Endpoint Detection and Response

Onboarding Guide

April 22, 2022

Copyright 2021-2022 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

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

Table of Contents

Introduction **4**

System Requirements **4**

Software Requirements 4

Hardware Requirements 5

Agents with EDR 5

Agents with EDR with Malware Protection Software 6

Supported Operating Systems for EDR **6**

Desktop Operating Systems (x86 and x64) 6

Server Operating Systems 6

Supported Operating Systems for EDR with Malware Protection Software **7**

Desktop Operating Systems 7

Server Operating Systems 7

System Resource Throttling **7**

Qualys EDR Onboarding Recommendations **8**

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 responses for your assets.

Qualys Multi-Vector EDR now includes integrated antimalware detection capabilities, providing additional real-time protection against the latest threats. Qualys EDR also expedites the inevitable convergence of Malware Protection software with EDR to deliver comprehensive protection against known and unknown threats.

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 significant 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.

Note: While Qualys offers its own Malware Protection, uninstall all other antimalware software if you are using malware protection capabilities by Qualys EDR. However, If you are not using the malware protection capabilities, Qualys EDR can still co-exist with other 3rd party antimalware software. Running the malware protection capabilities with another antimalware software might result in undefined system behavior.

Whitelist Requirements

Qualys EDR can co-exist with other antimalware software. However, if you are using Qualys EDR with the Malware Protection capabilities enabled, admins must whitelist appropriate processes, internal tools, and other corporate applications so that our Malware Protection does not inadvertently block their functionalities. Failing to whitelist processes might affect your operations and cause problems with the application functionality.

You can review the default AV configuration policy and make necessary changes based on your organizational requirements using the **Configuration** tab in the EDR module. For more information, refer to the online help.

For the malware protection, ensure that you whitelist the following domains:

- cloudfront.net
- bitdefender.net
- bitdefender.com

If you are using Qualys Gateway Service (QGS), you can whitelist the domains using the Qualys Gateway Appliance Configuration. For more information, refer to the Qualys Gateway Service User Guide.

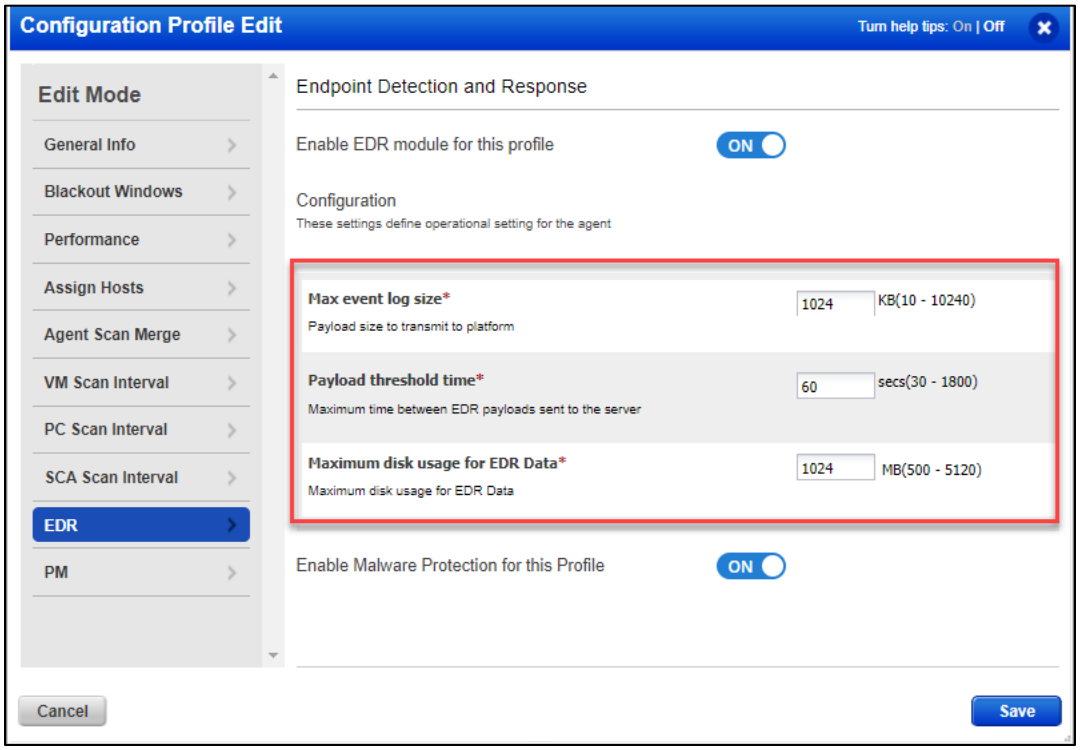
Hardware Requirements

Agents with EDR

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



Agents with EDR with Malware Protection Software

The following disk space and memory is required for EDR with Malware Protection software.

	CPU	Memory	Disk Space
Desktop	- Intel® Pentium compatible multi-core processors, 2 GHz or faster	6 GB	3 GB
Server	- Intel® Pentium compatible multi-core processors, 2.4 GHz - Intel® Xeon multi-core CPU, 1.86 GHz or faster	6 GB	3 GB

Important

Traffic for Desktop and Server: 15-25 GET requests per day

Bandwidth requirements for Desktop and Server:

- First time download (agent installer and Malware Protection definition update) consumes 900 MB.
- The daily requests and events require 3 MB.
- Upgrade (once in 2 months) requires 300 MB.

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

Supported Operating Systems for EDR with Malware Protection Capabilities

Desktop Operating Systems

- Windows 10 October 2020 Update (20H2)
- Windows 10 May 2020 Update (20H1)
- Windows 10 November 2019 Update (19H2)
- Windows 10 May 2019 Update (19H1)
- Windows 10 October 2018 Update (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10
- Windows 8.1
- Windows 8.0

Server Operating Systems

- Windows Server 2019
- Windows Server 2019 Core
- Windows Server 2016
- Windows Server 2016 Core
- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Server 2008 R2

System Resource Throttling

Due to the nature of the problem that antimalware products solve and 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.

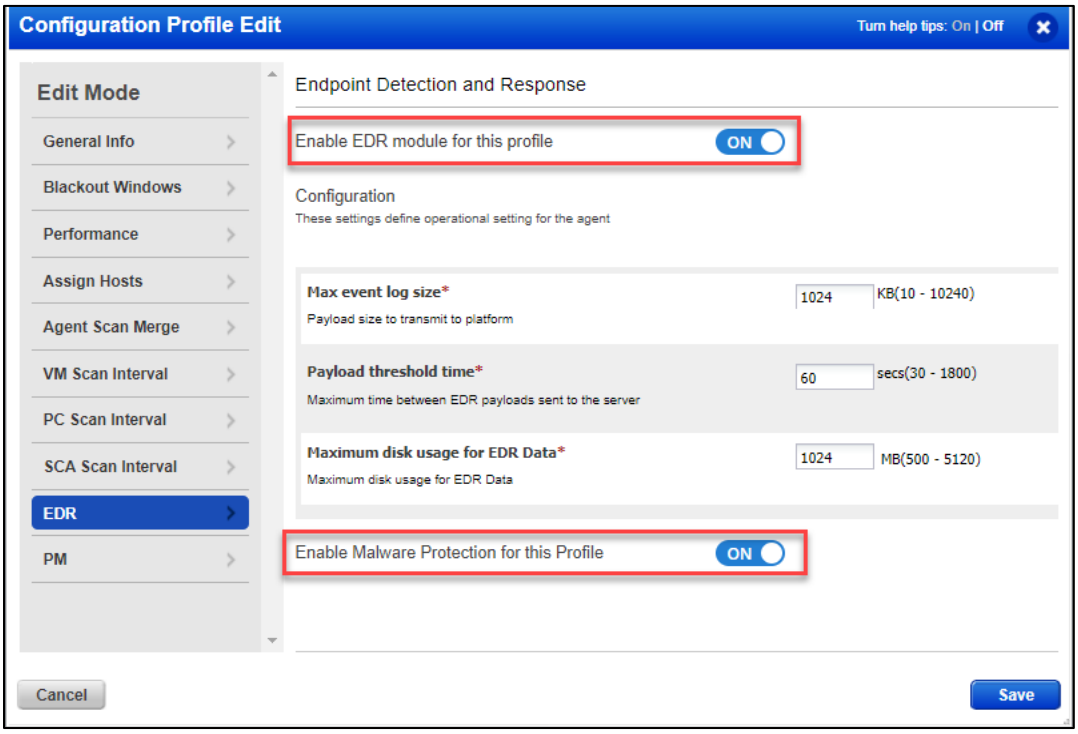
Note: While you can configure the Agent performance for other Qualys products from the Agent Configuration profile, these performance settings do not apply to Qualys EDR.

Qualys EDR Onboarding Recommendations

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

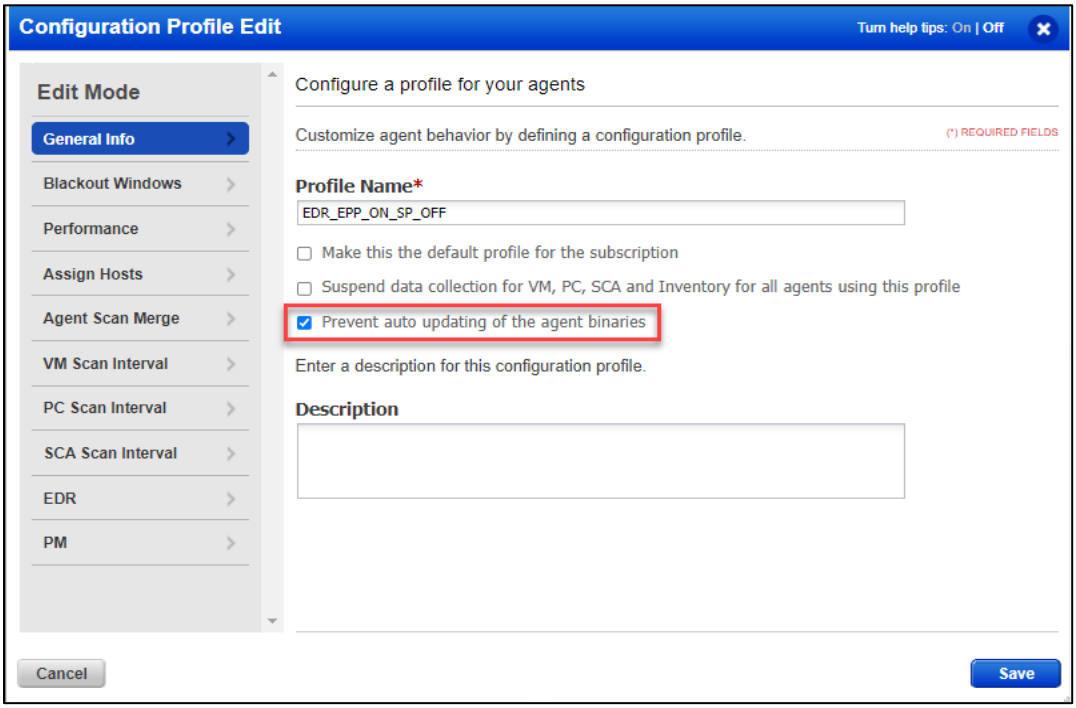
Given the nature of the product, Qualys has put together a set of recommendations to onboard the EDR product.

- Ensure the onboarding activities are carried out with the support of your TAM. This helps to escalate and take preventive 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, ensure the agent version is 4.5 or later. Refer to the Cloud Agent Windows Installation Guide for step-by-step instructions.
- Ensure the EDR module is enabled on the Configuration Profile. After you have enabled the EDR module, you can enable the Malware Protection capabitlies. Refer to the Getting Started Guide or the Online Help for step-by-step instructions.



Note: While Qualys offers its own Malware Protection, uninstall all other antimalware software if you are using malware protection capabilities by Qualys EDR. However, If you are not using the malware protection capabilities, Qualys EDR can still co-exist with other 3rd party antimalware software

- 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, create a new configuration profile for selected assets with the Prevent auto updating of the agent binaries setting disabled for the pilot tryout. This will automatically upgrade your Windows Agent on these assets to the latest version (4.5 or later).
- Continuously monitor asset performance for following in-progress activities:
  - Agent deployment or version upgrade
  - EDR enablement on endpoints
  - Malware Protection software enablement on top of EDR 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 an 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:

