

Seqrite Digital Risk Protection Services (DRPS)

SEQRITE



User Guide

www.seqrite.com

Copyright and License Information

© 2026 Quick Heal Technologies Limited. All Rights Reserved.

No part of this publication may be reproduced, duplicated, or modified in any form or incorporated into any information retrieval system, electronic or any other media or transmitted in any form without prior permission of Quick Heal Technologies Limited; having its registered address at CTS No. 1442 to 1445 Thube Park, Shivaji Nagar, Pune – 411005.

Marketing, distribution or use by anyone barring the people authorized by Quick Heal Technologies Limited is liable to legal prosecution.

Trademarks

Seqrite Digital Risk Protection Services is a trademark of Quick Heal Technologies Limited and its licensors, if any.

License Terms

Access to and use of Seqrite Threat Intel is subject to end-user's acceptance of the Seqrite Master End-User License Agreement. The license terms can be found at www.segrite.com/eula.

Contents

1. Introduction.....	5
2. On-Boarding Process.....	6
3. Account Creation and Authentication Process.....	7
4. Dashboard	9
Dashboard Metrics.....	9
Executive View Metrics.....	9
Analyst View Metrics	10
Global Search Bar.....	11
Notifications.....	11
User Actions on Notifications	11
Change Notification/Alert Status.....	11
Help and Support	12
Set up Screen Lock	12
User Profile	12
SIA ASSISTANT	12
5. Asset Management.....	13
Adding Asset	13
Category and Subcategory Details.....	14
Scan Asset	16
6. Incident Center	17
Filtering Incident List.....	17
Viewing Incident Details	18
Alert Types Generated	21
Dark Web Exposure.....	22
Credential Leaks.....	22
Stealer Logs	22
Exporting Dark Web Exposure List.....	23
7. Reports	24
Key Capabilities	24
Manage Scheduled Reports	24
Generate Standard Report.....	24
Viewing Report History	25
Filtering Report History.....	25
Exporting Incidents	25

8. Support Teams.....	26
General Support Request.....	26
War Team Request.....	26
Takedown Requests/Legal Team	27
9. Administration	28
Users	28
Grant Access/Add User	28
Activate/Deactivate the User.....	28
Delete Users.....	28
Integrations.....	29
Setup Custom Notifications	29
Authorization Documents.....	30
Uploading Authorization Document.....	30
License Information	31

Introduction

Seqrite DRPS is a brand protection platform developed by Seqrite to help businesses defend themselves against a wide range of online threats, safeguard their reputation, and protect critical digital assets. Seqrite DRPS combines cutting-edge technology, comprehensive threat intelligence, expert legal support, and proven crisis management methods into a single, unified solution for modern brand safety and security.

In today's fast-moving digital environment, where cyber threats, brand impersonation, and intellectual property violations are increasingly common, Seqrite DRPS empowers organizations with a robust and proactive way to maintain customer trust, avoid financial losses, and ensure regulatory compliance. With continuous digital monitoring, real-time alerts, and rapid incident response capabilities, Seqrite DRPS enables brands of all sizes to manage reputational risk and protect their digital presence more effectively than ever before.

On-Boarding Process

The user onboarding process for Seqrite DRPS is formally initiated upon receipt of a valid Purchase Order (PO) from the client. This PO serves as the contractual agreement to activate Seqrite DRPS services in accordance with the selected subscription plan and any associated add-ons.

- **PO Validation:** The received Purchase Order is carefully verified against the approved proposal and contractual terms to ensure alignment and accuracy.
- **Acknowledgment:** An official confirmation email is promptly sent to the client, clearly outlining the next steps, critical timelines, and expectations during the onboarding journey.
- **Plan Allocation:** The client's subscribed plan whether Essential, Professional, Enterprise, and any additional service packs or credits are confirmed and prepared for activation.
- **License Preparation:** License entitlements are provisioned according to the number of covered assets, premium features, and monitoring modules specified in the client's plan.
- **Customer Asset Onboarding:** Seqrite collects details of all customer assets to be scanned in a form of scoping sheet template.
- **Internal Kick-off:** A coordinated alignment of Seqrite DRPS delivery resources is performed, involving the Customer Success Manager (CSM), Threat Analyst, and where applicable, the War Team and Legal Team representatives to ensure seamless execution.

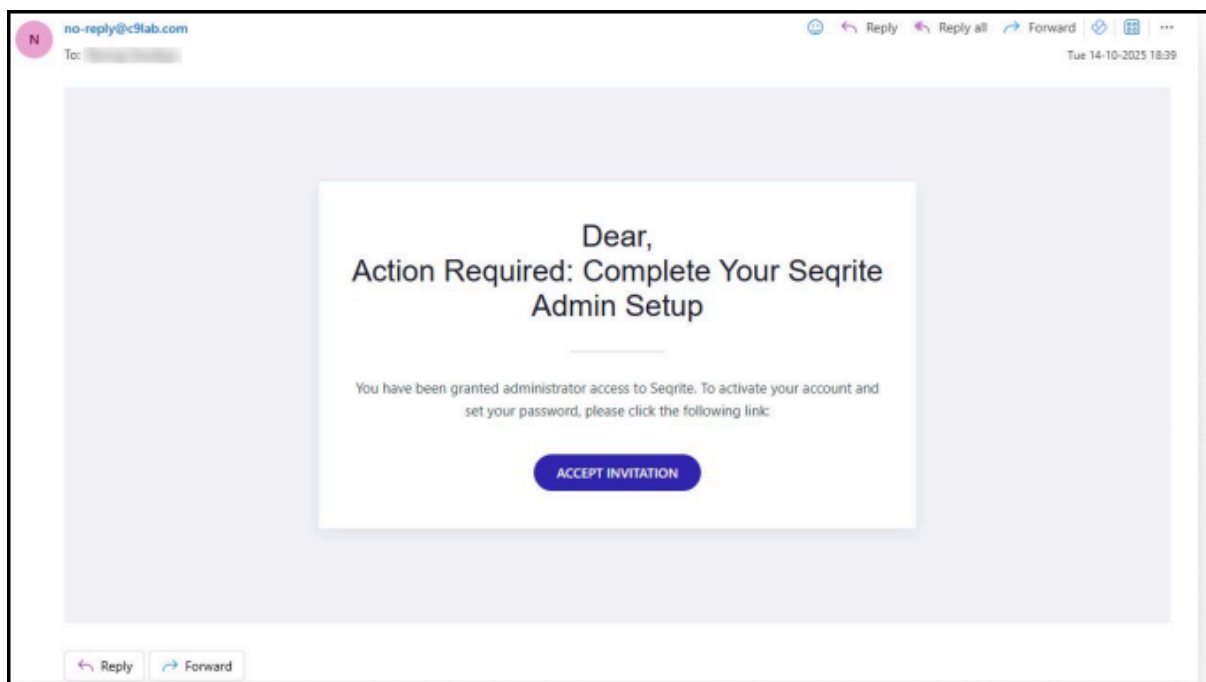
Account Creation and Authentication Process

The process of creating and authenticating an account involves three stages:

1. [Receive and Accept Your Seqrite DRPS Admin Invitation](#)
2. [Setup Your New Password](#)
3. [Login to Your Seqrite Account](#)

1. Receive and Accept Your Seqrite DRPS Admin Invitation

Once your onboarding process begins, you will receive an email title Action Required: Complete Your Seqrite Admin Setup. This email contains your administrative invitation, and next step is Account Activation.



- Click **Accept Invitation** in the email to start your account setup and proceed to create your password.

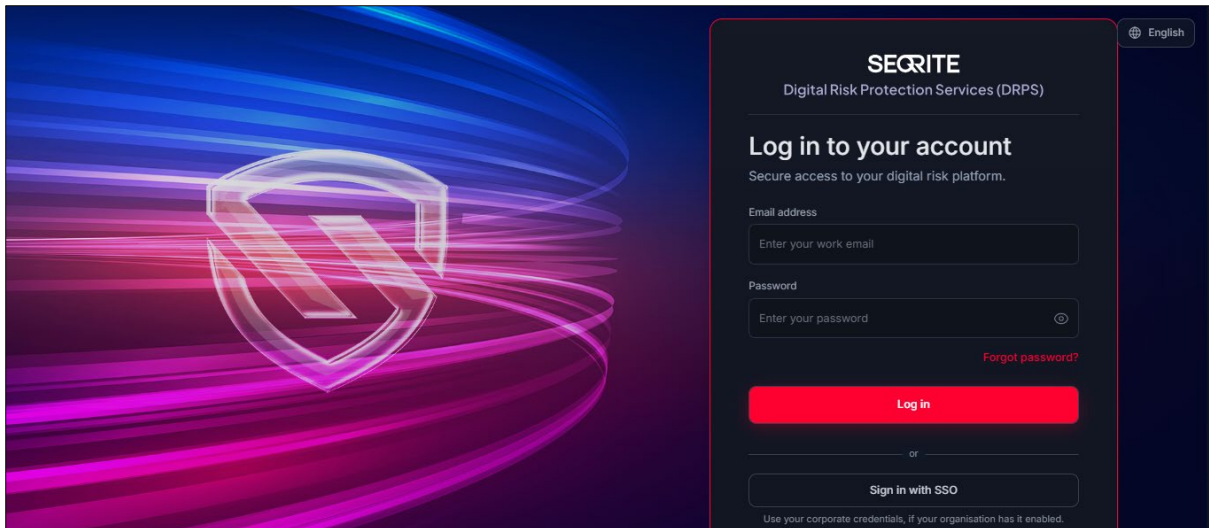
2. Setup Your New Password

After clicking the invitation link, you will be redirected to the password creation page.

1. Enter a secure, new password for your Seqrite DRPS account.
2. Re-enter the password to confirm and safeguard your credentials.
3. Click **Reset Password** to complete the setup.

3. Login to Your Seqrite Account

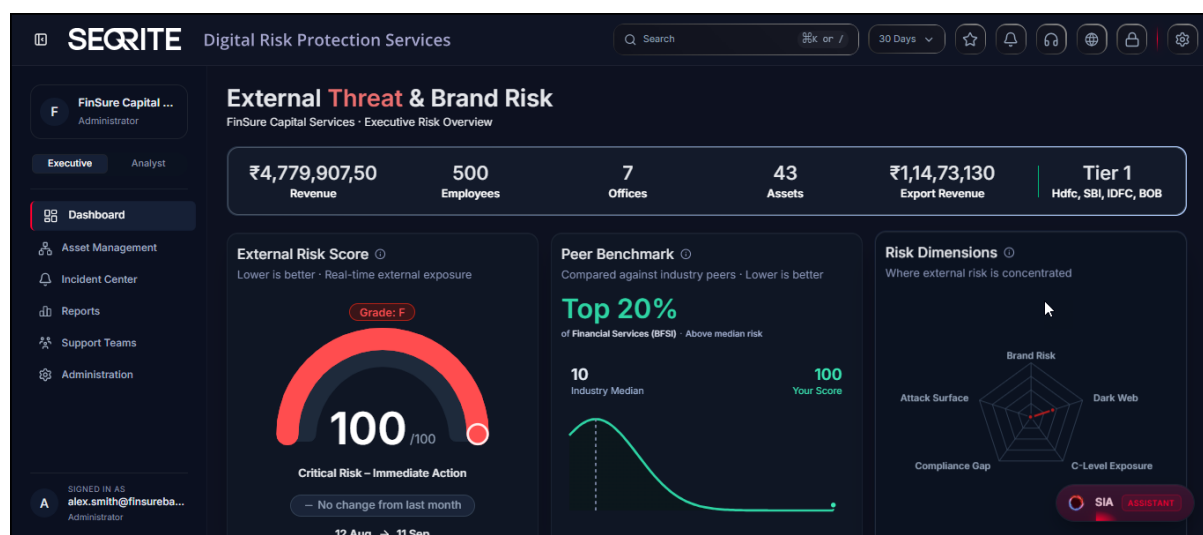
After setting your password, you will be directed to the Seqrite login screen.



1. Enter your registered email address and the new password you just created.
2. Click **Log in** to access your Seqrite DRPS Admin Portal.

Dashboard

The Seqrite DRPS dashboard provides a unified overview of all monitored asset categories, displays real-time alert statistics and trends via interactive cards and graphs, and summarizes incident responses and alert sources for quick assessment of your organization's security posture.



The dashboard provides two views:

- **Executive View:** Offers a high-level summary of key metrics and performance indicators.
- **Analyst View:** Provides detailed insights, including metric counts, breakdowns, and additional analysis to support deeper investigation.

Note: The detailed data displayed in the sample screenshots is for demonstration purposes only. These details are dummy/sample data and do not represent actual data from any environment.

Dashboard Metrics

The available metrics vary based on the selected dashboard view.

Executive View Metrics

The Executive View provides a quick overview of your organization's exposure and highlights the actions that leaders should focus on.

Metric Name	Description
External Risk Score	Shows your organization's risk score (0 to 100), risk grade, and the change compared to the previous month. Lower scores indicate lower risk.

Metric Name	Description
Peer Benchmark	Shows how your organization's risk score compares with other BFSI organizations and the industry average.
Risk Dimension	Shows risk levels across key areas such as Brand Risk, Dark Web Exposure, C-Level Exposure, Compliance Gaps, and Attack Surface.
Risk Trend & Journey	Shows external risk scores over time at the selected granularity.
Board Decisions Required	Shows the items that need board attention, including their priority, recommendation, and status.
Brand Sentiment	Shows detected and neutralized threats, the severity of incidents, and the exposure of organizational credentials on the dark web.
Monthly Investment vs Risk Avoided	Shows comparison between monthly platform investment against estimated risk avoided.
Threats: Detected vs Neutralized	Shows how many threats were detected versus neutralized in each category.
Threat Neutralization Rate	Shows share of identified threats have already been neutralized.
Incident Categories	Shows incident by severity.
Dark Web Credential Exposure	Shows tracked credentials exposed on dark web or breach monitoring sources.

Analyst View Metrics

The Analyst View helps analysts track metrics, investigate issues, and monitor activities daily.

Metric Name	Description
Credit & status tiles	Displays SOS credit usage, takedown credits, support ticket counts, and monitoring status.
Incidents Summary	Shows the total, active, and resolved incidents, resolution rate, and discovered versus total assets.

Metric Name	Description
Deep, Dark & Surface Web	Shows the number of brand-related threats and exposures found on the surface web and the deep/dark web.
Critical Incidents Trend	Shows recent incidents (live feed), top vulnerable categories and top 5 vulnerable assets.
Incident Categories	Displays incidents by risk category, along with the related asset count, incident count, and severity levels.

Global Search Bar

You can search the alert by status, alert name, alert ID, severity level, asset name, Email address, domain name, IP address, assignee name, and category along with the specified number of days.

Notifications

The upper-right section of the Seqrite DRPS console shows various types of notifications along with the following details:

- Description
- Incident Id
- Severity (Low, Medium, High, Critical)
- Incident details
- Source of alert
- Assigned to
- Alert status
- Evidence snapshot
- Affected assets

User Actions on Notifications

You can take required actions on notifications such as:

- **SOS** (Send urgent alerts for immediate assistance)
- **Take Down** (Request legal action to remove the threat)
- **Assign** (Assign alert to your team member)
- **General Support** (Ask Seqrite team for more details about this alert)

Change Notification/Alert Status

You can change the notification status to **Open** or **Report as false**.

Help and Support

Redirects you to Seqrite Technical Support for any assistance.

Set up Screen Lock

Set a 6-digit MPIN to secure your session. When the session is locked, you must enter the configured 6-digit MPIN to unlock it and continue using the application.

User Profile

The User Profile section on the upper-right corner of the dashboard shows following options:

- **Change Password:** Update your account password.
- **Setup 2FA:** Enable two-factor authentication for enhanced account security.
- **Screen Lock:** Lock your session with a 6-digit MPIN for added protection.
- **Active Session:** View and manage your currently active login sessions.
- **SSO Configuration:** Configure Single Sign-On settings for your organization.
- **Take a Tour:** Explore the application's key features through a guided walkthrough.
- **Logout:** Sign out securely from the application.

SIA ASSISTANT

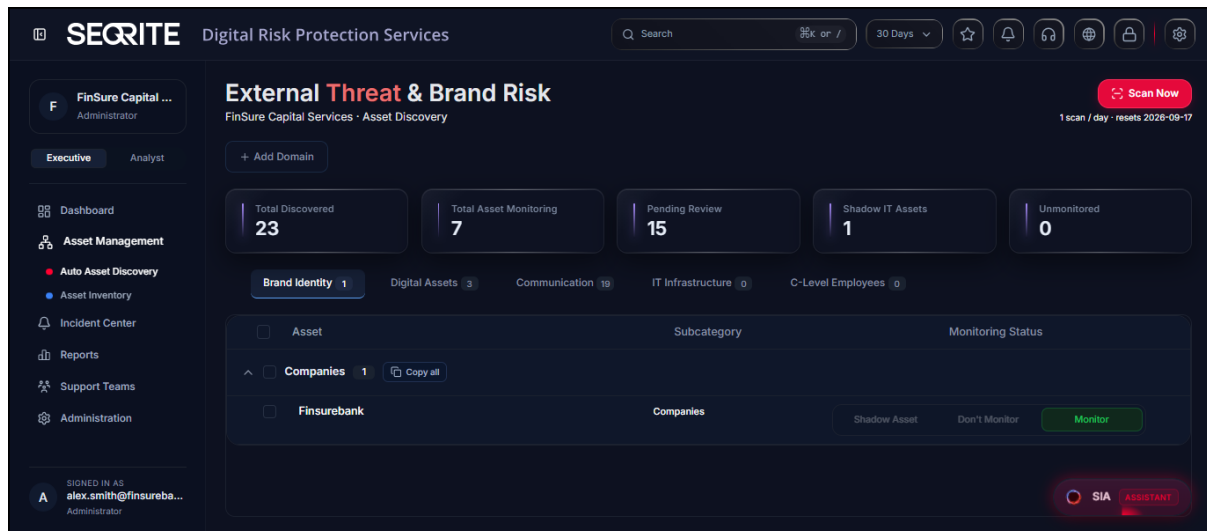
SIA Assistant is built-in AI analyst, available throughout the application to help you understand risks, incidents, and security scores.

Key Features

- **Available Everywhere:** Access SIA Assistant from the bottom-right corner of any screen.
- **Ask in Plain Language:** Ask questions about risk scores, incidents, exposures, or recommended actions using natural language.
- **Data-Driven Responses:** Receive instant answers based on your organization's live monitoring data and incident context.
- **Monthly Credits:** Your subscription includes **100** prompts per month, which are automatically refreshed at the beginning of each month.

Asset Management

In Asset Management, details of organization's asset such as are domain name, URL, social media handles is captured.



Collecting detailed asset information ensures comprehensive monitoring for security and compliance. This process verifies that your organization legitimately owns or manages each asset, enabling proactive protection and risk mitigation.

The **Asset Management** includes the following two sections:

Auto Asset Discovery(EASM Capability)

Automatically discovers your organization's internet-facing assets, including previously unknown or unmanaged assets (Shadow IT). Review each discovered asset and choose to **Monitor**, **Don't Monitor**, or classify it as a **Shadow Asset**.

Adding Domain

You can add domain domains to enable Asset Discovery and identify internet-facing assets associated with your organization.

To add a domain, follow these steps:

1. Go to **Asset Management** and click **Add Domain**.
2. Enter domain name and click **Add**.

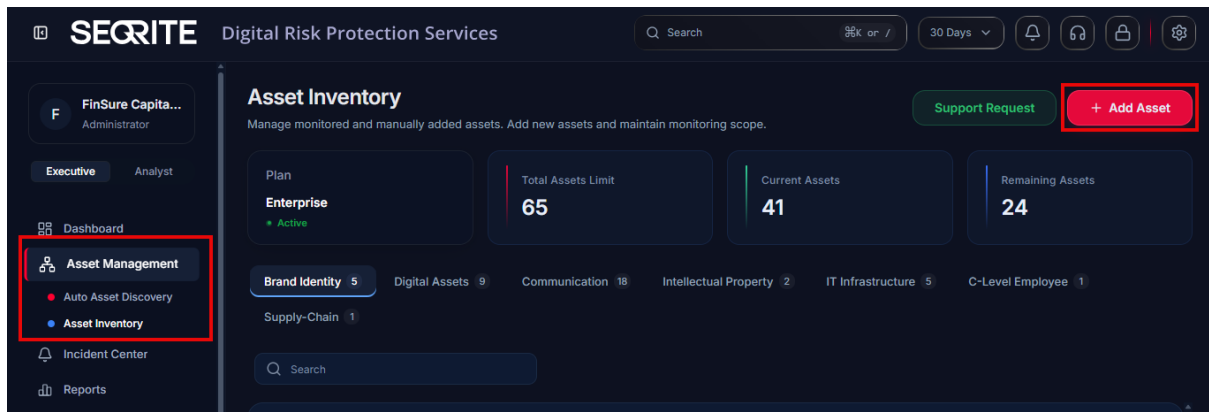
Asset Inventory

Provides a centralized view of all monitored assets. Use the Asset Inventory to view asset status, manage existing assets, and add new assets as required.

Adding Asset

To add assets, follow these steps:

1. Go to **Asset Management** and click **Asset Inventory**.
2. Click **Add Asset**.



3. Select category, subcategory.
4. Enter the details based on selected category and subcategory.
5. Click **Add Asset**.

Category and Subcategory Details

The following table lists the available asset categories and subcategories that can be selected while adding an asset and need to be collected from the organization to start monitoring.

Category	Subcategory	Description
Digital Assets	- Colour Scheme (Organization main website URL, website colour scheme, website content) - Application (Application type, application URL) - Owned Brand Domains - Product/Brand Media(Product/brand images, video URLs, application screenshot)	Covers official websites, domains, subdomains, mobile apps, and digital media assets.
Brand Identity	- Address (Organization Details such as Org Name, Registration number, Slogan, Industry they belong to, Address and other geo location details.) - Brand Details (Brand / Product details, Logos of that product, Trademark details and Logo.	Includes company name, logos, trademarks, slogans, and marketing materials to protect brand reputation.

Category	Subcategory	Description
	Card Information	
Communication	- Email - Phone Number - SMS Sender ID - Social Media Account - Chat Application	Corporate emails, customer service numbers, SMS sender IDs, and social media accounts monitored for fraud or impersonation.
IT Infrastructure	- Server - Operating System - Firewall and Firmware - On-Premise Software - Router & Switch	Details about servers, operating systems, firewalls, firmware, and on-premises software crucial for cybersecurity.
C-Level Employee	- Full Name - Position/Title - Email - Phone Number - Location - Photo	Records of top executives including contact details and photos to prevent impersonation attacks.
Intellectual Property	- Patent (Patent Number and Brief summary of invention) - Copyright (Title of Work, Registration Number, Short Description of Work)	Details about Patents, copyrights, trademarks, and trade secrets safeguarding your creative assets.
Supply Chain	- Vendor/Customer Name - Vendor's/Customer's Domain - Email - Phone Number	Information on vendors and partners, including their domains and contact details to detect third-party risks.

Note: After completing all asset information forms, allow up to 24 hours for the system to initialize monitoring and begin generating alerts. This initialization period ensures accurate threat detection and monitoring across all your registered assets.

Scan Asset

You can use **Scan Now** option to manually initiate an asset discovery scan and identify internet-facing assets associated with the selected domain.

To start scanning, follow these steps:

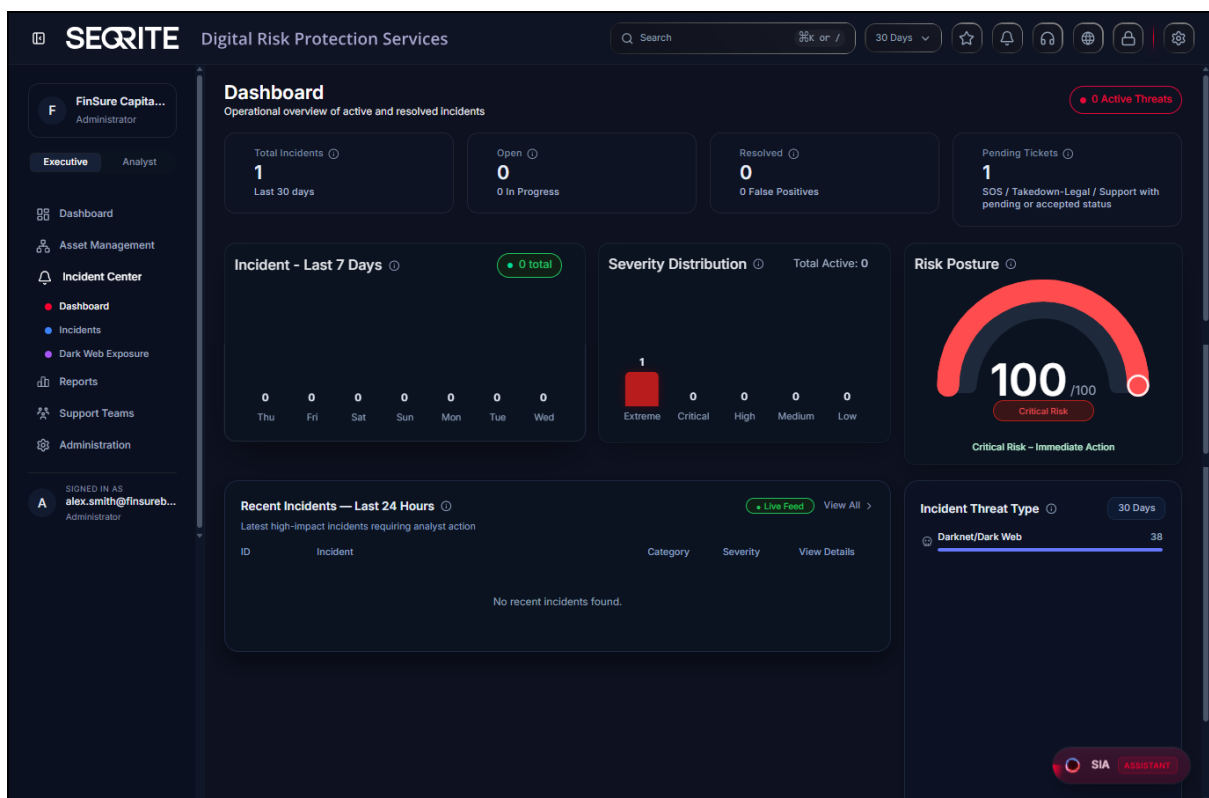
- Go to **Asset Management** and click **Scan Now**.

Note: Only **one scan per day** is allowed for each domain. The **Reset Date** indicates when the next scan can be initiated.

Incident Center

The **Incident Center** is the central dashboard where detected digital threats are collected, organized, and managed.

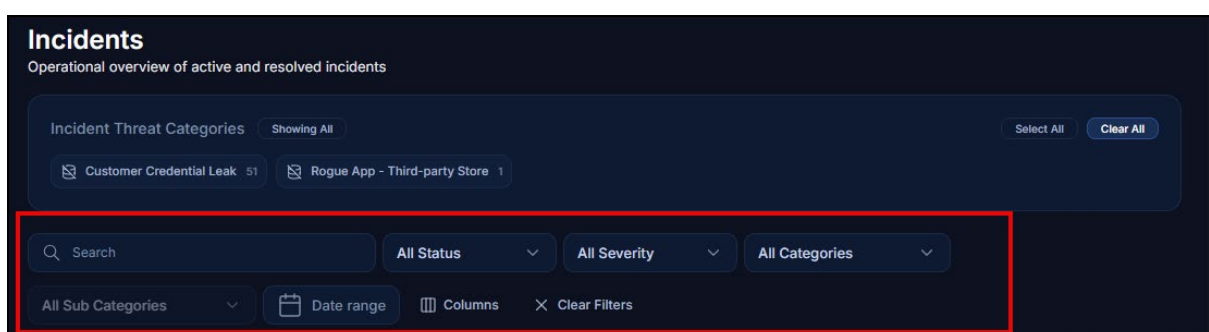
Incident Center gives a clear overview of all alerts in one place. It also includes an incident the Incident Response chart shows the number and severity of alerts assigned to each team member for efficient tracking and resolution.



It also gives a list of incidents along with details such as, incident ID, Title, Severity, Affected Asset, Assigned to, Status, and Date and Time.

Filtering Incident List

You can filter the incident list by category, subcategory such as Company, Address, Brand Details, Card Information, Incident Status (All, Open or Resolved), and by Date.



Viewing Incident Details

To view details of an incident, follow these steps:

1. After logging in to Seqrite DRPS, go to **Incident Center**.
2. Click the incident whose details you want to view.

Incident detail page appears with following details:

- Response Actions
 - SOS: For Immediate assistance and any kind of support required.
 - Takedown: To take down harmful and fraudulent content.
 - General Support: To ask more details about the incident to Seqrite team.
- History and Sharing
 - Show timeline: View the complete activity history for the incident, including status changes, actions taken, and comments.
 - PIN: Pin the incident for quick access.
 - Mail: Send the incident summary to stakeholders by email.
 - Export: Download the incident report for record-keeping, auditing, or further review.
- Incident Management
 - Assign: To assign alert to appropriate team members within the group to ensure prompt and efficient handling and resolution of incidents.
 - Progress: Mark that the incident is actively being worked on.
 - Re-open: Reopen a closed incident if the threat reoccurs or requires further investigation.
 - False Positive: Mark an incident as a false positive to remove it from the active incident queue.
 - Marked as Resolved: Mark the incident as resolved when the threat is no longer active.
- Overview tab
 - Incident Description: You can view full incident summary, impacted assets, and recommended actions.
- Evidence tab: Displays all the supporting images or documents collected for the incident.
- Incident Risk Profile: Displays the incident's risk score, financial impact, SLA status, and credit information.
- Confidence Score: Displays how likely the threat is to be real. A higher score indicates a higher level of confidence and priority.
- Total Risk: Displays the overall incident severity (0-100) based on impact, likelihood, and velocity.

- Incident Timeline: Displays the complete history of the incident, including status changes, actions taken, and updates from detection through resolution.
- Incident Metadata: Displays key incident details, such as the source, category, detection date, last updated date, and affected asset.
- Support Conversation: Chat with the support team about the incident. Comments posted here automatically create a linked General Support Request.

Digital Risk Protection Services

Q Search

or /

30 Days

Incidents
FINS-6063
Critical
Open

FINS-6064
17 / 51
FINS-6062

Pin

Mail

Export

Customer Credential Leak
SLA: 24h

Credentials linked to IT infrastructure 192.168.45.21 found in leaks.

Leaked credentials linked to 192.168.45.21 were detected on the dark web.

Created: Aug 05, 2026, 01:02 AM Source: Darknet/Dark Web

CONFIDENCE SCORE

90

TOTAL RISK

84%

SOS (1)

Re-Open

Assign

General Support

Show Timeline

In Progress

False Positive

Mark as Resolved

Overview

Evidence 0

Detailed Analysis

Short Description

Leaked credentials linked to **192.168.45.21** were detected on the dark web.

Description

A set of credentials linked to your monitored asset was discovered in malware-harvested / breach data circulating on the dark web.

Data exposure: **User account credentials exposed**

Username: **root**

Password: **TM@786@786**

Compromised URL: **https://192.168.45.21**

Leak Date: **19-12-2025**

Source: **192.168.45.21**

Immediate Actions Recommended:

- Reset the password immediately.
- Invalidate all active sessions.
- Enable multi-factor authentication (MFA).
- Review authentication logs for suspicious activity.
- Check for password reuse across other systems.
- Monitor the account for unusual or unauthorized activity.

Incident Risk Profile

Risk Level	critical
Total Risk	84%
Confidence Score	90
Base Score	64
Impact	4
Likelihood	4
Velocity	4
Compliance	10
Privacy	10
Financial Impact	₹25L – ₹1Cr
SLA	24h

Response Credits

1

SOS

12

Takedown

Ownership

Alex

Currently assigned

Reassign

Incident Timeline

Aug 05, 2026, 01:02 AM

Created

Alert generated by Automator

Support Conversation

Support Conversation

Analyst Online

☐ Markdown

Type a message... use @ to mention

Send

Incident Metadata

Incident ID

FINS-6063

Alert Type

Customer Credential Leak

Source

192.168.45.21

Status

SIA

ASSISTANT

Alert Types Generated

Following DRPS alert types will be generated and shown on portal:

Category	Use Case Description
Brand Identity	• Brand name misuse detection – Identifies unauthorized use of the brand name across the internet, including fake ads or promotions. • Trademark & Logo Infringement - Scans web, marketplaces, apps, and social platforms to detect unauthorized use of logos or brand visuals
Digital Assets (Domains, Web Presence)	• Domain abuse & lookalikes – Finds typo-squatted or impersonating domains designed to mislead users. • Domain expiry & SSL monitoring – Tracks certificate expiry and domain validity to avoid outages or security issues.
Communication Channels	• Monitoring of organizational emails & phone numbers – Alerts on exposure or misuse of official communication identifiers. • Fraudulent Support Number Detection – Searches all search engines for fake support numbers
Intellectual Property (IP Assets)	• Copyrighted content misuse – Detects illegal use of original content such as documents, images, software, or videos. • Patent Misuse Detection– Monitors patent metadata to identify unauthorized referencing or copying.
IT Infrastructure	• Server Misconfiguration Detection– Automatically identifies internet-facing servers and flags for any misconfigurations or Open Ports. • Vulnerability detection on exposed infra – Flags weaknesses such as open ports, outdated software, and misconfigurations.
C-Level Employee (VIP Monitoring)	• Credential leakage checks – Alerts when executive emails, passwords, or phone numbers appear in breaches.
Third-Party Risk Management	• Vendor reputation & exposure monitoring – Tracks cyber risks tied to key partners, suppliers, and outsourced teams.

Dark Web Exposure

The Dark Web Exposure displays sensitive organizational information and credential leaks identified on dark web sources, helping organizations detect potential data breaches and mitigate associated risks.

The page contains following two tabs:

- Credential Leaks
- Stealer Logs

Credential Leaks

The **Credential Leaks** tab displays exposed credentials detected from leaked or compromised sources. Users can review details such as source URL, Type, Email Address, Password, and Indexed At date. This information helps identify potentially compromised accounts and supports remediation activities.

The screenshot displays the SEQRITE Digital Risk Protection Services interface. The left sidebar shows the user is logged in as 'FinSure Capital... Administrator' with roles 'Executive' and 'Analyst'. The main content area is titled 'Dark Web Exposure' and shows 'Credentials belonging to your monitored assets found circulating in breach data.' The 'Credential Leaks' tab is selected and highlighted with a red box. Below the tab, there are filters for 'All Categories' (44), 'All Types' (44), and 'All Statuses' (44). A search bar and a 'Filter results...' button are present. A table lists 11 items, each with a checkbox, a URL, a type (all 'IP Address'), an email/username, a password, and an 'Indexed At' date. The table data is as follows:

	URL	Type	Email / Username	Password	Indexed At
☐	http://192.168.45.21/doc/page/login.asp	IP Address	admin	Car...	Aug 31 2026
☐	http://192.168.45.21/web/device/login	IP Address	qsw	lio...	Aug 31 2026
☐	http://192.168.45.21:8080	IP Address	admin	pa...	Aug 02 2026
☐	http://192.168.45.21:8080	IP Address	hiran.pavitt@gmail.com	#mc...	Jul 20 2026
☐	https://192.168.45.21	IP Address	admin	123...	Jul 15 2026
☐	https://192.168.45.21	IP Address	PAV_TO_IPP	Kur...	Jul 14 2026
☐	https://192.168.45.21	IP Address	admin	Kur...	Jul 14 2026
☐	http://192.168.45.42:888	IP Address	sql_hostplo_com	laxc...	Jul 14 2026
☐	http://192.168.45.21	IP Address	8080/ admin	dak...	

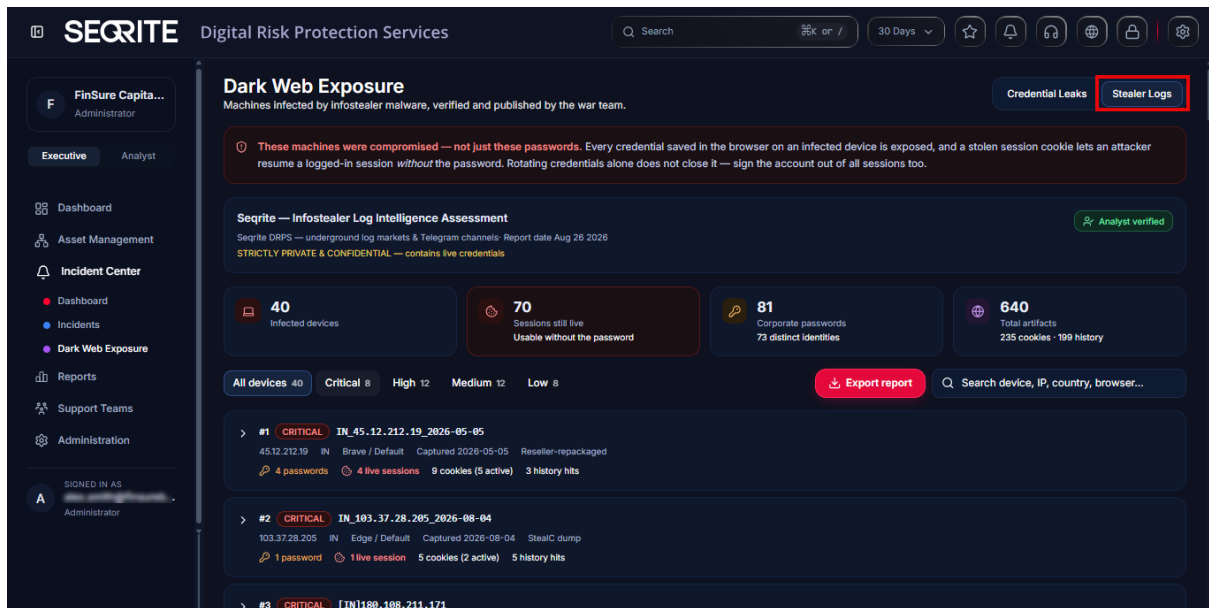
At the bottom right, there is a 'SIA ASSISTANT' button.

Filtering Credential Leaks List

You can filter the list by Category (Digital Asset, Communication, IT Infrastructure, C-level Employee/VIP Executive, Supply Chain/TPRM), Type (Email, Domian, Phone, IP Address), and by Status (Outstanding, Rotated, Not ours, In review).

Stealer Logs

The **Stealer Logs** tab displays details about the IP address associated with exposure and identifies exposed information, such as passwords, cookies, and autofill data. Cookies may represent active sessions that could pose a risk of unauthorized access if exploited. This information helps users investigate affected assets and assess potential security risks.



The page also includes a severity breakdown of exposures categorized as Critical, High, Medium, and Low, enabling users to prioritize investigation and remediation efforts.

Additionally, the page provides the following summary metrics:

- **Infected Devices:** Total number of assets identified in stealer logs.
- **Live Sessions:** Number of active cookie-based sessions that may pose a risk of unauthorized access.
- **Corporate Passwords:** Number of exposed corporate credentials identified.
- **Total Artifacts:** Total number of collected exposure artifacts, such as passwords, cookies, and autofill data.

These metrics help users assess the scope and potential impact of credential and data exposure.

Exporting Dark Web Exposure List

You can export the Dark Web Exposure data in CSV format. The export feature is available for both the **Credential Leaks** and **Stealer Logs** tabs.

To export the Dark Web Exposure list:

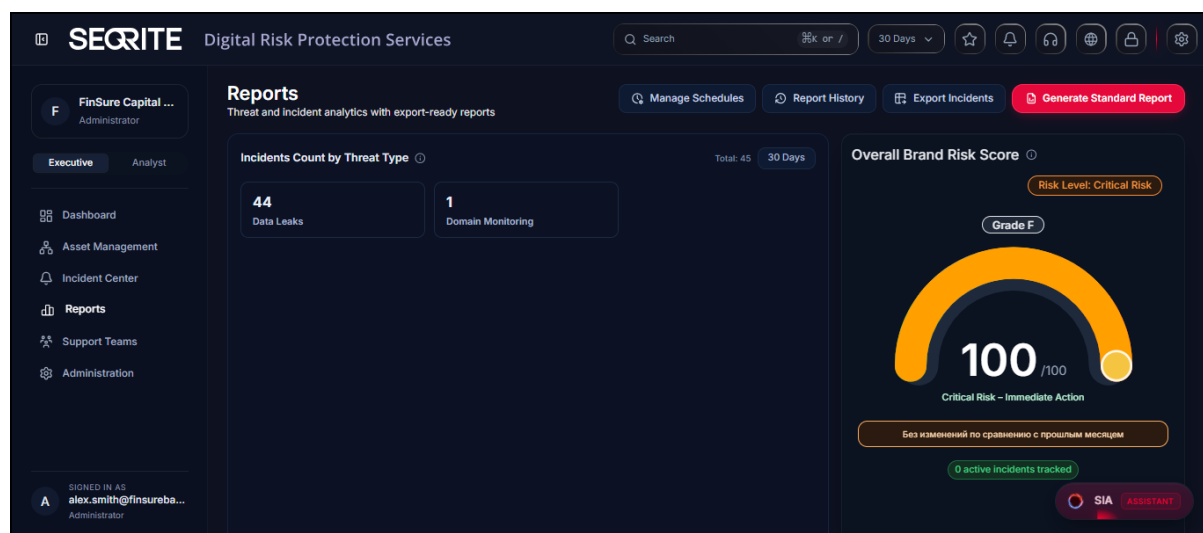
1. Navigate to the Incident Center >> Dark Web Exposure.
2. Select either the **Credential Leaks** or **Stealer Logs** tab.
3. Click **Export**.

The selected list is downloaded in CSV format.

Note: The exported file contains the records currently displayed in the selected tab.

Reports

Reports are assigned a unique score at the brand level, where a higher score indicates greater risk. You can retrieve a complete report for any given date, and the report will be delivered directly to your registered email address.



Key Capabilities

- **Manage Schedules/Scheduled Reports:** Configure reports to be generated and delivered automatically at predefined intervals.
- **Standard Reports:** Generate standard risk reports for analysis and review.
- **Export Incidents:** Download report data in CSV format for offline analysis and record-keeping.
- **Report History:** View brand-level risk scores to assess and track risk exposure over time.

Manage Scheduled Reports

You can configure reports to be generated and delivered automatically at predefined intervals.

To create scheduled reports, follow these steps:

1. Go to **Reports** and click **Manage Schedules**.
2. Click **New Schedule**.
3. In **Report Setup** section, enter Schedule Name.
4. In the Schedule section, enter frequency (once, daily, weekly, By weekly, monthly) run date, and delivery time.
5. Select export format in **Content** section.
6. View details in **Deliver** section and click **Create Schedule**.

Generate Standard Report

To generate a standard report, follow these steps:

1. After logging in to Seqrite DRPS, go to **Reports**.
2. Select a From and To date to filter the report data. Leave the fields blank to include all data, then click Download to generate the report.
The report will be sent to your registered email address.

Viewing Report History

Report History shows all reports that you export. It includes details such as the file name, report type, request date, reporting date, reporting period, status, and availability. You can also download a copy of a report in PDF format when it is available.

Note: Downloaded report PDFs are password-protected for security. Use your **license number** as the password to open the PDF.

Filtering Report History

You can filter the Report History by Name, report type (Incident Report, Incident Export), or Date Range.

Exporting Incidents

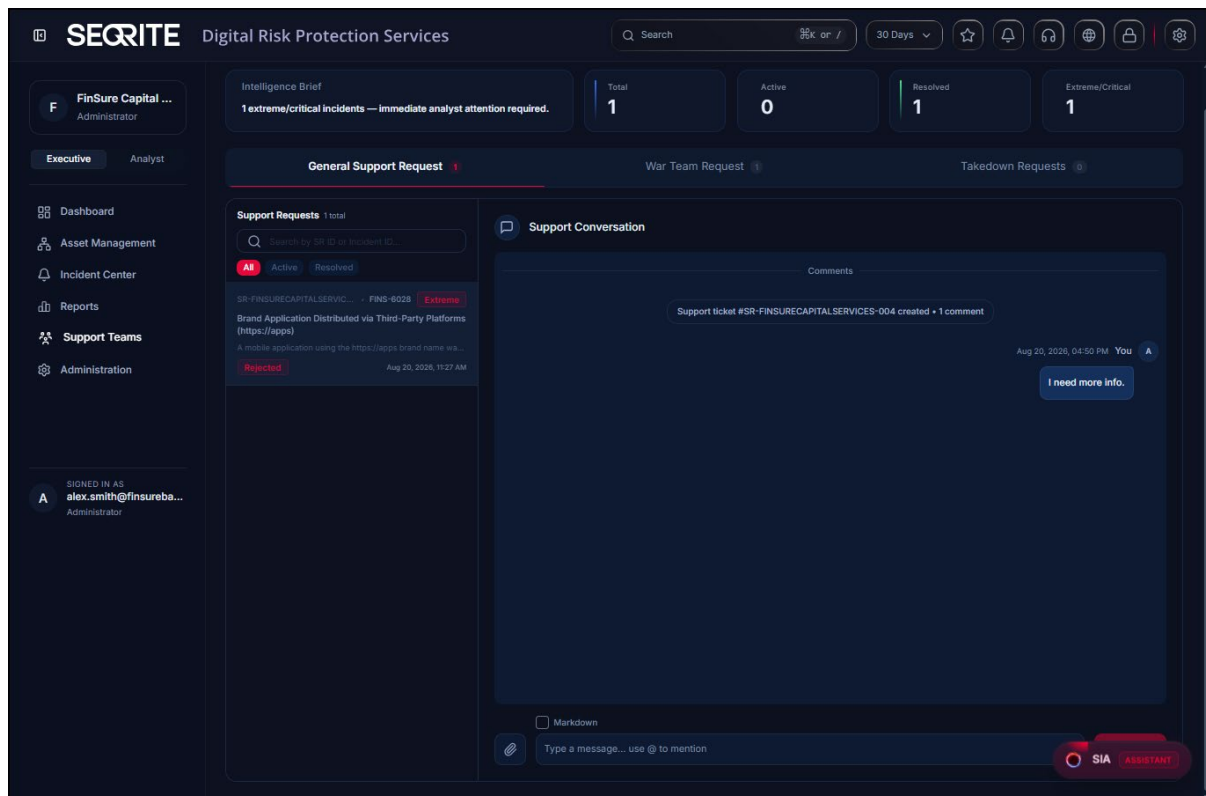
You can export the incidents list by category.

To export incidents, follow these steps:

1. After logging in to Seqrite DRPS, go to **Reports**.
2. Click **Export Incidents**.
3. Select From and To date, one or more categories, the columns that you want to include in the Excel sheet.
4. Click **Export to Excel**.

Support Teams

Support Teams are divided into three groups, the **War Team**, the **Legal Team**, and **General Support**, each responsible for handling incidents in their own area. Each gives incident details such as, Incident IDs, title, severity, affected asset, status, assignee, date and time and incident response chart.



The **Intelligence Brief** tile highlights extreme and critical items that require immediate analyst attention. It provides a summary of the total, active, resolved, and extreme-critical items.

General Support Request

Technical assistance provided by the team to address customer queries and issues.

- **Support Request**
Support Requests show all, active, and resolved support requests, helping you track the status of your requests.
- **Support Conversation**
It is the communication thread associated with the request. You can communicate with the support team regarding your request. It displays the complete conversation history, including updates, comments, and attachments, helping you track the progress of the request.

War Team Request

In the War Team, you can view all alerts assign for immediate action after an SOS is

triggered, including critical communication and social media exposure, along with their status and available team response action.

You can filter the requests by war status, alert status, and date range.

Takedown Requests/Legal Team

In the Legal Team, you can view and manage all alerts sent for takedown and legal review via the Take Down action. Track their legal status, access supporting documents, and monitor progress towards resolution.

Administration

The **Administration** section displays a list of all sub-admins added to the system and allows you to manage them efficiently. Within this section, admin can add new sub-admins, edit their details, and control their status by activating or deactivating accounts.

Users

In the **Users** section admin can manage user access, roles, and category permissions.

Grant Access/Add User

Admin can add new users and assign category-based monitoring scopes to control which categories the users can access and monitor.

To add user, follow these steps:

1. After logging in to Seqrite DRPS, go to **Administrator**.
2. Click **Users**.
3. Click **Grant Access**.
4. Enter first name, last name, and email address.
5. Select one or more roles from **Sub admin** (Manage users and account), **Executive** (executive dashboards and reports), or **Analyst** (Analyst dashboard and incident).
6. Select the categories for which you want to grant monitoring access to the user.
7. Select **Allow Re-opening Incidents** checkbox to allow users to reopen a resolved incident.
8. Click **Grant Access**.
The system sends an invitation email to the user.

Note: Users that you add become **Sub-Admins** with the assigned role. Users with the **Executive** role can access only the **Executive Dashboard**, while users with the **Analyst** role can access only the **Analyst Dashboard**. To grant access to both dashboards, assign both roles. The user can then switch between the **Executive** and **Analyst** dashboards using the **Executive/Analyst** toggle.

Activate/Deactivate the User

To activate or deactivate the Sub-Admin, follow these steps:

1. After logging in to Seqrite DRPS, go to **Administrator**.
2. Select the user you want to activate/deactivate and switch the **Activate** or **Deactivate** toggle.

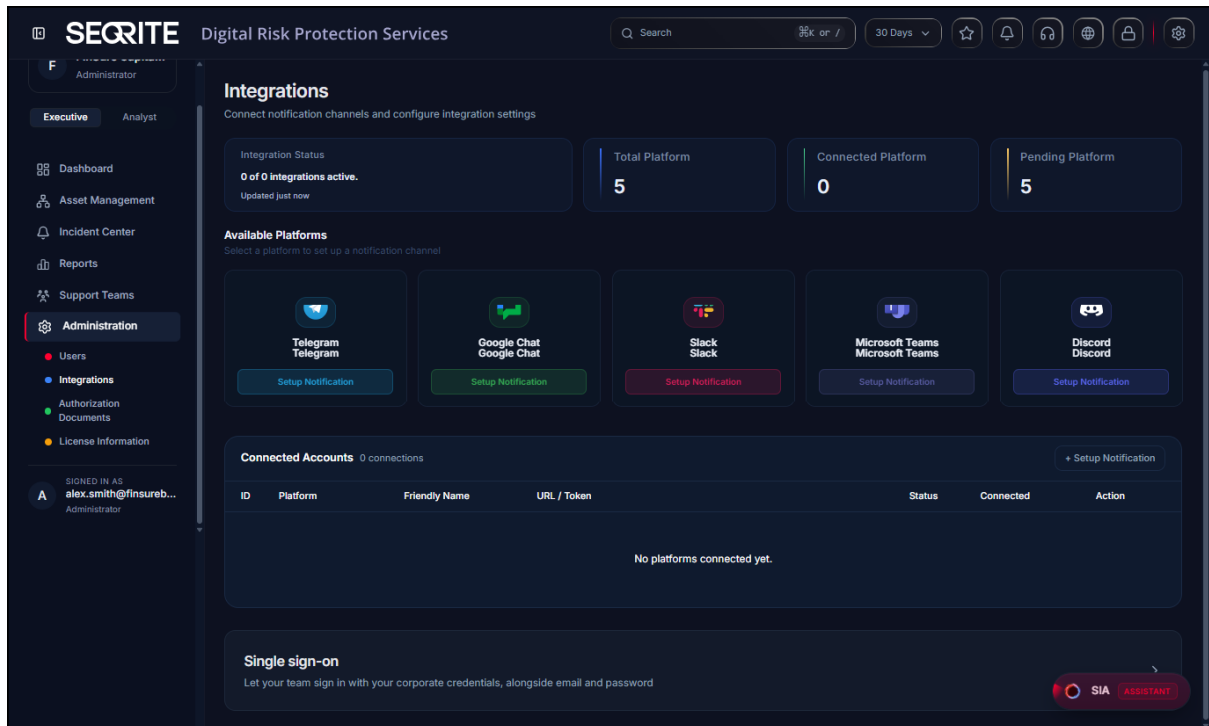
Delete Users

To delete the user, follow these steps:

1. After logging in to Seqrite DRPS, go to **Administrator**.
2. Select the user you want to delete and click .

Integrations

Seqrite DRPS also supports API integrations with chat applications like Microsoft Teams, Slack, Telegram, Google Chat, and Discord. You can set up custom notifications within these apps, allowing your teams to receive and respond to alerts directly in their preferred communication platform.

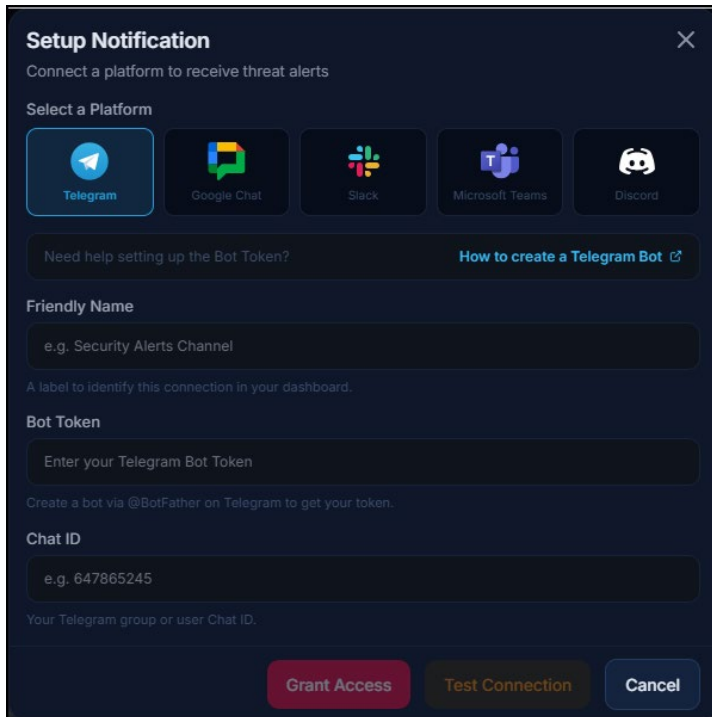


Setup Custom Notifications

To set up custom notifications with chat applications, follow these steps:

1. After logging in to Seqrite DRPS, go to **Administration >>Integrations**.
2. Choose the platform for which you want to set up custom notifications and click **Setup Notification**.

The **Setup Notification** screen appears.



3. Select the platform, enter name, your BOT API token, enter name, chat ID.
4. Click **Test**, if successful, click **Save**.

Authorization Documents

Authorization Documents is a centralized repository where users can upload and manage multiple documents. These documents are requested by the Legal Team during the review and processing of takedown requests.

Uploading Authorization Document

To upload authorization documents, follow these steps:

1. After logging in to Seqrite DRPS, go to **Administration >>Authorization Documents**.
2. Click **Upload document**.
3. Select document type, enter title, valid from, valid until dates, notes, select the document.
4. Select the confirmation checkbox and click **Save**.

Note:

- Supported file formats are **PDF**, **DOC**, and **DOCX**.
- The maximum file size allowed for each document is **10 MB**.

License Information

The **License Information** section provides a detailed record of customer information, licensing details, product and service coverage, available credit balances, and support entitlements. It includes customer and order information, covered services, license details, subscription term, and features such as Deep and Dark Web monitoring, Takedown and SOS services, AI-powered threat intelligence, EASM, and enhanced support options.