Seqrite
Malware Analysis Platform

User Guide

V 2.1 December 19, 2025

www.seqrite.com

Copyright and License Information

Trademarks

License Terms

Release Date

December 19, 2025

Contents

Introduction

In today’s interconnected world, devices frequently communicate over the Internet, leading to frequent data exchanges. This constant flow makes data susceptible to viruses and malware. As data travels through various host computers, it can become vulnerable to infection from malicious programs. To ensure data safety, it is crucial to check whether files are clean or infected. Malicious programs can silently spread and compromise data and legitimate program files without immediate detection.

The Seqrite Malware Analysis Platform is designed to help users submit and analyze suspicious files for potential threats.

How does SEQRITE Malware Analysis Platform Work?

The Seqrite Malware Analysis Platform is an automated system that can be deployed either on customer premises or in the cloud. It allows users to upload suspicious files for scanning and analysis to detect malware and viruses. Users can search for previously analyzed files using checksums like MD5, SHA1, or SHA256, or through various search parameters and keywords. Additionally, users can review the category of URLs before visiting them.
The platform operates with multiple microservices that perform static, dynamic, and manual analyses of the uploaded files. Users can view a consolidated analysis summary to determine whether a file is clean or malicious. After analysis, reports are available in both PDF and JSON formats.

On – Premise Deployment

Accessing Seqrite Malware Analysis Platform

If you are accessing the Seqrite Malware Analysis Platform for the first time, follow these three steps:

A. Register with Seqrite Malware Analysis Platform/Sign-Up with Seqrite Malware Analysis Platform
B. Set Password
C. Sign In to Seqrite Malware Analysis Platform

A. Registering with Seqrite Malware Analysis Platform/Sign-Up with Seqrite Malware Analysis Platform

To access Seqrite Malware Analysis Platform, you must first register using a product key To register with Seqrite Malware Analysis Platform, follow these steps:

1. Enter the URL in the browser. The **Sign In** page is displayed.
2. Click **Register Here**. The **Register for Malware Analysis Platform** page is displayed.
3. Enter the **Malware Analysis Product Key** and enter **Next**.
4. Enter the Administrator Details that are, First Name, Last Name, Business Email Address, Mobile No., Job Role, and then click **Next**.
5. Enter the Company Details like Company Name, Industry, Company Size, Company Address, Country, State, City, Pin Code, and click **Next**.
   The **Confirmation** page is displayed.
6. If the email address is incorrect, click **Click Here** to update it.
7. Select the checkbox to agree to the terms and conditions and click **Confirm**.
   You will receive an activation link on the registered email address.

B. Set Password

Once you register successfully, you will receive an email with activation link to set a password. To set a password, follow these steps:

1. Click the activation link given in the email.
2. Enter password and click **Set Password**.
   The **Sign-In** page is displayed.

C. Signing In

- On the sign-in page, enter the email ID and password and click **Sign-In**.

Cloud Deployment

Accessing Seqrite Malware Analysis Platform

If you are an existing user, follow the sign in process. If you are a new subscriber, follow the following three steps.

A. Register with Seqrite Malware Analysis Platform/Sign-Up with Seqrite Malware Analysis Platform
B. Set Password
C. Signing-In to Seqrite Malware Analysis Platform

A. Register with Seqrite Malware Analysis Platform/Sign-Up with Seqrite Malware Analysis Platform

To access Seqrite Malware Analysis Platform, you must first register using a product key. To register with Seqrite Malware Analysis Platform, follow these steps:

1. Enter the URL **https://qaint-csm.qhtpl.com/csm/signup/smap** in the browser. The **Sign-Up** page is displayed.
2. Click **Register Here**.
   Register for Centralized Security Management page is displayed.
3. Select the **Malware Analysis Platform (MAP) Product Key** checkbox, enter the product key, and click **Next**.
4. Enter the **Administrator Details** like First Name, Last Name, Business Email Address, Mobile No., Job Role, and click **Next**.
5. Enter the Company Details like, Company Name, Industry, Company Size, Country, State, City, Preferred Product Language, and click **Next**.
6. If the email address is incorrect, click **Click here to edit** to update the email address and click **Confirm**.

B. Set Password

Once you register successfully, you will receive an email with the activation link to set password. To set a password, follow these steps:

1. Click the activation link given in the email.
2. Enter password and click **Set Password**.
   The **Sign In** page is displayed.

D. Signing In

1. Enter the email ID, password and click **Sign In**.
   The **Two- factor Authentication** page is displayed.
2. Enter the OTP you have received on your registered email address or registered phone number and click **Verify**.
   The **Seqrite Centralized Security Management License Agreement** page is displayed.

3. Agree with the terms of **SEQRITE END-USER LICENSE AGREEMENT** and click. **Yes, I Agree**
   The Seqrite Centralized Security Management dashboard is displayed.
4. Click **SMAP** on the left pane.
   You will land on the home page that is on the **Seqrite Malware Analysis Platform** dashboard.

User Roles

In Seqrite Malware Analysis Platform, the user roles assigned to the users can be of the following:

1. Organization Analyst
2. Organization Admin
3. Organization Executive
4. Threat Researcher

The following table displays the features available for the users as per the assigned role.

Feature	Org Analyst	Org Admin	Org Executive	Threat Researcher
Dashboard	Yes	Yes	Yes	Yes
File Upload (Single File or Zip)	Yes	Yes	No	No
URL Reputation Lookup	Yes	Yes	Yes	Yes
Advanced Free Text Search	Yes	Yes	Yes	Yes
Download Report	Yes	Yes	Yes	Yes
Add Tags	Yes	Yes	No	Yes
Notifications	Yes	Yes	Yes	Yes
User Management	No	Yes	No	No
Manual Analysis	No	No	No	Yes

Dashboard

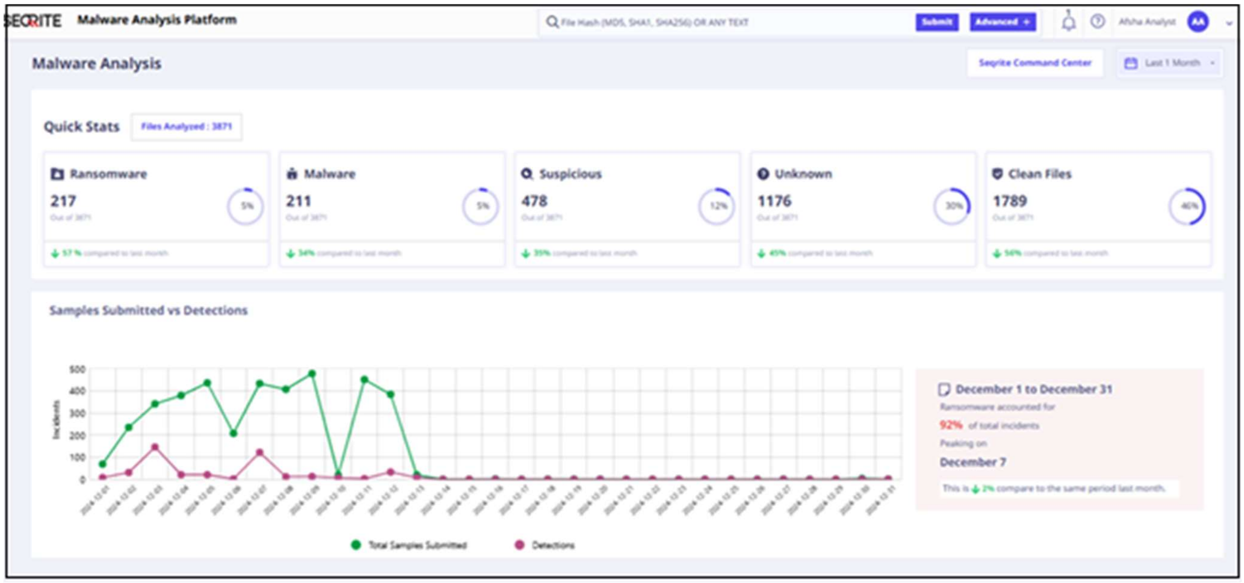
Post login, the dashboard is the default landing page for all the users. On the dashboard the following default metrics are provided:

A. Seqrite Malware Analysis Platform (SMAP) Metrics

B. Command Center

A. Seqrite Malware Analysis Platform (SMAP) Metrics

Seqrite Malware Analysis Platform metrics are used to evaluate and classify malicious samples. They help to understand malware behavior, detect threats, and improve security.



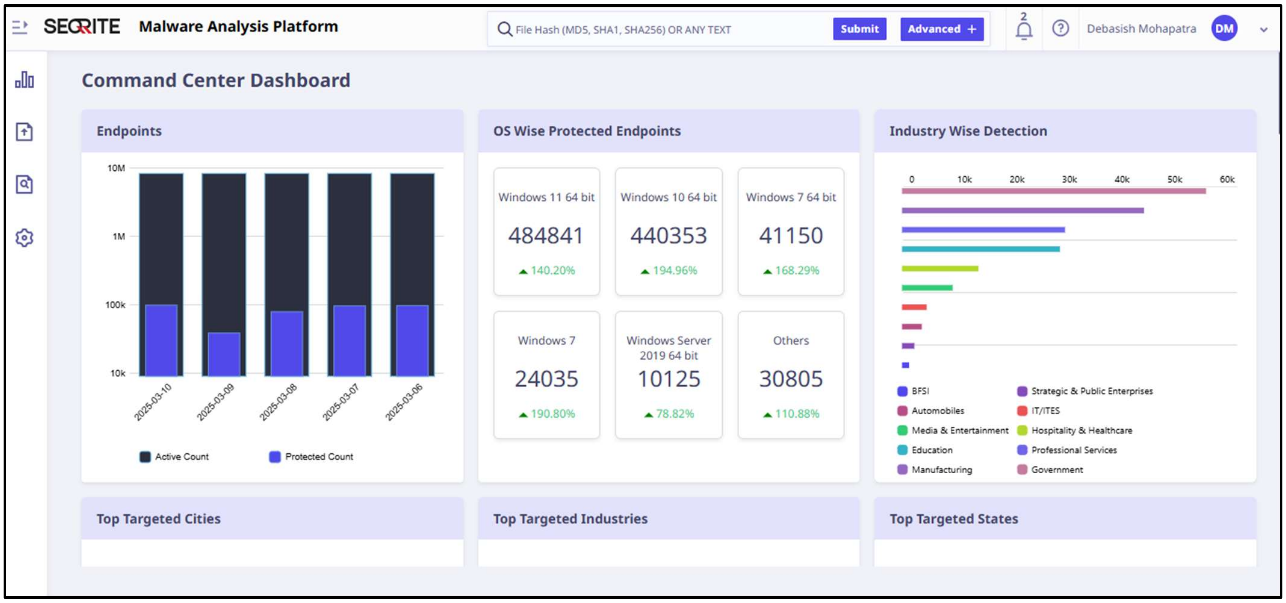
The dashboard shows the following SMAP metrics:

Metrics	Description
Quick statistics of analyzed file	It shows the bifurcation of analyzed files.
Samples Submitted vs Detection	It shows the total number of files submitted and detection.
Top malware categories	It shows the top malware categories along with their respective count.
Top Malicious File Types	It shows the top malicious files, sample submitted to analyze, number of detections, and detection percentage.
Submission Methods and Top sources contributing to detection	It shows the number of manual and auto submission of files, and top sources contributing to detection.

Metrics	Description
Top Malware Families Detected	It shows the top malware families along with their name, category, detection rate and detection date.
Trending Tags in Malware Analysis	It shows the top trending tags.

B. Command Center

Command Center projects insights from Seqrite's telemetry, which is gathered from our 10 million endpoints.



Accessing Command Center

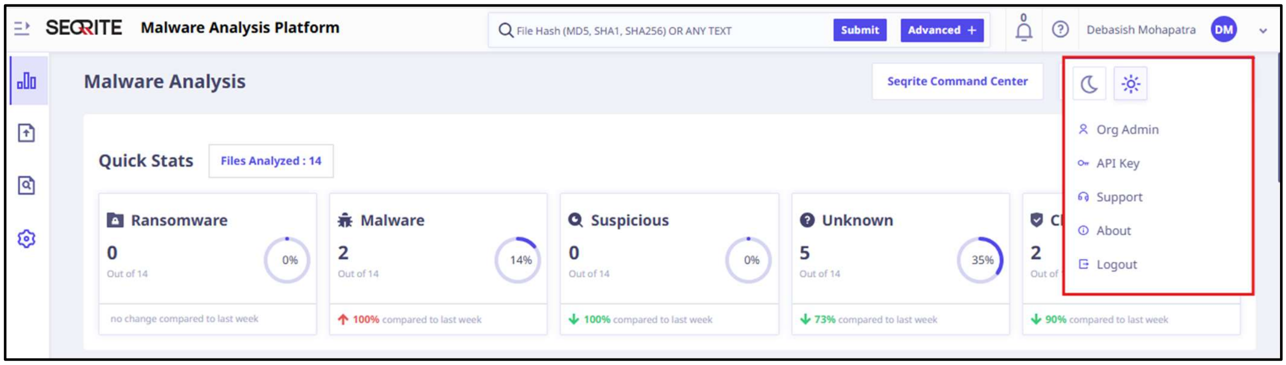
To access and view the command center, click the **Seqrite Command Center** on top right of the dashboard. The following are the key metrics on the command center:

Metrics	Description
Endpoints (Total active and Protected endpoints)	It shows the number of devices where Quick Heal antivirus is installed and among them how many endpoints were recently protected from Threats.
OS wise protected end points	It shows operating system wise protected end points numbers.
Top targeted states/cities	It shows the top 10 targeted cities and states by the number of detections.
Top targeted industries	It shows the top 10 target industries by number of detections.
Top Attacking Remote IPs	It shows the number of malicious active remote Ips.

Metrics	Description
Top Ransomware families	It shows the top 10 active ransomware families.
Top Vulnerabilities	It shows the top 10 detected vulnerabilities.
Threat Map	It is a visual representation of cyber threats across India.

User Profile

The User Profile section on the upper-right corner of the dashboard shows the name of the registered user.

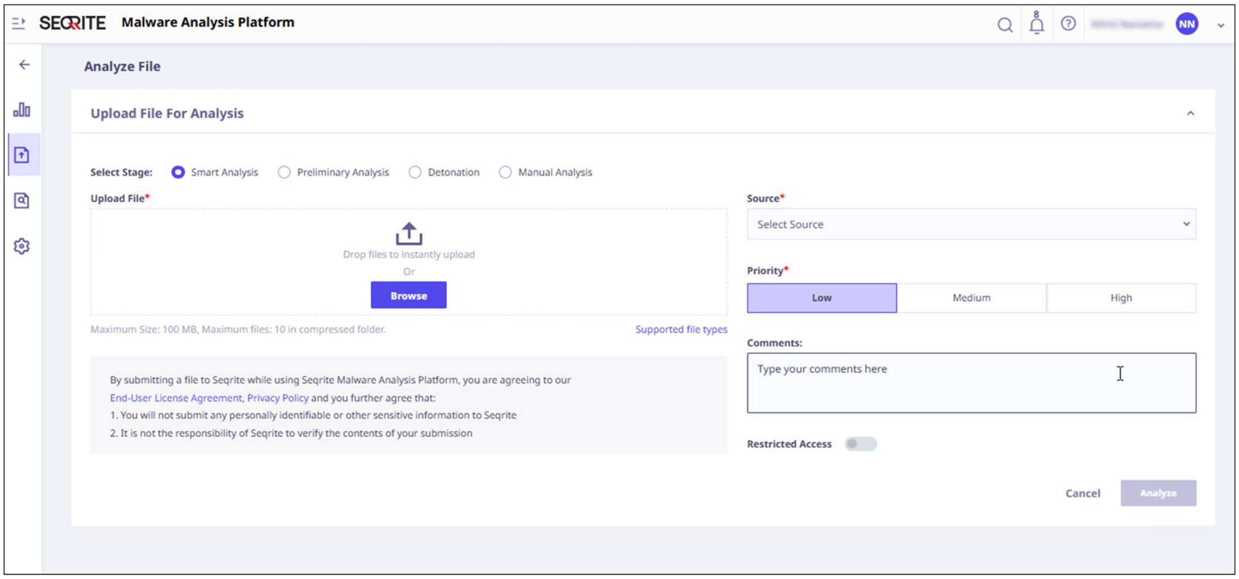


When you click the logged-in username, the options displayed are, screen appearance that is Dark Theme and Light Theme, Role, API Key (You can use the above API Key to submit files and retrieve verdicts through the SMAP APIs), Support, list of the open-source tools/library and licenses under About, and Logout.

Analyze File

For analyzing files, click **Analyze File** on the left pane. This page displays the following options:

- Upload file for analysis.
- File analysis report that is historical uploads in tabular format with sorting options. Ability to search through the upload history using filters such as days, status, and source of submission.
- Advanced Global Search using free text search and predefined filters.



Select Stage: ● Smart Analysis ○ Preliminary Analysis ○ Detonation ○ Manual Analysis

Upload File*

Maximum Size: 100 MB, Maximum files: 10 in compressed folder.

By submitting a file to Seqrite while using Seqrite Malware Analysis Platform, you are agreeing to our End-User License Agreement, Privacy Policy and you further agree that:
1. You will not submit any personally identifiable or other sensitive information to Seqrite
2. It is not the responsibility of Seqrite to verify the contents of your submission

Source*: Select Source

Priority*: [✓ Low] Medium High

Comments: Type your comments here

Restricted Access

Upload File for Analysis

You can upload a single file or ZIP file, which needs to be scanned by Seqrite Malware Analysis Platform and then view the generated analysis report. The file size must be less than 100 MB. Threats if any, are detected by various scanners and highlighted in the generated consolidated report. You can also upload password protected ZIP files for analysis.

The Seqrite Malware Analysis platform supports coverage for Windows, Linux and Android operating systems.

After analysis, if SMAP identifies a file as malicious or ransomware, you can choose to share it as intel (IoC) with the Seqrite Threat Intel (STI) through SMAP - STI integration. To learn more about sharing intel with STI refer to, **Share Intel with Seqrite Threat Intel**.

Note: SMAP - STI integration is an add-on feature and requires activation. Please contact support team to enable it.

Seqrite Malware Analysis Platform supports the following file types for analysis:

Category	**File Type**
Office Documents	.doc, .docx, .docm, .potx, .potm, .rtf, .xls, .xlsx, .xlsm, .xlsb, .ppt, .pptm, .pptx, .pps, .ppsx, .ppsm, .ppam, .odt, .ods, .odp, .CSV
Scripts	.js, .py, .ps1, .bat, .vbs, .hta, .sh, .vba, .vbe, .vb, .reg, .python
Executables	.exe, .dll, .msi, .jar, .bat, .ps1, .vbs, .hta, .sh, .lnk, .elf
Archives	.zip, .cab, .7z, .rar, .tgz, .gz, .lzma, .xar, .gzip
Web Content	.html, .xml, .swf, .js, .htm, .url
Linux Executable	.elf, .sh, .py
Email Files	.eml, .msg
PDF & Portable	.pdf, .txt, .chm, .fpx, .asf, .hwp
Android	.apk

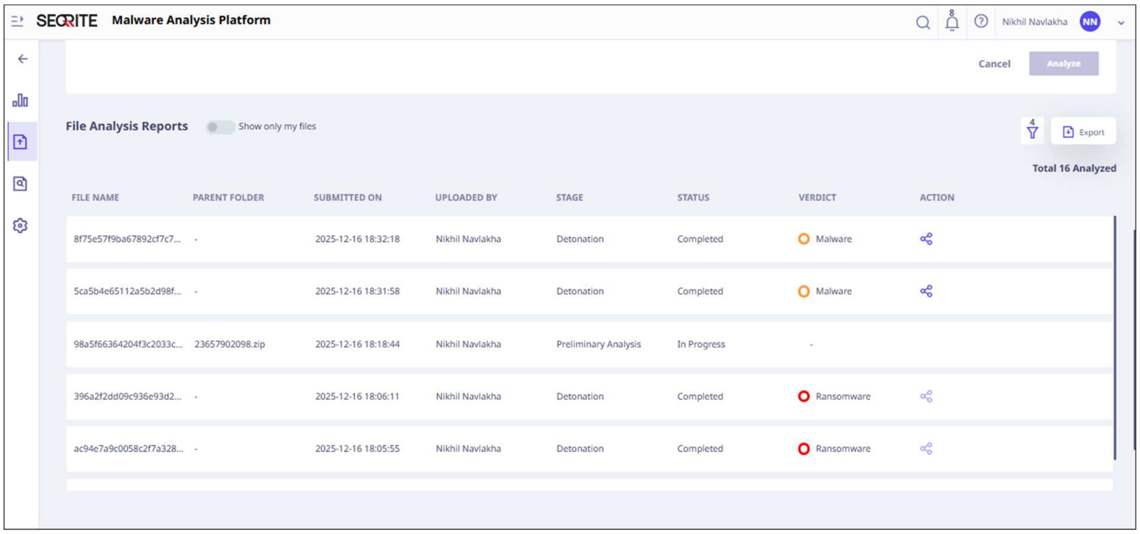
Note: You can upload zip files with max 10 files compressed within them.

To upload and submit the file for analysis, follow these steps:

1. Log in to the Seqrite Malware Analysis Platform and click the **Analyze File** on left pane.
2. On the **Analyze File** page, navigate to **Upload File for Analysis** and click **Browse**.
3. Select the file that you want to submit for analysis.
   Note: To analyze a password-protected ZIP file, you must provide the file’s password when uploading it.
4. Select **Stage** that is Smart Analysis, Preliminary Analysis, Detonation or Manual Analysis.
5. Select any predefined source from the **Source** list or select **Others**.
6. Select **Restricted Access**. You can restrict file access to users other than admin, if the file is of a sensitive nature.
7. Select Priority that is High, Medium or Low depending upon how fast you want to analyze the file.
8. Add **Comments** for reference and click **Analyze**.
   Once the file is submitted for analysis, the progress and status will be displayed in the list along with the submitted time stamp.
9. Click **View** to view the analysis of the submitted file. See Analysis Report for more information.

File Analysis Report (Upload History)

Seqrite Malware Analysis Platform displays the upload history for submitted files. It gives detailed information about uploaded files and helps to determine if it is malicious. You can filter the details by the Stage, Status, Verdict, Upload Period.



FILE NAME	PARENT FOLDER	SUBMITTED ON	UPLOADED BY	STAGE	STATUS	VERDICT	ACTION
8f75e57f9ba67892cf7c7...	-	2025-12-16 18:32:18	Nikhil Navlakha	Detonation	Completed	○ Malware	
5ca5b4e65112a5b2d98f...	-	2025-12-16 18:31:58	Nikhil Navlakha	Detonation	Completed	○ Malware	
98a5f66364204f3c2033c...	23657902098.zip	2025-12-16 18:18:44	Nikhil Navlakha	Preliminary Analysis	In Progress	-	
396a2f2dd09c936e93d2...	-	2025-12-16 18:06:11	Nikhil Navlakha	Detonation	Completed	○ Ransomware	
ac94e7a9c0058c2f7a328...	-	2025-12-16 18:05:55	Nikhil Navlakha	Detonation	Completed	○ Ransomware	

Stage

You can filter the history table by stage that is, Smart Analysis, Preliminary Analysis, Detonation, or Manual Analysis.

Status

You can filter the history table by Status. The Status Information for the uploaded files can be one of the following:

Sr. No.	Status	Description
1.	All	To view all the uploaded files.
2.	In Queue	Waiting to be processed.
3.	Failed	Analysis has failed.
4.	In Progress	File analysis in progress.
5.	Completed	Analysis is completed on time.

The history table displays the status of the files being analyzed along with the following details:

- File Name
- Parent File Name
- Submitted On
- Uploaded By

- Stage
- Status: In Progress, In Queue, Completed
- Verdict

You can view the report for the uploaded file by clicking **View**.

Verdict

You can filter the history table by Verdict such as Clean, Malware, Ransomware, and Suspicious.

Upload Period

The details of the uploaded files can be viewed for the following intervals:

- 1 Day
- 7 Days
- 1 Month
- 3 Months

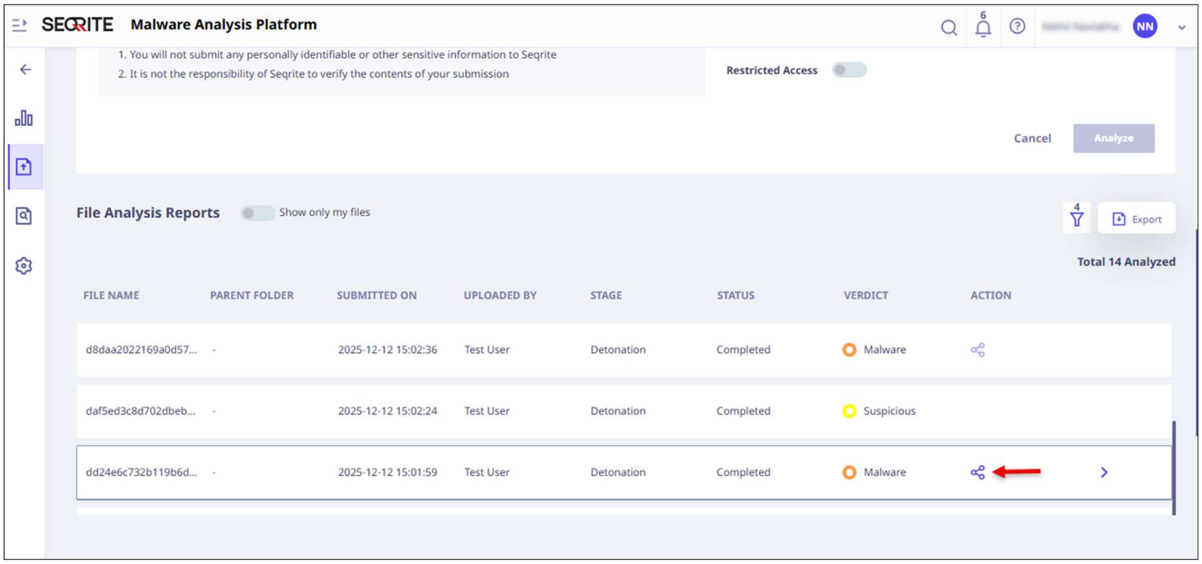
Share Intel with Seqrite Threat Intel

After analysis, if SMAP identifies a file as malicious or ransomware, you can share it as intel (IoC) with the Seqrite Threat Intel (STI) through SMAP - STI integration.

Note: Share Intel is available only for users who have subscribed for Seqrite Threat Intel.

To share a file as an intel, follow these steps:

1. On the **Analyze File** page, scroll down to **File Analysis Reports**.
2. Choose a file you want to share as intel and click .



1. You will not submit any personally identifiable or other sensitive information to Seqrite
2. It is not the responsibility of Seqrite to verify the contents of your submission

Restricted Access

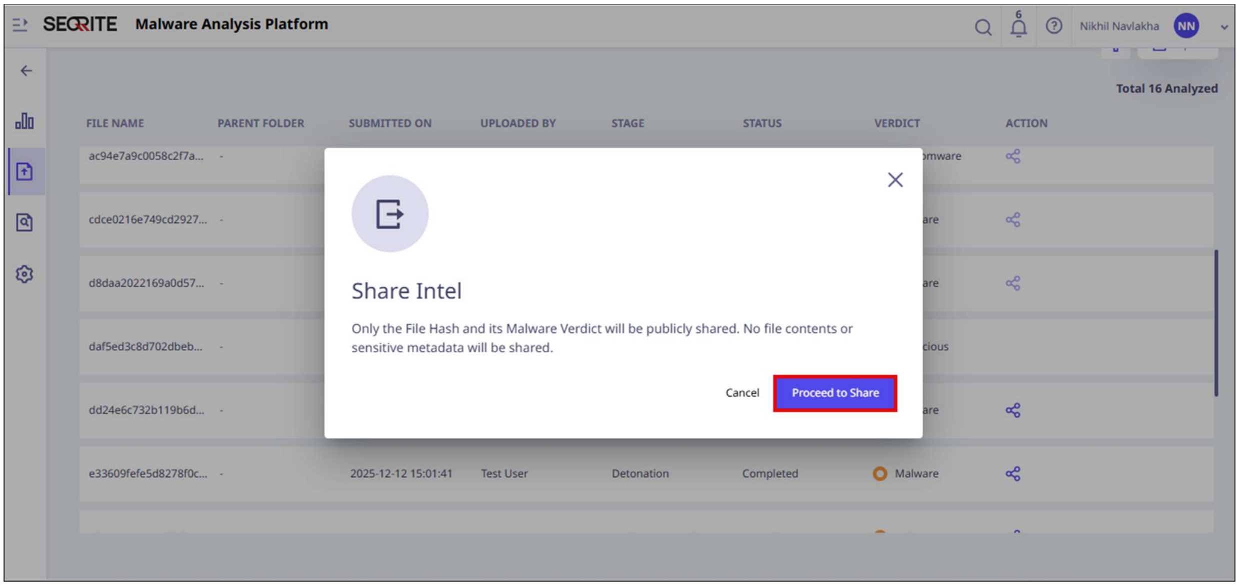
File Analysis Reports

Show only my files

Total 14 Analyzed

FILE NAME	PARENT FOLDER	SUBMITTED ON	UPLOADED BY	STAGE	STATUS	VERDICT	ACTION
d8daa2022169a0d57...	-	2025-12-12 15:02:36	Test User	Detonation	Completed	○ Malware	
daf5ed3c8d702dbeb...	-	2025-12-12 15:02:24	Test User	Detonation	Completed	○ Suspicious	
dd24e6c732b119b6d...	-	2025-12-12 15:01:59	Test User	Detonation	Completed	○ Malware	

3. Click **Proceed to Share**.



SEQRITE Malware Analysis Platform

Nikhil Navlakha NN

Total 16 Analyzed

FILE NAME	PARENT FOLDER	SUBMITTED ON	UPLOADED BY	STAGE	STATUS	VERDICT	ACTION
ac94e7a9c0058c2f7a...	-					mware	
cdce0216e749cd2927...	-					are	
d8daa2022169a0d57...	-					are	
daf5ed3c8d702dbeb...	-					cious	
dd24e6c732b119b6d...	-					are	
e33609fefe5d8278f0c...	-	2025-12-12 15:01:41	Test User	Detonation	Completed	Malware	

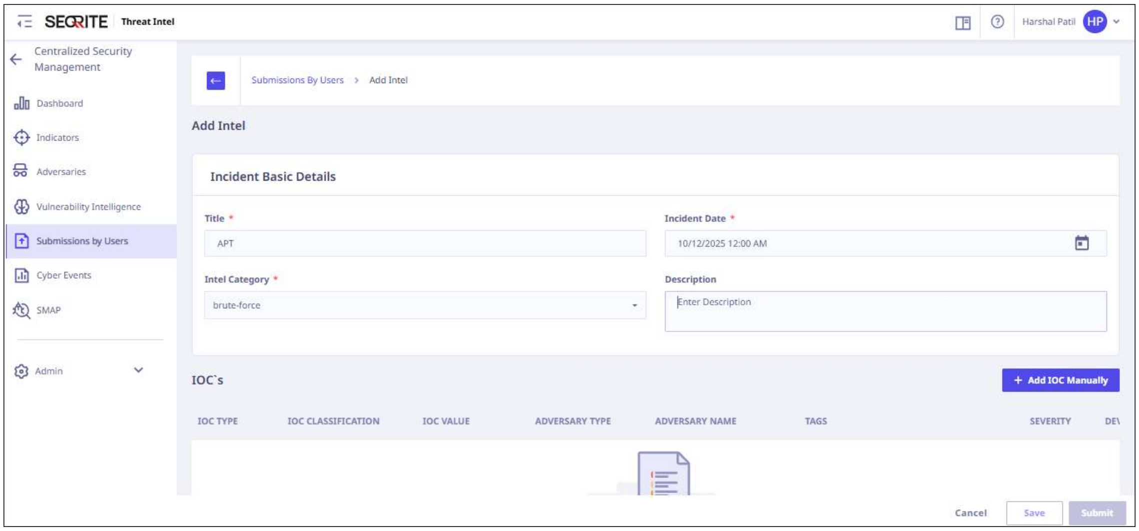
Share Intel

Only the File Hash and its Malware Verdict will be publicly shared. No file contents or sensitive metadata will be shared.

You will be redirected to the Seqrite Threat Intel page that is on **Submissions By Users** section to submit this intel and corresponding details.

Add New Intel

1. Enter **Incident Basic Details**, that are Title, Incident Date, Intel Category and Description, and click **Add IOC Manually**.
2. Enter IOC details that are, IOC Type, IOC Classification, IOC Value, Severity, Device Type/Source, Adversary Name, Adversary Type, Tag, and click **Add**.
3. If you want to review the intel before submission, click **Save** else click **Submit**.



SEQRITE Threat Intel

Harshal Patil HP

Centralized Security Management
Dashboard
Indicators
Adversaries
Vulnerability Intelligence
Submissions by Users
Cyber Events
SMAP
Admin
Submissions By Users > Add Intel

Add Intel

Incident Basic Details

Title * APT

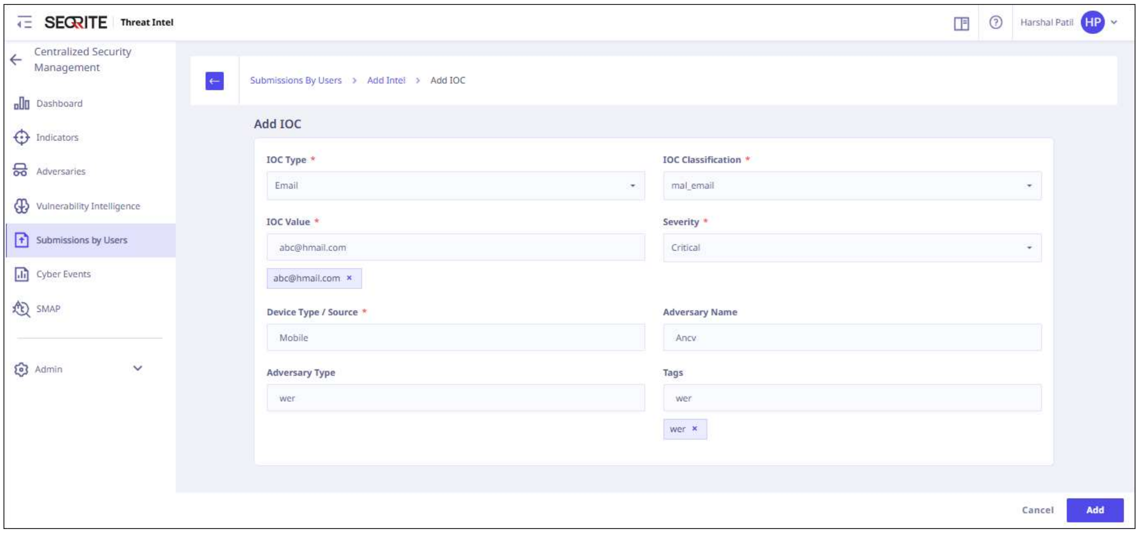
Incident Date * 10/12/2025 12:00 AM

Intel Category * brute-force

Description Enter Description

IOC`s

IOC TYPE	IOC CLASSIFICATION	IOC VALUE	ADVERSARY TYPE	ADVERSARY NAME	TAGS	SEVERITY	DE\

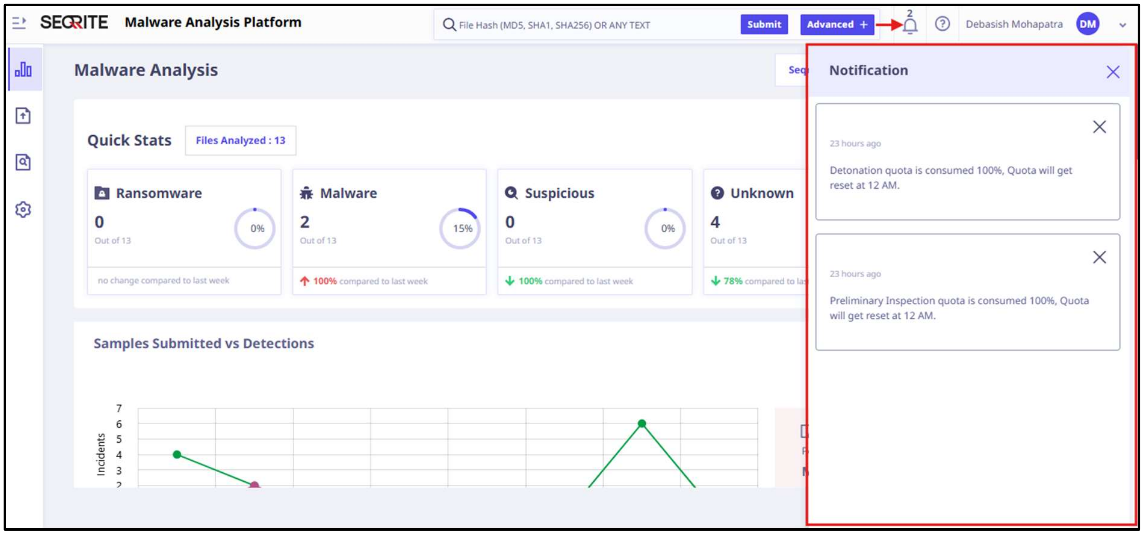


Add IOC

IOC Type *	Email
IOC Classification *	mal_email
IOC Value *	abc@hmail.com abc@hmail.com ×
Severity *	Critical
Device Type / Source *	Mobile
Adversary Name	Ancv
Adversary Type	wer
Tags	wer wer ×

Notifications

Seqrite Malware Analysis Platform displays notifications when you click the Notification icon (bell icon) on the top right.



23 hours ago

Detonation quota is consumed 100%, Quota will get reset at 12 AM.

23 hours ago

Preliminary Inspection quota is consumed 100%, Quota will get reset at 12 AM.

Notifications inform you about all the actions taken on the Seqrite Malware Analysis Platform. The number on the notification icon shows the count of newly received notifications.

On clicking the notification icon, a notification box appears. The notification dialog box shows a few of the newly received notifications with the description and time when the notification was received.

Viewing Notifications

To view a notification, follow these steps:

- Log in to the Seqrite Malware Analysis Platform and click the notification icon (bell icon) on the top right.
  A list of notifications appears.

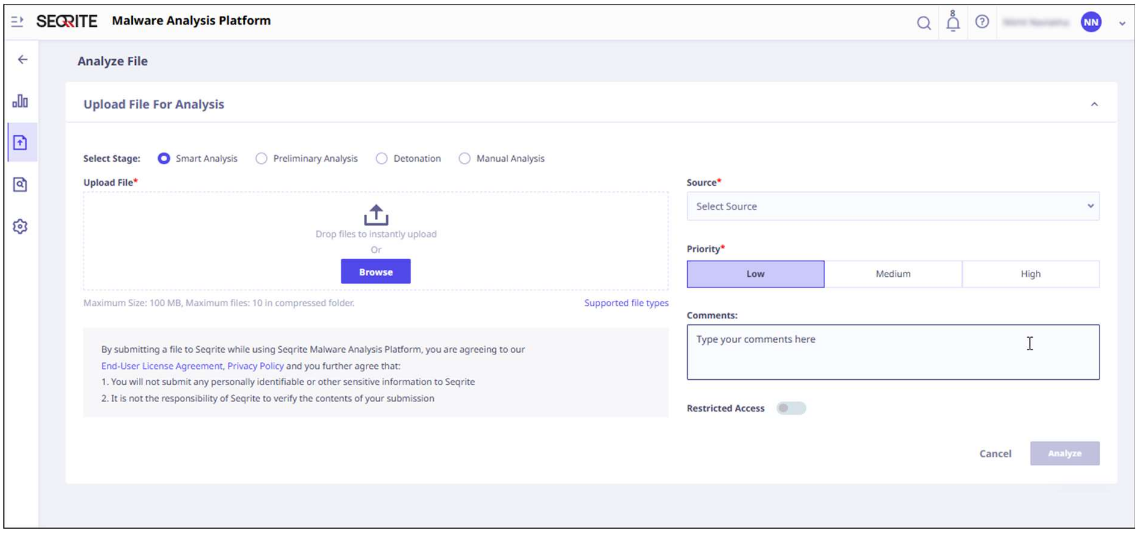
Types of Notifications

I. Analysis notification
After the user uploads a file for analysis, they will receive this notification updating them about the status of the uploaded file.

II. Quota usage notification
The admin will receive this notification informing them about their file upload quota usage. It provides details about their current consumption.

Analysis Report

After you upload a file for analysis through the Search tab on the left pane, an analysis report is generated for the uploaded file and searches hashes that are already present in the database. Various tabs in the report display the corresponding analysis data.



Select Stage: ● Smart Analysis ○ Preliminary Analysis ○ Detonation ○ Manual Analysis

Upload File*

Drop files to instantly upload
Or

Maximum Size: 100 MB, Maximum files: 10 in compressed folder.

Supported file types

By submitting a file to Seqrite while using Seqrite Malware Analysis Platform, you are agreeing to our End-User License Agreement, Privacy Policy and you further agree that:
1. You will not submit any personally identifiable or other sensitive information to Seqrite
2. It is not the responsibility of Seqrite to verify the contents of your submission

Source*: Select Source

Priority*: [✓ Low] Medium High

Comments: Type your comments here

Restricted Access

The following table provides the file details displayed on the analysis report page.

Item	Description
File Name	Displays the submitted file name.
Hash	Displays the submitted file hash.
File Type	Displays the file type.
Verdict	Displays analysis verdict such as Clean, Malware, Ransomware, Suspicious
Malware Category	Displays the malware category.
Malware Family	Displays the malware family.
Submission Time	Displays the time stamp when the file was submitted for analysis.
File Size	Displays the uploaded file size.
Restrict Access	Public or Private
Tags	Displays the system tags.

Add Tags

Detonation layer may automatically assign Tags during analysis. Threat Researchers has the provision to add Tags while conducting Manual Analysis. Additionally, Analyst or Threat researchers can add the following categories during any stage of analysis:

- Affected OS/Platforms

- Attack Type
- Attack Vector
- Indicators of compromise
- Targeted Attacks
- TTPs

Analyst or threat researchers can add tags under these categories by clicking the **Manage Tags** >**Select Category**>**Enter tag name**> **+Add Tag**>**Save**.

Note: It is mandatory to select the category while adding a tag name.

The added tags are visible under **Added Tags**. These tags help future researchers identify the file by these tagged attributes. Tags can also be removed just by click cross **X** sign next to the tag name and such removed tags are visible under **Removed Tags**.

Analysis Tabs

The visibility of some tabs is based on the availability of the data. The ability to add comments depends on your access permissions. You can view the following analysis tabs.

Summary

The submitted file or hash is scanned, and the summary is displayed. The displayed details may vary depending on the submitted file type. The Summery shows the following details:

- Submitted By
- First submission date
- Last submission dates
- Modified date
- Verified
- Verified date
- Machine type

Static Attribute

Malware analysis is incomplete without the analysis of files attributes. Threat researchers use various tools to collect attributes of submitted files. Seqrite Malware Analysis Platform collects and processes the data from these tools and generates the analysis report for the submitted sample.

The static attributes show the following details for the file:

Basic Properties

- MD5, SHA-1 values
- Type of files and file properties.
- Section information (e.g., Entropy value) of the file
- File version number, timestamp information, and digital signature details including certificate chains
- File content in string format
- File content in Hex format

Detonation Detail

Detonation detail will be available when the user has an option for Detonation analysis.

The following table shows the sections and detonation details displayed on the page.

Sections	Description
Verdict	The final assessment of the sample, typically classified as Clean, Unknown, suspicious, Malware or Ransomware based on the combined results of the analysis.
Sample Overview	A high-level summary of the sample, including its file type, size, hash values (MD5, SHA-1, SHA-256), submission date, and any initial observations.
Verdicts from Various Subsystems of Detonation Layer	Individual verdicts from different analysis engines or layers within the sandbox, such as static analysis, behavioral analysis, and network analysis.
Behavior Activities	Detailed description of the sample's behavior during execution, including actions like file manipulation, process creation, network activity, etc.
Process Tree	A hierarchical representation of all processes created or modified by the sample, showing parent-child relationships and the flow of execution.
Process Created	List of processes that were initiated by the sample during execution, along with their associated metadata (e.g., process ID, command line arguments).
Files Created	Information on any files that the sample created or modified, including file paths, names, and types, along with their hash values.
Registry Created	Details of any Windows registry entries created or modified by the sample, including paths and associated values.
Registry Keys Sets	A list of specific registry keys that were modified or set by the sample, potentially indicating persistence mechanisms or configuration changes.
DNS Requests	A record of all DNS queries made by the sample, including domain names, query types, and resolved IP addresses.

Sections	Description
IP Connections	Information on outbound or inbound network connections initiated by the sample, including IP addresses, ports, and protocols.
Screenshots	Captured screenshots of the virtual environment during the sample's execution, providing visual evidence of the sample's activity.

Manual Analysis

Manual Analysis detail will be available when the file is uploaded for Manual analysis.

Comments

You can add any comments.

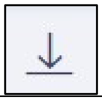
IOC Details

This section will be visible only for files detected as malicious and ransomware. IOC details section shows following details:

- **Indicator Overview**: Risk score, confidence score, and the description of the IoC.
- **Attributes**: Key properties such as source, detection date, type. Incase if IOC Type as IP address we can get additional attributes such as Country, City, ASN, Geolocation, Hostname, Registrant Information, Open Ports by leveraging enrichment connectors.
- **TTP Mappings**: Links to tactics, techniques, and procedures associated with the IoC.
- **Associations**: Known relations with Threats Actors, Malware or IoCs**.**
- **Recommendations:** Recommended action for selected IoC.

Additional options

The following table describes the options that are available on the analysis report page.

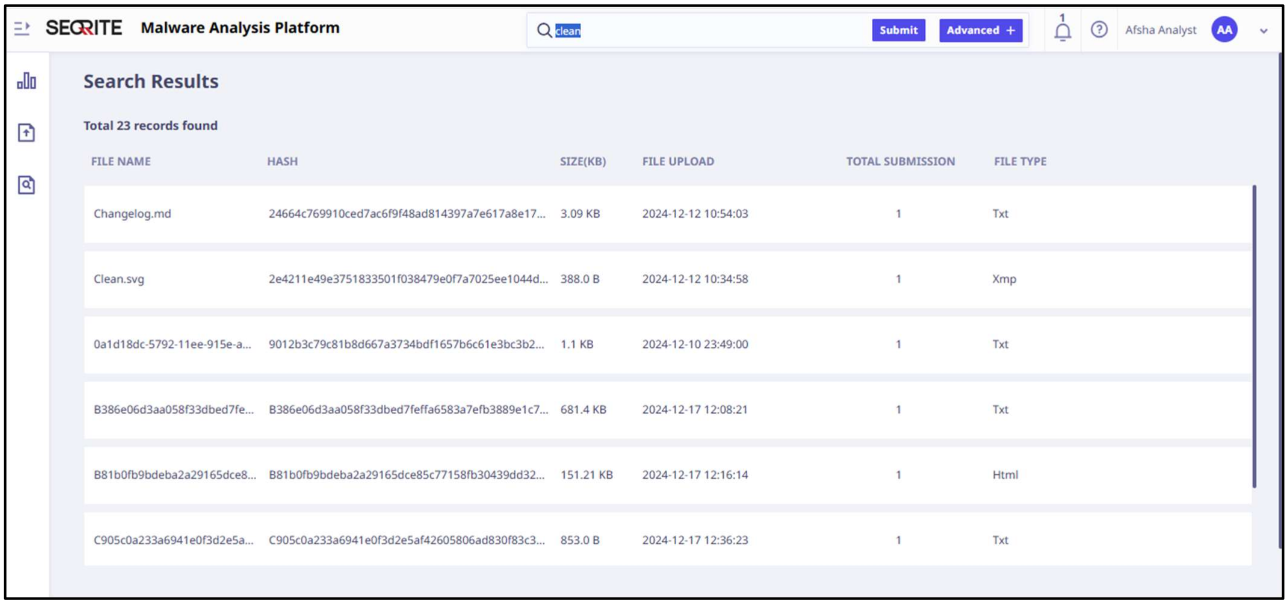
Sr. No.	Icon Name	Description	Images
1	**Download**	You can download reports in PDF, and JSON as required.	
2	**Send to Detonation**	You can send samples to the detonation stage for detailed analysis if sample was previously submitted only for Preliminary Analysis.	
3	**Send to Manual Analysis**	You can send samples for manual analysis if not satisfied with the detailed Detonation analysis report.	

Note: Large reports may take time to download.

Free Text and Advanced Search

You can search using any report content of a file. All the reports pertaining to this search will be fetched and displayed on the table.

If a file hash submitted does not exist in the Seqrite Malware Analysis Platform, then **No Record available** will be displayed.



Search Results

Total 23 records found

FILE NAME	HASH	SIZE(KB)	FILE UPLOAD	TOTAL SUBMISSION	FILE TYPE
Changelog.md	24664c769910ced7ac6f9f48ad814397a7e617a8e17...	3.09 KB	2024-12-12 10:54:03	1	Txt
Clean.svg	2e4211e49e3751833501f038479e0f7a7025ee1044d...	388.0 B	2024-12-12 10:34:58	1	Xmp
0a1d18dc-5792-11ee-915e-a...	9012b3c79c81b8d667a3734bdf1657b6c61e3bc3b2...	1.1 KB	2024-12-10 23:49:00	1	Txt
B386e06d3aa058f33dbed7fe...	B386e06d3aa058f33dbed7feffa6583a7efb3889e1c7...	681.4 KB	2024-12-17 12:08:21	1	Txt
B81b0fb9bdeba2a29165dce8...	B81b0fb9bdeba2a29165dce85c77158fb30439dd32...	151.21 KB	2024-12-17 12:16:14	1	Html
C905c0a233a6941e0f3d2e5a...	C905c0a233a6941e0f3d2e5af42605806ad830f83c3...	853.0 B	2024-12-17 12:36:23	1	Txt

Advanced Search

Additionally, you can further refine your search by adding more search criteria, by selecting one or more filter options to search for the file or hash in the Seqrite Malware Analysis Platform database. The following table gives detail about the filters:

Features	Description
All	Use the following filters as required: • Total Submission • File Size • Tag • Others • File Type
File Type	Search the file for 32-bit or 64-bit machine type. • File type includes Executable, Excel, Word, Power point, PDF, Image, and Compressed. • Machine types include Executable, Excel, Word, Power point, PDF, Image, and Compressed.
File Size (Bytes)	• File Size equal to • File Size Greater than • File Size Less than

Features	Description
Submission Date & Time	You can search for the file in the database, by specifying the date range (From & To).
Tag	• System Tags: System-generated tags. • User Tags: User generated customized tags.
Verdict	You can search the analyzed files by their respective verdicts, that are, • Clean • Unknown • Suspicious • Malware • Ransomware
Malware Family	You can search by Malware families.
Malware Category	You can search by Malware Categories.
Severity	You can search by Analyzed file's severity that is, • No Threat • Low • Medium • High • Critical

Applying Filters

To apply filters, follow these steps:

1. Click **Advanced+**.
2. On the Advanced Filter dialog box, select one or more filters as required, enter the required value in the text box and click **Apply**.

   For example:

   i. If you click File Size, further conditions are displayed as follows: File Size equal to, File Size Greater than, File Size Less than.

   ii. Select the required condition and enter the corresponding value in the text box.

   iii. Click **Add+**.

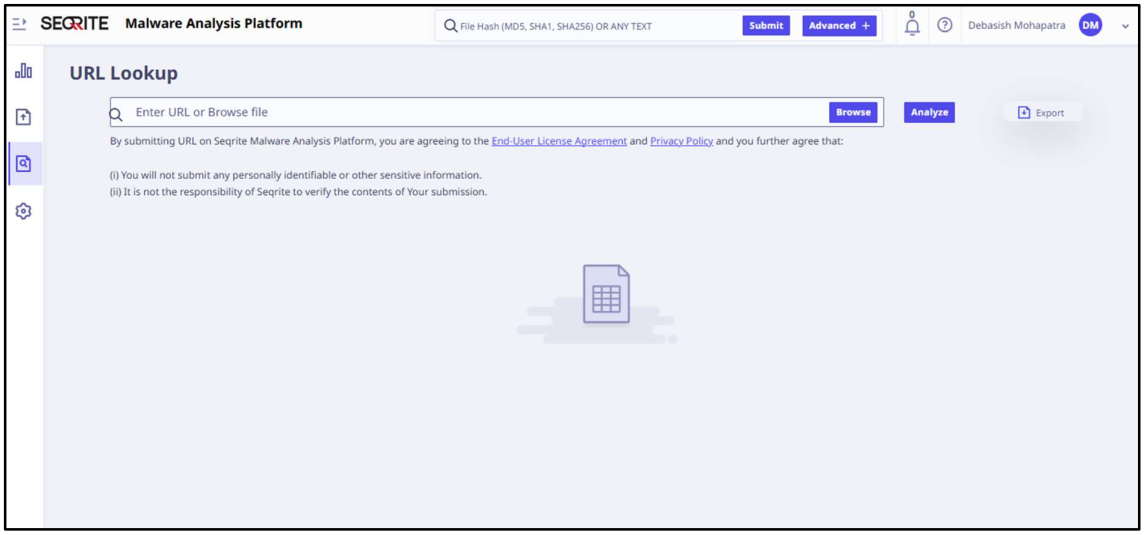
3. The selected filter with value is displayed in the SELECTED FILTERS

   section. For example: File Size is 10 MB, File Type is Word.

4. Select further filters with the conditions. Refer to the table below for available filters.
5. Click **Apply**.
   The report is displayed with related parameters that are, file name, hash, size, file upload, total submission and file type.
6. Click the view **>** icon to view the analysis report.

URL Lookup

URL Lookup is a process of examining a URL to determine its safety by scanning for threats like malware, phishing, or suspicious activity. It helps to identify and block harmful URLs.



By submitting URL on Seqrite Malware Analysis Platform, you are agreeing to the End-User License Agreement and Privacy Policy and you further agree that:

(i) You will not submit any personally identifiable or other sensitive information.
(ii) It is not the responsibility of Seqrite to verify the contents of Your submission.

To analyze the URL, follow these steps:

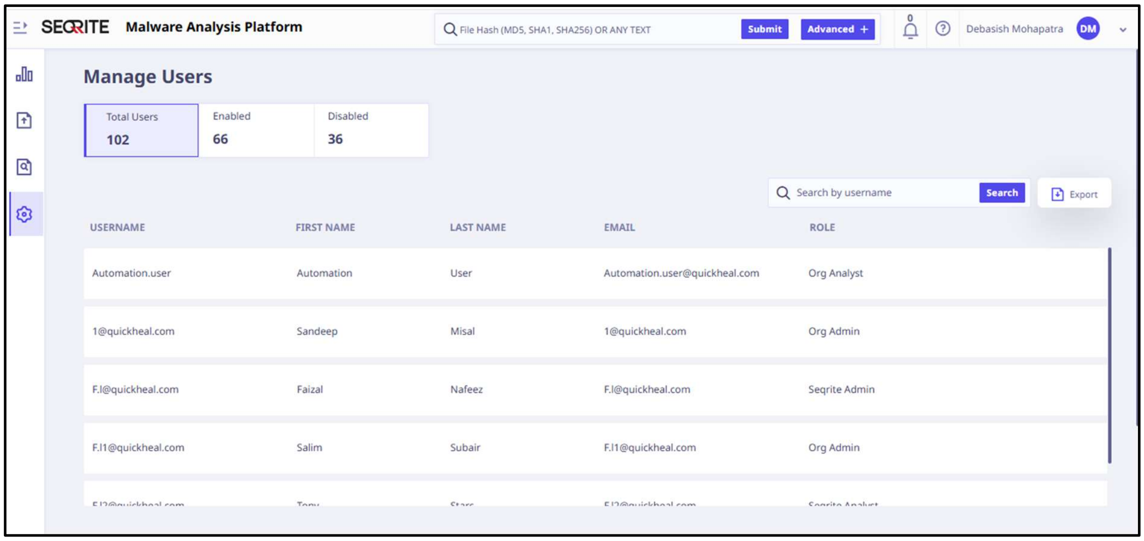
1. On the left pane, select **URL Lookup**.
2. Enter the URL and click **Analyze**.
   The submitted URL is checked against the Seqrite’ s database, and the corresponding categories are displayed. If the URL is safe, the verdict **Clean** is displayed else, it is marked as **Malicious** or **Unknown**.
   Note: This is an Add-on service.

Settings

The settings allow admin users to manage, view the usage quota of users and activity log of all users conducted on Seqrite Malware Analysis Platform.

Users

You, as an admin can add user, view user details, enable or disable the user, change user role, search user and download the users list as a CSV file.



Manage Users

Total Users	Enabled	Disabled
102	66	36

USERNAME	FIRST NAME	LAST NAME	EMAIL	ROLE
Automation.user	Automation	User	Automation.user@quickheal.com	Org Analyst
1@quickheal.com	Sandeep	Misal	1@quickheal.com	Org Admin
F.I@quickheal.com	Faizal	Nafeez	F.I@quickheal.com	Seqrite Admin
F.I1@quickheal.com	Salim	Subair	F.I1@quickheal.com	Org Admin
F.I2@quickheal.com	Tony	Stark	F.I2@quickheal.com	Seqrite Analyst

Adding New User

This section explains the steps to add users in both On-Prem and Cloud environments. Follow the appropriate instructions based on your deployment type.

For **Cloud Users,** Org Admin can add users through the Seqrite CSM console only.
To add a user, follow these steps:

To add a user from Seqrite CSM, follow these steps:

1. On the Seqrite CSM page, click Admin Users on the left pane.
2. Click **+ Add User.**
3. Enter the user details and click **Add**.

For **On Premise Users**, Org Admin can add users in the **Admin** section.
To add a user, follow these steps:

1. Go to **Settings** and select **Users**.
2. Click **+Add User**.
3. Enter user details and click **Save**.

Adding Bulk Users

Only cloud users can add bulk users through Seqrite CSM console.
To add bulk users, follow these steps:

1. On the Seqrite CSM page, click **Admin** Users on the left pane.
2. Click Import.
   The **Import User** page is displayed.
3. Click **Download**, to download the template for CSV file.
   A CSV template is downloaded.
4. Fill in the data in CSV file.
5. Click **Browse** to upload the CSV file and then click **Upload**.

Editing a User

For **Cloud Users**, Org Admin can edit users from the Seqrite CSM console only.

To edit the existing user from Seqrite CSM, follow these steps:

1. On the Seqrite CSM page, click **Admin Users** on the left pane.
2. Click the **Edit** icon for the user that you want to edit.
3. Edit the user details and click **Save**.

Deleting a User

For **Cloud Users**, Org Admin can delete users from the Seqrite CSM console only.

To edit the existing user from Seqrite CSM, follow these steps:

1. On the Seqrite CSM page, click **Admin Users** on the left pane.
2. Click the **Delete** icon for the user that you want to edit.

User Details

You can view user details such as personal details and login information. Along with this, you can enable or disable the user and change the user role.

Enable/Disable the User

To enable/disable the user, follow these steps:

1. Select the user and click **>**(**View**).
2. In the **ACTION** section switch the key to enable or disable the user.

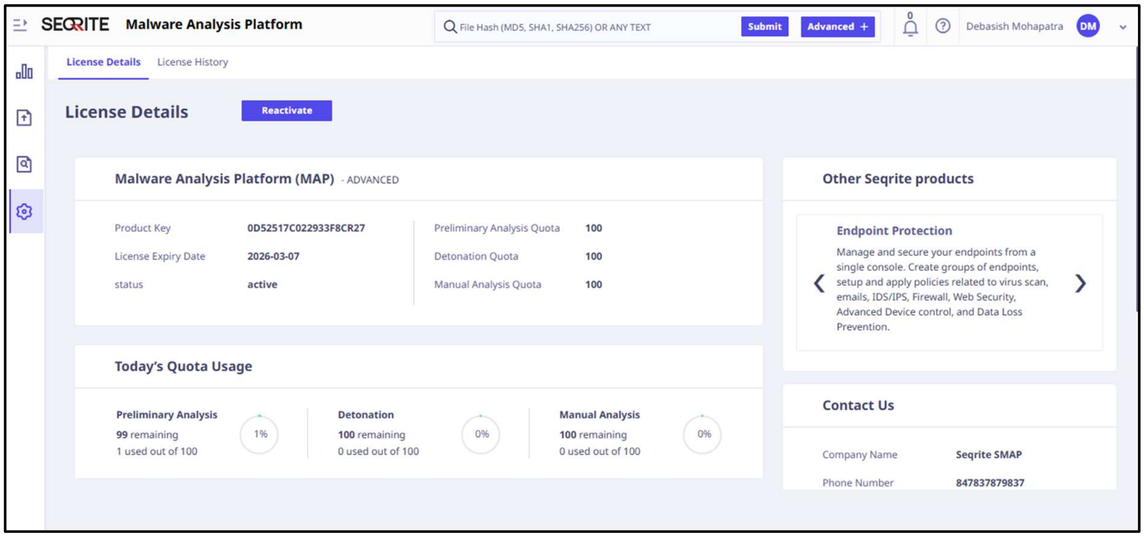
Change the User Role

To change the user role, follow these steps:

1. Select the user and click **>**(**View**).
2. In the **ACTION** section, select the role from the list and then click **Save**.

License

This page is visible only to the admin user. On this page, admin can check the status of Seqrite Malware Analysis license. The license details page gives details such as, license type, quota usage, past quota usage, and company details.



License Details

Malware Analysis Platform (MAP) - ADVANCED

Product Key	0D52517C022933F8CR27
License Expiry Date	2026-03-07
status	active
Preliminary Analysis Quota	100
Detonation Quota	100
Manual Analysis Quota	100

Other Seqrite products

Endpoint Protection

Manage and secure your endpoints from a single console. Create groups of endpoints, setup and apply policies related to virus scan, emails, IDS/IPS, Firewall, Web Security, Advanced Device control, and Data Loss Prevention.

Today's Quota Usage

Preliminary Analysis
99 remaining
1 used out of 100
1%

Detonation
100 remaining
0 used out of 100
0%

Manual Analysis
100 remaining
0 used out of 100
0%

Contact Us

Company Name	Seqrite SMAP
Phone Number	847837879837

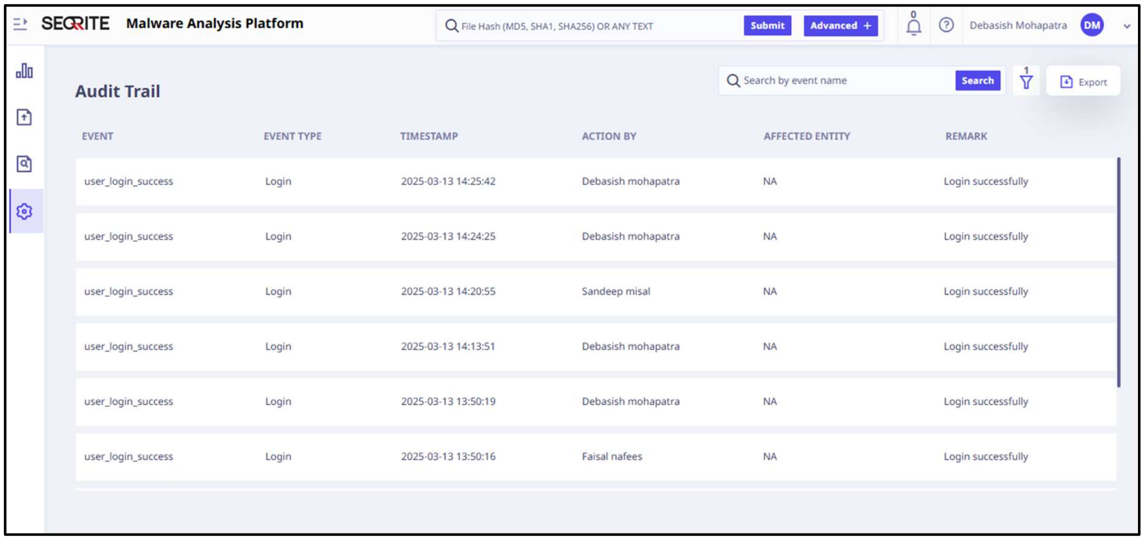
License Details

The license information includes the following details:

Title	Description
License Expiry Date	Displays the license expiry date of Seqrite Malware Analysis Platform.
Status	Displays the status of the license that is, Active or Inactive.
Preliminary Analysis Quota	Displays the allocated quota for the Preliminary Analysis stage.
Detonation Quota	Displays the allocated quota for the Detonation stage.
Manual Analysis Quota	Displays the allocated quota for the Manual Analysis stage.
Today's Quota Usage	Displays the quota consumption for Preliminary Analysis, Detonation, and Manual Analysis for the day.
Past Quota Usage	Displays the details of quota usage that are, quota type, total allocation, quota used, quota remaining, and quota usage in percentage.

Audit Trail

This page gives the activity log of all the user activities that are conducted on the Seqrite Malware Analysis Platform such as User Log in / Log out, User Addition / Deletion, Role assignment or other operation activities such as file upload for analysis. You can download these logs into a CSV file and can filter and export the activity log with the help of a time filter.



Audit Trail

EVENT	EVENT TYPE	TIMESTAMP	ACTION BY	AFFECTED ENTITY	REMARK
user_login_success	Login	2025-03-13 14:25:42	Debasish mohapatra	NA	Login successfully
user_login_success	Login	2025-03-13 14:24:25	Debasish mohapatra	NA	Login successfully
user_login_success	Login	2025-03-13 14:20:55	Sandeep misal	NA	Login successfully
user_login_success	Login	2025-03-13 14:13:51	Debasish mohapatra	NA	Login successfully
user_login_success	Login	2025-03-13 13:50:19	Debasish mohapatra	NA	Login successfully
user_login_success	Login	2025-03-13 13:50:16	Faisal nafees	NA	Login successfully

Support

Head Office Contact Details:

Quick Heal Technologies Limited
(Formerly known as Quick Heal Technologies Pvt. Ltd.)
Reg. Office: Solitaire Business Hub, 7th floor, Office No. 7010 C & D, Viman Nagar, Pune – 411 014, Maharashtra, India.
Official Website: http://www.seqrite.com
Emails to: support@seqrite.com
Contact No.:

- **1800-212-7377**
  Monday to Saturday 9:00 AM to 8:00 PM (IST)

- **+91 7066027377**
  Monday to Saturday 9:00 AM to 8:00 PM (IST)

- **+91 9168625686**
  Monday to Friday 8:00 PM to 9:00 AM (IST)