Alerts and Mail Configurations

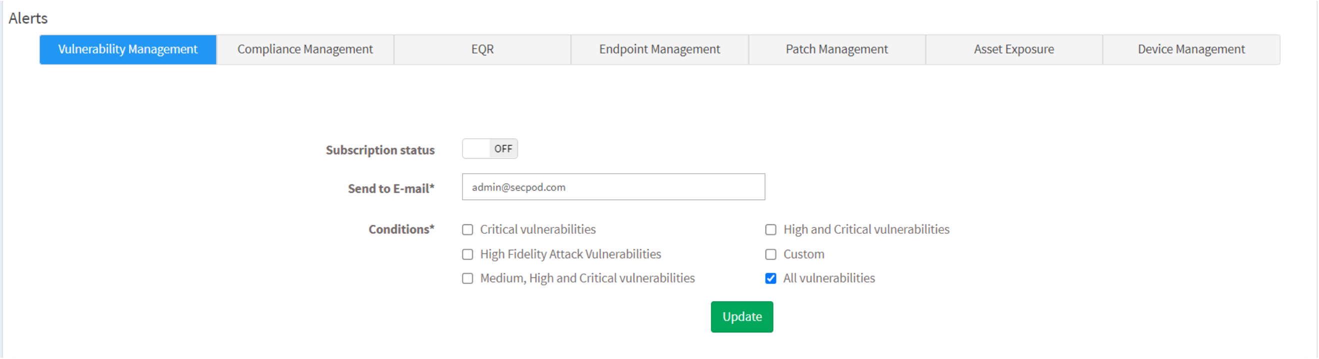
Alerts

Alerts keep an administrator informed about new vulnerabilities, misconfigurations, and any new non-compliance in the Saner agent-installed machines. The existing vulnerabilities will not be displayed if alerts are configured after the agent is deployed.

To Set Alerts

1. Select the **Alerts** option on the left pane of the visibility dashboard. The Alerts page shows different types of alerts (Vulnerability Management, Compliance Management, EQR, Endpoint Management, Patch Management, Asset Exposure, and Device Management) and the option to subscribe to an alert, as well as the individual settings for each alert type.
2. Turn on the **Subscription Status** for the alert type to receive status.
3. Specify an email ID to which the corresponding alerts must be sent in the **Send to an E-mail** box. Users can enter multiple email addresses separated by commas.
4. Select the Conditions option to receive alerts. Each alter type has different conditions.
5. Click on the **Update** button to set the alerts.

Note: For alerts to work successfully, configure a mail server as described in the ***Error! Reference source not found.*** *section.*



Subscription status: OFF

Send to E-mail*: admin@secpod.com

Conditions*:
□ Critical vulnerabilities
□ High Fidelity Attack Vulnerabilities
□ Medium, High and Critical vulnerabilities
□ High and Critical vulnerabilities
□ Custom
☑ All vulnerabilities

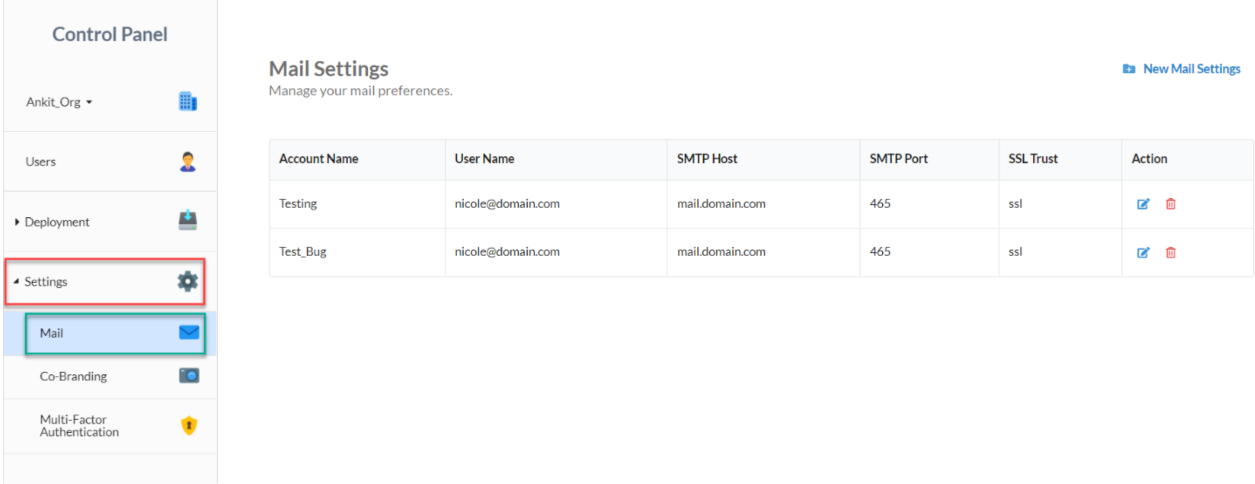
Alerts will be sent to the specified email IDs. Individual page settings for each alert type are explained under the respective tool's section.

Configuring Mail Settings

The Mail Settings allow users to send alerts related to a vulnerability, non-compliance, threats and malware, critical patches or necessary updates, new assets, new devices, and the failure and success of queries and actions related to these and send reports. The mail server should be set before deploying the agent on the network. Users can configure a public or local mail server.

To configure mail server settings, complete the following steps:

1. Click the **Control panel** icon on the top right corner of the visibility dashboard.
2. Select an organization or an account to configure mail settings from the Control Panel page.
3. Click on the **Mail** option under the **Settings** section, the **Mail Settings** page will

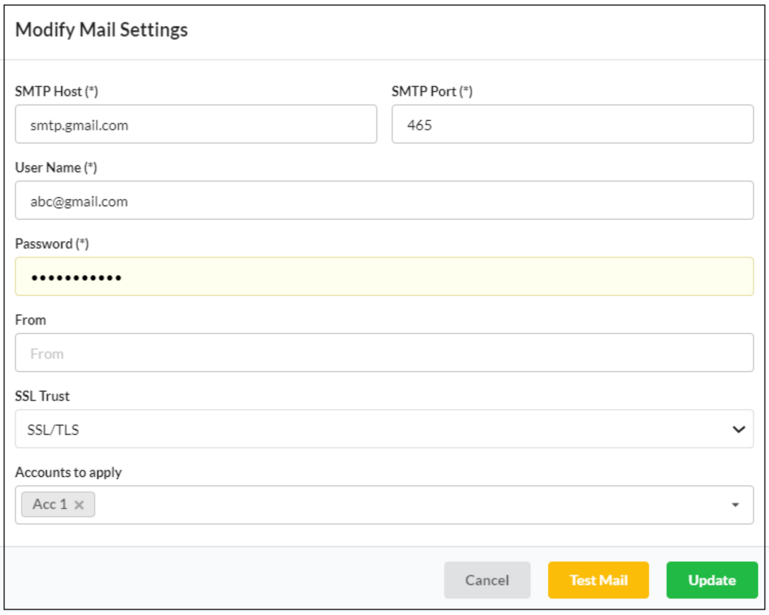


Mail Settings
Manage your mail preferences.

Account Name	User Name	SMTP Host	SMTP Port	SSL Trust	Action
Testing	nicole@domain.com	mail.domain.com	465	ssl	
Test_Bug	nicole@domain.com	mail.domain.com	465	ssl	

appear, as shown in

4. Click on the **New Mail Settings** at the top right corner.



Modify Mail Settings

SMTP Host (*): smtp.gmail.com
SMTP Port (*): 465
User Name (*): abc@gmail.com
Password (*): •••••••••••
From: From
SSL Trust: SSL/TLS
Accounts to apply: Acc 1 ×

5. Specify the **SMTP Host**, for example, smtp.gmail.com. The hosts supported for SMTP are 25, 465, 587. In this case, the supported port for Gmail is 465.
6. Enter the email ID (from which the mail will be sent) and the password in the **Username** and **Password** text fields, respectively.
7. Enter the **From** email address that will be displayed to the receiver. This is optional.
8. Specify an authentication type in the SSL Trust drop-down:
    - Select None if you do not want to set any security protocol.
    - Select **STARTTLS** or **SSL/TLS** to set a security protocol.
9. Click on the **Update** button.
10. Click on the **Test Mail** button to test the configuration, which will send a test mail to the respective email id.

Modify Mail Settings:

11. From the **Mail Settings** table, click the **Edit** icon in the Action column to modify mail settings.
12. Update the necessary changes and click **Update**.

Delete Mail Settings:

13. From the **Mail Settings** table, click the **Delete** icon in the Action column to delete mail settings.