

E-mailinstellingen configureren en e-mailmeldingen aanpassen op FindIT-netwerkproxy

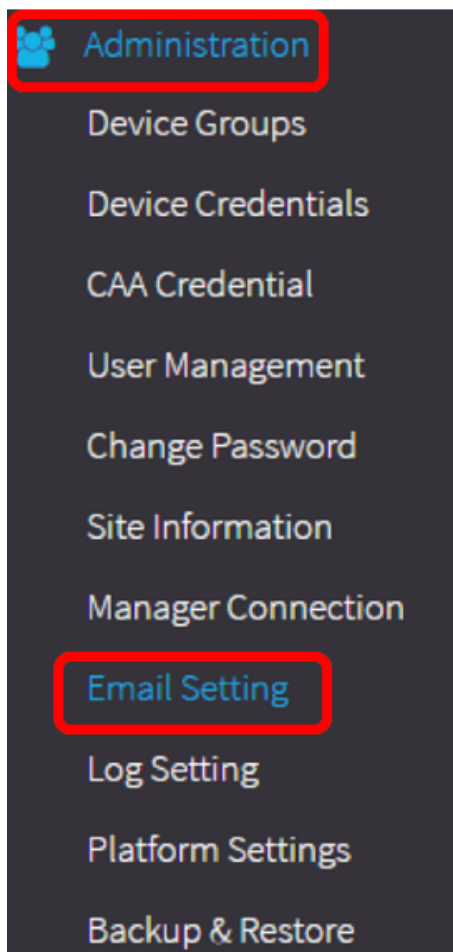
Doel

Cisco FindIT Network Probe dient een netwerkbeheerder uit met onmisbare tools die Cisco-apparaten veilig kunnen bewaken en beheren vanaf een webbrowser. De FindIT Network Probe kan worden geconfigureerd om e-mailberichten te genereren om u te informeren over geselecteerde netwerkgebeurtenissen die apparaten bevatten en meldingen van Cisco-ondersteuning zoals wijzigingen in netwerkinstellingen, nieuwe beschikbare firmware, status van apparaat en andere updates op apparaten die aangesloten zijn op het netwerk.

Dit document geeft aan hoe u de e-mailinstellingen kunt configureren en e-mailberichten kunt reguleren die zijn veroorzaakt door netwerkgebeurtenissen in de FindIT Network Probe.

E-mailinstelling instellen

Stap 1. Meld u aan bij de FormIT Network Probe Administration GUI en kies > **E-mailinstelling**.



Stap 2. In het veld *MTP-server* voert u de geldige hostnaam van de mailserver in.

Opmerking: Dit voorbeeld wordt smtp.gmail.com gebruikt.

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"/>	▼

Stap 3. Voer het poortnummer van de mailserver in in het veld *mtp*-poort. Het is een uitgaande poortnummer dat wordt gebruikt om e-mails te versturen. Het geldige havennummerbereik is van 0 tot 65535 en de standaardwaarde is 465 voor Eenvoudig Mail Transfer Protocol (MTP).

Opmerking: Bijvoorbeeld, wordt het havennummer 587 van de haven van MTP gebruikt.

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"/>	▼

Stap 4. Selecteer in de vervolgkeuzelijst E-mailencryptie een coderingsmethode om berichten naar uw e-mail te verzenden. Het is belangrijk dat de versleutelingsmethode ook overeenkomt met de MTP-poort.

De opties zijn:

- Geen — In de e-mails wordt geen encryptie gebruikt.
- TLS — Transport Layer Security (TLS) is een cryptografisch protocol dat beveiliging en gegevensintegriteit biedt voor communicatie via het internet. Deze encryptie gebruikt MTP-poort 587.
- SSL — Secure Socket Layer (SSL) is een standaard beveiligingstechnologie voor het maken van een versleutelde link tussen een webserver en een browser. Deze encryptie gebruikt MTP poort 465.

Opmerking: Bij dit voorbeeld wordt TLS gebruikt.

SMTP Server: ✓

SMTP Port: ✓

Email Encryption:

Authentication:

Username: ✓

Stap 5. Kies in de vervolgkeuzelijst Verificatie hoe u de toegang tot uw e-mail wilt authenticeren.

De opties zijn:

- Geen — Geen verificatie waarvoor gebruikersnaam en wachtwoord vereist is.
- duidelijk leesbare tekst — niet gecodeerd; heeft nog steeds naam en wachtwoord nodig.
- md5 — Message-Digest Algoritme 5 gebruikt een hashwaarde van 128 bits voor verificatie waarvoor gebruikersnaam en wachtwoord nodig is.
- aanmelding — Gebruikersnaam en wachtwoord worden gebruikt voor echtheidscontrole.

Opmerking: U gebruikt bijvoorbeeld de inlognaam.

SMTP Server: ✓

SMTP Port: ✓

Email Encryption:

Authentication:

Username:

Password:

Stap 6. (optioneel) Als u in Stap 5 voor de herkende tekst, md5 of inloggen hebt gekozen, typt u een gebruikersnaam in het veld *Gebruikersnaam*. Dit is het verzendende e-mailadres.

Opmerking: In dit voorbeeld wordt ccoesup@gmail.com gebruikt.

Username: ✓

Password: ✓

Send Email to 1: ✓

Send Email to 2:

From Email Address: ✓

Stap 7. (Optioneel) Voer uw wachtwoord in het veld *Wachtwoord in* voor de hierboven ingestelde gebruikersnaam.

Opmerking: Het is sterk aanbevolen om een aparte e-mailaccount te gebruiken in plaats van je persoonlijke e-mail om privacy te behouden.

Username: ✓

Password: ✓

Send Email to 1: ✓

Send Email to 2:

From Email Address: ✓

Stap 8. Voer een e-mailadres in in het veld *E-mail verzenden naar 1*. Het adres is de ontvanger van de netwerkupdates.

Opmerking: Het is sterk aanbevolen om een aparte e-mailaccount te gebruiken in plaats van je persoonlijke e-mail om privacy te behouden. In dit voorbeeld wordt ccoесup2@gmail.com als voorbeeld gebruikt.

Username: ✓

Password: ✓

Send Email to 1: ✓

Send Email to 2:

From Email Address: ✓

Stap 9. (optioneel) Voer een secundair e-mailadres in in het veld *E-mail verzenden naar 2*.

Username: ✓

Password: ✓

Send Email to 1: ✓

Send Email to 2: ✓

From Email Address: ✓

Stap 10. Voer het geauthentiseerde e-mailadres in dat in de velden Gebruikersnaam en Wachtwoord in stap 6 wordt gebruikt als het e-mailadres verzenden in het veld *Vanaf e-mailadres*.

Opmerking: In dit voorbeeld wordt ccoесup@gmail.com gebruikt.

Username: ✓

Password: ✓

Send Email to 1: ✓

Send Email to 2:

From Email Address: ✓

Stap 1. Klik op **Opslaan**.

Username: ✓

Password: ✓

Send Email to 1: ✓

Send Email to 2:

From Email Address: ✓

Stap 12. Klik op **Test Connectivity** om de ingestelde aanmeldingsgegevens van de mailserver te valideren. Dit stuurt een e-mail naar de geconfigureerde e-mailadressen om te controleren of de configuratie werkt.

Username: ✓

Password: ✓

Send Email to 1: ✓

Send Email to 2:

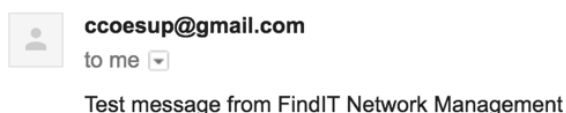
From Email Address: ✓

Stap 13. Als dit lukt, ziet u een bericht onder het Cisco-logo dat bevestigt dat de e-mail succesvol is verstuurd.

Opmerking: Dit bericht verdwijnt binnen enkele seconden nadat de e-mail met succes is verstuurd.



U dient ook een leeg e-mailbericht met de proefversie van FindIT Network Management te ontvangen.



U hebt de e-mailinstellingen met succes ingesteld op FindIT Network Probe.

E-mailmeldingen aanpassen

Stap 1. Klik in het hoofdvenster op het pictogram Meldingen centreren (bel) op de rechterbovenhoek van de werkbalk. Nummers boven het pictogram geven het aantal niet-erkende meldingen aan.

Opmerking: Als er meldingen zijn gedaan, worden deze weergegeven onder de pictogrammen in het dialoogvenster Log bekijken.



Stap 2. Klik in de rechterbovenhoek van het dialoogvenster Event Log op de taak (uurglas)

om naar Event Instellingen te gaan.

Event Log ☰ ⏸ ⚙️ ⓧ

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

Stap 3. Controleer in de kolom E-mail de vinkjes om de gebeurtenissen te selecteren of te filteren waarvan u meldingen wilt ontvangen.

Opmerking: Bijvoorbeeld, alle controlevakjes worden gecontroleerd. Dit betekent dat u alle apparaten en Cisco-ondersteuningsmeldingen zult ontvangen.

Event Settings ☰ ⏸ ⚙️ ⓧ

	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"/>

Stap 4. Klik op Opslaan.

Cisco Support Notifications

New Firmware Available

End of Life/Sale Notice 

Maintenance Expiry 

Save success

Save

Restore Defaults

Stap 5. (Optioneel) Meld u aan bij uw e-mailaccount en bekijk de e-mailmeldingen die u van het Cisco FindIT-netwerkbeheer hebt ontvangen.

Opmerking: Dit voorbeeld toont apparaten die door het netwerkbeheer van Cisco FindIT zijn ontdekt.



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.

U hebt uw e-mailberichten nu aangepast.