Seqrite

Endpoint Protection EDR

SEQRITE

EDR Deployment Guide

EDR 1.4.0

www.seqrite.com

Copyright Information

Trademarks

License Terms

Installation and usage of Seqrite Endpoint Security is subject to user's unconditional acceptance of the Seqrite end-user license terms and conditions.

To read the license terms, visit http://www.seqrite.com/eula and check the End-User License Agreement for your product.

Contents

Overview

The Endpoint Detection and Response (EDR) is a platform deployed on an organization's own infrastructure rather than on a cloud-based environment. It is a system designed to protect the endpoints from the network from potential cyber threats. EDR helps detect and respond to the threats that may evade the traditional antivirus and other security solutions deployed at the endpoint.

Audience

This guide is helpful for Seqrite Administrators and SOC Managers using EPP 8.4 with EDR edition.

Prerequisites

- EPP Server installed (Refer this link for more details on Installing EPP Server.)
- EPP server with EDR license activated.
- Update Manager must be installed. (Refer this link for more details on Update Manager Guide.)

System requirements for EDR

- Operating System: **Ubuntu** 24.04 LTS server edition
- VM requirements:
    - Master (1 VM) - 4 vCPU / 8GB RAM / 200GB Disk
    - Worker (1 VM) - 16 vCPU / 64 GB RAM / 500GB Disk

  NOTE:
    - 100 GB of free disk space on /var (both on Master & Worker nodes)
    - 30 GB of free disk space on /home on Master node
- As a part of best practice, all VMs must have a clean OS snapshot.
- Data Retention: 30 days
- High Availability: No

System requirements for EDR with required Endpoints

EDR	Master node			Worker node(s)			
Operating Sys	**Ubuntu 24.04 LTS**			**Ubuntu 24.04 LTS**			
Endpoints	**CPU**	**Memory**	**Disk (SSD)**	**Worker(s)**	**CPU**	**Memory**	**Disk (SSD)**
< =20	4 Core 2.60GHz or above	8 GB	200 GB	Worker 1	12 Core 2.60GHz or above	42 GB	500 GB
<1000	4 Core 2.60GHz or above	8 GB	500 GB	Worker 1	40 Core 2.60GHz or above	96 GB	3.7 TB
1000 - 2000	4 Core 2.60GHz or above	8 GB	500 GB	Worker 1	40 Core 2.60GHz or above	96 GB	7 TB
2000-4000	4 Core 2.60GHz or above	8 GB	500 GB	Worker 1	48 Core 2.60GHz or above	96 GB	12 TB
4000-5000	4 Core 2.60GHz or above	8 GB	500 GB	Worker 1	48 Core 2.60GHz or above	112 GB	15 TB
5000-10000	8 Core 2.60GHz or above	16 Gb	500 GB	Worker 1	64 Core 2.60GHz or above	128 GB	30TB
50000	8 Core 2.60GHz or above	16 GB	0.5 TB	Worker 1	72 Core 2.60GHz or above	144 GB	112 TB

				Worker 2	72 Core 2.60GHz or above	144 GB	112 TB
				Worker 3	72 Core 2.60GHz or above	144 GB	112 TB
				Worker 4	72 Core 2.60GHz or above	144 GB	11 TB

System requirements for EDR Update Manager

CPU	Memory	Disk	Supported Platforms
2 Core	4 GB	50 GB	• Linux Mint 19.2 • Linux Mint 20 64bit • Ubuntu 22 • openSUSE 42.3 64bit • openSUSE 15.2 64bit • Ubuntu 20.04 64bit • Red Hat Enterprise Linux 9.1 • BOSS 6 32bit • BOSS 8 64bit • Rocky Linux

Supported platforms for EDR Clients

Windows (64 bit)	Linux (64 bit)	Mac OS
Windows 8.1	RHEL 8.2	macOS 10.15 Catalina
Windows 10	RHEL 9.1	macOS 11 Big Sur
Windows 11	Linux Mint 20	macOS 12 Monterey
Windows server 2012 R2	Ubuntu 17.04	macOS 13 Ventura
Windows server 2016	Ubuntu 20.04	macOS 14 Sonoma
Windows Server 2019	Ubuntu 22.04	macOS 15 Sequoia
Windows Server 2022	openSUSE 15.2 64bit	
Windows Server 2025	openSUSE leap 42.3	
	Debian 11	
	Rocky 8.4	
	CentOS 8	
	CentOS 8.2	
	Fedora 32 64bit	
	BOSS 8 64bit	

Getting Started

Prerequisites

- Supported operating system**:** Ubuntu 24.04 LTS (Server Edition)
- User privileges**:** Sudo access is required
- Network connectivity**:** Internet or intranet connectivity must be established between the EPP, master, and worker nodes
- Minimum hardware requirements**:** Ensure that all systems meet the defined minimum hardware specifications
- Kernel version consistency**:** The kernel version must be identical on both the master and worker systems

Note: The recommended screen resolution to view Seqrite EDR Portal is below 1440 X 900.

Deployment Overview

The deployment process is designed to be simple and guided. It includes the following steps:

1. Download the installation package.
2. Run the installation shell script.
3. Provide required inputs through the CLI prompt (for example, master node IP, worker node details, passwords).
4. The installer will automatically configure and deploy all necessary components based on the provided.

Note: The installation script may take approximately one hour to complete execution, depending on system performance and network conditions.

Installation Steps

The following steps will guide you through the installation process to set up the Seqrite EDR platform on your environment.

1. Log in or switch to a user account that has sudo privileges**.**
2. Run the following command to download the installation **.sh** file provided by Seqrite:
   wget https://dlupdate.quickheal.com/builds/seqrite/83/ope/en/build/Seqrite_EDR_Installer_1_4_0.sh
   or, wget https://download.quickheal.com/builds/seqrite/83/ope/en/build/Seqrite_EDR_Installer_1_4_0.sh
3. Run the following command to make the script executable:
4. chmod +x ./Seqrite_EDR_Installer_1_4_0.sh
5. Run the following command to execute the installer script.
   sudo ./Seqrite_EDR_Installer_1_4_0.sh -c
6. When prompted, enter the necessary configuration details. These may include:
   - EPP FQDN or IP address
   - EPP License Key
   - EDR Master node FQDN or IP, Username, Password

     For example:

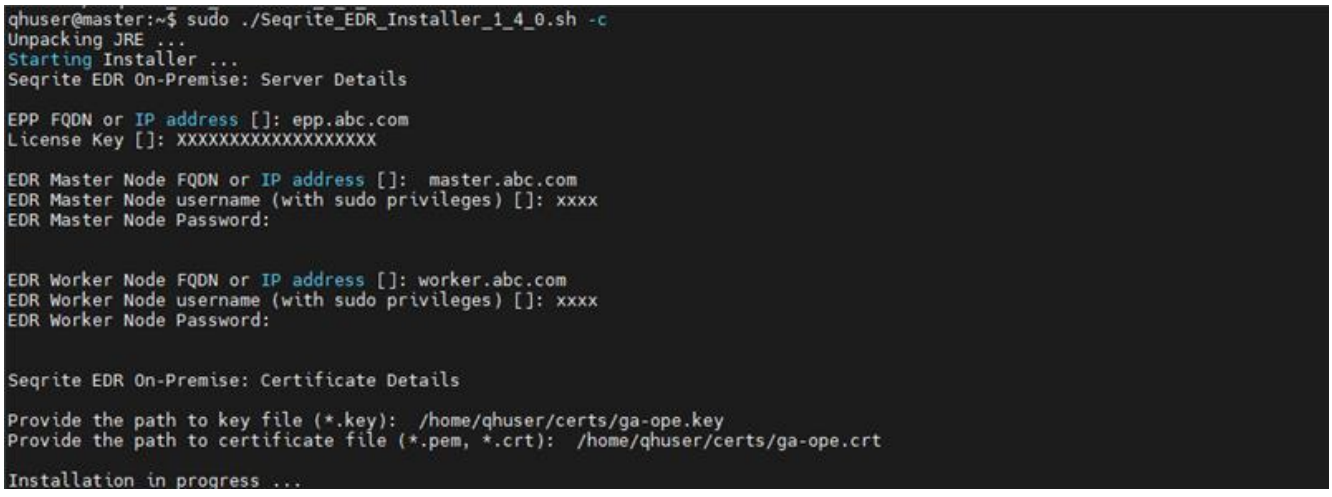
     IP ADDRESS: 192.168.x.x,

     FQDN: master.ope.com
   - EDR Worker node FQDN or IP, Username, Password

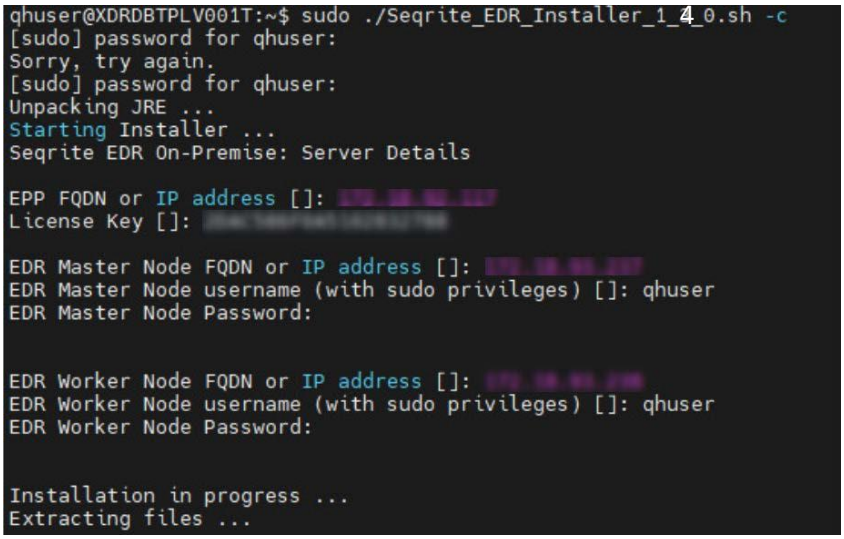
     For example:

     IP ADDRESS: 192.168.x.x,

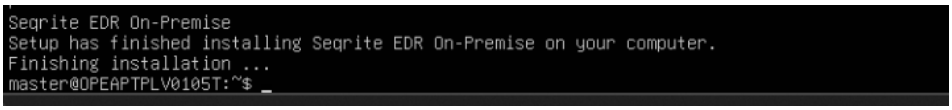
     FQDN: master.ope.com
7. In case of FQDN, provide the path as input on CLI, where the .key and .crt files are present.



8. In case of IP address, refer this image:



This message confirms that the script has run successfully, and all components have been installed.



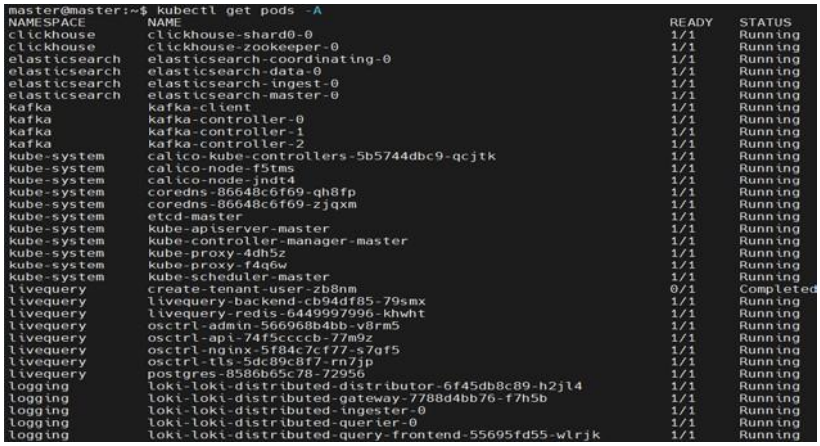
Installation Verification

After the installation is completed, verify that the deployment was successful by performing the following steps:

1. Run the following command to ensure all pods are in a running state:

   `kubectl get pods -A` -

   This command displays the status of all pods.



```
master@master:~$ kubectl get pods -A
NAMESPACE       NAME                                                READY   STATUS
clickhouse      clickhouse-shard0-0                                 1/1     Running
clickhouse      clickhouse-zookeeper-0                              1/1     Running
elasticsearch   elasticsearch-coordinating-0                        1/1     Running
elasticsearch   elasticsearch-data-0                                1/1     Running
elasticsearch   elasticsearch-ingest-0                              1/1     Running
elasticsearch   elasticsearch-master-0                              1/1     Running
kafka           kafka-client                                        1/1     Running
kafka           kafka-controller-0                                  1/1     Running
kafka           kafka-controller-1                                  1/1     Running
kafka           kafka-controller-2                                  1/1     Running
kube-system     calico-kube-controllers-5b5744dbc9-qcjtk            1/1     Running
kube-system     calico-node-f5tms                                   1/1     Running
kube-system     calico-node-jndt4                                   1/1     Running
kube-system     coredns-86648c6f69-qh8fp                            1/1     Running
kube-system     coredns-86648c6f69-zjqxm                            1/1     Running
kube-system     etcd-master                                         1/1     Running
kube-system     kube-apiserver-master                               1/1     Running
kube-system     kube-controller-manager-master                      1/1     Running
kube-system     kube-proxy-4dh5z                                    1/1     Running
kube-system     kube-proxy-f4q6w                                    1/1     Running
kube-system     kube-scheduler-master                               1/1     Running
livequery       create-tenant-user-zb8nm                            0/1     Completed
livequery       livequery-backend-cb94df85-79smx                    1/1     Running
livequery       livequery-redis-6449997996-khwht                    1/1     Running
livequery       osctrl-admin-566968b4bb-v8rm5                       1/1     Running
livequery       osctrl-api-74f5ccccb-77m9z                          1/1     Running
livequery       osctrl-nginx-5f84c7cf77-s7qf5                       1/1     Running
livequery       osctrl-tls-5dc89c8f7-rn7jp                          1/1     Running
livequery       postgres-8586b65c78-72956                           1/1     Running
logging         loki-loki-distributed-distributor-6f45db8c89-h2jl4  1/1     Running
logging         loki-loki-distributed-gateway-7788d4bb76-f7h5b      1/1     Running
logging         loki-loki-distributed-ingester-0                    1/1     Running
logging         loki-loki-distributed-querier-0                     1/1     Running
logging         loki-loki-distributed-query-frontend-55695fd55-wlrjk 1/1     Running
```

   [Screenshot: Successful pod status]

   For example: kubectl logs ope-misp-engine-7dc49b6f6c-jns8k -n service

   This command retrieves the logs of the ope-misp-engine pod within the service namespace. Use it to troubleshoot or confirm that services are running as expected.

2. Open a web browser and navigate to the Seqrite EDR interface using the configured IP address or hostname (FQDN).

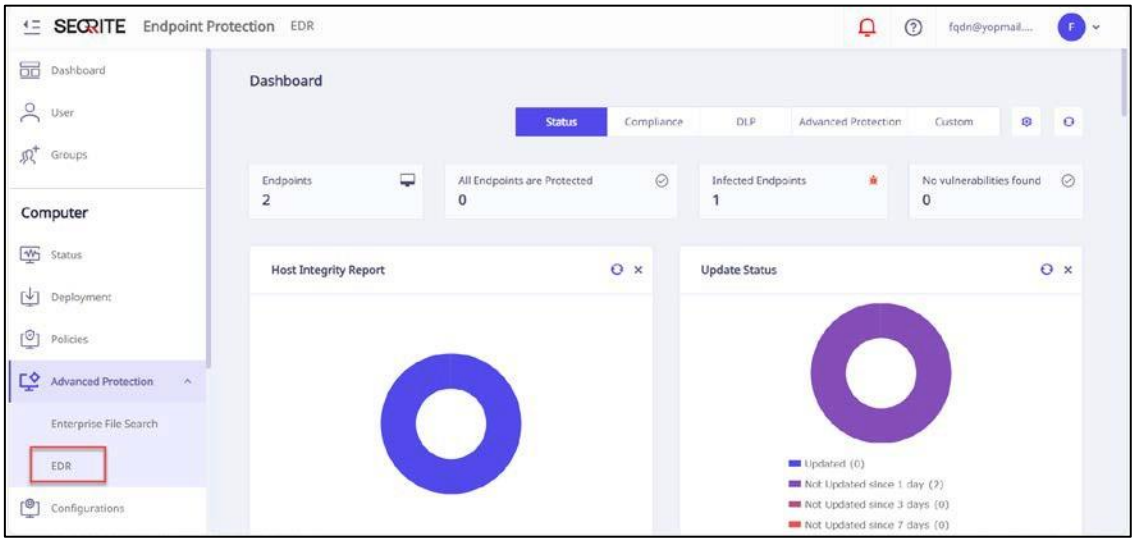
   Syntax: https://<IP_or_FQDN>/eps/login

   For example:

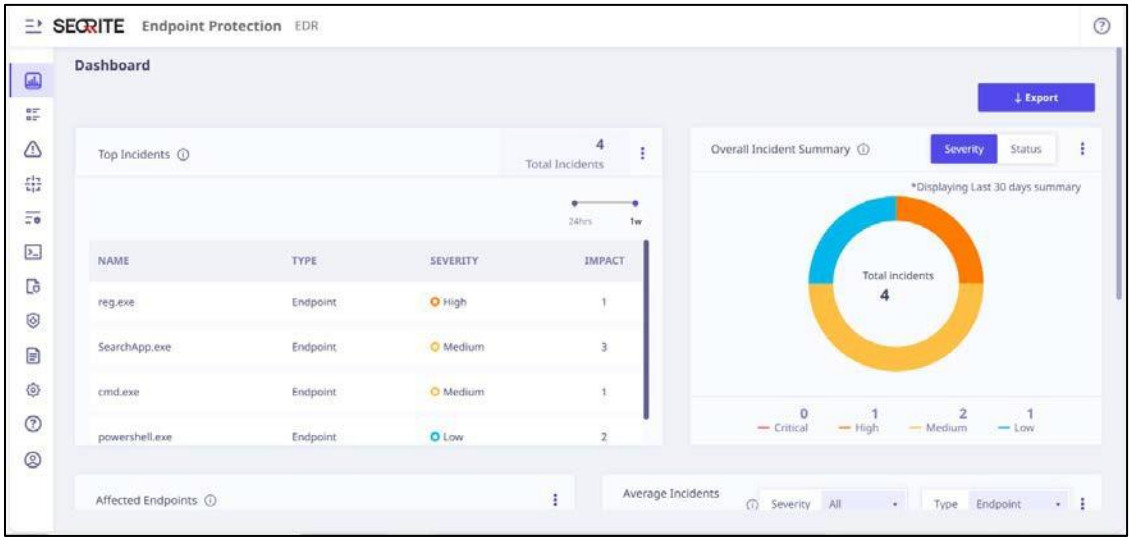
   - https://192.168.x.x/eps/login,
   - https://epp.abc.com/eps/login

3. Log in to the platform:

   a. First, log in to the **EPP**.



b. After successful authentication, click **Advanced Protection** > **EDR** from the left panel to be automatically redirected to the **EDR** dashboard.



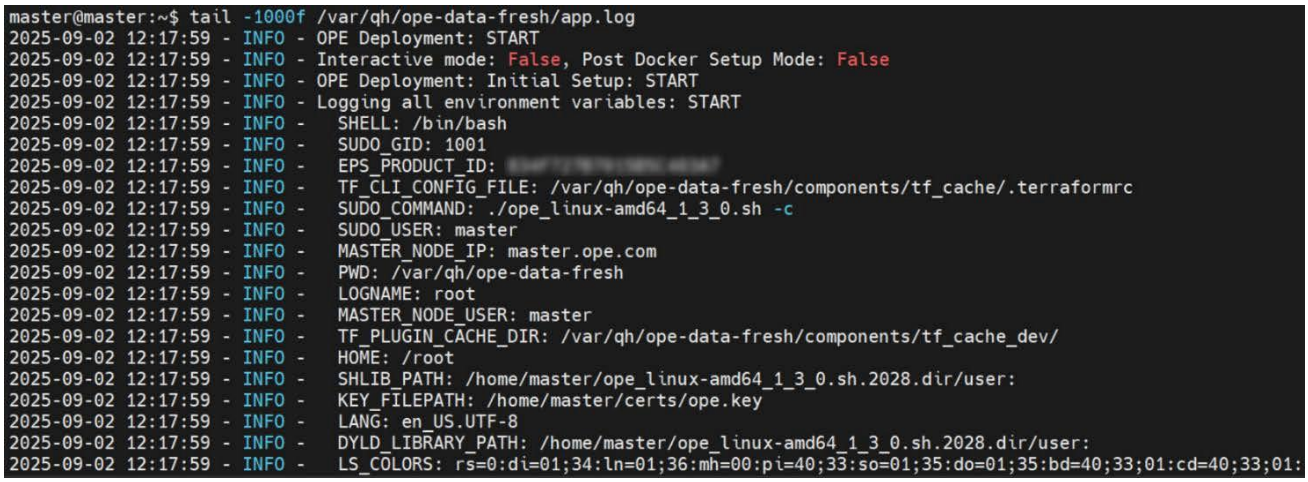
[Screenshot: Seqrite EDR login page]

Troubleshooting

If you encounter issues during installation, follow these steps:

1. **Verify the operating system version**
   Ensure that the system is running **Ubuntu 24.04 LTS**. Other versions are not supported.
2. **Validate system resources**
   Make sure that there is adequate **disk space** and **available memory** to support the installation process.
3. **Review installation logs**
   If the installation fails,
   a. check the log file at **/var/qh/ope-data-fresh/app.log** for detailed error messages.
   b. Open a separate terminal window and run the following command:

      tail -f /var/qh/ope-data-fresh/app.log



Post installation update set-up

Users can configure OPE updates post-installation and access the EDR updates file/folders from the specified locations.

- EDR files/folders restored at the predefined location.
- Update Manager: https://dlupdate.quickheal.com/builds/seqrite/cai/suum/installer/eng/SUUMunix64.zip

Configuring updates through predefined location

Users will automatically get the updated EDR files/folders from the predefined location.
To automatically fetch updates, user needs to modify the following path:

- /var/qh/ope-data-fresh/deploy/data/updater/updater.ini

Let's assume the files at the predefined location: **/home/qhuser/seqrite-update-manager-download**

- Modify: **/var/qh/ope-data-fresh/deploy/data/updater/updater.ini** the file using the above-mentioned path.
- In the below [checksum] section, the LocalPath and LocalChecksumJson should not be modified.
- UseNewCopy = true (suggests that the EDR should regularly check the folder at NewCopyPath for new-or-updated files)

  Note: Please do not modify any other entries on the updater.ini file.
- If Update-Manager is installed on the same machine where EDR is also installed, then only modify the **NewCopyPath** and **NewCopyChecksumJson** in the **updater.ini** located at the following path:
  - **/var/qh/ope-data-fresh/deploy/data/updater/updater.ini**

    [checksum]

    NewCopyPath = <http://<ip-of-update-manager>>:8080/edr

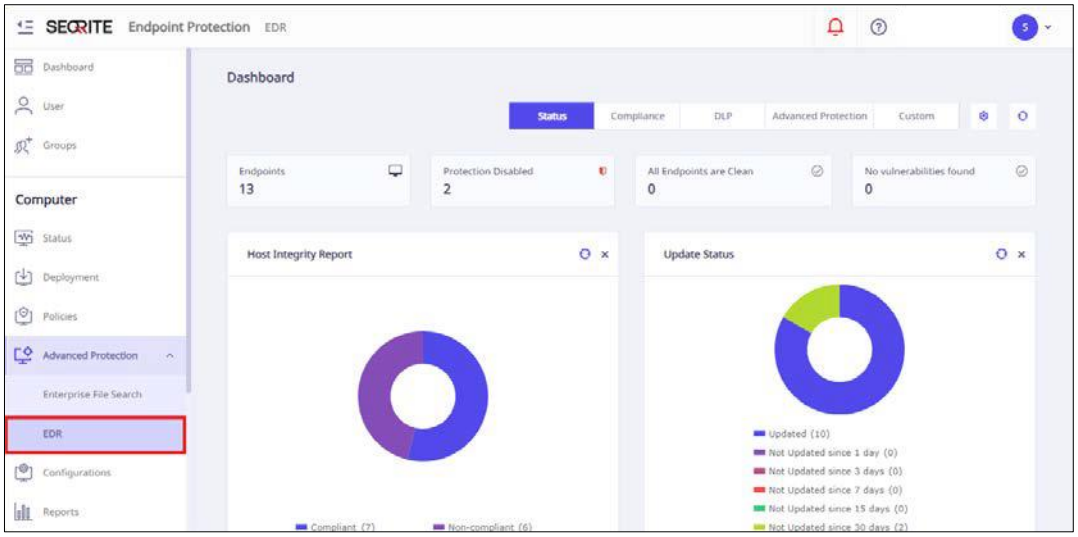
    NewCopyChecksumJson = http://<ip-of-update-manager>:8080/file-server

Steps to access EDR

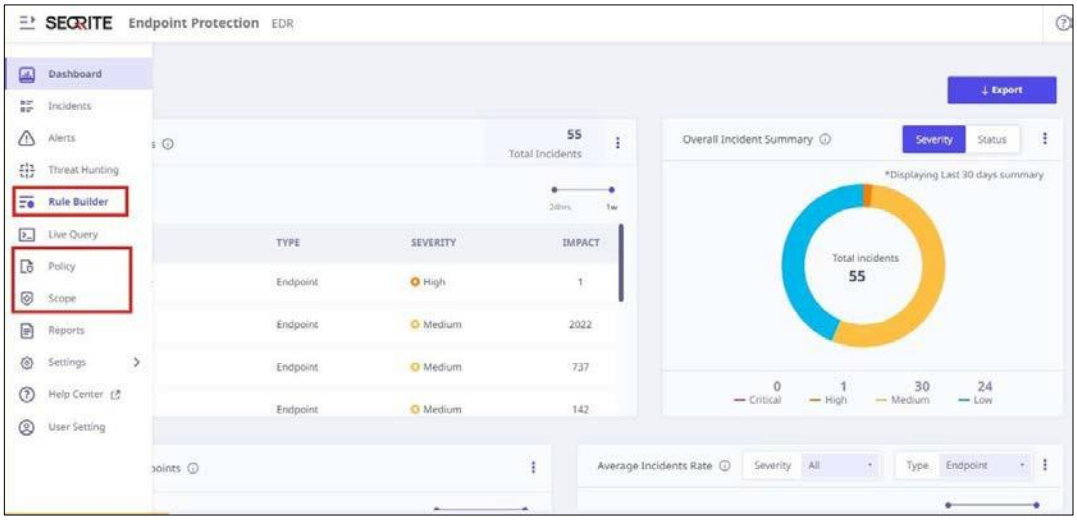
After the OPE set up, users can now access EDR by login to EPP. To begin follow these steps,

1. Login to EPP console page.
2. Create one user with SOC Manager role in EPP.
3. Logout.

4. Login again to EPP with the newly created user.
5. Access EDR Edition located under “Advanced Protection” tab on the EPP console page. The following screen appears.



6. EDR User Interface opens in a new tab verify “Rule Builder “, “Policy , and “Scope “sections those created EPP are synced with the EDR Edition.



Uninstalling EDR

To uninstall the EDR server, use the command below and provide the appropriate inputs when prompted.

sudo /var/qh/uninstall -c -Dinstall4j.log=/tmp/ope-uninstall.log

Note: Execute the above command from any location except /var/qh.