



User Guide

v3.1.0

Copyright & License Information

© 2018-2024 Quick Heal Technologies Ltd. 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, Reg. Office: Marvel Edge, Office No. 7010 C & D, 7th Floor, Viman Nagar, Pune 411014.

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

Trademarks

Seqrite MSSP is a registered trademark of Quick Heal Technologies Ltd. while Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and product titles are trademarks of their respective holders.

License Terms

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




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

Release Date

April 6, 2024

About This Document

This guide covers all the information required to use SEQRITE Managed Security Service Portal (Seqrite 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.
	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

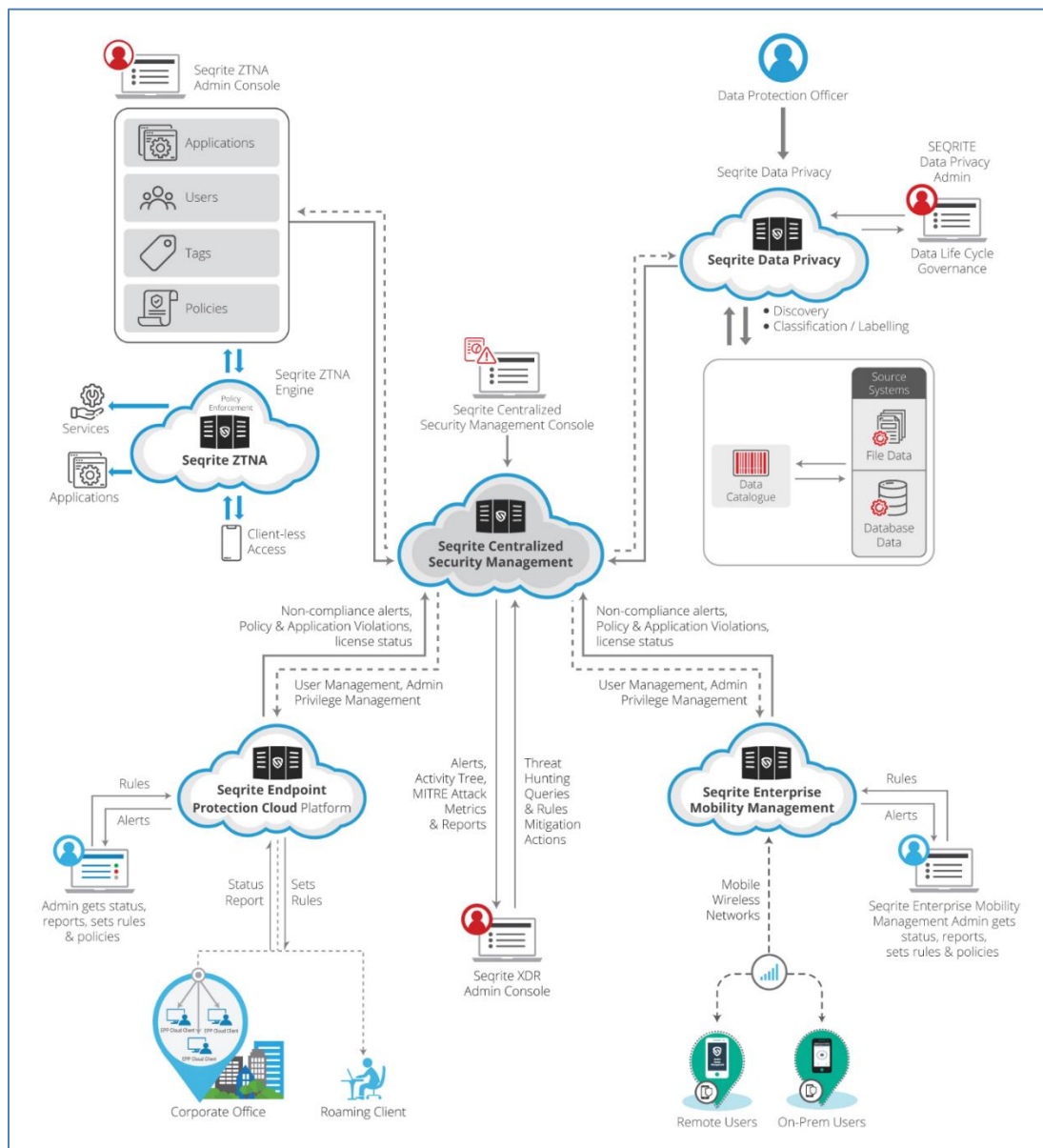
1. Seqrite MSSP Dashboard	8
2. Sites.....	12
Adding a Site.....	13
Viewing the Site details	13
Resending activation link.....	15
Managing sites.....	15
Retrying for failed sites	16
Editing the Site details.....	16
Deleting the failed and inactive Sites	17
3. Reports.....	18
Adding a report	18
Generating a report.....	19
Duplicating a report.....	19
Exporting a report	20
Editing a report.....	20
Removing a report.....	21
4. Manage Partners	22
Adding a partner.....	22
Activating a newly added Partner/MSP	23
Viewing the partner details.....	24
Resending activation link.....	24
5. Manage Users.....	25
Adding a user.....	25
Activating a newly added User	26
Using Two Factor Authentication (2FA)	26
Enabling or disabling a user.....	28
Enabling 2FA for Users (Bulk 2FA Authentication).....	28
Resending activation link.....	28
Editing a user	29
Deleting a user.....	30
6. Policies for Computer	31
Adding or duplicating a policy	31

Editing and publishing a policy	31
Deleting a policy	32
7. Editing Profile	33
Setting notifications	34
Setting time zone.....	34
8. Admin	35
Settings	35
Deleting Reports	35
9. Activity Logs	36
Observing the Activity Logs.....	36
10. License Telemetry.....	37
Generating the License Telemetry.....	37
11. Technical Support.....	38
Localization Support	38
Head Office	38
Other support contact.....	39

1. Seqrite MSSP Dashboard

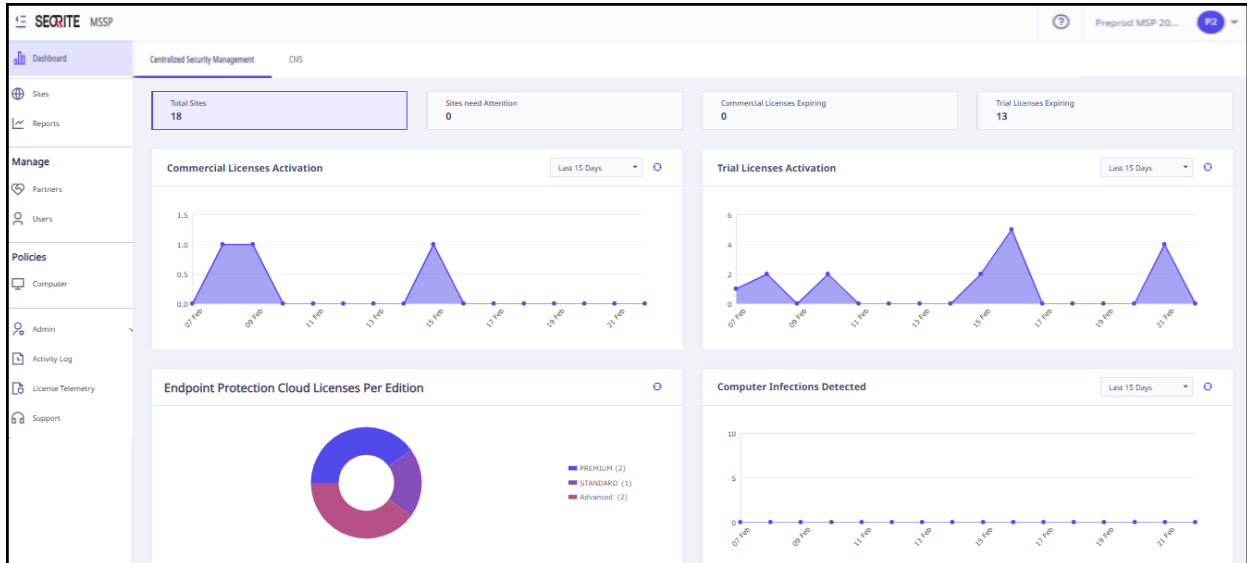
Seqrite MSSP is a web-based portal. Seqrite MSSP empowers managing multi-tenant Seqrite Centralized Security Management deployments with any combination of Seqrite products including Seqrite Endpoint Protection Cloud, Seqrite Enterprise Mobility Management, Seqrite ZTNA, Seqrite Data Privacy, and Seqrite XDR.

Seqrite Centralized Security Management enables to integrate any of the Seqrite products including Seqrite Endpoint Protection Cloud, Seqrite Enterprise Mobility Management, Seqrite ZTNA, Seqrite Data Privacy, and Seqrite XDR.



When you log on to the Seqrite MSSP portal, 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 Seqrite MSSP editions, and so on.

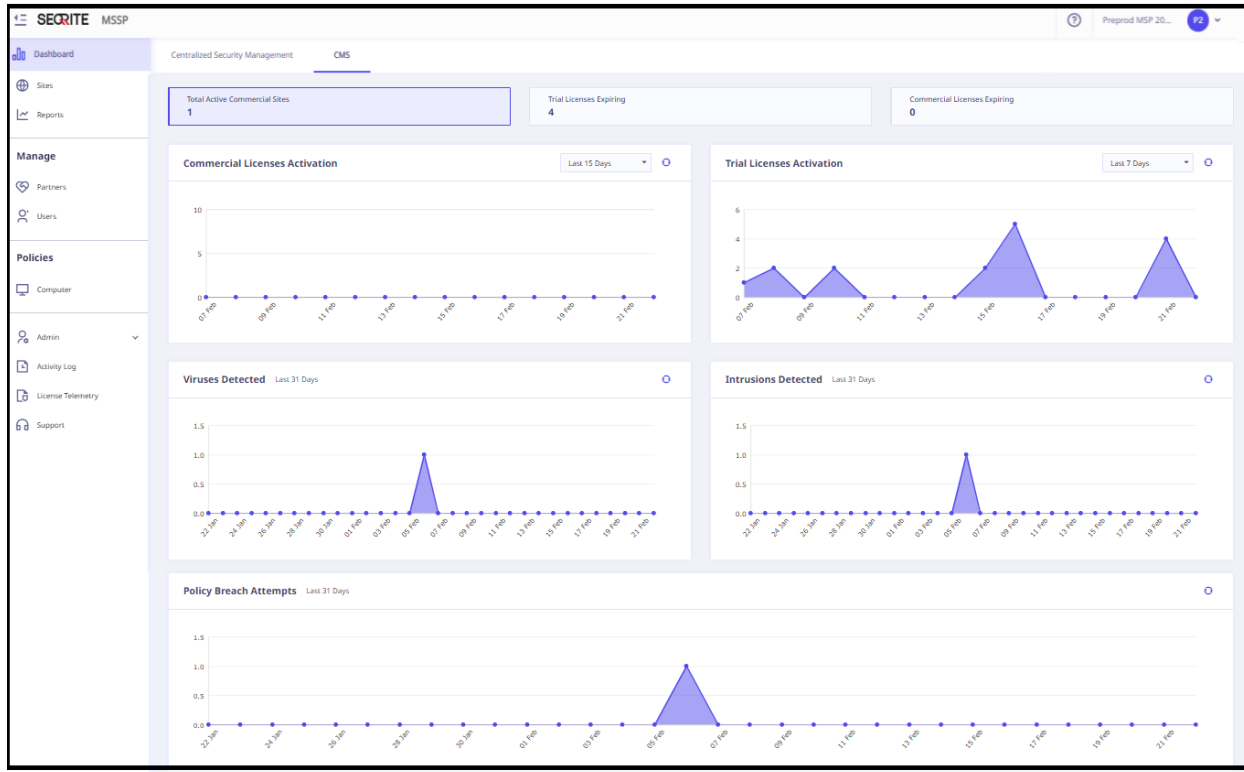
Seqrite MSSP Seqrite Centralized Security Management Dashboard



The following table describes the features of Seqrite MSSP 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.

Seqrite MSSP CMS Dashboard



The following table describes the features of Seqrite MSSP CMS displayed on dashboard.

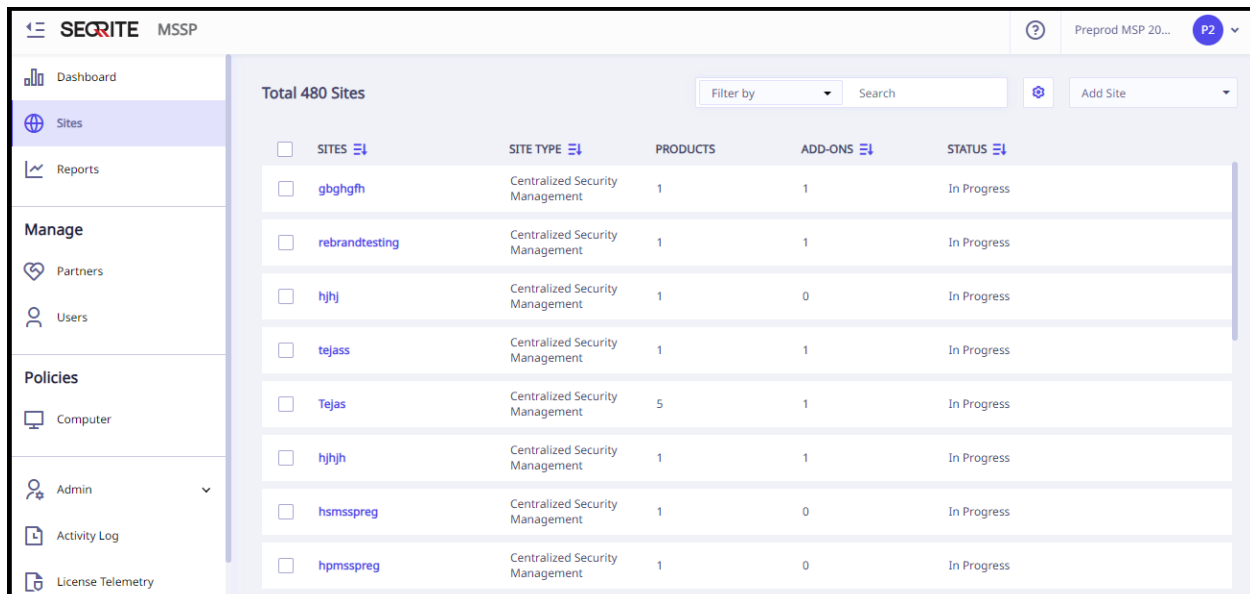
Features	Description
Total Active Commercial Sites	Displays the total number of active commercial sites.
Trial Licenses Expiring	Displays the number of trial licenses that are going to expire in about 7 days. To see the details, click the tab.
Commercial Licenses Expiring	Displays the number of commercial licenses that are going to expire in about 7 days. To see the details, click the tab.
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 the tab.
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 the tab.
Viruses Detected	Displays the count of viruses detected over the last 31 days.

Features	Description
Intrusions Detected	Displays the count of intrusion attempts over the last 31 days.
Policy Breach Attempts	Displays the count of policy breach attempts over the last 31 days.

2. Sites

A site is a virtual premise of an organization. In Seqrite 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.



<input type="checkbox"/>	SITES	SITE TYPE	PRODUCTS	ADD-ONS	STATUS
<input type="checkbox"/>	gbghgfh	Centralized Security Management	1	1	In Progress
<input type="checkbox"/>	rebrandtesting	Centralized Security Management	1	1	In Progress
<input type="checkbox"/>	hjhj	Centralized Security Management	1	0	In Progress
<input type="checkbox"/>	tejass	Centralized Security Management	1	1	In Progress
<input type="checkbox"/>	Tejas	Centralized Security Management	5	1	In Progress
<input type="checkbox"/>	hjhjh	Centralized Security Management	1	1	In Progress
<input type="checkbox"/>	hsmsspreg	Centralized Security Management	1	0	In Progress
<input type="checkbox"/>	hpmsspreg	Centralized Security Management	1	0	In Progress

This chapter includes the following sections.

[Adding a Site](#)

[Viewing the Site details](#)

[Resending activation link](#)

[Managing devices](#)

[Retrying for failed sites](#)

[Editing the Site details](#)

[Deleting a Site](#)

Adding a Site

To add a new site, follow these steps.

1. Log on to Seqrite 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 **Seqrite Centralized Security Management** 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.
5. 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.**
6. On the **Point of Contact Details** tab, enter the **First Name, Last Name, Email Address of Contact Person, 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.

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

You can add more products by clicking the **Add Product** link.

8. On the **Confirmation** tab, select the **Computer Policy** and then click **Next.**

This policy is applicable only to Seqrite Centralized Security Management having Seqrite Endpoint Protection 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.

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

Viewing the Site details

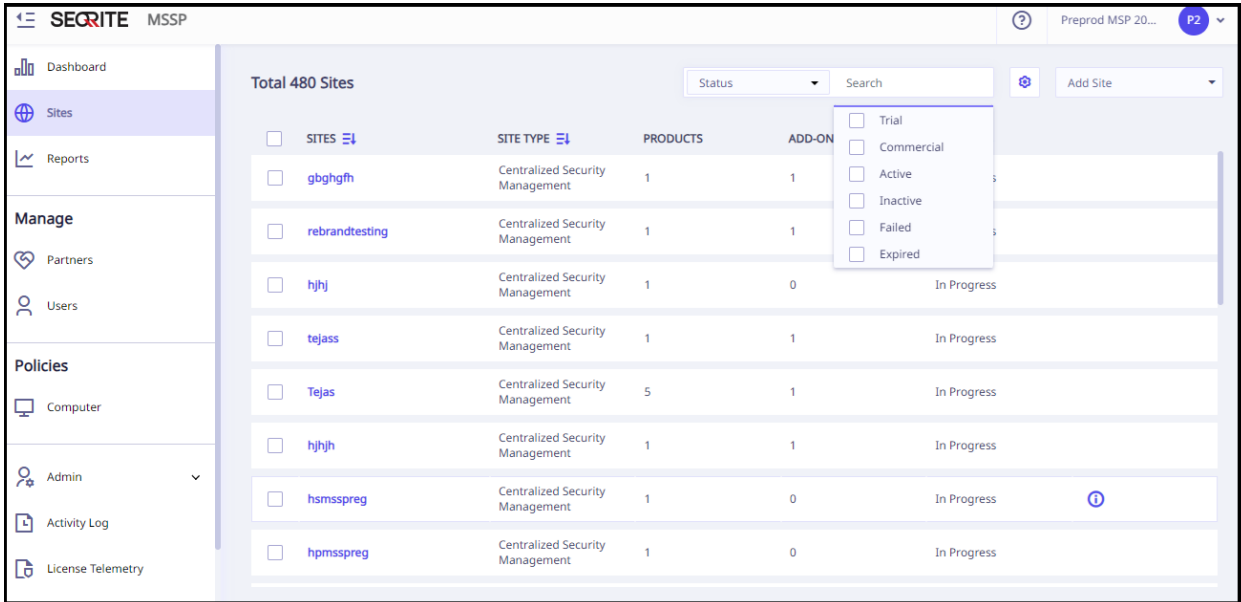
To view a site information, follow these steps.

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

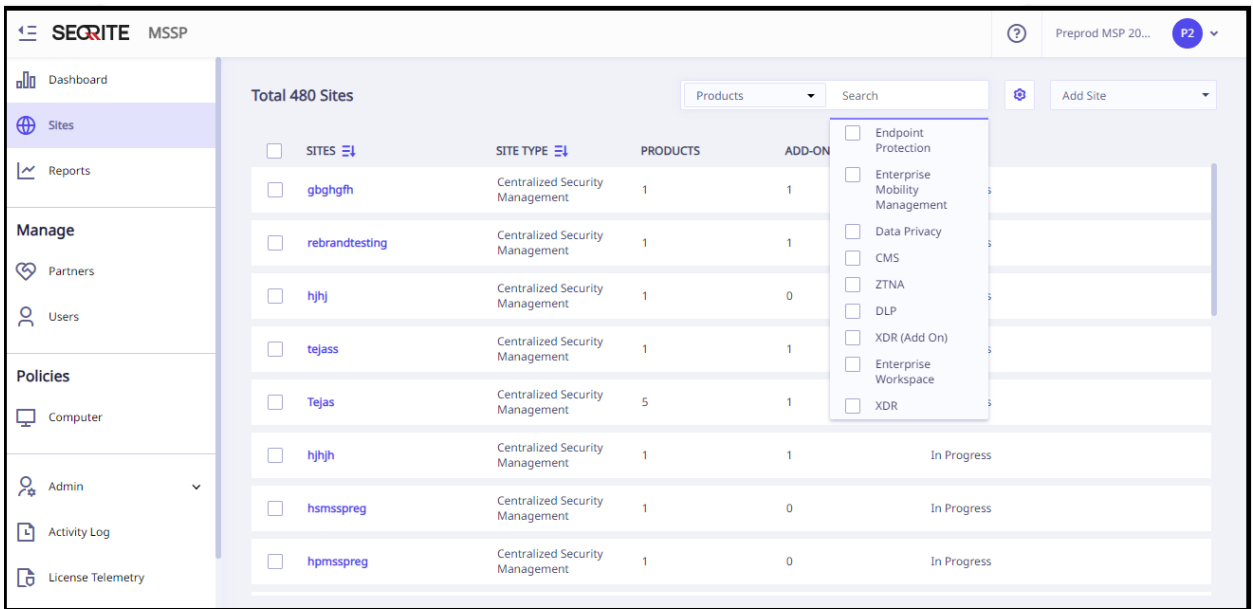
The Sites list appears.

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 Protection, Seqrite Enterprise Mobility Management, Seqrite Data Privacy, DLP, Seqrite XDR, 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 Seqrite 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 Seqrite MSSP with your credentials.
2. Click the **Sites** menu.
The Sites list appears.
3. Under the Actions column, click the **Manage** icon.
Seqrite Centralized Security Management 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 Endpoint Protection Cloud, Seqrite Enterprise Mobility Management, Seqrite ZTNA, Seqrite Data Privacy through Seqrite Centralized Security Management.

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 Seqrite 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 Seqrite 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**.

Deleting the failed and inactive Sites

To delete a site, follow these steps.

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

The Site list appears if you have added any sites.



The screenshot displays the Seqrite MSSP interface. On the left is a navigation sidebar with options: Dashboard, Sites (selected), Reports, Manage (Partners, Users), Policies (Computer), Admin (dropdown), Activity Log, and License Telemetry. The main content area shows a table of sites with 4 selected. A dropdown menu is open over the 'Please Select' button, showing 'Resend Activation Link' and 'Delete' options. A 'Submit' button is visible in the top right corner.

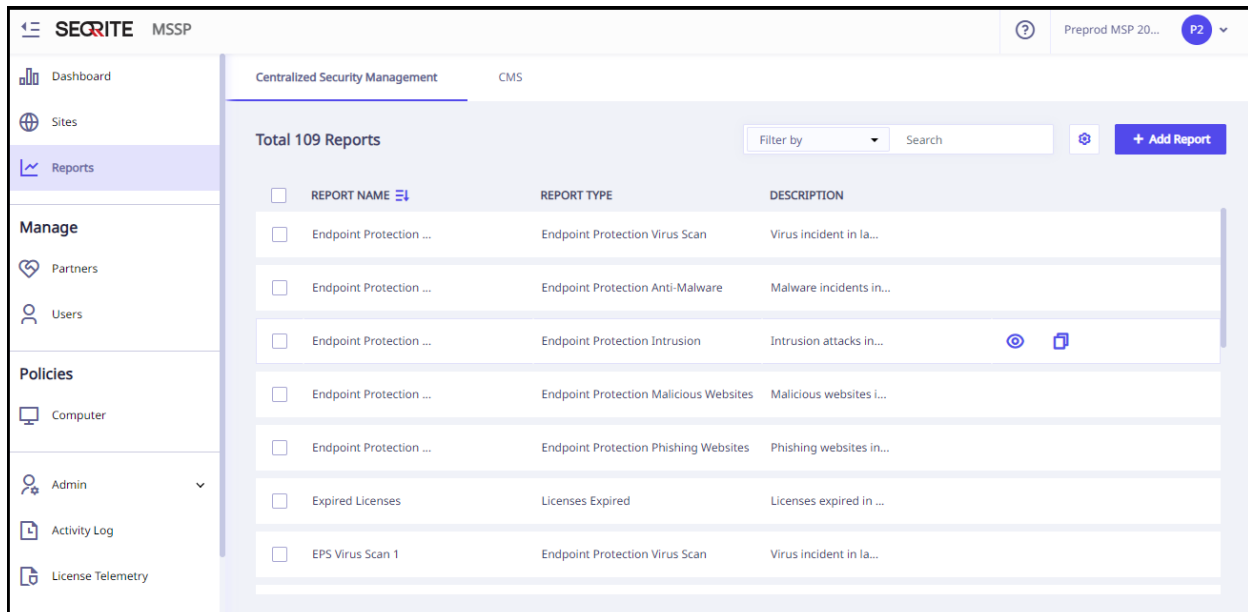
<input type="checkbox"/>	SITES	SITE TYPE	PRODUCTS	ADD-ONS	STATUS
<input checked="" type="checkbox"/>	EPS user	Centralized Security Management	1	1	Inactive
<input checked="" type="checkbox"/>	Quickheal	Centralized Security Management	1	0	Inactive
<input checked="" type="checkbox"/>	qause	Centralized Security Management	1	0	Inactive
<input checked="" type="checkbox"/>	mspuser	Centralized Security Management	1	0	Inactive
<input type="checkbox"/>	ssssss	Centralized Security Management	1	0	Inactive
<input type="checkbox"/>	sddssas	Centralized Security Management	1	1	Inactive
<input type="checkbox"/>	gbghgfh	Centralized Security Management	1	1	Inactive
<input type="checkbox"/>	rebrandtesting	Centralized Security Management	1	1	In Progress

3. Select the inactive or the failed site that you want to delete.
4. In the **Please Select** drop down on the upper right corner, click **Delete**.
5. Click **Submit** to confirm deletion.

The selected site is deleted.

3. Reports

You can add a new report for your query and generate reports for the existing queries for Seqrite Centralized Security Management. 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.



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 Seqrite 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 Seqrite 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.
A relevant report is displayed.

Duplicating a report

To duplicate a report, follow these steps.

1. Log on to Seqrite 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 Seqrite 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 Seqrite 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 Seqrite 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 partner's.

When you log on to Seqrite MSSP, the Partners list appears. The Partner's 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, partner's customers, and partner's endpoints.

This chapter includes the following sections.

[Adding a partner](#)

[Viewing the partner details](#)

[Resending activation link](#)

Adding a partner

To add a partner, follow these steps.

1. Log on to Seqrite 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) check box if required. By default, the Email-based OTP option is enabled for the user, select the SMS-based OTP if required. If the SMS-based OTP option is enabled for the user then that user will get the OTP on the email address as well as on the user's registered mobile number. Before that, the user needs to verify the mobile number from Edit Profile Section.

Note:

- Only the Super Administrator can Enable/Disable 2FA for users.

- When the Super Administrator enables 2FA for users, the users receive an email notification. Subsequently, every time the user logs in, they are required to provide an OTP that is sent to their registered mobile device or email address in order to access the MSSP portal.

7. 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.

8. Verify the information that you entered and then click **Confirm** to submit the information. The partner is onboarded, and success confirmation prompt is displayed.

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.

Activating a newly added Partner/MSP

After Admin has created a Partner/MSP account as mentioned in above procedure, an email with Set password link is sent to the registered email address. The newly added Partner/MSP must access the mail and set the password using the Set Password link to login to the new account.

Sign In

1. Log on to Seqrite MSSP with your credentials.
2. Enter the OTP received on your registered email address.

Note: The OTP is valid for 60 seconds only.

The License Agreement screen is displayed.

3. Read the agreement and then click **I Agree**.

The dashboard is displayed.

Viewing the partner details

To view a partner information, follow these steps.

1. Log on to Seqrite 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 Seqrite 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. Manage Users

The Seqrite 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 Seqrite MSSP platform.

This chapter includes the following sections.

[Adding a user](#)

[Enabling or disabling a user](#)

[Resending activation link](#)

[Editing a user](#)

[Deleting a user](#)

Adding a user

To add a user, follow these steps.

1. Log on to Seqrite 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 the Enable Two-Factor Authentication (2FA) if required.

By default, the Email-based OTP option is enabled for the user, select the SMS-based OTP if required. If the SMS-based OTP option is enabled for the user then that user will get the OTP on the email address as well as on the user's registered mobile number. Before that, the user needs to verify the mobile number from Edit Profile Section.

Note:

- Only the Super Administrator can Enable/Disable 2FA for users.
 - When the Super Administrator enables 2FA for users, the users receive an email notification. Subsequently, every time the user logs in, they are required to provide an OTP that is sent to their registered mobile device or email address in order to access the MSSP portal.
7. Click the **Add User** button. The user is added successfully.

Activating a newly added User

After Admin has created a user account as mentioned in above procedure, an email with Set password link is sent to the registered email address. The newly added user must access the mail and set the password from the password link to login to the new account.

Sign In

1. Log on to Seqrite MSSP with your credentials.
2. Enter the OTP received on your registered email address.

Note: The OTP is valid for 60 seconds only.

The dashboard is displayed.

Using Two Factor Authentication (2FA)

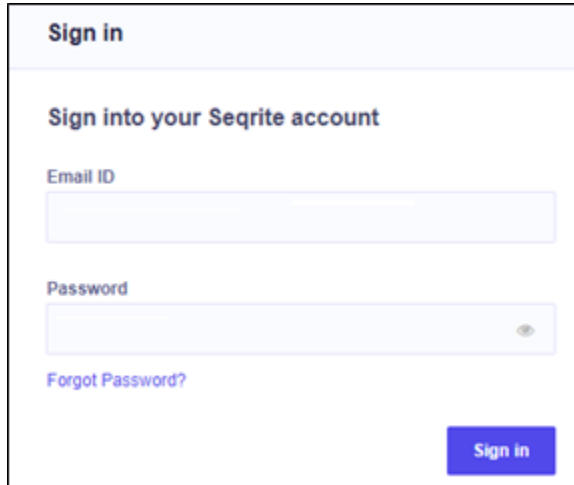
With MSSP 3.1 release dated 22/04/2023, the earlier Google Authenticator App based 2FA process has been eliminated. Now we have introduced Simple MFA with Email and SMS based OTP. By default, you will receive the OTP on your registered email address.

As a security enhancement, the Super administrator has the ability to enable 2FA for users. This feature requires a two-step verification process, thereby providing a higher level of security for the user's account. Apart from the regular username and password, the user must also provide an OTP that is generated on their email address or registered mobile number.

Note:

At present, SMS-based OTP authentication is available for mobile numbers with ISD code +91. This means that users with mobile numbers registered in India can receive a one-time password via SMS for authentication purposes.

1. Login to the MSSP portal using your regular username (email) and password.



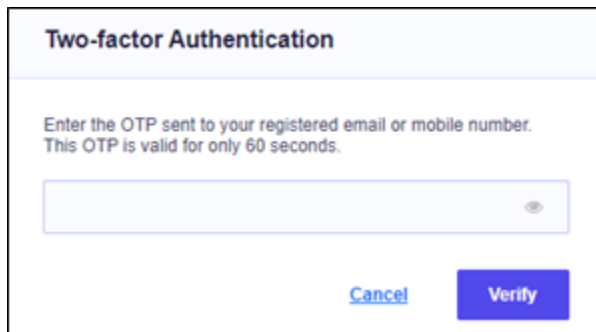
The screenshot shows a 'Sign in' form with the following elements:

- Title: **Sign in**
- Instruction: **Sign into your Seqrite account**
- Input field: **Email ID**
- Input field: **Password** (with an eye icon for visibility toggle)
- Link: [Forgot Password?](#)
- Button: **Sign in**

2. The Two-factor Authentication screen appears.

Note:

If 2FA authentication is not enabled, then the 2FA Authentication screen does not appear and you are automatically logged in to the MSSP portal.



The screenshot shows a 'Two-factor Authentication' screen with the following elements:

- Title: **Two-factor Authentication**
- Instruction: **Enter the OTP sent to your registered email or mobile number. This OTP is valid for only 60 seconds.**
- Input field: (with an eye icon for visibility toggle)
- Buttons: [Cancel](#) and **Verify**

3. Enter the OTP sent to your registered email or mobile number. This OTP is valid for only 60 seconds.
4. Click **Verify**.

You will be logged in to the MSSP portal.

Note:

2FA is enabled for Super admin role for all new tenants by default. When Super admin creates any user, he can enable 2FA for that user. Users will be notified by an email when Super admin enables or disables 2FA for any user.

Enabling or disabling a user

To enable or disable a user, follow these steps.

1. Log on to Seqrite 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.

Enabling 2FA for Users (Bulk 2FA Authentication)

1. Log on to Seqrite MSSP with your credentials.
2. Under the Manage list, click the Users menu.
A user list appears.
3. Select the users for whom you want to enable 2FA.
An action list titled **Please Select** is displayed.
4. From the **Please Select** drop down list, click **Enable 2FA**.
5. **Email OTP** is selected by default. Select **SMS OTP**.
6. Click **Submit**.
7. Click **Confirm** for the selected users.
A Success prompt is displayed.

Note:

- SMS authentication will be enabled for users with verified mobile numbers only.
- Users can verify their registered mobile number through the “Edit Profile” section.

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.

3. Log on to Seqrite MSSP with your credentials.
4. Click the **Users** menu.

The Users list appears.

5. Select a user.

An action list titled Please Select is added.

6. 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.

7. Click **OK**.

The resend activation link is sent successfully.

Editing a user

To edit a user information, follow these steps.

1. Log on to Seqrite 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. Select the Enable Two Factor Authentication (2FA) check box if required. By default, the Email-based OTP option is enabled for the user, select the SMS-based OTP if required. If the SMS-based OTP option is enabled for the user then that user will get the OTP on the email address as well as on the user's registered mobile number. Before that, the user needs to verify the mobile number from Edit Profile Section.

Note:

- Only the Super Administrator can Enable/Disable 2FA for users.
- When the Super Administrator enables 2FA for users, the users receive an email notification. Subsequently, every time the user logs in, they are required to provide an OTP that is sent to their registered mobile device or email address in order to access the MSSP portal.

6. Click **Update**.

The details are updated successfully.

Deleting a user

To delete a user, follow these steps.

1. Log on to Seqrite 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.

Seqrite MSSP provides system defined policies 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 Seqrite MSSP with your credentials.
2. Under the Policies list, click the **Computer** menu.
A Policies 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 Seqrite MSSP with your credentials.
2. Under the Policies list, click the **Computer** menu.
A Policies 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 Seqrite MSSP with your credentials.
2. Under the Policies list, click the **Computer** menu.

A Policies 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 Seqrite MSSP with your credentials.
2. Click the circular icon available on the upper-right corner.

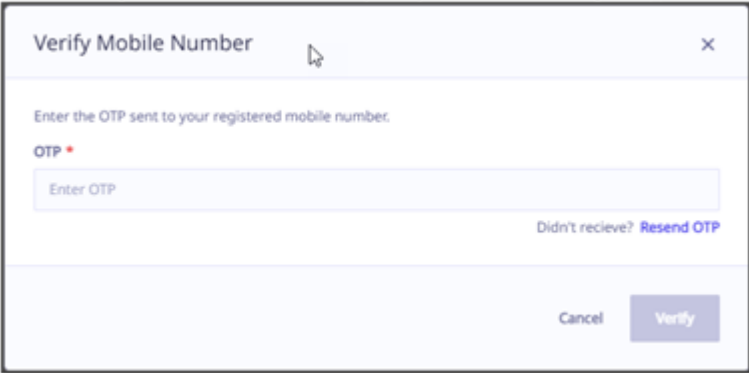
The Edit Profile page appears.

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

Note:

- At present, SMS-based OTP authentication is available for mobile numbers with ISD code +91. This means that users with mobile numbers registered in India can receive a one-time password via SMS for authentication purposes.

3. Verify the mobile number.
 - a. Navigate to Point of Contact Details tab, click **Verify**. Verify Mobile Number dialog box is displayed.



- b. Enter the OTP sent to your registered mobile number and click **Verify**.
 - If OTP is correct, confirmation message “Your mobile number has been successfully verified” is displayed and Verified status is shown against number.
 - If OTP is incorrect, you need to enter the correct OTP. Three incorrect attempts are allowed within 60 seconds.
 - If you haven’t received the OTP, click Resend OTP.

Note:

Follow the above procedure to verify mobile number if you change your mobile number anytime.

4. Click **Save**.

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.
 - EPS Virus infection detected at any site
 - EPS Virus Outbreak detected at any site

Note: These options may not appear in Seqrite Endpoint Protection.

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.

8. Admin

In this section, you can configure when the reports should be deleted automatically. As an administrator, you may generate hundreds of reports. Such reports keep on adding in the system. It is advisable that you should remove the old reports that you may not require.

Settings

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

Deleting Reports

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

1. Log on to Seqrite 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.

9. Activity Logs

The activity log contains the details for all the user activities that are carried out on the Seqrite MSSP console.

Some of the activity logs are as follows.

- A user logs in or logs out.
- A new site is added to a site type in Seqrite MSSP.
- A site is edited.
- A new policy is added to a site.
- A policy is applied to a site.
- A site with a policy is edited.
- A site with 2FA is added.
- A site with 2FA is edited.
- Failed sites are retried.
- Failed product is retried.
- Web console is accessed.
- A policy is updated.
- The license is synced to update the license information.
- The primary email address is changed.

Observing the Activity Logs

To observe the activity logs, follow these steps.

1. Log on to Seqrite MSSP with your credentials.
2. On the left panel, click the **Activity Log** menu.

All the activities are displayed.

You can modify your search criteria by changing the number of days for which the activity logs are required and the IP address.

10. License Telemetry

License Telemetry gives you a way to generate reports on the journey of subscription of the licenses for the Seqrite Endpoint Protection, Seqrite Centralized Security Management, Seqrite ZTNA, Seqrite Data Privacy, Seqrite XDR and Seqrite Enterprise Mobility Management products. You can observe how many trial licenses are active, how many of the trial licenses have been converted to commercial ones, how many licenses have expired, and how many licenses are due for renewal.

This data helps the Seqrite MSSP partners to plan how to pursue the potential buyers to buy the licenses.

Generating the License Telemetry

To generate license telemetry, follow these steps.

1. Log on to Seqrite MSSP with your credentials.
2. On the left panel, click the **License Telemetry** menu.
3. On the License Telemetry screen, select any of the following parameters.
 - Customer Segment
 - Customer Industry/Vertical
 - User Sizing
 - Annual Revenue in USD
 - Annual IT Budget in USD
 - Annual IT Security Budget in USD
 - Product
 - Period
 - Country
4. Click **Generate Report**.

The report is generated. You can observe the license metrics.

11. Technical Support

Seqrite MSSP provides extensive technical support for the registered users. It is recommended that you have all the necessary details with you during the call to receive efficient support from the support executives of Seqrite.

The Support option offers email support, live chat support, and contacts to seek support on calls.

To get the contact details, follow these steps.

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

A support page appears.

The Support page includes the following options:

FAQ: Includes frequently asked questions. If you have a query, please check our FAQ once. It is most possible that you may find your query answered in FAQ.

Live Chat support: Interact via chat with one of our experts to get a solution to your issues.

Contact Us: You can call us on our support numbers. Select your country and dial the corresponding number. The toll free numbers for India are listed along with the timings.

Raise Ticket: If you have an issue and you want us to resolve it, you can raise a ticket.

Email Support: Write to us at support@seqrite.com with your query and we will get back to you with a solution.

Localization Support

As part of our endeavor to extend support in multiple ways, we make Seqrite MSSP available in various languages.

Seqrite MSSP is supported in the following languages.

- English
- Japanese
- Korea

Head Office

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.segrite.com>.

Email: support@segrite.com

Other support contact

To know more support contacts, please visit:

<http://www.segrite.com/segrite-support-center>