FindIT 네트워크 프로브에서 디바이스 자격 증명 구성

소개

Cisco FindIT Network Management는 웹 브라우저를 사용하여 Cisco 100~500 Series 네트워크 장치(예: 스위치, 라우터, WAP)를 쉽게 모니터링, 관리 및 구성하는 데 도움이 되는 도구를 제공합니다.또한 새로운 펌웨어, 디바이스 상태, 네트워크 설정 업데이트 및 더 이상 워런티가 적용되지 않거나 지원 계약이 적용되는 연결된 모든 Cisco-디바이스의 가용성과 같은 디바이스 및 Cisco 지원 알림에 대해서도 알립니다.

FindIT Network Management는 두 개의 개별 구성 요소 또는 인터페이스로 구성된 분산 애플리케이션입니다.FindIT Network Probe라고 하는 하나 이상의 프로브 및 FindIT Network Manager라는 단일 관리자

네트워크의 각 사이트에 설치된 FindIT Network Probe의 인스턴스는 네트워크 검색을 수행하고 각 Cisco 디바이스와 직접 통신합니다.단일 사이트 네트워크에서 FindIT Network Probe의 독립형 인스턴스를 실행하도록 선택할 수 있습니다.그러나 네트워크가 여러 사이트로 구성된 경우 편리한 위치에 FindIT Network Manager를 설치하고 각 프로브를 관리자와 연결할 수 있습니다.Manager 인터페이스에서 네트워크에 있는 모든 사이트의 상태를 개괄적으로 볼 수 있으며 해당 사이트에 대한 자세한 정보를 보려면 특정 사이트에 설치된 Probe에 연결할 수 있습니다.

FindIT Network가 네트워크를 완전히 검색하고 관리하려면 FindIT Network Probe에 네트워크 디바이스로 인증하기 위한 자격 증명이 있어야 합니다.디바이스가 처음 검색되면 프로브는 기본 사용자 이름과 비밀번호 및 SNMP 커뮤니티(Simple Network Management Protocol)를 사용하여 디바이스로 인증하려고 시도합니다.디바이스 자격 증명이 기본값에서 변경된 경우 FindIT에 올바른 자격 증명을 제공해야 합니다.이 시도가 실패하면 알림 메시지가 생성되고 사용자가 유효한 자격 증명을 제공해야 합니다.

목표

이 문서의 목적은 Cisco 네트워크 프로브에서 디바이스 자격 증명을 구성하는 방법을 보여 주는 것입니다.

적용 가능한 디바이스

- IT 프로브 찾기

소프트웨어 버전

- 1.1

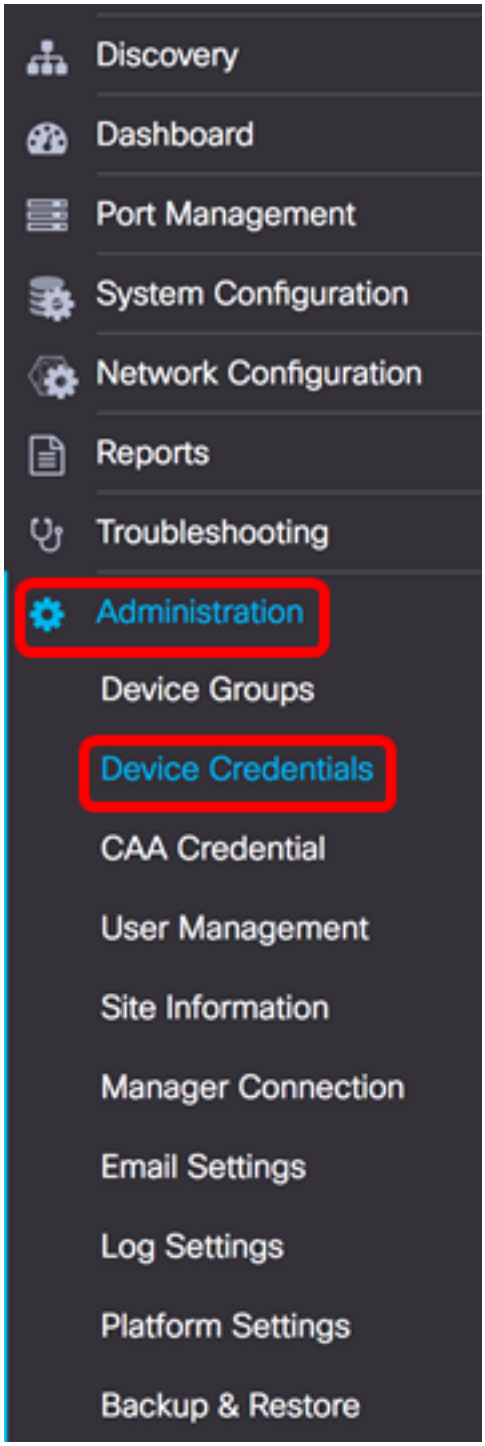
디바이스 자격 증명 구성

새 자격 증명 추가

아래 필드에 하나 이상의 자격 증명 집합을 입력하십시오.적용할 경우 각 자격 증명은 작업 자

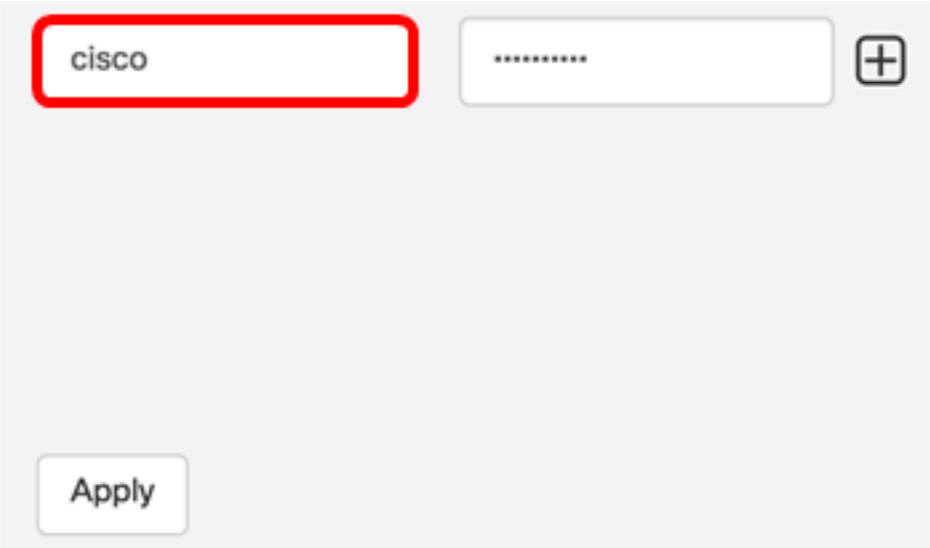
격 증명을 사용할 수 없는 적절한 유형의 모든 디바이스에 대해 테스트됩니다.자격 증명 집합은 사용자 이름/비밀번호 조합, SNMPv2 커뮤니티 또는 SNMPv3 자격 증명일 수 있습니다.

1단계. FindIT Network Probe Administrator GUI에 로그인하고 Administration(관리) **> Device Credentials(디바이스 자격 증명)를 선택합니다**.

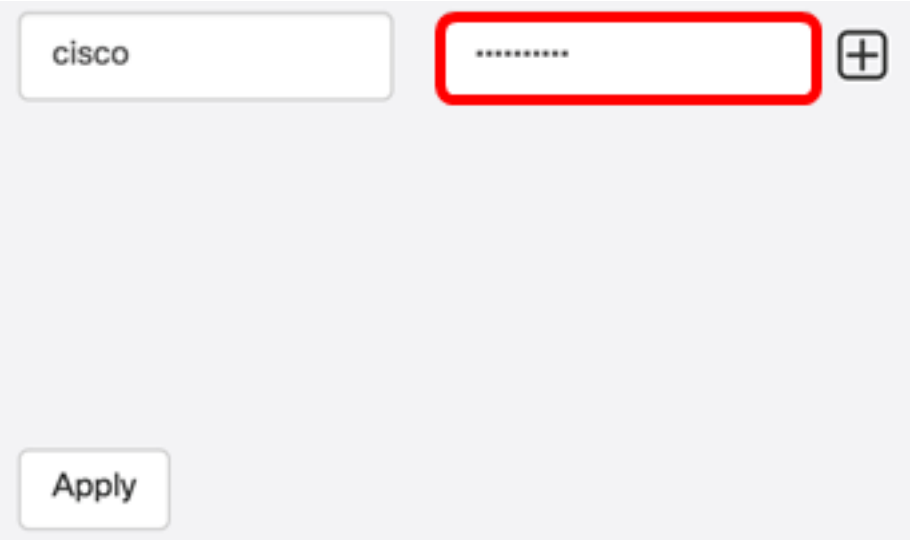


2단계. Add New Credentials(새 자격 증명 추가) 영역에서 Username(사용자 이름) 필드에 네트워크의 디바이스에 적용할 사용자 이름을 입력합니다.기본 사용자 이름과 비밀번호는 cisco입니다.

참고:이 예에서는 cisco가 사용됩니다.

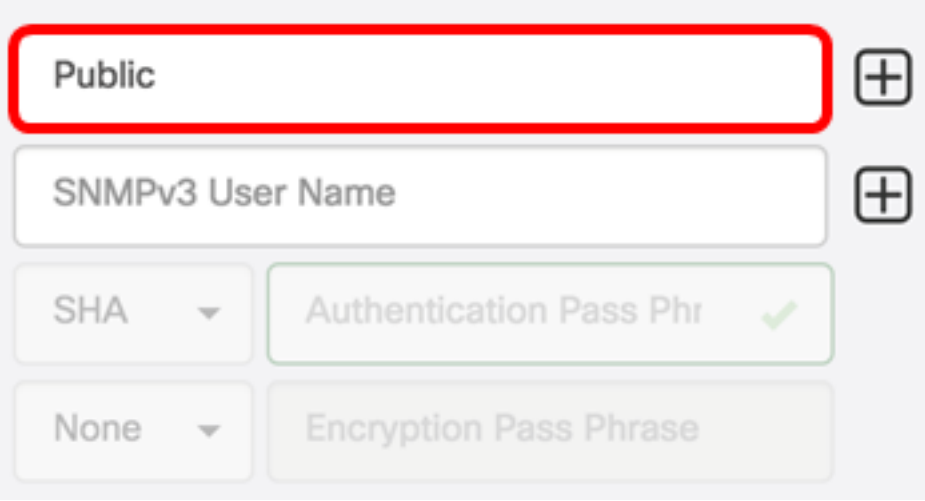


3단계. *비밀번호* 필드에 비밀번호를 입력합니다.



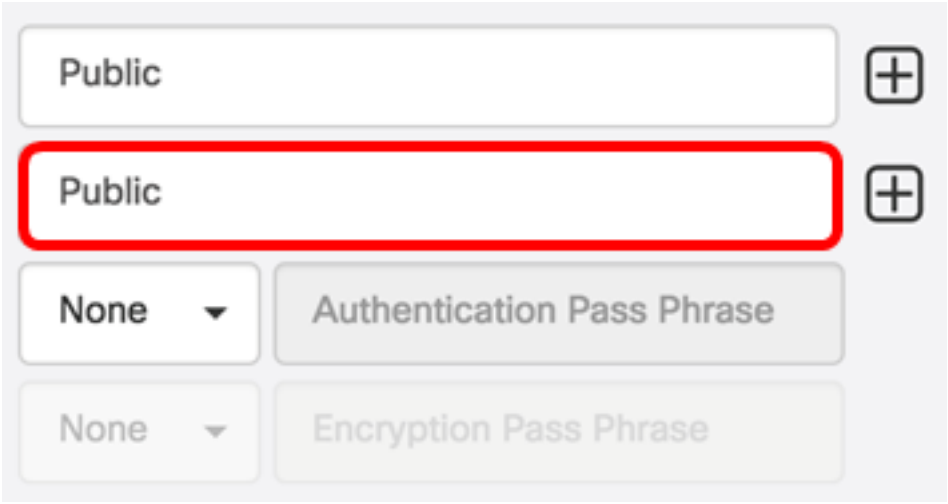
4단계. SNMP *Community*(SNMP 커뮤니티) 필드에 커뮤니티 이름을 입력합니다.SNMP Get 명령을 인증하는 읽기 전용 커뮤니티 문자열입니다.커뮤니티 이름은 SNMP 디바이스에서 정보를 검색하는 데 사용됩니다.기본 SNMP 커뮤니티 이름은 Public입니다.

참고:이 예에서는 Public이 사용됩니다.



5단계. SNMPv*3 User Name* 필드에 SNMPv3에 사용할 사용자 이름을 입력합니다.

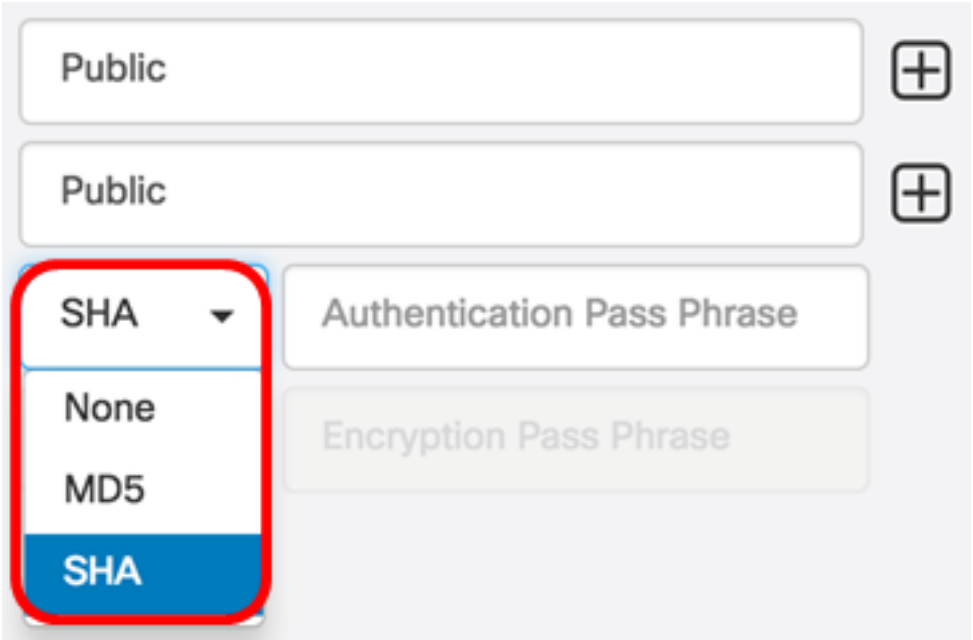
참고:이 예에서는 Public이 사용됩니다.



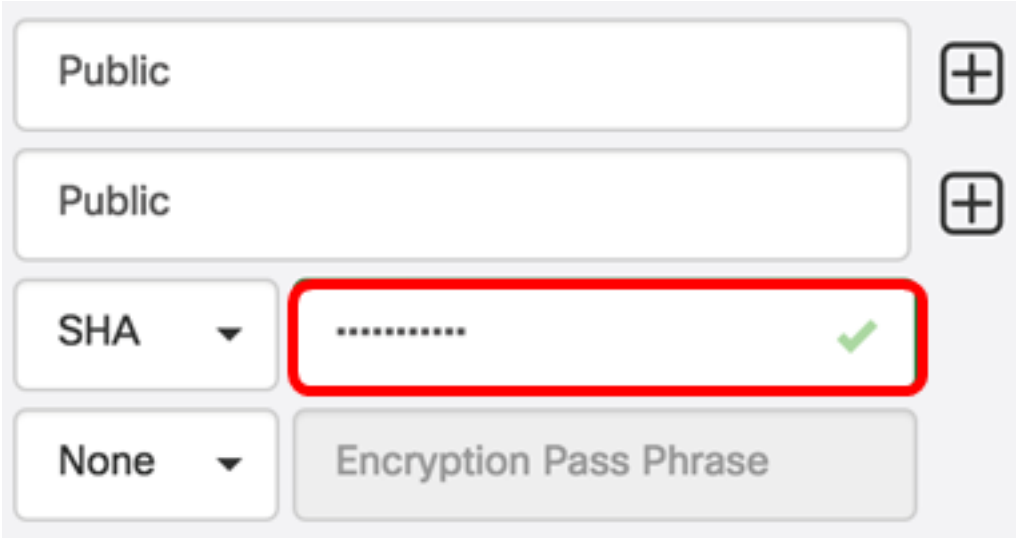
6단계. Authentication(인증) 드롭다운 메뉴에서 SNMPv3에서 사용할 인증 유형을 선택합니다 .옵션은 다음과 같습니다.

- 없음 — 사용자 인증이 사용되지 않습니다.이것이 기본값입니다.이 옵션을 선택하는 경우 11단계로 건너뜁니다.
- MD5 — 128비트 암호화 방법을 사용합니다.MD5 알고리즘은 공용 암호 시스템을 사용하여 데이터를 암호화합니다.이 옵션을 선택한 경우 인증 암호를 입력해야 합니다.
- SHA — SHA(Secure Hash Algorithm)는 160비트 다이제스트를 생성하는 단방향 해싱 알고리즘입니다.SHA는 MD5보다 느리지만 MD5보다 안전합니다. 이 옵션을 선택하면 인증 암호 구문을 입력하고 암호화 프로토콜을 선택해야 합니다.

참고:이 예에서는 SHA가 사용됩니다.



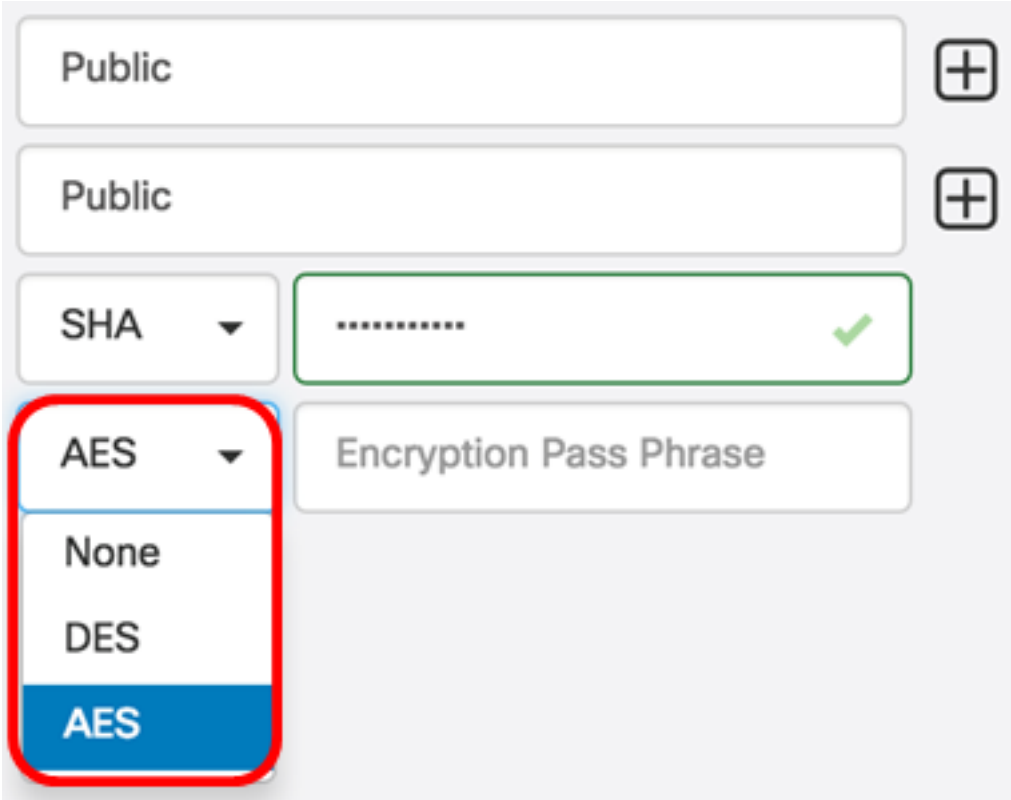
7단계. Authentication *Pass Phrase*(인증 암호문) 필드에 SNMPv3에서 사용할 비밀번호를 입력합니다.



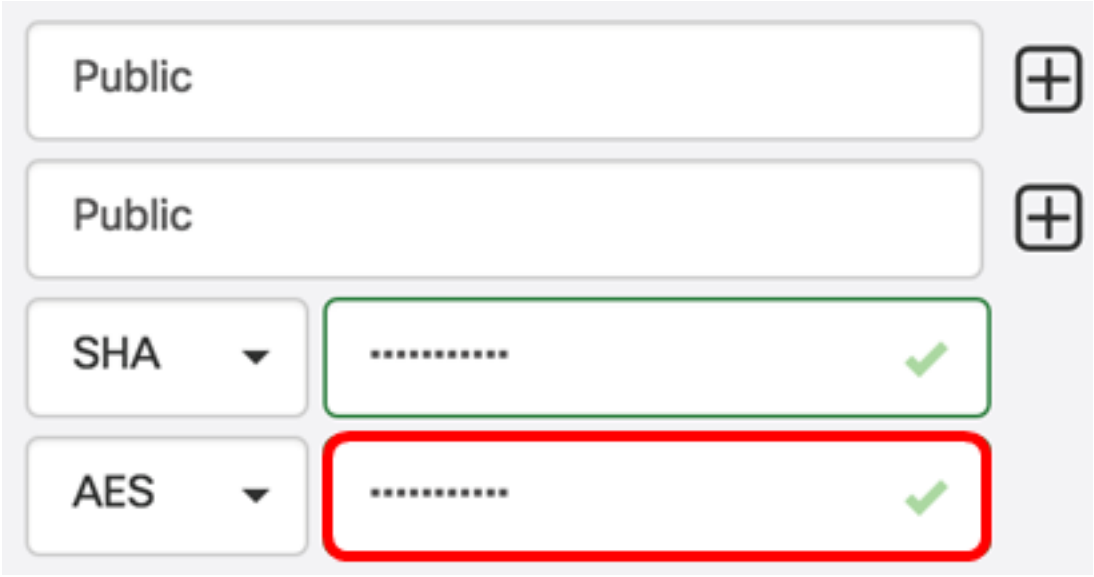
8단계. Encryption Type(암호화 유형) 드롭다운 메뉴에서 SNMPv3 요청을 암호화할 암호화 방법을 선택합니다.옵션은 다음과 같습니다.

- None — 암호화 방법이 필요하지 않습니다.
- DES — DES(Data Encryption Standard)는 64비트 공유 비밀 키를 사용하는 대칭 블록 암호입니다.
- AES128 — 128비트 키를 사용하는 고급 암호화 표준.

참고:이 예에서는 AES가 선택됩니다.

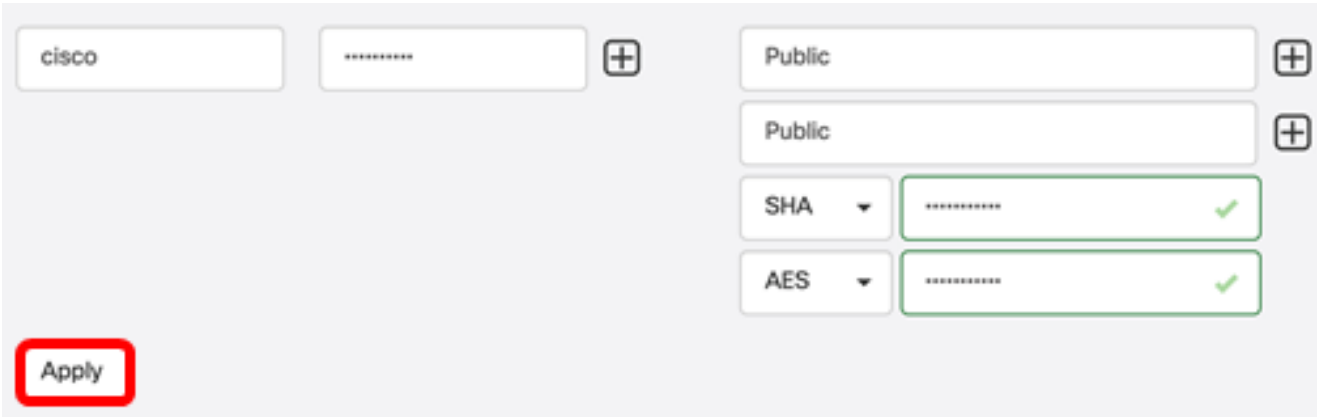


9단계. Encryption *Pass Phrase* 필드에 SNMP에서 암호화에 사용할 128비트 키를 입력합니다.

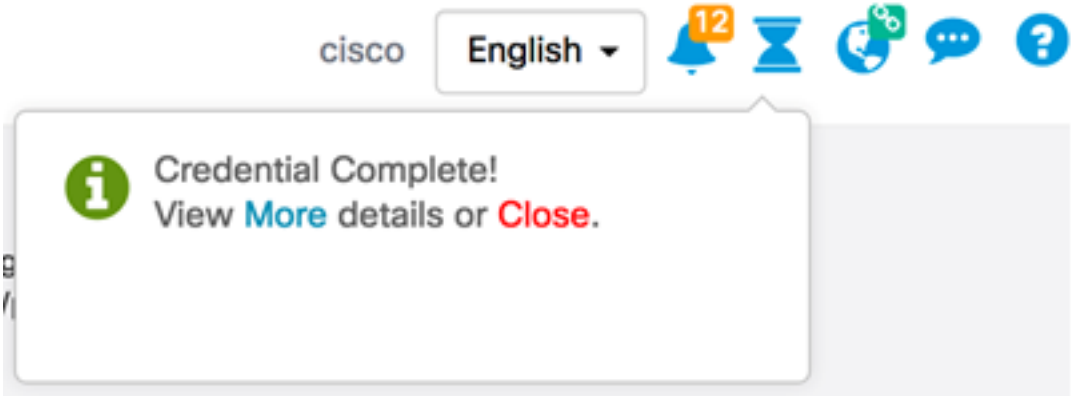


10단계. (선택 사항) 버튼을 클릭하여 사용자 이름과 제목의 새 항목을 생성합니다.자격 증명 유형에 따라 최대 하나 또는 두 개의 추가 항목을 추가할 수 있습니다.

11단계. 적용을 **누릅니다**.



필요한 컨피그레이션이 적용되었음을 알리는 창이 시간 표시 아이콘 아래에 나타납니다.



이제 FindIT Network Probe에서 디바이스 자격 증명을 구성했어야 합니다.

네트워크의 디바이스 보기

아래 표에는 Cisco FindIT Network Probe에서 검색한 디바이스가 표시됩니다.

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

- 디바이스 — 네트워크에서 검색된 디바이스의 이름입니다.서비스 가능한 자격 증명 유형에 따라 디바이스 이름이 여러 번 표시될 수 있습니다.
- 자격 증명 유형 — 관리자 사용자 ID/비밀번호 또는 SNMP일 수 있습니다.이는 디바이스에서 정보를 가져오는 데 사용됩니다.
- 자격 증명 확인?— 위 필드에 입력한 자격 증명이 적절한 장치에 적용되는지 여부를 확인하는 확인 또는 빨간색 X가 나타날 수 있습니다.디바이스 목록에서 빨간색 X를 클릭하면 디바이스 자격 증명에 대한 컨피그레이션이 표시됩니다.
- Failure Reason(실패 사유) — 디바이스가 프로브와 통신하지 못하는 경우 열에 실패 사유가 나타납니다.가능한 메시지에는 "Invalid credential" 또는 "SNMP disabled"가 포함됩니다.

참고:디바이스에서 SNMP를 활성화하여 보다 정확한 네트워크 토폴로지를 갖는 것이 좋습니다.

이제 네트워크에 있는 디바이스의 ID와 해당 자격 증명 유형을 성공적으로 확인했어야 합니다.