Configurare le credenziali del dispositivo su FindIT Network Probe

Introduzione

Cisco FindIT Network Management offre strumenti che semplificano il monitoraggio, la gestione e la configurazione dei dispositivi di rete Cisco serie 100-500, come switch, router e punti di accesso wireless (WAP), tramite il browser Web. Riceve inoltre notifiche relative ai dispositivi e al supporto Cisco, come la disponibilità di nuovo firmware, lo stato dei dispositivi, gli aggiornamenti delle impostazioni di rete e qualsiasi dispositivo Cisco connesso non più in garanzia o coperto da un contratto di assistenza.

FindIT Network Management è un'applicazione distribuita costituita da due componenti o interfacce separate: una o più sonde denominate FindIT Network Probe e un unico gestore denominato FindIT Network Manager.

Un'istanza di FindIT Network Probe installata in ciascun sito della rete esegue l'individuazione della rete e comunica direttamente con ciascun dispositivo Cisco. In una rete a sito singolo, è possibile scegliere di eseguire un'istanza autonoma di FindIT Network Probe. Tuttavia, se la rete è composta da più siti, è possibile installare FindIT Network Manager in una posizione comoda e associare ciascuna sonda a Gestione. Dall'interfaccia di Manager è possibile ottenere una visualizzazione di alto livello dello stato di tutti i siti della rete e connettersi alla sonda installata in un particolare sito per visualizzare informazioni dettagliate su quel sito.

Affinché FindIT Network possa individuare e gestire completamente la rete, FindIT Network Probe deve disporre delle credenziali per l'autenticazione con i dispositivi di rete. Quando un dispositivo viene rilevato per la prima volta, il probe tenterà di eseguire l'autenticazione con il dispositivo utilizzando il nome utente e la password predefiniti e la community SNMP (Simple Network Management Protocol). Se le credenziali del dispositivo sono state modificate rispetto a quelle predefinite, sarà necessario fornire le credenziali corrette per FindIT. Se il tentativo non riesce, verrà generato un messaggio di notifica e l'utente dovrà fornire credenziali valide.

Obiettivo

L'obiettivo di questo documento è mostrare come configurare le credenziali del dispositivo su Cisco Network Probe.

Dispositivi interessati

- FindIT Probe

Versione del software

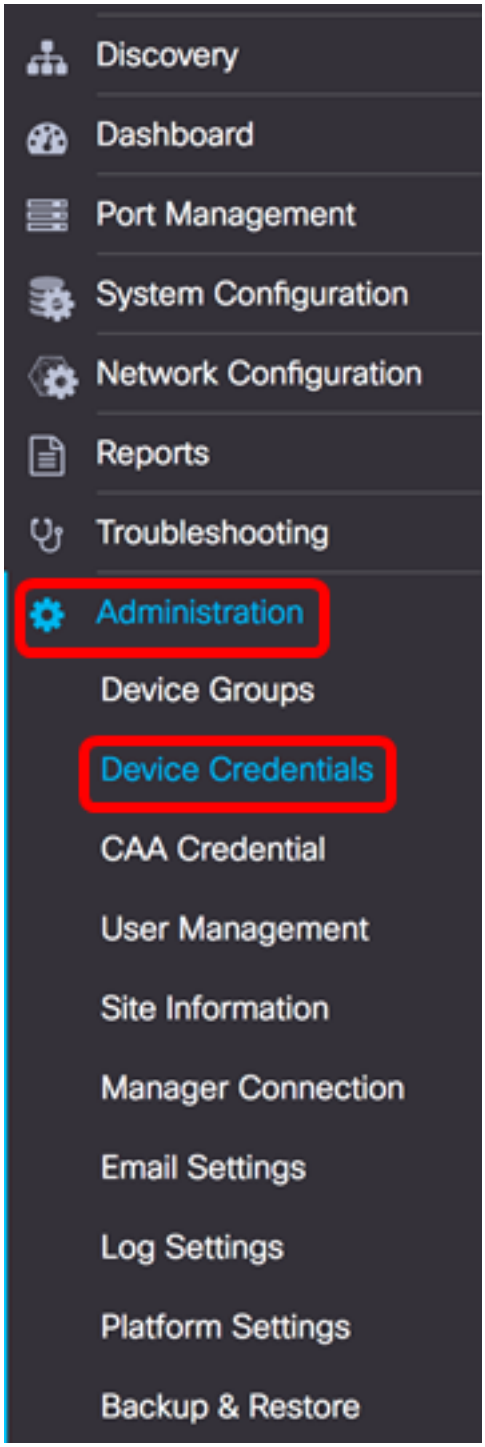
- 1.1

Configurare le credenziali del dispositivo

Aggiungi nuove credenziali

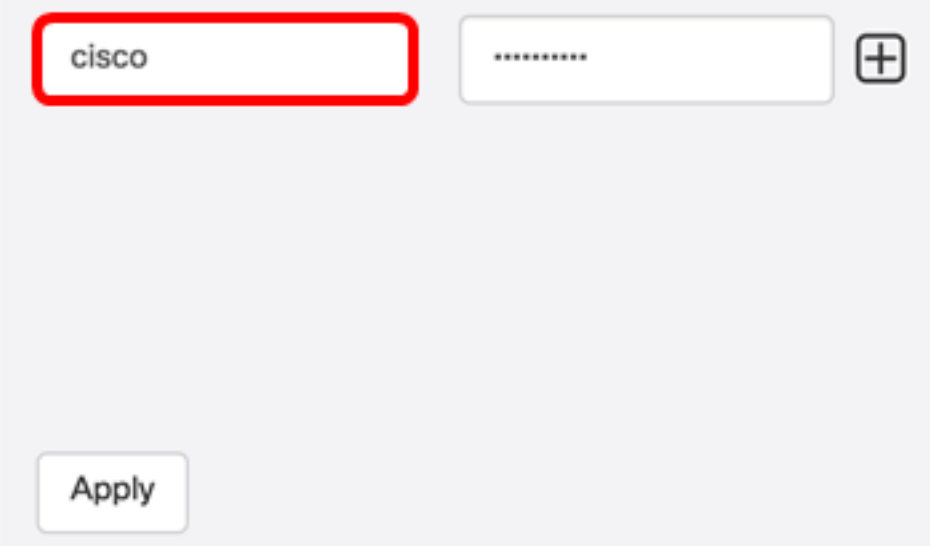
Immettere uno o più set di credenziali nei campi sottostanti. Quando applicate, ciascuna credenziale verrà verificata su qualsiasi dispositivo del tipo appropriato per il quale non sono disponibili credenziali operative. Un insieme di credenziali può essere una combinazione di nome utente/password, una community SNMPv2 o credenziali SNMPv3.

Passaggio 1. Accedere alla GUI di FindIT Network Probe Administrator e scegliere **Amministrazione > Credenziali dispositivo**.

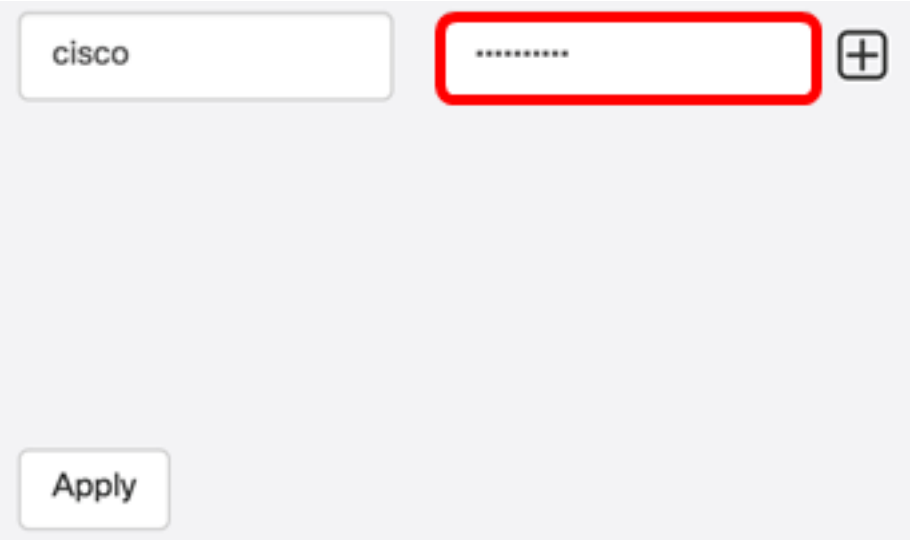


Passaggio 2. Nell'area Aggiungi nuove credenziali, immettere un nome utente da applicare ai dispositivi della rete nel campo *Nome utente*. Il nome utente e la password predefiniti sono cisco.

Nota: nell'esempio viene usato cisco.

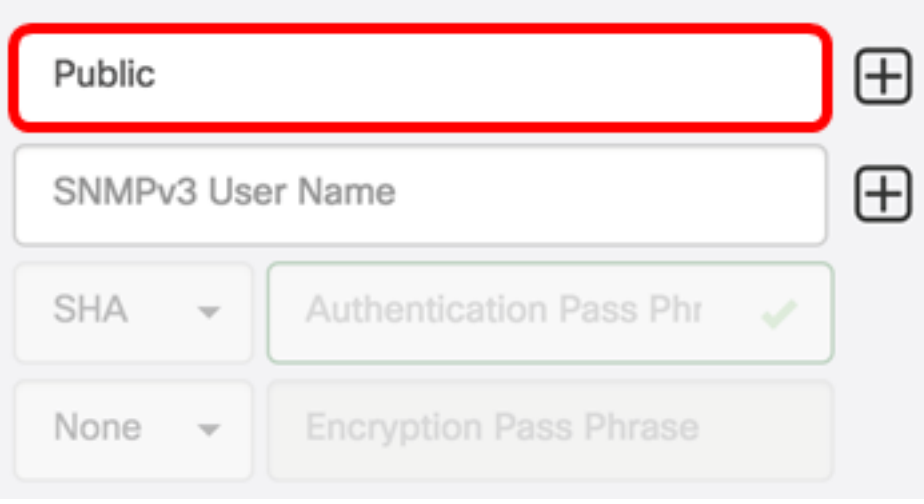


Passaggio 3. Nel campo *password*, immettere una password.



Passaggio 4. Nel campo *Community SNMP*, immettere il nome della community. È la stringa della community di sola lettura per autenticare il comando SNMP Get. Il nome della community viene utilizzato per recuperare le informazioni dal dispositivo SNMP. Il nome della community SNMP predefinito è Public.

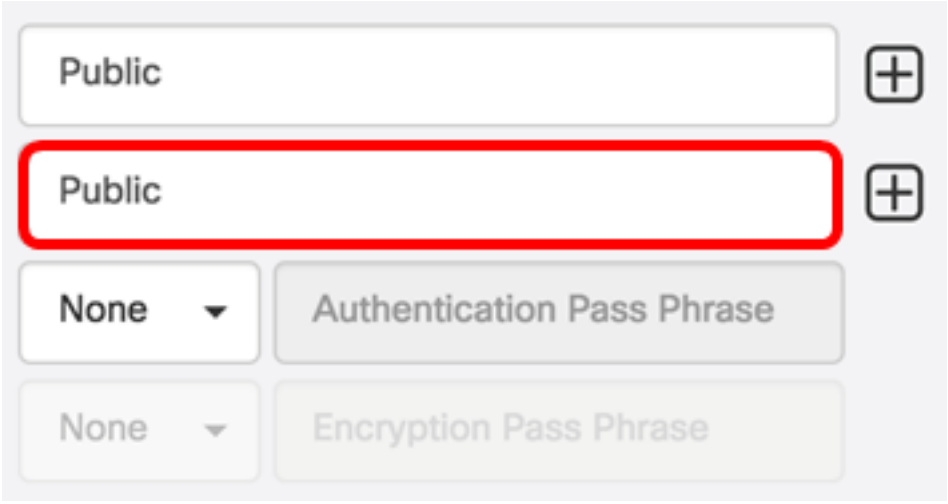
Nota: Nell'esempio viene utilizzato Public.



Passaggio 5. Nel campo *SNMPv3 User Name* (Nome utente SNMPv3), immettere un nome

utente da utilizzare in SNMPv3

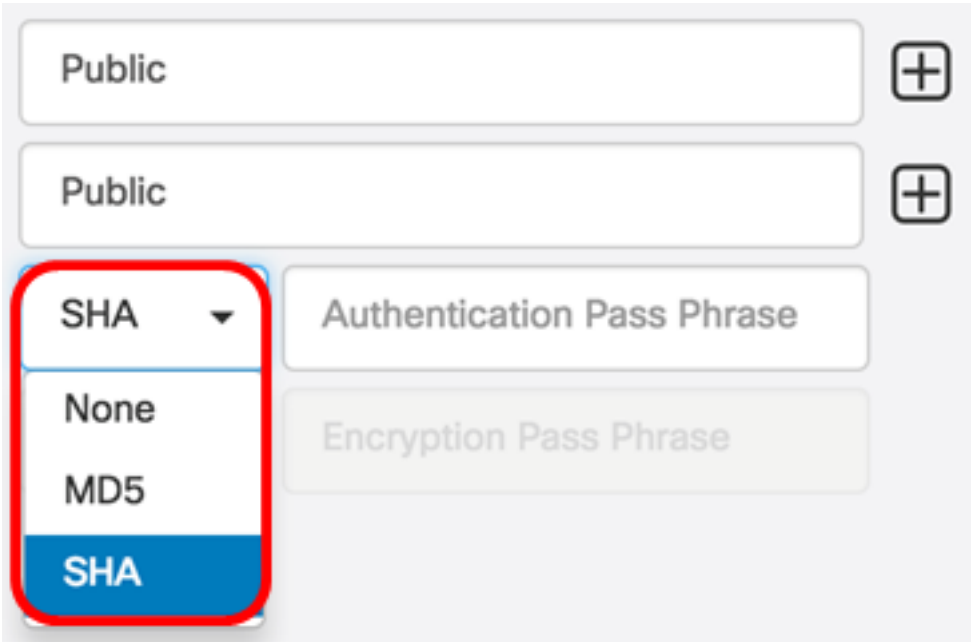
Nota: Nell'esempio viene utilizzato Public.



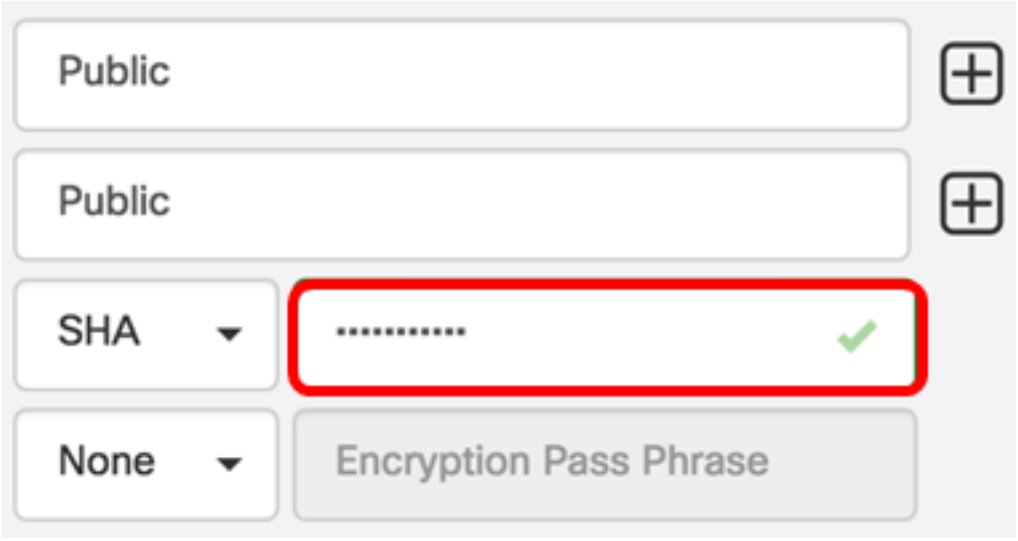
Passaggio 6. Dal menu a discesa Autenticazione, scegliere un tipo di autenticazione da utilizzare con SNMPv3. Le opzioni sono:

- Nessuno — non viene utilizzata l'autenticazione utente. Questa è l'impostazione predefinita. Se si sceglie questa opzione, andare al passaggio 11.
- MD5: utilizza il metodo di crittografia a 128 bit. L'algoritmo MD5 utilizza un sistema di crittografia pubblico per crittografare i dati. Se si sceglie questa opzione, sarà necessario immettere una frase di accesso all'autenticazione.
- SHA — Secure Hash Algorithm (SHA) è un algoritmo di hash unidirezionale che produce un digest a 160 bit. SHA è più lento di MD5, ma più sicuro di MD5. Se si sceglie questa opzione, sarà necessario immettere una frase di accesso autenticazione e scegliere un protocollo di crittografia.

Nota: Nell'esempio viene utilizzato SHA.



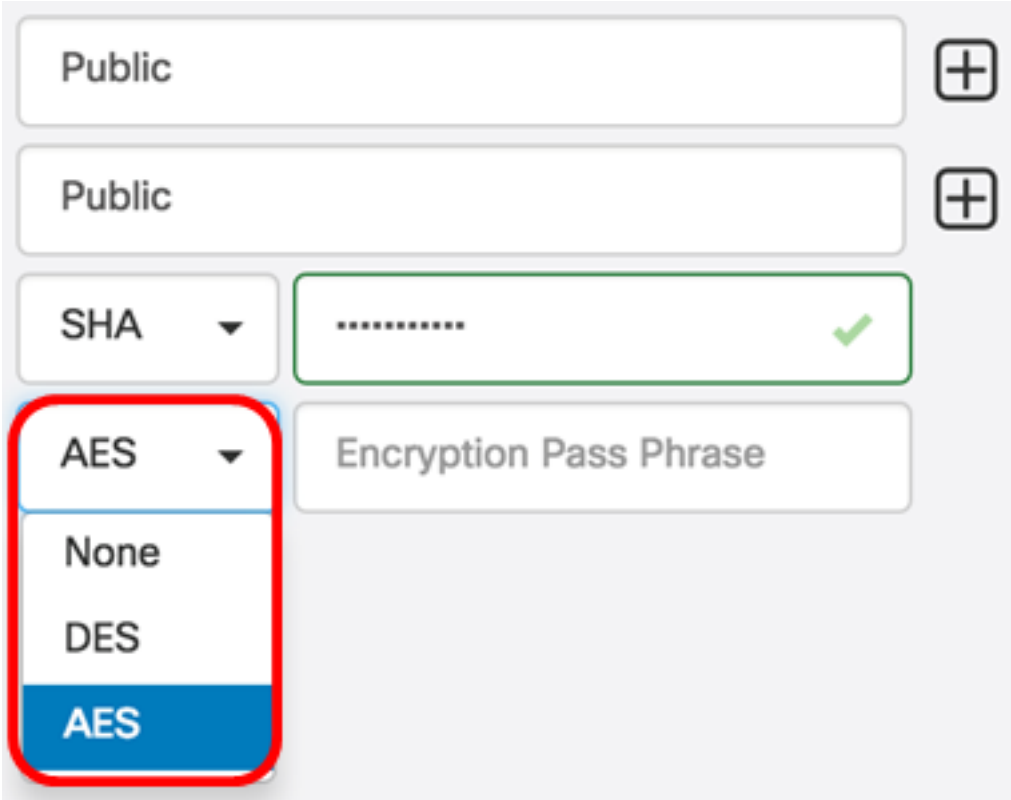
Passaggio 7. Nel campo *Authentication Pass Phrase* (Frase passaggio autenticazione), immettere una password che deve essere utilizzata da SNMPv3.



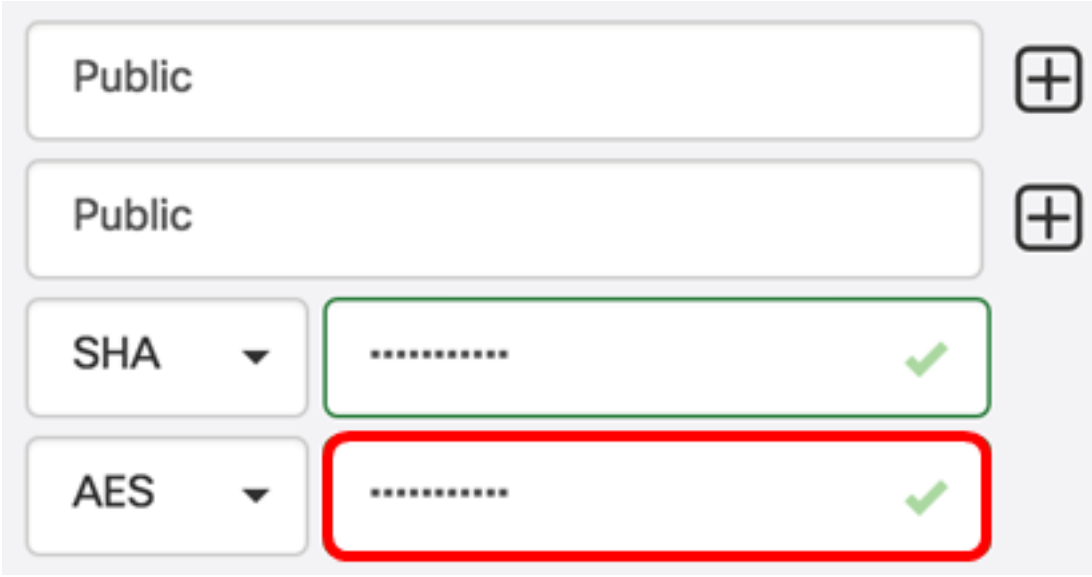
Passaggio 8. Dal menu a discesa Tipo di crittografia, scegliere un metodo di crittografia per crittografare le richieste SNMPv3. Le opzioni sono:

- Nessuno — non è richiesto alcun metodo di crittografia.
- DES: Data Encryption Standard (DES) è una cifratura a blocchi simmetrica che utilizza una chiave segreta condivisa a 64 bit.
- AES128 — Advanced Encryption Standard che utilizza una chiave a 128 bit.

Nota: Nell'esempio, viene scelto AES.

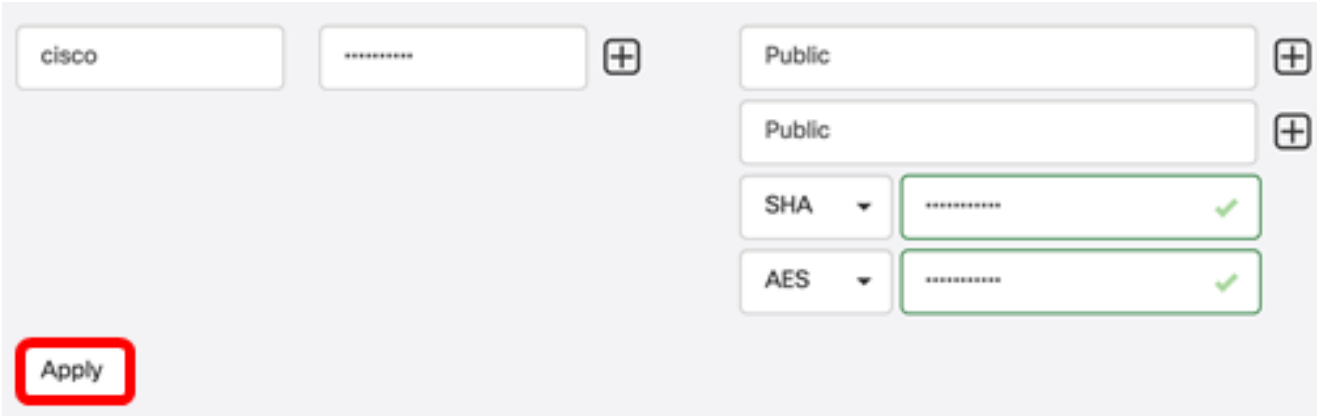


Passaggio 9. Nel campo *Encryption Pass Phrase*, immettere una chiave a 128 bit che SNMP dovrà utilizzare per la crittografia.

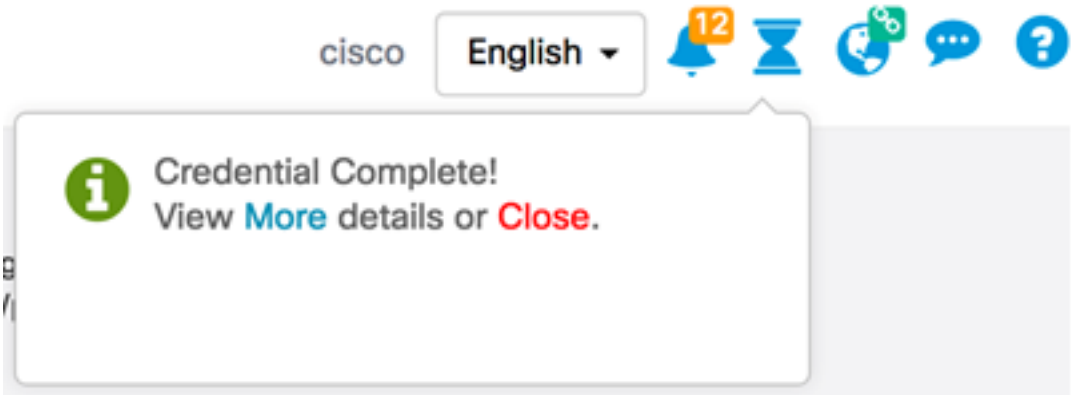


Passaggio 10. (Facoltativo) Fare clic sul pulsante per creare una nuova voce per il nome utente e il titolo. È possibile aggiungere fino a una o due voci aggiuntive, a seconda del tipo di credenziali.

Passaggio 11. Fare clic su **Applica**.



Sotto l'icona a forma di clessidra viene visualizzata una finestra che informa che le configurazioni necessarie sono state applicate.



Configurazione delle credenziali del dispositivo su FindIT Network Probe completata.

Visualizza dispositivi in rete

La tabella seguente mostra i dispositivi rilevati da Cisco FindIT Network Probe.

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

- Periferica — il nome della periferica rilevata sulla rete. Il nome di un dispositivo può apparire più volte a seconda del tipo di credenziali assistibili.
- Tipo di credenziale: può essere un ID utente/password di amministrazione o un protocollo SNMP. Utilizzato per estrarre informazioni dal dispositivo.
- Credenziali OK? — È possibile che venga visualizzato un segno di spunta o una X rossa per determinare se le credenziali immesse nei campi precedenti sono state applicate alla periferica corretta. Se si fa clic sulla X rossa nell'elenco dei dispositivi, verrà visualizzata la configurazione delle credenziali del dispositivo.
- Motivo dell'errore: nella colonna viene visualizzato il motivo dell'errore se un dispositivo non riesce a comunicare con la sonda. I messaggi possibili includono "Credenziali non valide" o "SNMP disabilitato".

Nota: Si consiglia di abilitare il protocollo SNMP sul dispositivo per ottenere una topologia di rete più accurata.

L'identità dei dispositivi sulla rete e il tipo di credenziali corrispondente sono stati visualizzati correttamente.