Configure Email Settings and Customize Email Notifications on FindIT Network Probe

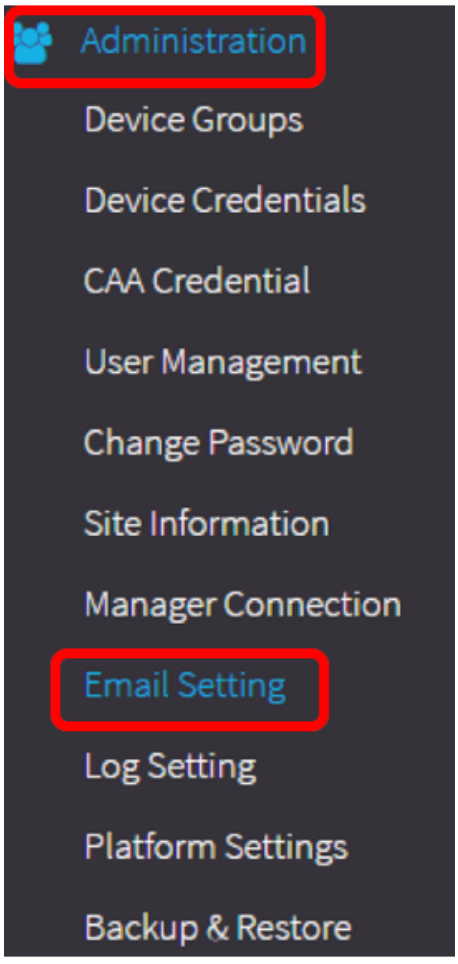
Objective

Cisco FindIT Network Probe equips a network administrator with indispensable tools that help securely monitor and manage Cisco devices from a web browser. The FindIT Network Probe can be configured to generate email notifications to inform you about selected network events containing device and Cisco Support notifications such as changes in network settings, new firmware available, device status, and other updates on devices connected to the network.

This document aims to show you how to configure the email settings and regulate email notifications caused by network events on the FindIT Network Probe.

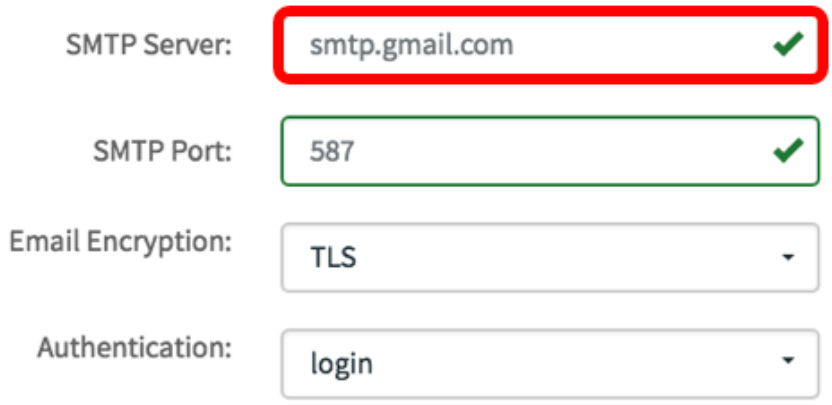
Configure Email Setting

Step 1. Log in to the FindIT Network Probe Administration GUI and choose **Administration > Email Setting**.



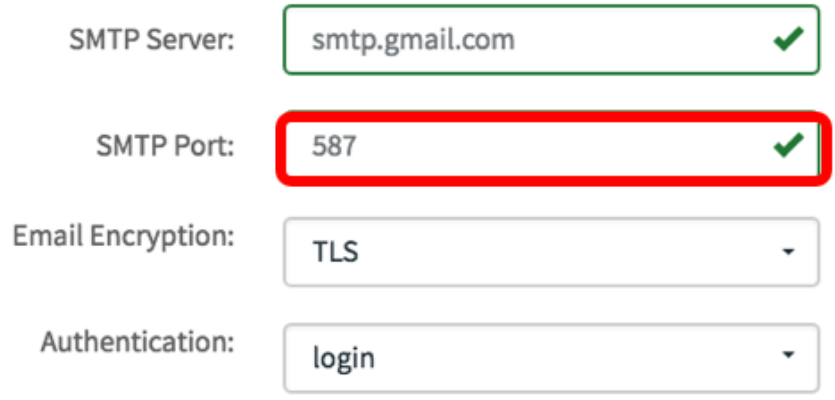
Step 2. In the *SMTP Server* field, enter the valid hostname of the mail server.

Note: For this example, smtp.gmail.com is used.



Step 3. Enter the port number of the mail server in the *SMTP* Port field. It is an outbound port number used to send emails. The valid port number range is from 0 to 65535 and the default value is 465 for Simple Mail Transfer Protocol (SMTP).

Note: For this example, SMTP port number 587 is used.

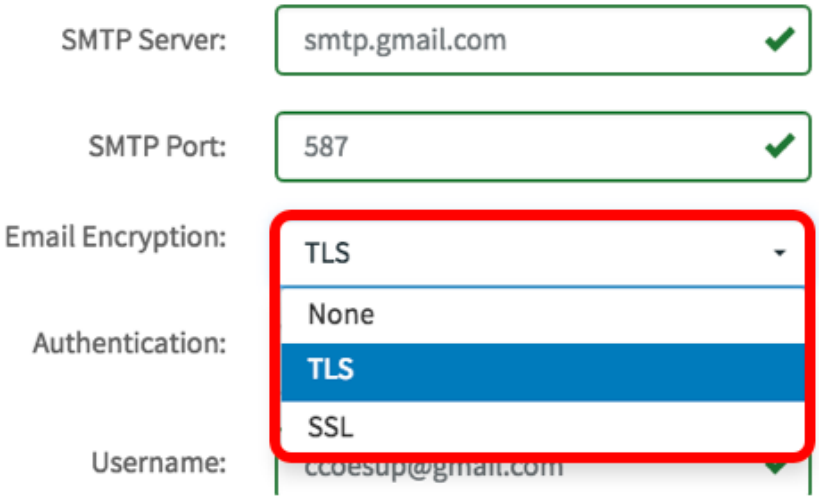


Step 4. From the Email Encryption drop-down list, select an encryption method to send messages to your email. It is important that the encryption method also matches the SMTP port.

The options are:

- None — No encryption will be used in the emails.
- TLS — Transport Layer Security (TLS) is a cryptographic protocol that provides security and data integrity for communication over the Internet. This encryption uses SMTP Port 587.
- SSL — Secure Sockets Layer (SSL) is a standard security technology for creating an encrypted link between a web server and a browser. This encryption uses SMTP port 465.

Note: For this example, TLS is used.

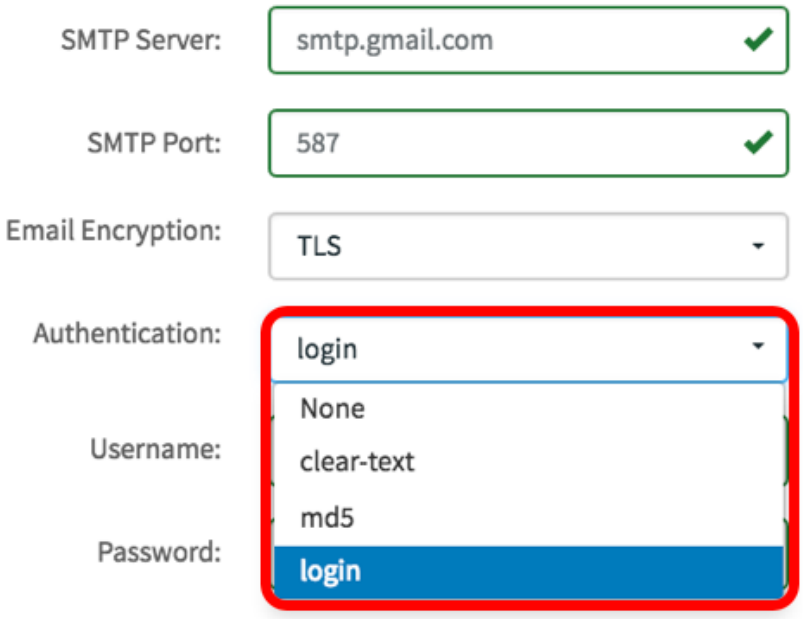


Step 5. From the Authentication drop-down list, choose how you want to authenticate the access to your email.

The options are:

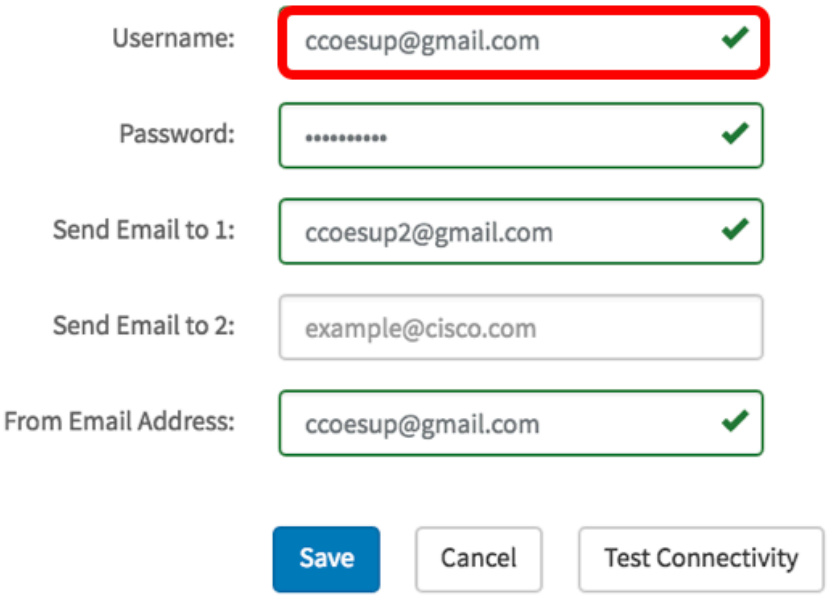
- None — No authentication that requires Username and Password.
- clear-text — Unencrypted; still requires Username and Password.
- md5 — Message-Digest Algorithm 5 uses a 128-bit hash value for authentication that requires Username and Password.
- login — Username and password are used for authentication.

Note: For this example, login is used.



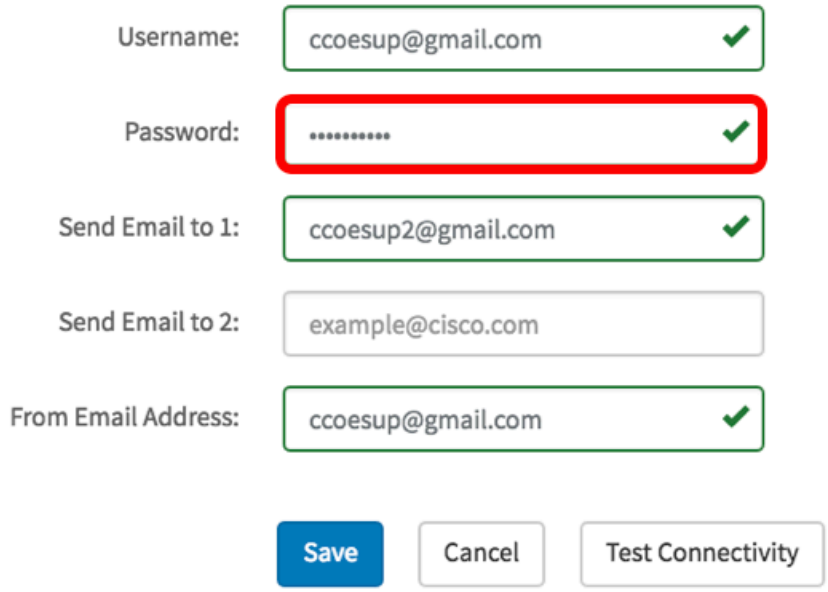
Step 6. (Optional) If clear-text, md5, or login was chosen in Step 5, enter a Username in the *Username* field. This would be the sending email address.

Note: In this example, ccoesup@gmail.com is used.



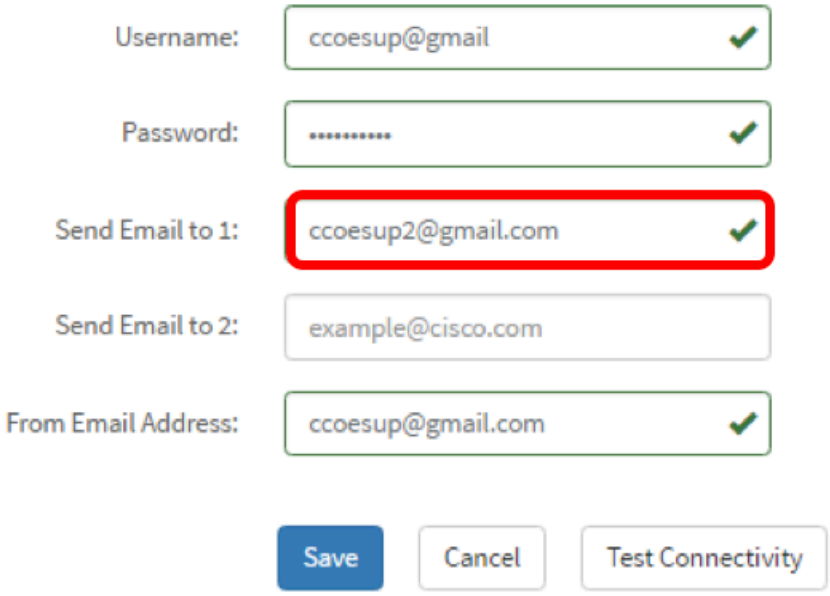
Step 7. (Optional) Enter your password in the *Password* field for the Username configured above.

Note: It is highly recommended to use a separate email account instead of using your personal email to maintain privacy.

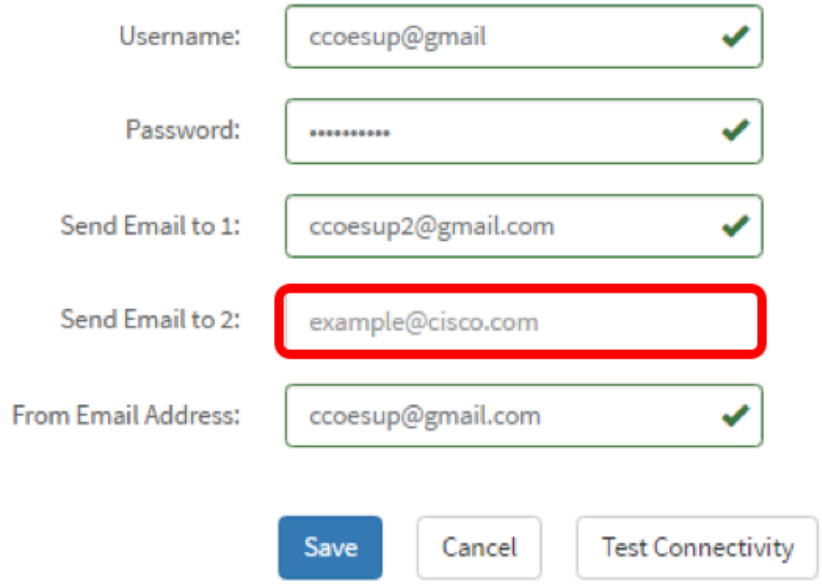


Step 8. Enter an email address in the *Send Email to 1* field. The address is the recipient of the network updates.

Note: It is highly recommended to use a separate email account instead of using your personal email to maintain privacy. In this example, ccoesup2@gmail.com is used as an example.

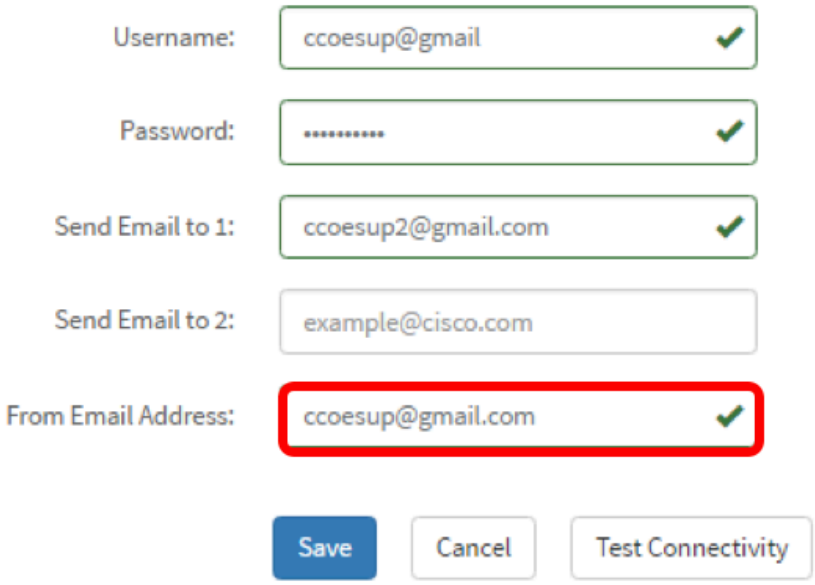


Step 9. (Optional) Enter a secondary email address in the *Send Email to 2* field.

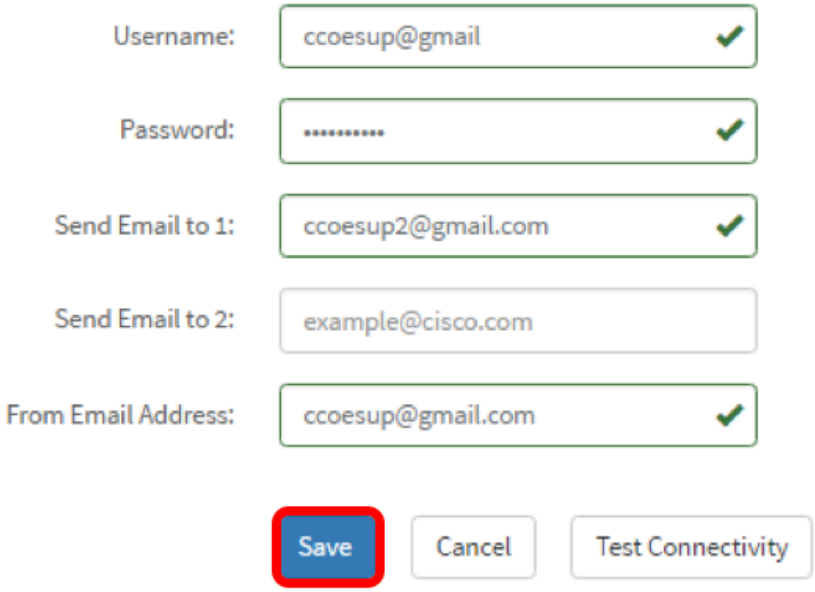


Step 10. Enter the authenticated email address used in the Username and Password fields in Step 6 as the sending email address in the *From Email Address* field.

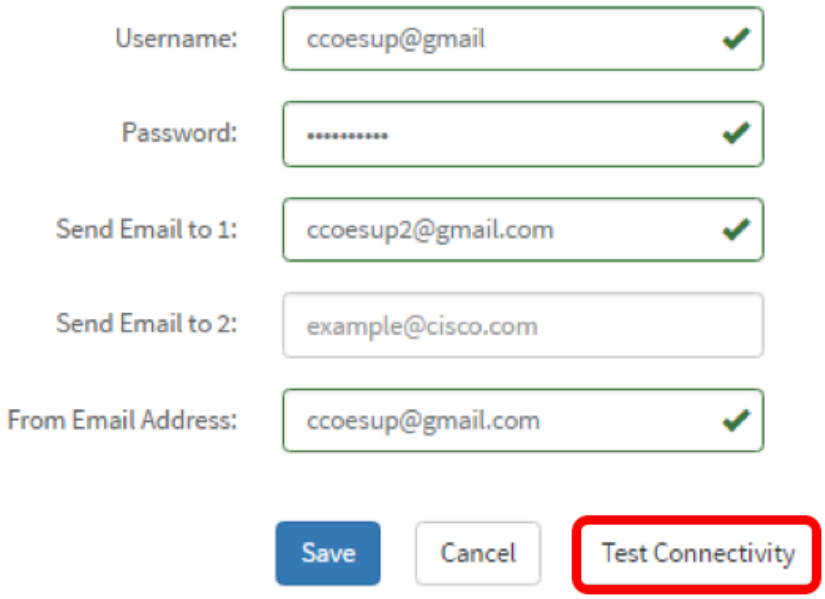
Note: In this example, ccoesup@gmail.com is used.



Step 11. Click **Save**.

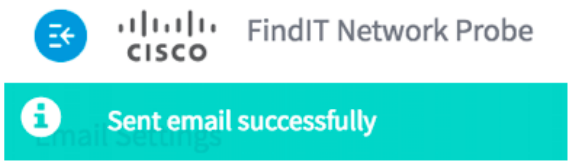


Step 12. Click **Test Connectivity** to validate the configured mail server credentials. This sends out an email to the configured email addresses to check that the configuration works.

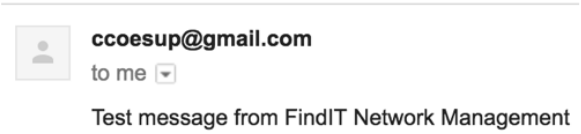


Step 13. If successful, you should see a message below the Cisco logo confirming that the email was sent successfully.

Note: This message disappears in a few seconds after the email has been successfully sent.



You should also receive an empty email notification with the subject Test message from FindIT Network Management.



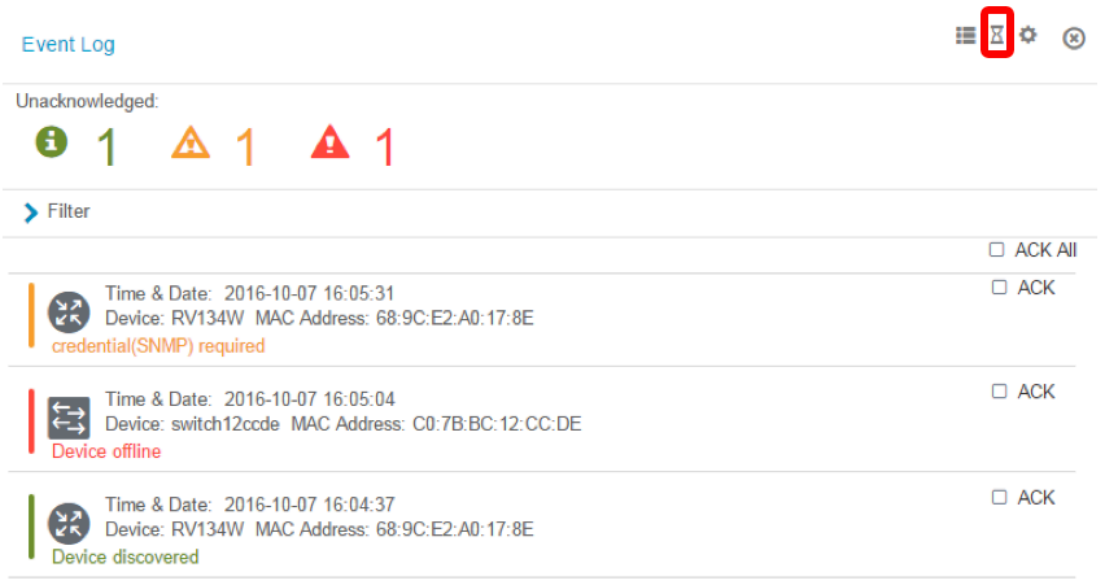
You have successfully configured the email settings on FindIT Network Probe.

Customize Email Notifications

Step 1. In the Home window, click the Notifications Center (bell) icon on the top right corner of the global toolbar. Numbers above the icon indicate the number of unacknowledged notifications.

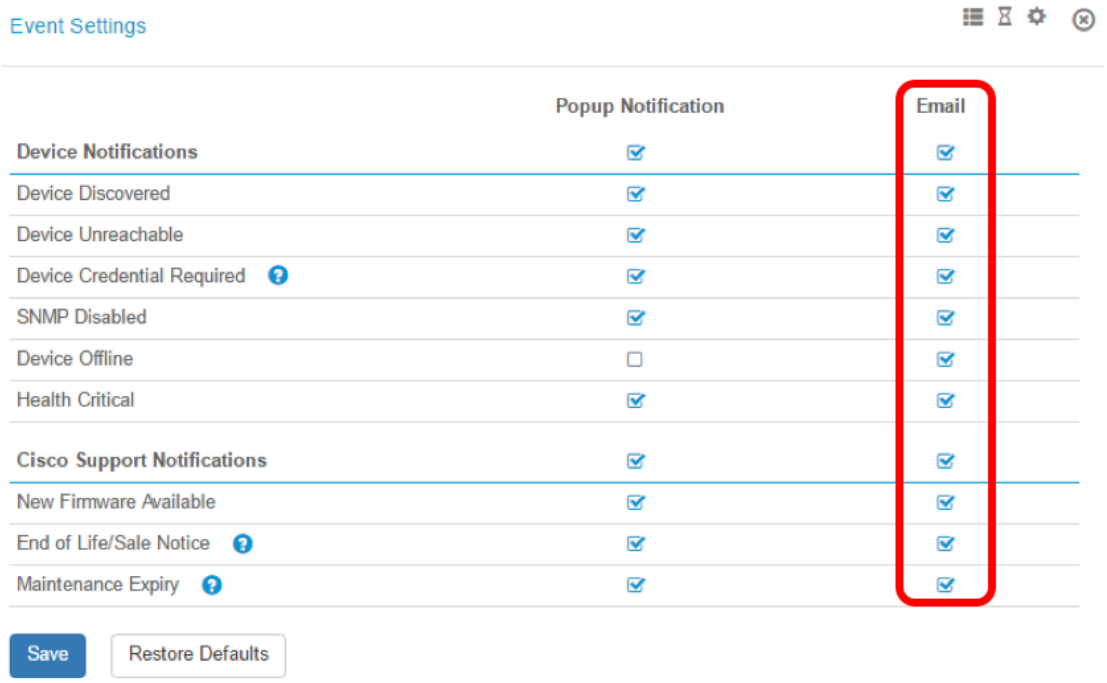
Note: If notifications have occurred, they are listed below the icons in the Event Log dialog box.

Step 2. In the top right corner of the Event Log dialog box, click the Task (hour glass) to go to Event Settings.

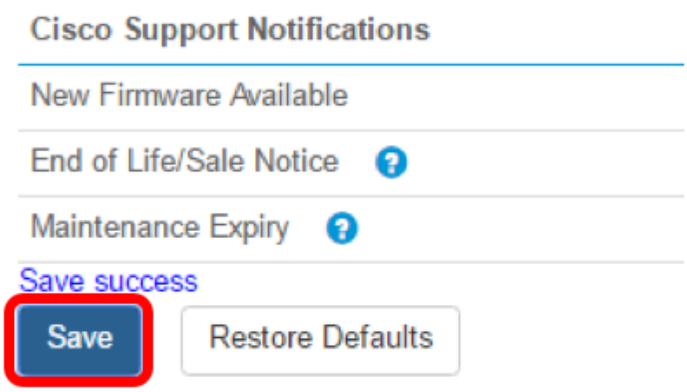


Step 3. In the Email column, check the check boxes to select or filter the events that you want to receive notifications from.

Note: For this example, all check boxes are checked. This means that you will receive all device and Cisco Support notifications.

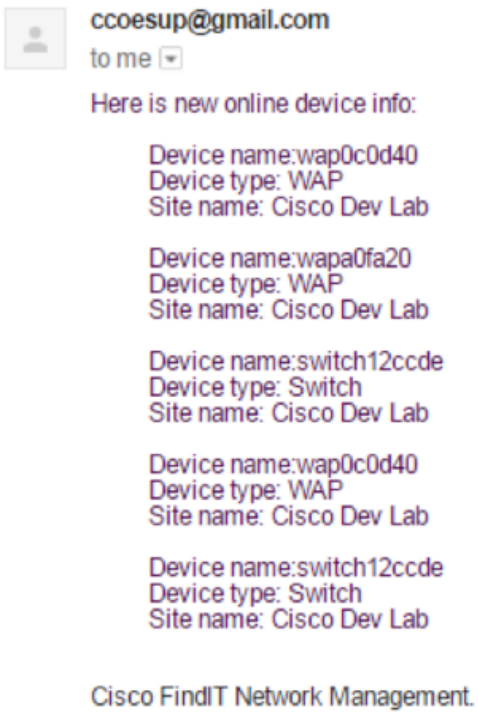


Step 4. Click **Save**.



Step 5. (Optional) Log in to your email account and view the email notifications received from the Cisco FindIT Network Management.

Note: This example shows devices that have been discovered by the Cisco FindIT Network Management.



You have now successfully customized your email notifications.