

# SDA 및 비 SDA 네트워크 시나리오에서 유선 및 무선 디바이스에 대해 Cisco Catalyst Center의 디바이스 자격 증명 변경

## 목차

---

[소개](#)

[배경 정보](#)

[개요](#)

[솔루션\(모범 사례\)](#)

[요구 사항](#)

[전제 조건](#)

[Cisco Catalyst Center의 자격 증명 변경 절차](#)

[Cisco Catalyst Center Managed AAA가 있는 사이트](#)

[사용자의 비밀번호를 변경해야 합니다\(enable 비밀번호는 변경하지 않음\).](#)

[사용자의 비밀번호 및 enable 비밀번호를 변경해야 합니다.](#)

[Cisco Catalyst Center Unmanaged AAA가 있는 사이트](#)

[사용자의 비밀번호를 변경해야 합니다\(enable 비밀번호는 변경하지 않음\).](#)

[사용자의 비밀번호 및 enable 비밀번호를 변경해야 합니다.](#)

## 소개

이 문서에서는 패브릭과 패브릭이 아닌 네트워크 시나리오에서 유선 및 무선 디바이스에 대한 Cisco Catalyst Center(이전의 Cisco DNA Center)의 자격 증명 변경 절차의 단계를 설명합니다.

## 배경 정보

이 문서는 Cisco Catalyst Center(Dynamic Network Access Control)가 관리되거나 관리되지 않는 AAA(Authentication, Authorization and Accounting)가 있는 사이트에도 적용됩니다.

## 개요

이 문서에서는 자동화를 위해 Cisco Catalyst Center에서 사용하는 자격 증명을 업데이트해야 하는 네트워크 요구 사항에 대해 설명합니다. 관리되는 디바이스는 사용자 이름과 비밀번호로 Cisco Catalyst Center에 의해 검색되며, 이러한 자격 증명은 Cisco Catalyst Center에서 관리되는 디바이스에 대한 SSH 연결(자동화/인벤토리 수집 등)에 사용됩니다. 이 문서에서는 Cisco Catalyst Center에서 관리되는 디바이스를 검색한 후 해당 디바이스의 비밀번호를 변경하는 모범 사례를 다룹니다.

## 솔루션(모범 사례)

## 요구 사항

1. Cisco Catalyst Center에서 관리하는 AAA가 있는 사이트
  - 사용자의 비밀번호를 변경해야 합니다(enable 비밀번호는 변경하지 않음).
  - 사용자의 비밀번호 및 enable 비밀번호를 변경해야 합니다.
2. Cisco Catalyst Center가 관리되지 않는 AAA가 있는 사이트
  - 사용자의 비밀번호를 변경해야 합니다(enable 비밀번호는 변경하지 않음).
  - 사용자의 비밀번호 및 enable 비밀번호를 변경해야 합니다.

## 전제 조건

- AAA가 모든 비 SDA 사이트에 대해 Cisco Catalyst Center에 구성되지 않았는지 확인합니다.
- 모든 Catalyst 9k 스위치(SDA 또는 비 SDA)가 VTY 회선에 대한 SSH 로그인에 RADIUS to ISE를 사용하는지 여부를 확인하려면 Python 스크립트를 사용합니다. 로컬 자격 증명을 사용하는 디바이스를 수정합니다.
- 확장 노드의 경우
  - 행 vty 0에서 4를 업데이트하려면 다음 컨피그레이션 명령을 사용합니다(확장 노드의 첫 번째 단계가 될 수 있음).

```
line vty 0 4
authorization exec VTY_author
login authentication VTY_authen
```

## Cisco Catalyst Center의 자격 증명 변경 절차

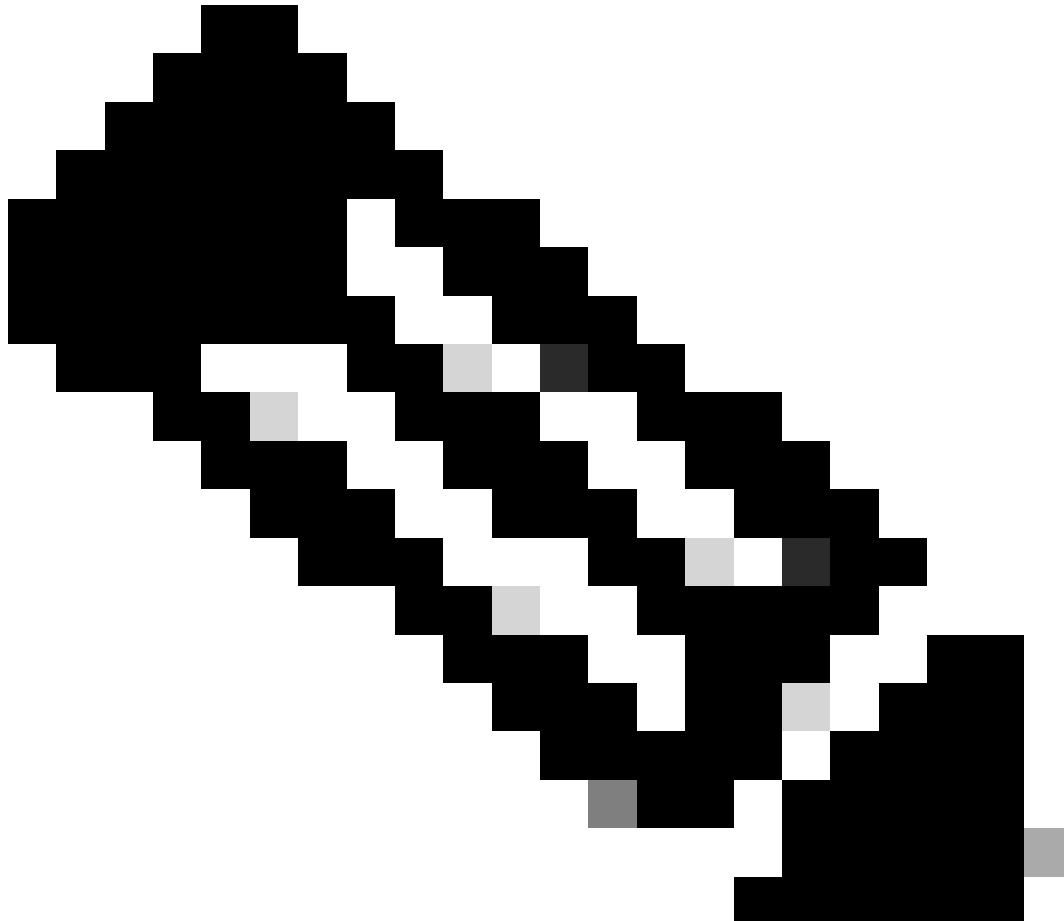
### Cisco Catalyst Center Managed AAA가 있는 사이트

사용자의 비밀번호를 변경해야 합니다(enable 비밀번호는 변경하지 않음).

1. 먼저 ISE에서 자격 증명(관련 사용자 이름에 대한 비밀번호)을 업데이트합니다. 그러면 인벤토리 수집이 실패하고 관리되는 디바이스 인벤토리 상태가 [도달 불가], [부분 수집 실패] 또는 [잘못된 자격 증명]으로 변경됩니다.
2. Provision(프로비저닝) > Inventory(인벤토리) 페이지에서 하나 이상의 디바이스를 선택하고 Actions(작업) > Inventory(인벤토리) > Edit Device(디바이스 수정) > Credentials(자격 증명) 탭을 선택합니다. 그런 다음 "Add device specific credential(디바이스별 자격 증명 추가)"을 새 사용자 이름 및/또는 비밀번호로 업데이트합니다(동일한 enable 비밀번호 유지). 이 시점에서 Cisco Catalyst Center는 업데이트된 자격 증명을 사용하여 디바이스에 로그인할 수 있으며 디바이스 인벤토리 상태는 Managed(관리됨)로 돌아옵니다.
3. 외부 AAA 서버에 연결할 수 없는 경우 Cisco Catalyst Center에서 디바이스에 로그인할 수 있도록 디바이스의 로컬 자격 증명을 대신 업데이트할 수 있습니다. 로컬 자격 증명은 Cisco Catalyst Center의 템플릿 편집기, 맞춤형 Python 스크립트 또는 수동으로 업데이트할 수 있습니다.

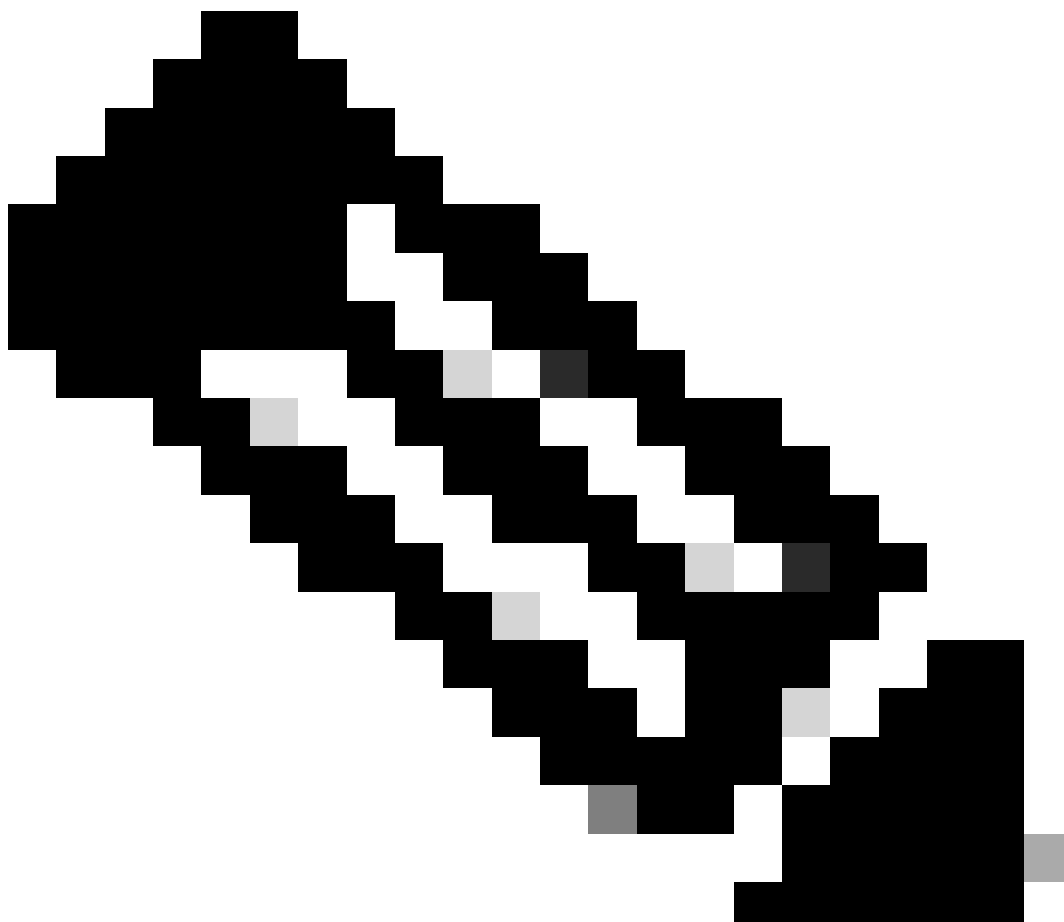
니다.

4. 마지막 단계는 Global Credentials(전역 자격 증명) 페이지에서 동일한 자격 증명을 업데이트 하는 것입니다. 이렇게 하면 새로 검색된 디바이스 또는 LAN Automation을 사용하는 디바이스가 Design(설계) 페이지 > Network Settings(네트워크 설정) > Device Credentials(디바이스 자격 증명) > CLI Credentials(CLI 자격 증명) > edit the username(사용자 이름 수정) > enable password(비밀번호 변경 없이 사용자 비밀번호 업데이트)에서 업데이트된 자격 증명을 사용 하게 됩니다.



참고: SSH/텔넷 로그인은 외부 AAA 서버에서 인증됩니다. 로컬 디바이스 자격 증명이 업데이트되지 않았습니다.

---



참고: 외부 AAA 서버가 사이트의 Cisco Catalyst Center 설계 페이지에 구성된 경우, Global Credentials(전역 자격 증명) 페이지에서 자격 증명을 변경/수정할 때 Cisco Catalyst Center는 관리되는 디바이스 또는 ISE에 대해 어떤 조치도 취하지 않습니다.

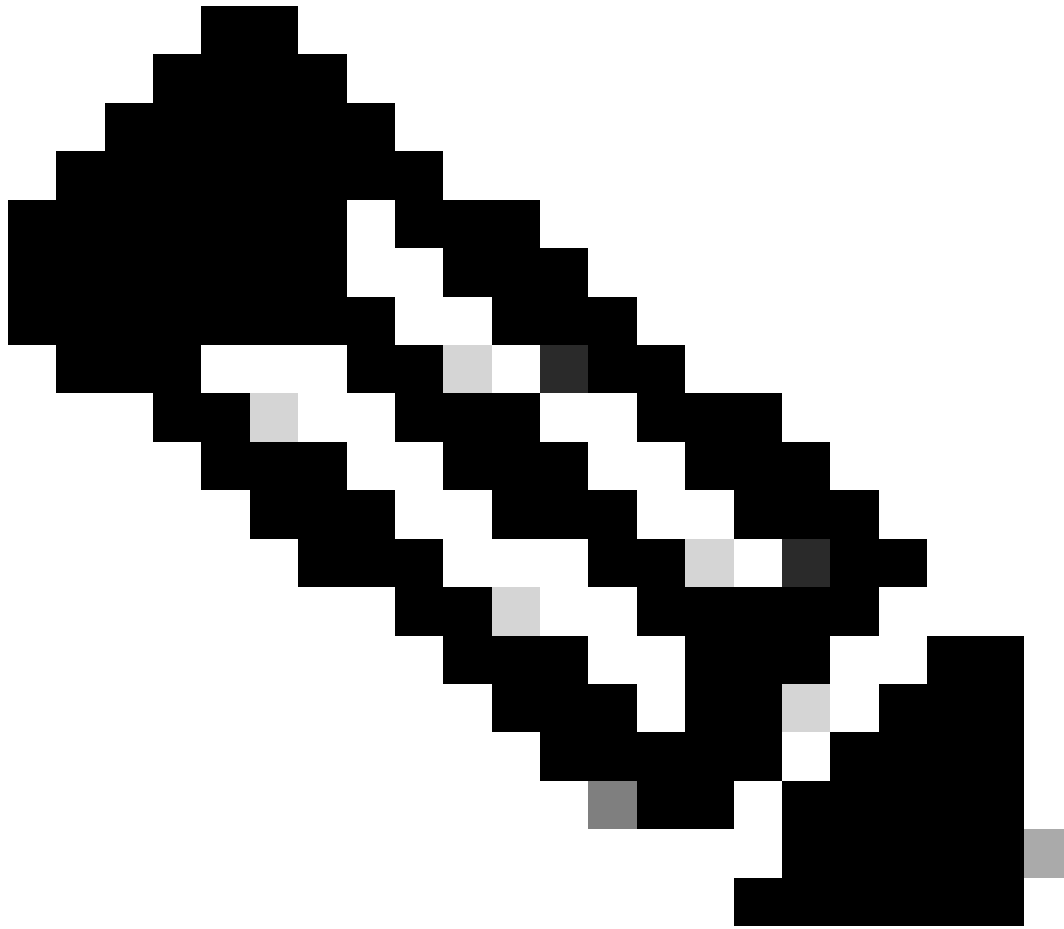
---

사용자의 비밀번호 및 enable 비밀번호를 변경해야 합니다.

1. 먼저 ISE에서 자격 증명(관련 사용자 이름에 대한 비밀번호)을 업데이트합니다. 그러면 인벤토리 수집이 실패하고 관리되는 디바이스 인벤토리 상태가 [도달 불가], [부분 수집 실패] 또는 [잘못된 자격 증명]으로 변경됩니다.
2. Provision(프로비저닝) > Inventory(인벤토리) 페이지에서 하나 이상의 디바이스를 선택하고 Actions(작업) > Inventory(인벤토리) > Edit Device(디바이스 수정) > Credentials(자격 증명) 탭을 선택합니다. 그런 다음 "Add device specific credential(디바이스별 자격 증명 추가)"을 새 사용자 이름 및/또는 비밀번호와 enable 비밀번호로 업데이트합니다. 이 시점에서 Cisco Catalyst Center는 업데이트된 자격 증명을 사용하여 디바이스에 로그인할 수 있으며 디바이스 인벤토리 상태는 Managed(관리됨)로 돌아옵니다.
3. 마지막 단계는 Global Credentials(전역 자격 증명) 페이지에서 동일한 자격 증명을 업데이트

하는 것입니다. 이렇게 하면 새로 검색된 디바이스 또는 LAN Automation을 사용하는 디바이스가 Design(설계) 페이지 > Network Settings(네트워크 설정) > Device Credentials(디바이스 자격 증명) > CLI Credentials(CLI 자격 증명) > edit the username(사용자 이름 수정) > update the user's password(사용자 비밀번호 및 enable 비밀번호 업데이트)에서 업데이트된 자격 증명을 사용하게 됩니다.

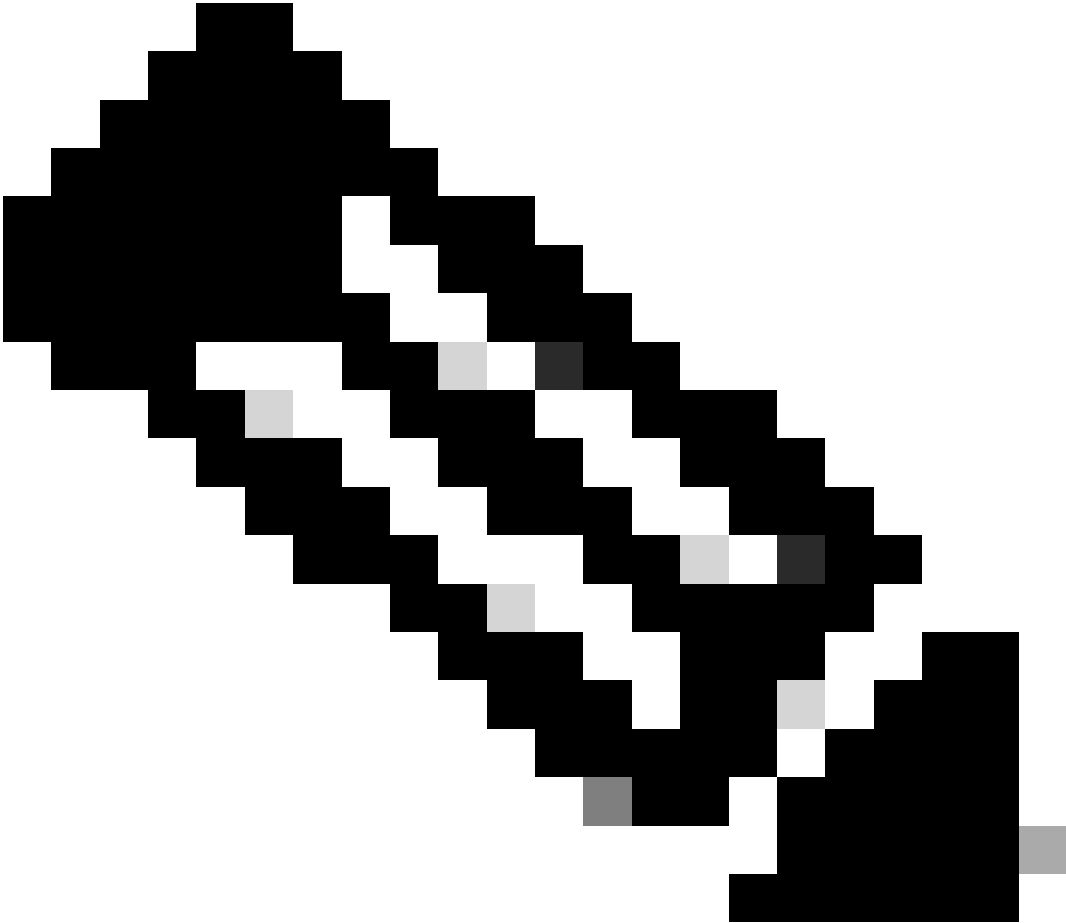
---



참고: 외부 AAA 서버에 연결할 수 있는 경우 사용자 이름과 비밀번호는 외부 AAA 서버에서 인증되고 enable 비밀번호는 관리되는 디바이스에서 로컬로 인증됩니다.

---

---



참고: 외부 AAA 서버가 사이트의 Cisco Catalyst Center 설계 페이지에 구성된 경우, Global Credentials(전역 자격 증명) 페이지에서 자격 증명을 변경하거나 수정할 때 Cisco Catalyst Center에서 디바이스 또는 ISE에 대해 어떤 조치도 취하지 않습니다.

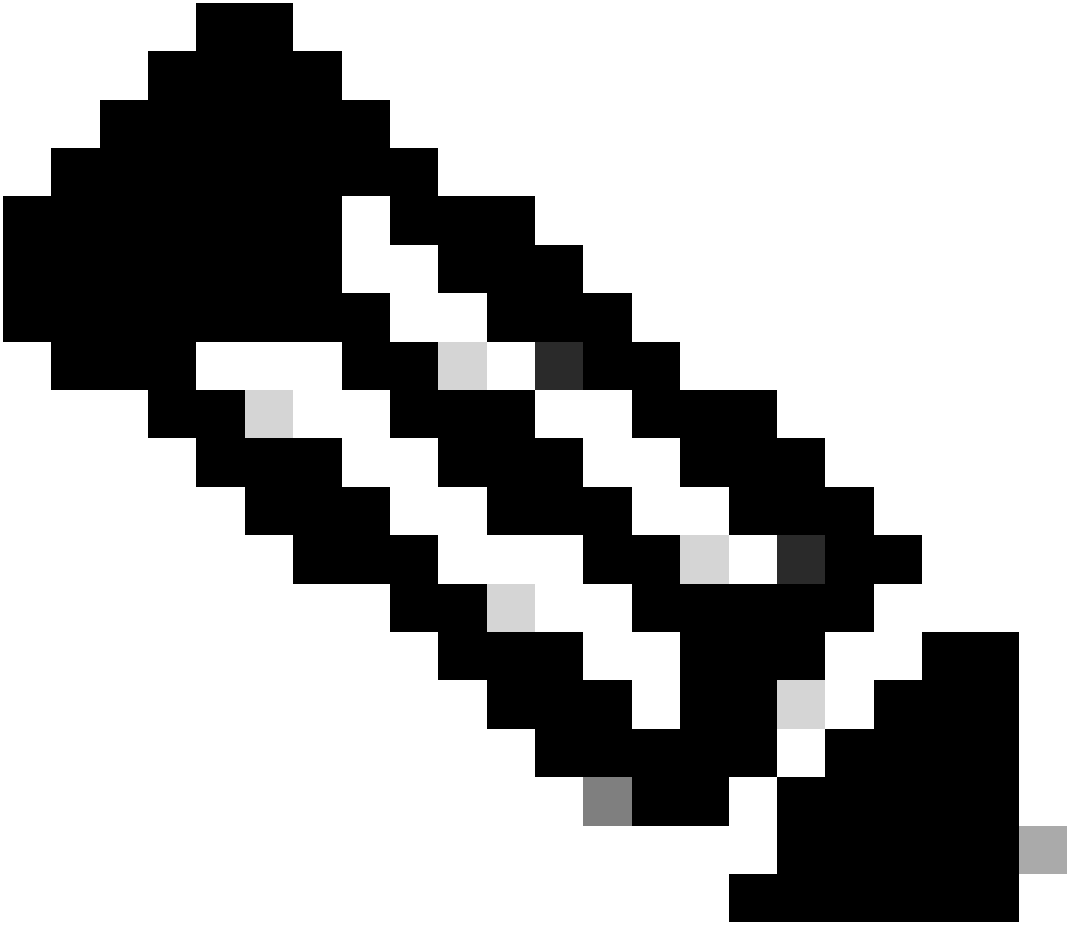
---

## Cisco Catalyst Center Unmanaged AAA가 있는 사이트

사용자의 비밀번호를 변경해야 합니다(enable 비밀번호는 변경하지 않음).

1. Design(설계) > Network Settings(네트워크 설정) > Device Credentials(디바이스 자격 증명) > CLI Credentials(CLI 자격 증명) > edit(편집) > enable password(비밀번호 활성화)를 변경하지 않고 사용자의 비밀번호를 업데이트하여 Global Credentials(전역 자격 증명) 페이지에서 자격 증명을 업데이트합니다.
2. Global Credentials(전역 자격 증명) 페이지에서 자격 증명이 수정되면 Cisco Catalyst Center에서 AAA를 관리하지 않는 사이트의 관리되는 디바이스를 업데이트된 자격 증명으로 다시 구성할 수 있습니다. Cisco Catalyst Center는 임시 EEM 스크립트를 푸시하여 자격 증명을 검증할 수 있습니다. 로그인에 성공하면 컨피그레이션을 유지할 수 있습니다.

---

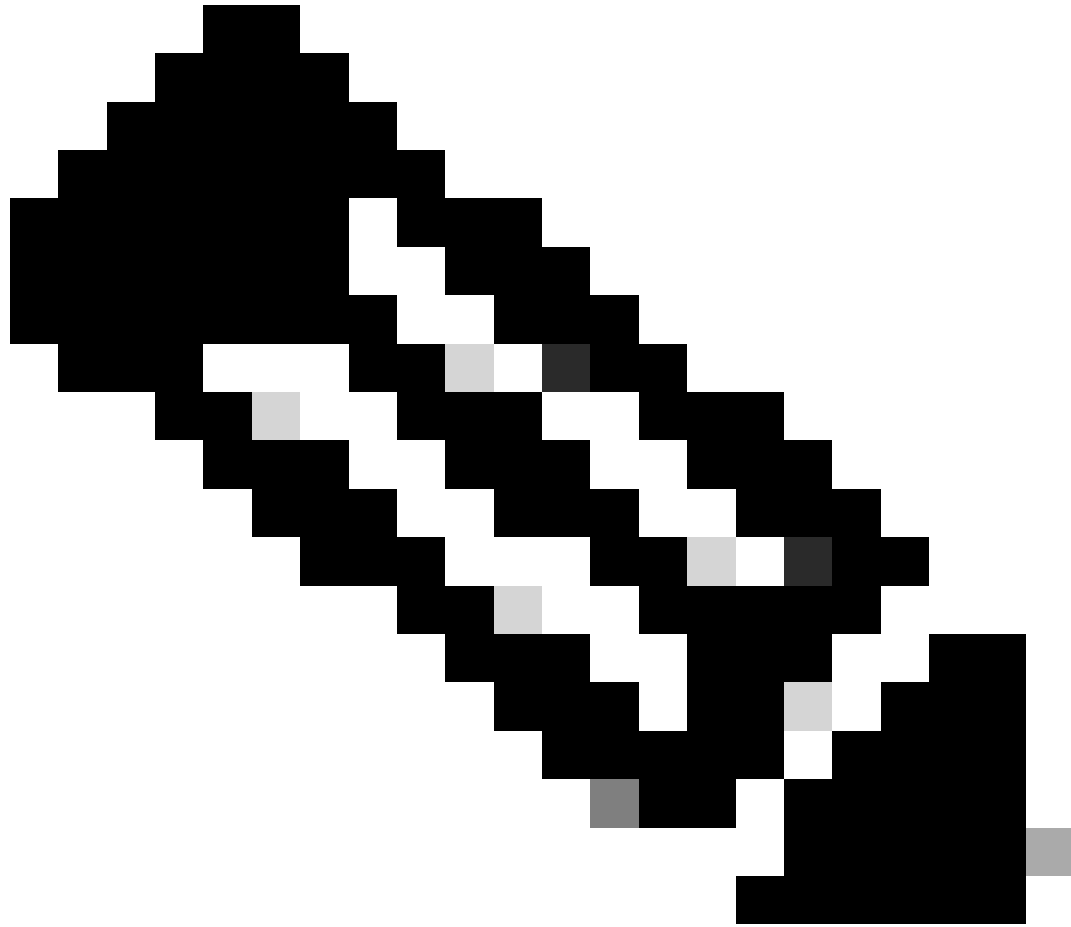


참고: Cisco Catalyst Center에서 AAA 컨피그레이션을 관리하지 않는 사이트의 관리되는 디바이스의 경우, Cisco Catalyst Center는 관리되는 디바이스가 외부 AAA 서버로 수동으로 구성되었는지 여부 또는 관리되는 디바이스가 로컬 자격 증명만 사용하는지 여부에 대한 지식이 없으므로 이러한 단계를 진행하기 전에 영향을 받는 관리되는 디바이스에 비밀번호를 구성한 경우 외부 AAA 서버에서 비밀번호를 업데이트해야 합니다.

---

사용자의 비밀번호 및 enable 비밀번호를 변경해야 합니다.

1. Design(설계) > Network Settings(네트워크 설정) > Device Credentials(디바이스 자격 증명) > CLI Credentials(CLI 자격 증명) > edit(편집) > enable password(비밀번호 활성화)와 함께 사용자의 비밀번호를 업데이트하여 Global Credentials(전역 자격 증명) 페이지에서 자격 증명을 업데이트합니다.
2. Global Credentials(전역 자격 증명) 페이지에서 자격 증명이 수정되면 Cisco Catalyst Center에서 AAA를 관리하지 않는 사이트의 관리되는 디바이스를 업데이트된 자격 증명으로 다시 구성할 수 있습니다. Cisco Catalyst Center는 임시 EEM 스크립트를 푸시하여 자격 증명을 검증할 수 있습니다. 로그인에 성공하면 컨피그레이션을 유지할 수 있습니다.



참고: Cisco Catalyst Center에서 AAA 컨피그레이션을 관리하지 않는 사이트의 관리되는 디바이스의 경우, Cisco Catalyst Center는 관리되는 디바이스가 외부 AAA 서버로 수동으로 구성되었는지 여부 또는 관리되는 디바이스가 로컬 자격 증명만 사용하는지 여부에 대한 지식이 없으므로 이러한 단계를 진행하기 전에 영향을 받는 관리되는 디바이스에 비밀번호를 구성한 경우 외부 AAA 서버에서 비밀번호를 업데이트해야 합니다.

---



이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.