



Qualys Log4Shell Service Playbook

January 4, 2022

Copyright 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

| | |
|----------------------------------------------------------------------------|-----------|
| Qualys Log4Shell Service | 1 |
| Qualys Log4Shell Service Playbook | 4 |
| <i>Let's Get Started</i> | <i>4</i> |
| Scan Your External Attack Surface | 4 |
| <i>Qualys Web Application Scanning</i> | <i>4</i> |
| Step 1 - Identify Web Applications to Scan | 4 |
| Step 2 - Use the Log4Shell Option profile to scan | 5 |
| Step 3 - Launch a Web Application Scan | 5 |
| Find Vulnerabilities and Prioritize | 6 |
| <i>Qualys Cybersecurity Asset Management (CSAM)</i> | <i>6</i> |
| Step 1 - Deploy and Setup Cloud Agent | 6 |
| Step 2 - Detect at-risk Assets & Applications | 7 |
| Step 3 - Visualize Log4j Exposure | 8 |
| <i>Qualys Vulnerability Management Detection and Response (VMDR)</i> | <i>9</i> |
| Step 1 - Detect Log4j vulnerability | 9 |
| Step 2 - Generate Prioritization Report | 9 |
| Step 3 - Detect Impacted Assets with Threat Protection | 10 |
| <i>Qualys Container Security (CS)</i> | <i>11</i> |
| Step 1 - Scan Containers | 11 |
| Step 2 - Scan Images | 11 |
| Remediate | 13 |
| <i>Qualys Patch Management (PM)</i> | <i>13</i> |
| Step 1 - Create Patch Jobs | 13 |
| Step 2 - Use VMDR to create Patch Jobs | 13 |
| Detect Exploits and Malware | 14 |
| <i>Qualys Endpoint Detection and Response (EDR)</i> | <i>14</i> |
| Step 1 - Enable EDR and Malware Protection in Configuration Profile | 14 |
| Step 2 - Configure Rule-Based Alerts for Events | 14 |
| Step 3 - View Events and Detections | 15 |

Qualys Log4Shell Service Playbook

Since the Log4Shell vulnerability was first discovered, the Qualys Research Team has analyzed the threat and updated Qualys Cloud Platform to help customers respond quickly.

We recognize that the scope of the challenge is significant for many organizations, as it involves all Java-based applications in their environment. Recognizing which application was written in Java, let alone if it uses a vulnerable version of Log4j, can be a challenge. As a result, Qualys recommends that organizations take a prioritized, layered approach to remediate and eliminate this vulnerability wherever it lives. Read more about Log4Shell in our blogs:

[Log4Shell – Follow This Multi-Layered Approach for Detection and Remediation](#)
[Out-of-Band Detection for Log4Shell](#)

Refer [Qualys blogs](#) to know more about Log4Shell and to [Qualys Documentation](#) to set up and configure Qualys apps, as required.

Let's Get Started

The primary objective is to determine the existence of any vulnerabilities. To begin this process, Qualys recommends that all organizations scan their external attack surface (public-facing websites and applications) to identify any potential vulnerabilities by simulating the attack using the Qualys Web Application Scanning module.

Scan Your External Attack Surface

Qualys Web Application Scanning

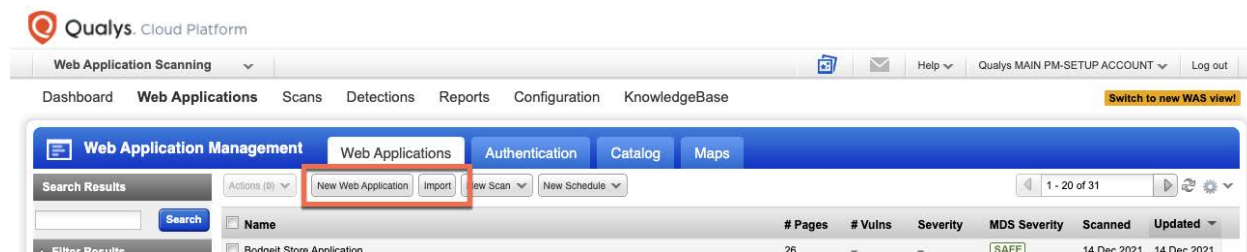
For details on Qualys WAS Log4Shell detection, please refer to our [blog](#)

Scan your internet-facing web applications and APIs to find applications vulnerable to Log4j2 (CVE-2021-44228) using Web Application Scanning (WAS).

The WAS module injects JNDI payloads into certain request headers and application-specific endpoints. It uses Out-Of-Band (OOB) detection methods where vulnerable instances will make a callback DNS query that will trigger the Qualys Periscope detection mechanism.

Step 1 - Identify Web Applications to Scan

Navigate to Web Applications > Web Applications tab and add a new application or import an application



For detailed steps, refer to [Adding Web Applications](#)

Refer to the following docs to get started with WAS

[WAS Videos](#) | [WAS Getting Started Guide](#) | [WAS Online Help](#) | [WAS Log4Shell Protection Playbook](#)

Step 2 - Use the Log4Shell Option profile to scan

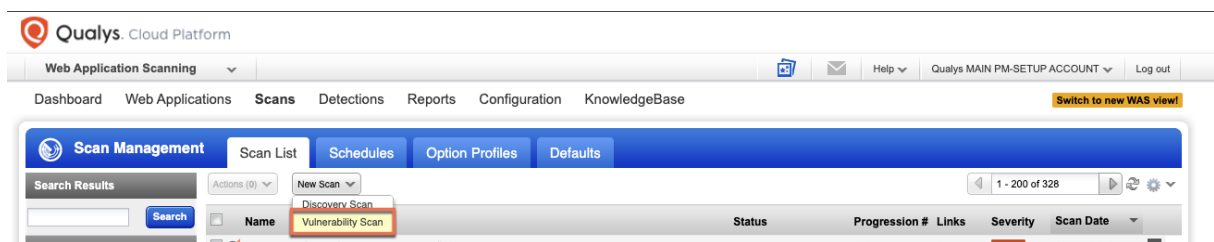
Navigate to the Configuration > Options Profile tab and click Import Profile to import the Log4Shell Options scanning option profile.

Scanning with this option profile will achieve two things to expedite testing your web applications in the most efficient way possible. First, we are only testing for two specific vulnerabilities, QIDs 150440 and 150441. Second, as this vulnerability is only tested at the base URL and several directories up and down as appropriate, there is no need to crawl and test every link in the application. These two changes will allow each web application to be scanned faster than full core detection scans while still providing you the necessary visibility of any vulnerable versions of Log4j2.

Refer to [Manage Options Profile](#)

Step 3 – Launch a Web Application Scan

Navigate to the Scan tab, and from Scan List, select Vulnerability Scan.



Select the Log4Shell Options scanning option profile and then select the external scanner.

The screenshot shows the 'Launch New WAS Vulnerability Scan' configuration window. On the left, a sidebar indicates 'Step 2 of 3' with 'Scan Settings' selected. The main area is titled 'Configure settings for your scan'. Under 'Option Profile', a dropdown menu is set to 'Log4Shell Options', which is highlighted with a red box. Below this, there's a checkbox for 'Make this selected profile the default profile for this web application.' Under 'Authentication', the 'Use*' dropdown is set to 'None'. Under 'Scanner Appliance', the 'External' radio button is selected, also highlighted with a red box. At the bottom right, the 'Continue' button is highlighted with a red box.

That's it! Select Continue and launch your scan. Once the scan is completed, reports can be generated to view the details of any Log4j2 vulnerabilities found.

Find Vulnerabilities and Prioritize

Detection is a key challenge posed by this vulnerability. As Log4Shell may affect any Java application that uses a vulnerable version of Log4j, Qualys offers a multi-layered approach to help our customers detect where they are vulnerable.

Qualys Cybersecurity Asset Management (CSAM)

To secure your infrastructure from Log4j vulnerability, first, you need to get in-depth visibility into all the vulnerable software components. Identification and updating these components will reduce the attack surface of your infrastructure.

Step 1 - Deploy and Setup Cloud Agent

Start building your inventory by installing cloud agents. You can have cloud agents on private clouds, public clouds, on-premises, and endpoints to continuously discover your IT assets providing 100% real-time visibility.

[Install Qualys Cloud Agents](#) | [Cloud Agent Getting Started Guide](#) | [Cloud Agent Onboarding Videos](#)

Navigate to Cloud Agent and create a new activation key for log4j. Select VM, EDR, and Patch Management and follow the wizard to install all the required agents to all endpoints you want to protect.

New Activation Key Turn help tips: On | Off

Create a new activation key

An activation key is used to install agents. This provides a way to group agents and better manage your account. By default this key is unlimited - it allows you to add any number of agents at any time.

Title: Select | Create

(no tags selected)

Provision Key for these applications

| | |
|------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| <input type="checkbox"/> CSAM CyberSecurity Asset Management Activations managed by CSAM | <input checked="" type="checkbox"/> PM Patch Management 100976 Activations Remain |
| <input checked="" type="checkbox"/> VM Vulnerability Management 99965 Activations Remaining | <input type="checkbox"/> PC Policy Compliance 9965 Activations Remainin |
| <input checked="" type="checkbox"/> EDR Endpoint Detection and Response 966 Activations Remaining | <input type="checkbox"/> FIM File Integrity Monitoring 966 Activations Remaining |
| <input type="checkbox"/> XDR Extended Detection and Response 3979 Activations Remaining | <input type="checkbox"/> SCA Secure Config Assessm 99966 Activations Remain |

☐ Set limits

Close Unlimited Key Generate

Once the agent is installed, it starts collecting and inventorying all the vulnerabilities and asset data. This helps you get visibility into affected log4j vulnerabilities and start mitigating them.

Step 2 - Detect at-risk Assets & Applications

CSAM enriches your asset inventory with in-context, relevant information to help you detect at-risk assets and applications. You can identify and set alerts for assets that have log4j vulnerabilities.

Refer to the following documentation to get started with CSAM.

[CSAM Quick Start Guide](#) | [CSAM Onboarding Videos](#) | [CSAM Online Help](#)

CSAM makes it easy to identify assets containing Log4j. Please use the following QQL query to identify such assets.

Query: software:(name:"log4j" or name:"liblog4j2")

The screenshot shows the Qualys Cloud Platform interface for CyberSecurity Asset Management. The 'Inventory' tab is active, displaying a search for 'software:(name:"log4j")'. The results show 17 total software items. A table lists the following items:

| RELEASE | TYPE | CATEGORY | LICENSE | LIFECYCLE | INSTANCES |
|----------------------------------------------------|-------------|------------------------------------------|---------------------------------------------|---------------------------------------|-----------|
| Apache Log4j 1.2.17 | Application | Application Development Development Tool | Open Source Apache License 2.0 (Apache-2.0) | EOL: Aug 05 2015 EOS: Aug 05 2015 | 9 |
| Apache Log4j 2.0 (Vulnerable) | Application | Application Development Development Tool | Open Source Apache License 2.0 (Apache-2.0) | GA: Jul 12 2014 EOL: Not Announced | 3 |
| Apache Log4j 1.2.15 | Application | Application Development Development Tool | Open Source Apache License 2.0 (Apache-2.0) | EOL: Aug 05 2015 EOS: Aug 05 2015 | 2 |
| Apache Log4j 1.2.14 | Application | Application Development Development Tool | Open Source Apache License 2.0 (Apache-2.0) | EOL: Aug 05 2015 EOS: Aug 05 2015 | 1 |
| log4j-eap6 1.2.16-11.redhat_2.ep6.e... | Utilities | Unidentified | | Unknown | 1 |
| log4j-jboss-logmana... 1.0.1-3.Final_redhat_2.e... | Utilities | Unidentified | | Unknown | 1 |

A new rule has been published in your Qualys CSAM account to list and tag all the software applications that are vulnerable or potentially vulnerable due to the use of the vulnerable Log4j component. Enable the Log4jShell detection rule and run a scan to identify vulnerable applications.

Navigate to CSAM > Rules and select the rule "Apps with Log4j(potentially vulnerable)" then Click on Actions and Enable the rule. You can then view and categorize all assets with the log4j component in the Inventory tab.

Enrich the Inventory

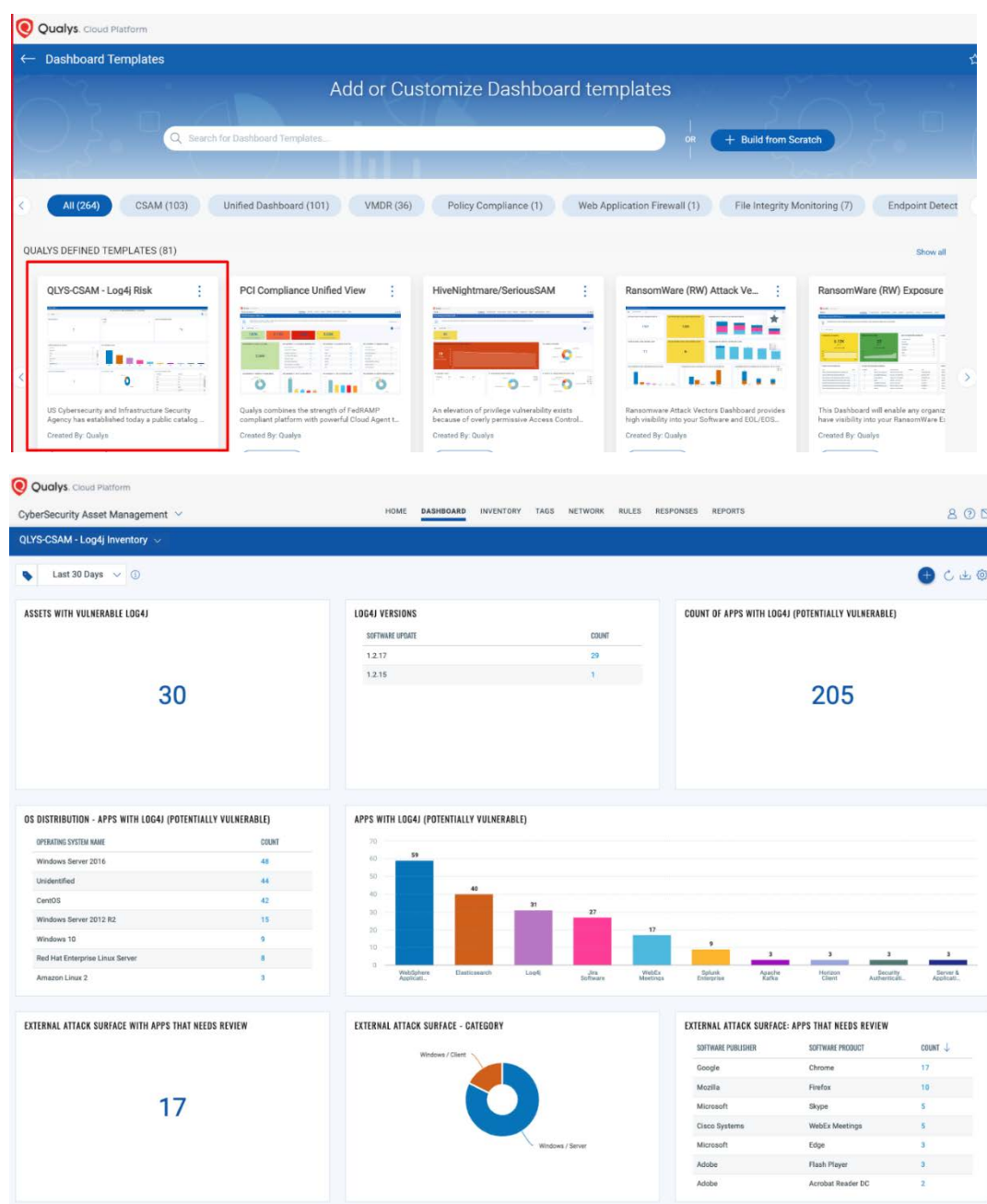
So that you can run more efficient inventory queries for suspected Java applications, the Qualys Research Team has enriched the inventory data collected by CSAM. We can now flag applications that are recognized by the community as vulnerable to the Log4Shell exploit (based on this [GitHub](#)). Furthermore, by utilizing CSAM's ability to tag internet-facing assets, those queries can focus first on your external facing Java-based applications that are flagged as vulnerable. CSAM integration with your CMDB provides another method for prioritization, as it will allow you to focus on your business-critical applications first.

Step 3 – Visualize Log4j Exposure

New dashboards are now available to help you quickly view all the vulnerable hosts and software. These dashboards have useful widgets listing all the vulnerable hosts, applications with vulnerable versions of log4j, and most importantly, all the vulnerable hosts visible on the Internet.

Dedicated widgets such as ‘External Attack Surface’ populate all vulnerable hosts visible on Shodan and are low-hanging opportunities for attackers. These widgets also list workloads hosted on shared cloud infrastructure with public IP addresses. All the apps containing log4j, in which the default bundled version of log4j is vulnerable, are listed as ‘potentially vulnerable apps.’

For example, create a new Dashboard using the “QLYS-CSAM-Log4j Risk” template.



Refer to the following Unified Dashboard [online help](#) on building and using dashboards.

Qualys Vulnerability Management Detection and Response (VMDR)

Now that your inventory is in place use VMDR to assess, prioritize, and remediate the log4j vulnerabilities on your assets.

VMDR helps you automatically detect and prioritize the specially researched log4j vulnerabilities, and the threat feed enables you to understand your asset exposure to high-profile exploited vulnerabilities.

Refer to the following documentation to get started with VMDR

[VMDR Onboarding Videos](#) | [VMDR Getting Started Guide](#) | [VMDR Online Help](#)

Step 1 – Detect Log4j vulnerability

With VMDR, you can detect the Log4j vulnerability in two ways.

- 1) View all your impacted hosts for this vulnerability in the vulnerabilities view by using the QQL query

Navigate to the VMDR > Vulnerabilities tab and search using the following query:

`vulnerabilities.vulnerability.qid:[`730297`,`376157`]`

| QID | TITLE | CVE IDS | SEVERITY | VULNERABILITY COUNT |
|--------|--------------------------------------------------------------------------------------|----------------|----------|---------------------|
| 376157 | Apache Log4j Remote Code Execution (RCE) Vulnerability (Log4Shell) | CVE-2021-44228 | 5/10 | 23 |
| 730297 | Apache Log4j Remote Code Execution (RCE) Vulnerability (Log4Shell) (Unauthenticated) | CVE-2021-44228 | 5/10 | 23 |

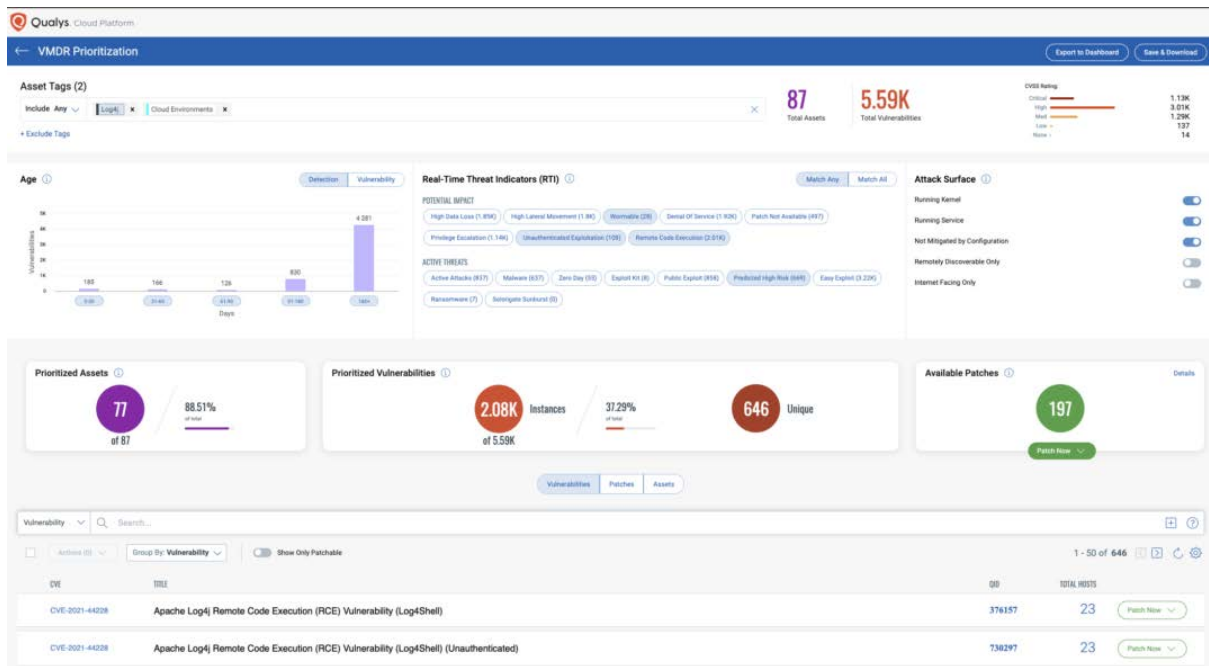
- 2) Prioritize Based on RTIs

Using VMDR, the Log4j vulnerabilities can be prioritized using the following real-time threat indicators (RTIs):

- Predicted_High_Risk
- Wormable
- Remote_Code_Execution
- Unauthenticated_Exploitation

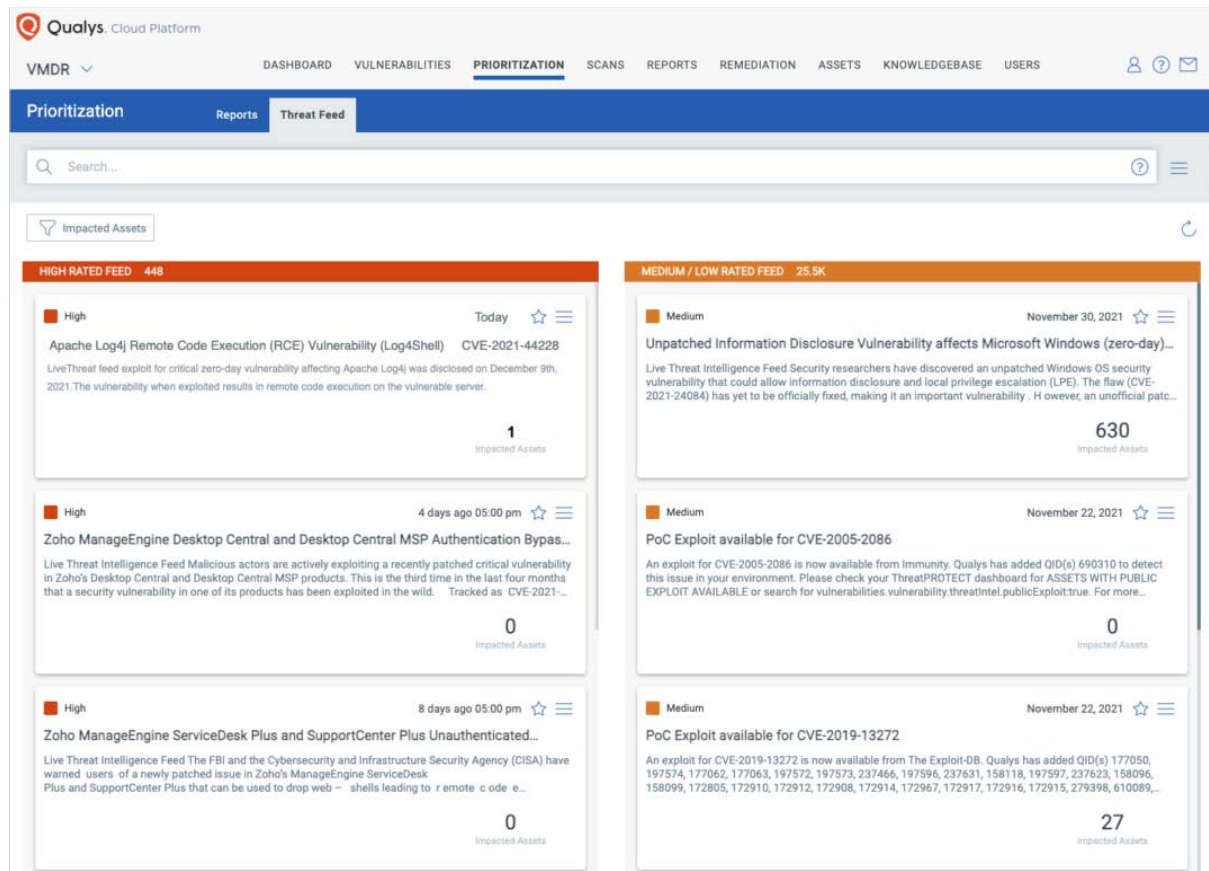
Step 2 – Generate Prioritization Report

Navigate to the VMDR > Prioritization tab and select all the necessary asset tags. Then choose the above-listed RTIs and generate the report.



Step 3 - Detect Impacted Assets with Threat Protection

VMDR also enables you to proactively stay on top of these threats via the ‘live threat feed’ provided for threat prioritization. With ‘live feed’ updated for all emerging high and medium risks, you can see the impacted hosts against threats.



Qualys Container Security (CS)

As containers are common in many environments, and Java is a commonly used language for building applications that run in containers, scanning for the Log4Shell vulnerability in your containers is a critical next step.

Container Security offers multiple methods to help you detect Log4Shell in your container environment for running containers and container images. We recommend running scans against containers as Java applications that run the containers are vulnerable to these exploits.

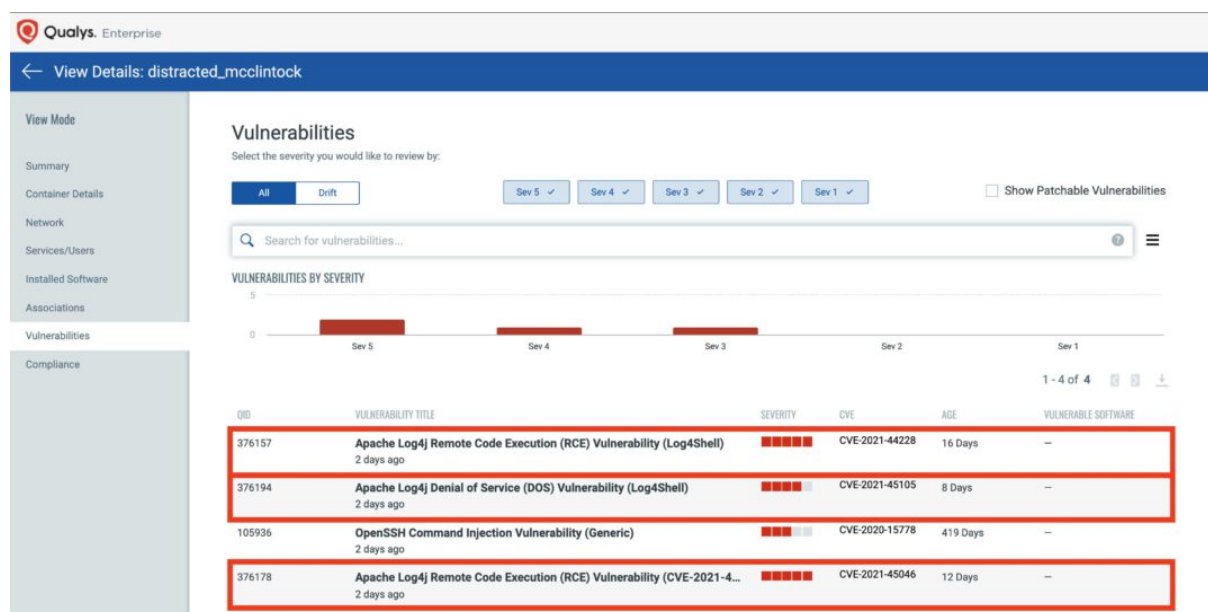
Step 1 - Scan Containers

Runtime scans will help identify all instances of this vulnerability in cases where the app uses the common methods of deploying Java and Log4j.

Navigate to the Container Security > Assets > Containers and search using the following query:

vulnerabilities.qid:376157 or vulnerabilities.qid:376178 or vulnerabilities.qid:376194

Click on the resulting vulnerable containers and go to the “Vulnerabilities” tab to learn more.



Qualys Enterprise

← View Details: distracted_mcclintock

Vulnerabilities

Select the severity you would like to review by:

All Drift

Sev 5 ✓ Sev 4 ✓ Sev 3 ✓ Sev 2 ✓ Sev 1 ✓

☐ Show Patchable Vulnerabilities

Search for vulnerabilities...

VULNERABILITIES BY SEVERITY

1 - 4 of 4

| QID | VULNERABILITY TITLE | SEVERITY | CVE | AGE | VULNERABLE SOFTWARE |
|--------|--------------------------------------------------------------------------------------|----------|----------------|----------|---------------------|
| 376157 | Apache Log4j Remote Code Execution (RCE) Vulnerability (Log4Shell) 2 days ago | Sev 5 | CVE-2021-44228 | 16 Days | — |
| 376194 | Apache Log4j Denial of Service (DOS) Vulnerability (Log4Shell) 2 days ago | Sev 4 | CVE-2021-45105 | 8 Days | — |
| 105936 | OpenSSH Command Injection Vulnerability (Generic) 2 days ago | Sev 3 | CVE-2020-15778 | 419 Days | — |
| 376178 | Apache Log4j Remote Code Execution (RCE) Vulnerability (CVE-2021-4...) 2 days ago | Sev 5 | CVE-2021-45046 | 12 Days | — |

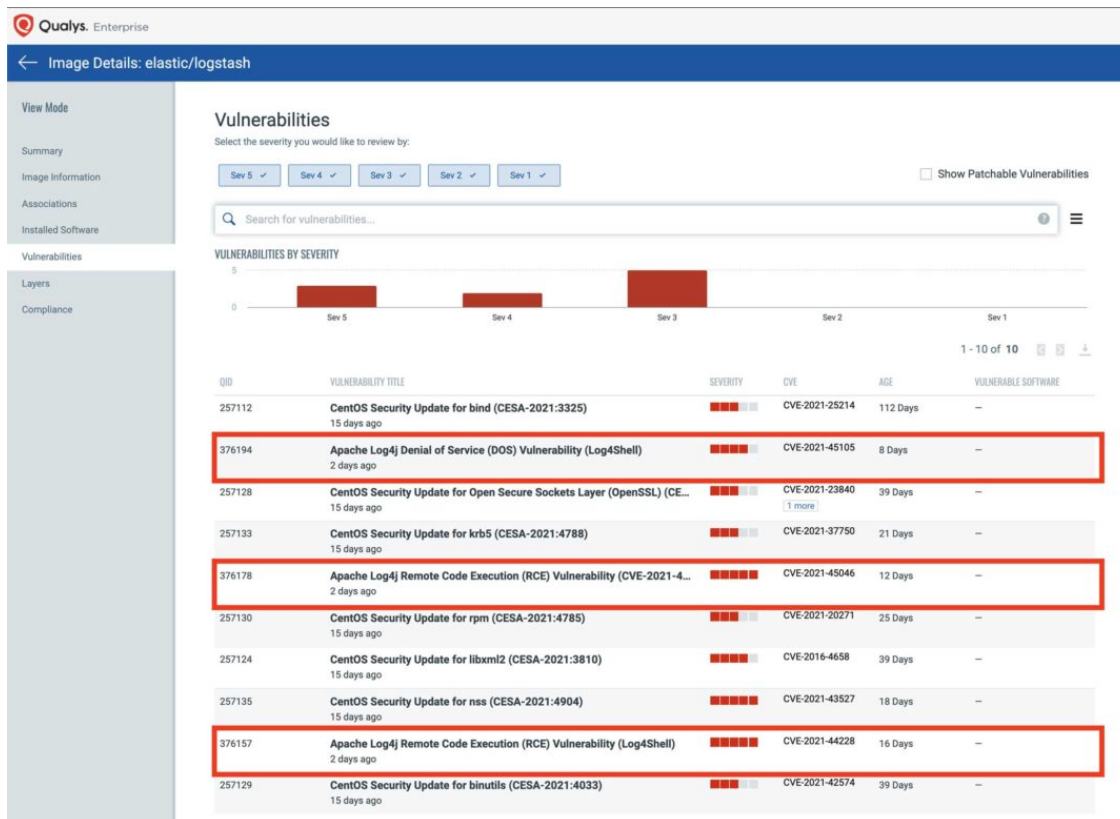
Step 2 – Scan Images

Qualys also recommends scanning your images. Running scans on images will mitigate vulnerabilities when the image is instantiated into a container later.

To scan Images, navigate to the Container Security > Assets > Images and search using the following query:

vulnerabilities.qid:376157 or vulnerabilities.qid:376178 or vulnerabilities.qid:376194

Click on the resulting vulnerable containers and go to the “Vulnerabilities” tab to learn more.



This in-depth container image scan can be triggered in three different stages of your container's image lifecycle: during the build process, as the image is uploaded to the register, and before the image is deployed to production.

Refer to the following documentation to get started with Container Security

[Container Security Videos](#) | [Container Security User Guide](#) | [Container Security Online Help](#)

Remediate

Qualys Patch Management (PM)

Remediating this vulnerability is not straightforward as the vulnerability is a library that is used by a Java application. Qualys Patch Management can be used for different types of remediations which depend on the specific vulnerable Java application.

1. In case the vendor of the Java application releases a patch, customers can use Qualys Patch Management to deploy the patch. Updating the version is not possible.
2. Customers can use Qualys patch management to remove the JndiLookup.class as recommended by Apache Log4j (<https://logging.apache.org/log4j/2.x/>) from the log4j jar. To do so, customers can create a pre action to execute the following command as recommended by Apache Log4j: `“zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class”`
3. Customers can use the pre-actions to create an action to replace the old log4j jar with the 2.16.0 jar.
4. In more complex situations, pre-actions can be used to update the environment variables or system properties as suggested by Apache Log4j

Note: A reboot will likely be needed after the above changes are applied. We recommend utilizing the pre-action ability to force a reboot to ensure the application is restarted.

Step 1 – Create Patch Jobs

You can create patch jobs from the Patch Management app or create patch jobs using your VMDR prioritization report.

Simply navigate to Patch Management > Jobs and create a Deployment Job. Follow the wizard to create and deploy the job. Refer to [Deploying Patch Jobs on Assets](#)

Step 2 – Use VMDR to create Patch Jobs

In the VMDR Prioritization Report, select the vulnerabilities you would like to remediate and add them to a new job. Qualys will automatically map all the selected vulnerabilities to the patches that remediate those vulnerabilities and are relevant in your environment. Only the latest patches are included, saving the need to deploy old patches that have been superseded. Configure the patch job and deploy the patches to your vulnerable assets.

You may also use the zero-touch patching capability to intelligently identify and automatically deploy proper patches required for remediating vulnerabilities. Refer to [Zero-Touch Patch Job](#)

Refer to the following resources to get started with Patch Management

[Deploying Patch Jobs on Assets](#) | [Patch Management Getting Started Guide](#) | [Patch Management Videos](#)

Detect Exploits and Malware

Qualys Endpoint Detection and Response (EDR)

Due to the complexity of detecting and remediating this vulnerability, we recommend utilizing Qualys EDR to help detect exploit attempts, malware, and Indicators of Compromise (IOC) associated with Log4Shell in real-time. EDR has been updated with specific content and workflows to help monitor and alert suspicious activities related to the Log4Shell exploit. Using the EDR capabilities, you can view real-time threat reports and triage exploits in cases where suspicious activity was detected.

Refer to the EDR blog for more information:

Log4Shell Exploit Detection and Response with Qualys Multi-Vector EDR

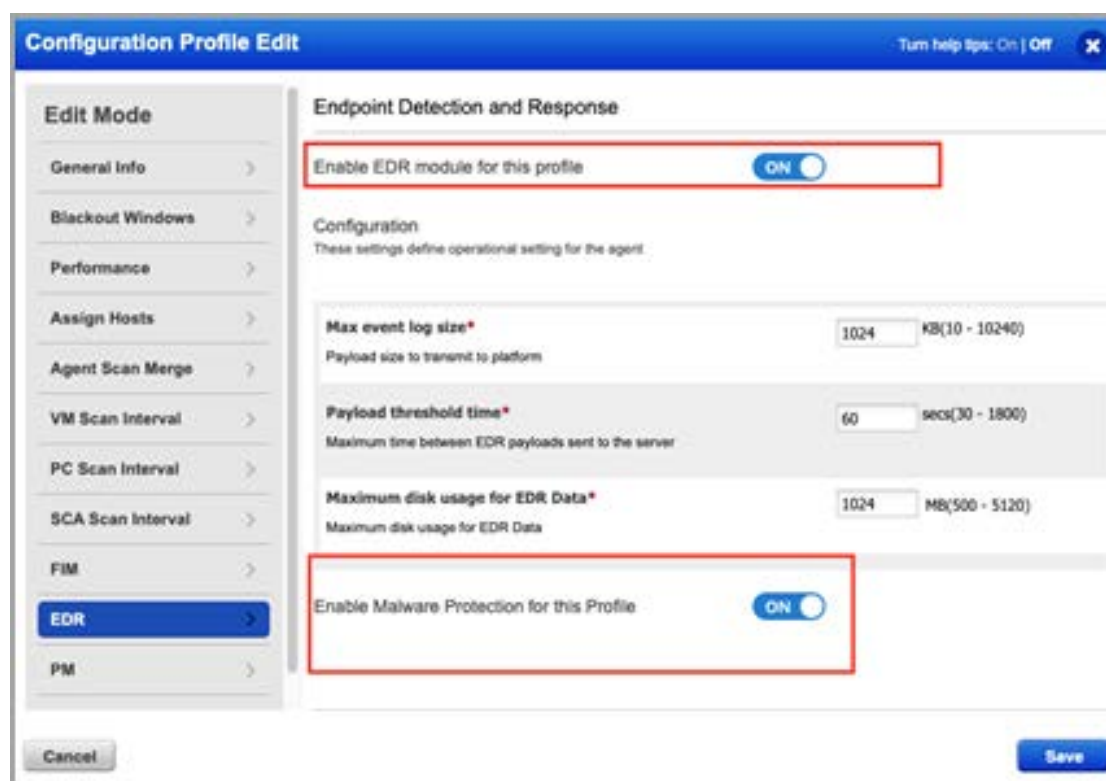
Step 1 - Enable EDR and Malware Protection in Configuration Profile

Ensure your cloud agents are enabled for EDR and Malware Protection.

Navigate to the Cloud Agent > Agents tab and identify the agent that has EDR enabled on it.

Toggle Enable EDR module for this profile to On. This is required for EDR data collection. Toggle the Enable Malware Protection for this Profile to On for anti-malware activation.

For detailed steps, refer to [Enable EDR module](#) | [Enable Malware Protection](#)

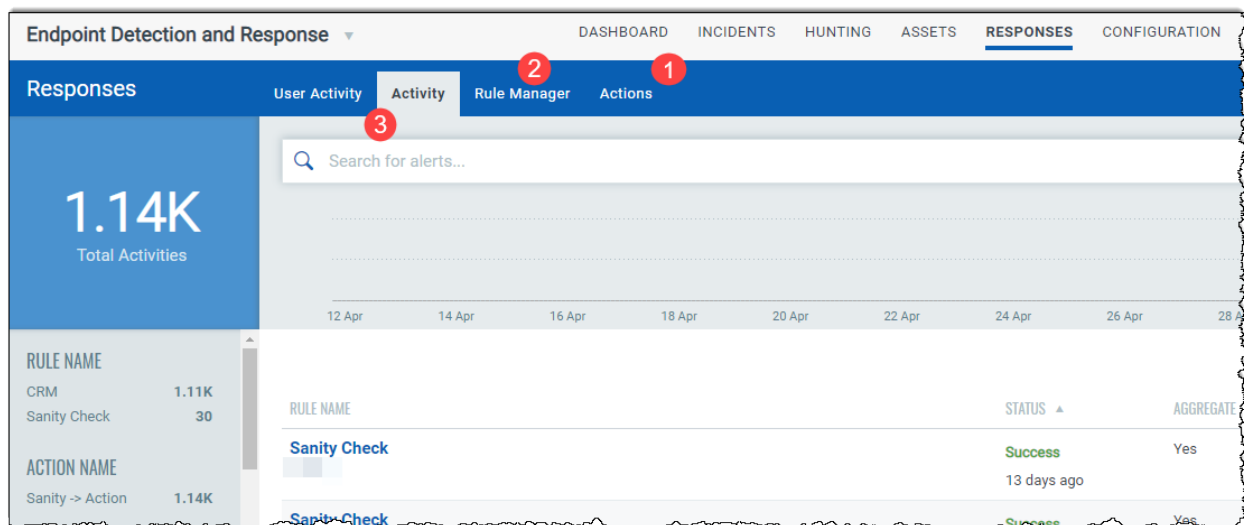


The screenshot displays the 'Configuration Profile Edit' window. On the left is a sidebar with 'Edit Mode' options: General Info, Blackout Windows, Performance, Assign Hosts, Agent Scan Merge, VM Scan Interval, PC Scan Interval, SCA Scan Interval, FIM, EDR (highlighted), and PM. The main area is titled 'Endpoint Detection and Response'. It features a toggle switch for 'Enable EDR module for this profile' set to 'ON'. Below this is a 'Configuration' section with three settings: 'Max event log size' (1024 KB), 'Payload threshold time' (60 secs), and 'Maximum disk usage for EDR Data' (1024 MB). At the bottom of the main area is another toggle switch for 'Enable Malware Protection for this Profile' set to 'ON'. 'Cancel' and 'Save' buttons are at the bottom of the window.

Step 2 - Configure Rule-Based Alerts for Events

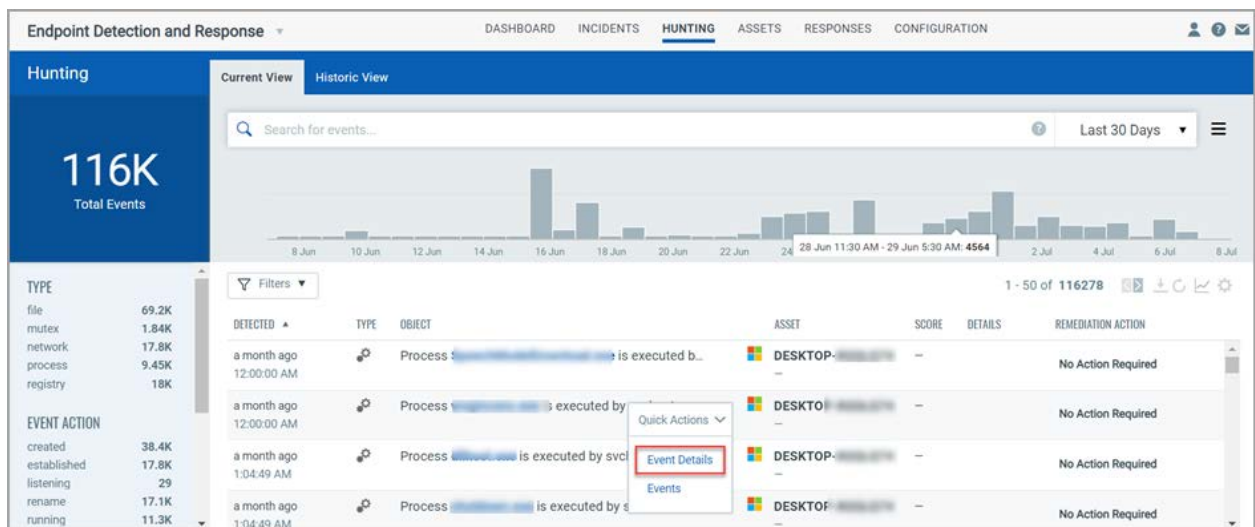
You can configure EDR to monitor events for conditions specified in a rule and send you alerts if events matching the condition are detected. For EDR to send alerts, you must first configure a rule action to specify the action taken when events matching a condition are detected. EDR will use the rule action settings to send you the alerts. Finally, create a rule to specify the conditions for triggering the rule and select rule actions for sending the alert when a rule is triggered.

For detailed steps, refer to [Configure rule-based alerts for events](#)



Step 3 - View Events and Detections

All detections and events are listed in the Hunting tab. You can view details of each event and perform remediation actions (Quarantine File/ Delete File/ Kill Process) on File, Mutex, Network, and Process events. Refer to [View Event Details](#)



Multi-Vector EDR collects endpoint telemetry and flags suspicious activity associated with the vulnerability. EDR capabilities help you:

1. Detect java.exe processes with an LDAP network connection
2. Search for Log4j Vulnerabilities by collecting and inventorying all .jar files on a system
3. Detect internal lateral movement attempts by flagging on curl.exe and Log4j payloads
4. Detect java.exe process that spawns unusual child processes

To search for assets with the Log4j vulnerability, search using the following query

Vulnerabilities.vulnerability.cveld:CVE-2021-44228

Qualys Express

Endpoint Detection and Response

DASHBOARD INCIDENTS HUNTING **ASSETS** RESPONSES CONFIGURATION

Assets

Active Threats By Host

1 Total Asset

TAGS

Cloud Agent 1

testtag 1

Search: vulnerabilities.vulnerability.cve2019-44228

1 - 1 of 1

| NAME | OPERATING SYSTEM | AGENT VERSION | LAST CHECKED IN | CREATED ON | AV STATUS | LAST LOGGED IN USER | TAGS |
|---------------------------------------------------------------------------|--------------------------------------------------------------------------|---------------|-----------------|--------------|-----------|---------------------|-------------|
| dmurphy-w7x86 70.112.205.112, fe80:0:0:0:0:0:0:0:1415:272e-9640 | Microsoft Windows 7 Enterprise 6.1.7601.32-bit Service Pack 1 Build 7601 | 4.1.0.51 | Sep 30, 2020 | Sep 21, 2020 | - | Administrator | Cloud Agent |

Refer to the following docs to get started with EDR

[EDR Onboarding Videos](#) | [EDR Getting Started Guide](#) | [EDR Online Help](#)