



Endpoint Detection and Response

Onboarding Guide for Linux (Beta)

December 1, 2022

Copyright 2022-2023 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
Linux Hardware Requirements.....	4
Linux Software Requirements	4
Root Access	4
SELinux Configuration	4
Configuration Script.....	4
Linux Operating Systems (x86 and x64).....	5
Qualys EDR Onboarding Recommendations	5

Introduction

Qualys Multi-Vector 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 includes integrated anti-malware 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.

The active monitoring and data collection are real-time, and 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 you carry out a performance pilot tryout before a full scale-out.

Linux Hardware Requirements

Following are the recommended Linux hardware requirements for deploying EDR 2.2.0 or later:

- **Linux Cloud Agent Version** - 5.8.0
- **CPU** - 8 Core Processor
- **Memory** - 8 GB of RAM
- **Disk Space** – 1024 MB. It is configurable from the **Configuration Profile** of the **Cloud Agent** application.

Linux Software Requirements

Following are the Linux software requirements for deploying EDR 2.2.0 or later:

Root Access

An agent requires sudo or root access.

SELinux Configuration

If SELinux is enabled for Enforcing or Permissive mode, install **semodule_package**, **checkmodule** and **restorecon**. If SELinux is disabled, package installation is not required.

Note: Debian and Ubuntu do not require the SELinux check.

Configuration Script

- **UseAuditDispatcher** – If the auditd service is used, the UseAuditDispatcher script value is set to 1. EDR will start the installed auditd service if the service is stopped. The auditd service is not required if UseAuditDispatcher is set to 0.
- **AuditBacklogLimit** – This is a recommended setting. By default, the EDR binary is set to 8192. You can change the value as per your requirement.
- **EDRCPULimit** – By default, the minimum CPU percentage assigned is 5% of the total CPU limit of the asset.
- **EDRMemory Limit** – By default, the minimum memory assigned is 5% of the total memory of the asset.

Linux Operating Systems (x86 and x64)

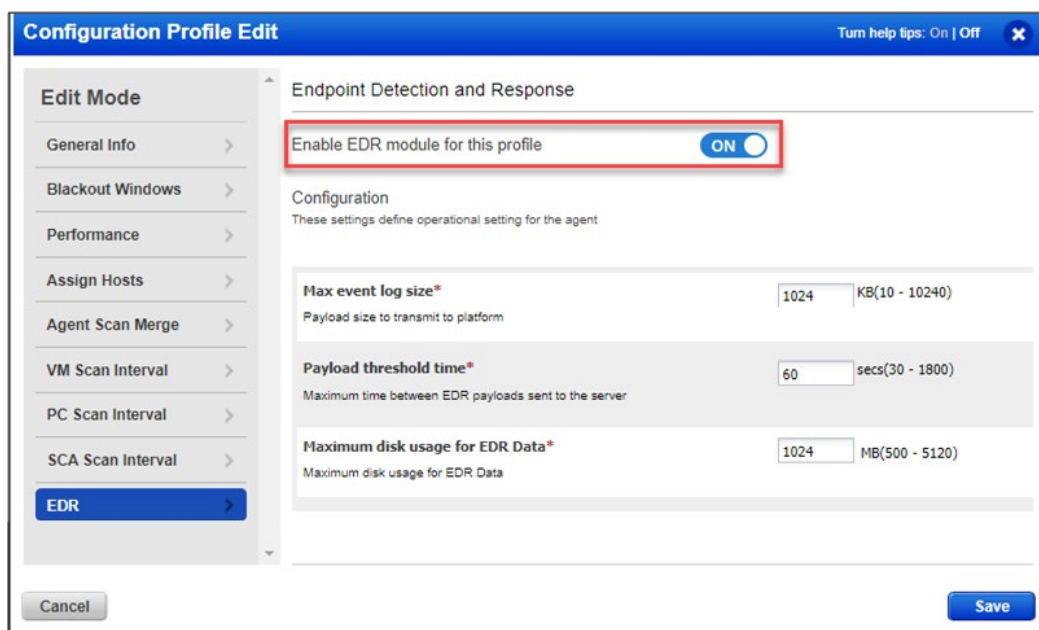
- Amazon Linux 2
- Amazon Linux AMI
- CentOS 6
- CentOS Linux 7.3.16.11
- Debian 10
- Oracle Enterprise Linux 7.5
- SUSE Linux Enterprise Server 15 SP2/SP3
- Red Hat Enterprise Linux 8
- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 7.5

Qualys EDR Onboarding Recommendations

EDR detects suspicious activity, confirms the presence of known and unknown malware, and provides remediation responses for your assets. Active real-time monitoring 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 on Linux systems.

- 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 Linux agent version is 5.8.0. Refer to the [Cloud Agent for Linux Installation Guide](#) for step-by-step instructions.
- Ensure the EDR module is enabled on the **Configuration Profile**.



The screenshot shows the 'Configuration Profile Edit' window. On the left is a sidebar with 'Edit Mode' and a list of categories: General Info, Blackout Windows, Performance, Assign Hosts, Agent Scan Merge, VM Scan Interval, PC Scan Interval, SCA Scan Interval, and EDR (which is highlighted with a blue bar). The main area is titled 'Endpoint Detection and Response'. At the top, there is a toggle switch for 'Enable EDR module for this profile' which is currently set to 'ON' and is highlighted with a red rectangle. Below this is a 'Configuration' section with the subtitle 'These settings define operational setting for the agent'. It contains three settings: 'Max event log size*' set to 1024 KB (range 10 - 10240), 'Payload size to transmit to platform' (no input field visible), 'Payload threshold time*' set to 60 secs (range 30 - 1800), and 'Maximum disk usage for EDR Data*' set to 1024 MB (range 500 - 5120). At the bottom left is a 'Cancel' button and at the bottom right is a 'Save' button.

Note: While Qualys offers its own Malware Protection, uninstall all other anti-malware 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 third party anti-malware 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** application. 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 Linux Agent on these assets to the latest version (5.8 or later).
- Continuously monitor asset performance for the 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 softwares (such as coexistence, slowness, and system crashes 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, ensure 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.

The following flowchart summarizes the recommended onboarding process:

