Configure Alerts in Email Security Appliance

Contents

Introduction

This document describes how to enable alerts in the Cisco Email Security Appliance.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

One of the key features of the Cisco Email Security Appliance is the ability to send alerts when certain events occur. These alerts can help administrators quickly identify and respond to potential security threats.

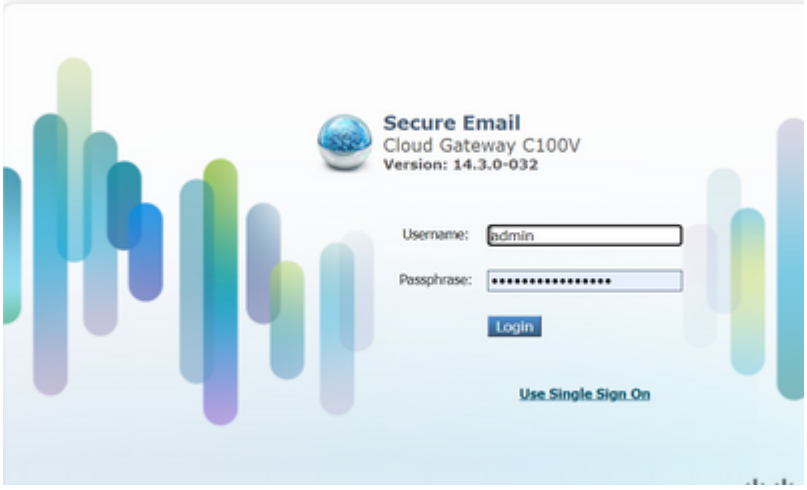
Before you begin, it is important to understand the different types of alerts that the Cisco Email Security Appliance can generate. The alerts that can be configured to notify administrators when features, system, hardware or software events occur are:

- Critical: Critical alerts require immediate attention.
- Warning: Warning alerts indicate a problem or error which requires attention.
- Informational: Informational alerts are generated in the routine functioning of this device.

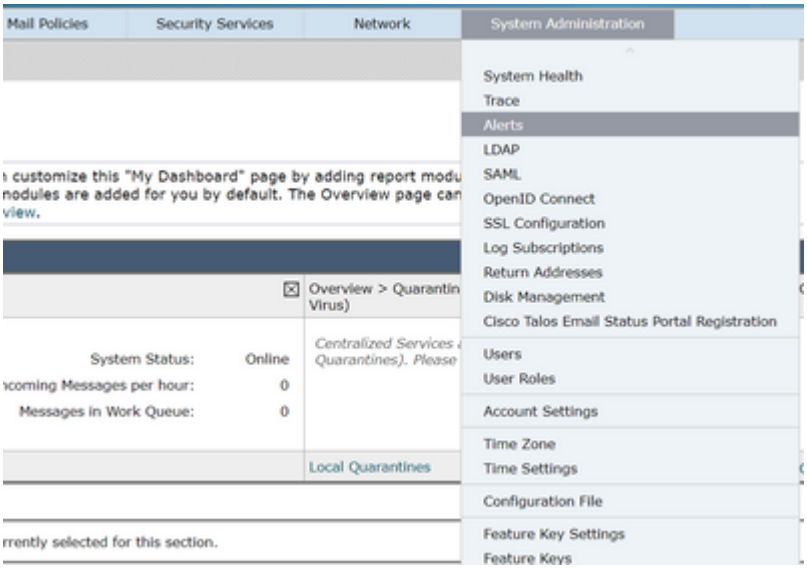
Procedure

In order to enable alerts in the Cisco Email Security Appliance, use these steps:

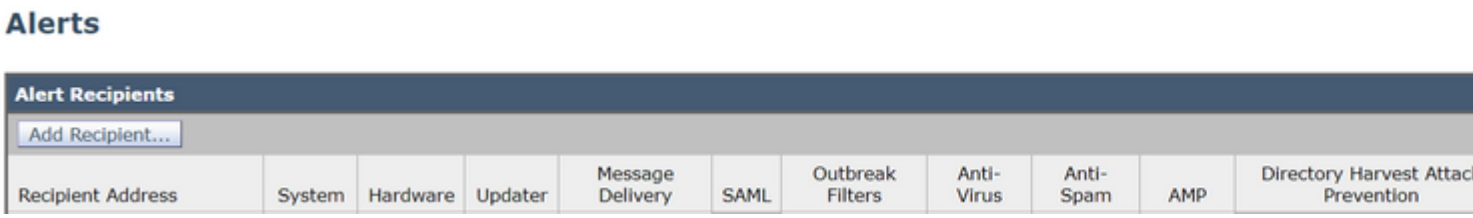
1. Log in to the Cisco Email Security Appliance with administrator credentials.



2 .Click **Alerts** under **System Administration** tab.



3. Click **Add Recipient**.



4. Enter the email address for the recipient of the alerts.

Caution: Support addresses (TAC@cisco.com, support@cisco.com) are not allowed. If you require assistance, please contact Technical Support.

5. Choose the Alert type and severity.

Alert Type	Alert Severities to Receive: All	Critical	Warning
System	☐	☐	☐
Hardware	☐	☐	☐
Updater	☐	☐	☐
Message Delivery	☐	☐	☐
SAML	☐	☐	☐
Outbreak Filters	☐	☐	☐
Anti-Virus	☐	☐	☐
Anti-Spam	☐	☐	☐
AMP	☐	☐	☐
Directory Harvest Attack Prevention	☐	☐	☐
Threatfeeds	☐	☐	☐

6. Click **Submit**.

7. Modify the From address of the alerts if desired in the **Edit Settings** option.

Alert Settings	
From Address to Use When Sending Alerts:	alert@ces.cisco.com
Initial Number of Seconds to Wait Before Sending a Duplicate Alert:	300
Maximum Number of Seconds to Wait Before Sending a Duplicate Alert:	3600

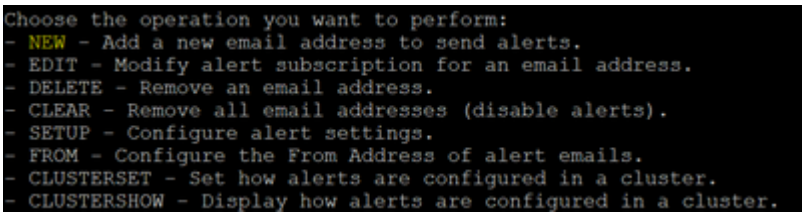
8. click **Commit Changes** to save the settings.

CLI Procedure:

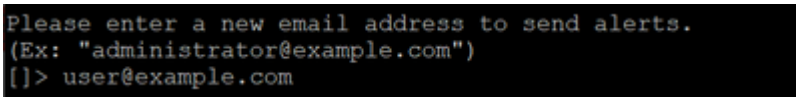
1. Login to the device with an administrator account.

2. Enter the command **alertconfig**.

3. Choose **NEW** from the displayed menu.

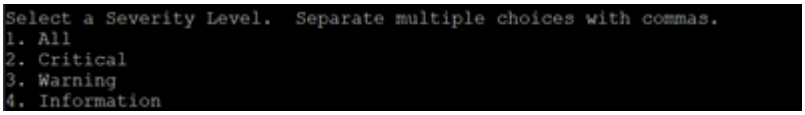


4. Add the email address that is to be used as recipient for the alerts.

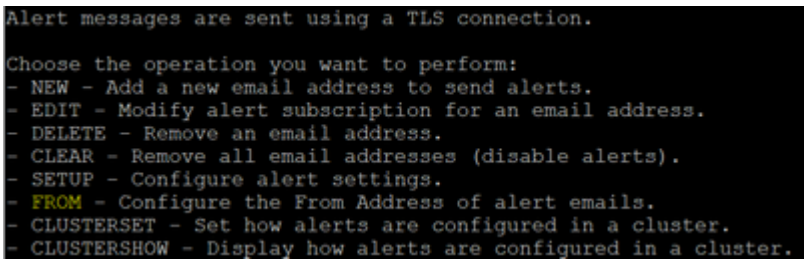


5. Choose the alert type from the list.

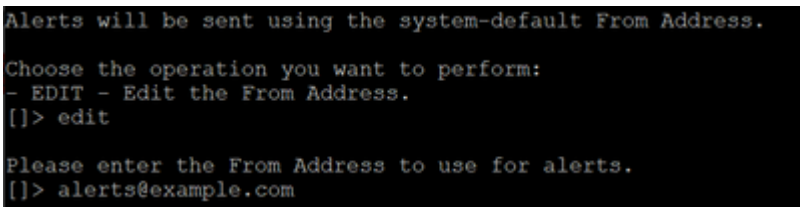
6. Choose the severity level from the list.



7. If a special From address is to be used as the sender for the alerts select **FROM** in the **alertconfig** main menu.



8. Choose **EDIT** from the menu and enter the from address to be used as the sender for the alerts.



Conclusion

Alerts in the Cisco Email Security Appliance are a simple but powerful way to proactively monitor your email traffic and respond quickly to potential security threats.

Note: This procedure is not available in cloud hosted appliances, please refer to the official document for Cloud Administrator Role Limitations.

Related Information

- **Cisco Technical Support & Downloads**