

Configureer de apparaatcrediteuren op de FindIT-netwerkmodule

Inleiding

Cisco FindIT Network Management biedt tools die u helpen uw Cisco 100 tot 500 Series netwerkapparaten zoals switches, routers en draadloze access points (WAP's) eenvoudig te controleren, beheren en te configureren met uw webbrowser. Het informeert u ook over machine- en Cisco-ondersteuningsmeldingen zoals de beschikbaarheid van nieuwe firmware, de status van het apparaat, netwerkinstellingen en alle aangesloten Cisco-apparaten die niet langer onder garantie zijn of onder een ondersteuningscontract vallen.

FindIT Network Management is een gedistribueerde toepassing die uit twee afzonderlijke onderdelen of interfaces bestaat: één of meer tests die als FindIT Network Probe en één enkele Manager worden genoemd, FindIT Network Manager.

Een geval van het Network van het Network van FindIT dat op elke plaats in het netwerk wordt geïnstalleerd voert netwerkontdekking uit, en communiceert direct met elk apparaat van Cisco. In één sitenetwerk kunt u ervoor kiezen een standalone exemplaar van het FindIT-netwerkproxy uit te voeren. Als uw netwerk echter uit meerdere sites bestaat, kunt u FindIT Network Manager op een handige locatie installeren en elke proxy koppelen aan de Manager. Vanuit de Manager-interface kunt u een weergave op hoog niveau van de status van alle sites in uw netwerk verkrijgen en verbinding maken met de proxy die op een bepaalde site is geïnstalleerd wanneer u gedetailleerde informatie voor die site wilt weergeven.

Voor FindIT-netwerk om het netwerk volledig te ontdekken en te beheren, moet de FindIT-netwerkproxy beschikken over aanmeldingsgegevens om het netwerk voor authenticatie te zorgen. Wanneer een apparaat voor het eerst wordt ontdekt, zal de Probe proberen om met het apparaat te authenticeren met de standaard gebruikersnaam en het wachtwoord en de Simple Network Management Protocol (SNMP-gemeenschap). Als de aanmeldingsgegevens op het apparaat van de standaard zijn gewijzigd, moet u correcte aanmeldingsgegevens aan FindIT geven. Als deze poging mislukt, wordt er een melding gegenereerd en worden er geldige aanmeldingsgegevens verstrekt door de gebruiker.

Doel

Het doel van dit document is om u te tonen hoe u de Credentials van het apparaat op de steekproeven van Cisco kunt configureren.

Toepasselijke apparaten

- FindIT-toets

Softwareversie

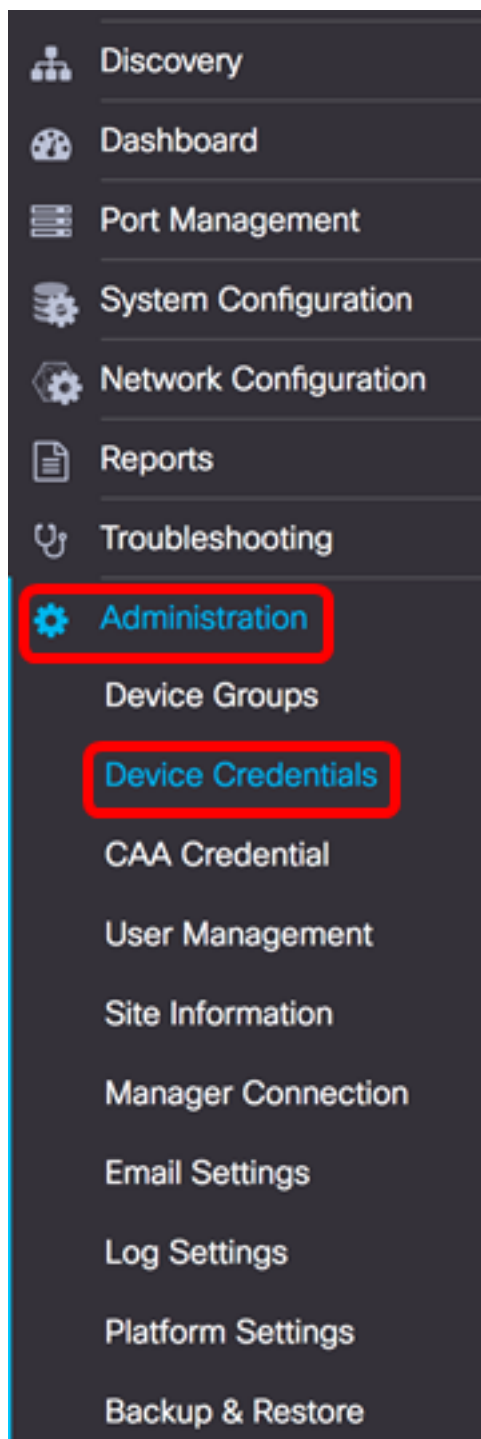
- 1.1

De apparaatreferenties configureren

Voeg nieuwe Credentials toe

Voer in de onderstaande velden een of meer aanmeldingsgegevens in. Indien van toepassing, wordt elke geloofsbrieven getest tegen alle hulpmiddelen van het juiste type waarvoor geen werkbrieven beschikbaar zijn. Een reeks aanmeldingsgegevens kan een gebruikersnaam/wachtwoordcombinatie zijn, een SNMPv2-community of SNMPv3-aanmeldingsgegevens.

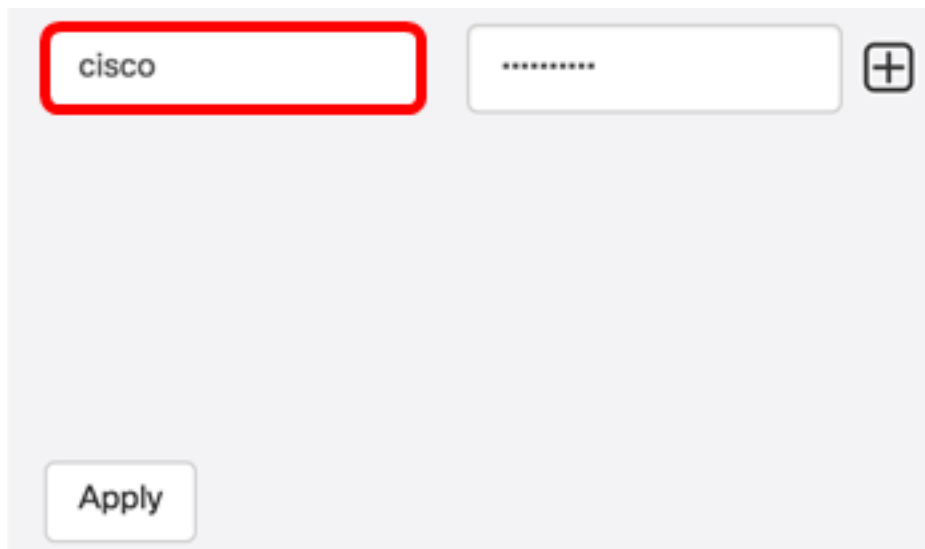
Stap 1. Meld u aan bij de beheerder GUI van het FindIT-netwerk en kies **Administratie > Credentials van het apparaat**.



Stap 2. Voer in het gebied Nieuwe Credentials toevoegen een gebruikersnaam in die op de

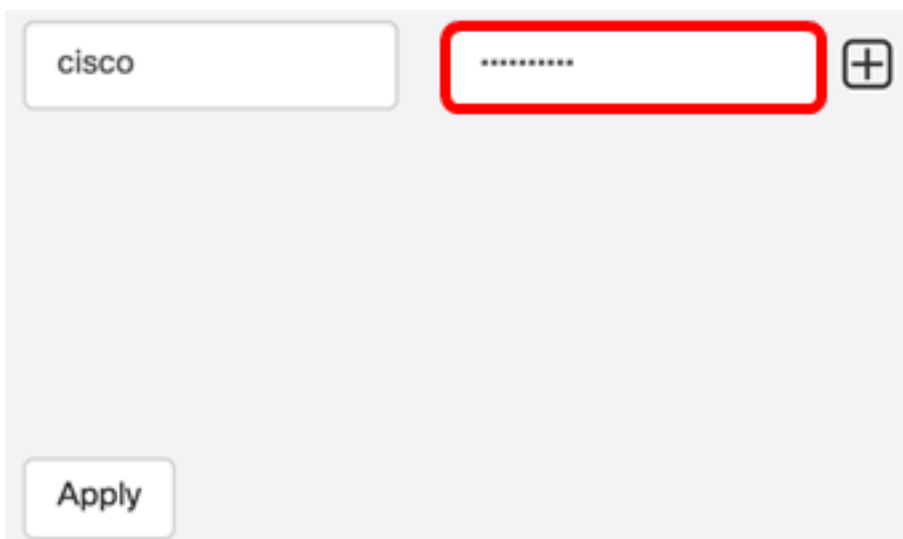
apparaten in het netwerk in het veld *Gebruikersnaam* moet worden toegepast. De standaard gebruikersnaam en wachtwoord zijn Cisco.

Opmerking: In dit voorbeeld wordt cisco gebruikt.



A screenshot of a network configuration interface. At the top, there are two input fields. The first field contains the text 'cisco' and is highlighted with a red rectangular border. The second field contains a series of asterisks '*****' and is also highlighted with a red rectangular border. To the right of the second field is a square button with a plus sign '+'. Below these fields is a larger 'Apply' button.

Stap 3. Voer in het veld *wachtwoord* een wachtwoord in.



A screenshot of a network configuration interface, similar to the one above. The first input field contains 'cisco'. The second input field contains '*****' and is highlighted with a red rectangular border. To the right of the second field is a square button with a plus sign '+'. Below these fields is a larger 'Apply' button.

Stap 4. Voer in het veld *SNMP Community*-naam in. Het is de gelezen enige gemeenschapsstring om de SNMP Get opdracht te authentifieren. De Community Name wordt gebruikt om de informatie van het SNMP apparaat te herstellen. De standaard SNMP Community-naam is Publiek.

Opmerking: In dit voorbeeld wordt het publiek gebruikt.

Public

SNMPv3 User Name

SHA Authentication Pass Phr ✓

None Encryption Pass Phrase

Stap 5. Voer in het veld *SNMPv3*-gebruikersnaam in om in het SNMPv3 te gebruiken

Opmerking: In dit voorbeeld wordt het publiek gebruikt.

Public

Public

None Authentication Pass Phrase

None Encryption Pass Phrase

Stap 6. Kies een verificatietype in het vervolgkeuzemenu Verificatie dat SNMPv3 zal gebruiken. De opties zijn:

- Geen — Er wordt geen gebruikersverificatie gebruikt. Dit is de standaard. Als u deze optie kiest, slaat u over naar [Stap 11](#).
- MD5 — gebruikt een 128-bits coderingsmethode. Het MD5-algoritme gebruikt een openbaar cryptosysteem om gegevens te versleutelen. Als dit geselecteerd is, moet u een Wachtwoord voor verificatie invoeren.
- SHA - Secure Hash Algorithm (SHA) is een eenrichtinggevend algoritme dat een 160-bits digest produceert. SHA compileert langzamer dan MD5, maar is veiliger dan MD5. Als dit is geselecteerd, moet u een verificatiepasser invoeren en een coderingsprotocol selecteren.

Opmerking: In dit voorbeeld wordt SHA gebruikt.

Public

Public

SHA

None

MD5

SHA

Authentication Pass Phrase

Encryption Pass Phrase

Stap 7. Voer in het veld *Verificatiepasser* een wachtwoord in dat door SNMPv3 moet worden gebruikt.

Public

Public

SHA

None

Encryption Pass Phrase

Stap 8. Kies een coderingsmethode in het vervolgkeuzemenu *Encryption Type* om de SNMPv3-verzoeken te versleutelen. De opties zijn:

- Geen — Er is geen coderingsmethode vereist.
- DES - Data Encryption Standard (DES) is een symmetrisch blokalgoritme dat gebruik maakt van een 64-bits gedeelde geheime sleutel.
- AES128 — Advanced Encryption Standard die een 128-bits toets gebruikt.

Opmerking: In dit voorbeeld wordt AES gekozen.

Public

Public

SHA

..... ✓

AES

None

DES

AES

Encryption Pass Phrase

Stap 9. Voer in het veld *Encryption Pass Phrase* in een 128-bits toets die door SNMP voor encryptie moet worden gebruikt.

Public


Public

SHA

..... ✓

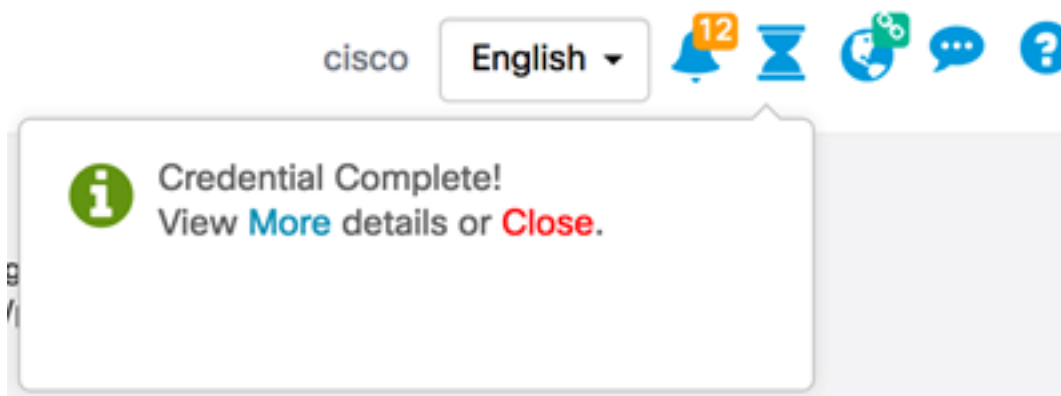
AES

..... ✓

Stap 10. (Optioneel) Klik op de  knop om een nieuwe vermelding voor de gebruikersnaam en de titel te maken. U kunt maximaal een of twee extra items toevoegen, afhankelijk van het type geloofsbrieven.

[Stap 11](#). Klik op **Toepassen**.

Onder het pictogram van het uur verschijnt een venster om u te laten weten dat de gewenste configuraties zijn toegepast.



U dient nu met succes de ApparaatCredentials te configureren op de FindIT Network Probe.

Apparaten op het netwerk weergeven

De onderstaande tabel toont de apparaten die door de Cisco FindIT-netwerkmodule zijn ontdekt.

Device	Credential Type	Credential Ok?	Failure Reason
WAP			
wap5e0940	Admin Userid/Password	✓	
wap5e0940	SNMP	✗	SNMP disabled
wampipti	Admin Userid/Password	✓	
wampipti	SNMP	✗	Invalid credential
WAP150	SNMP	✗	Invalid credential
WAP361	Admin Userid/Password	✗	Invalid credential

- Apparaat — De naam van het apparaat dat op het netwerk wordt ontdekt. Een naam van het apparaat kan meerdere malen verschijnen afhankelijk van het type geloofsbrieven die bruikbaar zijn.
- Credentials type — Dit kan zijn voor beheerder, Wachtwoord of SNMP. Dit wordt gebruikt om informatie van het apparaat te trekken.

- Kredietwaardigheid oké? — Een controle of een rood X kan verschijnen om te bepalen of de in de velden boven ingevoerde referenties op het juiste apparaat van toepassing zijn. Als u op de lijst rode X klikt, komt de configuratie van de apparaatreferenties voor.
- Reden van fout — er verschijnt een oorzaak van storing in de kolom als een apparaat niet met de sonde kan communiceren. Mogelijke berichten zijn "Ongeldige creditnota" of "SNMP uitgeschakeld".

Opmerking: Het wordt aanbevolen om SNMP op het apparaat toe te laten om een nauwkeuriger netwerktopologie te hebben.

U dient nu met succes de identiteit van de apparaten op het netwerk en het bijbehorende geloofstype te hebben bekeken.