

How to Configure Email Settings



Introduction

Configure Email Settings to get the Alerts and to export the different reports like Executive, Device, Asset, vulnerabilities, Compliance, patch, Threat indicator, CMD & Ctrl reports.

Steps to Configure Email Setting

Steps to configure email settings:

1. Login in to the viser through any latest browser.
2. Click **User info** (Account user) in the top right corner.
3. In Mail Settings, click **update**.

The screenshot shows the Viser dashboard for a user named 'supadmin'. At the top, there are four summary cards: Total Devices (5), Active Devices (3), Windows (4), and Linux (1). Below these are four columns: Account, Vulnerability, Compliance, and Threat Indicators. The Account column shows two teams: Finance Team and IT Team. The Vulnerability column shows a list of vulnerabilities with severity levels (Critical, High, Medium, Low). The Compliance column shows a list of compliance items (Compliant, Non-Compliant, Not scanned). The Threat Indicators column shows a list of threat indicators with severity levels (Critical, High, Medium, Low). On the right side, there is a user profile dropdown menu with the following settings: Name (supadmin), Organization (secpod), License Expiry (2020-12-31), Email ID (redacted@secpod.com), Two-Factor Authentication (Turn on), Password (Reset), Logo (Update), and Mail Settings (Update). A Sign out button is also visible at the bottom right of the menu.

4. In Update Account Mail Settings mention all details,

SMTP Host: Type the SMTP Host server belongs to using username of an Email account.

(Example if, xxx@gmail SMTP Host like smtp.gmail.com)

SMTP Port: Mention a port next to entered SMTP Host text box.

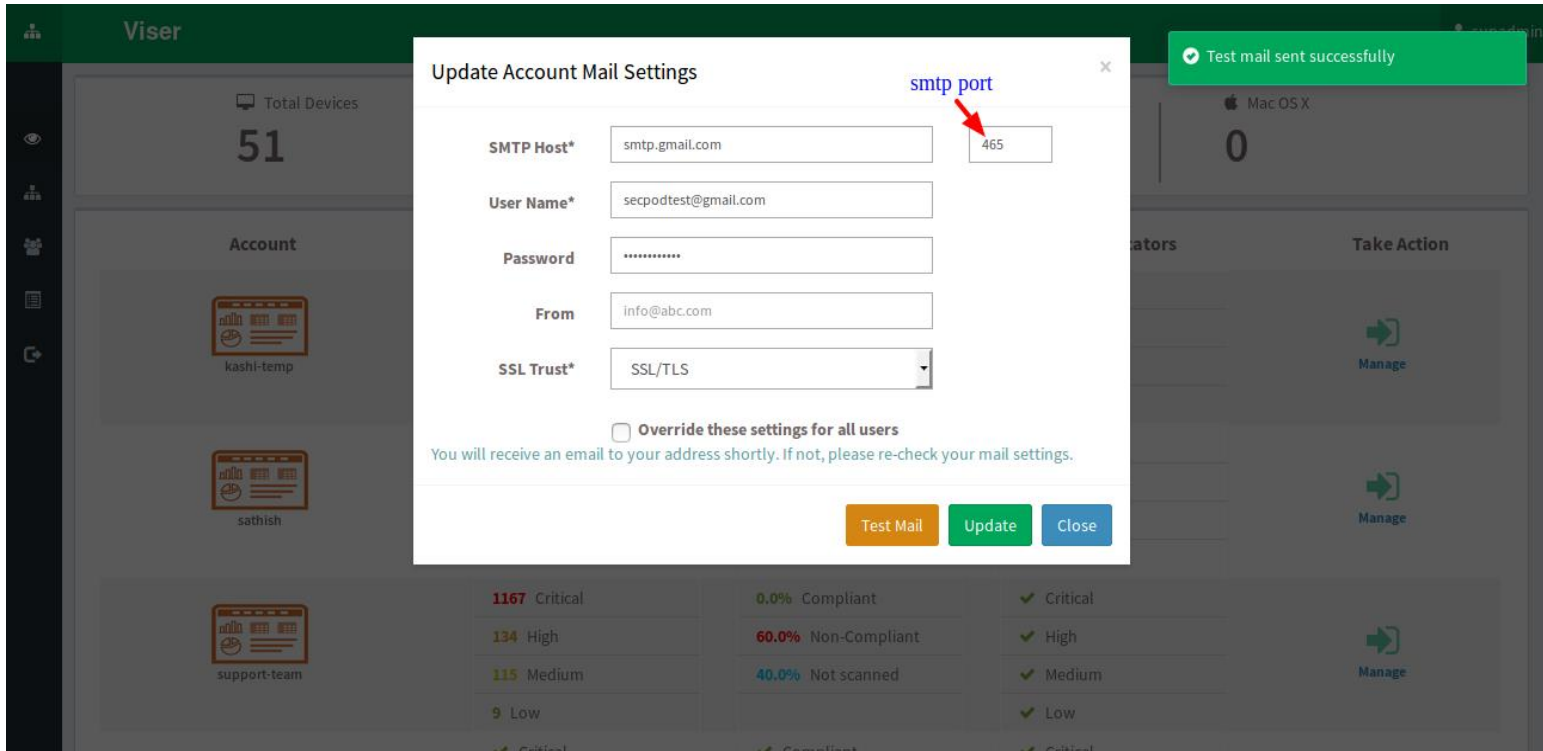
- SSL/TLS port is 465.
- STARTTLS port is 587
- None port is 25.

Username: Enter a username in the format of Email Address ex: abc@gmail.com

Password: Current password to the mentioned Email address.

SSL Trust: Select SSL Trust mode connection with the options,

- SSL/TLS port is 465.
- STARTTLS port is 587
- None port is 25.



5. If you want to override these settings for all users in your account **enable** on the menu box.
6. Click on **Test Mail** button, if mail sent successfully, it will pop up window and show a message.
7. Click **Update** to apply changes in Email setting.

Setup Alerts through Mail

To setup an alert to the mail settings:

1. Login in to the Viser.
2. Open the **Manage** page of an Account, Click on **Alert** in the right corner plane.

The screenshot shows the 'Alerts' management page. It features a table with columns for 'Alert Type', 'Description', 'Last sent', and 'Subscribe'. Below the table is a 'Vulnerability Alerts Configuration' section with input fields for 'Send to E-mail*' and 'Conditions*', and an 'Update' button.

Alert Type	Description	Last sent	Subscribe
Vulnerability	Notifications for vulnerabilities based on their criticality.	No information available	<input checked="" type="checkbox"/> ON
Compliance	Notifications for deviations based on the compliance benchmark.	No information available	<input type="checkbox"/> OFF
Threats	Notifications for threat indicators or indicators of compromise detected based on their criticality.	No information available	<input type="checkbox"/> OFF
Queries	Notifications for custom queries created.	No information available	<input type="checkbox"/> OFF

Vulnerability Alerts Configuration

Send to E-mail*

Conditions*

3. Subscribe to Enable the **Alert Type** with Vulnerability, compliance, threats, and query with the conditions.
4. In the **Send to E-mail** box, enter receiver email address and with multiple email separated by commas.
5. Use **Conditions** drop down box, Select the conditions to be based on the alert type.
6. Click **Update**. Alerts will be set, and receiver side gets alert in email message format.

Generating Report and Sending through Email

Generate Reports in different ways to download and send to in mail to multiple accounts.

1. Log in to the viser.
2. Open the **Manage** page of an Accounts.
3. Click **Reports** in the left plane. Report Section will show multiple options in the report.

Reports

- Executive Report
- Device Report
- Asset Report
- Vulnerability Report
- Compliance Report
- Patch Report
- Threat Indicator Report
- CMD & Ctrl Report

Export Backup

Executive Report

Generated for support-team on Fri, 10 Nov 2017 14:47:02 GMT

1. Risk Posture at a Glance

Consolidated risk posture covering vulnerabilities, mis-configurations and threat indicators.
This report provides a summary of monitored devices, vulnerability risk, configuration compliance and threat indicators.

1.1 Currently Monitored Devices

Total number of devices monitored and device family.

5	3	4	1	0
Total Devices	Active Devices	Windows	Linux	Mac OS X

4. Click **backup** button in the left corner. Automatic Backup Settings will open.
5. Select often in **Daily/weekly backup** and Specify number of latest backup reports will be kept with the server.
6. Enter the Receiver Email address and add multiple Emails separated by with commas.
7. Select **Backup time** needed to take reports and sending through emails. So, if daily wise report, click **save**.
8. For weekly report, choose **days of the week** that you need a report. Then, click **save**

Automatic Backup Settings ✕

How often Weekly

Days of the week Monday

Keep only the latest 7 backups (delete older ones)

E-mail [redacted]@sepod.com, [redacted]@secpod.co

Backup Time: 7:00

Save
Close

9. If user wants to download Instant report. Back to Home in **Report page**, click on **export**.

Select **PDF** to download. The File will get downloaded on the local machine.

The screenshot shows the SecPod Viser interface. The browser address bar displays `https://192.168.2.91/control.jsp?command=reports`. The page title is "Vulnerability Report". On the left sidebar, the "Vulnerability Report" option is highlighted. The main content area features a section titled "1. Vulnerabilities at a Glance" with a sub-section "1.1 Vulnerability Distributions by Severity". Below this is a pie chart. To the right of the pie chart, there are two columns: "1.2 Impacted Hosts" (Number of vulnerable devices) and "1.3 Impacted Assets" (Number of vulnerable assets). An "Export" button is visible in the top right corner, with a dropdown menu showing options for "PDF", "Email", and "Backed up Reports".

10. Select **Export** type as Email and email address or multiple email separated by commas. Click to **send**.

The screenshot shows the "Email Report" dialog box. It has a title bar with "Email Report" and a close button (X). Below the title bar, there is a section labeled "Email address" with a text input field containing two email addresses: `██████████@secpod.com, ██████████@secpod.com`. Below the input field, there is a note: "Add multiple email addresses separated by comma". At the bottom right, there are two buttons: a green "Send" button with a checkmark icon and a grey "Cancel" button with an X icon.



About Us

SecPod Technologies creates cutting edge products to ensure endpoint security. SecPod's deep information security expertise exceptionally positions the company to help solve complex endpoint security challenges. Headquartered in Bangalore with operations in USA, SecPod's products are deployed across diversified verticals.

Contact Us

Web Tel: +91-80-4121 4020

Email: info@secpod.com +1-918-625-3023