

Configurazione delle impostazioni di posta elettronica e personalizzazione delle notifiche di posta elettronica su FindIT Network Probe

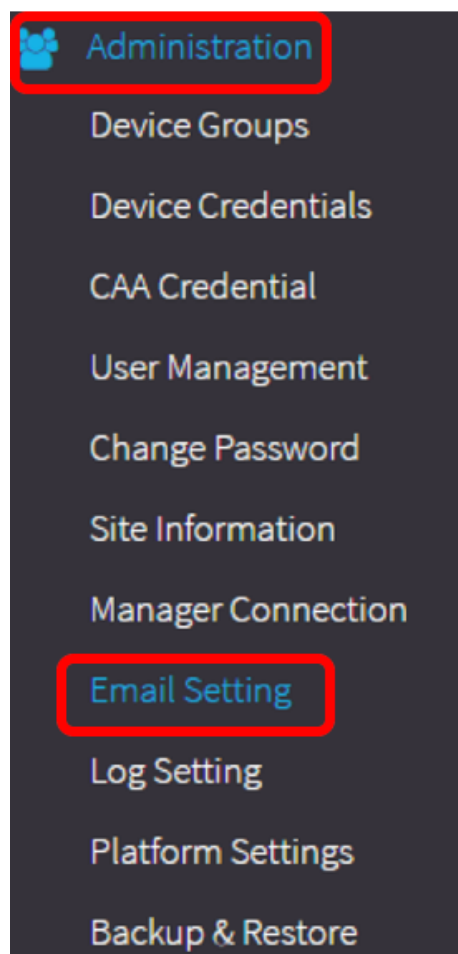
Obiettivo

Cisco FindIT Network Probe offre agli amministratori di rete strumenti indispensabili per monitorare e gestire in modo sicuro i dispositivi Cisco da un browser Web. FindIT Network Probe può essere configurato in modo da generare notifiche e-mail per informare l'utente sugli eventi di rete selezionati contenenti notifiche sul dispositivo e sul supporto Cisco, come modifiche alle impostazioni di rete, nuovo firmware disponibile, stato del dispositivo e altri aggiornamenti sui dispositivi connessi alla rete.

Questo documento ha lo scopo di mostrare come configurare le impostazioni e-mail e regolare le notifiche e-mail causate da eventi di rete su FindIT Network Probe.

Configura impostazione posta elettronica

Passaggio 1. Accedere alla GUI di FindIT Network Probe Administration e scegliere **Amministrazione > Impostazione e-mail**.



Passaggio 2. Nel campo *Server SMTP*, immettere il nome host valido del server di posta.

Nota: Nell'esempio viene utilizzato smtp.gmail.com.

SMTP Server:	<input type="text" value="smtp.gmail.com"/>	✓
SMTP Port:	<input type="text" value="587"/>	✓
Email Encryption:	<input type="text" value="TLS"/>	▼
Authentication:	<input type="text" value="login"/>	▼

Passaggio 3. Immettere il numero di porta del server di posta nel campo Porta *SMTP*. Si tratta di un numero di porta in uscita utilizzato per inviare messaggi di posta elettronica. L'intervallo di numeri di porta valido è compreso tra 0 e 65535 e il valore predefinito è 465 per il protocollo SMTP (Simple Mail Transfer Protocol).

Nota: Nell'esempio viene utilizzata la porta SMTP numero 587.

SMTP Server:	<input type="text" value="smtp.gmail.com"/>	✓
SMTP Port:	<input type="text" value="587"/>	✓
Email Encryption:	<input type="text" value="TLS"/>	▼
Authentication:	<input type="text" value="login"/>	▼

Passaggio 4. Dall'elenco a discesa Email Encryption, selezionare un metodo di crittografia per inviare i messaggi alla posta elettronica. È importante che il metodo di crittografia corrisponda anche alla porta SMTP.

Le opzioni sono:

- Nessuno - Non verrà utilizzata alcuna crittografia nei messaggi di posta elettronica.
- TLS — Transport Layer Security (TLS) è un protocollo crittografico che fornisce sicurezza e integrità dei dati per la comunicazione su Internet. Questa crittografia utilizza la porta SMTP 587.
- SSL: Secure Sockets Layer (SSL) è una tecnologia di protezione standard per la creazione di un collegamento crittografato tra un server Web e un browser. Questa crittografia utilizza la porta SMTP 465.

Nota: Nell'esempio viene utilizzato TLS.

SMTP Server: smtp.gmail.com ✓

SMTP Port: 587 ✓

Email Encryption: TLS

Authentication: TLS

Username: ccoesup@gmail.com ✓

Passaggio 5. Dall'elenco a discesa Autenticazione, scegliere la modalità di autenticazione dell'accesso alla posta elettronica.

Le opzioni sono:

- Nessuno — nessuna autenticazione che richiede Nome utente e Password.
- testo non crittografato; richiede ancora Nome utente e Password.
- md5 — L'algoritmo Message-Digest 5 utilizza un valore hash a 128 bit per l'autenticazione che richiede Nome utente e Password.
- login - per l'autenticazione vengono utilizzati il nome utente e la password.

Nota: Per questo esempio, viene utilizzato login.

SMTP Server: smtp.gmail.com ✓

SMTP Port: 587 ✓

Email Encryption: TLS

Authentication: login

Username: clear-text

Password: md5

Passaggio 6. (Facoltativo) Se nel Passaggio 5 è stato scelto non crittografato, md5 o login, immettere un Nome utente nel campo *Nome utente*. Questo sarebbe l'indirizzo e-mail di invio.

Nota: Nell'esempio viene utilizzato ccoesup@gmail.com.

Username: ✓

Password: ✓

Send Email to 1: ✓

Send Email to 2:

From Email Address: ✓

Passaggio 7. (Facoltativo) Immettere la password nel campo *Password* per il Nome utente configurato in precedenza.

Nota: si consiglia di utilizzare un account e-mail separato invece di usare l'e-mail personale per mantenere la privacy.

Username: ✓

Password: ✓

Send Email to 1: ✓

Send Email to 2:

From Email Address: ✓

Passaggio 8. Immettere un indirizzo di posta elettronica nel campo *Invia messaggio a 1*. L'indirizzo è il destinatario degli aggiornamenti di rete.

Nota: Si consiglia di utilizzare un account di posta elettronica distinto invece di utilizzare l'indirizzo di posta elettronica personale per mantenere la privacy. Nell'esempio riportato viene utilizzato ccoесup2@gmail.com.

Username: ✓

Password: ✓

Send Email to 1: ✓

Send Email to 2:

From Email Address: ✓

Passaggio 9. (Facoltativo) Immettere un indirizzo e-mail secondario nel campo *Invia e-mail a 2*.

Username: ✓

Password: ✓

Send Email to 1: ✓

Send Email to 2: ✓

From Email Address: ✓

Passaggio 10. Immettere l'indirizzo di posta elettronica autenticato utilizzato nei campi Nome utente e Password del passaggio 6 come indirizzo di posta elettronica di invio nel campo *Indirizzo di posta elettronica mittente*.

Nota: Nell'esempio viene utilizzato ccoесup@gmail.com.

Username: ✓

Password: ✓

Send Email to 1: ✓

Send Email to 2:

From Email Address: ✓

Passaggio 11. Fare clic su **Salva**.

Username: ✓

Password: ✓

Send Email to 1: ✓

Send Email to 2:

From Email Address: ✓

Passaggio 12. Fare clic su **Test connettività** per convalidare le credenziali del server di posta configurato. Verrà inviato un messaggio e-mail agli indirizzi configurati per verificare che la configurazione funzioni.

Username: ✓

Password: ✓

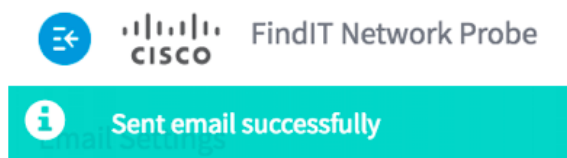
Send Email to 1: ✓

Send Email to 2:

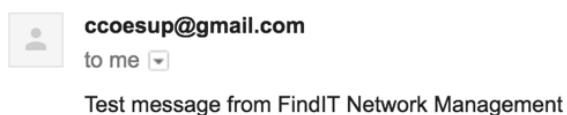
From Email Address: ✓

Passaggio 13. Se l'operazione ha esito positivo, sotto il logo Cisco dovrebbe essere visualizzato un messaggio che conferma l'avvenuto invio dell'e-mail.

Nota: Questo messaggio scompare dopo pochi secondi dall'invio.



Dovrebbe inoltre essere ricevuta una notifica e-mail vuota con l'oggetto Messaggio di prova da FindIT Network Management.



Configurazione delle impostazioni e-mail su FindIT Network Probe completata.

Personalizza notifiche di posta elettronica

Passaggio 1. Nella finestra Home, fare clic sull'icona Centro notifiche (bell) nell'angolo superiore destro della barra degli strumenti globale. I numeri sopra l'icona indicano il numero di notifiche non riconosciute.

Nota: Se sono state eseguite notifiche, queste vengono elencate sotto le icone nella finestra di dialogo Registro eventi.



Passaggio 2. Nell'angolo in alto a destra della finestra di dialogo Registro eventi, fare clic su Attività (icona a forma di ora) per andare a Impostazioni evento.




Unacknowledged:

 1  1  1[Filter](#)

	<input type="checkbox"/> ACK All
 Time & Date: 2016-10-07 16:05:31 Device: RV134W MAC Address: 68:9C:E2:A0:17:8E credential(SNMP) required	<input type="checkbox"/> ACK
 Time & Date: 2016-10-07 16:05:04 Device: switch12ccde MAC Address: C0:7B:BC:12:CC:DE Device offline	<input type="checkbox"/> ACK
 Time & Date: 2016-10-07 16:04:37 Device: RV134W MAC Address: 68:9C:E2:A0:17:8E Device discovered	<input type="checkbox"/> ACK

Passaggio 3. Nella colonna E-mail, selezionare le caselle di controllo per selezionare o filtrare gli eventi da cui si desidera ricevere le notifiche.

Nota: In questo esempio, tutte le caselle di controllo sono selezionate. Ciò significa che verranno ricevute tutte le notifiche relative ai dispositivi e al supporto Cisco.

	Popup Notification	Email
Device Notifications	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Discovered	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Unreachable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Credential Required 	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SNMP Disabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Offline	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Health Critical	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco Support Notifications	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
New Firmware Available	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
End of Life/Sale Notice 	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Maintenance Expiry 	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Passaggio 4. Fare clic su **Salva**.

Cisco Support Notifications

New Firmware Available

End of Life/Sale Notice 

Maintenance Expiry 

Save success

Save

Restore Defaults

Passaggio 5. (Facoltativo) Accedere al proprio account e-mail e visualizzare le notifiche e-mail ricevute da Cisco FindIT Network Management.

Nota: Nell'esempio vengono mostrati i dispositivi rilevati da Cisco FindIT Network Management.



ccoesup@gmail.com

to me 

Here is new online device info:

Device name:wap0c0d40
Device type: WAP
Site name: Cisco Dev Lab

Device name:wapa0fa20
Device type: WAP
Site name: Cisco Dev Lab

Device name:switch12ccde
Device type: Switch
Site name: Cisco Dev Lab

Device name:wap0c0d40
Device type: WAP
Site name: Cisco Dev Lab

Device name:switch12ccde
Device type: Switch
Site name: Cisco Dev Lab

Cisco FindIT Network Management.

Le notifiche di posta elettronica sono state personalizzate.