SEQRITE

Seqrite Managed Security Service Portal (MSSP)

User Guide

www.seqrite.com

Copyright & License Information

Trademarks

License Terms

Release date

May 13, 2022

About This Document

This guide covers all the information required to use Seqrite Managed Security Service Portal (MSSP). The following table lists the conventions that we have followed to prepare this guide.

Convention	Meaning
Bold Font	Anything highlighted in bold indicates that it is a menu title, window title, check box, drop-down box, dialog, button names, hyperlinks, and so on.
ℹ	This is a symbol used for a note. Note supplements important points or highlights reservation related to the topic being discussed.
💡	This is a symbol used for a tip. Tip helps users to apply the techniques and procedures to achieve the task related to the topic being discussed.
⚠	This is a symbol used for warning or caution. This is an advice either to avoid loss of data or damage to hardware.
<Step 1> <Step 2>	The instruction mentioned in the numbered list indicates actions that you need to perform.

Best Cybersecurity Practices for Enterprises to Stay Cyber Secure

In wake of the rising incidences of targeted attacks on enterprises, there is no way organizations can afford to ignore the importance of cyber security. Regardless of the size and type of enterprise, even a small data breach or cyber-attack could mean millions of dollars of loss, crippling the economy of the enterprise.

It is for this reason that as a thumb rule, enterprises should follow these cybersecurity practices, in order to be cyber secure against known and unknown threats.

#1 Invest in Security Solutions – An enterprise may be subjected to various kinds of threats and thus, to ensure enterprise-wide security, it is a good practice to invest in a variety of security solutions that cover the changing needs of an organization.

#2 Use Complex & Unique Password – As a thumb rule, enterprises must encourage employees to use strong and unique passwords and prohibit them from sharing their credentials to anyone.

#3 Invest in Training – Educate and train employees about cybersecurity so that they are absolutely cautious about clicking suspicious links, sharing sensitive data and responding to security alerts.

#4 Back up Your Data – Follow the 3-2-1 rule when it comes to data backup, meaning that maintain 3 varying copies of your crucial data in 2 different formats, where at least 1 of the data storage locations should be offline.

#5 Robust Security Policies – In order to ensure that both employees and third parties follow the security policies, it is important to strictly convey the enterprise security policies and expectations.

#6 Use Updated Software – Using an expired software is as good as counting on a dead security solution. Thus, it is a good practice to keep your software updated to the latest version to safeguard your organization against evolving threats.

#7 Data Encryption – It is advisable to encrypt all the saved and backed up data, while providing access rights to only limited and specific personnel.

#8 Two-Factor Authentication – An additional and reliable login procedure is to use two-factor authentication that uses a secondary device like mobile for access authentication.

#9 Implement MDM Plan – It is important to monitor and regulate the mobile device usage of employees since, they often use it for accessing sensitive data and company emails, while using company’s wireless network. This may serve as a soft vulnerability for attacks.

#10 Change Default Credentials – There are several IoT devices that come with default passwords that make it easy for malware to target such IoT devices. Thus, it is a good practice to replace the default credentials as soon as possible by a strong password.

#11 Secured Wi-Fi – A device can connect to only those Wi-Fi networks that have a known SSID. Thus, to prevent an unknown device from connecting to the Wi-Fi network of your enterprise, a good security mechanism is to use a hidden SSID to prevent it from getting broadcast.

#12 Limited Access Right Grant – The Principle of Least Privilege states that a subject (user/device/application) should be given ONLY "Just In Time" and "Just Enough" access privilege needed for it to complete its task. If a subject does not need the access rights, the subject should not have that right.

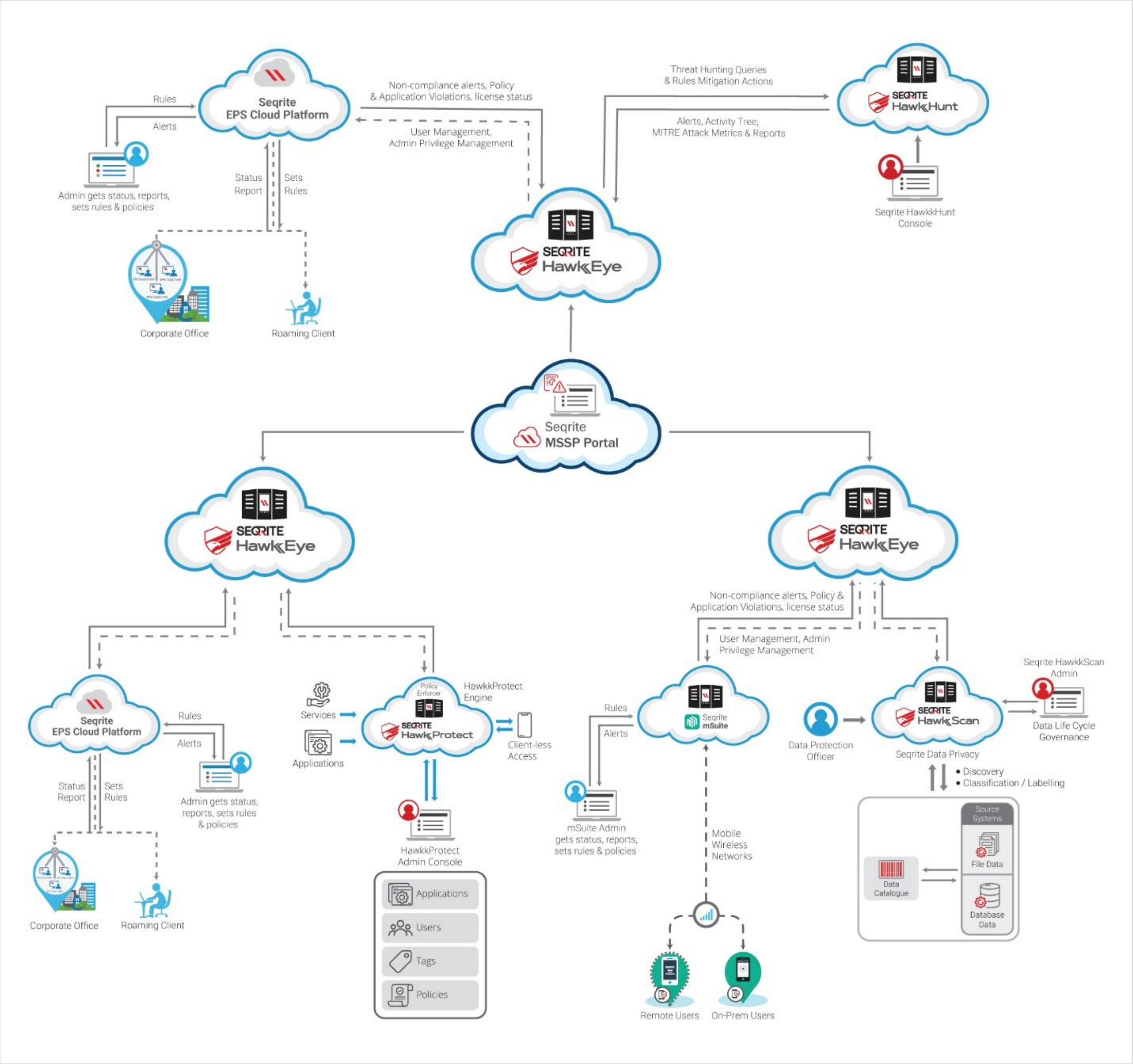
#13 Server OS Hardening – In order to address the security of your enterprise adequately, it is advisable to configure and harden the operating system. This typically involves removing all the unnecessary applications, services, and network protocols.

Contents

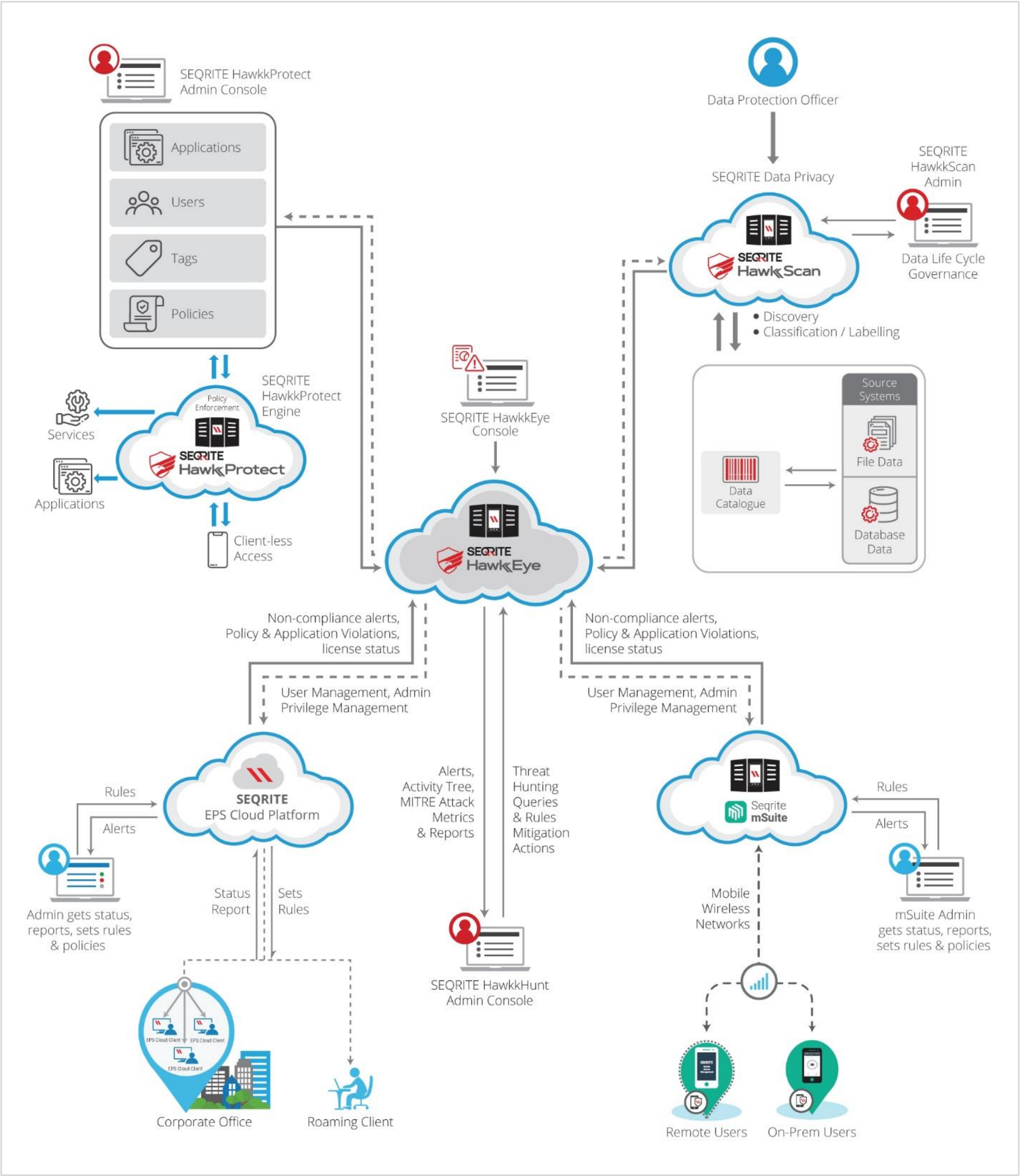
1. MSSP Dashboard

Seqrite Managed Security Service Portal or MSSP is a web-based portal. Quick Heal provides gateway security solutions such as Seqrite HawkkEye and Central Management System (CMS). Also, Quick Heal provides management of all gateway security solutions as service through MSSP. In MSSP, all the clients who will buy these security solutions can be listed and managed professionally.

Seqrite MSSP empowers managing multi-tenant Seqrite HawkkEye deployments with any combination of Seqrite product portfolios including Seqrite EPS Cloud, Seqrite mSuite, HawkkProtect, HawkkScan, and HawkkHunt.

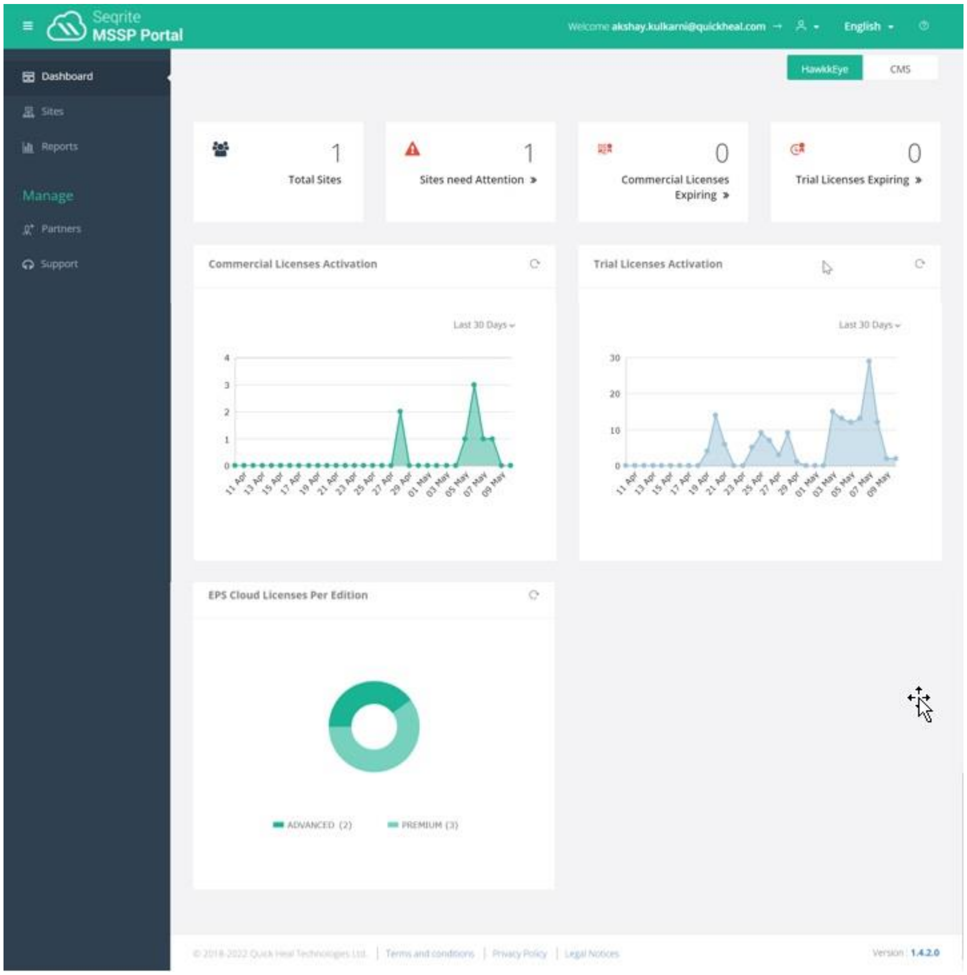


Seqrite HawkkEye enables integrated Seqrite product portfolios including Seqrite EPS Cloud, Seqrite mSuite, HawkkProtect, HawkkScan, and HawkkHunt.


SEQRITE HawkkProtect Admin Console
Applications
Users
Tags
Policies
SEQRITE HawkkProtect Engine
Policy Enforcement
SEQRITE HawkkProtect
Services
Applications
Client-less Access
Data Protection Officer
SEQRITE Data Privacy
SEQRITE HawkkScan Admin
SEQRITE HawkkScan
Data Life Cycle Governance
• Discovery
• Classification / Labelling
Source Systems
File Data
Data Catalogue
Database Data
SEQRITE HawkkEye Console
SEQRITE HawkkEye
Non-compliance alerts, Policy & Application Violations, license status
User Management, Admin Privilege Management
Non-compliance alerts, Policy & Application Violations, license status
User Management, Admin Privilege Management
SEQRITE EPS Cloud Platform
Rules
Alerts
Admin gets status, reports, sets rules & policies
Status Report
Sets Rules
EPS Cloud Client
EPS Cloud Client
EPS Cloud Client
Corporate Office
Roaming Client
Alerts, Activity Tree, MITRE Attack Metrics & Reports
Threat Hunting Queries & Rules Mitigation Actions
SEQRITE HawkkHunt Admin Console
Seqrite mSuite
Rules
Alerts
mSuite Admin gets status, reports, sets rules & policies
Mobile Wireless Networks
Remote Users
On-Prem Users

When you log on to MSSP, its dashboard appears. Dashboard displays current status on various situations such as the number of the sites listed until now, all the activated licenses, the sites that need immediate attention, the licenses that are expiring soon, the licenses that are under certain MSSP editions, and so on.

Dashboard of HawkkEye



Welcome akshay.kulkarni@quickheal.com

1 Total Sites

1 Sites need Attention »

0 Commercial Licenses Expiring »

0 Trial Licenses Expiring »

ADVANCED (2)

PREMIUM (3)

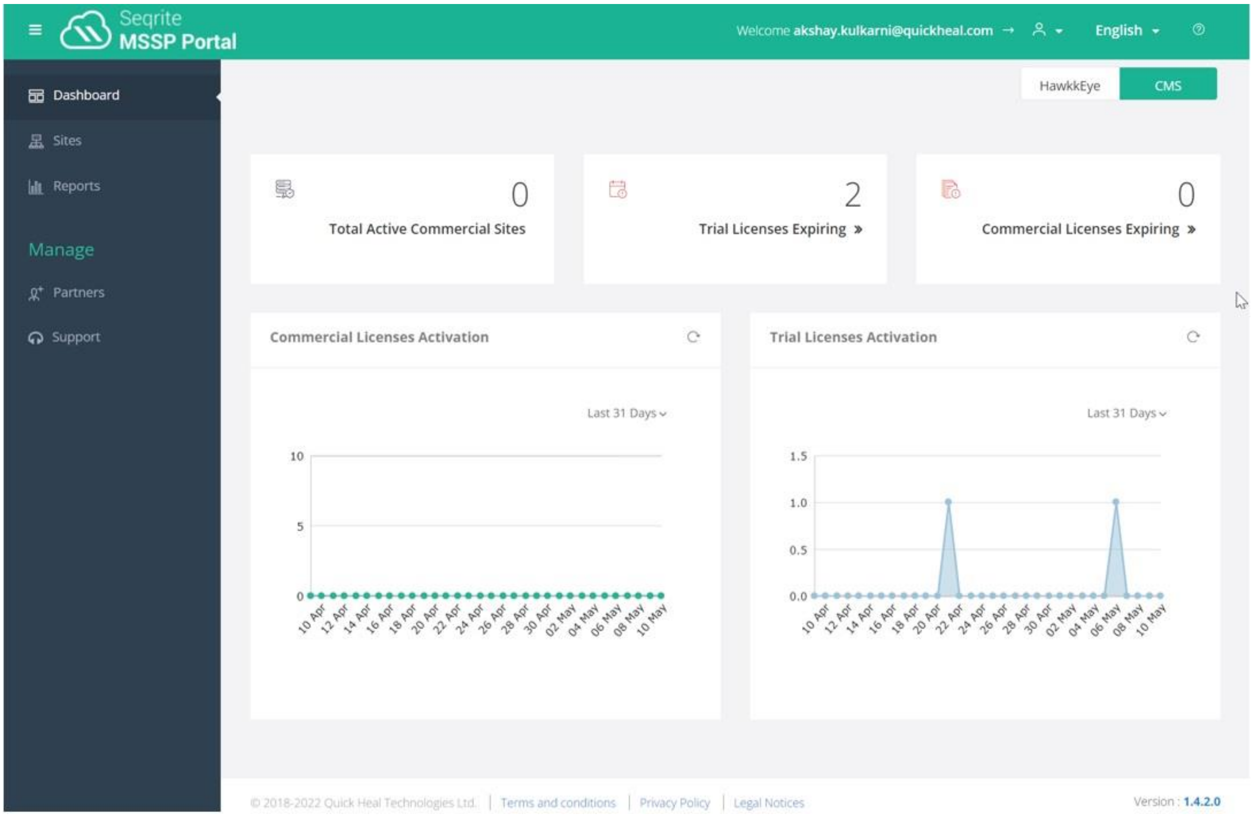
© 2018-2022 Quick Heal Technologies Ltd. | Terms and conditions | Privacy Policy | Legal Notices

Version : 1.4.2.0

The following table describes the features of HawkkEye displayed on dashboard.

Features	Description
Total Sites	Displays the total number of active commercial sites.
Sites Need Attention	Displays which sites need attention to fix the issue. To see the details, click on the link under the feature.
Commercial Licenses Expiring	Displays the number of commercial licenses that are going to expire in about 7 days. To see the details, click on the link under the feature.
Trial Licenses Expiring	Displays the number of trial licenses that are going to expire in about 7 days. To see the details, click on the link under the feature.
Commercial Licenses Activation	Displays the number of commercial licenses that have been activated in the last 7, 15, or 30 days. To see the details, click on the link under the feature.
Trial Licenses Activation	Displays the number of trial licenses that have been activated in last 7, 15, or 30 days. To see the details, click on the link under the feature.
EPS Cloud Licenses Per Edition	Displays the number of active commercial licenses under different editions.
Computer Infection Detected	Displays if any infection has been detected. You can see infection detected in the last 7, 15, and 30 days.

Dashboard of Central Management System (CMS)



The following table describes the features of Central Management System (CMS) displayed on dashboard.

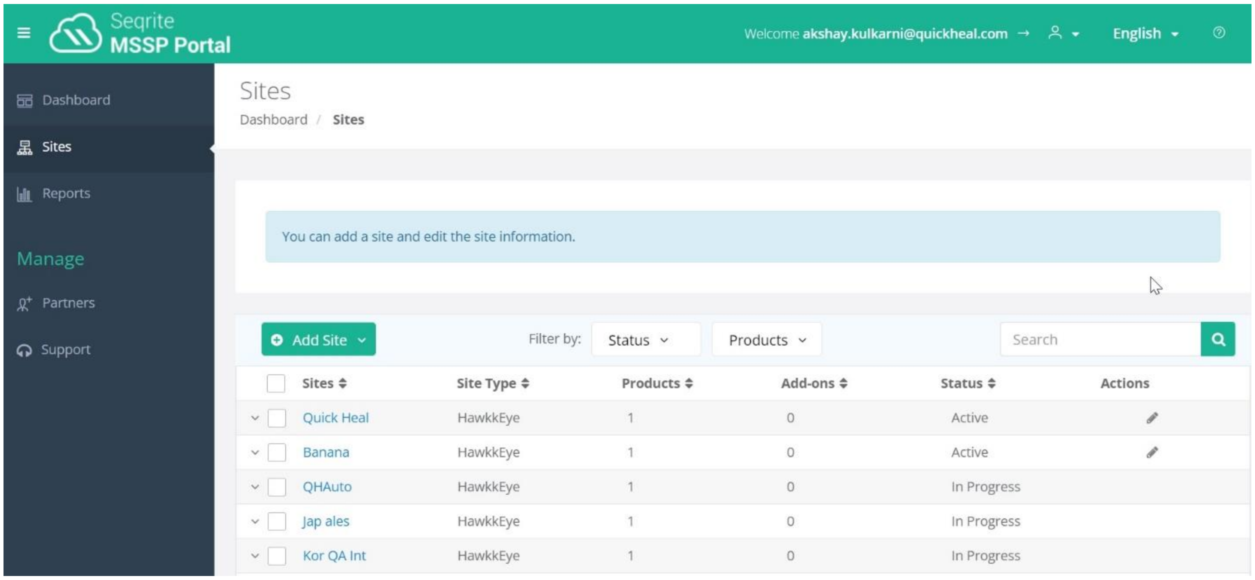
Features	**Description**
Total Active Commercial Sites	Displays the number of active commercial sites.
Trial Licenses Expiring	Displays the number of trial licenses that are going to expire in about 7 days. To see the details, click on the link under the feature.
Commercial Licenses Expiring	Displays the number of commercial licenses that are going to expire in about 7 days. To see the details, click on the link under the feature.
Commercial Licenses Activation	Displays the number of commercial licenses that have been activated in the last 7, 15, or 30 days. To see the details, click on the link under the feature.
Trial Licenses Activation	Displays the number of trial licenses that have been activated in last 7, 15, or 30 days. To see the details, click on the link under the feature.
Viruses Detected	Displays if any viruses have been detected. You can see viruses detected in the last 7, 15, and 30 days.

Intrusions Detected	Displays if any intrusions have been detected. You can see intrusion detected in the last 7, 15, and 30 days.
Policy Breach Attempts	Displays if there has been any policy breach attempts.

2. Sites

A site is a virtual premise of an organization. In Seqrite Managed Security Service Portal (MSSP), you can add a site to manage it and edit the site information based on your requirement.

You can see the status of the sites whether any of them are inactive or have expired, so you can take appropriate actions on time.



You can add a site and edit the site information.

	Sites	Site Type	Products	Add-ons	Status	Actions
□	Quick Heal	HawkkEye	1	0	Active	✎
□	Banana	HawkkEye	1	0	Active	✎
□	QHAuto	HawkkEye	1	0	In Progress	
□	Jap ales	HawkkEye	1	0	In Progress	
□	Kor QA Int	HawkkEye	1	0	In Progress	

This chapter includes the following sections.

Adding a Site

Logging in with 2FA

Viewing the Site details

Resending activation link

Managing devices

Retrying for failed sites

Editing the Site details

Adding a Site

To add a new site, follow these steps.

1. Log on to MSSP with your credentials.
2. Click the **Sites** menu and then click the **Add Site** button.
3. From the **Product Type** drop-down list, select either **CMS** or **HawwkEye** product for a client.

4. On the **Customer Details** tab, enter the **Name of Customer** and **Customer Address** of the organization, and select the **Country**, **State, City**, and **Zip Code** in the relevant fields.

   All asterisk fields are mandatory to select or fill.

   If you have selected CMS, click **Next**.

   If you have selected HawwkEye, fill the following information also.

   - Select **Customer Segment**, **Customer Industry/Vertical**, **Cloud Adoption**, **Cloud Type**, **User Sizing**, **Annual Revenue in USD**, **Annual IT Budget in USD**, and **Annual IT Security Budget in USD**. Click **Next**.

5. On the **Point of Contact Details** tab, enter the **First Name**, **Last Name**, **Contact Person Email Address**, **Job Role**, **Mobile Number**, and **Phone Number** of the contact person. Select **Enable Two-factor Authentication (2FA)** if you want to add an extra layer of security. Click **Next**.

   The person whose contact details are provided in this section will be responsible to provide support on all issues.

6. On the Add Product tab, select the **License Type** (Trail or Commercial), **Product**, and then click **Next**.

   You can add product by clicking the **Add Product** link.

7. On the **Configuration** tab, select the **Computer Policy** and then click **Next**.

   This policy is applicable only to HawwkEye having Seqrite EPS Cloud.

   Select a policy that you want to apply to your endpoints. If you do not select any policy, the default policy applies. (This step is applicable for MSP only.)

   A summary of the details that you entered appears. You can edit the information, if required. To edit the information, click **Previous** to go to the previous page or click the relevant tab and make the required change.

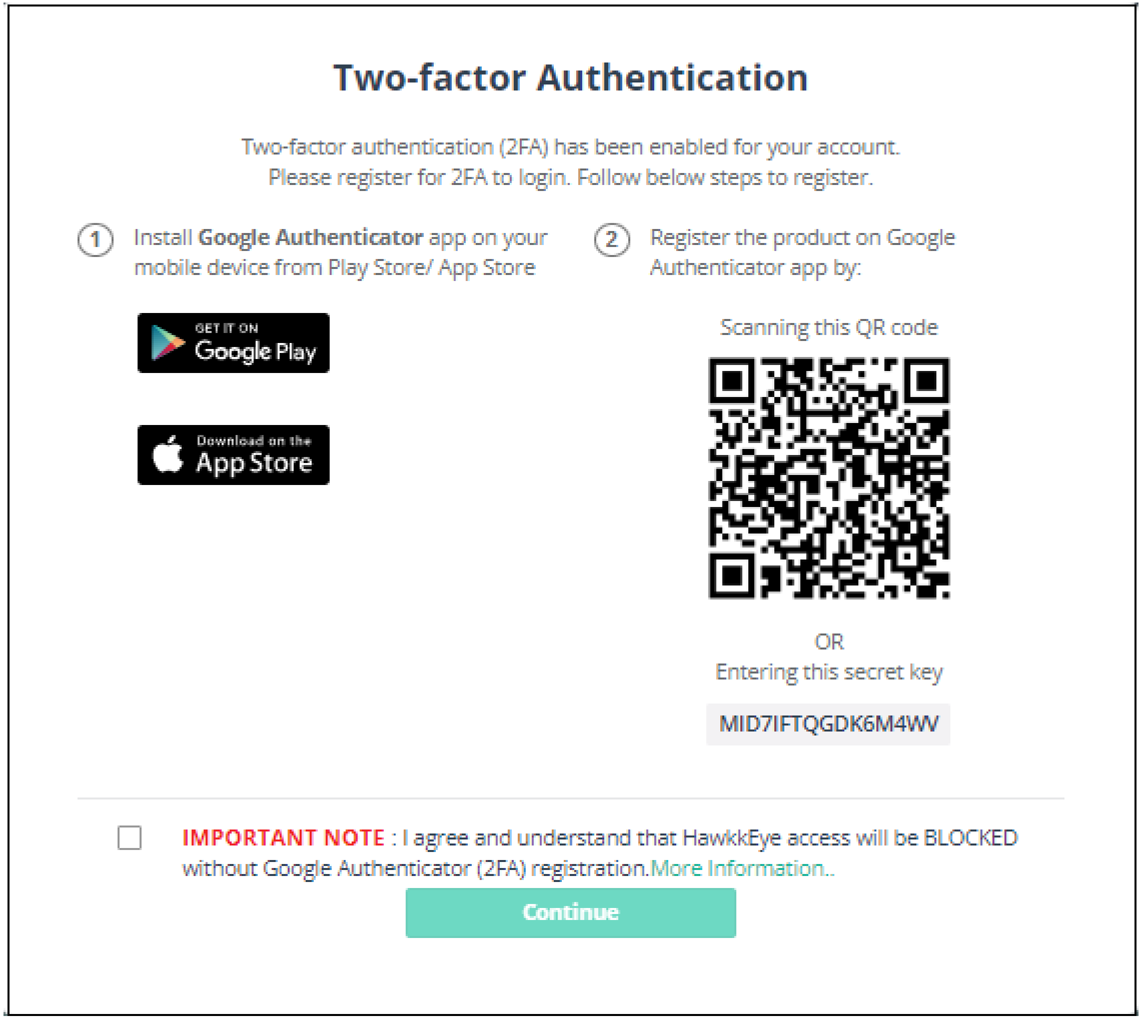
8. Verify the information and then click **Confirm** to submit the information.

Logging in with 2FA

If you have enable 2FA, in addition to your regular username and password, you would also need a code generated by the Google Authenticator app on the registered mobile number.

1. Log in to the Seqrite MSSP or HawkkEye portal using your regular username (email) and password.

2. You see the Two-factor Authentication screen prompting you to install Google Authenticator app from Google Play Store or Apple Store.



Two-factor Authentication

Two-factor authentication (2FA) has been enabled for your account. Please register for 2FA to login. Follow below steps to register.

(1) Install **Google Authenticator** app on your mobile device from Play Store/ App Store

(2) Register the product on Google Authenticator app by:

Scanning this QR code

OR

Entering this secret key

MID7IFTQGDK6M4WV

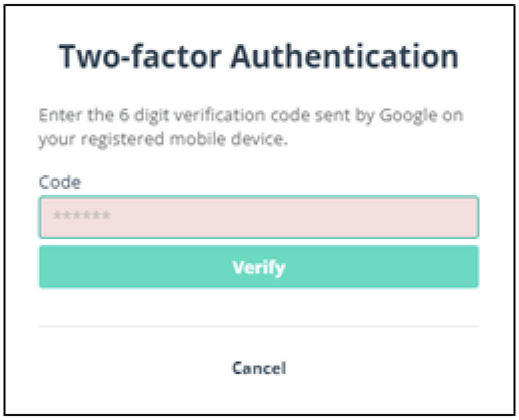
□ IMPORTANT NOTE : I agree and understand that HawkkEye access will be BLOCKED without Google Authenticator (2FA) registration.More Information..

3. After you install the Google Authenticator app on your registered mobile phone, you can proceed with either of the following options:

   - Scan the QR code displayed on the Two-Factor Authentication dialog. A 6-digit code will be generated and displayed on the mobile device.
   - Enter the secret setup key (displayed on the Two-Factor Authentication dialog). A 6-digit code is generated on the Google Authenticator app on your mobile phone.

4. On the Two-Factor Authentication dialog, select the **Important Note** check box. Seqrite MSSP or HawkkEye access will be blocked without Google Authenticator (2FA) registration. Click link ‘More Information’ to know more.

5. Click **Continue**. The Two- Factor Authentication dialog is displayed.



Two-factor Authentication

Enter the 6 digit verification code sent by Google on your registered mobile device.

Code: ******

6. Enter the 6-digit code received on your mobile as explained in the preceding step and click **Verify**.

   You are automatically logged on to the Seqrite MSSP or HawkkEye dashboard.

Note:

- The secret verification code will be sent each time to the user's registered mobile phone after 2FA is enabled for that user. If for some reason you enter the secret verification code incorrectly more than twice, the user account will be locked and user need to contact the administrator to get the 2FA reset.
- If you change your mobile or re-install the Google Authenticator on your mobile phone, you must request your Super Admin to reset the 2FA for your user account. You can log in again after you register for Google Authenticator and obtain your verification code.
- 2FA is enabled for Super Admin role for all new tenants by default. When Super Admin creates any user, 2FA will be enabled by default for that user. Users will be notified by an email when Super admin enables/disables/reset 2FA for any user.
- The Super Administrator can enable, disable or reset 2 Factor Authentication (2FA) for other users, as required.
- The process requires the end user to install a simple Google Authenticator app only the first time the user logs in to the portal after 2FA is activated for the user.

Viewing the Site details

To view a site information, follow these steps.

1. Log on to MSSP with your credentials.
2. Click the **Sites** menu.

   The Sites list appears.

   You can filter the sites based on status and products. Status of the sites may be Trial, Commercial, Active, Inactive, Failed, or Expired. Products may be Seqrite Endpoint Security, Seqrite mSuite, HawwkScan, CMS, DLP, HawkkHunt, and Workspace. You can view the details of a site and take actions as per requirement.

3. To view the site details, click on the site.

   The site details page appears.

4. On the Sites details page, you can do the following things.

   - Edit the site information: To edit the site information, click the **Edit** button on the upper right-hand.
   - Change policy: You can change the policy. (applicable to MSP only)
   - Resend Activation Link: To resend an activation link to the site, click the **Resend Activation Link** button and then click **Submit**.

Resending activation link

If a user does not receive the activation link, the administrator can resend the activation link to that user.

To resend an activation link, follow these steps.

1. Log on to MSSP with your credentials.
2. Click the **Sites** menu.

   The Sites list appears.

3. Select a site.

   An action list titled **Please Select** is added.

4. From the action drop-down list, select **Resend Activation Link** and then click **Submit**.

   A confirmation message appears.
   The activation link can also be sent from the site details.

5. Click **OK**.

   The resend activation link is sent successfully.

Managing sites

Note: This procedure is applicable only for MSP.

To manage sites, follow these steps.

1. Log on to MSSP with your credentials.
2. Click the **Sites** menu.

   The Sites list appears.

3. Under the Actions column, click the **Manage** icon.

   HawkkEye console opens in a new window.

4. If you are accessing for the first time, select the license agreement and privacy policy. Click **Yes, I Agree**.

You can navigate to Seqrite products such as Seqrite EPS Cloud, Seqrite mSuite, HawkkProtect, HawkkScan through HawkkEye.

Retrying for failed sites

If any site is not placed on board successfully, you can retry the process.

To retry to place the site on board, follow these steps.

1. Log on to MSSP with your credentials.
2. Click the **Sites** menu.

   The Sites list appears.

   Under the Status column, you can see the status whether a site has failed. If the site has failed, a new link for retrying appears.
3. Click the retry link.

   The process for placing the site on board gets initiated.

Editing the Site details

To edit a site information, follow these steps.

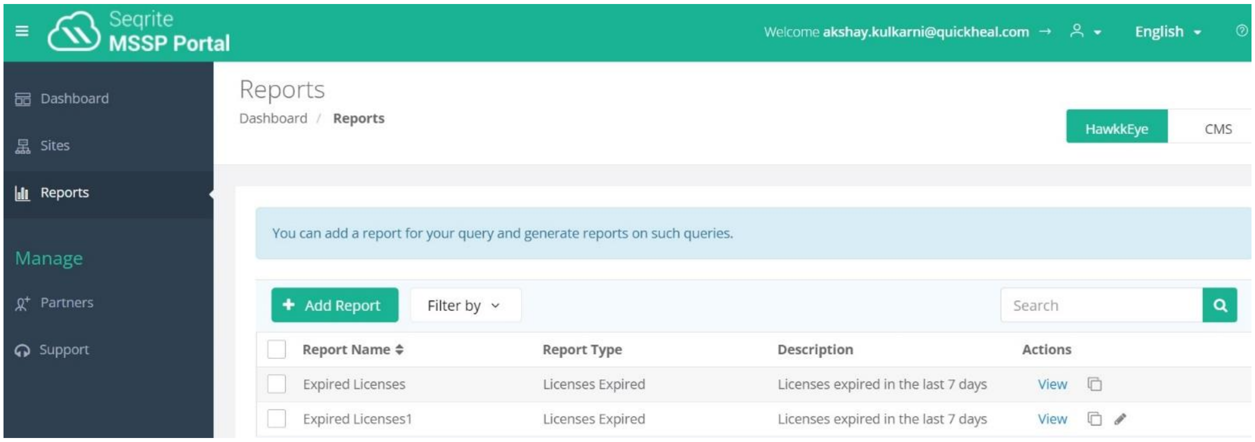
1. Log on to MSSP with your credentials.
2. Click the **Sites** menu.

   The Site list appears, if you have added any sites.
3. Under the Actions column, click the edit icon for the site that you want to edit. You can edit the **Customer Details**, **Point of Contact Details**, and **Configuration**.

   Editing the site information is similar to adding a new site.
4. After making the required changes, click **Confirm**.

3. Reports

You can add a new report for your query and generate reports for the existing queries. For example, you may like to know how many licenses under a partner have expired, whether there were any intrusion incidents during a certain period, or whether there were any virus attacks while a user was browsing online. You can generate reports for HawwkEye or Central Management System (CMS) product that you purchased.



You can add a report for your query and generate reports on such queries.

□	Report Name	Report Type	Description	Actions
□	Expired Licenses	Licenses Expired	Licenses expired in the last 7 days	View
□	Expired Licenses1	Licenses Expired	Licenses expired in the last 7 days	View

This chapter includes the following sections.

[Adding a report]

[Generating a report]

[Duplicating a report]

[Exporting a report]

[Editing a report]

[Removing a report]

Adding a report

To add a new report, follow these steps.

1. Log on to MSSP with your credentials.
2. Click the **Reports** menu and then click the **Add Report** button.
3. Select **Report Type**.

   Report Type may be License Expired and Virus Detected. Depending on the report type that you select, some parameters for report may vary. For example, if you select License Expired, the Partners list will appear. If you select Virus Detected, the Sites list will appear.
4. Write the Report Name and description.

5. From the Sites list, select the Site name.

   The Sites list appears, if you have selected Virus Detected.

6. From the Partners list, select the Partner name.

   The Partners list appears if you have selected License Expired.

7. Select the period for which the report is required.

   The periods may be 7, 15, 30 days. You can customize the period, if required.

8. Select the License Type.

   License Type may be Trail and Commercial.

9. Click the **Add** button.

   The new report is added successfully.

10. Click **Close**.

Generating a report

In the Reports menu, you can generate reports on various queries such as how many licenses under a partner have expired or what incidents occurred during a certain period.

To generate a report, follow these steps.

1. Log on to MSSP with your credentials.
2. Click the **Reports** menu.

   A report list appears that displays various queries. You can generate reports on any queries such as Licenses Expired or Virus Detected.

3. To generate a report on a query, click the **View** icon under the Actions column.

   A report page of the selected report type appears.

4. Select Sites or Partners (based on the report type), Period, or License Type to change the report data.
5. After setting the filtering criteria, click the **Generate Report** button to refresh the report.

Duplicating a report

To duplicate a report, follow these steps.

1. Log on to MSSP with your credentials.
2. Click the **Reports** menu.

   A report list appears.

3. Click the **Duplicate** icon on the report that you want to duplicate.

   Two icons, one green check mark for duplicating the report and one cross mark for canceling the action, appear.

You can duplicate a default report or any other report. The selected report is highlighted.

4. Change the name of the report and then click the green check mark displayed on the selected report.

   The duplicated report should have a new report name. However, the duplicated report inherits the information of all the fields. You can edit the report, if required.

Exporting a report

You can export a report that you generate for future reference. You can export the report in the CSV format. To export a report, follow these steps.

1. Log on to MSSP with your credentials.
2. Click the **Reports** menu.

   A report list appears.

3. Under the Actions column, click the **View** icon.

   A report page of the selected report type appears.

4. To export the report, click the **Export as CSV** button on the top-right corner.

   The report is exported.

Editing a report

To edit a report, follow these steps.

1. Log on to MSSP with your credentials.
2. Click the **Reports** menu.
3. On the Report page, you can see the reports that you have created.
4. Under the Actions column, click the **Edit** icon for the report that you want to edit.

   The Edit Report dialog box appears.

5. On the Edit Report dialog box, you can edit the information in any of the Report Type, Report Name, Description, Sites or Partners (based on the report type), Period, or License Type fields.
6. Click **Save**.

Removing a report

To remove a report, follow these steps.

1. Log on to MSSP with your credentials.
2. Click the **Reports** menu.

   A report list appears.

3. On the Report page, select the report that you want to remove.

   An action list titled **Please Select** is added.

4. Select **Remove Report** from the **Please Select** list and then click **Submit**.

   A confirmation message appears.

5. To confirm your action, click **Confirm**.

   The selected report is deleted.

4. Manage Partners

Under Manage Partners, you can create partners of MSP and Partner levels. Administrative level users can edit and disable their subordinate partners.

When you log on to MSSP, the Partners list appears. The Partners list is based on the privilege you have as a partner type. You can view the tree structure of all the partners under you. You can also view total number of MSPs, partners, partners' customers, and partners' endpoints.

This chapter includes the following sections.

Adding a partner

To add a partner, follow these steps.

1. Log on to MSSP with your credentials.
2. Under the Manage list, click the **Partners** menu.

   The Partners list appears, if you have added any.
3. Click the **Add Partner** button.
4. From the **Partner Type** drop-down list, select the partner type and then click **Next**.
5. On the **Company Details** tab, provide the **Name** and **Address** of the company, and select your **Country**, **State, City**, and **Zip Code** in the relevant fields. You may also add a logo of the relevant company. Click **Next**.
6. On the **Point of Contact Details** tab, provide the **Full Name**, **Email Address**, **Mobile Number**, and **Phone Number** of the contact person. Select **Enable Two-factor Authentication (2FA)** if you want to add an extra layer of security. Click **Next**.

   The Point of Contact will be responsible for providing support for all related issues.
   A summary is displayed on the **Confirmation** dialog box.
7. Verify the information that you entered and then click **Confirm** to submit the information.

   If you need to change the information, you may click **Previous** to go to the previous page or click the relevant tab to make any change.

Viewing the partner details

To view a partner information, follow these steps.

1. Log on to MSSP with your credentials.
2. Under the Manage list, click the **Partners** menu.

   The Partners list appears.
3. To view partners under a partner, click the arrow (>).
4. To view the details of a partner, click a partner under the **Partners** list.

   The partner details page appears.

   You can edit the partners that are directly under you and not indirect partners.
5. On the Partners list, you can do the following things based on your role.
   - Edit the partner information
     - To edit the partner information, click the **Edit** icon for the partner that you want to edit under the Actions column.
   - Resend Activation Link
     - To resend an activation link to the partners, select a partner. An action list titled Please Select is added. From the Please Selection action list, select **Resend Activation Link** and then click **Submit**.
       You may send reactivation link to multiple number of partners in one attempt.
       Note: You may send the activation link to the partners with pending verification status only.

Resending activation link

If any partner does not receive the activation link, the administrator can resend the activation link to the customer.

To resend an activation link, follow these steps.

1. Log on to MSSP with your credentials.
2. Click the **Partners** menu.

   The Partners list appears.
3. Select a partner.

   An action list titled Please Select is added.
4. From the action drop-down list, select **Resend Activation Link** and then click **Submit**.

   A confirmation message appears.

   The activation link can also be sent from the partner details.

   Note: You may send the activation link to the partners with pending verification status only.

5. Click **OK**.

   The resend activation link is sent successfully.

5. Users

The Seqrite Managed Security Service Portal (MSSP) portal allows partners to create users based on their roles.

Note: A Report Viewer can add, edit, and delete reports related to the organization. A Report Viewer cannot add/modify/delete any profiles in the MSSP platform.

This chapter includes the following sections.

Adding a user

To add a user, follow these steps.

1. Log on to MSSP with your credentials.
2. Under the Manage list, click the **Users** menu and then click the **Add User** button.

   The Add User dialog appears.
3. On the Add User dialog box, select the role for the user from the **User Type** drop-down list.
4. Select **Admin** and then click **Next**.
5. Enter **Name**, **Email Address**, **Mobile Number**, and **Phone Number** in the relevant boxes.

   All asterisk fields are mandatory to enter.
6. Select Enable Two-Factor Authentication (2FA).

   Two-Factor authentication is not a mandatory option.
7. Click the **Add User** button.

   The user is added successfully.

Enabling or disabling a user

To enable or disable a user, follow these steps.

1. Log on to MSSP with your credentials.
2. Under the Manage list, click the **Users** menu.

   A user list appears.

3. Select a user.

   An action list titled Please Select is added.

4. From the Please Select action list, click **Enable** or **Disable** and then click **Submit**.

   A confirmation dialog box appears.

5. To confirm your action, click **Confirm**.

   The user is disabled successfully.

Resending activation link

If any user does not receive the activation link, the administrator can resend the activation link to that user.

To resend an activation link, follow these steps.

1. Log on to MSSP with your credentials.
2. Click the **Users** menu.

   The Users list appears.

3. Select a user.

   An action list titled Please Select is added.

4. From the action drop-down list, select **Resend Activation Link** and then click **Submit**.

   A confirmation message appears.

   Note: You can send the activation link to the partners with pending verification status only.

5. Click **OK**.

   The resend activation link is sent successfully.

Editing a user

To edit a user information, follow these steps.

1. Log on to MSSP with your credentials.
2. Under the Manage list, click the **Users** menu.

   A user list appears.

3. Under the Actions column, click the **Edit** icon for the user that you want to edit.
4. On the **Edit User** dialog box, edit the user information as required.
5. Click **Save**.

   The details are updated successfully.

Deleting a user

To delete a user, follow these steps.

1. Log on to MSSP with your credentials.
2. Under the Manage list, click the **Users** menu.
3. Select a user.

   An action list titled Please Select is added.
4. From the Please Select action list, select **Delete**.

   A confirmation message appears.
5. To confirm your action, click **Confirm**.

   The user is deleted successfully.

6. Policies for Computer

Under Policies, you can add a new policy, edit a policy, and delete a policy for your computers.

MSSP provides system defined polices for various reasons such as how and what files should be scanned, what email protection should be applied, what firewall and online security should be applied, and other protection for security.

This chapter includes the following sections.

Adding or duplicating a policy

Editing and publishing a policy

Deleting a policy

Adding or duplicating a policy

To add a new policy you need to duplicate a policy and then you can configure the settings of the duplicated policy as per your requirement. The duplicated policy inherits the settings of the existing policy.

To add or duplicate a policy, follow these steps.

1. Log on to MSSP with your credentials.
2. Under the Policies list, click the **Computer** menu.

   A Polices list is displayed.
3. On the Policies list, select a policy and then click the duplicate icon under the Actions column.
4. Edit the **Policy Name** and then click the check mark to save the policy.

   The policy is added to the policy list.

Editing and publishing a policy

To edit a policy, follow these steps.

1. Log on to MSSP with your credentials.
2. Under the Policies list, click the **Computer** menu.

   A Polices list is displayed.
3. On the Policies list, select a policy and then click the edit icon under the Actions column.

   You can change the policy name, description, and policy settings.

   Note: The default policy cannot be edited.
4. To save your settings, click **Save**.

A confirmation message is displayed.

You may need to publish the new setting to the customers. To publish the setting, click the **Save & Publish** button. The new setting is applied to the customers to whom that policy is applied.

5. To close the confirmation screen, click **Close**.

Deleting a policy

To delete a policy, follow these steps.

1. Log on to MSSP with your credentials.
2. Under the Policies list, click the **Computer** menu.

   A Polices list is displayed.
3. On the Policies list, select a policy and then click the **Delete** button.

   The selected policy is deleted.

   Make sure if you want to remove a policy. A policy once deleted cannot be recovered.

   You cannot delete a default policy or a policy that is assigned to a customer.

   Tip: If you want to delete a policy that is assigned to a customer, you first need to unassign the policy from the customer. To unassign a policy, you have to apply a different policy to the customer so that the policy becomes unassigned to any customer and then you can delete the policy.

7. Editing Profile

You can edit the profile of a user or partner if required.

To edit a profile information, follow these steps.

1. Log on to MSSP with your credentials.
2. Click **Edit Profile** available on the upper-right corner.

   The Edit Profile page appears.

   You can edit the Company Details, Point of Contact Details, Notifications, and Settings.

Setting notifications

You can configure the setting for notification for various incidents such as if any license is going to expire soon, a license has been deactivated, and so on. The partners will get the notification as per the setting.

1. In the Edit Profile of a partner, click the **Notifications** tab.
2. Under **License/Site Notification**, configure the following settings.
   - License of a site is about to expire.
   - License of a site has expired.
   - License of a site is about to be deactivated.
   - License of a site has been deactivated.
3. Under **Virus Notifications**, configure the following settings.
   - Virus infection detected at any site
   - Virus Outbreak detected at any site

     Note: These options may not appear in Seqrite Endpoint Security.
4. To save your setting, click the **Save** button.

Setting time zone

In Settings, you can select the time zone for your geographical location. This helps you to adjust to your local time, wherever you are located.

1. On the Edit Profile, click the **Settings** tab.
2. Under **Time Zone**, select the time zone for your geographical location.

   This helps to set to your local time.
3. To save your setting, click the **Save** button.

Setting period for removing reports

In Settings, you can set the number of days after which the report should be deleted from the system. This helps you to remove the old reports that you do not need any longer.

To set the period for removing the reports, follow these steps.

1. Log on to MSSP with your credentials.
2. Under the Admin list, click the **Settings** menu.
3. In **After No. of days**, select the days (30 or 60) when the report should be deleted.

8. Technical Support

Seqrite Managed Security Service Portal (MSSP) provides extensive technical support for its users. In case you face any technical issue, you can contact us.

To get the contact details, follow these steps.

1. Log on to MSSP with your credentials.
2. Click the **Support** menu.

   A support page appears.

Support contacts

To know support contacts, please visit:

http://www.seqrite.com/seqrite-support-center

Head Office Contact Details

Quick Heal Technologies Limited

(Formerly known as Quick Heal Technologies Pvt. Ltd.)

Reg. Office: Marvel Edge, Office No.7010 C & D, 7th Floor,

Viman Nagar, Pune 411014, Maharashtra, India.

Official Website: http://www.seqrite.com.

Email: support@seqrite.com