vendor environments while integrating third-party firewall alerts into a unified incident view.

we will walk you through the steps required to ingest data from third-party devices into Qualys Context XDR. The setup process has three main steps:

1. Provision an appliance
2. Deploy a collector
3. Configure log sources

To know more information on above steps, refer the Online Help.
threat Management

Qualys Context XDR ingests logs from different sources and events from these logs are displayed on the threat management tab. All events from these logs are displayed under the events sub-tab. The signals sub-tab displays the various alerts raised by Qualys Context XDR based on the rules you have configured. The threat hunting sub-tab offers a summarized view of all signals raised by Qualys Context XDR.

Click each link below to learn more about each tab:

Events Tab
Signals Tab
Threat Hunting Tab
The threat hunting tab summarizes the details from the signals and events tab on a dashboard. This dashboard offers a single-pane view of your threat hunting posture. Use the time period filter on the top-left to focus on data related to a particular time frame.

**Signals breakdown by mitre attack stages** - This widget displays the different mitre attack stages and the number of signals generated per stage.

**Top 10 signals by mitre tactics** - This widget displays the top 10 types of mitre tactics signals that were generated.

**Top 10 triggered/notable users by signals count** - This widget displays the top 10 users in your organization with the most number of signals.

**Top 10 triggered/notable assets by signals count** - This widget displays the top 10 assets in your organization that have triggered the most signals.
Signals Tab

The signals tab displays all the alerts raised by Qualys Context XDR during the set time period, based on the rules you have activated. If you have not activated rules yet, see the Rules section to activate them.

For each signal triggered, the signals tab displays the risk score that is assigned based on several factors including the criticality of the rules triggering it. The signals tab also displays the notifications sent out in response to each signal under the response column. Each the number under the response column to view all the notifications sent.

For each signal triggered, you can also view detailed information about each signal and the details of the asset triggering it. Use the quick actions menu beside each signal to view the signal details and asset details page.

Note: Asset details are populated only when Qualys Context XDR associates the signal to an asset.

Use Qualys QQL on this page to search for specific signals. For a complete list of QQL tokens supported on this page, click here.

You can also use the quick filters from the left pane to narrow down to specific signals.
Events Tab

Qualys Context XDR ingests logs from all the configured data sources on a continuous basis. Events from these data sources are displayed on the events tab.

Let’s take a quick look at the information this page offers:

Event Details

The event details section displays the details of all events received from the data sources. Each event has its details categorized under two buckets:

- Event Values – Displays information as received from the data source
- Qualys Enriched Values – Displays the information that Qualys was about to enrich based on the correlations with data received from other integrations.

For example, if you have integrated your organization’s Active directory data with Qualys Context XDR, Qualys Context XDR attempts to correlate this data with the event. Similarly, using the IP address received on an event log, Qualys Context XDR enriches the event details with the asset details related to this IP.

Click the arrow in the event header to view details.
Search
Use Qualys QQL to search for specific events on this page. For information on how to search, see the How to search topic.

Time Filter
Use the time-filter dropdown to view events that occurred with a time range. You can define your own time range or choose a pre-defined time frame.

Events Bar Chart
The Events bar chart displays a graph of the number of events that occurred during the defined time range. The bar chart helps visualize the events data and identify patterns for when events occur.

Click each bar on the graph to get a focused view on the events that occurred during that time. Use the time-filter dropdown to reset the graph.

Enriched: Displays all the Enriched events.

Unparsed: Displays all the Unparsed events.

Quick Filters
Use the quick filters available in the left pane to view specific events.
Rules

Qualys Context XDR uses rules to analyze events from different data sources and trigger alerts. Qualys offers several out-of-the-box rules that are built on a variety of different MITRE tactics and techniques. For each rule, you can also define an appropriate action when triggered.

With Qualys Context XDR, you can either:

Create a New Rule
Activate Rules
Export/Import Rules
View Configured Rules

Create a New Rule

When you identify a threat, you can define specific rules for which you want Qualys Context XDR to raise alerts. Machine learning detection techniques can continuously refine rules to improve detection effectiveness and minimize false positives.

To know more about the steps to create a new rule, refer the Online Help.

Activate Rules

Qualys Context XDR offers an extensive out-of-the-box library of rules for you to leverage. These rules are built on a variety of MITRE tactics and techniques.

On the Qualys Context XDR UI, navigate to Rules > Rule Library to view all the pre-configured rules. The rule library page displays the MITRE tactic and technique used for each rule along with its criticality.
To activate a rule from the Rule Library, use the **Quick Activate** option from the corresponding **Quick Actions** menu on the Rule Library page.

To view the details of a rule, use the **View details** options from the corresponding quick actions menu. The rule details page describes each rule in detail. It also displays the signal condition in natural language for easy understanding. To activate a rule from this page, click **Quick Activate** from the Actions menu on the top-right corner.

Qualys Context XDR allows you to build your own rules by leveraging existing rules from the Rule Library. To configure an existing rule from the Rule Library, refer the **Online Help**.
**Export/Import Rules**

Qualys Context XDR allows you to configure new rules and export them for circulation. Follow these steps to export an existing rule:

1. First, on the Qualys Context XDR UI, navigate to the **Rules** sub-tab under the **Rules** tab.

![Image 1](image1.png)

2. From the Rule page, click the **Export rule** option from the rule’s **Quick Actions** menu.

![Image 2](image2.png)

3. On the Confirmation pop-up, click **Export** to export the rule to your local machine as a JSON file.

You can import this exported JSON file to automatically use a rule in other subscriptions. To import a rule in JSON format, follow these steps:

1. First, on the Qualys Context XDR UI, navigate to the **Rules** sub-tab under the **Rules** tab.

2. On the Rules sub-tab, click **Import Rule**.

3. On the Import Rule pop-up, drag and drop, or browse and upload the rule in JSON format.

4. Finally, click **Import** to import the rule. The imported rule is displayed on the Rules sub-tab in the Active state.
View Configured Rules

Navigate to the Rules > Rules sub-tab to view all your configured rules. The table on this page displays information around each configured rule.

Use this page to:

- Create a new rule. See the Create a New Rule section for more information.

- View the status of each rule. A rule can be in the Active or in the Inactive state. Use Activate/Deactivate options from the Quick Actions menu next to a rule to toggle between the Active and Inactive states.

- View details of each rule. Use the View details option from the rule’s Quick Actions menu to view the rule details.
- Use qualys QQL tokens to search for specific rules. Refer the Online Help to see complete list of QQL tokens that you can use on this page.

- View the signals associated with each rule. Click the signal count associated with a rule to view the entire list of signals.

- Delete the signals associated with a rule. Use the delete signals for this rule option from the quick actions menu next to a rule to delete its associated signals.

- Import/export a rule. See the Export/Import Rules section for more information.

- Delete a configured rule. Use the delete rule option from the quick actions menu next to a rule to delete it.

- Filter rule using the quick filters. Use the quick filter options from the left to quickly view the rules you are interested in. The filters are categorized under the following buckets:
  + **Tactic** – Use filters under this bucket to filter rules by their associated MITRE tactic.
  + **Technique** – Use filters under this bucket to filter rules by their associated MITRE technique.
  + **Status** – Use filters under this bucket to view rules in the Active or Inactive state.
  + **Criticality** – Use filters under this bucket to view rules by their criticality.
  + **Log Sources** – Use filters under this bucket to view rules by their log sources. For example, view rules associated with all firewall sources.
Advanced Analytics

The advanced analytics tab correlates your user data from active directory with the triggered signals and summarizes your user activity and risk score.

The Advanced Analytics tab has 2 sub-tabs: Click each tab to learn more.

Overview Tab

Users Tab

Overview Tab

The advanced analytics overview tab is a summary/dashboard that lists the users with the highest risk score. For each user, the risk is calculated based on the risk score of the user’s associated signals.

To view the signals associated with each user, click the number under the Signals column. Click each user to view the user details. For more information, see the Users Tab section.

You can add multiple widgets on this page that focus on smaller user groups in your organizations by creating user lists. To add widgets, see the Configure User Lists section.
Users Tab

The users tab displays the list of all users received from active directory and their risk scores. For each user, the risk is calculated based on the risk score of the user’s associated signals.

To view the details of each user, click view details from the quick actions menu.

The user details page offers several details about the user under four interactive widgets. Use the tab-level time range filter or the widget-level time range filter to view data accordingly.

Click each tab listed below to learn more about it.

General Details
Risk Score Trend
Timeline
Additional Details
**General Details**

The general details tab displays a summary of the signals triggered for the user:

- **By Mitre Attacks** - The different signals triggered for the user based on the type of Mitre attack used by the signal
- **Signals Timeline** - A timeline for when each signal was triggered
- **By Signals** - The list of signals that were triggered for the user
- **By Rules** - The list of rules that triggered the signals for the user
Risk Score Trend

The risk score trend tab displays a timeline of how the risk score moved with each signal triggered over the defined time range.

The tab also displays two widgets that show the user’s internal and external activities during the time period.

Timeline
The timeline tab displays all the signals displayed over the specific time period. Use the filters at the top-right corner of the graph to narrow the time period or filter by specific Mitre tactics.

Click each time frame in the table below the graph to view details of the signals and the events that occurred during that time frame.

### Additional Details

The additional details tab lists the other details captured about the user.

The additional details tab lists the other details captured about the user.
Configuration

The Qualys Context XDR Configuration overview screen summarizes your configurations for XDR on a single dashboard.

**Configure Data Collection** - Displays a summary of the appliances, collectors, and event sources configured. It also displays the total number of event sources in the catalog available for you to configure.

**Configure Response Templates** - Displays the number of response templates configured for each response supported.

**Configure Special Objects** - Displays the total number of special objects configured. It also displays the objects created and updated in the last 24 hours.

**Configure Threat Intel** - Displays a count of the Threat Intel source feeds configured.

**Configure a Cloud Agent Profile** - Displays a count of the log collection profiles configured for Qualys Context XDR.

**Configure User Lists** - Displays a count of the user lists configured for Qualys Context XDR.

*Note:* Installing **Sysmon** with Qualys XDR is recommended.

**Configure Data Collection**

The data collection configuration page consists of 4 tabs.

**Catalog**

**Sources**

**Collectors**

**Appliances**
Catalog

The catalog tab displays a list of all third-party data sources and the type of collectors Qualys Context XDR supports. Toggle between sources and collectors to view supported data sources and collectors.

For each supported data source, the catalog page also displays the count of sources you have already configured.

**Note:** The Catalog page also displays the data sources qualys is currently working on supporting and the data sources for which you have requested support.
Sources

The sources tab displays all the configured event sources. The page also displays the number of sources configured based on the supported log formats. Click each format tile on the top of the page to quickly filter configured event sources of a specific log format.

For information on configuring a new event source, refer to the configuring log sources section in the Online Help.

Use the quick filters on the left or Qualys QQL to search for specific data sources. For information on the supported QQL tokens on this page, click here.

For each configured event source, use the Quick Actions menu to:

View Details – Displays a summary of the configured event source. The source details page displays information like who configured the source and when. It also displays the date it was modified, if any. On the right pane, the page also displays a summary of the collector the source is configured on. Click the view all details link to view details of the collector.

View Events – Navigates to the Threat Management > Events to display all the events received through this event source.

Delete – Deletes the configured event source

Edit – Allows you to modify the configured event source
Collectors

The collectors tab displays all the configured collectors. For information on deploying a new collector, refer the deploying a collector section in the online help.

Use the quick filters on the left or Qualys QQL to search for specific collectors. For information on the supported QQL tokens on this page, click here.

For each configured collector, use the Quick Actions menu to:

**View Details** – Displays a summary of the configured collector. The collector details page displays information like who configured the source and when, along with the data collection details. The collector details page also displays the number of event sources configured on it. Click the Event Sources link to view a list of the event sources.

**Edit** – Allows you to modify the configured collector

**Refresh** – Refreshes the collector

**Delete** - Deletes the configured collector. When deleted, Qualys Context XDR stops ingesting data for any of the event sources configured on this collector.
Appliances

The appliances tab displays all the configured appliances. For information on deploying a new appliance, refer to deploying an appliance section in the online help.

Use Qualys QQL to search for specific appliances. For information on the supported QQL tokens on this page, click here.

For each configured appliance, use the Quick Actions menu to:

**View Details** – Displays a summary of the configured appliance. The appliance details page displays information like the appliance's IP address, Host name etc. The logs tab of the appliance details page displays a list of the logs received on the appliance.

**Delete** – Deletes the configured appliance

Configure Response Templates

Qualys Context XDR allows you to configure response templates for different types of responses based on the signals triggered. These responses can be sent over an email, or posted to Slack, or through a pager notification.

You can define multiple templates for each application and then use these templates as a response to rules.

See the Create a New Rule for more information on using the response templates in rules.

Configure Special Objects

A special object is basically an 'array' of sorts which can be used when defining rules. When you create a special object, you can use the object in multiple rules without having to repeat the list in every rule.

Refer the Online Help for the steps to configure a special object.
Configure Threat Intel

Qualys Context XDR offers the ability to enrich your data by integrating it with different 3rd party threat intelligence feeds. Qualys Context XDR correlates the event logs ingested from various sources with these threat feeds to offer interesting insights into your security data.

Refer the Online Help for steps to configure a threat intel feed.

Configure a Cloud Agent Profile

After you have enabled XDR via a configuration profile and activated agents for XDR, you now need to create a Cloud Agent Profile to define what logs you want to collect from hosts, where you want to collect them, and the assets you want to collect from.

Refer the Online Help for steps to configure a cloud agent profile.

Configure User Lists

Qualys Context XDR allows you to create smaller user groups to focus on risks associated with these users. For example, you might want to focus on the users in a certain department and monitor the scores around those users.

Refer the Online Help for steps to configure a new user list.