마더보드 교체 후 Intersight에서 독립형 C-Series 서버 구성 및 청구

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[배경 정보](#)
[문제/장애: 새 RMA 서버가 Intersight에서 클레임되지 않고 원래 실패한 서버가 클레임됨](#)
[솔루션](#)
[장치 클레임 문제에 대한 기본 확인](#)
[Cisco Intersight 일반 네트워크 연결 요구 사항](#)
[관련 정보](#)

소개

이 문서에서는 마더보드를 교체한 후 Cisco Intersight에서 독립형 C-Series 서버를 구성하고 요청하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CIMC(Cisco Integrated Management Controller)
- Cisco Intersight
- Cisco C-Series 서버

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco C240-M5 4.1(3d)
- Cisco Intersight SaaS(Software as a Service)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 문서는 다음 하드웨어 및 소프트웨어 버전에서도 사용할 수 있습니다.

- C-Series M4 3.0(4) 이상
- C-Series M5 3.1 이상
- C-Series M6 4.2 이상
- S-Series M5 4.0(4e) 이상

참고: 지원되는 하드웨어 및 소프트웨어의 포괄적인 목록을 보려면 다음 링크를 참조하십시오 . Intersight 지원 PID 및 Intersight 지원 시스템

배경 정보

- 이 문서의 가장 일반적인 사용 사례는 C-Series가 Cisco Intersight에 청구되고 마더보드가 RMA(Return Material Authorization)로 교체된 경우입니다. RMA가 발생할 때마다 원래 서버는 클레임을 취소해야 하며 새 서버는 Cisco Intersight에서 클레임을 받아야 합니다.
- 이 문서에서는 마더보드 RMA 이전에 원래 C-Series 서버가 성공적으로 클레임되었다고 가정하며, 클레임 프로세스 실패로 이어질 구성 또는 네트워크 문제가 없다고 가정합니다.
- Cisco Intersight Portal 또는 엔드포인트의 Device Connector에서 직접 대상의 클레임을 해제할 수 있습니다. Cisco Intersight Portal에서 대상의 클레임을 해제하는 것이 좋습니다.
- 대상이 Intersight 포털이 아닌 장치 커넥터에서 직접 클레임되지 않은 경우 Cisco Intersight 내의 대상이 클레임되지 않은 것으로 표시됩니다. 엔드포인트는 Cisco Intersight에서 수동으로 클레임을 취소해야 합니다.
- 원래 C-Series 서버는 Cisco Intersight에서 상태가 "연결되지 않음"으로 표시될 수 있습니다. 이는 마더보드를 교체해야 하는 이유에 따라 달라질 수 있습니다.

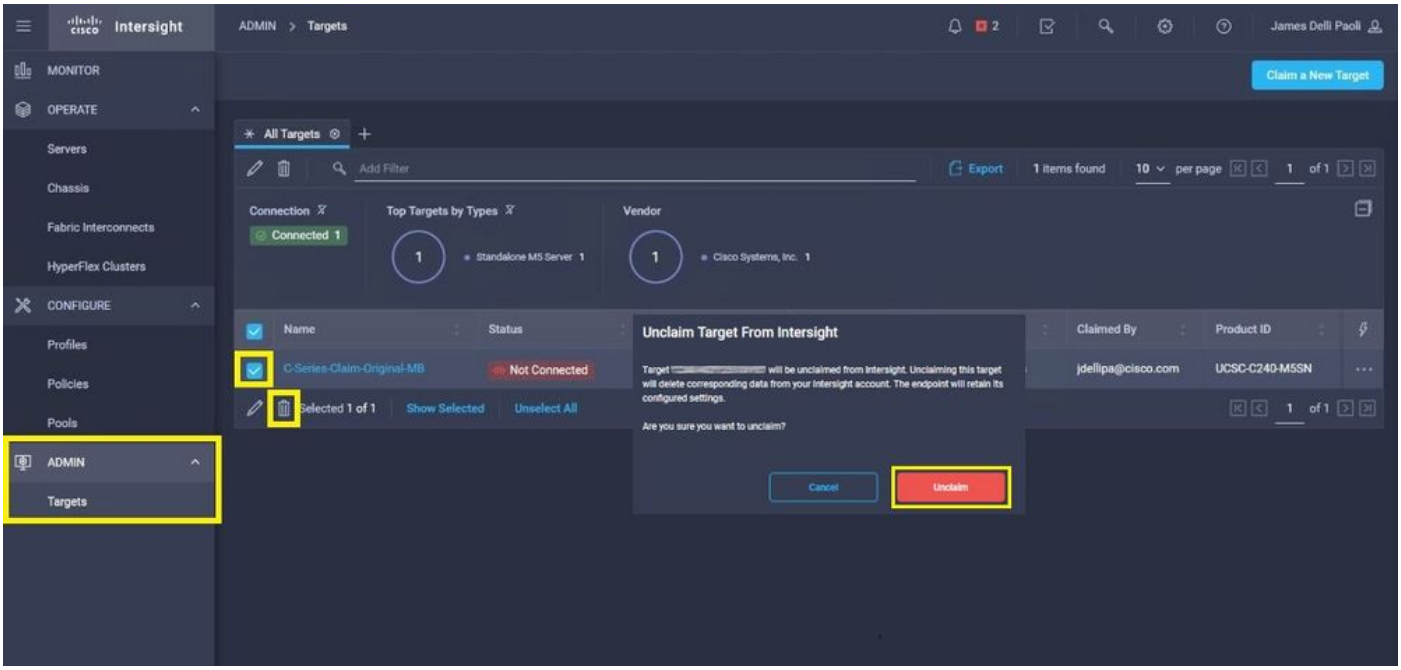
문제/장애: 새 RMA 서버가 Intersight에서 클레임되지 않고 원래 실패한 서버가 클레임됨

독립형 C-Series 서버가 Cisco Intersight에 청구된 경우 서버 일련 번호(SN)는 Cisco Intersight와 쌍을 이룹니다. 클레임된 서버에 장애 또는 기타 이유로 인해 마더보드 교체가 필요한 경우 원래 서버의 클레임을 취소하고 새 서버를 Cisco Intersight에서 클레임해야 합니다. C-Series SN이 마더보드 RMA에 따라 변경됩니다.

솔루션

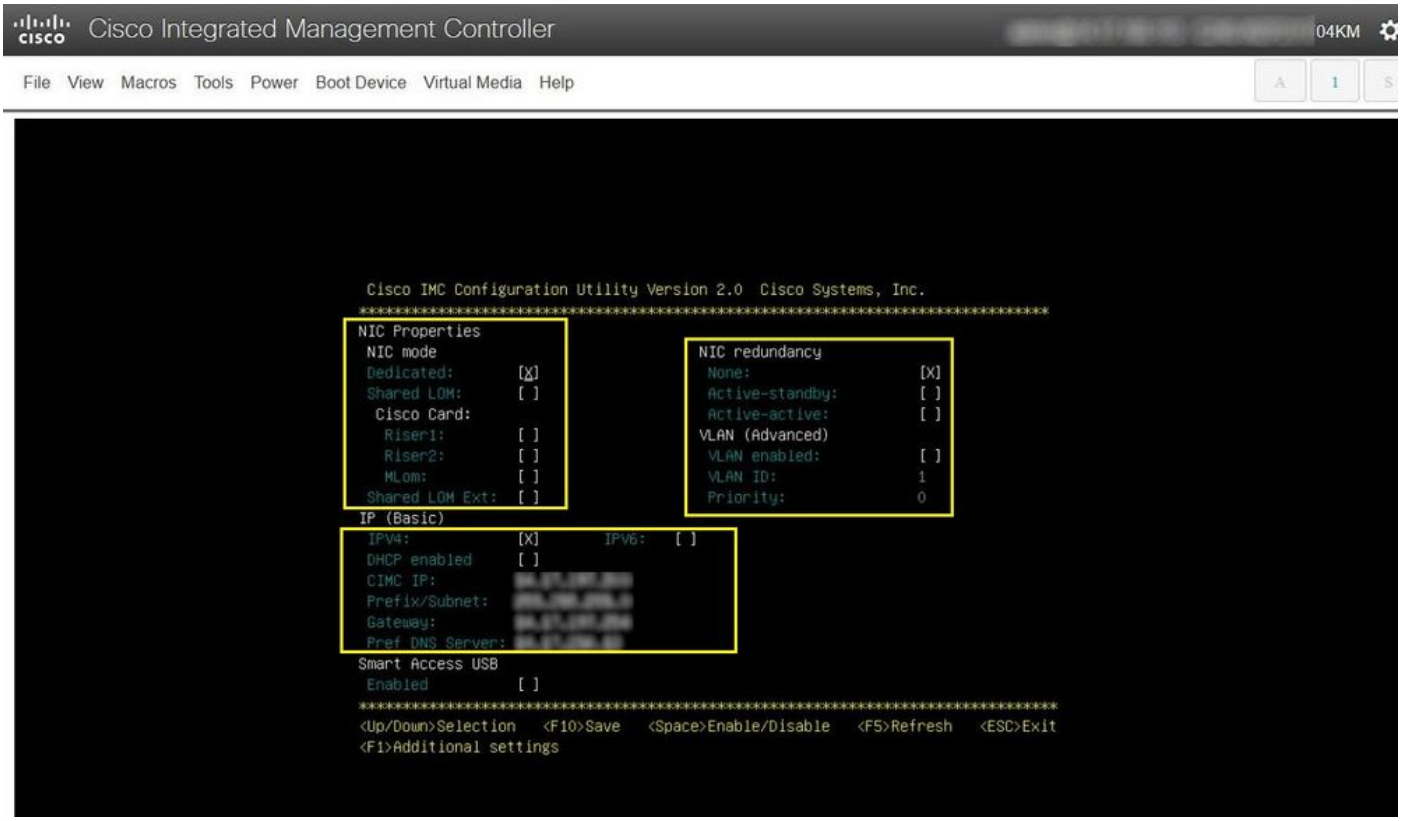
교체가 필요한 Cisco Intersight에서 C-Series 서버의 클레임을 해제합니다. 새 서버 CIMC 및 디바이스 커넥터를 구성하고 Cisco Intersight에 새 서버를 요청합니다.

1단계. Cisco Intersight를 시작하고 **Admin > Targets**. 교체 및 클레임되지 않을 대상의 상자를 선택하고 **Trash Can Icon > Unclaim** 이 그림에 표시된 것과 같습니다.



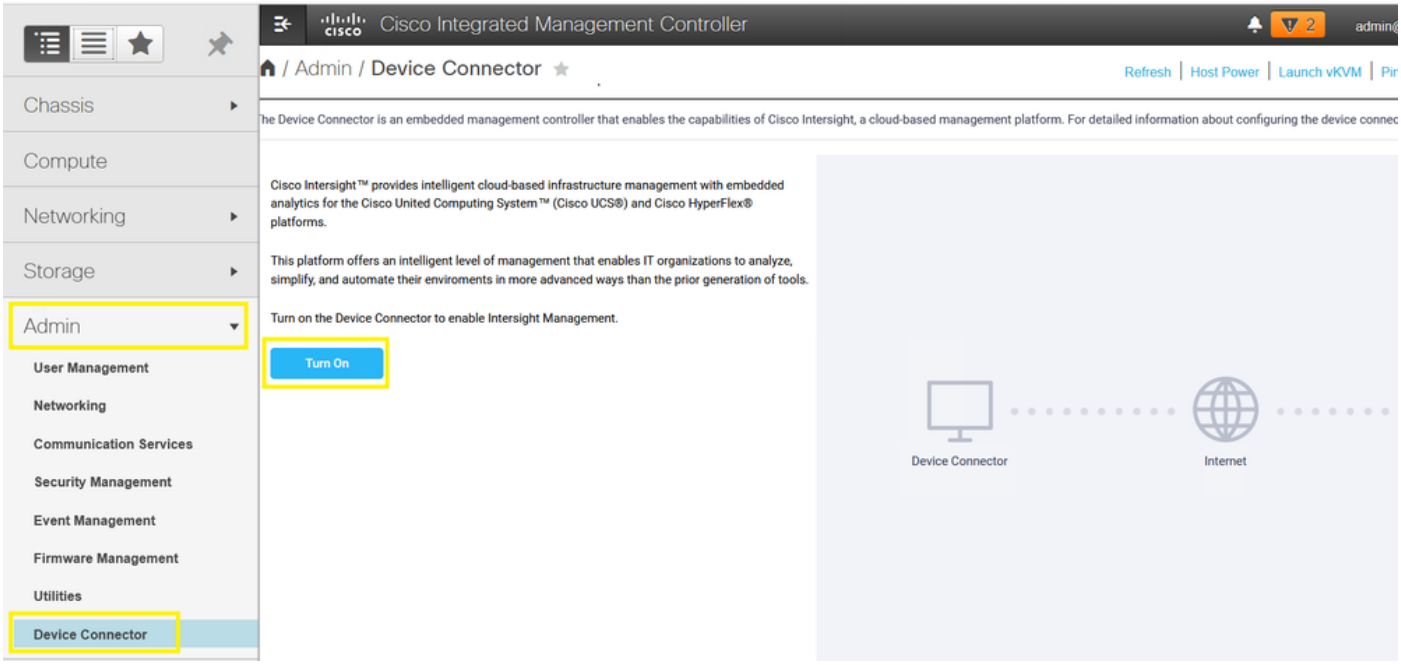
2단계. 새로 교체된 서버에 KVM(Keyboard Video Monitor)을 연결합니다(CIMC가 이미 구성된 경우 이 단계를 건너뛰십시오). Cisco 시작 화면의 부팅 화면에서 **F8** CIMC를 구성합니다. 적절한 구성 **Network Interface Card (NIC) Properties** 해당 환경에 대해 **F10** 수신 **Save.** 서버 및 연결된 디바이스에 물리적 케이블을 **NIC Properties** 관리에 사용됩니다.

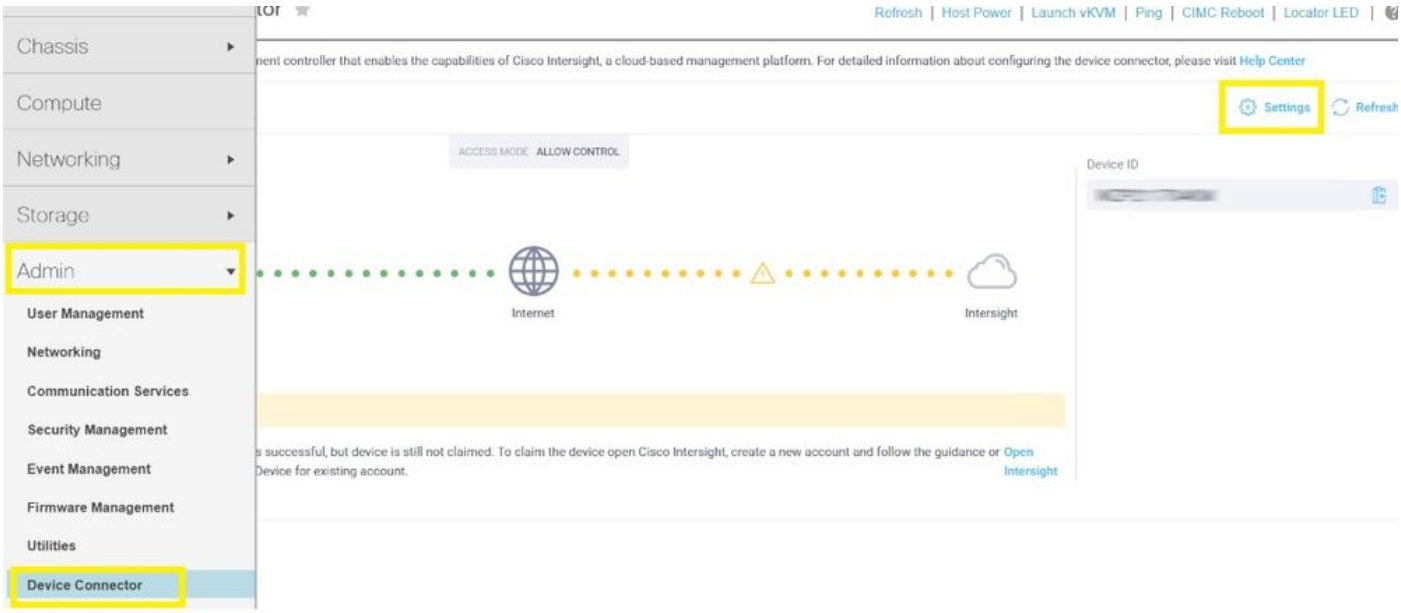
> **참고:** 2단계. C240-M5에 직접 연결된 KVM을 사용하여 CIMC를 로컬로 설정하는 방법을 설명하고 있습니다. 초기 CIMC 설정은 DHCP를 사용하여 원격으로 수행할 수도 있습니다. 사용 중인 서버 모델에 맞는 설치 가이드를 참조하여 가장 적합한 초기 CIMC 설정을 선택하십시오 .



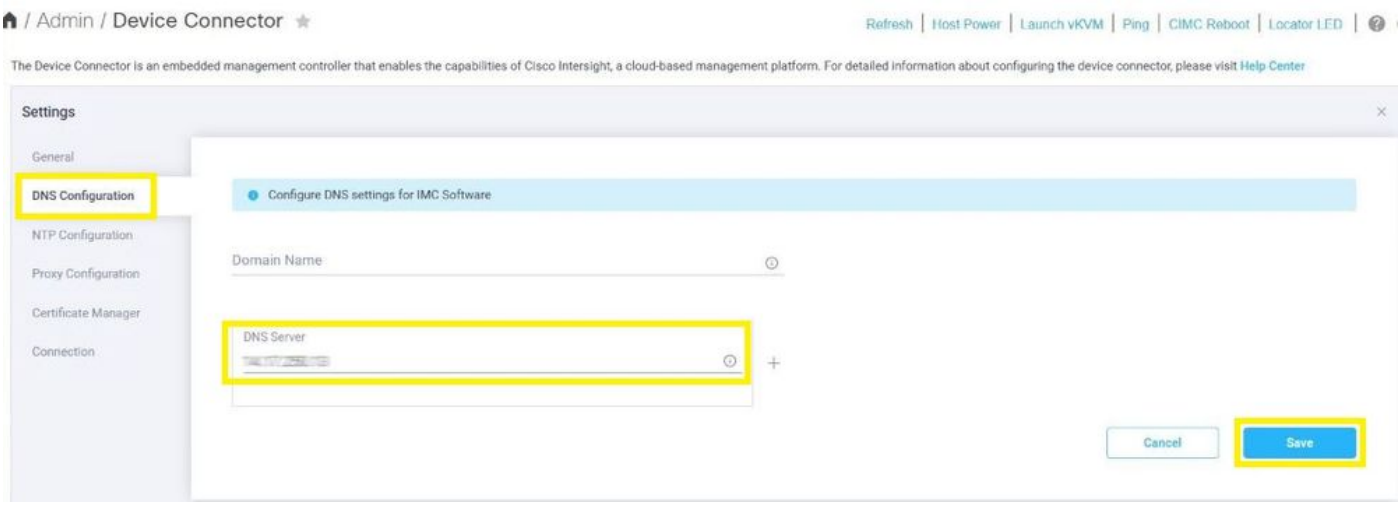
3단계. CIMC GUI를 시작하고 **Admin > Device Connector.** 경우 **Device Connector** 비활성화되어 있습니다. **Turn On.** 활성화된 후에는 **Settings.**

팁: CIMC GUI에서 **Chassis > Summary** Cisco의 **Firmware Version** Cisco Intersight에서 요청할 수 있는 최소 펌웨어 요구 사항을 충족하는지 확인합니다. 이 링크를 사용하여 특정 서버 모델에 대한 최소 요구 사항(Intersight Supported Systems)을 확인합니다. 펌웨어가 청구할 최소 요구 사항을 충족하지 않으면 서버에서 HUU(Host Upgrade Utility)를 실행하십시오. 자세한 내용은 다음을 참조하십시오. Cisco 호스트 업그레이드 유틸리티 프로세스.

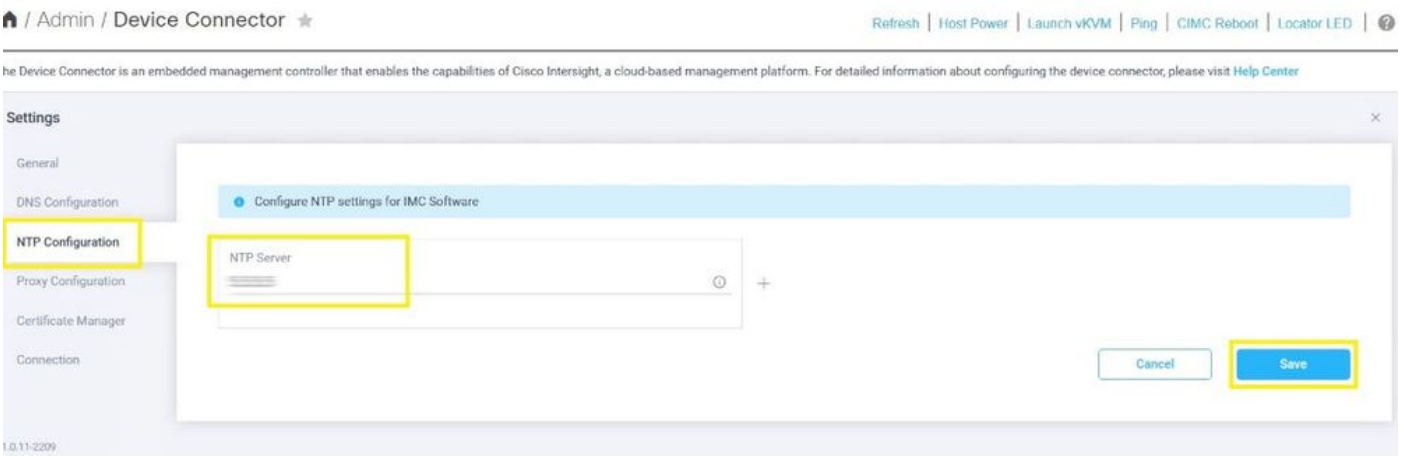




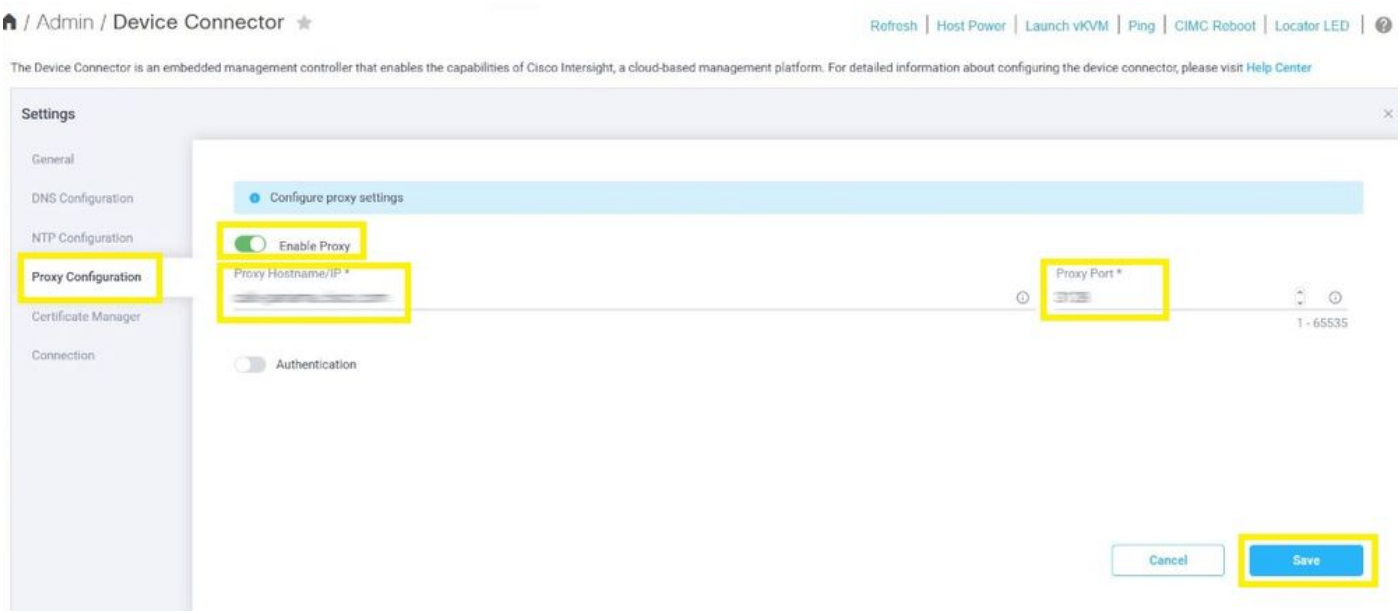
3.1단계. **Admin > Device Connector > Settings > DNS Configuration** 적절한 **DNS Server** 및 **Save** 이 그림에 표시된 것과 같습니다.



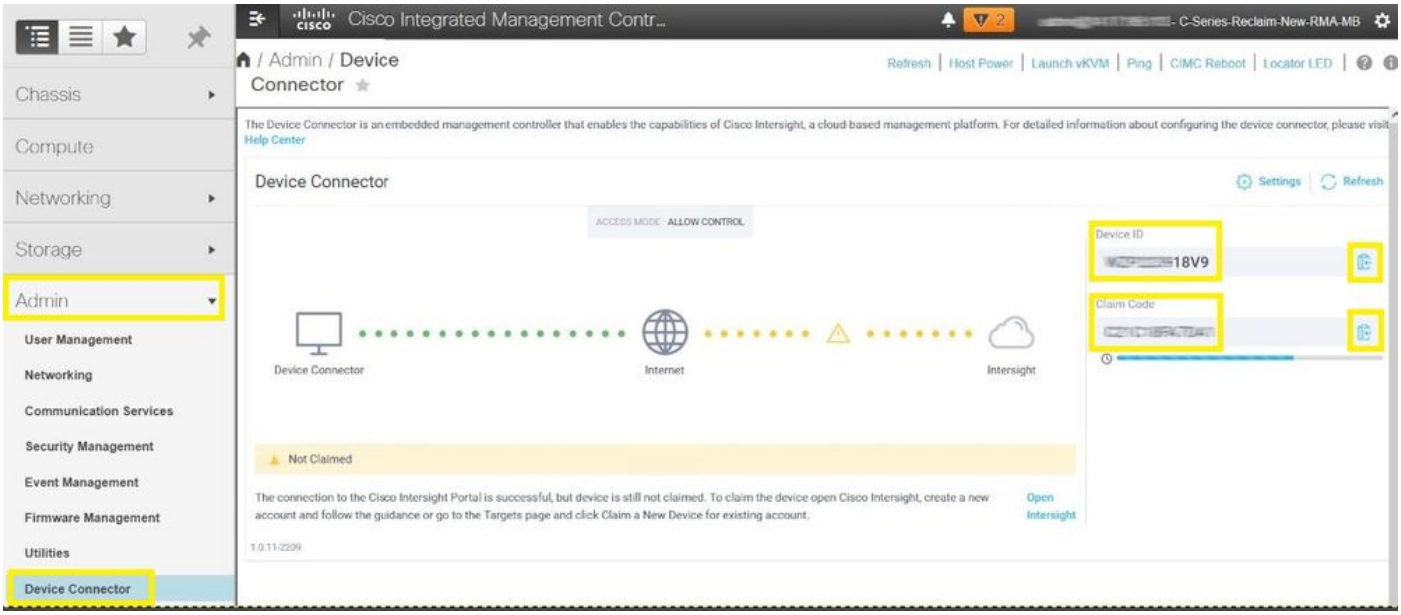
3.2단계. **Admin > Device Connector > Settings > NTP Configuration.** 구성 **NTP Server** 환경에 따라 주소를 지정하고 **Save** 이 그림에 표시된 것과 같습니다.



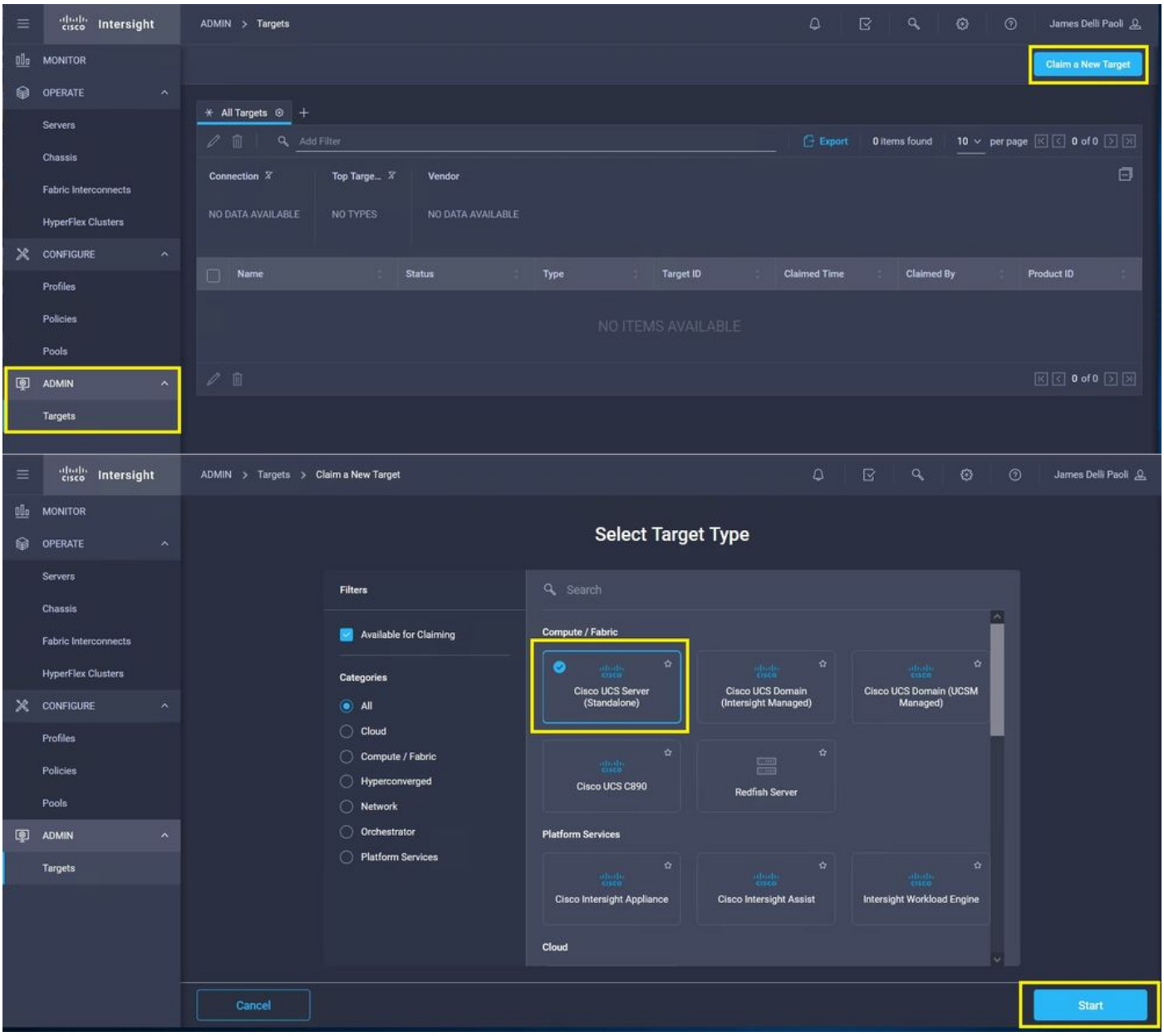
3.3단계. 필요한 경우 Cisco Intersight에 연결하기 위해 프록시를 구성할 수 있습니다. 탐색 **Admin > Device Connector > Settings > Proxy Configuration > Enable Proxy.** 구성 **Proxy Hostname/IP** 및 **Proxy Port** 및 **Save.**

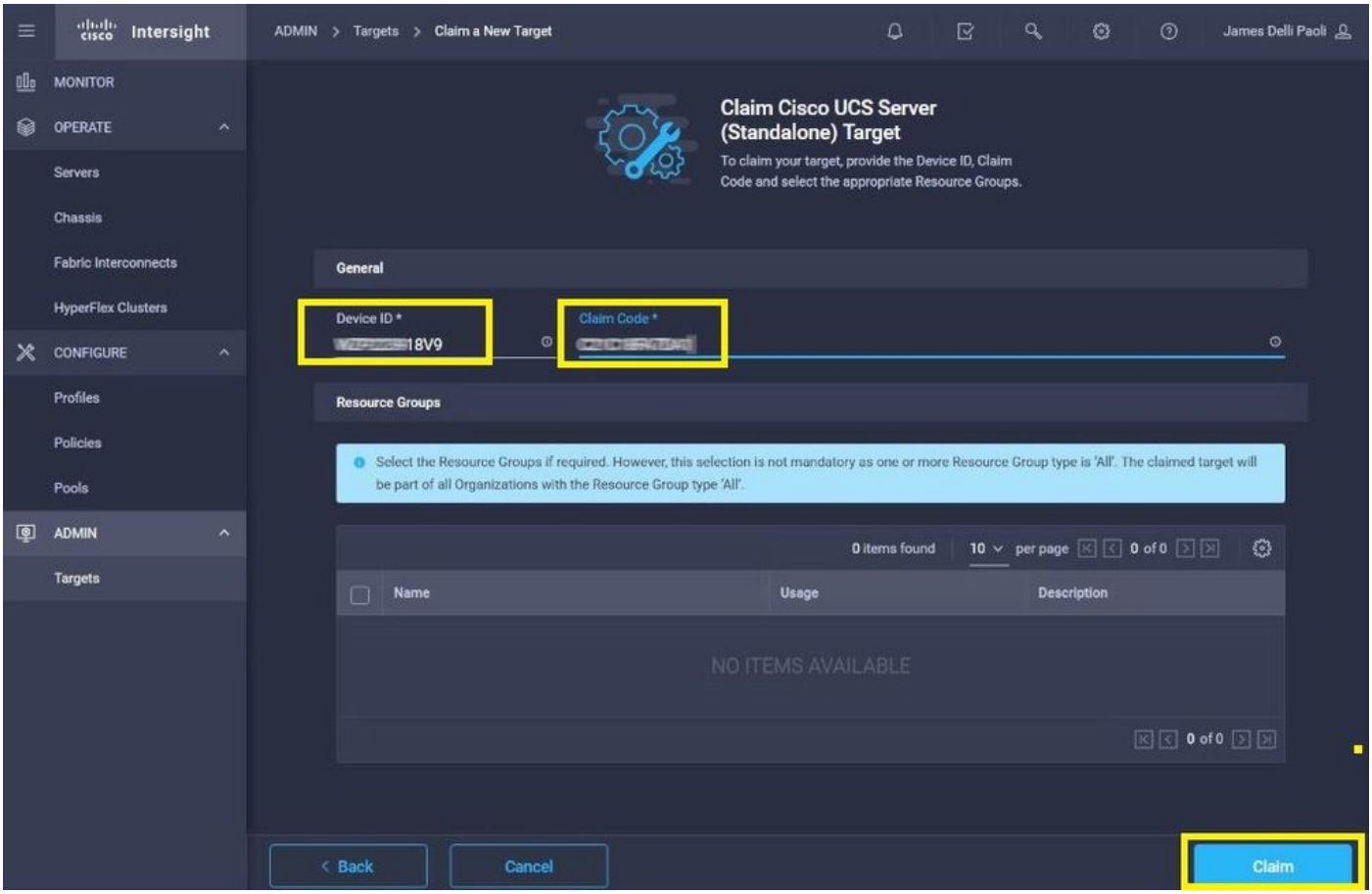


4단계. 선택 **Admin > Device Connector** 및 **Device ID** 및 **Claim Code.** 나중에 사용할 수 있도록 둘 다 메모장이나 텍스트 파일에 복사합니다.

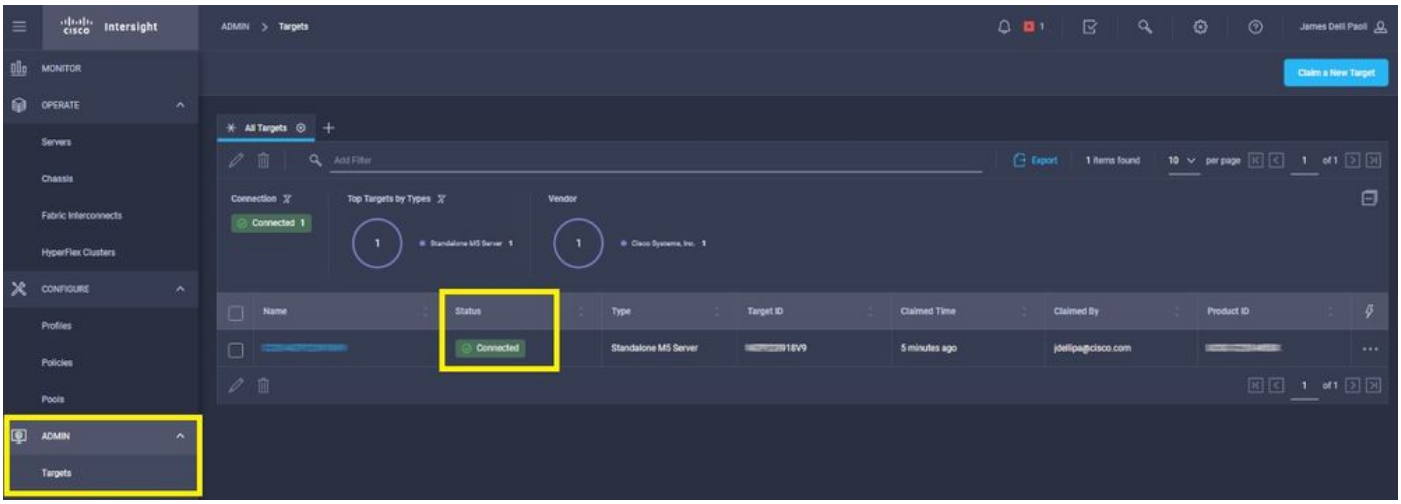


5단계. Cisco Intersight를 시작하고 **Admin > Targets > Claim a New Target > Cisco UCS Server (Standalone) > Start.** 다음을 입력합니다. **Device ID** 및 **Claim Code** CIMC GUI에서 복사한 다음 **Claim.**





6단계. **Admin > Targets.** 클레임에 성공하면 **Status > Connected,** 이 그림에 표시된 것과 같습니다.



장치 클레임 문제에 대한 기본 확인

참고: 오류 조건 및 교정의 포괄적인 목록은 Device Connector Error Conditions and Remediation Steps 링크를 참조하십시오.

장치 커넥터 연결 상태 설명	장치 커넥터 연결 상태 설명	가능한 교정
클레임됨	Cisco Intersight 플랫폼과의 연결에 성공했으며 연결을 요청했습니다.	해당 없음
클레임되지 않음	Cisco Intersight 플랫폼과의 연결에 성공했지만 아직 엔드포인트를 클레임하지 못했습니다.	Cisco Intersight를 통해 클레임 않은 연결을 청구할 수 있습니

관리상 사용 안 함	엔드포인트에서 Intersight 관리/디바이스 커넥터가 비활성화되었음을 나타냅니다.	엔드포인트에서 디바이스 커넥 활성화합니다.
DNS 잘못 구성됨	DNS가 CIMC에서 잘못 구성되었거나 전혀 구성되지 않았습니다.	시스템에 구성된 DNS 이름 서 연결할 수 없음을 나타냅니다. 이름 서버에 유효한 IP 주소를 했는지 확인하십시오.
Intersight DNS 확인 오류	DNS가 구성되었지만 Intersight의 DNS 이름을 확인할 수 없습니다.	Intersight에서 유지 관리 작업을 행 중인지 확인하려면 다음 링크 확인하십시오. Intersight 상태. Intersight가 작동 중이면 Intersi 서비스의 DNS 이름이 확인되지 았을 가능성이 있습니다.
UCS 연결 네트워크 오류	잘못된 네트워크 컨피그레이션을 나타냅니다.	확인 및 확인: MTU는 엔드 투 엔 서 올바르며 포트 443 및 80이 되며 방화벽은 엔드포인트에서 된 모든 물리적 및 가상 IP, DNS NTP를 허용합니다. 만료되었거나 유효한 인증서가 니다. NTP가 올바르게 구성되어 고 디바이스 시간이 Coordinate Universal Time과 동기화되어 있 지 확인합니다. DNS가 올바르게 성되었는지 확인합니다. 투명 웹 록시가 사용 중인 경우 인증서가 료되지 않았는지 확인합니다.
인증서 검증 오류	Cisco Intersight 플랫폼에서 제공한 인증서가 유효하지 않기 때문에 엔드포인트가 Cisco Intersight 플랫폼과의 연결 설정을 거부합니다.	웹 서버에서 제공한 인증서 이름 Intersight 서비스의 DNS 이름과 치하지 않습니다. DNS가 올바르 구성되었는지 확인합니다. 웹 프 관리자에게 문의하여 투명 웹 프 가 올바르게 구성되었는지 확인 시오. 특히 웹 프록시에서 제공 인증서의 이름은 Intersight 서비 DNS 이름(svc.intersight.com)과 치해야 합니다. 신뢰할 수 없는 CA(인증 기관)에 인증서를 발급했습니다. DNS가 바르게 구성되었는지 확인합니 명 웹 프록시가 올바르게 구성되 지 확인하려면 웹 관리자 또는 infosec에 문의하십시오. 특히 웹 록시에서 제공하는 인증서의 이 Intersight 서비스의 DNS 이름과 치해야 합니다.

Cisco Intersight 일반 네트워크 연결 요구 사항

- 엔드포인트의 디바이스 커넥터에서 Intersight 플랫폼에 대한 네트워크 연결이 설정됩니다
- 관리 대상과 Intersight 사이에 방화벽이 도입되었는지 또는 현재 방화벽에 대한 규칙이 변경되었는지 확인합니다. 따라서 엔드포인트와 Cisco Intersight 간에 엔드 투 엔드 연결 문제가 발생할 수 있습니다. 규칙이 변경된 경우, 변경된 규칙이 방화벽을 통과하는 트래픽을 허용하는지

확인합니다.

- HTTP 프록시를 사용하여 프레미스 외부로 트래픽을 라우팅하는 경우, HTTP 프록시 서버 컨피그레이션을 변경한 경우 디바이스 커넥터 컨피그레이션이 변경 사항을 반영하도록 변경해야 합니다. 이는 Intersight에서 HTTP 프록시 서버를 자동으로 탐지하지 않기 때문에 필요합니다.
- DNS를 구성하고 DNS 이름을 확인합니다. 장치 커넥터는 DNS 서버에 DNS 요청을 보내고 DNS 레코드를 확인할 수 있어야 합니다. 장치 커넥터는 svc.intersight.com을 IP 주소로 확인할 수 있어야 합니다.
- NTP를 구성하고 디바이스 시간이 시간 서버와 올바르게 동기화되었는지 확인합니다.

참고: Intersight 연결 요구 사항의 포괄적인 목록은 Intersight Network 연결 요구 사항을 참조하십시오.

관련 정보

- Cisco Intersight 시작하기 클레임 대상
- Cisco Intersight SaaS 지원 시스템
- Cisco Intersight SaaS 지원 PID
- Cisco Intersight Network 연결 요구 사항
- Cisco Intersight 교육 비디오
- Cisco 버그 ID CSCvw76806 - 독립형 C-Series 서버는 디바이스 커넥터 버전이 1.0.9 미만인 경우 Cisco Intersight에서 성공적으로 클레임하지 못할 수 있습니다.
- 기술 지원 및 문서 – Cisco Systems

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.