Endpoint Detection and Response

Onboarding Guide

June 25, 2021

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

Introduction

Qualys Endpoint Detection and Response (EDR) solution actively focuses on endpoint activity to detect attacks. EDR expands the capabilities of the Qualys Cloud Platform to deliver threat hunting and remediation response. EDR detects suspicious activity, confirms the presence of known and unknown malware, and provides remediation response for your assets.

Since this active monitoring and data collection is in real-time, EDR requires constant inspection, scanning, and data collection. EDR mandates specific system requirements for hardware and software compatibility.

This guide outlines the minimum hardware and software requirements for deploying EDR. Requirements might vary based on system utilization. We recommend that you carry out a performance pilot tryout before a full scale-out.

System Requirements

Software Requirements

Incompatibility with other Security Software

Qualys EDR is incompatible with other security EDR software. Running the Qualys EDR agent simultaneously with any other EDR security software on an asset might affect their operation and cause major problems with the system performance. Before installing the Qualys EDR agent, you must uninstall any other existing EDR software. Qualys EDR will not be able to provide support if other EDR software is installed.

Whitelist Requirements

Qualys EDR can co-exist with other antimalware software. However, admins should whitelist appropriate processes of the current antimalware software to avoid any false positive detection. Failing to whitelist processes might affect your operation and cause problems with the system performance. You may also review your internal tools and if required, whitelist them.

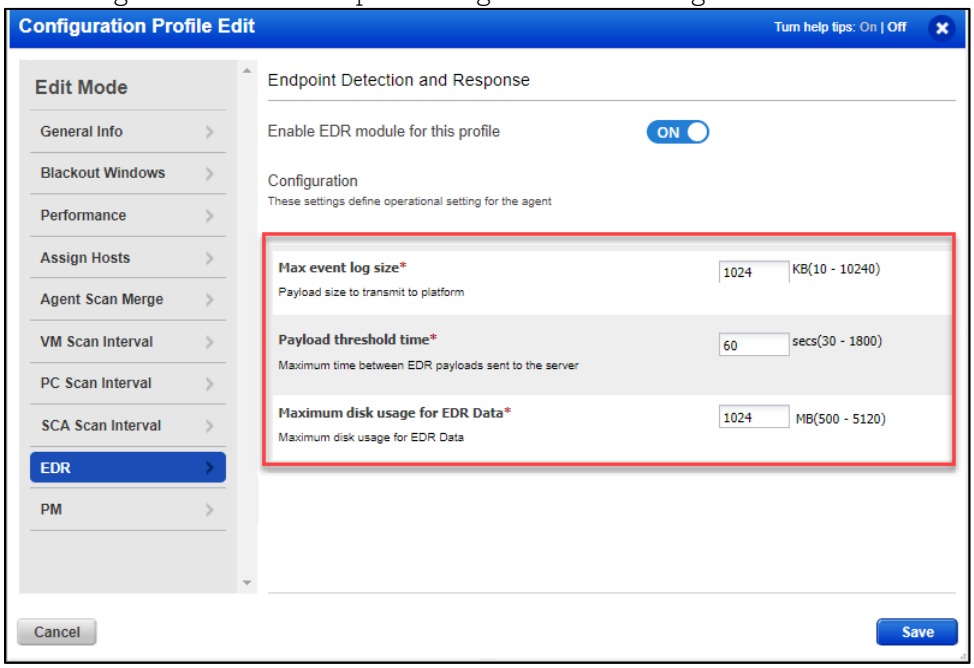
Hardware Requirements

	CPU	Memory	Disk Space
Desktop	4 Core processor	4 GB	1124 MB (100 MB for agent + 1024 MB for EDR cache)
Server	4 Core Processor	4GB	1124 MB (100 MB for agent + 1024 MB for EDR cache)

Default Disk Cache: EDR is configured with a default disk cache of 1024 MB and can be configured using the Cloud Agent module.

Traffic & connectivity: EDR is always connected to its backend services to post the event details continuously. By default, the agent connects to the backend services at an interval of 60 seconds or when the payload size is 1 MB.

You can configure these settings from the Cloud Agent module. To configure these settings, navigate to the **Cloud Agent module** > **Configuration Profiles**. Open the profile you are using and navigate to the EDR step to configure these settings.



Supported Operating Systems for EDR

Desktop Operating Systems (x86 and x64)

- Windows 10 21H1
- Windows 10 20H2
- Windows 10 2004
- Windows 10 1909
- Windows 10 1903
- Windows 10 1809
- Windows 10 1803
- Windows 10 1709
- Windows 10 1703
- Windows 10 1607
- Windows 8.1
- Windows 8
- Windows 7

Server Operating Systems

- Windows Server 20H2
- Windows Server 2004
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

System Resource Throttling

Due to the nature of the problem that antimalware products solve and the fact that they are real-time monitors, it is not a good practice to throttle these products. Throttling limits the product's ability to use the CPU, memory, disk I/O, and disk space.

Systems can encounter occasional resource usage spikes on the CPU, memory, disk I/O, or bandwidth usage. While this is normal, Qualys is actively working on allowing you to set resource usage limits for the EDR product.

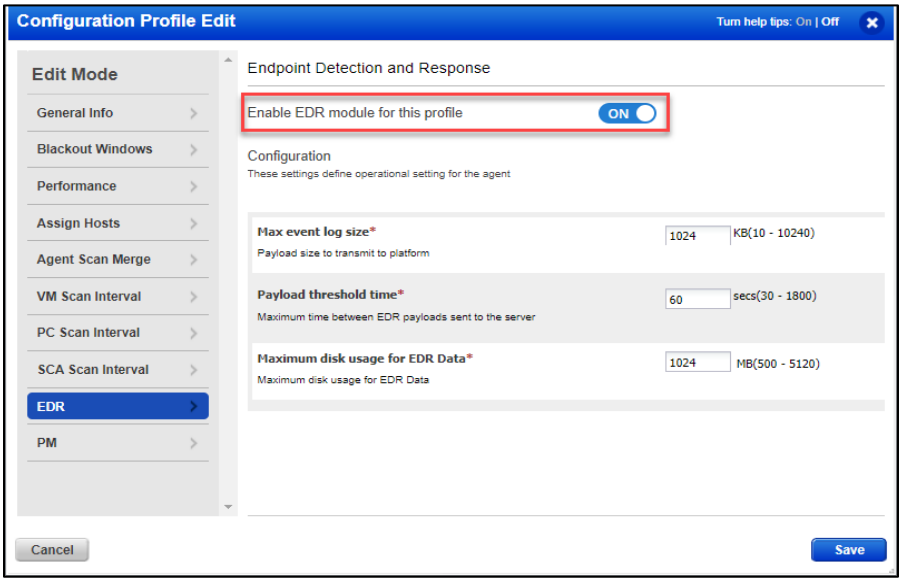
Note: While you can configure the Agent performance for other Qualys products from the Agent Configuration profile, these performance settings do not apply to Qualys EDR.

Qualys EDR Onboarding Recommendations

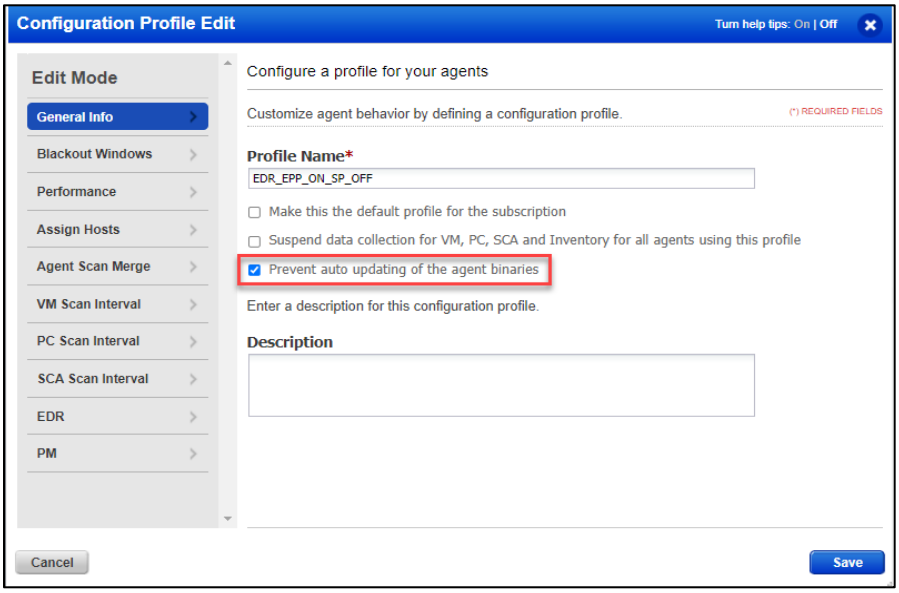
EDR detects suspicious activity, confirms the presence of known and unknown malware, and provides remediation response for your assets. This active monitoring in real-time requires constant inspection, scanning, and data collection.

Given the nature of the product, Qualys has put together a set of recommendations to onboard the EDR product.

- Ensure the onboarding activities are carried out with the support of your TAM. This helps to escalate and take precautionary measures in case of any issues.
- Perform a pilot tryout on a small set of assets. Select assets with varying software and hardware configurations for the pilot tryout.
- On the assets selected for the pilot tryout, make sure the agent version is 4.4.1.7 or later. Refer the Cloud Agent Windows Installation Guide for step-by-step instructions.
- Ensure the EDR module is enabled on the Configuration Profile. Refer the Getting Started Guide or the Online Help for step-by-step instructions.



- If you are a new Qualys customer, ensure that the agents do not self-patch (auto-update). To restrict agents from auto-updating, ensure that the **Prevent auto updating of the agent binaries** setting is selected for the Configuration Profiles in the Cloud Agent module. You can enable this setting after a successful pilot tryout.



- If you are an existing Qualys customer, for the pilot tryout, create a new configuration profile for the selected assets with the **Prevent auto updating of the agent binaries** setting disabled. This will automatically upgrade your Windows Agent on these assets to the latest version (version 4.4.1.7 or later).
- Continuously monitor asset performance for following in-progress activities:
  - Agent deployment or version upgrade
  - EDR enablement on endpoints

  Things to monitor:
  - CPU utilization
  - Memory utilization
  - High I/O
  - Network bandwidth
  - Number of EDR events captured (**Hunting** tab of Qualys EDR UI).
  - Endpoint performance with other antivirus software, Qualys products, and other software (coexistence, slowness, system crashes, etc. must be monitored closely)
- For the pilot tryout, monitor the assets for at least 1 to 2 business weeks.
- If you face issues during the pilot tryout, we recommend that you tune the configurations:
  - Increase CPU and memory if assets are underperforming.
  - Improve network bandwidth.
  - If you see unnecessary or high volume of events on the UI, contact the Qualys Support team to tune the policy.
- After a successful pilot tryout, when you are ready to deploy this across all assets, make sure you enable these assets in small batches.

- Keep a considerable gap between onboarding two batches. This ensures that the bandwidth and CPU utilization are under control on end points.

Here is a flowchart that summarizes the recommended onboarding process: