**A green and yellow logo

Description automatically generated**

**ISS Technologies**

**Document Name: Configuring Wazuh for Email Alerts via SMTP Server**

**Version No: 1.0**

**Created by: Tarun Samanta**

**Reviewed & Approved by: Sasidhar.**

**Version Control:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Version** | **Description of change** | **Prepared by** | **Reviewed and Approved by** |
| **30/08/2025** | **1.0** | **Original – created** | **Tarun Samanta** | **Sasidhar B** |

Table of Contents

[Configuring Wazuh for Email Alerts via SMTP Server 2](#_Toc210151102)

[Overview 2](#_Toc210151103)

[Instructions 2](#_Toc210151104)

[Conclusion 5](#_Toc210151105)

# Configuring Wazuh for Email Alerts via SMTP Server

## Overview

This document outlines the process of configuring Wazuh, an open-source security monitoring platform, to send email alerts through an SMTP server. It provides step-by-step guidance on setting up an SMTP server and integrating it with Wazuh to enable automated email notifications for security events and alerts. The document highlights key configuration steps, including defining SMTP server settings, authenticating credentials, and specifying email recipients within Wazuh’s configuration files. By following these instructions, users can ensure timely and reliable delivery of critical security alerts to designated email addresses, enhancing incident response and monitoring capabilities.

## Instructions

1. Install Postfix:

sudo apt install postfix ca-certificates libsasl2-modules

* + During installation, choose Internet Site if prompted

1. Configure Postfix to Use outlook SMTP:
   * Edit the Postfix configuration file /etc/postfix/main.cf:

sudo nano /etc/postfix/main.cf

* + Add the following lines:

relayhost = [smtp-mail.outlook.com]:587

smtp\_sasl\_auth\_enable = yes

smtp\_sasl\_password\_maps = hash:/etc/postfix/sasl\_passwd

smtp\_sasl\_security\_options = noanonymous

smtp\_tls\_security\_level = may

smtp\_tls\_CAfile = /etc/ssl/certs/ca-certificates.crt

* + Create a password file for outlook credentials:

sudo nano /etc/postfix/sasl\_passwd

Add:

[smtp-mail.outlook.com]:587 yourmail@domain.com:password

* + - Replace yourmail@domain.com with your Gmail address.
  + Secure and process the password file:

sudo postmap /etc/postfix/sasl\_passwd

sudo chown root:root /etc/postfix/sasl\_passwd /etc/postfix/sasl\_passwd.db

sudo chmod 600 /etc/postfix/sasl\_passwd /etc/postfix/sasl\_passwd.db

1. Restart Postfix:

sudo systemctl restart postfix

1. Configure Wazuh to Send Email Alerts
   * Now that Postfix is set up to relay emails through Gmail, configure Wazuh to use the system’s mail system.
   * Edit Wazuh Configuration File:

Sudo nano /**var**/ossec/etc/ossec.conf:

* + Add or modify the <global> section to enable email notifications:

**<ossec\_config>**

**<global>**

**<email\_notification>**yes**</email\_notification>**

**<smtp\_server>**localhost**</smtp\_server>**

**<email\_from>**yourmail@yourdomain.com**</email\_from>**

**<email\_to>**recipient@yourdomain.com**</email\_to>**

**<email\_maxperhour>**12**</email\_maxperhour>**

**</global>**

**</ossec\_config>**

* + - Set smtp\_server to localhost because Postfix is running locally.
    - Replace recipient@yourdomain.com with the recipient’s email address.

1. Set Alert Level:
   * In the same ossec.conf, configure the minimum alert level for emails:

**<ossec\_config>**

**<alerts>**

**<email\_alert\_level>**12**</email\_alert\_level>**

**</alerts>**

**</ossec\_config>**

* + Restart Wazuh Manager:

sudo systemctl restart wazuh-manager

1. Test the setup

* Add the option to alert by mail in rules which you want to be notified for example we will send email alert when the mimikatz process is detected.

**<group** name="windows,mimikatz,"**>**

**<rule** id="110601" level="12"**>**

**<if\_sid>**100000**</if\_sid>** <!-- Process creation (4688) -->

**<field** name="win.eventdata.newProcessName"**>**mimikatz.exe**</field>**

**<options>**alert\_by\_email**</options>**

**<description>**Mimikatz process creation detected**</description>**

**</rule>**

**</group>**

* run the mimikatz process.

A computer screen shot of a black screen

AI-generated content may be incorrect.

* You should get mail in you recipient mailbox.

A screenshot of a computer

AI-generated content may be incorrect.

## Conclusion

users can streamline their incident response process and maintain visibility into security events. This setup ensures that stakeholders receive real-time alerts, enabling rapid action to mitigate risks. Proper testing and validation of the configuration are essential to guarantee reliable email delivery and optimal performance of the alerting system.